IP-Netzwerke

1. IP-Netzwerke 2
1.1. Rechnernetze und das Internet 2
1.1.1 Was ist ein Netzwerk? 2
1.1.2 Programme „reden“ miteinander 2
1.1.3 Das OSI-Schichtenmodell 5
1.1.4 Die Funktionalitäten der OSI-Schichten 7
1.1.5 Der TCP/IP-Protokollstack 9
1.2 Die Sicherungsschicht 10
1.2.1 Das Point to Point Protocol 10
1.2.2 Sicherungsschicht: Das Serial Line Protocol 10
1.3 Vermittlungsschicht: Das Internet Protocol 11
1.3.1 Eigenschaften des IPv4 11
1.3.2 Wichtige Felder des IPv4 12
1.3.3 IPv6 - Das neue Format 13
1.4 Arten von Computernetzen 17

2. Lokale Netze -- Local Area Networks (LAN) 18
2.1 Die klassischen Topologien im LAN 19
2.2 Die Elemente eines Netzwerks 20
2.2.1 Passive Komponenten 21
2.2.2 Aktive Komponenten 23
2.2.2.1 Netzwerkkarte 23
2.2.2.2 Repeater 23
2.2.2.3 Hub 23
2.2.2.4 Bridge 24
2.2.2.5 Switch 25
2.2.2.6 Router 25
2.2.2.7 Gateway 27

3. Ethernet 28
3.1 Zugang zum Medium - CSMA/CD 28
3.2 Der Ethernet-Frame und Adressen 30
3.2.1 Ethernet Frameaufbau 31
3.2.2 Ethernet Frameaufbau (2) 32
3.3 Wichtige Ethernet-Vertreter 34
3.3.1 10Base2 34
3.3.2 10BaseT 34
3.3.3 Fast- und Gigabit Ethernet 35
3.3.4 Token Ring 35

4. Die Sicherungsschicht (Data Link Layer) 36

5. IP-Adressen 39
5.1 Vermittlungsschicht: Das Internet Protocol (IP) 39
5.2 Eigenschaften des IPv4 40
5.3 Adressierungsebenen bei der Datenkommunikation 43
5.4 IP-Adressen nach IPv4 44
5.5 Spezielle Adressen 46
5.6 Subnetze 48
5.6.1 Paketvermittlung im Subnetz 49

5.6.2 Bildung der Subnetzmaske 50
5.6.3 Beispiel für ein Router Topology Lab 51

6. Die Transportschicht TCP (Layer 4) 53
6.1 Funktionen der Transportschicht 53
6.2 Adressierung auf der Transport-Schicht 53
6.3 Aufbau des TCP-Protokollrahmens 54

7. Das Address Resolution-Protokoll (ARP) 56
7.1 Hardwareadressen 56
7.2 So löst ARP MAC-Adressen für den Remotedatenverkehr auf 58
7.3 Der ARP-Cache 59

8. Das Domain Name System Protocol (DNS-Protocol) 60
8.1 Der Domain-Name-Service (RFC-Spezifikation) 60
8.2 Aufbau eines Domain-Namens 60
8.3 Die Auflösung von Namen zu Nummern 61
8.4 NIC's und NOC's: 62

1. IP-Netzwerke

1.1. Rechnernetze und das Internet

1.1.1 Was ist ein Netzwerk?

Ein Netzwerk besteht im allgemeinen aus einer Gruppe von Computersystemen und Terminals, die über Kommunikationsleitungen miteinander verbunden sind und die Informationen und Ressourcen gemeinsam nutzen. Ein Netzwerk umfasst technische Einrichtungen (Leitwege, Vermittlungsstellen und Anschlussstellen) und entsprechende Übertragungs- und Vermittlungsverfahren. Die Terminals oder Netzwerkknoten liegen im Lokalen Netzwerk (LAN) auf engem geographischen Raum oder in Großnetzwerken weit verstreut. Sie sind über Kabel, Wähl- oder Standleitungen verbunden.

1.1.2 Programme „reden“ miteinander

Vernetzung hat nur einen Grund: Programme auf verschiedenen Rechnern sollen miteinaner `reden´, also Daten austauschen. Denn manche Rechner verfügen über viel freien Plattenspeicher, einen Drucker oder einen Datenbestand, den auch Anwender an anderen Systemen nutzen sollen. Jede einzelne dieser Dienstleistungen stellt ein eigenes Programm, ein `Server´ im Netz zur Verfügung. So gibt es beispielsweise Dateiserver, Druckserver oder WWW-Server.

Üblicherweise bezeichnet man einen Rechner, auf dem solche Server-Programme laufen, ebenfalls als Server. Er benötigt ein entsprechendes Betriebssystem, das unter anderem mehrere Serverprogramme gleichzeitig ausführen und die Daten der verschiedenen Benutzer vor unerlaubten Zugriffen schützen muß.

Der `Kunde´, der die Dienstleistung eines Servers nutzen will, ist ebenfalls eine Software und heißt `Client´. Die Sprache, in der Client und Server miteinander reden, muß genormt sein; eine solche genormte Sprache heißt Protokoll. Beim Abruf von WWW-Seiten ist es das Hypertext Transfer Protocol (HTTP), beim Zustellen von Briefen (EMail) über das Netz das Simple Mail Transfer Protocol (SMTP) - so hat jede Dienstleistung ihr eigenes Protokoll mit seiner kryptischen Abkürzung.

Losgelöst von seinen physischen Komponenten (Computern, Telefonleitungen etc.) ist das Internet eine Sammlung von Protokollen für Anwendungen, die dafür sorgt, daß netzweit Server und Clients miteinander kommunizieren können.

1.1.3 Kommunikation über Verbindungsleitungen

Netzwerke können unterschiedlich aufgebaut sein, je nach Aufbauschema bezeichnet man die Netzwerkstruktur als Bustopologie, Sterntopologie, Ringtopologie usw..

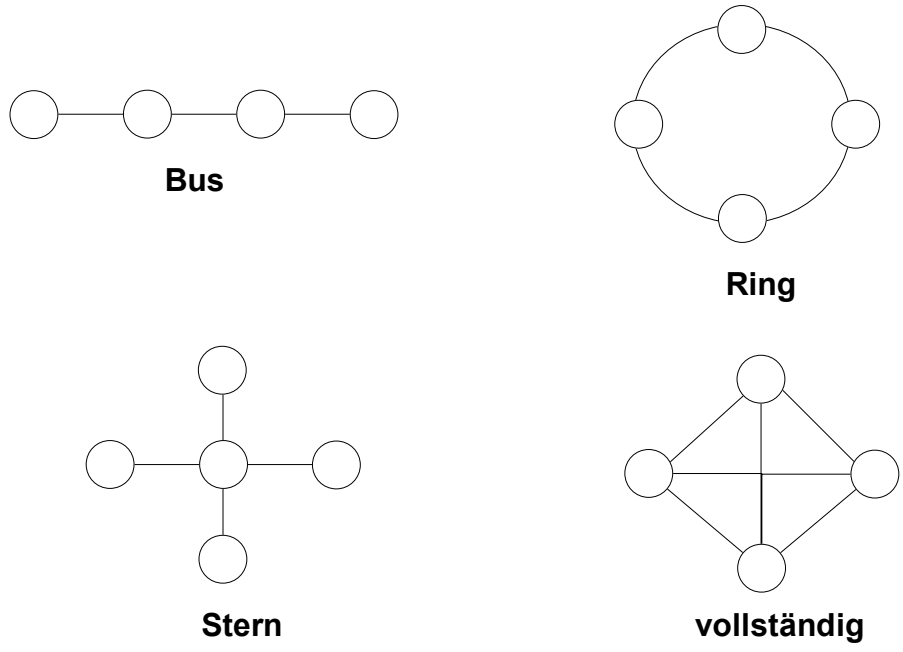


Bild: Verbindungstopologien

Vorteile von Netzen sind u.a.: flexibler Austausch von Daten und Programmen, die wirtschaftliche Ausnutzung teurer Peripheriegeräte sowie die effektive Informationsbeschaffung und -verteilung.

Von einem öffentlichen Netzwerk spricht man, wenn die Datenübertragung über öffentliche Leitungen, z.B. über Wählleitungen und/oder Datenpaketvermittlung, erfolgt und Telekommunikationsdienste angeboten werden.

Topologie	Anzahl der Verbindungen	Max. Grad eines Knotens	Max. Entfernung zwischen Knoten	Homogenität
Bus	n - 1	2	n - 1	inhomogen
Ring	n	2	n / 2	homogen
Stern	n -1	n - 1	2	inhomogen
Vollständig	n (n - 1) / 2	n - 1	1	homogen

Ein Netz ist homogen, wenn von allen Knoten gleich viele Verbindungen ausgehen.

Jede Verbindungstopologie hat ihre Vor- und Nachteile was Kosten und Kommunikation angeht.

Parallelrechner	Rechnernetz
gleiche Rechner	unterschiedliche Rechner
gemeinsame Aufgabe	im allgemeinen verschiedene Aufgaben
begrenzte Entfernung	kilometerlange Entfernungen
dichter Verkehr	die Datenübertragung - ein zusätzlicher Dienst

Die ganze Welt ist durch das Netz der Netze (Internet, www) verbunden.

Protokolle der Datenübertragung

- Regeln wie der Sender die Daten vor der Übertragung verschlüsselt und der Empfänger sie nach der Übertragung entschlüsselt
- die Datenmengen sind in die Pakete zerlegt
- die Fehlerlosigkeit wird durch Prüfzeichen gesichert
- Aufbau eines Pakets:

  Steuerungsblock (Empfänger, Typ der Information, Aufbau der Verbindung)

  Datenblock

  Schlußblock (Abbau der Verbindung)

Verschiedenheit der Probleme im Netz wird durch Schichten gelöst.

1.1.3 Das OSI-Schichtenmodell

Das OSI (Open System Interconnection)-Referenzmodell ging 1982 aus Arbeiten der ISO (Internationale Organisation für Standardisierung) hervor. Es handelt sich um einen offenen Kommunikationsstandard, welcher die Kommunikation zweier Computer untereinander beschreibt.

- Anwendersystem
    7. Anwendungsschicht (Application Layer)
    6. Darstellungsschicht (Presentation Layer)
    5. Kommunikationsteuerungsschicht – Sitzung (Session Layer)

- Transportsystem
    4. Transportschicht (Transport Layer)
    3. Vermittlungsschicht (Network Layer)
    2. Sicherungsschicht (Link Layer)
    1. Bitübertragungsschicht (Physical Layer)

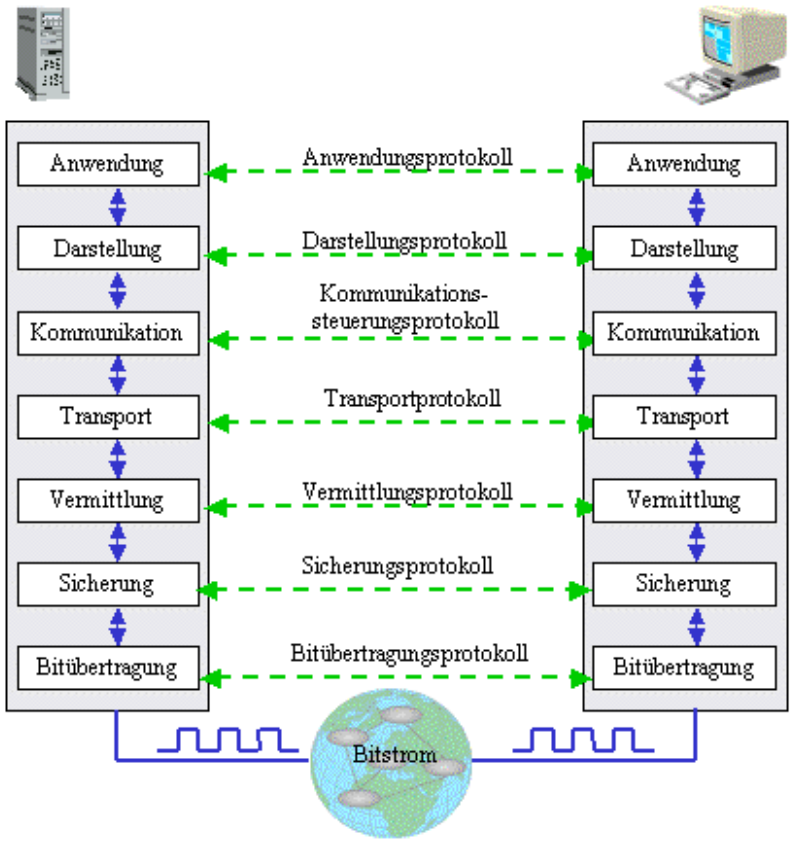


Bild: Das ISO-OSI-Protokollschichtenmodell

Beim Versenden von Informationen gibt jede Schicht die Daten zuzüglich eigener Protokollinformationen, genannt Header, an die darunterliegende Schicht bis zur Bitübertragungsschicht weiter. Die Protokollinformationen geben Auskunft darüber, wer die Daten abgesandt hat und wer sie empfangen soll, welchen Weg sie während der Über-

tragung nehmen sollen, wie sie weiterverarbeitet werden dürfen oder wie sie vom Empfänger behandelt werden sollen.

Auf der Empfangsseite werden die Schichten in umgekehrter Reihenfolge durchlaufen. Jede Schicht verarbeitet die für sie bestimmten Protokollinformationen, entfernt sie und leitet die verbleibenden Daten an die darüberliegende Schicht bis zur Anwendungsschicht weiter.

Die folgende Grafik verdeutlicht diesen Vorgang der Header-Addition auf Seiten des Senders und der Header-Abarbeitung auf Seiten des Empfängers.

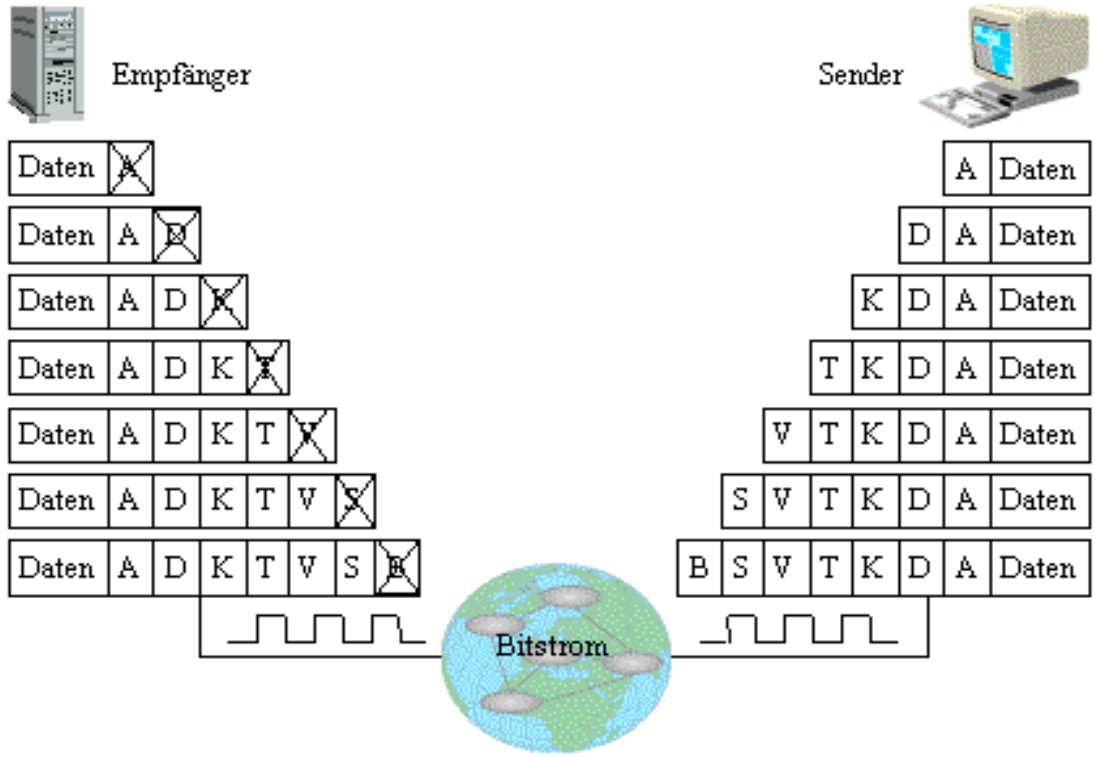


Bild: Encapsulation der einzelnen Protokollschichten

Da jeder Kommunikationspartner zugleich Sender und Empfänger sein kann, ist der Datenfluß auch in anderer Richtung als oben beschrieben möglich. Jede Schicht des OSI-Referenzmodells ist demnach in der Lage, von der ihr vor- oder nachgelagerten Schicht Daten zu empfangen oder ihr solche zu übergeben. Daher zeigen in der ersten Graphik die blauen Pfeile in beide Richtungen.

Wie bereits erwähnt, benutzen die einzelnen Schichten unterschiedliche Protokolle, sprechen sozusagen unterschiedliche Sprachen. Entsprechend verarbeitet auf der Empfangsseite jede Schicht die Protokollinformationen der entsprechenden Schicht auf der Versenderseite, so daß der Eindruck entsteht, die Schichten kommunizieren direkt miteinander. Die obere Graphik deutet dies durch die grün gestrichelten Pfeile an.

<table>
<tr><td>Anwendung</td><td>File Transfer</td><td>Electronic Mail</td><td>Terminal Emulation</td><td>Usenet News</td><td>Gopher</td><td>WAIS</td><td>WWW</td><td>Domain Name Service</td><td>Archie</td></tr>
<tr><td>Darstellung</td><td rowspan="2">File Transfer Protocol (FTP)</td><td rowspan="2">Simple Mail Transfer Protocol (SMTP)</td><td rowspan="2">Telnet Protocol (Telnet)</td><td rowspan="2">Network News Transfer Protocol (NNTP)</td><td rowspan="2">Internet Gopher Protocol</td><td rowspan="2">Z39.50</td><td rowspan="2">Hyper Text Transfer Protocol (http)</td><td rowspan="2">Domain Name System (DNS)</td><td rowspan="2">Prospero Protocol</td></tr>
<tr><td>Kommuni-kation</td></tr>
<tr><td>Transport</td><td colspan="7">Transmission Control Protocol (TCP)</td><td>User Datagram Protocol</td></tr>
<tr><td>Vermittlung</td><td colspan="2">Address Resolution Protocol (ARP)</td><td colspan="4">Internet Protocol (IP)</td><td>Internet Control Message Protocol (ICMP)</td></tr>
<tr><td>Sicherung</td><td colspan="9">Ethernet, Token Ring, DQDB, FDDI</td></tr>
<tr><td>Bitüber-tragung</td><td colspan="9">Übertragungsmedium
Doppelader, Koaxkabel, Lichtwellenleiter, drahtlose Übertragung</td></tr>
</table>

Bild: Protokolle im OSI-Modell

1.1.4 Die Funktionalitäten der OSI-Schichten

Anwendungs-Schicht	System-Steuerung, Autorisierung, Inhaltliche Kontrolle, Gültigkeitskontrolle, ..
Darstellungs-Schicht	Codierung, Syntax, Profilverwaltung, ..
Kommunikationssteuerungs-Schicht	Übertragungsrechte, Sitzungsverwaltung, Flusskontrolle, ..
Transport-Schicht	Verbindungsauf-/abbau, Packetverwaltung, ..
Vermittlungs-Schicht	Leitwegfindung, Netzadressierung, Multiplexing, ..
Sicherungs-Schicht	Fehlerkontrolle, Flusskontrolle, Synchronisation, ..
Bitübertragungs-Schicht	Aktivierung/Deaktivierung, Bitübertragung, Anschlusserkennung, ..

Bild: Schichten und ihre Aufgaben

Nachfolgend werden die einzelnen Schichten und ihre Aufgaben beschrieben.

Übertragungsschicht

Diese Schicht korrespondiert mit der zugrunde liegenden Hardware. Protokolle dieser Schicht legen die Eigenschaften der Schnittstellen fest wie Anschlusseigenschaften, zulässige Übertragungsraten, Signalpegel und elektrische Kodierung der einzelnen Bits (z.B. Modulationsverfahren bei Modems)...

Verbreitete Vertreter dieser Protokolle sind RS-232 (serielle Schnittstelle) und X.21.

Sicherungsschicht

Protokolle dieser Schicht gewährleisten die Unversehrtheit der übertragenen Daten. Dazu verpacken sie die Daten in für das Medium zulässige Einheiten, steuern den Fluss der Übertragung und fügen Prüfsummen an die eigentlichen Datenpakete an, anhand derer der Empfänger den Zustand der Daten überprüfen kann. Im Fehlerfall kümmern sich die Protokolle dieser Schicht automatisch um eine Wiederholung der Übertragung.

Hier offenbart sich eine Schwäche des OSI-Modells, das die Grenzen der Schichten nicht allzu konsequent gezogen hat. So unterteilen die Realisierungen lokaler Netzwerke diese Schicht nochmals in *Media Access Control (MAC)* und *Logical Link Control (LCC)*. So organisiert z.B. Ethernet den Zugang zum Übertragungsmedium mittels einer MAC-Schicht (oft CSMA/CD - Carrier Sense Multiple Access with Collision Detect), während LCC eine Schnittstelle zu übergordneten Diensten darstellt.

Weitere wichtige Protokolle der Sicherungsschicht sind High-Level Data Link Control HDLC, das darauf basierende Point-to-Point-Protocol PPP, und das Serial Line Protocol SLIP.

Vermittlungsschicht

Auch als Netzwerkschicht bezeichnet, ist diese Schicht für den Aufbau eines virtuellen Kommunikationskanals verantwortlich. Dazu zählen das Auffinden eines Weges zum Zielrechner, die Vermittlung der Nachrichten und Pakete (eine »lange« Nachricht wird ggf. in einzelne Pakete unterteilt).

Verfolgt man den Weg eines Paketes vom eigenen Rechner hin zu einem Rechner »am anderen Ende der Welt«, so stellt man fest, dass die Route durch zahlreiche Teilnetze führt, denen mitunter vollkommen unterschiedliche Technologien (Lichtwellenleiter, Funk, Ethernet, Modem...) zugrunde liegen. Für jeden Übergang in ein neues Teilnetz wird ein Protokollwechsel in den »unteren« Schichten notwendig. An welchen Rechner eines solchen Teilnetzes das Paket als nächstes zu »routen« ist, bleibt Angelegenheit der Vermittlungsschicht.

Den bekanntesten Vertretern dieser Schicht, IP, ICMP und ARP, wenden wir uns nachfolgend zu. Weitere Protokolle sind X.25, Exterior Gateway Protcol EGP, Border Gateway Proctocol BGP, Open Shortest Path First OSPF und Routing Information Protocol RIP.

