

Wolfgang Riggert

Rechnernetze

Grundlagen – Ethernet – Internet



4., aktualisierte und erweiterte Auflage



HANSER

Wolfgang Riggert

Rechnernetze

Grundlagen – Ethernet – Internet

4., aktualisierte und erweiterte Auflage

Mit 83 Bildern, 61 Beispielen und 120 Fragen zur Wissensüberprüfung



Fachbuchverlag Leipzig
im Carl Hanser Verlag

Wolfgang Riggert ist Professor für Netzwerke und Informationsmanagement an der Fachhochschule Flensburg. Er ist Autor zahlreicher Beiträge zu Netzwerkthemen und Bücher. Vor seiner Lehrtätigkeit war er sechs Jahre als Softwareentwickler bei Norsk Data tätig.

Alle in diesem Buch enthaltenen Programme, Verfahren und elektronischen Schaltungen wurden nach bestem Wissen erstellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund ist das im vorliegenden Buch enthaltene Programm-Material mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor und Verlag übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN: 978-3-446-43164-5

E-Book-ISBN: 978-3-446-43386-1

Dieses Werk ist urheberrechtlich geschützt.

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Buches, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren), auch nicht für Zwecke der Unterrichtsgestaltung – mit Ausnahme der in den §§ 53, 54 URG genannten Sonderfälle –, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© 2012 Carl Hanser Verlag München

Internet: <http://www.hanser-fachbuch.de>

Lektorat: Dr. Martin Feuchte

Herstellung: Dipl.-Ing. Franziska Kaufmann

Satz: Kösel, Krugzell

Coverconcept: Marc Müller-Bremer, www.rebranding.de, München

Coverrealisierung: Stephan Rönigk

Druck und Bindung: Friedrich Pustet KG, Regensburg

Printed in Germany

Vorwort

Längst sind Netzwerke zu einem festen Bestandteil des täglichen Lebens geworden. Verfügbarkeit und Bandbreite bilden wichtige Standortfaktoren für die Ansiedlungspolitik von Unternehmen. Diesem Aspekt wird auch auf politischer Ebene Rechnung getragen, indem immer wieder der Ausbau der Netzinfrastruktur in Richtung Breitbandnetz gefordert wird. Neben Energienetzen reifen Datennetze für die Kommunikation damit zu einem bedeutenden versorgungstechnischen Faktor heran.

Vor diesem Hintergrund wird ein Basiswissen über technologische Hintergründe und zukünftige Entwicklungen für Studierende informatikbezogener Studiengänge unerlässlich. Um die Rahmenbedingungen vieler Hochschulen oder studienbegleitender Einrichtungen entgegen zu kommen, ist das Buch in 12 Kapitel gegliedert. Diese Kapitel spiegeln Semesterwochen wider und sollen ein Grundgerüst für eine inhaltliche Strukturierung liefern. Weitere ergänzende Materialien stehen unter dem Link:

<http://www.rechnernetze-interaktiv.de>

bereit. Hier finden sich:

- Zwei Videos zu Migrationsszenarien auf neue Technologien
- Ein umfangreiches E-Learning-Modul zur Netzwerkthematik unter Berücksichtigung des Betriebssystems Windows 7
- Die Lösungen zu den Wissensüberprüfungen des Buches
- Ein Glossar
- Eine Sammlung hilfreicher Links gegliedert nach den einzelnen Themen.

Mehrere hilfreiche Hände haben die Erstellung des Buches und der Online-Präsenz ermöglicht. Besonders danken möchte ich Frau Monika Tinzmann, und den Herrn Hans-Peter Schmidt und Jörg Fischer für Korrektur und Anregungen zum Manuskript und den Bildern, sowie den Herrn Björn Gersmann und Jörn Fischer für die Realisierung des Internetauftritts.

Flensburg, im Juni 2012

Wolfgang Riggert

Inhalt

1	Netzwerkgrundlagen und -architektur	13
1.1	Basiselemente eines Netzes .	15
1.2	Netzwerkkategorien .	17
1.3	Netzzugang und Pakettransport .	20
1.4	ISO/OSI-Referenzmodell .	26
1.5	Zusammenfassung .	33
1.6	Wissensüberprüfung .	34
2	Übertragungsmethoden und -medien	35
2.1	Übertragungsverfahren .	36
2.2	Strukturierte Verkabelung .	40
2.3	Glasfaserverkabelung .	43
2.3.1	Historie .	44
2.3.2	Kabelaufbau .	44
2.3.3	Arbeitsweise .	45
2.3.4	Eingesetzte Technik .	45
2.3.5	Qualitätsparameter .	47
2.3.6	Glasfaserprofile .	49
2.3.7	Glasfaserkabelarten .	51
2.3.8	Steckverbindungen .	52
2.3.9	Bewertung .	53
2.4	Twisted-Pair-Verkabelung .	54
2.4.1	Qualitätsparameter .	55
2.4.2	EIA/TIA-568-Standard .	58
2.4.3	ISO/IEC-Standard 11801 und EN 50173 .	59
2.4.4	Bewertung .	62
2.5	Zusammenfassung .	63
2.6	Wissensüberprüfung .	64
3	Ethernet-Technologie	65
3.1	Historie .	65
3.2	Paketaufbau .	69
3.3	Zugriffsverfahren: CSMA/CD .	73
3.4	Signalverlauf .	78
3.5	Standards .	80

3.6	Fehlerquellen .	86
3.7	Verfahrensbewertung .	87
3.8	Zusammenfassung .	87
3.9	Wissensüberprüfung .	88

4 Ethernet-Standards 89

4.1	Die Gegenwart: Fast-Ethernet .	89
4.1.1	Vorteile .	90
4.1.2	Bestandteile .	91
4.1.3	Varianten .	92
4.1.4	Auto-Negotiations-Technologie .	94
4.1.5	Topologie .	95
4.1.6	Migration von Standard- zu Fast-Ethernet .	96
4.2	Der Trend: Gigabit-Ethernet .	97
4.2.1	Physikalische Grundlagen .	98
4.2.2	Varianten .	99
4.2.3	Besonderheiten .	102
4.3	Die Zukunft: 10-GbE .	103
4.3.1	Eigenschaften .	103
4.3.2	Vorteile .	106
4.4	Technologische Trends .	108
4.5	Zusammenfassung .	111
4.6	Wissensüberprüfung .	111

5 IP-Protokollfamilie 113

5.1	IP Internet Protocol .	114
5.1.1	Fragmentierung .	119
5.1.2	Routing-Optionen .	120
5.1.3	Routing .	121
5.2	Address Resolution Protocol ARP .	123
5.3	Reverse Address Resolution Protocol RARP .	126
5.4	Internet Control Message Protocol ICMP .	127
5.5	Zusammenfassung .	130
5.6	Wissensüberprüfung .	130

6 IP-Adressierung 131

6.1	IP-Adressstruktur .	132
6.1.1	Class-A-Adressen .	134
6.1.2	Class-B-Adressen .	134
6.1.3	Class-C-Adressen .	134
6.1.4	Adressinterpretation .	134
6.1.5	Internetadressen mit besonderer Bedeutung .	136
6.2	Subnetzbildung .	137
6.3	Variabellange Subnetzmasken VLSM .	141

6.3.1	Grenzen der Subnetzbildung .	142
6.3.2	VLSM-Voraussetzungen .	142
6.4	Private Adressvergabe oder Network Address Translation NAT .	145
6.5	Classless-Inter-Domain-Routing CIDR .	146
6.6	Verwaltungsfunktionen auf IP-Basis .	148
6.7	Zusammenfassung .	149
6.8	Wissensüberprüfung .	150

7 TCP-Protokoll 151

7.1	Transmission Control Protocol im Detail .	151
7.1.1	Besonderheiten .	152
7.1.2	Merkmale .	153
7.1.3	Verbindungsmanagement .	155
7.1.4	Fehlervermeidungsmechanismen .	157
7.1.5	User Datagram Protocol UDP .	159
7.2	Zusammenfassung .	161
7.3	Wissensüberprüfung .	161

8 IPv6 162

8.1	Historie .	163
8.2	Entwurfsziele .	163
8.3	Technische Betrachtung .	165
8.4	Die wichtigsten Merkmale .	166
8.4.1	IPv6-Header .	166
8.4.2	IPv6-Headererweiterungen .	168
8.4.3	IPv6-Adressformat .	172
8.4.4	Adressmanagement .	175
8.4.5	Begleitprotokolle .	176
8.5	Migrationswege .	178
8.5.1	Tunneling .	178
8.5.2	Dual-IP-Stack .	179
8.6	Mobile IPv6 .	180
8.6.1	Kommunikationsablauf .	180
8.6.2	Technischer Hintergrund .	181
8.7	Zusammenfassung .	183
8.8	Wissensüberprüfung .	185

9 Layer-2 – Geräte, Protokolle und Konzepte 186

9.1	Switches .	187
9.1.1	Eigenschaften .	187
9.1.2	Arbeitsweise .	189
9.1.3	Switchingverfahren .	190
9.1.4	Erweiterungsmöglichkeiten .	193

9.1.6	Switch-Architekturen .	194
9.2	Spanning-Tree .	196
9.3	Virtuelle LANs .	201
9.3.1	VLAN-Typen .	202
9.3.2	Trunking .	203
9.3.3	VLAN-Management .	204
9.4	Zusammenfassung .	205
9.5	Wissensüberprüfung .	205

10 Layer 3 – Geräte, Protokolle und Konzepte 207

10.1	Router .	207
10.1.1	Bedeutung .	208
10.1.2	Routing-Ablauf .	210
10.1.3	Routing-Methoden .	212
10.1.4	Unterschiede zwischen Routern und Switches .	214
10.2	Routing .	216
10.2.1	Bedeutung .	216
10.2.2	Routingprotokolle – allgemeine Klassifizierung .	217
10.3	Routingprotokolle .	221
10.3.1	Routing Information Protocol RIP .	221
10.3.2	Open Shortest Path First OSPF .	224
10.4	Routingprobleme .	226
10.5	Einsatzaspekte von Switches und Routern .	228
10.6	Zusammenfassung .	229
10.7	Wissensüberprüfung .	230

11 Verwaltung von Netzwerken 231

11.1	Netzwerkmanagement .	232
11.1.1	Netzwerkstatistiken .	233
11.1.2	OSI-Modell .	235
11.1.3	SNMP .	237
11.1.4	MIB .	239
11.1.5	SMI-Definition .	241
11.1.6	syslogd .	242
11.2	Netzwerksicherheit .	243
11.2.1	Allgemeine Bedrohungen .	243
11.2.2	Sicherheit für Switches und Router .	245
11.3	Zusammenfassung .	248
11.4	Wissensüberprüfung .	249

12 Wireless LAN 250

12.1	IEEE-802.11-Standards .	251
12.2	Wireless-Architekturen .	254
12.3	Kodierungsverfahren und Kanäle .	255

12.4	Zugriffsmethoden: CSMA/CA .	257
12.4.1	Besonderheiten .	259
12.4.2	Anmeldeverfahren .	260
12.5	Rahmentypen .	261
12.6	Sicherheit .	264
12.7	Bewertung .	267
12.8	Zusammenfassung .	270
12.9	Wissensüberprüfung .	270

Literatur .	271
--------------------	------------

Index .	274
----------------	------------

1

Netzwerkgrundlagen und -architektur

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Wie sind Netzwerke hinsichtlich ihrer Topologie aufgebaut?
- Aus welchen Basiskomponenten bestehen Netzwerke?
- Wie ist der Netzzugang geregelt?
- Was sind die Vorteile eines Schichtenmodells?
- Welche Funktionalität ist auf welcher Ebene des Schichtenmodells angesiedelt?

Kapiteleinführung

Netzwerke schlagen ein neues Kapitel in der Informationsverarbeitung auf. In vielen Unternehmen bilden sie heute das Rückgrat der Informationsinfrastruktur. Angefangen von Netzwerken, die nur fünf Rechner verbinden, reicht das Spektrum moderner Lösungen bis zu weltweiten Verbünden, in denen viele Rechnerwelten eine integrative Einheit mit größtmöglicher Produktivität bilden. Triebfeder für die fortschreitende Vernetzung, insbesondere im Weitverkehrsbereich, ist das Internet. Als leistungsfähige Werbeplattform und Vertriebskanal für viele Arten von Produkten und Dienstleistungen überwindet es traditionelle Marktgrenzen mit Geschäftsmodellen wie dem E-Commerce. Im Gefolge dieses Booms werden leistungsfähige Netzwerke, die eine Vielzahl von Nutzern mit akzeptablen Antwortzeiten bedienen, eine notwendige Voraussetzung.

Im Vordergrund für den Betrieb und den Ausbau von Netzwerken stehen drei Anforderungen:

- Die Geschwindigkeit muss für die Partner des Datenaustausches zufriedenstellend ausfallen, ohne dass große Schwankungen in der Antwortzeit, selbst zu Spitzenlastzeiten, auftreten.
- Das Management der Netzkomponenten und der Endstationen muss einfach sein.
- Die Kosten des Betriebes müssen in vertretbarem Rahmen liegen.

Getrost der Prämisse „*Nichts ist so beständig wie der Wandel*“ fällt es zunehmend schwerer, Leitlinien für eine zukunftssichere Netzplanung aufzustellen. In einer Welt, in der sich die Innovationszyklen ständig verkürzen, Produkte innerhalb eines Quartals veralten und das

Internet alle Geschäftsbereiche umwälzt, bleiben auch die Netzwerktechnologie und ihre Prinzipien kaum ausgespart. Dennoch lassen sich einige Trends erkennen:

- Zukünftige Anwendungen verlangen die Übertragung großer Datenmengen. Dazu zählen die 3D-Visualisierung komplexer Objekte oder die Herstellung farbiger Broschüren hoher Qualität, die direkt digitalen Druckmaschinen zugestellt werden. Aber auch die Übermittlung von Röntgenbildern hoher Auflösung zwischen medizinischen Einrichtungen oder gar die Übertragung des Operationsgeschehens zwischen Krankenhäusern ist keineswegs nur Vision, sondern ansatzweise schon Realität.
- Die Zukunft zeigt eine Applikationslandschaft, die hohe Ansprüche an Antwortzeit und Güte der Übertragung stellen wird. Den durch die neuen Anwendungen dramatisch wachsenden Ansprüchen an die Bandbreite gesellt sich eine revolutionäre Veränderung des Verkehrsmusters hinzu. Die alte 80-20-Regel nach der 80 % der Datenlast im Segment oder dem Unternehmen verbleiben und nur 20 % die Segmentgrenze überschreiten, wird durch Client-Server-Architekturen, das Internet und die VLAN-Bildung regelrecht auf den Kopf gestellt. Dieser Wandel, gekoppelt mit der Dezentralisierung der Datenquellen allgemein, macht die Datenflüsse eines Netzes unvorhersagbar und hochdynamisch.

- Serverbandbreite und -geschwindigkeit steigen
- Latenzzeit-Reduktion
- Multimedia-Anwendungen
- Multicast-Anwendungen

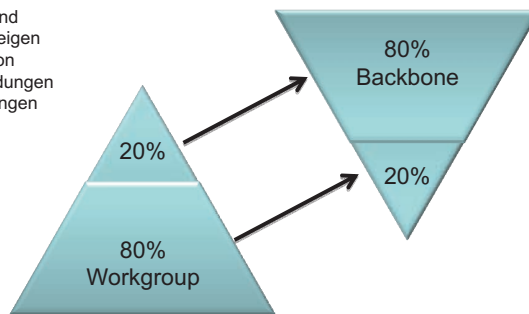


Bild 1.1 Veränderte 80-20-Regel

- Die Veränderungen in den Anwendungen, in der Zahl der Netzbenutzer und im Verkehrsmuster machen verständlich, warum Organisationen gezwungen sind, permanent Teile ihres Netzes zu restrukturieren und auf Technologien mit höherer Bandbreite umzustellen.

Dennoch existieren auch in diesem Meer von Unwägbarkeiten einige Fixpunkte. Zu den Grundprinzipien gehören Aspekte wie:

- Kommunikationsrichtung und Anzahl der Kommunikationspartner
- Topologie/Architektur und Ausdehnung
- Protokolle und Dienste
- Signalkodierung und Übertragungsmedium
- Fehlerbehandlung und Datenflusskontrolle
- Wegewahl/Routing

Diese Begriffe bilden praktisch die unverrückbaren Säulen des Netzgebäudes, um die sich alle neuen Entwicklungen ranken und an denen sie sich orientieren.

Netzwerke bieten mehr als nur die Befreiung des PCs aus seinem isolierten Wirkungsbereich. Häufig fallen in diesem Zusammenhang Begriffe wie Server, Netzwerkbetriebssysteme oder Adapter sowie der Verweis auf zahlreiche Vorteile wie Kostenreduzierung oder Produktivitätssteigerung.

■ 1.1 Basiselemente eines Netzes

Eine Netzstruktur basiert auf vier Elementen:

- den **Rechnern oder Knoten**, die verbunden werden sollen,
- den **Infrastrukturkomponenten**, die den Anschluss und die Kopplung der Rechner im Gesamtkontext leisten. Zu ihren Aufgaben gehört es, Datensignale zu regenerieren und dann zu übertragen, Informationen über die möglichen Wege im Netzwerk bereitzustellen, andere Geräte über Fehler im Netz zu informieren, Datenverkehr gemäß den Dienstgüteanforderungen zu klassifizieren oder Datenströme anhand von Sicherheitsrichtlinien zu erlauben oder zu unterbinden,
- der **Verkabelung**, die die physikalische Verbindung der einzelnen Elemente sicherstellt. Neben der kabelgebundenen Möglichkeit existiert die Anbindung von Endgeräten an die Netzwerkinfrastruktur über drahtlose Alternativen,
- dem **Protokoll**, das die Regeln für einen Nachrichtenaustausch festlegt. Dazu gehört die Definition von Nachrichtentypen und der Übertragungseinheit, d.h. des Paketes, seines Inhaltes und seiner Größe und Struktur, sowie den Austauschprinzipien zwischen den Netzteilnehmern.

Damit sich der Netzwerkzug in Bewegung setzen kann, fehlen noch die Schienen, die Weichen und der Fahrplan:

- **Netzwerkkarte:** In jedem in das Netzwerk zu integrierenden Rechner muss eine Netzwerkkarte installiert sein. Erst über diese Weiche kann der Teilnehmer an den Leistungen des Verbundes partizipieren. Jede Anfrage oder Mitteilung an andere Teilnehmer wird über dieses Medium in das Netzwerk eingespeist. Die Netzwerkkarte ist zuständig für die Übertragung und den Empfang aller Nachrichten. Alle Kommunikationsvorschriften sind vollständig auf diesem Adapter enthalten. Befürchtungen, der Netzknoten könnte durch einen Netzanschluss langsamer werden, sind, was die Verarbeitungsleistung anbetrifft, unbegründet. Wohl aber kann der Datentransport von und zur Netzkarte eine Leistungsminderung verursachen.
- **Kabel:** Die Verbindung zwischen den Netzwerkkarten und damit zwischen den einzelnen Teilnehmern in Form der Schienen wird über Netzkabel hergestellt. Zwei Typen stehen zur Auswahl: Twisted-Pair-Kabel oder Lichtwellenleiter. Sie unterscheiden sich hinsichtlich der zulässigen Geschwindigkeit und technischer Parameter des Übertragungsmediums: elektrischer oder Lichtimpuls.

- **Netzwerkbetriebssystem:** Diese Software stellt den Fahrplan dar und ist für die gesamte Funktionalität des Netzwerkes verantwortlich. Eine effiziente Bearbeitung aller Aufgaben erfordert eine geschickte Organisation aller Rechner, die in ein Netzwerk eingebunden sind. Dazu gehören auch detaillierte Schutzmechanismen. Jeder Anwender muss sich mit einer Kennung und einem Passwort beim Netzwerk anmelden, um sich als rechtmäßiger Anwender auszuweisen. Das Netzwerkbetriebssystem wacht dann über die ordnungsgemäße Zuteilung der Daten und unternimmt umfangreiche Sicherungsmaßnahmen gegen alle Arten des Datenverlustes. Daneben zählt die Geschwindigkeit des Datenzugriffs zu den wichtigsten Eckpfeilern eines Netzwerkbetriebssystems. Heutige Betriebssysteme wie Linux oder Windows beinhalten diese Funktionalität. Der Weg dahin führte aber über spezielle Varianten wie Novell Netware, das zu Spitzenzeiten einen Marktanteil von 80 % besaß.

Die Vorteile eines Netzwerkes erstrecken sich auf unterschiedliche Bereiche:

- **Datenverbund** gewährt den Zugriff auf räumlich verteilte Daten.
- **Lastverbund** gestattet eine optimale Prozessorauslastung. Damit kann eine Verteilung der Rechenlast zu Spitzenzeiten erreicht werden.
- **Funktionsverbund** erweitert die lokale Funktionalität durch den Zugriff auf gemeinschaftlich netzweit genutzte Ressourcen.
- **Leistungsverbund** ermöglicht im Falle einer algorithmischen Zerlegung eines Problems die Verteilung der Rechenlast auf mehrere Knoten. Ein typisches Beispiel hierfür ist die Berechnung von Schlüsseln der symmetrischen Verschlüsselungsalgorithmen.
- **Verfügbarkeitsverbund** stellt eine Mindestleistung bei Ausfall einzelner Komponenten zur Verfügung. Fällt ein Netzknoten aus, kann der Anwender im Idealfall einen Nachbarrechner nutzen, ohne auf die netzweiten Ressourcen verzichten zu müssen. Lediglich die lokalen Anwendungen bleiben von der Bearbeitung ausgeschlossen. Damit wächst die Verfügbarkeit des Gesamtsystems.

Die Leistungsfähigkeit eines Netzwerkes lässt sich anhand dreier Faktoren beurteilen:

- **Bandbreite:** sie ist der Ausdruck für die Kapazität, die das Medium bewältigen kann. Sie misst das Informationsvolumen, das von einem zu einem anderen Ort in einer gegebenen Zeitspanne übertragen werden kann. Die übliche Maßeinheit ist Bit/s.
- **Durchsatz:** er gibt die aktuell transportierte Menge an Daten an und spiegelt damit die augenblickliche Verkehrssituation und kein theoretisches Maximum wider.
- **Goodput:** er ist das Maß für die übertragenen Nutzdaten, d.h. der reinen Nettodaten ohne den verwaltungsmäßig notwendigen Protokolloverhead.

■ 1.2 Netzwerkkategorien

Netzwerke werden zur besseren Systematisierung, zur einfacheren Verwaltung und zur übersichtlicheren Fehlersuche in Kategorien eingeteilt. Eine gängige Typisierung unterscheidet nach:

- Reichweite
- Administrativer Verantwortung
- Topologie
- Technologie

Der geographische Bereich, den ein Netzwerk abdeckt, wird üblicherweise dreigeteilt:

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

Ein LAN ist dabei auf das Firmen- oder Campusgelände begrenzt und in seiner Ausdehnung ohne Zusatzmaßnahmen auf 500 m beschränkt.



Die eingesetzte Technologie und der verwendete Kabeltyp bestimmen wesentlich die exakten Entfernungseinschränkungen und die Anzahl der Knoten, die ein LAN bilden.

Unter einem **MAN** ist ein Regionalnetz mit einem Ausdehnungsradius von ca. 100 km zu verstehen. Ein **WAN** hingegen ist keiner geographischen Beschränkung unterworfen.

LANs sind Netzwerke des Unternehmens. Jedes Unternehmen hat ein starkes Interesse daran, diese Infrastruktur unter eigener Kontrolle zu betreiben und zu warten, um das Herzstück der Informationstechnologie autonom zu halten.

MANs bilden häufig Verbindungsnetze zwischen Institutionen. Ihr Hauptaugenmerk liegt auf der Bildung von Kommunikationsverbünden jenseits der geographischen Unternehmensgrenzen unter eigener Administration und Kontrolle.

WANs verbinden die unterschiedlichen LANs der Unternehmen über eine gesonderte Infrastruktur, die sich im Besitz spezialisierter Dienstleister befindet. Ähnlich wie das Autobahnnetz, das Orte nicht direkt verbindet, besitzt ein WAN keine explizit angebotenen Teilnehmerstationen. Benutzer sind also immer Teil eines LANs oder MANs, die entweder regional begrenzt verbunden werden oder aber unter Zuhilfenahme eines WANs räumlich unbegrenzt gekoppelt werden.



WANs sind Netzwerke, die Routingprotokolle zur Wegwahl der zu übertragenden Informationen nutzen. LANs hingegen beruhen in der Regel auf dem Broadcastprinzip, wie es vom Rundfunk her bekannt ist.

Die Einteilung von Netzen nach verwaltungstechnischen Gesichtspunkten kennt zwei Ausprägungen, die sich danach richten, wer und durch wen die Ressourcen betreut werden:

- In einer **Peer-to-Peer Umgebung** arbeitet jeder Rechner gleichberechtigt und jeder Nutzer administriert seine eigenen Betriebsmittel.
- In einer **Client/Server-Architektur** läuft die Verwaltung zentralisiert auf einem spezifischen Rechner mit einer gesonderten Betriebssystemerweiterung, die bestimmte Sicherheitsmerkmale, Passworte und Zugriffsberechtigungen prüft.

Dem letzten Gedanken folgend lassen sich Rechner grundsätzlich in zwei verschiedene Gruppen einteilen: Server und Clients. Server sind Rechner, die ihre Ressourcen und Dienste der Allgemeinheit zur Verfügung stellen, Clients sind Leistungsnehmer. Diese Art der Gruppierung ist das heute vorherrschende Verarbeitungsprinzip und wird als Client/Server-Architektur bezeichnet. Es beschreibt die Vorstellung, dass die Kooperation einem Grundschema folgt:

- Die Initiative einer Zusammenarbeit geht vom Client aus, indem er Aufträge an einen Diensteanbieter, den Server, schickt, der seine Bereitschaft bekundet hat, für bestimmte Dienste verfügbar zu sein. Dabei gilt eine „1:n-Beziehung“ in beide Richtungen. Der Client kann im Laufe der Verarbeitung auf mehrere Server zugreifen und ein Server kann verschiedene Clients bedienen. Aus der Sicht des Servers – also des Empfängers einer Anforderung – heißt diese Verteilung, er bietet nur bestimmte Dienste an, so dass ihn keine beliebigen überraschenden Nachrichten erreichen können. Auch nimmt er Anforderungen nur entgegen, wenn er „frei“ ist.



Die Dezentralisierung von Knoten hat positive und negative Auswirkungen auf die Nutzer. Drei Aspekte spielen eine wesentliche Rolle:

- **Räumliche Trennung:** Ressourcen in einem Netz haben zu ihrem Kommunikationspartner eine räumliche Distanz. Daraus ergibt sich eine Verzögerung der Signale, die sich letztlich in der Übertragungsdauer niederschlägt. Dem Nutzer begegnet dieser Aspekt durch die Antwortzeit. Aber auch die verfügbare Bandbreite, die Verzögerung von Sendungen oder die Fehlerrate des Mediums können den Nutzer beeinträchtigen.
- **Unabhängigkeit der Knoten:** Die einzelnen Rechner eines Netzes handeln autonom, d. h. sie unterliegen keinem Abstimmungsmechanismus hinsichtlich anderer Teilnehmer. Die Entscheidung zum Senden einer Nachricht treffen die Rechnerknoten ohne Rücksicht auf den Zustand des Netzes und seiner Elemente.
- **Heterogenität der Knoten:** Die Knoten des Netzes unterscheiden sich hinsichtlich Hardware, Betriebssystem und Anwendung. Zur Teilnahme am Netzbetrieb bestehen keine Voraussetzungen hinsichtlich bestimmter Ausstattungsmerkmale. Zum Datenaustausch zwischen den Knoten ist damit keine Kenntnis der genauen Konfiguration eines Partners erforderlich.

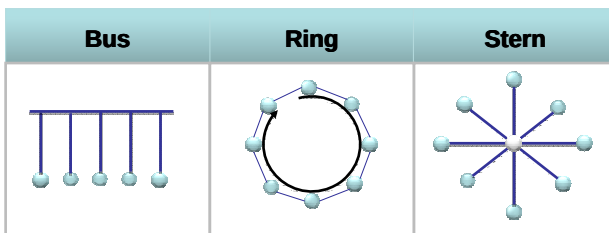
Tabelle 1.1 Vor- und Nachteile von Peer-to-Peer und Client/Server-Netzwerken

Vorteile Peer-to-Peer	Vorteile Client/Server
Preiswerte Implementierung	Zentralisierte Administration – Alle Daten können zentral gesichert werden
Kein Netzwerkbetriebssystem vorausgesetzt	Skalierbarkeit und flexible Architektur
Kein Netzwerkadministrator notwendig	Verbesserte Sicherheit
Nachteile Peer-to-Peer	Nachteile Client/Server
Schlechte Skalierbarkeit bei großen Netzwerken	Server verlangen höherwertige Ausstattung
Sicherheitsprobleme	Administrator notwendig
Jeder Nutzer benötigt Administrationskenntnisse	Single Point of Failure in Form des Servers

Ein flexibler, zukunftsfähiger Netzaufbau setzt ein entsprechendes Design voraus. Der Topologie kommt große Bedeutung zu, denn schließlich bildet sie das Rückgrat des Netzes, das nur mit großem Aufwand verändert werden kann. Eine Topologie lässt sich hinsichtlich dreier Merkmale beurteilen:

- Wie verhält sich der Aufbau bei einer Erweiterung oder Reduzierung von Stationen?
- Wie reagiert das Netz auf den Ausfall einer Station oder einer Verbindung zwischen Rechnern?
- Welcher Verkabelungsaufwand entsteht, um alle Stationen anzuschließen?

Unter Berücksichtigung dieser Fragestellungen lassen sich drei Grundformen bewerten:

**Bild 1.2** Topologie-Übersicht

- **Bus:** Dieser Aufbau verwendet ein zentrales Kabel. Die einzelnen Rechner müssen sich vergleichbar den Haltestellen einer Buslinie gesondert an dieses Medium anschließen. Dazu ist ein eigenes Anschlusskabel für jeden Rechner notwendig. Die Enden der Buslinie müssen durch einen Abschlusswiderstand ordnungsgemäß terminiert werden. Bei dieser Topologie wird nur sehr wenig Kabel benötigt. Rechner können sehr einfach am Netzverkehr teilnehmen, aber auch durch Lösen der Verbindung zum zentralen Kabel wieder zu Kommunikationsinseln werden. Sobald aber das Buskabel unterbrochen wird, kommt das gesamte Netzwerk zum Erliegen.
- **Ring:** Jede Station besitzt genau einen linken und einen rechten Nachbarn. Der Ring ist gerichtet, d. h. die Nachrichten werden in definierter Weise weitergeleitet. Diese Tat-

sache birgt allerdings das Problem, dass bei Ausfall einer Station, der Ring unterbrochen ist, d.h. Signale diese Stelle nicht passieren können und demzufolge das Gesamt-netz seine Funktionsfähigkeit verliert. In der Praxis werden durch einen zweiten gegengerichteten Ring entsprechende Vorkehrungen getroffen, um immer einen ge-schlossenen Ring zu gewährleisten. Als Vorteil zeichnen diese Struktur die einfache Erweiterbarkeit und der geringe Kabelbedarf aus.

- **Stern:** Bei diesem Aufbau besitzt jeder Rechner eine eigene Verbindung zu einer zen-tralen Verteilereinheit. Zwar wird deutlich mehr Kabel als bei der busförmigen Vari-ante benötigt, jedoch sind bei einem Ausfall eines Netzkabels keine anderen Rechner betroffen. Herausragendes Merkmal eines Sterns ist seine leichte Ausbaufähigkeit und seine Ausfallsicherheit. Einziger Schwachpunkt ist die zentrale Verteilerstelle, deren Ausfall nicht kompensiert werden kann.

Tabelle 1.2 Topologievergleich

	Stern	Bus	Ring
Verkabelungsaufwand	-	++	+
Skalierbarkeit	++	+	++
Fehlertoleranz	+	+	-

Derzeit hat sich der Stern als „State-of-the-Art“ durchgesetzt. Praktisch jede Technologie lässt sich auf diese Struktur abbilden.



Die physikalische Topologie beschreibt den Aufbau des Netzwerkes, d. h. die Form in der die Kabel verlegt sind. Die logische Topologie verweist auf den Pfad, den die Daten von der Quelle zum Ziel nehmen. Beide Formen können übereinstimmen (Ethernet), müssen es aber nicht (Token-Ring).

Ein weiterer Ansatz ein Netzwerk zu beschreiben, legt seine verwendete Technologie zu Grunde. Dabei werden Merkmale wie Topologie, Kabeltyp, Entfernungseinschränkungen, Kontrollinformationen oder Adressen beleuchtet.

1.3 Netzzugang und Pakettransport

Eine Kernfrage ist die Regelung des Zugangs der einzelnen Stationen zum Übertragungs-medium. Für die Ankopplung eines Rechners sind zwei Verfahren denkbar:

- **aktive Ankopplung:** Der Netzteilnehmer nimmt das gesamte Paket vom Medium, prüft es daraufhin, ob es an ihn gerichtet ist, und generiert es für die Nachfolgestationen vollständig neu. Der Netzknoten fungiert als Paketregenerator, ein Konzept, das bei Einsatz von Glasfaserkabeln geboten ist, da optische Signale nicht aufspaltbar sind.
- **passive Ankopplung:** Jede Station auf dem Weg zum Ziel analysiert das Paket. Damit wird das Ursprungssignal des Paketes im Zeitverlauf immer schwächer, so dass nach

einer bestimmten Anzahl passierter Teilnehmer, die Qualität nicht mehr ausreicht, um die Wertigkeit des Signals eindeutig zu erkennen.

Auf die Art der Ankopplung hat die einzelne Station jedoch keinen Einfluss. Sie wird von der zugrunde liegenden Technologie bestimmt. Ebenso verhält es sich mit der Steuerung der Konkurrenzsituation der einzelnen Teilnehmer, die sich um das Senderecht und die Übertragungskapazität bewerben. Auch für die Koordination des Zugriffs kommen zwei Strategien in Frage:

- **wahlfreier Zugriff:** Alle Stationen arbeiten unabhängig voneinander und versuchen autonom einen Zugriff, sobald das Medium nicht belegt ist. Für diesen Vorschlag sind keine Kontroll- und Steuerinformationen notwendig.
- **verteilt gesteuerter Zugriff:** Alle Stationen erhalten einen Zugriff, sobald sie im Besitz einer Sendeberechtigung sind, die sie zuvor beantragen und erhalten müssen. Die Existenz dieser Sendeberechtigung macht ein Management für die Vergabe und ihren Fehler- und Verlustfall notwendig.

Die grundlegende Idee des Informationstransportes in Netzwerken besteht darin, Nachrichten in kleine Einheiten, sog. Pakete oder Frames, zu zerlegen, diese mit Adress- und Steuerdaten zu versehen und sie dann zuzustellen. Vor einer Übertragung der Daten erfolgt ihre logische Gruppierung in Pakete. Diese Fragmente der Ursprungsdaten sind leichter zu handhaben und für den Nutzer besser zu interpretieren. Darüber hinaus besitzen Pakete mehrere Vorteile:

- Die Paketeinteilung hindert Rechner daran, die Netzwerkbandbreite zu monopolisieren.
- Gehen Pakete auf dem Übertragungsweg verloren, muss nicht die gesamte Information neu gesendet werden, sondern nur Teile.
- Abhängig von der Auslastung können Pakete unterschiedliche Wege zum Ziel nehmen.

Das Konzept erinnert an die Versendung von Postpaketen. Auch dort wird eine Sendung zunächst in mehrere Einzelteile gestückelt, die den Größen- und Gewichtsanforderungen der Post entsprechen. Anschließend werden sie verpackt und mit den Empfängerdaten beschriftet. Als letzter Schritt erfolgt dann die Übergabe an das Verteilsystem der Post. Damit wird die Übertragung beliebig großer Informationsblöcke möglich, d.h. das Volumen unterliegt keinerlei Größenbeschränkungen. Allerdings können die einzelnen Pakete verschiedene Wege durch das Netz nehmen und müssen – abhängig von der Technologie – möglicherweise häufiger fragmentiert werden.

Je nach Distanz zwischen den kommunizierenden Rechnern unterscheiden sich die für die Paketzustellung verwendeten Verfahren:

- **Teilstrecken- oder Store-and-Forward-Netze** übertragen die einzelnen Pakete als eigenständige Einheiten vollständig getrennt voneinander. Für das Auffinden des optimalen Weges durch den Netzdschunzel nutzen sie spezielle Algorithmen. Die Folge dieser Art des Paketversands ist, dass die einzelnen Pakete ihren Empfänger in beliebiger Reihenfolge erreichen und dort erst wieder zu einer einheitlichen Sendung zusammengesetzt werden müssen. Allerdings können die einzelnen Pakete auf ihrem Weg zum Ziel auch Staus umgehen und trotz längerer Strecke ihr Ziel schneller erreichen

als Pakete, die auf den kürzesten aber verstopften Weg warten. Voraussetzung für eine erfolgreiche Paketvermittlung ist eine ausreichende Zwischenspeicherkapazität der Vermittlungsstellen, denn erst nach genauer Kenntnis des Ziels und der Informationen über die Strecke dorthin kann der Knoten eine verlässliche Entscheidung über den weiteren Weg in Richtung Ziel treffen.

- **Diffusions- oder Broadcastnetze** sind auf kleine Entfernungen ausgerichtet. Die Nachricht erreicht alle angeschlossenen, aktiven Knoten und der Empfänger wählt das an ihn gerichtete Paket aus. Dieses Verfahren verlangt keine aufwendige Wegewahl und keine Zwischenspeichermöglichkeit. Wohl aber müssen alle potenziellen Empfänger das Paket daraufhin prüfen, ob es an sie adressiert ist. Hierfür sind einerseits CPU-Ressourcen der einzelnen Netzknoten notwendig, andererseits verlangt die Prüfung eine gewisse Zeitdauer.

Der Kommunikationsfluss zwischen den Netzteilnehmern verläuft abhängig von der Technologie in drei Formen:



Kommunikationsrichtungen

simplex: In dieser Variante läuft der Nachrichtenfluss nur in eine Richtung, nämlich vom Sender zum Empfänger – Kabelfernsehen oder Rundfunk.

halbduplex: Hier kann zwar jeder Knoten senden und empfangen, aber nicht beides gleichzeitig – Ampelregelung zur Verkehrsführung auf einer normalen Straße mit halbseitiger Baustelle.

vollduplex: Jeder Knoten kann sowohl Nachrichten senden als auch gleichzeitig empfangen. Für den Netzbetrieb ist dieses Verfahren charakteristisch, da kein Netzteilnehmer ausschließen kann, dass er während einer Sendung Kontrollinformationen empfangen muss, um seine Übertragung einzustellen. Gleiches gilt für einen Server, der Anforderungen von vielen Clients erhält und diese simultan verarbeitet.



Das Standardethernetverfahren wird im Halbduplex-Modus betrieben, das modernere Switched-Ethernet häufig im Vollduplex-Modus.

Die unterschiedlichen Formen können als Gradmesser der Übertragungskapazität gelten. Dabei lassen Vollduplex-Verbindungen als die ausgereifteste Variante das größere Volumen zu. Aber auch die Zahl der involvierten Netzteilnehmer kann Rückschlüsse auf die Netzleistung geben.



Anzahl der Kommunikationsteilnehmer

Unicast: Hierbei handelt es sich um die klassische Form des Datenaustausches in Form einer Punkt-zu-Punkt-Verbindung, bei der einem Sender genau ein Empfänger zugeordnet ist.

Anycast: Stellt eine Unicast-Verbindung zu der nächstgelegenen Station einer Gruppe her.

Multicast: Eine ausgewählte Gruppe ist das Ziel der Nachricht. Daraus ergeben sich mehrere Einsatzfelder:

- **Content-Push-Distribution:** Informationsdienste wie Wetter, Nachrichten, Börsenkurse, Software-Updates
- **Verteilung zentraler Datenbestände:** Informationskioske, Produktdatenblätter, Service- und Schulungsunterlagen, Videokonferenzen

Broadcast: Eine Sendung wird allen erreichbaren Stationen des Netzes zugestellt. Dieser Mechanismus findet z. B. bei der Ermittlung der logischen Adresse eines Rechners oder im Netzwerkmanagement Anwendung.



Das Any-Cast-Konzept wird insbesondere durch die neue Internet Protokoll IP Version 6 unterstützt.

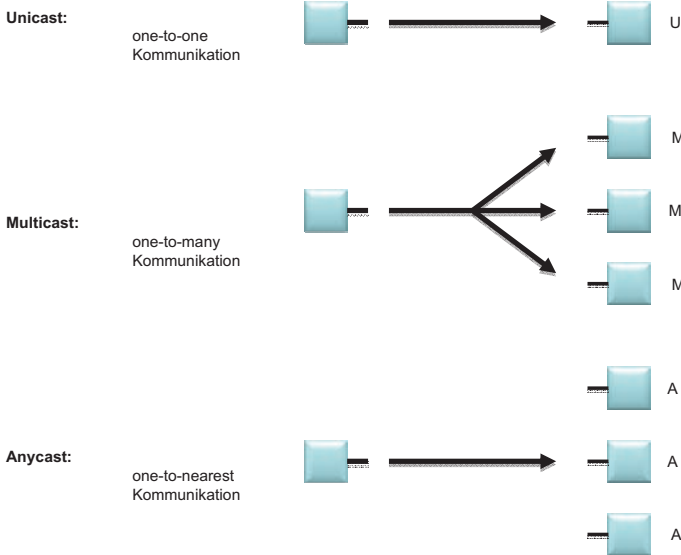


Bild 1.3 Anzahl der Kommunikations-
teilnehmer

Die Übertragungsform selbst trennt zwischen **Leitungs- und Paketvermittlung**. In Analogie zum Telefondienst wird bei der Leitungsvermittlung für die Dauer der Sitzung bzw. des Telefongesprächs eine exklusive Verbindung zwischen den Kommunikationspartnern aufgebaut. Eine Alternative bietet sich mit der Paketvermittlung an, deren Ablauf dem der Briefpost entspricht. Die zu übermittelnde Nachricht wird zu mehreren Paketen zusammengestellt, mit Absender- und Empfängeradresse versehen und einer bekannten Versandstelle übergeben. Jedes Paket nimmt nun – ähnlich wie ein Brief – einen Weg durch das Beförderungnetz, ohne dass der Absender den genauen Weg kennen muss. Im Gegensatz zur Leitungsvermittlung besteht zwischen Absender und Adressat keine ständige Verbindung.

Die **Leitungsvermittlung** hat den Vorteil, dass Dienstgütern im Hinblick auf die Übertragungsgeschwindigkeit jederzeit eingehalten werden können und die Signallaufzeiten konstant sind, d. h. keine Verzögerungen zwischen Sender und Empfänger auftreten. Allerdings ist der Verbindungsaufbau zeitintensiv. Kommunikationsbeziehungen mit mehreren Partnern bedürfen eines wiederholten Aufbaus und beide Teilnehmer müssen mit gleicher Kapazität senden und empfangen. Gleiches gilt, wenn nur kurze Nachrichten übertragen werden. Dann kann die Verbindungsverwaltung mehr Zeit als die eigentliche Übertragung beanspruchen.

Bei der **Paketvermittlung** durchqueren die Pakete als unabhängige und eigenständige Einheiten das Netz und können in den Vermittlungsknoten zwischengespeichert werden. Dies ist ein wesentlicher Vorteil, da nun die Übertragungsgeschwindigkeit zwischen einzelnen Teilstrecken keine Begrenzung mehr darstellt. Allerdings erscheint die Architektur als ein Netzwerk von Warteschlangen. Jeder zu passierende Netzknoten empfängt das Paket und leitet es an seine Ausgangsschnittstelle, die aber Ziel vieler Sendungen sein kann, so dass die Neigung zu Überlastsituationen entsteht. Die Existenz der Warteschlangen erzeugt Verzögerungen in der Paketzustellung oder Paketverluste, die eine Retransmission und damit eine weitere Belastung des Übertragungsweges zur Folge haben. Für den Anwender ist dieser Ablauf intransparent. Er benötigt und erhält keinerlei Informationen über den Übertragungsweg. Im Regelfall kann er diese Informationen auch nicht erlangen, da sich Übertragungswege dynamisch ändern.

Ein lokales Netz besitzt nur eine begrenzte Ausdehnung. Häufig ist es auf eine Abteilung oder ein Gebäude ausgelegt. Im Zeitalter des Intra-/Internets sind Kommunikationsinseln aber ein Fremdkörper, so dass es nur folgerichtig sein kann, eine unternehmensweite Vernetzung anzustreben. Welche Vorteile sich daraus ergeben können, zeigen folgende Sachverhalte:

- **Gemeinsame Datenbestände sorgen für aktuelle Information:** Die wohl wichtigste Aufgabe eines Netzwerkes ist die zentrale Speicherung von Datenbeständen. Änderungen und Aktualisierungen der Daten finden ihren sofortigen Niederschlag im System, ohne dass es der individuellen Abstimmung und des bidirektionalen Austausches der Anwender bedarf.
- **Transparenz:** Zu den Basiseigenschaften verteilter Systeme gehört es, ihre Komplexität vor dem Benutzer geheim zu halten. Dies geschieht hinsichtlich des Ortes, des Zugriffs, der Namen, der Replikation oder des Ausfalls. Der Zugriff auf Netzressourcen bildet damit keinen gesonderten und schwierigen Vorgang, sondern im Gegenteil, das Netzwerk erweitert die Möglichkeiten des Anwenders, ohne dass dieser seine bisherigen Arbeitsgewohnheiten ändern muss.
- **Teilung teurer Peripherie:** Aufgrund der Ablage von Programmen und Daten auf einer zentralen Station muss auch nur diese mit großen Speichermedien ausgestattet sein. Die einzelnen Rechnerknoten selbst benötigen nur noch eine geringe Speicherkapazität. Darüber hinaus können hochwertige Geräte in das Netzwerk integriert werden, die, einmal angeschafft, allen Anwendern gleichermaßen zur Verfügung stehen.
- **Zentrale Programmverteilung:** Da jeder Rechner über das Netzwerk erreicht werden kann, gibt es die Alternative, ein Anwendungsprogramm nur einmal auf einem zentralen Server zu installieren und von allen Anwendern gleichermaßen nutzen zu lassen

oder eine gezielte Verteilung dieses Programms über das Netzwerk auf bestimmte Rechnerknoten vorzunehmen. Auf diese Weise ist es nicht mehr notwendig, jeden einzelnen Arbeitsplatz aufzusuchen, um dort Installation, Wartung oder Aktualisierung auszuführen.

- **Kontrollmöglichkeiten:** Da Netzwerkressourcen nicht im Überfluss existieren, besteht der Bedarf nach einer gerechten Zuteilung. Spätestens hier sind Einsichten in das Nutzungsmuster nötig, um die Erfassung, Abrechnung und Aufbereitung der Leistungen zu ermöglichen. Dass diese Auswertung zuvor erfasste Daten voraussetzt, zeigt, dass eine gewisse Nutzerkontrolle unumgänglich ist.
- **Verschlechterung der Antwortzeiten:** Da ein Wesensmerkmal eines Netzwerkes die gemeinsame Nutzung von Ressourcen ist, besteht auf dem Weg zu zentralen Elementen eine Konkurrenz zwischen allen Teilnehmern. Diese Situation schließt ein, dass jeder Nutzer nur über einen bestimmten Anteil der Übertragungskapazität verfügen kann. Je höher die Nutzerzahl, desto geringer die Kapazität des Einzelnen. Als Folge eines sinkenden Bandbreitenanteils steigt die Antwortzeit. Der Verteilungsaspekt der Software selbst erlangt damit eine bedeutende Rolle. Geleitet von dem Verlangen nach hoher Performance und kurzen Antwortzeiten, ist die Frage nach der optimalen Verteilung keineswegs trivial, sondern hängt im Gegenteil von einer Vielzahl von Rahmenbedingungen wie Lokalität oder Netzdesign ab.
- **Notwendigkeit eines Netzadministrators:** Durch die Verteilung der Daten und Programme auf heterogene, autonome, miteinander kooperierende Rechnersysteme erhöht sich die Komplexität des Gesamtsystems, dessen Pflege, Wartung und Ausbau viel Aufwand und technisches Know-how erfordert.
- **Sicherheit:** Da verteilte Systeme allen Benutzern den gemeinsamen Gebrauch der Ressourcen ermöglichen, treten Sicherheitsanforderungen auf:



- **Autorisierung** – ist der Benutzer berechtigt, auf Netzressourcen zuzugreifen?
- **Vertraulichkeit** – werden die Daten nur von den Berechtigten verarbeitet?
- **Integrität** – erreicht die Nachricht den Empfänger unverändert?
- **Authentisierung** – ist der Kommunikationspartner derjenige, der er vorgibt zu sein?
- **Nichtabstreitbarkeit** – ist das Absenden bzw. Empfangen der Nachricht eindeutig beweisbar?

Auf dem Weg zu einem Netzwerk ist es aber nicht nur bedeutsam, die genauen Anforderungen festzulegen, sondern auch deren Umsetzung.

- **Skalierbarkeit:** Einem Netz müssen problemlos weitere Knoten hinzuzufügen sein. Mit dieser Eigenschaft wird dem weiteren Ausbau und der flexiblen Reaktion auf geänderte Rahmenbedingungen sowie der stetigen Zunahme des Vernetzungsgrades Rechnung getragen.
- **Robustheit:** Die Netzinfrastruktur muss durch Stabilität und Fehlertoleranz geprägt sein. Da Netzwerke in Client-/Server-Umgebungen zu einer kritischen Komponente für

das gesamte Unternehmen geworden sind und der Unternehmenserfolg entscheidend auf einem funktionstüchtigen Netz beruht, bedeuten minimale Ausfallzeiten einen Wettbewerbsverlust.

- **Migration:** Das Netzdesign muss den leichten Übergang auf neue Techniken und Netztopologien zulassen. Der stete Wandel in der Informationsverarbeitung bringt die Notwendigkeit mit sich, einen Übergang auf technologische Änderungen zu ermöglichen, ohne die gesamte Netzinfrastruktur auszutauschen. In diesem Sinne wird Investitionssicherheit für ein Netzdesign groß geschrieben.
- **Autokonfiguration:** Neue Netzkomponenten müssen ohne großen Aufwand integrierbar sein. Nicht nur höhere Bandbreite für Multimedia-Anwendungen steht auf der Wunschliste der Netzbetreiber, sondern auch zunehmend die Möglichkeit, alle Daten von Sprache bis Video über eine Netzinfrastruktur abzuwickeln. Derartig komplexe Anforderungen können nur durch spezielle Kopplungsgeräte erbracht werden. Der einfache Austausch alter gegen neue Geräte, ohne Störung des Netzbetriebs, ist hier die Idealvorstellung.

■ 1.4 ISO/OSI-Referenzmodell

Die Beschreibung der Möglichkeiten, wie eine Station in das Netzwerk integriert wird, zeigt, dass es allgemeiner Verhaltensrichtlinien bedarf, auf deren Grundlage sich Stationen miteinander unterhalten und sich gegenseitig verstehen. Sende- und Empfangsstationen müssen sich an bestimmte Spielregeln halten, damit die Übertragungswünsche der Netzteilnehmer nicht im Chaos enden.

Zur Veranschaulichung der Struktur eines Kommunikationsablaufs zwischen zwei Teilnehmern dient ein logisches Modell. Die Grundidee besteht darin, den Kommunikationsvorgang in eine Hierarchie von Funktionsschichten zu gliedern. Jede Schicht bietet der ihr übergeordneten Schicht Funktionen an und kann Dienste der unter ihr liegenden Schicht in Anspruch nehmen, ohne ihre Funktionsweise zu kennen. Dem Anwender bleibt die Schichtung verborgen. Die Schichten der gleichen Ebene kommunizieren über Protokolle miteinander. Sie beinhalten definierte Regeln, nach denen die beiden Kommunikationspartner zusammenarbeiten und der nächst höheren Ebene ihre Dienstleistung anbieten.

Die Kommunikation zwischen Rechnern in offenen, heterogenen Systemen wird heutzutage durch das ISO/OSI-Referenzmodell beschrieben. Das Referenzmodell ist ein konzeptioneller Rahmen, der Funktionen und Schemata für den Kommunikationsvorgang enthält. Dieser Rahmen teilt den Kommunikationsvorgang in sieben aufeinander aufbauende Schichten ein, denen allgemeine Vereinbarungen und Inhalte zugrunde liegen. Allerdings enthält diese Spezifikation keine Implementierungsvorgaben, so dass eine generelle Umsetzung in Produkte nicht möglich ist. Sie dient lediglich als Leitlinie für den Entwurf und die Implementierung von Standards, Geräten und Internetworkingverfahren. Der Vorteil dieser Vorgabe beruht in erster Linie auf der offenen allgemein verbindlichen Vorstellung eines Kommunikationsvorganges in Form eines Architekturmodells. Darüber hinaus dient die Beschreibung der Funktionen der einzelnen Schichten als Basis für eine präzise Spezifikation von Protokollen und schafft dadurch letztlich eine weitgehend herstellereu-

trale Begriffswelt. Daher ist es theoretisch möglich, das Protokoll einer einzelnen Schicht durch eine Neuentwicklung zu ersetzen, ohne die Funktionen der anderen Schichten zu beeinträchtigen.

Die Protokolle regeln den Kommunikationsablauf, ähnlich wie die Unterhaltung zweier Personen bestimmten Vereinbarungen folgt. Jede Schicht des Senders nutzt ihr eigenes Protokoll, um virtuell mit der entsprechenden Schicht des Empfängers zu kommunizieren. Die ausgetauschten Informationen werden in sog. **PDUs** (Protocol Data Units) übertragen. Diese PDUs enthalten je nach Schicht Prüfdaten, Adressen oder Informationen über übergeordnete Protokolle.



Der Prozess des Durchwanderns der OSI-Schichten macht eine permanente Neuaufteilung der Informationen notwendig, da alle Protokolle nur bestimmte Paketgrößen akzeptieren – **Fragmentierung**. Zur Übertragung selbst werden die PDU-spezifischen Informationen an die zu übertragenen Daten angeheftet – **Encapsulation**. Auf Empfängerseite verläuft der Prozess analog – **De-Encapsulation**:

1. Lesen der schichtspezifischen Information
2. Abtrennen der PDU-spezifischen Daten
3. Weiterleiten der verbliebenen Daten an die übergeordnete Schicht

Den Ablauf auf drei Ebenen verkürzt, zeigt folgendes Beispiel:



Verkürztes Philosophenmodell

Der Philosoph Hill in England möchte seinem chinesischen Kollegen Xiu eine wichtige Fachfrage stellen. Ihr Kommunikationsmedium wäre die Fachsprache der Philosophen. Nun spricht Herr Hill nur englisch, Herr Xiu nur chinesisch. Um dennoch eine Verständigung zu ermöglichen, bedienen sich beide der Hilfe von Dolmetschern. Wie gewöhnlich verfasst Herr Hill seine Frage in Englisch und übergibt diese einem Dolmetscher, der sie in eine beliebige Zwischensprache z. B. italienisch übersetzt. Wie kommt nun die Nachricht vom Dolmetscher des Herrn Hill zum Dolmetscher des Herrn Xiu? Da beide Philosophen Computer-Freaks kennen, die ständig über das Internet miteinander Nachrichten austauschen, lassen sie ihre ins Italienische übersetzte Frage einfach von diesen übermitteln. Beide Computernutzer müssen dazu kein Wort italienisch kennen; sie haben lediglich die Aufgabe, die Worte korrekt zu übertragen. Sobald die Nachricht den chinesischen Computer-Freak erreicht, übergibt er diese dem Dolmetscher, der sie ins Chinesische transformiert und Herrn Xiu überreicht. Auf diese Art können zwei Philosophen miteinander sprechen, ohne die Muttersprache ihres Partner zu beherrschen.

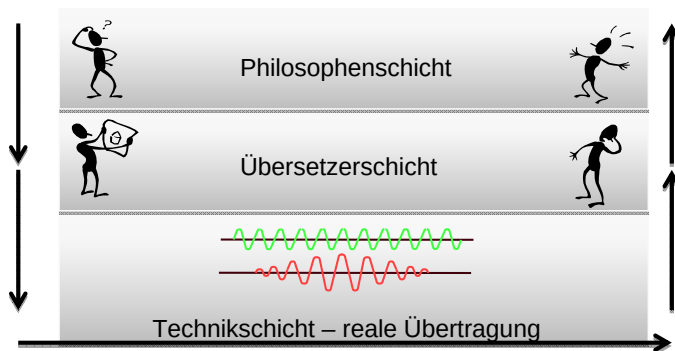


Bild 1.4 Philosophenmodell mit drei Schichten

Wie Bild 1.4 verdeutlicht, findet die eigentliche Übertragung ausschließlich auf der untersten, der Technischschicht statt. Diese Ebene und die Übersetzungsschicht können ohne Funktionseinbuße ausgetauscht werden. Falls der italienische Dolmetscher ausfällt, könnte Französisch als Zwischensprache dienen bzw. falls die Internetnutzung nach China untersagt ist, kann auf Fax ausgewichen werden. Damit wird deutlich, dass die Protokolle bis auf die Schnittstellen voneinander unabhängig und beliebig ersetzbar sind.

Im Unterschied zu den Diensten oder Funktionen, die für die vertikale Kommunikation zwischen den Schichten verantwortlich sind, regeln Protokolle die Kommunikation zweier Partner auf gleicher Ebene, also in horizontaler Richtung. In diesem Sinne ist die Einigung auf Italienisch als Übersetzungs- und das Internet als Transportmedium die Verständigung auf Protokolle.



Die detaillierte und standardisierte Kommunikation nach dem ISO-/OSI-Referenzmodell im Netzwerkumfeld basiert auf sieben Schichten. Die Gesamtheit der sieben OSI-Schichten wird oft als Stack bezeichnet. Die untersten Schichten dieses Modells präsentieren netzorientierte Funktionen, die Oberen werden als anwendungsbezogen eingestuft. Der Ablauf erfolgt beim Sender streng von oben (Schicht 7) nach unten (Schicht 1) und beim Empfänger in der umgekehrten Richtung.

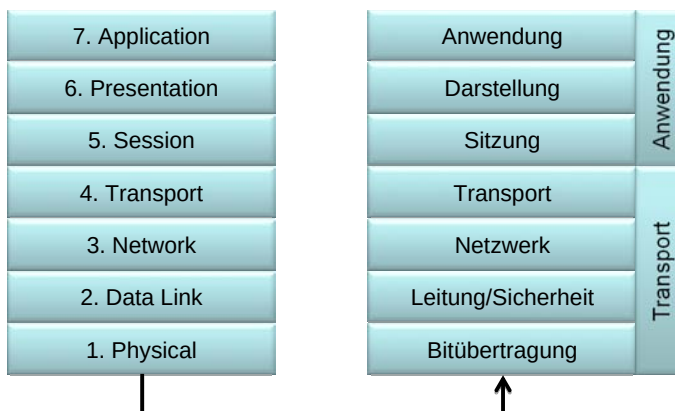


Bild 1.5 ISO-/OSI-Referenzmodell

Neben dem OSI-Modell existiert die Vorstellung der Internetwelt in Form des DoD-Modells über eine funktionale Gliederung des Kommunikationsvorganges. Eine Gegenüberstellung beider Konzepte zeigt das nachfolgende Bild 1.6.

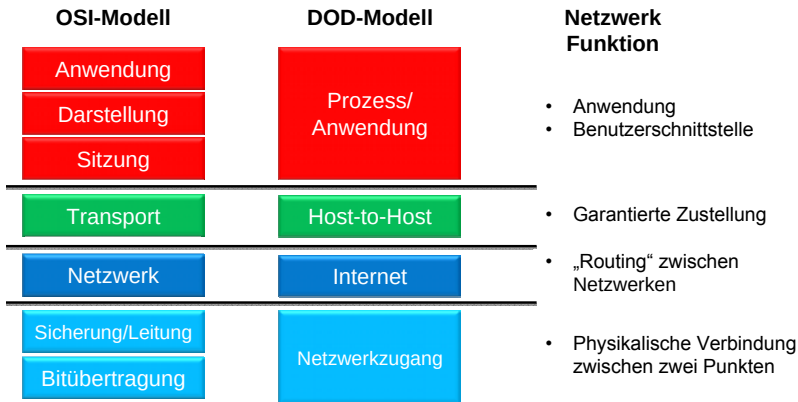


Bild 1.6 Vergleich: ISO-/OSI-Referenzmodell – DoD-Modell

Was ist nun der Inhalt der einzelnen Schichten?

- **Bitübertragungsschicht:** Hier werden die elektrischen, mechanischen und funktionalen Parameter zur physikalischen Übertragung festgelegt. Die Grundfunktion besteht in der Bereitstellung der physikalischen Verbindung und deren kontinuierlicher Betriebsbereitschaft. Zur Gewährleistung dieser Anforderungen sind mehrere grundlegende Details zu klären:



- Wie wird gewährleistet, dass ein Bit der Wertigkeit 1 sowohl vom Sender als auch vom Empfänger als solches erkannt wird?
- Welcher elektrischen Größe entspricht eine logische Eins, welcher eine logische Null?
- Wie viele Mikrosekunden soll die Dauer der Übertragung eines Bits dauern?
- Wie wird eine Verbindung aufgebaut und wie wird sie eingestellt?
- Kann eine Übertragung in beide Richtungen erfolgen?

In Netzwerken werden drei Medien genutzt:

- **Kupfer:** hier beruht die Signalisierung auf elektrischen Impulsen
- **Glasfaser:** hier bildet ein optisches Signal die Grundlage der Signalisierung
- **Wireless:** hier werden Radiowellen verwendet.

In allen drei Formen ist es notwendig, den Beginn und das Ende einer Übertragung mitzuteilen. Dies geschieht über besondere Bitfolgen. Um die Bitfolgen selbst mit semantischem Inhalt zu versehen, ist ein Codierungsschema erforderlich, das Gruppen von Bits zu logi-

schen Einheiten zusammenfasst. Auf diese Weise gelingt es, Buchstaben und Zahlen abzubilden. Die Bitfolgen selbst müssen entsprechend des Mediums signalisiert werden. Hierzu sind bestimmte Schemata notwendig, die vor allem auch eine zweifelsfreie Erkennung des übermittelnden Symbols durch den Empfänger ermöglichen müssen. Zur Spezifikation der Funktionalität gehören außerdem Vereinbarungen der Festlegung von Kabeln und Steckern.

- **Sicherungsschicht:** Die primäre Aufgabe dieser Schicht besteht in der Gruppierung des übertragenen Bitstroms in logische Einheiten. In Abhängigkeit von der eingesetzten Netztechnologie entstehen Rahmen oder Frames unterschiedlichen Inhalts und variierender Größe. Die auf diese Weise zusammengefassten Rohdaten enthalten eine Prüfsumme, so dass auf der Übertragungsstrecke entstehende Veränderungen der Bitfolge erkannt werden. In Abhängigkeit davon, ob eine Fehlerkorrektur eingeleitet wird oder nicht, wird zwischen gesichertem und ungesichertem Dienst unterschieden. Darüber hinaus findet eine funktionale Trennung in zwei Aufgabenbereiche statt:
 - **Media Access Control (MAC):** Steuerung des Zugriffs auf das Übertragungsmedium. Dazu lassen sich zwei Methoden unterscheiden: **kontrolliert**, d.h. jede Station nutzt ein ihr zugeteiltes Zeitintervall zur Übertragung, **wettkampfbasiert**, d.h. die sendewilligen Stationen konkurrieren um die Übertragungsmöglichkeit.
 - **Logical Link Control (LLC):** Verwaltung der logischen Verbindung, Fehleranalyse und Flusskontrolle. Dafür gilt es drei Fragen zu beantworten: welche Knoten kommunizieren miteinander, wann beginnt und endet eine Kommunikation, welche Fehler können während der Kommunikation auftreten?

Die Adressen dieser Ebene werden als physikalische Adressen angesehen. Sie erlauben den Pakettransport innerhalb eines lokalen Netzwerkes, geben aber keine Auskunft darüber, in welchem Netzwerk und wo sich die Station befindet. Damit haben diese Adressen keine Bedeutung über die Grenze des lokalen Netzes hinaus. Die Bedeutung im lokalen Netzwerk ergibt sich daraus, dass üblicherweise keine Punkt-zu-Punkt-Verbindungen existieren, sondern viele Stationen miteinander vermascht sind.

- **Netzwerkschicht:** Um ein Paket zustellen zu können, ist eine Adresse erforderlich. Dazu dient eine logische Adressierung, auf deren Grundlage im nächsten Schritt ein Paketleitweg der Nachricht vom Quell- zum Zielrechner gewählt wird. Dieses als **Routing** bekannte Verfahren sucht einen günstigen Pfad nach unterschiedlichen Kriterien. Dazu können eine gleichmäßige Lastverteilung, hoher Durchsatz, geringe Kosten oder höchstmögliche Sicherheit zählen. Durch ein hierarchisches Adressschema entsteht zudem ein logisches Netzwerk, das im Gegensatz zum physikalischen Netzwerk der Sicherungsschicht keine Verbindungseinheiten wie Kupfer- oder Glasfaserkabel oder die Signalisierung kennt. Dementsprechend lässt sich eine **physikalische Topologie**, die die Anordnung der Knoten und deren Verbindung kennt, von **der logischen Topologie**, die den Weg beschreibt, wie ein Netzwerk Pakete zwischen den Knoten transferiert, unterscheiden.
- **Transportschicht:** Diese Ebene stellt einen universellen Transportservice bereit. Sie richtet sich schwerpunktmäßig auf den Verbindungsaufbau, den Unterhalt und den Abbau mit gesicherten Qualitätsmerkmalen. Die Transportqualität sichert, dass

- die richtigen Bits übertragen,
- die Reihenfolge nicht verändert,
- keine Bits verschluckt,
- keine Sequenzen doppelt übertragen

werden. Um den Datenstrom zwischen Sender und Empfänger den Netzcharakteristika optimal anzupassen, existieren Datenkontrollalgorithmen, die für eine gleichmäßige Auslastung der Verbindung sorgen, bei Überlast das Übertragungsvolumen drosseln oder bei freiem Medium die Übertragungskapazität bis zur Leistungsgrenze ausschöpfen.



Die logischen Einheiten der Ebene 2 bis 4 tragen unterschiedliche Bezeichnungen. Die Packet Data Units (PDUs) auf der Transportebene heißen Segmente, diejenigen der Schicht 3 Pakete und auf Schicht 2 wird von Frames gesprochen.

- **Sitzungsschicht:** Hier werden die Synchronisation und der Dialogablauf zwischen zwei Kommunikationsteilnehmern geregelt. So wird diese Schicht zum Ort, an dem das Netzwerkbetriebssystem einen wichtigen Teil seiner Funktionalität entfaltet.
- **Darstellungsschicht:** Prozessoren stellen Informationen in einem bestimmten Code dar. Big-Endian-CPU's wie die meisten RISC-Prozessoren verwenden das MSB-Format (Most Significant Bit), Little-Endian CPU's wie die Intelfamilie stützen sich auf die LSB-Darstellung (Least Significant Bit). Unterscheiden sich die Darstellungsformate der am Kommunikationsprozess beteiligten Rechner, kommt es notgedrungen zu Fehlinterpretationen. Um diesen Effekt zu vermeiden, erfolgt eine Umsetzung auf ein einheitliches Format.

Ablage des Wortes

31	54	32	10	0
76	54	32	10	

 =76543210₁₆

Little Endian		Big Endian	
Adresse			
76	N+3	10	N+3
54	N+2	32	N+2
32	N+1	54	N+1
10	N	76	N
z.B. Intel		z.B. SUN	

Bild 1.7 Bytedarstellung nach Prozessortyp

Neben der reinen Darstellung der Daten erfüllt diese Schicht noch zwei weitere wichtige Aufgaben:

- **Datenkompression:** die Reduktion der Datenumfänge verringert die Netzlast.
- **Verschlüsselung:** die Umwandlung der Daten in eine Form, die durch Unberechtigte nicht gelesen werden kann.

- **Anwendungsschicht:** Der Inhalt dieser Ebene zielt auf Programme, die als Erweiterungen der Betriebssystemfunktionalität angesehen werden können. Hierunter fallen viele Protokolle, die im Zuge der Internetverbreitung Popularität erlangt haben, wie FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) oder auch EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport). Die Anwendungen selbst sind dieser Schicht allerdings nicht zuzurechnen. Sie stehen außerhalb dieser Modellvorstellung.

Das Schichtenmodell gibt einen Einblick in die Merkmale, die bei einer fehlerfreien und nach einem Standardverfahren ablaufenden Kommunikation berücksichtigt werden müssen. Im Einzelfall, wenn alle Schichten für den Datenaustausch gefüllt sind, entsteht nicht nur der Bedarf nach Verarbeitungskapazität in Form leistungsfähiger Rechner, sondern auch nach Sicherung einer Dienstqualität bezüglich der Antwortzeit. Dabei ist zu beachten, dass jede Schicht ihre spezifischen Steuer-, Kontroll- und Verwaltungsfunktionen der ursprünglichen Nutzlast hinzufügt. Damit wird bei einem Durchlauf durch die Kommunikationshierarchie das Verhältnis von Nutz- zu Protokollinformation immer ungünstiger. Die ursprünglich kleine Nachricht wird durch schichtspezifische Daten derart aufgebläht, dass ein hoher Anteil der Übertragungskapazität nur für den Transfer dieser Steuerdaten verbraucht wird:

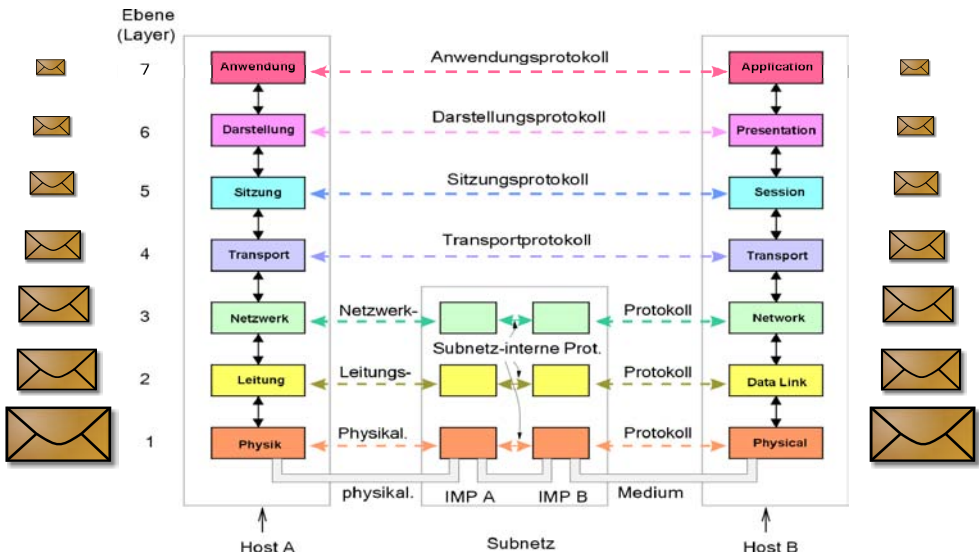


Bild 1.8 Nutzdaten vs. Overhead

Die bisherige Beschreibung des Kommunikationsvorganges macht keine Aussagen über die Reaktion bzw. Rückmeldung des Empfängers einer Nachricht. Tatsächlich kann der Ablauf danach unterschieden werden, ob eine Antwort erwartet wird oder nicht.

Verbindungsorientierte Protokolle richten vor Aufnahme des Datenaustausches eine Verbindung mit dem Partner ein und erwarten hierfür dessen Zustimmung. Sollte diese ausbleiben, kommt es zu keiner Verbindung, ansonsten wird eine dauerhafte Kommunikationsbeziehung eingerichtet.

Verbindungslose Protokolle hingegen leiten einen Kommunikationsvorgang ein, ohne sich der Zustimmung des Partners zu vergewissern. Daher können Reaktionen des Partners auf den Sendewunsch nicht berücksichtigt werden. Aber auch elementare Dienste wie die Paketwiederholung im Verlustfall oder die Reduktion der Übertragungsleistung bei Überlast bleiben unbeantwortet. Grundsätzlich ist dem Sender unbekannt, ob der Empfänger erreichbar ist, ob er die Nachricht erhält und wenn, ob er sie lesen kann. Der Empfänger hingegen ist nicht darüber informiert, dass eine Nachricht an ihn verschickt wurde.

Diese Einschränkung mutet strikter an als sie tatsächlich ist. Da während eines Nachrichtenaustausches mehrere Protokolle des Schichtenmodells genutzt werden, können diese sowohl der einen wie der anderen Klasse angehören. Täglich lässt sich dieses Szenario in der Internetkommunikation beobachten, bei der das Internet-Protokoll in die Kategorie der verbindungslosen und das TCP-Protokoll in die Kategorie der verbindungsorientierten Dienste fällt. Dieses Nebeneinander ergänzt sich in der Funktionalität und sichert einen angemessenen Overhead, da nicht jede Schicht die gleiche Funktionalität wiederholt anbieten muss.



Noch Fragen ...? Ja ...

Welches ist die weitreichendste Entwurfsentscheidung?

Die Entscheidung jegliche Daten in Paketform zu übertragen, dominiert die gesamte Netzarchitektur.

Was ist ein großes Problem dieses Konzeptes?

Da jedes Protokoll ein eigenes Paketformat definiert, kommt es zu unterschiedlichen Paketlängen. Folge dieser Abweichungen sind Fragmentierungen und häufiges „Umpacken“.

Hat das OSI-Modell noch eine Relevanz?

Ja, nach wie vor richten sich alle Hersteller nach dieser Schichteneinteilung oder der des DoD-Modells.

Gibt es dokumentierte Standards im Netzwerkbereich?

Ja, Standards sind hier als Übereinkommen definiert und werden als Request for Comment (RFC) bezeichnet. Die Gesamtheit dieser RFCs finden sich unter <http://www.rfc-editor.org>

■ 1.5 Zusammenfassung

Die Weiterentwicklung des Netzwerkgeschehens bleibt schwer vorherzusagen. Dennoch sind einige Trends unverkennbar: die zunehmende Nutzung mobiler Dienste auf unterschiedlichen portablen Geräten, der steigende Bedarf an multi-medialen Inhalten verknüpft mit der Erwartung nach Dienstgütern und die Verschmelzung der Dienste, die vormals analog nun die digitale Welt erobern.

Das Kapitel gibt einen Überblick über Basisbegriffe von Netzwerken, der natürlich nicht erschöpfend sein kann. Sowohl zusätzliche Aspekte wie Protokolle oder Betriebssystemdetails als auch eine feinere Untergliederung bestehender Technologien sind denkbar. Neben dem Wissen um grundsätzliche Inhalte sollte der Leser in der Lage sein, Vor- und Nachteile von Netzwerken abzuwägen, aber auch erste technische Merkmale wie Zugang der Stationen zum Übertragungsmedium, Bausteine einer Netzstruktur oder Leitungs- versus Paketvermittlung detailliert beurteilen zu können.

Besonderes Gewicht dieses einführenden Kapitels liegt auf der Basisidee des ISO-/OSI-Referenzmodells, das entscheidend den Standardisierungsgedanken in der Netzwerkwelt geprägt hat. Die sieben Schichten und ihre Funktionen sollten daher jedem, der sich mit Netzwerken auseinandersetzt, geläufig und vertraut sein.

■ 1.6 Wissensüberprüfung

1. Auf welcher Schicht findet eine Segmentierung des Datenstroms statt?
2. Wie heißt die PDU der Sicherungsschicht?
3. Welche Schicht ist für die Datendarstellung, die Kompression und die Verschlüsselung zuständig?
4. Welche Vorteile besitzt die Schichtenbildung des ISO-/OSI-Referenzmodells?
5. Wie lauten die vier Schichten des DoD-Modells?
6. Welche Netzwerktopologien kennen Sie?
7. Welche Vorteile besitzt das leitungsvermittelnde Verfahren im Vergleich zum paketvermittelnden Dienst?
8. Beschreiben Sie, wie verbindungsorientierte Protokolle des Internets eine zuverlässige Übertragung bereitstellen.
9. Skizzieren Sie die wahlfreie Zugriffsmethode.
10. Erläutern Sie die Begriffe:
 - Unicast
 - Anycast
 - Multicast
 - Broadcast

2

Übertragungsmethoden und -medien

Lernziele

Nach Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Was ist der Zweck der Signalisierung und der Kodierung in Netzwerken?
- Welche Verfahren existieren, um Bits zu signalisieren?
- Was bedeutet die strukturierte Verkabelung für den Netzwerkaufbau?
- Welche Bedeutung kommt der Backbonearchitektur zu?
- Was sind die Charakteristika der Medien Kupfer und Glasfaser?

Kapiteleinführung

In den Anfängen der Netzwerke erforderte jede Kommunikationstechnologie ihre eigene spezifische Verkabelung. Token-Ring war zunächst nur für den Kabeltyp 1 und 3 von IBM definiert, Ethernet kannte nur Koaxialkabel. Die Folge war ein Nebeneinander verschiedener Topologien, Medien und Steckverbindungen. Dies wirkte sich insbesondere bei Umzügen von Mitarbeitern folgens schwer aus. Neu- und Nachverkabelungen waren an der Tagesordnung. Um diese Schwäche zu mildern, entstand der Wunsch nach einer einheitlichen Verkabelung unabhängig von der bisher und zukünftig eingesetzten Technik. Die Struktur soll es ermöglichen, Veränderungen im Unternehmen flexibel zu begegnen, ohne dass es zu Störungen oder Unterbrechungen des Netzbetriebs kommt.

Als weitere Anforderung kommen Ansprüche an die Verkabelung hinzu, die sich aus dem Verkehrsmuster ergeben, wie es die Client-Server-Architektur erzeugt. Der typische Datenpfad verläuft wie folgt: ein Client sendet einen Auftrag an einen Server. Dieser erledigt den empfangenen Auftrag indem er dem Client eine für ihn unbestimmte Menge von Paketen zurück gibt. So löst ein Druckauftrag nur eine Ausführungsbestätigung, das Laden einer Software aber einen Strom von Paketen aus. Damit entsteht ungleichgewichtiger Datenverkehr durch Clients, die Anfragen stellen, und Server, die diese beantworten. Besitzen die Server nicht die ausreichende Bandbreite, um die Ergebnisse zuzustellen, bleiben die Anfragen der Clients unbeantwortet. Zusätzlich kommt erschwerend ein stetiges Wachstum der Anzahl der Clients hinzu. Vor diesem Hintergrund wird deutlich, dass der Anordnung und Platzierung der Server und Clients im Netzwerk eine herausragende Bedeutung zukommt. Hierbei spielen nicht nur Verkabelungsaspekte eine Rolle. Auch die strategisch günstige Einbindung aller Arten von Internetworkingkomponenten wird zu einem zentralen Gesichtspunkt.

■ 2.1 Übertragungsverfahren

Gemäß der Modellvorstellung des ISO-/OSI-Referenzmodells erfolgt der Datenaustausch zwischen zwei oder mehreren räumlich getrennten Rechnern logisch über Pakete, physikalisch aber als Bitstrom. Zur Darstellung der einzelnen Bits kommen grundsätzlich zwei Übertragungsvarianten in Betracht:

- **Analog:** Die Menge der codierten Werte ist kontinuierlich und entspricht einem unendlichen Zahlenvorrat. Die Übertragung von Informationen nutzt stetige Veränderungen elektrischer Spannungen, um die Werte Null und Eins darzustellen.
- **Digital:** Ein digitales Zeichen gehört zu einem endlichen Zeichenvorrat mit gut unterscheidbaren Elementen. Der Übergang von einem digitalen Zeichen zu einem anderen erfolgt sprunghaft, im Gegensatz zum fließenden ineinander Übergehen des analogen Verfahrens.

Bei der analogen Übertragung wird der Verlauf der Spannung in Form einer Sinuskurve interpretiert. Dabei wird die Variation der Amplitude, der Frequenz oder der Phase als Maßstab für die Codierung der beiden Zustände Null und Eins verwendet. Die Frequenzmodulation nutzt eine vollständige Schwingung als Interpretation für eine Eins und zwei Schwingungen für eine Null, die Amplitudenmodulation interpretiert eine „flache“ Schwingung als Null und eine „hohe“ als Eins und die Phasenmodulation interpretiert eine Schwingung von unten nach oben als Null und von oben nach unten als Eins. In den Übertragungsnormen V.xx finden praktisch alle Verfahren Eingang. So basieren die Normen V.27 auf der Phasen-, V.23 auf der Frequenz- und V.32 auf der Amplitudenmodulation.

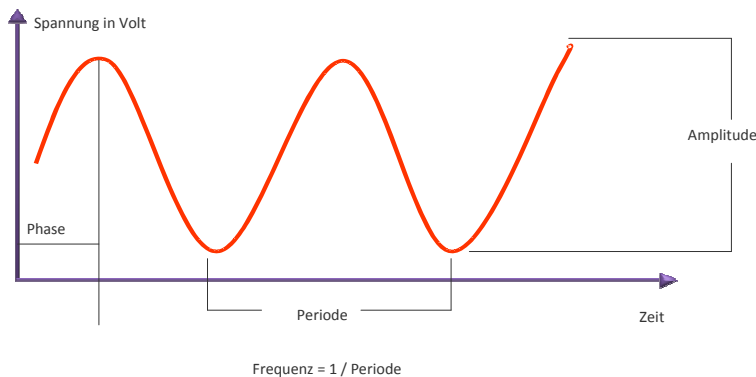


Bild 2.1 Analoge Übertragung

Paradoxerweise wird häufig die Meinung vertreten, die digitale Übertragung löse alle Probleme der Datenübermittlung, da sie exakt zwischen zwei Zuständen unterscheiden kann. Tatsache ist jedoch, dass die analoge Technik aufgrund ihres fließenden Charakters weit mehr Informationen darstellen kann. Dazu bedient sie sich wechselnder Spannungsgrößen oder variierender Frequenzen. Diese Übertragungsverfahren werden als Multilevel-Codierung bezeichnet und von den digitalen Formen wie ISDN oder ADSL nachgebildet, um die gewünschten Datenraten zu erreichen.

Durch eine geeignet gewählte Übersetzung wird aus den digitalen Informationen ein analoges Signal erzeugt und umgekehrt. Die Aufgabe dieser Konvertierung ist es, den zu übertragenden Bitstrom an die Eigenschaften des Übertragungsmediums so anzupassen, dass Verfälschungen ausgeschlossen sind und das höchstmögliche Volumen transportiert werden kann.

Die einfachste Form der Codierung wäre diejenige, die Zustände Null und Eins in zwei verschiedenen Spannungen abzubilden. Dieser als reine Bitcodierung bekannte Vorschlag leidet jedoch unter dem Problem, dass bei langen Sequenzen von Nullen oder Einsen der Takt zwischen Sender und Empfänger verloren geht. Das Ergebnis wäre eine Fehlinterpretation bzw. ein Verlust von Bits. Die Ursache hierfür liegt darin, dass die Abstimmung zwischen Sender und Empfänger über den Zeitpunkt und die Zeitdauer der Sendung niemals exakt sein kann. Kleine Schwankungen bewirken eine Verschiebung des Fensters für Beginn und Ende des Bits, so dass mit zunehmender Zeitspanne das Fenster auswandern kann. Zur Unterdrückung dieses Problems dient die Manchester-Codierung. Dieses Konzept sieht einen Sprung zwischen den Zuständen „hoch“ und „niedrig“ für jedes Bit vor. Die Pegeländerung findet jeweils zur Intervallmitte der Bitdarstellung statt und zwar nach der Systematik:

- 0: von niedrig nach hoch
- 1: von hoch nach niedrig

Dieser Spannungswechsel pro Bit macht die Taktrückgewinnung unproblematisch, so dass es zu keinen Fehlinterpretationen kommt. Dabei wird der erste Teil der Darstellung als Taktinformation, der zweite als eigentlicher Dateninhalt interpretiert.

Im Laufe der Zeit haben sich immer ausgereifere Verfahren entwickelt, um die Taktinformationen möglichst effizient mit den Daten zu mischen. Das NRZI-Verfahren (Non-Return-to-Zero-Inverted) ändert bei jedem Wert von Eins den Pegel, lässt ihn aber bei einer Null unverändert. Um lange Folgen von Nullen vor einer Fehlinterpretation zu schützen, erfolgt eine Transformation von jeweils 4 Bits in eine 5 Bitfolge. Diese redundante Konstruktion lässt aus den ursprünglich $2^4 = 16$ jetzt $2^5 = 32$ Zeichengruppen entstehen. Diese Aufteilung dient mehreren Zwecken:

- Neue Zeichengruppen können neuen Anwendungen dienen.
- Nicht belegte Zeichengruppen werden als verboten definiert. Ihr Auftreten ist ein untrügliches Zeichen für Übertragungsfehler.
- Die Codierung der Gruppen ist so gewählt, dass die Lauflänge von Bitmustern limitiert ist. Auf diese Weise kann sichergestellt werden, dass nie mehr als eine maximale Anzahl von Nullen oder Einsen hintereinander gesendet werden.

Von den 32 Zeichen werden 16 als Datensymbole verwendet, 6 als Kontrollindikatoren und die restlichen bleiben undefiniert.

Das MLT-3-Verfahren (Multi-Level 3) leitet sich vom NRZI-Konzept ab, nur dass jetzt die Kodierung der Einsen über drei Ebenen erfolgt.

Die Umrechnung für die 16 ursprünglichen auf 32 neue Datenwerte zeigt Tabelle 2.1:

Tabelle 2.1 4Bit/5Bit-Kodierung

HEX-Wert	4-Bit	5-Bit
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	10111
C	1100	11010
D	1101	11011
E	1110	11100
F	1111	11101

Einen Vergleich der unterschiedlichen Codierungsverfahren zeigt Bild 2.2:

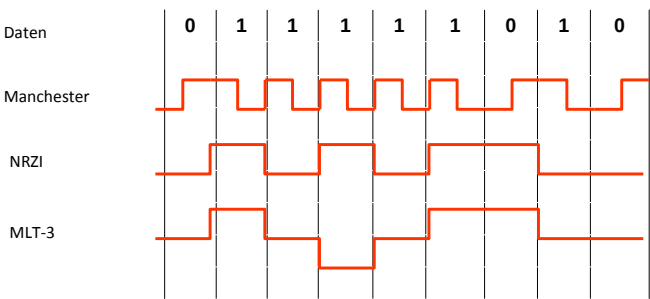


Bild 2.2 Codierungsverfahren

Multiplexing ist eine Methode, unterschiedliche logische Datenströme über ein physikalisches Medium zu versenden. Dieses Konzept kommt sowohl bei analogen wie auch bei digitalen Verfahren in mehreren Realisierungen vor:

- **Frequenzmultiplexing:** Analoge Signale nutzen typischerweise diese Form. Dazu werden mehrere Kanäle über eine physikalische Verbindung geführt und jedem Kanal eine andere Frequenz zugewiesen.

- **Zeitmultiplexing:** Digitale Signalübertragungen basieren vornehmlich auf diesem Konzept. Die Benutzer wechseln sich zu verschiedenen Zeitpunkten in der Benutzung der Verbindung ab, so dass ein ineinander verschachtelter Datenstrom von Paketen der verschiedenen Anwendungen entsteht.

Zur erfolgreichen Übertragung ist Synchronität zwischen Sender und Empfänger notwendig; dabei werden die beteiligten Taktgeneratoren zeitlich aufeinander abgestimmt. Da es bei der Datenkommunikation per Definition keinen gemeinsamen Takt gibt, muss immer explizit synchronisiert werden. Doch wie wird dies erreicht?

- **synchron:** Sender und Empfänger werden durch eine Bitfolge in den gleichen Zeittakt versetzt. Dazu kann die Taktinformation in ein Datenpaket verpackt werden wie es durch die Präambel bei Ethernet geschieht. Aber auch die Übertragung eines Taktsignals über einen gesonderten Kanal ist möglich (z.B. der D-Kanal bei ISDN).
- **asynchron:** Die Zeichenfolgen einer Übertragung werden für den Empfänger zu einem zufälligen, nicht voraussehbaren Zeitpunkt gesendet. Um die Nachricht als solche zu erkennen, versieht der Sender sie mit besonderen Anfangs- und Endsymbolen.

Als Folge der Synchronität muss der Empfänger das erhaltene Signal zur richtigen Interpretation für eine gewisse Zeitdauer zum richtigen Zeitpunkt abtasten. Dazu ist ein bestimmtes Abtastintervall notwendig, bis das Signal auf dem Medium in eine stabile Form übergeht. Die Zwischenzeiten, in denen das Signal ungültige Messwerte annimmt, werden ignoriert. In dieser scheinbaren Selbstverständlichkeit liegt eine große Herausforderung; denn die ständig steigenden Übertragungsbedürfnisse münden in immer schnellere Übertragungsverfahren, die zu einer Verkürzung der Zeitschranken zur Sendung und Erkennung eines Symbols führen. Folglich muss die Technologie zur eindeutigen Erzeugung und Identifizierung eines Signals immer präziser werden.



Noch Fragen ...? Ja ...

Warum werden Signale überhaupt kodiert?

Würden Signale nicht kodiert, kämen sie als reine Wellenform, die nicht interpretierbar wären. Nur kodierte Signale geben die Möglichkeit, darin Daten zu übertragen.

Wie viele Arten der Datenkodierung gibt es?

Im Laufe der Zeit haben sich unterschiedliche Kodierungsschema mit unterschiedlichen Vorteilen entwickelt. Bekannt sind das Manchester-Verfahren, die NRZ- und NRZI-Kodierung für die Datenübertragung bzw. ASCII, BCD und Unicode für Zeichen.

Welche Verfahren werden in heutigen Netzwerken genutzt?

4B/5B und 8B/10B werden in Fast Ethernet und Gigabit-Ethernet verwendet, 100G-Ethernet setzt 66B/68B ein.

■ 2.2 Strukturierte Verkabelung

Die Entwicklung im Netzwerkbereich hat zu einigen Vereinfachungen geführt. So hat sich die Starrheit der Kombination von LAN-Technologie und Verkabelung gelöst. Die Standardisierungsbestrebungen in diesem Bereich haben es ermöglicht, die wichtigsten LAN-Varianten durch unterschiedliche Übertragungsmedien zu realisieren. So entsteht die Wahlfreiheit, ein LAN durch Twisted-Pair- und Glasfaserkabel aufzubauen.

Die Weiterentwicklung der Verkabelungsmethoden mündete darin, alle denkbaren Kommunikationsarten von Sprache über Text bis Video zu erlauben. Ausdruck der Umsetzung dieses Anspruchs ist ein allgemeines Strukturmodell für die Verkabelung, das als Prinzip der strukturierten Verkabelung Eingang in die Normung gefunden hat.



Strukturiertheit

Strukturiert bedeutet, dass möglichst wenig unterschiedliche Übertragungsmedien die Übertragung möglichst vieler Anwendungen erlauben.

Diese Anforderungen wurden durch den internationalen Standard ISO/IEC 11801 sowie durch die Europeanorm EN 50713 Rechnung getragen. Die EN 50713 definiert die Topologie und die übertragungstechnischen Kenndaten hersteller- und anwendungsneutraler Verkabelungen für unabhängige, flexible und zukunftssichere Verkabelungen. Die Umsetzung erfolgt durch die Bildung von Hierarchiestufen, die topologisch und administrativ zusammengehören. Der Übergang von einer Hierarchiestufe zur nächsten findet dabei an definierten Punkten mit bestimmten Geräten statt.



Strukturierte Verkabelung

Primärbereich: Hierbei handelt es sich um eine gebäudeübergreifende Verkabelung mittels redundanter Kabeltrassen auf Lichtwellenleiterbasis, die an Gebäudeverteiltern beginnen bzw. enden. Aufgrund der relativ großen Entfernungen kommen hierfür ausschließlich Glasfaserkabel zum Einsatz.

Sekundärbereich: Grundlage ist eine gebäudeinterne Verkabelung, die die Gebäudeverteiler mit einzelnen Etagenverteilern auf Grundlage von Kupfer- oder Glasfaserkabeln verbinden.

Tertiärbereich: Eine sternförmige Verkabelung auf Etageebene, die die Endgeräte mit Etagenverteilern verbindet, bildet die Strukturierungsebene zum Endgerät.

Die Umsetzung dieses Stufenkonzeptes ist zukunftssicher, einfach zu warten und betriebsicher. Die strukturierte Verkabelung lässt auf den einzelnen Ebenen unterschiedliche Kabelarten zu. So schlägt der EIA/TIA 568 Commercial Building Wiring Standard drei grundsätzliche Kabelarten für den Tertiärbereich vor: Koaxial-, Twisted Pair- und Glasfaserkabel.

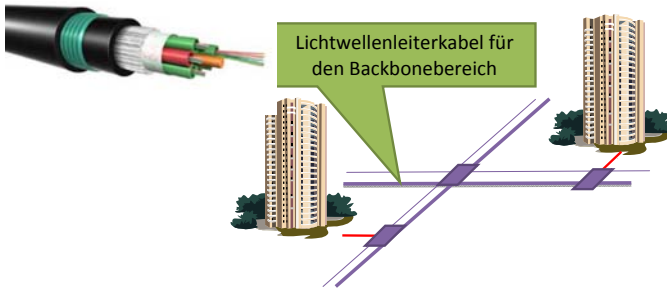


Bild 2.3 Primärverkabelung

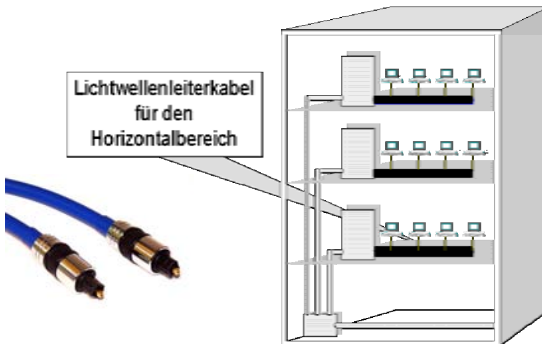
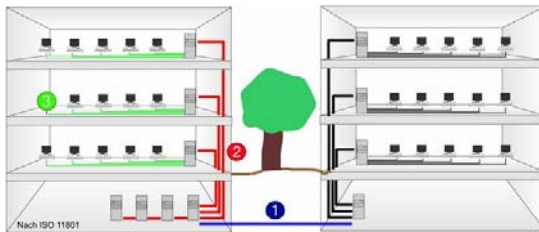


Bild 2.4 Tertiärverkabelung



- 1 Primärbereich
- 2 Sekundärbereich / Vertikalverkabelung
- 3 Tertiärbereich / Horizontalverkabelung

Bild 2.5 Strukturierte Verkabelung auf einen Blick

Mit der Realisierung der strukturierten Verkabelung gehen zwei Konzeptionen für das Netzdesign einher.

