NETZWERK GRUNDLAGEN

André Creutz

28.06.2004

INHALTSVERZEICHNIS

HARDWARE

DIE KABELARTEN

KABEL FÜR ETHERNET (10MBIT):

- Koaxialkabel (weitere Beschreibung siehe unten)
- Patchkabel (Twisted Pair) Cat3

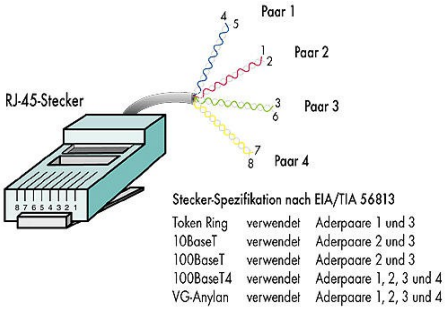
KABEL FÜR FAST ETHERNET (100MBIT):

- Patchkabel (weitere Beschreibung siehe unten)
- zu unterscheiden ist dabei 100BaseT4 (Cat3) nach altem Standart und 100BaseTx (Cat5) nach neuem Standart

TWISTED PAIR KABEL:

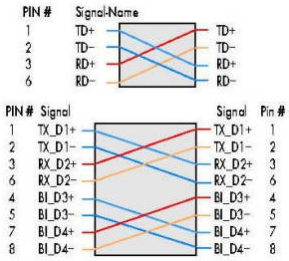
Twisted Pair ist nicht gleich Twisted Pair. In den Ethernet-Standards sind mehrere Versionen spezifiziert. Darüber hinaus gibt es noch Unterschiede in der Abschirmung. Es gibt mehrere Kategorien, jedoch spielen nur Cat3 (Kategorie 3) und Cat5 (Kategorie 5) bei Netzwerken eine Rolle. Die beiden Kabelarten unterscheiden sich nur in maximaler zulässiger Frequenz und den Werten für Dämpfung (Abschwächung des Signals auf einer bestimmten Strecke).

- Cat 3:
  - achtadriges Kabel, bei welchem immer zwei Adern miteinander vertrillt werden
  - wie im unteren Schema dargestellt wird für den 10Mbit betrieb nur Aderpaar 2 und 3 verwendet
- Cat 5:
  - auch das ist ein achtadriges Kabel bei welchem jeweils zwei Adern miteinandre verdrillt werden
  - im obrigen Schema ist gezeigt das auch 100BaseT(x) nur Kabelpaar 2und 3 verwendet



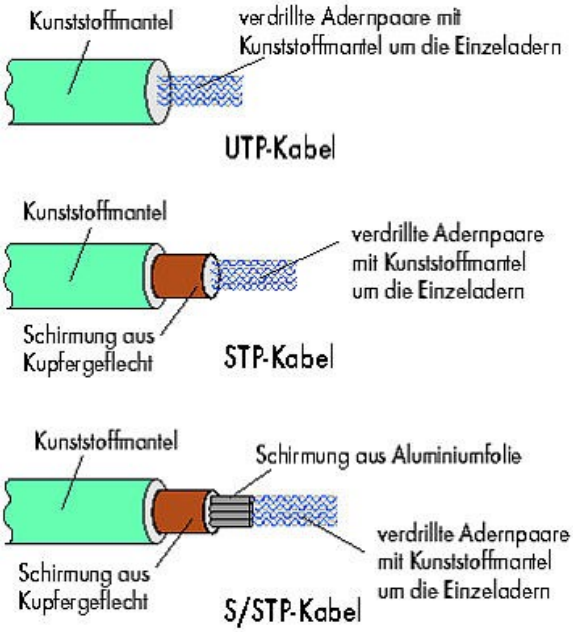
Cat 3 und Cat 5 werden auch als UTP (Unshielded Twisted Pair) bezeichnet. Das drückt aus das diese Kabel nicht abgeschirmt sind und somit Störungen von außen eintreten können. Es gibt aber auch abgeschirmte Kabel z.B. das STP oder auch S/UTP genannt (Shielded Twisted Pair) welches einen Gesamtschirm um alle Aderpaare hat und das S/STP (Shielded/Screened Twisted Pair) welches zusätzlich zu dem Gesamtschirm noch um jedes Aderpaar einen Mantel hat

Falls sie nur zwei Computer miteinander verbinden wollen ist das Crossed Kabel das richtige. Dieses Kabel wird nur zwischen die beiden Computer gesteckt. Ein Crossed ist fast wie ein normales Twisted Pair Kabel nur dass die Polung im Kabel überkreuz verläuft



KOAXIAL-KABEL:

Koaxial ist ein einadrigen Kabel mit Abschirmung. Man darf das Koaxial für Netzwerke nicht mit dem von Radio und TV verwechseln. Der Unterschied ist, dass das LAN-Kabel 50-Ohm Widerstand und das für TV und Radio 75-Ohm Widerstand hat.