Transportschicht

Diese Schicht stellt den »anwendungsorientierten« Schichten einen logischen Übertragungskanal zur Verfügung, so dass diese ihre Daten sequentiell an die Schnittstelle senden. Protokolle der Transportschicht steuern die Blocklängen, die Geschwindigkeit, mit der Pakete an die unteren Schichten weiter gegeben werden und realisieren (oft) eine Fehlersicherung.

Damit sich Sender und Empfänger auch verstehen, muss auf beiden Seiten dasselbe Transportprotokoll zum Einsatz gelangen, d.h. beide Kommunikationspartner müssen »dieselbe Sprache sprechen«.

Bekannte Protokolle sind TCP und UDP.

Sitzungsschicht

Protokolle der Sitzungsschicht realisieren die logische Adressierung, d.h. sie sind u.a. zuständig, einen Zielrechner zu finden, der die geforderte Anforderung erfüllen kann. Weitere Funktionen sind Nutzeridentifikationen, die erneute Verbindungsaufnahme nach einem Abbruch, Wechsel der Kommunikationsrichtung usw...

Zu den Protokollen zählen der Remote Procedure Call und LU6.2.

Darstellungsschicht

Ein Protokoll der Darstellungssicht organisiert die Umwandlung von Daten und Texten in ein bestimmtes Format. Auch die Terminalemulationen ordnen sich in diese Schicht ein.

XDR und ASN.1 zählen in diese Gruppe.

Anwendungsschicht

Letztlich bilden die Protokolle der Anwendungsschicht die Schnittstelle zu den Anwendungsprogrammen.

Mit FTP und HTTP seien nur zwei Vertreter erwähnt.

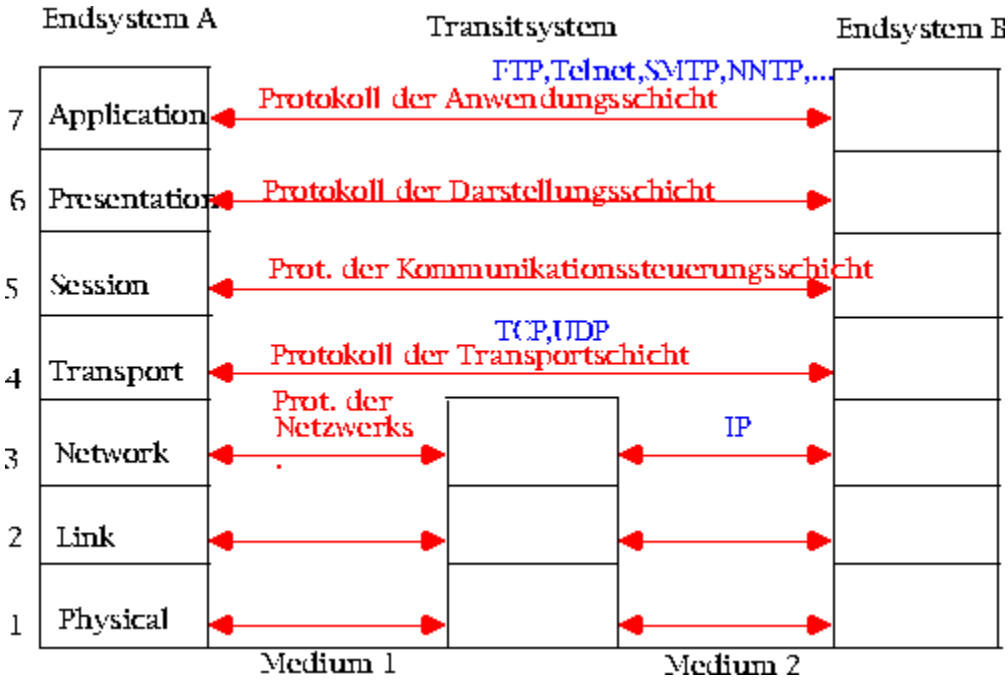


Bild: Kommunikation zwischen den ISO/OSI-Ebenen

1.1.5 Der TCP/IP-Protokollstack

Die TCP/IP-Architektur hatte sich bereits durchgesetzt, als die *International Standardisation Organisation* (ISO) ihr Modell eines Internet-Protokollstacks *Open System Interconnection* (OSI) veröffentlichte.

Es hat sich auch gezeigt, dass die gewählte Struktur den Zusammenhängen zwischen den Komponenten der Hardwareebene wie auch der Anwendungsebene besser gerecht wird. So liefern Hersteller der Übertragungstechnik die Software der Ebenen 1 und 2 mit dieser aus, während der Anwendungsentwickler seine Applikation mit Eigenschaften der »oberen« OSI-Schichten ausstattet.

Nicht zuletzt verfügt jedes Betriebssystem, das den Zugang zum Internet ermöglicht, eine Implementierung des TCP/IP-Protokollstacks.

Im weiteren Verlauf wird zu den beschriebenen Protokollen deren Einordnung in das OSI-Referenz-Modell angegeben.

1.2 Die Sicherungsschicht

1.2.1 Das Point to Point Protocol

Flag	Adresse	Prüfung	Protokoll	Daten	FCS	Flag

Das **Point-to-Point-Protokoll** ermöglicht permanente Punkt-zu-Punkt-Verbindungen. Häufigster Einsatzbereich sind Wählverbindungen (Modem).

Das enthaltene Protokollfeld ermöglicht die Unterstützung beliebiger Vermittlungsprotokolle; die Prüfsumme erlaubt die Verifizierung des Dateninhalts.

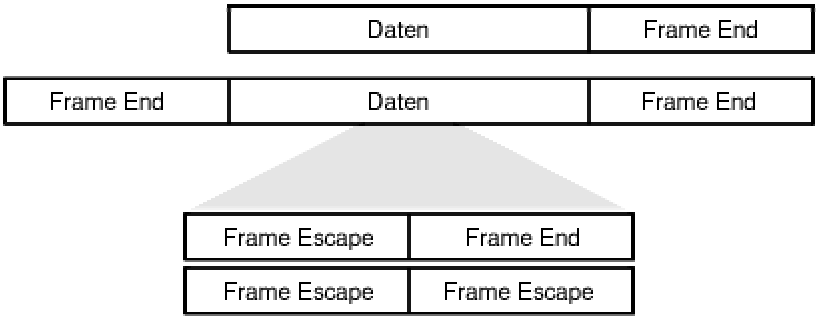
Als optionale Eigenschaften können Implementierungen Folgendes enthalten:

- Einwahl nach Bedarf, Verbindungsabbau nach Zeit- oder Gebührenüberschreitung
- Parallele Verwendung mehrerer Leitungen
- Einfache Filtermechanismen
- Komprimierung der Daten und/oder des Headers

Das PPP handelt mit der Gegenseite eine Maximale Empfangspaketgröße aus, das ist der Grund für den verzögerten Verbindungsaufbau über analoge Telefonleitungen.

1.2.2 Sicherungsschicht: Das Serial Line Protocol

Das **Serial Line Protokoll** ist das zweite Protokoll der Sicherungsschicht, das bei Modemverbindungen zum Einsatz gelangt. Wie der Name bereits besagt, dient es der Verbindung zweier Rechner über eine serielle Leitung. Als Protokoll der Schicht 3 kommt allerdings einzig IP in Frage; auch beinhaltet das Protokoll keinerlei Sicherungsmaßnahmen.



Mögliche Einsatzgebiete sind sichere Leitungen, bspw. ein Nullmodemkabel.

Auf SLIP baut das **CSLIP** (Compressed SLIP) auf, das den Header von TCP-Paketen nach einem Verfahren von Van Jacobsen komprimiert.

1.3 Vermittlungsschicht: Das Internet Protocol

Die heute gebräuchlichen Adressen des Internet-Protokolls sind 32 Bit lang, die häufigste Notation erfolgt byteweise als Dezimalzahl, bspw. »127.211.7.9«. Der Mathematiker errechnet rasch, dass mit 32 Bit 2^{32} = 4.294.967.292 Rechner adressierbar wären. Der Praktiker interveniert, dass sich nicht alle Adressen nutzen lassen, da etliche Adressen und Adressbereiche für bestimmte Funktionen reserviert sind. Auch existieren genügend Lücken im Adressraum, da IP's im Block an lokale Netzwerke vergeben werden, diese aber nur selten ihr Kontingent voll ausschöpfen.

Fazit ist, dass schon heute die Zahl der verfügbaren Adressen den Bedarf bei weitem nicht mehr decken kann und eine Aufweitung der Adressen erforderlich ist. Aus diesem Grund steht der designierte Nachfolge des korrekt als IPv4 bezeichneten Protokolls seit Jahren (erste Spezifikation 1995) in den Startlöchern. Anliegen dieses IPv6 ist nun die Definition eines Protokolls der Vermittlungsschicht, das mit 128 Bit Adressen arbeitet. Die damit erzielte Größe erscheint übertrieben (jedem Quadratmillimeter auf dem Globus ließen sich hiermit ca. 667 Billiarden IP's zuweisen), jedoch ist man auf weite Sicht auf der sicheren Seite.

Mit dem Adressformat nach IPv4 befasst sich der Abschnitt Netzwerkstrukturen, IP-Adressen.

1.3.1 Eigenschaften des IPv4

Bei der immensen Bedeutung, welche gerade dieses Protokoll für die Paketvermittlung im Internet erlangt hat, lohnt sich ein tieferer Einblick in dessen Fähigkeiten.

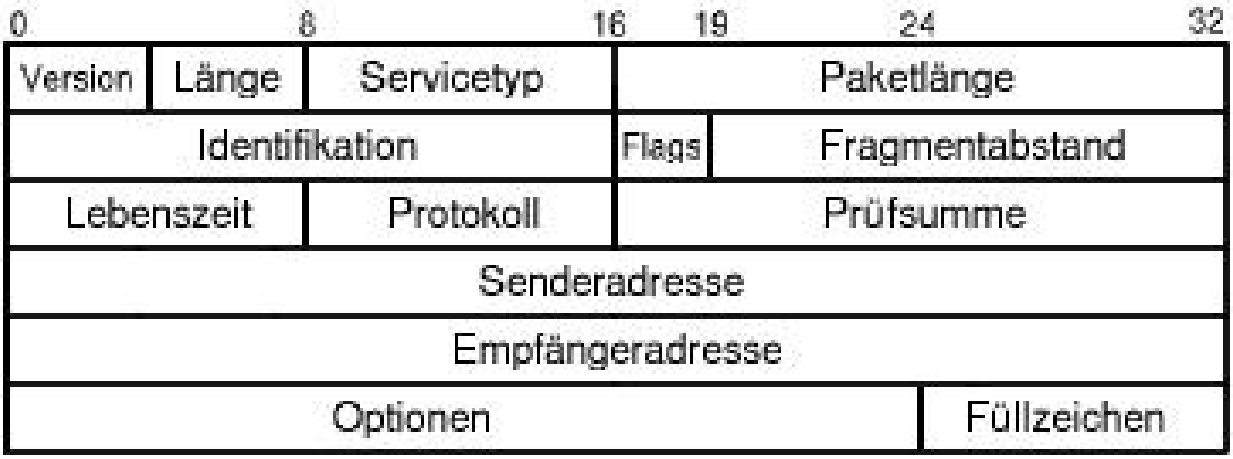
Zunächst gilt zu vermerken, dass es sich um ein **verbindungsloses** Protokoll handelt, d.h. es arbeitet, ohne dass eine Verbindung zum Partner zuvor aufgebaut wurde (analog zum Unterschied zwischen einem Telegramm und einem Telefonat). Die maximale **Paketgröße beträgt 65535 Bytes**. Ein Paket durchläuft auf seinem Weg zum Empfänger meist verschiedenste Subnetze, die ihrerseits nur eine kleinere Paketgröße unterstützen. Das IP beinhaltet deswegen einen Mechanismus zur **Fragmentierung** von Paketen, d.h. dass ein für ein zu durchlaufendes Subnetz zu großes Datenpaket zerlegt wird und nun mehrere IP-Pakete ihren Weg zum Empfänger suchen. Der

Zusammenbau der Paketteile erfolgt erst beim endgültigen Empfänger, da die Teilpakete durchaus auf unterschiedlichen Routen ihr Ziel finden.

Eine **Prüfsumme** stellt die Unversehrtheit des IP-Kopfes sicher, nicht jedoch die der enthaltenen Daten. Dessen Überwachung obliegt dem Protokoll der nächsthöheren Schicht; ein Code im IP-Kopf (**Protokoll**-Feld) verweist auf den Typ des Protokolls (bspw. steht eine 6 bei TCP und eine 17 bei UDP).

Die letzte erwähnte Eigenschaft, die die **Lebensdauer** eines IP-Pakets begrenzt, garantiert, dass ein nicht vermittelbares Paket nicht endlos im Netz kursiert, sondern nach Ablauf seiner Lebenszeit verworfen wird. Früher wurde hier tatsächlich mit einer Zeiteinheit gearbeitet, jedoch wich diese bald der maximalen Anzahl Stationen (»Hops«), die ein Paket maximal durchlaufen darf. Jeder Rechner, der das Paket weiterleitet, verringert diesen Wert um 1. Erreicht er in einem Rechner den Wert 0 und handelt es sich nicht um den Zielrechner, so sendet dieser Rechner ein ICMP-Protokoll an den Absender und verwirft das eigentliche Paket.

1.3.2 Wichtige Felder des IPv4



Die Bedeutung mancher Felder ergibt sich schon aus deren Namen, diejenige, deren Bedeutung nicht sofort ersichtlich ist, sollen nun erläutert werden:

Versionsnummer

Version des Protokolls, also 4 bei IPv4 und 6 bei IPv6

Länge

Größe des IP-Kopfes in Worten (32 Bit = 1 Wort); hierdurch ist die Angabe von Optionen variabel

Servicetyp

In der Linux-Implementierung wird dieses Feld nicht berücksichtigt. Es dient dazu, ein Paket mit unterschiedlicher Priorität oder erhöhter Zuverlässigkeit... zu vermitteln

Paketlänge

Länge inklusive der IP-Kopfes in Worten

Identifikation

Vom Absender vergebene eindeutige Nummer, anhand derer einzelne Fragmente im Zielrechner in der richtigen Reihenfolge zusammen gesetzt werden können

Flags

Das erste Bit wird nicht benutzt, das zweite Bit gibt an, dass ein Paket nicht fragmentiert werden darf. Ist ein solches Paket zu groß für ein Teilnetzwerk, muss es verworfen werden. Das dritte Bit gibt an, ob dem Paket noch weitere Teile folgen

Fragmentabstand

Relative Lage des Paketes, wenn dieses Teil eines zuvor größeren Paketes war (Fragmentierung)

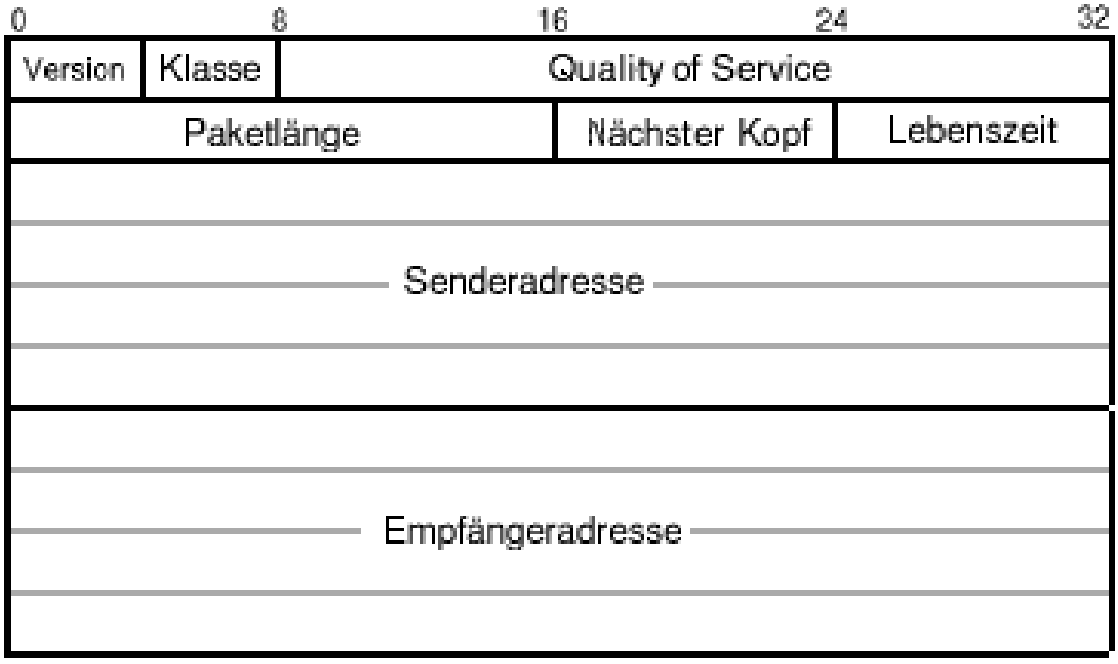
Lebenszeit und **Protokoll**

Siehe unter Eigenschaften des IPv4

Optionen

In erster Linie werden diese Optionen von Netzwerkadminstrationswerkzeugen genutzt. Sie können bspw. verwendet werden, um jeden durchlaufenden Rechner anzuweisen, seine IP-Adresse und/oder einen Zeitstempel zu hinterlegen. Ebenso kann eine Route, die ein Paket zurücklegen soll, festgeschrieben werden.

1.3.3 IPv6 - Das neue Format



Eine Prüfsumme wie bei IPv4 ist nicht mehr vorgesehen, da die Neuberechnung auf jeder Zwischenstation recht teuer ist (geändertes »Lebenszeit«-Feld) und unter- bzw. übergeordnete Protokolle i.d.R. ohnehin eine Fehlerbehandlung beinhalten.

Transportschicht: Das Transmission Control Protocol

Aus Sicht einer Anwendung eröffnet das *Transmission Control Protocol* einen bidirektionalen, virtuellen Datenkanal zwischen den beiden Kommunikationsendpunkten. Die Daten werden scheinbar in einem Fluss übertragen. Intern gehen diese natürlich blockweise übers Netz, wobei die Blockgröße dynamisch anhand von Parametern wie der Netzauslastung, der Fenstergröße oder der Empfangs- bzw. Sendepuffer angepasst wird. Im Unterschied zum nachfolgend erwähnten *User Datagram Protocol* kümmert sich TCP selbst um die sichere Übertragung. Es verwendet hierzu Sequenznummern, Prüfsummen, Quittungen und Wiederholung des Transfers bei einer Zeitüberschreitung. Andere wesentliche Eigenschaften sind das Sliding-Window-Verfahren und die Kennzeichnung von Vorrangdaten.

Die Felder des Protokollkopfes bedeuten:

Senderport, Empängerport

Analog zum Telefonat spielt der Sender einen aktiven und der Empfänger einen passiven Teil. Der Sender adressiert den Partner über IP-Adresse des Zielrechners und eine 16-Bit lange Portnummer. Beide zusammen bezeichnet man unter Unix als **Socket**. Um den Empfänger adressieren zu können, muss der Sender dessen Portnummer kennen. Der Sender wiederum kann (meist) eine beliebige freie Portnummer wählen, da er seine eigene Nummer dem Kommunikationspartner mitteilt. Für die Standarddienste stehen die Portnummern in der Datei /etc/services. Des Weiteren ist anzumerken, dass UDP einen eigenen Adressraum verwendet und gleiche Portnummern sich somit nicht überschneiden.

Sequenznummer

Dieser 32-Bit Wert kennzeichnet eindeutig die Stellung eines Pakets innerhalb des Datenstroms in Senderichtung. Die initiale Sequenznummer wird zu Beginn des Verbindungsaufbaus von jedem Kommunikationspartner festgelegt, wobei gilt, dass sie für die maximal mögliche Lebensdauer des Pakets (TimetoLive des Internet Protokolls) bez. der verbundenen Rechner eindeutig ist.

Die Sequenznummer eines folgenden Pakets berechnet sich aus der initialen Sequenznummer und der Anzahl bisher gesendeter Bytes. Somit ist es möglich, bei Verlust oder Beschädigung eines Pakets gezielt dieses wiederholt zu senden.

Quittungsnummer

Die Quittungsnummer sendet der Empfänger eines Pakets als Bestätigung für den Empfang. Sie gibt an, wie viele Bytes bislang beim Partner unversehrt eingetroffen sind. Sollten Sequenznummer oder Quittungsnummer im Laufe einer Sitzung einmal überlaufen, so wird bei 0 fort gefahren.

Offset

Das Feld enthält die Länge des TCP-Kopfes in 32-Bit Worten. Anhand dieser wird der Beginn der enthaltenen Daten ermittelt.

Reserve

Wird nicht verwendet.

Steuerbits

Die 6 Steuerbits bedeuten:

UR
G

Die Daten im Feld "Vorrangdaten" sind gültig

ACK

Die Quittungsnummer ist gültig

PSH

Die Daten sollten sofort der Anwendung übergeben werden

RES

Rücksetzen der Verbindung

SYN

Wunsch nach Aufbau einer Verbindung

FIN

Beenden der Verbindung. Ein Partner, der dieses Bit setzt, muss seinerseits die Verbindung offenhalten, bis auch der Gegenüber das FIN-Bit sendet. Er selbst darf aber keine weiteren Daten senden (Ausnahme sind die Quittungen auf eintreffende Pakete).

Fenstergröße

Momentane Kapazität des Empfangspuffers auf Absenderseite. Sein Gegenüber darf maximal so viele Daten (auch aufgeteilt auf mehrere Pakete) senden, wie durch die Fenstergröszlig;e angegeben ist. TCP arbeitet nun so, dass es versucht, die Fenstergröße automatisch an die Kapazität des Übertragungsmediums anzupassen. Dazu wird das Fenster allmählich vergrößert, bis Pakete aufgrund des zu hohen Datenaufkommens verworfen werden müssen. Treten nun vermehrt solche Übertragungsfehler auf, wird das Fenster wieder verkleinert, um es anschließend erneut mit einer Erhöhung zu versuchen. Dieses Sliding-Window-Prinzip lässt sich sehr gut beim Download von Dateien beobachten, wobei die Datentransferrate ständig schwankt.

Prüfsumme

Prüfsumme über das gesamte Paket.