- **Distributed Backbones** beinhalten die genaue Abbildung der strukturierten Verkabelung. Gebäudeverteiler stellen dabei Switches dar. Der Übergang von einem LAN-Segment in ein anderes erfordert stets das Passieren zweier Koppelungselemente was Leistungseinbußen nach sich ziehen kann. Bei den derzeit angebotenen leistungsfähigen Switches spielt dieses Argument jedoch eine zunehmend geringere Rolle.
- **Collapsed Backbones** verdichten das Etagenbackbone durch Verzicht auf die Sekundärebene auf einen einzelnen sehr leistungsfähigen Netzknoten. Dadurch entsteht eine Sterntopologie mit der Möglichkeit zum zentralen Management. Da der Switch bzw. Layer-3-Switch das Backbone darstellt und diese Komponenten sehr ausgeprägte Leistungsmerkmale aufweisen, ergibt sich die Möglichkeit der Skalierung der Backbone-

leistungsfähigkeit. Andererseits stellt der zentrale Netzknoten einen „Single Point of Failure“ dar, so dass es hier besonders ausfallsicherer Komponenten bedarf.

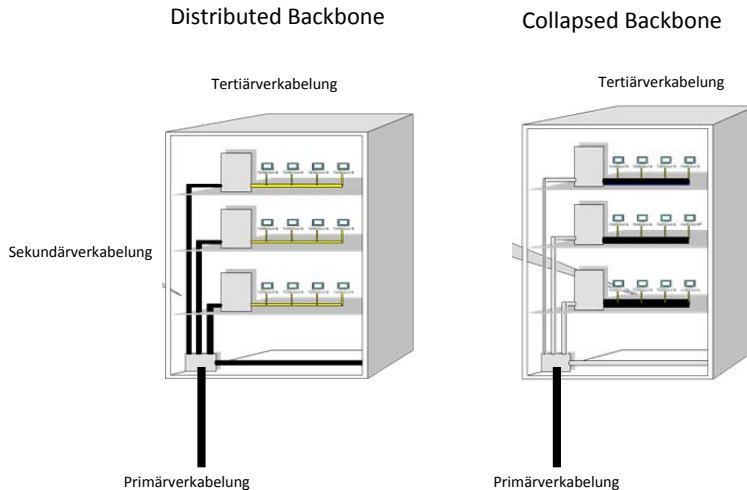


Bild 2.6 Distributed und Collapsed Backbone

Die Struktur des Distributed Backbones besticht durch ihre leichte Administrierbarkeit und ihr ausreichendes Leistungsverhalten, wenn Server und Arbeitsstationen im gleichen, relativ kleinen Segment angesiedelt sind. Zunehmend komplexere Organisationen fördern den Trend, dezentrale Komponenten zugunsten eines zentralen Informationszugriffs und -managements aufzugeben. Sinkende Kosten und die Verwaltung nur einer Netzkomponente motivierten diese Strukturänderung in Richtung Collapsed Backbones zusätzlich. Dennoch lassen sich beide Backbone-Konzepte kontrovers diskutieren:

Distributed Backbone:

- ☺ Der Aufbau einer Ringstruktur ermöglicht eine gute Fehlerredundanz.
- ☺ Ein geringer Verkabelungsaufwand reduziert die Investitionskosten.
- ☺ Durch die geringere Ausdehnung des Tertiärbereiches besteht eine Präferenz für den Erhalt der Kupferverkabelung.
- ☺ Strukturelle Änderungen können nur mit großem Aufwand realisiert werden.
- ☺ Übergänge in andere Segmente verlangen das Passieren mehrerer Koppelungskomponenten.
- ☺ Mehrere Kopplungskomponenten steigern die Komplexität und stellen einen „Point of Failure“ dar.
- ☺ Dezentrale Strukturen erfordern Stromzuführungen und gesonderte Klimaanlage.

Collapsed Backbone:

- ☺ Jede Verbindung kann die gesamte Bandbreite in Anspruch nehmen.

- ☹ Durch einen zentralen Verteiler verringert sich die Zahl der aktiven Komponenten, es lässt sich leichter eine redundante Infrastruktur aufbauen und es fallen geringere Verwaltungs- und Wartungskosten an.
- ☹ Die Notwendigkeit nur eines zentralen Verteilerraumes verringert die Gebäudekosten.
- ☹ Zum Übergang in andere Segmente wird allenfalls die Hälfte der Kopplungselemente des Distributed Backbones benötigt.
- ☹ Durch die Zentralisierung entsteht erheblicher Verkabelungsaufwand.
- ☹ Die Anzahl der benötigten Anschlussports in der zentralen Komponente entspricht der Anzahl anzuschließender Geräte.
- ☹ Mit dem zentralen Knoten entsteht ein „Single Point of Failure“.

■ 2.3 Glasfaserverkabelung

Die strukturierte Verkabelung wird zunehmend zum entscheidenden Aspekt der gesamten Gebäudevernetzung. Dabei nimmt die Bedeutung der Glasfaser durch ihre herausragenden Übertragungseigenschaften stetig zu.

Der Markt für Glasfaserprodukte ist bei weitem kein Nischenmarkt mehr. Interessanterweise wird er in den USA, dem Land der ungeschirmten Twisted-Pair-Verkabelung, stark vorangetrieben. Eine Vorreiterrolle übernehmen dabei zwei Arbeitsgruppen, die FOLS (Fiber-Optic LAN Section) der TIA (Telecommunications Industry Association) und die OIDA (Optical Industry Developing Association). Sie beeinflussen die Standardisierung maßgeblich. Glasfaser war lange das bevorzugte Medium für Backbones im Primär- und Sekundärbereich, nicht aber für den Tertiärbereich. Diese etablierte Verteilung wandelt sich stetig dahingehend, dass Lichtwellenleiter aus mehreren Gründen verstärkt Einzug in die Etagen halten:

- Glasfaser bis zum Arbeitsplatz erspart die gesamte EMV-Problematik (Elektromagnetische Verträglichkeit).
- Eine unbemerkte Verletzung der mikroskopisch kleinen Faser ist praktisch nicht möglich.
- Für eine Kupferleitung gestaltet sich die Fehlersuche sehr aufwendig, weil die Störquelle in der Buchse, im Stecker oder im Kabel liegen kann. Zur konkreten Analyse ist demzufolge eine aufwendige Messtechnik erforderlich. Bei LWL-Leitung treten Störungen sehr viel seltener auf. Im Fehlerfall ist die Erkennung einer defekten Faser per Sichtprüfung ohne Einsatz von Werkzeugen möglich, was eine erhebliche Erleichterung der Administration bedeutet.
- Durch die steigende zulässige Leitungslänge für Glasfaser reduziert sich die Anzahl der Schnittstellen und damit der potenziellen Störquellen. Diese systembedingte Eigenschaft wirkt sich äußerst vorteilhaft auf die Kosten des Netzbetriebs aus. Glasfaser reift damit zu einer sicheren und wirtschaftlichen Alternative der Übertragungstechnik heran.

2.3.1 Historie

Im Jahre 1966 entwickelte Charles Kao das erste Glasfaserkabel. Die kommerzielle Fertigung begann 1970 mit einem Stufenprofil und 20 dB/km Dämpfung. Bereits 1972 wurde das Kabel so weit verbessert, dass Werte von 4 dB/km erzielt wurden. In den Folgejahren nahm die Entwicklung von Kabeln, Steckverbindungen, Lichtquellen und Detektoren einen stürmischen Verlauf, so dass bereits 30 Jahre später die Technik als weitgehend ausgereift gilt.

2.3.2 Kabelaufbau

Bei Glasfaser wird Licht einer bestimmten Wellenlänge zur Datenübertragung genutzt. Der für das menschliche Auge sichtbare Bereich liegt im Spektrum von 400 – 720 nm. Für die LWL-Technik wird ein Bereich ab 800 nm genutzt, weil es dort drei Bereiche gibt, in denen ein Dämpfungsminimum existiert. Diese sog. Fenster liegen bei 850 nm, 1310 nm und 1550 nm. Eine Ausnahme bildet lediglich die Plastik-LWL-Technik, deren geringste Dämpfung bei 650 nm zu finden ist.



Das Fenster um 850 nm mit einer theoretischen Dämpfung von ca. 2 dB/km wird hauptsächlich für kurze Verbindungen mit kostengünstigen Lasern oder LEDs (Light Emitting Diode) verwendet.

Pro Verbindung werden zwei Fasern – Sende- und Empfangsleitung – benötigt. Glasfasern werden durch den Durchmesser des Faserkerns charakterisiert, in dem sich das Licht ungebrochen ausbreitet und durch den Glasmantel, der dafür sorgt, dass kein Licht aus der Faser austritt. Als Außendurchmesser hat sich eine Größe von 125 μm durchgesetzt, für den Durchmesser des Kerns sind Werte von 50 bzw. 62,5 μm typisch. Alle Glasfasern bestehen aus Substrukturen:

- dem optischen Kern (Core) als Träger des Lichtes aus dotiertem Siliziumdioxid, der einen Durchmesser von 8 μm , 50 μm oder 62,5 μm aufweist und umgeben ist von
- dem optischen Mantel (Cladding) aus hochreinem Quarzglas, der das Licht beugt, es auf den Kern begrenzt und einen Durchmesser von 125 μm besitzt, umgeben von
- einer substraten Ebene (nicht in allen Fasern) aus Glas, die zwar kein Licht transportiert aber den Durchmesser und die Kabelstärke beeinflusst, umgeben von
- dem primary Coating aus Acrylat als erster mechanischer Schutzschicht, umgeben von
- einem secondary Coating, das die relativ empfindliche erste Schicht und den Kern schützt. Der Gesamtdurchmesser der Glasfaser summiert sich somit auf 250 bis 900 μm .

Kern und Mantel bilden eine mechanisch nicht trennbare Einheit. Nur bei PCS-Fasern (Polymer-Cladding-Silicia) bestehen sie aus separaten Schichten.

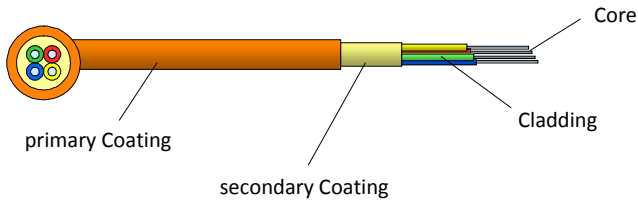


Bild 2.7 Glasfaseraufbau
(Quelle: Kerpen)

2.3.3 Arbeitsweise

Quelle: Kerpen

Glasfaser weist durch die Art des Mediums einige Besonderheiten auf:

- Das Licht wird im Kern geführt; an der Grenzfläche von Kern und Mantel wird es reflektiert. Der Brechungsindex des Lichtes im Kern muss folglich größer als der des Mantels sein.
- Der Einkopplungswinkel des Lichtes als Winkel zwischen Ausbreitungsrichtung des einfallenden Lichtes zur optischen Achse darf einen maximalen Öffnungswinkel nicht überschreiten. Der zulässige Wert kann zwischen 0 und einem Wert liegen, dessen Größe von der lokalen Brechzahl abhängt.
- Die Ausbreitungsgeschwindigkeit des Lichtes verringert sich in Abhängigkeit vom Brechungsindex. Dieser gibt den Faktor an, um den sich die Ausbreitungsgeschwindigkeit des Lichtes in einem Medium im Vergleich zum freien Raum reduziert.

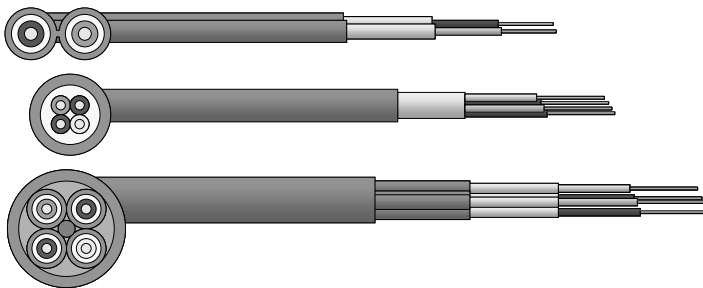


Bild 2.8 Unterschiedliche Glasfaserkabel
(Quelle: Kerpen)

2.3.4 Eingesetzte Technik

Quelle: Kerpen

Eigentlich ist es eher Zufall, dass für Lichtwellenleiter Quarzglas verwendet wird. Jedes andere lichtdurchlässige Material wäre bei entsprechend geringer Dämpfung ebenfalls geeignet. Das zeigt die Verwendung von Polymeren bei Plastikfasern, die preiswerter und einfacher zu fertigen sind, deren Dämpfung aber leider sehr hoch ist. Glas hingegen ist ein sehr reines, zugfestes und elastisches Material, das eine geringe Dämpfung aufweist. Die folgende Tabelle zeigt eine Übersicht von Plastikfasern:

Tabelle 2.2 Plastikfasern

Kürzel	Faserart	Kerndurchmesser
POF	Reine Plastikfaser	980 – 1000 μm
PCS	Glas mit Weichplastik	200 μm
PCF	Glasfaser mit Plastik	verschieden
HCS	Glas mit Hartplastik	50 – 1000 μm

Zur Steigerung der Übertragungsrate für das Glasfasermedium bedienen sich die Entwickler eines physikalischen Tricks. Da sich Licht unterschiedlicher Wellenlänge nicht gegenseitig beeinflusst, werden zukünftig über eine Glasfaser nicht nur Licht einer Wellenlänge (= Farbe, z.B. weiß) verschickt, sondern mehrere Wellenlängen (etwa die Farben blau, grün, rot). Dense Wavelength Division Multiplexing (DWDM) teilt eine einzelne Faser damit in viele „virtuelle“ Verbindungen, von denen jede eine unterschiedliche Wellenlänge darstellt. Da jede Wellenlänge eine bestimmte Datenmenge transportiert, lässt sich der Datendurchsatz der bereits bestehenden Glasfaserinfrastruktur um das n -fache steigern, wobei n der Anzahl der verwendeten Farben entspricht. Da die Zahl der Farben praktisch unbegrenzt ist, sind der Bandbreite kaum Grenzen gesetzt. Fast alle DWDM-Systeme arbeiten mit einer Wellenlänge von 1550 nm. In der Norm G.692 sind Wellenlängen und Kanalabstände definiert. Der typische Kanalabstand, d.h. die Wellenlängenunterschiede zwischen benachbarten Kanälen liegt bei 1,6 oder 0,8 nm. Der Vorteil dieser dichten Anordnung liegt in der Möglichkeit, optische Verstärker einzusetzen, mit denen alle Kanäle simultan auf rein optischer Ebene verstärkt werden können. Kritischer technischer Faktor eines DWDM-Systems ist die Stabilität des Sendelasers. Um eine Wellenlängenkonstanz im Nanometer-Bereich zu erreichen, sind weitgehende elektrische und thermische Stabilisierungen notwendig, die die Komponenten im Vergleich zu Standardlasern aufwändig und teuer machen.

Im Gegensatz zur konventionellen Technik auf Basis von Kupferkabeln erfordert der Einsatz von Glasfaserkabeln neuartige Komponenten und Verbindungstechniken:

- **Verbindungstechnik:** Die Verbindung von Faserenden erfolgt durch die Spleißtechnik, wobei Heiß- und Kaltspleißen unterschieden wird. Beide Faserenden müssen dazu an der Stirnseite genau aufeinanderstoßen, um das Licht verlustarm passieren zu lassen. Nur dann kann eine niedrige Dämpfung garantiert werden. Um diese Anforderung zu gewährleisten, werden spezielle Werkzeuge eingesetzt, sog. Cleaver, die die Faser zunächst anritzen und dann ruckartig auseinanderziehen. Das Zusammenfügen beider Enden erfolgt auf mechanische Weise oder durch relativ hohe Temperaturen. Beim mechanischen kalten Spleißen werden beide Faserenden mittels eines Metallspleißes verbunden, in dem die Fasern in einer V-Nut zusammengepresst werden. Beim Schmelzspleißen erfolgt die Faserverbindung mittels einer Funkenstrecke eines Lasers oder Gasbrenners. Dementsprechend ist diese Technik aufwändig und teuer.
- **Optoelektrische Wandler:** Auf der Einkoppelseite wird ein elektrisches Signal, wie es die Netzkarte erzeugt, in einen Lichtimpuls umgesetzt. Wird die Strahlungsquelle direkt an die Faser angekoppelt, wird eine geringe Leistung (ca. 10 – 15 %) in den Faser-

kern eingekoppelt. Durch eine zwischengeschaltete Optik lässt sich der Strahl wesentlich besser bündeln, so dass sich die Leistung auf 30 % erhöhen lässt. Für eine **Pigtail-Ankopplung**, bei der die Strahlungsquelle unmittelbar mit der Faser verbunden ist, lassen sich grundsätzlich zwei Instrumente verwenden: **LEDs** sind Halbleiter, die unter steuerbaren Bedingungen Licht aussenden. Sie sind preiswert, erzeugen aber ein Licht hoher Strahlungsbreite (hohe Modendispersion) und eignen sich daher nur für kurze Übertragungsstrecken. **Laser** erzeugen stark gebündeltes Licht mit deutlich weniger Eigenwellen und erreichen demzufolge größere Reichweiten. Der Unterschied zwischen der Verwendung von LEDs und Lasern liegt in der Einkopplungsart des Lichtes. LED nutzt die Vollenregung, Laser aktiviert nur wenige Moden. Der Betrieb einer Mehrmodefaser mit LED regt mehrere Hundert Lichtmoden an. Durch das parabelförmige Brechzahlprofil der Gradientenfaser werden die Laufzeitunterschiede zwar auf ein Minimum reduziert, dennoch kommt es auf Grund der Vielzahl der Moden zu einer verhältnismäßig hohen modalen Dispersion. Wird hingegen eine Mehrmodefaser mit einem Laser betrieben, so wird die Lichtleistung mit wenigen Moden im Faserzentrum betrieben, mit der Folge, dass die Dispersion sinkt. Umgekehrt wird beim Empfang eines Signals auf der Auskoppelseite das Licht auf eine Fotodiode geführt, um optische Impulse wieder in elektrische zurückzuverwandeln. Oft werden relativ großflächige Detektoren (ca. 1 mm^2) verwendet, da ihre Ankopplung besonders leicht ist.

2.3.5 Qualitätsparameter

- **Geschwindigkeit und Brechungsindex:** Alle elektromagnetischen Strahlungen breiten sich im Vakuum mit Lichtgeschwindigkeit, d.h. ca. $300\,000 \text{ km/s}$ aus. In einem dichteren Medium wie Glas sinkt die Geschwindigkeit. Dabei laufen kürzere Wellenlängen etwas langsamer als die längeren. Das Verhältnis der Laufzeit zur Lichtgeschwindigkeit ergibt den Brechungsindex, der gemäß dieser Definition von der Wellenlänge abhängig ist. Im Glas beträgt er ca. 1,5, das entspricht einer Ausbreitungsgeschwindigkeit von $200\,000 \text{ km/s} = 20 \text{ cm/ns}$.
- **Modenanzahl und -höhe:** Das eingekoppelte Licht besteht aus vielen Eigenwellen, die als Moden bezeichnet werden. Ein hoher Mode als Ausbreitungsweg des Lichtes im GlasfasermEDIUM – erzeugt durch einen spitzen Einkopplungswinkel des Lichtes – führt zu häufigen Totalreflexionen. Die Signallaufzeit erhöht sich dadurch, wobei gleichzeitig die Signalintensität infolge der Vielzahl von Brechungen stark abnimmt. Da ein einzelnes Signal aus mehreren Moden besteht, erhöht sich die zeitliche Differenz ihres Eintreffens am Faserende, je länger die Entfernung ist. Dieser Effekt wird als **Modendispersion** bezeichnet und fällt umso bedeutender aus, je größer der Kerndurchmesser ist. In Gradientenfasern wird dieser Effekt durch konzentrische Brechzahlen weitgehend kompensiert. Strahlungsquellen besitzen verschiedene spektrale Breiten. Laserdioden sind mit einer Strahlungsbreite von $< 1 \text{ nm}$ viel schmäler als LEDs mit $> 50 \text{ nm}$, so dass allein durch den Unterschied des Einspeisungsmediums Differenzen in der Laufzeit entstehen.
- **Bandbreiten - Längenprodukt:** Die Bandbreite stellt ein Maß für das Dispersionsverhalten und die erzielbare Bitrate in einem Glasfaserkabel dar. Je länger der Impuls durch eine Faser wandert, desto stärker verbreitert er sich und desto größer müssen

die Abstände zwischen den einzelnen Impulsen ausfallen. Deshalb ist es sinnvoll, in die Beurteilung der maximal möglichen Übertragungsfrequenz die Länge zu integrieren. Die Maßzahl drückt aus, dass die Bandbreite umgekehrt proportional zur Länge ist und damit das Produkt aus Bandbreite und Länge konstant bleibt. Die Einheit ist MHz*km. Eine Faser mit 1200 MHz*km kann also eine Frequenz von 1200 MHz über einen Kilometer übertragen bzw. eine Übertragungsfrequenz von 2400 MHz über 0,5 km.

- **Lichtverluste:** Inhomogenitäten der Quarzfaser verändern den Brechungsindex. Auch in den hochwertigsten Glasfasern treten leichte Inhomogenitäten und Verunreinigungen auf. Ein kleiner Teil der Energie des Lichtstrahls wird von diesen Unregelmäßigkeiten des Materials zerstreut, wie Sonnenstrahlen in einem rauchgefüllten Raum. Dieser als **Rayleigh-Streuung** bezeichnete Effekt wächst mit zunehmender Wellenlänge. Darüber hinaus können mechanische Belastungen der Faser den Kerndurchmesser und den Brechungsindex verändern und Strahlungsverluste erzeugen. Hinzu kommen externe Fehler, die auf schlecht polierte oder verschmutzte Faserendflächen und Steckverbindungen zurückzuführen sind.
- **Dämpfung:** Von einer punktförmigen Quelle breitet sich die Strahlung gleichmäßig in alle Richtungen aus. Die Leistung pro Fläche nimmt aber im Quadrat der Entfernung ab. Anders als bei Kupferkabeln fällt mit steigender Wellenlänge die Dämpfung und steigt dann wieder an. Diese Wellenbewegung führt zur Existenz dreier optischer Fenster mit niedriger Dämpfung bei 850 nm, 1310 nm und 1550 nm.



Definition: Leistungsverlust

Die Größe des Leistungsverlustes D bestimmt sich nach der Formel:

$$D = 10 \log(P_1/P_2) \text{ in dB mit:}$$

P_1 = Lichtleistung am Kabeleingang, P_2 = Lichtleistung am Kabelausgang

Die Dämpfung als Minderung der Übertragungsleistung eines Signals über eine Übertragungsstrecke ist von der Wellenlänge abhängig. Sie wird als logarithmisches Verhältnis von Eingangs- zu Ausgangsleistung angegeben und beruht auf zwei Ursachen: der Absorption (ein kleiner Teil wird reflektiert, ein weiterer Rest dringt in die Materie ein) und der Streuung durch Inhomogenitäten (Dichteveränderungen) im Glasfaserkabel. Für die Energieentnahme durch Absorption sind Molekularstrukturen des Basismaterials und Verunreinigungen des Faserkerns verantwortlich. Zusätzlich kann bei starken Biegungen der Totalreflexionswinkel überschritten werden, so dass die Moden in die Mantelhülle reflektiert werden. Die Dämpfung ist damit nicht nur durch die Kabelspezifikation gegeben, sondern kann auch durch fehlerhafte Verlegung oder Produktion verändert werden. Die Lichtsignale erleiden aber nicht nur eine Dämpfung, sondern auch eine Verzerrung. Ausgesendete Lichtimpulse treffen beim Empfänger verschwommen ein, weil die Moden des Signals leichte Laufzeitunterschiede aufweisen.

- **Numerische Apertur:** Der Sinus des Akzeptanzwinkels gibt an, bis zu welchem Grad das Licht auf die Stirnfläche der Faser auftreffen darf, um noch durch den Kern reflektiert zu werden. Je größer er ist und je größer der Kabeldurchmesser ausfällt, desto

mehr Strahlung kann die Faser aufnehmen und führen. Werden zwei Fasern mit unterschiedlicher Apertur zusammengefügt, dann sollte die sendende Faser eine kleinere Apertur und einen geringeren Kerndurchmesser aufweisen.

- **Reflexion:** An der Grenzfläche zweier Medien unterschiedlicher Brechzahl entsteht eine Reflexion. Sie beträgt bei Glas und Luft 3.5 %, was einer Dämpfung von 0,15 dB entspricht. Mit Glas/Luft/Glas wie bei einer Steckverbindung addiert sich dieser Wert zu 0,3 dB (**Fresnel-Verlust**). Bei balliger Politur wird die gesamte Luft zwischen den Faserenden herausgedrückt, so dass der Übergang Glas/Glas fast keine Reflexion mehr erzeugt. In Kombination mit einem Schrägschliff sind die verbleibenden Reflexe so steil, dass sie den Akzeptanzwinkel überschreiten und die Faser verlassen. Ein anderes Mittel gegen Reflexe bei Steckerübergängen ist das Einfügen von Indexpaste. Diese Technik ergibt einen reflexfreien Glas/Gel/Glas-Übergang. Nicht zu vermeiden sind Reflexionen an den freien Enden der Faser d.h. beim Sender oder Empfangen. Das dann rückläufige Signal kann durch Überlagerung zu Störungen führen.
- **Spektrales Dämpfungsfenster:** Die Dämpfung in einer Faser entsteht durch die Rayleigh-Streuung und die Filterwirkung des Kernglases. Für 950, 1200 und 1400 nm existieren Dämpfungsmaxima, dazwischen bei 850, 1300 und 1550 nm liegen Bereiche geringer Dämpfung. Es gelten etwa folgende Richtwerte (für Gradientenfasern): Dämpfung bei 850 nm max. 3,5 dB/km und bei 1300 nm max. 1,0 dB/km. Völlig anders verhalten sich Plastikfasern. Sie weisen zwei Minima mit vergleichsweise hoher Dämpfung bei 660 nm mit ca. 140 dB/km und bei 780 nm mit ca. 300 dB/km auf.
- **Regenerierung:** Auf langen Verbindungen werden die Lichtsignale gedämpft und verzerrt. Zur Überbrückung großer Distanzen müssen die Signale daher regeneriert werden. Drei Möglichkeiten werden dafür unterschieden:
 - „1R“ – Reamplify
 - „2R“ – Reamplify, Reshape
 - „3R“ – Reamplify, Reshape, Retime

Reshaping und Retiming erfolgen nach der opto/elektrischen Umwandlung durch elektronische Schaltungen, für das Reamplifying existieren rein optische Lösungen. Verbreitet ist die Erbium-Variante. Erbium wird dem Siliziumkern der Faser auf einer Länge von einigen Metern beigemischt. Die Erbium-Ionen werden durch eine externe Quelle geladen. Da der geladene Zustand instabil ist, lösen Photonen der eintreffenden Lichtsignale eine Entladung in Lichtform aus und verstärken auf diese Weise das Eingangssignal.

2.3.6 Glasfaserprofile

- **Monomodefaser:** Bei einem Kerndurchmesser von 9 μm kann sich Licht, das eine Wellenlänge von 1,3 μm besitzt, nur noch annähernd gradlinig ausbreiten. Folglich bleiben die qualitätsbeeinträchtigenden Wirkungen gering. Die verwendeten Laser liefern weitgehend „reines“ Licht, so dass die Wirkung der chromatischen Dispersion relativ gering ausfällt. Monomodefasern zeichnen sich durch besondere Qualitätsmerkmale hinsichtlich Dämpfung (weniger als 0,5 dB/km) und Entfernung aus. Das Bandbreiten-Längen-Produkt liegt bei 100 GHz*km. Verglichen mit 1 GHz*km für Multimodefasern

zeigen sich die Vorzüge dieses Kabeltyps. Das primäre Einsatzgebiet ist daher im Weitverkehrsbereich zu sehen.

- **Multimode-Stufenfaser:** Der Glasfaserkern besitzt einen konstanten, aber höheren Brechungsindex als der Mantel, so dass es an der Grenzfläche zu einer Totalreflexion des Lichtes kommt, die diesem Typ ihren charakteristischen „Zick-Zack-Lauf“ des Lichtes verleiht. Der Faser-Durchmesser ist mit $50\text{ }\mu\text{m}$ relativ groß im Vergleich zur Wellenlänge des Lichtes. Diese unterschiedlichen Größenverhältnisse bedeuten, dass im Gegensatz zur Monomodefaser der Effekt der Modendispersion auftritt, mit der Folge, dass das Bandbreiten-Längen-Produkt wesentlich geringer ausfällt. Aufgrund der unterschiedlichen Wege, die die verschiedenen Wellenlängen des Lichtes durch die Faser nehmen, benötigen die einzelnen Moden eine unterschiedliche Zeitspanne, um die Glasfaserstrecke zu durchqueren. Die einzelnen Moden erreichen folglich das Faserende zu unterschiedlichen Zeiten, so dass der Outputimpuls wesentlich länger zur Erkennung eines Signals sein muss, als der Inputimpuls. Dieses als Modendispersion bekannte Phänomen beschränkt die mögliche Anzahl von Lichtimpulsen pro Zeiteinheit und bildet eine Obergrenze für die zu übertragende Bandbreite. Der Kabeltyp eignet sich damit vornehmlich für den Campusbereich. Charakteristisch sind die Außenmaße von 50 und $62,5\text{ }\mu\text{m}$. In Europa dominiert der Kerndurchmesser von $50\text{ }\mu\text{m}$ mit einem Manteldurchmesser von $125\text{ }\mu\text{m}$, in Amerika herrscht die Faser des Typs $62,5/125\text{ }\mu\text{m}$ vor.

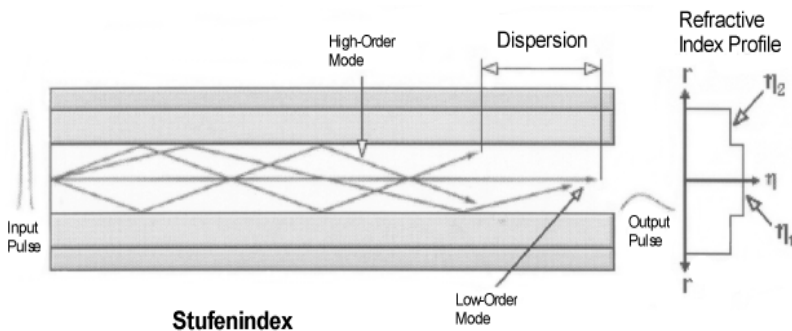


Bild 2.9 Multimode-Stufenfaser

- **Multimode-Gradientenfaser:** Dieser Kabeltyp besitzt einen von der Kernmitte zur Grenzfläche parabelförmig verlaufenden Brechungsindex, so dass sich das Licht sinusförmig im Kern bewegt. Dieses Design nutzt den Effekt aus, dass Moden sich im Bereich eines niedrigeren Brechungsindex schneller als bei einem höheren ausbreiten. Die Laufzeit der unterschiedlichen Moden durch den Faserkern konvergiert folglich, so dass die zeitliche Ausdehnung von Input- und Outputimpuls nahezu übereinstimmen. Damit sinkt die Modendispersion und das Bandbreiten-Längen-Produkt steigt. Dieser Glasfasertyp hat sich zum Standard im Campusbereich entwickelt.

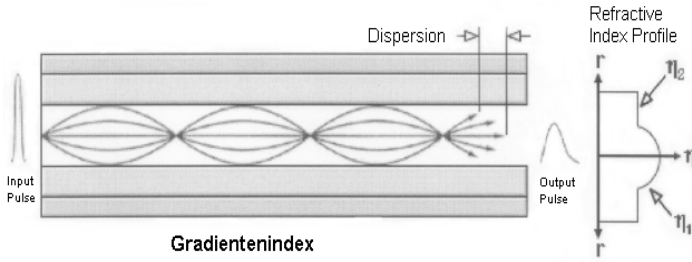


Bild 2.10 Multimode-Gradientenfaser

Eine Gegenüberstellung der einzelnen Glasfasertypen bezüglich der Qualitätsparameter zeigt Tabelle 2.3.

Tabelle 2.3 Vergleich der Glasfasertypen

	Multimode-Stufenfaser	Multimode-Gradienten-faser	Monomodefaser
Reichweite	1 – 2 km	2 – 4 km	> 20 km
Dämpfung	5 dB/km bei 850 nm 3 dB/km bei 1300 nm	2,7 dB/km bei 850 nm 0,8 dB/km bei 1300 nm	1 dB/km bei 850 nm 0,5 dB/km bei 1300 nm
Numerische Apertur	0,29	0,2	0,0

2.3.7 Glasfaserkabelarten

Neben den Fasertypen gibt es bei Glasfaserkabeln noch ein weiteres Unterscheidungsmerkmal und zwar danach, ob die einzelnen Fasern direkt ummantelt sind oder ob sie in einem gelgefüllten Röhrchen einzeln oder mit anderen Fasern zusammen geführt werden. Dabei dient das Coating dem Schutz der Faser vor mechanischen Belastungen über einen Temperaturbereich von $-20\text{ }^{\circ}\text{C}$ bis $+80\text{ }^{\circ}\text{C}$:

- **Vollader:** Alle an das Kabel angreifenden Längs- und Querkkräfte wirken direkt auf die Adern, so dass eine Zugentlastung notwendig wird. Gleiches gilt für Temperaturunterschiede, die ungleich auf Mantel und Faser wirken und ausgeglichen werden müssen. Vor diesem Hintergrund kommt dieser Typ am häufigsten im Tertiärbereich zum Einsatz, insbesondere als Patch- und Anschlusskabel. Für den Außenbereich ist er hingegen ungeeignet.
- **Hohl- oder Bündelader:** Bei diesem Typ verlaufen mehrere Fasern gemeinsam mit Kunststoff umhüllt in einem gelgefüllten Hohlraum, der einen optimalen Schutz gegen Feuchtigkeit und Querkräfte (Nagetierschutz) bietet. Damit ist insbesondere eine Eignung für den Primärbereich gegeben, allerdings verträgt dieses Kabel nur kleine Biegradien und benötigt einen hohen Aufwand beim Spleißen für Steckerverbindungen.
- **Break-Out-Kabel:** Sie vereinen mehrere komplette Volladerkabel durch einen gemeinsamen Kabelmantel und kombinieren quasi die beiden Kabeltypen. Dementsprechend weisen sie einige Vorteile auf, wie die Stressfreiheit der Fasern gegenüber Temperaturschwankungen. Ihr Einsatzgebiet ist bevorzugt der Sekundär- und Tertiärbereich.

2.3.8 Steckverbindungen

Stecker ermöglichen eine lösbare Verbindung zwischen zwei Faserenden und sollten selbst nach vielen Steckvorgängen nur eine geringe Dämpfung aufweisen, möglichst wenig Reflexionen erzeugen, stabil, preiswert und einfach in der Montage sein. Steckerarten gibt es in mehreren Varianten: **zylindrische** bzw. **konische Faserführungen** mit und ohne Berührung der Enden, **Schrägschliff** der Fasern mit und ohne Linsen und Materialien von Keramik über Hartmetall bis Kunststoff. Dabei ist zu beachten, dass Hartmetall und Keramik präziser zu bearbeiten sind als weiche Materialien.

Fast alle Stecker besitzen eine Verdrehsicherung, damit die Faserenden nicht aufeinander reiben. Sie werden durch eine Überwurfmutter oder einen Bajonettverschluss in ihrer Position gehalten. Überwurfmutter können sich bei Vibration lockern und lösen, Bajonethalterungen erfordern einen Federweg. Konische Führungen müssen gut zusammenpassen. Sie sind ungefedert, nicht nachpolierbar und weisen fast immer einen Luftspalt auf. Kleben und Polieren der Faser ist zwar umständlicher, aber stabiler als Ritzen und Brechen.

Die häufigsten Fehlerquellen bei allen LWL-Steckern mit der Folge einer hohen Dämpfung beruhen auf folgenden Ursachen:

- **Stirnflächenabstand:** Um eine konstante Dämpfung bei vielen Steckzyklen zu erreichen, wird ein kleiner Spalt eingehalten, dessen Genauigkeit die Dämpfung entscheidend beeinflusst.
- **Achsenversatz:** Dieser Effekt entsteht bei unpräziser Führung der Fasern in der Kuppelung oder bei zu großer Bohrung, wenn der Kern nicht genau in der Mitte des Mantels liegt.
- **Kippwinkel:** Bei konischen Steckern, die zu lang sind oder sich berühren, kippen die Faserenden gegeneinander.
- **Oberflächenfehler:** Bei schlechter Politur oder nach wenigen Steckzyklen durch Zerreiben von Staub kann es zu Beschädigungen der Faserstirnflächen kommen.
- **Kerndurchmesser:** Werden zwei Fasern mit unterschiedlichem Kerndurchmesser gespleißt oder gesteckt, entsteht ein Dämpfungsverlust, da die Faserenden nicht präzise aufeinander passen.

Prinzipiell lassen sich Steckertypen in drei Kategorien einteilen:



Steckertypen

NC-(non contact) Verbinder: Sie gehören der ersten Generation von Fasersteckern an. Die Faserenden liegen nicht aneinander, sondern sind durch einen Luftspalt getrennt. Ein Vertreter ist der im LAN-Bereich selten anzutreffende SMA-Stecker.

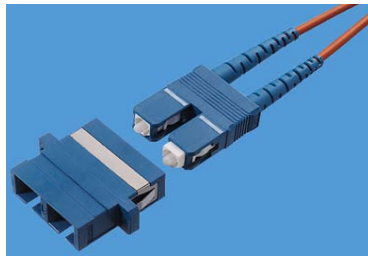
PC-(physical contact) Verbinder: Diese Stecker besitzen Führungsnuten, die die Verbindung nur noch mit einer definierten Winkelstellung erlauben (rüttelfeste Bajonethalterung). Sie werden konvex poliert, so dass die Faserkerne direkt

zueinander in Kontakt kommen (Glas/Politur/Glas) und sind mit einem Federmechanismus versehen, so dass die Verbindung mit hoher Präzision und definiertem Anpressdruck hergestellt werden kann. Bekanntester Vertreter ist der ST-Stecker.

APC-(angled physical contact) Verbinder: Ein rechteckiges Plastikgehäuse mit einem Schnapphalter kennzeichnen diesen Steckeraufbau. Die Endflächen und damit die Faserstirnflächen stehen in einem definierten Winkel zueinander, der bewirkt, dass das von der Fasergrenzfläche zurückgestreute Licht in den Mantel reflektiert wird (Schrägschliff). Typische Vertreter sind FC und SC-Verbindungen.



ST-Stecker



SC-Stecker

Bild 2.11 Steckertypen

2.3.9 Bewertung

Da Glas ein Isolator ist und die Glasfaser ein geschlossenes System darstellt, werden externe Störfelder weder aufgenommen noch abgegeben. Aus diesem Aufbau resultieren eine Menge von Vorteilen. Die Bewertung erstreckt sich auf mechanische, übertragungstechnische und wirtschaftliche Aspekte:

Mechanische Vorteile

- ☺ Kleine Kabeldurchmesser wirken platzsparend bei gleichzeitig geringem Gewicht. Dies macht sich insbesondere beim Management von Patchfeldern bemerkbar.
- ☺ Flexible und handliche Kabel ermöglichen eine einfache Verlegung.
- ☺ Glasfasern weisen eine geringere Brandlast als Kupferkabel auf.

Mechanische Nachteile

- ☹ Das Anbringen von Steckern und das Spleißen ist aufwändig.
- ☹ Im Gegensatz zu anderen Medien sind Biegeradien zu beachten.
- ☹ LWL-Komponenten und hier insbesondere die LEDs unterliegen einem Alterungsprozess.

Übertragungstechnische Vorteile

- ☺ Bei hoher Signaldichte ist eine große Bandbreite erzielbar.
- ☺ Die geringe Signaldämpfung und damit ein geringer Leistungsverlust des Lichtes entlang des Kabels ermöglichen große Übertragungsdistanzen. Da bei Glasfaser die Dämpfung nicht von der Übertragungsrate sondern von der Wellenlänge des Lichtes abhängt, sind Übertragungsgeschwindigkeiten im MBit/s- und GBit/s-Bereich ohne große Dämpfungsverluste möglich.
- ☺ Da keine aktive und passive Beeinflussung der Übertragung durch elektromagnetische Störungen existiert, sind niedrige Fehlerraten, Abhörsicherheit und eine hohe Netzverfügbarkeit gegeben.
- ☺ Beschädigungen durch Überspannungen, statische Entladungen oder Blitzschlag sind nicht möglich.
- ☺ Die Trennung von Sender und Empfänger lässt keine Signalüberlagerung zu.

Wirtschaftliche Vorteile

- ☺ Die Energie- und Betriebskosten eines virtuellen Kanals sind gering.
- ☺ Es sind keine Etagenverteiler erforderlich, da im Gegensatz zu üblichen LAN-Technologien die maximale Netzausdehnung größer ist. Alle aktiven Komponenten gemäß des Collapsed Backbone befinden sich an zentraler Stelle, was das Netzmanagement erleichtert.
- ☺ Durch die große Bandbreite und Übertragungsdistanz ergibt sich eine Flexibilität bei der Gestaltung des Netzaufbaus.
- ☺ Die außergewöhnlich hohe Zuverlässigkeit der Glasfaser verringert die Betriebskosten durch eine Minimierung der Netzausfälle.
- ☺ Die Glasfaser verlängert den Lebenszyklus einer Verkabelung. Damit steigt die Investitionssicherheit der Netzwerkinfrastruktur.

Wirtschaftliche Nachteile

- ☺ Es existiert ein höherer Investitionsbedarf für aktive Komponenten.
- ☺ Die Anbindung analoger Sprachverbindungen ist aufwändig.
- ☺ Der Konfektionierungsaufwand ist abhängig vom Steckertyp.
- ☺ Die Bestimmung des Dämpfungsbudgets ist schwierig.

■ 2.4 Twisted-Pair-Verkabelung

Twisted-Pair ist die generelle Bezeichnung für Kupferkabel mit einem oder mehreren verdrehten Leitungsparen. Ursprünglich wurde dieser Kabeltyp im Fernmeldebereich eingesetzt. Der Durchbruch in die Computerwelt kam zu Beginn der 80er Jahre als ein Ersatz für die teuren Koaxialkabel gesucht wurde. Die wachsende Leistungsfähigkeit machte es

bald notwendig, Twisted Pair in Bereiche zu untergliedern, um den Netzbetreibern die Entscheidung bei der Wahl der angemessenen Kabel zu erleichtern.

Fast alle Dienste benötigen zur Signalübertragung zwei Paare, d. h. vier Adern: ein Paar für das Senden, das andere für den Datenempfang. Um eine Störung der Signale auf den Leitungsparen zu verhindern, sind die Adern symmetrisch gegeneinander verdreht. Dadurch neutralisieren sich die elektromagnetischen Felder, die von stromleitenden Adern ausgehen, weitgehend. Der Grad der Verdrehung wird durch die Schlagzahl pro Längeneinheit angegeben.

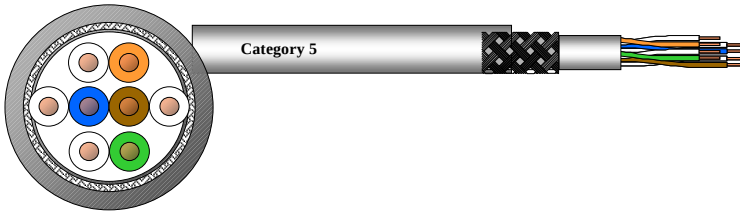


Bild 2.12 Aufbau eines Kupferkabels mit 8 Adern

Quelle: Kerpen

Bei der Übertragung digitaler Signale gibt es eine Vielzahl von Merkmalen, die die Qualität des Kabels bestimmen. Hochfrequenz-Eigenschaften wie Wellenwiderstand, Rückflussdämpfung, Nebensprechdämpfung und Rauschabstand sind die wichtigsten Faktoren. TP-Kabel werden grundsätzlich nach zwei Kriterien unterschieden: geschirmt oder ungeschirmt. Geschirmte TP-Kabel gibt es mit einer gemeinsamen Abschirmung (S-UTP), die als Mantel alle Adern umschließt, mit einer Einzelabschirmung für jedes Adernpaar (STP) und mit einer Kombination aus Einzelabschirmung und gemeinsamer Abschirmung um alle Adern (S-STP):

Tabelle 2.4 Twisted-Pair Kabeltypen

Kabeltyp	Beschreibung
STP 100 Ω	paarweise geschirmtes Kabel mit einem Gesamtschirm aus Metallgeflecht. Beispiel: IBM Typ N-Kabel
FTP 100 Ω (Foiled-TP)	Aufbau wie STP 100 Ω , jedoch mit einer äußeren Gesamtabschirmung aus aluminiumbeschichteter Kunststoffolie. Bevorzugter Typ für Kabel der Kategorien 6 und 7
S/UTP 100 Ω	keine Schirmung für die einzelnen Adernpaare, wohl aber eine Gesamtschirmung aus Metallfolie und/oder Metallgeflecht
UTP 100 Ω	Kabel ohne jede Schirmung der Adernpaare

2.4.1 Qualitätsparameter

Mehrere Eigenschaften spiegeln die Leistungsfähigkeit der Kupferkabel wider. Für die Wahl von symmetrischen Kabeln spielen insbesondere Widerstand und Dämpfung eine entscheidende Rolle:

- **Wellenwiderstand:** Dieses Maß ist neben dem mechanischen Aufbau vor allem von der Übertragungsfrequenz abhängig. Gute Übertragungsergebnisse werden bei einem homogenen Widerstand nahe 100Ω erreicht.
- **Dämpfung:** Ein elektrisches Signal erfährt im Zuge seiner Ausbreitung über ein Medium Leistungsverluste. Das bedeutet, dass das empfangene Signal kleiner als das gesendete ist. Diese Einbußen werden in erster Linie vom Widerstand und dem Isolationsmaterial bestimmt. Ziel ist es, diese Verluste möglichst gering zu halten, um eine große Übertragungsentfernung zu gewährleisten. Die Berechnung der Dämpfung D erfolgt nach der Formel:



Dämpfungsberechnung

$$D(L) = -20 \times \log (|U_{\text{ein}}| / |U_{\text{aus,L}}|)$$

mit: U_{ein} Spannung am Leitungseingang

$U_{\text{aus,L}}$ Spannung am Leitungsausgang der Leitung der Länge L

Der Dämpfungswert wird in dB/100 m oder dB/km angegeben, da die Dämpfung mit der Länge des Kabels wächst.

- **Nebensprechen:** Dieser Vorgang beschreibt einen unerwünschten Leistungsübergang von einem Adernpaar auf ein anderes. Das Übersprechen entsteht auf der gesamten Länge der Übertragungsstrecke und ist eine Folge unvermeidlichen Kapazitätsbelags im Kabel. Die Messung erfolgt an beiden Enden der Übertragungsstrecke.
- **Nahnebensprechdämpfung (NEXT):** Der Wert bezeichnet das Leistungsverhältnis zwischen Eingangssignal (TX) und dem am nahen Ende gemessenen Übersprechen (Nah). Je höher die Signalfrequenz ist, desto größer ist das Übersprechen:



$$NEXT[\text{dB}] = -10 \times \log (Nah/TX) \text{ in dB/km}$$

- **Attenuation to Crosstalk Ratio (ACR):** Der ACR-Parameter setzt die beiden Werte NEXT und Dämpfung ins Verhältnis. Ist die Dämpfung des Nutzsignals gleich oder größer der Dämpfung des Übersprechens, so kann der Empfänger das Signal nicht mehr vom störenden Übersprechen trennen.
- **Ausbreitungsgeschwindigkeit des Signals:** Das elektrische Signal breitet sich in einem Kupferkabel wie eine Welle aus:



$$V = a \times c$$

mit: c Lichtgeschwindigkeit = 300 000 km/s

a Nennausbreitungsgeschwindigkeit

Der Parameter a hat unmittelbare Auswirkungen auf die maximale Ausdehnung von LANs.

- **Induktivität:** Dieser Effekt tritt in jedem stromdurchflossenen Leiter auf und bewirkt eine lineare Verzerrung des Signals. Der Wert steigt mit zunehmendem Abstand der Adern eines Paares und sinkt mit zunehmendem Leiterquerschnitt sowie Abstand des Schirms. Der Abstand der Adern eines Paares kann dabei durch die Dicke der Isolationsmaterialien beeinflusst werden.
- **Kapazität:** Auch dieser Parameter führt zu Signalverzerrungen und ist abhängig vom Abstand der Adern. Jedoch steigt die Kapazität mit sinkendem Abstand. Dieser Umstand zeigt, dass die Forderung nach geringer Induktivität und gleichzeitig abnehmender Kapazität einen Kompromiss beim Abstand der Leiter voneinander fordert. Im Gegensatz zur Induktivität besitzt die Wahl des Isolationsmaterials einen entscheidenden Einfluss auf die Kapazitätseigenschaft. Brandverhalten, Verarbeitungsmöglichkeiten, Langzeitstabilität und Materialfestigkeit schränken die Auswahl erheblich ein.
- **Maximale Bitrate:** Die Übertragungskapazität eines Übertragungsmediums C ist nicht unendlich, sondern nach einem Gesetz von Shannon durch den Störabstand SNR und die Bandbreite B begrenzt: $C = B \times \log_2(1 + SNR)$
Nach dieser Gesetzmäßigkeit ist die gleiche Bitrate auch durch eine Steigerung der Bandbreite bei Verringerung von SNR zu erzielen.
- **Minimaler Biegeradius:** Dieser Parameter spielt für das Verlegen eine große Rolle, denn beim Biegen oder Knicken verändert sich der Adernabstand und damit die elektrische Eigenschaft des Kabels. Eine Verringerung des Adernabstandes induziert einen wachsenden Wellenwiderstand und eine abnehmende Übertragungsenergie und folglich eine „Fehlinterpretation“ der Signale.

Neben der Betrachtung der Schlüsseleigenschaften stellt sich bei jeder Verkabelung auch die Frage nach einer optimalen Schirmung. Dabei besteht für Kabel mit einer hochfrequenten Übertragung die Wahl zwischen Kabeln mit Folienschirmung (Pimf-Kabel = paarweise in Metallfolie) oder einer Kombination aus Folie und Geflecht. Die konstruktiven Unterschiede zwischen Folien- und Geflechtsschirm bewirken ein unterschiedliches Schirmungsverhalten. Während sich eine Folie besser zur Abschirmung von hohen Frequenzen eignet, zeigt ein Geflechtsschirm bei niedrigen Frequenzen die bessere Wirkung. Den idealen Schutz bietet folglich die Kombination aus beiden. Eine Schirmung besitzt allgemein den Vorteil, dass elektromagnetische Felder, die durch die Stromführung in den Adern entstehen, sich nicht über andere Leitungspaare ausdehnen. Andererseits bieten sie auch Schutz gegen äußere Störfelder. Geschirmte Kabel sind wesentlich stabiler und umfeldunabhängiger als ungeschirmte.

Aber nicht nur die geschirmten TP-Kabel stehen im Blickpunkt, auch im Bereich ungeschirmter Kabel hat sich eine stürmische Entwicklung vollzogen. Derzeit haben in Europa UTP-Kabel einen Marktanteil an Neuverkabelungen von 50 %, weltweit sogar 75 %. Dies ist vor allem darauf zurückzuführen, dass mit ihnen auch Gigabit-Ethernet-Übertragungen möglich sind.

2.4.2 EIA/TIA-568-Standard

Um ein einfaches und herstellerübergreifendes System zur Qualitätsbestimmung von Netzkabeln einzuführen, hat sich ein Standard herausgebildet, der Grenzwerte für den Wellenwiderstand, die Dämpfung und das Nahnebensprechen vorschreibt. Diese Norm – als EIA/TIA 568 (Electronic Industries Association/Telecommunications Industry Association) Titel: Commercial Building Wiring Standard bekannt – beschränkt sich ausschließlich auf die Tertiärebene der strukturierten Verkabelung (Wiring Closet). Ihr Ziel ist die Sicherstellung diensteneutraler Anforderungen. Dabei finden insbesondere die Eigenheiten des amerikanischen Marktes Berücksichtigung. Für die vier grundsätzlichen Kabelarten, die zwischen Endgeräten und Etagenverteiler verwendet werden können – Koaxial-, STP-, UTP- und Glasfaserkabel – werden sieben Anwendungsklassen: Category 1 bis 7 unterschieden. Dabei ist wichtig, dass alle Komponenten des Verkabelungssystems die Ansprüche der Anwendungsklasse erfüllen. Zum System gehören neben dem Kabel auch Waddosen, Patchkabel, Steckverbindungen und Verteilerschränke.

Die Pinbelegung der 8 Adern eines Twisted-Pair-Kabels nach dem Standard TIA568A folgt einem festen Prinzip. Die orangefarbenen und grünen Adern senden und empfangen Daten, blaue und braune Adern dienen als Reserve für höhere Bandbreiten. Ab dem Gigabit-Ethernet-Standard werden alle acht Adern für Übertragungszwecke genutzt. Die Streifen der Adern zeigen darüber hinaus die Polarität an. Gestreifte Adern sind positiv, einfarbige negativ.

Pin	Ader-Farben
1	weiß/grün
2	grün
3	weiß/orange
4	blau
5	weiß/blau
6	orange
7	weiß/braun
8	braun

Bild 2.13 Pinbelegung für TIA568A

Der Standard TIA568B besitzt eine geringfügig veränderte Adernfolge. Hier gilt die Adernzuordnung: orange gestreift, orange, grün gestreift, blau, blau gestreift, grün, braun gestreift, braun. Ein Vergleich zeigt, dass die grünen und orangefarbenen Adern vertauscht sind.



Eine Fehlerquelle besteht in der gleichzeitigen Verwendung beider Standards TIA568A und TIA568B. Für eine einwandfreie Funktion müssen beide Kabelenden den gleichen Anschlussstandard verwenden.

Jede Kabelader muss mit einem bestimmten Kontakt des Steckers verbunden werden. Im TP-Umfeld hat sich der RJ-45 Stecker als Standard durchgesetzt.



Bild 2.14 RJ-45 Stecker

2.4.3 ISO/IEC-Standard 11801 und EN 50173

Bezieht sich die Definition nicht nur auf die Kabel, sondern schließt die gesamte Übertragungsstrecke mit Steckern und Anschlussdosen ein, wird nicht mehr von Category, sondern von Klasse gesprochen. Dabei entspricht Klasse D der Category 5, Klasse E der Category 6 und Klasse F der Category 7. Als weltweiter Standard jenseits der speziellen Gegebenheiten des US-Marktes entstand auf der Grundlage des EIA/TIA 568-Standards ein Vorschlag der ISO/IEC (International Electrotechnical Commission) mit dem Titel: „Customer Premises Cabling“, der durch die CENELEC (Comite Europeen de Normalisation Electrotechnique) im Juli 1995 in die EN 50173 umgesetzt und als DIN EN 50173 unter der Überschrift „Leistungsanforderungen an strukturierte Verkabelungsschemata“ auf deutsche Verhältnisse übertragen wurde. Dieses Konzept beschreibt die Leistungsanforderungen für:

- die Topologie der Verkabelung
- die Spezifikation der Kabel und der Anschlusstechnik
- die Leistungsfähigkeit der Übertragungsstrecke
- die Prüfverfahren.

Die zugrunde liegenden Prüfverfahren beziehen sich auf die Spezifikation TSB-67 als Teil des EIA/TIA-Standards. Diese legt alle elektrischen Parameter von Netzkabeln bis zur Category 5 und die Genauigkeit der Testgeräte fest. Ferner enthält sie Angaben dazu, was genau zu einer Verkabelung gehört und welche Komponenten nicht mehr das Ergebnis beeinflussen.

Die Angaben für Kabel und Anschlusstechniken beziehen sich auf die durch die EIA/TIA 568 vorgegebenen Kategorien 1 bis 5, erweitert um entsprechende Werte für die gesamte Übertragungsstrecke (Link). Angepasst für ISO/IEC 11801 bzw. EN 50173 können die Anwendungsklassen A bis F folgendermaßen beschrieben werden:

Tabelle 2.5 Anwendungsklassen

Anwendungs- klasse	Beschreibung
Klasse A	Diese Klasse ist für Sprach- und andere Niederfrequenzübertragungen mit Frequenzen bis maximal 100 KHz gedacht. Hierunter fallen Nebenstellenanlagen und ISDN CCITT X.21 und S ₀ -Anschlüsse.
Klasse B	Anwendungen mit mittleren Datenraten bis 1 MHz Bandbreite fallen in diese Klasse. Dazu gehören in erster Linie Telefondienste.

Tabelle 2.5 Anwendungsklassen (Fortsetzung)

Anwendungs- klasse	Beschreibung
Klasse C	Diese Kategorie ist für Anwendungen mit hohen Bitraten bei kurzen Entfernungen bis zu einer maximalen Frequenz von 16 MHz spezifiziert. Kandidaten hierfür sind alle konventionellen LAN-Technologien.
Klasse D	Diese Klasse beschreibt Anforderungen für eine maximale Bandbreite von 100 MHz. Damit werden zwar viele LAN-Technologien erfasst, Hochgeschwindigkeitstechniken liegen aber jenseits des Definitionsbereichs.
Klasse E	Normvorschlag der ISO/IEC für 200 MHz auf Basis von RJ-45 Steckverbindungen, die zu Category 5 kompatibel sind.
Klasse F	Normvorschlag der deutschen Sektion der ISO mit Frequenzen bis zu 600 MHz auf der Basis neuer Stecker.

Die Beziehung der Anwendungsklassen ISO/IEC 11801 zu den Übertragungsmedien gemäß TIA/EIA 568A zeigt Tabelle 2.6.

Tabelle 2.6 Anwendungsklasse und Kategorie

Kategorie	Category 5	Category 5e	Category 6	Category 7
Klasse	D	D+	E	F
Bandbreite	100 MHz	100 MHz	200 MHz	600 MHz
Reichweite	100 m	100 m	100 m	100 m
Stecker	RJ-45	RJ-45	RJ-45	GG45



Ein allgemeines Problem der Verkabelung stellt die Ähnlichkeit zwischen alten und neuen Standards dar. Category 5 oder Klasse D Kabel, die zwischen 1995 und 1999 produziert wurden, erfüllen die Bedingungen nach TSB67. Die nach dem ab 1999 geltenden Standard TSB95 hergestellten Kabel erfüllen strengere Anforderungen. Aus der Kennzeichnung der entsprechenden Kabel ist dieser Unterschied oft nicht ersichtlich.

Ähnliches gilt für die Category 6 oder Klasse E Kabel. Die Differenz in den definierten Parametern betrifft insbesondere den Übergang zu Category 6A bzw. Klasse E_A.

Die EMV (Elektro-Magnetische Verträglichkeit) stellt ein Problem für Kupferkabel dar. Der Inhalt von Gesetzen (EMVG, Bundesgesetzblatt 1992, Teil I) könnte vermuten lassen, dass die Verkabelung selbst ein unkritischer Faktor ist. In der Theorie sorgt zwar die Verdrillung der ungeschirmten Twisted-Pair-Kabel dafür, dass sich die EMV-Wirkung der einzelnen Adern gegenseitig aufhebt, Störungen in der Symmetrie der Verdrillung können in der Praxis jedoch dazu führen, dass die Schutzanforderungen nicht mehr eingehalten werden können. Ein Ausweg besteht nur in der Verwendung gut geschirmter Kabel. Da die UTP-Kabel im Gegensatz zum geschirmten Kabel kein geschlossenes System bilden, können

nennenswerte Nebensprechwirkungen auf benachbart liegende Kabel auftreten. Dieser als **Impulse Noise oder Random Noise** bezeichnete Effekt hängt im Wesentlichen von der Schlaglänge der Paare ab und lässt sich durch eine Wahrung des Abstandes zu anderen elektrischen Quellen reduzieren.

Alle Gigabit-Verfahren übertragen die Signale bidirektional auf allen vier Paaren. So werden unter Gigabit-Ethernet durch das PAM-5-Schema (pulse-amplitude modulation) 250 Mbit/s über jedes Paar transferiert. Damit werden aber auch die Qualitätsparameter der bisherigen zwei-paarigen Übertragungen irrelevant. Die Arbeitsgruppe der ISO/IEC und das EIA/TIA als Anwenderkonsortium bemühen sich daher, neue Grenzwerte für kritische Parameter zu definieren:

- **PS-Next (power sum near-end-crosstalk)** misst den kumulativen Effekt von Next auf alle vier Adernpaare. PS-Next wird für jedes Paar auf der Grundlage des Next-Effektes auf die anderen drei Paare bestimmt.
- **PS-ACR (power sum attenuation-to-crosstalk ratio)** gibt in dB an, um wie viel das Datensignal auf dem einen Paar stärker ist als das Rauschen auf den verbleibenden drei Paaren sein darf.
- **Rückflusssämpfung** gibt Aufschluss über die Kabelgüte hinsichtlich der Signalreflektion. Da das Eingangssignal und der reflektierte Anteil entgegengesetzte Ausbreitungsrichtungen aufweisen, ist das Verhältnis zwischen Sendesignal und reflektiertem Anteil negativ.
- **Propagation Delay** beschreibt die Zeitspanne in ns, die eine Signalausbreitung für 100 m benötigt.
- **Delay Skew** misst die Differenz der Signalausbreitung in ns zwischen dem schnellsten und langsamsten Kabelpaar. Ein Unterschied entsteht durch die Verdrillung der Kabel, die zur Unterdrückung von Störeinflüssen für jedes Paar individuell ist oder durch die Verwendung unterschiedlichen Isoliermaterials.
- **Fernnebensprechdämpfung FEXT:** Da sich das Übersprechen entlang der gesamten Kabellänge ausbreitet, entsteht auch am Ende der Übertragungsstrecke ein Effekt. Aufgrund der Dämpfung ist der Fernpegel jedoch wesentlich niedriger als der Nahpegel.

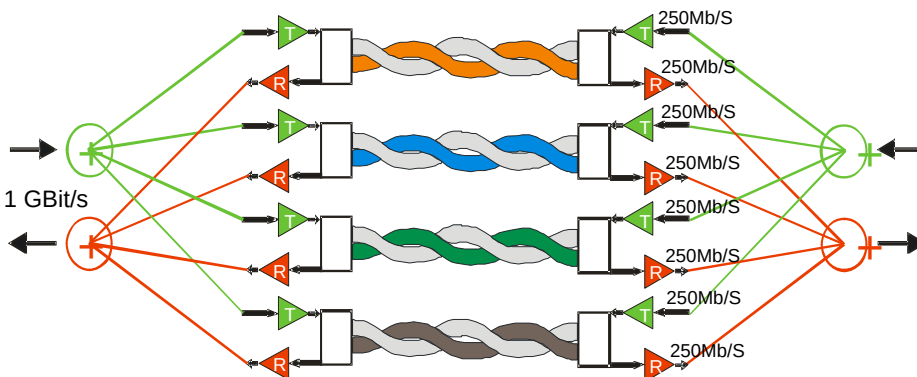


Bild 2.15 PSNEXT bei Gigabit-Ethernet

- **Alien Crosstalk:** Die größte technische Herausforderung bei der Übertragung von 10GBase-T war die Unterdrückung bzw. das Vermeiden des Alien Crosstalk. Durch das aufwändige PAM16-Kodierungsverfahren bei 10G-Ethernet ergeben sich wesentlich kleinere Spannungsunterschiede zwischen den einzelnen logischen Zuständen als beispielsweise bei 100Base-T. Dies führt zu einer deutlich höheren Empfindlichkeit des Signalwegs gegenüber eingekoppelten Störsignalen. Störsignale auf dem Signalweg der betreffenden Übertragungsstrecke können insbesondere durch benachbarte Datenkabel- oder Steckverbinder hervorgerufen werden, aber auch durch systemfremde Quellen.

2.4.4 Bewertung

Die Bewertung erstreckt sich wie bei Glasfaser auf mechanische, übertragungstechnische und wirtschaftliche Aspekte:

Mechanische Vorteile

- ☺ Flexible und handliche Kabel ermöglichen eine leichte Verlegung.
- ☺ Das Anbringen von Steckern ist einfach.

Mechanische Nachteile

- ☹ Ein höherer Aufwand entsteht durch notwendige bautechnische Maßnahmen. Im Gegensatz zur Glasfaser müssen bei Kupfer und dessen EMV-Anfälligkeit Kabel und Stromleitungen gesondert verlegt und gegeneinander abgesichert werden.
- ☹ Brandschutzmaßnahmen verursachen weit höhere Kosten als bei Glasfaserkabeln, die ohne metallische Komponenten gegenüber Feuer unempfindlicher sind.
- ☹ Kupferkabel sind nur für eine bestimmte Zuglast ausgelegt. Werden die Grenzwerte etwa beim Verlegen überschritten, drehen sich Kabel teilweise auf, was zu einer Veränderung der elektrischen Eigenschaften führt.

Übertragungstechnische Vorteile

- ☺ Bei Ethernet-Installationen unterstützt der Autosensing-Mechanismus die Erkennung der Übertragungsgeschwindigkeit. Aufgrund der Komplexität der unterschiedlichen optischen Fenster und anderer Parameter ist dies bei Glasfaser nicht möglich.

Übertragungstechnische Nachteile

- ☹ LWL-Kabel lassen größere Bandbreiten als Kupferkabel zu.
- ☹ Eine hohe Signaldämpfung durch eine schlechte Leitfähigkeit verursacht Leistungsverluste.

Wirtschaftliche Vorteile

- ☺ Das Kabel und die aktiven Komponenten sind preiswert.
- ☺ Daten- und Telefonverkehr können über eine Verkabelung geführt werden, während der Telefonverkehr über Glasfaser teurere elektro/optische Wandler an der Benutzerschnittstelle erfordert.

- ☹ Der Investitionsschutz der Verkabelung ist weitgehend sichergestellt. Mittlerweile unterstützen alle LAN-Technologien Twisted-Pair-Kabel als Übertragungsmedium.

Wirtschaftliche Nachteile

- ☹ Die Investitionssicherheit für zukünftigen Technologien z.B. 100G-Ethernet ist nicht gegeben, da aufgrund des physikalischen Aufbaus der Leistungsfähigkeit Schranken gesetzt sind.
- ☹ Die Längenrestriktion der LAN-Technologien erfordert oftmals zusätzliche Etagenverteiler.

Neben diesen Aspekten sind aber auch noch andere Faktoren von Bedeutung. So besteht in einigen EU-Ländern und in den USA eine große Präferenz für UTP-Kabel aufgrund ihrer weiten Verbreitung und ihrer bisherigen Nutzung als Telefonkabel. Ihre Verwendung auch für die Vernetzung senkt die Installations- und Investitionskosten in die Infrastruktur beträchtlich.



Patchpanel sind ein Mittel, um Kabel und Kabelverbindungen in einem Schrank zu organisieren. Die von den Wandanschlüssen kommenden Kabel werden hinten in den Patchpanels gesteckt und mit kurzen Patchkabeln anschließend von vorn separat mit den Anschlüssen der Netzwerkgeräte verbunden. Dieses Vorgehen vereinfacht es, die Verbindungen zwischen zwei Geräten zu verändern. Um eine Verbindung zu modifizieren, bedarf es nur eines Umsteckens des Patchkabels auf der Vorderseite des Panels.



Noch Fragen ...? Ja ...

Was ist eigentlich „Dark Fiber“?

Bei Dark Fiber handelt es sich um eine vorhandene, aber unbenutzte Glasfaserinfrastruktur, die von Anwendern gemietet werden kann. Zukünftige Nutzer müssen daher die optischen Komponenten selbst hinzufügen.

■ 2.5 Zusammenfassung

Kupfer- und Glasfaserverkabelungen besitzen unterschiedliche Charakteristika hinsichtlich technischer Faktoren, Geschwindigkeit und Kosten. Die Wertung dieser Merkmale ist notwendig, um in konkreten Fall eine Entscheidung für einen Verkabelungstypen zu treffen. Häufig ist mit dieser Entscheidung zusätzlich eine Architekturvorgabe verknüpft, deren Beachtung das Layout und die Zukunftsfähigkeit des Netzes festlegen.

Die Bedeutung der Verkabelung schlägt sich in neuen Normen und der ständigen Anpassung bestehender Vorgaben nieder. Ende 2007 wurde die EN 50173 unter dem Titel „Informationstechnik – anwendungsorientierte Kommunikationskabelanlage“ verabschiedet. Teil 1 nimmt auch die Singlemode-Faser OS2 und Kunststofffasern (POF: Polymer-Optical-

Fiber) auf, die für Wellenlängenmultiplexing (CWDM) geeignet sind. Damit erweitert sich der Anwendungsbereich der OS2-Fasern vom WAN- auf den LAN-Bereich.

Im Sekundärbereich kommen seit einiger Zeit verstärkt laseroptimierte Fasern (OM3) zum Einsatz. Diese ermöglichen kostengünstige Verbindungen bis 300 m, bei denen VCSEL-Dioden (Vertical Cavity Surface Emitting Laser) die 10-GBit/s-Signale erzeugen. Die OM3-Faser ist für die Wellenlänge von 850 nm optimiert.

Neue Technologien bedeuten zumeist auch neue Steckertypen und neue Qualitätsparameter für die eingesetzte Verkabelung. Damit besteht immer auch eine Wechselwirkung zwischen technologischem Fortschritt und dessen Umsetzung in physikalischen Komponenten.

■ 2.6 Wissensüberprüfung

1. Welche Strukturbereiche unterscheidet die strukturierte Verkabelung?
2. Welches Medium wird am wenigsten durch elektromagnetische Störungen beeinträchtigt?
3. Entspricht ein Distributed Backbone der strukturierten Verkabelung?
4. Welchen Mechanismus nutzt die asynchrone Übertragung zur Taktsynchronisation?
5. „Die Modenanzahl beeinträchtigt die Reichweite der Glasfaser“. Stimmen Sie zu?
6. Aufgrund welcher Eigenschaft wird der Informationsgehalt von Zeichen gemessen?
7. Welche Modulationsarten gibt es?
8. Geben Sie einen Überblick über Fehlerquellen bei LWL-Steckverbindungen.
9. Lässt sich IP-Telephonie über Glasfaserkabel abwickeln? Diskutieren Sie!
10. Welche Qualitätsparameter bei Twisted-Pair-Kabeln werden üblicherweise verwendet?

3

Ethernet-Technologie

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Welche Varianten von Ethernet sind gebräuchlich?
- Welche Bedeutung besitzen die Felder eines Ethernetrahmens?
- Welches sind die Merkmale von Ethernet bezüglich der Schicht 1 und 2?
- Was ist die Funktion und die charakteristische Methode des Medienzugriffs bei Ethernet?
- Welche Eigenschaften machen Ethernet zur weit verbreitetsten LAN-Technologie?

Kapiteleinführung

Ethernet ist eine Familie von Standards für LANs unter dem Schirm der IEEE. Die Technologie hat sich gegen mehrere Mitbewerber wie Token Ring oder Apple Talk durchgesetzt. In Zuge dieses Prozesses entstanden unterschiedliche Varianten hinsichtlich der genutzten Medien und der unterstützten Geschwindigkeit. Eines hat sich jedoch nicht verändert: das Rahmenformat. Hierin liegt einer der Gründe für den Erfolg von Ethernet. Unabhängig von der konkreten Implementierung blieb die Basistransporteinheit konstant. Diese Konstanz bildet die Voraussetzung für eine nahtlose Migration zwischen den einzelnen Varianten gepaart mit einer automatischen Erkennung der jeweiligen Geschwindigkeit. Die folgenden Abschnitte zeichnen die Entwicklung nach und geben einen Überblick über die herausragenden Merkmale.

■ 3.1 Historie

Ethernet ist die weltweit am häufigsten installierte LAN-Technologie. Sie beantwortet die Frage, wie einzelne Stationen des Netzwerkes Zugang zu dem sie verbindenden Medium erhalten, wie sie sich untereinander abstimmen und in welchen Informationseinheiten sie Nachrichten austauschen. Die Einfachheit der Installation, die Flexibilität und die Vielseitigkeit der Technologie machten Ethernet in kurzer Zeit zum Schlüssel der Kommunikation im lokalen Bereich.

Ethernet wurde Anfang der 70er Jahre entwickelt und als IEEE 802.3-Standard bekannt. Die Arbeitsgruppe P802 des IEEE beschäftigt sich in zahlreichen Untergruppen mit allen Aspekten der LAN-Technologie.

Tabelle 3.1 IEEE-Standardisierungsgruppen

802.0	802.2						802.10
Overview,	Logical Link Control						SILS
Architecture,	ISO 8802-2						1992
Management	1989						
	802.1						
	MAC Bridging						
	802.3	802.4	802.5	802.6	802.11	802.12	802.14
	CSMA/CD	Token Bus	Token Ring	MAN	WLAN	Demand Priority	CATV
	ISO 8802-3	ISO 8802-4	ISO 8802-5				
	1990	1990	1990				

Die Wurzeln des Ethernets liegen in Hawaii. Die dortige Universität baute Anfang der 70er Jahre ein Funknetz auf, um für die Inselgruppe eine Kommunikationsplattform zu schaffen. Robert Metcalfe, damals noch Student und späterer Gründer der Firma 3Com, verfeinerte das einfache Verfahren und prägte in Anlehnung an die ursprüngliche Übertragung via Äther den Namen Ethernet. Das Ethernet ähnelt in seiner Funktionsweise der Funktechnik, die Informationen in ein homogenes, passives Medium entlässt. Ohne Intelligenz auf dem Übertragungsweg übernehmen die Endstationen die Verarbeitung. Am 22.5.1973, so die Legende, notierte Metcalfe erstmals den Begriff Ethernet in einem Entwurf. Damals arbeitete er in den Forschungslabors des Xerox Palo Alto Research Centers an dem Problem, Workstations mit Laserdruckern zu verbinden und griff dazu auf die Prinzipien des Alohanet (Netz auf Hawaii) zurück. 1976 veröffentlichte Metcalfe erste Ergebnisse in der Literatur.

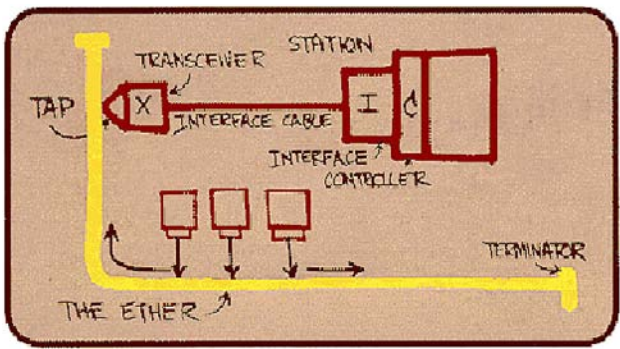


Bild 3.1 Ethernetentwurf von Metcalfe

Daraufhin trat DEC 1979 an Metcalfe mit der Bitte heran, ein LAN-Verfahren zu entwerfen, das die Xerox-Patente nicht berührte. Metcalfe erreichte jedoch, dass Xerox in die Entwicklung einbezogen wurde. Zusammen mit der Firma Intel formte sich schließlich die DIX-Gruppe (DEC, Intel, Xerox), die das 3 MBit/s Experimentiernetz von Xerox schnell auf die Ethernet Version 1.0 umstellte. Die weitere Ethernet-Geschichte gibt gleichzeitig einen Einblick in die Entwicklung von Netzwerken generell:

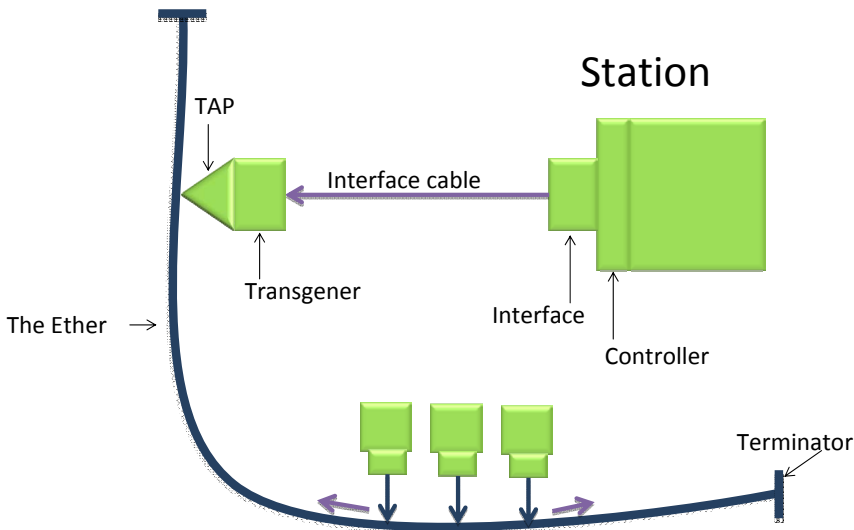


Bild 3.2 Ethernetentwurf

Tabelle 3.2 Ethernethistorie

Jahr	Ereignis
1973	Die Firma Xerox entwickelt den Prototypen eines Kommunikations-Controllers mit der Übertragungsrate von 3 Mbit/s.
1976	Ethernet wird erstmals der Öffentlichkeit vorgestellt.
1979	Die Entwickler R. Metcalfe (Xerox-PARC) und G. Bell (DEC) entwickeln Ethernet zu einem LAN-Standard weiter.
1980	Ein Konsortium der Firmen DEC, Intel und Xerox, die sog. DIX-Gruppe, veröffentlicht die erste Ethernet-Spezifikation: Ethernet Version 1.
1982	Das IEEE nimmt die Idee des Ethernet in die neu gegründete Arbeitsgruppe 802.3 auf und erarbeitet die neue Spezifikation mit dem CSMA/CD-Verfahren für das „gelbe“ Kabel: Ethernet Version 2.
1983	Arbeiten an der Cheapernet-Variante beginnen.
1985	Der Ethernet-Standard wird als ISO/DIS 8802/3 veröffentlicht. Das RFC 948 ermöglicht erstmals die Unterstützung der TCP/IP-Protokolle auf IEEE-802.3-Netzwerken.
1986	Der Ethernet-Standard für die 10Base2-Verkabelung mit Cheapernet wird verabschiedet.
1990	Die IEEE-802.3-Spezifikation wird als ISO-Standard akzeptiert.
1991	Der 10Base-T-Standard wird veröffentlicht.
1992	Ethernet ermöglicht mit 10Base-F auch den Betrieb über Glasfaser-Strecken.
1993	Zwei 100 MBit/s-Varianten werden als Fast-Ethernet und 100 VG Anylan standardisiert.
1998	Gigabit-Ethernet auf Glasfaser wird standardisiert.

Einen wahrhaften Boom erlebte Ethernet mit der Verbreitung der PCs. Zwischen 1989 und 1993 stieg der Anteil vernetzter Rechner in den USA von 10 % auf 60 %, in den meisten Fällen auf der Basis von Ethernet.

Die Architektur basiert auf der Definition von Funktionen der beiden unteren Schichten des ISO-/OSI-Referenzmodells für die Festlegung der physikalischen Eigenschaften der benötigten Netzkomponenten, des Zugriffsverfahrens der Stationen auf das Netz und des Aufbaus der versendeten Nachrichten.

Das Zugriffsverfahren und die Spezifikationen der physikalischen Ebene werden von der IEEE in unterschiedlichen Arbeitsgruppen durchgeführt:

Tabelle 3.3 IEEE-Ethernet-Arbeitsgruppen

Arbeitsgruppe	Spezifikation
IEEE 802.3 a	10Base2
IEEE 802.3i/3l	10Base-T
IEEE 802.3j	10Base-F
IEEE 802.3r	10Base5
IEEE 802.3k	10-Mbit/s-Repeater
IEEE 802.3t	120-Ω-Koax in 10-Mbit/s-Segmenten
IEEE 802.3u	100Base-X
IEEE 802.3v	150-Ω-Koax in 10-Mbit/s-Segmenten
IEEE 802.3x	Vollduplex mit Flusskontrolle
IEEE 802.3z	1000Base-X Gigabit-Ethernet
IEEE 802.3 aa	100Base-T Revision Nr. 1
IEEE 802.3 ab	1000Base-T auf vierpaarigem 100-Ω-Kabel der Category 5
IEEE 802.3 ac	Frame Tagging (4 zusätzliche Bytes für die VLAN-Bildung)



Auf Grund der Entwicklungshistorie wohnt dem Begriff „Ethernet“ eine Zweideutigkeit inne. Er kann sich sowohl auf die Version der DIX-Gruppe beziehen als auch auf den Standard nach IEEE 802.3

Die unterschiedlichen Implementierungen von Ethernet folgen einer **Namenskonvention**: der erste Abschnitt verweist auf die Übertragungsgeschwindigkeit, der zweite auf den Übertragungstypus und der Dritte auf das Medium bzw. die zulässige maximale Entfernung. Auf diese Weise entstehen die Bezeichnungen 10Base5 oder 100Base-T.

Base bedeutet, dass das übertragene Signal die gesamte verfügbare Bandbreite nutzt und nicht auf eine Trägerfrequenz moduliert wird.

3.2 Paketaufbau

Neben der Bezeichnung hat die Historie auch im Paketformat ihre Spuren hinterlassen. Für die ursprüngliche Ethernet-Definition gemäß 10Base5 auf Koaxialkabeln existieren drei Rahmenformate:

- der Standard der DIX-Gruppe
- der Standard nach IEEE 802.3
- das Novell NetWare-Format.

Allgemein besteht der Ethernet-Rahmen aus mehreren Einzelfeldern:

Tabelle 3.4 Ethernet-Paketaufbau

Präambel	7 Bytes zur Synchronisation der Stationen
Start Frame Delimiter	1 Byte
Destination-Adresse	6 Bytes zur Identifikation der Zielstation, z. B. 08-00-04-60-50-01 ⁽¹⁶⁾
Source-Adresse	6 Bytes zur Identifikation der Datenquelle z. B. 08-00-04-67-45-31 ⁽¹⁶⁾
Pakettyp (DIX-Gruppe) oder Längenfeld (IEEE)	2 Bytes: IP 0800 ⁽¹⁶⁾ , ARP 0806 ⁽¹⁶⁾
Nutzdaten	maximal 1500 Bytes, minimal 38 Bytes
Prüfsumme CRC	4 Bytes für eine zyklische Redundanzprüfung

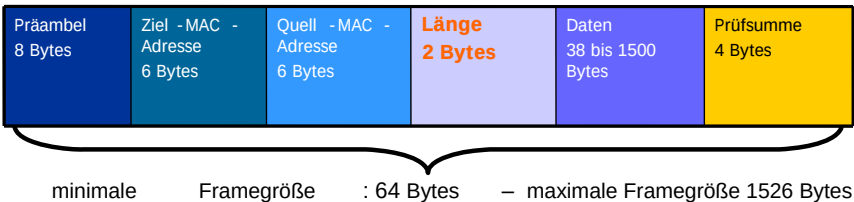


Bild 3.3 Ethernet-Paketaufbau

Unabhängig vom benutzten Rahmenformat ist die digitale Signalkodierung bei allen Varianten gleich. Da in einem Ethernet-Netzwerk eine Übertragung gleichbedeutend mit dem Vorhandensein eines Signals auf dem Übertragungsmedium ist und kein synchroner Taktmechanismus besteht, muss im Falle einer Kommunikation eine Station ein Signal erkennen. Die **Präambel** dient diesem Erkennungsprozess. Sie besteht aus sieben Bytes alternierender Nullen und Einsen und dem achten Byte mit der Folge „11“ am Ende. Eine Station entdeckt den Spannungswechsel, wenn ein anderer Rechner mit einer Übertragung beginnt und nutzt die Präambel zur Einstellung auf den Sendetakt.

In der DIX-Version des Rahmens bestanden zunächst zwei Felder Präambel und Start-of-Frame, deren Bitmuster aber gemeinsam der Präambel der späteren Version der IEEE entsprach. Ähnliches gilt für das Längenfeld der IEEE-Ausprägung, das dem Typfeld der DIX-

Version gleicht. Die Unterscheidung, ob es sich bei einem Frame um eine Längen- oder Typangabe handelt, geschieht über den Inhalt. Ist der Wert größer oder gleich 0x0600 Hex bzw. 1536 dezimal, handelt es sich um eine Typangabe, andernfalls um einen Längeneintrag.

Die traditionellen 10 MBit/s Ethernet-Varianten arbeiten asynchron, d.h. jede Empfängerstation nutzt die Präambel, um die Empfangseinheit auf die ankommenden Daten einzustellen. Moderne Netzwerkkarten garantieren das Erreichen der Synchronität bereits nach 14 Bit. Fast Ethernet und alle folgenden Implementationen sind synchron, so dass sie die Präambel nicht nutzen. Aus Kompatibilitätsgründen bleibt der Rahmenaufbau jedoch unverändert.

Jedes an ein Netzwerk angeschlossene Gerät muss nach der Spezifikation der ISO über eine eigene unverwechselbare Hardwareadresse verfügen. Die Vergabe der 6-Byte-Zahl hat eine Unterorganisation der IEEE nach folgender Systematik übernommen:

I/G	U/L	Herstellerkennung	Gerätenummer
1 bit	1 bit	22 bit	24 bit

Das I/G-Bit (Bit 47) unterscheidet zwischen einer individuellen Adresse (I/G=0) und einer Gruppenadresse für Multicasts oder Broadcasts (I/G=1).

Das U/L-Bit (Bit 46) wird zur Abgrenzung der von der IEEE (U/L=0) und lokalen Netzbetreibern (U/L=1) vergebenen Adressen benutzt. Die gesamte 48-Bitsequenz wird als MAC-Adresse bezeichnet und als eine 12-stellige Hexadezimalzahl ausgedrückt, wobei die linken/ersten 6 Ziffern den Hersteller beschreiben und die letzten/zweiten 6 Ziffern die Seriennummer des Interfaces spezifizieren.

Heute sind allerdings Netzwerkkarten verfügbar, deren MAC-Adresse per DIP-Switches oder gar per Software beliebig einstellbar ist. Damit geht die Eindeutigkeit verloren.

Tabelle 3.5 gibt einen Auszug einiger Hersteller, mit denen ihnen zugewiesenen Werten für die erste Zahlengruppe. Die vollständige Liste ist unter: <http://standards.ieee.org/regauth/oui/index.shtml> einsehbar.

Tabelle 3.5 Herstellerkennungen der MAC-Adresse

Ziffern in Hexadezimal	Hersteller
00000C, 00067C, 0006C1, 00070D, 001011	Cisco Systems
00104B, 002085, 0020AF, 006008, 006097	3Com Corporation
000063, 00060D, 0060B0, 080009	Hewlett-Packard
0000F4, 00A0D2	Allied Telesyn

Tabelle 3.5 Herstellerkennungen der MAC-Adresse (*Fortsetzung*)

Ziffern in Hexadezimal	Hersteller
000143	IEEE 802
0004AC, 000629, 002035, 08005A	IBM

Die **Source-Adresse** ist jeweils eine Unicast-Adresse des jeweiligen Hosts bzw. dessen Netzwerkkarte. Die **Destination-Adresse** kann eine Unicast-, Multicast- oder Broadcast-Adresse sein. Dementsprechend bedeutet ein „FFFF FFFF“ als Destination-Adresse eine Broadcast an alle erreichbaren Ethernetknoten. Im TCP/IP-Umfeld beschreiben mehrere Spezifikationen die Kapselung der Rahmen auf ethernetbasierten Netzen:

- RFC 894 (1984): „Standard for the Transmission of IP Datagrams over Ethernet Networks“ legt die Werte für das Typfeld fest. Die Vergabe der zulässigen Werte des Typfeldes wird von XEROX verwaltet und beinhaltet folgende Zuweisung:

Tabelle 3.6 Typfeldwerte

Wert in Hexadezimal	Beschreibung
000-05DC	IEEE 802.3 Längenfeld des Wertebereiches 0 bis 1500
0101-01ff	Experimentelle Zwecke
0800	DoD Internet Protocol (Department of Defense)
0806	ARP
8035	RARP
6003	DECNET Phase IV, DN Routing
8037	IPX (Internetworking Packet Exchange von Novell)
809B	EtherTalk (AppleTalk over Ethernet)
814C	SNMP over Ethernet (<u>S</u> imple <u>N</u> etwork <u>M</u> anagement <u>P</u> rotocol)
86DD	IPv6

Die **Prüfsumme** wird nach dem zyklischen Redundanzverfahren (Cyclic Redundancy Check) auf der Basis eines Polynoms berechnet:

- Das Verfahren basiert auf einem Polynom vom Grade k , wobei Bitketten mit den Koeffizienten 0 und 1 nach folgender Systematik betrachtet werden:

$$1\ 1\ 0\ 0\ 0\ 1 \approx x^5 + x^4 + x^0 \quad \text{mit } k = 6$$

- Zur Polynomberechnung werden die Regeln des Exclusive OR verwendet, d.h. kein Übertrag berücksichtigt.
- Zu Beginn der Berechnung werden k Nullbits an der niederwertigen Seite des Ethernet-Paketes angehängt. Anschließend wird die neu entstandene Bitkette durch das Polynom gemäß des Exclusive OR verknüpft und die Bitsumme mit dem Divisionsrest übertragen.



Prüfsummenberechnung

1. Bitsumme eines Paketes: 1101011011
2. Polynom: $10011 \approx x^4 + x^1 + x^0$
3. Anhängen von $k = 4$ Nullbits: 11010110110000
4. Berechnung:

11010110110000 : 10011 = 1100001010

10011

10011

10011

00001

00000

00010

00000

00101

00000

01011

00000

10110

10011

01010

00000

10100

10011

01110

00000

1110

Rest

Übertragener Rahmen: 11010110111110

Ursprungsrahmen + Rest

Auf Grund der stürmischen Entwicklung der Netzwerktechnologie und den damit verbundenen sich wandelnden Anforderungen an die Infrastruktur hat das Ethernetpaket einige Erweiterungen erfahren:

- Das Aufkommen von virtuellen LANs machte es notwendig, eine Kennung für die einzelnen VLANs einzuführen. Ein Tag Protocol Identifier und ein Tag Controll Feld von jeweils 2 Bytes verlängern das Paket von 1518 Bytes auf 1522 Bytes (ohne Präambel). VALN tagging ist in IEEE 802.1 Q definiert und erlaubt die Bildung logischer Netze in einem lokalen Netz über Gebäude hinweg. Neben der Identifizierung von VLANs erlaubt der Tag zusätzlich die Bildung von Prioritäten zur Übertragung. Die Bedeutung der dafür reservierten 3 Bits im TCI-Byte regelt der Standard IEEE 802.1p

- Der IEEE 802.3z (Gigabit Ethernet) Standard führt einen Burstmodus ein. Dieser erlaubt die Übertragung mehrerer Pakete hintereinander. Dieser Mechanismus ist nur für Gigabit-Ethernet und neuere Varianten des Halbduplex-Verfahrens definiert. Es soll die Übertragung vieler kleiner Pakete beschleunigen.
- Jumbo-Pakete mit einer Größe von 9000 Bytes sind auf Vollduplex-Verbindungen beschränkt und setzen ein angepasstes Auto-Negotiation-Protokoll voraus.

■ 3.3 Zugriffsverfahren: CSMA/CD

Die MAC-Ebene – als Schicht 2a in das ISO-/OSI-Referenzmodell eingeordnet – legt das Zugriffsverfahren der Stationen auf das Übertragungsmedium fest. Das gewählte Konzept ist vollständig unabhängig von den darunter liegenden physikalischen Gegebenheiten in Form von Kabelspezifikationen oder Steckverbindungen. In Ethernet kommt der CSMA/CD-Mechanismus (Carrier Sense Multiple Access with Collision Detection) zum Einsatz. Dieser gewährleistet allen Stationen jederzeit einen gleichberechtigten Zugriff auf das Netz, so dass Ethernet das alle Stationen verbindende Kabel als gemeinsames Übertragungsmedium sieht. Das CSMA/CD-Verfahren dient als Steuerungsinstanz, das jeder Station Sende- und Empfangsmöglichkeiten einräumt, Sendekonflikte vermeidet und die Datenintegrität erhält.



Ausdehnung eines Ethernetnetzwerkes

Kollisionsdomäne

Eine Kollisionsdomäne umfasst alle Netzwerkgeräte, die gemeinsam um den Zugriff auf ein Übertragungsmedium der Schicht 2 des OSI-Referenzmodells konkurrieren.

Broadcastdomäne

Eine Broadcastdomäne umfasst alle Netzwerkgeräte, die als Broadcast gesendete Pakete erhalten. Da Geräte auf OSI-Schicht 2 Broadcasts weiterleiten, umfasst eine Broadcastdomäne häufig mehrere Kollisionsdomänen.



Die Konkurrenz um das Medium ist typisch für das ursprüngliche Ethernet. Durch die schnelle Verbreitung von Switches und der wachsenden Zahl von Hosts mit Vollduplex-Verbindungen verliert der CSMA/CD-Mechanismus ständig an Bedeutung. In den neuen Varianten ab 10G-Ethernet ist er in der Standardisierung nicht mehr enthalten.

Allerdings nutzen WLANs mit CSMA/CA weiterhin eine Variante des CSMA/CD-Verfahrens.

Die grundlegende Vorstellung von CSMA/CD ist, dass alle Netzwerkteilnehmer die Chance zur gleichberechtigten Nutzung des Netzwerkes besitzen. Das Übertragungsmedium ist daher eine zwischen allen Netzstationen geteilte Ressource. Dennoch kann nur eine Sta-

tion zur gleichen Zeit Informationen übertragen. Diese Tatsache erfordert Regeln, die den Zugriff sendewilliger Stationen auf das Medium steuern.

Ein gesendeter Rahmen durchquert das Netz vollständig und wird von jeder Station daraufhin geprüft, ob er an sie adressiert ist. Diese Prüfung findet anhand der Zieladresse statt. Trifft dies zu, wird der Rahmen kopiert, ansonsten verworfen. Die Folge dieses Konzeptes ist, dass jede Station jede Übertragung „sieht“. Damit liegt eine Sendung nach dem Broadcastprinzip vor. Der Steuerungsmechanismus unterscheidet mehrere Phasen:

- **Carrier Sense – Überwachung von Aktivitäten auf dem Kabel:** Bevor eine Ethernet-Station Daten senden darf, muss sie sich vergewissern, dass das Medium nicht durch eine andere Station belegt ist. Sie erreicht dies durch eine Überwachung des Kabels (**Busy Waiting**). Diese Fähigkeit zur Entdeckung von Aktivitäten konkurrierender Stationen wird „**Carrier Sense**“ genannt. Für die betreffende Station bedeutet dies, sie muss ihren Übertragungswunsch zurückstellen (**Deferring**). Wird das Medium allerdings als frei erkannt (**Idle State**), erfolgt nach Verstreichen einer bestimmten Zeitspanne (**Interframe Gap**) die Übertragung bei weiterhin gleichzeitigem Abhören des Mediums auf Kollisionen (**Listening while Talk**). Die Zustände des Belegtseins bzw. Nichtbelegtseins werden anhand der Pegelwerte nach 0,75 bzw. 1,25 Bitzeiten ermittelt. Tritt nach diesen Zeitpunkten ein Pegelwechsel auf, so ist ein Trägersignal auf dem Kabel und das Medium somit belegt:

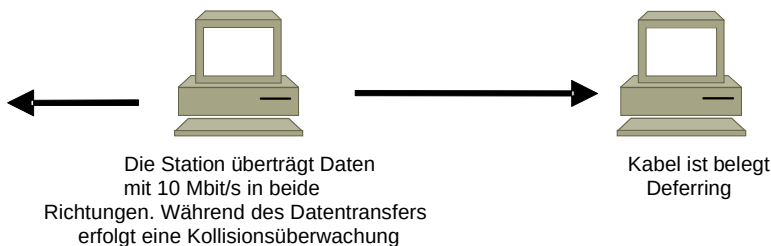


Bild 3.4
Überwachung

- **Sendevorgang:** Die Datenübertragung des bitseriellen Datenstroms beginnt mit der Präambel (10101010) und dem anschließenden Ethernet-Rahmen. Hierbei kann es vorkommen, dass mehrere Stationen zur gleichen Zeit das Medium als frei erkannt haben und aktiv auf das Netz zugreifen. Dadurch entsteht zwangsläufig eine Überlagerung der von den einzelnen Stationen gesendeten Signale, so dass die codierte Information verloren geht. Dieser Vorgang wird als **Kollision** bezeichnet. Da jede Station gleichzeitig den Empfang überwacht, wird diese Signalverfälschung sofort entdeckt (**Collision Detection**).