DIE NETZWERKÜBERGÄNGE

Mit dem Begriff **Netzwerkübergänge** faßt man eine Vielzahl technisch verschiedenartiger Geräte zusammen, die dazu da sind Verbindungen zwischen Netzwerken zu schaffen. Es kann sich dabei je nach Komplexität um einfache Verstärker bis hin zu vollständigen Rechnern handeln.

Solche Übergänge sind erforderlich, wenn das vorhandene Netzwerk

- *strukturiert* werden soll, d.h. es soll der Übersichtlichkeit und Verwaltung nach in Subnetze unterteilt werden,
- *erweitert* werden soll, d.h. das Netz soll physikalisch vergrößert werden,
- mit weiteren Netzwerken *verbunden* und *vernetzt* werden soll, d.h. es sollen mehrere **LAN**'s (***L**ocal **A**rea **N**etwork*) miteinander verknüpft oder eine **WAN**-Anbindung (***W**ide **A**rea **N**etwork*) realisiert werden, so daß ein heterogenes Netz entsteht.

Erweiterungen lokaler Netzwerke ziehen in den meisten Fällen automatisch eine Strukturierung nach sich, da die zugelassene Ausdehnung oder die maximale Anzahl für Teilnehmeranschlüsse überschritten werden. Aber eine Strukturierung ist auch dann erforderlich, wenn die Netzlast zu groß geworden ist und die verfügbare Bandbreite nicht mehr ausreicht.

Jedoch werden auch innerhalb dieser physikalischen Grenzen Netzwerke durch Übergänge untergliedert, da

- *ein LAN-Verbund* gebildet werden soll:
  - Räumlich getrennte Subnetze werden zusammengeschlossen.
  - Die Gesamtlast des Netzwerkes soll verteilt werden. Dabei kann durch Abtrennung und Gruppenbildung ein hohes Maß an interner Kommunikation auf das Teilnetz einer Gruppe beschränkt werden, wodurch das Gesamtnetz entlastet wird.
- *Sicherheitsaspekte* dies erfordern:
  - Da die Verbreitung von sicherheitsrelevanten Informationen auf Teilnetze beschränkt bleibt, vermindert sich das Risiko des unberechtigten Zugriffs auf diese Daten.
- *Fehlersituationen* eingegrenzt werden können und auch nicht mehr das Gesamtnetz belasten.
- die *Verwaltung* des Gesamtnetzes vereinfacht wird:
  - Die Bildung von Subnetzen ermöglicht ein dezentrales Management und erhöhte Übersichtlichkeit.

Die eben genannten Ziele können jedoch nicht von allen Netzübergängen gleich gut realisiert werden. Da die verschiedenen Übergänge auf unterschiedlichen Schichten

des OSI-Modells arbeiten, steht ihnen auch jeweils ein anderer Funktionsumfang zur Verfügung. **Generell gilt:** Je höher die Kopplung von zwei Netzwerken im OSI-Modell (***O**pen **S**ystems **I**nterconnection*) vorgenommen wird, desto mehr der Ziele lassen sich verwirklichen ➔ desto größer wird jedoch auch die Komplexität des Übergangs.

Es gibt insgesamt vier Grundformen, die sich aufgrund ihrer Funktionalität unterscheiden:

I. Repeater arbeiten gemäß OSI-Schicht 1,
II. Bridges gemäß OSI-Schicht 2,
III. Router gemäß OSI-Schicht 3 und
IV. Gateways gemäß OSI-Schicht 4 und 7.

DER REPEATER

Repeater sind simple Verstärkereinrichtungen und dienen der direkten Signalweiterleitung. Ihr Aufbau ist relativ einfach und kommt vollkommen ohne Software aus.

Wie Abbildung 1.1 zeigt operieren Repeater gemäß ihrer Funktionalität auf der *Bitübertragungsschicht*. Auf dieser Ebene gibt es keine Daten mit logischer Struktur, sondern nur Bits (also nur zwei Zustände: Strom oder kein Strom) die übertragen werden müssen. Diese elektrischen Signale werden vom Repeater empfangen, verstärkt und wahllos weitergegeben.