Zeiger auf Vorrangdaten

Der Zeiger gibt einen Offset innerhalb der Daten im Paket an. Die dem Zeiger folgenden Daten werden somit als besonders wichtig deklariert. Eine Anwendung wird beim Eintreffen solcher Daten unterrichtet. Sie sollte nun ihre bisherige Arbeit unterbrechen und die dringliche Nachricht bearbeiten. Gebrauch von diesem Mechanismus macht wohl nur Telnet.

Optionen

Beim Verbindungsaufbau wird meist "MaximumSegmentSize" gesendet, um dem Partner mitzuteilen, dass größere Pakete empfangen werden

können. Die weiteren Optionen sind "EndOfOptionList" und "NoOperation".

Das Zusammenspiel von Sequenz- und Quittungsnummer wird in den meisten Fällen die Unversehrtheit der übertragenen Daten garantieren. Jedoch verlangt eine ausstehende Quittung das Warten auf diese. Ist nun der Partner ausgefallen, würde ein Sender bis in alle Ewigkeit auf die Bestätigung des Empfangs seines Pakets lauern. Um einen solchen "Hänger" zu verhindern, werden beim Versand eines Pakets gleich mehrere Zeitgeber gestartet.

Der wichtigste Ticker stoppt die seit dem Senden vergangene Zeit. Läuft er ab, ohne dass eine Quittung eintraf, muss das Paket erneut auf die Reise geschickt werden. Diese Zeitspanne wird allerdings dynamisch berechnet (aus dem Mittelwert der bisherigen Paketlaufzeiten), sodass sie sich an veränderte Situationen (hohe Netzlast, alternative Route) allmählich anpasst.

Ein weiterer Wecker wird verwendet, um die Bereitschaft des Empfängers zu überprüfen. Dieser Zeitgeber garantiert, dass eine Datentransfer nicht blockiert, weil dessen Fenstergröße auf 0 steht, das Paket zum Öffnen des Empfangsfensters aber verloren ging.

Der letzte hier vorgestellte Timer hält einen Port noch eine gewisse Zeit geschlossen, nachdem die Verbindung schon abgebaut wurde. Die Zeitspanne entspricht in etwa der maximalen Lebensdauer (TimeToLive) eines Datenpakets und ist nützlich, um die nächste auf dem selben Port eröffnete Verbindung nicht durch alte irrgeleitete Pakete durcheinander zu bringen.

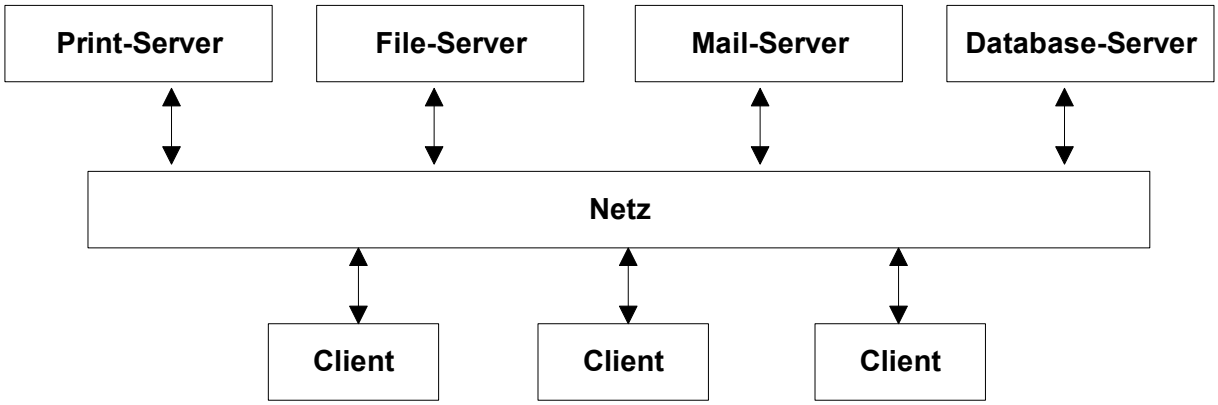
1.4 Arten von Computernetzen

- **LAN** (local area net) - Verbindungen über besondere Leitungen
- **MAN** (metropilitan area net) – Regionalnetz
- **WAN** (wide area net) Weitverkehrsnetz - Verbindungen über öffentliche Netze
- **GAN** (Global Area Network, Weltweites Netzwerk, z.B. Internet)

Warum Rechnernetze?

- Datenverbund - Austausch von Daten
- Funktionsverbund - Rechner mit verschiedener Leistungsfähigkeiten
- Lastverbund - Verteilung der Auslastung

Client-Server-Modell



Client - Auftraggeber,
Server - Anbieter (Auftragnehmer)

Verteilte Systeme

Rechnernetz	Verteiltes System
jeder Benutzer weiß auf welchem Netzknoten das Programm läuft	Netz ist unsichtbar
jeder Benutzer weiß, wo sich seine Daten befinden	

Vorteile des verteilten Systems:

- Besseres Kosten/Nutzen - Verhältnis, da viele zusammenarbeitende Mikrocomputer billiger als ein Großrechner sind
- Einfache Erweiterbarkeit
- Größere Zuverlässigkeit

Nachteile des verteilten Systems:

- Datenaustausch zwischen den Prozessoren ist sehr zeitaufwendig
- Das verteilte Betriebssystem ist sehr kompliziert

2. Lokale Netze -- Local Area Networks (LAN)

- Ein lokales Netz untersteht einer einzigen Organisation bzw. Unternehmen.
- Es erstreckt sich über ein Gebiet von wenigen Quadratkilometern.

- Es hat eine hohe Übertragungsrate von 4 MBits/s bis zu mehr als 1 Gbit/s (Gigabit-Ethernet).

2.1 Die klassischen Topologien im LAN

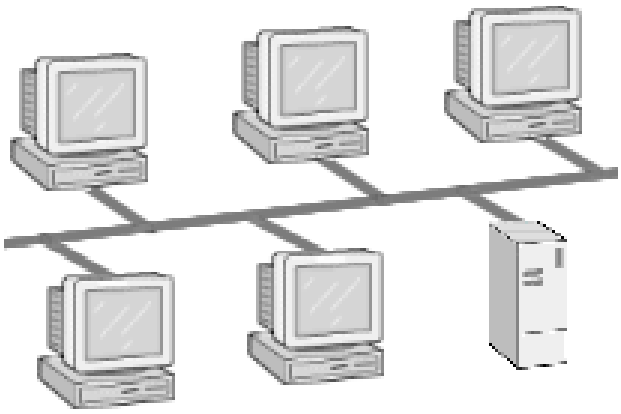


Bild 1: Die Busstruktur

Fakt ist, dass die **Busstruktur** (Bild 1) das verbreitetste Schema der Rechnerverbindung darstellt. Alle Rechner eines Netzwerks teilen sich denselben Bus, genauso wie es rechnerintern Prozessor, Speicher und Peripherie handhaben. Analog zum Systembus eines Computers ist auch die mögliche Anzahl der Rechner an einem Netzwerk-Bussystem begrenzt. Kritisch bei Bussystemen ist die Zugangssteuerung zum Verbindungsmedium, da zu einem Zeitpunkt stets nur eine Verbindung aktiv sein kann. Die Verfahren reichen von vorsorglicher Vermeidung konkurrierender Zugriffe bis hin zur Erkennung von Kollissionen. Der typische Vertreter bez. LANs ist das Ethernet.

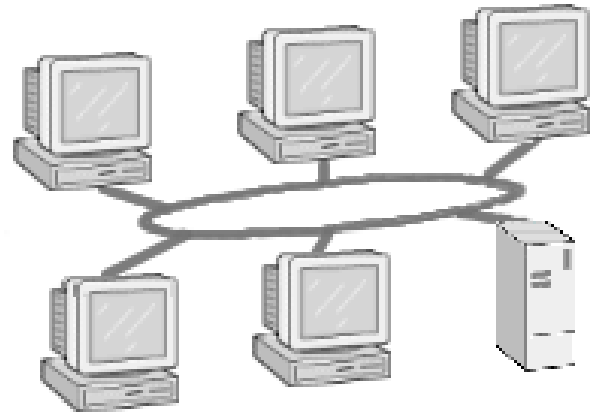


Bild 2: Die Ringstruktur

Vor allem mit Token Ring hat bei lokalen Netzwerken die **Ring-Topologie** als Vertreter der so genannten Punkt-zu-Punkt-Verbindungen eine gewisse Verbreitung erlangt. Ein Rechner kann (theoretisch) nur mit seinen unmittelbaren Nachbarn kommunizieren. Eine Verbindung zu weiteren Rechnern im Ring gelingt nur unter Verwendung der Zwischenrechner als »Vermittlerstationen«. »Theoretisch« deutet bereits eine weitere Einschränkung an, da in praktischen Vermittlungsverfahren in Ringstrukturen die Kommunikation nur in eine Richtung funktioniert, d.h. ein Rechner kann bspw. direkt zu

seinem rechten Nachbarn senden, benötigt aber alle weiteren Rechner, um dem linken Nachbarn ein Paket zukommen zu lassen. Ring-Netzwerke arbeiten ausschließlich mit »Token«, einem Rahmen, der fortwährend im Ring kreist und in den ein Rechner - insofern das Token nicht belegt ist - seine Nachricht platzieren kann. Der Zielrechner entnimmt dem Token die Daten und markiert dieses wieder als frei, sodass ein anderer sendewillige Rechner das Token nun belegen kann. Dieses Token-Verfahren kann ebenso auf reinen Bussystemen angewendet werden.

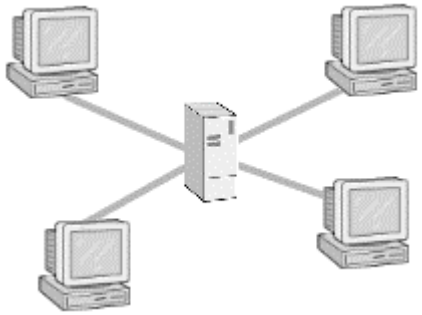


Bild 3: Die Sternstruktur

Die Beschreibung der **Sternstruktur** ist simple: Jeder Rechner im Netzwerk ist direkt mit der zentralen Komponente verbunden, welche im einfachsten Fall auf einer Leitung eintreffender Daten diese auf alle anderen Leitungen durchreicht. Betrachtet man sich die Struktur realer Ethernet- und Token-Ring-Netzwerke, wird man immer wieder auf Analogien zur Sternstruktur stoßen.

Ein auf Ethernet basierendes LAN größeren Umfangs besteht nur selten aus einem einzelnen Bussystem. I.d.R. werden mehrerer solcher Busse gekoppelt, häufig gar in einer zentralen Komponente (allgemein als »Sternkoppler« bezeichnet) , sodass tatsächlich eine Sternstruktur resultiert. Je nach »Intelligenz« der Komponente fügt sie die einzelnen Stränge des Netzes zu einem großen Bussystem zusammen, indem sie alle Daten ohne Rücksicht auf deren Zieladresse in jeden Anschluss einspeist oder aber sie »filtert« die Pakete und reicht sie nur in den Teil des Netzwerks weiter, indem der Empfängerrechner liegt.

Auch bei Token-Ring-Netzwerken mit mehreren Teilnehmern werden keine kilometerlangen Leitungen verlegt. Der Ring selbst ist in einem einzelnen Hardwarebaustein (»Ringleitungsverteiler«) realisiert, von welchem aus Stränge zu den einzelnen Rechnern gehen. Rein optisch gleicht es somit einem Stern.

2.2 Die Elemente eines Netzwerks

Um die einzelnen Endgeräte (Computer, Terminals, Netzwerkdrucker etc.) miteinander zu koppeln, gelangen verschiedenste Komponenten zum Einsatz. Eine grobe Unterteilung erfolgt anhand der Signalbehandlung. Für Bauteile, die Signale unverändert weiter reichen, wird oft der Begriff der **passiven Komponente** angewandt. Demzufolge sind **aktive Komponenten** Elemente, die eine Signalaufbereitung vornehmen. Den Aufgaben der wichtigsten Verteter beider Gruppen soll sich die folgende Abhandlung widmen.

2.2.1 Passive Komponenten

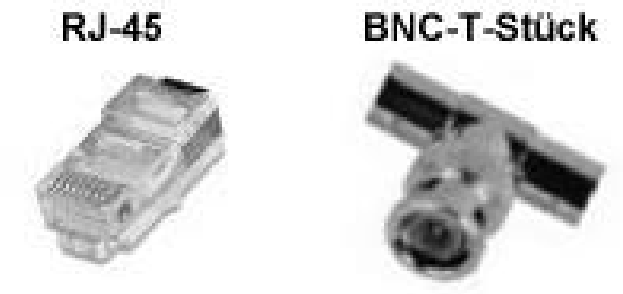


Bild 6: Verbreitete Steckverbindungen

Zu den passiven Bauelementen zählen die **Steckverbindungen** und **Kabel**. Erstere werden in lokalen Netzwerken in den Ausführungen **BNC** und **RJ45** angeboten.

BNC wird im Zusammenhang mit 10base2 (»Ethernet-Jargon« für Koaxial-Kabel) benutzt. Die Anbindung einer Station erfolgt entweder durch Auftrennung des Kabels und Einfügen eines BNC-T-Stücks (Bild) oder auch ohne Unterbrechung des Leiters (»Vampirstecker«). Im Falle dieser klassischen Bus-Topologie müssen alle freien Enden durch einen **Abschlusswiderstand** »geschlossen« werden, da Pakete ansonsten an diesen reflektiert werden und nachfolgende Pakete damit verwischen würden.

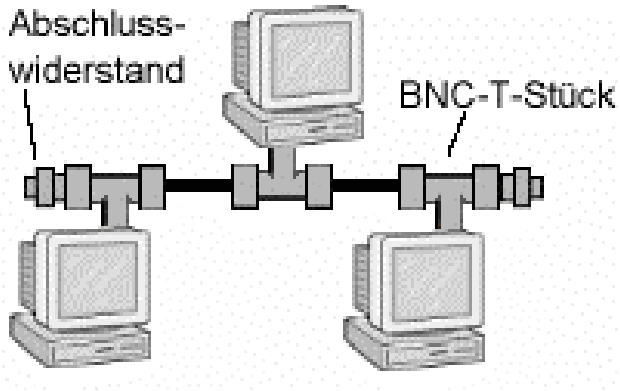


Bild 7: Koax-Netz

RJ45 ist die zum 10BaseT ([Un]shieled Twisted Pair) Anschluss passende Verbindung. Im Zusammenhang mit Ethernet bedingen Twisted-Pair-Kabel den Einsatz von aktiven Verteilerelementen (Bridges), um die einzelnen Stationen miteinander zu verbinden (daraus resultiert eine Sternstruktur).

Die Leistungsdaten eines Netzwerks werden durch die Kabel bestimmt, die Ausführung der Steckverbindungen ist letztlich irrelevant.

Bild 8: Verkabelungstechnik

Die einzusetzende **Kabeltechnik** hängt vor allem von zwei Faktoren ab. Zum einen von der Anzahl der Teilnehmer im Netz und somit von der benötigten Bandbreite und zum zweiten vom finanziellen Budget, das der Chef zur Verkabelung zur Verfügung stellt.

In beider Hinsicht die Höchstnoten verdienen sich **Lichtwellenleiter**, wobei Monomode-Leiter die Daten schneller übertragen und die Kosten rasanter in die Höhe katapultieren als die technisch einfacher herzustellenden - weil dickeren - Multimode-Leiter. Je dünner das Medium, desto geradliniger muss ein Lichtstrahl hindurch. Und die Gerade ist bekanntlich die kürzeste Verbindung zwischen zwei Punkten. Ein nicht unwesentlicher Kostenfaktor sind die notwendigen Umsetzer, die die elektrischen Signale in Lichtimpulse und umgekehrt wandeln. Wohl wegen der Kosten finden sich Lichtwellenleiter vorwiegend in so genannten **Backbones**, also Hochgeschwindigkeits-Verbindungen zwischen räumlich getrennten Teilen eines Netzwerks. Ein anderes Anwendungsfeld erschließt sich durch dessen Unempfindlichkeit gegenüber elektromagnetischer Einflüsse.

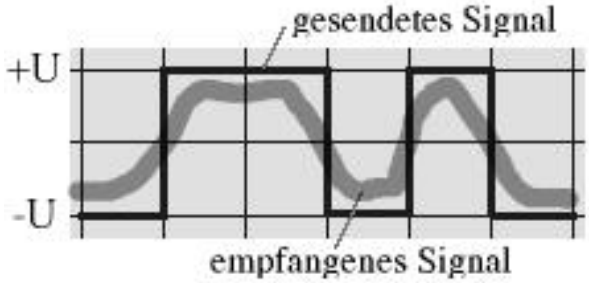


Bild 9: Störeinflüsse auf die Signalübertragung

Wegen fehlender Unterstützung von Hochgeschwindigkeitstechnologien nimmt die Verbreitung des Einsatzes von Koaxial-Kabeln weiterhin ab. Die »dickere« Ausführung (Thick Koax) ist gar noch seltener anzutreffen als das »schlankerer« Thin Koax. Thick Koax ermöglicht theoretisch den Anschluss von mehr Stationen (ca. 100) pro Kabelsegment als Thin Koax (32) und auch größere Segmentlängen (bis zu 500m gegenüber 185). Allerdings bedingt Thick Koax auch eine aufwändigere Abschirmung, um das Signal über die weiten Wege stabil zu halten und das spiegelt sich im Preis wider. Auch zeigte die Praxis, dass der Aufbau von Netzwerken, die aus vielen »kleinen« Segmenten bestehen, sowohl den möglichen Durchsatz als auch die

Ausfallsicherheit erhöht (vergleiche: Entkopplung durch Bridges). Bei beiden Typen von Koaxialkabeln ist die Übertragungsgeschwindigkeit auf maximal 16 MBit/s begrenzt.

Obwohl die Eigenschaften der Koaxial-Kabel prinzipiell höhere Übertragungsgeschwindigkeiten als Twisted-Pair-Kabel (»verdrillte Vierdrahtleitung«) zulassen, genügt letztere Verkabelungstechnik vollkommen zum Aufbau eines 100 MBit-Ethernets. Und auch hier erwies sich, dass die teureren geschirmten Twisted-Pair-Kabel den günstigeren ungeschirmten gegenüber kaum Vorteile bringen.

2.2.2 Aktive Komponenten

2.2.2.1 Netzwerkkarte

Die wichtigste Komponente, um einen Rechner in ein Netzwerk zu integrieren, ist die Netzwerkkarte (oft als Network Interface Card *NIC* bezeichnet). Für jeden Netzwerktyp existieren eigene Karten, die den Zugang zum Medium ermöglichen; die Karte muss also zum Netzwerk »passen«. Die Aufgaben der Netzwerkkarte bestehen im Senden und Empfangen von Daten.

2.2.2.2 Repeater

Repeater sind Netz-Komponenten, die auf Ebene 1 des OSI-Modells arbeiten.

In Netzen größerer Ausdehnung (wobei »größer« von Netzwerktyp, Verkabelung usw. abhängig ist) ist ggf. eine Signalverstärkung notwendig, um die Daten auch über weite Distanzen unverfälscht übertragen zu können. Sie können auch dazu verwandt werden, die Anpassung zwischen verschiedenen Übertragungsmedien vorzunehmen, wie z.B. von Twisted Pair auf Lichtwellenleiter.

2.2.2.3 Hub

Für Repeater mit mehr als zwei angeschlossenen Segmenten hat sich der Begriff des **Hub** (Englisch für (Rad)Nabe) etabliert. Ein Hub leitet das in einem Anschluss ankommende Signal verstärkt auf alle anderen Anschlüsse (oft 5, 8 oder 16) weiter. Ein Port des Hubs ist als so genannter Uplink-Port ausgelegt, der zum Anschluss weiterer Hubs dient. Auf diese Art und Weise lassen sich große Netze aufbauen.

Hubs gibt es in Ausführungen mit Bandbreiten zu 10 MBit, 100 MBit und 10/100 MBit. Nur bei letzterer Variante können in einem Netz Rechner mit 10 MBit-Netzwerkkarten und solche mit 100 MBit-Karten kombiniert eingesetzt werden, wobei allerdings die Bandbreite für alle Stationen auf 10 MBit sinkt.

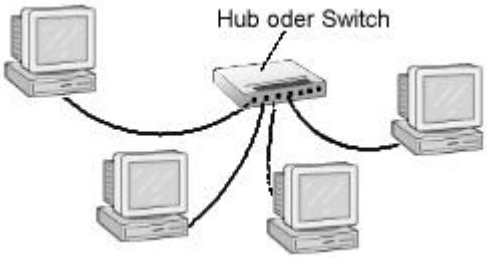


Bild 10: Hubs oder Switches verbinden Teilnetze

Ein Hub ist ein Gerät, das als Verbindung in einem Netzwerk der Sterntopologie eingesetzt wird.

Alle Daten (in Form von Spannungssignalen) werden an alle (per Patch-Kabel angeschlossenen) Geräte weiterverteilt. Ein Switch hingegen leitet die Daten nur in das Segment weiter, in dem sich der angesprochene Computer befindet.

2.2.2.4 Bridge

Eine Bridge koppelt Netzsegmente auf Ebene 2 des OSI-Modells. Quasi »intelligente Repeater« stellen **Bridges** (Brücken) dar, indem sie das Signal nicht nur verstärken, sondern für eine Lastentkopplung zwischen den beiden angeschlossenen Segmenten sorgen. Brigdes speichern hierzu die ankommenden Pakete, werten sie aus und leiten sie erst anschließend weiter (»Store&Forward«) und zwar nur, wenn der Empfänger im anderen Segment liegt. Intern halten sich Brücken hierzu Tabellen mit Hardwareadresse und zugehörigem Segment (nicht bei Token Ring); zum Standard gehört es unterdessen, dass die Brücken diese Tabelle dynamisch anpassen um auch auf Änderungen in der Netzkonfiguration reagieren können. Neben selbstlernenden Brücken lassen sich die »besseren« zusätzlich manuell konfigurieren (bspw. als einfacher Adressfilter).