Da im Falle des klassischen Ethernets nach dem Broadcastverfahren übertragen wird und die Ausbreitung der Sendung den Bereich der möglichen Kollisionen umfasst, entsprechen sich Broadcast- und Kollisionsdomäne. Werden Switches oder Router als Verbindungselemente zwischen Stationen eingesetzt, unterscheiden sich Kollisions- und Broadcastdomäne.

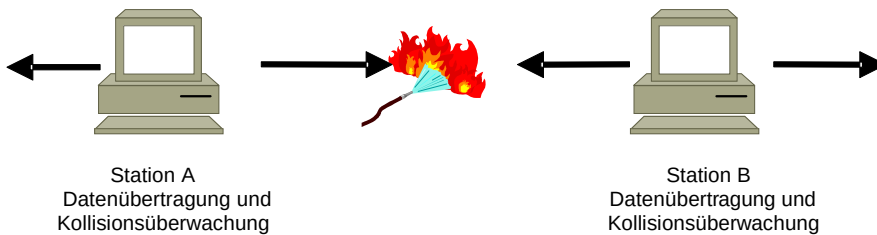


Bild 3.5 Kollisionserkennung

- **Multiple Access – erneuter Zugriff:** Dieser Begriff bezeichnet die Tatsache, dass sich eine Station nach erfolgter Sendung sofort erneut um das Senderecht bemühen kann.



Die Eigenschaft des Multiple Access steht im Gegensatz zu anderen Zugriffsverfahren wie Token Ring, bei denen aus Fairnesserwägungen zunächst die anderen sendewilligen Stationen den Vorzug erhalten.

- **Collision Detection – Kollisionserkennung:** Hat eine der Stationen der Kollisionsdomäne eine Kollision festgestellt, erzeugt sie ein **32-Bit JAM-Signal**, das zur Erkennung an alle Stationen weitergereicht wird und die Unterbrechung jeglicher Übertragung veranlasst. Dieses Signal besteht aus der Bitkombination: 10101010-10101010-10101010-10101010. Kollisionen können nur innerhalb eines sehr kurzen Intervalls nach Übertragungsbeginn auftreten, wenn die Signale noch nicht alle aktiven Stationen des Segmentes passiert haben. Diese **Slot-Time** definiert den maximalen Zeitraum bis zur eindeutigen Belegung des Mediums durch eine Station.
- **Übertragungswiederholung:** Nachdem eine Kollision aufgetreten ist, warten die beteiligten – durch das JAM-Signal informierten – Stationen eine zufällige Zeitspanne – definiert in Einheiten von Slot-Time – und beginnen den Sendeprozess erneut. Da die Wartelänge nicht koordiniert ist, sondern pro Station zufallsabhängig ist, besteht die Erwartung, dass eine Station diesen Vermittlungsvorgang gewinnt und das Medium belegt, bevor die Konkurrenten zum Zuge kommen. Nach der ersten Kollision warten die Stationen 0 oder 1 Slot-Time, nach der zweiten 0,1,2 oder 3, nach der dritten wird die nächste Wartezeit zufällig zwischen 0 und $2^3 - 1$ gewählt. Allgemein wird nach i Kollisionen eine Zufallszahl zwischen 0 und $2^i - 1$ bestimmt und diese Anzahl Time-Slots übersprungen. Dieser Prozess endet mit dem 16. Sendeversuch (**Attempt Limit**) und friert bereits nach dem 10. Versuch die Wartezeit ein. Der Algorithmus erlaubt eine dynamische Anpassung an die Anzahl sendebereiter Stationen; denn die Wahrscheinlichkeit, dass zwei Stationen bei einem Zufallsintervall von $2^{10} = 1024$ erneut kollidieren würden, ist sehr gering.



Bild 3.6 Erneuter Sendeversuch

Den Kollisionsvorgang in Form des Backoff-Algorithmus verdeutlicht das folgende Diagramm:

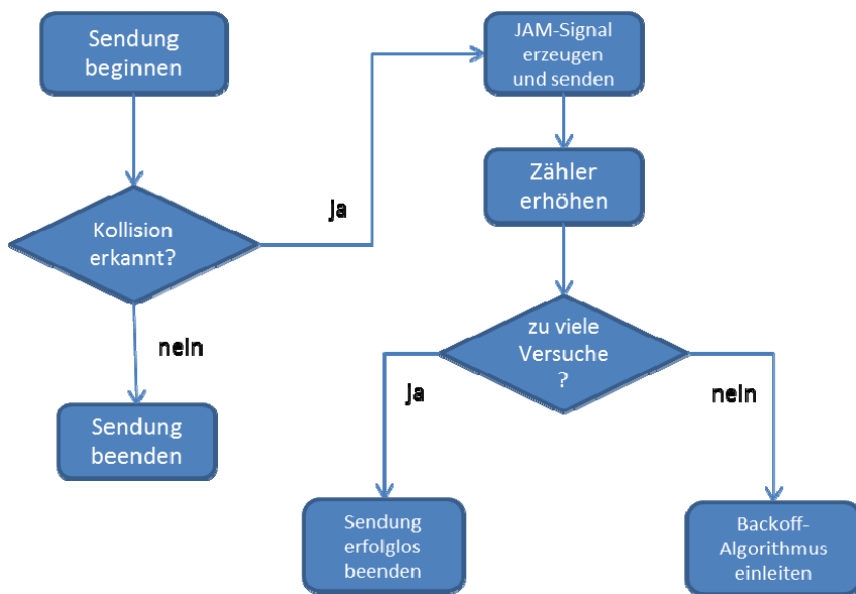


Bild 3.7 Backoff-Algorithmus

Kollisionen können in zwei Gruppen eingeteilt werden:

- **Early Kollisionen** sind eine normale Erscheinung in Ethernet-Netzen und bedeuten demzufolge keine Fehlfunktion. Typischerweise benötigt eine Station nicht länger als 2 – 3 ms, um ihre Sendung trotz des Auftretens von Kollisionen erfolgreich abzuschließen.
- **Late Kollisionen** im Gegensatz dazu deuten immer auf einen Fehler in der Verkabelung oder in der Netzwerkkarte hin. Sie treten auf, weil eine Station auf Grund der Überlänge des Kabels ein JAM-Signal empfängt, obwohl sie ihre Übertragung bereits beendet hat und daher glaubt, ihre Sendung erfolgreich abgeschlossen zu haben.

Neben diesen Ausnahmesituationen definiert die 802.3-Spezifikation eine Reihe von Schritten, die jede Station beim Empfang von Ethernet-Paketen auszuführen hat, da der CSMA/CD-Mechanismus keine Quittungen liefert:

- **Fragmentprüfung:** In Ethernet sehen alle Stationen alle Pakete ohne Rücksicht darauf, ob sie der Adressat sind oder nicht. Die erste Station in Senderichtung prüft die Vollständigkeit des Paketes und nimmt es im Fehlerfall vom Netz. Handelt es sich um ein gültiges Paket wird die Empfängeradresse geprüft und gegebenenfalls die Information interpretiert.
- **Integritätsprüfung:** Wenn eine Station ein Paket als an sich gerichtet erkennt, prüft sie es auf seine Integrität. Dazu zählen die Prüfung der korrekten Länge und der Prüfsumme als Fehlererkennungsmechanismus.

Das Ursprungsethernet versteht sich als Halbduplex-Verfahren. Um die der einzelnen Station zur Verfügung stehende Bandbreite zu erhöhen, kann Ethernet jedoch auch im Vollduplex-Modus betrieben werden. In diesem Fall spielt der CSMA/CD-Algorithmus keine Rolle, da keine Konkurrenzsituation zwischen Stationen zu klären ist.



Vollduplex-Ethernet kann in drei Situationen genutzt werden. Eine Verbindung:

- von einem Switch zu einem ausgewählten Host
- von einem Switch zu einem Switch
- von einem Host zu einem Host über ein Crossover-Kabel.

Im Laufe der Zeit erfuhr der CSMA/CD-Mechanismus einige Anpassungen:

- **Datenflusskontrolle** ist ein Verfahren, das von der IEEE unter 802.3x standardisiert wurde, um die Übertragung zwischen zwei im Vollduplex-Modus operierenden Stationen unter 10, Fast, Gigabit und 10G Ethernet zu steuern. Ein Knoten, der keine Pakete mehr verarbeiten kann, ist nun in der Lage, dem Sender mitzuteilen, seine Übertragungsleistung zu reduzieren. Dieser Mechanismus betrifft nur benachbarte Knoten, keine vollständigen Ende-zu-Ende-Verbindungen über viele Vermittlungsstellen. Die verlangsamte Datenübertragung gilt für eine bestimmte Zeitspanne. Sie reduziert den Durchsatz und führt in der Folge zu einer längeren Übertragungsdauer. Das Pause-Paket besitzt den Feldtypen 8808 und legt in den Nutzdaten die Länge der Pause fest.
- **Auto-Negotiation** erlaubt zwei Knoten, die bestmögliche Verbindung zwischen ihnen festzulegen. Die Stationen tauschen Informationen über die Übertragungsgeschwindigkeit, den Operationsmodus (halbduplex, vollduplex) und das Vorhandensein der Datenflusskontrolle aus. Auf Twisted-Pair-Verbindungen wird zur Aushandlung der Parameter eine modifizierte Form des Normal Link Pulse (NLP) Signals genutzt. Auf Glasfaserkabeln muss ein anderer Mechanismus verwendet werden. 10G-Ethernet unterstützt dieses Verfahren nicht. Die Prioritätsreihenfolge zeigt folgende Übersicht:

Auto-Negotiation Prioritätsreihenfolge	
A	1000Base-T voll duplex
B	1000Base-T halb duplex
C	100Base-TX voll duplex
D	100Base T4
E	100Base-TX halb duplex
F	10Base-T voll duplex
G	10Base-T halb duplex

- **Link Aggregation** ist eine weitere Ethernetfunktion nach IEEE 802.3ad, die ausschließlich für Vollduplex-Verbindungen gilt. Dieses Konzept kombiniert mehrere physikalische Verbindungen zu einer Logischen, um die Bandbreite zwischen zwei Knoten zu erhöhen. Damit wird das Spanning Tree-Protokoll umgangen, dass keine redundanten Verbindungen in einem Netzwerk erlaubt. Voraussetzung für die Nutzung ist, dass es sich um eine Punkt-zu-Punkt-Verbindung im Vollduplex-Modus handelt, deren Teilnehmer die gleiche Übertragungsrate verwenden.

■ 3.4 Signalverlauf

Die zeitliche Dimension des CSMA/CD-Verfahrens lässt sich folgendermaßen skizzieren:

Zu einem Zeitpunkt t_0 beginnt die Station A mit dem Versenden eines Ethernet-Frames. Das Aussenden selbst nimmt die Zeit T_1 in Anspruch, also die Spanne von t_0 bis $t_0 + T_1$ wird für die Rahmengenerierung benötigt. Die Signallaufzeit von A zu einer Station B beträgt T_2 , so dass der Frame um die Zeit T_2 verzögert bei B eintrifft. Die Ankunft bei B findet demnach in der Zeitspanne $t_0 + T_2$ bis $t_0 + T_2 + T_1$ statt. Hat die Station B ebenfalls einen Sendewunsch, prüft sie die Leitung und findet diese vor Eintreffen des Rahmens von A also zeitlich vor $t_0 + T_2$ als unbesetzt vor, so dass sie mit dem Sendeprozess beginnen kann. Beginnt B mit der Sendung seines Rahmens zum Zeitpunkt $t_0 + T_1 - T_2$, trifft der Rahmenanfang bei A zum Zeitpunkt $t_0 + T_1 - T_2 + T_2 = t_0 + T_1$ ein, da die Signallaufzeit von A nach B der von B nach A entspricht. Genau zu diesem Zeitpunkt hat A die Framegenerierung beendet, so dass keine Kollision entsteht. Erzeugt die Station B in der Zeitspanne $[t_0 + T_1 - T_2, t_0 + T_2]$ ihren Rahmen, bleibt eine mögliche Kollision von A unerkannt. Für den korrekten Ablauf des CSMA/CD-Verfahrens muss daher gelten: $t_0 + T_1 - T_2 \geq t_0 + T_2$ bzw. $T_1 \geq 2T_2$.



Alle Netztechnologien definieren eine **Slot Time**, als Zeitspanne, in der ein Bit gesendet werden kann. Damit die elektronischen bzw. optischen Komponenten eine binäre 1 oder 0 erkennen, benötigen sie eine minimale Dauer, in der das Bit gesetzt oder ungesetzt ist. Ethernet nutzt 100 Nanosekunden (ns) als Slot-Time bzw. **Bitzeit**, d. h. diese Zeitspanne wird benötigt, um ein Bit zu signalisieren. Ein Byte erfordert folglich 800 ns. Für einen 64-Byte-Frame (als kleinster zulässiger 10Base-T Frame) als Folge von 512 Bit werden folglich 51,2 Mikrosekunden (64×800) benötigt. Die **Slot-Time** ist die Grundlage für die Bestimmung der Kabellänge als der größten zulässigen Ausdehnung.



Ethernet-Distanz

Da T_1 von der Framelänge und T_2 von der Leitungslänge abhängt, gilt, dass bei fester Rahmengröße die Netzausdehnung begrenzt sein muss. Beide Parameter bestimmen sich als:

$$T_1 = (\text{Framelänge in bit}) \times 10^{-7} \text{ s}$$

$$T_2 = \text{Kabellänge} / (0,66 \times \text{Lichtgeschwindigkeit})$$

Damit ergibt sich durch Einsetzen:

$$(\text{Framelänge in bit} \times 10^{-7} \text{ s} \geq 2 \times \text{Kabellänge} / (2/3) \times 3 \times 10^8 \text{ m/s})$$

$$\text{bzw. } (\text{Framelänge in Bits}) \geq \text{Kabellänge} / 10 \text{ m}$$

Da die minimale Framelänge in Ethernet 64 Byte = 512 bit beträgt, ergibt sich für die Kabellänge ein Wert von 5120 m. Leider kommt ein weiteres Problem hinzu. Repeater übertragen die Signale nicht verzögerungsfrei, sondern benötigen zur Regenerierung etwa 3 μs . Um die maximale Netzausdehnung zu bestimmen, müssen also die Signallaufzeiten berechnet werden.

$$T_2 = 5120 \text{ m} / [(2/3) \times 3 \times 10^8] \text{ m/s}$$

$$= 25 \mu\text{s}$$

Die Signallaufzeit durch ein 500 m Segment beträgt damit ca. 2,5 μs . Für ein Ethernet-Netzwerk mit vier Repeatern, das fünf Segmente nach der 5-4-3-Regel verbindet, ergibt sich eine maximale Signallaufzeit von

$$5 \times 2,5 \mu\text{s} + 4 \times 3 \mu\text{s} = 24,5 \mu\text{s}.$$

Die minimale Paketgröße von Ethernet basiert auf ähnlichen Überlegungen: Da jede Station den Sendevorgang beginnen kann, wenn sie das Medium als frei erkennt, muss ein Ethernet-Paket eine Mindestlänge aufweisen, um zu verhindern, dass die sendende Station bereits mit der Übertragung endet und an einen erfolgreichen Abschluss glaubt, obwohl eine Kollision auftrat. In diesem Falle würde eine Kollision erst nach Sendeabschluss erkannt und es bestände keine Möglichkeit der Retransmission. Nur wenn das Paket eine entsprechende Länge aufweist und alle Stationen passiert, kann ein vorzeitiges Senden einer weiteren Station unterbunden werden. Die minimale Paketlänge P hängt damit von der Weglänge D zur entferntesten Ethernet-Station und zurück ab.



Berechnung der minimalen Paketlänge

$$\text{Framelänge in bit} = (\ddot{U} \times (2 \times \text{Kabellänge})) / V$$

mit $\ddot{U}$ = Übertragungsgeschwindigkeit

V = Signalausbreitungsgeschwindigkeit

Für Ethernet gilt: $\ddot{U}$ = 10 Mbit/s

Kabellänge = max. 2500 m

V = 33 % der Lichtgeschwindigkeit

$$\text{Framelänge} = (10 \times (2 \times 2500)) / 100 = 500 \text{ bit} \approx 64 \text{ Byte}$$



Die Interframe Gap von 96 Bitzeiten als die Zeitspanne zwischen zwei Ethernetrahmen erfüllt eine besondere Funktion: sie ermöglicht es, anderen Stationen das Senderecht zu erlangen und verhindert damit die Monopolisierung der Übertragung durch eine Station.

Auf Grund der Interframe Gap besteht zwischen der Paketgröße und der übertragenden Paketanzahl keine lineare Beziehung. Die folgende Graphik drückt diesen Sachverhalt aus:

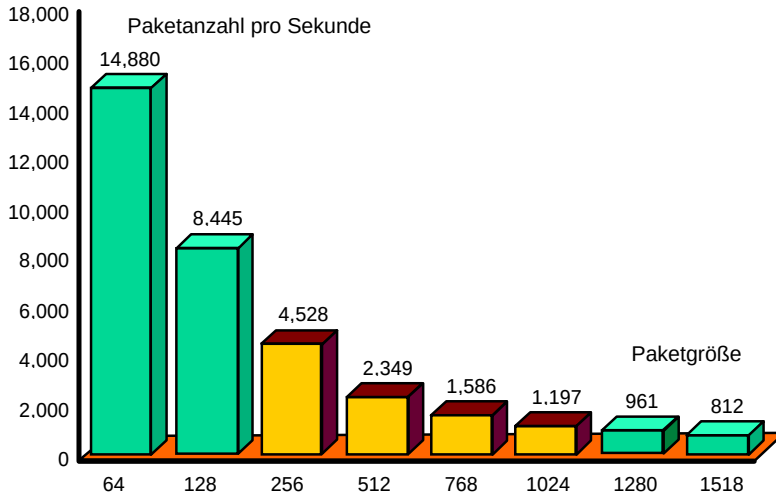


Bild 3.8 Zusammenhang Paketgröße – Paketanzahl

3.5 Standards

Ethernet wurde im Laufe der Zeit auf unterschiedliche Medien adaptiert. Obgleich CSMA/CD-Netzwerke damit physikalisch sehr verschiedene Formen unterstützen, müssen sie einige Standardvereinbarungen bezüglich Übertragungsrate, Übertragungsart oder maximaler Segmentlänge einhalten. Ethernet basiert auf der Basisband-Signalisierung, die Teil des Namens der Varianten ist. Dieses Verfahren nutzt die gesamte Bandbreite des Mediums. Im Gegensatz dazu wird im Broadband-Konzept zunächst das Signal moduliert, bevor es gesendet wird. Radio- und Kabelfernsehübertragungen gehören in diese Kategorie. Um dem Anwender ein Maximum an Konfigurationsmöglichkeiten einzuräumen, wurden vier Basisband-Varianten standardisiert:

- 10Base5 (thicknet)
- 10Base2 (cheapernet)
- 10Base-T (UTP)
- 10Base-F (Glasfaser)

10Base5

Diese Spezifikation bildete den Ausgangspunkt für Ethernet-Netzwerke. Sie ist als „gelbes Kabel“ bekannt geworden. Alle Stationen sind über diesen Kabeltyp an Transceiver gebunden, die ihrerseits untereinander das eigentliche Netz bilden:

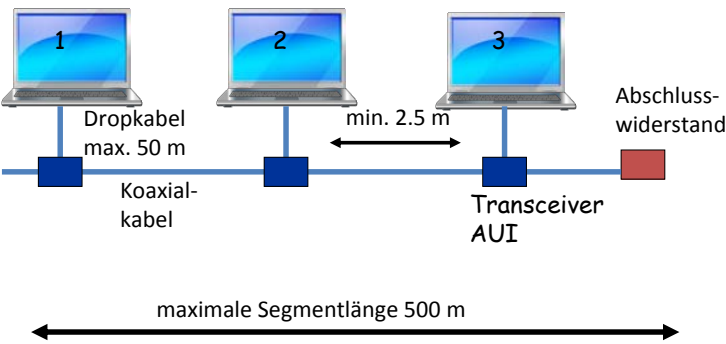


Bild 3.9 10Base5-Konfiguration

Die Länge des auf diese Weise entstehenden Ethernet-Busses darf 500 m nicht überschreiten. Bei Längen jenseits dieser Grenze kommen Repeater zur Signalregeneration zum Einsatz. Beide Enden des Kabels sind mit einem Abschlusswiderstand zu versehen, um Signalreflexionen zu unterdrücken. Diese entstehen an den Kabelenden und erzeugen Stehwellen. Übertragene Daten interferieren dort, erzeugen Datenverfälschungen und verhindern eine weitere Übertragung. Auf dem Kabel selbst sind im Abstand von 2,5 m Markierungen als Anhaltspunkte für die Transceiver-Montage angebracht. Der Anschluss einer Ethernet-Station erfolgt ausschließlich über einen Transceiver und niemals direkt. Der Transceiver stellt das Verbindungsglied zwischen Koaxialkabel und Endgerät her. Gemäß der Definition von Ethernet und seiner Positionierung auf der unteren Schicht des ISO-/OSI-Referenzmodells, enthält er einen Leitungstreiber zur Sendung, einen Signalempfänger und einen Mechanismus zur Kollisionserkennung. Zur zweifelsfreien Signalerkennung und -generierung erfüllt er strenge Implementationsvorschriften, z. B. kontrollierte Signalanstiegs- und -abfallzeiten von 25 ± 5 ns. Zusätzlich unterbricht er den Sendevorgang nach einer Kollisionserkennung (JAM-Funktion). Die wesentlichen Kennwerte des 10Base5-Standards zeigt folgende Übersicht:

Tabelle 3.7 Parameter des 10Base5-Standards

Eigenschaft	Wert
Kabeltyp	Koaxialkabel 50 Ω
Signalisierungstechnik	Basisband
Codierung	Manchester
Topologie	Bus
max. Segmentlänge	500 m

Tabelle 3.7 Parameter des 10Base5-Standards (*Fortsetzung*)

Eigenschaft	Wert
max. Stationszahl pro Segment	100
max. Netzausdehnung	2500 m
Mindestabstand zwischen zwei Stationen	2,5 m
max. Anzahl Kopplungselemente	5 Segmente über 4 Repeater
Stecker	AUI – 15-poliger Transceiverkabelanschluss
max. Länge des Drop-Kabels	50 m
Übertragungsgeschwindigkeit	10 Mbit/s

10Base2

Netze auf der Basis dieses Kabeltyps schließen die Stationen direkt an das Kabel über T-Verbinder gemäß BNC-Technik an. BNC (Bayonet-Neill-Concelmann)-Stecker verbinden zwei Koaxialkabel und zeichnen sich durch gute Hochfrequenzeigenschaften aus. Netzwerkkarten dieser Technologie verwenden On-board-Transceiver und können wesentlich leichter Endgeräte in das Netz integrieren. Zudem sind sie aufgrund des geringeren Hardware-Aufwandes (Einsparung von Transceiverkabel und Transceiver) auch wesentlich preisgünstiger. Diese Vorteile gehen aber zulasten der maximalen Ausdehnungsparameter.

Tabelle 3.8 Parameter des 10Base2-Standards

Eigenschaft	Wert
Kabeltyp	Koaxialkabel 50 Ω
Signalisierungstechnik	Basisband
Codierung	Manchester
Topologie	Bus
max. Segmentlänge	185 m
max. Stationszahl pro Segment	30
max. Netzausdehnung	925 m
Mindestabstand zwischen zwei Stationen	0,5 m
max. Anzahl Kopplungselemente	5 Segmente über 4 Repeater
Stecker	BNC
Übertragungsgeschwindigkeit	10 Mbit/s

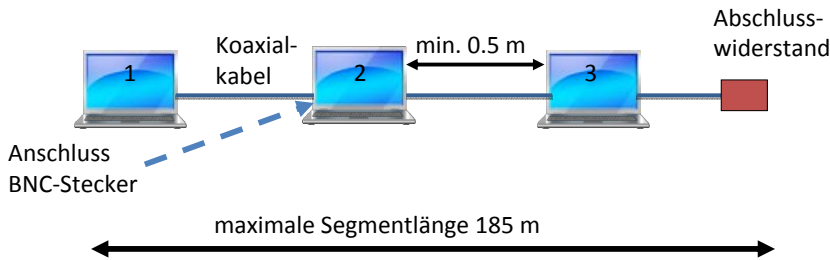


Bild 3.10 10Base2 Konfiguration

Die auf Koaxialkabel beruhenden Varianten von Ethernet unterliegen einer Beschränkung, die unter dem Namen **5-4-3-Regel** bekannt ist. Die Zahlen beschreiben folgende Limitierung:

- 5 – die Zahl der maximalen Kabelsegmente
- 4 – die Zahl der maximal einsetzbaren Repeater, um ein Segment auszudehnen
- 3 – die Zahl der Segmente, die Teilnehmerstationen besitzen dürfen.

In die Berechnung fließt nur die maximale Entfernung ein. Die Länge der Dropkabel spielt bei der Ausdehnung keine Rolle.

10Base-T

Die Standardisierung bezüglich dieses Mediums richtet sich in erster Linie auf die Bedürfnisse des amerikanischen Marktes mit seiner weit verbreiteten UTP-Verkabelung. Eine wesentliche Änderung, abgesehen von Längenbegrenzungen, ist dabei die Topologie in Form eines Sterns. Dies macht den Einsatz von Hubs als Konzentratoren mit Ports für jede angeschlossene Station notwendig. Bevorzugter Stecker dieses Mediums ist der RJ45-Stecker oder „Westernplug“, der auch aus der ISDN-Technik als Anschluss für den S_0 -Bus bekannt ist, mit der Belegung:

Tabelle 3.9 PIN-Belegung

Kontakt	Signal
1	Transmit +
2	Transmit -
3	Receive +
4	nicht belegt
5	nicht belegt
6	Receive -
7	nicht belegt
8	nicht belegt

Die Adernpaare eines CAT-5-Kabels sind farbig markiert. Jede Farbe hat eine bestimmte Bedeutung. Das orangene Adernpaar sendet Daten, das grüne hingegen empfängt Daten. Ist die Ader gestreift, bedeutet das, dass sie positiv ist, ist die Ader einfarbig, so ist sie negativ. Blaue und braune Adern dienen als Reserve. Sie werden erst ab Gigabit-Ethernet genutzt. Bei TP-Kabeln wird also zwischen Sende- und Empfangsleitungspaaren unterschieden. Diesem Sachverhalt muss bei der Kaskadierung von Repeatern durch ein Kabel, das Sende- und Empfangsleitungen kreuzt oder durch Umschaltbarkeit am Repeaterport Rechnung getragen werden.

Dieser Ethernet-Standard nutzt Hubs als Vermittlungsinstanz. Innerhalb des Hubs entspricht das Signalisierungssystem einem Bus, wie in den Koaxialvarianten. Sollen nur zwei Stationen miteinander verbunden werden, ist kein Hub erforderlich. Die Verbindung kann über Crossover-Kabel hergestellt werden.

Tabelle 3.10 Parameter des 10Base-T-Standards

Eigenschaft	Wert
Kabeltyp	TP-Kabel 100 Ω
Signalisierungstechnik	Basisband
Kodierung	Manchester
Topologie	Stern
max. Länge zwischen Station und Hub	100 m
max. Anzahl Kopplungselemente	5 Segmente über 4 Repeater
Stecker	8-poliger RJ45
Übertragungsgeschwindigkeit	10 Mbit/s

Die 5-4-3-Regel gilt für das Twisted-Pair-Ethernet gleichermaßen. Statt Repeater gehen hier die Hubs in die Berechnung ein.

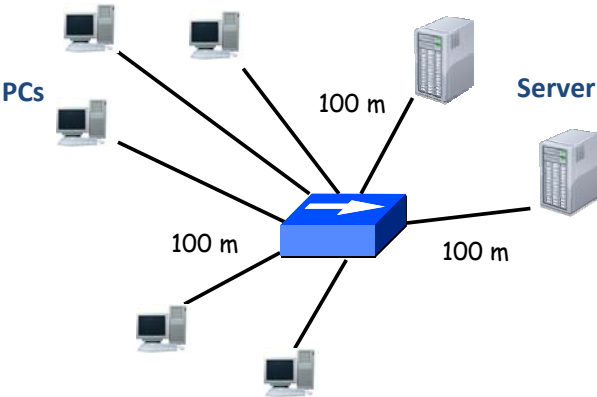


Bild 3.11 10Base-T-Konfiguration

10Base-F

Das jüngste Mitglied in der Gruppe der Ethernet-Übertragungsmedien ist die Glasfasertechnik, die sich in drei Teilgruppen gliedert:

- **10Base-FP** beschreibt die Verbindung von einem Transceiver zu einem passiven Hub. Da die durch dieses Verfahren übertragenen Signale nicht kompatibel zu den beiden anderen Ethernet-Glasfasertechniken sind, erfordert eine Verbindung von Segmenten unterschiedlicher Glasfaserstandards den Einsatz von Repeatern.
- **10Base-FL** beschreibt die Funktionen der Datenübertragung zwischen einem Transceiver und einem aktiven Hub. Die Daten werden allerdings asynchron weitergeleitet. Als weitere Besonderheit kommt hinzu, dass eine Signalauffrischung durch Repeater vorgeschrieben ist, so dass die üblichen Repeater-Regeln für Ethernet auch für diese Glasfaser-Variante zutreffen.
- **10Base-FB** verbindet sowohl aktive Hubs untereinander als auch Endgeräte mit Hubs. Dieser Standard stellt damit das flexibelste und realistische Szenario dar. Hinzu kommt, dass dieses Verfahren die synchrone optische Übertragung in repeaterfreien Backbone-Strukturen ermöglicht, die es auch erlaubt, Ports als redundante Verbindungen zu konfigurieren. Hierbei wird bei einem Verbindungsausfall automatisch auf den Ersatzport umgeschaltet und auf diese Weise ein erhebliches Maß an Fehlertoleranz erreicht.



Die Glasfaservarianten haben sich nicht in einer nennenswerten Installationszahl niedergeschlagen, so dass ihre Bedeutung gering blieb.

Tabelle 3.11 Parameter des 10Base-F-Standards

Eigenschaft	Wert
Kabeltyp	Glasfaserkabel
Signalisierungstechnik	Basisband
Codierung	Manchester
Topologie	Stern
max. Segmentlänge	2000 m
Stecker	ST
Übertragungsgeschwindigkeit	10 Mbit/s

■ 3.6 Fehlerquellen

Neben Verkabelungsproblemen in einem Netzwerk gibt es Fehlerquellen, die direkt mit der eingesetzten LAN-Technologie zusammenhängen. Durch Ethernet verursachte Fehler und Störungen lassen sich in folgende Kategorien einteilen:

- **Local Collisions:** Kollisionen sind das Ergebnis mehrerer gleichzeitig sendender Stationen. Eine übermäßig hohe Kollisionsrate lässt häufig auf einen Verkabelungsfehler schließen.
- **Late Collisions:** Diese Kollisionen ereignen sich außerhalb des Fensters von 512 Bitlänge. Verantwortlich dafür können zwei Umstände sein: Eine Station ist defekt und hält sich nicht an die CSMA/CD-Konventionen oder die Konfigurationsregeln bezüglich der Kabellänge sind verletzt worden. Dann wird die max. Signallaufzeit von 57,6 ms überschritten.
- **Short Frame:** Aufgrund fehlerhafter Netzkarten können Rahmen unterhalb von 64 Byte erzeugt werden.
- **Jabber:** Pakete, die die max. Länge von 1526 Byte überschreiten, deuten ebenfalls auf eine defekte Netzkarte hin.
- **Negative Frame Check Sequence:** Hier stimmt die Prüfsumme des Ursprungspaketes mit der beim Empfänger erzeugten nicht überein. Die Ursache liegt häufig in der Verkabelung.
- **Ghosts:** Als Ergebnis einer fehlerhaft arbeitenden Netzkarte können Paketfragmente entstehen.

Tabelle 3.12 Ethernetfehler und Ursachen

Ursache/Fehlertyp	Kollisionen	Short Frames	Jabber	FCS	Ghost
CSMA / CD	✓				
Software-Treiber		✓	✓	✓	✓
defekte Netzkarte	✓	✓	✓	✓	✓
fehlerhafter Transceiver	✓		✓	✓	✓
zu viele Repeater	✓				
Kabel zu lang	✓			✓	
Kabel fehlerhaft	✓		✓	✓	✓
Terminierung	✓		✓	✓	✓

■ 3.7 Verfahrensbewertung

- ☺ CSMA/CD ist ein einfach zu implementierendes Verfahren. Es benötigt durch die Verwendung des Backoff-Algorithmus kein zentrales Management.
- ☺ Bei geringer Last erhält eine sendewillige Station schnell Zugang zum Übertragungsmedium.
- ☺ Das JAM-Signal wird von allen Stationen als Kollisionsindikator erkannt, so dass der Zeitverzug für eine erneute Übertragung meist gering ist.
- ☺ Kollidieren Pakete einer Station häufig, wird diese benachteiligt.
- ☺ Der Sendeversuch kann prinzipiell mit einem Misserfolg enden. Allerdings ist die Wahrscheinlichkeit hierfür denkbar gering.
- ☺ CSMA/CD ist kein deterministisches Verfahren, das den Stationen einen Zugriff innerhalb einer Zeitspanne garantiert. Folglich ist es nicht echtzeitfähig und für Multimedia-Anwendungen ungeeignet.

■ 3.8 Zusammenfassung

Ethernet ist der populärste LAN-Standard in heutigen Netzwerken. Er ist darauf angepasst, sporadisch auftretenden Datenverkehr zu handhaben. Die Ursprungsversion nutzt den CSMA/CD-Algorithmus, um den Stationen einen geregelten Zugang zum Übertragungsmedium zu gewähren. Die Entwurfskriterien umfassten Aspekte wie Einfachheit, geringe Kosten, Fairness oder hohe Übertragungsleistung. In der Entwicklungsgeschichte hat sich Ethernet gegen alle weiteren Technologien im LAN-Sektor wie Token Ring oder Apple Talk durchgesetzt und stete Verbesserungen sowohl in der Geschwindigkeit wie auch in den Kopplungsgeräten sichern diese Position bis heute. Lernende sollten nicht nur die Basistechniken und das Paketformat beherrschen, sondern auch Kenntnisse über die unterschiedlichen Varianten besitzen und die von Ethernet zu Ethernet unterschiedlichen Verkabelungsmöglichkeiten beurteilen können.

Die Originalinformationen zu Ethernet sind unter folgenden Links zu finden:

<http://standards.ieee.org/getieee802/download/802.2-2-1998.pdf>

<http://standards.ieee.org/getieee802/802.3.html>



Noch Fragen ...? Ja ...

Kennt Ethernet keine Sicherheits- oder Fehlererkennungsmerkmale?

Nein, lediglich die Prüfsumme weist auf Übertragungstechnische Probleme hin. Ob ein Empfänger eine Sendung erhält, wird nicht geprüft.

Erweist sich die Paketgröße von 1500 Bytes bei heutigen Anwendungen nicht als zu klein?

Doch, daher existiert eine Modifikation zu größeren Frames den sog. Jumbo-Frames mit einer Nutzlast von 9000 Bytes.

■ 3.9 Wissensüberprüfung

1. Welche Entfernungsrestriktionen gelten bei 10Base2, 10Base5 und 10Base-T?
2. Zwischen welchen Geräten können Vollduplex-Verbindungen genutzt werden?
3. Welche drei elementaren Mechanismen verbergen sich hinter der Abkürzung CSMA/CD?
4. „Mit Ethernet sind keine Multimedia-Übertragungen möglich“. Warum?
5. Ethernetframes müssen für die Kollisionserkennung mindestens 64 Byte lang sein. Warum?
6. Wie unterscheiden sich die Rahmenstrukturen von 10Base-T und 10Base5?
7. Welche Bedeutung hat die Prüfsumme im Ethernetframe?
8. Was bedeutet die 5-4-3-Regel?
9. Was sind die Vor- und Nachteile der MAC-Adresse?
10. „Wenn ein Zielrechner einen Fehler entdeckt, verwirft er das Paket und informiert den Sender“. Stimmt diese Aussage für Ethernet?

4

Ethernet-Standards

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Welches ist ein weitverbreitetes Einsatzszenario?
- Wie hat sich der Ethernetrahmen entwickelt?
- Welches sind die neuen Eigenschaften und Herausforderungen an Ethernet?
- Wie lässt sich ein nahtloser Übergang zwischen den Standards organisieren?

Kapiteleinführung

Die Konstanz des Frames über alle Varianten hinweg bildet die Voraussetzung für eine nahtlose Migration zwischen den einzelnen Standards gepaart mit einer automatischen Erkennung der jeweiligen Geschwindigkeit. Die folgenden Abschnitte zeichnen die Entwicklung nach. Es zeigt sich, dass der Hunger nach Bandbreite allgegenwärtig ist und die Anpassung von Ethernet an diese Herausforderung dominiert. Während sich die physischen Grundlagen wie Verkabelung und Infrastrukturgeräte wie Switches ständig weiterentwickeln, bleibt der Kern des Ethernets eine Konstante in der Rasanz des technologischen Fortschritts.

■ 4.1 Die Gegenwart: Fast-Ethernet

Dank der fortschreitenden IT-Durchdringung aller ökonomischen Bereiche verlangen die heutigen Netzanwendungen hohe Geschwindigkeiten und eine wachsende Verarbeitungskapazität. Das Netzwerk dient dabei nicht nur zur Übertragung von Programm- und Datendateien, es soll vor allem multimediale Inhalte wie Sprache, Musik und Video transportieren. Diese Informationen sind nicht nur wesentlich umfangreicher, sondern verlangen auch garantierte Übertragungskapazitäten. Kollisionen von Datenpaketen wie im Standard-Ethernet machen es also unmöglich, Sprache so zu übertragen, dass die Daten den Empfänger in der korrekten Reihenfolge mit angemessener Qualität erreichen.

Zur „Temposteigerung“ des alten Ethernets stehen prinzipiell zwei Wege offen:

- 1. Erhöhung der Übertragungsgeschwindigkeit:** Der naheliegendste Weg besteht zweifellos darin, die Übertragungsgeschwindigkeit zu erhöhen. Dieser Weg wurde auch eingeschlagen mit der Konsequenz, dass die Signalisierung geändert werden musste. Die Signale eines mit 100 MBit/s arbeitenden Netzes müssten bei der Manchester-

Kodierung mit 200 MHz schwingen, was bereits weit in den Frequenzbereich von UKW-Sendern reichen würde.

2. **Verwendung mehrerer paralleler Leitungen:** Bei einer Beibehaltung der bisherigen Signalisierung hieße eine Temposteigerung, dass statt zwei mehrere Adernpaare erforderlich wären. Dieser Vorschlag liefe möglicherweise auf eine neue Spezifikation von Kabeln hinaus.

Fast-Ethernet nutzt den ersten Aspekt zur Steigerung der Übertragungsgeschwindigkeit.

4.1.1 Vorteile

Die Vorzüge einer beschleunigten Übertragung wirken sich in sehr unterschiedlicher Form aus:

- **Investitionsschutz herkömmlicher LAN-Technologien:** Weil sowohl die MAC-Layer-Definitionen als auch das Rahmenformat für Fast-Ethernet mit den Festlegungen für das traditionelle Ethernet übereinstimmen, verlangt die Verbindung beider Techniken keine teure Formatanpassung oder neue Werkzeuge für die Verwaltung und Prüfung unterschiedlicher Protokolle. Aus diesem Grund kann die bisher eingesetzte Soft- und Hardware ohne Modifikationen weiter betrieben werden. Dies bezieht sich insbesondere auf Netzwerkkarten.
- **Investitionsschutz der Verkabelungsinfrastruktur:** Fast-Ethernet benutzt in Anlehnung an den EIA/TIA Commercial Building Telecommunications Wiring Standard UTP-Kabel der Category 3 und 5, sowie STP-Kabel. Diese Abstützung auf existierende Techniken garantiert eine Rückwärtskompatibilität, so dass die Investitionen für die Kabelinfrastruktur gesichert sind.
- **Flexibilitätsgewinn im Netzdesign:** Durch die Differenzierung der Geschwindigkeiten kann das Netzdesign dem Client-/Server Architekturprinzip angepasst werden. Da die Verkehrsströme in derartigen Umgebungen von den Clients zum Server fließen, werden Server mit höheren Geschwindigkeiten angebunden als Clients. Hierfür stehen an den Switches Uplink-Ports zur Verfügung.
- **IEEE 802.3 Standard:** Die 10 MBit/s-Ethernet-Technologie wurde vom IEEE 802.3-Komitee standardisiert. 1993 wurden der IEEE zwei konkurrierende Vorschläge für Nachfolgetechnologien vorgelegt. Das eine Konzept basierte auf den 100Base-X und 100Base-4T+-Spezifikationsentwürfen und stützte sich auf das altbewährte CSMA/CD-Verfahren, der andere Vorschlag das 100Base-VG führte eine vollkommen neue Technologie auf der Basis des Demand Priority Access Protocols ein, das sich vom traditionellen Ethernet grundlegend unterschied. Nach langen Debatten kam das IEEE zum Entschluss, dass das ursprüngliche 802.3-Komitee nun auch die Standardisierung von Fast-Ethernet auf der Grundlage von 100Base-X und 100Base-4T+ übernehmen sollte. Die neue Technologie erhielt die Bezeichnung 100Base-T. Die Standardisierung des Konkurrenzvorschlages lag in den Händen eines neuen 802.12-Komitees, das die Technik unter dem Namen 100VG-AnyLAN festlegte.

4.1.2 Bestandteile

Der 100Base-T-Standard umfasst fünf Komponenten, die MAC-Schicht, die MII-Schicht (Media Independent Interface) und die drei physikalischen Schichten 100Base-TX, 100Base-T4 und 100Base-FX. Ihre Beziehung zueinander zeigt das folgende Diagramm:

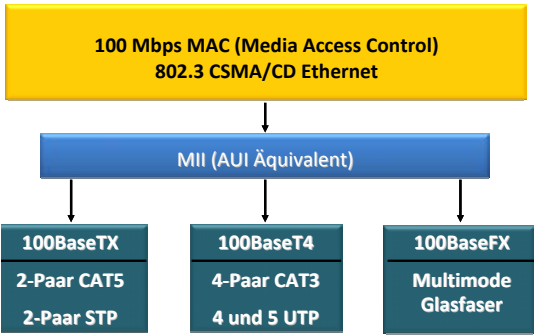


Bild 4.1 Fast-Ethernet – Medienunterstützung

Die **MAC-Schicht** bleibt unberührt und basiert weiterhin auf dem traditionellen CSMA/CD-Protokoll des ursprünglichen 10-MBit/s-Ethernets. Für Anwender besteht folglich nicht die Notwendigkeit, eine neue Technologie erlernen zu müssen.

Die MII-Schicht ist eine neue Spezifikation der Schnittstelle zwischen der MAC-Schicht und den drei physikalischen Schichten. Sie unterstützt alternativ sowohl 10 MBit/s als auch 100 MBit/s und besitzt ein Management-Interface zur Überwachung und Kontrolle der Konfiguration der unteren Schichten. Ein Reconciliation Layer als logische Schnittstelle übernimmt die Aufgabe, die MAC-Signalisierung in die MII-Signale zu transformieren, die MII-Schicht ihrerseits leitet diese an die entsprechenden physikalischen Medien weiter. Die MII-Schnittstelle kennt folgende Signale:

Tabelle 4.1 Signale der MII-Schnittstelle

Signal	Bedeutung
Transmit Clock	Kontinuierliches Signal, das 25 % der nominalen Übertragungsrate beträgt und von der physikalischen Schicht generiert wird.
Transmit Enable	Signalisierung des Reconciliation Layers an die MII-Schicht, dass Daten zur Übertragung anstehen.
Transmit-Coding-Error	Der Empfänger erhält eine Mitteilung über fehlerhafte Datensymbole.
Receive-Data-Valid	Das Signal zeigt die Datenübertragung vom physikalischen an den Reconciliation Layer an.
Receive-Error	Die physikalische Schicht meldet dem Empfänger, dass ungültige Datensymbole übermittelt wurden.
Carrier-Sense	Bei einer Medienbelegung wird dieses Signal durch die physikalische Schicht auf 1 gesetzt.
Collision-Detected	Bei einer Kollision erhält dieses Signal den Wert 1.

4.1.3 Varianten

Die Spezifikation der physikalischen Schicht hängt vom jeweiligen Substandard ab. Der 100Base-X Standard für die unterste Schicht gliedert sich in drei Teilbereiche: Physical Medium Dependant (PMD), Physical Coding Sublayer (PCS) und Physical Medium Attachment (PMA).

Die Schicht 1 des neuen Standards unterstützt drei Medientypen:

- 100Base-TX: Kategorie 5
- 100Base-T4: Kategorie 3
- 100Base-FX: Glasfaser

100Base-TX definiert die Spezifikationen für 100Base-T-Ethernet über zwei Leiterpaare. Dabei dient ein Paar zum Senden, das andere zum Empfangen der Daten. Zugelassen sind das UTP-Kabel der Kategorie 5 mit dem RJ-45-Anschluss und das STP-Kabel des Typs 1 mit dem DB-9-Anschluss der Token Ring-Netze. Damit ist gewährleistet, dass die amerikanische FCC-Class-B-Regeln und die noch strengeren europäischen Vorschriften EN 55022B zur elektromagnetischen Abstrahlung bei einer Übertragungsgeschwindigkeit von 100 MBit/s eingehalten werden. Die Länge eines TP-Segmentes beträgt auf Grund der maximal zulässigen Dämpfung von 13 dB bei 12,5 MHz nur 100 m. Diese Spezifikation führt zu einer maximalen Signallaufzeit von 570 ns.

Da die Übertragungsrate um den Faktor 10 höher liegt als bei Standard-Ethernet, wächst die Frequenz ebenfalls. Diese Tatsache führt zu Kodierungsschwierigkeiten. Standard-Ethernet nutzt die Manchester-Kodierung, um ein Taktsignal mit jedem Bit zu übertragen, so dass 10 MBit/s in einer 20 MHz Wellenform aufgehen. Für Fast-Ethernet würde das analoge Vorgehen 200 MHz bedeuten. Da Kategorie 5 UTP-Kabel aber nur für 100 MHz konzipiert sind, muss eine Alternative zur Manchester-Kodierung gefunden werden. 100Base-TX nutzt daher das MLT-3-Verfahren.

Der **100Base-T4**-Substandard gehört zu den neuen Ethernet-Spezifikationen. Die Bezeichnung T4 definiert die Anforderungen an die Kabel, die die Übertragung über vier Leiterpaare der Kategorie 3, 4 und 5 zulassen. Hierbei dienen drei Leiterpaare zum Senden und Empfangen, das vierte dagegen überprüft die Verbindung auf Kollisionen. Die Länge eines Segmentes ist bei einer Signallaufzeit von 570 ns auf 100 m beschränkt. Als Standard-Stecker ist die RJ-45-Technologie definiert, wobei die zwei zusätzlichen Kabelpaare die vier freien Pins des RJ-45-Steckers benutzen.

Zur Datenübertragung findet ein 8B/6T-Code Verwendung, bei der jeweils ein Byte in einen sechsstelligen Code umgewandelt und jede Codegruppe separat auf einer der drei Datenleitungen übermittelt wird. Durch diese Art der Codierung werden die 100 Mbit/s Datenrate auf drei Adernpaare mit jeweils 33,33 Mbit/s unterteilt. Die frequenzvermindernde 8B/6T-Kodierung, die jeweils ein Byte auf sechs Symbole abbildet, reduziert die Rate weiter auf $\frac{6}{8} \times 33,33 \text{ MHz} = 25 \text{ MHz}$. Zusätzlich erfolgt der Datentransfer als Einschränkung unidirektional also im Halbduplex-Betrieb, so dass dieses Verfahren in der Praxis nur für Punkt-zu-Punkt-Verbindungen geeignet ist. Eine Station kann nur senden oder empfangen, aber nicht beides parallel.

100Base-FX beschreibt die Übertragung auf Glasfaseradern des Typs 62,5/125 Mikron. Eine Ader empfängt, die andere sendet Daten. Die Segmentausdehnung kann bei einer Signallaufzeit von 570 ns bis zu 400 m erreichen. Als Steckverbindungen sind drei Alternativen zugelassen:

- Duplex SC-Stecker gemäß ANSI X3T9.5 LCF-PMD Revision 1.3 für FDDI
- MIC (Media Interface Connector) mit einer Codierung als M-Verbinder analog zu FDDI
- ST-Stecker wie er in 10Base-F Ethernetnetzen verwendet wird.

Die **PCS-Schicht** stellt die direkte Verbindung zur MII-Schicht her und erbringt folgende Funktionen:

- Codierung/Decodierung der Ethernetframes in 4B/5B- bzw. 8B/6T-Codegruppen.
- Erzeugung von Carrier-Sense- und Collision Detect-Signalen.

Die 4B/5B-Codierung für 100Base-FX und 100Base-TX anstelle der Manchester-Codierung ist ein etabliertes Verfahren. Sie wandelt jeweils 4 Bit eines Paketes in eine 5 Bit-Codegruppe um, so dass ein zusätzliches Bit zur Verfügung steht. Aus den ursprünglich $2^4 = 16$ Codegruppe ergeben sich damit $2^5 = 32$ Kombinationen, so dass bei einer effektiven Datenrate von 100 MBit/s tatsächlich 125 MBit/s übertragen werden. Diese Aufteilung hat mehrere Gründe:

- Es entstehen weitere Codegruppen, die neben der Nutzdatenübertragung für andere Zwecke genutzt werden können.
- Die Codierung ist derart gewählt, dass die Länge gleicher Bitfolgen begrenzt ist. Dieses Verfahren stellt sicher, dass bei einer beliebigen Codegruppe eine maximale Anzahl von Nullen oder Einsen nicht überschritten wird. Der Datenstrom enthält auf diese Weise ausreichend Taktinformation für den Empfänger, der jederzeit die 100 MBit/s-Datenrate rekonstruieren kann. Damit hat das verwendete Codierungsverfahren eine Effizienz von $100/125 = 80\%$ gegenüber nur 50% bei der Manchesterkodierung des ursprünglichen Ethernets. Der Code ist derart gewählt, dass im Durchschnitt der Anteil von Nullen und Einsen ausgewogen ist. Dies ist aus physikalischen Gründen von Bedeutung, weil sich bei einem Übergewicht einer Art eine Gleichspannungsdrift ergibt, die die Empfindlichkeit des Empfängers reduziert und zum Abbruch der Übertragung führen kann.
- Einige Codes sind als verboten gekennzeichnet. Das Auftreten solcher Sequenzen als untrügliches Zeichen für Übertragungsfehler hilft, die Qualität der Übertragung zu sichern.

Der **Physical Media Attachment Sublayer (PMA)** passt die 4B/5B-Codegruppen der NRZI-Codierung an, bei der eine logische 1 mit einem Wechsel des Signalpegels verbunden ist, eine logische 0 hingegen keinen Wechsel hervorruft. Da eine der wesentlichen Eigenschaften der 4B/5B-Codegruppen in der limitierten Länge der Nullen und Einsen liegt, entstehen keine langen Sequenzen von Nullen, so dass der Empfänger stets über ausreichende Taktinformationen verfügt.

4.1.4 Auto-Negotiations-Technologie

Diese Technologie bildet einen Teil der 100Base-T-Definition IEEE 802.3u. Sie dient zur Festlegung des Betriebsmodus jeden Knotens, so z. B. ob ein Rechner über eine 10 Mbit/s oder 100 Mbit/s-Netz Karte verfügt, über welchen Kabeltyp er angeschlossen ist und ob er den Vollduplex-Modus versteht. Damit entstehen vier mögliche Kombinationen: 10Base-T Halbduplex, 10Base-T Vollduplex, 100Base-TX Halbduplex und 100Base-TX Vollduplex. Zwei Knoten teilen einander ihre Übertragungsfähigkeiten mit, indem sie untereinander Parameter austauschen und sich auf den größten gemeinsamen Nenner einigen. Der Auto-sensing-Prozess liefert eine elegante Möglichkeit der Migration.



Bei Standard- und Fast-Ethernet ist Auto-Negotiation optional, für Gigabit-Ethernet ist diese Technologie vorgeschrieben. Auf Grund verschiedener Wellenlängen in den einzelnen Standards ist Auto-Negotiation nicht für optische Links einsetzbar. Da zudem eine Punkt-zu-Punkt-Verbindung Voraussetzung ist, arbeitet Auto-Negotiation nur in Switched-Ethernet-Umgebungen.

Die Basis des Auto-Negotiation-Prozesses bildet der Link-Integrity-Test-Puls Mechanismus, auch als Fast Link Puls Burst (FLP) bekannt. Zu Übertragungsbeginn und während Sendepausen werden FLPs moduliert, um den verfügbaren Modus zu signalisieren. Aus den Bits des FLP-Bursts extrahiert jede Station ein Link-Codewort, anhand dessen der Empfänger die gemeinsam unterstützten Parameter und Funktionen bestimmen kann. Dabei gilt folgende Prioritätsabstufung:

- 100Base-TX vollduplex
- 100Base-T4
- 100Base-TX
- 10Base-T vollduplex
- 10Base-T



Beispiel 1: Prioritätsschema

Unterstützt eine Station 100Base-T4, 100Base-TX und 10Base-T und der Kommunikationspartner 100Base-TX vollduplex, 100Base-TX und 10Base-T erkennen beide durch den Auto-Negotiation-Prozess, dass sie 100Base-TX und 10Base-T als Gemeinsamkeit besitzen. Da 100Base-TX in Prioritätsschema höher angesiedelt ist, einigen sich beide auf diesen Betriebsmodus.



Beispiel 2

Annahme: Gerät A ist auf 100 Mbit/s im Vollduplex-Modus eingestellt, Gerät B ist mit Auto-Negotiation konfiguriert.

Ergebnis: Der Auto-Negotiation-Prozess stellt Gerät B auf 100 MBit/s halbduplex ein und erwartet „Ruhe auf der Empfangsleitung“ während der Sendung. Jedes Signal auf der Empfangsleitung wird als Kollision interpretiert. Da aber das fest auf Vollduplex-Betrieb eingestellte Gerät A gleichzeitig sendet und empfängt, unterbricht B häufig auf Grund zu vieler Kollisionen.

Konsequenz: Der Datendurchsatz liegt wesentlich unter dem bei Vollduplex-Betrieb möglichen und unterschreitet wahrscheinlich sogar denjenigen bei korrekt eingestelltem Halbduplex-Modus.

4.1.5 Topologie

Ein Fast-Ethernet-Segment wird als Stern konfiguriert und umfasst höchstens zwei Repeater. Da Fast-Ethernet weiterhin das CSMA/CD-Verfahren verwendet, basiert der maximale Netzdurchmesser auf der Summe der Zeiten für Hin- und Rückweg zur am weitesten entfernten Station. Auf Grund des zehnmal schnelleren Fast-Ethernets wird die entstehende Zeitdifferenz durch eine Verringerung der Entfernungen und der Anzahl zulässiger Repeater pro Segment kompensiert. Die Kabeldistanz zwischen den entferntesten Endbenutzerstationen der gleichen Kollisionsdomäne schrumpft auf 205 m gegenüber 500 m beim herkömmlichen Ethernet und anstelle der 5-4-3-Regel gilt nur noch die 2-1-Regel, d.h. es sind je nach Repeater-Klasse nur noch ein oder zwei Repeater erlaubt, wobei zwei Repeater über ein ca. 5 m langes TP-Kabel zu einer Kaskade zusammengeschlossen werden können. Während alle Repeater der 10Base-T-Klasse grundsätzlich als funktional gleichwertig gelten, teilt Fast-Ethernet die Repeater in zwei Klassen:

- **Repeater der Klasse I** verstärken die an einem Port ankommenden Signale und übertragen sie zum Zielport, indem sie intern eine Umwandlung in Digitalsignale und anschließend wieder eine Rückwandlung in Analogsignale vornehmen. Dadurch entsteht eine größere interne Verzögerung. Diese Umsetzung wird bei der Nutzung **unterschiedlicher physikalischer Medien** innerhalb der gleichen Kollisionsdomäne erforderlich, z.B. können Repeater dieser Klasse 100Base-TX-Leitungen mit zwei Leiterpaaren von 100Base-T4-Produkten mit vier Leiterpaaren verbinden.
- **Repeater der Klasse II** verstärken die an einem Port ankommenden Signale und übertragen sie ohne Translation auf den Zielport. Mit diesem Repeater-Typ können nur **gleichartige Medien** innerhalb der Kollisionsdomäne verbunden werden, z.B. TX-Leitungen mit TX-Leitungen.

Um steigenden Bandbreitenanforderungen von Applikationen zu genügen, können einzelne Ports auf Fast-Ethernet aufgerüstet oder Fast-Ethernet-Switches eingesetzt werden. Die Wirkungsweise beider Lösungen verdeutlicht folgende Analogie:

- Stellt Ethernet ein Fahrrad dar und Fast-Ethernet einen PKW, die beide auf einer einspurigen Straße fahren, so beträgt die Geschwindigkeit 10 km/h zu 100 km/h. Solange kein Verkehr herrscht, können beide Fahrzeuge mit maximaler Geschwindigkeit fahren, sobald aber weitere Verkehrsteilnehmer hinzukommen, müssen sie ihre Geschwindigkeit drosseln. Switching bedeutet in diesem Szenario einfach das Hinzunehmen weiterer Spuren. Bei geringem Verkehr kann das Fahrrad weiterhin 10 km/h fahren, steigt die Zahl der Verkehrsteilnehmer können diese möglicherweise auf ihrer separaten

raten Spur ebenfalls mit 10 km/h fahren. Dennoch: ein Fahrrad erreicht nie die Geschwindigkeit eines PKW und bei weiter steigender Verkehrsdichte müssen die Fahrräder ihr Tempo drosseln.

- Wie Ethernet liefert Fast-Ethernet zunächst nur eine Spur. Bei geringem Verkehr kann der PKW mit 100 km/h fahren. Erst switched Fast-Ethernet liefert eine Autobahn mit mehreren Spuren, auf denen Höchstgeschwindigkeit erreicht werden kann.

4.1.6 Migration von Standard- zu Fast-Ethernet

Die zwei wichtigsten Bereiche bei einem Übergang betreffen die Verkabelung und die Hubs. Fast-Ethernet verlangt TP-Kabel der Kategorie 5 oder 4-paariges TP-Kabel der Kategorie 3. Der Einsatz von Hubs reduziert sich von vier auf zwei in einer Kollisionsdomäne. Ob es sich hierbei um eine echte Einschränkung handelt, ist mehr als fraglich, da die Switching-Technologie eine elegante Umgehung erlaubt.

Eine typische Überführung eines kleinen, an seine Grenzen stoßenden Ethernet-Netzes in eine größere effizientere Struktur unter Verwendung beider Technologien und einer Kombination von shared und switched-Verbindungen ist in vier Phasen vorstellbar:

1. Fast-Ethernet 10/100-Netzkarten werden an alle neuen Teilnehmer aus Gründen des Investitionsschutzes vergeben.
2. Der Datendurchsatz des 10Base-T-Netzes wird durch eine Verkleinerung der Kollisionsdomäne und dem Einsatz von Switching-Technologie verbessert.
3. Fast-Ethernet-Switching mildert die Bandbreitenengpässe für Server und Power User.
4. Server werden über Voll-Duplex-Verbindungen erreicht.

Unterstützend wirkt bei einem Übergang vor allem die Auto-Negotiation-Technologie.

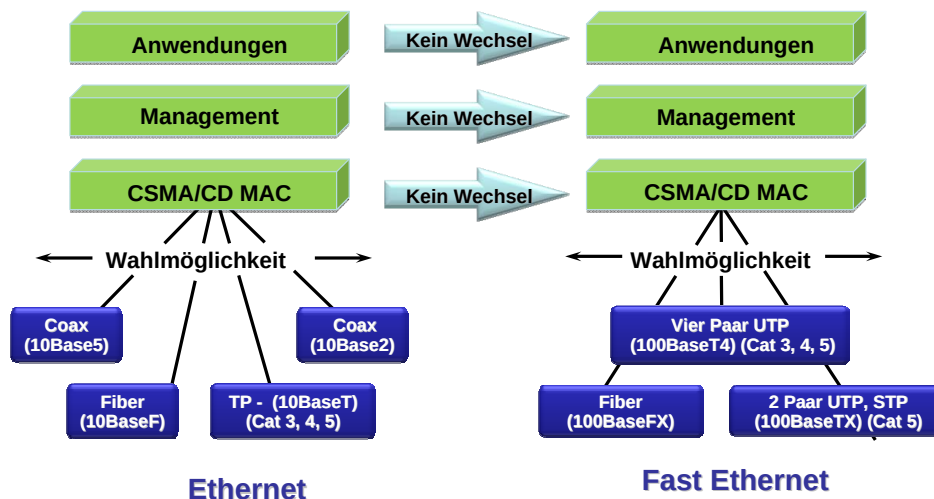


Bild 4.2 Übergang von Ethernet zu Fast-Ethernet

■ 4.2 Der Trend: Gigabit-Ethernet

Eine der wichtigsten Fragen, die sich Netzwerkadministratoren stellen, ist die, wie sie höhere Bandbreiten in ihre Knoten integrieren können, ohne das bestehende Netz zu zerstören. Gigabit-Ethernet geht hier den gleichen Weg wie seine Vorgängertechnologien und erlaubt eine einfache, inkrementelle Migration.

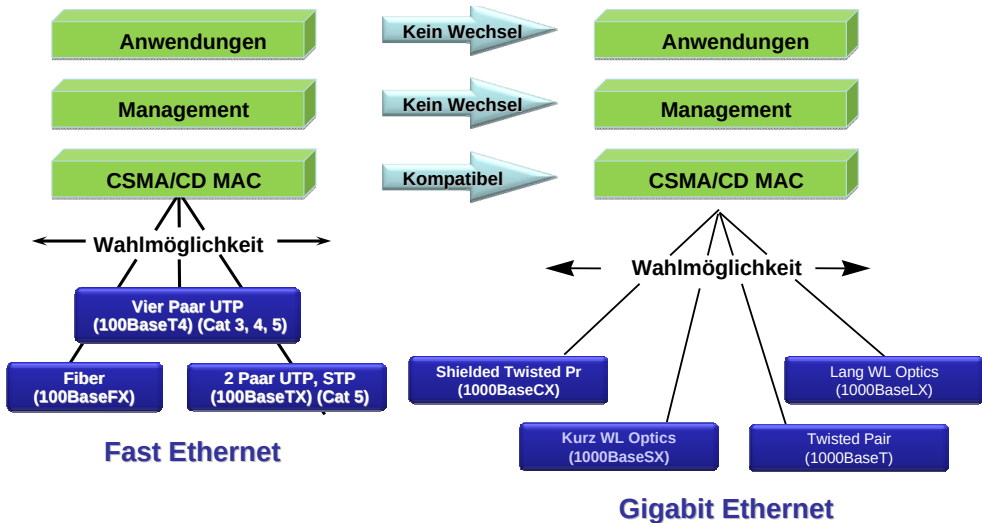


Bild 4.3 Übergang von Fast-Ethernet zu Gigabit-Ethernet

Die Netztopologie für Gigabit-Ethernet folgt den traditionellen Regeln des Ethernets: alle Ethernettechniken nutzen den gleichen Rahmenaufbau nach IEEE 802.3 und die Voll-duplex-Möglichkeit. Im Halbduplex-Modus bleibt auch das Zugriffsverfahren mit CSMA/CD unverändert. Damit gilt: Gigabit-Ethernet ist Ethernet, nur schneller. Die Abbildung 3.14 zeigt die Randbedingungen des Überganges von Fast-Ethernet zu Gigabit-Ethernet.

Gigabit-Ethernet wurde innerhalb der Arbeitsgruppe IEEE 802.3 als 802.3z im Juni 1998 über Glasfaserkabel standardisiert. Diese Gruppe formulierte mehrere Ziele für das neue Ethernet:

Tabelle 4.2 Merkmale von Gigabit-Ethernet

Merkm
eine Bandbreite von 1000 Mbit/s
die weitere Nutzung des 802.3 Ethernet-Rahmenformats
das Erfüllen der 802 Funktionsanforderungen
eine einfache Migration zwischen 10 Mbit/s-, 100 Mbit/s- und 1000 Mbit/s-Ethernet
das Beibehalten der minimalen und maximalen Paketgrößen

Tabelle 4.2 Merkmale von Gigabit-Ethernet (*Fortsetzung*)

Merkmal
die Unterstützung des Halb- und Voll-Duplex-Betriebes
die Unterstützung von Sterntopologien
die Weiterverwendung des CSMA/CD-Mechanismus mit mindestens einem Repeater pro Kollisionsdomäne
die Unterstützung der ANSI Fibre Channel Spezifikation FC-1 und FC-0
eine Datenflusskontrolle
die Festlegung eines GMII (Gigabit-Ethernet Media Independent Interface)

4.2.1 Physikalische Grundlagen

Der 1000Base-X-Standard basiert auf physikalischer Ebene auf der Fibre Channel Technologie, einem Konzept zur Verbindung von Rechnern und Speichersystemen. Die Architektur von Fibre Channel besteht aus vier Ebenen, von denen die beiden unteren FC-0 (Interface und Medium) und FC-1 (Encode/Decode) in Gigabit-Ethernet benutzt werden. Durch diesen Rückgriff ließ sich die Entwicklungszeit des neuen Standards beschleunigen. Zur Stationsverbindung gibt es drei Varianten:

- eine Multimode-Verbindung mit einer maximalen Länge von 550 m
- eine Monomode-Verbindung mit einer maximalen Entfernung von 3 km
- eine kupferbasierte Verbindung mit einer maximalen Länge von 25 m.

Um Verbindungen auch für UTP-Kabel der Kategorie 5 über 100 m zu ermöglichen, waren Vorarbeiten zu leisten. Die Standardisierung dieser Option ist deshalb in eine gesonderte Arbeitsgruppe 802.3ab ausgelagert worden. Die Übertragungsdistanzen liegen ganz erheblich unter den bisher in den Normierungen festgelegten Längen. Würde Gigabit-Ethernet wie die herkömmlichen Technologien über lediglich zwei Leiterpaare übertragen, wäre eine Übertragungsfrequenz von 166 MHz die Folge, womit eine Cat-5-Verkabelung von 100 MHz überfordert wäre. Die gleichzeitige Nutzung aller vier in den Verkabelungsstandards vorgesehenen Leiterpaare halbiert die Frequenz auf 83 MHz. Dieser Vorschlag und die gleichzeitige Übertragung in beide Richtungen stellen erheblich höhere Anforderungen an ein Verkabelungssystem und gefährden zusätzlich die Rückwärtskompatibilität der Steckverbindungen.

Das Zusammenspiel der funktionalen Elemente von Gigabit-Ethernet zeigt die Abbildung 4.4.

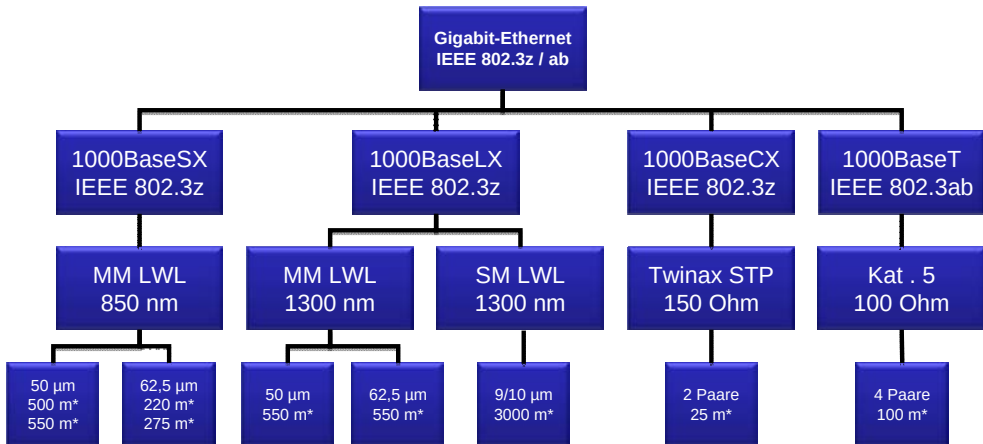


Bild 4.4 Gigabit-Ethernet-Schichten (Quelle: Kerpen)

Quelle: Kerpen

4.2.2 Varianten

Zwei physikalische Definitionen erlauben die Übertragung von Gigabit-Ethernet über Glasfaserkabel. Die Variante 1000Base-SX (Short Wave) zielt dabei auf den „Low-Cost“-Bereich als Tertiär-Verkabelung oder den Sekundärbereich. Die Wellenlänge des Lasers beträgt 770 – 860 nm, die Signalisierung basiert auf der Fibre-Channel-Spezifikation. Die 1000Base-LX (Long Wave) Definition legt die Wellenlänge des Lasers auf den Bereich von 1270 – 1355 nm fest, basiert auf der gleichen Fibre-Channel-Spezifikation wie die 1000Base-SX-Variante und zielt auf den Campus-Backbone. Während für die SX-Variante oft aus Kostengründen eine LED-Quelle eingesetzt wird, kennt die LX-Form nur einen Laser. Auf Grund der Schaltzeiten eines LEDs oder Lasers wird das Licht mit geringer oder hoher Intensität auf das Medium gegeben. 1000Base-X nutzt die 8B/10B Kodierung in Verbindung mit dem non-return to zero (NRZ) Verfahren.

Ergänzt werden die Spezifikationen durch weitere zwei Festlegungen für Kupferkabel. 1000BaseCX benutzt ebenfalls die 8B/10B-Codierung auf seriellen Leitungen mit 1,25 Gbit/s und 150-Ohm. Dabei ist zu beachten, dass der IBM-Kabeltyp 1 – die traditionelle Token-Ring-Verkabelung – im IEEE 802.3-Standard explizit als nicht empfehlenswert eingestuft wird.

1000Base-T ist unter der Bezeichnung IEEE 802.3ab standardisiert und überbrückt 100 m auf herkömmlichen UTP-Kabeln der Kategorie 5. 1000Base-T nutzt alle vier Adernpaare des UTP-Kabels und reduziert die Übertragungsgeschwindigkeit auf 250 Mbit/s pro Paar. Dabei erfolgt die Übertragung auf jedem Adernpaar bidirektional. Ob dabei eine aufwendige Neuverkabelung überflüssig ist, hängt davon ab, ob eine vierpaarige Verkabelung bis zur Endstation vorhanden ist und ob gewisse Qualitätsparameter eingehalten werden können. Diese hängen mit dem Übertragungsverfahren zusammen. 1000Base-T nutzt das 4D-PAM5 Kodierungsverfahren, das Vollduplex-Übertragungen gestattet. Diese gleichzeitige Kabelnutzung führt naturgemäß zu permanenten Kollisionen, was komplexe Span-

nungsmuster zur Folge hat. Mit entsprechenden Schaltkreisen für Echo-Unterdrückung, Layer 1 Forward Error Correction und weiteren Konzepten wird der 1-Gigabit-Durchsatz erreicht. In einer übertragungsfreien Periode finden sich neun Spannungsniveaus auf dem Kabel, während einer Übertragung hingegen 17, die das Signal eher analog denn digital erscheinen lassen.

Wie schon Fast-Ethernet kennt auch 1000Base-T das Auto-Negotiation-Prinzip, also die automatische Festlegung der Verbindungsparameter. Die Auto-Negotiation bezieht sich auf die Geschwindigkeit und den Duplexmodus und erfolgt sowohl beim Einschalten als auch beim Umstecken eines Kabels.

Durch die Nutzung aller vier Adernpaare kommt es zu Übersprechen von mehreren signalführenden Adernpaaren auf ein anderes Adernpaar. Die Powersum-Parameter der neuen Kabelkategorien nehmen diesen Effekt in die Kabelmessung als Qualitätsparameter auf. Sie bilden die effektive Summe der Störeinflüsse, wenn auf allen vier Paaren gleichzeitig übertragen wird. Die beiden Maße, die diesen Effekt berücksichtigen, werden als FEXT und ELFEXT bezeichnet. Sie drücken eine Kennzahl aus, die die Signaleinkopplung von einem Leitungspaar auf ein benachbartes misst. Anders als beim Nah Nebensprechen NEXT wird das Übersprechsignal am entferntesten Ende der Verbindung bestimmt. Beim FEXT-Verlust handelt es sich dabei um das Verhältnis der am entferntesten Ende der Verbindung gemessenen Signalamplitude und der Signalamplitude, die am nahen Ende der Verbindung an ein anderes Leiterpaar gelegt wird. Der ELFEXT-Parameter ist demgegenüber das errechnete Verhältnis zwischen dem gemessenen FEXT-Verlust und der Dämpfung. Dieser Wert wird dann kritisch, wenn zwei oder mehr Leitungspaare Signale in dieselbe Richtung übertragen.

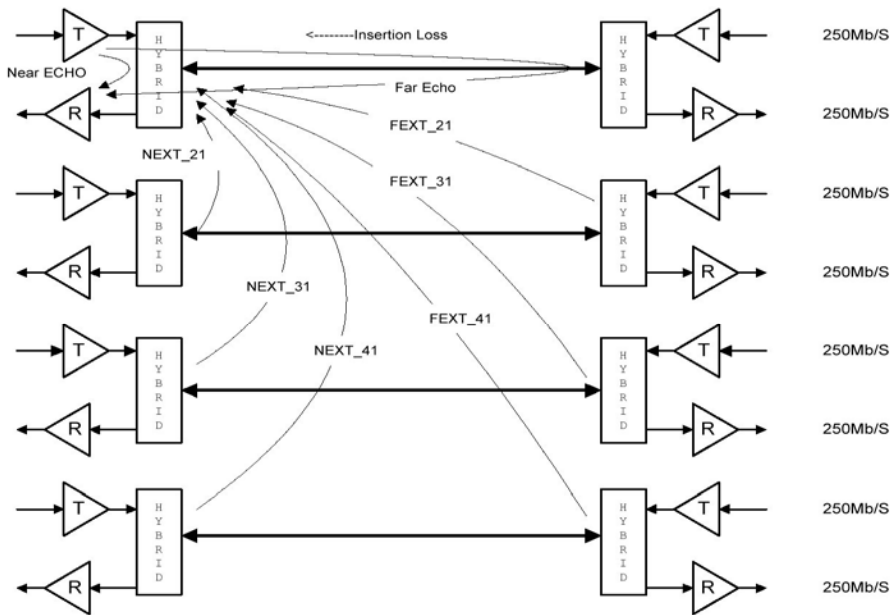


Bild 4.5 ELFEXT-Werte

Zur weiteren Beurteilung der Übertragungsgüte spielen zwei Parameter eine Rolle: Delay-Skew bezeichnet die Differenz der Signallaufzeiten von Paar zu Paar und der Return-Loss oder Rückflusdämpfung misst das reflektierte Signal, das auf dem Impedanzunterschied der Komponenten und des Kabels beruht. Je höher dieser Wert ausfällt, desto schlechter ist die Übertragungscharakteristik.

Die Spezifikation der physikalischen Schicht lehnt sich an diejenige der Fast-Ethernet-Variante an. Sie gliedert sich wie dort in drei Teilbereiche:

- **Physical Coding Sublayer (PCS)** für die Signalcodierung, die hier nach dem 8B/10B-Schema des Fibre Channels erfolgt. Das Verfahren wandelt Gruppen von 8 Bit in Symbole von 10 Bit Länge um, so dass zu den ursprünglichen Datensymbolen weitere Kontrollzeichen hinzukommen.
- **Physical Medium Attachment (PMA)** für die Serialisierung der Daten.
- **Physical Medium Dependent (PMD)** als die unterste physikalische Schicht für die Definition von Kabeln, Steckern und Treibern.

Gigabit-Ethernet ist als Halbduplex- und Vollduplex-Technologie standardisiert. Durch das CSMA/CD-Protokoll wird im Halbduplex-Betrieb die maximale Entfernung zweier Stationen allerdings reduziert.

Um die Arbeitsweise zu erhalten, muss das minimal zulässige Ethernet-Paket erweitert werden. Diese Modifikation basiert auf folgendem Umstand: Da jede Station den Sendevorgang beginnen kann, wenn sie das Medium als frei erkennt, muss ein Ethernetpaket eine Mindestlänge aufweisen, um zu verhindern, dass die sendende Station bereits mit der Übertragung endet und an einen erfolgreichen Abschluss glaubt, obwohl eine Kollision auftrat. In diesem Falle würde eine Kollision erst nach Sendeabschluss erkannt, und es bestände keine Möglichkeit der Retransmission. Nur wenn das Paket eine entsprechende Länge aufweist und alle Stationen passiert, kann ein vorzeitiges Senden einer weiteren Station unterbunden werden. Die minimale Paketlänge hängt von der Weglänge zur entferntesten Ethernetstation und zurück ab. Um dieses Problem zu lösen – Gigabit-Ethernet Pakete werden mit der 100-fachen Geschwindigkeit transportiert – muss die unterstützte Paketlänge auf 512 Byte erhöht werden. Dabei ist offensichtlich, dass die Zahl 512 einen Kompromiss darstellt, denn um die Übertragungsrate von 64 Byte bei Fast-Ethernet nachzubilden, wären 640 Byte erforderlich. Die IEEE 802.3z-Arbeitsgruppe hielt die 640-Byte-Erweiterung aber für zu ineffizient und entschied sich für eine verkürzte Variante. Als Tribut an dieses Vorgehen wird die Zahl der zulässigen Repeater auf einen beschränkt und zum anderen die bei den anderen Ethernet-Standards eingebaute Sicherheitsmarge beschnitten. Das ausgewählte Verfahren verlängert Pakete, die kleiner als 512 Byte sind, während Pakete größer als 512 Byte unverändert bleiben. Dieses Verfahren wird als Carrier Extension bezeichnet. Die zusätzlichen Extension Symbole werden beim Empfänger vor der Berechnung der Prüfsumme wieder aus dem Paket entfernt. Diese Modifikation beeinflusst insbesondere Applikationen mit einem hohen Volumen an kleinen Paketen. Datenverkehr mit exzessivem Anteil an 64-Byte-Paketen kann den Durchsatz auf 120 Mbit/s drücken; ein Wert, der nur knapp oberhalb von Fast-Ethernet liegt und nur 12% der Bandbreitenkapazität ausnutzt. In allgemeinen Anwendungsszenarien variiert die Rahmengröße allerdings im Bereich von 200 bis 500 Byte, was einem Auslastungsgrad von 300 bis 400 Mbit/s entspricht. Diesen Nachteil soll ein spezielles Bursting-Verfahren ausgleichen.

4.2.3 Besonderheiten

Um die Unterauslastung des Mediums im Falle vieler kleiner Rahmen zu verringern, bietet Gigabit-Ethernet das „**Packet-Bursting**“ an, d.h. die Zusammenfassung vieler Minimalpakete zu einem Größeren. Mit einer Carrier Extension kann es im Extremfall zur Versendung von 448 Füllbytes kommen, ein Ergebnis, das den effektiven Datendurchsatz stark reduziert. Möchte eine Station mehrere Pakete senden, wird das Erste gemäß Carrier Extension aufgefüllt. Alle Nachfolger lassen sich mit dem kleinstmöglichen Abstand bis zu einer maximalen Größe von 8 KByte anfügen. Die Schwierigkeit besteht jedoch darin, dass die meisten Applikationen mit diesem Mechanismus nicht umgehen können und demzufolge neu implementiert werden müssen. Außerdem ergeben sich anwendungsabhängige Probleme. Sendet ein Client in einem Online-Transaktionssystem einen kleinen Rahmen, so kann das Packet Bursting dazu führen, dass die Station sehr lange auf die Bestätigung warten muss, weil keine weiteren Rahmen zur Übertragung anstehen.

Diese Korrekturen treffen nur für Stationen zu, die im Halbduplex-Modus arbeiten. Im Vollduplex-Modus senden und empfangen die Stationen auf getrennten Leitungen, so dass niemals Kollisionen auftreten können und sie nicht darauf warten müssen, die Übertragungsberechtigung zu erhalten. Folglich können weiterhin der reguläre Ethernet-Rahmen und die 96-Bit Interframe Gap Verwendung finden. Die Eigenschaften des MAC-Layers der unterschiedlichen Ethernet-Varianten fasst die Tabelle 4.3 zusammen:

Tabelle 4.3 MAC-Layer Eigenschaften der Ethernetvarianten

Merkmal	Ethernet	Fast-Ethernet	Gigabit-Ethernet
Slottime	512	512	4096
Interframe Gap in ms	9,6	0,96	0,096
Max. Framesize	1518	1518	1518
Min. Framesize	64	64	64
Extend Size in bits	0	0	448
Burstlänge	0	0	8 KByte

- Ein Vollduplex-Port stellt einen Puffer zur Verfügung, um Daten zwischenspeichern, die von einer Station einlaufen, aber vom Empfänger nicht zeitgerecht verarbeitet werden können. Damit ein Pufferüberlauf nicht einen Paketverlust zur Folge hat, integriert Ethernet nun eine **Flusskontrolle**. Sie verhindert, dass eine Station weiterhin sendet, obwohl der Empfänger keine Pakete mehr entgegennehmen kann. Hierzu wird nach Erreichen eines Schwellwertes ein PAUSE-Paket an den Sender geschickt, das diesen veranlasst, die Sendung einzustellen und erst nach einer definierten Pausenzeit fortzusetzen. Die Abstimmung der Flusskontrolle erfolgt über die Auto-Negotiation.

■ 4.3 Die Zukunft: 10-GbE

Die Highspeed Study Group (HSSG) zur Fortentwicklung von Ethernet hat hoch gepokert und gewonnen. Der 10-GbE-Standard ignoriert zwar den Kern des Ethernets – das CSMA/CD-Verfahren – darf sich aber dennoch Ethernet nennen. Ausgangsmotiv für diesen Sinneswandel war die Anforderung, das Zehnfache der Ethernet-Geschwindigkeit in Kombination mit einer Entfernung von 80 km zu verwirklichen. Beiden Anliegen steht jedoch das herkömmliche Kollisionsverfahren im Wege. Ein Verzicht darauf bedeutete die Gefahr, vom Standardisierungsgremium der IEEE nicht als Arbeitsgruppe unterhalb des 802.3-Standardkomitees anerkannt zu werden. Dass das Gremium dennoch im Sinne der beteiligten Unternehmen entschied, ermöglicht, dass das Hochgeschwindigkeitsverfahren das bewerbwirksame Etikett Ethernet führen darf.

Was war der Auslöser für die Fortentwicklung von Ethernet? Unternehmen sehen sich hohen Bandbreitenanforderungen im Tertiärbereich durch neuartige Anwendungen wie Storage Area Networks (SAN), Multimedia, Data Warehousing oder Grid-Computing gegenüber. Die sich daraus ergebenden Ansprüche an Zugriffs- und Antwortgeschwindigkeit lassen sich nur mit einer neuen Technologien ausreichend beantworten. 10-GbE als logische Weiterentwicklung der bisher genutzten Standards liefert durch die Skalierbarkeit für unterschiedliche Entfernungen, die Verwaltungsmöglichkeit mit herkömmlichen Ethernetwerkzeugen und die preiswerte Beschaffung die folgerichtige Alternative.

4.3.1 Eigenschaften

Die HSSG einigte sich auf einige Kernpunkte für das neue Verfahren: So sollen nur Voll-duplex-Verbindungen, d.h. getrennte Hin- und Rückkanäle sowie Sternstrukturen mit Punkt-zu-Punkt-Verbindungen als Netztopologie unterstützt werden. Grundlage hierfür bilden Glasfaserkabel für die eine neue Glasfaserstandardkategorie OM3 für laseroptimierte Multimode-Fasern (LOMMF) entwickelt wurde. Begleitet wird diese Technologie durch VCSELs (Vertical Cavity Surface Emitting Laser), die eine schnellere, besser fokussierende Konversion in Licht innerhalb des 850 nm Fensters erlaubt. 10-GbE lässt sich daher als MAN- und WAN-Übertragungsmedium positionieren. Derzeit existieren mehrere Optionen:

- 10GBase-SR zum Anschluss von Multimode-Glasfaser im 850 nm-Bereich.
- 10GBase-SX zum Anschluss von Multimode-Glasfaser über eine Entfernung von maximal 300 m.
- 10GBase-LX für Mono- oder Multimode Glasfaser, mit denen sich eine Reichweite von 15 km erzielen lässt.
- 10GBase-EX für Monomode Glasfaser, mit der sich Distanzen bis zu 40 km überbrücken lassen.

Mit der letzten Möglichkeit betritt Ethernet Neuland, denn erstmals wird die Wellenlänge von 1550 nm benutzt und mit der Entfernung von 40 km und mehr der WAN-Markt erschlossen. Mit dem Schritt in das WAN hat die HSSG sich jedoch ein weiteres Problem

geschaffen. Da die Hersteller von WAN-Geräten nicht an der Standardisierung beteiligt sind, ist eine Diskussion um die exakte Geschwindigkeit entbrannt. Die LAN-Vertreter favorisieren den exakten Wert von 10 Gbit/s als Vielfachem der anderen Ethernet-Varianten, während die WAN-Fraktion eine Geschwindigkeit von 9,58464 Gbit/s anstrebt. Dieser Wert leitet sich als Vielfaches der weitgehend identischen WAN-Verfahren SONET und SDH ab, deren Übertragungsraten mit der Bezeichnung OC-192 bzw. STM-64 angegeben werden. Die Schwierigkeit entsteht an der Nahtstelle des LANs zum WAN, wenn der Ethernet-Verkehr in das WAN-Backbone übergeht. Die HSSG schlägt einen Kompromiss vor, der beide Geschwindigkeiten vorsieht, aber den Nachteil besitzt, zwei physikalische Schnittstellen unterstützen zu müssen. Werden Ethernet-Daten zwischen LAN und WAN übertragen, wird ein Koppellement für die entsprechende Umsetzung sorgen. Der MAC-Layer unterstützt damit zwei Datenraten: für LANs die Übertragungsgeschwindigkeit von exakt 10 Gbit/s und für WAN-Verbindungen 9,58464 Gbit/s, sowie ein medienunabhängiges Interface XGMII.

Der Verzicht auf das CSMA/CD-Verfahren wird ebenso wie der geringfügige Geschwindigkeitsunterschied keine tiefgreifenden Konsequenzen haben. Da die Spezifikation weiterhin das ursprüngliche Rahmenformat verwendet, ist die Abwärtskompatibilität gesichert. Der Ersatz der Netzkarten für Server oder Endstationen ist damit nicht notwendig. Die Übernahme der Framedefinition garantiert auch, dass Standards wie die Paketpriorisierung oder die Bildung virtueller LANs ihre Gültigkeit behalten. Die Zielvorgaben der neuen Ethernet-Version lassen sich gemäß Tabelle 4.4 zusammenfassen:

Tabelle 4.4 Merkmale von 10-GbE

Merkmal
Beibehaltung des ursprünglichen Frameformates
Einhaltung der IEEE 802 Vorgaben mit Ausnahme des Hamming-Abstandes
Beibehaltung der minimalen und maximalen Rahmenlänge
Vollduplex-Modus nach IEEE 802.3 x
Sterntopologie mit Punkt-zu-Punkt-Verbindungen
Optionales Medien-unabhängiges Interface
Unterstützung von IEEE 802.3 ad (Link Aggregation)
Zwei physikalische Schnittstellen: LAN: 10 Gbit/s und WAN: OC-192 bzw. SDH STM-64
Drei Interfaces: 10GBase-SX, 10GBase-LX und 10GBase-EX

Für das Zusammenwachsen der Netze spielt der neue 10GBase-T-Standard eine herausragende Rolle. Im Juni 2006 verabschiedete die IEEE die Norm 802.3an, die 10 GbE über symmetrische Kupferkabel spezifiziert. Wie bei Gigabit-Ethernet überträgt jedes der vier Adernpaare 2,5 Gbit/s bidirektional. Als Kodierung einigte man sich auf das PAM-16 Verfahren. Triebfeder des neuen Standards sind amerikanische Unternehmen, die traditionell nur ungeschirmte Verkabelungen einsetzen. Im Verlauf der Diskussion türmten sich einige technische Hürden auf, von denen insbesondere das Alien Crosstalk hervorsticht.

Alien Crosstalk, das im Rahmen dieser Standardisierungsbemühungen das erste Mal auftritt, gibt an, wie stark Signale eines Adernpaares von einem oder mehreren benachbarten Kanälen beeinflusst werden. Leider lässt sich dieses Phänomen nur schwer erfassen, da es zufällig und unregelmäßig auftritt. Bei geschirmten Verkabelungssystemen ist es allerdings nicht notwendig Alien Crosstalk in der Installation zu messen, wenn die Kabel definierte Anforderungen an die Kopplungsdämpfung erfüllen. Der Grund hierfür liegt darin, dass sich durch das komplexere Kodierungsverfahren geringere Spannungsunterschiede zwischen den einzelnen logischen Zuständen ergeben, die eine deutliche Zunahme der Empfindlichkeit gegenüber eingekoppelten Störsignalen verursachen. Die Ursache für Störsignale können dabei sowohl benachbarte Kabel und Steckverbindungen als auch systemfremde Quellen sein. Die höheren Frequenzen haben ihren Ausdruck auch in spezifischen Anforderungen für die Dämpfung, PSNEXT, PSFEXT und Return Loss. Gleichzeitig müssen die Verkabelungssysteme einen hohen Signal-Rausch-Abstand und eine hohe Fremdnebensprechdämpfung aufweisen. Der Alien Crosstalk-Effekt lässt sich im Gegensatz zu NEXT oder Dämpfung nicht elektronisch kompensieren. Er kann jedoch durch Doppelschirmung von S/FTP-Kabeln und durch modular geschirmte Anschlusstechnik vermieden oder unterdrückt werden.

Eine Beschreibung des Alien Crosstalk-Phänomäns in Formeln oder Regeln ist nicht möglich. Dennoch bestimmt Alien Crosstalk wesentlich die erreichbaren Längenrestriktionen. Die typischen Einsatzszenarien für 10GBase-T beschreibt die folgende Tabelle 4.5:

Tabelle 4.5 MAC-Layer Eigenschaften der Ethernetvarianten

Länge	Alien Crosstalk	Kabeltyp
100 m	62 dB	Cat 7 STP
55 m	47 dB	Cat 6 UTP
100 m	60 dB	Cat 6 STP
100 m	60 dB	Cat 6a

 Für 10-GbE gibt es keine Repeater, da der Halbduplex-Modus nicht unterstützt wird.

Die Spezifikation der physikalischen Schicht hängt vom jeweiligen Substandard ab. Der Standard für die unterste Schicht gliedert sich in drei von Fast-Ethernet bekannte Teilbereiche, die zusammen die PHY-Spezifikation der Schicht 1 bilden:

- Physical Medium Dependant (PMD)
- Physical Coding Sublayer (PCS)
- Physical Medium Attachment (PMA)

Die PMD-Ebene ist verantwortlich für die Signalübertragung. Zu ihren typischen Funktionen gehören die Verstärkung, Modulation und Glättung von Signalen. Unterschiedliche PMD-Devices unterstützen dabei unterschiedliche Medien. Optische Transceiver sind ein

Beispiel für Geräte der PMD-Schicht. Die PCS-Schicht ist für Codierung/Decodierung der Ethernetframes zuständig. Als Codierverfahren für WAN-Anwendungen dient eine Block-Codierung nach 64B/66B, die nur zwei zusätzliche Bits für einen 64 Bit Datenblock benötigt. Für den LAN-Bereich kommt die bekannte 8B/10B-Codierung zum Einsatz.

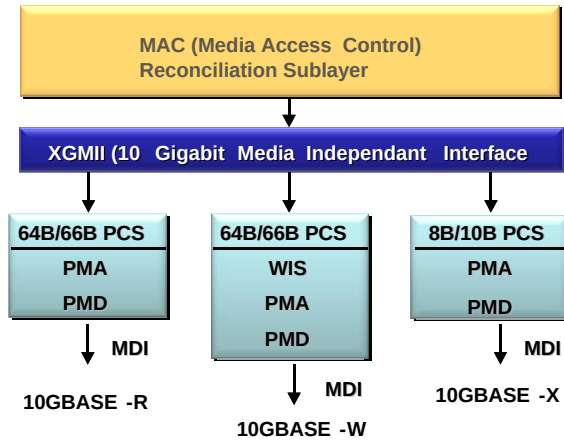


Bild 4.6 10-GbE Schichten

4.3.2 Vorteile

Da 10-GbE nur den Vollduplex-Modus unterstützt, lässt sich das Ethernet-Protokoll auf unbegrenzte Distanzen ausdehnen. Nur die physikalische Übertragung und deren Medien wirken als begrenzende Faktoren. Damit ist 10-GbE gegenüber Ethernet nicht nur schneller, sondern erschließt sich darüber hinaus völlig neue Anwendungsbereiche.

Worin liegen die Vorteile dieser Variante?

- Es eröffnet sich ein einfacher Weg, Unternehmensnetze auszubauen.
- Die bisher installierten Ethernet-Ports werden nicht wertlos.
- Die Technologie ist schneller, preiswerter und einfacher als alle Alternativen.

Da für die neue Technologie ein Interface spezifiziert wird, das die Datenrate und die Anforderungen von SONET (Synchronous Optical Network) OC-192 bzw. SDH (Synchronous Digital Hierarchy) STM-64 erfüllt, wird Ethernet kompatibel mit den Weitverkehrstechniken und ermöglicht eine direkte Verknüpfung von paketbasierten IP/Ethernet-Switches mit der time-division-multiplexed Infrastruktur von SONET/SDH. Damit wird erstmals der Transport von Ethernet über WAN-Strecken möglich. Die SONET/SDH-Kapselung erlaubt damit eine Ende-zu-Ende-Verbindung auf Ethernet-Basis.

10-GbE entspricht Ethernet und arbeitet folglich mit dem gleichen Paketformat und dem gleichen MAC-Protokoll. Geringfügige Anpassungen sind lediglich für die ergänzenden Protokolle notwendig.