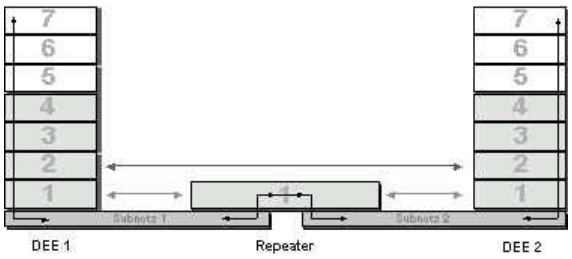


Abbildung 1.1: Die Einordnung von Repeatern in das OSI-Modell

Von "wahllos" spricht man deshalb, weil Repeater keinerlei Filter- oder Wegfindungsfunktionen übernehmen können. Solche Funtionsweisen bleiben Übergängen vorbehalten, die auf höheren OSI-Schichten arbeiten. Repeater leiten alle Daten unkontrolliert und unabhängig von deren Herkunft oder Ziel weiter.

Wegen ihre bitweise Übertragung von Daten werden die Signale auf den Leitungen zwar regeneriert, die verbundenen Netzsegmente werden aber nicht entkoppelt, d.h. die beiden Netzsegmente arbeiten wie ein einzelner Netzabschnitt. Das bedeutet, daß die Längenbeschränkungen für einzelne Netzsegmente die sich durch die Dämpfung der Signale auf der Leitung ergeben mit Hilfe von Repeatern zwar überwunden

werden können, nicht jedoch die Längenbeschränkungen die sich Aufgrund der Signallaufzeiten ergeben. Es ist also nicht möglich, beliebig viele Netzsegmente mit Repeatern zu verbinden.

Durch ihre Eigenschaft der einfachen Weitergabe von Signalen lassen sich Repeater nicht zur Strukturierung von Netzwerken einsetzten. Eine Entlastung von Netzwerkteilen würde beispielsweise das Auswerten von Zieladressen der Übertragungsdaten notwendig machen, damit entschieden werden kann, ob die Zielstation jenseits des Geräts oder diesseits liegt. Im zweiten Fall sollten die Daten das Subnetz nicht verlassen, da der Empfänger nicht außerhalb dieses zu finden ist, und würden somit auch nicht in das restliche Netz übertragen werden, um dieses zu belasten.

Die auf die OSI-Ebene 1 beschränkte Arbeitsweise eines Repeaters hat zur Folge, daß die Schichten 2 bis 7 nicht ausgewertet werden. Dies bedeutet, daß es für den Repeater keine Rolle spielt, welche Netzwerk-Software auf den über ihm liegenden Schichten eingesetzt wird. Er ist deshalb in dieser Weise universell einsetzbar.

Die Verbindung unterschiedlicher Netzwerk-Technologien (z. B. *Ethernet* und *Token Ring*) ist mit Repeatern nicht möglich. Sie können lediglich zur Erweiterung *eines* Netzwerktyps eingesetzt werden. So lassen sich beispielsweise Ethernet-Stränge mit Hilfe von Repeatern verlängern.

Die früher üblichen, einfachen Repeater-Arten werden heute zunehmend von aufwendigeren Typen abgelöst:

- **Multiport-Repeater** können nicht nur zwei, sondern mehrere Subnetz-Stränge koppeln
- **Sternkoppler** können als zentrale Kopplungseinheiten eingesetzt werden. Sie verbinden eine große Zahl von Netzsegmenten und sind zusätzlich in der Lage, verschiedenartige Medien miteinander zu koppeln. Ein Übergang von Kupfer- auf Glasfaserkabel wird dadurch auf einfachste Weise möglich.
- **Hubs** oder **Konzentratoren** sind aus der eben genannten Sternkopplertechnik entstanden. Zusätzlich zu der Möglichkeit, verschiedenartige Medien zu koppeln, sind in einen Hub weitere Module mit Bridge- oder Router-*Funktionalität* integriert. Dies macht sie zu universell einsetzbaren Koppelelementen, weshalb sie sich heute aus leistungsfähigen, komplexen Netzen nicht mehr wegdenken lassen.

DIE BRIDGE

Eine **Bridge** ist ein Netzübergang, der gemäß der Spezifikation auf der zweiten Ebene des OSI-Modells arbeitet. Hierbei ist die verwendete Technik etwas aufwendiger als

die von Repeater und erfordert normalerweise auch eigene Software. Eine Bridge ist meist ein kleines Bauteil mit eigener Schaltungslogik und Netzschnittstellen. Einige setzen aber auch bevorzugt einen ausgedienten PC, der mit der entsprechenden Software ausgestattet ist als Bridge ein.