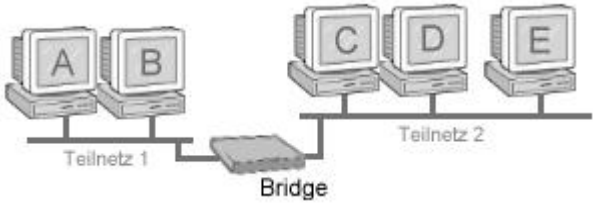


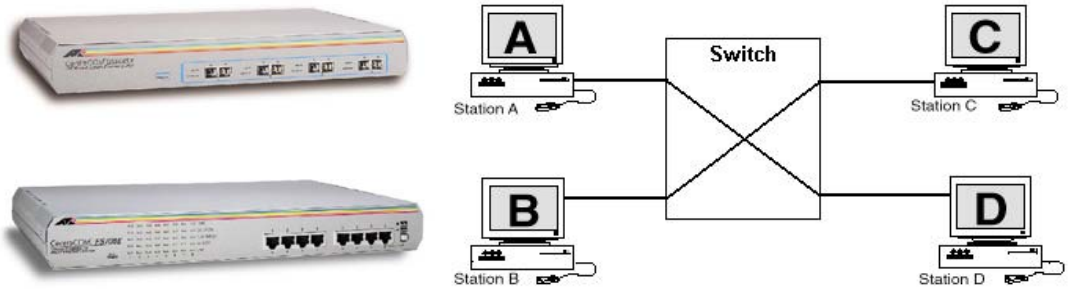
Bild 11: Brücke

Beispiel: Die Bridge aus der obigen Bild wird alle Pakete aus Teilnetz 1 nach Teilnetz 2 leiten, wenn ihr Ziel der Rechner C, D oder E ist. Ein Paket von A an B bzw. B an A hingegen wird von der Bridge ignoriert. Pakete werden vom Teilnetz 2 in Teilnetz 1 vermittelt, wenn und nur wenn der Empfänger Rechner A oder B ist.

Des Weiteren führen moderne Brücken zusätzlich eine Überprüfung der Pakete auf Korrektheit durch. Da notwendige Zwischenspeicherung und Prüfung Zeit beanspruchen, gehört der Durchsatz »Datenpakete pro Sekunde« zu den Kenndaten einer Bridge.

2.2.2.5 Switch

Bei **Switches** handelt es sich um Multiport-Brücken.



Äußerlich gleichen Switches somit den Hubs, jedoch bieten sie die Funktionalität einer Bridge.Die herausragende Eigenschaft von Switches ist die Bereitstellung der vollen Bandbreite unabhängig von der Zahl der angeschlossenen Rechner.

Indem der Hub ein einkommendes Signal an einem Port auf alle ausgehenden Ports legt, erscheinen alle angebundenen Stationen in einem einzigen großen Netz. Diese Stationen müssen sich die verfügbare Übertragungskapizität teilen.

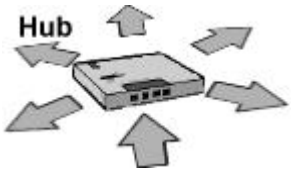


Bild: Datentransport im Hub

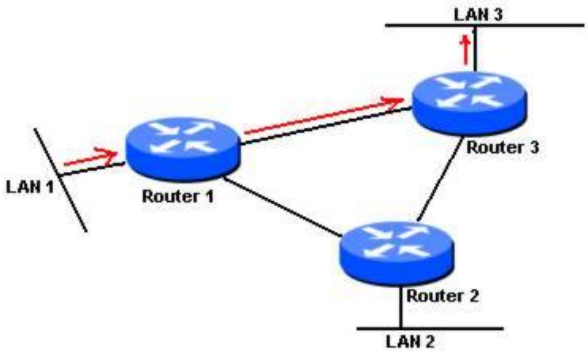
Bild: Datentransport im Switch (nach Lernphase)

Ein Switch hingegen leitet das Paket nur an den Port weiter, in dessen Segment sich auch der Empfänger befindet. Switches mit entsprechender Leistung können parallel mehrere »virtuelle« Verbindungen zwischen verschiedenen Ports gleichzeitig aufbauen, wobei für jede Verbindung die volle Übertragungsbandbreite zur Verfügung steht.

Wie auch Hubs lassen sich Switches über einen Uplink-Port kaskadieren.

2.2.2.6 Router

Während alle bisher genannten Komponenten typisch für ein lokales Netzwerk sind, dient ein **Router** vorrangig zur Verbindung mehrerer unabhängiger Netzwerke.



Ein Router stellt ein Gerät der Schicht 3 des ISO-OSI-7-Schichten Basisreferenzmodells dar, er kann also Netzwerke mit unterschiedlichen Topologien der Layer 1 und 2 verbinden. Alle über einen Router verbundenen Netzwerke müssen allerdings dieselben Adressierungsmechanismen verwenden. Um Pakete zwischen den angeschlossenen Teil-LANs weiterleiten zu können, interpretiert ein Router im Gegensatz zur Bridge die Adressangaben in ihnen. Er arbeitet also nicht mit den Adressen des MAC-Layers. In Netzwerken, die über Router gekoppelt sind, muß die Ausgangsstation also nicht die MAC-Adresse der Zielstation wissen, um sie ansprechen zu können - die Adresse aus der Protokoll-Ebene (etwa die IP-Adresse) genügt. Damit lassen sich, unabhängig von der Topologie der angeschlossenen Netze, Pakete gezielt von einem Netzsegment in ein anderes weiterleiten.

Ein Router entscheidet anhand der in einem IP-Paket enthaltenen Empfängeradresse und seiner (dynamisch aktualisierten) Routing-Tabelle, in welches der angeschlossenen Netzwerke die Daten weiter zu leiten sind. Dabei ist ein Router auch in der Lage, Netzwerke unterschiedlicher Topologie miteinander zu koppeln. Während vor einigen Jahren ausschließlich teure Spezialhardware als Router zum Einsatz gelangte, wird heute auch gern ein (Linux)Rechner mit dieser Aufgabe betraut. Bei geringem zu erwartenden Datenaufkommen genügt ein äterer Prozessor (Pentium I, K5) durchaus.

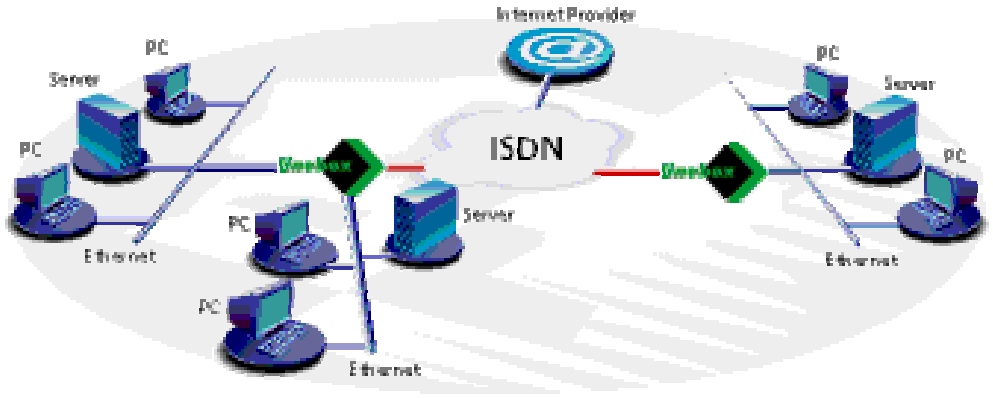


Bild: Kommunikationsserver mit integriertem Router, DHCP- und Mail-Server, für Arbeitsgruppen, Unternehmen etc.

LAN-Router gleichen ihre internen Tabellen mit denen benachbarter Router über das *Routing Information Protocol* (RIP) oder mittels des neueren *Open Shortest Path First* (OSPF) ab. WAN-Router verständigen sich über *Exterior Gateway Protocol* (EGP) oder das *Border Gateway Protocol* (EGP) .

2.2.2.7 Gateway

Verbindet ein Rechner gar Netzwerke unterschiedlicher Technologie (bspw. IP und IPX), so wird eine Protokollumsetzung (des IP-Protkollstacks) notwendig. Für diese über die Aufgaben eines normalen Routers hinausgehenden Aufgaben gelangen **Gateways** zum Einsatz.

Eine gewisse Begriffsverwirrung hat leider dazu geführt, daß in vielen Fällen Router mit Gateways gleichgesetzt werden. Dies nicht zuletzt deshalb, weil manche TCP/IP-Software für den PC eine Router-Adresse als Gateway-Adresse abfragt. Gateways sind aber im Gegensatz zu Routern auf dem Layer 7 des ISO-OSI-7-Schichten Basisreferenzmodells angesiedelt, sie ermöglichen also die Koppelung von LANs mit völlig unterschiedlicher Adressierung, nicht kompatiblen Protokollen und ähnlichem. Entsprechend hoch ist der Aufwand, der für ein Gateway betrieben werden muß.

Zwar lassen sich heutzutage Gateways problemlos über Software realisieren (beispielsweise IPX-IP-Gateways auf Novell-Servern), die Verzögerungen, die durch Protokollumsetzung und ähnliches auftreten, sind aber sehr groß. Dass Linux auch als Gateway betrieben werden kann, sollte kaum mehr verwundern.

OSI Ebene (Medium)	**Komponente** (transceiver)	**Funktion**
Anwendungs-Schicht	Gateway	Kopplungsansatz über alle Ebenen hinweg
Darstellungs-Schicht		
Kommunikationssteuerungs-Schicht		

Transport-Schicht		
Vermittlungs-Schicht	Router	Kopplungsansatz auf der Ebene 3
Sicherungs-Schicht	Bridge / Switch	Kopplungsansatz auf der Ebene 2 (MAC-Layer)
Bitübertragungs-Schicht	Repeater / Hub	Kopplungsansatz auf der Ebene 1

Bild: ISO-OSI Ebenen und Netzkopplung

3. Ethernet

Der Name *Ethernet* - ein Kunstgefüge aus *Äther* und *Netz* - wurde gewählt, um die prinzipielle Unterstützung jedes Computertyps durch die Technologie zu untermauern.

Der IEEE diente diese Spezifikation maßgeblich als Vorlage für einen Standard für LAN's, der 1982 als 802.3-Standard (10Base5) verabschiedet wurde. Die Weiterentwicklung *Ethernet V. 2.0* (1985) wurde schließlich in den ISO-8802.3-Standard überführt.

Weitere Standards legten die Richtlinien für 10Base2 und das kaum verbreitete 10BroadT (1985) fest. 1988 wurde Ethernet in Verbindung mit Twisted-Pair eingeführt, was den noch heute weit verbreiteten Standard 10BaseT (1991) formulierte. Schließlich hielt 1995 mit 100BaseT ein Standard Einzug, der wohl eher unter dem Begriff *Fast Ethernet* geläufig ist.

Während Produkte des Gigabit-Ethernets über Glasfaserkabel (802.3z, 1998) und über Kupferleitungen (802.3ab, 1999) trotz der langen Verfügbarkeit nur selten anzutreffen sind, steht der nächste Standard des 10 Gigabit-Ethernets bereits zur Debatte.

Und was hat es mit den Bezeichnungen 10Base5... auf sich? Die erste Zahl gibt die Bandbreite in MBit/s an, *Base* steht für Basisband- und *Broad* für Breitbandübertragung. "2" bzw. "5" geben in Zusammenhang mit Koaxialkabel die maximale Segmentlänge in 100m-Einheiten an; ein "T" kennzeichnet eine Twisted-Pair-Verkabelung. Seltener wird man ein "F" vorfinden, was auf ein Ethernet auf Basis von Lichtwellenleitern hinweist.

3.1 Zugang zum Medium - CSMA/CD

Jede Station in einem Ethernet arbeitet unabhängig von den anderen; es existiert keine zentrale Instanz, die die Kommunikation auf dem gemeinsamen Medium regelt (*Medium* soll hier allgemein für das Verbindungssystem stehen, bspw. Twisted-Pair-Kabel).

Signale werden bitweise übertragen, wobei jede am Medium angeschlossene Station jedes Signal empfängt. Wünscht eine Station zu senden, so »lauscht« sie zunächst auf dem Medium, ob zur Zeit eine Übertragung im Gange ist. Trifft dies zu, wartet die

Station eine zufällige Zeitspanne und lauscht dann erneut. Ist die Leitung frei ist, schickt die Station das Paket, verpackt in einen definierten Rahmen (*Ethernet Frame*) auf die Reise. Nach Abschluss einer jeden Übertragung müssen sich stets alle sendewilligen Stationen neu um den Zugang zum Medium bewerben. So ist sichergestellt, dass der Zugang zum Medium fair abläuft und keine Station »verhungert«, weil andere permanent Daten durch das Netz schicken.

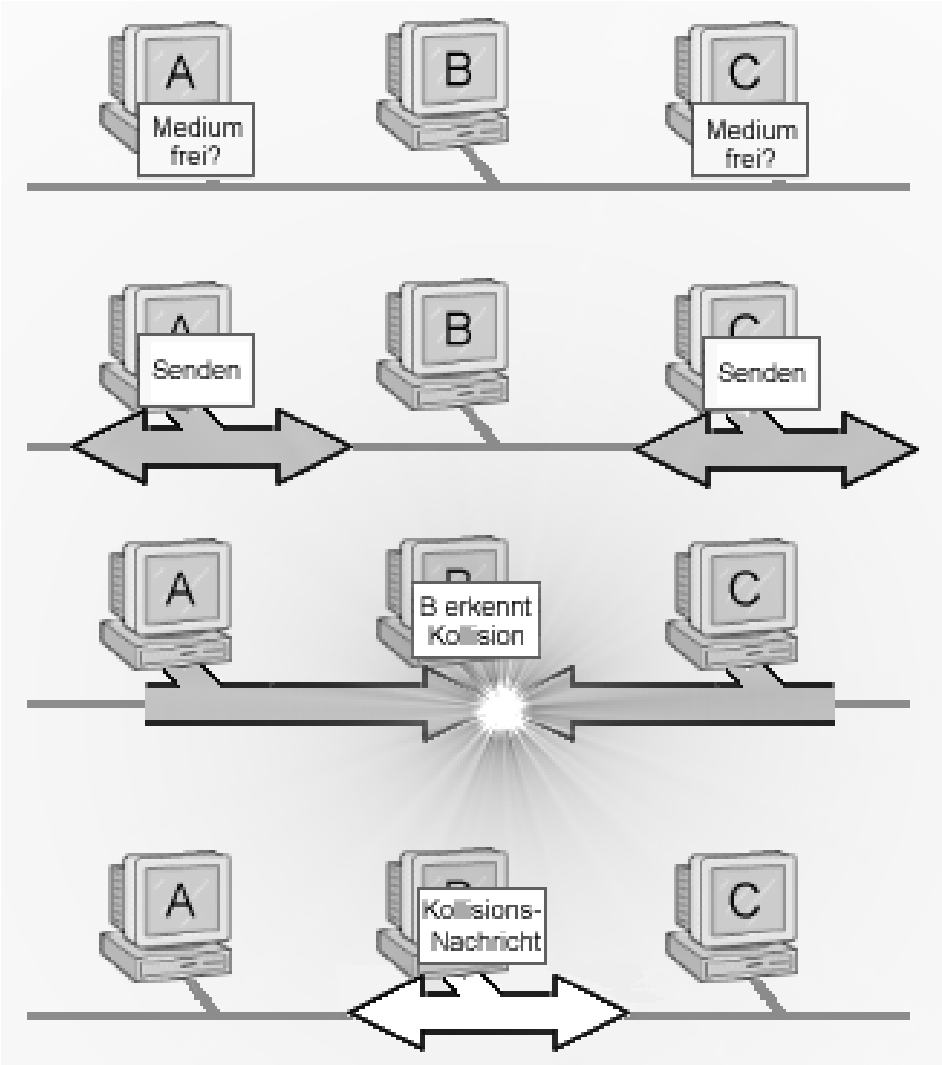


Bild 14: Kollisionen im Ethernet-Netzwerk (CSMA-Prinzip)

Nun kostet jede Übertragung bekanntlich Zeit. Und weil eine Station soeben ihr Paket versendet, da sie das Medium als frei erkannte, könnte zur gleichen Zeit eine andere Station genau zu demselben Schluss gelangt sein und schickt ihrerseits Daten auf die Strecke. Eine Kollision der Pakete und damit die Unbrauchbarkeit ihrer Inhalte sind die Folge. Um für solche Situationen gewappnet zu sein, definiert das **CSMA/CD-Protokoll** (*Carrier Sense Multiple Access with Collision Detection*) exakte Regeln für den Medienzugriff.

Nach CSMA/CD lauschen alle beteiligten Stationen permanent auf dem Medium. Das müssen sie ja auch, um für sie bestimmte Daten erkennen zu können.

Gedenkt eine Station nun zu senden, so wartet sie, bis das Medium frei ist (Carrier Sense). Nach einer Zeitspanne von 9,6 Mikrosekunden beginnt die Station mit der Übertragung. Diese Zeitspanne entspricht genau dem vorgeschriebenen Mindestabstand zwischen zwei Ethernetpaketen.

Mit Beginn des Sendevorgangs hört die Station weiterhin das Medium ab, um eine eventuelle Kollision mitzubekommen (Collision Detection). Trat keine Kollision auf, erkennt die Zielstation anhand der im Paket vermerkten Adresse die für sie bestimmten Daten, empfängt sie und die Übertragung ist somit beendet.

Da aber der Zugang zum Medium im Ethernet für alle Stationen gleichberechtigt ist (Multiple Access), sind Kollisionen nicht ausgeschlossen, weil zwei oder mehrere Stationen nahezu zeitgleich den Sendevorgang anstrengten und das Medium als frei erkannten. In dem Fall wird durch Überlagerung der Signale der Inhalte der Pakete zerstört. Die Station, die die Kollision zuerst registrierte, schickt deshalb ein spezielles »Überlagerungssignal« aus, worauf die sendenden Stationen mit sofortiger Einstellung ihrer Übertragung reagieren.

Die Stationen, deren Senden mit einer Kollision endete, wiederholen den Sendevorgang nach Ablauf einer (relativ) zufälligen Wartezeit. Kommt es wiederholt zu einer Kollision, so wird die »Auszeit« stetig erhöht.

CSMA/CD vermeidet also keine Kollisionen, minimiert jedoch durch die interne Verfahrensweise (flexible Wartezeiten) die Wahrscheinlichkeit ihres Auftretens.

3.2 Der Ethernet-Frame und Adressen

Daten, die über ein Ethernet übertragen werden, werden nochmals in einen Rahmen verpackt. Die Rahmen können geringfügig zwischen den verschiedenen Ethernet-Standards differieren; über eine Präampel, die Ziel- und Absenderadresse sowie über eine Prüfsumme verfügen sie jedoch alle, sodass die folgende Darstellung (Ethernet V2.0) durchaus repräsentativen Charakter besitzt:

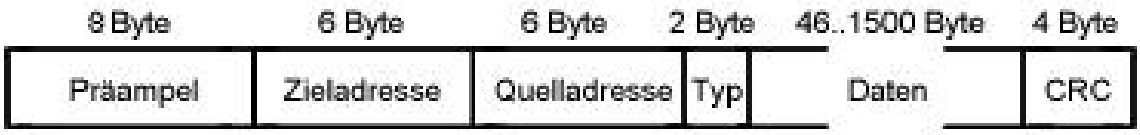


Bild 15: Ethernet-Frame

Die **Präampel** enthält die Bitfolge "010101...01". Sie ermöglicht den Stationen, den Beginn eines Pakets zu erkennen. Bei Ethernet nach IEEE 802.3 wird das 8. Byte »Start Frame Delimiter« genannt; wobei dessen Wert sich nicht vom 8.Byte des Ethernet-Frames nach V2.0 unterscheidet.

Die **Adressen** des Empfängers und Absenders umfassen jeweils 48 Bit. Die »oberen« 24 Bit dieser so genannten **MAC-Adresse** werden einem potentiellen Kartenhersteller vom IEEE zugewiesen; die »unteren« 24 Bit vergibt der Hersteller, wobei er jede

Adresse nur einmalig an eine Karte vergibt. Die gesamte Hardwareadresse ist fest in die Firmware der Karte »eingebrannt«. Bei manchen Karten kann sie umkonfiguriert werden, wobei beachtet werden muss, dass sie im lokalen Netz stets eindeutig ist.

Der **Typ** kennzeichnet das eingebettete Protokoll; zumeist wird hier 2048 als Kennzeichnung des IP-Protokolls stehen. Nach 802.3-Standard steht hier stattdessen die Länge des Pakets ohne Präampel.

Zwischen 46 und 1500 Bytes Nutzdaten können in den Rahmen eingebettet werden, sodass ein Ethernet-Paket eine Gesamtlänge von maximal 1526 Bytes besitzt.

Eine über das Gesamtpaket gebildete Prüfsumme (CRC) ermöglicht dem Empfänger, Übertragungsfehler zu erkennen.

3.2.1 Ethernet Frameaufbau

Ethernet basiert auf einer Entwicklung der Hersteller Digital, Intel und Xerox (DIX-Firmengruppe). Die 4 Frametypen werden von den Herstellern verschieden bezeichnet.

IEEE	Novell	Cisco
802.3	IEEE 802.2	LLC
V II	Ethernet II	ARPA
802.3 SNAP	SNAP	SNAP
802.3 Raw	802.3	Novell

Bild: Ethernet-Frametypen

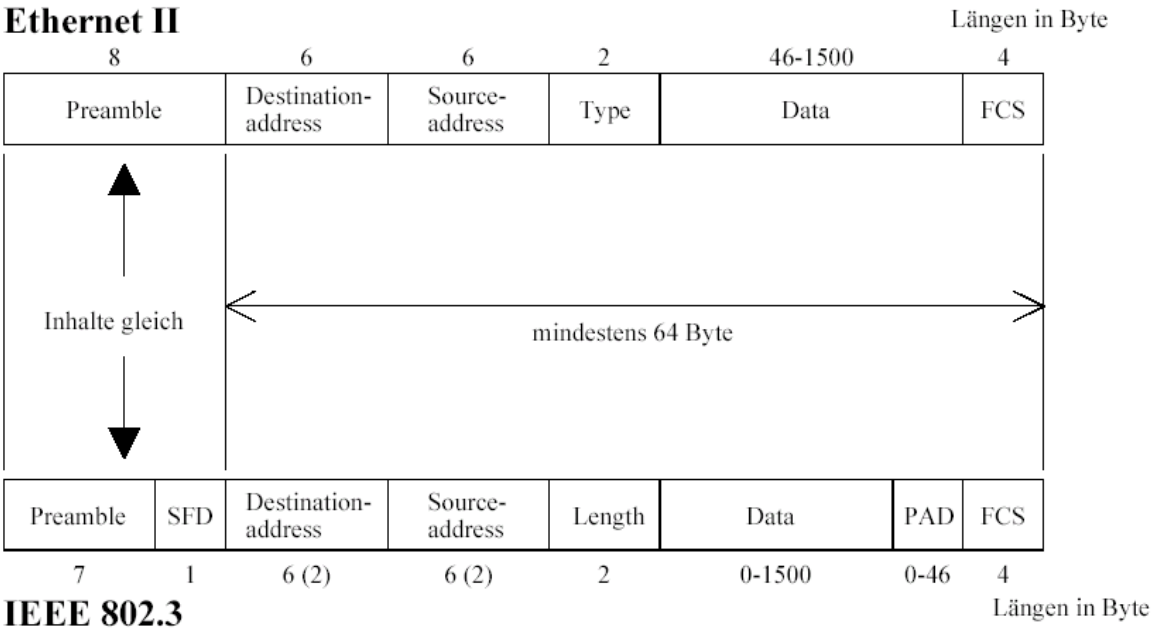


Bild: Vergleich der Ethernet Frames: Ethernet II und IEEE 802.3

IEEE 802.3 Frames haben statt des Typenfeldes ein 2 Byte langes Längenfeld. eingefügt. Es gibt die Anzahl der Bytes im Datenfeld einschließlich 802.2 LLC-Header an. Statt Typfeld mit der Protokoll-ID ist der Destination Service Access Point (DSAP) und der Source Service Access Point (SSAP) vorhanden. Das Control Field enthält den Typ des LLC-Frames.