Tabelle 4.6 Anzupassende Protokolle

Name	Beschreibung
802.3ad	Link Aggregation
802.1p	Prioritätssteuerung
802.1Q	VLAN-Unterstützung
MPLS	Layer-3-Switching Dienst
SNMP	Ethernet-Management
RMON	Remote Monotoring für Ethernet

Der 10-GbE Standard IEEE 802.3ae definiert zwei PHY-Typen: LAN PHY und WAN PHY. Der WAN-Typ ist lediglich eine einfache Erweiterung des LAN-Merkmals.

Tabelle 4.7 LAN/WAN-Spezifikationen

	Bezeichnung	Reichweite	PMD	LWL-Typ
LAN	10GBase-LX4	300 m	1310 nm WDM	Multimode
	10GBase-SR	65 m	850 nm seriell	Multimode
	10GBase-LR	10 km	1310 nm seriell	Monomode
	10GBase-ER	40 km	1550 nm seriell	Monomode
WAN	10GBase-LW4	300 m	1310 nm WDM	Multimode
	10GBase-SW	65 m	850 nm seriell	Multimode
	10GBase-LW	10 km	1310 nm seriell	Monomode
	10GBase-EW	40 km	1550 nm seriell	Monomode

LAN PHY und WAN PHY arbeiten über das gleiche PMD und unterstützen daher die gleiche Distanz. Sie unterscheiden sich allein durch die Kodierung.

Tabelle 4.8 LAN PHY und WAN PHY Unterschiede

PHY	Seriell LAN	Seriell WAN	4-Adern-LAN
	64B/66B	64B/66B	XAUI 8B/10B
PMD	Seriell		WDM
	850 nm (65 m)		1310 nm (300 m)
	1310 nm (10 km)		1310 nm (10 km)
	1550 nm (40 km)		

Langfristig wird erwartet, dass LAN PHY über einen optischen Switch verläuft und eine Unterscheidung beider Varianten überflüssig wird. Damit definiert 10-GbE einerseits ein LAN PHY, das mit einfacher Kodierung die Ethernetpakete über Glasfaser überträgt und andererseits ein WAN PHY, das Ethernet über die SONET/SDH-Infrastruktur in den Weitverkehrsbereich verlängert. Die WAN PHY-Schnittstelle verbindet Netzwerkkomponenten wie Router und Switches mit SONET/SDH. Dies erlaubt die Erweiterung von Ethernet auf dieser Technologie bisher verschlossene Bereiche. Über die WAN PHY-Schnittstelle verhalten sich zwei Router als wären sie direkt über einen Ethernetlink miteinander verbunden.

■ 4.4 Technologische Trends

In den vergangenen Jahren hat sich die Übertragungsrate von 10 GBit/s als wirtschaftliche Lösung zum Aufbau der erforderlichen Kapazität in den Weitverkehrsnetzen der Service Provider erwiesen. Mit der Spezifikation von 40- und 100-Gigabit-Ethernet nach der Norm IEEE 802.3ba steht seit 2010 die Basis für die nächste Generation von Ethernet bereit. Die Reichweite wird sich von wenigen Metern auf Kupferkabeln bis zu 40 km auf Monomodefasern erstrecken. Dabei wird nur noch der Vollduplex-Betrieb unterstützt, während beim Rahmenformat und der minimalen und maximalen Rahmengröße aus Kompatibilitätsgründen keine Änderung erfolgt. Bei den Standards für Kupferkabel und für Multimodefasern werden Varianten spezifiziert, bei denen parallel auf zehn Kabeln/Fasern übertragen wird. Bei Monomodefasern stützt sich die Übertragung auf die WDM-Technik, d.h. einer Datenübertragung mittels vier Wellenlängen auf einer Faser und einer Datenrate von je 25 GBit/s. Der Standard 802.3ba spezifiziert folgende Parameter:

Tabelle 4.9 100 GBit/s Standards

Bezeichnung	Reichweite und Medium	Anmerkungen
100GBase CR10	7 m mit Kupferkabeln	10 Adern mit je 10 GBit/s
100GBase SR10 (Short Reach)	100 m mit Multimodefasern	10 Multimodefasern mit je 10 GBit/s
100GBase LR 4 (Long Reach)	10 km mit Monomodefasern	4 Wellenlängen mit je 25 GBit/s auf einer Faser (WDM-Technik)
100GBase ER 4 (Extended Reach)	40 km mit Monomodefasern	4 Wellenlängen mit je 25 GBit/s auf einer Faser (WDM-Technik mit Halb-leiterverstärker)

Ersichtlich ist, dass für jede Übertragungsrichtung mehrere Adern/Fasern benötigt werden. So nutzt 40 GBit/s vier Übertragungswege zu 10 GBit/s. Komplexer erweist sich die Übertragung bei 100 GBit/s. Die theoretische Option bietet einmal 100 GBit/s, zweimal 50 GBit/s, viermal 25 GBit/s, fünfmal 20 GBit/s oder 10 mal 10 GBit/s an. Die letzte Variante ist bisher bei Multimodefasern eingesetzt und die viermal 25 GBit/s-Variante wird bei Monomode bevorzugt. Um die Daten auf die einzelnen Adern/Fasern zu verteilen, kommt ein Round-Robin-Konzept zum Einsatz.

Mit dem veränderten Übertragungskonzept sind auch andere Verbindungstechniken notwendig. Drei Formfaktoren werden diskutiert:

- CFP (C Formfaktor Pluggable) für 40 und 100 GbE. Er besteht aus 12 Sende- und Empfangsleitungen zu jeweils 10 GBit/s. Aufgrund seiner mechanischen Dimensionierung passt er für Anforderungen von Kupferkabeln und Glasfasern
- CXP ist dem CFP vergleichbar nur deutlich kleiner
- QSFP (Quad Small Formfactor Pluggable) entspricht dem CXP in der Größe, erlaubt aber nur je vier Adern für Sende- und Empfangsaktivitäten.

Die Hochgeschwindigkeitsübertragung bleibt naturgemäß nicht ohne Rückwirkung auf die Durchsatzraten von Switches. Switches mit 44 Ports zu 40 GBit/s benötigen rein rechnerisch 1,76 TBit/s Übertragungskapazität.

Die 100 GBit/s Technologie wird abgesehen von einzelnen Spezialanwendungen noch nicht in nennenswerter Zahl verwendet. In bestimmten Bereichen steigt der Bandbreitenbedarf jedoch massiv. Dazu gehören die Core-Netzwerke, die die zentralen Internetknoten verbinden und die Plattformen der sozialen Netzwerke wie YouTube oder Facebook. So liegt der Bandbreitenbedarf beim Amsterdamer Internet Exchange schon bei einem TBit/s. Dennoch dürfte insbesondere der Preis der Einführung im Vergleich zur etablierten 10 GBit/s Variante einem großflächigen Einsatz noch entgegenstehen. Ob der 40 GBit/s Standard eine Zukunft hat, ist ebenfalls ungewiss, da vielfach die Ansicht besteht, dass dieser Zwischenschritt übersprungen werden sollte, um für die Aufwendungen einen doppelten Technologiewechsel zu vermeiden.

Neben den Kernstandards entwickeln sich rund um Ethernet begleitende Vereinbarungen, die die Akzeptanz der Technologie weiter sichern und die in erster Linie den Stromverbrauch im Auge haben. 10 Gigabit-Ethernet ist zwar hundertmal schneller als Fast-Ethernet, verbraucht aber auch die sechsfache Strommenge. Hinzu kommen die steigende Abwärme in den Switches und die damit verbundene notwendige Regulierung der Raumtemperatur.

- Ein erster Trend versucht die zahlreichen Netzwerkkarten zu vereinheitlichen. Converged Interface Adapters vereinen die traditionellen Network Interface Cards mit den Host Bus Adaptern der Fibre Channel Technologie auf der Basis von 10 Gigabit-Ethernet. Diese Vereinheitlichung reduziert den Stromverbrauch um die Hälfte.
- Energy Efficient Ethernet möchte erreichen, dass ein LAN-Port nur dann Strom verbraucht, wenn auch wirklich Daten übertragen werden. Im Leerlauf soll der Stromverbrauch auf Null sinken. Damit hält eine Idee im LAN Einzug, die im Umfeld von DSL-Zugängen bereits verwirklicht ist. Für eine neue Übertragung werden die beteiligten Kommunikationsports anschließend mit einem Wecksignal in den aktiven Übertragungsmodus versetzt. Diese IEEE-Norm unter der Bezeichnung 802.3az wurde 2010 verabschiedet. Einen Haken hat dieses Konzept für die Anwender: die Technologie greift nur, wenn beide Endpunkte den Standard unterstützen.
- Power-over-Ethernet (PoE) widmet sich der Stromversorgung der Ethernet-Komponenten. Wurde die Stromversorgung der angeschlossenen Endgeräte bisher individuell über ein integriertes Netzteil gelöst, etabliert sich zunehmend die zentrale Versorgung

über das Datenkabel als Alternative. Insbesondere Voice-over-IP Telefone und WLAN Access Points spielen hier die Vorreiter. Grundlage ist die Erweiterung des Ethernet-Standards durch die Variante IEEE 802.3af.

Bei der Ethernet-Übertragung werden traditionell nur vier Adern des Kabels für Geschwindigkeiten bis 100 MBit/s genutzt. Die restlichen vier Adern liegen brach. Der neue Standard spezifiziert eine Versorgungsspannung von 48 V bei einem maximalen Strom von 350 mA pro Verbraucher. Unter Berücksichtigung der auf dem Datenkabel entstehenden Verluste führt dies zu einer Leistung von 13 W pro Verbraucher. Neben dem Vorteil einer Verbindung der Bereiche Daten, Sprache und Stromversorgung existiert durch die erhöhte Netzsicherheit in Form einer zentralen unterbrechungsfreier Stromversorgung ein weiterer Nutzen, den Anwendungen wie Webcams, Zugangskontroll- und Zeiterfassungssysteme oder RFID-Scanner zu schätzen wissen.

Schwierigkeiten ergeben sich im Fall von Gigabit-Ethernet, wenn alle acht Adern des Datenkabels genutzt werden. Herstellerabhängig werden dann zwei Adernpaare doppelt verwendet (Phantom Power). Der PoE-Standard lässt aber die Aderbelegung und die Steckverbinder identisch. Generell sind zwei Arten der Leistungseinspeisung möglich:

- Endpunkteinspeisung: der Switch oder Router übernimmt neben der eigentlichen Funktion auch die Einspeisung elektrischer Leistung
- Mitteneinspeisung: eine separate Stromversorgungseinheit wird zwischen Switch oder Router und Netzelement geschaltet. Während das Datensignal transportiert wird, fügt die Stromversorgung die elektrische Leistung hinzu.

Geeignete Endgeräte signalisieren ihre Gegenwart über definierte elektrische Bedingungen:

- einen Widerstand zwischen 19 K Ω und 26,5 k Ω
- eine Kapazität von weniger als 110 nF
- einem Signaturspannungsoffset von wenigstens 2 V
- einem Signaturstrom von maximal 12 μ A

Diese Parameter gewährleisten eine sichere Erkennung der PoE-fähigen Geräte ohne dabei andere nicht PoE-fähige Geräte zu gefährden. Im Verlauf des Signaturprozesses wird eine geringe Spannung an das Endgerät gelegt und der sich ergebende Strom gemessen. Damit ist der Widerstand bestimmbar. Bewegt sich der Widerstand im definierten Bereich, wird die Spannung schrittweise erhöht. Die Erkennung erfolgt innerhalb von 500 ms, die elektrische Leistung wird in weniger als 400 ms nach Erkennen des Gerätes geschaltet.

Dem IEEE-802.3af Standard entsprechend wird pro Port eine Leistung von maximal 15 W zur Verfügung gestellt. Bei einem 48-Port Switch ergibt sich daraus eine Versorgungsleistung von 720 W. Die Einführung von Leistungsklassen mit der Möglichkeit einer optimierten Stromversorgung liegt folglich nahe. Zur richtigen Einstufung der Stromversorgung signalisiert das Endgerät seine Leistungsklasse durch eine Variation des Signaturwiderstandes.

Tabelle 4.10 PoE Leistungsklassen

Klasse	Einsatzgebiet	Eingangsleistungsbereich des Endgerätes	Nomineller Klassifizierungsstrom
0	voreingestellt	0,44 W – 12,95 W	< 5,0 mA
1	optional	0,44 W – 3,84 W	10,5 mA
2	optional	3,84 W – 6,49 W	18,5 mA
3	optional	6,49 W – 12,95 W	28,0 mA
4	nicht erlaubt	zukünftig	40,0 mA

■ 4.5 Zusammenfassung

Ethernet ist der populärste LAN-Standard in heutigen Netzwerken. Daher ist den drei Hauptausprägungen von Ethernet, wie sie sich in der Netzwerkinfrastruktur der Unternehmen wiederfinden, jeweils ein eigener Abschnitt gewidmet. Die Trends am Ende des Kapitels geben einen kurzen Überblick über die stete Fortentwicklung und den ungebrochenen Drang nach technologischen Verbesserungen und steigender Bandbreite.

Die Originalinformationen zu Ethernet sind unter folgenden Links abgelegt:

<http://standards.ieee.org/getieee802/download/802.2-2-1998.pdf>

<http://standards.ieee.org/getieee802/802.3.html>



Noch Fragen ...? Ja ...

Kann Ethernet seinen Wirkungsbereich ausdehnen?

Ja, die Konvergenz von LAN und Speichernetzwerken macht nicht nur schnelle, sondern auch sichere Varianten notwendig. Ein erster Schritt zu Ethernet im Rechenzentrum ist der Standard DCB (Data Center Bridging) bzw. FCoE (Fibre Channel over Ethernet).

■ 4.6 Wissensüberprüfung

1. Kann sich Ethernet im WAN-Bereich etablieren? Geben Sie ihre Einschätzung wieder?
2. Warum ist der Autonegotiation-Prozess so wichtig?
3. Hat sich der CSMA/CD-Algorithmus für alle Ethernet-Standards erhalten?
4. Geben Sie einen Überblick über die in den einzelnen Standards verwendeten Codierungsverfahren.
5. Wird die Präambel des Frames in den aktuellen Ethernet-Varianten noch benötigt?

6. Kann zwischen den einzelnen Standards ohne Berücksichtigung der Verkabelung gewechselt werden?
7. Welche Übertragungsrate erreicht vollduplex Fast Ethernet?
8. Nach welcher Topologie ist 100Base-TX Ethernet aufgebaut?
9. Wie unterscheiden sich Fast-Ethernet und Gigabit-Ethernet?
10. Gibt es ein Anwendungsszenario für 100-Gigabit-Ethernet?

5

IP-Protokollfamilie

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Welche Informationen enthält ein IP-Paket?
- Was bedeuten im Zusammenhang mit TCP/IP ein zuverlässiger Dienst und das Best-Effort-Merkmal?

Kapiteleinführung

Früher kannten nur eine Handvoll Netzwerkspezialisten den Begriff, doch jetzt besteht kein Zweifel mehr: TCP/IP regiert die Netzwelt. Netzwerkprotokolle arbeiten im Verborgenen. Selbst ihre Auswirkungen sind nur über die Anwendungen zu spüren. Trotzdem kann sich niemand des enormen Erfolges von TCP/IP verschließen. Die Protokollfamilie ist zum Star des Netzbereiches geworden. Beinahe alle Dienste sind auf TCP/IP zugeschnitten: Management über SNMP, Internet-Zugang mit DSL oder Telefonie mit Voice over IP.

Der enorme Erfolg des Internets begründet dabei die starke Stellung des Protokolls. Auch wenn es der breiten Öffentlichkeit erst seit kurzem im Bewusstsein ist, TCP/IP gehört zu den Veteranen der Netzwelt. Zum Einsatz kam es, als das amerikanische Verteidigungsministerium den Datenaustausch mittels eines universellen Protokolls vereinheitlichen wollte. Die Umstellung begann Anfang der 80er Jahre und war offiziell 1983 beendet – das Ergebnis hieß und heißt bis heute Internet.

Als die ersten lokalen Netze entstanden, entwickelten die Hersteller ihre Kommunikationsinfrastrukturen selbst. Ein paar dieser Bestrebungen wie IPX von Novell, haben sich lange gehalten, andere sind im Laufe der Jahre vom Markt verschwunden. Von IP war zunächst kaum die Rede. Dieses Bild änderte sich erst, als der PC auch von der Unternehmenswelt ernst genommen wurde. So entstanden PC-gerecht aufgearbeitete TCP/IP-Protokollstacks mit dazugehörigen Programmen. Selbst Microsoft konnte sich diesem Trend nicht verschließen und integrierte das TCP/IP-Protokoll ab Windows 95.

Jede Webseite im Internet, jedes Photo, Bild oder Film – überall sorgt TCP/IP für den Kommunikationsaufbau. Viele Netzwerkspezialisten halten diese Fähigkeit, als Medium für beliebige Anwendungen zu fungieren, als die wichtigste Eigenschaft von TCP/IP. Dennoch: momentan kranken viele Multimediaanwendungen an der schlecht regulierbaren Bandbreite. Quality-of-Service-Merkmale waren in der Ursprungsversion nicht vorgesehen. Niemand dachte vor zwanzig Jahren daran, Filme über IP zu transportieren. Um nachträglich auch diese Anwendungen zu ermöglichen, muss TCP/IP nachgerüstet werden. Dies geschieht durch Protokollzusätze wie RSVP (Ressource Reservation Protocol).

Die grundlegenden Bestandteile der aktuellen Version (IPv4) wurden seit ihrer Einführung nicht verändert, trotzdem sind Kompatibilitätsprobleme sehr selten. Dies ist beeindruckend im Hinblick auf die Aktualisierungsflut moderner Programme. Und noch ein Merkmal sticht hervor: das Internet hat keinen eigentlichen Betreiber. Vielmehr ist es ein sozialer Mechanismus zur Kommunikation, der sich als Verbund tausender Einzelnetze darstellt ohne zentrale Kontrolle und Verwaltung.

■ 5.1 IP Internet Protocol

IP ist ein Standardprotokoll, dessen Spezifikation in den RFCs 791, 950, 919 und 922 mit Aktualisierungen in RFC 1349 zu finden ist. Seine Hauptfunktion besteht darin, Daten vom Sender zum Ziel zu leiten. IP stellt hierfür einen ungesicherten verbindungslosen Dienst zur Verfügung, d.h. es existiert keine Garantie der Paketauslieferung. IP-Pakete können verloren gehen, dupliziert werden oder in unterschiedlicher Reihenfolge das Ziel erreichen. Die Übertragung erfolgt nach dem Best-Effort-Prinzip, bei dem jedes Paket eines Datenstroms isoliert behandelt wird. Das IP-Paket wird gemäß der Modellvorstellung des OSI-Referenzmodells in einem Rahmen der zugrunde liegenden Schicht 2 transportiert, für den Längenrestriktionen existieren. So ist für Ethernet z.B. eine Größe von 1500 Byte typisch. IP selbst kennt keine Obergrenze für seine Paketgröße, da es in der Lage ist, Pakete zu fragmentieren und wieder zusammensetzen. Lediglich eine Untergrenze von 576 Byte ist vorgesehen. IP-Fragmente besitzen alle einen Header, der im Wesentlichen der Kopie des Originals entspricht. Schwierigkeiten entstehen nur bei Verlust eines Fragmentes, da IP das Fehlen eines Bruchstückes als Totalverlust interpretiert.

Zur Realisierung seiner Funktion definiert IP ein eigenes Paketformat, mit einem Header, der im Minimum 20 Byte umfasst:

0	4	8	16	31
Version	Headerlänge	Dienstgüte	Paketlänge in Byte	
Identifikation			Flags	Fragment Offset
Time to Live		Protokoll	Headerprüfsumme	
Quell-IP-Adresse				
Ziel-IP-Adresse				
Optionen				Padding
Nutzdaten				

Bild 5.1 IP-Header

Die Headerfelder haben folgende Bedeutung:

- **Version:** Spezifiziert die genutzte IP-Version. Gegenwärtig wird ein Wechsel von der Version 4 auf die neue als IP Next Generation bekannte Version 6 vorbereitet.

- **Länge (IHL=IP-Header-Length):** Gibt die Länge des Paketheader, gemessen in 32-Bit-Worten, an. Diese Angabe ist aufgrund der variablen Länge des Optionsfeldes notwendig.
- **Dienstgüte:** Dieses Feld enthält drei Teilfelder:

0 – 2	3 – 6	7 Bit
Priorität	ToS	MBZ

Das Prioritätsfeld, d. h. die Bits 0 – 2, unterscheidet folgende Klassen:

Tabelle 5.1 Prioritätsklassen

Bits	Bedeutung
000	Standard
001	Priorität
010	Sofort
011	Flash
100	Flash überschreiben
101	Kritisch
110	Internetzwerkkontrolle
111	Netzwerkkontrolle



Die beiden höchsten Prioritäten (6 und 7) sind für Netzmanagement wie z. B. Routingprotokolle reserviert, verzögerungssensitive Daten wie Voice over IP nutzen die Klasse 5. Der Defaultwert für regulären Datenverkehr beträgt Null, so dass für individuelle Unterscheidungen die Werte 1 – 4 verbleiben.

Das ToS-Feld (Type-of-Service) spezifiziert die Dienstgüte:

Tabelle 5.2 ToS-Feld Spezifikation

Bits	Bedeutung
1000	Minimale Verzögerung
0100	Maximaler Durchsatz
0010	Maximale Zuverlässigkeit
0001	Minimale Kosten
0000	Normaler Dienst

Das MBZ (Must Be Zero)-Bit ist für zukünftige Zwecke reserviert. Alle Felder dieses Dienstgütebytes werden von der Version 4 nicht genutzt, so dass alle Werte mit 0 vorbelegt sind. Die Folge hiervon ist allerdings, dass IP keine Übertragungsqualität berücksichtigt.

 Routingprotokolle wie OSPF unterstützen zwar nach Definition die Auswertung der ToS-Bits, jedoch gibt es keine Implementation, die dies realisiert.

Dieser pragmatische Ansatz ist jedoch nicht das einzige Konzept geblieben, einem IP-Netz Leben in Form von Dienstgütern einzuhauchen. Die IETF schlägt in RFC 2475 das Diffserv-Verfahren vor, das das ToS-Feld in DS-Byte umbenennt und über dieses neue Feld IP-Paket-Dienste abbildet. Ein IP-Paket wird bei seinem Eintritt in das Netz einer Klasse – die IETF nutzt den Begriff „Behaviour aggregate“ – zugeordnet und dann anhand vorgegebener Regeln gemäß seiner Serviceklasse behandelt. Die Dienstqualität wird damit pro Paket definiert. Voraussetzung für dieses Verfahren ist eine zuvor vorgenommene Klassifizierung der Pakete.

 Diffserv ist für alle Hersteller im Netzwerkbereich mittlerweile der Standard zur Festlegung von Dienstgütern. Damit können alle Kommunikationsströme priorisiert werden, unabhängig davon, ob sie über UDP, TCP oder RTP transportiert werden.

- **Paketlänge:** Hier wird die Gesamtlänge des Datenpaketes inklusive Header vermerkt. Zulässig sind Werte im Bereich von 576 bis 65 535 Byte. Die genaue Obergrenze kann konfiguriert werden.
- **Identifikation:** Jedes Datenpaket wird durch eine eindeutige Integerzahl gekennzeichnet.
- **Flags:** Kennzeichen kontrollieren zusammen mit dem Identifikations-Feld die Paketfragmentierung. Sie geben an, ob das Paket geteilt werden muss (MF-Bit = 1) oder ob das aktuelle Teilstück das letzte der Übertragung ist:

1. Bit	2. Bit	3. Bit
0	DF	MF

mit der Bedeutung: DF (Don't Fragment) = 0 Fragmentierung erlaubt; DF = 1 Fragmentierung untersagt; MF (More Fragments) = 0 letzte Fragment des Paketes; MF = 1 mehrere Fragmente folgen.

- **Fragmentation Offset:** Da Pakete den Zielrechner in unterschiedlicher Reihenfolge erreichen können, muss dieser in der Lage sein, die korrekte Ursprungssequenz herzustellen. Dazu dient dieses Feld, das die relative Lage des Paketes zum Anfangspaket in Byte misst. Dadurch ergeben sich Rückwirkungen auf einige andere Felder der nachfolgenden Pakete des Datenstroms, da sich durch die Fragmentierung die Länge des

Gesamtpaketes ändert und die Prüfsumme demzufolge angepasst werden muss. Im ersten Fragment ist dieser Wert immer 0.

- **Time to Live (TTL):** Dieses Feld gibt an, wie lange ein Paket im Internet verbleiben darf. Der Defaultwert beträgt 255. Er dient vor allem dazu, fehlgeleitete oder kreisende Pakete vom Netz zu nehmen. Jeder zu passierende Knoten dekrementiert den Wert bis dieser Null ist. Der Router, der den Wert Null setzt, verwirft das Paket.



Ein TTL-Wert von 0 bedeutet, dass das Paket verworfen wird. Dieses Vorgehen beschreibt die Selbstheilung des Netzes gegen endlos kreisende oder nicht zustellbare Pakete.

- **Protokoll:** Diese Angabe betrifft das logisch gemäß des ISO-Referenzmodells darüber liegende Protokoll, an das IP die Daten seiner Pakete weiterreicht:

Tabelle 5.3 Protokollnummern

Protokollnummer	Protokoll
1	ICMP
2	IGMP
4	IP encapsulation
6	TCP
8	EGP
17	UDP
89	OSPF

- **Header-Prüfsumme:** Zur Erhaltung der Integrität der Header-Einträge wird das 1er-Komplement der 16-Bit-Summe des Protokollkopfes gebildet.



Die Header-Prüfsumme muss von jedem Router auf dem Weg zum Ziel wegen der Anpassung des TTL-Eintrags neu berechnet werden.

- **Adressen:** Die Identifikation der einzelnen Stationen im Netzwerk erfolgt anhand logischer Adressen. Die Zuweisung geschieht nach einem einheitlichen Standard durch eine dazu autorisierte Institution (in Deutschland z. B. der DFN-Verein oder DE-NIC).
- **Optionen:** Eine IP-Implementation muss nicht notwendigerweise über die Fähigkeit verfügen, Optionen zu generieren, aber sie muss in der Lage sein, Pakete, die Optionen beinhalten, zu verarbeiten. Es gibt zwei Arten von Optionsformaten, die vom Wert der Optionszahl im ersten Byte abhängen: ein separates Typebyte oder ein Typebyte, ein Längenbyte und ein oder mehrere Optionsdatenbytes. Das Typebyte besitzt in beiden Fällen den gleichen Aufbau:

0	1	2	3	...	7
Fc	Klasse			Optionsnummer	

wobei Fc (Flag copy) anzeigt, ob das Optionsfeld im Falle einer Fragmentierung in jedes Fragment kopiert werden soll. Die Optionsklasse unterscheidet vier Arten:

Tabelle 5.4 Klassennummern

Klassennummer	Bedeutung
0	Kontrolle
1	Reserviert
2	Debugging
3	Reserviert

Die Optionsnummer ist eine 5-Bit Zahl mit folgender Bedeutung:

Tabelle 5.5 Bedeutung des Optionsfeldes

Options-nummer	Bedeutung
0	End of Option List: Zeigt das Ende der Optionsliste an und wird insbesondere dann verwendet, wenn Optionen die zulässige Paketlänge überschreiten.
1	No Operation: Bewirkt eine Ausrichtung der einzelnen Optionen auf die 32-Bit-Grenze.
2	Security: Wird für Sicherheitsinformationen genutzt (Klasse 0, Fc-Bit = 1).
3	Loose Source and Record Route: Der Sender bietet über diesen Mechanismus den zu passierenden Knoten Routing-Informationen auf der Basis von IP-Adresslisten an. Loose bedeutet in diesem Zusammenhang, dass Zwischenknoten die Informationen wahlweise nutzen dürfen.
4	Internet Timestamp: Klasse 2, Fc-Bit = 0, variables Datenfeld bis zu einer maximalen Länge von 40 Byte.
7	Record Route: Diese Option bietet die Möglichkeit, den Weg eines Paketes durch das Internet aufzuzeichnen (Klasse 0, Fc-Bit = 0).
8	Stream Identifier: Klasse 0, Fc-Bit = 1.
9	Strict Source Routing: Aufzeichnung des Weges durch das Internet (Klasse 0, Fc-Bit = 1) und bindende Nutzung

- **Padding:** Sobald eine Option genutzt wird, besteht die Notwendigkeit, das Paket bis zur nächsten 32-Bit-Grenze mit Nullbits aufzufüllen.

IP kann auf verschiedene Protokolle der Schicht 2 aufsetzen und erweist sich so als äußerst flexibel:

Tabelle 5.6 RFCs für IP

RFC	Protokoll
877	IP on X.25 Networks
948	IP on IEEE 802.3 Networks
894	IP on Ethernet Networks
1005	IP on Serial Lines SLIP
1088	IP on Netbios Networks
1188	IP on FDDI Networks
1201	IP on ARCNET Networks

5.1.1 Fragmentierung

Wenn ein IP-Paket von einem Netzknoten zu einem anderen weitergeleitet wird, durchquert es verschiedene physikalische Netze mit unterschiedlichen zulässigen Paketgrößen. Daraus resultiert die Notwendigkeit, IP-Pakete zu zerlegen und am Ziel wieder zusammenzusetzen. Die IP-Implementation verlangt eine Mindestpaketgröße von 68 Byte als Summe der maximalen Headergröße von 60 Byte und einer minimalen Datenlänge von 8 Byte. Auf der anderen Seite lassen die meisten IP-Realisierungen eine maximale Paketgrößen von 8192 Bytes oder mehr zu. Sobald eine Fragmentierung einsetzt, laufen in einem Knoten folgende Schritte ab:

- Das DF-Flag wird geprüft, um festzustellen, ob eine Fragmentierung erlaubt ist. Ist das Bit gesetzt, wird ein die maximale Größe überschreitendes Paket verworfen.
- Gemäß der zulässigen Paketgröße wird das Datenfeld des Ursprungspaketes in mehrere Teile zerlegt. Alle neu entstandenen Pakete weisen, mit Ausnahme des letzten Paketes, eine Länge in Vielfachen von 8 Byte auf.
- Alle Datenteile werden in neu erzeugte IP-Pakete eingebettet. Die Header dieser Pakete sind Kopien des Ursprungskopfes mit einigen Modifikationen:
 - Das MF-Flag ist in allen Fragmenten mit Ausnahme des letzten gesetzt.
 - Das Fragment-Offset-Feld enthält Angaben darüber (in 8-Byte-Einheiten), wo das Datenfeld in Relation zum Beginn des unfragmentierten Paketes zu finden ist.
 - Enthält das Ausgangspaket Optionen, entscheidet das MSB-Bit des Typebytes darüber, ob die Option in jedes Paketfragment aufgenommen wird. Dies ist bei der Source-Route-Option der Fall.
 - Headerlänge und die Paketlänge sind jeweils neu zu bestimmen.
 - Die Header-Prüfsumme ist neu zu berechnen.

Die Zielstation setzt alle Paketfragmente zu einem einheitlichen Paket zusammen. Die Zusammengehörigkeit liest sie am Identifikationsfeld ab, das von einer Fragmentierung unberührt bleibt. Dazu werden die empfangenen Pakete am Ziel zunächst in einen Puffer

gestellt und ein Timer gestartet. Ist der Timer abgelaufen bevor alle Fragmente eingelaufen sind, wird das Paket verworfen.



Der Zusammenbau (Reassemblierung) fragmentierter Pakete erfolgt nur beim Empfänger (Endgerät).

5.1.2 Routing-Optionen

Das IP Optionsfeld erlaubt mehrere Methoden, IP-Pakete mit Routing-Informationen zu versehen.

- Die **Loose Source Routing Option** liefert für den Sender eine Möglichkeit, Routern explizite Informationen über den Weg zur Zielstation anzubieten und den eingeschlagenen Pfad aufzuzeichnen. Das zugehörige Optionsfeld besitzt folgenden Aufbau:

10000011	Länge	Zeiger	Pfaddaten
----------	-------	--------	-----------

wobei das Längenfeld die Länge der Option angibt, der Zeiger auf die Daten der nächsten zu bearbeitenden IP-Adresse verweist und die Pfaddaten eine Folge von 32-Bit-IP-Adressen darstellen. Sobald ein Paket die Zielstation erreicht und das Pfadangabefeld nicht leer ist (Zeiger < Länge), leitet der Empfänger folgende Verarbeitungsschritte ein:

- Er setzt die nächste IP-Adresse des Pfadfeldes in das Destination-Feld des IP-Headers ein.
- Er trägt die lokale IP-Adresse in die Pfadangabenliste an die Stelle ein, auf die der Zeiger verweist.
- Er inkrementiert den Zeiger um 4.
- Er überträgt das Paket an die neue Zieladresse.

Dieses Vorgehen stellt sicher, dass die korrekte Route im Pfadfeld eingetragen ist. Dieser Ablauf wird als **loose** bezeichnet, weil ein Rechnerknoten auf dem Weg jede Route und eine beliebige Anzahl von Zwischenstationen eintragen kann, um die nächste Adresse zu erreichen.

- Die **Strict-Source-Routing-Option** nutzt das Prinzip der Loose-Source-Option allerdings müssen die passierten Knoten die Pfadvorgabe des Optionsfeldes einhalten. Der Feldaufbau ist für beide Varianten gleich mit dem einzigen Unterschied, dass nun im ersten Feld die Bitkombination 1000 1001 (dezimal 137) steht.
- **Recorded Routing** liefert eine Möglichkeit, den Weg eines IP-Paketes zu verfolgen. Es entspricht dem Mechanismus des Source-Routing, allerdings ist zu Beginn das entsprechende Optionsfeld leer und füllt sich erst, wenn das IP-Paket das Netz durchquert. Dabei ist zu beachten, dass das Optionsfeld ausreichend groß gewählt wird, da sonst vor Erreichen des Ziels kein weiterer Rechnereintrag mehr möglich ist und die Routenaufzeichnung unterbleibt. Auch hier entspricht der Feldaufbau dem der anderen Routingvarianten, im ersten Feld steht nun die Bitkombination 0000 0111 (dezimal 7).

- **Internet Timestamp** ist eine Option, die die Router auf dem Weg zum Ziel zwingt, einen Zeitstempel in das Optionsdatenfeld einzufügen. Der Zeitstempel wird in Sekunden gemessen, kann aber aus zweierlei Gründen nicht zur Performanceoptimierung eingesetzt werden: Die Genauigkeit lässt zu wünschen übrig, da IP-Pakete in weniger als einer Sekunde weitergeleitet werden. Die Messung ist nur bedingt vergleichbar, da Router ihre Uhren nicht synchronisieren.

5.1.3 Routing

Ein Router im IP-Umfeld besitzt Informationen über mehrere Arten von Zielen:

- Rechner, die direkt an das gleiche physikalische Netzwerk angebunden sind wie der Router selbst
- Rechner oder Netzwerke, für die der Router explizite Einträge enthält
- Rechner, die keinen expliziten Eintrag besitzen, werden über einen Defaulteintrag erreicht.

Indirektes Routing tritt auf, wenn der Zielrechner nicht direkt zum Netzwerk der Quelle gehört. Der einzige Weg, das Ziel zu erreichen, besteht darin, einen oder mehrere Router als Vermittlungsstation zu benutzen. Die Adresse des ersten dieser Folge von Routern wird als die indirekte Route bezeichnet. Diese Adresse ist die einzige, die die Quellstation bei unbekanntem Ziel benötigt. Der Router, der das Paket erhält, trägt dann die Verantwortung für die Weiterleitung in Zielrichtung. Durch eine Aneinanderreihung von Routern nach diesem Prinzip entsteht schließlich der vollständige Pfad zur Zielstation. Um den jeweils günstigsten Vermittlungsknoten hinsichtlich bestimmter Merkmale wie Durchsatz, Kosten oder Weglänge auszusuchen, bedarf es weiterer Protokolle, die als Wegewahlalgorithmen oder Routingprotokolle bekannt sind.

Die Verbindung zwischen IP-Routing-Algorithmen und den Zielarten zeigt folgendes Diagramm:

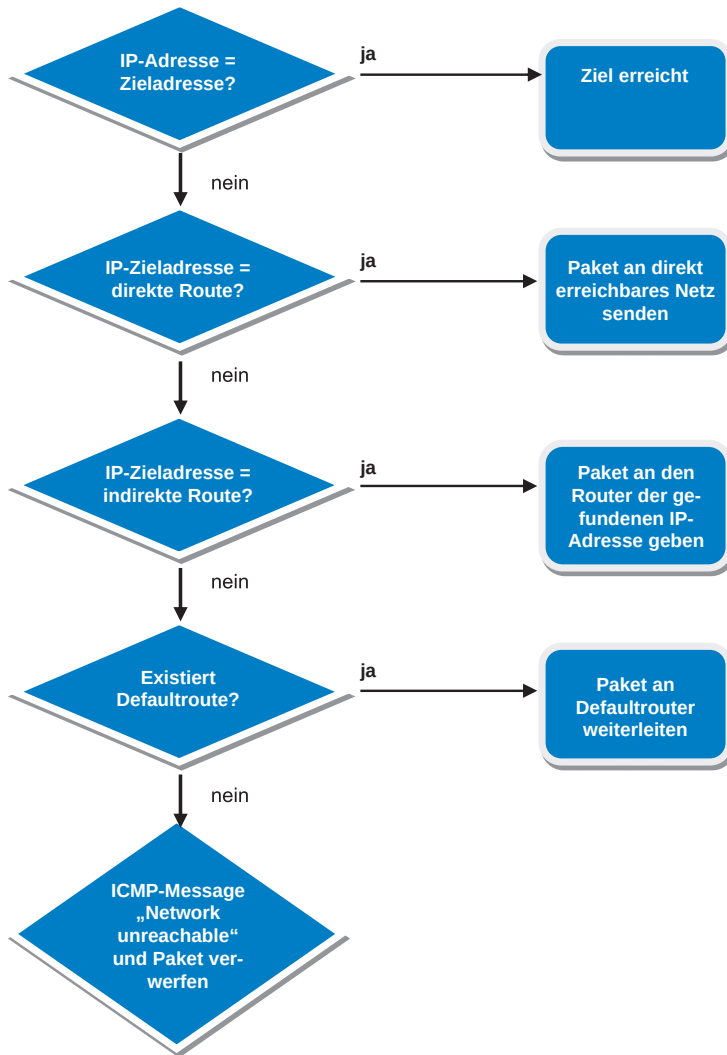


Bild 5.2 Routing-
entscheidung



Noch Fragen ...? Ja ...

Warum benötigt ein Rechner eine IP-Adresse und eine MAC-Adresse?

Die MAC-Adresse ermöglicht den Austausch von Ethernet-Paketen. Diese werden dem Rechner vom Switch im LAN zugestellt. Die IP-Adresse ist für die logisch eindeutige Adressierung notwendig, aber nicht für die direkte Paketzustellung.

Wie erhält der Endnutzer eine IP-Adresse?

In Europa ist das Reseaux IP Europeens Network Coordination Centre (RIPE NCC) für die Adressvergabe zuständig. Diese Zentrale hat die Verwaltung an Länderorganisationen weitergegeben. In Deutschland ist die DENIC die zentrale Registrierungsstelle (www.denic.de).

■ 5.2 Address Resolution Protocol ARP

ARP übersetzt die bekannte IP-Adresse eines Rechners in seine eindeutige Hardware-Adresse (MAC-Adresse). Dies ist wichtig zur Übergabe des IP-Paketes an die entsprechende LAN-Technologie wie z.B. Ethernet, da auf dieser Ebene Rechner über die MAC-Adresse angesprochen werden. ARP arbeitet vollständig automatisch. Die Quellstation verwaltet in einem dynamischen Cache (ARP-Cache) eine Tabelle mit allen bekannten Adressinformationen. Wird die Zieladresse nicht in diesem Cache gefunden, wird der Rechner mit der bekannten IP-Adresse mittels Broadcast aufgefordert, in einem gesonderten ARP-Response-Paket seine MAC-Adresse mitzuteilen. Die Adresse des ARP-Replies wird dem ARP-Cache hinzugefügt. Um auf dynamische Situationen wie den Austausch einer Netzkarte mit der zugehörigen MAC-Adresse reagieren zu können, steuert ein Timer die Löschung der Tabelleneinträge. Defaultmäßig geschieht dies alle 20 Min. Damit ergibt sich der folgende Verfahrensablauf:

- Alle in einem Netz zu übertragenden Pakete werden letztlich an ein lokales Netz übergeben. Dabei können zwei Situationen auftreten:
1. Der Zielrechner befindet sich im lokalen Netz. Der Sender erkennt dies, indem er seinen Netzteil der IP-Adresse mit demjenigen des Ziels vergleicht.
 2. Der Zielrechner ist Teil eines entfernten Netzes, da der Netzteil der IP-Adresse des Senders nicht mit der des Ziels korrespondiert. In diesem Fall nimmt der Sender die MAC-Adresse des Gateways/Routers als sein Ziel. Dieses Gateway in Form eines Router-Interfaces wird als Proxy-ARP bezeichnet. Es nimmt das Paket entgegen und bestimmt über den IP-Routing-Mechanismus anschließend die IP-Adresse des nächsten Knotens. Dieser kann sowohl bereits das Ziel als auch ein Router auf dem Weg zum Ziel darstellen.



Der Inhalt des ARP-Caches lässt sich unter Windows 2000/XP/Vista/7 mit dem Befehl `arp -a` ansehen.

Proxy-ARP ist standardmäßig auf Cisco-Routern aktiviert. Dieses Merkmal kommt auch dann zum Tragen, wenn kein explizites Default-Gateway auf einem Host eingetragen ist. In diesem Fall liefert der Proxy-ARP Mechanismus die MAC-Adresse des Router-Interfaces.

Ein ARP Request/Reply-Paket weist folgende Struktur auf:

Hardware-Adressraum		2 Byte
Protokoll-Adressraum		2 Byte
Hardwareadresslänge in Byte	Protokolladresslänge in Byte	2 Byte
Operation Code		2 Byte
Hardwareadresse des Senders		N Byte
Protokolladresse des Senders		M Byte
Hardwareadresse des Ziels		N Byte
Protokolladresse des Ziels		M Byte

Bild 5.3 ARP-Header

Die Headerfelder haben folgende Bedeutung:

- **Hardware-Adressraum** spezifiziert den Hardwaretypen, z. B. Ethernet.
- **Protokoll-Adressraum** legt den Protokolltyp fest, z. B. gemäß der Typfeld-Definition in Ethernet.
- **Hardwareadresslänge** beschreibt die Länge der physikalischen Adresse, z.B. 6 für IEEE 802.3 und IEEE 802.5.
- **Protokolladresse** definiert die Länge der logischen Adresse, z. B. 4 für IP.
- **Operation Code** bietet als Auswahl 1 für ARP-Request und 2 für ARP-Reply.
- **Quell-/Zieladresse** enthält die physikalische Netzadresse, z.B. MAC-Adresse mit 48 Bit.
- **Quell-/Zielprotokolladresse** enthält die logische Adresse, z. B. die 32-Bit-IP-Adresse.

Anders als die meisten Protokolle besitzt ARP kein festes Headerformat, sondern hängt von der unterliegenden LAN-Technologie wie Ethernet oder Token-Ring ab. Grund hierfür ist, dass Hardware- und Protokolladressen generisch definiert wurden. Sobald eine Station ein ARP-Paket erhält, läuft folgender Entscheidungsprozess ab:

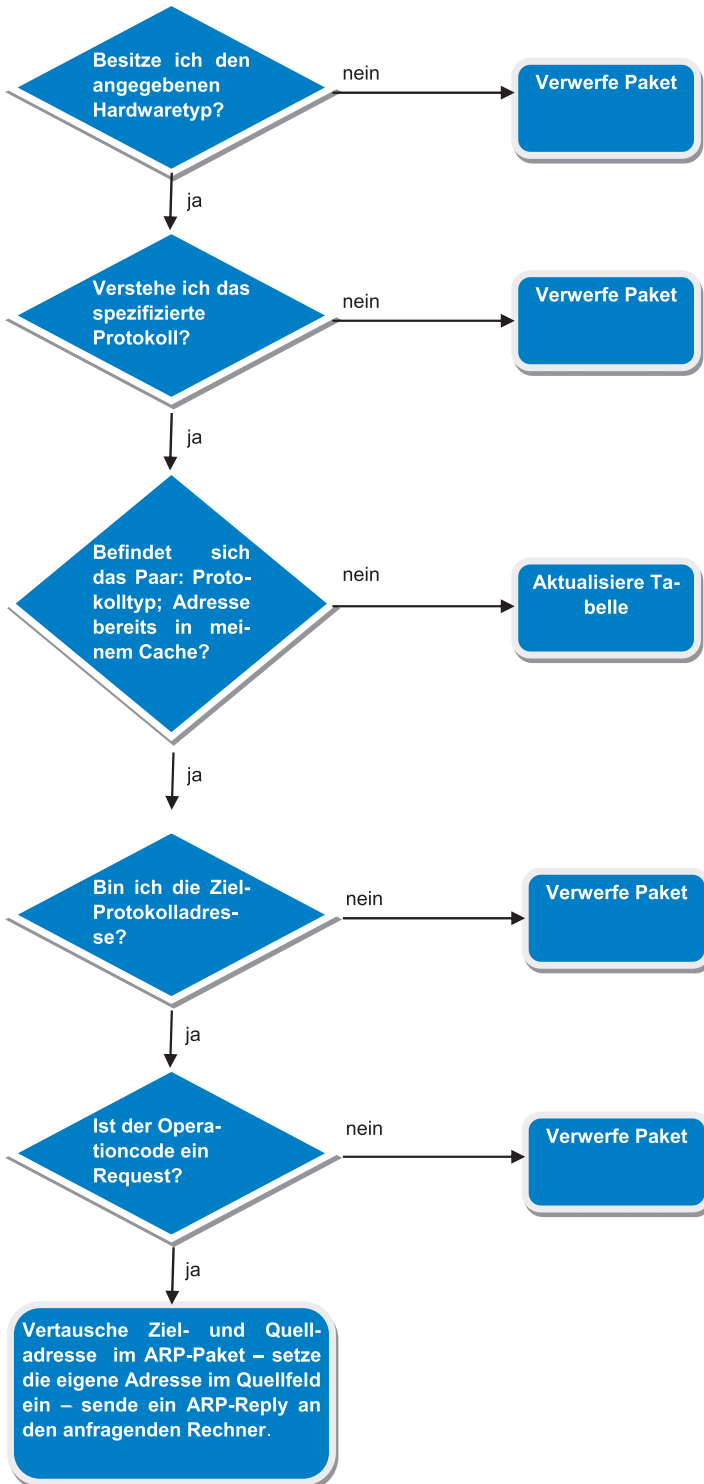


Bild 5.4 ARP-Prüfung

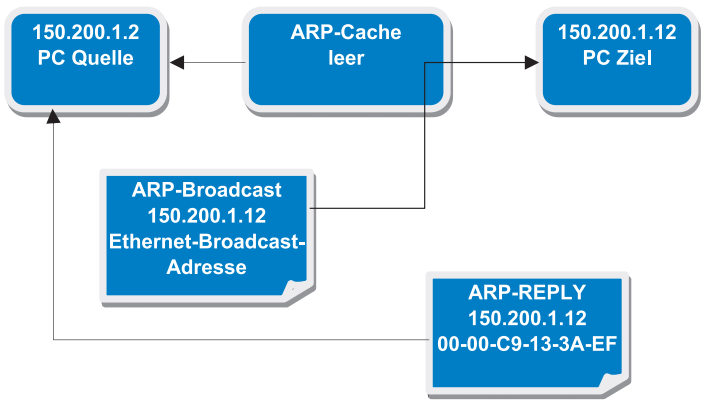


Bild 5.5 ARP-Ablauf

■ 5.3 Reverse Address Resolution Protocol RARP

Aber auch der umgekehrte Fall zu ARP ist denkbar, bei der zu einer bekannten MAC-Adresse eine unbekannte IP-Adresse erfragt wird. Diese Situation tritt bei Diskless-Rechnern auf, die ihre IP-Adresse nicht speichern können. Sie müssen also einen Mechanismus implementieren, mit dem sie Kontakt zu einem Rechner aufnehmen können, der ihre IP-Adresse verwaltet. RARP ermittelt durch einen Broadcast den Server, der anhand der eingegangenen MAC-Adresse den Absender erkennt und ein Antwortpaket mit der IP-Adresse zurückschickt. Die Header der Protokolle ARP und RARP gleichen sich in der Struktur:

1	8	16	32
Hardware		Protokoll	
Länge der HW-Adresse	Protokolllänge	Operation	
HW-Adresse des Senders: Byte 0 – 3			
HW-Adresse des Senders: Byte 4, 5		IP-Adresse des Senders Byte: 0, 1	
IP-Adresse des Senders: Byte 2, 3		HW-Adresse des Ziels Byte: 0, 1	
HW-Adresse des Ziels-Bytes: 2 – 5			
IP-Adresse des Ziels-Bytes: 0 – 3			
Diese Aufteilung trägt dem Umstand Rechnung, dass eine IP-Adresse aus 4 Byte = 32 Bit und eine Hardware-Adresse aus 6 Byte = 48 Bit besteht.			

Bild 5.6 RARP-Protokoll-Header

Die Felder entsprechen der Bedeutung des ARP-Headers mit der Ausnahme des Optionsfeldes:

- **Optionen:** Hier spiegelt sich der Befehlsvorrat wider: ARP Request = 1, ARP-Reply = 2, RARP-Request = 3, RARP-Reply = 4

Bei RARP-Requests ist die eigene IP-Adresse unbekannt und das entsprechende Feld deshalb leer, bei ARP-Requests hingegen ist die Hardware-Adresse zu ermitteln und der zugeordnete Eintrag zunächst mit Zufallswerten gefüllt.

■ 5.4 Internet Control Message Protocol ICMP

ICMP behandelt Fehler- und Kontrollmeldungen bezüglich IP. Es ist ein integraler Bestandteil jeder TCP/IP-Implementation und in RFC 792 mit einer Aktualisierung in RFC 950 beschrieben. Jeder zu passierende Netzknoten kann auf seiner Basis Reports an die sendende Station übertragen. ICMP dient daher zur Information der Quelle über mögliche Fehler auf dem Übertragungsweg.

- ICMP benutzt IP als Kommunikationsbasis, indem es sich selbst als Protokoll einer höheren Schicht interpretiert, d. h. ICMP-Nachrichten werden in IP-Paketen gekapselt.
- ICMP erkennt einige Fehlerzustände, macht aber IP zu keinem zuverlässigen Protokoll.
- ICMP analysiert Fehler in jedem IP-Paket, mit Ausnahme solcher, die eine ICMP-Nachricht tragen.
- ICMP-Nachrichten werden nicht als Antwort auf Pakete an Zieladressen versendet, bei denen es sich um Multicast- oder Broadcast-Adressen handelt.
- ICMP-Nachrichten antworten nicht auf eine ICMP-Nachricht.
- ICMP-Nachrichten antworten nur einer eindeutigen Quell-IP-Adresse.

ICMP sendet und empfängt eine Vielzahl von Nachrichten. Im IP-Header wird die ICMP-Nachricht durch die Protokollnummer 1 angezeigt. Das ICMP-Nachrichtenformat besteht aus nur wenigen Feldern:

0	8	16	31
Type	Code	Prüfsumme	
ICMP-Daten, abhängig vom Nachrichtentyp			

Tabelle 5.7 ICMP-Nachrichtentypen

Typ	Nachrichtenart
0	Echo Reply
3	Ziel unerreichbar
4	Drosselung der Sendeleistung der Quelle
5	Umleitung
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Zeitüberschreitung

Tabelle 5.7 ICMP-Nachrichtentypen (Fortsetzung)

Typ	Nachrichtenart
12	Parameterprobleme
13	Anforderung eines Zeitstempels
14	Zeitstempelantwort
15	Informationsanforderung
16	Informationsantwort
17	Adressmaskenanforderung
18	Adressmaskenantwort

Das Typfeld spezifiziert die Nachricht. Das Codefeld interpretiert die Nachrichtenart genauer. Die Daten enthalten typischerweise einen Teil der ursprünglichen IP-Nachricht. Im Einzelnen besitzen die Nachrichten folgende Bedeutung:

- **Echo Reply (0) und Echo (8)** wird benutzt, um eine andere Station des Netzes als aktiv zu erkennen. Dazu initialisiert der Sender einen Identifier und eine Sequenznummer, fügt einige Daten hinzu und überträgt die ICMP-Echonachricht an die Zielstation. Der Empfänger ändert das Typfeld auf Echo Reply und sendet die Nachricht zurück. Diesen Mechanismus verwendet das Ping-Kommando.
- **Destination Unreachable (3)** teilt einem Router auf dem Übertragungsweg die Unerreichbarkeit der Zieladresse mit. Das Codefeld des ICMP-Headers kann folgende Werte aufweisen:

Tabelle 5.8 Codes des ICMP-Headers

Code	Bedeutung
0	Netzwerk nicht erreichbar
1	Zielstation nicht erreichbar
2	Protokoll unbekannt
3	Port unerreichbar
4	Fragmentierung benötigt, aber <i>Do Not Fragment</i> -Bit gesetzt
5	Weg fehlerhaft
6	Zielnetz unbekannt
7	Zielstation unbekannt
8	Quellstation isoliert
9	Zielnetz durch Management untersagt
10	Zielstation durch Management untersagt
11	Netz für diesen Servicetyp unerreichbar
12	Zielstation für diesen Servicetyp unerreichbar

Tabelle 5.8 Codes des ICMP-Headers (*Fortsetzung*)

Code	Bedeutung
13	Kommunikation durch Filter untersagt
14	Zielprioritätsverletzung
15	Priorität nicht vorhanden

- **Source Quench (4)** zeigt einer Zwischenstation an, dass sie nicht über ausreichend Pufferplatz verfügt, um die Pakete zur Folgestation weiterzuleiten. Stammt diese Nachricht vom Zielrechner, gibt er damit zu erkennen, dass die Pakete für eine ordnungsgemäße Verarbeitung zu schnell einlaufen. Die Sendestation reagiert auf diese Meldung mit einer Drosselung der Übertragungsrate. Das Codefeld dieser Nachricht trägt stets den Wert 0.
- **Redirect (5)** verlangt die Versendung zukünftiger Pakete über den Router, dessen IP-Adresse im ICMP-Paket angegeben ist. Diese neue Station befindet sich stets im gleichen Subnetz wie diejenige, die die Nachricht initialisierte. Handelt es sich bei der angegebenen Adresse um die Quelle, entsteht eine Routing-Schleife.
- **Router Advertisement (9) und Router Solicitation (10)** sind optionale Nachrichten. Sie werden in RFC 1256 gesondert beschrieben.
- **Time Exceeded (11)** weist darauf hin, dass das TTL-Feld abgelaufen ist. Stammt diese Nachricht von der Zielstation, zeigt diese an, dass die Zeit zum Zusammensetzen der IP-Fragmente überschritten wurde. Das Codefeld kann dementsprechend zwei Werte annehmen:

Code	Bedeutung
0	TTL-Wert überschritten
1	TTL-Wert beim Reassemblieren der Fragmente überschritten

- **Parameter Problem (12)** zeigt an, dass bei der Verarbeitung des IP-Headers ein Fehler aufgetreten ist. Das Codefeld kann zwei Werte annehmen:

Code	Bedeutung
0	unspezifizierter Fehler
1	eine geforderte Option fehlt

- **Timestamp Request (13) und Timestamp Reply (14)** dienen der Performance-messung und dem Debugging. Sie werden nicht zur Synchronisation der Rechnerknoten verwendet. Die sendende Station wählt einen Identifier, setzt eine Sequenznummer, trägt einen Originalzeitstempel ein und überträgt den Rahmen. Der Empfänger füllt weitere Zeitfelder, ändert das Typfeld des ICMP-Header auf Timestamp Reply und sendet die Nachricht an die Quellstation zurück.

- **Information Request (15) und Information Reply (16)** werden von Rechnerknoten verwendet, um eine gültige IP-Adresse für das Netz zu bekommen. Dieser Mechanismus ist durch das RARP-Protokoll überflüssig geworden.
- **Address Mask Request (17) und Address Mask Reply (18)** werden verwendet, um die im Netz benutzte Subnetzmaske zu erfahren. Die meisten Stationen werden mit ihrer Subnetzmaske konfiguriert, Diskless Rechner hingegen müssen diese Information von einem Server erhalten. Zum Erhalt einer IP-Adresse setzt ein Rechner zwar RARP ein, für die Subnetzmaske nutzt er aber weiterhin diese Nachricht. Da keine Varianten erforderlich sind, ist das Codefeld mit einer 0 belegt.
- **ICMP-Anwendungen:** Die häufig benutzten Anwendungen PING und TRACEROUTE beruhen auf ICMP-Nachrichten. PING verwendet das Echo und Echo Reply, TRACE-ROUTE sendet Time Exceeded-Nachrichten mit geringer TTL, so dass diese bei der Durchquerung des Netzes abläuft, und wertet die Informationen über die rückmel-dende Station aus. Eine systematische Veränderung des TTL-Wertes führt dazu, dass die Nachricht durch die steigende Lebenszeit des Paketes immer weiter im Netz vor-dringt und auf diese Weise die Sendestation die Zusammensetzung der Route erfährt.

■ 5.5 Zusammenfassung

IP ist das Protokoll im Internet, dem die Paketweiterleitungsfunktion zufällt. Daraus resultiert die immense Wichtigkeit. Nicht nur die Existenz einer weltweit eindeutigen Adresse ermöglicht eine Paketzustellung, auch der Transport über die Netzinfrastruktur basiert auf den Adressinformationen. Sie bleiben zwar im Paket unverändert, dienen aber zur Entscheidungsfindung hinsichtlich des Leitweges.

■ 5.6 Wissensüberprüfung

1. Ein Rechner sendet Daten an einen Rechner in einem anderen Netz. Welche Adresse gibt er im IP-Header an?
2. Was ist die Folge, wenn ein Datenpaket keine Ziel-IP-Adresse besitzt?
3. Was ist die Bedeutung des TTL-Feldes?
4. Warum enthält ein IP-Paket nur eine Headerprüfsumme?
5. Für welche Anwendungen sind Dienstgüten bedeutsam?
6. Nach welchem Übertragungsprinzip arbeitet ARP?
7. Welche Situation löst ein ARP-Request aus?
8. Was ist die Zieladresse eines ARP-Requests?
9. Worin besteht der Unterschied zwischen ARP und RARP?
10. Was ist die primäre Funktion von ICMP?

6

IP-Adressierung

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Welchen Adressierungstyp verwendet IPv4?
- Welche Bedeutung haben Netzwerk- und Hostteil einer Adresse?
- Welche Rolle spielt die Einteilung in Subnetze?
- Welche Verfahren zur Nutzung der Subnetzbildung gibt es?
- Wie lässt sich die Netzkonnektivität prüfen?

Kapiteleinführung

Verschiedene Adresstypen sind notwendig, um eine Nachricht im Netzwerk korrekt zustellen zu können. Die Hardware- oder MAC-Adresse stellt eine physikalische Kennung dar, die zur endgültigen Nachrichtenzustellung im lokalen Bereich dient. Die IP-Adressierung definiert logische Netzwerkadressen für die TCP/IP-Protokollfamilie. Diese sind unabhängig von der Hardware, vom Hersteller oder vom Netzwerkmedium und werden zur Identifikation eines Teilnehmers im weltweiten Verbund benötigt. An der Grenze des lokalen Netzes werden die eintreffenden Pakete daher auf die Hardwareadresse analysiert und dann dem entsprechenden Gerät übergeben. Umgekehrt wird im Falle einer Sendung an einen entfernten Teilnehmer das Paket mit einer logischen IP-Adresse versehen und über das Internet transportiert.

Die Bedeutung beider Adresstypen unterstreicht folgende Analogie:

Ein Mietshaus besitzt mehrere Mietparteien. Die Straße und Hausnummer symbolisieren die MAC-Adresse als unveränderliches Merkmal, die Namensschilder an den Wohnungstüren repräsentieren die IP-Adresse als ein veränderliches Attribut, denn Mieter können wechseln. Ein Brief, nur mit Straße und Hausnummer versehen, würde alle Mieter erreichen, der zusätzliche Name identifiziert den Empfänger jedoch eindeutig. Auf diese Weise kann durch eine Adressbildung auf höherem Abstraktionsniveau wie hier dem Layer 3 mit der IP-Adresse eine detaillierte Empfängerauswahl stattfinden.

In den vergangenen Jahren hat das Internet und mit ihm die Nachfrage nach IP-Adressen einen enormen Aufschwung genommen. Dieses Wachstum äußert sich in Merkmalen, die der ungezügelten Verbreitung des Internets Grenzen aufzeigen:

- die Erschöpfung des Adressraumes für IP-Adressen
- die Vergrößerung der Routingtabellen zur Weiterleitung der IP-Pakete in den Kernknoten des Internets.

Der Adressraum der gegenwärtigen IP-Adressen basiert auf 32-Bit Kennungen, was $2^{32} = 4.294.967.296$ potenziellen Adressen entspricht. Obwohl diese Zahl sehr groß anmutet, ergibt sich durch die Strukturierung und Vergabe des Adressraumes ein Engpass. Das zweite Problem rührt daher, dass die Internet-Vermittlungsrouter die vollständige Wegewahlinformation für das Internet beherrschen müssen. Mit der Zunahme der vergebenen IP-Adressen nahm in der Vergangenheit auch der Umfang der entsprechenden Tabellen zu. Ein ungebremses Wachstum ohne entsprechende Eingriffe führt über kurz oder lang dazu, dass Router einige Wege verwerfen und damit Teile des Internets unerreichbar machen könnten.

■ 6.1 IP-Adressstruktur

Eine IP-Adresse besteht aus zwei Teilen: einer Netzkennung (Netz-Präfix) und einer Stationskennung (Hostadresse).

- **Netzwerkadressen:** Um eine offizielle IP-Adresse zu bekommen, muss diese beim „Network Information Center“ NIC (in Deutschland: DE-NIC) oder einer autorisierten Unterorganisation beantragt werden.
- **Hostadressen:** Der Systemadministrator weist den einzelnen Geräten aus dem ihm offiziell zugeteilten Adressbestand in eigener Regie Adressen zu. Eine Strukturierung des Adressbestandes nicht nur durch eine geordnete Vergabe sondern auch durch die Bildung von Subnetzen liegt im Kompetenzbereich der Institution, die die offizielle IP-Adresse besitzt.

Das Internetadress-Schema besteht aus drei Kategorien:

- den IP-Adressen der Geräte
- den Netzwerk- und Broadcast-Adressen
- der Loopback-Adresse

Die IP-Adresse ist eine weltweit eindeutige 32-Bit-Binärzahl, die der besseren Lesbarkeit wegen in vier Gruppen zu je 8 Bit eingeteilt wird. Im Dezimalformat werden die einzelnen Bestandteile durch einen Punkt abgetrennt (decimal-dotted-Darstellung).

- Netzwerk-ID = Identifikation des physikalischen Netzwerkes
- Host-ID = Identifikation des Rechners am Netzwerk

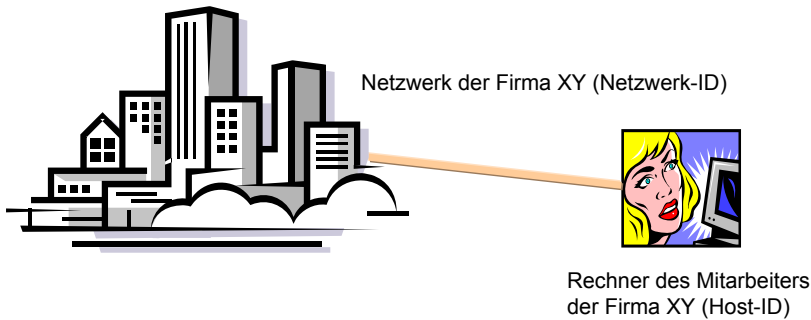


Bild 6.1 IP-Adressteile

Alle Rechner eines gegebenen Netzwerkes teilen sich den gleichen Netzpräfix, besitzen aber unterschiedliche Stationskennungen. Umgekehrt müssen zwei Rechner verschiedener Netze zwar eine unterschiedliche Netzkennung aufweisen, können aber über die gleiche Hostnummer verfügen.

Um die notwendige Flexibilität zur Unterstützung verschiedener Netzwerkgrößen zu gewährleisten, unterscheidet IP fünf Klassen von Internetadressen: Class A – E. Jede Klasse setzt die Grenze zwischen Netzwerkpräfix und Hostnummer an einem anderen Punkt der 32 Bit-Adresse und bestimmt die Zugehörigkeit einer Adresse zu einer Klasse durch die ersten Bits des ersten Bytes:

Tabelle 6.1 IP-Adressklassenidentifikation

Class A	Bit 1	0
Class B	Bit 1 und 2	1 0
Class C	Bit 1 bis 3	1 1 0
Class D und E	Bit 1 bis 4	1110 bzw. 1111

?	145	63	12
---	-----	----	----



- 1 – 12: Class A
- 128 – 191: Class B
- 192 – 223: Class C
- 224 – 239: Class D
- 240 – 254: Class E

Jede Adresse besitzt durch das erste Byte damit einen impliziten Schlüssel, der angibt, an welcher Stelle der Adresse in Netzkennung und Hostnummer unterschieden werden muss. Diese Konstruktion vereinfacht das Routing beträchtlich. Sie wird als klassenbasiertes Routing bezeichnet.

6.1.1 Class-A-Adressen

Class A Adressen bestehen aus einem 8-Bit-Netzwerkteil und einer 24-Bit Hostadresse. Das erste Bit des Netzwerkteils bestimmt die Adressklasse, so dass 7 Bit für die Nummerierung der zu vergebenden Netze verbleiben. Von den dadurch möglichen 128 eindeutigen Netznummern sind zwei für spezielle Zwecke reserviert: 0 für Testzwecke und 127 für die lokale Rückkopplung. Damit ergeben sich max. 126 ($2^7 - 2$) Class-A-Netze mit jeweils 16.777.214 ($2^{24} - 2$) lokalen Stationen. Die Berechnung verlangt, dass zwei Adressen unberücksichtigt bleiben, „alles-0“ für das eigene Netz und „alles-1“ für Broadcasts:

Netzwerkteil (8 Bit)	lokaler Adressteil (24 Bit)
1 bis 126	0.0.1 bis 255.255.254

6.1.2 Class-B-Adressen

Class-B-Adressen bestehen aus einem 16-Bit-Netzwerkteil und einer 16-Bit Hostadresse. Die ersten beiden Bits des globalen Netzwerkteils bestimmen die Adressklasse, so dass 14 Bit für die Nummerierung der zu vergebenden Netze verbleiben. Damit ergeben sich 16.384 (2^{14}) mögliche Class-B-Netze mit jeweils 65.536 lokalen Stationen.

Netzwerkteil (16 Bit)	lokaler Adressteil (16 Bit)
128 bis 191	0.1 bis 255.254

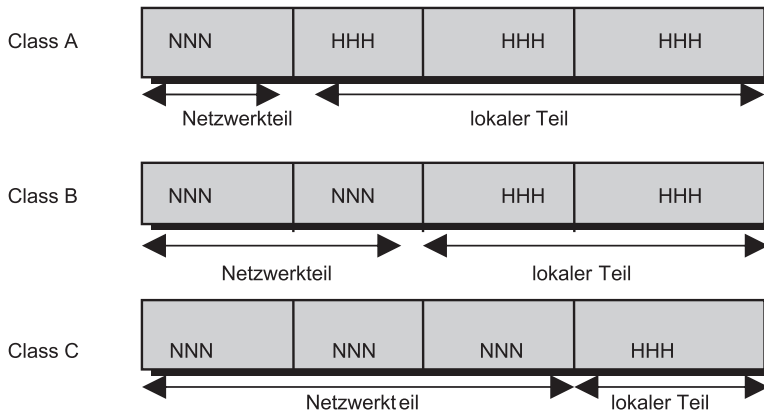
6.1.3 Class-C-Adressen

Class-C-Adressen bestehen aus einem 24-Bit-Netzwerkteil und einer 8-Bit Hostadresse. Die ersten drei Bits des globalen Netzwerkteils bestimmen die Adressklasse, so dass 21 Bit für die Nummerierung der zu vergebenen Netze verbleiben. Damit ergeben sich 2.097.152 mögliche Class-C-Netze mit jeweils 254 lokalen Stationen.

Netzwerkteil (24 Bit)	lokaler Adressteil (8 Bit)
192 bis 223	1 bis 254

6.1.4 Adressinterpretation

Das von IP unterstützte Adressschema lässt sich hinsichtlich mehrerer Gesichtspunkte interpretieren:

**Bild 6.2** IP-Adressinterpretation

Eine feinere Granulierung ergibt sich bei der Berücksichtigung der ersten Bits des ersten Bytes:

Class A



Class B



Class C



Class D



Eine dritte Möglichkeit bezieht sich auf die Nummernkreise der Adressen und ihre Dezimaldarstellung:

Adressklasse	Dezimaldarstellung
A – 8 Bit Netzpräfix	1.xxx.xxx.xxx bis 126.xxx.xxx.xxx
B – 16 Bit Netzpräfix	128.0.xxx.xxx bis 191.255.xxx.xxx
C – 24 Bit Netzpräfix	192.0.0.xxx bis 223.255.255.xxx

6.1.5 Internetadressen mit besonderer Bedeutung

- Class-D-Adressen bestehen aus einem fixen 4-Bit-Netzwerkteil und einer 28-Bit Host-adresse. Die ersten vier Bit 1110 dienen als Multicast-Adressen, während die Kennung 1111 auf Class-E-Adressen hinweist. Beide Adresstypen verfügen über keine explizite Zuweisung an Hosts.

Class D (4 Bit)	Class E (4 Bit)
224 bis 239	240 bis 255

- **Netzkennung:** Wenn eine Class-C-Adresse in ihrem lokalen Teil eine 0 enthält (z.B. 192.9.200.0), verweist sie auf das Netz. Das bedeutet, dass alle Stationen mit einer Class-C-Adresse der Form 192.9.200.x erreicht werden.
- **Lokale Loopback Adresse:** IP definiert die Adresse 127.0.0.1 als lokale Loopback Adresse, unter der Stationen zu Testzwecken Nachrichten an sich selbst schicken können.



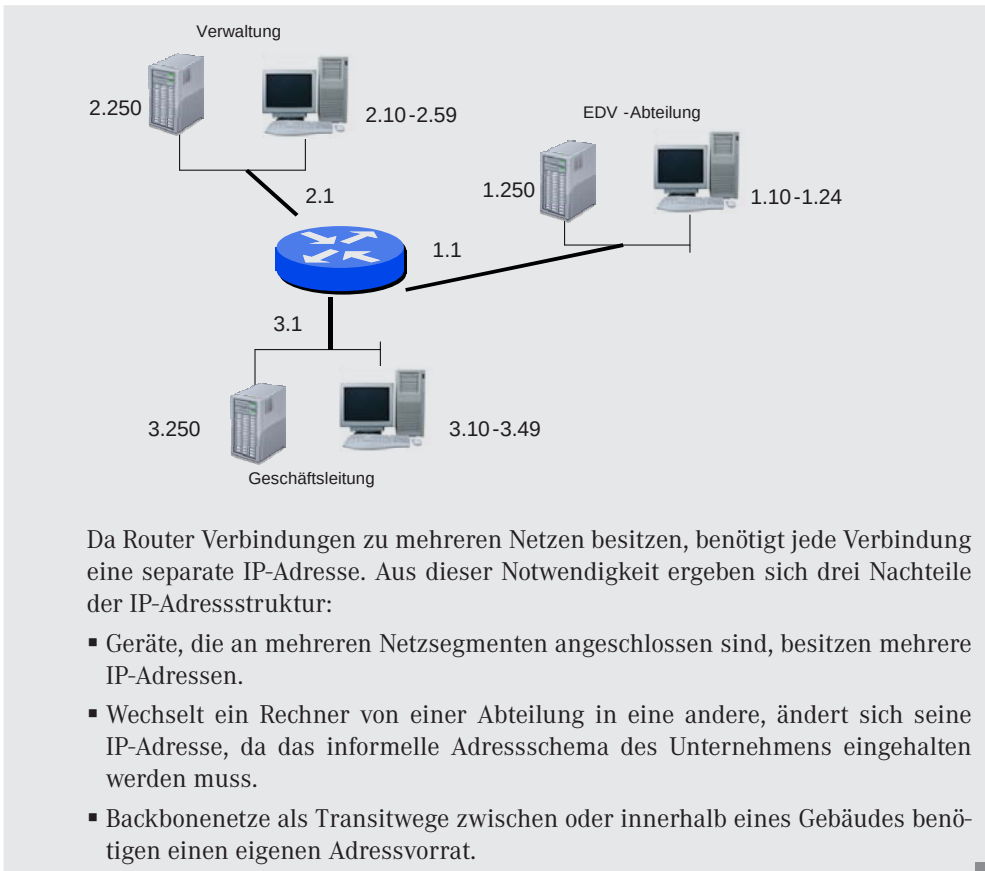
Die Funktionsfähigkeit eines Rechners hinsichtlich IP lässt sich durch die Eingabe von „ping 127.0.0.1“ leicht überprüfen.

- **Broadcastadressen:** IP kann Daten an alle Stationen eines speziellen IP-Netzes senden. Für diesen Fall werden Broadcastadressen verwendet, die sich dadurch auszeichnen, dass ihr Hostteil aus „alles Einsen“ besteht. Beispiel: Adressierung der Stationen des Class-B-Netzes 191.130.0.0 durch die Broadcastadresse 191.130.255.255.



Beispiel: IP-Adressvergabe

Ein Unternehmen besitzt die offizielle IP-Adresse der Class B: 140.25.0.0. Das 3. und 4. Byte können zur Bildung eines individuellen, informellen Adressierungsschemas der Abteilungen dienen. Die konkrete Zuteilung der Nummern führt zu einer leichteren Unterscheidbarkeit der Adressen und wird durch organisatorische Kriterien determiniert. Daher wäre folgende Struktur denkbar: das 3. Byte dient zur Differenzierung der einzelnen Abteilungen und das 4. Byte erlaubt eine Nummerierung der Geräte mit: 1 – 9: Internetworking-Komponenten; 10 – 249: PCs und 250 – 254: Server. Für die drei Abteilungen des Unternehmens ergäbe sich dann die folgende Adressverteilung:



■ 6.2 Subnetzbildung

Die Bildung von Subnetzen ermöglicht es Unternehmen, ihren Adressbestand nach eigenen Kriterien weiter zu unterteilen. Dadurch können organisatorische Gegebenheiten nachgebildet werden. Die Strukturierung des Adressbestandes liegt allein im Verantwortungsbereich des Unternehmens. Es sind dabei jedoch einige Regeln einzuhalten.

Die Einteilung kann ausschließlich nach organisatorischen Gesichtspunkten oder erwartetem Wachstum der Teilnehmerzahlen in bestimmten Abteilungen getroffen werden. Die einzigen Restriktionen sind:

- Der Netzwerkteil ist die eigentliche IP-Adresse nach außen und darf nicht zur Subnetzbildung benutzt werden.
- Die Subnetzadresse ist ein Feld konstanter Größe für das gesamte Netz. Ein Wert von 0 zeigt an, dass keine Subnetzstruktur existiert.
- Die lokale Rechneradresse besteht aus einem mindestens 2 Bit großen Feld.

Da der Bestand nur homogen unterteilt werden kann, betrifft eine Basisentscheidung die Anzahl und die Größe der Subnetze. Ein systematisches Vorgehen könnte folgendermaßen aussehen:

- 1. **Festlegung der Anzahl Bits, die einer Subnetzbildung dienen.** Dabei ist zu bedenken, dass eine Abhängigkeit zwischen der Anzahl der Subnetze und der Anzahl der darin befindlichen Hosts existiert: Je nachdem welchem Kriterium Vorrang eingeräumt wird, ergibt sich das andere gezwungenermaßen: Sollen 6 Subnetze gebildet werden, müssen dafür 3 Bit reserviert werden. Im Falle von Class-C-Netzen stehen dann nur noch fünf Bit für die Hostadressierung zur Verfügung.
- 2. **Festlegung der neuen Subnetzmaske zur Bekanntmachung der Substrukturierung.** Den Hintergrund hierfür liefert folgende Überlegung: Der Weg vom Internet zu einem beliebigen internen Subnetz bleibt der gleiche, unabhängig davon, welchem Subnetz der ausgewählte Rechner angehört. Erst der Router im Unternehmen differenziert zwischen den unterschiedlichen Teilstrukturen. Das bedeutet, dass der Grenzüter des Unternehmens alle Subnetze als einen eigenen Routingtabelleneintrag führt.

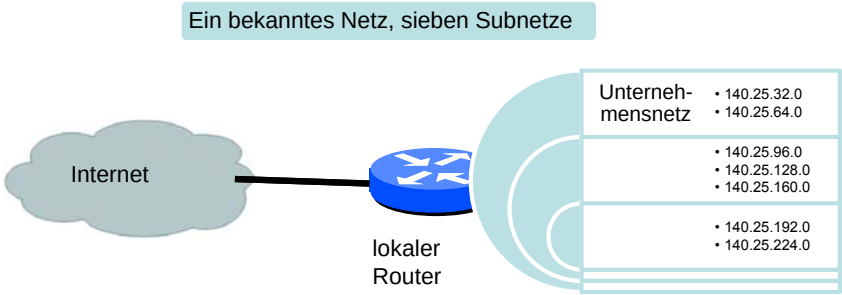


Bild 6.3 Subnetzanbindung

Der lokale Router akzeptiert alle IP-Pakete an die Adresse 140.25.xxx.xxx und leitet sie entsprechend der Subnetzbildung intern weiter.

Die Fähigkeit zur Bildung von Subnetzen ermöglicht es also, ein lokales, physikalisches Netzwerk in mehrere IP-Domänen zu teilen. Zur konkreten Einrichtung wird der Hostteil der IP-Adresse in einen Subnetz- und einen neuen Hostteil aufgespalten.

Eine Class-B-Adresse besteht aus einem 16-Bit-Netzwerkteil und einem 16-Bit-Hostteil. Um ein Subnetz einzurichten, wird der Hostpart in zwei Nummernkreise geteilt:

Netzwerkteil (16 Bit)	Hostteil (16 Bit)	
128 bis 191	0.0 bis 255.255	
Netzwerkteil (16 Bit)	Hostteil (16 Bit)	
	Subnetz-Adresse	Hostadresse
128 bis 191	8 Bit	8 Bit

Ein Sender außerhalb des Unternehmens leitet seine Nachricht an den Netzwerkteil der IP-Adresse. Das lokale System übernimmt die Verantwortung dafür, die Daten an das entsprechende Subnetz und dessen angeschlossene Rechner weiterzureichen. Eine Station außerhalb des lokalen Netzes sieht die interne Struktur dabei nicht, sondern identifiziert einen Empfänger weiterhin nur über den Netzwerkteil der Adresse.

Die Bits, die ein Subnetz identifizieren, müssen nicht notwendig einen zusammenhängenden Bereich bilden, da sie durch eine Bit-Maske isoliert werden können. Dennoch empfiehlt es sich, Subnetzidentifikatoren aus einem kontinuierlichen Bereich der „most significant“ Bits der lokalen Adresse zu wählen. Standardmäßig sind für die einzelnen Adressklassen keine Subnetze vorgesehen.

Für die einzelnen IP-Adressklassen existieren Standard-Subnetzmasken. Bei Adressen der Class B identifiziert die Standard-Subnetzmaske beispielsweise das erste und zweite Byte als Netzwerkteil und das dritte und vierte als Stationskennung. Eine IP-Adresse 140.25.1.33 und eine Subnetzmaske 255.255.0.0 ergeben z. B. 140.25.0.0 als Netzkennung und 1.33 als Stationskennung. Zum Einrichten von Subnetzen ist es daher notwendig, die Standard-Subnetzmasken zu modifizieren:

Tabelle 6.2 Standard-Subnetzmasken

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Sendet ein Rechner eine Nachricht an eine Zielstation, muss er erkennen, ob sich das Ziel im gleichen Netzwerk wie die Quelle befindet oder ob es nur durch eine Internetworking-Komponente erreicht werden kann. Dazu vergleicht das System die Zieladresse mit der Quelladresse anhand der Subnetzmaske. Ist das Ziel nicht lokal, werden die Daten an einen Router weitergeleitet, der den beschriebenen Vergleich erneut durchführt. Ein Router muss daher mit der Subnetzmaske und den Informationen bezüglich des Subnetzes konfiguriert sein. Anschließend kann er entscheiden, ob das Ziel außerhalb des Netzes liegt oder ob es sich in seinen angeschlossenen Subnetzen befindet.



Beispiel: Bestimmung der Subnetzzugehörigkeit

Ein Router erhält ein an den Rechner 193.1.1.51 adressiertes Paket. Durch die Verwendung des logischen AND und der Subnetzmaske kann er die Netzwerkadresse ermitteln.

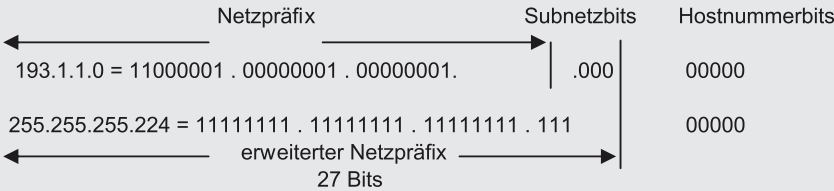
Zieladresse	193.1.1.51	11000001.00000001.00000001.00110011
Subnetzmaske	255.255.255.0	11111111.11111111.11111111.00000000
Netzwerkadresse	193.1.1.0	11000001.00000001.00000001.00000000



Beispiel: Subnetze in Class C Netzen

Einem fiktiven Unternehmen wird die Class-C-Adresse 193.1.1.0 zugewiesen. Da das Unternehmen aus sechs Abteilungen besteht, sollen diese jeweils einen eigenen Adressbereich erhalten und zudem jede Station über eine offizielle IP-Adresse erreichbar sein. Das größte Subnetz umfasst 25 Rechner. Um diesen Anforderungen zu genügen, ist eine Subnetzbildung für die Class-C-Adresse in sechs separate Einheiten notwendig.

Der erste Schritt besteht darin, zu bestimmen, wie viele Bits die gewünschte Subnetzzahl abbilden. Da $2^3 = 8$, sind drei Bits notwendig, um die sechs Subnetze zu kennzeichnen. Da die Class-C-Adresse 24 Bits zur Netzkennung nutzt, kommen drei weitere hinzu, so dass insgesamt 27 Bits den erweiterten Netzpräfix bilden. Dies kann dezimal als Subnetzmaske 255.255.255.224 ausgedrückt werden.



Folglich kann jedes Subnetz mit einem 27-Bit-Netzpräfix einen Block von $2^5 = 32$ individuellen IP-Adressen verwalten. Da die Adressen mit „alles 0“ und „alles 1“ nicht vergeben werden dürfen, können jedem Subnetz nur 30 Rechner angehören:

Basisnetz	11000001.00000001.00000001.00000000	193.1.1.0 / 24
Subnetz 0	11000001.00000001.00000001.00000000	193.1.1.0 / 27
Subnetz 1	11000001.00000001.00000001.00100000	193.1.1.32 / 27
Subnetz 2	11000001.00000001.00000001.01000000	193.1.1.64 / 27
Subnetz 3	11000001.00000001.00000001.01100000	193.1.1.96 / 27
Subnetz 4	11000001.00000001.00000001.10000000	193.1.1.128 / 27
Subnetz 5	11000001.00000001.00000001.10100000	193.1.1.160 / 27
Subnetz 6	11000001.00000001.00000001.11000000	193.1.1.192 / 27
Subnetz 7	11000001.00000001.00000001.11100000	193.1.1.224 / 27

Im Hinblick auf die „Alles-0“-Subnetzproblematik verlangt jeder Routingtabellen-Eintrag die Angabe der Netzpräfixlänge, um zwischen einer zulässigen und unzulässigen Kennung zu unterscheiden. So differenziert das Routingprotokoll RIP-1 z.B. nicht zwischen 193.1.1.0/27 und 193.1.1.0/24. RIP-1 identifiziert beide als 193.1.1.0, da es keine Länge der Präfixe berücksichtigt. Ohne Präfixerkennung kann also ein Router nicht entscheiden, ob ein „Alles-0“-Subnetz oder das gesamte Netz gemeint ist. Erst RIP in der Version 2 kann diesen Unterschied erkennen.

24 Bit Subnetzmaske an. Wäre die neue Adresse jedoch 131.25.0.0, würde der Router die ursprüngliche 16 Bit-Maske zugrunde legen. Der Router berücksichtigt also die entsprechende Subnetzmaske, falls der Port entsprechend konfiguriert ist.

VLSM erlaubt Organisationen, ihren bereits durch Subnetze organisierten Adressbestand nochmals zu unterteilen und damit flexibler zu verwalten. Ein Hauptproblem der starren Subnetzbildung rührt daher, dass nachträglich keine Änderung des gewählten Schemas ohne beträchtlichen manuellen Konfigurationsaufwand möglich ist.

6.3.1 Grenzen der Subnetzbildung

Ein Class B-Netz mit einem erweiterten Präfix auf 22 Bit erlaubt die Bildung von $2^6 = 64$ Subnetzen mit maximal 1022 ($2^{10}-2$) Rechnern. Diese Möglichkeit kommt gleichmäßig belegten Teilnetzen sehr entgegen. Doch was passiert mit Netzen, die lediglich über 20 – 30 Rechner verfügen? Da die Subnetzmaskenbildung keine Revidierung der Einteilung zulässt, werden in diesem Szenario ca. 1000 IP-Adressen verschwendet. Eine Lösung des Problems bestünde darin, mehr als eine Subnetzmaske zu verwenden. Wäre der Netzadministrator in der Lage, auch einen auf 26 Bit erweiterten Netzpräfix zuzugreifen, könnte er 1022 ($2^{10}-2$) Subnetze mit einer maximalen Rechnerzahl von 62 (2^6-2) bilden. Dieser Präfix wäre ideal für kleine Netze, während der 22 Bit Präfix die Gegebenheiten großer Organisationseinheiten abbildet.



Beispiel: Subnetzbildung

Besitzt ein Unternehmen drei Standorte, wird es sich voraussichtlich dazu entschließen, 3 Bits entsprechend 8 Subnetzen für eine zukünftige problemlose Expansion zu verwenden. Nun befinden sich an jedem Standort mehrere Gebäude oder Abteilungen, was eine zweite Stufe der Subnetzbildung erfordert. Letztlich befinden sich in den einzelnen Gebäuden unterschiedliche Arbeitsgruppen, die eine dritte Stufe der Strukturierung verlangen. Gemäß dieser hierarchischen Vorstellung, bildet die Zahl der Standorte die oberste Stufe, gefolgt von den Gebäuden an jedem Standort und auf unterster Ebene die Anzahl der zu berücksichtigenden organisatorischen Einheiten.

6.3.2 VLSM-Voraussetzungen

Der erfolgreiche Einsatz von VLSM ist an zwei Voraussetzungen geknüpft:

- Das Routingprotokoll muss die erweiterten Netz-Präfixinformationen in die Routingtabelle aufnehmen und verarbeiten können. Vor diesem Hintergrund ist RIP-1 nicht geeignet. An seiner Stelle sollten RIP-2 oder OSPF zum Einsatz kommen.
- Alle Router müssen einen Weiterleitalgorithmus auf der Basis des „longest match“ implementiert haben. Ein Weg mit einem längeren Netzpräfix beinhaltet eine kleinere Menge von Zielrechnern als ein kurzer Präfix. Dementsprechend ist ein Weg mit umfangreicherem Präfix spezifischer. Router müssen nun in der Lage sein, den „longest match“ Präfix zu isolieren, d.h. den genaueren Weg zu finden.



Beispiel: VLSM-Routing

Besteht die Zieladresse eines Paketes aus dem Eintrag 140.25.2.133 und die Routingtabelle kennt hierfür drei in Frage kommende Einträge: 140.25.2.0/24, 140.25.0.0/16 und 140.25.2.128/27, muss der Weg 140.25.2.128/27 ausgewählt werden, weil sein Präfix die größte Anzahl Bits besitzt, die mit der Zieladresse übereinstimmt:

Ziel	140.25.2.5	11001100.00011001.00000010 . 10000101
Route 1	140.25.2.0/24	11001100.00011001. 00000010 . 00000000
Route 2	140.25.0.0/16	11001100.00011001. 00000000 . 00000000
Route 3	140.25.2.128/27	11001100.00011001.00000010 . 10000000



Beispiel: VLSM Strukturierung

Einem Unternehmen wurde die IP-Adresse 140.25.0.0/16 zugewiesen. Es plant, das VLSM-Verfahren einzusetzen.

Der erste Schritt des VLSM-Prozesses besteht darin, 4 Bit zu reservieren, um 16 Subnetze zu konfigurieren. Damit verbleiben im Falle der Class-B-Adresse für den Hostteil noch 12 Bit und damit $2^{12} = 4.096$ Netzadressen.

Basisnetz	11001100.00011001.00000000.00000000	140.25.0.0/16
Subnetz 0	11001100.00011001.00000000.00000000	140.25.0.0/20
Subnetz 1	11001100.00011001.00010000.00000000	140.25.16.0/20
Subnetz 2	11001100.00011001.00100000.00000000	140.25.32.0/20
Subnetz 3	11001100.00011001.00110000.00000000	140.25.48.0/20
...	11001100.00011001.xxxx0000.00000000	140.25.xx.0/20
Subnetz 13	11001100.00011001.11010000.00000000	140.25.208.0/20
Subnetz 14	11001100.00011001.11100000.00000000	140.25.224.0/20
Subnetz 15	11001100.00011001.11110000.00000000	140.25.240.0/20

Für die Rechner des Subnetzes 3 (140.25.48.0/20) gilt folglich folgendes Adressschema:

Subnetz 3	10001100.00011001.00110001.00000000	140.25.48.0/20
Rechner 1	10001100.00011001.00110001.00000001	140.25.48.1/20
Rechner 2	10001100.00011001.00110001.00000010	140.25.48.2/20
Rechner 3	10001100.00011001.00110001.00000011	140.25.48.3/20
...	10001100.00011001.0011xxxx.xxxxxxxx	140.25.xx.xx /20
Rechner 4093	10001100.00011001.00111111.11111101	140.25.63.253 /20
Rechner 4094	10001100.00011001.00111111.11111110	140.25.63.254/20

Im zweiten Schritt erweist sich für Subnetz 14 diese Einteilung als zu grob. Daher besteht der Wunsch, eine feinere Struktur einzuführen. Dazu wird das Subnetz erneut in weitere Subnetze eingeteilt, so dass eine Form von „Subnetzen von Subnetzen“ entsteht. Im vorliegenden Beispiel werden vier Bits reserviert, so dass die Netzpräfix-Länge auf 24 Bits ansteigt:

Subnetz 14	11001100.00011001.11100000.00000000	140.25.224.0/20
Subnetz 14-0	11001100.00011001.1110<u>0000</u>.00000000	140.25.224.0/24
Subnetz 14-1	11001100.00011001.1110<u>0001</u>.00000000	140.25.225.0/24
Subnetz 14-2	11001100.00011001.1110<u>0010</u>.00000000	140.25.226.0/24
Subnetz 14-3	11001100.00011001.1110<u>0011</u>.00000000	140.25.227.0/24
...	11001100.00011001.1110<u>xxxx</u>.00000000	140.25.2xx.0/24
Subnetz 14-14	11001100.00011001.1110<u>1110</u>.00000000	140.25.238.0/24
Subnetz 14-15	11001100.00011001.1110<u>1111</u>.00000000	140.25.239.0/24

Den einzelnen Subnetzen können nun mit den verbleibenden 8 Bits (= letztes Byte der Adresse) 254 einzelne Rechner zugeordnet werden:

Subnetz 14-3	11001100.00011001.11100011.00000000	140.25.227.0/24
Rechner 1	11001100.00011001.1110<u>0011</u>.00000001	140.25.227.1/24
Rechner 2	11001100.00011001.1110<u>0011</u>.00000010	140.25.227.2/24
Rechner 3	11001100.00011001.1110<u>0011</u>.00000011	140.25.227.3/24
Rechner 4	11001100.00011001.1110<u>0011</u>.00000100	140.25.227.4/24
...	11001100.00011001.1110<u>0011</u>.xxxxxxx	140.25.227.xx/24
Rechner 253	11001100.00011001.1110<u>0011</u>.11111101	140.25.227.253/24
Rechner 254	11001100.00011001.1110<u>0011</u>.11111110	140.25.227.254/24

In einem dritten Teilungsschritt wird Subnetz 14-14 erneut in acht Netze unterteilt. Dazu sind 3 weitere Bits erforderlich, so dass die verfügbare Rechnerzahl pro Subnetz der dritten Stufe auf 30 sinkt:

Subnetz 14-14	11001100.00011001.11101110.00000000	140.25.238.0/24
Subnetz 14-14-0	11001100.00011001.11100011.00000000	140.25.238.0/27
Subnetz 14-14-1	11001100.00011001.11100011.00100000	140.25.238.32/27
Subnetz 14-14-2	11001100.00011001.11100011.01000000	140.25.238.64/27
Subnetz 14-14-3	11001100.00011001.11100011.01100000	140.25.238.96/27
...	11001100.00011001.11100011.0xx00000	140.25.238.xx/27
Subnetz 14-14-6	11001100.00011001.11100011.11000000	140.25.238.192/27
Subnetz 14-14-7	11001100.00011001.11100011.11100000	140.25.238.224/27

Das Beispiel zeigt das systematische Vorgehen einer Strukturierung mit einer beliebigen Anzahl von Ebenen. Dieses Vorgehen schränkt die Adressverschwendung vor allem bei Transitnetzen ein, wenn nur für die Kommunikationsendpunkte eindeutige Adressen benötigt werden.

■ 6.4 Private Adressvergabe oder Network Address Translation NAT

Ein einfacher Weg, um die Adressknappheit im Internet zu umgehen, besteht darin, spezielle private Adressen zu verwenden. Der RFC 1918 reserviert drei Blöcke für den privaten Gebrauch, die nicht im Internet weitergeleitet werden:

- **Class A** Netze mit 10.0.0.0 bis 10.255.255.255
- **Class B** Netze mit 172.16.0.0 bis 172.31.255.255
- **Class C** Netze mit 192.168.0.0 bis 192.168.255.255.

Ursprünglich waren diese Adressen für den internen Gebrauch und für Testzwecke vorgesehen. Die Adressknappheit veranlasste aber viele Unternehmen, durch diese nicht genutzten Adressen ihre individuelle Netzstruktur hinter Firewalls oder Routern mit Paketfiltern zu verbergen. Wie werden nun diese speziellen Adressen in allgemeingültige IP-Adressen übersetzt? Die Lösung besteht im NAT-Verfahren, das in RFC 1631 definiert ist. Eine Firewall oder ein Router mit der NAT-Option ersetzen für den „Outbound-Verkehr“, d.h. Verkehr vom internen Netz zum Internet, die Quelladresse durch die registrierte IP-Adresse des Router- oder Firewall-Interfaces. Für die empfangenen Pakete arbeitet der Prozess umgekehrt: der NAT-Mechanismus wandelt die Zieladresse in diejenige des privaten Netzes um. Dazu muss der Router die entsprechenden Zuordnungstabellen pflegen. NAT ist interface-unabhängig. Das bedeutet, dass NAT mit jeder Routerschnittstelle assoziiert werden kann, die das interne mit dem externen Adressschema verbindet.