Da die Bridge auf der OSI-Schicht 2 operiert (siehe Abbildung 2.1), sind für sie alle darüber aufsetzenden Protokolle transparent. Ihre Funktion ist deshalb unabhängig vom eingesetzten Protokoll, ob es sich dabei nun um *DECnet*-, TCP/IP-, *NetBIOS*- oder *IPX*-Protokolle handelt. Für die Funktionen einer Bridge entstehen dabei keine Unterschiede. Die verschiedenen Protokolle können alle mit der gleichen Bridge übertragen werden.

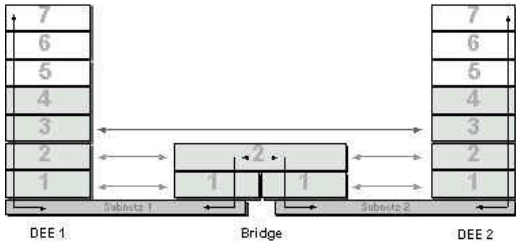


Abbildung 2.1: Eine Bridge arbeitet auf der zweiten Ebene des OSI-Modells

Diese Eigenschaft macht sie zu einem sogenannten "Plug-and-Play-Gerät", das nur eingebaut werden muß und nach dem Anschluß sofort funktionstüchtig ist. Eine aufwendige Konfiguration aller Netzteilnehmer, wie der Einbau von Routern es erfordert, ist bei Bridges nicht notwendig.

Eine Bridge läßt sich zur Verbindung *gleichartiger* Netze einsetzen. Bei dieser Verbindung unterscheidet man zwei verschiedene Typen:

- Die "normale" *MAC-Layer-Bridge* arbeitet in der unteren Hälfte der OSI-Ebene 2, der sogenannten ***M**edium **A**ccess **C**ontrol (MAC)*. Ihre Funktionalität entspricht den ursprünglichen OSI-Spezifikationen der Schicht 2. Damit die Bridge eingesetzt werden kann, muß (oberhalb der MAC) der Medienzugriff der beiden Subnetzte übereinstimmen. Die Verbindung eines *Ethernet* mit einem *Token Ring* wäre hier also nicht möglich.
- Es gibt aber auch Bridges, die oberhalb der MAC-Schicht eine Verbindung schaffen und somit Subnetze mit verschiedenartigen Medienzugriffsverfahren koppeln können. Die Kopplung erfolgt auf der Ebene der ***L**ogical **L**ink **C**ontrol (LLC)*. In einer solchen Bridge werden, im Gegensatz zu der MAC-Bridge, die MAC-Adressen auf das zweite Subnetz umgesetzt und die Datenpakete in das neue Format umgewandelt (*Translation*).

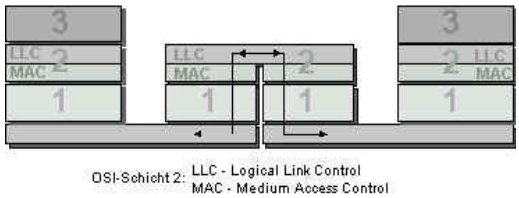


Abbildung 2.2: Bridges können auch verschiedenartige MAC verbinden

Im Vergleich zu *Repeatern* fällt bei Bridges ein höherer Arbeitsaufwand an, denn die Datenpakete werden erst auf der zweiten Ebene verarbeitet und weitergeleitet. Da Bridges also die Funktionalität der OSI-Ebene 2 bereitstellen müssen, benötigen sie eine größere Verarbeitungszeit. Das kann zur Folge haben, daß eine Bridge zum Engpaß (*Bottleneck*) eines Netzes wird und dieses stark verlangsamt. Daher müssen Bridges einerseits über ausreichende Ressourcen (z.B. Speicher) verfügen, andererseits sollte ihr Einsatz zuvor sorgfältig geplant worden sein.