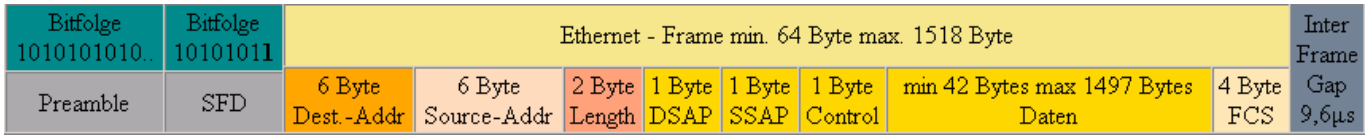


Bild: Ethernet Frame IEEE 802.3

3.2.2 Ethernet Frameaufbau (2)

Präambel

Die dient zur Realisierung der Kollisionserkennung und der Synchronisation der Stationen vor der Übertragung.

Sie besteht aus 7 Bytes. Es werden Bits in der Folge 10101010 ... gesendet.

SFD (start frame delimiter)

Der SFD ist ein Byte lang und weist die Bitfolge 10101011 auf. Er steht unmittelbar vor Beginn des eigentlichen Frames.

Die Präambel und der SFD zählen nicht zur Frame-Länge.

Header

Der Header besteht aus der Zieladresse, der Absenderadresse und der Länge des Datenpaketes.

Sie besteht aus 7 Bytes. Es werden Bits in der Folge 10101010 ... gesendet.

Zieladresse (Destination Address)

Adresse des Empfängers (6 Byte).

Absender-Adresse (Source Address)

Adresse des Absenders (6 Byte).

Die ersten beiden Bits der Ziel- und Absenderadresse haben eine bestimmte Kodierung:

Bit 1 = 0 Einzeladresse (Unicast) 1

Bit 1 = 1 **Gruppenadresse (für Multi- oder Broadcasts)**

Bit 2 = 0 **global verwaltete Adresse handelt (nach IEEE)**

Bit 2 = 1 lokal verwaltete Adresse handelt (für private Netze), falls alle Bits =1 liegt Broadcast vor.

Länge

Länge des Datenpakets (max. 1500 Datenbytes)

Daten

Enthält die eigentlichen Nutzdaten. Zusätzlich sind Steuerinformationen höherer Schichten enthalten (LLC).

FCS

Die FCS (Frame Check Sequence) besteht aus einer 32 Bit Prüfsequenz, welche nach dem CRC-32 Verfahren berechnet wird.

Der Abstand zwischen einzelnenn Frames (Rahmenabstand) beträgt mindestens 9,6 us Interframe-Gap).

Bei der Version Ethernet II entfällt das Längenfeld und wird vom Typenfeld ersetzt. Dies Auskunft über den Frame-Typ.

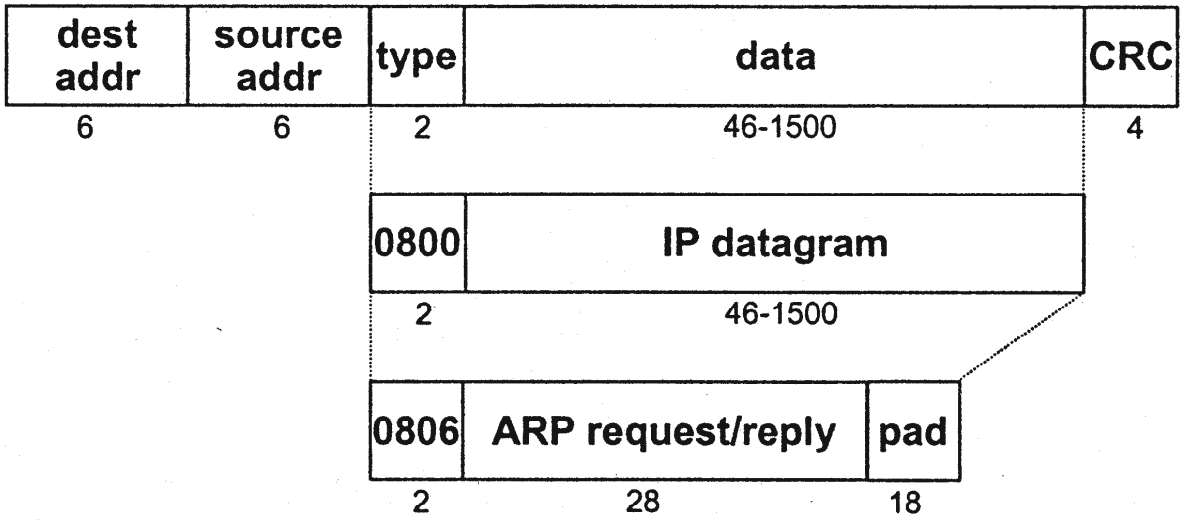


Bild: Aufbau von Ethernet Frames gemäß RFC 894

Ethertype	Protocol
0x600	Xerox XNS IDP
0x800	IP
0x806	ARP
0x8035	Reverse ARP
0x8137 / 0x8138	Novell
0x6001	DEC MOP Dump/Load Assistance
0x6002	DEC MOP Remote Console
0x6003	DEC DECnet Phase IV
0x6004	DEC LAT
0x6005	DEC DECnet Diagnostics

Bild: Weitere Protokolltypen

3.3 Wichtige Ethernet-Vertreter

3.3.1 10Base2

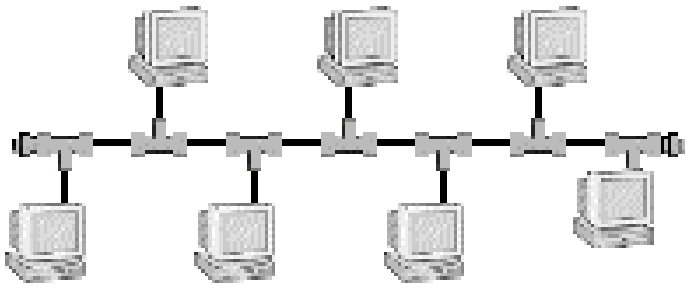


Bild 16: Busstruktur des 10Base2

Als Vertreter der klassischen Busstruktur des Ethernets hat sich einzig 10Base2 bis in heutige Zeit gehalten. Das Argument für den Einsatz der Technik - die Ersparnis der Kosten für eine zentrale Kopplerkomponente - hat sich jedoch mit sinkenden Hardwarepreisen verflüchtigt, was kurz über lang wohl auch für 10Base2 selbst zutreffen wird.

Als Verbindungsmedium gelangt ausschließlich Koaxial-Kabel zum Einsatz, an das mittels BNC-T-Steckern die Stationen angeschlossen werden. Die Enden des Kabel müssen mit einem Endwiderstand (»Terminator«) abgeschlossen werden. Maximal 32 Stationen lassen sich an einem Kabelsegment betreiben, wobei der Mindestabstand zweiter Anschlüsse 0.5m und der maximale Abstand 185m beträgt.

3.3.2 10BaseT

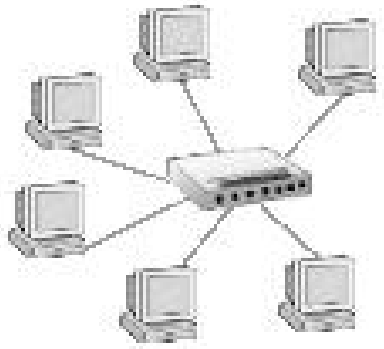


Bild 17: Sternstruktur des 10BaseT

Die physische Struktur heutiger Ethernet-Installationen gleicht zumeist einem Stern. 10BaseT war die erste Realisierung eines Ethernets, die zum Anschluss der Stationen auf eine zentrale Komponente (Hub oder Switch) setzte. Zur Verbindung dient zumeist Twisted-Pair-Kabel, wobei die Auslegung des zentralen Koppelelements die maximale Anzahl zu verbindender Stationen bestimmt. Typische Hubs verfügen über 5, 8 oder 16 Anschlüsse; aber auch Ausführungen mit 150 und mehr Anschlüssen sind erhältlich. Die maximale Kabellänge zwischen Station und Koppelkomponente darf 100m nicht übersteigen.

Zum Aufbau größerer Netzwerke lassen sich mehrere Koppelelemente miteinander verbinden.

3.3.3 Fast- und Gigabit Ethernet

Beide Typen unterscheiden sich vom 10BaseT hinsichtlich des Übertragungsmediums und der Schnittstellenadapter; d.h. auch ihre Grundstruktur formt einen Stern.

Um die Übertragungsraten von 100 MBit zu erzielen, gelangt bei 100BaseT ein aufwändiger verarbeitetes Twisted-Pair-Kabel (»Typ 5«; ein Typ legt die elektrischen Eigenschaften fest) zum Einsatz, als es für 10Base2 (»Typ 3«) erforderlich ist; auch die Netzwerkkarte muss für die hohen Datenraten gewappnet sein. Aktuelle Karten, die 100 MBit unterstützen, beherrschen i.d.R. ebenso den 10 MBit-Datentransfer; so dass sie ggf. die Geschwindigkeit anpassen, falls ihr »Gegenüber« nur die gemächlichere Korrespondenz beherrscht.

Datenraten von 1000 MBit/Sekunde im Gigabit-Ethernet werden entweder über Glasfaserleitungen oder über geschirmte Twisted-Pair-Kabel erzielt. Vor allem wegen der extrem teuren Netzhardware (Hubs, Repeater) sind Gigabit-Lösungen heute fast ausschließlich im Backbone-Bereich zur Kopplung separater Netzwerke zu finden.

3.3.4 Token Ring

Neben Ethernet hat sich einzig IBM's Token Ring als LAN-Technologie durchsetzen können, wenn auch bei weitem nicht mit dem durchschlagenden Erfolg, der dem Ethernet beschieden war. Dabei entstand das Konzept des »kreisenden« Tokens bereits Anfand der 70er Jahre (Willemjin) bei IBM. Vielleicht ließ sich IBM mit der Vorstellung eines ersten Prototypen (1983) einfach zu viel Zeit; als IEEE802.5 endlich als Standard anerkannt wurde (1985), dominierte Ethernet schon längst den Markt.

4. Die Sicherungsschicht (Data Link Layer)

Funktionen der Sicherungsschicht

- Unterteilung des Bitstroms in Datenpakete
- Erkennung und evtl.Behebung von physikalischen Übertragungsfehlern
- Transformation der physikalischen Übertragungseinrichtung in eine *virtuelle Leitung* zwischen unmittelbaren Kommunikationspartnern
- Unterteilung:
  - Schicht 2a: Media Access Control Layer (MAC-Layer)
  - Schicht 2b: Logical Link Control Layer (LLC-Layer)
- Geräte: Netzwerkkarte, Bridge, Switch

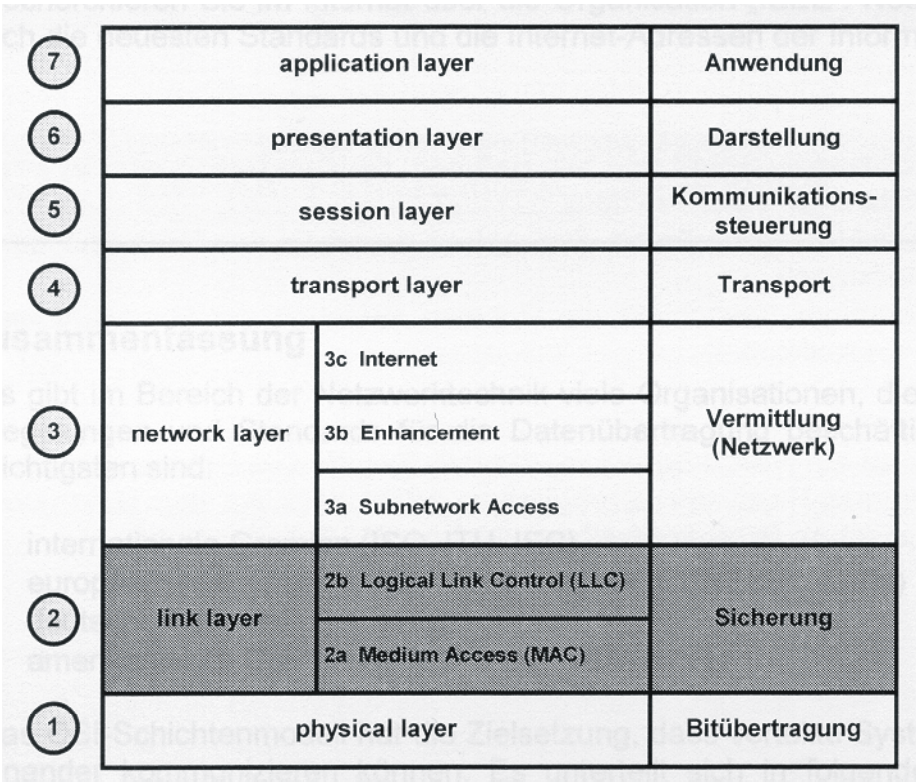


Bild: Strukturierung Data Link Layer (LLC, MAC)

MAC-Adressen (Media Access Control)

Eigenschaften:

Jede Netzwerkkarte (NIC) hat **eine 48-Bit-Hardware-Kennung (6 Bytes)**, die sogenannte MAC-Adresse (Media Access Control).

Identifikation auf Ethernet-Ebene (Layer 2)

Sie ist fest auf dem Adapter eingebrannt (in einem PROM oder EPROM) und **für jede Karte global eindeutig**. Vergeben werden diese Nummern prinzipiell vom IEEE (Institute of Electrical and Electronical Engineers).

Das IEEE weist jedem Hersteller einen sogenannten OUI (Organizationally Unique Identifier) zu, der die ersten 24 Bit der Kartenadresse darstellt. Die restlichen Bits der Adresse darf der Hersteller für jede Karte selbst vergeben, wobei er darauf zu achten hat, dass jede Karte auch wirklich eine einmalige Adresse erhält.

Im Prinzip unveränderlich, aber in der Praxis fälschbar

MAC-Adressen Datenbank (sog. OUI-Listing) http://standards.ieee.org/regauth/oui/index.shtml

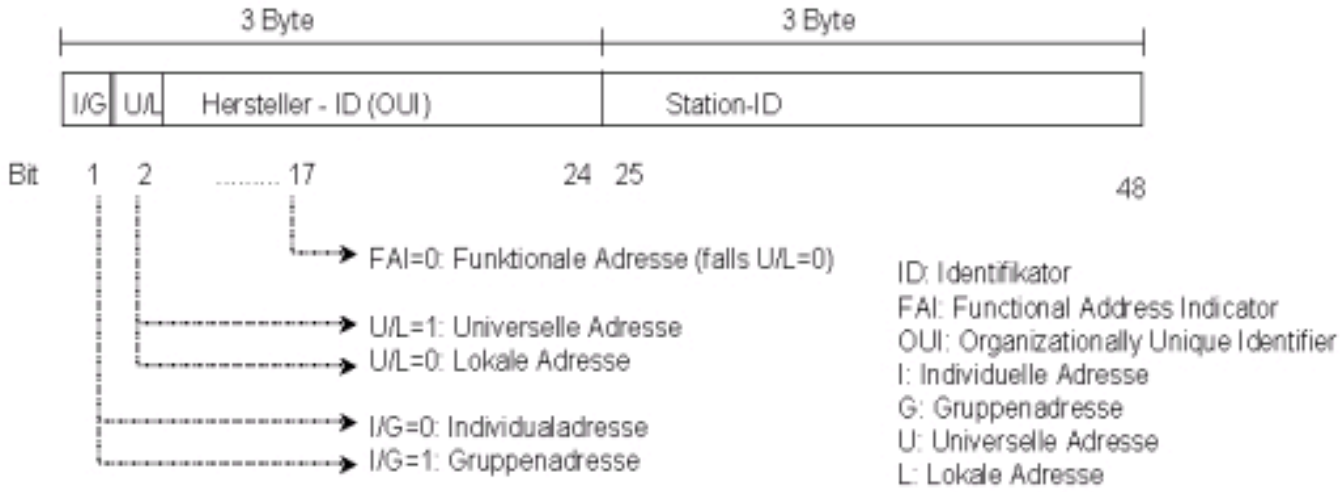


Bild: Struktur der MAC-Adresse

Die ersten beiden Bits der Ziel- und Absenderadresse haben eine bestimmte Kodierung:

Bit 1 = 0 **Einzeladresse (Unicast)**

Bit 1 = 1 **Gruppenadresse (für Multi- oder Broadcasts)**

Bit 2 = 0 **global verwaltete Adresse (nach IEEE)**

Bit 2 = 1 lokal verwaltete Adresse (für private Netze), falls alle Bits =1 liegt Broadcast vor.

ETHERNET VENDOR ADDRESS COMPONENTS
or ORGANIZATIONALLY UNIQUE IDENTIFIERS (OUI)

Unter Linux: $ ***ifconfig***

eth0 Link encap:Ethernet HWaddr 00:50:BF:1C:DE:F6

unter Windows 2000/XP: ***ipconfig /all***

```
Verbindungsspezifisches DNS-Suffix: my.router
Beschreibung. . . . . : SiS 900-Based PCI Fast Ethernet

Physikalische Adresse . . . . . : 00-05-EB-10-0E-9C
DHCP-aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
IP-Adresse. . . . . : 192.168.0.100
Subnetzmaske. . . . . : 255.255.255.0
Standardgateway . . . . . : 192.168.0.1
DHCP-Server . . . . . : 192.168.0.1
DNS-Server. . . . . : 192.168.0.1
                                    192.168.0.1
Lease erhalten. . . . . : Sonntag, 29. Juni 2003 06:29:52
Lease läuft ab. . . . . : Mittwoch, 2. Juli 2003 06:29:52
```

Beispiel:

00-A0-24-A8-70-19

Herstellerkennung (OUI) lautet 00-A0-24

Netzwerkkarten-Identifier A8-70-19

Ethernet hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits which specify the interface serial number for that interface vendor.

These high-order 3 octets (6 hex digits) are also known as the Organizationally Unique Identifier or OUI.

Ethernet addresses might be written unhyphenated (e.g., 123456789ABC), or with one hyphen (e.g., 123456-789ABC), but should be written hyphenated by octets (e.g., 12-34-56-78-9A-BC).

Another list of Ethernet vendor address components is maitained by Michael A. Patton and is accessible at:

www.cavebear.com/CaveBear/Ethernet/vendor.html

00-00-0C Cisco

00-00-0F NeXT
00-00-10 Sytek
00-00-1D Cabletron
00-AA-00 Intel
02-60-8C 3Com IBM PC; Imagen; Valid; Cisco
02-CF-1F CMC Masscomp; Silicon Graphics; Prime EXL
08-00-2B DEC

5. IP-Adressen

Um am Datenaustausch in TCP/IP-basierten Netzwerken teilzunehmen, benötigt der Rechner eine in seinem Netzwerk eindeutige IP-Adresse. Für jeden Teilnehmer im Internet folgt damit, dass seine Adresse weltweit eindeutig sein muss. Dass dies bei dem knappen 32-Bit Adressraum schon heute nicht mehr praktikabel ist, führte zu Techniken der Maskierung, wobei ein Rechner, der über eine offizielle IP-Adresse verfügt, stellvertretend für andere Rechner aus seinem Verwaltungsbereich im Internet auftritt. Aber derartige Belange sollen uns erst an anderer Stelle interessieren.

5.1 Vermittlungsschicht: Das Internet Protocol (IP)

Die heute gebräuchlichen Adressen des Internet-Protokolls sind 32 Bit lang, die häufigste Notation erfolgt byteweise als Dezimalzahl, bspw. 127.211.7.9.

Der Mathematiker errechnet rasch, dass mit 32 Bit 2^{32} = 4.294.967.292 Rechner adressierbar wären. Der Praktiker interveniert, dass sich nicht alle Adressen nutzen lassen, da etliche Adressen und Adressbereiche für bestimmte Funktionen reserviert sind. Auch existieren genügend Lücken im Adressraum, da IP's im Block an lokale Netzwerke vergeben werden, diese aber nur selten ihr Kontingent voll ausschöpfen.

Zukünftig wird Ipv4 von IPv6 abgelöst werden, welches mit 128 Bit Adressen arbeitet.