Der Umwandlungsprozess selbst benötigt einen zusätzlichen Prozess und Prozessor Kapazität, so dass die Performance geringfügig leiden kann. In seiner einfachsten Form tauscht NAT lediglich die IP-Adressen aus. Da das IP-Protokoll aber eine Prüfsumme über die Headerfelder bildet, muss diese neu berechnet werden. Dieser Prozess der Neuberechnung setzt sich auf der TCP-Ebene fort.

Die Adresskonversion ist nur ein Vorteil von NAT. Die zusätzliche Sicherheit ist ein weiterer Aspekt, da ein potentieller Angreifer nicht hinter den Router sehen kann und ihm folglich die interne Adressstruktur verborgen bleibt. Obwohl NAT die interne Adresse maskiert, kann allerdings kein IP-Spoofing-Angriff abgewendet werden, weil in einem derartigen Fall der Angreifer auf eine bestehende IP-Verbindung springt und so unbemerkt in das Intranet gelangt.

Als Nachteil des NAT-Konzeptes ist der Verlust der Ende-zu-Ende-Verfolgung anzusehen. Dies gilt insbesondere für Server wie z. B. Webserver, die über das Internet erreichbar sein müssen. Daher können diese nicht am NAT-Prozess partizipieren.

Für die Implementation des NAT-Mechanismus stehen drei Alternativen zur Auswahl:

- Statisches NAT
- Dynamisches NAT
- Port-Level NAT (PAT)

Bei statischem NAT konvertiert das Verfahren jede private IP-Adresse in eine öffentliche IP-Adresse. Die Tabelle muss daher für jede Station des Intranets die entsprechende öffentliche Adresse beinhalten. Das dynamische NAT hingegen verwaltet einen Vorrat an öffentlichen IP-Adressen, aus dem es dynamisch eine dem anfordernden internen Rechner zuordnet. Der wiederholte Verbindungsaufbau einer Station kann daher zu einer jeweils anderen IP-Adresse aus dem Bestand führen. Das PAT wiederum überträgt interne Verbindungen auf eine einzelne öffentliche IP-Adresse und unterscheidet die Verbindungen durch die Hinzunahme der TCP-Port-Nummern.

Abhängig von der Implementation müssen einige Anpassungen an der Installation vorgenommen werden. Dazu zählen:

- die Modifikation der Filterregeln, da NAT die Quell- und Zieladresse verändert
- die Privatisierung der Netzadressen verlangt meist eine Neuvergabe der IP-Adressen für die Rechner des Intranets.

Neben den drei klassischen IPv4-Privatadressbereichen steht noch ein weiterer Adressbestand von 169.254.1.0 bis 169.254.254.255 zur Verfügung. Auch dieser reservierte Bereich wird nicht geroutet und ist als Automatic Private IP Addressing nach RFC 3927 bekannt. Sinn dieser Adressen ist eine automatische Konfigurationsmöglichkeit. Dazu wird mit Hilfe der MAC-Adresse und einem Zufallsgenerator eine entsprechende Adresse erzeugt, die über ARP auf Eindeutigkeit überprüft wird. Dazu wird ein ARP-Paket mit 0.0.0.0 als Absenderadresse und der eigenen IP-Adresse als Empfängeradresse gesendet. Dieses Paket wird insgesamt dreimal verschickt. Erhält die Ausgangsstation innerhalb von zwei Sekunden nach Versenden des letzten Pakets eine Antwort, bei der die Absenderadresse mit der errechneten IP-Adresse übereinstimmt, muss der Erzeugungsprozess neu gestartet werden, da ein Duplikat entdeckt wurde. Dieser so genannte Zeroconf-Mechanismus ist in jedem Betriebssystem unter einer anderen Bezeichnung vorhanden:

- bonjour bei MAC-OS
- avahi-Dämon in Linux
- APIPA bei Windows

■ 6.5 Classless-Inter-Domain-Routing CIDR

Mit der zunehmenden Attraktivität des Internets steigt gleichzeitig die Menge der im weltweiten Datennetz bekannten Netze und Routen und damit die Gefahr, in den zentralen Backbone-Routern Überlastprobleme durch ausufernde Routingtabellengrößen auszulösen. Um die Anzahl der Routen zu senken oder zumindest konstant zu halten, erarbeitete die IETF einen Vorschlag, um die Adressklassen von IP in Blöcken zusammenzufassen und auf diese Weise die Alternativen der Wegewahl zu reduzieren. Diese Idee lässt sich sowohl

für die bestehenden IP-Adressklassen als auch für die Weitergabe der Subnetzinformation einsetzen. Ein einziger Eintrag einer zusammengefassten Route übernimmt dann die gleiche Funktion wie eine Vielzahl von Routingtabelleneinträgen. Das resultierende Verfahren wird seit April 1994 im Internet als CIDR (Classless Inter Domain Routing) eingesetzt und in den RFCs 1517 bis 1520 spezifiziert.

Die Zuteilungspraxis aufgrund der Adressknappheit von Class-B-Adressen jeder Institution ein Bündel von Class-C-Adressen zuzuweisen, führt zu steigenden Tabelleneinträgen in den Routern; denn statt eines Class-B-Eintrages sind nun viele Class-C-Routen zu verwalten. Abhilfe schafft hier eine Strukturierung des Adressraums auf Blöcke, die nicht willkürlich, sondern zusammenhängend in Größen von Zweierpotenzen vergeben werden und an einem Vielfachen seiner Größe beginnen. So reicht für den gesamten Block ein einziger Routereintrag mit der zugehörigen Netzmaske.



Beispiel: CIDR

Für einen Block mit 8 Class-C-Adressen wird ein passender Startblock gesucht. Da $8 = 2^3 = 00001000_2$ gilt, sind geeignete Startpunkte solche IP-Adressen, bei denen mindestens ebensoviele Nullen am Ende des 3. Bytes vorhanden sind, wie bei der Blockgröße (im Beispiel 3):

Blockstart	Binärschreibweise
geeignet	
193.1.8.0	11000001.00000001. 00001000 .00000000
193.1.64.0	11000001.00000001. 01000000 .00000000
193.1.136.0	11000001.00000001. 10001000 .00000000
ungeeignet	
193.1.4.0	11000001.00000001. 00000100 .00000000
193.1.37.0	11000001.00000001. 00100101 .00000000
193.1.165.0	11000001.00000001. 10100101 .00000000

Durch die Zusatzangabe der Subnetzinformation teilen Router anderen Routern die Größe des ermittelten Adressbereiches mit. Ein Beispiel für diese Art Routingprotokoll ist das RIP-2, das neben der Adressinformation auch die Netzmaske eines Weges anzeigt, eine wesentliche Voraussetzung für den Einsatz von CIDR. Ein Netz in CIDR-Notation lautet dann: 193.1.16.0/20. Hinter dieser Angabe verbergen sich die Netze 193.1.16.0 bis 193.1.31.0, die 20 bedeutet, dass die Netzmaske die ersten 20 Bit für den Netzwerkteil setzt, während die restlichen 12 Bit den Hostteil repräsentieren. Werden diese 16 Netze in einen Block „geroutet“, führt das zu einer Ersparnis von 15 Routingtabelleneinträgen. Durch rekursive Anwendung steigt der Vorteil dieses Konzeptes weiter. Berücksichtigt ein Router nur Netze, die aus einem Block stammen, so müssen Router außerhalb dieses IP-Adress-Blockes nur einen Weg zum gesamten IP-Adress-Block kennen. Das bedeutet, dass die Kenntnis von Routen pro Aggregationsstufe abnimmt und auf höherer Ebene weitere Routen zu einer einzigen zusammengefasst werden können.



Beispiel: CIDR-Subnetzbildung

Das Class-C-Netz eines Unternehmens 193.1.1.0 ist in mehrere Subnetze unterteilt: 193.1.1.0/27, 193.1.1.32/27, 193.1.1.64/27 und 193.1.1.96/27. Um eine zusammengefasste Route abzuleiten, bietet sich folgendes Vorgehen an:

- Darstellung der Netzadresse in Binärform
- Um die einheitliche Subnetzmaske zu identifizieren, sollte der Prüfprozess mit dem linken Bit beginnen
- Fortführung der Prüfung auf Gleichheit der Bits von „links nach rechts“
- Das erste Bit, dass keine Übereinstimmung ergibt, stoppt den Prozess
- Im Beispiel:

11000001.00000001.00000001.00000000

11000001.00000001.00000001.00100000

11000001.00000001.00000001.01000000

11000001.00000001.00000001.01100000

Eine Übereinstimmung ist bis einschließlich des 25. Bits gegeben. Daher ist die propagierte Route 193.1.1.0/25

Problematisch werden bei einer strengen Strukturierung nach dem CIDR-Konzept solche Netze, die aus dem Schema ausbrechen. Wechselt z.B. ein Internetnutzer seinen Provider und möchte seine IP-Adresse behalten, muss der neue Provider dieses Netz versorgen, d.h. er muss eine spezifische Route zu diesem IP-Adress-Block für lediglich einen Nutzer bekannt machen.

6.6 Verwaltungsfunktionen auf IP-Basis

Netzwerkmanagement ist als die Summe aller Verfahren und Methoden anzusehen, um Netzwerke:

- zu planen
- zu konfigurieren
- zu steuern
- zu überwachen
- zu verwalten.

Um im Kontext der IP-Adressierung bereits erste Schritte in diese Richtung unternehmen zu können, stehen einige Basisfunktionen bereit.

- **ping:** basiert auf den ICMP-Nachrichten echo und echo reply. Durch Eingabe einer IP-Adresse wird die Erreichbarkeit des Teilnehmer auf der Grundlage des Layer-3-Protokolls geprüft. Dieser Mechanismus dient daher dazu, die korrekte Funktion des Layer-3-Protokolls zu verifizieren.

- **tracert**: diese Funktion ermittelt den Paketleitweg vom Sender zum Empfänger. Auf diese Weise lässt sich feststellen, auf welchem Wege die Pakete ans Ziel gelangen und im Falle einer erfolglosen Zustellung, wo der Pfad unterbrochen ist.
- **ipconfig**: gibt die Netzkonfiguration eines Endgerätes an. Die Ausgabe dient zur Überprüfung, ob die Station über eine korrekte IP-Adresse verfügt, ob ein Defaultgateway eingetragen ist und die Subnetzmaske den Vorgaben entspricht.
- **netstat**: zeigt statische Auswertungen der einzelnen Protokolle wie Ethernet oder IP an. Mit Hilfe dieser Angaben lassen sich Fehlersituationen ermitteln oder ein Eindruck von der Netzlast gewinnen.
- **nslookup**: dieser Befehl dient der Ermittlung der IP-Adresse bzw. des Domainnames eines Rechners mithilfe des Domainnameservices DNS. Neben den reinen Adressdaten werden weitere Informationen angezeigt.

Weitere auf dem Layer-3 basierende Probleme können Ursachen in Konfigurationsproblemen sowohl der Geräte als auch der Protokolle haben. Dazu zählen:

- unterschiedliche Duplex-Einstellungen der Switchports
- doppelte Vergabe von IP-Adressen
- fehlerhafte Konfiguration von Routen auf Hosts oder Servern



Noch Fragen ...? Ja ...

Warum nutzen viele Unternehmen private IP-Adressen, obwohl sie genügend öffentliche Adressen besitzen?

Ein Grund dafür liegt darin, dass die Adressvergabe nicht revidiert werden muss, wenn der Provider gewechselt wird.

6.7 Zusammenfassung

Die IP-Adressierung ist eine logische Funktion. Sie hilft, die Einzelheiten des physischen Netzaufbaus vor den Nutzern zu verbergen. Das entstehende Internet als Verbindung vieler Einzelnetze wirkt dabei wie eine Einheit. Konzeptionell besteht jede Adresse aus einem Paar, deren Komponenten sowohl ein Netzwerk als auch einen Rechner identifizieren. Das ursprüngliche Adressierungsschema ist klassenbestimmt, d. h. die Grenze zwischen Präfix und Suffix einer Adresse kann berechnet werden. Damit ist der Aufbau selbstidentifizierend. Mit fortschreitender Adressknappheit ist diese Stringenz modifiziert worden, so dass Konzepte jenseits der Klassenbindung entstanden. Dazu gehören CIDR und VLSM, deren Bedeutung stetig gewachsen ist. Administratoren müssen daher in der Lage sein, sowohl die Subnetzbildung als auch die neueren Verfahren der Adresszuweisung zu verstehen, um potentielle Fehler zu erkennen und eine sparsame Vergabe zu ermöglichen. Bei einer strukturierten Vergabe haben sich einige Kriterien als sinnvoll erwiesen:

- von vielen Teilnehmern genutzte Geräte wie Server oder Drucker sollten eine statische IP-Adresse besitzen

- Router sind Konzentrationspunkte des Netzwerkgeschehens und kommunizieren mit Geräten außerhalb des lokalen Netzes. Daher müssen sie notwendigerweise über eine unverwechselbare Adresse verfügen
- Endgeräte, die einen spezifischen Dienst anbieten, müssen ebenfalls von außerhalb erreichbar sein
- alle anderen Geräte benötigen nicht zwingend eine öffentliche Adresse. Sie sind Kandidaten für ein privates Adressschema

An der Schwelle zur Ablösung von IPv4 durch IPv6 zeigen sich die Schwächen des ursprünglichen Entwurfs. Das klassenbasierte Adressierungsschema ist der großen Nachfrage nach Adressen nicht gewachsen, eine durchgehende hierarchische Struktur, die das Routing erleichtern würde, existiert nicht und die Routingtabellen zentraler Vermittlungsstellen im Internet wachsen bis zur Grenze des Handhabbaren. Dennoch bleiben die grundsätzlichen Strukturen bestehen, so dass deren Verständnis für die Administration unerlässlich ist.

Die Vergabeinstitutionen für Internetadressen besitzen folgende Adresse:

- Zentrale Behörde: <http://www.iana.net>
- Europa: <http://www.ripe.net>

Für die Konzeption zulässiger Subnetze gibt es frei verfügbare Subnetzkalculatoren, z.B. unter: <http://www.solarwinds.com>

■ 6.8 Wissensüberprüfung

1. Ist die Adresse 147.14.255.255 eine Broadcast-Adresse für ein Class-B-Netz mit der Standardsubnetzmaske?
2. Wie viele IP-Adressen sind in einem Class-C-Netz nutzbar? Begründen Sie Ihre Ansicht.
3. Welchen Wertebereich besitzt das erste Byte einer Class-A-Adresse?
4. Welche der folgenden Adressen gehören zur Class-C?
129.219.95.193 – 209.101.218.30 – 151.13.27.114 – 192.119.15.17
5. Zu welcher Klasse gehört die Adresse 129.21.89.77?
6. Ein Unternehmen möchte fünf Subnetze mit jeweils 20 Hosts für ein Class-C-Netz aufbauen. Welche Subnetzmaske muss es wählen?
7. Wie viele nutzbare Subnetze existieren für ein Class-B-Netz mit der Subnetzmaske 255.255.255.0?
8. Wie viele Bits sind bei einer Standardsubnetzmaske in einem Class-B-Netz für die Hosts reserviert?
9. Welches Kriterium entscheidet über die Zugehörigkeit einer Adresse zur Class B?
10. Worin besteht der Nutzen der Subnetzbildung?

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Welche Merkmale beinhaltet TCP zur sicheren Datenübertragung?
- Wie läuft der Drei-Wege-Handshake ab und was ist seine Bedeutung?
- Welche Merkmale trennen TCP von UDP?

Kapiteleinführung

TCP ist das unverzichtbare Begleitprotokoll des Internetprotokolls IP. Auch wenn es weniger bekannt ist, kommt ihm dennoch eine wichtige Funktion zu: es initiiert und verwaltet sichere virtuelle Verbindungen zwischen Kommunikationspartnern. Dabei spielt TCP die Rolle eines „Staubereiters“. Es veranlasst die Drosselung des IP-Verkehrs, meldet Staus und ermittelt über die Qualität der Verbindung, ob ein Paket/Segment als verloren anzusehen ist. Die Diskussion um die neue IPv6-Version betrifft TCP nicht unmittelbar. Anpassungen struktureller Natur werden durch einen Wechsel des IP-Dialektes nicht ausgelöst.

■ 7.1 Transmission Control Protocol im Detail

TCP ist ein Protokoll der Schicht 4 des ISO/OSI-Referenzmodells und gewährleistet die zuverlässige Nachrichtenübermittlung zwischen Sender und Empfänger. Der Status ist trotz seiner Beschreibung in RFC 793 der einer Empfehlung, was seiner großen Verbreitung aber keinen Abbruch getan hat. Zu Beginn des Übertragungsvorganges erhält TCP Nachrichten oder einen Datenstrom von einem Anwendungsprogramm. Daraufhin werden die Daten in kleinere Pakete – als Segmente bezeichnet – geteilt, Kontrollinformationen hinzugefügt und der neu entstandene Paketstrom an die nächst tiefere Schicht 3 weitergeleitet. Hier werden die einzelnen Segmente um Adressinformationen erweitert, die einen geeigneten Weg durch das Netz festlegen. Die Ergänzung der Ursprungsdaten hat zum Ziel, durch Prüf- und Leitinformationen eine stabile und schnelle Route durch das Gewirr der Netzknoten zum Empfänger zu finden:

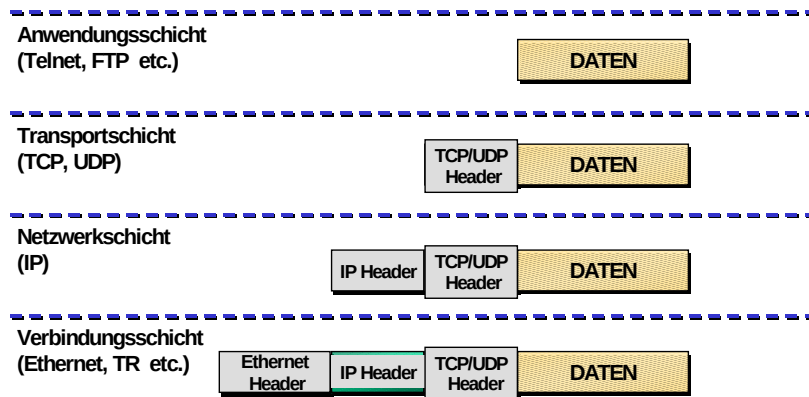


Bild 7.1
Header versus
Nutzdaten

Segmente, die beim Empfänger eintreffen, wandern in umgekehrter Richtung durch die Protokollhierarchie. Jede Schicht entfernt die entsprechende Headerinformation bis auf der Anwendungsebene die reinen Daten zurückbleiben. Gemäß dieses Ablaufs bestehen die Kernfunktionen von TCP darin,

- die individuelle Kommunikation zwischen Sender und Empfänger zu überwachen
- den Nachrichtenstrom in Form von Segmenten einzuteilen und diese in entsprechender Reihenfolge wieder zusammen zu setzen
- die genutzten Anwendungen eindeutig zu identifizieren

7.1.1 Besonderheiten

TCP/IP zeichnet sich durch mehrere Eigenschaften aus, die es gleichermaßen für Hersteller und für Anwender attraktiv machen:

- **Weit verbreitet:** TCP/IP ist auf vielen Hardwareplattformen zum etablierten Standard geworden. Hersteller haben TCP/IP als Industrienorm akzeptiert.
- **Offen, nicht proprietär:** TCP/IP ist an keinen Hersteller gebunden, sondern als Teil der Aktivitäten der Internet Engineering Task Force (IETF) unabhängig von einschlägigen Interessen. Die Protokolle können mit jeder Standard-Hardwarekonfiguration eingesetzt und in den Netzbetrieb eingebunden werden.
- **Skalierbarkeit:** Ein bestehendes Netzwerk auf TCP/IP-Basis kann mühelos um weitere Stationen erweitert werden. Dazu ist lediglich neuen Rechnern eine Adresse zuzuweisen.
- **Grundlage des Internets:** Seine Verbreitung verdankt TCP/IP zwei Umständen. Einerseits ist es als Bestandteil von UNIX und seit dessen verstärktem Aufkommen praktisch mit jeder UNIX-Workstation verfügbar, andererseits basiert der Information-Highway in Gestalt des Internets auf diesem Protokoll.

7.1.2 Merkmale

TCP liefert eine zuverlässige virtuelle Verbindung zwischen Hosts, die über IP verbunden sind. TCP verwendet das IP-Protokoll als Grundlage des Segmenttransportes zwischen Kommunikationsendpunkten. Die Endpunkte sind die Ports des Betriebssystems.

TCP sichert die Transportqualität des Segmentes, indem es kontrolliert, dass die Daten nicht verändert werden, nicht verloren gehen, nicht dupliziert werden und in der richtigen Reihenfolge eintreffen.

Mehrere Punkte beschreiben die operationalen Charakteristiken:

- **Basisdatentransfer:** TCP überträgt einen kontinuierlichen Fluss von 8-Bit-Gruppen bidirektional in jede Richtung. Diese Gruppen werden in TCP-Segmente zusammengefasst und durch Sequenznummern unterschieden. Eine Anwendung muss dabei sicher sein, dass alle an TCP übergebenen Daten übertragen wurden. Um diese Sicherheit herzustellen, existiert eine Push-Funktion, die dafür sorgt, dass alle im Puffer befindlichen TCP-Segmente an den Empfänger weitergeleitet werden.
- **Zuverlässigkeit:** TCP erreicht ein gewisses Zuverlässigkeitsniveau durch die Zuweisung von Sequenznummern: Außerdem muss der Segmenterhalt vom Empfänger bestätigt werden (ACK). Wird diese Bestätigung nicht innerhalb des Time-Out-Intervalls zugestellt, erfolgt eine Retransmission des betroffenen Segmentes. Dabei wird die Zeitschranke dynamisch für jede Verbindung auf der Basis der Round-Trip-Time festgelegt. Der Empfänger setzt die Nachricht anhand der Sequenznummern zusammen und kann erkennen, ob Duplikate vorliegen oder ob Segmente fehlen. Fehlerhafte Segmente werden durch die Prüfsumme identifiziert und verworfen.
- **Datenflusskontrolle:** TCP unterstützt das Sliding Window-Prinzip, nach dem eine Seite eine Anzahl Segmente (= Windowgröße) ohne explizite Bestätigung senden darf. Der Empfänger des TCP-Segmentes gibt dem Sender Auskunft über die Anzahl der Bytes, die er ohne Gefahr eines Überlaufens der internen Empfangspuffer verarbeiten kann.



Die Windowgröße ist für die Dauer einer Verbindung keineswegs konstant. Jedes Acknowledgement enthält ein Windowadvertisment, das die Zahl der Bytes angibt, die der Empfänger problemlos verarbeiten kann.

- **Multiplexing:** TCP gestattet vielen Prozessen eines Rechners, die TCP Kommunikationsdienste zu nutzen. Dazu besitzt TCP eine Portmenge, deren Nummer mit der Netzadresse zu einem eindeutigen Schlüssel kombiniert wird. Diese als Sockets bezeichneten Kommunikationspunkte identifizieren für Sender und Empfänger einen eindeutigen Übertragungsweg.
- **Verbindungen:** TCP muss für jede Verbindung Statusinformationen initialisieren und pflegen. Dazu gehören Sequenznummern und die Windowgröße. Zusätzlich liefert TCP die Vollduplex-Fähigkeit, d. h. die simultane Übertragung in beide Richtungen.

Der TCP-Protokoll-Header besteht aus folgenden Feldern:

0		16		32	
Quell-Portnummer		Ziel-Portnummer			
Sequenznummer					
Acknowledgementnummer					
Offset	reserviert		Flags	Windowgröße	
Prüfsumme				Urgent Pointer	
Nutzdaten					

Bild 7.2 TCP-Header

Die TCP-Felder sind wie folgt definiert:

- **Quellport** identifiziert die Portnummer des Anwendungsprogramms des Senders.
- **Zielpport** identifiziert die Portnummer der Anwendung des Ziels.
- **Sequenznummer** definiert eine während der Verbindungsdauer eindeutige Nummer zur Identifikation des Datenstroms. Sie entspricht der Sequenznummer des Vorgängersegmentes vergrößert um die Datenanzahl des laufenden Segmentes.
- **Acknowledgementnummer** ist eine eindeutige Nummer, die gemäß des Window-Prinzips den Empfang einer Anzahl von Segmenten bestätigt. Fehlt diese Bestätigung innerhalb einer Zeitschranke, erfolgt eine Retransmission der Segmentfolge. Sie umfasst das vorhergehende Acknowledgement plus dem Betrag der erhaltenen Daten.
- **Offset** gibt die Länge des TCP-Headers in 32-Bit Worten an und damit die Stelle, ab der die eigentlichen Daten beginnen.
- **Reserviert** besitzt keine Verwendung.
- **Flags** ist ein Kontrollbit zur Identifikation des Segmentzwecks:
 - **URG:** Urgent-Zeiger-Feld.
 - **ACK:** Acknowledgementnummer-Feld.
 - **PSH:** Die Daten sollen sofort an die nächsthöhere Schicht weitergereicht werden.
 - **RTS:** Rücksetzen der Verbindung.
 - **SYN:** Synchronisation der Sequenznummern, die eine Bestätigung verlangt.
 - **FIN:** Verbindungsabbau, der quittiert werden muss.
- **Windowgröße** erlaubt es einem Empfänger, dem Sender über ACK-Messages mitzuteilen, wie viel Pufferplatz in Byte zum Empfang der Daten zur Verfügung steht. Ein Eintrag von 0 stoppt den Sendevorgang.
- **Prüfsumme** verifiziert das gesamte Segment (Header + Daten) nach dem in IP festgelegten Algorithmus.
- **Urgent-Zeiger** beschreibt die Position priorisierter Daten, die so schnell wie möglich

verarbeitet werden sollen. Damit können außergewöhnliche Zustände signalisiert werden.

- **Optionen** können entweder aus einem einzelnen Byte – der Optionsnummer – bestehen oder eine variable Form aufweisen:
 - **End of Option List** zeigt das Ende der Optionsliste an und wird insbesondere dann verwendet, wenn Optionen die zulässige Segmentlänge überschreiten. Option = 0; keine weiteren Einträge.
 - **No Operation** kennzeichnet Grenzen zwischen Optionen. Sie bewirkt eine Ausrichtung der einzelnen Optionen auf die 32-Bit-Grenze. Option = 1; keine weiteren Einträge.
 - **Maximum Segment Size** bestimmt die max. Segmentgröße von TCP. Diese Option sollte nur zur Initialisierung benutzt werden (bei gesetztem SYN-Bit). Option = 2; Länge = 4; Optionsdaten = max. Segmentgröße.

Der Multiplexingmechanismus von TCP ermöglicht die Koexistenz einer Vielzahl höherer Protokolle und Verarbeitungsprozesse auf einem Rechner. TCP/IP-Anwendungen verwenden für die Kommunikation Socket-Schnittstellen. Ein Socket bietet im Netzwerk eine einfache und direkte Methode gegenseitig Daten auszutauschen. Ein TCP/IP-Socket besteht aus der Portnummer, der Stationskennung (IP-Adresse) und dem Transporttyp (TCP oder UDP). Portnummern werden verwendet, um Anwendungen zu unterscheiden. Zu den Well-Known-Services auf Well-Known-Ports gehören auch die ursprünglichen UNIX-Dienste (vgl. Tabelle 7.1).

Tabelle 7.1 Well-Known-Ports und Well-Known-Services

Portnummer	Protokoll
23	Telnet
20, 21	FTP – File Transfer Protokoll
25	SMTP – Simple Mail Transfer Protokoll
80	http – Hypertext Transfer Protokoll
179	BGP – Border Gateway Protokoll

7.1.3 Verbindungsmanagement

Die Herstellung und der Abbau einer virtuellen Verbindung zwischen zwei Partnern und deren beteiligten Prozessen verlaufen in mehreren Phasen:

- **Verbindungsaufbau:** Die Initialisierung zwischen zwei TCP-Prozessen erfolgt nach dem „Three-Way-Handshake“.



Ein weiterer Grund liegt darin, dass die Sequenznummern nicht nach einem netzweiten Zeitprotokoll vergeben werden und auf diese Weise Duplikate entstehen können.

Zu Übertragungsbeginn legt jede Station einen Anfangswert der Sequenznummer fest. Diese Zahl wird durch eine 32-Bit-Uhr betrieben, die ihren Wert alle 4 ms inkrementiert. Dieser Mechanismus führt dazu, dass die Sequenznummern sich nach einer Verbindungsdauer von ca. 5 Std. wiederholen. Der Three-Way-Handshake-Mechanismus durchläuft drei Stadien:

- **SYN sent:** Ein TCP-Segment mit gesetztem SYN-Flag wird zur Zielstation gesendet.
- **SYN Received:** Der Zielrechner antwortet mit einer inkrementierten Acknowledgementnummer und einem gesetztem SYN- und ACK-Flag.
- **Established:** Die Verbindung ist hergestellt und ermöglicht die Vollduplex-Datenübertragung. Dieser Zustand wird durch ein gesetztes ACK-Flag signalisiert.

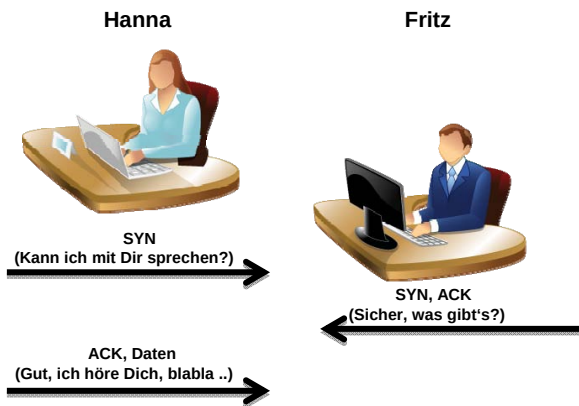


Bild 7.3 TCP-Verbindungs Aufbau mit entsprechenden Flags

- **Datenaustausch:** Bei gesetztem ACK-Flag werden Sequenz- und Acknowledgementnummer in Abhängigkeit vom Datenumfang entsprechend inkrementiert. Virtuelle Verbindungen, die keine aktive Übertragung abwickeln, erzeugen auch keine Datenlast. Zur individuellen Steuerung der Datenübertragung dient das Push-Flag. Nur wenn dieses gesetzt ist, werden alle Daten, die sich im Sendepuffer befinden, in einem oder mehreren Segmenten verschickt. Ist das Push-Flag nicht gesetzt, werden die Daten zwischengespeichert.

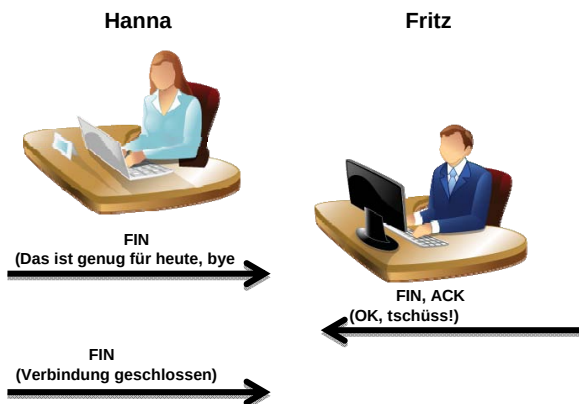


Bild 7.4 TCP-Verbindungsabbau und entsprechende Flags

- **Verbindungsabbau:** Die Auflösung einer Verbindung geschieht ebenso wie der Verbindungsaufbau in mehreren Schritten unter Zuhilfenahme der Flags FIN und ACK:
 - **FIN Wait:** Ein Teilnehmer A überträgt ein Segment mit gesetztem FIN-Flag und wartet auf das ACK des Partners.
 - **Close Wait:** Der gerufene Partner B quittiert den einseitigen Verbindungsabbauwunsch durch eine inkrementierte Acknowledgementnummer bei gesetztem ACK-Flag. Danach dürfen keine Daten mehr von A nach B, wohl aber von B nach A fließen.
 - **Time Wait:** Teilnehmer B wartet so lange, bis sichergestellt ist, dass Partner A das ACK erhalten hat.

Ein höheres Protokoll wie IP kann einseitig den Abbruch einer Verbindung erzwingen. Unter diesen Umständen kontrolliert TCP nicht mehr die geregelte Auflösung der Kommunikation, so dass ein Datenverlust auf dem Weg zwischen den beiden TCP-Partnern in Kauf genommen werden muss.

7.1.4 Fehlervermeidungsmechanismen

- **Acknowledgement:** Sequenznummer und Acknowledgement lösen das Problem verloren gegangener Segmente. Fehlt ein Segment in der Reihenfolge der Sequenznummern, stellt der Empfänger keine Bestätigung aus. Erhält der Sender innerhalb einer bestimmten Zeitspanne keine Bestätigung, wiederholt er die Datenübertragung.
- **Maximale Segmentgröße (MSS):** Dieser Wert gibt die maximale Anzahl von Daten spezifiziert in Bytes an, die zwischen zwei Endpunkten übertragen werden kann. Sender und Empfänger müssen dieser Angabe zustimmen. Sie bestimmt wesentlich den Durchsatz. Ein optimaler Wert ist schwierig festzulegen, weil eine zu geringe Segmentgröße das Netz unterauslastet, ein zu hoher Wert aber zu IP-Paketen führt, die fragmentiert werden müssen. Eine ideale Größe vermeidet gerade diese Zerlegung.



Während des Verbindungsaufbaus sendet die Quelle eine Segmentgrößenangabe, die aus der MTU des Ausgangsinterfaces verringert um die Headergröße von TCP und IP besteht, z. B. MTU von 1500 Bytes als Ethernetstandard abzüglich 40 Bytes für die TCP/IP-Header, so dass die Segmentgröße 1460 Bytes beträgt.

- **Datenflusskontrolle (Window-Prinzip):** Um zu verhindern, dass Daten wegen fehlender Ressourcen auf der Empfängerseite nicht entgegengenommen werden können, beeinflusst TCP den Datenfluss.



Der Grund hierfür kann in der unterschiedlichen Übertragungs- und Verarbeitungsgeschwindigkeit der am Kommunikationsprozess beteiligten Komponenten liegen.

Dies geschieht durch das Window-Prinzip, das dynamisch die Rechnerressourcen in Form eines Fensters verwaltet. Dieses Fenster gibt als „Kredit“ die Anzahl Datensegmente an, die ohne Bestätigung empfangen werden können. Ein Wert von Null zeigt dabei an, dass keine Möglichkeit besteht, Segmente entgegenzunehmen. In der Regel tritt dies nur unter zwei Umständen auf: die Empfängerressourcen sind erschöpft oder der Empfänger baut die Verbindung ab. Ein einfaches Transportprotokoll könnte daher nach folgendem Prinzip verfahren: Ein Segment wird gesendet und das folgende wird erst dann übertragen, wenn die Eingangsbestätigung des Empfängers für das erste vorliegt. Erfolgt die Bestätigung nicht innerhalb einer bestimmten Zeitspanne, wird eine Retransmission vorgenommen. Dieser Mechanismus arbeitet sehr zuverlässig, nutzt jedoch nur einen Teil der verfügbaren Bandbreite. Die Modifikation dieses Protokollablaufs sieht daher eine Gruppierung von Segmenten gemäß folgender Regeln vor:

- Der Sender versendet eine Anzahl von Segmenten innerhalb eines Windows ohne ACK. Für alle einzelnen Segmente ist ein gesonderter Timer erforderlich.
- Der Empfänger muss die Segmentgruppe mit der letzten erhaltenen Sequenznummer gemeinsam bestätigen.
- Der Sender verändert die Windowgröße mit jedem erfolgreich erhaltenen ACK.

Da die Übertragungszeit der Datensegmente und ihrer Acknowledgements aufgrund der Verzögerungszeiten im Netzwerk nicht konstant ist, ist ein adaptiver Retransmissionsmechanismus notwendig, der die Übertragung überwacht und ein angemessenes Time-Out-Intervall auf der Basis einer Round-Trip-Time berechnet.

TCP-Window: Dieses Fenster ist ein Verfahren zur Datenflusskontrolle. Es verhindert Überlastsituationen durch die Angabe eines Datenbetrags den der Sender ohne Bestätigungserhalt senden darf. Beträgt der Wert 64 KB kann der Sender lediglich 64 KB übertragen. Anschließend muss er die Sendung einstellen und auf eine Bestätigung warten. Erhält der Sender ein Acknowledgement für die ersten 32 KB, kann er nur 32 KB übertragen, weil er sonst sein Limit von 64 KB überschreiten würde. Die Merkmale, die die Größe des TCP-Windows bestimmen, betreffen sowohl die Quelle als auch das Ziel:

- **Empfängereinfluss:** Die vom Empfänger benötigte Zeit für die Verarbeitung der erhaltenen Daten und die Versendung der Bestätigung kann die Datenerzeugung des Senders übersteigen, so dass es notwendig ist, die Übertragungsrate des Senders zu kontrollieren, um einer Überlastung des Empfängers vorzubeugen.
- **Sendereinfluss:** Der Sender muss den Datenfluss der verfügbaren Bandbreite und den sich wechselnden Netzwerkbedingungen anpassen.
- **Windowsanpassung:** Der TCP-Header erlaubt lediglich 16 Bit für die Fensterangabe. Dies entspricht einem maximalen Segmentgrößenwert von 64 KB. Damit wird der Durchsatz begrenzt. RFC 1323 bietet eine Skalierungsoption, die diese Grenze hinausschiebt. Die Option erweitert die Festlegung auf 32 Bit und nutzt dann einen Skalierungsfaktor zur Anpassung an das 16-Bit-Feld. Der Skalierungsfaktor wird in einer TCP-Option angegeben und nur in einem Verbindungsaufbausegment bei gesetztem SYN-Bit übertragen. Damit ist die Windowsgröße in beide Richtungen bereits beim Verbindungsaufbau fixiert.

Überlastkontrolle: TCP verwendet Überlastkontrollalgorithmen, um die Netzwerkkapazität zu bestimmen. Wenn eine Überlastung erkannt wird, wird der Slow-Start-Algorithmus aktiviert. Zwei Parameter: das Überlastwindow W und die Slow-Start-Schwelle S bestimmen seine Funktion. Der Anfangswert von W beträgt eine maximale Segmentgröße MSS , für S gilt keine Einschränkung. S kann bis zu 65 535 Bytes betragen, muss aber als Antwort auf eine Überlast reduziert werden.

Der Slow-Start-Algorithmus tritt in Aktion, wenn $W < S$ ist, wohingegen ein Überlastvermeidungsverfahren aktiviert wird, wenn $W > S$ gilt. Bei Gleichheit beider Parameter existiert Wahlfreiheit. Die Funktionsweise des Slow-Start-Prinzips lässt sich wie folgt beschreiben: jedes Mal wenn eine Bestätigung eintrifft, wird das W um Eins vergrößert. Der Sender beginnt mit der Übertragung eines Segmentes. Sobald ein Acknowledgement eintrifft, wird der Wert von Eins auf Zwei angehoben. Sobald ein Time-Out oder ein doppeltes Acknowledgement registriert wird, senkt sich S auf die Hälfte des Wertes von W und W wird auf Eins zurückgesetzt.

Zwar steigt der Wert von W bei erfolgreicher Übertragung, der genaue Ablauf hängt aber davon ab, ob TCP das Slow-Start- oder das Überlastvermeidungsverfahren nutzt. Falls $W < S$ gilt, startet der Slow-Start-Algorithmus. Gab es bereits eine Überlastsituation, tritt der Überlastvermeidungsprozess in Kraft, sobald die Hälfte des Wertes erreicht ist, der die Überlastung auslöste. In diesem Fall wird W nur noch um den Wert $(MSS)^2/W$ angehoben.

Wenn ein Empfänger eine Segmentnummer erhält, die größer als diejenige ist, die er als nächstes erwartet, erkennt er, dass die Segmente in veränderter Reihenfolge ankommen. Er erzeugt daraufhin ein Acknowledgement mit der letzten Sequenznummer der korrekten Reihenfolge, d. h. es entsteht eine doppelte Bestätigung. Im Falle dreier derartig erzeugter Bestätigungen, geht der Sender von einem Paketverlust aus und reagiert hierauf mit einer unmittelbaren Retransmission ohne den Ablauf der Timer abzuwarten. Dieses Verfahren ist als Fast Retransmit bekannt. Anschließend wird als Fast Recovery der Überlastvermeidungsalgorithmus anstelle des Slow-Start-Verfahrens aktiviert.

7.1.5 User Datagram Protocol UDP

UDP stellt eine vereinfachte Form von TCP dar und liefert wie dieses Protokoll ein Kommunikationsmittel zwischen Applikationen auf unterschiedlichen Internetknoten.

Anwendung	E-Mail	FTP	SNMP
Transport	UDP		TCP
Internet	IP	ICMP	
	ARP	Routingprotokolle	
Netzwerkschnittstelle	Ethernet	Token Ring	Frame Relay
	Kupferkabel		Glasfaser

Bild 7.5 UDP-Einordnung

UDP bietet eine unzuverlässige, verbindungslose Datenübertragung. Es werden keine Empfangsbestätigungen für Segmente erstellt und eingehende Nachrichten werden weder in einer Reihenfolge sortiert, noch gibt es eine Rückmeldung über die Frequenz gesendeter Nachrichten. UDP-Messages können daher ohne Kontrolle verloren gehen, in falscher Reihenfolge gesendet oder dupliziert werden. Eine Anwendung auf UDP-Basis muss in der Lage sein, mit diesen Problemen umzugehen. Die Leistungsfähigkeit hängt daher weitgehend von der Programmierung der Anwendung ab. Trotz dieser Mängel besitzt UDP den Vorteil der Schnelligkeit. Gegenüber TCP weist UDP etwa die dreifache Übermittlungsgeschwindigkeit auf.

Der UDP-Header zeigt folgenden Aufbau:

0	16	31
Quell-UDP-Port	Ziel-UDP-Port	
Länge	Prüfsumme	
Nutzdaten		

Bild 7.6 UDP-Header

- **Quell-Portnummer** ist die Nummer des sendenden Ports.
- **Ziel-Portnummer** ist die Nummer des empfangenden Ports.
- **Länge** entspricht der Größe des UDP-Segmentes in Byte inklusive des UDP-Headers.
- **Prüfsumme** prüft das gesamte Segment auf der Grundlage des in IP verwendeten Algorithmus.

Die wichtigsten UDP-Portnummern und deren Protokolle sind:

Tabelle 7.2 UDP-Portnummern wichtiger Protokolle

Portnummer	Protokoll
53	DNS – Domain Name Service
69	TFTP – Trivial File Transfer Protokoll
161	SNMP – Simple Network Management Protokoll
520	RIP – Routing Information Protokoll



Noch Fragen ...? Ja ...

Was ist der Vorzug virtueller Verbindungen wie sie TCP unterstützt?

Durch dieses Prinzip können eine Vielzahl simultaner Verbindungen unterhalten werden und jeder Nutzer hat den Eindruck, den Zielrechner exklusiv zu nutzen.

■ 7.2 Zusammenfassung

TCP/IP ist die Kombination zweier einzelner Protokolle. Während IP auf der Schicht 3 arbeitet und einen verbindungslosen Dienst nach dem Best-Effort-Prinzip darstellt, richtet TCP seinen Dienst auf Schicht 4.

Die primäre Aufgabe von TCP besteht darin, den Datenfluss vom Sender zum Empfänger zuverlässig und korrekt sicherzustellen. Dazu gehören Mechanismen wie die Datenflusskontrolle oder das Sliding-Window-Prinzip ebenso wie die Felder Sequenznummer und Acknowledgement des Headers. Durch die Zuordnung der Portnummern zu Anwendungen lassen sich zusätzlich wertvolle Informationen für die Dienstgüte und die Lenkung von Verkehrsströmen gewinnen.

Zum grundsätzlichen Verständnis der Arbeitsweise von TCP/IP sind daher viele Einzelelemente wichtig. Dazu gehören: die Headerfelder und -funktionen, die Portnummern, das Verbindungsmanagement und die speziellen Mechanismen, die die Transportqualität sichern. Der Leser sollte daher über diese Einzelheiten fundierte Kenntnisse besitzen, um ein sachkundiges Urteil über Erweiterungen und Anpassungen an neue Aspekte wie Quality of Service oder Voice over IP fällen zu können.

■ 7.3 Wissensüberprüfung

1. Welche Größe besitzt der TCP-Header?
2. Was ist unter Datenflusskontrolle zu verstehen?
3. Durch welche Flags leitet TCP den Verbindungsaufbau ein?
4. Die Windowgröße betrage 1. Wann wird eine Bestätigung an den Sender übertragen?
5. Welche Protokolle nutzen UDP als Transportmechanismus?
6. Was ist der Zweck des 3-Wege-Handshake-Verfahrens von TCP?
7. Ist TCP ein verbindungsorientierter Dienst? Begründen Sie Ihre Ansicht.
8. Welche Informationen liefern Ports?
9. Welche Portangaben enthält der Header, falls der Sender eine http-Verbindung zum Ziel aufbaut?
10. Erkennt IP, dass als nächsthöheres Protokoll TCP verwendet wird?

8

IPv6

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Welche Adressierungstypen kennt IPv6?
- Welche Adressformate und welche Schreibweise kennzeichnen die neue IP-Variante?
- Welche konstruktiven Unterschiede bestehen zwischen den beiden IP-Varianten?
- Welche neuen Möglichkeiten bietet IPv6?

Kapiteleinführung

Das schnelle Wachstum des Internets verleiht der Umstellung von der bisherigen Version 4 des Internetprotokolls auf die nächste Generation IPv6 eine gewisse Dringlichkeit. Den treibenden Ausschlag gibt hierbei vor allem der Bedarf nach einem größeren Adressraum, der nicht nur den Ausbau bestehender Netze ermöglicht, sondern auch die Integration neuer mobiler Systeme gestattet und das Routing im Internet vereinfacht. Die Zuteilung von IPv4-Adressen hat sich in den vergangenen Jahren deutlich verlangsamt. Grund hierfür ist die Einführung von NAT (Network Address Translation) und die Verwendung privater Adressen. NAT und andere Erweiterungen von IPv4 besitzen allerdings entscheidende Nachteile. Sie erlauben z. B. keine direkte Adressierbarkeit der Endgeräte. Für einen PC, der nur zum Surfen und Lesen von E-Mails dient, ist dies keine Einschränkung. Wer aber selbst Informationen ins Internet stellen möchte, benötigt feste Adressen. Gleiches gilt, wenn Nachrichten direkt auf Geräte wie Laptops, Mobiltelefone oder Bordcomputer im Auto versendet werden sollen. Die noch verfügbaren Adressen, die vielfach in kleine Blöcke fragmentiert sind, reichen dazu nicht aus.

Neben dem Adressraum wurden einige weitere Verbesserungen in das Protokoll aufgenommen. Dazu zählt die automatische Rechnerkonfiguration, ein Merkmal, das die Installation und das Management von TCP/IP-Netzen erleichtert. Dieser Punkt dürfte in unternehmensweiten Netzen den größten Vorteil bringen, da gerade dort die Zuweisung und Pflege von IP-Adressen einen großen Kostenfaktor darstellt.

Die endgültig neue Version des Internet-Protokolls trägt den Namen „IPv6“, wird jedoch in der Internetwelt auch häufig als IPnextGeneration (IPnG) bezeichnet.

■ 8.1 Historie

Grund für das Entstehen einer neuen Protokollgeneration war die sich abzeichnende Adressmisere, insbesondere im Raum der Class-B-Adressen, die mittelfristig jedes Wachstum im Internet verhindert hätte. Bereits 1991 begann das IAB (Internet Activity Board) damit, den zukünftigen Größen- und Funktionsbedarf des Internets abzuschätzen. Die schnell wachsende Zahl vernetzter Rechner und die Ausdehnung auf neue Anwendungsfelder wie Fahrzeugsysteme und mobile Geräte ließ eine Erschöpfung der Internetressourcen in absehbarer Zukunft erwarten. Im Juli 1992 ernannte die IETF (Internet Engineering Task Force) einen Ausschuss, der die Spezifikation eines neuen Internetprotokolls entwerfen sollte. Das Ergebnis lag im Dezember 1993 als Request for Comments RFC 1550 vor. Der ausgewählte Vorschlag basiert auf einem Konzept von S. Deering, trug zunächst die Bezeichnung SIPP (Simple Internet Protocol Plus) und wurde im August 1994 öffentlich vorgestellt bzw. im Januar 1995 als RFC 1752 unter dem Titel „The Recommendation for the IP Next Generation Protocol“ veröffentlicht. Die neuen Funktionen des IPv6 – in den weiteren RFCs 1883 bis 1887 beschrieben – beseitigen einige Engpässe im Betrieb des alten IPv4-Protokolls an erster Stelle natürlich die Ausdehnung des Adressraumes, hervorgerufen durch die Erweiterung des Adressformates von 32 auf 128 Bits. Darüber hinaus wurden in IPv4 implementierte aber kaum benutzte Funktionen entfernt und eine Anpassung an zukünftige Multimedia-Anwendungen durch die Berücksichtigung einer Reihe von Merkmalen vorgenommen.

SIPP stand in Konkurrenz zu zwei weiteren Vorschlägen:

- **Common Architecture for the Internet (CATNIP):** Hierbei handelt es sich um die Weiterentwicklung eines älteren Protokolls, das sowohl IPv4, als auch Novell IPX und OSI Connectionless Networking Protocol (CLNP) verschmilzt. Es ist sehr stark an CLNP angelehnt, enthält alle für die drei zugrundeliegenden Protokolle wichtigen Informationen in komprimierter Form und verwendet einen Paketheader von 16 Bytes. Die spezifizierte Adresslänge ist allerdings variabel.
- **TCP and UDP with Bigger Addresses (TUBA):** Dieser Vorschlag basiert ebenfalls auf CLNP. Die Überführung von IPv4 in TUBA geschieht durch einen Dual-Stack-Ansatz. Zwei unabhängige Protokollstacks versuchen miteinander zu kommunizieren und verwenden dazu das Domain Name System für beide IP-Adressen, sowie den Network Service Access Point, um die Verbindung zu CLNP herzustellen.

Das IAB stimmte zwar keinem Vorschlag vorbehaltlos zu, wählte aber SIPP aus, weil es den verlangten Anforderungen am nächsten kam und entschied, passende Merkmale der anderen Konzepte zu integrieren.

■ 8.2 Entwurfsziele

- **Erweiterte Adressierungsfunktionen:** Um im globalen Internet erreichbar zu sein, muss ein Rechner eine eindeutige IP-Adresse besitzen. Zwar ist bei einer Länge von 32 Bit die Bildung von ca. 4,2 Milliarden Adressen möglich, da aber Adressklassen für Zuweisungs- und Routingzwecke notwendig sind, verringert sich diese theoretische

Obergrenze erheblich. Durch die Vergrößerung des Adressraumes können hierarchische Schemata unterstützt werden, so dass eine wesentlich größere Zahl von Rechnern pro Adressgruppe zulässig wird. Ohne einen hierarchischen Adressaufbau sind die zentralen Netzknoten gezwungen, sehr große Routingtabellen zu speichern. Durch eine Strukturierung der Einträge, können Router kurze Präfixe zur Suche nutzen, was den Weiterleitvorgang erheblich beschleunigt. Das Classless Inter Domain Routing (CIDR) in IPv4 ist ein Kunstgriff, um sich diesem Zustand zu nähern.



Der große Adressraum von IPv6 ermöglicht einerseits ein globales hierarchisches Adressierungsschema, um das Routing zu optimieren und die Routingableneinträge zu reduzieren, andererseits stellt es genügend Adressen für neue Dienste und Geräte bereit.

- **Vereinfachung des Headers:** In der Version 4 des IP-Protokolls wurden einige Felder nur selten genutzt. Um die notwendige Bandbreite zu optimieren, sind in der neuen Version unnötige Felder eliminiert worden.
- **Flexibilität bei Optionen:** Durch eine Auslagerung aus dem Header ist es möglich, jederzeit neue Optionen zu integrieren.
- **Dienstgüte:** Neue Steuerungsfelder im Header erlauben die Übermittlung gesonderter Qualitätsparameter zwischen Sender und Empfänger. Dies ist insbesondere im Hinblick auf Multimedia-Applikationen, die Anforderungen hinsichtlich Bandbreite, Ressourcenmanagement und Antwortzeit stellen, eine wesentliche Verbesserung.
- **Authentizität:** Die heutigen Kommunikationsstrukturen insbesondere unter dem Blickwinkel der Kommerzialisierung des Internet, erfordern umfangreiche Sicherheitsfunktionalität bis zur Verschlüsselung der zu übertragenden Daten.

Neben diesen auf der bestehenden Protokollversion basierenden Merkmalen integriert IPv6 einige echte Erweiterungen:

- Eine **Bandbreitenreservierung** in Form von Ressourcenallokation: Anstelle des IPv4-Feldes ToS erlaubt IPnG die Markierung von Paketen und ermöglicht auf diese Weise die Unterstützung von Multimedia-Datenflüssen.
- Zwei neue Mechanismen zur **Datensicherheit**. Auf Optionsebene existieren Header für Authentifikation und Verschlüsselung. Beide Pakettypen besitzen, um unbefugte Verkehrsanalysen zu erschweren, unabhängig von der tatsächlichen Länge immer ein festes Format.
- Ein **Multicasting**, dass die Broadcast-Adresse überflüssig macht. Soll ein Paket an alle Hosts eines Segmentes gesendet werden, wird eine spezielle Multicast-Adresse mit der Bedeutung „ALL Nodes“ verwendet. Ebenso ist auch das IGMP (Internet Group Management Protocol) ersetzt worden. Seine Funktion übernehmen ICMPv6-Messages als Multicast Listener Discovery (RFC 2710).
- Einen **Anycast-Dienst** als einen Kompromiss zwischen Uni- und Multicast. Er erlaubt es, zwei oder mehr Interfaces zu einer Anycast-Gruppe zu verbinden. Ein Paket mit

einer Anycast-Adresse wird nur einem, im allgemeinen dem nächstgelegenen Interface der Gruppe zugestellt. Im Gegensatz zu Multicast-Umgebungen, die Pakete für alle Gruppenmitglieder erzeugen, existiert hier nur ein einzelnes Paket. Dieses Konzept ermöglicht es Unternehmen, eine isolierte Anycast-Adresse zu nutzen, um ein Paket mehreren Routern des Providers zuzustellen. Besitzen die Router des Providers nur eine Anycast-Adresse, hat das Unternehmen mehrere Zugangspunkte zum Internet, so dass der Ausfall einer Komponente sofort durch eine andere der gleichen Gruppe kompensiert werden kann. Der Sender hat jedoch keine Möglichkeit das Empfangsinterface zu wählen. Das Ziel wird durch das Routingprotokoll bestimmt.

- Eine **Auto-Address-Konfiguration**, die eine dynamische Zuweisung von IPv6-Adressen erlaubt. Die durch eine manuelle Konfiguration der Rechner entstehenden Supportkosten können durch diesen Mechanismus erheblich reduziert werden. Im Extremfall zieht der Wechsel eines Providers keinen manuellen Eingriff nach sich, da die Stationen die neue IPv6-Adresse selbständig aus ihrer MAC-Adresse und einem Präfix bilden, den sie vom Nachbarrouter erfahren.
- Einen verbesserten **Options-Mechanismus** dergestalt, dass Paketoptionen gesondert zwischen dem IP-Header und dem nachfolgenden Transportheader platziert werden und auf diese Weise getrennt von einem Router ausgewertet werden können. Der Hintergrund für dieses Konzept liegt in der Beobachtung, dass die meisten Optionen nicht an die Router gerichtet sind und eine Auslagerung somit die Performance bei der Wegegwahl erhöht.

■ 8.3 Technische Betrachtung

Der IPv6-Header ist beträchtlich einfacher als sein Vorgänger, was seine Verarbeitungseffizienz durch Router stark erhöht. Während der IPv4-Header in der Länge variabel sein kann, sind die IPv6-Angaben im Standardfall auf 40 Bytes begrenzt. Diese Beschränkung erlaubt den Routern eine weit schnellere Prüfung der einzelnen Felder. Eine der ersten Angaben des IPv4-Headers, auf die durch das neue Design verzichtet werden kann, ist das Längenfeld des Headers. Das Feld für die Angabe zur Nutzlast kann wie bisher durch seine Länge von 16 Bit eine Paketgröße von 64 KB beschreiben. Im Gegensatz zur bisherigen Version sind aber „Jumbograms“ möglich, wenn das Feld einen Eintrag von Null aufweist und das Paket selbst einen speziellen Erweiterungsheader trägt. Das ursprüngliche Time-to-Live-Feld ist in Hop-Limit umbenannt, besitzt mit 8 Bit aber weiterhin die gleiche Größe. Da die Anzahl der Bits die Markierung von 255 Hops erlaubt, dürfte in absehbarer Zukunft selbst die Durchquerung großer Netzwerke kein Problem darstellen. Die weiteren Anpassungen betreffen drei Feldarten:

- Die Funktionalität des ToS-Feldes ist auf zwei neue Felder aufgeteilt: Flow Control und Priorität.
- Die zur Fragmentierung gehörenden Felder werden in einen speziellen Header verlagert.
- Auf die Prüfsumme wird verzichtet, da diese Funktion von den vor- und nachgelagerten Protokollen bereits zuverlässig ausgeführt wird.

■ 8.4 Die wichtigsten Merkmale

8.4.1 IPv6-Header

Der Vergleich beider Protokollgenerationen zeigt weiterhin, dass die aufwendige Berechnung der Prüfsumme in jedem Hop wegfällt, was für den weitaus größten Teil der Anwendungen einen Performancevorteil verspricht. Das Feld „Protocol“ heißt nun „Next Header“. Umbenannt wurde auch das „Length“-Feld in „Payload-Length“. Es umfasst nicht mehr das gesamte IPv6-Paket, sondern nur das Paket nach dem Header. Trotz der Tatsache, dass die Adressen in IPv6 viermal so lang sind wie in IPv4, ist der IPv6-Header mit 320 Bits oder 40 Bytes nur doppelt so lang wie der herkömmliche IPv4-Header. Zudem wurde die kleinste Übertragungseinheit von 384 Bits = 48 Bytes auf 4 068 Bits = 576 Bytes angehoben. Von allen IPv6-Knoten wird zudem erwartet, dass sie die maximale Paketgröße (MTU = Maximum Transfer Unit) dynamisch aushandeln (beschrieben in RFC 1191 – Path MTU Discovery) und der Quellrechner nur Pakete sendet, die diesen Wert nicht übersteigen. Als Folge dieses Vorgehens müssen IPv6-Router auf dem Weg vom Sender zum Empfänger keine Pakete fragmentieren, da die Paketgröße von allen Knoten als verarbeitbar akzeptiert wird.

Version	Headerlänge	Dienstgüte	Paketlänge in Byte	
Identifikation			Flags	Fragment Offset
0	4Time to Live 8	Protokoll 16	Headerprüfsumme 31	
Quell-IP-Adresse				
Ziel-IP-Adresse				
Optionen				Padding
Nutzdaten				

Bild 8.1 IP-Headerveränderungen

Das Design des neuen Headers und seine Ausrichtung auf 64 Bit sind für eine schnelle Verarbeitung konzipiert.

0	4	12	16	24	31
Version	Klasse	Flow Label			
Nutzlastlänge		Nächster Header	Hop Limit		
128 Bit Quelladresse					
128 Bit Zieladresse					

Bild 8.2 IPv6-Header

- Feldname in IPv4 und IPv6 gleich
- Name und Position wechseln in IPv6
- Neue Felder in IPv6
- Entfernte Felder

Die Bedeutung der Felder im Einzelnen:

- **Version:** Die Versionskennung trägt die Nummer 6.
- **Flow-Label:** Dieses Merkmal erlaubt IP-Stationen die spezielle Kennzeichnung von Paketen und die Realisation von zusammenhängenden Datenflüssen, wie sie bei Sprach- oder Videoanwendungen unter Einbeziehung des Resource Reservation Protocols (RSVP) notwendig sind. Router leiten eine gesonderte Verarbeitung, beispielsweise die Priorisierung von Stationen, ein, können aber auch als Filter fungieren. Das Feld ist 28 Bit lang und in zwei Subfelder unterteilt: TCLASS oder Priorität und FlowID, von denen die Priorität 4 Bit umfasst, um lastgesteuertem Datenverkehr Vorrang zu gewähren:

Tabelle 8.1 TCLASS/Priorität: Bedeutungen

TCLASS/Priorität	Bedeutung
0	nicht charakterisierter Verkehr
1	„Füllverkehr“ - netnews
2	unerwarteter Datentransfer- E-Mail
3	reserviert
4	erwarteter bulk-Verkehr - FTP, NFS
5	reserviert
6	interaktiver Datenverkehr - Telnet
7	Internetkontrollinformation - Routing, SNMP

Für den Real-Time-Datenverkehr stehen die Klassen 8 -15 zur Verfügung. Der Wert 8 gilt dabei für die von einem Router bei Überlast verworfenen Pakete, der Wert 15 für zeitkritische Audio-/Videodaten. Tondaten dürften z.B. bei einer Videowiedergabe die höchste Priorität 15 genießen, während Bilddaten mit hoher Auflösung nur dann übertragen werden, wenn die Bandbreite vorhanden ist.

Die 24-Bit lange Flow-ID ermöglicht die Definition von Ressourcen wie z. B. Bandbreite für einzelne Datenströme. Der Sender signalisiert mittels einer Flow-ID, bestehend aus der Source-Adresse und dem Flow-Wert, dem Router, welche Pakete einer individuell ausgehandelten Vereinbarung unterliegen. Die dafür notwendigen Informationen werden mit Hilfe eines gesonderten Protokolls z.B. dem Resource Reservation Protocol (RSVP) oder dem Hop-by-Hop-Header zwischen Sender und Router ausgehandelt. Da dies ein Feld fester Länge im Haupthead von IPv6 ist, ermöglicht seine Lage und Größe eine effiziente Handhabung durch Router.

- **Nutzdatenlänge:** Dieses Feld legt die Länge der auf den Header folgenden Nutzdaten als Zahl in Bytes fest. Übersteigt die Länge 64 KB ist dieses Feld 0 und ein optionaler Header enthält die aktuelle Angabe.
- **Next Header:** Diese Angabe definiert das in der Hierarchie des ISO-/OSI-Referenzmodells nachfolgende höhere Protokoll oder wählt einen zulässigen Erweiterungsheader als Option aus. Für die einzelnen Extension-Header sind die zulässigen Werte in RFC 2460 definiert:

Tabelle 8.2 Werte des Next-Header-Feldes

Wert	Protokoll
0	Hop-by-Hop Options Header
1	ICMP
6	TCP
8	EGP (Exterior Gateway Protocol)
17	UDP
43	Routing Header
44	Fragment Header
51	Authentication Header (RFC 1826) und ESP Header (RFC 1827)
60	Destination Options Header
89	OSPF (Open Short Path First)
135	Mobility Header

Diese Architektur ist für die Entwicklung des Internets wesentlich, erlaubt sie doch, in Zukunft weitere Header für neue Anforderungen zu definieren, ohne das Konzept und die grundsätzliche Struktur verändern zu müssen.

- **HOP Limit:** Die Zahl der Router, die auf dem Weg zum Ziel passiert werden dürfen, ist begrenzt. Jeder Router entlang dieser Strecke dekrementiert den Wert und verwirft das Paket sobald der Wert Null erreicht wird. Dieses Feld ersetzt das in der alten Version enthaltene TTL-Feld.
- **Source-Adresse:** 128 Bit lange Adresse des Senders.
- **Destination-Adresse:** 128 Bit lange Adresse des Empfängers.

8.4.2 IPv6-Headererweiterungen

IPv6 erlaubt die optionale Festlegung von speziellen Funktionen in separaten Headern, die direkt an den originären Header angehängt werden. Die Existenz eines optionalen Headers wird durch das Next-Header-Feld signalisiert und in Form einer Verkettungstechnik gehandhabt. Das Next-Header-Feld wählt aus der Reihe der möglichen optionalen Header einen bestimmten Header aus, der dem Hauptkopf folgen darf. Die Verkettung weiterer

Optionen kommt durch einen Eintrag in das Next-Header-Feld dieser Option zustande. In der Spezifikation wird eine bestimmte Reihenfolge der Header festgelegt, obgleich die Empfänger von IPv6-Paketen diese nicht verifizieren. Damit kann ein IPv6-Paket aus:

- einem reinen IPv6-Header ohne Erweiterungen bestehen
- einem IPv6-Header mit einer oder mehrerer Extensions zusammengesetzt sein.

Die in IPv4 üblichen Optionsheader werden in IPv6 durch flexible Erweiterungsheader ersetzt, die sich zwischen dem primären IPv6-Header und dem Transportheader des nachfolgenden Protokolls befinden. Ihr Einsatz ist an einen bestimmten Verwendungszweck gekoppelt.



Bild 8.3 Verkettung der IPv6-Erweiterungsheader

Zur Zeit sind sechs optionale Header definiert, die in einer bestimmten Reihenfolge auftreten und typischerweise nur einmal pro Paket vorkommen. Eine Ausnahme bildet lediglich der Destination-Header, der häufiger vertreten sein darf:

Tabelle 8.3 IPv6 Erweiterungsheader

IPv6 Header	<i>40 Byte</i>
Hop-by-Hop Options Header	<i>variabel</i>
Source Routing Header	<i>variabel</i>
Fragment Header	<i>8 Byte</i>
Authentication Header	<i>variabel</i>
Encapsulation Header	<i>variabel</i>
Destination Options Header	<i>variabel</i>
TCP Header	<i>20 Byte</i>

- **Hop-by-Hop Options Header:** In diesem ersten Erweiterungsheader werden Informationen abgelegt, die von jedem Router entlang des Übertragungsweges geprüft werden müssen. Da dieser Header allen Knoten der Übertragungsstrecke bekannt ist, bietet es sich an, hierin Managementinformationen oder Debugging-Befehle zu transportieren. Ein Beispiel können die Ressource Reservation-Nachrichten des RSVP-Protokolls sein.
- **Destination Options Header:** Für diesen Header existieren zwei Ausprägungen, abhängig von der Position im Paket. Die erste Form überträgt Information an das als erstes im IPv6 Adressfeld genannte Ziel. Die zweite Möglichkeit besteht darin, dem Endpunkt der Übertragung Informationen zu übermitteln. Aus Effizienzgründen befindet sich die erste Headerform direkt hinter dem IPv6-Header, die letzte aber am Ende der Headerkette.
- **Source Routing Header:** Dieser Header erlaubt dem Sender, eine Liste von IP-Adressen festzulegen, die auf dem Weg zum Ziel passiert werden müssen. Der Routing-Header wird durch eine 43 im Next-Header-Wert angezeigt. Die RFC 1883 definiert einen Routing-Headertypen Null, der dem Sender einen Großteil der Kontrolle über den Weg des Paketes einräumt. Dazu enthält der Erweiterungsheader ein 24-Bit-Feld, das anzeigt, wie ein Knoten das Paket zu verarbeiten hat. Jedes Bit wird als Prüfvorschrift für einen Knoten interpretiert, wobei Eins dafür steht, dass die nächste Station ein direkter Nachbar sein muss und Null die Nachbarschaftsbeziehung offen lässt. Wird dieser Headertyp für ein „Strict Forwarding“ genutzt, passiert das Paket nur dort angegebene Knoten. Im „Loose Forwarding“-Fall können auch nicht verzeichnete Router angelaufen werden. Die Folge dieser Angabe ist, dass z.B. zwei Router B und C, die nicht benachbart sind aber einen „Strict Forwarding“-Eintrag besitzen, nicht miteinander kommunizieren können. Router B verwirft die Pakete. Dieses Merkmal ist besonders unter dem Sicherheitsaspekt sinnvoll, wenn Pakete einen vorgegebenen Leitweg einhalten sollen.

Routing Type	Header Extension Length	Routing Type	Segments Left
spezifische Daten			



Die bekannten Wege eines Rechners im Netz in Form der Routingtabelle lassen sich unter Windows mit dem Befehl `route -6 print` ausgeben.

- **Fragment Header:** IPv4 verfügt über die Möglichkeit, Pakete an jedem Punkt des Netzweges in kleinere Transporteinheiten in Abhängigkeit von den zulässigen Paketobergrenzen des Übertragungsprotokolls aufzuteilen. Dieses Merkmal wurde in IPv6 zugunsten einer Ende-zu-Ende-Fragmentierung aufgegeben. Eine Paketzerlegung findet daher nur noch im Anfangs- und Endknoten statt, auf dem Übertragungsweg selbst ist jede Anpassung der Paketgröße unzulässig. Um zu erkennen, welche Pakete logisch zusammengehören, besitzt der Header ein Identifikationsfeld und Sequenznummern. Diese Aufteilung entspricht derjenigen von TCP. Da eine automatische Größenanpassung auf dem Paketweg unmöglich ist, trägt der Sender nun die Verantwortung, ein Paket zu erzeugen, das den Anforderungen der Ende-zu-Ende-Verbindung entspricht.

Besteht das Netzwerk z. B. in der Verbindung zweier Netze mit einer Paketgröße von 4500 Bytes über ein Ethernet-Segment mit 1500 Bytes, muss der Sender in der Lage sein, dies zu erkennen und die MTU (Maximum Transfer Unit) auf 1500 Bytes begrenzen. Um die kleinste Paketgröße auf dem Weg zum Ziel zu ermitteln, bedient sich der Sender des MTU-Path-Discovery-Prozesses. Dazu sendet die Quelle zunächst ein Paket mit der größten zulässigen MTU seines Interfaces. Übersteigt diese Angabe den Schwellwert eines Verbindungsteils, antwortet der entsprechende Knoten mit einer ICMP-Nachricht. Der Sender reduziert daraufhin die Paketgröße auf den erhaltenen Wert und startet einen erneuten Versuch. Erst wenn ihn keine ICMP-Nachricht mehr erreicht, kann er die Übertragung beginnen.

Next Header	reserviert	Fragment Offset	reserviert	M-Flag
Identifikation				

Dabei gibt der Fragment Offset die Lage der Daten relativ zum Anfang des Datenfeldes des Ursprungspaketes als Vielfaches von 8 Byte an. Das M-Flag kennzeichnet durch einen Wert von 1, dass weitere Fragmente folgen, durch einen Wert von 0, dass das letzte Fragment empfangen wurde. Die Identifikation wird für das erste fragmentierte Paket des Originals als 32 Bit-Zähler festgelegt und dient in den nachfolgenden Fragmenten zur eindeutigen Zuordnung der Pakete zum Original.

- **Authentication Header:** Dieser Header gibt Netzanwendungen die Gewissheit, dass das Paket von der vorgegebenen Quelle stammt. Mit der Verwendung dieses Headers erhalten die Stationen eine Möglichkeit, sichere Verbindungen aufzubauen.
- **Encapsulation Header:** IPv6 ermöglicht die Verschlüsselung des Transport-Headers des nachfolgenden Protokolls gemeinsam mit der Nutzlast oder die separate Verschlüsselung des vollständigen IP-Headers. Beide Verfahren setzen die Existenz dieses Headers voraus, da er Informationen zum Verschlüsselungsprozess beinhaltet. Wird die erste Variante gewählt, wird der Erweiterungsheader direkt zwischen die bisherigen Erweiterungsheader des IPv6-Paketes und vor die Nutzlast- bzw. den Transportheader platziert. In diesem Fall werden daher der Ursprungs- und die Erweiterungsheader nicht verschlüsselt (Transport-Modus). Wird die Verschlüsselung des gesamten IP-Paketes angestrebt, ist es notwendig, sowohl einen neuen IP- als auch einen angepassten Erweiterungsheader zu erzeugen und diese vor das Ausgangs-IP-Paket zu setzen (Tunnel-Modus). Der Paketinhalt ist dann nur noch für die Endpunkte der Kommunikation sichtbar. Diese Variante dürfte unter Sicherheitsgesichtspunkten besser sein, weil der verschlüsselte Header bei einer unzulässigen Verkehrsanalyse keine Rückschlüsse auf Sender und Empfänger zulässt. Sie hat allerdings den Nachteil, dass Verarbeitungsoverhead entsteht und die Geschwindigkeit deutlich sinkt. Authentication- und Encapsulation-Header können in unterschiedlichen Kombinationen genutzt werden. In einigen Anwendungen kann ein Authentication-Header innerhalb eines voll- oder teilweise verschlüsselten Paketes übertragen werden, um ein zusätzliches Niveau an Datenintegrität zu garantieren, in anderen Szenarien kann der Authentication-Header vor den Verschlüsselungsteil platziert sein. Dieser Ansatz ist vorzuziehen, wenn der Authentication-Prozess vor der Entschlüsselung stattfindet.

8.4.3 IPv6-Adressformat

Der Vergleich des neuen mit dem alten IP-Header zeigt ein schlankeres Design. Obwohl Source- und Destinationadresse viermal so lang geworden sind und damit den Adressbestand auf 3.4×10^{38} pro Person der momentanen Weltbevölkerung ausdehnen, ist der neue Header mit fixen 40 Byte nur doppelt so groß wie der alte. Dies entspricht ca. 6.6×10^{23} Adressen pro Quadratmeter Erdoberfläche. Die Vergabepaxis der alten IP-Adressen führte anfänglich dazu, dass große Institutionen wie das MIT oder AT&T eine Class-A-Adresse erhielten. Damit verfügen sie über einen Adressbestand von nahezu 16 Millionen Adressen, weit mehr als die gesamte Volksrepublik China, die es auf gerade mal 9 Millionen Adressen bringt. Dies verdeutlicht das Problem der Adressverteilung und unterstreicht, warum die allgemeine Akzeptanz von IPv6 im asiatischen Raum besonders hoch ist.

Für die Wahl eines großen Adressraumes sprechen mehrere Gründe: Erstens steht damit ausreichend Platz für eine tiefe hierarchische Gliederung zur Verfügung, die für eine logische Netzstruktur genutzt werden kann, um das Routing zu vereinfachen, zweitens ermöglicht ein großes Adresspotential die Implementierung automatischer Konfigurationsprozeduren und letztlich bildet eine großzügige Adressstruktur ein Reservoir für die Zukunft. Pessimisten befürchten allerdings, dass selbst eine 16 Byte-Adresse nicht ausreichen könnte, wenn beispielsweise Energieversorger ihre Messgeräte für Strom und Heizung zur automatischen Erfassung mit einer IP-Adresse versehen.

IPv4 ist als klassenbasiertes Adressschema entworfen worden, das seine Adressen zwischen Netzwerk und Stationen aufteilt, aber keine Rücksicht auf eine hierarchische Anordnung nimmt, bei der eine einzelne Adresse mehrere nachgeordnete Rechner repräsentieren kann.

Während bei der Version 4 die byteweise Interpretation der Adressen üblich war, wird dieses Schema durch die wortweise Schreibweise abgelöst, bei der der Doppelpunkt die Funktion des einfachen Punktes als Trennzeichen übernimmt. Zusätzlich werden die Adressen statt wie bisher dezimal nun hexadezimal ausgedrückt.



Beispiel

IPv4: 128.127.240.32

IPv6: FEDD:BC32:0000:0000:0000:0050:0743:DF36

IPv6: **2001:0638:0713::/48**

IPv6-Adresse der FH Flensburg

Die IPv4-Adressen besitzen ein festes Format. Demgegenüber können die neuen IPv6-Adressen abgekürzt werden. Da die längeren Adressen voraussichtlich viele Nullen beinhalten werden, schlägt die Spezifikation eine Kurzschreibweise vor:

- vorangestellte Nullen können ausgelassen werden.
- eine Hexadezimalzahlenfolge, die ausschließlich mit dem Wert 0 belegt ist, kann durch zwei Doppelpunkte ersetzt werden. Die Schreibweise mit den Doppelpunkten darf

jedoch nur einmal innerhalb der Adresse verwendet werden, da sonst Mehrdeutigkeiten nicht auszuschließen wären.



Beispiel

FEDD:BC32:0000:0000:0000:0050:0743:DF36

oder in Kurzschreibweise

FEDD:BC32::50:743:DF36

0000:0000:0000:0000:0000:0000:128:127:240:32

oder in Kurzschreibweise

::128:127:240:32

Eine unspezifizierte Adresse wird als :: geschrieben, weil sie ausschließlich Nullen enthält.

Wie bei IPv4 ist der IPv6-Adressvorrat in Gruppen spezifischer Funktionalität unterteilt.

- **Globale Unicastadressen** bestehen aus einem 48-Bit globalen Routingpräfix und einer 16-Bit Subnetz-ID. Unternehmen oder Organisationen, denen eine derartige Adresse zugewiesen wird, können die Subnetz-ID dazu verwenden, ihr eigenes lokales hierarchisches Adressierungsschema aufzubauen. Die Länge von 16 Bit erlaubt die Bildung von 65 535 Subnetzen. Der Routingpräfix wird ebenfalls zur Hierarchisierung verwendet mit den drei Stufen: Registrierungsbehörde, Internet Service Provider und Teilnehmer.

Die gegenwärtige freigegebenen Adressen, die durch die IANA verwaltet werden, beginnen mit dem binären Block 001 bzw. 2000::/3 in hexadezimaler Form. Damit ist lediglich ein Achtel des gesamten verfügbaren Raums freigegeben. Die IANA vergibt dabei den Bereich 2001::/16 an die fünf Unterorganisationen: ARIN, RIPE (Europa), APNIC (Asien, Pazifik), LACNIC (Lateinamerika), AfriNIC (Afrika). Genaue Informationen sind unter dem Link: <http://www.iana.org/assignments/ipv6-tla-assignments> einsehbar.



Die Begriffe TLA (Top-Level Aggregator), NLA (Next-Level Aggregator) und SLA (Subnet Local Aggregator) besitzen keine Bedeutung mehr. Sie wurden durch die neue Einteilung in Routingpräfix und Subnetz-ID gemäß RFC 3587 ersetzt.



Beispiel

Die Telekom besitzt den Präfix 2003:0::/19. Damit sind die ersten 19 Bit jeder IPv6-Adresse der Telekom gleich: 2003:0. Aus diesem Bereich wird die Telekom als Internet Provider in Zukunft den DSL-Kunden bei der Einwahl einen /56-Präfix zuweisen. Diese 56 Bit liegen für den Endkunden fest. Die folgenden 8 Bit sind dann jeweils zur eigenen Bildung von Substrukturen gedacht. Erst dann folgt der Interface Identifier mit einer Länge von 64 Bit.

- **Reservierte Adressen** sind vergleichbar denen in IPv4 und gegenwärtigen bzw. zukünftigen Forschungszwecken vorbehalten. Sie umfassen 1/256 des gesamten Adressraumes.
- **Private Adressen** erfüllen den gleichen Zweck wie unter IPv4. Sie werden nicht geroutet, beginnen mit FE in hexadezimaler Form, an die sich eine Ziffer zwischen 8 und F anschließt. Gemäß ihrer Reichweite werden sie in zwei Gruppen eingeteilt:
 - **Site-local addresses** entsprechen den Vereinbarungen in RFC 1918 bezüglich IPv4. Sie beziehen sich auf ein Unternehmen oder eine Organisation als ganzes. Ihre Definition erfolgt in RFC 3879. Nach den ersten beiden einleitenden Zeichen FE folgen Zeichen zwischen C und F, so dass die Adressen FEC, FED, FEE oder FEF lauten.
 - **Link-local addresses** bilden ein neues Konzept in IPv6. Ihr Gültigkeitsbereich bezieht sich auf ein physikalisches Segment. Außerhalb ihres Verwendungszweckes für die automatische Adresskonfiguration oder die Erkennung der Nachbarn werden sie nicht weitergeleitet, d.h. jedes Netzinterface benötigt für die automatische Adresskonfiguration und die Verwendung des Neighbor Discovery Protocols diese Adresse. Auch dieser Adresstyp beginnt mit FE, gefolgt von einem Zeichen zwischen 8 und B, so dass gültige Adressen mit FE8, FE9, FEA oder FEB starten.
- **Multicast-Adressen:** Im Unterschied zu IPv4 verzichtet IPv6 auf Broadcasts und verwendet an deren Stelle Multicasts als Aufruf für eine bestimmte Gruppe von Geräten. Der Präfix besteht aus der Folge FF und deckt den Bereich FF00-FFFF ab. Je nach Wert des 3. oder 4. Zeichens liegt die Reichweite der Multicasts zwischen site-local, link-local oder global. Diese Differenzierung erlaubt es, den Wirkungsbereich der Multicasts genau zu spezifizieren.
- **Loopback Adressen** senden Daten für Testzwecke an die sendende Adresse zurück. IPv6 kennt lediglich eine Loopback Adresse und reserviert keinen ganzen Block. Die Adresse lautet 0:0:0:0:0:0:1 oder abgekürzt ::1.
- **Unspezifizierte Adressen** bestehen aus einer Folge von Nullen. Diese spezielle Adresse wird als Quelladresse von Stationen genutzt, die ihre IP-Adresse suchen. Ihre abgekürzte Schreibweise ist ::.



Damit besitzt ein Rechner bei seiner Konfiguration drei IPv6-Adressen: Loopback, link-local- und Uni- bzw. Anycast-Adresse

Windows-Betriebssysteme erzeugen den zweiten Teil der link-lokalen Adresse – den Interface Identifier – automatisch durch eine Zufallszahl. Besitzt ein Rechner mehr als eine IPv6-Netzwerkkarte wird an das Ende der link-lokalen Adresse ein Prozentzeichen und eine Zahl angehängt.

Tabelle 8.4 IPv6 Adresstypen

Adresstyp	erstes Byte binär	hexadezimale Darstellung
globale Unicast	0010 0000 0000 0001	2001::/16
link-local Unicast	1111 1110 1100	FEC::/10
site-local Unicast	1111 1110 1000	FE8::/10
Multicast	1111 1111 0000 0000	FF00::/16

8.4.4 Adressmanagement

Als weitere Neuerung kann IPv6 die Konfiguration von IP-Adressen in Netzen automatisch/dynamisch oder manuell/statisch ausführen. Unter automatisch ist zu verstehen, dass ein Rechner die Informationen ohne manuellen Eingriff ermitteln kann, manuell bedeutet eine Konfiguration über Befehle. Beide Arten unterscheiden wiederum zwei Unterarten der Adresszuweisung:

Die statische Variante kennt:

- die **manuelle Interface-ID**, die eine direkte Zuweisung der Werte zum Routingpräfix und zur Interface-ID über Betriebssystembefehle vornimmt.
- die **EUI-64 Interface-ID**, die den Routingpräfix zuweist, für die Interface-ID aber die MAC-Adresse nutzt. Die Erweiterung der 48 Bit Layer-2-Adresse auf die 64 Bit der Interface-ID geschieht dabei in der Form, dass die MAC-Adresse nach 24 Bit aufgetrennt, durch die Folge FF:FE ergänzt und das 7. Bit des 1. Bytes „gekippt“ wird.

Dynamische Formen der Adresszuweisung sind:

- stateless Autoconfiguration
- DHCPv6

Die komfortabelste Form ist der Autokonfigurationsvorgang über das Neighbor Discovery Protocol (ND). Dieser Vorgang wird als **stateless Autoconfiguration** bezeichnet. ND besteht aus einer Menge ergänzender ICMP-Nachrichten, die es IPv6-Knoten erlauben, Layer-2-Adressen zu entdecken und Netzwerkparameter und Erreichbarkeitsinformationen zu verteilen. Im weitesten Sinne stellt das neue Protokoll einen Ersatz für ARP und ICMP dar.



In IPv6 gibt es das ARP-Protokoll nicht mehr: Seine Funktion wird vom ICMPv6 Neighbor Discovery (RFC 2461) übernommen.

In einem typischen Szenario wird der Autokonfigurationsprozess durch eine Endstation ausgelöst, die eine Link Local Adresse temporär nutzt. Sobald diese Adresse als Kombination aus einem generischen lokalen Präfix und der MAC-Adresse gebildet ist, sendet die Station ND-Nachrichten, um sicherzustellen, dass die neue Adresse eindeutig ist. Antwortet keine Station mit einer ICMP-Nachricht, ist das Ziel erreicht, ansonsten muss eine neue

Adresse gebildet werden. Die neue Link Local Adresse wird zukünftig als Quelladresse verwendet. Im Ablauf wird mit ihr im nächsten Schritt unter Ausnutzung des Multicast-Mechanismus ein Solicitation Request an ND-Router verschickt. Anders als im ARP-Broadcast-Fall verarbeiten nicht alle Knoten diese Nachricht. Router antworten auf die Multicast-Message mit einem Unicast-Router Advertisement, das Prefix-Informationen der angeschlossenen Netze enthält. Diese Informationen werden allerdings auch ohne vorherigen Erhalt einer Solicitation Nachricht in regelmäßigen Abständen gesendet. Die Auswertung der Rückantwort ermöglicht dem Router festzustellen, ob Stationen die Stateless oder Stateful Autokonfigurationsmethode verwenden.

Die zweite Variante der Stateful-Fall nutzt die dynamische Zuweisung in Form des **DHCPv6-Protokolls**. Hier wird analog zu IPv4 aus einem Adresspool einer Station für eine bestimmte Zeitspanne eine Adresse zugeteilt. Aufgrund der Wiederverwendbarkeit ergibt sich eine effiziente Nutzung des Adressbestandes.



Im Gegensatz zu IPv4, dass nur eine Adresse pro Netzkarte zulässt, akzeptiert IPv6 mehrere Adressen unterschiedlicher Art (unicast, anycast, multicast) pro Netzwerkkarte. Jedes IPv6-Interface muss jedoch mindestens eine Loopback- und eine link-local-Adresse besitzen.

Um den zunehmenden Anforderungen aus dem Bereich des Mobile Computings gerecht zu werden, existieren bereits **Erweiterungsvorschläge**, IPv6-Stationen trotz räumlicher Bewegung mit einer festen IP-Adresse auszustatten. Dazu muss lediglich der lokale Router angewiesen werden, jeglichen Verkehr zur betreffenden Station temporär an eine Zwischenadresse zu lenken. Die Zwischenadresse wird automatisch aus der MAC-Adresse der mobilen Station und dem Prefix des Transitnetzes gebildet. Dieses Konzept reduziert auch die Probleme der Namensauflösung, wenn lokale Rechner nicht an ihrem festen Platz vorgefunden werden.



Beispiel

Im Flughafen ist ein Nutzer mit dem öffentlichen WLAN verbunden. Verlässt er das Gebäude, möchte er in ein anderes Netz wechseln und über GPRS oder UMTS mit dem Netz verbunden bleiben, ohne die Verbindung neu aufbauen zu müssen.

Netzwerkhersteller haben mit Automobilproduzenten bereits den Prototypen eines vernetzten Autos hergestellt, das einen Router mit Mobile IPv6 verbindet und die Internetnutzung während der Fahrt gestattet.

8.4.5 Begleitprotokolle

Mit ICMPv6 können Hosts und Router Fehler melden und einfache Nachrichten versenden. ICMPv6 gibt den Rahmen für zwei neue Protokolle vor:

- **MLD:** hierbei handelt es sich um drei ICMPv6-Nachrichten, die IGMP Version 2 (Inter-

net Group Management Protokoll) des IPv4 ersetzen. Verwaltet wird die Multicastmitgliedschaft in Subnetzen

- **ND:** stellt eine Folge von fünf ICMPv6-Nachrichten bereit, die die Kommunikation der Knoten untereinander verwaltet. ND ersetzt ARP, die ICMPv4-Routersuche und das ICMPv4-Redirect. Darüber hinaus stellt es weitere Funktionen bereit.

ICMPv6-Nachrichten werden in der Regel automatisch gesendet, wenn ein IPv6-Paket das gewünschte Ziel nicht erreicht. ICMPv6-Nachrichten werden in IPv6-Pakete als Nutzlast gekapselt.

Die verschiedenen Arten von ICMPv6-Nachrichten werden im ICMPv6-Header gekennzeichnet. Eine Nachricht besteht aus folgenden Feldern:

- Type – identifiziert die Nachricht oder Aktion
- Code – ist ein type-spezifischer Subidentifizier, z. B. Destination Unreachable, Paket too big
- Checksum – über die gesamte ICMPv6-Nachricht berechnet
- Next Headervalue – beträgt 58

Das Neighbor-Discovery-Protokoll ND ersetzt ARP, die ICMP-Routersuche (Selection, Typ=10) und die ICMP-Umleitung (Redirect, Typ=5). Es wird in RFC 2461 beschrieben und umfasst fünf Nachrichten:

Router solicitation (ICMPv6 type 133)

Router advertisement (ICMPv6 type 134)

Neighbor solicitation (ICMPv6 type 135)

Neighbor advertisement (ICMPv6 type 136)

Redirect (ICMPv6 type 137)

MLD wird zum Austausch von Statusinformationen zwischen IPv6-Routern und Mitgliedern der Multicastgruppe verwendet. Der Status der Mitgliedschaft wird periodisch von den Multicastroutern abgefragt. MLD ist in RFC 2710 definiert. MLD kennt drei Nachrichtentypen:

- **MLD-Abfrage:** ein Multicastrouter erfragt Gruppenmitgliedschaften in einem Netzabschnitt
- **MLD-Bericht:** eine Nachricht, die von einem Host bei einem Gruppenbeitritt oder als Antwort auf eine MLD-Abfrage gesendet wird
- **MLD-Beendigung:** eine Nachricht, die der Host beim Verlassen der Gruppe sendet, wenn er das letzte Mitglied des Netzsegmentes ist

■ 8.5 Migrationswege

Einen zentralen Diskussionspunkt um die Nachfolge des alten IP-Protokolls bilden die Konzepte für einen Übergang. Dabei sollen ein reibungsloser Wechsel und ein problemloses Zusammenarbeiten bei einem evolutionären Übergang von Hosts und Routern auf IPv6 ebenso möglich sein wie der Big-Bang, d. h. der Wechsel in einem Schritt. Um möglichst flexible Migrationspfade beschreiten zu können, beschreibt der RFC 1933 „Transition Mechanisms for IPv6-Hosts and Routers“ die technischen Randbedingungen der Migration:

- IPv6-Encapsulation over IPv4, d. h. IPv6-Datagramme werden durch die IPv4-Topologie gekapselt. Diese Technik wird auch als Tunneling bezeichnet.
- eine Dual-IP-Layer-Strategie für Rechner und Router, die zwischen beiden Protokollversionen vermitteln muss.

Der allgemeine Ratschlag lautet: „Verwendung des Dual-Stacks wo möglich, Tunneling nur wo keine andere Möglichkeit existiert“.

8.5.1 Tunneling

Diese Technik kapselt IPv6-Verkehr in IPv4-Pakete und überträgt sie über ein IPv4-Kernnetz. Damit wird lediglich IPv6-Funktionalität an den Rändern des Netzes verlangt, erfordert aber zum Verpacken des IPv6-Datagramms in einen IPv4-Header mehrere Funktionen:

- Bei Bedarf muss das Paket fragmentiert werden können.
- Beim Auspacken eines IPv6-Paketes aus einem IPv4-Frame wird der IPv6-Header nicht modifiziert. Leitet der Rechner das entpackte IPv6-Paket weiter, so ist das HOP-Limit zu dekrementieren.
- Die sendende Station oder der Router ist derart konfiguriert, dass der Weg sowohl einen nächsten Knoten kennt als auch das Tunnelende, das immer eine IPv4-kompatible Adresse sein muss, weil der Knoten aus beiden Teilnetzen erreicht werden kann.

Um die administrativen Begleiterscheinungen zu mildern, existieren zwei Typen des Tunneling-Verfahrens: automatisch/dynamisches 6to4 tunneling und konfiguriert/manuelles IPv6-over-IPv4 tunneling.

- Um konfigurierte Tunnel einzurichten, muss an den Endpunkten jeweils eine IPv6-zu-IPv4-Abbildung vorgenommen werden. Jenseits der Einstiegspunkte zum Tunnel werden die Pakete mit IPv4-Adressen transportiert.
- Die automatische Tunnelvariante nutzt IPv4-kompatible Adressen zur Übertragung auf IPv4-Verbindungen zwischen IPv6-Inseln. Dabei wird an den Tunnelendpunkten jeweils der IPv4-Header entfernt und durch einen IPv6-Header mit einer entsprechenden Adresse ersetzt. Dieses Konzept läuft zwar automatisch ohne manuellen Eingriff, besitzt aber den Nachteil, dass der Nutzen des größeren Adressraumes nicht zum Tragen kommt.

- Neben den beiden Standardverfahren gibt es eine Methode, die einem isolierten Dual-Stack-Host die Kommunikation mit einem anderen IPv6-Host ermöglicht. Dieses Konzept ist als Teredo-Tunneling bekannt.

8.5.2 Dual-IP-Stack

Damit ein IPv6-Knoten mit der restlichen Netzinfrastruktur kommunizieren kann, besitzt er zusätzlich den kompletten IPv4-Protokollstack. Dieses Konzept ist sinnvoll für Anwendungen, die sowohl IPv4 als auch IPv6-Devices nutzen. Bei diesem Vorschlag sind folgende Funktionen zu beachten:

- **Adressierung:** Da dieser Typ beide Protokollvarianten beherrscht, sind auch beide Adressversionen zu konfigurieren. Eine direkte Beziehung zwischen beiden ist nicht zwingend erforderlich.
- **IPv4-Loopback-Adresse:** Die Netzadresse 127.0.0.1 wird bei IPv4-Rechnern als Loopback-Funktion verwendet, d.h. ein Datenpaket mit dieser Adresse wird an den Sender zurückgeschickt. Alle IPv4/IPv6-Implementierungen behandeln diese Adresse deshalb auch als IPv6-Loopback-Funktion.
- **Domain-Name-Service:** Die aktuellen Server können keine Namen in IPv6-Adressen von 128 Bit Größe auflösen. Dazu bedarf es einer Anpassung des DNS-Protokolls (RFC 1886: DNS Extensions to Support IP Version 6). Diese Spezifikation führt einen neuen Resource-Record-Typ „AAAA“ (Quad A) ein, der Domännennamen auf IPv6-Adressen abbildet. Netzanwendungen, die direkt IP-Interfaces verwenden, müssen auf das neue Adressschema vorbereitet werden. So kann eine Applikation nicht mehr auf DNS zugreifen, wenn sie nicht in der Lage ist, 128-Bit Records für eine Adresse zu verarbeiten.
- **Routing:** Router, die beide Protokolle parallel verwenden, können in der gleichen Art und Weise verwaltet werden, wie Router mit nur einem IP-Dialekt. Sollte der Wunsch bestehen, beide Infrastrukturen auf dem gleichen physikalischen Device getrennt zu verwalten, so kann dies wie in einer Multiprotokoll-Umgebung geschehen. Oft dürfte es sich als vorteilhaft erweisen, zumindest gleiche Domänengrenzen, Areas und Subnetzbereiche beizubehalten. Andererseits stellt eine unabhängige IPv6-Architektur die Chance dar, einen neuen hierarchischen Adressplan aufzustellen.

Tabelle 8.5 Migrationsstrategien

Strategie	Beschreibung
Tunnel 6to4	Tunnelendpunkte werden automatisch erkannt; sendet IPv6 über ein IPv4 Netzwerk zwischen Routern
Tunnel manuell	Manuelle Konfiguration und Sendung von IPv6 über ein IPv4 Netzwerk
Tunnel Teredo	Üblicherweise zwischen Hosts eingesetzt; Erstellung von IPv6-Paketen und deren Kapselung und Transport über IPv4 Netzwerke
Dual-Stack	Unterstützt beide Protokolle und ermöglicht eine IPv4 zu IPv4 und eine IPv6 zu IPv6 Kommunikation

■ 8.6 Mobile IPv6

Mobile IP ähnelt im Ablauf dem Nachsendeantrag der Post. Die Briefe landen zunächst im heimatlichen Briefkasten – dem Heimatnetz, für dessen Leerung der Nachbar – der Home-Agent – zuständig ist. Dieser korrigiert die Adresse durch die Urlaubsanschrift und schickt den Brief erneut los. Die Post stellt die Sendung dann am Urlaubsort – Fremdnetz – zu. Um dieses Szenario abzubilden, sind Erweiterungen des ursprünglichen IP notwendig. Sie werden in RFC 3775 von 2004 im Detail beschrieben.

Mobile IP erlaubt einer IP-Station ihr „Heimat-Subnetz“ zu verlassen, ohne den Kontakt zum Internet zu verlieren. Während der Abwesenheit vom Ursprungsort sendet die Station Informationen über ihren aktuellen Ort an einen „Home-Agenten“ auf dem „Home-Link“. Der „Home-Agent“ fängt alle Nachrichten an den Knoten ab und leitet sie an die gegenwärtige Position weiter. Diese Umleitung basiert auf so genannten Care-of-Adressen, die aus dem Erhalt von Router Advertisements oder der Zuweisung von DHCP-Servern stammen. Diese Adresse nimmt die Rolle eines temporären Empfängers ein. Die Station bleibt weiterhin durch die „Homeadresse“ bekannt, unabhängig vom Standort. Nachrichten an das mobile Endgerät werden also an den temporären Aufenthaltsort auf der Grundlage der Care-of-Adresse weitergeleitet. Die Nutzung zielt damit auf WLAN und WIMAX.

8.6.1 Kommunikationsablauf

Der geänderte Kommunikationsablauf unter Mobile IP zwischen einem mobilen Knoten A und einem stationären Rechner X lässt sich in mehrere Phasen gliedern:

1. Station X sendet ein an den mobilen Knoten A gerichtetes IP-Paket an die Heimatadresse von A.
2. Auf dem Heimatnetz wird das einlaufende Paket vom Home-Agent abgefangen und in ein neues IP-Paket eingepackt, dass nun als Empfängeradresse die Care-of-Adresse des Foreign-Agents trägt.
3. Der Foreign-Agent als Registrierungspunkt des mobilen Knotens am neuen Netz entfernt den äußeren Header, erhält somit das Originalpaket und stellt es A über sein Netzwerk zu.
4. Im umgekehrten Fall stellt sich der Ablauf unverändert dar. A überträgt IP-Pakete an X und nutzt dazu wie bisher die fixe IP-Adresse von X.

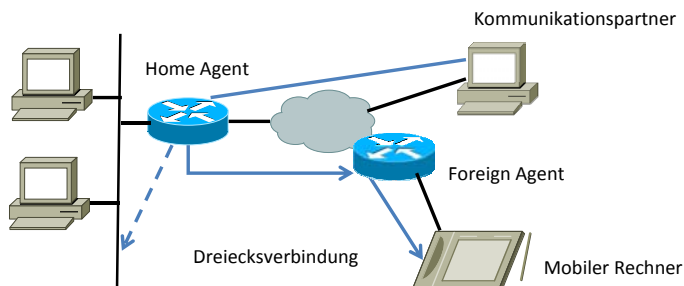


Bild 8.4 Kommunikationsstruktur von Mobile IPv6 (Quelle: Cisco Systems)

8.6.2 Technischer Hintergrund

IP leitet Pakete von einer Quelle zum Ziel über mehrere Zwischenknoten. Diese Knoten in Form von Routern empfangen die Pakete und entscheiden anhand ihrer Routingtabelle, auf welches Interface und damit an welches Netzwerk sie das Paket in Richtung Ziel weiterreichen. Ein mobiler Knoten, der ständig seine Position verändert, muss folglich seine IP-Adresse unverändert lassen. Da die IP-Adresse sich aber gerade dem Netz anpassen muss, dessen Teilnehmer der mobile Knoten ist, entsteht ein Problem. Mobile IP löst diesen Widerspruch durch die Vergabe von zwei IP-Adresse: der „Home-Adresse“ und der „Care-of-Adresse“.

Während die **Home-Adresse** statisch ist, passt sich die **Care-of-Adresse** jeder neuen Örtlichkeit an. Jede räumliche Veränderung wird durch die Registrierung der neuen Care-of-Adresse beim Heimatrechner bekannt. Um das Paket vom Heimatnetz zum mobilen Knoten zu übertragen, transportiert der Heimatrechner es zur Care-of-Adresse. Dazu muss die Zieladresse des Paketes entsprechend angepasst werden. Dieser Umleitungsprozess vom Heimatnetz auf die Care-of-Adresse geschieht durch die Konstruktion eines neuen IP-Headers, der die Care-of-Adresse des mobilen Knotens als IP-Zieladresse enthält. Der neue Header umschließt das bisherige IP-Paket, so dass die Heimatadresse des mobilen Knotens darin verschwindet und keine Auswirkungen auf das Routing hat.

Was passiert, wenn ein mobiler Knoten ein Fremdnetz betritt? Bewegt sich der Benutzer, muss das Gerät die ständige Veränderung in Relation zu seinem bisherigen Netz erkennen. Da ein Übergang von einem Heimatnetz in ein Foreign-Netz jederzeit erfolgen kann, ist die Discovery-Routine für einen mobilen Knoten ein stetiger Prozess. Für diesen Vorgang sind Router-Advertisements notwendig. Diese Nachricht enthält die IP-Adresse des Routers, Erweiterungen enthalten Angaben über die Rolle des Routers als Agent. Dazu zählen:

- Type 16, der anzeigt, dass es sich um ein Agent-Advertisement handelt
- eine Sequenznummer, die die Zahl der Advertisement-Nachrichten seit der Initialisierung angibt
- die Lifetime, die maximale Zeitdauer für die ein Agent Registrierungsanfragen annimmt.
- eine Reihe von Flags, die Auskunft darüber geben, ob ein Agent als Foreign-Agent arbeitet, welchen Tunneling-Mechanismus er verwendet, ob er Registrierungen akzeptiert etc.
- die Care-of-Adresse als neue Adresse des mobilen Knotens

Um die Veränderung der Zugehörigkeit zu einem Netz zu erkennen, dient in Mobile IPv6 das Neighbor Discovery-Protokoll ND (RFC 1256). Anhand von zwei Angaben kann der mobile Knoten nun entscheiden, ob sich seine Position verändert hat:

1. **Lifetime-Feld:** Sobald ein mobiler Knoten von einem Foreign-Agent ein Router Advertisement erhält, wertet er die Zeitangabe aus. Läuft die Zeitschranke ab, bevor ein neues Advertisement eintrifft, nimmt der mobile Knoten an, dass er den Kontakt zum Foreign-Agent verloren hat.

- 2. Verwendung des Netzwerkpräfixes:** Anhand des im Router-Advertisement befindlichen Netzwerkpräfixes lässt sich ausmachen, ob sich die Station noch im selben Subnetz befindet. Wenn nicht, versucht der mobile Knoten sich bei einem anderen Agent zu registrieren, dessen Advertisement er empfängt.

Ein Advertisement führt also dazu, dass der mobile Knoten entdeckt wird, er Eigenschaften der Foreign-Agents erfährt, er erkennt, ob der Agent ein Home-Agent oder ein Foreign-Agent ist und welche Netzwerknummer und welchen Verbindungsstatus seine Internetanbindung besitzt.

Sobald der mobile Rechner Kontakt zum Fremdnetz herstellen möchte, benötigt er eine IP-Adresse. Diese kann er per DHCP beziehen, was als zustandsbehaftete Autokonfiguration bezeichnet wird. Alternativ kann er bei Verwendung von IPv6 eine lokale IP-Adresse über die zustandslose Autokonfiguration (RFC 2462) ermitteln.

Auch für den Fall, dass eine mobile Station die IP-Adresse ihres Home-Agenten verliert, ist Vorsorge getroffen worden. Sie sendet dann Binding Updates an die Home-Agenten Anycast-Adresse mit ihrem eigenen Home-Subnetz-Präfix und erreicht auf diese Weise einen der Router auf dem Home-Link.

Ein mobiler Rechner M muss seinem Heimagenten H mitteilen, dass er Pakete für ihn entgegennehmen und an die Care-of-Adresse schicken soll. Dieser Registrierungsprozess verläuft in vier Schritten:

1. Der Prozess beginnt damit, dass der mobile Knoten eine Registrierungsanforderung an den Foreign-Agent mit der Care-of-Adresse versendet.
2. Der Foreign-Agent leitet diese Anfrage an den Home-Agent weiter
3. Sobald der Home-Agent diese Nachricht erhält, fügt er die Information seiner Routingtabelle hinzu und antwortet dem Foreign-Agent mit einer Bestätigung. Mit der Entgegennahme der Anforderung verbindet der Home-Agent die Home-Adresse des mobilen Rechners mit der Care-of-Adresse und weist dieser Assoziierung einen Timer zu. Das Tripel aus Home-Adresse, Care-of-Adresse und Registrierungstimer wird als Binding bezeichnet. Um das Ablaufende der Gültigkeit von Binding-Einträgen zu verhindern, können Knoten Binding Requests zur Aktualisierung des Eintrages an den mobilen Knoten versenden. Dadurch werden wiederum Binding-Updates ausgelöst.
4. Mit der Entgegennahme der Antwort stellt der Foreign-Agent eine Verbindung zum mobilen Knoten her.

Der Registrierungsprozess nutzt zwei Nachrichtentypen: die Registrierungsanfrage und die Registrierungsantwort. Beide Nachrichten enthalten Angaben zur Lifetime, zur Home-IP-Adresse des mobilen Knotens, seinem Home-Agent, eine Identifikationsnummer und eine Typbezeichnung. Der Ablauf des Registrierungsprozesses verdeutlicht aber auch die Notwendigkeit der Authentifizierung. Der Home-Agent muss sicher sein, dass der mobile Knoten die Registrierung ausgelöst hat. Ein potentieller Angreifer könnte den Home-Agenten veranlassen, seine Routingtabellen mit Fehleinträgen falscher Care-of-Adressen zu versehen. Mobile IP versucht diese Art von Angriff abzuwehren und darüber hinaus ein Replay alter Registrierungsnachrichten zu erkennen. Dazu enthält jede Registrierungsnachricht eine Authentifikationserweiterung. Jeder mobile Knoten muss in der Lage sein,

mit Message Digest 5 und einem 128 Bit Schlüssel eine eindeutige digitale Signatur der Registrierungsanforderung zu erzeugen. Diese wird als MD5 „One-Way-Hash“-Algorithmus über den Header der Registrierungsnachricht und eventuelle Erweiterungen berechnet. Um die Eindeutigkeit sicherzustellen, muss jede Anfrage unverwechselbare Daten enthalten. Mobile IP benutzt dazu ein spezielles Identifikationsfeld der Registrierungsnachricht. Dabei kann die Eindeutigkeit auf zwei Wegen erreicht werden: als Zeitstempel oder als Pseudozufallszahl. Schwierigkeiten entstehen allenfalls, wenn zwei Stationen für eine Synchronisierung über Zeitstempel zu weit auseinander liegen oder sie Zufallszahlen verlieren.

Im Szenario von Mobile IP spielen die Foreign-Agents eine vorwiegend passive Rolle. Sie stellen Registrierungsanfragen zu und vermitteln zwischen Home-Agent und mobilem Knoten. Darüber hinaus entfernen sie die Hülle gekapselter Pakete des Home-Agents und leiten sie an die mobile Station. Während dieses gesamten Vorganges hat sich ein Foreign-Agent weder gegenüber dem Home-Agent noch dem Mobilknoten zu authentifizieren.

Will ein Knoten ein Paket versenden, prüft er zunächst den Binding-Cache, ob für das Ziel ein Eintrag vorhanden ist. Trifft dies zu, sendet er das Paket mit dem neuen IP-Header an die angegebene Care-of-Adresse, andernfalls verschickt er es wie herkömmlich. Der neue IP-Header spezifiziert indirekt zwei Hops. Der erste Hop ist die Care-of-Adresse, die zweite die mobile Adresse. Das Ergebnis ist die direkte Zustellung an die Care-of-Adresse des mobilen Knotens. Dort wird das Paket empfangen und zum nächsten Hop transportiert, der aber der Knoten selber ist.

Wenn der mobile Knoten ein Paket versenden möchte, stellt er es dem Ziel zwar direkt zu, er muss aber neben der Care-of-Adresse als der Quelladresse noch seine Heimatadresse als Option eintragen. Dieser Eintrag ist für Protokolle wichtig, die oberhalb des Layers 3 die statische Ursprungsadresse verwenden. Die Kommunikation der mobilen Station mit einem beliebigen Knoten im Internet gestaltet sich als Dreiecksbeziehung: Pakete vom Zielrechner werden zum Home-Agenten geleitet und von dort anhand der Care-of-Adresse zur Mobilstation, während sie in der Richtung von der Mobilstation zum Ziel direkt zugestellt werden. Um diesen Umweg zu vermeiden, kann die mobile Station Binding Updates an alle ihr bekannten Stationen versenden. Dies erlaubt einem Knoten, die Care-of-Adresse in einem Cache abzulegen und die Daten der Mobilstation direkt zu übertragen.

Sobald der mobile Rechner am Netzpräfix erkennt, dass er in sein Heimatnetz zurückgekehrt ist, löscht er die bestehende Binding. Dazu setzt er seine Care-of-Adresse, also die Quelladresse des IP-Headers, auf seine Heimatadresse.

■ 8.7 Zusammenfassung

IPv6 wartet gegenüber seinem Vorgänger mit zahlreichen Verbesserungen und Modifikationen auf. Nicht alle Entscheidungen zu IPv6 fanden die ungeteilte Zustimmung der Internetgemeinde. Viele Aspekte wurden kontrovers diskutiert:

- Als wichtigstes Merkmal besitzt IPv6 gegenüber IPv4 längere Adressen, die dem Problem der Adressknappheit entgegenwirken.

- Die zweite Verbesserung betrifft die Vereinfachung des Headers. Überflüssige Felder wurden gestrichen mit dem Ziel, den Durchsatz deutlich zu verbessern. Wie zweischneidig dieses Thema ist, zeigt die Entfernung der Prüfsumme. Viele Stimmen wurden laut, die den Verzicht mit dem Ausbau der Bremsen eines Autos verglichen. Das Auto werde zwar leichter und schneller, kommt aber spätestens dann in Schwierigkeiten, wenn ein Hindernis auftaucht.
- Mobile Hosts sind ein weiterer Streitpunkt. Verändert ein Rechner seinen Standort, soll er mit der gleichen Adresse weiterarbeiten und einen Mechanismus mit Heimat- und Fremdagenten zur Identifikation benutzen. Eigens für dieses Verfahren wurde das Mobile IPv6 entworfen.
- Ein Bereich, in dem IPv6 deutliche Verbesserungen gegenüber seinem Vorgänger aufweist, ist die Sicherheit. Mit den Merkmalen wie Authentifikation und Verschlüsselung kann IPv6 die aktuellen Anforderungen an die Netzwerksicherheit erfüllen.
- Mit dem 6bone steht ein Test- und Forschungsnetz zur Verfügung, an das sich jeder Interessierte anschließen kann. Für Deutschland existiert an der Universität Münster ein Referenzzentrum als unterstützende Institution.

Die Schwelle zum Umstieg auf IPv6 ist in greifbare Nähe gerückt. So werden bereits Ende 2012 die DSL-Anschlüsse des privaten Internetzugangs weitgehend den neuen Dialekt sprechen.

Der Entwurf und die Standardisierung von IPv6 stammen aus den 90er Jahren. Daran richtet sich die Kritik, die bezüglich der Sicherheit häufig geäußert wird. Der erste Punkt betrifft die automatische Netzwerkkonfiguration über das Neighbor Discovery Protocol. Über Router-Advertisements als Teil des Neighbor Discovery Protocols ermitteln IPv6-taugliche Geräte, Router sowie Netzwerk-Präfixe des lokalen Netzsegments (local link). Leider können IPv6-Rechner mit NDP nicht verifizieren, ob die so gewonnenen Informationen gültig und unverfälscht sind: Gibt sich etwa ein beliebiger Rechner in einem IPv6-Netz als Router aus, kann er ähnlich wie unter IPv4 auch den Netzwerkverkehr an sich ziehen und kontrollieren. Mit der NDP-Erweiterung SEND (SEcure Neighbor Discovery, RFC 3971) lässt sich dies vermeiden, allerdings nicht ohne zusätzlichen Aufwand: IPv6-Router müssen sich über Zertifikate ausweisen, die jedes IPv6-Gerät über eine Zertifizierungsstelle abgleicht.

Ein zweiter Kritikpunkt richtet sich an die Adressen: die neuen statischen IPv6-Adressen und deren Erzeugung machen Geräte zu einem unverwechselbaren Identifizierungsmerkmal lautet der Vorwurf. Hierbei gilt es allerdings zu bedenken, dass die Nutzer auch über andere Mechanismen wie Logins, Cookies, Sozialen-Netze-Buttons, E-Mail-Abrufe, Tweets oder Werbebanner erkannt werden können.

Die Originalinformationen finden sich als RFC 2460 unter dem Link:
<http://www.ietf.org/rfc/rfc2460.txt>

**Noch Fragen ...? Ja ...**

Gibt es eine Webseite, auf der alle wesentlichen Parameter der Internetprotokolle zu finden sind?

Ja, die Internet Assigned Numbers Authority (IANA) verwaltet diese Informationen unter der Adresse: <http://www.iana.org/assignments>

Können die alten IPv4-Adressen weiterverwendet werden?

Ja, eine IPv4-Adresse 192.168.1.1 wird hexadezimal zu C0:A8:1:1 und als IPv6-Adresse durch ::FFFF:C0:A8:1:1 dargestellt.

Bleiben ARP und NAT erhalten?

Nein, ARP geht in das Neighbor Discovery Protocol auf, für NAT ist kein Ersatz vorgesehen.

Wie wird IPv6 in Windows aktiviert?

Windows 7 aktiviert IPv6 automatisch. In dem Fenster „Eigenschaften von LAN-Verbindungen“ ist der entsprechende Haken gesetzt.

8.8 Wissensüberprüfung

1. Auf welche Headerfelder verzichtet IPv6?
2. Stimmen Sie folgender Aussage zu? „Wenn ein IPv6-Tunnel durch einen IPv4-Router führt, behandelt IPv6 einen IPv4-Tunnel wie ein Protokoll der Schicht 2“.
3. Muss das ARP-Protokoll für die Nutzung von IPv6 geändert werden?
4. Wie wird die IPv4-Adresse 193.174.250.1 in IPv6 umgesetzt?
5. Wie sieht die Binärdarstellung der IPv6-Adresse C22F:1582 aus?
6. Eine Anwaltskanzlei bekommt neue Rechner. Wie erklären Sie dem Seniorchef die automatische Adresskonfiguration?
7. Warum kann auf das Feld Fragment Offset verzichtet werden?
8. Erklären Sie die Funktionsweise von Anycasts.
9. „IPv6 überträgt in einer Session nur Pakete gleicher Größe“. Stimmen Sie dieser Aussage zu?
10. Wie sehen die Hierarchieebenen des IPv6-Adressaufbaus aus?

9

Layer-2 – Geräte, Protokolle und Konzepte

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Wie arbeitet ein Switch?
- Welche Switchingmethoden existieren?
- Welche Anforderungen an die Paketweiterleitung gibt es?
- Wie unterscheiden sich Switcharchitekturen?
- Welche Rolle spielt das Spanning-Tree-Protokoll für die Schicht 2?
- Was sind VLANs und wo spielen sie ihre Bedeutung aus?

Kapiteleinführung

Heutige Unternehmensnetze sind komplexe, heterogene Hochgeschwindigkeitsinfrastrukturen. Eine Kombination von Switches und Routern wird eingesetzt, um die Anforderungen der Benutzer nach hoher Bandbreite und kurzen Antwortzeiten zufriedenstellend zu erfüllen. Worin liegen die Gründe für die ständige Forderung nach höherer Geschwindigkeit im Netz?

- „Alles hat sich verändert, auch das Netzwerk“ könnte eine These zur Datenverarbeitung der letzten Dekade lauten. Vergangene broadcast-basierte Shared-Media-Netze ächzten unter der Datenlast. Als Resultat hat sich beinahe jeder Aspekt der Informationsverarbeitung geändert – Tools, Technologie, Methoden. Obgleich Netzwerke nur einen Teil der Gesamtstruktur ausmachen, sind sie doch besonders kritisch, weil sie das Nervensystem einer Unternehmung bilden. Unglücklicherweise liefern die meisten Netzwerke keinen konstanten Level an Dienstqualität. Gleichbleibende Antwortzeiten oder einfaches Management sind vielfach Fremdworte. Doch neue Anwendungen verlangen die Übertragung von mehr Daten in einer kürzeren Zeit über größere geographische Entfernungen. Der Weg, diesen Anforderungen erfolgreich zu begegnen ohne die Komplexität zu steigern, ist eine permanente Herausforderung.
- Im Zeitalter des Internets, der Multi-Media-Anwendungen, des Cloud-Computings und der zentralen Serverfarmen haben sich die netzübergreifenden Datenströme verstärkt. Als Folge dieser Entwicklung sind Backbones mit höherer Bandbreite erforderlich, um eine ausreichende Antwortzeit für die Benutzer zu garantieren. Switches übernehmen im lokalen Bereich dabei die zentrale Vermittlungsrolle.

- Überschreitet die Netzlast aufgrund konkurrierender Zugriffe der Anwender und der dadurch ausgelösten Serverengpässe ein bestimmtes Maß, muss die Infrastruktur leicht erweiterbar sein. Switches leisten hierzu einen signifikanten Beitrag.

■ 9.1 Switches

Switches bilden heute den Kern der Netzwerkinfrastrukturen und lösen die lange vorherrschenden HUBs und Bridges ab. Hersteller bieten Switches für alle Ethernetvarianten an. Dabei bezeichnet der Name Switch im Allgemeinen einen Switch auf Ethernetbasis, da alle anderen LAN-Technologien faktisch bedeutungslos geworden sind. Switches sind die Arbeitspferde heutiger Netzinfrastrukturen.



Switch

Switches leiten Pakete auf der Schicht 2 unter Verwendung von Quell- und Ziel-MAC-Adresse weiter. Um diese Aufgabe zu erfüllen, bauen sie in einem Selbstlernprozess Tabellen auf, die die Zieladresse mit dem entsprechenden Port verbindet.

9.1.1 Eigenschaften

Anders als ihre Vorgänger die Bridges, die Software für den Aufbau und die Verwaltung der Adresstabelle verwenden, basieren Switches auf ASICs. Mit dem hardwarebasierten Design lassen sich eine Vielzahl nutzbringender Eigenschaften realisieren:

- Switches verbessern die **Datensicherheit**, da Informationen, die zwischen Knoten ausgetauscht werden, nicht in anderen Netzteilen sichtbar sind.
- Switches optimieren den **Datendurchsatz**, da sie Pakete zwischen ihren Ports simultan übertragen können. Dadurch kann die Leistung des Gesamtnetzes beträchtlich erhöht werden. In einem LAN, in dem alle Knoten direkt mit einem Switchport verbunden sind, steigt der Durchsatz durch bidirektionale Verbindungen. Da jeder Rechner getrennt mit einem Port assoziiert ist, bildet er eine eigene Kollisionsdomäne und ein eigenes Segment. Damit ergeben sich drei Vorteile:
 - dedizierte Bandbreite für jeden Port
 - kollisionsfreie Umgebung
 - Vollduplexmöglichkeit

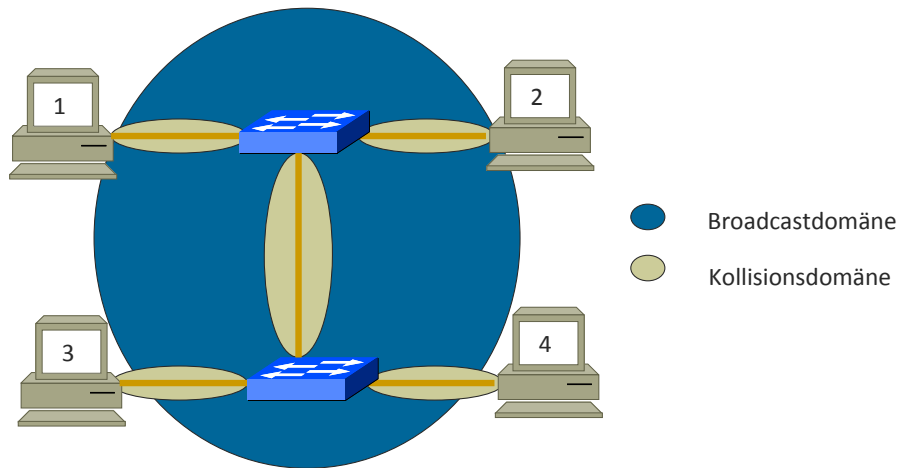


Bild 9.1 Layer 2-Switches trennen Kollisions- aber keine Broadcastdomänen in Switchingumgebungen

- Switches dehnen ein Netz bezüglich der Stationen durch eine wachsende Portzahl und bezüglich der Länge durch eine Kaskadierung aus.
- Switches erlauben die Trennung der angeschlossenen Stationen in organisatorische Einheiten auf der Grundlage von virtuellen Netzen.



Switches erhöhen die Anzahl der Kollisionsdomänen, verringern aber die Teilnehmerzahl pro Kollisionsdomäne.

Bridges als Vorgänger von Switches tauchten in den 80er Jahren auf, zunächst zur Koppelung homogener Technologien dann zur Verbindung unterschiedlicher Typen von Netzwerken. Als logischer Entwicklungsschritt lösten Anfang der 90er Jahre Switches die Bridging-Technologie ab, indem sie:

den Durchsatz erhöhten, die Kosten pro Port verringerten und die Portdichte signifikant steigerten.

Diese Merkmale äußern sich im Netzdesign:

- **Steigerung der Anzahl Rechner:** Ein Stationsausbau bedeutet, dass der Switch mehr Anschlussmöglichkeiten in Form von Ports zur Verfügung stellen muss. Dies kann auf zwei Arten erreicht werden: zum einen können durch Trunkleitungen weitere Switches kaskadiert, zum anderen kann durch Stackable Switches die ursprüngliche Portdichte erhöht werden.
- **Migration und Investitionssicherheit:** Nutzer, die über ältere Netzwerkkarten nach den Ethernetvorläuferstandards arbeiten, können ohne Austausch der Netzkarte an 10/100-Mbit/s-Autosensing-Ports des Switches angebunden werden.

- **Aufrüsten der Serveranbindung:** Server als potenzieller Engpass der Client-/Server-Kommunikation können über spezielle Uplink-Ports mit einer schnelleren Technologie – z.B. 10-Gigabit-Ethernet – angeschlossen werden.

9.1.2 Arbeitsweise

Die zentrale Funktion eines Switches nämlich das Weiterleiten der Datenpakete beruht auf einer Adresstabelle, deren Inhalt in einem Selbstlernprozess vollständig transparent für die Nutzer erstellt wird. Zur Weiterleitung führt der Switch drei Aktionen aus:

1. Zunächst entscheidet er, ob das Paket auf Basis der Zieladresse weitergeleitet werden kann oder verworfen werden muss. Damit erhöhen Switches die **Sicherheit**, da unvollständige oder unzulässige Pakete gefiltert werden können. Switches leisten damit eine rudimentäre Fehlerbegrenzungsmöglichkeit.
2. Im nächsten Schritt wird die Quelladresse des Paketes auf ihr Vorhandensein in der Adresstabelle geprüft, um den Adresslernprozess einzuleiten.
3. Als letzte Phase prüft der Switch die Zieladresse hinsichtlich eines Eintrags.

Der Adresslernprozess stellt sich damit wie folgt dar: Sobald ein Datenpaket den Switch erreicht, fügt dieser die Ethernet Quell-MAC-Adresse und den Port, über welchen die Stationen angebunden ist, in eine Adresstabelle ein. Existiert bereits ein Eintrag für die Quelladresse, wird lediglich der Aging-Timer aktualisiert. Anschließend prüft der Switch die Zieladresse daraufhin, ob es sich um eine Broadcast-, eine Multicast- oder eine unbekannte Unicast-Adresse handelt. Nur im Fall, dass die Ziel-MAC-Adresse bereits in der Adresstabelle verzeichnet ist, findet eine gerichtete Paketweiterleitung zum Ziel statt.

Switches lernen nur Unicast-Quelladressen. Der mit der Adresstabelle verbundene Lernprozess hat zwei Aufgaben zu erfüllen:

- einerseits müssen neu angeschlossene Stationen entdeckt werden
- andererseits müssen Stationen, die das LAN wechseln, in ihrer Erreichbarkeit aktualisiert werden.

Zur Sicherstellung dieser Anforderungen überprüft der Switch alle Pakete, die er an einem Port empfängt auf die Quell-MAC-Adresse und führt zusätzlich eine Zeitangabe als Aktivitätszeit der einzelnen Station.

Erhält ein Switch ein Paket das erste Mal für eine noch unbekannte Zieladresse, verfügt er über keinen entsprechenden Eintrag in der Adresstabelle. Um eine Entscheidung darüber zu treffen, ob für das Paket ein korrekter Pfad existiert, sendet der Switch dieses Paket an alle Ports mit Ausnahme desjenigen, auf dem er es empfangen hat. Dieser Prozess wird als Flooding bezeichnet. Neben den unbekannten Unicast-Paketen „flutet“ ein Switch auch Broadcast- und Multicast-Sendungen.

Die folgende Abbildung verdeutlicht das als **Learn-and-Stay-Verfahren** bekannte Adresslernen von Switches.

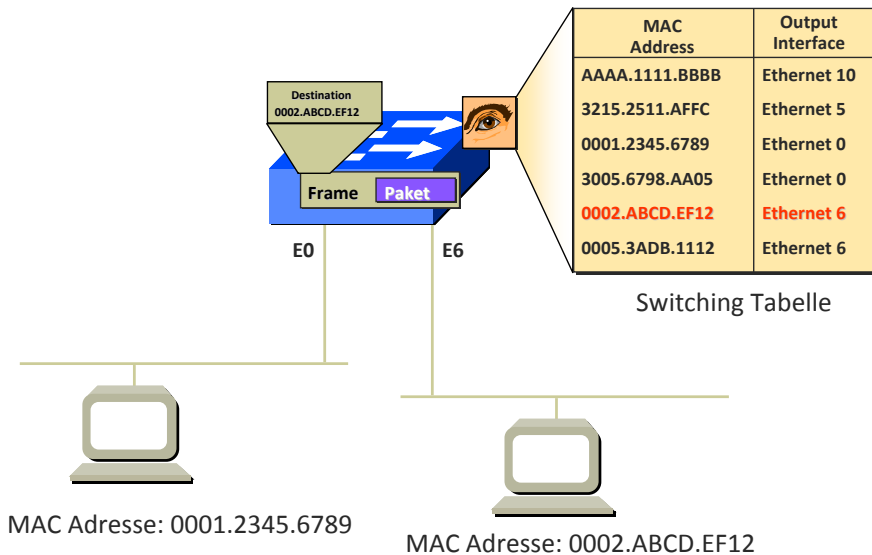


Bild 9.2 Learn-and-stay-Verfahren von Switches

- Die **Aging-Funktion** ermöglicht es, Umzüge einer Station in ein anderes LAN zu erkennen. Sollte nämlich innerhalb der durch den Zeitstempel vorgegebenen Zeitspanne die betreffende Station nicht aktiv sein, wird sie aus der Adresstabelle gelöscht. Ihr Neueintrag erfolgt mit dem ersten Weiterleitwunsch nach Ablauf des Zeitstempels.
- Der Zeitstempel legt fest, wie lange die MAC-Adresse der Quellstation in der Adresstabelle gehalten werden muss. Diese Zeitspanne hat Einfluss auf die Weiterleitungsgeschwindigkeit, da es bei zu kurzen Zeitintervallen zu einem wiederholten „Flooding“ kommt. „Flooding“ bedeutet neben Netzlast aber auch steigende Verzögerungszeiten, so dass der Wahl der Zeitspanne eine große Bedeutung zukommt. Der Eintrag kann als „Lebenszeit“ der Station interpretiert werden.

9.1.3 Switchingverfahren

Aufgrund ihrer Einfachheit können Switches in Hardware realisiert werden. Sie analysieren die MAC-Adresse des Paketheaders schon nach den ersten 20 – 30 Byte ohne sie in einem Puffer abzulegen, entscheiden dann den Weg für die Daten und schalten unverzüglich den entsprechenden Ausgangsport. Eine Zwischenspeicherung von Informationen wird nur notwendig, wenn der gewünschte Ausgangsport belegt ist. Die Verweilzeit von Paketen in einem Switch ist kleiner als 30 μ s, verglichen mit 500 – 4000 μ s bei Routern eine sehr geringe Zeitspanne.

Switches können prinzipiell nach unterschiedlichen Verfahren arbeiten. Sie unterscheiden sich in der Weiterleitmethode = Switchingverfahren, der Portgeschwindigkeit = symmetrisches/asymmetrisches Switching, der Zwischenspeicherung von Paketen = portbasiert oder Shared-Memory. Drei Switchingverfahren lassen sich unterscheiden:

- **Cut-Through (Fast Forward):** Der Bearbeitungszyklus eines Switches für das einlaufende Paket beginnt bereits dann, wenn unmittelbar nach Einlesen der MAC-Adresse klar ist, wohin der Rahmen weitergeleitet werden muss. Während das Ende des Datenpaketes eingelesen wird, wird bereits der Anfang des Paketes dem betreffenden Ausgangsport zugestellt. Das Ergebnis ist eine extrem geringe Latenzzeit, unabhängig von der Länge des Datenpaketes. Durch den Verzicht auf die Zwischenspeicherung der empfangenen Datenpakete und auf die Bearbeitung des Prüffeldes erreichen Switches zwar eine hohe Vermittlungsgeschwindigkeit, allerdings mit einigen Nachteilen:
 - ⊙ Da alle Steuerfelder hinter der MAC-Adresse nicht geprüft werden, können fehlerhafte Pakete auf das Netz gelangen.
 - ⊙ Die alleinige Auswertung der Adresse beschränkt die Filtermöglichkeiten auf eine reine Adressprüfung.
 - ⊙ Das Verfahren kann nur zwischen Ports gleicher Geschwindigkeit arbeiten. Ein ungepufferter 100-MBit/s-Fast-Ethernet-Datenstrom kann an einem 10 MBit/s Port nicht verarbeitet werden.

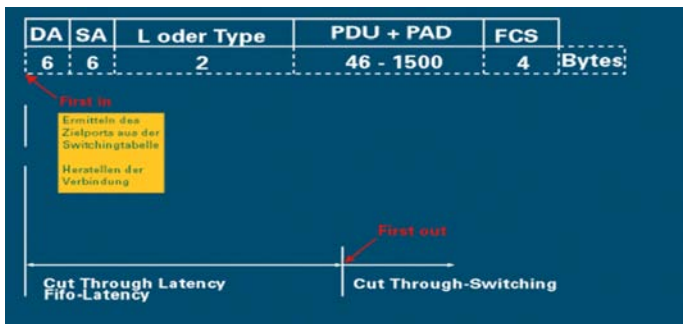


Bild 9.3 Cut-Through-Verfahren (Quelle: Bildungsinitiative Networking)

Quelle: Bildungsinitiative Networking

- **Store-and-Forward:** Der Switch liest die ankommenden Datenpakete vollständig ein. Dadurch vergrößert sich die Verweilzeit der Pakete im Switch, so dass die Latenz damit abhängig von der Paketlänge wird. Weil jedes gepufferte Byte eine Verzögerung von $8 \mu\text{s}$ bewirkt, benötigt ein 64-Byte-Paket $51,2 \mu\text{s}$ im Switch und 1518 Byte eines Ethernet-Pakets bereits $1200 \mu\text{s}$, eine Tatsache, die aber nicht überbewertet werden sollte, denn im Prinzip geht es um den Datendurchsatz. Durch das Einlesen des Gesamtpaketes wird eine Anpassung der Transferraten an unterschiedlich schnellen Ports über Puffer möglich. Schnellere Ports müssen auf das vollständige Paket eines langsamen Ports warten und umgekehrt.
 - ⊙ Alle Steuerfelder des Paketes können auf Vollständigkeit und Fehlerfreiheit überprüft werden.
 - ⊙ Der Einsatz komplexer Filtermechanismen auf Basis der verwendeten LAN-Technologie ist möglich.

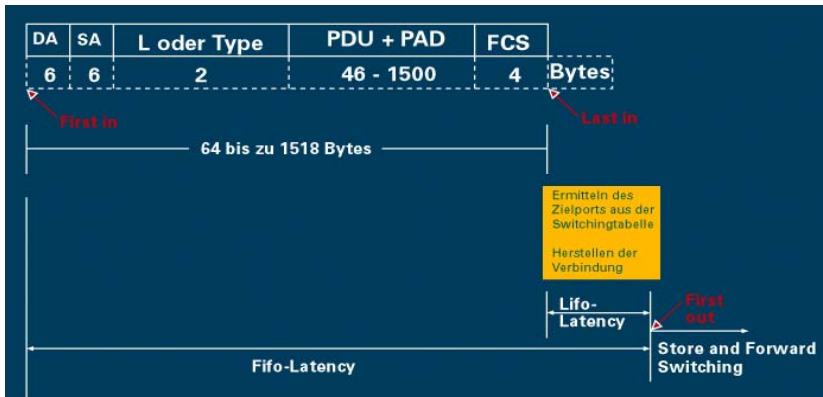


Bild 9.4 Store-and-Forward-Verfahren (Quelle: Bildungsinitiative Networking)

- **Fragment Free (Modified Cut-Through):** Switches, die beide bisher vorgestellten Modi unterstützen, kennen eine dritte Form des Switching als Kompromiss zwischen Cut-Through- und Store-and-Forward-Technik. Bei langen Intervallen fehlerfreier Frames schaltet der Switch vom Store-and-Forward in den Cut-Through-Modus um, den er erst wieder bei Erreichen eines vordefinierten Fehlerschwellwertes verlässt. Beim Fragment Free-Konzept als besonderer Realisierung des Cut-Through prüft der Switch die ersten 64-Byte eines Rahmens vor einer Weiterleitung, um sicher zu sein, keine Paketfragmente als Ergebnis einer Kollision erhalten zu haben.

Der Unterschied zwischen Cut-Through und Store-and-Forward-Verfahren sollte hinsichtlich der Latenzzeit nicht überschätzt werden. Differenzen treten nur auf, wenn die Warteschlange des Ausgangsports leer ist. Nur in diesem Fall erzeugt die vollständige Speicherung des Paketes eine Verzögerung. Ansonsten muss das Paket in der Warteschlange gepuffert werden, so dass kein Unterschied darin besteht, wie das Paket übertragen wird.

Das **symmetrische und asymmetrische Switching** unterscheidet nach der Gleichförmigkeit der Anschlussgeschwindigkeit der Ports. Im Falle eines asymmetrischen Switchings, d.h. wenn Send- und Empfangsports unterschiedliche Geschwindigkeiten aufweisen, kommt das Store-and-Forward-Prinzip zum Einsatz. Dieser Fall ist der Standard in heutigen Client/Server-Architekturen. Bei symmetrischem Switching also der Kopplung gleicher Ethernetgeschwindigkeiten kann nach dem Cut-Through-Konzept verfahren werden.

Layer 2 und Layer 3-Switches unterscheiden sich darin, welche Adressen die Weiterleitung bestimmen. Layer2-Switches verwenden MAC-Adressen und sind folglich unabhängig vom Layer 3 und den darüber liegenden Anwendungen. Layer 3-Switches hingegen nutzen auch IP-Adressen, so dass sie Routingentscheidungen treffen können. Diese Eigenschaft verringert die Notwendigkeit des Einsatzes von Routern. Die Entwicklung dieser Gerätevariante ist allerdings auf die alleinige Verwendung des Internet-Protokolls beschränkt.

9.1.4 Erweiterungsmöglichkeiten

- **VLANs:** Virtuelle LANs begrenzen die Broadcast-Domäne, erhöhen die Sicherheit und steigern die Performance und die Netzflexibilität. Um einen maximalen Nutzen zu erhalten, konfigurieren Switches Trunk-Ports als physischen Kanal zu anderen Switches. Auf diese Weise lassen sich VLANs flexibel über mehrere Switches ausdehnen.
- **Virtuelle Switches:** mit dem Edge Virtual Bridging (EVB) der IEEE-Arbeitsgruppe 802.1Qbg gibt es einen Standard, der den Datenverkehr zwischen virtuellen Maschinen (VM) über einen virtuellen Switch koordiniert. Das Protokoll legt fest, wie sich mehrere virtuelle Maschinen eine physikalische Verbindung zu einem Switch teilen. Auf diese Weise kann ein Server einen eingebetteten virtuellen Switch enthalten über den er den Datenverkehr zwischen virtuellen Maschinen überträgt.
- **Non-Blocking mit Wire-Speed auf allen Ports:** Wire-Speed erlaubt die theoretische Geschwindigkeit des Mediums, also 10 Mbit/s für 10Base-T und 100 Mbit/s für 100Base-T. Non-Blocking beschreibt die Fähigkeit, dass der Verkehr auf einem Port keine Rückwirkungen auf die Abarbeitung auf anderen Ports erzeugt. Eine Art, die Switchperformance zu bestimmen, besteht darin, die notwendige Backplane-Geschwindigkeit als die Summe aller individuellen Port-Geschwindigkeiten zu addieren.



Switchperformance

Besitzt ein Switch 24 Ports zu 10 Mbit/s und 2 Ports mit 100 Mbit/s, so sollte die Backplane als interner Bus, im Falle des Voll-Duplex-Betriebes, mindestens folgende Leistung abwickeln können:

$$2 \times ((24 \times 10 \text{ Mbit/s}) + (2 \times 100 \text{ Mbit/s})) = 880 \text{ Mbit/s}$$

9.1.5 Kapazitätssteigerung

- Ein Switch ermöglicht den Aufbau mehrerer **simultaner und unabhängiger Verbindungen** zwischen einzelnen disjunkten Switch-Ports. Die Kommunikation erfolgt dann nicht mehr nach dem Shared-Media-Prinzip, nach dem sich die Teilnehmer die verfügbare Bandbreite teilen.



Es gilt eine Analogie zum Aufbau eines Telefonnetzes. Jedes Telefon auf dem Schreibtisch ist mit einem zentralen Punkt, der Telefonzentrale, verbunden. In diesem Netz könnte ein sprechender Teilnehmer gleichzeitig von allen anderen Teilnehmern gehört werden. Die Zahl der Telefongespräche pro Tag wäre begrenzt, andererseits ist die Analogie zur LAN-Technologie und dem Wettbewerb um das Shared Medium unübersehbar. Die Installation eines Sprachvermittlers in Form einer privaten Nebenstellenanlage macht es möglich, dass viele Telefongespräche unabhängig voneinander geführt werden können. Auf ähnliche Weise, jedoch sehr viel schneller, arbeitet ein Switch. Ein Port als Analogon zum Telefon kann mit einem anderen Port kommunizieren, wobei dieser bilaterale Kommuni-

kationspfad nur für die Dauer des Datenaustausches bzw. des Gespräches besteht und alle anderen Teilnehmer von diesem Datenaustausch weder etwas bemerken noch von ihm beeinträchtigt werden.

An einen zentralen Switch werden einzelne Endgeräte oder Segmente geringer Rechnerzahl sternförmig angeschlossen. Der Vorteil für den Anwender liegt nun darin, dass eine virtuelle Punkt-zu-Punkt-Leitung realisiert wird. Ein Ethernet-Switch mit 20 Ports schaltet also maximal $20 \times 10 \text{ Mbit/s} = 200 \text{ Mbit/s}$ Daten parallel durch, so dass 10 Verbindungen mit 20 Teilnehmern über die volle Bandbreite verfügen.

- Die **Kaskadierung** von Switches bildet eine Möglichkeit der Anpassung an steigende Leistungsanforderungen, wobei die Kaskadierungstiefe nicht limitiert ist. Pro Port wird allerdings nur die übliche Übertragungsrate bereitgestellt.
- Reicht die Bandbreite trotz einer Kaskadierung nicht aus, unterstützen Switches den **Vollduplex**-Modus. Stationen oder weitere Switches können dann mit der doppelten Übertragungskapazität angeschlossen werden.
- Sollte auch diese Variante keine nennenswerte Netzentlastung bringen, bleibt noch die Möglichkeit der Parallelschaltung mehrerer physikalischer Ports zu einem logischen. Dieses Verfahren ist als **Link Aggregation** bekannt und ermöglicht eine Lastteilung unter Umgehung des Spanning-Tree-Protokolls.

Diese Vorteile werden aber auch durch einige Probleme erkauft. Dazu gehört insbesondere die „Abflachung“ der Netzhierarchie. Da keine logische Unterteilung in Subnetze stattfindet, ergibt sich eine wachsende Ausdehnung der Broadcast-Domäne. Größere Broadcast-Domänen bedeuten aber eine Reduktion der verfügbaren Bandbreite. Zwei Ereignisse reduzieren die Netzeffizienz weiter: zum einen können den Switch Ethernet-Broadcasts erreichen, die dann an alle Ports weitergegeben werden müssen, zum anderen kann im Zuge des Lernprozesses ein Fluten unbekannter Zieladressen eintreten. Einen Ausweg aus dieser Misere besteht in der Bildung von VLANs.

9.1.6 Switch-Architekturen

Den Kern eines Switches bildet die Switch-Fabric, durch die die Pakete vom Eingangs- zum Ausgangsport transferiert werden. Die Switch-Fabric ist vollständig in Hardware implementiert, um geringe Latenzzeiten und einen hohen Durchsatz zu gewährleisten. Zusätzlich zur reinen Verarbeitungsaufgabe, sammelt sie statistische Daten, wie transferierte Paketzahl, Durchsatz oder Fehler. Die Vermittlungstätigkeit lässt sich auf drei Arten durchführen:

- **Shared Memory Switching:** Dieses Konzept lehnt sich an die Vorstellung an, dass Rechner und Switch in ähnlicher Weise arbeiten. Sie erhalten Daten über Eingangsschnittstellen, bearbeiten diese und geben sie über Ausgangsports weiter. Der Prozessor extrahiert dazu die Zieladresse, sucht den entsprechenden Ausgangsport und kopiert das Paket in den gemeinsamen Shared-Memory-Puffer. Als Folge ergibt sich eine Geschwindigkeitsabschätzung aus der Überlegung, dass wenn N Pakete/s simul-

tan in den und aus dem Speicher ein- und ausgelesen werden können, die Vermittlungsrate $N/2$ Pakete/s nicht übersteigen kann.

- **Bus Switching:** Bei diesem Ansatz überträgt der Empfangsport ein Paket ohne Eingriff des Prozessors über einen gemeinsamen Bus an den Ausgangsport. Den Engpass bildet der Bus, über den jeweils nur ein Paket zur Zeit transferiert werden kann. Ein Paket, das am Eingangsport eintrifft und den Bus besetzt vorfindet, wird daher in die Warteschlange des Eingangsports gestellt. Da jedes Paket den Bus separat durchqueren muss, ist die Switchinggeschwindigkeit auf den Busdurchsatz beschränkt.
- **Matrix Switching:** Das Matrixprinzip ist eine Möglichkeit die Durchsatzbegrenzung des gemeinsam genutzten Busses aufzuheben. Ein Switch dieses Typs verbindet Ein- und Ausgangsports durch ein Gitter von separaten Verbindungen. Ein Paket, das an einem Eingangsport eintrifft, wird auf den horizontalen Bus übertragen bis es sich mit dem vertikalen Bus schneidet, der zum gewünschten Ausgangsport führt. Ist diese Leitung durch die Übertragung eines anderen Paketes blockiert, muss das Paket in die Warteschlange des Eingangsports gestellt werden.



Cisco-Switches der Serie Catalyst 8500 arbeiten nach dem Shared-Memory-Verfahren, die Serie 1900 nach dem Busprinzip und die 12000-Familie nach dem Matrix-Aufbau.

Die Platzierung der Puffer eines Switches lässt grundsätzlich zwei Möglichkeiten zu:

- **Portbasierter Speicher** bei dem Warteschlangen für die einzelnen Ports existieren
- **Shared-Memory** als gemeinsamer Speicher auf den alle Ports Zugriff haben wie im Falle des Shared-Memory-Switchings

Bei der Inputport-Technik als Variante portbasierter Speicher werden Pakete auf der Empfangsseite zwischengespeichert und für den Output in Abhängigkeit vom Zustand des Outputports freigegeben. Die Wahl ist nahe liegend, weil jeder Port nur die Pufferkapazität benötigt, die die bei ihm ankommenden Pakete verlangen.

Die Pufferung auf Sendeseite verlangt einen Pakettransfer durch den Switch. Da der Verkehrsstrom innerhalb eines Switches theoretisch von jedem Inputport zu einem einzigen Outputport verlaufen kann, muss die Pufferkapazität jedes Ports die gesamte ankommende Paketlast aufnehmen können. In Zeiten von Überlast kann ein Outputport Pakete verwerfen. Da diese Pakete aber zuvor im Switch transportiert wurden, werden wertvolle Ressourcen verschwendet.

Wenn die Geschwindigkeit der Ein- und Ausgangsverbindungen gleich ist, es N Eingangs- und N Ausgangsports gibt und die Geschwindigkeit der Switch-Fabric N mal größer als die der Eingangsleitung ist, können keine Warteschlangen auftreten, denn sogar unter diesen Umständen wenn alle N Ports Pakete empfangen ist die Fabric in der Lage, die Pakete zu vermitteln. Die Situation an den Ausgangsports sieht aber anders aus. Ist das Ziel aller Pakete im Extremfall nur ein Ausgangsport wie im Falle eines Servers, kommen dort N Pakete gleichzeitig an. Da der Port aber nur ein Paket übertragen kann, müssen die restlichen zwischengespeichert werden und auf die Übertragung warten. Die Situation ver-

schärft sich, wenn weitere Pakete den Port ansteuern. Auf diese Weise kann der Speicherplatz des Ausgangsports erschöpft werden, so dass Pakete verworfen werden müssen. Ein möglicher Paketverlust hängt damit von der Verkehrslast, der Geschwindigkeit der Switching-Fabric, der Leitungsgeschwindigkeit des Ausgangsports und der Länge der Warteschlange ab.

Eine besondere Situation entsteht, wenn ein Server A überlastet ist und keine Pakete mehr entgegennehmen kann, die Pakete an Server B in der Reihenfolge aber nach denen an Server A kommen und nur ein Bus im Switch zur Verfügung steht. Dann unterbleibt die Paketzustellung an Server B. Dieses Phänomen wird als HOL-Blocking (Head-of-Line-Blocking) bezeichnet. Ein in einer Eingangswarteschlange stehendes Paket muss auf seine Übertragung durch die Switching-Fabric warten, weil es durch ein anderes Paket am Anfang der Schlange blockiert wird.



Noch Fragen ...? Ja ...

Gibt es Sicherheitsmechanismen für Switches?

Ja, die so genannte Port-Security. Dazu wird ein Port derart konfiguriert, dass er nur ein Interface mit der erwarteten MAC-Adresse akzeptiert. Mehrere MAC-Adressen pro Port sind zulässig. Die Reaktion auf eine Verletzung kann abgestuft erfolgen bis zu einem Shutdown des Ports.

■ 9.2 Spanning-Tree

Der **Spanning-Tree Algorithmus** ist ein vitaler Teil von Switch-Infrastrukturen. Netzwerke können mit einer Vielzahl von Switches als Koppelungselement aufgebaut werden. Allerdings muss die LAN-Technologie sicherstellen, dass zwischen zwei Rechnern jeweils nur ein Datenpfad existiert, um Pakete eindeutig weiterleiten zu können. Die Schwierigkeiten, die sonst entstehen können, zeigt folgendes Beispiel:

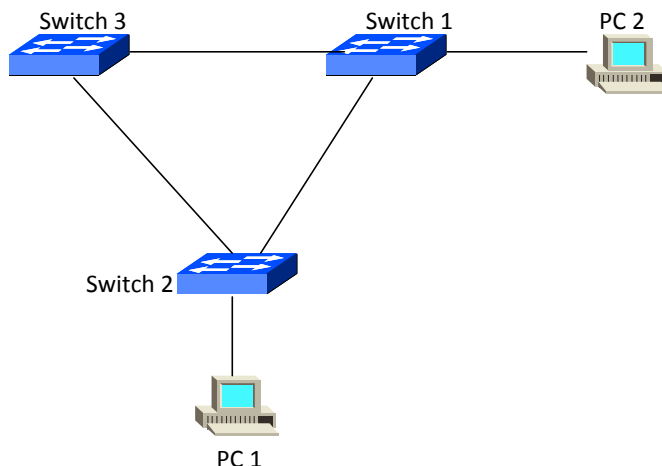


Bild 9.5 Broadcast-Schleife

Ethernet-Frames als Transporteinheit der Schicht 2 besitzen kein TTL-Feld, das die Lebensdauer eines Paketes steuert. Dies ist der Grund für das Entstehen von Broadcast-Schleifen. Wie sie erzeugt werden, lässt sich an der Topologie des Bildes verdeutlichen:

- PC 1 sendet eine Broadcast an den Switch 2.
- Sobald die Broadcast den Switch erreicht, wird die Quelladresse von PC 1 in die Adresstabelle eingetragen.
- Da es sich um eine Broadcast handelt, wird sie an Switch 1 und 3 weitergegeben.
- Switch 1 und 3 aktualisieren jeweils ihre Adresstabelle mit einem Eintrag für PC 1.
- Auf Grund der Broadcastnatur des erhaltenen Paketes wird es auf alle Ports außer dem Empfangenen weitergeleitet. Insbesondere sendet Switch 3 das Paket an Switch 1 und umgekehrt.
- Switch 1 und 3 erhalten die entsprechende Broadcast und aktualisieren ihre Adresstabelle mit der „falschen“ MAC-Adresse von PC1.
- Jeder Switch leitet die Broadcast weiter, insbesondere geben beide Switches das Paket an Switch 2 zurück.
- Als Reaktion aktualisiert Switch 2 die Adresstabelle mit dem letzten der beiden erhaltenen Einträge von Switch 1 und 3.
- Dieser Prozess setzt sich fort, bis die Schleife durch ein externes Ereignis unterbrochen wird.
- Sendet auch PC 2 eine Broadcast kulminiert die Menge der Broadcasts im Netz, so dass **ein Broadcast-Storm** entsteht.

Ein Broadcast-Storm ist nicht der einzige unerwünschte Effekt in einem Layer-2-Netz. Unter Berücksichtigung besonderer Umstände können auch **doppelte Unicast-Pakete** entstehen:

- PC 1 sendet ein Unicastpaket an PC 2.
- Switch 2 besitzt keinen Eintrag für PC 2, so dass er das Paket „fluten“ muss.
- Switch 1 und 3 erhalten das Paket.
- Switch 1 verfügt über einen Eintrag für PC 2, so dass er das Paket an PC 2 weiterreicht.
- Switch 3 besitzt ebenfalls einen Eintrag für PC 2, so dass er das Paket an Switch 1 weiterleitet.
- Switch 1 erhält das Ausgangspaket doppelt.

Die Vermeidung beider Effekte wird nur erreicht, wenn ein Algorithmus existiert, der die Schleifenfreiheit der Topologie sicherstellt. Im Beispiel bedeutet dies, dass ein Switch in einen Zustand versetzt wird, in dem er keine Pakete weiterleitet. Der **Spanning-Tree Algorithmus** sorgt nun dafür, dass es keine unerwünscht kreisenden Pakete gibt. Er identifiziert Mehrfachwege, indem er Topologien mit redundanten Wegen durch eine logische Blockierung bestimmter Pfade in eine Baumtopologie überführt, die keine Schleifen besitzt. Die inaktiven Switches werden in einen Standby-Modus geschaltet. Bei Ausfall der

primären Verbindung können diese sofort aktiviert werden und erzeugen auf diese Weise ein hohes Maß an Fehlertoleranz.

Der Spanning-Tree Algorithmus wurde von Radia Perlman entworfen und 1990 als IEEE 802.1D standardisiert. Um Schleifenfreiheit zu erzeugen, versetzt STP die Ports, die den Spanning Tree bilden in einen Weiterleitstatus, die verbleichenden Ports werden blockiert. Voraussetzung für die Funktionsfähigkeit dieses Konzeptes ist, dass der aufspannende Baum für den Nutzer vollkommen transparent erstellt werden kann. Als einzige Aktion muss der Spanning-Tree-Algorithmus auf den Switches aktiviert sein. Zum Austausch von Konfigurationsnachrichten wird eine **Bridge Protocol Data Unit** (BPDU) als Multicast-Paket genutzt, dass standardmäßig alle 2 Sekunden versendet wird und damit eine nicht unerhebliche Netzlast verursacht.

Die BPDU enthält als ein wesentliches Element die Bridge-ID als eindeutige Kennung eines Switches. Sie setzt sich aus einem Prioritätswert (2 Bytes) und der MAC-Adresse (6 Bytes) zusammen. Der Standardprioritätswert beträgt 32 768, kann aber durch einen Konfigurationsbefehl verändert werden. Der Switch in einem lokalen Netz, der die kleinste Bridge-ID besitzt, wird automatisch zur **Root-Bridge**, d. h. zur Wurzel des Baumes. Diese Funktion ist bedeutsam, da die verbleibenden Swiches als Knoten des Baumes sie als Referenzpunkt betrachten und die Baumstruktur an ihr ausrichten. Die Initialisierung des Spanning Trees beginnt folglich immer mit der Wahl der Root-Bridge. Anschließend beginnt die Auswahl der Pfade von den Nonroot-Switches zur Root-Bridge, die Ports eine bestimmte Funktion zuweist und sie gemäß dieser Funktion in einen entsprechenden Status versetzt. Grundlage der Pfadauswahl sind die Portkosten, die durch eine Zahl, abgeleitet aus der Geschwindigkeit, ausgedrückt werden.

Tabelle 9.1 Portkosten

Ethernetgeschwindigkeit	Originale IEEE Kosten	Angepasste IEEE Kosten
10 MBit/s	100	100
100 MBit/s	10	19
1 GBit/s	1	4
10 GBit/s	1	2

Ein Port kann unterschiedliche Rollen im Spanning-Tree-Protokoll annehmen. Die möglichen Ausprägungen zeigt folgende Tabelle:

Tabelle 9.2 Portrollen

Rolle	Beschreibung
Root-Bridge	Wurzel des Spanning-Tree; besitzt die kleinste Bridge-ID des Netzes
Root Port	der Port einer Nicht-Root-Bridge mit den geringsten Pfadkosten in Richtung Root Bridge
Designated Bridge	Switch im LAN-Segment, der den Datenverkehr in Richtung Root-Bridge überträgt.

Tabelle 9.2 Portrollen (*Fortsetzung*)

Rolle	Beschreibung
Designated Port	Port der Designated Bridge in Richtung des nächsten Switches des Baumes. Er besitzt die geringsten Pfadkosten bezüglich der Verbindungssegmente.
Non-Designated Port	Port einer Nicht-Root-Bridge, der blockiert ist, d. h. keine Pakete weiterleitet

Um den logischen Spanning-Tree kennenzulernen, geht jeder Switch durch einen Ablauf von Portzuständen, die durch drei Timer beeinflusst werden. Wenn ein Switchport unmittelbar von einem Blocking- in einen Weiterleitstatus versetzt würde, bestünde die Gefahr, Topologieinformationen zu verlieren und eine Schleife zu erzeugen. Dies ist der Grund, warum fünf Portzustände unterschieden werden.

Tabelle 9.3 Portzustände

Portzustand	Beschreibung
Blocking	Verwirft Pakete; lernt keine Adressen; empfängt und verarbeitet BPDUs
Listening	Verwirft Pakete; lernt keine Adressen; empfängt, verarbeitet und überträgt BPDUs
Learning	Verwirft Pakete; lernt Adressen; empfängt, verarbeitet und überträgt BPDUs
Forwarding	Leitet Pakete weiter, lernt Adressen; empfängt, verarbeitet und überträgt BPDUs
Disabled	Verwirft Pakete; lernt keine Adressen; empfängt und verarbeitet keine Pakete

Die Zeitspanne, die ein Port in einem Zustand verweilt, wird durch Timer bestimmt. Nur die Root-Bridge kann die Einstellungen verändern. Drei Timer beeinflussen den Zustandswechsel und damit die Performance des Algorithmus:

- Der **Hello-Timer** gibt die Zeitspanne zwischen zwei BPDUs an. Er beträgt standardmäßig zwei Sekunden.
- **Forward-Delay** ist die Zeit, die im Listening- und Learning-Zustand verbracht wird. Hierfür sind 15 Sekunden vorgesehen, insgesamt für beide Stati damit 30 Sekunden.
- **Maximum Age** kontrolliert, wie lange ein Switchport die Konfigurationsinformation behält. Der Standardwert beträgt 20 Sekunden.

Wenn STP aktiviert ist, passiert jeder Switch die Zustände in der Reihenfolge: Blocking – Listening – Learning – Forwarding. Für diesen Zustandsübergang werden in der Standardkonfiguration 50 Sekunden benötigt – eine im Netzwerkbereich relativ lange Zeitspanne. Die Konvergenz als die Zeit, die benötigt wird, um den Spanning Tree im Falle des Ausfalls einer Verbindung neu zu berechnen, ist damit nicht unerheblich und ein Kritikpunkt an diesem Verfahren.

Um die Konvergenzzeit von 50 Sekunden auf unter 10 Sekunden zu verringern hat die IEEE eine neue Fassung des STP in Form des Rapid STP unter IEEE 802.1w veröffentlicht. Die Gemeinsamkeiten von STP und Rapid STP beziehen sich auf folgende Merkmale:

- Beide nutzen zur Wahl der Root-Bridge das gleiche Verfahren und die gleichen Parameter.
- Auch in die Bestimmung der Designated Ports stimmen beide Konzepte überein.
- Beide verwenden als zentrale Zustände Blocking und Forwarding.

Die Hauptunterschiede werden in Falle einer Netzwerkstörung sichtbar. Rapid STP arbeitet dabei insbesondere bezüglich der Ports nach einer veränderten Methode:

- Endgeräte werden zur Verbesserung der Konvergenzzeit unmittelbar in den Status Forwarding versetzt, wenn sie über einen physikalisch aktiven Link verfügen.
- RSTP erkennt den Pfadverlust eines Switches mit einer Vollduplex-Verbindung in Richtung Root-Bridge durch den Hello-Timer innerhalb von drei Hello-Intervallen, d. h. bei einer Standardkonfiguration innerhalb von 6 Sekunden. Damit wird ein Pfadausfall wesentlich schneller diagnostiziert.

Die Terminologie bezüglich der Portstati unterscheidet sich jedoch bei beiden Varianten. Alle Portzustände nehmen BPDUs entgegen und verarbeiten sie. Die Stati Blocking, Listening und Learning in STP leiten keine Pakete weiter. Sie sind in den RSTP-Zustand discarding übergegangen. Die folgende Tabelle gibt einen Überblick über die Differenzen:

Tabelle 9.4 RSTP und STP Portstati

Arbeitszustand	STP Status	RSTP Status	Weiterleitung in diesem Status?
Enabled	Blocking	Discarding	nein
Enabled	Listening	Discarding	nein
Enabled	Lernaning	Lernaning	nein
Enabled	Forwarding	Forwarding	ja
Disabled	Disabled	Discarding	nein

Die Philosophie hinsichtlich der Informationsgewinnung hat sich bei RSTP grundsätzlich verändert. RSTP verzichtet auf den Listeningzustand und verkürzt die Learningphase durch ein aktives Entdecken der Switchzustände. Während STP passiv auf das Eintreffen von BPDUs in beiden Phasen wartet, verhandelt RSTP mit den Nachbarswitches durch das Versenden von RSTP-Nachrichten. Diese Nachrichten versetzen einen Switch in die Lage, zu entscheiden, ob ein Interface unmittelbar in den Forwardingzustand übergehen kann. Diese Vorgehensweise verkürzt die Konvergenzzeit signifikant. Zusätzlich kennt RSTP drei neue Rollen für den Rootport und die Designated Ports. Die nachfolgende Tabelle gibt über diese Funktionserweiterung Aufschluss:

Tabelle 9.5 RSTP und STP Portrollen

RSTP Rolle	STP Rolle	Erklärung
Rootport	Rootport	Der Port jeden Nicht-Root-Switches, der in Richtung Root zeigt. In einer stabilen Topologie gibt es nur einen derartigen Port, der sich zudem im Forwarding-Status befindet
Designated Port	Designated Port	Jedes Segment verfügt über einen Designated Port. Dabei handelt es sich um einen Port im Forwarding-Zustand, der nicht in Richtung Root zeigt.
Alternate Port	-	Dieser Port bietet einen alternativen Weg zur Root-Bridge an. In einer stabilen Topologie befindet er sich im Discarding-Zustand. Er ist Bestandteil eines Nondesignated Switches
Backup Port	-	Hierbei handelt es sich um einen Port eines Designated Switches, mit einem redundanten Link zu dem Segment, für das der Switch als Designated ausgewählt wurde. Dieser Porttyp hat eine höhere Port-ID als der Designated Port und befindet sich im Discarding-Zustand.
Disabled	-	Ein Port der aus Administrationsgründen disabled ist



Noch Fragen ...? Ja ...

Gibt es vor dem Hintergrund der unbefriedigenden Konvergenz von STP Bemühungen um ein Nachfolgeprotokoll?

Ja, als Nachfolger gelten das Transparent Interconnection of Lots of Links (TRILL) und das Provider Link State Bridge (PLSB). Im April 2010 haben viele Hersteller die Unterstützung von TRILL angekündigt. Eine Alternative wäre PLSB nach IEEE 802.1(Q)aq. Dieser Standard steht in engem Zusammenhang mit IEEE 802.1 Ethernet OAM.

■ 9.3 Virtuelle LANs

Virtuelle lokale Netzwerke (VLANs) beruhen auf der Switching-Technologie und verbessern die Übertragungskapazität eines Netzwerkes durch die Teilung einer einzelnen Broadcastdomäne in mehrere Kleinere. Durch die Separation entstehen Kommunikationsinseln, deren Design mehrere Gründe und Vorteile besitzt:

- Nutzer können nach logischen Gesichtspunkten gruppiert werden, z.B. nach Zugehörigkeit zu einer Organisationseinheit. Dieses Merkmal erhöht die Flexibilität beim Design von Netzwerken.
- Der Sicherheitsaspekt kann verstärkt berücksichtigt werden, da der Datenverkehr eines VLANs von dem anderer VLANs getrennt wird.
- Bestimmte Verkehrsarten wie Sprachdaten können von anderen Übertragungsformen isoliert werden.

- Die Performance wächst, wenn ein flaches Layer-2-Netz in mehrere logische Broadcastbereiche geteilt wird.
- Broadcaststürme als Effekt einer Missfunktion in einem Netz können auf einen kleineren Bereich begrenzt bleiben.



VLAN Beispiel: Campus

Eine kleine Fachhochschule besitzt neben dem Fakultätsgebäude auf dem Campus ein Studentenwohnheim. Da die Gebäude und ihre Nutzer getrennt sind, bietet sich die Einrichtung zweier LANs an. Im Laufe der Zeit erfährt die Fachhochschule aber einen Zulauf von neuen Studenten was die Einrichtung neuer Fachbereiche nach sich zieht. Um dem Ansturm gerecht zu werden, sind neue Gebäude notwendig. In diesen Gebäuden mischen sich unterschiedliche Fachbereiche mit Studentenarbeitsplätzen, so dass die ursprüngliche Trennung nicht mehr aufrecht zu erhalten ist.

Die Lösung besteht in der Einrichtung von VLANs, die nach Fachbereichen und Studenten getrennt unterschiedliche Gebäude überspannen können. Die Gruppen bilden logische Netzwerke, die vollkommen unabhängig voneinander eine physikalische Infrastruktur benutzen.

Die Schaffung einzelner VLANs bedeutet neben den zweifelsfrei bestehenden Vorteilen aber auch, dass eine Kommunikation zwischen den Mitgliedern verschiedener VLANs nur über Router möglich ist. Der Zugriff kann durch Filter und Zugriffslisten gut gesteuert werden, was die Sicherheit weiter erhöht, aber auch den Verwaltungsaufwand wachsen lässt.

9.3.1 VLAN-Typen

Neben den strategischen Überlegungen der Einrichtung von VLANs zum Zwecke der Erhöhung der Sicherheit oder der Steigerung der Performance können auch Aspekte der Struktur der übertragenden Daten und des Managements eine Rolle spielen. Aus diesem Grund liegt eine Strukturierung von VLANs in folgende Typen nahe:

- **Daten-VLANs** sind konfiguriert, um allgemeinen Nutzerverkehr zu übertragen.
- **Black Hole VLAN** ist ein Dummy-VLAN, das dazu dient, nicht zugewiesene Ports eines Switches aufzunehmen. Alle ungenutzten Ports können auf diese Weise nicht am regulären Netzgeschehen teilnehmen, was die Sicherheit erhöht.
- **Native VLANs** ermöglichen die Kommunikation von Stationen, die keine VLAN-Fähigkeit besitzen. Sie sind einem IEEE 802.1Q Trunkport zugewiesen, der Verkehr von normalen VLANs als auch von nicht-VLANs entgegennimmt. Üblicherweise ist ein Native VLAN ausschließlich für die Aufnahme von Hubs oder Endstationen, die keine VLAN-Fähigkeit besitzen, vorgesehen.
- **Management VLAN** wird von einem Administrator definiert, um auf die Verwaltungsfunktionen eines Switches Zugriff zu haben. Standardmäßig ist dieses VLAN oft das

VLAN1. Aus Sicherheitsgründen wird dazu geraten, ein separates VLAN für diesen Zweck zu verwenden.

- **Voice VLANs** übertragen den Sprachverkehr, um eine Trennung des QoS-sensitiven Verkehrs vom herkömmlichen Datenverkehr zu erreichen.

Eine Herausforderung, die mit der modernen Konzeption von Netzwerken nach dem Client-/Server-Prinzip verbunden ist, besagt, dass Server als zentrale Diensteanbieter Mitglied mehrerer VLANs sein müssen. Dies verlangt die Anbindung an einen Trunkport des Switches.

9.3.2 Trunking

Ein Trunk ist eine Punkt-zu-Punkt-Verbindung zwischen zwei Ports unterschiedlicher Switches auf Ethernetbasis. Eine derartige Verbindung transportiert den Verkehr mehrerer VLANs, allerdings gilt die Definition nur für Fast- und Gigabit-Ethernet. Da diese Konstruktion die Möglichkeit einräumt, viele Switches zu integrieren, ergibt sich eine mögliche Ausdehnung der VLANs über das gesamte lokale Netzwerk.

Die Funktionsweise lässt sich folgendermaßen veranschaulichen: wenn ein Paket auf einem Trunk übertragen werden soll, muss diesem Paket Information über die VLAN-Zugehörigkeit hinzugefügt werden, denn ein Ethernetframe enthält keine VLAN-Information. Der entsprechende Standard IEEE 802.1Q ist für die Kennzeichnung durch das so genannte Frame-Tagging verantwortlich. Sobald ein Switch ein Paket empfängt, das für einen Trunk vorgesehen ist, versieht er das Ethernetpaket mit einem VLAN-Tag, berechnet die Prüfsumme neu und überträgt das modifizierte Paket.

Das VLAN-Tag-Feld besteht aus einem 16 Bit Ether-Typ-Feld und einem 16 Bit Tagkontrollinformationsfeld. Das Ether-Typ-Feld ist mit der Hexadezimalerkennung 0x8100 vorbelegt, während das Tagkontrollinformationsfeld in drei Subfelder unterteilt ist:

- **Priorität** kennzeichnet mit 3 Bit die Servicequalität, z. B. für den Sprachverkehr
- **Canonical Format Identifier** spezifiziert aus historischen Gründen einen Token Ring Frame
- **VAN-ID** gibt die eindeutige Kennung für ein VLAN in 12 Bit an.

Durch das Einfügen eines Tags in ein Ethernetpaket kann es zur Überschreitung der maximalen Framelänge kommen. Aus Kompatibilitätsgründen werden derartige Frames nicht weitergeleitet. Dies bedeutet, dass der Anwender seine Infrastruktur so konfigurieren muss, dass die maximal zulässige Paketlänge (MTU) unterschritten wird.

Die Abbildung zeigt den Zusammenhang zwischen Ethernet-Paket und den neu eingefügten Feldern nach IEEE 802.1Q:

Ethernetframe

Zieladresse	Quelladresse	Länge/Typ	Nutzdaten	Prüfsumme
-------------	--------------	-----------	-----------	-----------

Ethernetframe mit eingefügtem Tag

Zieladresse	Quelladresse	Tag	Länge/Typ	Nutzdaten	Prüfsumme
-------------	--------------	-----	-----------	-----------	-----------

Aufbau des Tags

Type (16 Bits) 0x8100	Priorität 3 Bits	Flag 1 Bit	VLAN-ID 12 Bits
-----------------------	------------------	------------	-----------------

Bild 9.6 IEEE 802.1Q und Ethernet

9.3.3 VLAN-Management

Ein Switchport kann auf zwei Arten konfiguriert werden, um ihm eine VLAN-Zugehörigkeit zuzuweisen:

- Bei einem **statischen VLAN** wird der Port manuell über eine Befehlssequenz der Administrationsoberfläche einem VLAN zugeordnet. Diese Methode ist die am häufigsten genutzte.
- Bei einem nicht sehr weit verbreiteten **dynamischen VLAN** wird die Mitgliedschaft eines Ports in einem VLAN über einen VLAN Membership Policy Server (VMPS) gesteuert. Basis ist die Quell-MAC-Adresse. Der Vorteil dieses Konzeptes ergibt sich im Falle eines Umzuges, wenn ein Host von einem Switchport an einen anderen Switchport eines neuen Netzes wechselt. Der Switch weist dann dynamisch dem neuen Port das entsprechende VLAN zu.

Eine der wichtigsten Aufgaben in einer VLAN-Umgebung ist die konsistente Verwaltung der Konfiguration über mehrere Switches hinweg. Um nicht alle Switches einzeln konfigurieren zu müssen, hat Cisco das **VLAN Trunk Protocol (VTP)** entwickelt, das ein zentrales Management erlaubt. Dazu überträgt ein VTP-Server die Definition auf alle Mitglieder. Innerhalb einer VTP-Domäne können die Geräte in drei unterschiedlichen Modi arbeiten: als VTP-Server, als VTP-Client oder im transparent Modus.

1. **VTP-Server:** dieses Device ist die Wurzel der Domäne. Sie kann als einzige Station VLANs hinzufügen, löschen oder umbenennen. Um die Konfiguration konsistent zu halten, sendet sie periodisch Konfigurationsinformationen und eine Revisionsnummer. Diese Nummer wird von jedem Mitglied überprüft. Bei Nichtübereinstimmung liegen unterschiedliche Konfigurationsstände vor.
2. **VTP-Client:** dieser VTP-Typ kann keine VLANs hinzufügen, löschen oder umbenennen. Er erhält seine VLAN-Konfiguration vom VTP-Server. Um ein neues VLAN zu integrieren, muss dieses dem Server hinzugefügt werden, der es dann in der VLAN-Domäne bekannt macht.
3. **VTP-transparent:** Geräte dieses Typs leiten VTP-Nachrichten an Clients und Server weiter, verarbeiten sie aber nicht.

Zur Adressierung nutzt VTP eine reservierte Multicastadresse. VTP-Nachrichten können drei Kategorien angehören:

1. **Summary:** diese Nachrichten werden vom Server als auch vom Client alle fünf Minuten oder nach einem Konfigurationswechsel gesendet. Sie enthalten Basisinformationen und die Revisionsnummer.
2. **Subset:** diese Message wird verwendet, um detaillierte VLAN-Informationen zu liefern. Sie sind eine Antwort auf Konfigurationsänderungen oder Requests.
3. **Request:** diese Nachrichtenform wird vom Client an den Server in folgenden Fällen geschickt: Wechsel des Domänennamens, eine Subset-Nachricht wird vermisst, der Switch wird neu gestartet oder der Switch hat eine abweichende Revisionsnummer erhalten.

In heutigen LANs auf Switch-Basis entspricht jedes VLAN einem eindeutigen IP-Subnetz. Haben zwei Hosts im gleichen VLAN unterschiedliche Subnetzadressen, können sie nicht miteinander kommunizieren. Dieser Fehlertyp ist nicht ungewöhnlich, aber leicht zu korrigieren.

■ 9.4 Zusammenfassung

Ein Switch als Kopplungselement der OSI-Schicht 2 ist in der Lage, die MAC-Adressen zu interpretieren, um die Datenpakete gezielt weiterzuleiten. Switches haben Bridges und Hubs vollständig vom Markt verdrängt. Sie eignen sich zur Aufteilung eines LANs in Anwendergruppen nach logischen und organisatorischen Gesichtspunkten. Die Realisierungen unterscheiden sich jedoch erheblich, was nicht nur mit der Ausstattung, der Portdichte oder der Technologie zusammenhängt, sondern vornehmlich in der Architektur begründet liegt. Hochleistungsswitches beruhen auf der Matrixarchitektur und sind meist im oberen Preissegment angesiedelt.

Durch ihre Realisierung in Hardware und ihre Funktionalität sind Switches zu einem bedeutenden Element des Netzwerkdesigns geworden. Mit der Möglichkeit von Vollduplexverbindungen, einer hohen Anschlussdichte und einer Wire-Speed-Option bieten sie hinsichtlich Bandbreite und Skalierung einen flexiblen und dynamischen Aufbau eines Netzwerkes. Zusätzlich lassen sich organisatorische Gegebenheiten durch VLANs auf die jeweiligen Unternehmensstrukturen zugeschnitten umsetzen, was die Flexibilität weiter erhöht und die Sicherheitsanforderungen stärkt.

■ 9.5 Wissensüberprüfung

1. Beschreiben Sie die drei verschiedenen Typen von Switch-Architekturen.
2. Warum werden an den Aus- und Eingangsports von Switches Puffer benötigt?
3. Ist FragmentFree-Switching auch bei asymmetrischen Switching möglich? Begründen Sie Ihre Ansicht.
4. Welchen Effekt besitzen Switches auf Kollisionsdomänen?

5. Welches Gerät ermöglicht die höchste Transferrate: HUBs, Switches oder Router?
6. Store-and-Forward-Switches weisen die geringste Latenzzeit auf. Stimmen Sie dieser Behauptung zu?
7. Beschreiben Sie die Modified Cut-Through-Methode.
8. Was unternimmt ein Switch, wenn ein Paket eintrifft, dessen Zieladresse nicht in der Adresstabelle vorhanden ist.
9. Switches werden nur im Ethernet-Umfeld eingesetzt. Können sie dieser Einschätzung zustimmen?
10. Variiert bei dem Store-and-Forward-Prinzip die Übertragungszeit mit der Rahmengröße?

10

Layer-3 – Geräte, Protokolle und Konzepte

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Wie ist die Funktionsweise von Routern?
- Was ist der Inhalt einer Routingtabelle?
- Wie läuft der Routingprozess ab?
- Welche Routingmethoden existieren?
- Wo liegen Unterschiede zwischen Routern und Switches?
- Welche Routingprotokolle haben sich etabliert?

Kapiteleinführung

Die Existenz von Intranets, die organisatorische Aufteilung in lokale Arbeitsgruppen oder die Nutzung des Internet für multimediale Inhalte haben die Unternehmensnetze zu Infrastrukturen werden lassen, die unterschiedlichste Anwendungsszenarien berücksichtigen müssen. Hohe Verzögerungszeiten im Netzwerk würden dazu führen, dass steigende Antwortzeiten die Anwender verstimmen. Router als die wesentliche Kopplungskomponente neben Switches sind deshalb im besonderen Maße gefordert, ihre Funktionalität in Geschwindigkeit umzusetzen und den Endnutzer transparent und schnell zu bedienen.

■ 10.1 Router



Router

Router verknüpfen zwei Netzwerke über die Vermittlungsschicht 3 des OSI-Referenzmodells also auf der Grundlage von IP-Adressen. Die Weiterleitung der Pakete beruht dabei auf Einträgen in der Routingtabelle.

Da jedes ankommende Datenpaket bis zur Schicht 3 interpretiert wird, eignen sich Router zur Verbindung unterschiedlicher LAN-Technologien wie Ethernet und Token-Ring und zur Interpretation logischer Netzadressen. Ein Router kann das Protokollformat der

Schicht 3 ändern, wenn er heterogene Netzwerke miteinander verknüpft, die darunter liegende LAN-Technologie ist für ihn jedoch transparent. Dennoch benötigt er für eine korrekte Paketweiterleitung Kenntnisse und Umsetzungsmöglichkeiten für die Protokolle der Schicht 2.

10.1.1 Bedeutung

Traditionelle Router leiten Pakete auf Grundlage der Adressen der OSI-Schicht 3 weiter und beziehen ihre Bedeutung aus dieser Position und einiger weiterer hinzukommender Eigenschaften:

- Router dehnen ein Netz hinsichtlich Länge und Stationszahl aus.
- Router verbinden unterschiedliche Subnetze. Die Notwendigkeit hierfür entsteht bei IP-basierten Netzen aus den Beschränkungen des IP-Adressschemas.
- Router gestatten die Handhabung mehrere Protokollstacks und erlauben damit auch eine Protokollumsetzung, z. B. von IP nach IPX (Protokoll der Schicht 3 von Novell) und umgekehrt.
- Router steuern den Netzzugang. Da sie die Protokolle der Schicht 3 interpretieren, können sie Filter bzw. Zugriffslisten zum Schutz vor unberechtigtem Zugriff konfigurieren. Mehrere Einschränkungen sind denkbar:
 - **nach Richtung:** Ein Router kann Ein- und Ausgangsverbindungen beschränken, so dass z. B. alle Mitarbeiter einer Abteilung eines Unternehmens mit allen anderen Abteilungen kommunizieren können, aber niemand das Unternehmensnetz betreten kann.
 - **nach Protokoll:** Ein Router kann den FTP- oder Telnet-Verkehr unterbinden, aber den SMTP-Transfer für E-Mails zulassen.
 - **nach Adresse:** Internet-Benutzern kann der Zugriff auf WWW- und FTP-Server einer Firma eingeräumt, aber auf weitere Ziele untersagt werden.
 - **nach Datum/Uhrzeit:** Der Zugriff kann auf Wochentage und Tageszeiten begrenzt werden.

Wie der Name Router nahelegt, besteht seine Hauptaufgabe darin, einen Leitweg für Pakete durch das Netzwerk zu bestimmen und das Paket selbst auf diesen Pfad zu bringen. Die aktive Paketweiterleitung besteht aus dem Auswahlprozess des Weges aus Alternativen. Dazu wird die Routingtabelle auf Einträge nach der Ziel-IP geprüft. Die Prüfung kann zu drei Ergebnissen führen:

1. Das Zielnetz ist nicht erreichbar: in der Routingtabelle gibt es keinen Eintrag, der das gewünschte Netz identifiziert und es existiert keine Defaultangabe. In diesem Fall wird das Paket verworfen.
2. Das Zielnetz ist über einen anderen Router erreichbar: die Routingtabelle enthält einen Eintrag für das Zielnetz. Die Prüfung ergibt den nächsten Knoten auf dem Weg zum Ziel.

3. Das Zielnetz ist direkt an den Router angeschlossen: in diesem Fall ist die Ermittlung der zugehörigen MAC-Adresse aus dem Hostanteil der IP-Adresse mit Hilfe der ARP-Tabelle notwendig, um das Paket der Zielstation direkt zustellen zu können. Enthält die ARP-Tabelle keinen entsprechenden Eintrag, muss der Router über das ARP-Discovery die MAC-Adresse ermitteln.

In den letzten beiden Fällen schließt der Router den Prozess durch die Weiterleitung des Paketes an das entsprechende Routerinterface ab. Dazu wird das IP-Paket gemäß des Protokolls der Schicht 2 in eine Transporteinheit eingepackt. Der Typ dieser Transporteinheit leitet sich aus der Technologie des Interfaces ab und kann, z. B. für ein serielles Interface ein PPP-Frame sein.

Um die Paketweiterleitung zu beherrschen, muss der Router mehrere Funktionen ausführen können:

- die Zieladresse identifizieren
- Nachbarrouter kennen, von denen er weitere erreichbare Netzwerke lernt
- den besten Weg zu entfernten Netzen bestimmen
- die Weginformation speichern und aktualisieren.

Um diese Aufgaben umzusetzen, benötigt er:

- einen Prozessor, um Zieladressen zu prüfen und Pakete vom Eingangs- zum Ausgangsport zu transportieren
- einen Routingalgorithmus, um seine Nachbarn zu erkennen und den besten Weg zu bestimmen
- eine Routingtabelle, um die Wegeinformation zu speichern.



Routingtabelle

Die Routingtabelle enthält Angaben zu möglichen Wegen, zum „optimalen“ Weg, zum Status, zur Metrik, d. h. dem Bewertungsmaßstab des Weges und zum Alter. Grundlage ist die Verknüpfung der Ziel-IP-Adresse mit einer Richtungsangabe in Form des Folgerouters und des Interfaces über den der Paketstrom zu lenken ist.

Die Geschwindigkeit der Paketweiterleitung hängt auch von der Anzahl der Einträge ab. Je mehr Einträge zu prüfen sind, desto mehr sinkt die Vermittlungsgeschwindigkeit, so dass ein wichtiger Aspekt des Netzdesigns darin besteht, die Tabellengröße zu minimieren.

Netzwerk	Interface	Nächster Knoten	Metrik	Alter	Protokoll
198.113.151.0	Ethernet0	192.150.42.177	[170/304793]	02:03:50	D
198.113.178.0	Ethernet0	192.150.42.177	[110/9936]	02:03:50	O
192.168.96.0	Ethernet0	192.150.42.177	[120/3]	00:00:20	R
192.168.97.0	Ethernet0				C

Bild 10.1 Routingtabelle

Die Routingtabellenprüfung ist ein wesentlich komplexerer Vorgang als die Prüfung der Tabelle eines Switches. Der Grund hierfür liegt darin, dass die IP-Adresse eine flexible Einteilung zwischen Netz- und Hostteil besitzt und damit Klassen oder Hierarchien abbilden kann. Die Routingtabellenprüfung erstreckt sich nur auf den Netzteil der Adresse, der auf Grund der Struktur unterschiedlich lang sein kann. Anders als ein Switch, der einen exakten Match auf eine Adresse fester Länge ausführt, sucht ein Router den längsten übereinstimmenden Part des variabel langen Netzteils der IP-Adresse.



Um dem Benutzer Sicherheit durch Redundanz bezüglich des Ausfalls des Default Routers zu bieten, wurde das Virtual Router Redundancy Protokoll (VRRP, RFC 2338) entwickelt. Die Grundidee besteht darin, einen virtuellen Router zu definieren und dessen IP-Adresse als Default Router Adresse auf den Endstationen zu konfigurieren.

10.1.2 Routing-Ablauf

Die Grundlage des Routing besteht in der Versendung und Zustellung von Paketen. Diese Idee lässt sich an einem Diagramm mit zwei Routern und mehreren Endstationen veranschaulichen:

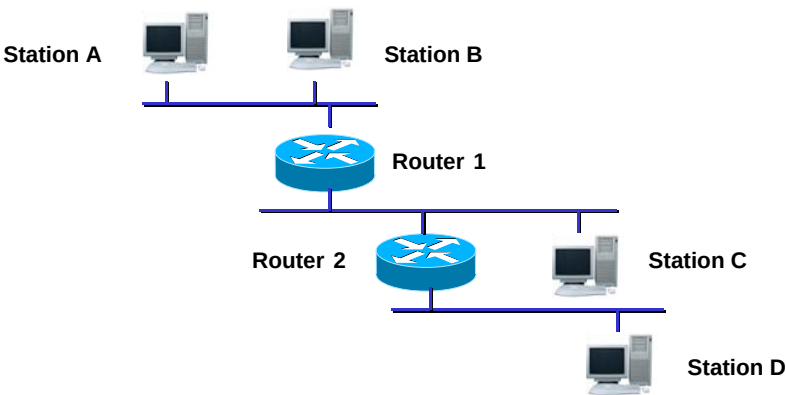


Bild 10.2 Netz mit Routern

Zur Paketzustellung an seine Kommunikationspartner nutzt Station A unterschiedliche Wege:

- **Zielstation B:** Da sowohl Quelle als auch Ziel im gleichen Segment liegen, prüft A zunächst den ARP-Cache auf die Existenz der Hardwareadresse von B. Ist kein Eintrag vorhanden, bringt A die Adresse durch einen ARP-Request in Form einer Broadcast in Erfahrung. Für diesen Vorgang ist keiner der beiden Router vonnöten.
- **Zielstation C:** Station A erkennt, dass das Ziel nicht im eigenen Subnetz liegt. Daraufhin prüft A seine Routingeinträge und findet Router 1 als Defaulteintrag. Unter Nutzung von ARP identifiziert A die Hardwareadresse des Interfaces von Router 1, der das Paket an die direkt angeschlossene Station C weitergibt.
- **Zielstation D:** Station A folgt dem gleichen Verfahren wie bei der Sendung an Station C. Sobald die Pakete an Router 1 adressiert sind, wird ihre IP-Adresse in der Routingtabelle von Router 1 geprüft und Router 2 als nächste Station auf dem Weg zum Ziel identifiziert.

Der Routingprozess ist für die Endstationen nicht transparent: Eine Ethernet-Station, die mit einer anderen Ethernet-Station jenseits des Routers kommunizieren möchte, adressiert ihr Ethernetpaket an den Router und nicht an den Zielrechner. Der Router entfernt den Ethernet-Header und prüft die darunter liegende Information der Schicht 3, um das Paket dann auf der Grundlage seiner Routingtabelle in Richtung Ziel weiterzuleiten. Im Einzelnen lassen sich die Phasen des Prozesses, das die obigen Schritte des Beispiels präzisiert, wie folgt beschreiben:

1. Der Quellrechner trägt in das zu übertragende Paket als Ziel-MAC-Adresse die Adresse des Interfaces des nächsten Routers auf dem Weg zum Ziel ein, sowie seine MAC-Adresse als Quelle. In der logischen Adresse stehen die Quell-IP und Ziel-IP-Adresse. Zuvor überprüft der Rechner allerdings seine IP-Adresse mit der Subnetzmaske des Empfängers, um festzustellen, ob beide Stationen dem gleichen Subnetz zugeordnet sind. Falls der Zielrechner zum gleichen Subnetz gehört, ist kein Routing notwendig. Die Zielstation wird allein durch den ARP-Prozess ausfindig gemacht. Im verbleibenden Fall ermittelt der Quellhosts die MAC-Adresse des Routerinterfaces. Im Allgemeinen existiert hierfür ein Eintrag. Falls nicht, muss die entsprechende Adresse über ARP festgestellt werden.
2. Der nächste Netzknoten, d. h. der erste Router auf dem Weg zum Ziel, prüft das empfangene Paket auf Zulässigkeit. Dies ist möglich, da Router nach dem Store-and-Forward-Prinzip arbeiten und das gesamte Paket zur Bearbeitung einlesen. Daher können sie feststellen, ob eine Zugriffsberechtigung besteht.
3. Im anschließenden Schritt wird die MAC-Adresse auf Übereinstimmung mit derjenigen des Routerinterface geprüft und im positiven Fall entfernt.
4. Im Anschluss daran wird die IP-Ziel-Adresse mit der Routingtabelle verglichen, der einem Tabelleneintrag entsprechende Port entnommen und das Paket an den Ausgangsport weitergeleitet. Wird kein Eintrag gefunden, wird die Defaultroute verwendet, ist hierfür kein Eintrag vorhanden, wird das Paket verworfen.

- 5. Am Outputport wird die Ziel-MAC-Adresse des nächsten Netzknotens eingetragen und der CRC-Wert generiert, so dass ein neuer Paket-Header entsteht. Die logischen Adressen bleiben unverändert, allerdings wird das Time to Live-Feld des IP-Headers dekrementiert.
- 6. Der letzte Router auf dem Weg zum Ziel erkennt anhand seiner Routingtabelle, dass die Ziel-IP-Adresse zu einem direkt verbundenen Netzwerk gehört. Zur Ermittlung der genauen MAC-Adresse leitet der Router den ARP-Prozess mit der Ziel-IP-Adresse ein, sofern kein Eintrag im ARP-Cache vorliegt.
- 7. Die Zielstation empfängt letztlich den an sie adressierten Ethernet-Rahmen, der als Ziel-MAC-Adresse die Stationsadresse und als Quell-MAC-Adresse die des letzten Routers enthält. Die logischen Adressen bleiben auf dem gesamten Weg unverändert.

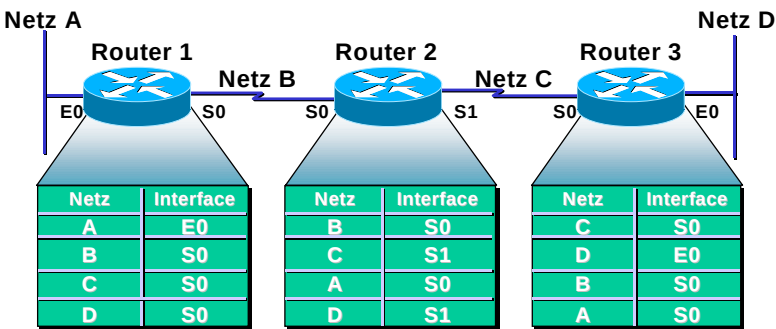


Bild 10.3 Routingablauf

Auf dem Weg von der Quelle zum Ziel passt jeder passierte Knoten die MAC-Adressen an. Die IP-Adressen hingegen bleiben unverändert, damit Empfänger und Sender jederzeit zu identifizieren sind.

10.1.3 Routing-Methoden

Routing

Routing als die Wahl eines „optimalen“ Weges ist eine Basiseigenschaft jeden Netzwerkes. Dabei ist das Routing auf die Aktualität der Information in der Routingtabelle angewiesen. Diese wird durch den Austausch der gesamten Routingtabelle zwischen Nachbarn oder durch Informationen über die Verbindung zwischen ihnen erreicht.