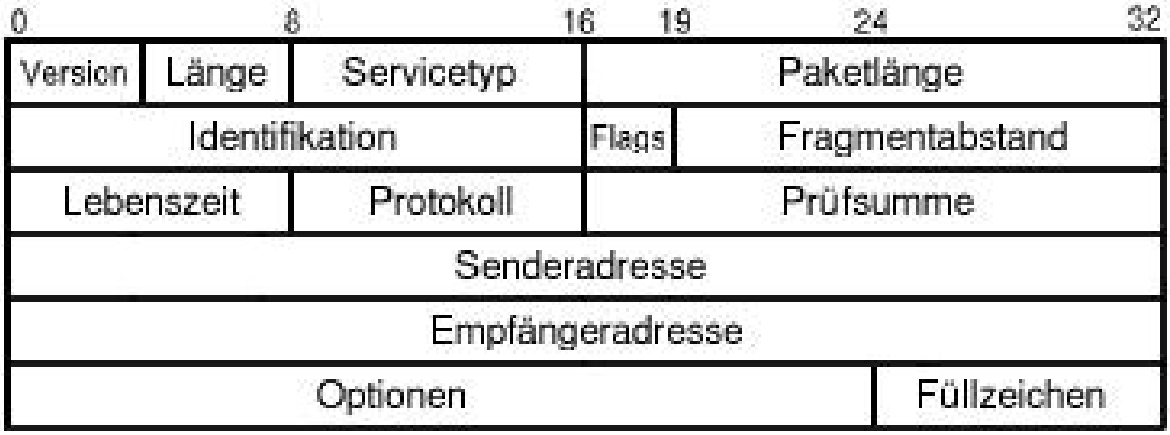


Bild: Aufbau des IP-Protokollrahmens

5.2 Eigenschaften des IPv4

- IP stellt ein **verbindungsloses** Protokoll dar, d. h. es arbeitet, ohne dass eine Verbindung zum Partner zuvor aufgebaut wurde.
- Die maximale **Paketgröße beträgt 65535 Bytes**. Ein Paket durchläuft auf seinem Weg zum Empfänger meist verschiedenste Subnetze, die ihrerseits nur eine kleinere Paketgröße unterstützen. Das IP beinhaltet deswegen einen Mechanismus zur **Fragmentierung** von Paketen, d.h. dass ein für ein zu durchlaufendes Subnetz zu großes Datenpaket zerlegt wird und nun mehrere IP-Pakete ihren Weg zum Empfänger suchen. Der Zusammenbau der Paketteile erfolgt erst beim endgültigen Empfänger, da die Teilpakete durchaus auf unterschiedlichen Routen ihr Ziel finden.
- Eine **Prüfsumme** stellt die Unversehrtheit des IP-Kopfes sicher, nicht jedoch die der enthaltenen Daten. Dessen Überwachung obliegt dem Protokoll der nächsthöheren Schicht; ein Code im IP-Kopf (**Protokoll**-Feld) verweist auf den Typ des Protokolls (z. B. eine 6 für TCP und eine 17 für das UDP-Protokoll).
- Die letzte erwähnte Eigenschaft, die die **Lebensdauer** eines IP-Pakets begrenzt, garantiert, dass ein nicht vermittelbares Paket nicht endlos im Netz kursiert, sondern nach Ablauf seiner Lebenszeit verworfen wird. Früher wurde hier tatsächlich mit einer Zeiteinheit gearbeitet, jedoch wich diese bald der maximalen Anzahl Stationen (»Hops«), die ein Paket maximal durchlaufen darf. Jeder Rechner bzw. Router, der das Paket weiterleitet, verringert diesen Wert um 1. Erreicht er in einem Netzkoppler den Wert 0 und handelt es sich nicht um den Zielrechner, so sendet dieser Rechner ein ICMP-Protokoll an den Absender und verwirft das eigentliche Paket.

Wichtige Felder des IP-Protokollrahmens (IPv4)

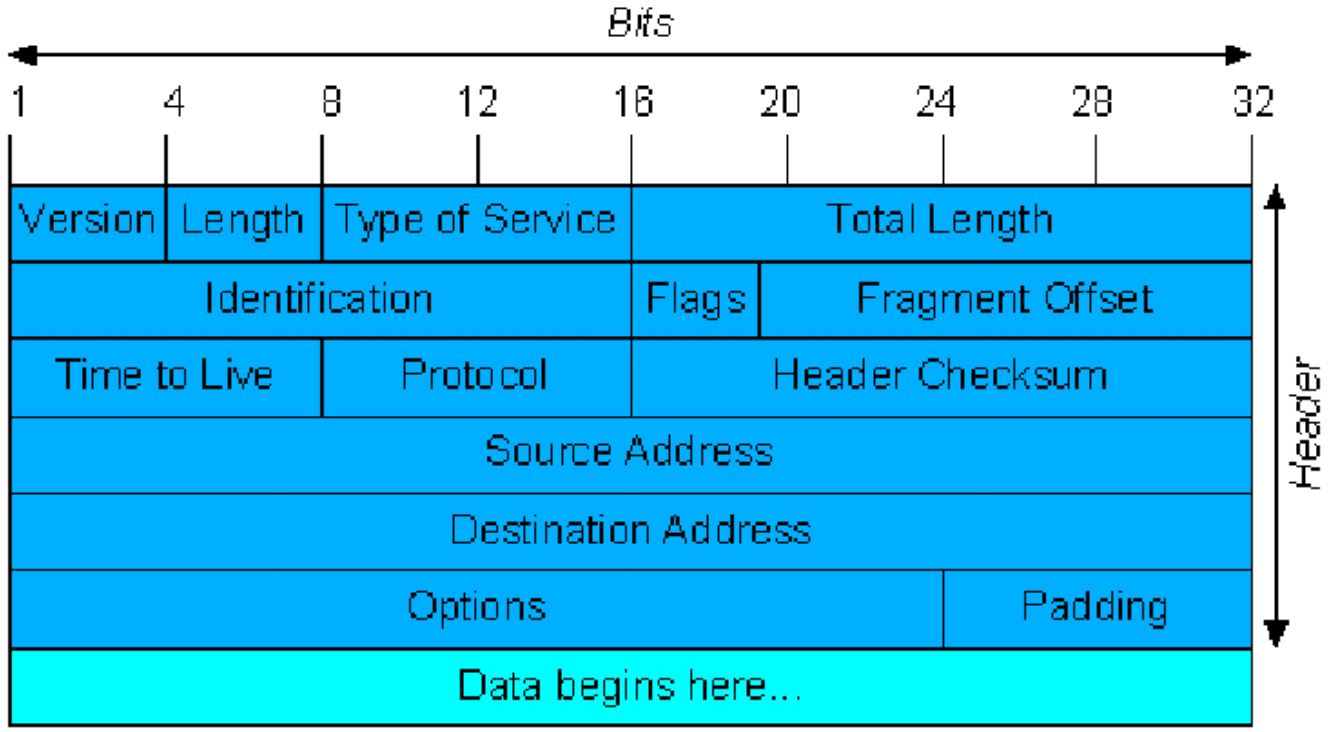


Bild: Aufbau des IP-Protokollrahmens

Versionsnummer (Version)

4 Bit	Version des Protokolls, somit 4 bei IPv4 und 6 bei Ipv6

Länge IHL (Internet Header Lenght)

4 Bit	Größe des IP-Kopfes in 32-Bit-Einheiten (notwendig wegen variabler Länge des Options-Feldes) Der kleinste Wert ist 5 (= 20 Byte; Header ohne Optionen). Der größte Wert ist 15 (= 60 Bytes); hierdurch ist die Angabe von Optionen variabel.

Servicetyp (Typ of Service ToS)

8 Bit	Definiert Dienste, wie Durchsatzsteuerung, Zuverlässigkeit und Verzögerung. Es dient dazu, ein Paket mit unterschiedlicher Priorität oder erhöhter Zuverlässigkeit zu vermitteln. Priorität 0 (normal) bis 7 (hohe Priorität, z.B. Steuerungspaket).

Paketlänge (Length)

16 Bit	Gesamtlänge des Datagramms inkl. Header und Datenteil (mind. 576 Bytes, max. 65 535 Bytes). Länge inklusive des IP-Headers in 32-Bit-Einheiten

Identifikation (Identification)

16 Bit	Kennwert (meist durch höhere Schicht festgelegt) zur Zuordnung von Fragmenten zu einem Datagramm. Vom Absender vergebene eindeutige Nummer, anhand derer einzelne Fragmente im Zielrechner in der richtigen Reihenfolge zusammen gesetzt werden können

Flags (Flags)

3 Bit	Bit 1: unbenutzt, ist immer 0 Bit 2: 1 = DF (Don't Fragment), d. h. Paket darf nicht fragmentiert werden. Ist ein solches Paket zu groß für ein Teilnetzwerk, muss es verworfen werden. Bit 3: 1= MF (More Fragment), d.h. dem IP-Paket folgen weitere Teilpakete

Fragmentabstand (Fragment Offsets)

13 Bit	Relative Lage des Paketes (Fragmentdaten) relativ zum Anfang des Datenblocks im Originaldatagramm), wenn dieses Teil eines zuvor größeren Paketes war (Fragmentierung). Mit Hilfe dieser Angabe kann der Zielhost das Originalpaket wieder aus den Fragmenten zusammen setzen.

Lebenszeit (Time To Live TTL)

8 Bit	Zähler, mit dem die Lebensdauer von IP-Paketen begrenzt wird (max 255 Hops) Der Zähler wird von jedem Netzknoten, der durchlaufen wird um mindestens 1 verringert. Bei TTL-Wert = 0 wird das Paket verworfen. Damit werden endlos zirkulierende Pakete im Netzwerk verhindert):

Protokoll (Protocol)

8 Bit	Enthält die Nummer des Transportprotokolls, an das das Paket weitergeleitet werden muss. Die Numerierung von Protokollen ist im gesamten Internet einheitlich und im RFC 1700 definiert. Z.B. 1 für ICMP, 6 für TCP, 8 für EGP, 9 für IGRP, 10 für UDP etc.

Prüfsumme (IP Header Checksum)

16 Bit	Prüfsumme zur Erkennung von Fehlern im IP-Header. (nicht des Datenfeldes, dieses müssen übergeordnete Protokolle absichern.

Sendeadresse (Source IP address)

32 Bit	Internetadresse des Quellrechners (pro NIC eine Adresse);

Empfängeradresse (Destination IP address)

32 Bit	Internetadresse des Zielrechners (pro NIC eine Adresse);

Optionen (Options)

Variabel	Möglichkeit für weitere Informationen

Padding (Füllzeichen)

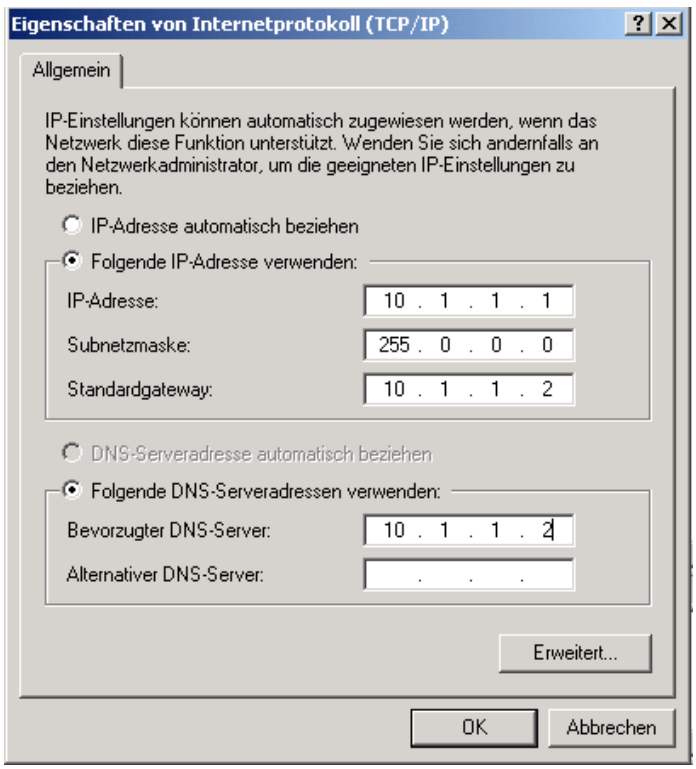
Variabel	Füllzeichen, die sicherstellen, dass der Header stets im 32-Bit-Format endet.

5.3 Adressierungsebenen bei der Datenkommunikation

- **Link-Level-Adressierung**: Adresse des unmittelbaren Kommunikationspartners (MAC-Adresse: z.B. Ethernetadresse einer Netzwerkkarte)
- **Endsystemadressierung**: Adresse des letztendlichen Zielsystems (z.B. Internet-Adresse)
- **Transportprotokolladresse** (z.B. TCP oder UDP)
- **Port-Nummer** zur Identifizierung einer Anwendung (Anwendungsprozeß)

Funktionen der Vermittlungsschicht

- Routing, Wegfindung
  - Kopplung mehrerer Netze zu einem logischen Gesamtnetzwerk
  - Austausch von Routinginformation
- Vermittlung zwischen verschiedenen Technologien
  - Umsetzung des Datenformates zwischen verschiedenen Technologien
  - Fragmentierung, Reassemblierung
- Geräte: Router



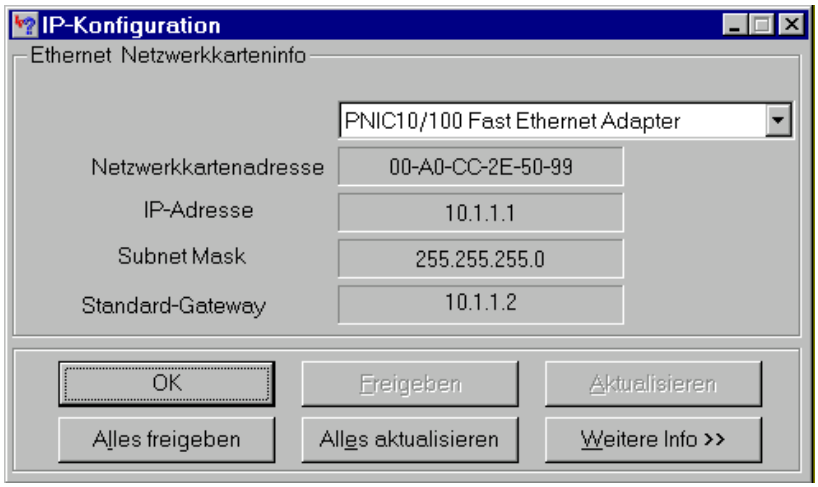


Bild: IP-Konfiguration unter Windows 98

5.4 IP-Adressen nach IPv4

Mit 32 Bit Adressen ließen sich theoretisch 2^{32} (4294967296) Rechner ansprechen. Praktisch ist es allerdings kaum zu realisieren, dass ein Rechner wahllos aus dem Pool der Adressen eine freie zugewiesen bekommt (zur Paketvermittlung müssten dann zumindest einige Rechner im Netz mit definiertem Standort die Adressen aller Teilnehmer verwalten). Ähnlich zu einer Telefonnummer, bei der das Ziel durch Länderkode, Ortswahl und Teilnehmernummer lokalisiert wird, werden IP-Adressen in Netzwerk- und Rechnernummer unterteilt. Die (klassische) Interpretation der 32 Bit ist abhängig vom ersten auf 0 gesetzten Bit (von links):

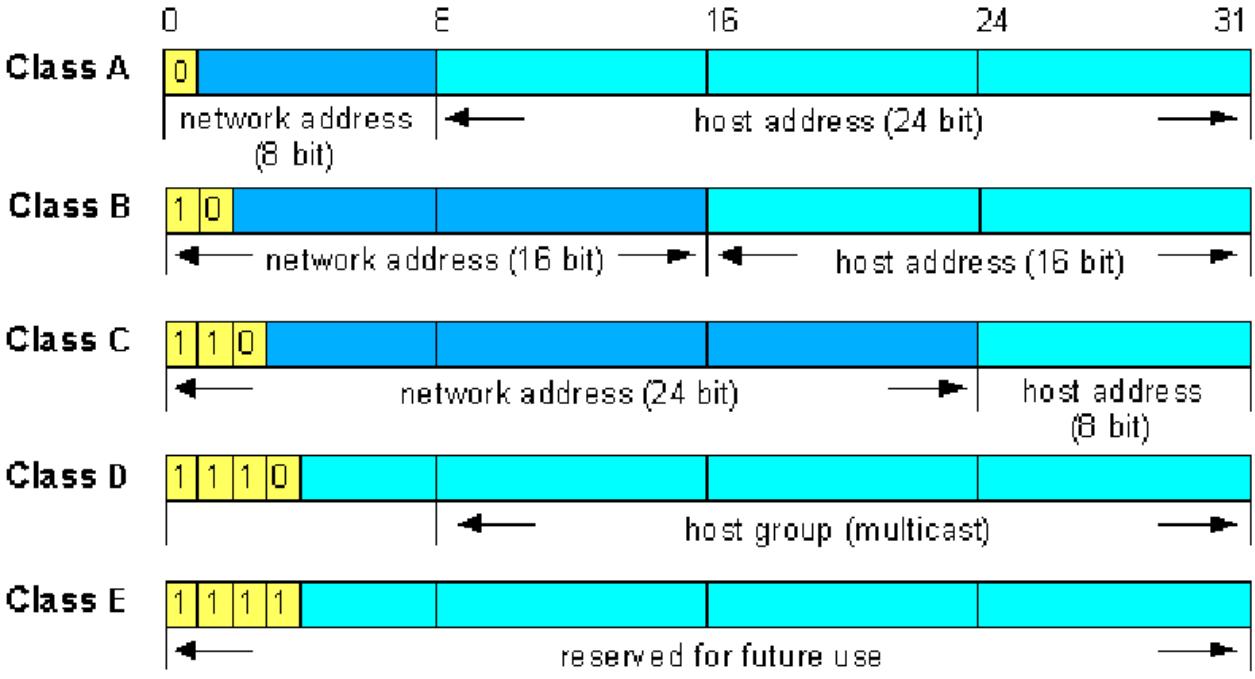


Bild 18: Adressklassen nach IPv4

Klasse A

Klasse A:

A: 001.x.x.x - 126.x.x.x

Standard-Subnetzmaske: 255.0.0.0

Host IP-Bereich (host address range) A: 1.0.0.0 - 126.255.255.255

0. und 127. Netz sind reserviert.

7 Bit Netzadresse, 24 Bit Hostadresse
126 Klasse A-Netze mit jeweils maximal 16.777.214 Hosts

Eine Adresse der Klasse A liegt vor, wenn das erste Bit (Bit 0) der IP-Adresse auf 0 gesetzt ist. Bit 1 bis 7 werden als Netzwerkadresse behandelt, womit 2^7 (128) Netzwerke mit je 2^{24} (16777216) Hosts adressierbar sind.

Klasse B

Klasse B:

B: 128.1.x.x - 191.254.x.x

Standard-Subnetzmaske: 255.255.0.0

Host IP-Bereich B: 128.1.0.0 - 191.254.255.255
14 Bit Netzadresse, 16 Bit Hostadresse
16384 Klasse B-Netze mit jeweils maximal 65534 Hosts.

Eine IP-Adresse der Klasse B ist durch die ersten beiden Bits 10 gekennzeichnet. Die folgenden 14 Bits bilden die Netzwerkadresse (16348). Je Netzwerk stehen 2^{16} (65536) Adressen für die Hosts zur Verfügung.

Klasse C

Klasse C:

C: 192.0.1.x - 223.255.254.x

Standard-Subnetzmaske: 255.255.255.0Host IP-Bereich C: 192.0.1.0 - 223.255.254.255
2.097.150 Klasse C-Netz mit jeweils maximal 254 Hosts.

Startet die IP-Adresse mit den Bits 110, wird sie als Klasse C interpretiert, d.h. 21 Bits (2^{21}=2097152) bilden die Netzwerk- und 8 Bit (256) die Hostadressen.

Klasse D

Klasse D:

Host IP-Bereich C: 224.0.1.x - 239.255.255.254

Klasse D Adressen, sogenannte **Multicast-Adressen**, werden dazu verwendet ein Datagramm an mehrere Hostadressen gleichzeitig zu versenden.

Adressen der Klasse D beginnen mit der Bitfolge 1110 und sind als **Multicastadressen** bekannt. Die gesamten 28 »Restbits« bilden eine Multicastadresse; hinter der sich letztlich eine Gruppe von Rechnern verbirgt, wobei die zugehörigen Rechner nicht zu einem einzigen lokalen Netzwerk gehören. Zur Vermittlung solcher Adressen sind spezielle Multicast-Router erforderlich. Wichtigste Anwendung sind Videokonferenzen.

Klasse E

> Adressen, die mit vier 1-Bits starten, ist keine konkrete Bedeutung zugeordnet. Sie dienen in erster Linie zu Forschungszwecken, weshalb auch von einer »experimental class« gesprochen wird.

Die 32 Bit einer IP-Adresse werden als Quadrupel zu je 8 Bits angegeben, wobei die dezimale Schreibweise bevorzugt angewendet wird. Bezugnehmend auf die ersten 8 Bit bedeutet dies für eine Adresse:

- Beginnt sie mit 1-128, so handelt es sich um eine Klasse-A-Adresse
- Beginnt sie mit 129-191, so handelt es sich um eine Klasse-B-Adresse
- Beginnt sie mit 192-223, so handelt es sich um eine Klasse-C-Adresse
- Beginnt sie mit 224-239, so handelt es sich um eine Multicast-Adresse

Die Klassenstruktur der IP-Adressen ist historisch bedingt, schien doch zu jener Zeit der Adressraum von 32 Bit als ungemein groß. Um die Suche nach dem Empfänger eines Pakets in vertretbarem (Zeit)Rahmen zu realisieren, bewertete ein Router eine Adresse nur anhand des Netzwerkteils; anstatt sich bspw. die 65535 Adressen eines beliebigen Klasse-B-Netzwerks zu merken, genügt dem Router somit ein einziger Eintrag für das Netz selbst, um den folgenden Empfänger eines Datenpakets auf dem Weg zu dessen Ziel zu identifizieren. Bei dem damaligen Stand der Rechentechnik war dies eine signifikante Erleichterung.

Aus heutiger Sicht erweisen sich die 32 Bit der IP-Adresse als viel zu klein (und Abhilfe ist mit der 128 Bit-Adresse aus IPv6 bereits geschaffen worden.

5.5 Spezielle Adressen

Zunächst einmal stehen die Adressen mit erstem Byte größer als 223 (Multicast und Experimental) nicht für die eigentliche IP-Adressierung zur Verfügung.

Private IP-Adressen

	von Adresse	bis Adresse	Anzahl der Netze	Standardsubnetzmaske
Klasse A	10.0.0.0	10.255.255.255	1	255.0.0.0
Klasse B	172.16.0.0	172.31.255.255	16	255.255.0.0
Klasse C	192.168.0.0	192.168.255.255	256	255.255.255.0

Bild: Private IP-Adressen

Aus jedem der Klassen A, B und C ist ein Adressbereich als so genannter **privater Bereich** ausgewiesen. Solche Adressen werden vom keinem Router im Internet vermittelt, womit sie sich zum Aufbau lokaler Netzwerke eignen (theoretisch kann jede

Adresse hierfür heran gezogen werden, jedoch nur, wenn das lokale Netz über keine direkte Verbindung zum Internet verfügt).

Standardroute-Adresse (default route, Standard-Gateway)

Die Adresse 0.0.0.0 wird als **Standardroute** bezeichnet und wird für die Weiterleitung von Adressen mit unbekannter Route verwendet.

Die Adresse 0.0.0.0 hat eine Bedeutung für das Routing. Jedes Datagramm, das an eine Adresse geschickt wird, die nicht im lokalen Netz liegt, wird an die *default route* geschickt. Diese voreingestellte Route weist dann zum nächsten Gateway, der schon wissen wird, wohin er das Paket senden soll. Falls er keine Route kennt, die zum entsprechenden Ziel führt, so hat auch er eine default route, an die er das Paket dann schickt.

Loopback-Adressen (loopback interface)

Das **Loopback**-Netzwerk umfasst die Adressen 127.0.0.0 - 127.255.255.255, wobei der gültige nLoopback-Adressrange von 127.0.0.1 bis 127.255.255.254 reicht und 127.0.0.0 die Loopback-Netzadresse darstellt. Über derartige Adressen ist es Netzwerkprogrammen möglich, den lokalen Rechner auf gleiche Art und Weise wie entfernte Rechner zu adressieren.

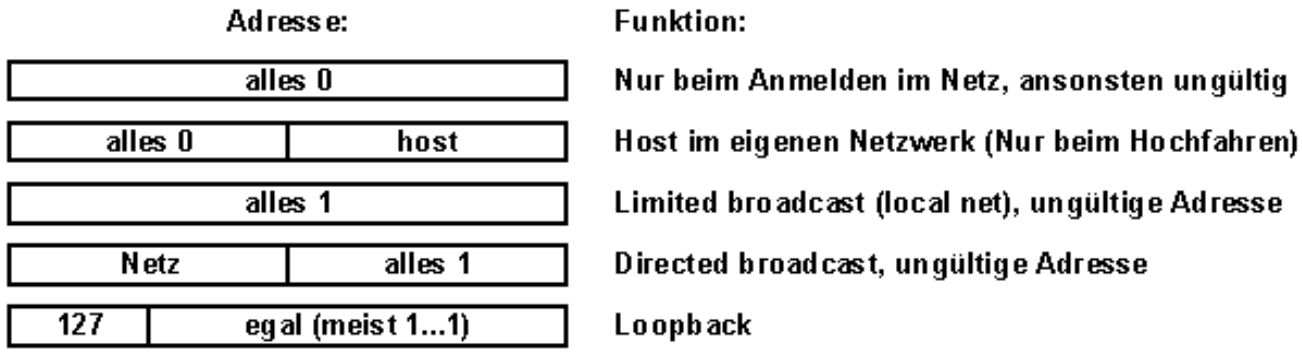
IP-Netzwerkadresse

Jede IP-Adresse, dessen Hostteil nur aus Nullen besteht, bezeichnet das Netzwerk selbst (**Netzwerkadresse**), z. B. 128.1.0.0 Rechner, die ihre IP-Adresse zum Bootzeitpunkt nicht kennen (können), verwenden bspw. diese Adresse, um via DHCP oder BOOTP diese von einem IP-Adressen-Server zu erfahren.

Broadcast-Adresse

Ein komplett aus Einsen bestehender Rechnerteil adressiert alle im Netzwerk befindlichen Rechner auf einmal und wird als **Broadcastadresse** bezeichnet.

Zusammenfassung der speziellen Adressen



Bei Host-Adressen:

- Sind alle Werte einer Hostadresse = 0, wird damit das Netz selbst adressiert.

- Sind alle Werte einer Hostadresse = 255, steht dies für die Broadcast-Adresse, mit der alle Endgeräte in einem Netzwerk angesprochen werden.
- Die 1. mögliche Adresse eines Subnetzes wird üblicherweise als die „Standard-Gateway“- Hostadresse verwendet.

Beispiele:

Ordnen Sie folgende IP-Adressen den Netzwerkklassen zu:

135.2.3.4 -> Host in Klasse B-Netz 135.2 Subnetzmaske 255.255.0.0

10.2.76.19 -> Host in Klasse A-Netz 10 Subnetzmaske 255.0.0.0 (privater Bereich)

158.1.255.255 -> Broadcast-Adresse Klasse B-Netz 158.1 Subnetzmaske 255.255.0.0

5.6 Subnetze

Die Administration von Netzwerken mit nahezu 64000 (Klasse B) oder gar 16 Millionen von Rechnern (Rechner) erweist sich als nicht praktikabel. Zum einen kann keine heutige Technologie einen befriedigenden Durchsatz bei einer solchen Menge von Teilnehmern in einem einzigen Netz garantieren. Zum Anderen wäre wohl jeder Administrator mit einem solch gigantischen Verantwortungsbereich überfordert. Aus diesem Grund wird die Struktur der IP-Adresse - genau genommen, deren Hostteil - zumindest in Klasse-A- und Klasse-B-Netzwerken, in selteneren Fällen auch bei Klasse-C-Netzwerken, segmentiert.

Der Hostteil einer IP-Adresse wird bei der Subnetzbildung nochmals in zwei Teile untergliedert. Die führenden Bits repräsentieren lokal die Adresse des **Subnetzwerks**; die verbleibenden Bits adressieren einen Rechner eindeutig innerhalb eines solchen Teilnetzes.

Realisiert wird die Abbildung durch Bitmasken (Subnetzmaske). Bei einem gesetzten Bit dieser Maske wird das korrespondierende Bit der IP-Adresse als Netzwerkbit interpretiert; bei einem nicht gesetzten Bit gehört das entsprechende Bit der IP-Adresse zur Hostadresse. Da letztlich einzig die Anzahl gesetzter Bits und nicht deren relative Lage innerhalb der Maske das Verhältnis von Anzahl Subnetze zu Anzahl Hosts bestimmt, werden die gesetzten Bits stets »linksbündig« angeordnet.

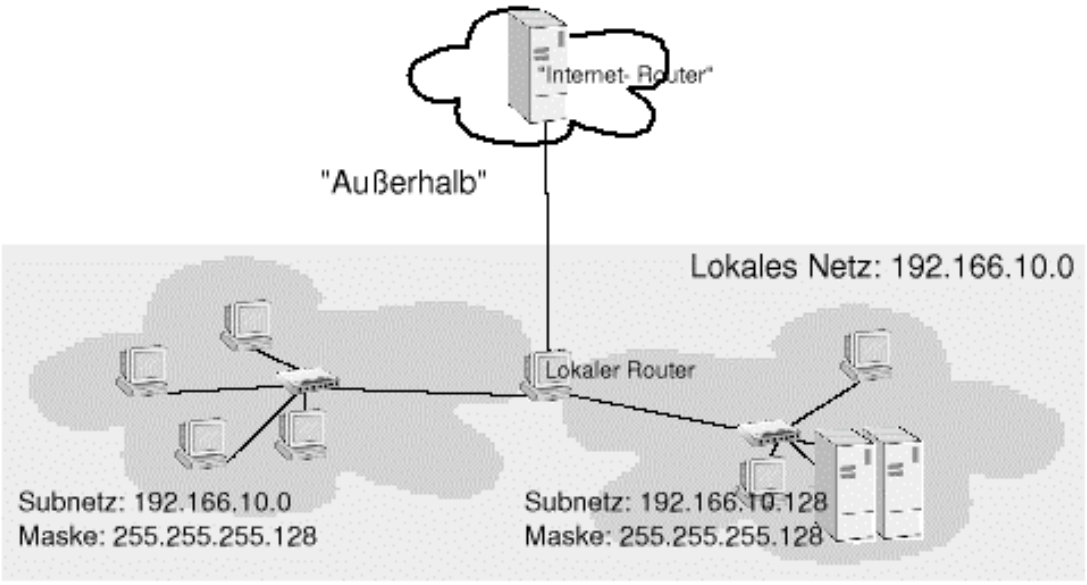


Bild 19: Paketvermittlung im Subnetz

5.6.1 Paketvermittlung im Subnetz

Unser lokales Netz mit der Class C-Netzwerkadresse 192.166.10.0 soll in zwei Teilnetze gesplittet werden. Hierfür genügt ein Bit des Hostteils, woraus sich als Subnetzmaske 255.255.255.128 ergibt. Durch diese Maske gehören alle Rechner mit IP-Adressen 192.166.10.1 bis 102.166.10.127 zu dem einen und alle Rechner mit IP-Adressen 192.166.10.129 bis 102.166.10.254 zum anderen Subnetz. Beachten Sie, dass es sich bei 192.166.10.0 und 192.166.10.128 um die Subnetzwerkadressen selbst und bei 192.166.10.128 bzw. 192.166.10.255 um die Broadcastadressen handelt.

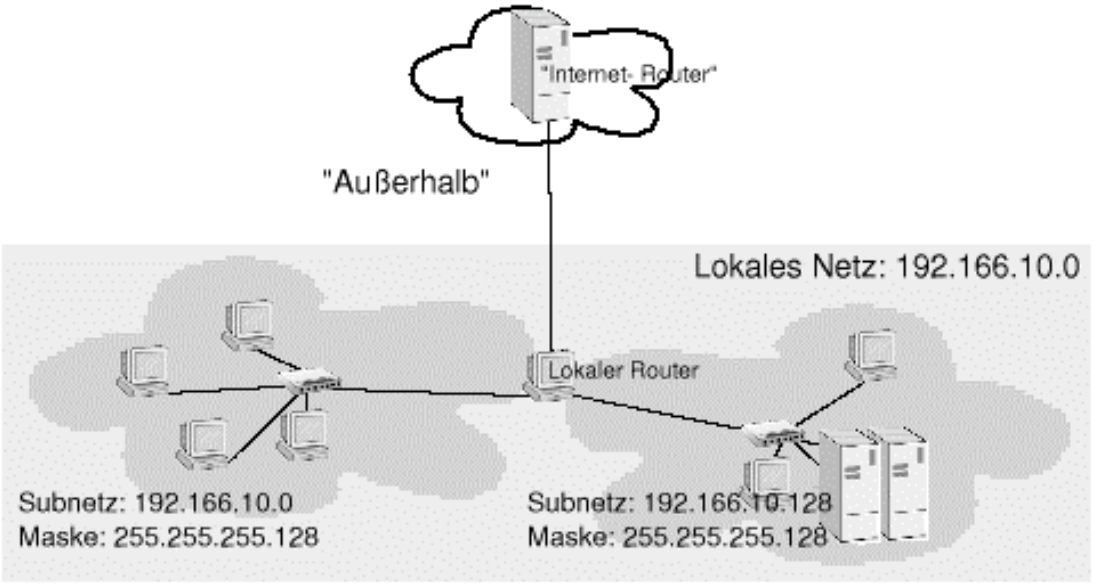


Bild: Paketvermittlung im Subnetz

Jeder Rechner im gesamten lokalen Netzwerk kennt nun sowohl seine eigene Adresse als auch die Subnetzmaske. Um herauszufinden, ob der Empfänger eines Datenpakets sich im selben Subnetz befindet, muss der Rechner sowohl seine eigene IP (Quelladresse) als auch die des Adressaten (Zieladresse) bitweise UND-verknüpfen. Sind beide Ergebnisse gleich, befindet sich der Empfänger im selben Subnetz und das

Paket kann direkt an diesen gesendet werden, andererseits muss das Paket über die „Standard-Gateway“-Adresse in das andere Subnetz geleitet werden.

Hostadresse binär:	1100 0000 . 1010 1000 . 0001 1011 . 0010 0000
Bitweise UND-Verknüpfung	
SM Klasse C:	1111 1111 . 1111 1111 . 1111 1111 . 0000 0000
Ergebnis der UND-Verknüpfung:	1100 0000 . 1010 1000 . 0001 1011 . 0000 0000

Bild: Ermittlung der Netz-Adresse (Netz-ID) durch UND-Verknüpfung mit der Subnetzmaske

Das Koppelglied (Router oder Gateway) zwischen den einzelnen Subnetzen ist Mitglied beider Netze; es besitzt also mehrere Netzwerkschnittstellen mit unterschiedlichen IP-Adressen. In der Beispielabbildung stellt ein Router gleichzeitig die Verbindung zur Außenwelt (Internet) her; die auf dieser Schnittstelle verwendete IP-Adresse kann allerdings im Subnetzwerk nicht nochmals vergeben werden.

Subnetting erfordert somit gleichzeitig ein Routing, falls Daten zwischen beiden Teilnetzen ausgetauscht werden sollen.

5.6.2 Bildung der Subnetzmaske

Ein Teil der Host Adresse kann auch intern als Subnetzadresse gewertet werden um große Netze nochmal zu segmentieren. So kann der Host mit der Nummer 12.4 im B-Klasse Netz 149.76 in den Host Nummer 4 im Subnetz 12 des Netzwerks 149.76 interpretiert werden. Welche Bits der 32 Bit Adresse als Netz- und welche als Hostadresse gewertet werden wird in der sogenannten Netzmaske festgelegt.

Die Netzmaske (Netmask) wird in vier Oktetts angegeben ist. Jedes Bit dieser Maske, das gesetzt ist, bestimmt, dass das entsprechende Bit in der Adresse zur Netzadresse gehört.

Beispiel 1:

Die B-Klasse Adresse 149.76.0.0 wird normalerweise gewertet als B-Class Adresse, deren erste 2 Bytes als Netzadresse gelten, und deren letzte 2 Bytes die Hostadresse darstellt. Dies ergibt folgende Netzmaske :

	Netzadresse	Hostadresse
149.76.0.0	-->	10010101.01001100.00000000.00000000
Netzmaske		11111111.11111111.00000000.00000000
	-->	255.255.0.0

Soll dieses Netz nun in mehrere Unternetze aufgeteilt werden, so wird z. B. das dritte Byte als Subnetz-Adresse und das letzte Byte als Hostadresse interpretiert. Für die Netzmaske ergäbe sich somit:

	Netzadresse	Hostadresse
149.76.0.0	-->	10010101.01001100.00000000.00000000
Netmask		11111111.11111111.11111111.00000000

--> 255.255.255.0

Beispiel 2:

Das C-Klasse Netzwerk 192.168.200.0 soll in zwei Unternetze aufgeteilt werden. Um zwei Netze anzusprechen genügt ein Bit der Hostadresse für die Subnetzangabe:

192.168.200.0	-->	11000000.10101000.11001000.00000000
Netzmaske		11111111.11111111.11111111.10000000
Netzadresse		NNNNNNNN.NNNNNNNN.NNNNNNNN.N
Host-Adresse		HHHHHHH
	-->	255.255.255.128

Die Netzmaske verändert sich von 255.255.255.0 (Class-C-Subnetzmaske) nach 255.255.255.128. Damit wissen die Netzteilnehmer, dass kein normales C-Class Netz vorliegt.

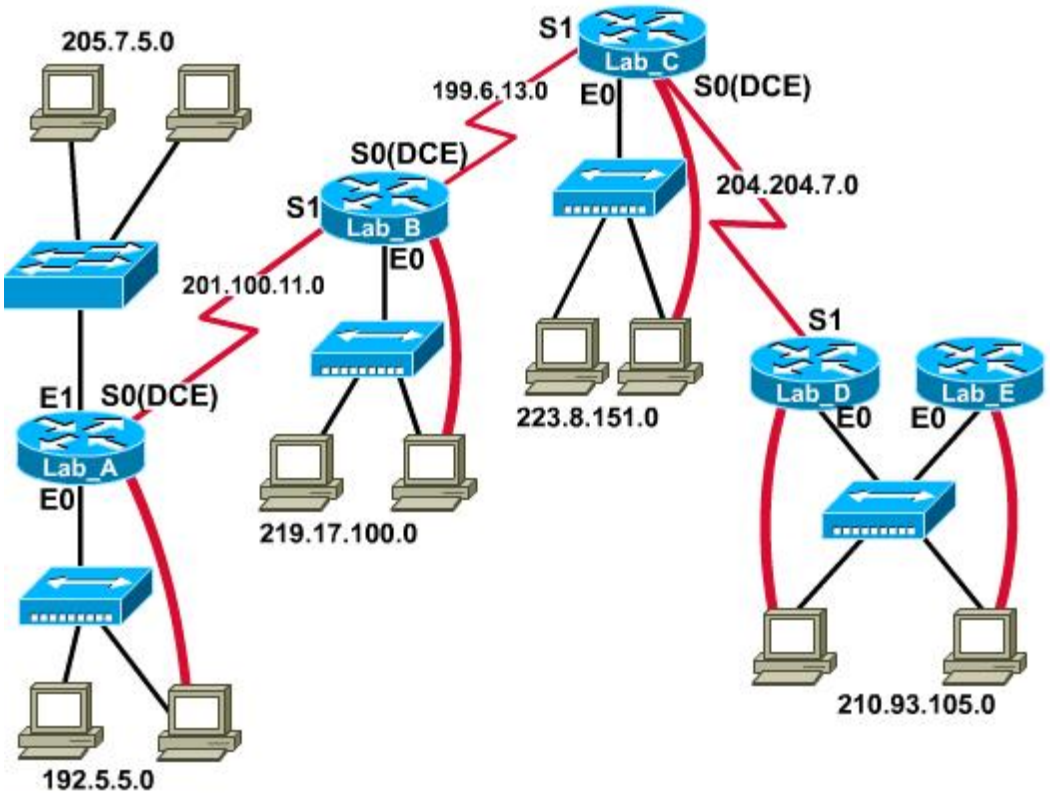
Subnetz 0: Subnetzadresse 192.168.200.0

1. Hostadresse	-> 192.168.200.00000001	im Subnetz 0
2. Hostadresse	-> 192.168.200.00000010	im Subnetz 0
3. Hostadresse	-> 192.168.200.00000011	im Subnetz 0
:	:	
letzte Hostadresse	-> 192.168.200.01111110	im Subnetz 0
Broadcast-Adresse	-> 192.168.200.01111111	im Subnetz 0

Subnetz 1: Subnetzadresse 192.168.200.128

1. Hostadresse	-> 192.168.200.10000001	im Subnetz 1
2. Hostadresse	-> 192.168.200.10000010	im Subnetz 1
3. Hostadresse	-> 192.168.200.10000011	im Subnetz 1
:	:	
letzte Hostadresse	-> 192.168.200.11111110	im Subnetz 1
Broadcast-Adresse	-> 192.168.200.11111111	im Subnetz 1

5.6.3 Beispiel für ein Router Topology Lab



Router Name	Router Type	E0	E1	S0	S1	SM	Enable Pass-word	Vty Pass-word
Lab_A	2514	192.5.5.1	205.7.5.1	201.100.11.1	--	255.255.255.0	class	cisco
Lab_B	2501	219.17.100.1	--	199.6.13.1	201.100.11.2	255.255.255.0	class	cisco
Lab_C	2501	223.8.151.1	--	204.204.7.1	199.6.13.2	255.255.255.0	class	cisco
Lab_D	2501	210.93.105.1	--	--	204.204.7.2	255.255.255.0	class	cisco
Lab_E	2501	210.93.105.2	--	--	--	255.255.255.0	class	cisco

Bild: Router Topology Lab

6. Die Transportschicht TCP (Layer 4)

Aus Sicht einer Anwendung eröffnet das *Transmission Control Protocol* einen bidirektionalen, virtuellen Datenkanal zwischen den beiden Kommunikationsendpunkten. Die Daten werden scheinbar in einem Fluss übertragen. Intern gehen diese blockweise übers Netz, wobei die Blockgröße dynamisch anhand von Parametern wie der Netzauslastung, der Fenstergröße oder der Empfangs- bzw. Sendepuffer angepasst wird.

Im Unterschied zum *User Datagram Protocol* (UDP) kümmert sich TCP selbst um die sichere Übertragung. Es verwendet hierzu Sequenznummern, Prüfsummen, Quittungen und Wiederholung des Transfers bei einer Zeitüberschreitung.

Andere wesentliche Eigenschaften sind das Sliding-Window-Verfahren und die Kennzeichnung von Vorrangdaten.

6.1 Funktionen der Transportschicht

- transparente Datenübertragung zwischen Endsystemen
- verbindungsorientierte Übertragung (sicherer Datentransport zwischen Endsystemen):
  - Prüfsumme (Checksum)
  - Paketfolgenummer (Sequence Number)
  - Empfangsbestätigungen (Acknowledgement)
  - Übertragungswiederholung (Retransmission)
  - Datenflußsteuerung (Flow Control)
- verbindungslose Übertragung
  - *Best-Effort-Prinzip*
  - für einfache Anwendungen mit Frage-Antwort-Charakter

6.2 Adressierung auf der Transport-Schicht

Zur Adressierung eines Kommunikationspartners in Form eines Applikationsprogramms müssen beim Durchlaufen der vier TCP/IP- Schichten auch vier verschiedene Adressen angegeben werden.

1. Eine Netzwerkadresse (z. B. die MAC-Adresse: 00-AA-00-3F-89-4A)
2. Eine Internet-Adresse (z.B. die IP-Adresse: 10.0.0.99)
3. Eine Transportprotokoll-Adresse (z.B. 10 - UDP)
4. **Eine Portnummer (z. B. Telnet)**

Im IP-Header befinden sich die Internet- und die Transportprotokoll-Adresse.

6.3 Aufbau des TCP-Protokollrahmens

Bild: Struktur des „Transmission Control Protocol“-Frames

Die Felder des Protokollkopfes bedeuten:

Senderport (Source Port), Empängerport (Destination Port)

Der Sender adressiert den Partner über IP-Adresse des Zielrechners und eine 16-Bit lange Portnummer. Beide zusammen bezeichnet man unter Unix als **Socket**.
Um den Empfänger adressieren zu können, muss der Sender dessen Portnummer kennen. Der Sender wiederum kann (meist) eine beliebige freie Portnummer wählen, da er seine eigene Nummer dem Kommunikationspartner mitteilt. Für die Standarddienste stehen die Portnummern in der Datei /etc/services.
UDP verwendet einen eigenen Adressraum, so dass gleiche Portnummern sich somit nicht überschneiden.

Sequenznummer (Sequence Number)

Dieser 32-Bit Wert kennzeichnet eindeutig die Stellung eines Pakets innerhalb des Datenstroms in Senderichtung. Die initiale Sequenznummer wird zu Beginn des Verbindungsaufbaus von jedem Kommunikationspartner festgelegt, wobei gilt, dass sie für die maximal mögliche Lebensdauer des Pakets (TimetoLive des Internet Protokolls) bzgl. der verbundenen Rechner eindeutig ist.

Die Sequenznummer eines folgenden Pakets berechnet sich aus der initialen Sequenznummer und der Anzahl bisher gesendeter Bytes. Somit ist es möglich, bei Verlust oder Beschädigung eines Pakets gezielt dieses wiederholt zu senden.

Quittungsnummer (Acknowledgement Number)

Die Quittungsnummer sendet der Empfänger eines Pakets als Bestätigung für den Empfang. Sie gibt an, wie viele Bytes bislang beim Partner unversehrt eingetroffen sind. Sollten Sequenznummer oder Quittungsnummer im Laufe einer Sitzung einmal überlaufen, so wird bei 0 fort gefahren.

Offset (Data Offset)

Das Feld enthält die Länge des TCP-Kopfes (TCP-Headers) in 32-Bit Worten. Anhand dieser wird der Beginn der enthaltenen Daten ermittelt.