Erst die Möglichkeit, gezielt die gewünschte Station des Netzes zu erreichen, gestattet die Nutzung von Anwendungen. Dazu schafft Routing:

- die Verbindung zwischen unterschiedlichsten Netzen, seien es private Netze, Unternehmensnetzwerke oder das Internet.
- den Anschluss von Remote-Usern über sehr unterschiedliche Techniken wie DSL, WiMAX, ISDN oder Frame Relay.

Um das Grundkonstrukt der Routingtabelle jedoch mit Leben füllen zu können, bedarf es Einträge bezüglich der erreichbaren Netze. Router können Wege auf drei verschiedene Arten lernen und mit diesem Wissen dann die Routingtabelleneinträge erzeugen:

- **direkt verbundene Netze:** Sie werden automatisch in eine Routingtabelle übernommen, wenn ein Interface mit einer IP-Adresse konfiguriert wird.
- **statische Routen:** Diese Wege werden durch einen Administrator eingetragen. Sie dienen zum einen der Sicherheit, sind andererseits aber nur verwaltbar, wenn ihre Zahl begrenzt ist, d. h. die Skalierbarkeit ist für diese Methode ein limitierender Faktor.
- **dynamische Routen:** In diesem Fall lernen Router erreichbare Netze durch ein Routingprotokoll, das Informationen über das Netzwerk und seine Teilnehmer sammelt und an die Mitglieder verteilt.

Die Routingtabelle ist in ihrer Funktion einem Adressbuch vergleichbar, in dem nachgeschlagen wird, ob eine Ziel-IP-Adresse bekannt ist, d. h. ein Weg zu diesem Netz existiert.

Da ein Router nicht für alle IP-Adressen hierfür eine Antwort weiß, muss es eine Standardvorgabe geben. Diese wird in Cisco-Routern als Last Resort bezeichnet.



Praxis: Routingtabelle

Der Befehl **show ip route** zeigt die Routingtabelle eines Cisco-Routers. Dabei zeigt der erste Buchstabe des Eintrags, wie der Router den Pfad erhalten hat: in diesem Fall durch direkt verbundene Netzwerke und statische Einträge. Der zweite Eintrag verweist auf das Zielnetz und der letzte Eintrag gibt an, über welches Interface dieses Netz erreicht wird. Ausgewählt ist durch die Markierung eine statische Route.

In diesem Beispiel fehlen dynamische Routen. Sie würden z. B. mit einem R für RIP oder einem O für OSPF eingeleitet. Auch eine Defaultroute ist hier nicht festgelegt.

R1#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

```
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.12.0/24 is directly connected, Serial2/0
C 192.168.13.0/24 is directly connected, Serial3/0
S 192.168.23.0/24 [1/0] via 192.168.12.2
R1#
```

Durch die Komplexität heutiger Netzinfrastrukturen steigt die Bedeutung dynamischer Routingverfahren beträchtlich. Das Internet wäre ohne ihre Existenz nicht denkbar. Dennoch haben sich statische Routen behaupten können, insbesondere in kleineren Umgebungen, die nur über wenige dezidierte Verbindungen verfügen. Eine Gegenüberstellung beider Konzepte zeigt folgende Tabelle:

Tabelle 10.1 Vergleich dynamisches – statisches Routing

Merkmal	Dynamisches Routing	Statisches Routing
Topologiewechsel	Automatische Erkennung und Aktualisierung, d. h. automatisches Re-Routing	Administratoreingriff notwendig, d. h. kein Re-Routing
Skalierbarkeit	Ausgelegt für komplexe Topologien, unbegrenzt erweiterbar	Nur für kleine Netzwerke angemessen, begrenzte Ausbaufähigkeit
Sicherheit	Unsicher	Tendenziell sicherer als die dynamische Variante
Vorhersage des Weges	Weg ist von der aktuellen Topologie abhängig	Stets der gleiche Weg zum Ziel



Große Netze mit mehreren Subnetzen und Routern können auch in LAN-Umgebungen den Aufwand des Einrichtens von Routingprotokollen rechtfertigen. Existieren mehrere Wege zum gleichen Ziel, könnten zwar statische Routen Pakete stets auf einem Weg zum Empfänger leiten, ein solches Konzept würde aber nicht auf Änderungen im Netz reagieren können.

10.1.4 Unterschiede zwischen Routern und Switches

Dadurch, dass Switches und Router auf unterschiedlichen Ebenen des OSI-Referenzmodells arbeiten, bestehen zwangsläufig Unterschiede zwischen ihnen.

- Router bestimmen den Weg, den ein Paket von der Quelle zum Ziel wählt, bezüglich einer Metrik. Switches kennen diese Möglichkeit der Paketlenkung nicht und sind durch den Spanning-Tree Algorithmus begrenzt.
- Die Zahl der durch Router unterstützten Knoten ist unbegrenzt, da der Adressraum durch Bereichs- oder Domänenbildung hierarchisiert ist. Switches besitzen demgegenüber nur ein flaches Adressschema, das keine logische Klassifikation erlaubt. Die Zahl der mit ihnen verbundenen Stationen hängt von der Portdichte und den Kaskadierungsmöglichkeiten ab.
- Router bilden eine Barriere gegen Broadcasts, Switches hingegen lassen Broadcasts passieren.
- Router fragmentieren und setzen Datenpakete wieder zusammen. Switches verfügen nicht über diese Fähigkeit, sondern werfen fehlerhafte Pakete, ohne den Sender hierüber zu informieren.

- Router leisten eine Überlastkontrolle in dem sie die sendende Station zu einer Reduktion der ausgesendeten Pakete veranlassen, Switches hingegen kennen keine Datenflusskontrolle.

Tabelle 10.2 Vergleich Router - Switch

Merkmal	Switch	Router
Wegewahl	anhand der physikalischen MAC-Adresse	anhand der logischen Netzwerkadresse
Protokolltransparenz bezüglich Schicht 3	ja	Router gehören einer bestimmten Protokollfamilie an oder sind multi-protokollfähig
Adressierung	direkte Adressierung der Zielstation auf der Basis eines eindeutigen herstellerabhängigen Adressbestandes	indirekte Adressierung auf der Basis eines hierarchischen globalen Schemas
Adresstabellen	Adresstabellen nach dem Learn-and-stay-Verfahren	Routingtabelle mit Subnetzadressen und Zuordnung zwischen logischer Netzwerk- und physikalischer MAC-Adresse
Broadcastunterdrückung	nein	ja
Überlast-Feedback	nein	ja
redundante Wege	nein	Router kennen die Netztopologie und wählen den optimalen Weg gemäß einer Metrik



Mit dem Kommando *tracroute* unter Linux bzw. *tracert* unter Windows erhält der Nutzer eine Liste aller passiertten Knoten auf dem Weg von der Quelle zum Ziel.



Noch Fragen ...? Ja ...

Muss ein Rechner immer mit einem Switch verbunden werden?

Im Prinzip ja. Router vermitteln zwischen Netzwerken und besitzen daher nur an den Endpunkten Switches als Teilnehmer.

Diese Regel gilt nicht für DSL-Router?

Richtig; es gibt Switches die Routerfähigkeiten besitzen und Router die Switchaufgaben übernehmen. Der Unterschied zum DSL-Router ist nicht nur die Software, sondern auch die Prozessorleistung. Hochspezialisierte Router besitzen besonders leistungsfähige Prozessoren.

Sind Router bereits ab Werk konfiguriert?

Bei der Auslieferung besitzen die Router keinerlei Konfiguration. Das bedeutet, dass alle Einstellungen individuell vorgenommen werden müssen.

Können Router mehrere Arten von Schnittstellen besitzen?

Ja, Router können verschiedene Technologien wie Ethernet, Frame Relay, ATM oder DSL miteinander verbinden.

Kann ein einzelner Router Interfaces für unterschiedliche Medien unterstützen?

Ja, Glasfaser, Kupferkabel oder drahtlose Netzwerke können gemeinsam an einem Router vorkommen.

■ 10.2 Routing

Das Problem der Wegewahl tritt in allgemeinen „vermaschten“ Netzstrukturen auf, da nicht eindeutig deterministisch zu entscheiden ist, auf welchem Weg ein Datenpaket sein Ziel erreichen soll. Die Wahl eines passenden „optimalen“ Routingalgorithmus ist daher für die Leistungsstärke eines Netzes von entscheidender Bedeutung. Schlechte Verfahren bewirken in erster Linie eine Verlängerung und damit eine Verteuerung der Übertragung. Die meisten Algorithmen arbeiten tabellengesteuert. Wesentliches Element ist hierfür die Routingtabelle jedes Knotens, die für jeden möglichen Zielknoten Wegeinformation bereithält. Routingalgorithmen müssen also einerseits die Entscheidung bezüglich eines bestimmten Pfades zum Ziel treffen, andererseits aber ihre hierfür erforderliche Entscheidungsbasis – die Routingtabelle – ständig aktualisieren, wollen sie einen optimalen Leitweg bei geringer Systembelastung bestimmen. Der Begriff „optimal“ ist in diesem Kontext allerdings interpretationsbedürftig. Bewertungskriterien für Netzverbindungen können durch unterschiedliche Merkmale ausgedrückt werden:

- Hop Counts – Anzahl passierter Knoten
- Verzögerung – Variation in der zeitlichen Zustellung der Pakete
- Kosten – Bandbreite der Verbindung
- Zuverlässigkeit – Bitfehlerrate jeder Verbindung

10.2.1 Bedeutung

Routingalgorithmen sollten so konzipiert sein, dass sie die Bewertungskriterien des Weges für den Benutzer transparent erfüllen. Steht der Gesichtspunkt der Gebührenminimalität an oberster Stelle der Präferenzskala, ist der optimale Weg nicht notwendig der geographisch kürzeste, da die Tarifierung der Einzelstrecken berücksichtigt wird; spielt der hohe Datendurchsatz die wichtigste Rolle, kommt der Anzahl der Teilstrecken, den so genannten HOPS eine große Bedeutung zu. Diese unterschiedlichen Anforderungen unterstreichen einerseits die Qualität und andererseits die Aktualität der Einträge in der Routingtabelle. So wünschenswert es ist, sofort einen Überblick über die dynamischen Veränderungen des Gesamtnetzes zu haben, so schwierig ist dieses Ideal durch die permanente Erfassung von Netzdaten zu erreichen. Eine gewaltige Netzbelastung durch die Übertragung einer Fülle von Statusinformationen wäre die unerwünschte Folge. Eine ereignisgesteuerte

ad-hoc Aktualisierung ist deshalb praktisch undurchführbar. Andererseits wächst mit der Länge des Aktualisierungsintervalls die Gefahr, dass die getroffene Wegentscheidung auf veralteten Statusinformationen beruht. In der Praxis muss also ein geeigneter Kompromiss zwischen Routingeffizienz und -aktualität getroffen werden.

10.2.2 Routingprotokolle – allgemeine Klassifizierung

Routingkonzepte können aufgrund ihrer Charakteristik in unterschiedliche Gruppen eingeteilt werden:

- Interior und Exterior Gateway Protokolle
- Distance und Link-State Protokolle
- Classless und Classful Protokolle

Tabelle 10.3 Klassifikation der Routingprotokolle

Interior Gateway Protokolle			Exterior Gateway Protokolle
	Distance Vector	Link-State	Path Vektor
Classful	RIP		
Classless	RIPv2	OSPF	BGPv4

Die erste Unterscheidung richtet sich an autonome Systeme. Zu den autonomen Systemen gehören Netzwerke des gleichen Administrationsbereiches. Dies gilt vor allem für große Unternehmensnetze und die Netze von Internet Service Providern. Für ihre Administration werden **Interior Gateway Protokolle** benötigt, die ein Routing innerhalb dieser Netze ermöglichen. Soll zwischen diesen Inseln vermittelt werden, kommen **Exterior Gateway Protokolle** zum Einsatz.

Interior Gateway Protokolle (IGP) tauschen also Informationen zwischen Routern eines einzigen autonomen Systems aus. Zu ihren bekanntesten Vertretern gehören:

- das Routing Information Protokoll (RIP)
- das Open Shortest Path First Protokoll (OSPF)

Beide Protokolle lassen sich durch ihre Zugehörigkeit zu einer weiteren Teilklasse differenzieren. Das RIP-Protokoll lässt sich den Distance-Vector-Algorithmen zuordnen, während OSPF in die Klasse der Link-State-Protokolle fällt.

Distance-Vector-Protokolle bestimmen die Erreichbarkeit durch einen Vektor aus Entfernung und Richtung. Die Metrik wird in der Anzahl zu passierender Knoten ausgedrückt. Für die Wegbestimmung wird üblicherweise der Bellman-Ford-Algorithmus verwendet.

Sobald Änderungen der Netzwerktopologie bekannt werden, spiegeln sich diese in Update-Nachrichten wider. Entdeckt ein Router eine unterbrochene Verbindung oder den Ausfall seines Nachbarn, berechnet er die betroffenen Wege neu und verschickt Änderungsmeldungen an alle erreichbaren Knoten. Jeder Router, der eine derartige Meldung erhält,

passt seine Routingtabelle an und propagiert diese Änderung. Das Verfahren ist „optimistisch“ in dem Sinne, gute Nachrichten, d.h. neue kürzere Wege, schnell bekannt zu machen, schlechte Nachrichten hingegen lange zu verheimlichen. Der Grund hierfür liegt darin, dass die Netzknoten ihre eigene Routingtabellen in kurzen Intervallen als Broadcast an alle anderen Netzknoten versenden. Die Entfernung zu anderen Knoten wird dabei relativ zur eigenen Routingtabelle angegeben, so dass jeder Knoten eine individuelle Anpassung der Routinginformation vornehmen muss. Dabei können folgende Fälle auftreten:

- der versendende Router besitzt eine kürzere Entfernung zum Ziel
- der versendende Router kennt ein Ziel, das dem Empfänger noch unbekannt ist
- die Entfernung vom sendenden Router zu einem Ziel, dessen Pfad über den empfangenen Router führt, hat sich geändert.

Diese Form, ein Abbild der Netztopologie herzustellen, besitzt mehrere Nachteile:

- Ändern sich die Netzgegebenheiten sehr schnell durch einen Verbindungsausfall, erscheint das Netzabbild in den Routingtabellen wenig stabil, da die Konvergenzgeschwindigkeit gering ist.
- Die Anpassung erfolgt über den Austausch der gesamten Routingtabelle in regelmäßigen Zeitintervallen.

Distance-Vector-Protokolle nutzen als alleiniges Entfernungsmaß die Anzahl der Knoten. Sie berücksichtigen damit keine weiteren Merkmale wie Kosten oder Geschwindigkeit. Die größte Herausforderung dieser Klasse von Algorithmen besteht darin, Instabilität zu verhindern, die Konvergenz gegen einen stabilen Zustand in einer angemessenen Zeit zu sichern und die Skalierbarkeit des Netzes durch neue Vermittlungsknoten zu gewährleisten.

Link-State-Protokolle gelten als Alternative zu Distance-Vector-Ansätzen und versuchen demzufolge einige ihrer Schwächen auszugleichen. Im Gegensatz zu Distance-Vector-Protokollen, die nur eine eingeschränkte Sicht auf die Netztopologie haben, haben die Router bei Link-State-Protokollen einen vollständigen Überblick über den Aufbau des Netzes.

- Netze werden dazu in Bereiche so genannte Areas aufgeteilt.
- Alle Router innerhalb einer Area verfügen über die gleiche Datenbasis. Diese Datenbasis beschreibt die vollständige Topologie der Area.
- Jeder Router benutzt diese Datenbasis, um den optimalen Pfad abzuleiten und diesen in seine Routingtabelle zu stellen. Die Bestimmung des Weges beruht auf dem Shortest Path First Algorithmus von Dijkstra.
- **Hello-Pakete** stellen den Kontakt zu den Nachbarroutern her. Unter Ausnutzung des Multicast-Mechanismus werden alle Nachbarrouter angesprochen.

Zur Aktualisierung der Datenbasis verwendet das Link-State-Protokoll keine periodischen Updates, sondern sendet nur bei einem Topologiewechsel ein Link-State-Update. Dieser Bedarf entsteht, wenn:

- ein neuer Router entdeckt wird
- ein Router seinen Dienst einstellt
- die Kosten einer Verbindung sich ändern
- periodisch alle 30 Minuten.

Link-State-Pakete werden zum Informationsaustausch benötigt. Auf diese Informationen stützt sich der Shortest Path First Algorithmus und bildet für jeden Router individuell den optimalen Routingbaum. Als Metrik zur Erstellung der Routingtabelle kommt dabei der Kostengesichtspunkt in Form der Geschwindigkeit des Interfaces zum Tragen.

Ein Hauptunterschied zu Distance-Vector-Protokollen liegt darin, dass Link-State-Protokolle den Verbindungszustand als Bestimmungsgrundlage des kürzesten Weges austauschen und nicht die gesamte Routingtabelle. Durch dieses Vorgehen werden wesentlich weniger Netzressourcen benötigt.

Als dritter konzeptioneller Unterschied von Routingprotokollen dient die Behandlung der Subnetzinformation. **Classful Protokolle** reichen die Informationen über die Strukturierung von IP-Netzen nicht weiter. Die ersten für das Internet entworfenen Protokolle wie das Routing Information Protocol (RIP) gehörten zu dieser Klasse. Bei einer strikten Orientierung IP-basierter Netzstrukturen an den Klassen A, B und C bestand keine Notwendigkeit dafür, diese Informationen bekannt zu machen. Die Klassenzugehörigkeit einer IP-Adresse ergibt sich durch die Anwendung der Standardsubnetzmaske. Dementsprechend unterstützen Classful Protokolle nicht den VLSM-Mechanismus. Um diesen Mangel, der vor allem in großen Netzstrukturen durch die ineffiziente Nutzung des IP-Adressvorrates auftritt, zu beheben, entstand der Vorschlag der Classless Protokolle. Diese berücksichtigen die flexible Einteilung des Adressbereichs über die Klassengrenzen hinweg. Zu ihnen gehören alle modernen Protokolle wie RIP Version 2, OSPF oder das Border Gateway Protocol (BGP) als exterior Protokolltyp.

Nicht immer reicht die Metrik als Entscheidungskriterium für einen Weg aus. Lernt ein Router für ein Ziel zwei Routen, z. B. weil der Administrator eine statische Route konfiguriert hat und das dynamische Routingprotokoll eine Alternative anbietet, muss er auswählen, welchen Pfad er in der Routingtabelle eintragen will. Zur Lösung dieser Entscheidungssituation dient die **administrative Distanz**, die die Vertrauenswürdigkeit des Weges wiedergibt. Gemäß dieses Kriteriums genießen direkt angebundene Netze das größte Vertrauen, gefolgt von statischen Routen und dann abgestuft nach Routingprotokoll den dynamischen Konzepten.

Ein gravierender Nachteil der Distance-Vector-Protokolle besteht darin, dass sie im Gegensatz zu den Link-State-Varianten, die auf einem eindeutigen aufspannenden Baum beruhen, Schleifen erzeugen können. Diese entstehen, wenn ein Paket ständig zwischen einer Folge von Routern übertragen wird, ohne das Zielnetz zu erreichen. Dieser Umstand beruht in erster Linie auf unkorrekten Weginformationen, deren Grund häufig im unzureichenden Konvergenzverhalten zu suchen ist. Die Ursachen des zeitlichen Auseinanderklaffens der Aktualisierungsinformation und seiner Folgen zeigt das Beispiel:

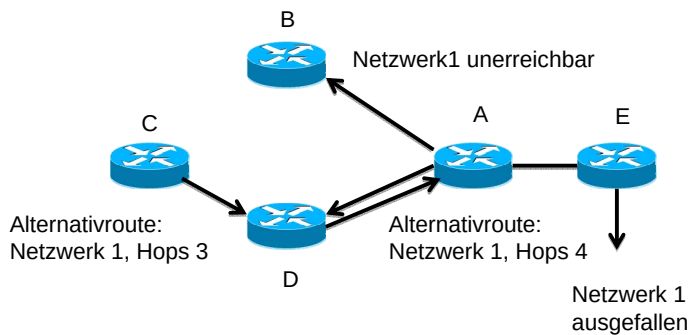


Bild 10.4 Routingschleife



Beispiel: Routingschleife

1. Zum Zeitpunkt des Ausfalls von Netz 1 verfügen alle Router über konsistente Tabellen und die bevorzugte Verbindung des Routers C zum Netz 1 führt über Router B.
2. Als Reaktion des Netzausfalls sendet Router E eine Aktualisierung der Routingtabelle an Router A. Router A beendet daraufhin die Übertragung von Paketen an Netz 1, während die Router B, C und D weiterhin senden, da sie noch nicht über die aktuelle Information verfügen. Sobald Router A eine Aktualisierung verschickt, stellen Router B und D die Sendung ein, Router C hat immer noch keine Information über den Ausfall.
3. Sendet Router C vor Erhalt der Aktualisierung turnusgemäß seine Routingtabelle an D, so zeigt die Tabelle fälschlicherweise die Erreichbarkeit von Netz 1 an. Router D ändert daraufhin erneut seinen Eintrag und leitet diese Daten an Router A weiter. Router A teilt die neuen Informationen nun B und E mit. Jedes Paket, das für Netz 1 bestimmt ist, läuft nun im Kreis: von C zu B zu A zu D und wieder zurück zu C.

Als Reaktion auf diese Unzulänglichkeit werden Distance-Vector-Protokolle um einige Merkmale ergänzt, die die Stabilität bei raschen Topologiewechseln gewährleisten sollen:

- **Hop-Count-Limit** legt die maximale Anzahl zu passierender Knoten fest. Diese Definition beugt einem „count to infinity“ endlos kreisender Pakete vor; denn das Beispiel 8.1 beschreibt eine Endlosschleife, die ohne Eingriff von außen nicht beendet werden kann. RIP kennt für diesen Fall ein Maximum von 15 Hops, d. h. 16 Knoten würden die ICMP-Meldung „network unreachable“ auslösen.
- **Hold Downs** veranlassen einen Router, Änderungen erst nach Ablauf einer bestimmten Zeitspanne bekannt zu geben. Die Zeitspanne ist geringfügig größer gewählt als diejenige, die notwendig ist, um das gesamte Netz mit einer Aktualisierung der Routinginformation zu versorgen. Wenn ein Pfad als nicht verfügbar erkannt wird, wird jede weitere Information diesen Weg betreffend, die schlechter oder gleich bezüglich der Metrik ist, ignoriert.

- **Split Horizon** beschreibt eine Regel, die besagt, dass Routinginformation nicht in die Richtung weiterleitet werden darf, aus der sie stammt. Diese Vorschrift verhindert, dass eine bessere Metrik an die Quelle zurückgeliefert wird.
- **Route Poisoning** markiert in den Routingaktualisierungen einen Weg als unerreichbar. Unerreichbar wird als maximaler Wert der Metrik interpretiert.
- **Triggred Updates** senden eine Routingtabellenaktualisierung sofort nach Bekanntwerden einer Topologieänderung. Sie warten nicht das Ablaufen von Timern ab, sondern geben die Veränderung unmittelbar an die Nachbarn weiter.
- **TTL-Feld** vermeidet das Kreisen von Paketen, die unzustellbar sind. Da das TTL-Feld eines IP-Paketes durch jeden Hop dekrementiert wird, erreicht es irgendwann den Wert Null. In diesem Moment verwirft der Router das Paket als unzustellbar.

■ 10.3 Routingprotokolle

Menschen können Pfade durch ein Netzwerk durch einfaches Hinschauen erkennen, Router benötigen zur Pfadbestimmung eine Netztopologie, die sie mathematisch analysieren. Dazu bedarf es Algorithmen, was die Bestimmung eines Weges umständlich und rechenintensiv macht. Zur Auswahl eines optimalen Pfades werden darüber hinaus zusätzliche Attribute benötigt. Die Grundfragen der Berechnung konzentrieren sich auf drei Fragenkomplexe:

- Sind zwei beliebige Knoten benachbart, also direkt miteinander verbunden?
- Wenn zwei Knoten nicht benachbart sind, gibt es einen Weg zwischen ihnen?
- Wenn ein Weg zwischen zwei Knoten existiert, ist dieser gemäß den gewählten Kriterien optimal?

Alle Router des Netzwerkes sollten über den gleichen Wissensstand verfügen, um konsistente Routingentscheidungen zu treffen. Daran knüpfen sich weitere Fragen:

- Wie werden Aktualisierungsmeldungen gesendet?
- Welche Informationen beinhalten diese Nachrichten?
- Wann und wie häufig werden die Aktualisierungen verschickt?
- Wie werden die Empfänger der Nachrichten bestimmt?

Wie unterschiedlich die Antworten auf diese Fragen ausfallen können, zeigen die beiden nachfolgenden Implementierungen der Routingidee.

10.3.1 Routing Information Protocol RIP

Das **Routing Information Protocol (RIP)** verdankt seine Verbreitung der Tatsache, dass es als Standard RFC 1058 von 1988 zur TCP/IP-Protokollfamilie gehört und sich über das UNIX 4BSD schnell einen großen Anwenderkreis erschloss. Als *routed-Daemon* wurde es Bestandteil jeder UNIX-Implementation. Um Mängel wie die Klassenorientierung zu beheben, wurde 1994 eine zweite Version unter dem Namen RIPv2 in RFC 1723 publiziert.

Die Anpassung an IPv6 erfolgte 1997 mit dem RFC 2080 unter der Bezeichnung RIPv6 (RIP next generation).

RIP als das älteste classful Distance-Vector-Protokoll für IPv4 ermöglicht den automatischen Austausch von Routinginformationen bestehend aus Ziel, nächstem Knoten und Metrikangaben, um in allen Netzknoten konsistente Routingtabellen zu führen. Das Entscheidungskriterium für die Wahl einer Route bildet die Entfernung, gemessen in Hops, d.h. der Anzahl der Vermittlungsstellen auf dem Weg zum Ziel. Die maximale Entfernung darf dabei 15 Hops nicht überschreiten, denn der Wert 16 steht bereits für „nicht erreichbar“. Die Routingtabelle, auf deren Basis die Wegeentscheidung getroffen wird, enthält vier Einträge:

- **Netz:** gibt die IP-Adressen der erreichbaren Netze an
- **Port:** enthält Angaben über das Routerinterface, über das die einzelnen Netze zu erreichen sind
- **Metrik:** misst die Entfernung zu den bekannten Netzen in Gestalt von Hops
- **Timer:** gibt die Zeitspanne seit der letzten Aktualisierung des Tabelleneintrages an.

Für den Austausch der Routingtabelleneinträge zwischen den erreichbaren Routern nutzt RIP das UDP-Protokoll mit der Portnummer 520 bei einer Paketlänge von 512 Byte. Die Pakete werden standardmäßig alle 30 Sekunden als Broadcast versendet.

1	8	16	32
Befehl	Version	0	
Adressfamilienkennung		0	
IP-Netzadresse			
0			
0			
Metrik(1, ..., 16)			
Die Felder haben im Einzelnen folgende Bedeutung:			
Befehl: Eine Eins symbolisiert einen Request durch einen Router bezüglich neuer Routinginformationen, eine Zwei kennzeichnet die Antwort auf diese Anforderung.			
Version: Dieses Feld enthält eine Angabe über die verwendete RIP-Version.			
Adressfamilienkennung: Da RIP für das Routing in heterogenen Netzen mit unterschiedlichen Adressarten konzipiert wurde, ist es notwendig, die verwendete Adressierung zu kennzeichnen. IP trägt den Wert 2.			
IP-Netzadresse: Allgemein können auch die mit null belegten Felder zur Subnetzadressbildung herangezogen werden. Durch den IP-Adressaufbau ist jedoch lediglich ein 32-Bit-Feld möglich.			
Metrik: Dieser Wert stellt die Anzahl Hops vom sendenden Router zum betreffenden Netz dar.			

Bild 10.5 Protokollheader RIPv1

Die Felder Adressfamilienkennung bis Metrik dürfen sich 25-mal wiederholen, d. h. bis zu 25 Ziele können in einem einzigen RIP-Paket aufgeführt werden. Mit 25 Einträgen ist die Nachricht 504 Bytes lang ($25 \times 20 + 4$), was der Länge von 512 Byte für ein UDP-Paket entspricht.

Zu Beginn sendet ein neuer Router auf jedem RIP-konfigurierten Interface eine Aufforderung an alle seine Nachbarn mit der Bitte, um Zusendung ihrer vollständigen Routingtabelle. Aus den erhaltenen Antworten errechnet der anfragende Router die ersten Einträge seiner noch ungefüllten Routingtabelle. Im Anschluss daran schickt er ein triggered Update mit seiner neu erstellten Routingtabelle an alle RIP-Nachbarn, so dass diese ihrerseits über eventuelle neue Wege informiert werden. RIPv1 kennt keine Subnetzinformationen. Ein Router kann daher Subnetze nur auf zwei Wegen berücksichtigen: entweder er nutzt die an seinem Interface speziell konfigurierte Subnetzmaske oder er zieht die Standardsubnetzmaske heran. Auf Grund dieser Einschränkung können über RIPv1 verwaltete Netze nicht VLSM oder verteilte Subnetze berücksichtigen.

RIPv2 stellt den nahtlosen Übergang auf eine neue Version des RIPv1 dar, mit dem Anspruch unter weitgehender Beibehaltung des Paketformates und seines Transportmechanismus die Begrenzung durch die Nichtweitergabe der Subnetzinformation aufzuheben. RIPv2 wandelt sich daher zu einem classless Protokoll als wichtigstem Unterschied zur Vorgängerversion, besitzt darüber hinaus aber noch weitere kleinere Anpassungen wie die Nutzung von Multicast-Adressen für Updates oder Authentifizierungsmöglichkeiten. Viele Merkmale, die RIPv1 prägen, bleiben bei RIPv2 jedoch erhalten. Dazu zählen die Erreichbarkeitsgrenze mit 16 „Hops“, die Verwendung der Mechanismen zur Schleifenunterdrückung und triggered Updates zur schnelleren Konvergenz:

1	8	16	32
Befehl (=1 oder =2)	Version=2	0	
Adressfamilienkennung (IP=2)		Route Tag 1	
IP-Adresse 1			
Subnetzmaske 1			
Nächster Knoten 1			
„Hop“-Metrik für Adresse 1			
Felder Adressfamilienkennung, Route Tag bis „Hop“-Metrik für die nächsten 23 Knoten			

Bild 10.6 Protokollheader RIPv2

Die Felder besitzen die gleiche Bedeutung wie bei RIPv1. Das **Route-Tag-Feld** enthält Informationen über den Ursprung der Routinginformationen. Es dient auf diese Weise zur Interoperabilität mit anderen Routingprotokollen, da sich nun entscheiden lässt, ob es sich um einen internen RIP-Weg oder einen importierten Pfad handelt.



Praxis

Die Basiskonfiguration von RIP auf einem Router ist denkbar einfach. Die nachfolgende Sequenz zeigt die notwendigen Befehle für einen Cisco-Router.

Router:

```
router rip
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
network 172.16.0.0
network 209.165.200.0
```

10.3.2 Open Shortest Path First OSPF

Um die Nachteile von RIP auszugleichen, wurde ab 1988 das **Open-Shortest-Path-First-Verfahren** (OSPF) entwickelt. Die Hauptvorteile von OSPF gegenüber RIP bestehen in der schnelleren Konvergenz und der besseren Skalierbarkeit für größere Netzwerke. Wie der Name andeutet, besitzt OSPF zwei Charakteristika, das der Offenheit im Sinne einer öffentlichen Spezifikation als RFC 2328 und das der Verwendung des SPF-Algorithmus. In UNIX-Systemen ist OSPF als **gated**-Dämon implementiert. OSPF gehört zur Klasse der **Link-State-Routing**-Protokolle. Für IPv6 existiert eine 1999 entworfene Version als RFC 2740.

Der Paketaufbau zeigt im Header den Pakettyp an. OSPF unterscheidet fünf Typen:

- Das **Hellopaket** dient dazu, eine Nachbarschaft mit weiteren OSPF-Routern herzustellen.
- Das **Database-Description-Paket** enthält eine Liste der Link-State-Datenbanken der Nachbarrouter. Diese Liste wird zum Abgleich mit der lokalen Link-State-Datenbank benutzt.
- Das **Link-State-Request-Paket** dient zur Anforderung weiterer Informationen zu einem Eintrag der Database Description.
- **Link-State-Update-Pakete** sind die Antwort auf Link-State-Requests. Sie können 11 unterschiedliche Link-State-Advertisements enthalten.
- **Link-State-Advertisements** bestätigen den Erhalt eines Link-State-Updates.

Neben diesen Headerinformationen enthält ein OSPF-Paket weitere Felder:

- eine Router-ID als Identifikation für den Ursprungsrouten
- eine Area-ID, um die Zugehörigkeit zu einer administrativen Einheit zu dokumentieren
- eine Netzwerkmaske als Subnetzinformation des sendenden Interfaces.

Als Beispiel für ein OSPF-Paket kennt das Hello-Paket zusätzliche Felder:

- das Hello-Intervall als Zeitspanne zwischen zwei Hello-Paketen

- die Router-Priorität zur Bestimmung eines Designated und Backup Designated Routers
- die Router-ID des Designated Routers
- die Router-ID des Backup-Designated Routers
- die Liste der Router-IDs der OSPF-Nachbarn

Hello-Pakete werden eingesetzt, um:

- OSPF-Nachbarn zu entdecken und eine Nachbarschaft zu implementieren.
- Parameter bekannt zu machen, um eine Nachbarschaft zu begründen.
- Die Wahl eines Designated und Backup-Designated Routers durchzuführen.

Standardmäßig werden Hello-Pakete als Multicasts über die Adresse 224.0.0.5 alle 10 Sekunden übertragen. OSPF nutzt das IP-Protokoll. Im IP-Paket wird OSPF durch den Eintrag des Wertes 89 in das Typ-Feld gekennzeichnet.

Der OSPF-Initialisierungsablauf setzt sich aus mehreren Schritten zusammen:

1. **Entdeckung der Nachbarn:** Die Initialisierung eines OSPF-Routers besteht im Erkennen seiner unmittelbaren Nachbarn. Dieser Prozess basiert auf dem Versenden von Hello-Paketen, die die bidirektionale Kommunikation einleiten und die Nachbarschaft begründen.
2. Der Router konstruiert ein **Link-State-Paket**, das den Zustand jeder direkt angeschlossenen Verbindung widerspiegelt. Dazu gehören Router-ID, Linktyp und Bandbreite.
3. Jeder Router flutet dieses LSP an alle Nachbarn und speichert alle empfangenen LSP-Pakete in seiner Datenbank. Die Nachbarn selbst geben ihrerseits das LSP an ihre Nachbarn weiter, so dass die ganze Area abgedeckt wird.
4. Jeder Router nutzt die Datenbank, um eine Topologielandkarte zu erstellen und auf dieser Basis den besten Weg zu bestimmen. Hierzu wird der Shortest Path First-Algorithmus verwendet. Jeder Router einer Area besitzt zwar die gleiche Topologieinformation, da er aber individuell jeweils die Wurzel des Baumes bildet, ergibt sich auch individuelle Routinginformation.

Die Grundlage des SPF-Algorithmus bilden nicht wie der Name nahelegt die Anzahl der Hops, sondern die Pfadkosten. Entscheidungskriterium für die Vorteilhaftigkeit eines Weges und damit Metrik wird die nominale Bandbreite. Einen Überblick über die in OSPF verwendeten Pfadkosten zeigt folgende Tabelle:

Tabelle 10.4 OSPF Pfadkosten

Interfacetyp	Kosten (= 10 ⁸ /bps)
Fast Ethernet und schneller	1
Ethernet	10
E1	48
64 Kbps	1562

Um die Menge der zu übertragenden LSAs einzudämmen, wird in Netzwerken, die nicht aus isolierten Punkt-zu-Punkt-Verbindungen bestehen, ein Designated Router gewählt. Der DR ist verantwortlich dafür, die Aktualisierungsinformation innerhalb einer Area zu verteilen. Der DR steigt damit zum verwaltungsmäßigen Zentrum einer Area auf. Der Backup-Designated Router nimmt die Rolle seines Stellvertreters ein.

Die Wahl eines Designated Routers erfolgt transparent. Entscheidungskriterium ist die höchste Router-ID, die im Allgemeinen die IP-Adresse darstellt. In besonderen Fällen kann eine Router-ID konfiguriert oder eine Loopback-Adresse als Ersatz erzeugt werden. Der Wahlprozess findet über den Austausch von Hello-Paketen statt. Fällt der DR aus, übernimmt der BDR seine Rolle ohne erneuten Wahlvorgang selbst dann, wenn zwischenzeitlich ein neuer Router mit höherer IP-Adresse hinzugekommen sein sollte. Die Unterschiede zwischen den Routing-Protokollen zeigt folgende Tabelle:

Tabelle 10.5 RIP vs. OSPF

RIP	
Vorteile	Nachteile
einfach einzurichten	Datenflut, da standardmäßig die Routingtabelle alle 30 sec. übertragen wird
interoperabel	lange Konvergenzzeit
	Hop-Count ist einzige Metrik
	Routen werden ohne Sicherheitsmechanismen bezogen
OSPF	
Vorteile	Nachteile
schnelle Konvergenz	Einrichtung ist komplex
Metrik berücksichtigt Bandbreite	verlangt mehr Ressourcen als RIP
Routen verlangen Authentifizierung	

■ 10.4 Routingprobleme

Um die Existenz und die Qualität einer Verbindung zu einem Zielnetzwerk zu prüfen, gibt es zwei Programme:

- **ping:** dieser Befehl sendet ein ICMP-Paket Echo über das Netz an die angegebene IP-Adresse und wartet auf Antwort in Form eines Echo-Reply. Als Ergebnis erhält der Nutzer die Erreichbarkeit und eine Angabe darüber, wie lange der Datentransfer dauert. Ping kann sowohl von einem Router als auch von einer Endstation gestartet werden.

ping

```
PC>ping 192.168.12.2
```

```
Pinging 192.168.12.2 with 32 bytes of data:
```

```
Reply from 192.168.12.2: bytes=32 time=121ms TTL=120
```

```
Reply from 192.168.12.2: bytes=32 time=141ms TTL=120
```

```
Reply from 192.168.12.2: bytes=32 time=133ms TTL=120
```

```
Reply from 192.168.12.2: bytes=32 time=128ms TTL=120
```

```
Ping statistics for 192.168.12.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 121ms, Maximum = 141ms, Average = 130ms
```

- **tracert:** dieser Befehl zeichnet die Route auf, die das Paket im Netzwerk nimmt. Die Ausgabe besteht aus einer Folge von IP-Adressen der Zwischenknoten. Auch hier werden Zeitangaben mitgeliefert, so dass leicht erkennbar wird, wo die Engpässe im Datentransfer liegen.

tracert

Tracert-Ergebnisse (icmp) von www.heise.de zu www.fh-flensburg.de:

Hop#	IP	Hostname	avg [ms]
1	193.99.144.252		0,78
2	82.98.98.97	c101.f.de.plusline.net	1,16
3	80.81.192.222	zr-fra1-te0-0-0-3.x-win.dfn.de	2,69
4	188.1.145.125	zr-han1-te0-7-0-5.x-win.dfn.de	25,68
5	188.1.145.6	xr-kiel-te1-1.x-win.dfn.de	23,90
6	188.1.233.90	kr-fhflen2.x-win.dfn.de	26,37
7	193.175.191.205	www.fh-flensburg.de	26,25
8	193.175.191.205	www.fh-flensburg.de	27,61

Über beide Befehle kann jede IP-Adresse erreicht werden. Sollte eine Antwort ausbleiben, ist die Ursache in der Konfiguration von Firewalls zu sehen, die diesen Verkehr aus Sicherheitsgründen blockieren. Ping lässt sich weitgehend konfigurieren. So ist wählbar, wie viele Pakete bei einem ping gesendet werden.

Tracert verwendet als zentralen Mechanismus das TTL-Feld des IP-Headers. Um das Ziel zu erreichen, wird systematisch der Wert des TTL-Feldes inkrementiert. Da ein Router alle Pakete verwirft, die nach Erhalt und Dekrementierung einen Wert von Null aufweisen, aber dem Sender mit einem ICMP-Paket „Destination unreachable“ antwortet, entsteht eine Folge der Knoten bis zum Ziel.

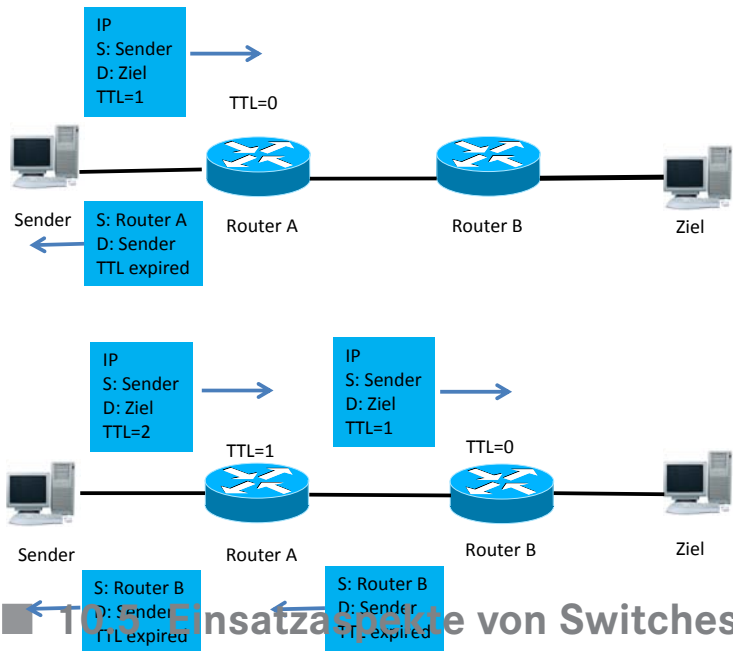


Bild 10.7
Funktionsweise
von traceroute

10.3 Einsatzszenarien von Switches und Routern

Die folgende Skizze zeigt die Optionen eines möglichen Zusammenspiels von Routern und Switches. Sie bezieht als wesentliche Möglichkeit die Bildung virtueller Netze (VLAN) ein. Ein VLAN entspricht einer Broadcast-Domäne. Da LAN-Segmente einer Kollisionsdomäne gleichzusetzen sind, können VLANs als Gruppe von Stationen interpretiert werden, die auf unterschiedlichen physikalischen LAN-Segmenten residieren, aber logisch zusammenarbeiten, als gehörten sie dem gleichen LAN an.

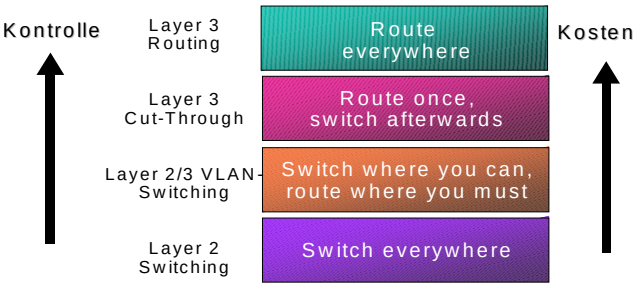


Bild 10.8 Switch-Router Taxonomie

Der „**Switch everywhere**“-Ansatz klammert ein Routing vollständig aus der LAN-Umgebung aus. Routing bleibt ausschließlich WAN-Verbindungen vorbehalten. Da der gesamte Datenverkehr über Switches transportiert wird, stellt dies die Alternative mit der besten Performance und den geringsten Kosten dar. Voraussetzung für einen reibungslosen Ablauf ist eine logisch flache Netzstruktur ohne Subnetze.

Die Schranken dieses Konzeptes liegen in der Struktur. So gibt es keinen Mechanismus, der eine Begrenzung von Broadcasts erzwingt. Broadcasts binden aber Verarbeitungskapazität der Rechner und verschwenden neben Bandbreite auch CPU-Leistung. Zudem erschweren flache Netze ab einer bestimmten Größenordnung das Fehler- und Netzmanagement beträchtlich, ganz abgesehen davon, dass die Adressverwaltung und die Kontinuität des Adressraumes bei steigender Nutzerzahl schwer überschaubar wird.

Der **„Switch where you can, Route where you must“**-Ansatz verlässt die Idee einer flachen Netzhierarchie zugunsten der Integration eines Routers, um die Nachteile durch unzureichende Sicherheit, mangelndes Adressmanagement und Begrenzung der Broadcasts auszugleichen. Das primäre Ziel besteht jedoch weiterhin darin, das Ausmaß des Datenverkehrs, der Routing benötigt, möglichst gering zu halten. Zeigt das Verkehrsmuster des Netzes eine ausreichende Stabilität, in dem Sinne, dass Datenströme mit einer hohen Wahrscheinlichkeit zu prognostizieren sind, bietet sich die Einrichtung von VLANs an. Die Aufgabe von Routern besteht dann darin, die Datenströme zwischen unterschiedlichen VLANs zu vermitteln. Diese Aufgabenteilung erlaubt eine Steigerung der Performance innerhalb des VLANs, allerdings zulasten der Inter-VLAN-Kommunikation. Die Verkehrslast die VLAN-Grenzen überschreitet, kann durch die Zuordnung von Servern zu mehreren VLANs beträchtlich reduziert werden.

Der **„Route everywhere“**-Ansatz verteidigt die Philosophie einer paketweisen Verarbeitung nach intensiver Prüfung. Einsatzgebiet und Kosten lassen diese Verarbeitungsform aber für die Mehrzahl der Anwendungen als ungeeignet und viel zu aufwändig erscheinen.

Gibt es einen „besten“ Ansatz? Die Antwort hängt von zugrunde liegenden Netz, der gewünschten Performance, den Kontroll- und Applikationsrestriktionen und nicht zuletzt von der Größe und dem prognostizierten Wachstum des Netzes ab. Eine Lösung könnte in der Kombination von Elementen der unterschiedlichen Konzepte bestehen: preiswerte aber schnelle Layer-2-Switches in der Arbeitsgruppe ergänzt um den Aufbau von VLANs, sowie Layer-3-Switches für die VLAN-Verknüpfung und das Routing.

■ 10.6 Zusammenfassung

Router als Drehscheibe der Datenströme in Netzwerken besitzen mehrere Schnittstellen mit unterschiedlichen IP-Adressen. Während im lokalen IP-Netz die Kommunikation zwischen Endstationen auf der Basis von physischen Adressen stattfindet, d.h. eine ausgeprägte Wegewahl nicht notwendig ist, ist im WAN-Bereich ein Informationsaustausch ohne logische Adressen in Form der IP-Adressen unmöglich. Router werden damit zu einem essentiellen Bestandteil jeglichen Weitverkehrsnetzes allein durch ihre Funktion unabhängig von der eingesetzten Technologie. Daraus leiten Mechanismen wie Wegewahlverfahren, Routingtabellen und Probleme des Routingvorganges ihre Bedeutung ab. Ohne ein ausgefeiltes Routing ist das Internet nur eine Fiktion.

Dieser Schlüsselposition verdanken Unternehmen wie Cisco Systems ihre Stellung im IT-Bereich. Router sind Rechner mit den typischen Komponenten wie CPU, RAM, ROM und einem Betriebssystem. In ihrer Bedienung und Konfiguration verlangen sie jedoch spezifisches Know-how. Das IOS (Internet Operating System) der Cisco-Geräte ähnelt zwar denen

der Mitbewerber in ihrer Grundsätzlichkeit, Abweichungen existieren dennoch. Mit einem Verständnis der Anforderungen, die an den Weiterleitprozess von Paketen gestellt werden, wird die konkrete Bedienbarkeit der Netzkomponenten jedoch signifikant erleichtert.

■ 10.7 Wissensüberprüfung

1. Stimmen Sie folgender Aussage zu? „Distance-Vector-Protokolle entwickeln eine Netzwerklandkarte, wohingegen Link-State-Protokolle topologische Daten von den Routingtabellen der Nachbarn erhalten“.
2. Wie werden die topologischen Informationen bei Distance-Vector-Protokollen und Link-State-Protokollen aktualisiert?
3. „Statische Routen werden manuell konfiguriert“. Stimmen Sie dieser Aussage zu?
4. Wozu werden Hello-Pakete genutzt?
5. Warum sind Hold-Downs nützlich?
6. Warum treten Routingschleifen auf und wie wird das Problem gelöst?
7. Was passiert, wenn der maximale Hop-Count erreicht wird?
8. Beschreiben Sie den Begriff der Konvergenz und warum eine schnelle Konvergenz wünschenswert ist.
9. Nennen Sie die Nachteile der Distance-Vector-Protokolle.
10. Welcher Typ von Routingprotokollen verlangt keinen Administratoreingriff?

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Was ist das Ziel des Netzwerkmanagements?
- Was ist unter dem FCAPS-Modell zu verstehen?
- Welche Funktionen führt das Protokoll SNMP aus?
- Welche allgemeinen Bedrohungen der Netzwerksicherheit existieren?
- Wie kann mit Mechanismen der Switches und Router die Gefahr eingedämmt werden?

Kapiteleinführung

Mit dem unvergleichlichen Wachstum des Internet geht auch eine noch nie da gewesene Gefährdung persönlicher Daten und Unternehmensressourcen einher. Täglich wächst die Bedrohung durch Hacker und die Zahl immer neuer Arten von Angriffen auf Rechner. Das zunehmende Interesse, das Internet zu einem sicheren Handelsplatz zu machen, forciert Technologien wie Public Key Interface (PKI) oder Virtuelle Private Networks (VPN). Dennoch: Netzwerkangriffe sind ebenso vielfältig wie die Systeme denen sie gelten.

Zu Beginn der Entwicklung von TCP/IP-basierten Netzwerken bestand das Internet lediglich aus einem Verbund weniger Universitäten in den USA, die ausschließlich den Zweck verfolgten, das Lernen und Forschen zu unterstützen. Die Designer konnten damals nicht ahnen, welchen Siegeszug das Internet bis heute antreten würde. Daher spielte zu Beginn der Entwicklung der Internet-Protokoll-Festlegung das Thema Sicherheit noch keine Rolle. Eben dies ist der Grund, warum die meisten IP-Installationen grundsätzlich unsicher sind und warum es unabdingbar ist, IP-Implementierungen um Methoden, Dienste und Protokolle zu ergänzen. Damit entsteht der Zwang, das Netzwerk zu steuern und zu überwachen. Da Netzwerkinfrastrukturen komplexe Gebilde sind, ist es unumgänglich diese Steuerung Remote vorzunehmen, d.h. einen Mechanismus zur Verfügung zu haben, der von einer zentralen Stelle aus Informationen sammelt und Konfigurationen zulässt. SNMP bildet hierzu die Basis. Um Sicherheit jedoch individuell für die Schlüsselkomponenten wie Router und Switches zu ermöglichen, verfügen diese über Filterfunktionen, die angepasst an die IP-Gegebenheiten, die Einschränkung und Steuerung des Verkehrsflusses bis zu seiner kompletten Unterbindung zulassen.

Letztlich wird klar: Netzwerkmanagement und Sicherheit bedingen zum Teil einander und bedürfen fundierter Kenntnisse, um sie zum Nutzen einer Infrastruktur einsetzen zu können.

■ 11.1 Netzwerkmanagement

Aufgrund des rasanten Wachstums der vernetzten Rechner, der steigenden Komplexität der Installationen, der Heterogenität der Netzkomponenten und der räumlichen Ausdehnung heutiger Kommunikationssysteme setzt sich die Erkenntnis durch, dass ohne ausreichendes Netzmanagement eine IT-Infrastruktur nicht mehr zu betreiben ist. Dabei geht es nicht nur um eine passive Netzüberwachung, sondern auch um die Möglichkeit, aktiv Fehlerquellen aufzuspüren, zu analysieren und zu beseitigen. Viele Untersuchungen zeigen, dass die Verwaltung der Netze einen erheblichen Teil des IT-Budgets verschlingt.



Netzwerkmanagement

Netzwerkmanagement umfasst die Verwendung, Integration und Koordination von Hard- und Software sowie Elemente zum Überwachen, Testen, Konfigurieren, Analysieren und Bewerten des Netzwerkes und seiner Elemente, um die Operationalität und die Dienstgüte zu angemessenen Kosten sicherzustellen.

Das Spektrum reicht von der Infrastruktur-, Kabel- und Performanceüberwachung bis zum Management der kompletten Systemumgebung mit allen im Netz angeschlossenen Geräten vom PC bis zum Router sowie allen im Netz verteilten Applikationen.

Welche Folgen ein unzureichendes Netzmanagement haben kann, zeigen folgende Beispiele:

Netzausfälle und ihre Folgen

- Aufgrund eines Fehlers im Netz eines Telekommunikationsunternehmens fiel der Passagier- und Gepäck-Check-In einer Airline für mehrere Minuten aus
 - alle Flugzeuge mussten 30 Minuten länger am Boden bleiben
- Die Speicherknappheit in einem Switch führte zum Netzausfall bei einer europäischen Bank
 - geschätzte Kosten: 1 Million Dollar pro Minute Ausfall
- Die Gigabit-Ethernet-Verbindung zwischen Front-End und Back-End Server eines Online-Buchhändlers fiel aufgrund falscher QoS-Konfiguration aus:
 - 10 000 unzufriedene Kunden pro Sekunde des Ausfalls

Um den komplexen Anforderungen der Überwachung der Infrastruktur gerecht zu werden, haben sich Teilkomplexe mit bestimmten Aufgabenschwerpunkten herausgebildet:

- Das **Netzwerkmanagement** im engeren Sinne richtet sein Augenmerk auf alle Kommunikationseinrichtungen.
- Das **Systemmanagement** schließt die Berücksichtigung der im Netz eingebundenen Rechner ein.

- Das **Applikationsmanagement** umfasst auch die auf den einzelnen Netzknoten laufenden Anwendungen und bildet damit die umfassendste Sichtweise auf das Netz.

Um in diesem Umfeld agieren zu können und um diese Anforderungen zu meistern, sollte ein Managementtool folgende Merkmale aufweisen:

- **Offene Plattform** auf der Basis von Standards, um sowohl Zusatzwerkzeuge von Herstellern besonderer Netzkomponenten zu integrieren, als auch um dem Gebot der Heterogenität Folge zu leisten.
- **Autotopology** zur automatischen Ermittlung und Darstellung der Netztopologie d. h. der selbständigen Erzeugung einer Netzlandkarte.
- **Autodiscovery** zur Entdeckung neu hinzukommender Geräte im Netz. Leider besteht hier oft die Einschränkung auf TCP/IP-Komponenten.
- **Eventhandling** zur Konfiguration und Behandlung von Alarmen und Ausnahmesituationen durch komplexe, frei definierbare Filter.
- **Polling** einzelner kritischer Komponenten nach einer definierbaren Strategie.

11.1.1 Netzwerkstatistiken

Die Analyse und Lösung von Netzwerkproblemen beruht zu einem großen Teil auf der Sammlung von Informationen über die im Netzwerk existierenden Geräte. Der Befehl ping ist ein naheliegendes Werkzeug, um einen schnellen Überblick über den Zustand und die Verbindungsgüte im Netzwerk zu gewinnen. Sollte ping zu keinem Ergebnis führen, kann die Ursache unterschiedliche Gründe haben: die Firewalls der angerufenen Geräte unterbinden ICMP-Verkehr oder der Anschluss des Rechners selbst ist fehlerhaft. Deshalb sind banale Fragen wie:

- Ist das Kabel oder die Netzwerkkarte beschädigt?
- Ist der Rechner überhaupt mit dem Netzwerk verbunden?
- Ist die Steckverbindung in Ordnung?

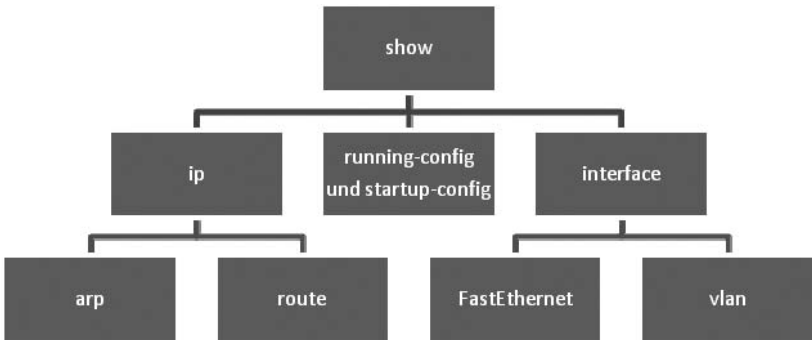
zu beantworten. Als nächster Schritt bietet sich eine Überprüfung der Schnittstellenstatistik an. Sie sagt aus, wie der Status des Gerätes ist, welche Paketanzahlen transportiert wurden und welcher Anteil der Pakete fehlerhaft war. Einige Fehler sind tolerierbar. Steigt die Zahl allerdings über ein Normalmaß hinaus, ist Vorsicht geboten.

Schnittstellenstatistik

Windows-Rechner kennen zur Auswertung der Netzschnittstelle den Befehl **netstat**. Mit unterschiedlichen Optionen lässt er erste Auswertungen zu.

C:\>netstat -e		
Schnittstellenstatistik		
	Empfangen	Gesendet
Bytes	2874271	853633
Unicastpakete	3487	2919
Nicht-Unicastpakete	398	408
Verworfen	0	0
Fehler	0	0
Unbekannte Protok.	0	0

Auf Cisco-Routern gibt der hierarchisch gegliederte **show-Befehl** Auskunft über unterschiedliche Kategorien von Informationen.



R1#show ip interface brief			
Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/0	unassigned	YES unset	administratively down down
FastEthernet0/1	10.0.0.1	YES manual up	up
Serial0/0/0	172.16.0.1	YES manual up	up
Serial0/0/1	172.16.0.9	YES manual up	up
Serial0/1/0	unassigned	YES unset	administratively down down
Serial0/1/1	unassigned	YES unset	administratively down down

oder

R1#show interfaces S0/0/0

Serial0/0/0 is up, line protocol is up

Hardware is GT96K Serial

Internet address is 172.16.0.1/30

MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255

Encapsulation PPP, LCP Open

Listen: CDPCP

Open: IPCP, loopback not set

Keepalive set (10 sec)

Der Befehl **arp** zeigt den Inhalt der MAC-Adressen an, die die Endstation kennt. Sie ähnelt damit der Weiterleittabelle eines Switches.

```
PC>arp -a
Internet Address      Physical Address      Type
10.10.10.1            0005.5e4e.8a38        dynamic
10.10.10.13           000d.bd62.d826        dynamic
```

11.1.2 OSI-Modell

Als eine Vorstellung zur Strukturierung unterschiedlicher Aufgabenbereiche des Netzwerkmanagements hat sich das FCAPS-Modell herauskristallisiert, das von der ITU-T und der ISO 1997 in der Spezifikation M.3400 definiert wurde. Es differenziert fünf Ebenen und gibt einen Anhalt dafür, was eine zufriedenstellende Überwachung der Infrastruktur im Idealfall leisten soll.

Tabelle 11.1 FCAPS-Ebenen

Ebene	Beschreibung
Fault /Fehler	Fehlerlokalisierung und -behebung, Überwachung von Schwellwerten
Configuration	Netzwerkplanung, Installation, Status und Kontrolle
Accounting	Nutzungsprofile und Abrechnung
Performance	Performanceüberwachung, -kontrolle und -analyse
Securitivity	Recovery, Zugriffssteuerung, Firewallüberwachung, Kontrolle des externen Netzverkehrs

Bei der Realisierung des FCAPS-Modells treten aber erhebliche Probleme auf. Ein Netzwerkmanagementsystem umfasst in der Regel nur einen kleinen Teil des Modells, da die Vielzahl der Geräte, ihrer Nutzer und der verwendeten Software hochdynamisch ist und

permanent neue Anforderungen erzeugt. Konsequenz aus dieser Einsicht ist, dass Netzwerkmanagement nicht als ganzheitliches System betrieben werden kann, sondern sich punktuell auf individuelle Aspekte konzentriert.

Welche Komplexität hinter den fünf Bereichen verborgen sein kann, zeigt die nachfolgende Übersicht:

- **Fault-Meldungen (Events)** informieren über ein Ereignis, das keine unmittelbare Systemgefahr darstellt wie Port up/down oder Speicherplatz zu 85 % gefüllt. **Alarmmeldungen (Alarms)** hingegen weisen auf ein Ereignis, das eine unmittelbare Systemgefahr darstellt wie Power Failure, Uplink down oder Speicherplatz zu 100 % gefüllt, hin. Hier besteht unmittelbarer Handlungsbedarf, wobei die Benachrichtigungswege eher „outbound“, d. h. unabhängig vom überwachten System über SMS, Voice-Mail oder E-Mail laufen.
- **Configuration** setzt sich aus seiner Vielzahl von Einzelaspekten zusammen. Dazu gehören Inventur von Hard- und Software, Verbindungen, Kabelwege, Konfigurationen der Netzwerkgeräte und Änderungsmanagement (Change Control).
- **Performance-Verfügbarkeit (Availability)** ist der Prozentsatz der Zeit, die das System während der vereinbarten Betriebszeiten zu den vereinbarten Bedingungen arbeitet. Diese Zahl bildet die Basis der Dienstgütevereinbarung (Service Level). Als weiteres Merkmal kommen **Antwortzeiten (Response time)** als die Zeit, die eine Anwendung von der Eingabe bis zur Reaktion benötigt, hinzu; allerdings liegt die Ursache hier nicht ausschließlich beim Netzwerk. Der **Durchsatz (Throughput)** bezeichnet die korrekt übertragene Datenmenge pro Zeiteinheit und ist ebenfalls wie die Antwortzeit ein Maßstab für die Güte des Datentransportes. Als letzte Disziplin ist die **Kapazitätsplanung (Capacity)** für die Trendanalyse, die Vorhersage der weiteren Entwicklung oder die Maßnahmen zur Anpassung der Kapazitäten verantwortlich.
- **Accounting** umfasst Aspekte wie Investitionssicherung, Kostenüberwachung, Nutzungs- und Kostenverrechnung und offenbart damit einen Bezug zu betriebswirtschaftlichen Bereichen.
- **Security** deckt einen weiten Bereich ab, der von allgemeine Richtlinien (Policy) und Befugnissen (Authority) über Zugriffs-Ebenen (Access Level) und Protokollierungen (Logging) bis zu Regelverstößen (Exceptions) reicht.



Es gibt eine Vielzahl von Open Source Tools für die Bereiche Netzwerk- und Systemmanagement. Zu den verbreitesten gehören Nagios und Bigbrother.

- Nagios: Systemmanagement
- Bigbrother: Netzwerkmanagement
- net-snmp: Open Source Tool
- Zenoss: Open Source Monitoring-Software

11.1.3 SNMP

SNMP (Simple Network Management Protocol) ist eine Möglichkeit, mit den Netzwerkgeräten zu kommunizieren und Informationen abzurufen. Dazu ist es nicht notwendig, mit jedem dieser Geräte explizit verbunden zu sein. Die Idee hinter diesem Verfahren ist einfach: der Zustand und die Arbeitslast lassen sich durch Befehle in Erfahrung bringen, indem die Datenbank auf der betreffenden Netzkomponente nach den gewünschten Daten abgefragt wird.

SNMP ist Teil des Internet Network Management Frameworks und in den RFCs 1155, 1157 und 1212 definiert. Es nutzt UDP als Transportprotokoll. Mittlerweile liegt das Protokoll in der Version 3 vor (RFC 2271-2275). Während SNMPv2 eine reine Erweiterung des Ausgangsvorschlags ist, handelt es sich bei SNMPv3 um eine vollständige Neufassung, bei der vor allem die Authentifizierung integriert ist. Die Modellvorstellung basiert auf mehreren Bestandteilen:

- **Managed Object:** Hierunter werden die Netzwerkelemente also Rechner, Router, Terminalserver etc. verstanden. In dem Client/Server-Modell das SNMP zu Grunde liegt, handeln sie als Clients bzw. Agents.
- **Management Information Base (MIB):** Hierbei handelt es sich um eine Sammlung von managed objects, d.h. Netzwerkobjekten wie Protokollen oder Switches in einem virtuellen Speichermodell.
- **Syntax Notation:** Um die managed objects einer MIB maschinenunabhängig zu beschreiben, ist eine bestimmte Notation notwendig. Das Managementmodell benutzt eine Teilmenge der ASN.1 (Abstract Syntax Notation No.1), um sowohl die ausgetauschten Management-Pakete als auch die managed objects zu definieren.
- **Structure of Management Information (SMI):** Die SMI legt die Regeln zur Beschreibung der Management-Information unter Nutzung von ASN.1 fest.
- **Netzwerk-Managementstation:** Dieses Gerät bildet die Steuerzentrale der Management-Applikation. In einer Netzwerkmanagementumgebung muss mindestens eine Station dieses Typs existieren.
- **Management-Protokoll (SNMP):** Zum Austausch der gesammelten Informationen ist ein Protokoll zwischen Agents und Managementstation notwendig.

SNMP ist ein asynchrones Request-/Response-Protokoll der Schicht 7 des ISO-Referenzmodells und löst ein klassisches Problem der Informationstechnologie: Daten aller Netzkomponenten werden im Überfluss gesammelt, verweilen aber dezentral in den einzelnen Bausteinen. Was fehlt, ist die Konzentration der Daten an einem Ort und deren gleichzeitige graphische Aufbereitung. Angesichts dieses Verteilungsmusters und der daraus resultierenden Anforderungen, ist SNMP im Wesentlichen aus zwei Teilen konzipiert: Agenten in Form von Software, die in allen Bestandteilen des Netzes Daten sammeln und auf Anfrage bereitstellen und die Managementstation, in der alle Informationen zusammenlaufen und zentral ausgewertet werden können. Die Merkmale, die für die Managementstation von Bedeutung sind, werden durch Variable der Agenten beschrieben. Die Managementstation hat daher die Aufgabe, die Werte dieser Variablen mit dem tatsächlichen Zustand der

Agenten konform zu halten, was auch eine Umkonfigurierung durch Schreibzugriffe umfassen kann.

Im Standard sind zwei Ports zur Kommunikation zwischen den beiden Instanzen Agent und Managementstation festgelegt:

- Port 161: für den Empfang aller SNMP-Requests. Manager senden Anforderungen auf diesem Port und Agents ihre Antworten.
- Port 162: für den Empfang von Ausnahmen bzw. Fehlerzuständen. Agents senden die damit verbundenen Trap Meldungen zum Manager.

Zur Abwicklung des Request/Response-Diagrams benötigt SNMP lediglich fünf Befehle. Zwei davon fordern Daten vom Agenten an, zwei weitere übertragen Daten vom und zum Agenten und über den fünften stellt der Agent von sich aus einen Kontakt zur Managementstation her, um Ausnahmesituationen bekannt zu machen.

Tabelle 11.2 SNMP-Befehle

Nachrichtentyp	Bedeutung
GetRequest	Die Managementstation fordert von einem Agenten Variablenwerte an, der diese mit GetResponse beantwortet. Dabei wird eine identische RequestID verwendet
GetNextRequest	Analog zu GetRequest, allerdings werden die Werte der hierarchisch nachfolgenden Objekte der MIB-Datenbasis geliefert, so dass eine Liste von Variablen ausgelesen werden kann
GetResponse	Erwiderung auf GetRequest, GetNextRequest und SetRequest
SetRequest	Setzen neuer MIB-Variablenwerte. Dadurch kann auf Agentenseite eine beliebige Operation ausgelöst werden.
Trap	Unaufgeforderte Nachricht vom Agenten an die Managementstation

Mit SNMP sind mehrere Probleme verbunden:

- Agents sind weitgehend passive Komponenten, d. h. sie können zwar Fehler erkennen aber nicht beheben.
- SNMPv1 ist unsicher, da die Passwortvariable Community, die einen Schutz vor unerlaubtem Zugang gewähren sollte, im Klartext übermittelt wird.
- Die Transportbasis von SNMP ist UDP und damit anders als TCP kein gesicherter Dienst. Traps oder andere Meldungen können daher ohne Warnung verloren gehen.
- Die Aktualisierung der Netzdatenbasis erfordert Übertragungskapazität. Netzwerkmanagement bedeutet demzufolge auch, eine bestimmte Netzlast für Verwaltungsaufgaben bereitzustellen. SNMP ist bandbreitentechnisch ineffektiv, insbesondere über WAN-Verbindungen.

SNMPv2 wurde im April 1993 vorgestellt, jedoch weder als offizieller Standard verabschiedet noch in die Praxis umgesetzt. Durch die Neudefinition in RFC 1905 wurde vor allem die Menge der Nachrichtentypen erweitert:

- Zur Übertragung größerer Datenmenge steht der Nachrichtentyp **GetBulkRequest** zur Verfügung. Hierdurch wird es ermöglicht, einen kompletten MIB-Baum mit nur einer Anfrage auszulesen. Dazu wird durch die Angabe von Wiederholungsfeldern eine bestimmte Anzahl von Variablen ab einer bestimmten Position festgelegt.
- Die Message **InformRequest** dient dem Informationsaustausch zwischen Managementstationen und ermöglicht eine hierarchische Strukturierung des Managements.

SNMPv3 basiert auf den Spezifikationen RFC 1902 bis 1908 und 2271 bis 2275, berücksichtigt aber die SNMPv1-Definitionen. Die wichtigsten Änderungen betreffen die Sicherheit, die Administration und die Kommunikationsstruktur. Um die Sicherheitsstruktur zu verbessern, setzt SNMPv3 eine Kombination aus Verschlüsselungsverfahren, verbessertem Authentifizierungsmechanismus und Zeitsynchronisation ein. Das „User-based-Security-Model“ USM gemäß RFC-2274 bildet das Herzstück. Zum Schutz gegen passives Mitlesen des Datenstroms wird das AES-Verfahren eingesetzt. Der Hash-Algorithmus MD5 fügt jedem SNMP-Paket einen digital unterschriebenen Hashwert hinzu, die der Kommunikationspartner verifiziert und so die Datenintegrität garantiert. Zur Unterstützung der Authentifizierung nutzt SNMPv3 eine Zeitsynchronisation, die die Übertragungsdauer und die Ankunftszeit der Pakete überwacht. Auf diese Weise wird eine Manipulation des Datenstromes verhindert.

Für eine Verteilung von Zugriffsrechten sorgt das in RFC-2275 beschriebene „View-based Access Control Model“ VACM. Die Rechte jeden Netznutzers werden wie Passwörter zentral von einem Server aus verwaltet. Dabei unterscheidet SNMPv3 die Zugriffsrechte individuell für jedes MIB-Objekt. Die tatsächliche Kontrolle führt jeder Agent anhand der Security-Policy des Nutzers durch.

Das SNMP-Paket besteht aus zwei Hauptstrukturen: der Präambel und dem eigentlichen Paket, dass selbst wieder in einen Header und einen Body zerfällt. Die Präambel enthält Informationen zur Nachrichtenlänge, zur Version und zum Commodity-String, der Header identifiziert den Nachrichtentyp und der Body nimmt die eigentliche Information auf.

11.1.4 MIB

Die Informationen der einzelnen Netzwerkmerkmale wie Protokolle oder Gerätespezifika werden in einer Management Information Base gesammelt. Es gibt einerseits allgemein standardisierte MIBs, die eine für eine Komponente/Protokolle vorgegebene und definierte Zahl von Merkmalen enthält und andererseits herstellerspezifische MIBs. Die MIB ist als hierarchischer Baum organisiert und definiert standardisierte Variablen und Felder, die von den Herstellern international einheitlich interpretiert werden. Die so genannte MIB-II beinhaltet z.B. 171 Objekte in 11 Funktionsgruppen. Alle Standard-SNMP-Komponenten unterstützen die MIB-II nach RFC1213.



MIB-Object

Der Begriff „Internet“ besitzt folgende Darstellung:

INTERNET Object Identifier::={iso 3 6 1}

Die Werte in der Klammer können sowohl Zahlen als auch zuvor definierte Begriffe sein. In diesem Falle ist „ISO“ bereits als (1) definiert worden. In dieser Form entsteht eine Variablenhierarchie. Die Variable „MGMT“ lässt sich als: MGMT Object Identifier::={ Internet 2} ausdrücken und bezeichnet in der dotted-decimal-Darstellung: 1.3.6.1.2

Einen Auszug aus dem MIB-Baum für IP zeigt die folgende Abbildung:

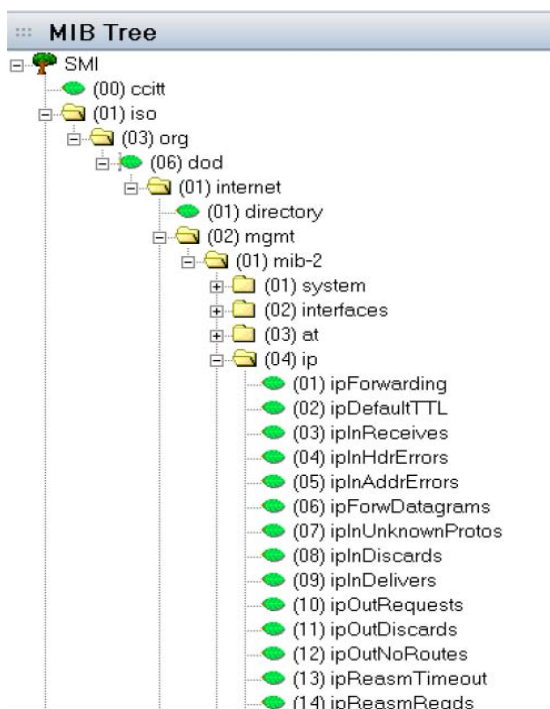


Bild 11.1 MIB-Baum

Eine MIB stellt einen abstrakten Baum mit einer namenlosen Wurzel dar. Er dient zur weltweit eindeutigen Identifizierung und zur Definition der einzelnen Objekttypen, die durch Object identifier in dotted-decimal-Darstellung vorgenommen wird. Object identifier entsprechen Telefonnummern, die ebenfalls hierarchisch organisiert sind und bei denen die einzelnen Zifferngruppen eine unterschiedliche organisatorische Zugehörigkeit charakterisieren. Die Object-ID-Struktur einer SNMP-MIB kennt drei Hauptzweige: CCITT, ISO und ISO/CCITT gemeinsam. Viele der Aktivitäten konzentrieren sich im ISO-Zweig auf das Internet definiert als Object-ID 1.3.6.1. So verweist die Folge 1.3.6.1.2.1.4.1 auf das Element ipForwarding (s. Bild 11.1). Die aktuelle Standard-MIB gruppiert die Objekte nach Protokollen, Systemen, Interfaces und anderen Kategorien:

- **system:** Informationen über die Konfiguration der verwalteten Netzknoten
- **interfaces:** Informationen über Netzkarten und Adapter
- **at, ip, icmp, tcp, udp, cmot snmp:** Protokollspezifische Eigenschaften
- **egp:** Beschreibung des Routing-Protokolls egp (Exterior Gateway Protocol)
- **transmission:** Objektbeschreibungen der LAN-Technologien der Schichten 1 und 2, also insbesondere Ethernet

Ergänzt wird der Baum durch herstellereigene so genannte private MIBs, die die Erfordernisse neuer Gerätetypen und deren spezieller Merkmale abdecken. Zur Auswertung dieser MIBs existieren MIB-Compiler und MIB-Browser, mit deren Hilfe sich SNMP-Requests absetzen und die vorhandenen MIB-Variablen graphisch und tabellarisch darstellen lassen.

11.1.5 SMI-Definition

Die Netzwerkmanagementdaten sind aber nicht nur in lesbarer Form, sondern auch in einer speziellen systemunabhängigen Syntax abgelegt. Die „Regeln zur Definition“ von managed objects und zum Erzeugen der Strukturen von MIBs werden SMI genannt. Die gesamte Management-Information ist in Management-Objekten strukturiert, zu deren Beschreibung SMI (Structure and Identification of Management Information) als Teilmenge von ASN.1 (Abstract Syntax Notation No. 1) verwendet wird. ASN.1 dient der unabhängigen Beschreibung von Daten, wird in der CCITT X.208 beschrieben und ist eine Sprache mit Syntax, Grammatik und Konventionen. Diese Teilmenge bildet letztlich die Management-Informationbasis, die damit kein Datenhaltungssystem, sondern ein logisches Datenmodell beschreibt. SMI legt fest, dass alle managed objects über einen Namen, eine Syntax und eine Kodierung verfügen müssen. Die Syntax definiert den Datentyp des Objects (z. B. „integer“ oder „string“) in ASN.1-Schreibweise, die Kodierung beschreibt die Formatierung der Daten für die Übertragung über Netzwerke. SMI Datentypen werden in drei Kategorien eingeteilt:

- **Einfache Typen** umfassen vier ASN.1-Konstrukte:
 - Integer als positive oder negative ganze Zahlen.
 - Octet Strings als geordnete Folge mehrerer Bytes.
 - Object ID als eindeutiger Wert der Menge aller Object Identifier.
 - Bit Strings als Zusammenfassung mehrerer bezeichneter Bits.
- **Anwendungsweite Datentypen:**
 - Netzwerkadresse.
 - Zähler wie z. B. der Anzahl empfangener Bytes auf einem bestimmten Port in 32-Bit oder 64-Bit-Darstellung.
 - Gauges als positive oder negative sich verändernde Zahl wie beispielsweise die Länge einer Warteschlange.

- Time-Tickets in Einheiten von 1/100-Sek, z. B. um die Aktivitätszeit einer Station festzustellen.
- Opaque als Datentyp, um beliebige Informationsketten, die keinem strikten Datentyp entsprechen, durch SMI zu nutzen.
- **Einfache Datenkonstrukte** zur Definition von Tabellen und Listen:
 - Zeilen als Element einer Tabelle. Jede Zeile kann einem der Typen : einfach oder applikationsweit entsprechen.
 - Tabellen bei der jede Zeile die gleiche Anzahl Spalten umfasst.

Die SMI für SNMPv2 basiert auf RFC 1443 – Textkonventionen zur Definition von Datentypen innerhalb der MIB-Module – und 1444 – Kompatibilitätsanforderungen. Außerdem legt sie zwei Zweige der Internet-MIB fest: Security 1.3.6.1.5. und SNMPv2 1.3.6.1.6



Beispiel: SMI

Die Variable genDiagnostics hätte als Object-Typ folgende Struktur:

```
genDiagnostics OBJECT-TYPE
```

```
SYNTAX INTEGER {
```

```
passed(1),
```

```
failed(2)
```

```
}
```

```
ACCESS read-only
```

```
STATUS mandatory
```

```
DESCRIPTION
```

```
The result of this .....
```

```
::={gen 4}
```

11.1.6 syslogd

syslog ist ein De-facto-Standard definiert in RFC 3164 und 3195 zur Übermittlung von Log-Meldungen in einem IP-basierten Netzwerk. Dabei werden die Fehlermeldungen nicht an der Konsole angezeigt, sondern an einen syslogd-Server gesendet. Dieser Mechanismus erlaubt eine zentrale Kontrolle und Auswertung von Alarmen und Fehlermeldungen. Wird der Server derart konfiguriert, dass er die Informationen über einen weiteren Dienst wie E-Mail oder SMS weiterleitet, kann syslogd als proaktives Medium verstanden werden, das auf Probleme aufmerksam macht, bevor sie eintreten. So kann ein Hinweis auf Temperaturschwankungen an einem Router auf ausgefallene Lüfter oder eine mangelhafte Klimatisierung hindeuten.

Auf den meisten Netzwerkgeräten besteht die Möglichkeit der Konfiguration von syslogd. Eine syslog-Nachricht besteht aus drei Komponenten:

- einer Selektor-Priority von einem Byte, die seinerseits zwei Teile umfasst: das Facility-Feld und das Severity-Feld. Damit lassen sich die Syslog-Meldungen entsprechend ihrer Herkunft und ihres Schweregrades klassifizieren. Das die letzten drei Bits des Priority umfassende Severity-Feld enthält einen numerischen Wert zwischen 0 und 7, wobei 0 die kritischste oder dringlichste Stufe ist. Das die ersten fünf Bits der Priority umfassende **Facility**-Feld enthält einen numerischen Wert, der den Dienst oder die Komponente angibt, der die syslog-Nachricht erzeugt hat.
- einem Header: hier ist ein Zeitstempel sowie Name oder IP-Adresse des Absenders der syslog-Nachricht vermerkt.
- den Nutzdaten.

Eine sehr verbreitete Implementierung ist syslog-ng, dessen Erweiterungen des Syslog-Protokolls mittlerweile als Industriestandard angesehen werden.

■ 11.2 Netzwerksicherheit

Die wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden infolge mangelnder Sicherheit erhöhen den Handlungsdruck, durch geeignete Maßnahmen das Risiko eines Missbrauchs der Netzwerkressourcen zu verhindern. Zu den gefährdeten Teilen eines Netzwerkes gehören letztlich alle Geräte, die ein Netzwerk bilden einschließlich der sie bedienenden Personen. Damit schälen sich Switches, Router, Endgeräte und Nutzer als die kritisch zu betrachtenden Komponenten heraus.

11.2.1 Allgemeine Bedrohungen

Mit der verstärkten Zunahme von E-Business-Anwendungen und der Nutzung des Internets allgemein, steigt auch das Risiko, Opfer einer Attacke zu werden. Administratoren geraten damit in die Zwickmühle einerseits einen bequemen Netzzugang für jedermann gewähren zu müssen, andererseits aber auch für die bestmögliche Sicherheit der Nutzung des Netzes zu sorgen. Dieser Spagat erfordert nicht nur Know-how über Gefährdungen, sondern auch die Kenntnis wie solchen Gefährdungen zu begegnen ist. Dabei gibt es zwei Strategien, um die Sicherheitsanforderungen umzusetzen:

- Jeder Dienst ist zugelassen, wenn er nicht explizit untersagt wurde. Dieses Vorgehen besitzt einige Vorteile: es ist einfach zu konfigurieren, komfortabel für die Nutzer und preiswert in der Wartung und Pflege.
- Im Gegensatz zum offenen Ansatz verbietet das restriktive Vorgehen alle Dienste, es sei denn, ein Dienst wird explizit freigegeben. Nachteilig hierbei sind die komplexere Konfiguration, die geringe Transparenz für die Nutzer und die höheren Kosten.

Die Entscheidung für eine dieser Sicherheitsstrategien entbindet eine Organisation jedoch nicht von der Notwendigkeit, eine verbindliche Sicherheitspolitik festzulegen. Sicherheitsrichtlinien beschreiben, wie sich die Organisation und ihre Mitarbeiter verhalten, um den Zugriff auf die physischen und logischen Ressourcen zu schützen. Bei der Definition kommen den Mitarbeitern unterschiedliche Rollen zu: die IT-Leitung formuliert die Richtlinien,

die Geschäftsführung setzt die Richtlinie um und sorgt für deren Beachtung, der Sicherheitsbeauftragte gewährleistet die Wirksamkeit indem er Audits durchführt und die Einhaltung überwacht, der Netzwerkadministrator erzwingt die Einhaltung der Regeln durch Geräte wie Firewalls oder Router, der Systemadministrator sorgt für Zugriffsberechtigungen und sichere Passwörter und die Mitarbeiter befolgen die Vorgaben.

In welchen Bereichen liegen Schwächen einer Netzwerkinfrastruktur, auf die eine Organisation ein besonderes Augenmerk richten sollte? Drei Kategorien lassen sich isolieren:

- **Technologische Schwächen** wie konzeptionelle Mängel des TCP/IP-Protokollstacks, Sicherheitslöcher im Betriebssystem oder zentralen Anwendungen wie Browser und die Möglichkeit Netzwerkgeräte zu manipulieren.
- **Konfigurationsmängel** wie unsichere Mitarbeiterzugänge oder Gästekonten, falsch eingerichtete Internetdienste und unsichere oder unveränderte Standardeinträge.
- **Lücken in der Sicherheitspolitik** wie fehlende Notfallpläne, unvollständige Backups, mangelnde Überwachung, keine geregelte Updatepolitik für Hard- und Software.

Aber auch physische Herausforderungen bestehen. Viele Netzwerkgeräte sind empfindlich gegenüber hohen Temperaturen und hoher Luftfeuchtigkeit. Auch muss eine kontinuierliche Stromversorgung gewährleistet sein. Neben diesen allgemeinen Aspekten besteht eine besondere Gefährdung für das Netzwerk, da es eine ständige Erreichbarkeit symbolisiert.

Zur Vorbereitung eines Angriffs könnte ein potentieller Angreifer mehrere Maßnahmen ergreifen:

- Informationen sammeln: Werkzeuge wie nslookup oder whois offenbaren Informationen über IP-Adressen und administrative Details.
- Ports scannen: der Angreifer versucht, offene Ports über aktive IP-Adressen zu finden.
- Pakete beobachten: Anwendungen wie wireshark erlauben den Mitschnitt des Netzwerkverkehrs.

Um sich Zugang zu einem System zu verschaffen, können als Folge der vorbereitenden Maßnahmen, mehrere Formen eines Angriffs eingeleitet werden:

- **Brute-Force** Angriffe zielen darauf ab, sich über das Erraten oder das systematische Ausprobieren von Passwörter Zugang zu einer Netzressource wie Server oder Router zu verschaffen.
- **Man-in-the-Middle** Angriffe lenken den Netzwerkverkehr auf den Rechner des Angreifers um.
- **Vertrauensverletzungen** versuchen, einen vertrauenswürdigen Rechner zu kompromittieren, um ihn für weitergehende Angriffe zu nutzen.

Eine weitere Angriffsform besteht darin, eine Netzressource derart zu beeinflussen, dass sie ihren Dienst einstellt. In diese Kategorie fallen:

- **Ping-of-Death** Angriffe, die größere als die erwarteten Pakete versenden und auf diese Weise ein Netzwerkgerät überfordern.
- **SYN-Flood** Angriffe, bei dem eine Netzressource mit Verbindungsaufbauwünschen überschwemmt wird, denen sie nicht mehr nachzukommen vermag.

- **Distributed Denial-of-Service** Angriffe, die von einer Vielzahl von Rechnern simultan gegen ein Netzwerkziel „gefahren“ werden und das Angriffsziel zwingen, seinen Dienst einzustellen.

Daneben existieren die Malware-Angriffe, die über das Einschleusen von Software versuchen, die Kontrolle über Netzgeräte zu erlangen, Ressourcen zu schädigen oder Informationen und Daten zu entwenden. Hierzu zählen:

- **Würmer** als Programme, die sich verbreiten indem sie Kopien von sich selbst erstellen und sich dann über Einträge z. B. im Adressbuch der E-Mail-Software an andere Ressourcen weiterleiten.
- **Viren** als eine Software, die ein Programm zur Ausführung unerwünschter Funktionen veranlasst. Viren benötigen einen Verteilungsmechanismus in Form einer ausführbaren Datei, eines ZIP-Files, eines Dokumentenmakros oder eines E-Mail-Anhanges.
- **Trojaner** als Programme, die vorgeben legitime Software zu sein, in Wahrheit jedoch versteckte schädliche Funktionen ausführen.

Jeder Typ eines Netzwerkangriffs verlangt eigene Verteidigungsvorkehrungen. Dazu gehören im Bereich der Hosts und Server eine Vielzahl von Techniken und Maßnahmen:

- **Gerätehärtung:** Unter diesem Begriff ist ein Bündel von Maßnahmen zu verstehen. Dazu gehören: der Wechsel von Standardvorgaben für Nutzernamen und Passwörtern, die Beschränkung des Zugriffs der Administratorressourcen, die Vermeidung der Installation unnötiger Geräte und Programme und eine zuverlässige Systemüberwachung.
- **Antivirus-Software:** Diese Software soll gegen bekannte Angriffstypen schützen und stets auf dem aktuellen Stand gehalten werden.
- **Personal Firewalls:** Sie stellen ein Mittel dar, um Rechner, die mit dem Internet verbunden sind, effektiver abzusichern.
- **Aktualisierung des Betriebssystems:** Sicherheitskorrekturen gewährleisten die Unverwundbarkeit gegen bekannte Fehler oder Schwächen.

Intrusion Detection Systeme stellen sich als eine umfassende Lösung dar, weil sie Angriffe gegen das Netzwerk versuchen zu erkennen oder in Form eines Intrusion Prevention Systems im Voraus zu erahnen.

11.2.2 Sicherheit für Switches und Router

Switches sind in erster Linie durch eine Fälschung der MAC-Adressen gefährdet. Durch Fälschungen dieser Art kann sich ein Angreifer als ein zulässiges Netzwerkgerät ausgeben und andere Rechner davon überzeugen, dass es unbedenklich ist, ihm Daten zu schicken oder Daten von ihm entgegenzunehmen. Dazu ändert der Angreifer seine MAC-Adresse in die eines am Switch registrierten Gerätes und verlangt nun geheime Informationen. Router sind von dieser Form des Angriffs nicht betroffen, weil sie mit IP-Adressen arbeiten. Um diese Angriffsform zu blockieren, besteht die beste Verteidigung darin, Server als diejenigen Geräte, die die begehrten Informationen besitzen, hinter einem Router zu platzieren. Damit hat das Design des Netzwerkes einen unmittelbaren Einfluss auf die Sicherheit.

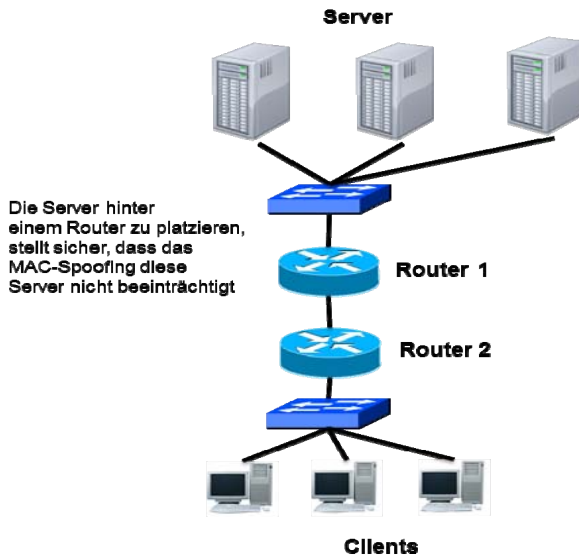


Bild 11.2 Server-Platzierung

Eine weitere Angriffsart gegen Switches besteht in der Manipulation der ARP-Tabellen. Dazu sendet der Angreifer ein Paket mit einer korrekten IP-Adresse, aber einer gefälschten MAC-Adresse. Die Empfänger dieses Paketes in Form eines Endgerätes oder Switches aktualisieren daraufhin seine ARP-Tabelle mit gefälschten Daten. Da ARP nicht prüft, ob die MAC-Adresse und deren Verknüpfung mit der angegebenen IP-Adresse gültig ist, bleibt diese Manipulation zunächst unbemerkt. Für den Angreifer ergeben sich damit drei Szenarien: Denial-of-Service, Man-in-the-Middle oder MAC-Flooding. Der beste Schutz gegen diese Form des Angriffs ist das Absichern des Switches. Ein Mittel ist die PortSecurity, bei der der Zugriff auf den Port eines Switches nur auf das erwartete Gerät – ausgedrückt durch die MAC-Adresse – beschränkt wird. Eine Verletzung führt dann zu einer abgestuften Reaktion: der Switch kann Nachrichten über die Verletzung versenden, er kann die empfangenen Pakete der unzulässigen MAC-Adresse verwerfen oder er kann alle an diesem Port empfangenen Pakete verwerfen und das Interface deaktivieren.



Um festzustellen, ob jemand das Netzwerk über ARP-Manipulationen angreift, existieren Intrusion Detection Systeme. Zu ihnen gehört das für UNIX-basierte Rechner kostenlose **Snort**. Um gefälschte Pakete zu erzeugen, gibt es Programme wie **Dsniff**, das Anwendungen wie **arpspoof** enthält.

Ziel eines Man-in-the-Middle-Angriffs ist es, sich unbemerkt in die Kommunikation zwischen zwei oder mehreren Partnern einzuschleichen, um Informationen mitzulesen oder zu manipulieren. Als erstes leitet der Angreifer eine Verbindungsanfrage des Senders auf seinen Rechner um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Gelingt ihm dies, kann er alle Informationen, die der ursprüngliche Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auch auf die Antworten des Empfängers kann der Angreifer nach dem gleichen Prinzip reagieren. Der schwie-

rigste Teil des Man-In-The-Middle-Angriffs besteht für den Angreifer darin, den Verbindungsaufbau auf sich umzuleiten. Hierzu dient die ARP-Manipulation.



Beispiel: WLAN-Angriff

Um Man-in-the-Middle-Attacken in einem WLAN durchzuführen, können zusätzliche Access Points in das WLAN eingeschleust werden („Rogue-APs“). Wenn ein derartiger Access Point einem in der Nähe befindlichen WLAN-Client eine stärkere Sendeleistung anbietet als der echte Access Point, wird der Client diesen als Basisstation nutzen. Voraussetzung für die unbemerkte Funktion ist, dass keine beidseitige Authentisierung erzwungen wird.

MAC-Flooding versucht die ARP-Tabelle zu „übervölkern“. Wenn ein Angreifer Pakete mit unterschiedlichen Quell-MAC-Adressen sendet, speichert der Switch diese MAC-Adressen in seiner ARP-Tabelle. Sobald der Speicherplatz für die ARP-Tabelle gefüllt ist, sendet ein Switch sämtliche Pakete an alle Switch-Port in Gestalt des Floodings. Durch dieses „Fluten“ mit sinnlosen MAC-Adressen kann ein Switch nicht mehr feststellen, an welche Ports tatsächliche Ziel-MAC-Adressen angeschlossen sind. Diese Angriffsmethode wird verwendet, um das Mitlesen von Paketen in geschwächten Netzen zu ermöglichen.

„Denial of Service“-Attacken zielen darauf ab, die Benutzer daran zu hindern, Dienste oder Geräte zu verwenden, die ihnen normalerweise zur Verfügung stehen. Dieser Angriff steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass andere Benutzer an der Arbeit gehindert werden. Im Fall der ARP-Manipulation werden Geräte des Netzwerkes dazu gebracht, Datenverkehr an eine gültige IP-Adresse zu versenden, der eine gefälschte MAC-Adresse zugeordnet ist. Sind alle ARP-Tabellen der Switches mit den Fehleinträgen versehen, schicken Rechner im Netz für den Router gedachten Verkehr an ein Gerät, das nicht existiert. Folglich gelangt kein Datenverkehr über den Router aus dem Netzwerk heraus.

Das wichtigste Werkzeug um Angriffe gegen Router abzuwehren, sind Access Control Lists (ACLs). Sie beschreiben in sequentieller Form, welche IP-Adressen oder Protokolle den Router passieren dürfen. Standardmäßig leitet ein Router den ihn erreichenden Netzwerkverkehr weiter, sofern für die Pakete ein Weg in der Routingtabelle existiert. ACLs schränken den Netzwerkverkehr nach Zulässigkeit ein. Der mit ACLs verbundene Prüfprozess benötigt Zeit, so dass die Latenz steigt. Besteht eine ACL aus einer Vielzahl von Einträgen, ist eine Kombination mit einer Firewall daher eine geeignetere Schutzmaßnahme als nur ACLs zu definieren.