Reserve

Reserviert für spätere Nutzung. Wird nicht verwendet.

Steuerbits

Die 6 Steuerbits bedeuten:

URG (Urgent-Ponter)

Die Daten im Feld "Vorrangdaten" sind gültig

ACK (Acknowledgement)

Die Quittungsnummer ist gültig

PSH (PUSH)

Das Segment sofort der Anwendung übergeben werden

RST (Reset)

Rücksetzen der Verbindung

SYN (Synchronice)

Wunsch nach Aufbau einer Verbindung

FIN (Finish)

Beenden der Verbindung. Ein Partner, der dieses Bit setzt, muss seinerseits die Verbindung offenhalten, bis auch das Gegenüber das FIN-Bit sendet. Er selbst darf aber keine weiteren Daten senden (Ausnahme sind die Quittungen auf eintreffende Pakete).

Fenstergröße (window)

Momentane Kapazität des Empfangspuffers auf Absenderseite. Sein Gegenüber darf maximal so viele Daten (auch aufgeteilt auf mehrere Pakete) senden, wie durch die Fenstergröße angegeben ist. TCP passt die Fenstergröße automatisch an die Kapazität des Übertragungsmediums an. Dazu wird das Fenster sukzessive vergrößert, bis Pakete aufgrund des zu hohen Datenaufkommens verworfen werden. Treten nun vermehrt Übertragungsfehler auf, wird das Fenster wieder verkleinert usw.. Dieses Sliding-Window-Prinzip lässt sich sehr gut beim Download von Dateien beobachten, wobei die Datentransferrate ständig schwankt.

Prüfsumme (Checksum)

Prüfsumme über das gesamte Paket.

Zeiger auf Vorrangdaten (Urgent Pointer)

Der Zeiger gibt einen Offset innerhalb der Daten im Paket an. Die dem Zeiger folgenden Daten werden als besonders wichtig deklariert. Eine Anwendung wird beim Eintreffen solcher Daten unterrichtet. Sie sollte nun

ihre bisherige Arbeit unterbrechen und die dringliche Nachricht bearbeiten (z.B. Telnet). Das URG-Bit muss gesetzt sein.

Optionen

Austausch von Informationen auf TCP-Ebene: Beim Verbindungsaufbau wird meist "MaximumSegmentSize" gesendet, um dem Partner mitzuteilen, dass größere Pakete empfangen werden können. Weitere Optionen sind "EndOfOptionList" und "NoOperation".

7. Das Address Resolution-Protokoll (ARP)

ARP (Address Resolution Protocol) ist ein erforderlicher TCP/IP-Standard, der in RFC 826 "Address Resolution Protocol (ARP)" festgelegt ist. ARP löst von TCP/IP-Software verwendete IP-Adressen in von LAN-Hardware verwendete MAC-Adressen auf. ARP bietet Hosts, die sich in demselben physischen Netzwerk befinden, die folgenden Protokolldienste:

MAC-Adressen werden mit einer Netzwerkbroadcastanforderung in Form der Frage "Welche ist die MAC-Adresse für ein Gerät, das mit der übergegebenen IP-Adresse konfiguriert ist?" abgerufen.

Wenn eine ARP-Anforderung beantwortet wird, zeichnen sowohl der Sender der ARP-Antwort als auch der ursprüngliche ARP-Anfordernde gegenseitig ihre IP-Adressen und MAC-Adressen als Eintrag für zukünftige Verweise in einer lokalen Tabelle auf, die als ARP-Cache bezeichnet wird.

7.1 Hardwareadressen

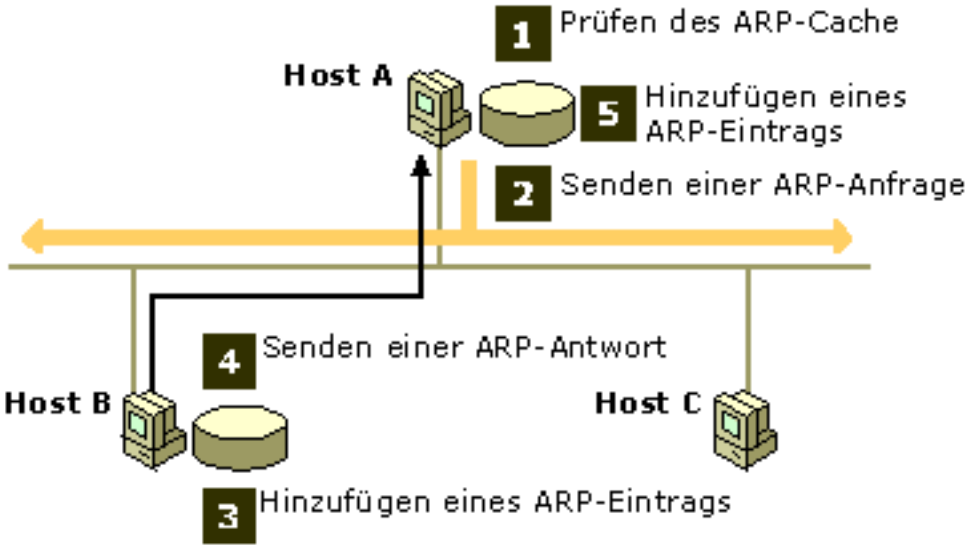
Hardwareelemente für die Verwendung in LANs müssen eine eindeutige, vom Hersteller in das Gerät programmierte Adresse beinhalten. Bei Ethernet- und Token Ring LAN-Hardware wird diese Adresse als MAC-Adresse (Media Access Control-Adresse) bezeichnet.

Jede MAC-Adresse weist das Gerät in einem eigenen physischen Netzwerk mit einer 6-Byte-Nummer aus, die im ROM (Read-Only Memory) auf jedem physischen Hardwaregerät (z. B. einem Netzwerkadapter) programmiert ist. MAC-Adressen werden i. d. R. hexadezimal (z. B. 00-AA-00-3F-89-4A) angezeigt.

Vertrauenswürdigkeit und Registrierung von MAC-Adressen werden vom IEEE (Institute of Electrical and Electronics Engineers) überwacht. Zum gegenwärtigen Zeitpunkt ist das IEEE zuständig für die Registrierung und Zuweisung von eindeutigen Nummern für die ersten drei Byte der MAC-Adressen zu den einzelnen Herstellern. Jeder Hersteller kann dann die letzten drei Byte der MAC-Adresse einzelnen Netzwerkadaptern zuweisen.

So löst ARP MAC-Adressen für den lokalen Datenverkehr auf

In der folgenden Darstellung wird erläutert, wie ARP IP-Adressen in Hardwareadressen für Hosts in demselben lokalen Netzwerk auflöst.



In diesem Beispiel befinden sich zwei TCP/IP-Hosts (Host A und B) in demselben physischen Netzwerk. Host A wurde die IP-Adresse 10.0.0.99 zugewiesen, und Host B wurde die IP-Adresse 10.0.0.100 zugewiesen.

Wenn Host A versucht, mit Host B zu kommunizieren, wird in den folgenden Schritten die der Software zugewiesene Adresse (10.0.0.100) von Host B in die der Hardware zugewiesene MAC-Adresse von Host B aufgelöst:

1. Auf der Grundlage des Inhalts der Routingtabelle auf Host A bestimmt IP, dass die IP-Adresse für die Weiterleitung an Host B 10.0.0.100 lautet. Host A überprüft dann seinen lokalen ARP-Cache auf entsprechende Hardwareadressen für Host B.

2. Wenn Host A im Cache keine Entsprechung finden kann, sendet er einen ARP-Anfragerahmen mit der Frage "Welche ist die Hardwareadresse für 10.0.0.100?" an sämtliche Hosts im lokalen Netzwerk. Sowohl die Hardware- als auch die Softwareadressen für die Quelle, Host A, sind in der ARP-Anfrage enthalten.

   Jeder Host im lokalen Netzwerk empfängt die ARP-Anfrage und überprüft sie auf eine Übereinstimmung mit seiner eigenen IP-Adresse. Wird keine Übereinstimmung gefunden, wird die ARP-Anfrage verworfen.

3. Host B stellt fest, dass die IP-Adresse in der ARP-Anfrage mit der eigenen IP-Adresse übereinstimmt und fügt seinem lokalen ARP-Cache eine Zuordnung der Hardware- und Softwareadresse für Host A hinzu.

4. Host B sendet eine ARP-Antwortnachricht mit seiner Hardwareadresse direkt an Host A.

5. Wenn Host A die ARP-Antwortnachricht von Host B empfängt, aktualisiert er seinen ARP-Cache mit der Zuordnung der Hardware-/Softwareadresse für Host B.

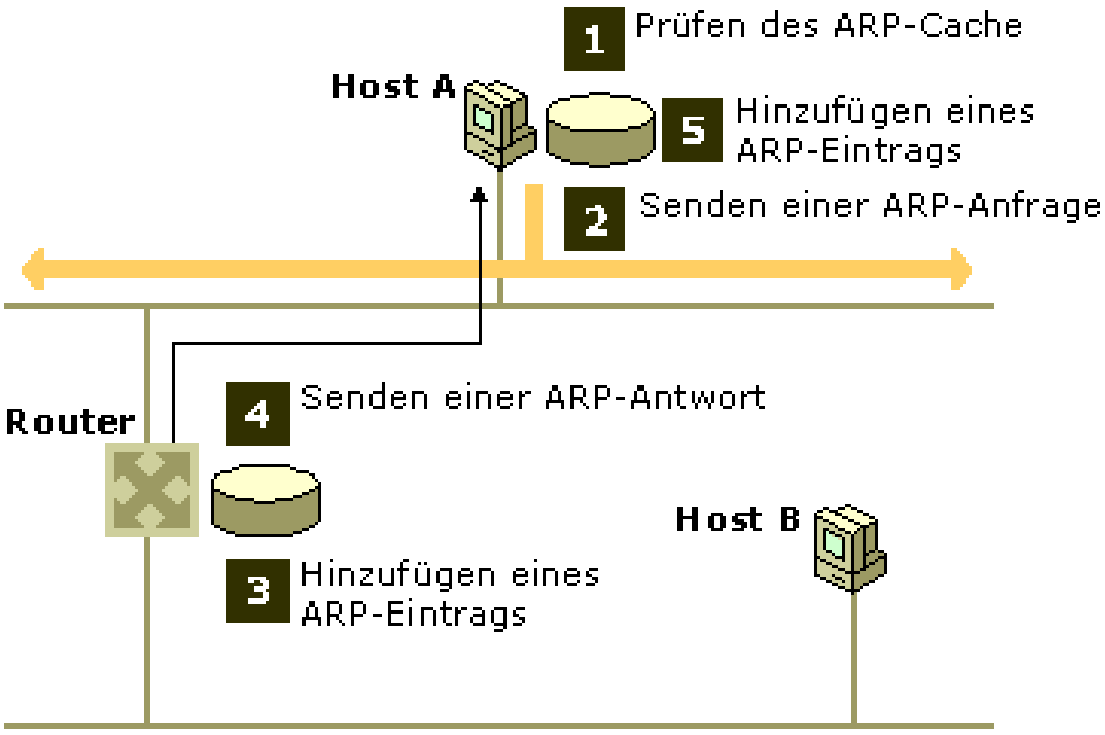
Wenn die MAC-Adresse für Host B ermittelt wurde, kann Host A IP-Datenverkehr an Host B senden, indem er die MAC-Adresse von Host B für die Adressierung verwendet.

7.2 So löst ARP MAC-Adressen für den Remotedatenverkehr auf

ARP wird auch zur Weiterleitung von IP-Datagrammen an lokale Router für Ziele verwendet, die sich nicht im lokalen Netzwerk befinden. In diesem Fall löst ARP die MAC-Adresse einer Routerschnittstelle im lokalen Netzwerk auf.

In der folgenden Darstellung wird erläutert, wie ARP IP-Adressen in Hardwareadressen für zwei Hosts mit einem gemeinsamen Router in verschiedenen physischen Netzwerken auflöst.

In diesem Beispiel wurde Host A die IP-Adresse 10.0.0.99 zugewiesen, und Host B verwendet die IP-Adresse 192.168.0.99. Die Routerschnittstelle 1 befindet sich in demselben physischen Netzwerk wie Host A. Sie hat die IP-Adresse 10.0.0.1. Die Routerschnittstelle 2 befindet sich in demselben physischen Netzwerk wie Host B. Sie hat die IP-Adresse 192.168.0.1.



Wenn Host A versucht, mit Host B zu kommunizieren, wird die der Software zugewiesene Adresse (10.0.0.1) der Routerschnittstelle 1 in den folgenden Schritten in die der Hardware zugewiesene MAC-Adresse aufgelöst:

1. Auf der Grundlage des Inhalts der Routingtabelle auf Host A bestimmt IP, dass die IP-Adresse für die Weiterleitung an Host B 10.0.0.1 lautet. Dies ist die IP-Adresse des entsprechenden Standardgateways. Host A überprüft dann den eigenen lokalen ARP-Cache auf entsprechende Hardwareadressen für die IP-Adresse 10.0.0.1.

2. Wenn Host A im Cache keine Entsprechung finden kann, sendet er einen ARP-Anfragerahmen mit der Frage "Welche ist die Hardwareadresse für 10.0.0.1?" an sämtliche Hosts im lokalen Netzwerk. Sowohl die Hardware- als auch die Softwareadressen für die Quelle, Host A, sind in der ARP-Anfrage enthalten.

   Jeder Host im lokalen Netzwerk empfängt die ARP-Anfrage und überprüft sie auf eine Übereinstimmung mit seiner eigenen IP-Adresse. Wird keine Übereinstimmung gefunden, wird die ARP-Anfrage verworfen.

3. Der Router stellt fest, dass die IP-Adresse in der ARP-Anfrage mit der eigenen IP-Adresse übereinstimmt und fügt seinem lokalen ARP-Cache eine Zuordnung der Hardware- und Softwareadresse für Host A hinzu.

4. Der Router sendet anschließend eine ARP-Antwortnachricht mit seiner Hardwareadresse direkt an Host A.

5. Wenn Host A die ARP-Antwortnachricht vom Router empfängt, aktualisiert er seinen ARP-Cache mit der Zuordnung der Hardware-/Softwareadresse für 10.0.0.1.

Wenn die MAC-Adresse für die Routerschnittstelle 1 ermittelt wurde, kann Host A IP-Datenverkehr an die Routerschnittstelle 1 senden, indem er die MAC-Adresse von Routerschnittstelle 1 für die Adressierung verwendet. Der Router leitet den Datenverkehr dann an Host B weiter. Der dabei ablaufende ARP-Vorgang entspricht den in So löst ARP MAC-Adressen für den lokalen Datenverkehr auf erläuterten Schritten.

7.3 Der ARP-Cache

Zur Minimierung der Anzahl von Broadcasts unterhält ARP einen Cache mit Zuordnungen von IP-Adressen zu MAC-Adressen für die zukünftige Verwendung. Der ARP-Cache kann dynamische und statische Einträge enthalten. Dynamische Einträge werden automatisch hinzugefügt und entfernt. Statische Einträge verbleiben im Cache, bis der Computer neu gestartet wird.

Jeder dynamische ARP-Cacheeintrag verfügt über eine mögliche Lebensdauer von zehn Minuten. Neue Einträge, die dem Cache hinzugefügt werden, erhalten einen Zeitstempel. Wenn ein Eintrag nach dem Hinzufügen nicht innerhalb von zwei Minuten erneut verwendet wird, läuft er ab und wird aus dem ARP-Cache entfernt. Wenn ein Eintrag verwendet wird, verlängert sich seine Lebensdauer um zwei weitere Minuten. Wenn ein Eintrag wiederholt verwendet wird, verlängert sich seine Lebensdauer auf bis zu zehn Minuten.

Sie können den ARP-Cache mit Hilfe des Befehls **arp** anzeigen lassen. Geben Sie an der Windows 2000-Eingabeaufforderung **arp -a** ein, um den ARP-Cache auf einem Windows 2000-Computer anzeigen zu lassen. Geben Sie zum Anzeigen der **arp**-Befehlszeilenoptionen an der Eingabeaufforderung **arp /?** ein.

8. Das Domain Name System Protocol (DNS-Protocol)

Was ist eine Domain?

Domain bedeutet soviel wie (Geltungs-)Bereich und ist ein Teil der Namenshierarchie in den Internet-Adressen.

8.1 Der Domain-Name-Service (RFC-Spezifikation)

Im Internet erfolgt die Kommunikation auf der Basis von sog. "Adressen". Einzelne Rechner werden über eine sogenannte Internet-Protokoll-Adresse (IP-Adresse) eindeutig identifiziert. Die Spezifikation zu DNS ist zu finden im RFC 1480.

Die Verteilung der Adressen erfolgt als sog. MAC-Adressen auf den Netzwerkkarten durch die Hardware-Hersteller. Diesen MAC-Adressen werden durch das Netzwerk-Protokoll (z. B. TCP/IP) sog. IP-Adressen zugeordnet; diese Adressen folgen dem Schema 255.255.255.255 und können Nummern von 0-255 enthalten, z. B. 129.100.33.2

Damit die Adressen "sprechender" gestaltet werden können gibt es im Internet das Domain-Name-System (DNS). Dieses System ordnet den Adressen der Form 255.255.255.255 "sprechende" Namen zu (Domains).

Das DNS ist eine verteilte Datenbank im Internet, die verständliche (Domänen-)namen mit den Nummernadressen verknüpft. Das DNS ist hierarchisch gegliedert.

8.2 Aufbau eines Domain-Namens

Die Internet-Adressen setzen sich mindestens aus Top-Level-Domain (TLD) und Second-Level-Domain (SLD) zusammen - Internet-Adressen werden immer von rechts nach links gelesen! Die Trennung der einzelnen Domainnamen erfolgt durch Punkte.

Ein Domainname besteht aus dem eigentlichen Domain-Namen und der Top-Level-Domain:
z. B.

telekom.info

wobei ***telekom*** der Domain-Name und ***info*** der Top-Level-Domain-Name ist.

Als Top Level Domain bezeichnet man den letzten Teil nach dem Punkt eines Domain-Namens. Dieser Teil des Domain-Namens bezeichnet einen geographischen oder auch thematischen Zusammenhang mit der Domain:

.GOV	Regierungseinrichtungen
.MIL	Militärische Einrichtungen

.EDU	Einrichtungen des Bildungswesens
.NET	Netzwerk-Organisationen
.ORG	Nicht-Regierungs-Organisationen (NGO's)
.COM	Kommerzielle Einrichtungen
.DE	Deutschland

8.3 Die Auflösung von Namen zu Nummern

Die Umwandlung der IP-Adressen in einen Domain-Namen kann sowohl über Host-Tabellen erfolgen als auch über das weltweit verteilte DNS-Datenbanksystem, in der die Namensserver hierarchisch aufgebaut sind. Zur Datenübertragung wiederum wird der Domain-Name mittels dieses Datenbanksystems entschlüsselt, d.h. der Domain-Name wird wieder in seine numerische computerlesbare IP-Adresse übersetzt. Die eigentliche Adressierung im Internet erfolgt durch numerische Adressen.

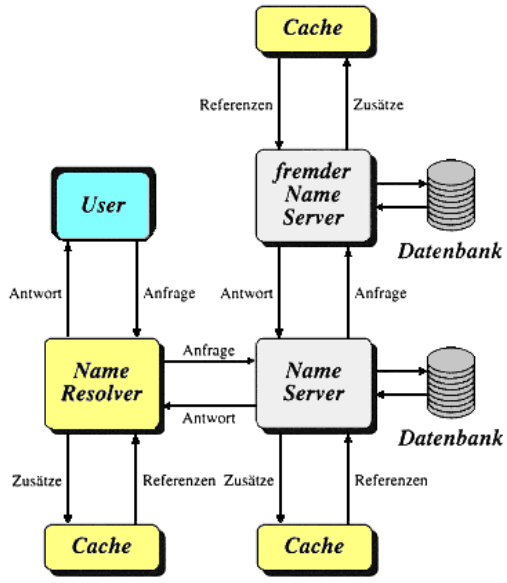


Bild: Der Servie DNS

Jeder Rechner, der an das Internet angeschlossen wird, muß die Adresse eines oder mehrerer Nameserver wissen, damit die Anwendungen auf diesem Rechner mit Namen benutzt werden können. Die Nameserver sind für bestimmte Bereiche, sogenannte 'domains' oder 'Zonen', zuständig (Institute, Organisationen, Regionen) und haben Kontakt zu anderen Nameservern, so daß jeder Name aufgelöst werden kann.

Der **Nameserver** des DNS verwaltet also einzelne Zonen, die einen Knoten im DNS-Baum und alle darunterliegenden Zweige beinhalten. Auf jeder Ebene des DNS-Baums kann es Namesever geben, wobei jeder Nameserver seinen nächsthöheren und nächstniedrigeren Nachbarn kennt.

8.4 NIC's und NOC's:

NICs (Network Information Centers) und NOCs (Network Operation Centers) arbeiten als ausführende Organisationen auf weltweiter, kontinentaler, nationaler und regionaler Ebene. Aufgabe eines NIC ist die Vergabe und Koordination von eindeutigen Adressen und Namen im Internet. So vergibt das zentrale InterNIC in USA ganze Adressbereiche an das europäische NIC (das RIPE- NCC (Reseaux IP Europeens - Network Coordination Center). Das RIPE wiederum versorgt alle europäischen NICs - auch das deutsche DE-NIC mit einem gültigen Adreßbereich.

Das DE-NIC vergibt eigenständig aus diesem zugewiesenen Nummernbereich Adressen an Provider, der die Adressen an seine Endbenutzer weiterverteilt. Ein NOC kümmert sich um den Betrieb des Netzes. Dazu gehören die Konfiguration der Netzkomponenten (Router, Leitungen), die Behebung von Störungen und Netzfehlern sowie die Beratung und Koordination der Netzteilnehmer. Basis des Nameservice bilden die "Root-Nameserver", die für die Top-Level-Domains zuständig sind. Die Mehrheit dieser Server ist in den USA beheimatet:

Name	Typ	Betreiber	URL
a	com	InterNic	http://www.internic.org
b	edu	ISI	http://www.isi.edu
c	com	PSINet	http://www.psi.net
d	edu	UMD	http://www.umd.edu
e	usg	NASA	http://www.nasa.gov
f	com	ISC	http://www.isc.org
g	usg	DISA	http://nic.mil
h	usg	ARL	http://www.arl.mil
i	int	NordUnet	http://www.nordu.net

j	()	(TBD)	http://www.iana.org
k	int	RIPE	http://www.ripe.net
l	()	(TBD)	http://www.iana.org