ACLs sind Befehlslisten, die an ein Routerinterface gebunden sind und die zu akzeptierenden oder zu verwerfenden Pakete pro Richtung und Protokoll beschreiben. Um zu bestimmen, ob ein Paket akzeptiert oder blockiert wird, wird es gegen die Einträge der ACL geprüft. Sobald eine Prüfung erfolgreich ist, werden die folgenden Einträge übersprungen und das Paket entsprechend dem Test weitergereicht oder verworfen. ACLs werden üblicherweise in Standard- und Extended-ACLs unterschieden, je nach Komplexität der Prüfung. Die folgenden Abbildungen zeigen je ein Beispiel für beide Typen:

access-list 2 deny	172.16.1.1	
access-list 2 permit	172.16.1.0	0.0.0.255
access-list 2 deny	172.16.0.0	0.0.255.255
access-list 2 permit	172.0.0.0	0.255.255.255

Bild 11.3 Standard-ACL

access-list 114 permit tcp	172.16.6.0 0.0.0.255	any eq telnet
access-list 144 permit tcp	172.16.6.0 0.0.0.255	any eq ftp
access-list 114 permit tcp	172.16.0.0 0.0.0.255	any eq ftp-data

Bild 11.4 Extended-ACL

Die Konfiguration der ACLs geschieht über entsprechende Befehle, die eine Zugriffsliste definieren (z. B. Liste Nr 2), das zu schützende Interface (ethernet0) festlegen, die Richtung (in/out) beschreiben und die IP-Adressen, die geprüft werden sollen, präzisieren (172.0.0.0).

Router (config)#		
access-list 2 deny	172.16.1.1	
access-list 2 permit	172.16.1.0	0.0.0.255
access-list 2 deny	172.16.0.0	0.0.255.255
access-list 2 permit	172.0.0.0	0.255.255.255
interface ethernet 0		
ip access-group 2 in		

Bild 11.5 Konfiguration einer ACL

Am Ende jeder ACL legt ein implizites deny any fest, dass alle Pakete, die keinem Kriterium entsprechen, verworfen werden. Da die Prüfung in sequentieller Reihenfolge stattfindet, kommt der Anordnung der Einträge eine große Bedeutung zu. Spezifische Prüfungen sollten daher möglichst vor allgemeinen und häufig auftretende vor seltenen platziert werden.

■ 11.3 Zusammenfassung

Eine der wesentlichen Aufgaben für die Überwachung und Fehlersuche in Netzwerken ist die Festlegung einer „baseline“. Eine „baseline“ zeigt das Netzwerk mit seinen kritischen Parametern im laufenden störungsfreien Betrieb. Sie spiegelt faktisch die „Netzwerkgesundheit“ wider und stellt die Referenz beim Auftreten von fehlerhaften Situationen dar.

Die Messung der Funktionsfähigkeit eines Netzwerkes ist häufig das Ergebnis der Reports des Netzwerkmanagements oder von konkreten Messungen durch ping oder traceroute.

Für die Behebung unmittelbarer Fehlerzustände wird ein strukturiertes Vorgehen empfohlen, dem mehrere Phasen zu Grunde liegen:

1. die genaue Identifikation und Isolierung des Problems
2. die Prüfung, ob das Problem wiederholt erzeugt werden kann
3. die Lokalisierung der Ursache durch ein Vorgehen nach dem Prinzip des divide-and-conquer
4. die Formulierung und Implementierung einer Lösung des Problems
5. die Prüfung, ob der Fehlerzustand tatsächlich behoben ist
6. die Dokumentation des Problems mit seiner Lösung für die Behebung zukünftiger, ähnlich gelagerter Fälle

Die ideale Strategie ist naturgemäß eine proaktive, bei der Fehler gar nicht erst auftreten, sondern bereits im Vorwege erkannt werden. Um dieser Vorstellung zu genügen, muss der Netzwerkverkehr überwacht und hinsichtlich seines Durchsatzes und seiner Güte beurteilt werden. Hierzu bedarf es ausführlichen statistischen Materials und realistischer Prognosen der zukünftigen Entwicklung des Datenaufkommens. Damit wird klar, dass es sich hier um eine schwierige und bedeutsame Frage handelt, die vor allem die Zukunftsfähigkeit der bestehenden Infrastruktur und die Zufriedenheit der Nutzer betrifft. Ohne ein ausreichendes Antwortzeitverhalten bei gleichzeitig hohem Sicherheitsniveau ist keine Benutzerakzeptanz zu erlangen. Netzwerkmanagement und Sicherheit werden folglich zu Themen, die zentrale Bedeutung für die Basisinfrastruktur heutiger Unternehmen besitzen.

■ 11.4 Wissensüberprüfung

1. Können Bootsektoren von Viren infiziert werden und was wäre der Schaden?
2. Wie unterscheiden sich Würmer von Trojanern?
3. Weshalb sollten ACLs in Routern möglichst wenige Einträge beinhalten?
4. Wie müsste eine ACL aussehen, die Verkehr des Subnetzes 172.16.4.0 blockiert und allen weiteren ausgehenden Verkehr an das Interface Ethernet0 zulässt?
5. Lässt sich ICMP-Datenverkehr durch eine ACL unterbinden?
6. Welche SNMP-Aktion wird von einem Agent ausgelöst und warum?
7. Können Einträge in einer MIB verändert werden?
8. Geben Sie einen Überblick über die Mächtigkeit des Befehls netstat.
9. Welche Bedeutung besitzt der Community-String in SNMP?
10. Welche Basisfunktionalität sollte ein Netzwerkmanagementtool besitzen?

Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Was sind die Komponenten eines Wireless LANs?
- Wie arbeitet ein WLAN?
- Welche Architekturen stehen zur Auswahl?
- Welche Pakettypen dienen welchem Zweck?
- Wie steht es um die Sicherheit?

Kapiteleinführung

Unaufhaltsam dringen Wireless LANs (WLANs) in das Blickfeld der Anwender. Neue Entwicklungen, die gebührenfreie Nutzung der Funk-LAN-Technik, die Erhöhung der Reichweite und die Existenz von Standards versprechen für die Zukunft ein weiter wachsendes Interesse.

WLANs gehören in die Gruppe der lokalen Netze, wie es der Name bereits ausdrückt. Wie die kabelgebundene Technik Ethernet besitzen sie das gleiche Einsatzspektrum und decken einen ähnlichen Entfernungsbereich ab. Allerdings besteht eine Abhängigkeit von lokalen Gegebenheiten. Im Idealfall werden in Gebäuden 30 m und im Freiraum 300 m überbrückt. Der Einsatz von Antennen erlaubt es, diese Entfernungen auszudehnen. Die Übertragungsraten liegen im Bereich von 600 Mbit/s und reichen damit an die Leistung kabelgebundener Netzwerke heran.

WLANs vergrößern die Netzausdehnung durch die Abdeckung von kabelgebunden nicht erreichbaren Bereichen. Ihre Vorteile schöpfen sie aus mehreren Eigenschaften:

- **Installationsgeschwindigkeit und Einfachheit** – WLANs können leicht und ohne den Verlegeaufwand kabelgebundener Netze installiert werden.
- **Flexibilität** – Bereiche, die durch Kabel nicht zugänglich sind, oder wo aufgrund von Denkmalschutzbestimmungen keine Kabel verlegt werden dürfen, werden problemlos abgedeckt.
- **Skalierbarkeit** – WLANs können an praktisch jede Topologie angepasst werden. Ihr Einsatzspektrum reicht von Netzen mit wenigen Nutzern bis zu Infrastrukturen mit Tausenden von Knoten.

Im Gegensatz zu LAN-Technologien wie Ethernet, die ihre Signale durch eine kabelgebundene Infrastruktur transportieren, nutzen WLANs elektromagnetische Wellen aus dem Mikrowellenbereich, ohne eine physikalische Infrastruktur vorauszusetzen. Mehrere Sender können im gleichen Raum zur gleichen Zeit existieren, ohne sich zu stören, sofern sie auf unterschiedlichen Radiowellen übertragen. Um Daten zu extrahieren, wählt der Empfänger eine Frequenz aus und verwirft die anderen. In einer typischen WLAN-Konfiguration verbindet ein Access-Point das kabellose Netz mit der kabelgebundenen LAN-Technologie. Dieser Access-Point empfängt, speichert und überträgt die Daten zwischen WLAN und LAN. Access-Points sind Teil der drahtgebundenen Infrastruktur und als solche nicht mobil. Sie sind vergleichbar den Basisstationen der Mobiltelefonie. Im Aufbau vereinen sie einen Hub und eine Bridge in der Form, dass das Hubelement die Verbindung der WLAN-Clients herstellt und die Bridgekomponente die Weiterleitung des WLAN-Paketes an das LAN vornimmt. Nahezu jeder Endknoten besitzt heutzutage eine WLAN-Karte. Sie besteht aus einer Antenne, einer Übertragungseinheit und der Möglichkeit, analoge elektromagnetische Wellen in digitale Impulse des Rechners zu konvertieren. Die Existenz einer drahtlosen Verbindung ist für Betriebssysteme weitgehend transparent.

■ 12.1 IEEE-802.11-Standards

Seit 1997 existiert für WLANs der Standard IEEE 802.11, der Übertragungen von ein oder zwei Mbit/s im 2,4-GHz-Band auf dem physikalischen Layer und der MAC-Schicht definiert. Der LLC-Bereich verwendet wie die anderen 802-Standards eine 48-Bit-Adressierung, so dass ein einfaches Bridging zwischen Wireless und Wired LAN möglich ist.

Für die drahtlose Übertragung kommen drei lizenzfreie Frequenzbänder in Frage. Die beiden Bänder im Gigahertzbereich werden durch die aktuellen Standards genutzt. Ein hervorstechender Unterschied liegt in der Reichweite. Hier gilt: je geringer die Wellenlänge (höhere Frequenz) ist, desto größer fällt die Signaldämpfung aus bzw. je länger die Wellenlänge (geringe Frequenz) ist, desto geringer ist die Signaldämpfung. Daher fällt tendenziell die Dämpfung im 5 GHz-Band stärker ins Gewicht vgl. Tabelle 12.1. Standards in diesem Bereich verfügen folglich über eine geringere Reichweite.

Tabelle 12.1 Frequenzbänder für Wireless

Frequenzbereich	Name	Verwendung
900 KHz	Industrial, Scientific, Medical (ISM)	schnurlose Telefone
2,4 GHz	Industrial, Scientific, Medical (ISM)	802.11b und 802.11g: 2.4 - 2.5 GHz
5 GHz	Unlicensed National Information Infrastructure (U-NII)	802.11a: 5.725 - 5.875 GHz

Einen Überblick über die allgemeine Frequenzbelegung gibt die folgende Abbildung. Insbesondere in Hinblick auf potentielle Störquellen zeigt sich, dass der Mikrowellenbetrieb Auswirkungen auf eine WLAN-Infrastruktur haben kann. In der Praxis ergeben sich jedoch eher geringe Interferenzen.

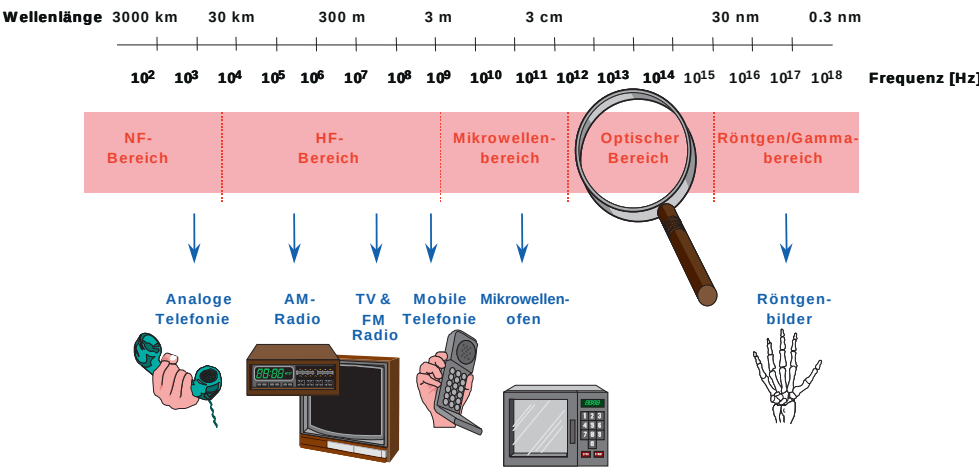


Bild 12.1 Frequenzbänder verschiedener Anwendungen

Ende 1999 wurde die erste Definition zur Version 802.11b erweitert. Bei ausreichender Qualität des Funkweges erhöht sich die Übertragungsgeschwindigkeit von 1 bzw. 2 Mbit/s auf 5,5 bis 11 Mbit/s. Das Umschalten zwischen den einzelnen Geschwindigkeiten erfolgt adaptiv in Abhängigkeit von der Qualität der Funkverbindung. Zeitgleich entstand der Standard 802.11a, der allerdings mit der 5 GHz-Frequenz arbeitet. Seit 2010 existiert die Variante 802.11n, die eine Geschwindigkeit von nominal 600 MBit/s aufweist. Die folgende Tabelle stellt die wichtigsten Merkmale der bisherigen Standards einander gegenüber:

Tabelle 12.2 WLAN-Standards

Merkmal	802.11a	802.11b	802.11g	802.11n
Datenrate	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, abhängig von SNR	1, 2, 5.5, 11 Mbit/s, abhängig von SNR, Nutzdatenrate max. ca. 6 Mbit/s	6, 12, 24 Pflicht, 18, 36, 48, 54 optional	150, 300, 450, 600 MBit/s
Standardisierungsjahr	1999	1999	2003	2010
Modulationsverfahren	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DHSS)	OFDM	MIMO-OFDM
Reichweite	100 m Außen-, 10 m Innenbereich	300 m Außen-, 30 m Innenbereich	300 m Außen-, 30 m Innenbereich	300 m Außen-, 70 m Innenbereich
Frequenz	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz und 5 GHz

Tabelle 12.2 WLAN-Standards (*Fortsetzung*)

Merkmal	802.11a	802.11b	802.11g	802.11n
Kanäle	23 davon 12 nicht überlappend	11 davon 3 nicht überlappend	11 davon 3 nicht überlappend	
Sicherheit	WEP/WPA2	WEP/WPA2	WEP/WPA2	WPA2
Verwaltbarkeit	begrenzt (keine automatische Schlüsselverteilung, symmetrische Verschlüsselung)	begrenzt (keine automatische Schlüsselverteilung, symmetrische Verschlüsselung)	begrenzt (keine automatische Schlüsselverteilung, symmetrische Verschlüsselung)	

Entwicklungsschwerpunkt für IEEE 802.11 ist die Kommunikation in Gebäuden. Es unterstützt wie die bisherigen Konzepte auf Ethernet-Grundlage einen Best-Effort-Dienst mit der Option, zeitkritische Anwendungen zu einem späteren Zeitpunkt zu integrieren.

WLANs auf Basis des 802.11n Standards versprechen wesentlich höhere Geschwindigkeiten. Die maximale Datenrate von bis zu 600 MBit/s wird durch neue Modulationsverfahren und die Verwendung eines 40 MHz breiten Übertragungskanals erreicht. Davon geht zwar durch den Protokoll-Overhead und interne Daten für die Netzsteuerung einiges verloren, dennoch lässt sich eine nutzbare Übertragungsrate von 150 MBit/s erwarten. Zudem werden mehrere Antennen eingesetzt. Dieser Mechanismus wird als „Multiple Input Multiple Output“ (MIMO) bezeichnet. Er beruht auf dem Multipath-Phänomen, das unterschiedliche Ausbreitungswege eines Funksignals durch Reflexionen an Wänden, Einrichtungsgegenständen und Menschen beschreibt. Dabei trifft das gesendete Signal mehrfach, zeitlich verzögert und mit unterschiedlicher Signalstärke beim Empfänger ein. Dort werden die Signale überlagert und erscheinen als Verwischung des Ausgangssignals. Die MIMO-Technologie nutzt diesen Effekt für die Übermittlung der Signale über mehrere Pfade und etabliert damit simultane Datenübertragungen. In der Regel soll über drei Antennen gleichzeitig gesendet und empfangen werden. Sind mehrere Empfänger mit eigenen Antennen vorhanden, kann das Gemisch aus unterschiedlichen Datenströmen entwirrt werden. Dabei steigt die Datenrate linear mit der Anzahl der Sender-/Empfängerverbindungen. Bei drei Sender-/Empfängerantennen, die einzeln mit 54 MBit/s übertragen, ergibt sich ein Volumen von $0,7 \times 3 \times 54 \text{ MBit/s} = \text{ca. } 113 \text{ MBit/s}$ mit 0,7 als Korrekturfaktor. Werden Antennen im Abstand einer halben Wellenlänge der Trägerfrequenz genutzt, erhält der Empfänger zusätzliche Informationen über die Einfallsrichtung der Funkwellen. Dadurch lässt sich die räumliche Signatur (Spatial Signature) zweier Signale unterscheiden und die Kanalkapazität steigern. Wird das Sendesignal von mehreren Antennen ausgestrahlt, ist es möglich, durch die zeitliche Verzögerung eine Richtwirkung an den Antennen zu erreichen. Dieses Verfahren ist als Beamforming bekannt.

Eine weitere Neuerung gegenüber den bisherigen WLAN-Spezifikationen ist ein Stromsparprotokoll. Der PSMP-Mechanismus (Power Save Multi Poll) sorgt dafür, dass 802.11n-Geräte bei Inaktivität in einen Schlafmodus übergehen. Dieser Modus ist insbesondere für VoIP-Geräte von Bedeutung, bei denen das Verkehrsmuster durch kurze Über-

tragungsdauern und längere Ruheperioden gekennzeichnet ist. Auf diese Weise reduziert sich der Stromverbrauch trotz höherer Datenraten.

Bei der Migration auf den 802.11n-Standard sind einige Besonderheiten zu beachten. Durch die gesteigerte Datenrate können die bisherigen WLAN-Switches nicht mehr die gleiche Zahl von Access-Points überwachen, sondern lediglich eine reduzierte Zahl. Da die Access-Points nun Stationen höherer Geschwindigkeit verbinden, ist zudem eine Gigabit-Ethernet Anbindung an das LAN erforderlich. Einen weiteren Problemfall könnte die Power over Ethernet-Versorgung darstellen. Werden gleichzeitig das 2,4- und das 5 GHz-Band genutzt, reicht die Energieversorgung mit maximal 15,4 Watt nicht aus.

■ 12.2 Wireless-Architekturen

Ein 802.11-WLAN basiert in seiner üblichen Form auf einer Zellenstruktur. Jede Zelle (Basic Service Set BSS) wird durch eine Basisstation (Access-Point) kontrolliert. Obwohl für den Aufbau eines WLAN bereits eine einzelne Zelle ausreicht, bestehen die meisten Installationen aus mehreren BSS, deren Access-Points eine Art Backbone (Distributed System) bilden. Dieser Backbone nutzt üblicherweise Ethernet als LAN-Technologie. Das gesamte WLAN wird von den höheren Schichten des OSI-Modells als einzelnes 802-Netz betrachtet.

Für die Topologie von WLANs existieren vier Möglichkeiten:

- Bei **Ad hoc-Netzen** sind zwei oder mehrere mobile Funkstationen in Reichweite, die untereinander Daten austauschen können. In diesem Modus kommuniziert jeder Rechner mit jedem anderen, ohne die Existenz eines Servers oder eines LAN-Anschlusses zu benötigen, d.h. es existiert keine feste Kommunikationsinfrastruktur. Diese Art des Netzaufbaus bildet die Alternative für den kurzfristigen Aufbau für Konferenzen oder temporäre Arbeitsgruppen.
- Einen Schritt weiter geht das „Basic Service Set“ (BSS), das **als Infrastruktur-Modus** den einzelnen Funkstationen Zugang zum drahtgebundenen LAN über einen Access-Point gewährt. Daher benötigt der Access-Points einen Ethernet-Anschluss. Der **Access Point (AP)** konvertiert 802.11 Frames in Ethernet und umgekehrt und wird deshalb oft als Translation Bridge bezeichnet. Die gesamte BSS Kommunikation läuft über den AP. Stationen kommunizieren **nicht** direkt miteinander, sondern immer über den AP.

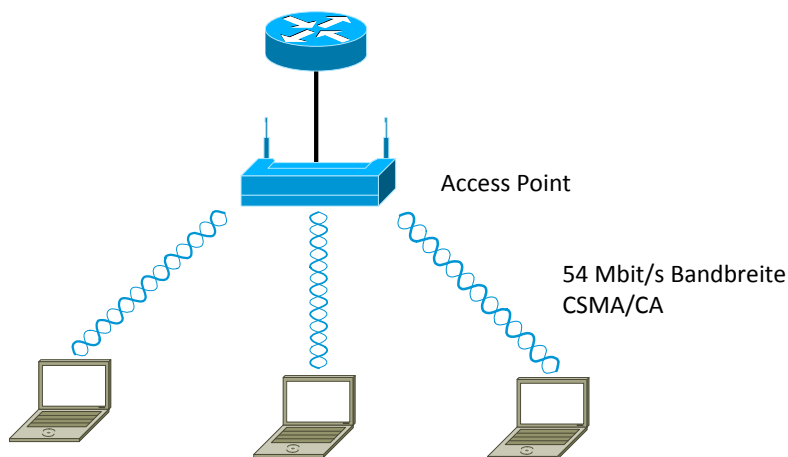


Bild 12.2 Infrastruktur-Modus

- Die letzte Erweiterungsmöglichkeit stellt ein „**Extended Service Set**“ (ESS) dar, das aus mehreren BSS-Zellen besteht. **Mehrere APs** bilden ein Wireless LAN, das einen höheren Abdeckungsbereich hat und Roaming erlaubt. Die **SSID** ist die gleiche für alle BSS in der ESS (wenn nicht mehrere BSSs eingerichtet werden).
- Ferner können Access-Points als Funkbridges miteinander kommunizieren und auf diese Weise zwei drahtgebundene LANs koppeln, die sich in zwei unterschiedlichen Gebäuden befinden. Dabei dürfen auch Grundstücksgrenzen überschritten werden. Hierfür bedarf es keiner Genehmigung durch die Regulierungsbehörde, sondern lediglich der Anzeige einer eingerichteten Funkverbindung.

■ 12.3 Kodierungsverfahren und Kanäle

Wie jedes andere 802.x-Protokoll deckt auch der 802.11-Standard den MAC- und den physikalischen Layer ab. Dazu definiert der Standard eine MAC-Schicht, die mit mehreren möglichen Schicht-1-Varianten zusammenarbeitet: Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) und Orthogonal Frequency Division Multiplexing (OFDM). Die Techniken arbeiten im Industrial-Science-Medical-Frequenzband (ISM). Wie Tabelle 12.1 zeigt, werden nur das DSSS- und das OFDM-Verfahren in Standards genutzt.

Der Standard 802.11b basiert auf dem DSSS-Verfahren. Das Prinzip dieses Verfahrens besteht darin, dass sowohl Sender als auch Empfänger ein- bis zweimal pro Sekunde die Trägerfrequenz wechseln. Die genaue Abfolge kennen nur der Absender und der Adressat. 802.11 sieht bis zu 79 nicht überlappende Frequenzbereiche mit einer Bandbreite von 1 MHz vor, wobei drei Gruppen zu je 26 Mustern zusammengefasst werden.

Das DSSS-Verfahren verwendet zur Erhöhung der Übertragungsrate ein spezielles Kodierungsverfahren, das allerdings die Reichweite verkürzt. Es teilt das 2,4-GHz-Band in 13 Kanäle mit einer Breite zu je 22 MHz auf, so dass sich die Kanäle teilweise überschneiden und nur drei Kanäle existieren, die keine gemeinsame Frequenz besitzen.

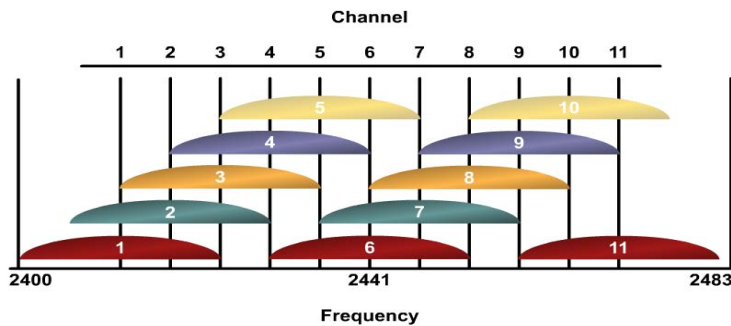


Bild 12.3 Kanäle des DSSS-Verfahrens

Für die Übertragung wird ein Kanal ausgewählt und das Signal mit zwei Methoden behandelt:

1. DSSS verwirklicht die Frequenzspreizung durch die Verknüpfung der Daten mit einer Zufallszahlenfolge. Für einen Dritten verschwindet so das Nutzsignal im Grundrauschen und nur der berechtigte Empfänger kann dieses herausfiltern.
2. Die Kombination mit Pseudozufallszahlen dehnt das Leistungsspektrum über den verfügbaren Frequenzbereich aus. Dabei ergibt sich eine Bandbreite von 22 MHz pro Sequenz. Allerdings werden für eine zuverlässige Implementierung 25 MHz benötigt, um Interferenzen zwischen den Kanälen zu vermeiden. Im verfügbaren 80-MHz-Spektrum lassen sich daher drei gleich breite, sich nicht überlappende Kanäle unterbringen. So ist es z.B. möglich, drei Access-Points in unmittelbarer Nähe zueinander zu platzieren, um die Bandbreite auf das Dreifache zu steigern. Das bedeutet aber nicht, dass eine Endstation über die gesamte akkumulierte Bandbreite verfügen kann, da ein Endgerät zur gleichen Zeit nur mit einem Access-Point verbunden sein darf.

OFDM wird von 802.11a verwendet. OFDM nutzt mehrere Frequenzen für eine simultane Übertragung. Jedes Signal belegt seinen eigenen Frequenzbereich. OFDM belegt orthogonale Frequenzen, die eine Überlappung ohne Interferenzen erlauben. Dazu teilt OFDM die Frequenzen in mehrere Teilfrequenzen, die eine parallele Übertragung gestatten. Jede Frequenz ist 20 MHz breit und wird ihrerseits in 52 Teilkanäle mit 300 KHz Breite unterteilt. OFDM verwendet 48 dieser Teilkanäle für die Datenübertragung und vier für die Fehlerkorrektur. Durch die geringeren Frequenzabstände nutzt OFDM das Spektrum sehr effizient.

Generell richtet sich die dem Benutzer zur Verfügung stehende Bandbreite nach der Dichte der Access-Points. Diese Dichte ist wiederum abhängig von der Sendeleistung der einzelnen Access-Points und deren Abdeckungsgebiet. Demzufolge ist die richtige Platzierung der APs eine der wichtigsten Aufgaben. Werden in einer Umgebung zwei Access-Points parallel eingesetzt, so verdoppelt sich die verfügbare Bandbreite. Voraussetzung ist allerdings, dass nicht überlappende Kanäle verwendet werden. Mögliche Kanalpaare wären: 1 und 6, 1 und 11 bzw. 6 und 11.

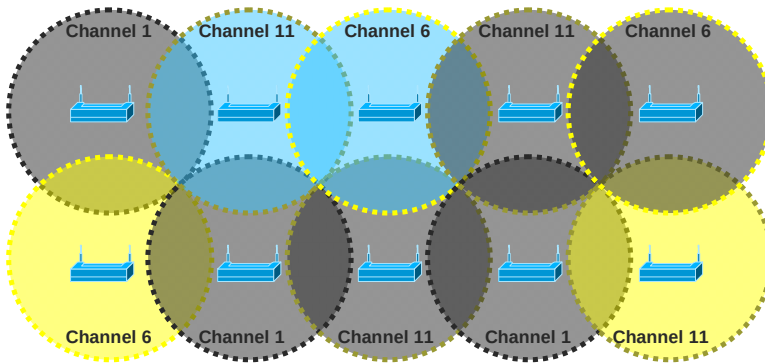


Bild 12.4 Kanalabdeckung

■ 12.4 Zugriffsmethoden: CSMA/CA

Anders als bei der Switching-Technologie für Ethernet lässt sich das Signal eines Rechners nicht isolieren, so dass Stationen, die zur gleichen Zeit senden, Kollisionen erzeugen mit der Folge, dass kein Empfänger die Nachricht zweifelsfrei erkennt. Zusätzlich kann eine WLAN-Station nicht gleichzeitig senden und empfangen und damit auch keine Kollision identifizieren. Um diese Schwierigkeiten zu umgehen, wird das CarrierSenseMultipleAccess-Verfahren mit Collision Avoidance (CSMA/CA) eingesetzt. Dieses Verfahren dient als Steuerungsinstanz, die jeder Station Sende- und Empfangsmöglichkeiten einräumt, Sendekonflikte vermeidet und die Datenintegrität erhält. Der Verfahrensablauf stellt sich wie folgt dar:

1. Wie im bekannten CSMA/CD-Ablauf des Ethernets hört eine sendewillige Station das Übertragungsmedium ab.
2. Um ein gleichzeitiges Senden mehrerer Stationen zu verhindern, wird eine **DIFS-Zeitspanne** (Distributed Interface Space) gewartet. Nach Ablauf der DIFS, können Knoten sich um den Zugriff bewerben.
3. Für die konkrete Zuteilung der Sendeberechtigung wird eine Zufallszeitspanne gewartet, die für jede Station individuell ist. Die Nutzung des **random backoff algorithm** dient zur differenzierten Zuteilung des Mediums an die sendewilligen Stationen. Der vom **random backoff algorithmus** gewählte Wert liegt zwischen **0 und 255**. Die Station mit der geringsten Zahl gewinnt den Auswahlprozess.
4. Nach Ablauf der Zufallszeitspanne vergewissert sich die Station, dass das Medium weiterhin unbelegt ist und beginnt die Übertragung. **Andere Stationen** sehen die Übertragung und müssen warten, da es sich wie im Ursprungsethernet um ein Shared Medium handelt.
5. Nachdem der Rahmen vollständig übertragen ist, wird ein Acknowledgement erwartet.
6. Trifft keine Bestätigung ein, wird der Rahmen erneut gesendet.

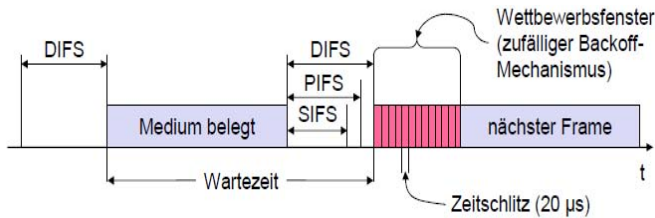


Bild 12.5 CSMA/
CA-Ablauf (Quelle: Piger,
Grimm RRZN Hannover)

Backoff ist eine Methode, um Stationen, die gemeinsam um ein Medium konkurrieren, einen gesicherten, wohldefinierten Zugang zu verschaffen. Die Idee verlangt das unabhängige Ziehen von Zufallszahlen aus einem bestimmten Bereich. Unter ständigem Prüfen, ob eine andere Station bereits das Medium belegt hat, wartet eine Station die durch den Zufallswert angezeigte Anzahl Slot Times, bevor sie selbst zugreifen darf. Die Größe dieser Zeitschranke ist dabei so festgelegt, dass eine Station jeweils erkennen kann, ob ein Konkurrent das Medium mit Beginn der vorangegangenen Slot Time zugeteilt bekommen hat. Bei wiederholten Kollisionen wird der Wertebereich der Zufallszahlen exponentiell ausgedehnt.

Diese Art des Vorgehens ist bei geringer Auslastung sehr effektiv, der Wirkungsgrad nimmt aber ab, wenn viele Stationen simultan senden möchten.

In drahtlosen Umgebungen tritt ein weiteres Problem auf: es kann nicht vorausgesetzt werden, dass sich alle Stationen gegenseitig „hören“. Dieses Problem wird als „Hidden Node“ bezeichnet und tritt auf, wenn zwei Knoten im Bereich des Access-Points liegen, sich aber nicht „sehen“. Die Tatsache, dass eine Station das Medium als frei identifiziert, bedeutet folglich nicht, dass kein anderer Teilnehmer bereits eine Übertragung eingeleitet hat. Um die Wahrscheinlichkeit zu reduzieren, dass die Sendungen zweier Teilnehmer kollidieren, die sich nicht hören, also über eine dritte Station miteinander kommunizieren, führt der Standard ein Virtual-Carrier-Sense-Konzept ein. Sind z. B. drei Stationen A, B und C in einer Funkzelle vorhanden und C möchte Daten an B senden, könnte bereits eine Kommunikation zwischen A und B stattfinden, die außerhalb des Empfangsbereiches von C liegt. C erkennt dieses Muster nicht und versucht ebenfalls an B zu übertragen. Um diese Situation zu vermeiden, wird die Distributed Coordination Function (DCF) implementiert:

- Eine sendewillige Station verschickt zunächst nur ein verkürztes Paket RTS (Rquest to Send), das die Quelle, das Ziel und die Dauer der nachfolgenden Übertragung enthält und als Anmeldung interpretiert wird.
- Der Access Point empfängt das RTS-Paket und antwortet mit einem Kontrollpaket CTS (Clear to Send), das die gleichen Informationen ergänzt um die Dauer der Übertragung enthält. Alle Stationen des WLAN empfangen bei diesem Ablauf entweder das RTS- oder das CTS-Paket und können für die darin angegebene Dauer ihren Übertragungswunsch unterdrücken.
- Die sendewillige Station muss das CTS-Paket zurückerhalten, bevor sie die Datenübertragung beginnen darf.
- Dieser Mechanismus reduziert die Wahrscheinlichkeit einer Kollision erheblich, da während des RTS-Zeitfensters keine weiteren Übertragungen eingeleitet werden können. Der RTS/CTS-Handshake kontrolliert also die Nutzung des Shared Mediums.

- Allerdings gilt auch, dass für den Fall, dass das WLAN keine Hidden Nodes aufweist, RTS/CTS lediglich den Overhead vergrößert und keine positiven Auswirkungen auf die Übertragungsgeschwindigkeit ausübt.

Der Ablauf zeigt, dass im Falle einer Sendung die Quelle, ein positives Acknowledgment (ACK) erwartet. Diese Rückversicherung kann bis zu 50 % der verfügbaren Bandbreite ausmachen. Ein weiterer einschränkender Faktor besteht in der Adaptive Rate Selection (ARS). Die Übertragungsrate fällt je nach Signalstärke bei 802.11 b/g in Stufen von 11 Mbps auf 5,5 Mbps, von 5,5 Mbps auf 2 Mbps oder 2 Mbps auf 1 Mbps zurück.

12.4.1 Besonderheiten

Typische LAN-Technologien verwenden Pakete, die eine Länge von mehreren hundert Bytes aufweisen. In WLAN-Umgebungen sprechen mehrere Gründe für kleine Übertragungseinheiten:

- Gemäß der höheren Bitfehlerrate bei drahtloser Kommunikation wächst die Wahrscheinlichkeit beschädigter Pakete mit steigender Paketgröße.
- Je kleiner die Pakete im Falle einer Beschädigung sind, desto weniger Overhead verursacht eine Retransmission.

Fragmentierung bildet daher ein optionales Merkmal des 802.11-Standards für Unicast-Sendungen. Da die Quellstation die einzelnen Fragmente unabhängig voneinander überträgt, erhält sie auch die Bestätigungen für jedes Einzelpaket. Zur Kontrolle der Vollständigkeit einer Sendung, schließt das Sequence-Control-Feld jeden Headers eine Fragment-Nummer ein, anhand derer eine Rekonstruktion möglich ist. Analog zum IP-Header zeigt ein Flag „More Fragments“ an, ob das Paket Teil eines Datenstroms ist. Die Verwendung der Fragmentierung kann die Zuverlässigkeit der Übertragung steigern, da mit kleinen Paketen auch die Wahrscheinlichkeit von Kollisionen abnimmt. Typische Werte der Paketgröße liegen zwischen 256 und 2048 Bytes. Dennoch kann der bessere Weg zur Vermeidung von Kollisionen im RTS/CTS-Verfahren gesehen werden.

Zur Differenzierung unterschiedlicher Stationszustände kennt der WLAN-Standard vier Inter-Frame-Space-Typen:

- **SIFS (Short Inter Frame Space)** ist der Zeitraum, den eine Empfängerstation wartet, bevor sie ein Acknowledgement sendet. Der Wert wird durch die physikalische Schicht bestimmt und beträgt derzeit 28 ms.
- **PIFS (Point Coordination IFS)** wird ausschließlich vom Access-Point genutzt und definiert die Zeitspanne, die erforderlich ist, um vor allen anderen Stationen Zugriff auf das Medium zu bekommen. Sie ist die Summe aus SIFS und Slot Time und beträgt 78 ms.
- **DIFS (Distributed IFS)** bezeichnet die Zeitspanne, für die eine Station ihren Übertragungswunsch zurückstellen muss. Ihr Wert berechnet sich als Summe von PIFS und Slot Time und beträgt 128 ms.
- **EIFS (Extended IFS)** beschreibt die Zeitspanne, die eine Station benötigt, um ein empfangenes, aber „unverständliches“ Paket zu analysieren. Diese Funktion ist notwendig,

damit eine Station keine Kollisionen mit zukünftigen Paketen des aktuellen Dialogs auslöst.

12.4.2 Anmeldeverfahren

Aufgrund des „unsicheren“ Mediums Luft begnügt sich eine WLAN-Karte nicht wie ihre kabelgebundenen Gegenstücke mit einem einfachen Link-Status. Sie verlangt eine Einbuchung beim Access-Point nach festgelegten Regeln. Dieser Prozess durchläuft drei Phasen:

Als ersten Schritt muss eine Station herausfinden, bei welchem Access-Point sie ankopeln darf, um die Mitgliedschaft zu einem BSS zu erhalten. Dazu durchläuft die Station die verfügbaren Kanäle und prüft, ob die SSID des empfangenen WLAN mit der konfigurierten SSID übereinstimmt. Um diese Prüfung durchzuführen, existieren zwei Methoden:

- Beim **passiven Scanning** wartet die Station ohne eigene Aktivität auf den Erhalt eines Beacon Frames vom Access-Point. Beacon Frames werden vom Access-Point in regelmäßigen Abständen verschickt. Sie enthalten die SSID und die Station vergleicht die empfangene mit der konfigurierten SSID. Diese Methode bietet sich bei öffentlich zugänglichen WLANs an.
- Im Falle des **aktiven Scanning** teilt der AP die SSID nicht im Beacon-Frame mit. Der Teilnehmer versucht, den zugehörigen Access-Point durch Probe Request Frames, die die gewünschte SSID enthalten, ausfindig zu machen. Die Station registriert die Antworten auf diese Broadcast und besitzt demzufolge nach kurzer Zeit ein genaues Bild der WLAN-Infrastruktur. Aus der Tabelle aller vorhandenen Access-Points wird gemäß der SSID der entsprechende Access-Point ausgewählt.

Anschließend durchläuft die Station einen Authentifikationsprozess, zu dem auch der Austausch von Passwörtern gehören kann. Verbreitet ist momentan die Open-System-Authentifizierung, bei der der AP die Station ohne weitere Prüfung zulässt.

Nach erfolgreichem Abschluss dieser Phase beginnt der Assoziationsprozess. Dazu sendet die Station einen Association Request MAC-Frame. Der AP übermittelt als Reaktion eine Association ID, die die Beziehung zwischen Teilnehmer und AP identifiziert. Erst nach Beendigung dieses Schrittes ist eine Station in der Lage, Daten zu senden und zu empfangen. Die Assoziierung entspricht damit einem aufgebauten Ethernet-Link.

Wandert der Teilnehmer über die Grenzen eines APs hinaus und die Verbindung soll trotz des Wechsels der Zelle aufrechterhalten bleiben, kommt es zum Roaming. Wenn sich die Funkbereiche der Access Points gegenseitig überlappen, dann kann sich der Client zwischen den Access Points bewegen, ohne dass die Netzwerkverbindung unterbrochen wird. Der einfachste Weg dies zu realisieren ist, alle Access Points mit der gleichen SSID auszustatten. Ferner müssen die Access Points die erweiterte Form der SSID unterstützen: ESSID (Extended Service Set Identifier). Dabei ist zu beachten, dass die Access Points unterschiedliche Kanäle belegen, da sich sonst die Funkverbindungen überlagern. Das WLAN-Roaming-Verfahren stößt allerdings bei der Nutzung der zentralen Authentifizierungstechnik 802.11x an ihre Grenzen. Hier muss sich der Teilnehmer beim Wechseln der Funkzelle erneut einloggen.

Der Roamingablauf lässt sich wie folgt vorstellen:

- Die Station erkennt, dass die Sendeleistung eines AP zu niedrig ist
- Sie sucht daraufhin nach einem neuen AP
 - passiv (durch Mithören)
 - aktiv (durch das Versenden spezieller Frames)
- Ist die Suche erfolgreich, registriert sie sich und der neue AP muss Zellenwechsel-Information im Netz bekannt geben, da der alte AP erfahren muss, dass er nicht mehr zuständig ist.

WLANs gleichen in vielen Gesichtspunkten mobilen Anwendungen. Insbesondere die Abhängigkeit von Batterien als knapper Ressource verbindet beide. 802.11 berücksichtigt daher explizit eine Power-Sparfunktion, indem sie Stationen einen Schlafmodus ohne Informationsverlust gewährt. Der diesem Mechanismus zugrunde liegende Gedanke ist, dass der AP einen kontinuierlich aktualisierten Zustandsdatensatz über die „schlafende“ Station pflegt und alle an sie gerichteten Pakete puffert. Diese Situation bleibt so lange bestehen, bis die Station entweder einen Polling Request sendet oder ihren Arbeitsmodus ändert und den „Schlafzustand“ verlässt. Als Teil des Beacon Frames überträgt der AP auch Informationen über das Power-Saving-Verhalten der einzelnen Stationen, für die der AP Pakete zwischengespeichert hat. Auf diese Weise können durch die Beacon Frames die Stationen in der Reihenfolge der Puffereinträge aufgeweckt werden.

■ 12.5 Rahmentypen

WLANs verlangen einen hohen Koordinationsaufwand. Diese Notwendigkeit kommt im Aufbau des Paketheaders, sowie in den Paketarten zum Ausdruck. Der Standard 802.11 kennt drei Rahmentypen:

- **Datenframes**, die die Nutzlast übertragen.
- **Kontrollframes**, die für den Zugriff auf das Medium benutzt werden, wie z.B. RTS, CTS und ACK.
- **Managementframes**, die für den Austausch von Steuerinformationen zuständig sind, wie z.B. Beacon Frames.

Jeder Typ enthält wieder mehrere Subtypen gemäß der speziellen Aufgabe. Die Grundstruktur aller 802.11-Rahmen besteht aus vier Feldern:

Präambel	PLCP-Header	MAC-Daten	Prüfsumme
----------	-------------	-----------	-----------

- **Die Präambel**, die abhängig von der physikalischen Ebene eine Synchronisationssequenz von 80 Bit enthält, dient dazu, die entsprechende Antenne zu wählen. Hinzu kommt ein Start Delimiter Frame, der durch die Folge 0000 1100 1011 1101 den Paketbeginn signalisiert.

- **Der PLCP-Header**, der stets mit 1 Mbit/s übertragen wird, enthält logische Informationen für die Dekodierung der physikalischen Schicht. Er besteht aus drei Teilfeldern:
 - der Wortlänge, die die Anzahl der Bytes des Paketes anzeigt und die genutzt wird, um das Paketende zu erkennen;
 - dem Signalisierungsfeld, das die aktuelle Übertragungsrate in 0,5-Mbit/s-Schritten für den Bereich 1 ... 4,5 Mbit/s angibt;
 - der Prüfsumme aus 16 Bit.
- **Die MAC-Daten**, deren Struktur eine sehr große Variationsbreite einnehmen kann. Die folgende Skizze zeigt ein allgemeines MAC-Format. Ein Teil der Felder tritt nur in besonderen Rahmen auf:

Byte 2	2	6	6	6	2	6	0-2312	
Frame Control	Duration	Adresse 1	Adresse 2	Adresse 3	Sequence Control	Adresse 4	Frame Body	CRC

Das Frame-Control-Feld besitzt eine komplexe Unterstruktur:

Protocol Version	Typ	Subtyp	ToDS	FromDS	More Frag	Retry	Power Mgm.	More Data	WEP	Order
------------------	-----	--------	------	--------	-----------	-------	------------	-----------	-----	-------

Die **Protokollversion** besitzt momentan den Standardeintrag null, das **Typfeld** identifiziert, ob es sich um einen Daten-, Kontroll- oder Managementrahmen handelt, und der **Subtyp** spezifiziert zu diesen Klassen jeweils eine Teilstruktur wie z.B. RTS, Beacon oder Daten. Das **ToDS-Bit** enthält eine Eins, falls der Rahmen an den AP gerichtet ist, sonst eine Null; das **FromDS** ist auf eins gesetzt, wenn das Paket vom Distributed System kommt. Das **More-Fragment-Bit** zeigt an, ob die Sendung aus mehreren Fragmenten besteht. Das **Retry-Bit** wird auf eins gesetzt, falls es sich um ein wiederholt übertragenes Fragment handelt. Das **Power-Management-Bit** signalisiert, dass die Station nach erfolgter Sendung in den Power-Save-Modus schaltet, ein gesetztes **WEP-Bit** verweist auf eine verschlüsselte Nutzlast und das **Order-Bit** deutet auf eine unveränderte Sendereihenfolge hin. Die kurze Vorstellung der einzelnen Steuerbits skizziert die Komplexität des Übertragungsverfahrens.

Das **Duration-Feld** der MAC-Daten kann zwei Bedeutungen annehmen:

- Im Falle einer Power-Save-Poll-Nachricht enthält es die Stations-ID.
- In den übrigen Fällen steht hier die Dauer gemäß der RTS- oder CTS-Nachricht.

Im Gegensatz zu den zwei Adressangaben in Ethernet oder IP, kennen WLANs vier Adressen, abhängig davon, ob die Stationen direkt miteinander kommunizieren oder einen AP als Vermittlungsstelle benötigen. Die Adressangaben schwanken je nach Eintrag im ToDS- oder FromDS-Feld des Frame-Control-Feldes:

- **Adresse 1** ist die Empfängeradresse. Falls das ToDS gesetzt ist, steht hier die AP-Adresse, sonst die Adresse der Zielstation.
- **Adresse 2** enthält die Angabe der Übertragungsstation. Falls das FromDS-Bit gesetzt ist, ist dies die AP-Adresse, sonst die Stationsadresse.
- **Adresse 3** enthält bei gesetztem FromDS-Bit die Quelladresse, bei gesetztem ToDS-Bit die Zieladresse.
- **Adresse 4** wird nur in den Fällen genutzt, in denen eine Übertragung über mehrere APs erfolgt. Da dann sowohl ToDS als auch FromDS gesetzt sind, würden sonst Quell- und Zieladresse fehlen.

Tabelle 12.3 Adresseinträge

ToDS	FromDS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	Ziel	Quelle	Access-Point	N/A
0	1	Ziel	Access-Point	Quelle	N/A
1	0	Access-Point	Quelle	Ziel	N/A
1	1	Access-Point	Access-Point	Ziel	Quelle

Der erste Fall bildet die Kommunikation von Endgerät zu Endgerät, der zweite von Access-Point zu Endgerät, der dritte von Endgerät zu Access-Point und der letzte Fall von Access-Point zu Access-Point ab.

Die Sequenz-Kontrolle wird benötigt, um die korrekte Reihenfolge der Fragmente zu rekonstruieren und um eventuelle Duplikate zu erkennen. Sie besteht aus zwei Teilfeldern, der Fragment- und der Reihenfolgenummer, die den Frame und innerhalb des Frames die Lage des Fragmentes beschreiben.

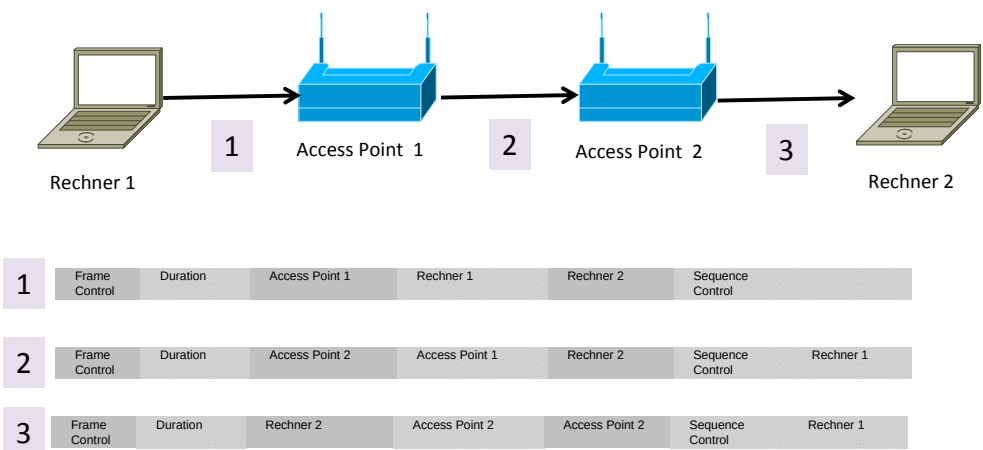


Bild 12.6 Kommunikationsblauf (Quelle: Piger, Grimm RRZN Hannover)

Zu den am häufigsten auftretenden Rahmen in einem WLAN gehören der RTS, der CTS und das ACK. Ihr Aufbau ähnelt sich stark, besitzt aber naturgemäß einige Besonderheiten:

Byte 2	2	6	6	4
Frame Control	Duration	Empfänger	Sender	CRC

Der ACK-Frame enthält kein Senderfeld. Die Empfängeradresse ist der Adresse 2 des Vorgängerrahmens entnommen. Falls dort das More-Fragment-Bit auf null gesetzt war, wird der Duration-Wert ebenfalls zu null, sonst wird der Wert des Vorgängers um die Zeit reduziert, die die Übertragung des ACK-Frames verlangt.



Viele frei verfügbare Werkzeuge liefern Informationen über WLANs. So können mit **Wireshark** auch WLAN-Pakete abgefangen und analysiert werden. Die Free-ware **Netstumbler** liefert Informationen über die in Reichweite liegenden WLANs sowie über die Güte der Sendeleistung und die eingerichteten Sicherheitsmerkmale.

12.6 Sicherheit

Der Sicherheit eines WLANs dienen mehrere Mechanismen:

Die erste Sicherheitsmaßnahme ist die Vergabe eines **Netzwerknamens (Service Set Identifier)**. Allerdings muss ein WLAN-Client keinen Netzwerknamen (SSID) kennen, um sich an einem Access-Point anzumelden. Der Eintrag von „ANY“ als Namen ist für einen Zugang ausreichend. Sobald aber eine SSID eingetragen ist, müssen alle partizipierenden Stationen die gleiche SSID besitzen. Die SSID stellt aber aus einem weiteren Grund ein Risiko dar. Um Kollisionen zu vermeiden, sendet der Access-Point in periodischen Abständen ein Beacon-Signal, mit dem existierende Stationen nach einem Sendewunsch gefragt bzw. neue Stationen aufgefordert werden, sich anzumelden. Neben Informationen wie Zeit oder Takt wird auch die SSID übertragen, so dass einem erfolgreichen Abhören nichts im Wege steht. Selbst wenn die SSID-Übertragung unterdrückt wird, erfährt ein neuer Rechner die SSID, in dem er zum Verbindungsaufbau einen Probe-Request-Paket versendet. Der Access-Point antwortet auf die Anfrage nämlich mit einem Probe-Response-Paket, das die SSID enthält.

Die nächste Stufe der Beschränkung ist ein Zugriffsschutz in Form von **Access Control Lists**. Hierbei wird nur ausgewählten Geräten mit ihrer spezifischen MAC-Adresse der Zugriff gestattet. Da viele WLAN-Karte allerdings die Konfiguration von MAC-Adressen gestatten und die MAC-Adresse zudem auch im Beacon-Paket übertragen wird, ergibt sich kein wirksamer Schutz. Außerdem scheitert der Einsatz der MAC-Filter daran, dass die Pflege der entsprechenden Tabelle einen erheblichen administrativen Aufwand verursacht. Während in Heimnetzwerken dieser Aufwand zu leisten ist, erweist er sich im Unternehmenskontext als unpraktikabel oder in öffentlichen Netzen als unerwünscht.

Die entscheidende Sicherheitsfunktion von WLANs ist die Verschlüsselung. Das **WEP-Verfahren** ist Teil des 802.11-Standards und damit der Vorläufer aller Verschlüsselungsbestrebungen. Der WEP-Algorithmus (**W**ired **E**quivalent **P**rivacy) erfüllt zwei wesentliche Aufgaben: Erstens soll er verhindern, dass unerwünschte Lauscher den WLAN-Verkehr abhören, zweitens soll er ein unerlaubtes Einbuchten in das WLAN unterbinden. Die Funktionsweise des WEP basiert darauf, dass zwischen einer mobilen Station und einem Access-Point ein geheimer Schlüssel ausgetauscht wird, d. h. WEP dient zum einen dazu einen WLAN-Client an einem Access-Point zu authentifizieren und zum anderen die Übertragung zu verschlüsseln. Statt allerdings komplizierte Key-Management-Systeme zu verwenden, wird lediglich ein Schlüssel genutzt, der von einem Access-Point und seinen zugeordneten Clients angewendet wird. Eine weitere Schwachstelle bildet das eingesetzte RC4-Verfahren, ein Verschlüsselungsalgorithmus, dessen Vor- und Nachteile bereits hinlänglich bekannt sind. Vor den RC4-Schlüssel wird ein 24-Bit-Initialisierungsvektor (IV) gesetzt, so dass ein 64- bzw. 128-Bit-Schlüssel entsteht. Mittels des WEP-Schlüssels erzeugt der Sender durch einen Pseudozufallsgenerator eine Bytefolge (Keystream), die er durch die XOR-Operation mit der eigentlichen Nachricht verknüpft. Die zuvor über einen linearen Algorithmus gebildete 32-Bit-Prüfsumme wird anschließend verschlüsselt und beide Teile sowie der unverschlüsselte Initialisierungsvektor werden übertragen. Der Empfänger erzeugt mit Hilfe des Initialisierungsvektors und des RC4-Schlüssels den ursprünglichen Keystream und durch die Umkehrung der XOR-Operation den Ausgangstext. Erkennt ein Angreifer nun zwei mit dem gleichen Schlüssel chiffrierte Pakete, kann er den zugrunde liegenden Schlüssel berechnen. Über die Schwachstellen waren sich die Designer des WEP im Klaren. Um Angriffe abzuwehren, implementierten sie zwei Verteidigungsstrategien: die Integritätsprüfung und den Initialisierungsvektor. Die Aufgabe der Prüfsumme ist dabei zu gewährleisten, dass kein Paket modifiziert wurde. Allerdings dient hierzu ein lineares CRC32-Verfahren, das bereits hinreichend bekannt ist und die Chance einer Veränderung nicht vollständig abfängt. Auch der Initialisierungsvektor bietet Schwächen, da er auf der Basis des gemeinsamen geheimen Schlüssels erzeugt wird. Da er nur 24 Bit groß ist, besteht die Gefahr einer Wiederholung durch einen zu kleinen Wertebereich. Nach einer ausreichenden Zeitspanne kann ein Angreifer daher in den Besitz zweier gleich chiffrierter Pakete kommen.

Der Initialisierungsvektor weist damit zwei Schwächen auf: Er ist mit 24 Bit relativ kurz und er wird im Klartext übertragen. Zudem arbeitet WEP mit statischen Schlüsseln. Für jede Übertragung wird der gleiche Schlüssel verwendet. Da WEP kein Schlüsselmanagement enthält, gibt es auch keine Möglichkeit, die Schlüsselverteilung dynamisch zu organisieren. Im Regelfall muss der Administrator bei Clients und Access-Point manuell eingreifen.

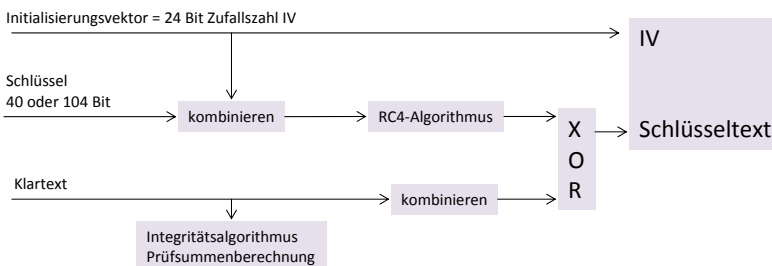


Bild 12.7 WEP-Verschlüsselung (Quelle: Klaus, Hochschule Winterthur)

Untersuchungen der University of California machten auf diese Sicherheitslücken aufmerksam. WEP gilt daher als unsicher.

Auch wenn WEP keinen optimalen Schutz darstellt: Keinen Schutz zu verwenden, ist ein allemal größeres Problem. Ein Beispiel mag dies verdeutlichen. Ein kleines WLAN verbindet einige PCs über einen Access-Point. Ein Nachbar des Büros kauft sich eine WLAN-Karte und stellt fest, dass der Access-Point ungeschützt ist. Fortan surft er über den Access-Point des Büros kostenlos im Internet.

Zur Behebung der Schwächen von WEP wurde 2003 Wi-Fi Protected Access (WPA) eingeführt. WPA verwendet das Temporal Key Integrity Protocol (TKIP) als Verschlüsselungsalgorithmus. TKIP kann auf der unveränderten Hardware betrieben werden und nutzt einen 128 Bit langen Schlüssel. Obwohl WPA einen Fortschritt in der Sicherheit eines WLANs bedeutet, basiert es weiterhin auf der bereits von WEP eingesetzten Hardware. Dieser Mangel kann nicht durch das Umschalten auf einen anderen Verschlüsselungsmechanismus gelöst werden. Daher entwarf die Wi-Fi Alliance 2004 einen neuen Standard WPA2, der offiziell 2005 zu 802.11i wurde. WPA2 setzt auf den Advanced Encryption Standard (AES) als Verschlüsselungsalgorithmus. Um die Migration zu unterstützen, ist WPA2 Hardware rückwärtskompatibel. Dieser Umstand ermöglicht es, auf neue Access-Points zu migrieren und weiterhin die älteren Geräte mit WEP oder WPA zu nutzen. Router hingegen besitzen bereits eine WPA2-Hardware implementiert. Zur einfacheren Verwaltung ist der dynamische Schlüsselaustausch in 802.11i integriert. Einen Vergleich der Sicherheitsmerkmale der einzelnen Verfahren zeigt Tabelle 12.4:

Tabelle 12.4 WLAN-Sicherheitsmerkmale

Standard	Schlüsselverteilung	Geräteauthentifikation	Benutzerauthentifikation	Verschlüsselungsstandard/-protokoll
WEP	statisch	ja	nein	RC4
WPA	dynamisch	ja	ja	TKIP
WPA2	dynamisch	ja	ja	AES

802.1x teilt den Netzwerkport in zwei logische Ports auf, von denen der kontrollierte Port zum LAN zeigt und der unkontrollierte Port die Authentifizierungsanfrage an den entsprechenden Server leitet. Erst wenn der Authentifizierungsserver den WLAN-Client identifiziert hat, gibt der Access-Point den kontrollierten Port frei und der Anwender kann auf das LAN zugreifen. Dieses Verfahren bietet den Vorteil, der Benutzerauthentifikation über einen separaten RADIUS-Server. Zusätzlich kann in bestimmten Zeitabständen eine erneute Authentifizierung erzwungen werden. Da das Zeitfenster sehr klein konfiguriert werden kann, können Angriffe während einer Übertragung nahezu ausgeschlossen werden.



Fallbeispiel

Die Restaurantkette Quick-Burger möchte für ihre Gäste einen kostenlosen Internetzugang einrichten. Die Gäste sollen mit ihrem Laptop ins Restaurant kommen und sich uneingeschränkt mit dem Internet verbinden können. Um dies kabellos

zu ermöglichen, muss zunächst ein Access-Point eingerichtet werden. Dabei muss beachtet werden, dass der AP so aufgestellt/montiert wird, dass eine komplette Ausleuchtung des Restaurants gewährleistet ist. In Abhängigkeit von der Größe und den baulichen Umständen können mehrere APs erforderlich sein. Der/die APs müssen anschließend mit dem hauseigenen LAN verbunden werden.

Doch wie bekommen nun die Gäste eine Verbindung zum AP? Obwohl auf den Laptops die Existenz der WLANs angezeigt wird, muss den APs gesagt werden, wer sie nutzen darf. Die manuelle Zuweisung einer IP-Adresse an die Gästerechner scheidet dabei als eine zu aufwändige Maßnahme aus. Es muss also einen Mechanismus geben, der eine IP-Adresse dynamisch zuweist. Dies ist die Funktion des Dynamic Host Configuration Protocols (DHCP).

DHCP funktioniert wie folgt: im ersten Schritt sendet der Client (hier der Gäste-Laptop) eine Broadcast, um einen DHCP-Server in Reichweite zu finden. Dazu bedarf es einer IP-Schnittstelle, die für die Verwendung von DHCP konfiguriert ist. Der DHCP-Server im AP des WLANs antwortet dem Anfrager mit dem Angebot einer IP-Adresse. Diese IP-Adresse stammt aus dem Bereich, der zuvor in der Konfiguration des DHCP-Servers (hier im AP) durch den Administrator von Quick-Burger festgelegt wurde. Der Client kann prinzipiell mehrere Angebote erhalten. Deshalb sendet er seinerseits eine Broadcast an die DHCP-Server, in der er die Annahme eines der Angebote mitteilt. Der ausgewählte DHCP-Server bestätigt dies und teilt die Dauer mit, für die der Client die Adresse nutzen darf. Dieser Ablauf scheint genau auf die Bedürfnisse von Quick-Burger zu passen.

Doch wie wird DHCP eingerichtet? Dazu muss DHCP auf dem AP aktiviert werden. Nachdem dem AP mitgeteilt wurde, dass er als DHCP-Server arbeiten soll, muss der IP-Adress-Vorrat definiert und die Dauer festgelegt werden, für die eine IP-Adresse vergeben wird. Abschließend muss Quick-Burger nur dafür sorgen, dass auf den Gäste-Laptops der automatische Bezug von IP-Adressen eingestellt ist.

Aus Sicht der Sicherheit darf der AP keine Filterung der MAC-Adressen vornehmen. Da die MAC-Adressen der Gäste-Laptops unbekannt sind, würde ein derartiger Mechanismus allen Gästen eine Verbindung untersagen. Zum anderen muss die Verschlüsselung entweder ausgeschaltet oder der Schlüssel muss den Gästen leicht zugänglich sein. Der verwendete WLAN-Standard dürfte kein Problem darstellen, da die meisten Karten und APs die gängigen „Dialekte“ simultan beherrschen. Soll der Adressvorrat effizienter genutzt werden, könnte Quick-Burger anstelle der Zuweisung öffentlicher IP-Adressen das NAT-Verfahren verwenden und den Gäste-Laptops private Adressen zuweisen, die im AP dann in die öffentliche IP-Adresse von Quick-Burger umgewandelt wird.

■ 12.7 Bewertung

Neben vielen positiven Aspekten besitzt IEEE 802.11 aber auch einige Schwächen:

- **Frequenzbereich:** Da das 2,4-GHz-Band allgemein zugelassen ist, muss mit Beeinträchtigungen durch andere Systeme gerechnet werden. Ein Beispiel hierfür ist die Mikrowelle, die ebenfalls bei 2,4 GHz arbeitet und eine Störquelle darstellen kann.

Aber auch die Verwendung vieler WLANs durch Nachbarabteilungen oder weitere Unternehmen kann zu einem Problem werden, dem nur begrenzt durch ein Ausweichen auf einen anderen Kanal begegnet werden kann.

- **LAN-Anforderungen:** Radiosignale können unterschiedliche Wege vom Sender zum Empfänger nehmen, eine als Multipath bekannte Eigenschaft. Mehrwegeausbreitungen treten auf, wenn ein WLAN in Gebäuden betrieben wird, in denen Reflektionen von Wänden, Decken, Fenstern und Fußböden eine Abschwächung oder Verstärkung bewirken. Aufgrund der unterschiedlichen Signalwege kommt das gleiche Signal mehrfach und gegebenenfalls zeitversetzt beim Empfänger an. Gegen diesen Störeffekt muss die Funkübertragung robust sein. Moderne Funkkarten analysieren deshalb ankommende Signale und werten gleichartige Informationen nur einmal aus. Die genauen Übertragungsmerkmale hängen aber nicht nur von der Umgebung, sondern auch von der Entfernung, dem Produktdesign und der Technologie ab.
- **Funkzellen:** Um eine störungsfreie Übertragung sicherzustellen, ist es erforderlich, dass benachbarte Funkzellen nicht den gleichen Kanal benutzen. Das Übertragungsverfahren mit 11 bzw. 13 Kanälen lässt drei Kanäle zu, auf denen ohne Überlappung gleichzeitig gesendet werden kann. Bei richtiger Planung überschneiden sich in einem WLAN niemals mehr als drei Funkzellen.

Positiv ist zu bewerten, dass sich eine aufwändige Gebäudeverkabelung umgehen lässt. Bei häufig wechselnden Netztopologien, wenn Gruppen bei Meetings oder Workshops Daten austauschen wollen, stellt sich dies als unschätzbare Flexibilitätsgewinn heraus. Aber auch in Gebäuden mit bautechnischen oder kulturhistorischen Beschränkungen stellen WLANs oft die einzige Möglichkeit dar, eine zufrieden stellende Vernetzung zu realisieren. Neben diesen Aspekten spielt auch die Zuverlässigkeit der Kommunikation eine Rolle. WLANs sind sicher gegen Störungen durch Radio- und TV-Wellen und eine außergewöhnliche Empfangsempfindlichkeit in Verbindung mit reichweitenstarken Antennen gewährleistet eine stabile Funkübertragung.

Hinsichtlich des infrastrukturellen Einsatzes bestehen keine Restriktionen. Eine Haus-zu-Haus-Verbindung unterliegt keinerlei gesetzlichen Vorschriften, wenn der Betrieb auf dem eigenen Grundstück erfolgt. Unternehmen mit räumlich getrennten Standorten können demzufolge von dieser Regelung durch die Einsparung kostspieliger Standleitungen in hohem Maße profitieren.

In kabelgebundenen Netzwerken erkennen Stationen eine Kollision bereits während der Übertragung. Im WLAN verhindert die Hidden Node Problematik diese Möglichkeit, so dass auf Bestätigungspakete ausgewichen werden muss. Ein Empfänger sendet daher an den Übertragenden ein gesondertes Paket zurück, das durch eine Karenzzeit gesichert ist. Für ein 802.11a-WLAN entspricht dieser Mechanismus einem Overhead von 50 ms/Paket. Da ein WLAN-Paket nicht nur Nutzdaten, sondern auch die Information darüber liegender Protokolle beinhaltet, kommen weitere 20 ms/Paket hinzu. Insgesamt dauert die Übertragung von 1500 Bytes Nutzlast bei 54 MBit/s 325 ms, was eine Nettorate von 37 MBit/s ergibt. Ergänzt um Wiederholungen auf Grund von Funkstörungen sinkt die Nettorate in den Bereich von 25 MBit/s. Um diese Verringerung auf ca. die Hälfte der Nominalgeschwindigkeit auszugleichen, existieren verschiedene Ansätze:

- **Bursting:** Der Sender verkürzt die Wartezeit nach dem letzten ACK-Paket auf SIFS anstelle von SIFS+DIFS und gewinnt auf diese Weise den Wettbewerb um das Medium. Der Nachteil ist offenkundig: das Verfahren ist asozial, da die Station auf Kosten der Mitbewerber die Bandbreite belegt.
- **Paketbündelung:** Im Gegensatz zu Ethernet erlaubt der WLAN-Standard Paketgrößen bis 2304 Byte. Längere Pakete verringern den insgesamt notwendigen Overhead. Werden mehrere Pakete zu einem zusammengefasst, ergibt sich ein Übertragungsvorteil. Dieses Konzept hat zwei Schwächen: zum einen steigt die Gefahr, dass längere Pakete das Opfer von Störungen werden, zum anderen steigt die Latenz, da der Sender erst Pakete sammeln und aggregieren muss bevor er sie verschickt.
- **Modulation:** Bei Datenübertragungen ist zwischen Bit- und Symbolrate zu unterscheiden. Hohe Bitraten entstehen durch die gleichzeitige Übertragung mehrerer Symbole auf verschiedenen Unterträgern im Kanal (OFDM – Orthogonal Frequency Division Multiplexing) und durch die Verwendung komplexer Modulationsverfahren, die pro Symbol mehr als ein Bit transportieren. Bei der niedrigsten OFDM-Rate von 6 MBit/s trägt jedes Symbol lediglich ein Bit bei 24 OFDM-Unterträgern. Bei 54 MBit/s wird die QAM64-Modulation genutzt, die pro Symbol 6 Bit bei 36 Unterträgern überträgt.
- **Nutzungs einschränkung:** Möchte ein Unternehmen ein 802.11a-Netz einsetzen, um zwei Gebäude zu verbinden, müssen die Geräte in der Lage sein, ihre Übertragungsleistung automatisch anzupassen. Der Hintergrund für diese Transmission Power Control-Funktion (TPC) ist das Fehlen einer Funktion, die Konflikte mit anderen Anwendungen im 5 GHz-Band ausschließt. Nur wenn Systeme sowohl über eine dynamische Frequenzwahl nach dem Dynamic Frequency Selection-Verfahren (DFS) verfügen und TPC beherrschen, ist innerhalb von Gebäuden eine Sendeleistung von 200 mW zulässig. Für den Außenbereich steht dann im Fenster von 5,47 GHz bis 5,725 GHz die volle Leistung von 1000 mW zur Verfügung. Fehlen weiterhin bei der 802.11a-Lösung die DFS/TPC-Erweiterungen, so reduziert sich der erlaubte Frequenzbereich auf 5150 bis 5250 MHz, was lediglich die Nutzung von vier Kanälen gestattet. Auf diesen verbleibenden Kanälen (gegenüber 12 in den USA) ist eine maximale Sendeleistung von 50 Milliwatt zugelassen. Sind DFS und TPC jedoch implementiert, so sind 200 Milliwatt auf acht Kanälen möglich. Die Reichweite entspräche damit ungefähr der von 802.11b-Netzen, also rund 100 m.



Noch Fragen ...? Ja ...

Gibt es noch weitere Standards rund um WLANs?

Ja, im Folgenden eine kurze Übersicht: 802.11 d Roaming, 802.11 e Quality of Service; 802.11 i Sicherheit und Authentifikation

Wie sieht die Perspektive bei der Geschwindigkeit aus?

Seit Mai 2010 gibt es eine Spezifikation für Gigabit im WLAN. Dieses Konzept beruht auf dem lizenzfreien 60-GHz Bereich und soll Datenraten bis zu 7 GBit/s ermöglichen, vgl. <http://www.wigig.org>

■ 12.8 Zusammenfassung

Der durchschnittliche Mitarbeiter eines Unternehmens verbringt bis zu 60 Stunden im Monat in Besprechungen, viel Arbeitszeit vor dem Rechner und nutzt dabei überwiegend ein mobiles Gerät wie einen Laptop oder ein Smartphone. Die zusätzliche Möglichkeit über drahtlose Netzwerke mit den zentralen Anwendungen verbunden zu sein, schafft Produktivitätsgewinne für die Unternehmen und spart dem Arbeitnehmer Arbeitszeit. Kein Warten auf Daten, die bei Sitzungsbeginn nicht vorlagen und kein aufwändiges Nachbearbeiten führen zu einer deutlichen Steigerung der Arbeitsproduktivität. Diese Beispiele unterstreichen die Attraktivität der WLANs und zeigen darüber hinaus, dass mit einem stetigen Wachstum der Anzahl der drahtlos kommunizierenden Geräte zu rechnen ist und das der Bandbreitenhunger noch längst nicht gestillt sein dürfte.

Da künftige Infrastrukturen zu einem Großteil auf mobilen Standards beruhen, ist eine Kenntnis der Basismechanismen selbst für den Gelegenheitsnutzer heute unerlässlich.

Informationen zur Sicherheit und zur Kompatibilität finden sich unter:

- <http://www.wi-fi.org>
- <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

■ 12.9 Wissensüberprüfung

1. Erklären Sie den Unterschied zwischen CSMA/CD und CSMA/CA.
2. Was sind die Voraussetzungen für ein erfolgreiches War-Driving?
3. Welche Informationen zeigen Freewaretools wie netstumbler an?
4. Wozu wird die MAC-Filterung genutzt?
5. Warum nutzt ein Extended Service Set mehrere unterschiedliche Kanäle?
6. Wann ist der Einsatz von DHCP in einem WLAN sinnvoll?
7. Welche Bedeutung kommt der SSID zu?
8. Was versteht man unter Interferenzen und wo können Sie auftreten?
9. Können Clients auf der Basis unterschiedlicher WLAN-Standards über einen AP zusammenarbeiten?
10. Was ist unter der MIMO-Technik zu verstehen?

Literatur

Verwendete Quellen und weiterführende Literatur, sowie wertvolle Internetlinks

Lehrbücher zum Thema

P. Mandl, A. Bakomenko, J. Weiß: Grundkurs Datenkommunikation, Teubner + Vieweg, 2008

A. Schlemberg, M. Linten, K. Surendorf: PC-Netzwerke, Galileo Computing, 2009

H. Zisler: Computer-Netzwerke, Galileo Computing, 2012

Kapitel 1

D. Shinder: Computer Networking Essentials – Kapitel 2 und 3, Cisco Press, 2002

Informationen zum OSI-Modell unter <http://www.lex-con.com/protocol.htm>

Video zum OSI-Modell unter <http://www.learntcpip.com/OSIModel/default.htm>

Kapitel 2

A. Anderson, R. Benedetti: Netzwerke von Kopf bis Fuß, O'Reilly, 2010

Basisnetzwerkkonzepte unter: <http://compnetworking.about.com/od/basicnetworking/concepts>

Glasfaserkabel: Aufbau und Eigenschaften unter: http://www.corning.com/r_d/technology_exploration/telecommunications.aspx

Kapitel 3 und 4

D. Comer: TCP/IP – Konzepte, Protokolle und Architekturen, Kapitel 2.4, mitp, 2011

J. Kurose, K. Ross: Computernetze – 5., aktualisierte Auflage, Kapitel 5, Pearson Studium, 2012

Netzwerkkompodium unter: <http://www.wildpackets.com/resources/compendium/overview>

Einführung unter: <http://www.firewall.cx/networking-topics/ethernet.html>

Technologie unter: http://www.tecchannel.de/netzwerk/lan/431828/grundlagen_ethernet_co

Linkliste und Überblick unter: <http://www.ethermanage.com/ethernet/ethernet.html>

10 Gigabit-Ethernet Alliance unter: <http://www.10gea.org>

Kapitel 5

D. Comer: TCP/IP – Konzepte, Protokolle und Architekturen, Kapitel 7, mitp, 2011

J. Kurose, K. Ross: Computernetze – 5., aktualisierte Auflage, Kapitel 4, Pearson Studium, 2012

IP-Adressing verstehen unter: <http://holdenweb.com/static/docs/3comip.pdf>

Internetworking Technology Handbook unter: http://docwiki.cisco.com/wiki/Internet_working_Technology_Handbook

Detaillierte Beschreibung der Felder und Optionen aller TCP/IP-Protokolle unter: <http://www.networksorcery.com>

Übersicht aller Protokolle der TCP/IP-Familie unter: <http://www.protocols.com/pbook/tcpip1.htm>

Kapitel 6

D. Comer: TCP/IP – Konzepte, Protokolle und Architekturen - Kapitel 4, mitp, 2011

Subnetz kalkulator unter: <http://www.ipprimer.com/subnet.cfm>

IP-Adress-Tutorial unter: <http://www.semsim.com/ccna/tutorial/ip-addressing/ip.html>

Subnetztutorial unter: <http://www.ralphb.net/IPSubnet/>

Video unter: <http://www.learn tcpip.com/TCPIP/default.htm>

Kapitel 7

D. Comer: TCP/IP – Konzepte, Protokolle und Architekturen, Kapitel 13, mitp, 2011

J. Kurose, K. Ross: Computernetze – 5., aktualisierte Auflage, Kapitel 3, Pearson Studium, 2012

D. Rodriguez, J. Gatrell, J. Karas, R. Peschke: TCP/IP Tutorial and Technical Overview, IBM Redbook, 2001

Internetworking Technology Handbook unter: http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook

Kapitel 8

D. Comer: TCP/IP – Konzepte, Protokolle und Architekturen, Kapitel 33, mitp, 2011

S. Hagen, IPv6, Sunny Edition, 2004

Lernmodule unter: <http://www2.rad.com/networks/2000/ipv6/ipv6.htm>
und <http://www.microsoft.com/ipv6>

Tutorials unter: <http://www.laynetworks.com/ipv6.htm>

Audiopräsentation unter: http://www.6deploy.org/e-learning/english/what_is_ipv6/

IPv6 Testnetz unter: <http://www.6bone.net>

IPv6 Forum unter: <http://www.ipv6forum.com>

Kapitel 9

J. Kurose, K. Ross: Computernetze – 5., aktualisierte Auflage, Kapitel 5, Pearson Studium, 2012

Einführung unter: <http://www.firewall.cx/switches.php>

Tutorial unter: <http://www.lantronix.com/learning/tutorials/switching.html>

Kapitel 10

D. Comer: TCP/IP – Konzepte, Protokolle und Architekturen – Kapitel 16, mitp, 2011

J. Kurose, K. Ross: Computernetze – 5., aktualisierte Auflage, Kapitel 4, Pearson Studium, 2012

D. Rodriguez, J. Gatrell, J. Karas, R. Peschke: TCP/IP Tutorial and Technical Overview, IBM Redbook – Kapitel 4, 2001

Arbeitsweise von Routern unter: <http://www.firewall.cx/routers.php>

Routinggrundlagen unter : http://www.ictglobal.com/ICT009/routing_basics.html

Kapitel 11

J. Kurose, K. Ross: Computernetze – 5., aktualisierte Auflage, Kapitel 9, Pearson Studium, 2012

B. Studer: Netzwerkmanagement und Netzwerksicherheit, Hochschulverlag, 2010

MIB-Browser und SNMP Agent Simulator unter: <http://www.ireasoning.com/>

SNMP-Demo unter: <http://snmp.cs.utwente.nl/tutorials/demo/snmp/v2c/>

Kapitel 12

J. Kurose, K. Ross: Computernetze – 5., aktualisierte Auflage, Kapitel 6, Pearson Studium, 2012

WLAN-Monitore unter: <http://www.xirrus.com>

<http://www.metageek.net>

Index

10Base 67, 85, 88, 93f., 104, 193
80-20-Regel 14
80/20Regel 14
100Base 88, 92, 94, 193
802.11 251f., 261, 267

A

Abschlusswiderstand 19, 81
Abstract Syntax Notation No.1 237
Access Control 30
Access Control Lists 247
Access-Point 251, 259f., 263ff.
Acknowledgement 153, 157, 161
ACR 56, 61
Address Resolution 123, 126
Adresskonfiguration, automatisch 165
Aging 189f.
Alien-Crosstalk 61
Alohanet 66
Amplitudenmodulation 36
Antenne 251, 261
Antivirus-Software 245
Anwendungsklasse 58f.
Anwendungsschicht 32
Anycast 23, 34, 164
Applikationsmanagement 233
ARP 69, 71, 123f., 126f., 130, 159, 175, 185, 211
ARP-Broadcast 176
ARP-Cache 123, 211
arpspoof 246
asynchron 39, 85
ATM 189, 213
Attempt Limit 75
Attenuation 56
Authentication Header 169, 171
Autodiscovery 233
Autonegotiation 96, 100, 102

Autonome Systeme 217
Autosensing 62, 94, 188
Autotopology 233

B

Backbone 40ff., 64, 85, 99, 104, 146
Backoff 258
Bandbreite 14, 26, 35, 42, 47, 50, 54, 57, 59, 60, 97, 113, 158, 186, 194
Beacon Frame 260f.
Best Effort 114, 161
Biegeradius 57
Bigbrother 236
Bitcodierung 37
Bitübertragungsschicht 29
BNC 82
Break-Out Kabel 51
Brechungsindex 45, 47f., 50
Broadcast 23, 123, 126f., 132, 193, 194, 211, 218, 260
Broadcast-Domäne 193f., 228
Brute-Force 244
Bündelader 51
Bus 19, 20, 66, 81ff., 195
Bus Switchingarchitektur 195
Busy Wait 74

C

Cache 123, 211
Carrier Extension 101f.
Carrier Sense 73f.
Category 58ff., 68, 90
CATNIP 163
CheaperNet 67
Cladding 44
Class A 133ff., 139, 141, 145
Class B 133ff., 139, 142, 145, 150

Class C 133 ff., 139, 145
Class D 133 ff.
Class E 133
Clear-to-Send (CTS) 258, 261 f., 264
Client-/Server-Architektur 18, 25, 189
Coating 44, 51
Codierungsverfahren 38, 93, 99
Collapsed Backbone 41 f.
Collision Detection 73 ff.
Core 44
Crosstalk 56, 61
CSMA 66 f., 73, 77 f., 80, 86 f., 98, 101, 103 f.
CSMA/CA 257
CSMA/CD 66 f., 73, 77 f., 80, 86 ff., 90 f., 95, 97 f., 101, 103 f., 111
Cut-Through 191 f., 206

D

Darstellungsschicht 31
Datenfluss 157, 161
Datenfluß 157
Datenintegrität 257
Datenverbund 16
Default Router 210
Deferring 74
Delay 61, 101
Destination Options Header 169 f.
Dienstgüte 115, 164
Dispersion 47
Distance Vector Protokolle 217 ff.
Distributed Backbone 41 ff.
Distributed Denial-of-Service 245
Distributed Inter Frame Space (DIFS) 259
Domain Name System 163
DS-Byte 116
Dual-IP 178 f.
Durchsatz 30, 101, 115, 121, 184, 188, 194

E

Echo 127 f., 130
Einkopplungswinkel 45, 47
ELFEXT 100

E-Mail 159, 162, 167, 208
Encapsulation Header 169, 171
Eventhandling 233
Extended-ACL 247

F

Faser 43 f., 46 ff., 51 f.
Fast Ethernet 67, 89 ff., 94 ff., 101, 102
FCAPS-Modell 235
Fibre Channel 98 f., 101
FIN 154, 157
Flags 116, 157, 161
Flooding 189 f.
Flow Control 161, 165
Flow-Label 167
Flusskontrolle 30, 68, 102
Forwarding 170
Fragment Free 192
Fragment Header 169 f.
Fragmentierung 27, 116, 118 f., 128, 165, 170, 259
Frame Check Sequence 86
Frequenzmodulation 36
Fresnel-Verlust 49
FromDS 262 f.
FTP 32, 55, 159, 167, 208
Füllbytes 102
Funktionsverbund 16

G

Gerätehärtung 245
GetBulkRequest 239
GetNextRequest 238
GetRequest 238
GetResponse 238
Gigabit-Ethernet 57, 67 f., 97 ff., 101 ff., 106 ff., 189
Gradientenfaser 47, 50 f.

H

Halbduplex 22, 94 f., 97, 101 f., 105
Header 114, 116 f., 119, 126 f., 129, 154, 160, 211 f.
Hello-Paket 218, 225

Hold Down 220
Hold Down Timer 220
Hop 220, 223
Hop-by-Hop Options Header 169 f.
Hop Count 216, 220
Hop-Limit 165
Hub 84 f.

I

IAB 163
Idle 74
IEEE 802.3 65, 68 f., 71, 90, 94, 97, 99,
101, 104, 107, 119, 124
IEEE 802.5 124
IETF 146, 152, 163
I/G-Bit 70
Induktivität 57
InformRequest 239
Initialisierungsvektor 265
Interface 91, 93, 98, 104, 106, 165
Interframe Gap 74, 80, 102
Inter Frame Space 259
Intranet 145
Intrusion Detection Systeme 245
Intrusion Prevention Systems 245
IPv4 114, 162 ff., 169 f., 172, 178 f.
IPv6-Encapsulation 178

J

Jabber 81, 86
JAM-Signal 75 f., 87
Jumbograms 165

K

Kanal 38 f.
Kapazität 24 f., 57
Kaskadierung 84, 194
Kern 44 f., 48, 50, 52, 103, 187, 194
Key-Management 265
Keystream 265
Klassifizierung 116
Kodierungsverfahren 38, 99
Kollision 257
Kollisionserkennung 75, 81, 88

Kontrollpaket 258
Konvergenz 230

L

Laser 47, 49
Lastverbund 16
Late Collisions 86
Latenz 191
Layer-3 107, 229
Learn-and-Stay 189, 215
Least Significant Bit 31
LED 47, 53
Leitungsvermittlung 23 f.
Lichtwellenleiter 15, 40, 43, 45
Link Aggregation 104, 107, 194
Link Local Adresse 175
Link-State 224
Link-State Protokolle 217 ff., 230
Local Collisions 86
Logical Link Control 30, 66
Long Wave 99
Loopback 132, 136, 179
Loose Source Routing 120

M

MAC-Adresse 70, 88, 123 f., 126, 131, 165,
175 f., 189 ff., 211 f., 215
MAC-Flooding 246
Malware 245
MAN 17, 19, 66, 103
Managed Object 237
Management Information Base (MIB) 237
Manchester Codierung 37, 81 f., 84 f., 89,
92 f.
Man-in-the-Middle 244
Matrix Switchingarchitektur 195
Maximum Transfer Unit (MTU) 203
MBZ 115 f.
Metrik 209, 214 f., 219, 222 f.
MIB 237
MIB-Browser 241
MIB-II 239
MLT-3 37, 92
Mode 22, 47
Modendispersion 47, 50

Modulation 105
Monomode 60, 98
Most Significant Bit 31
MTU 166, 171
Multicast 23, 34, 127, 136, 164, 176, 189, 218
Multimode 50, 51, 98, 103, 107
Multipath 268
Multiprotokoll 179

N

Nagios 236
Nebensprechen 56
Neighbor Discovery Protocol 175
netstat 233
Network Address Translation (NAT) 145, 146, 162
Netzwerk 15 f., 19, 24 ff., 35, 79, 86, 117, 121, 128, 138 f., 152, 155, 171 f., 186, 215
Netzwerkbetriebssystem 16, 18 f., 31
Netzwerkpräfix 133
Netzwerkschicht 30
NEXT 56, 100
Next Header 166, 168, 171
NIC 117, 132
Non-Blocking 193
NRZI 37, 92 f.
Numerische Apertur 48, 51

O

Offset 116, 119, 171, 185
Open Shortest Path First (OSPF) 116 f., 142, 168, 217
Option 98, 118 ff., 129, 155, 168, 169
Optionen 103, 117 ff., 126, 155
OSI-Referenzmodell 26, 28, 34, 36, 68, 73, 81, 114, 151, 168, 207, 214

P

Padding 118
Paketvermittlung 22 ff., 34
Payload 166
PCS-Faser 44

Personal Firewalls 245
Physical Coding 92, 101, 105
Physical Medium Dependent 101
Pigtail 47
Ping 130
Ping-of-Death 244
PLCP-Header 261 f.
Port 102, 128, 188 ff., 193, 194, 211
PortSecurity 246
Power Save 262
Präambel 69, 74, 261
Präfix 132, 142 f., 149, 165, 175, 176
Primärverkabelung 40, 51
Priorität 115, 129, 165, 167
Prüfsumme 30, 69, 71, 77, 86, 101, 117, 119, 127, 153 f., 160, 165, 261 f., 265
PS-ACR 61
Punkt-zu-Punkt 22, 92, 94, 103 f., 194

Q

Quittungsnummer 154, 156 f.

R

Radiowellen 251
Rayleigh-Streuung 48 f.
RC4 265
Recorded Routing 120
Referenzmodell 26, 28, 73
Reflexion 49
Repeater 68, 79, 81, 82 ff., 95, 98, 101, 105
Reply 123 f., 126 ff.
Request 123, 126 f., 129, 130, 163, 176, 211, 222, 258, 260 f.
Request Frame 260
Request-to-Send (RTS) 258, 261 f., 264
Reserviert 118, 133, 154
Retransmission 24, 79, 101, 153, 154, 158, 259
RJ45-Stecker 83 f.
Roaming 260
Rogue-APs 247
Routing 30, 71, 118, 120 f., 123, 129, 134, 210, 212
Routing Information Protokoll (RIP) 140 ff., 147, 217

Routingstabelle 142 f., 209, 211, 215 f.,
218 ff., 222
RSVP 113, 167, 170
Rückflussschäpfung 55, 61, 101

S

SC-Stecker 93
Segment 14, 41 f., 79, 82 f., 95, 155, 171,
211
Sekundärverkabelung 40, 43
Sequenznummer 128 f., 154, 156 ff., 161
Server 14 f., 18, 22, 24 f., 42, 104, 126,
130, 136, 179, 186, 189, 208
Service Set Identifier (SSID) 264
SetRequest 238
Shared Memory Switchingarchitektur
194
Short Frame 86
Short Inter Frame Space (SIFS) 259
Short Wave 99
Sicherheitslöcher 244
Sicherheitspolitik 244
Sicherungsschicht 30, 34
Signalisierung 90 f., 99
simplex 22
Singlemode 103, 107
Sitzungsschicht 31
Skalierbarkeit 19 f., 25, 152, 250
skew 61
Sliding Window 153
Slot 75, 78
Slot Time 258 f.
SMI 237
SMI Datentypen 241
SNMP 71, 107, 113, 159, 167
SNMPv2 237
SNMPv3 237
Snort 246
SNR 57
Socket 155
Source Routing 118, 120, 169 f.
Source Routing Header 169 f.
Spanning Tree 197, 214
Split Horizon 220
Spoofing 145
Stackable 188

Standard-ACL 247
Start Delimiter 261
Stateful 176
Stateless 176
Sterntopologie 20, 41, 84 f., 95, 104
Store and Forward 21, 191 f., 206, 211
Strict Source Routing 118, 120
Structure of Management Information
(SMI) 237
ST-Stecker 53, 93
Stufenfaser 50 f.
Subnetz 129, 138 f., 140 f., 143 f., 211,
222
Subnetz-Adressen 132
Switch 188, 190 ff., 215
synchron 39
SYN-Flood 244
Syntax Notation 237
Systemmanagement 232

T

TCLASS 167
Tertiärverkabelung 40, 43, 51
Three-Way-Handshake 155
Timer 222
Timestamp 118, 121, 129
Time to Live 117, 212
ToDS 262 f.
Topologie 250
TOS 115 f.
ToS-Feld 116
Traceroute 130
Transceiver 81 f., 85, 86, 105
Transparent Bridge 206
Transport-Modus 171
Transportschicht 30
Trap 238
Trojaner 245
TTL 117, 129 f., 168
TUBA 163
Tunneling 178
Tunnel-Modus 171
Twisted Pair 15, 40, 54, 63

U

Überlastkontrolle 215
U/L-Bit 70
Unicast 22 f., 34, 176, 189
Uplink 189
URG 154
UTP-Kabel 57, 60, 63, 90, 92, 98 f.

V

Verbindungsaufbau 24, 30, 146, 155, 157, 161
Verfügbarkeitsverbund 16
Verschlüsselung 31, 34, 164, 171, 184
Version 66 f., 104, 114, 116, 162, 164 f., 167 f., 172, 179
Verzögerung 18, 95, 115, 191 f., 216
Viren 245

Virtual Router Redundancy Protocol (VRRP) 210
VLAN 14, 68, 107, 193 f., 228 f.
Vollader 51
Vollduplex 68, 101 ff., 156, 194

W

WAN 17, 103 f., 106 ff., 228 f.
Wegewahl 14, 17, 146, 165, 215 f., 229
Wellenlänge 44, 47 ff., 54, 99, 103
Well-Known-Port 155
Widerstand 55 f.
Window-Prinzip 153 f., 157 f., 161
Wires Equivalent Privacy (WEP) 262, 265 f.
wireshark 244
Wire-Speed 193
Wiring Closet 58
Würmer 245

Informatikwissen kompakt.



Schneider (Hrsg.)

Taschenbuch der Informatik

7., neu bearbeitete Auflage

736 Seiten, 271 Abb., 99 Tab.

ISBN 978-3-446-42638-2

Eine umfassende Gesamtübersicht zu den wichtigsten Teilgebieten der Informatik in einem Taschenbuch – das macht die Einzigartigkeit dieses Werkes aus.

Es spannt den Bogen von den theoretischen und technischen Grundlagen der Informatik über die verschiedenen Teilgebiete der praktischen Informatik bis hin zu vielen aktuellen Anwendungen in technischen und (betriebs-)wirtschaftlichen Bereichen. Die kompakte und übersichtliche Darstellung ermöglicht eine konzentrierte Wissensvermittlung.

Für die 7. Auflage wurde das Werk komplett überarbeitet und aktualisiert.

Wolfgang Riggert

Rechnernetze

Dieses Lehrbuch vermittelt die Grundlagen der Netzwerktechnik und der Netzwerkarchitektur. Es erläutert die Voraussetzungen, die Funktionsweise und die technischen Hintergründe von Computernetzwerken. Nach der Hardware des Netzes mit Übertragungsmethoden und Übertragungsmedien werden wichtige Entwicklungsstufen des Ethernet erläutert.

Ausgehend vom OSI-Schichtenmodell werden die IP-Protokollfamilie, die Netzwerkadressierung sowie Geräte und Protokolle betrachtet. Das Buch befähigt nicht nur zur Beurteilung der Technik sondern hilft auch, praktische Abwägungen und Entscheidungen bei der Netzwerkplanung zu treffen. Es zeigt neben den Basis-komponenten, Übertragungsverfahren und Verbindungskomponenten auch strategische Aspekte, Trends und zukünftige Entwicklungslinien und vermittelt die Grundlagen zu Strategien und Methoden der Computervernetzung.

Für die 4. Auflage wurde das Lehrbuch aktualisiert, didaktisch verbessert und u.a. um Kapitel zur Netzwerkverwaltung und zum Thema Wireless LAN erweitert.



Im Internet finden sich zum Buch unter
www.rechnernetze-interaktiv.de

Aufgaben mit Lösungen, multimediale Präsentationen, der CBT Kurs »Technischer Netzwerkassistent« zu Netzwerken unter Windows und ein Glossar mit Internet-Links.

Wolfgang Riggert ist Professor für Netzwerke und Informationsmanagement an der Fachhochschule Flensburg. Er ist Autor zahlreicher Beiträge zu Netzwerkthemen und Bücher. Vor seiner Lehrtätigkeit war er sechs Jahre als Softwareentwickler bei Norsk Data tätig.

Inhalt:

- Netzwerkgrundlagen
- Netzwerkarchitektur
- Übertragungsmethoden
- Übertragungsmedien
- Ethernet-Technologie
- Standards
- IP-Protokollfamilie
- IP-Adressierung
- TCP-Protokoll
- IPv6
- Layer 2 und 3: Geräte, Protokolle, Konzepte
- Netzwerkverwaltung
- Wireless LAN

HANSER

www.hanser-fachbuch.de

€ 29,90 [D] | € 30,80 [A]

ISBN 978-3-446-43164-5



9 783446 431645