MÖGLICHKEITEN UND EINSCHRÄNKUNGEN

Der Einsatz von Bridges in einem Netzwerk eröffnet einige neue Möglichkeiten:

- *Physikalisches Entkoppeln*, also eine Trennung von Netzsegmenten
- *Fehlerbegrenzung*, denn fehlerhafte Datenpakete werden von einer Bridge nicht weitergeleitet
- *Überschreitung hardwaremäßiger Längenrestriktionen*, denn Bridges empfangen und versenden alle Pakete die zwischen einzelnen Netzabschnitten ausgetauscht werden neu
- *Lastentrennung* auf Basis der MAC-Adressen, mit denen die Endstationen adressiert werden. Bridges werden daher auch *selektive Repeater* genannt. Die Möglichkeit, den Datenverkehr auf Subnetze zu begrenzen, ist sicherlich der entscheidenste Unterschied zum Repeater, der alle Datenpakete unabhängig von deren Ziel überträgt.

Jedoch dürfen auch die folgenden Einschränkungen einer Bridge nicht außer acht gelassen werden. Insbesondere grenzen sie die Funktionalität einer Bridge zu einem Router ab.

- Grundsätzlich transportiert eine Bridge Pakete auf *alle Ports* (Subnetzanschlüsse) mit Ausnahme desjenigen, auf dem sie die Pakete empfangen hat.
- Eine *echte* Lastentrennung kann nur dann erfolgen, wenn die Bridge, die in der Regel mit einem Selbst-Lern-Algorithmus ausgestattet ist, die Quell- und Zieladressen der Pakete richtig zuordnen kann. Ihre Informationen hierüber müssen deshalb stets auf dem neusten Stand sein.

FUNKTIONEN VON BRIDGES

Um die zuvor genannten Möglichkeiten realisieren zu können, muß eine Bridge folgende **Funktionen** aufweisen:

- Eine Bridge leitet, ähnlich wie ein Repeater, Daten weiter, es kommte jedoch zusätzlich noch die Aufgabe des *aktiven Filterns* der Daten hinzu. Nur Pakete, die eine MAC-Adresse einer Station außerhalb desjenigen Subnetzes aufweisen, aus dem sie kommen, werden transportiert.
- Die Bridge muß entsprechende Informationen über die Stationsadressen sammeln (*Selbst-Lern-Algorithmus*), damit sie überhaupt zur Lastentrennung und selektiven Übertragung in der Lage ist. Dazu muß sie über eine ausgeprägte Informationshaltung und ein Informationsmanagement verfügen, das ständige Auffrischungen erlaubt. Hierzu hält sich die Bridge eine Adreßtabelle, die die MAC-Adressen der in den verschiedenen Subnetzen erreichbaren Endstationen enthält. Mit ihrer Hilfe kann sie darüber entscheiden, ob ein Paket transportiert wird oder nicht.
- Bridges lassen sich einfach in ein Netzwerk aufnehmen, da die an das Netzwerk angeschlossenen Stationen nach wie vor die Adresse der Endstation als Zieladresse verwenden. Sie müssen deshalb beim Einsatz von Bridges nicht umkonfiguriert werden.

Durch die genannten Funtionen sind Bridges dazu geeignet den Datenverkehr zugunsten von höherer Sicherheit und verteilter Last zu begrenzen. Die dabei eingesetzten Funktionsweisen bewirken jedoch auch, daß es bei der Verwendung von Bridges zu Performance-Verlusten zwischen den verschiedenen Subnetzen kommt.

Der lokale Datenverkehr innerhalb eines Subnetzes gewinnt dagegen an Durchsatz, da es durch den Einsatz von Bridges nach außen abgeschlossen wird und somit das Gesamtdatenaufkommen in diesem Subnetz sinkt.

DIE VERSCHIEDENEN BRIDGE-TYPEN

Bridges gibt es in mehreren Varianten, die sich hinsichtlich ihrer Funktionalität und ihres Einsatzgebietes unterscheiden:

DIE LOCAL BRIDGE

Die Local Bridge hat zwei Ports, an welche jeweils der gleiche Netzwerktyp angeschlossen werden kann. Somit ist sie in erster Linie für die direkte Kopplung einzelner lokaler Subnetze z.B. innerhalb eines Unternehmens-Netzwerks geeignet. Sollen verschieden schnelle LAN's gekoppelt werden, so muß in der Bridge ein

ausreichend großer Pufferspeicher vorhanden sein, um die Geschwindigkeitsanpassung vornehmen zu können.

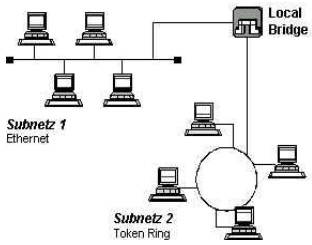


Abbildung 2.3: Verbindung eines Ethernet mit einem Token Ring via Local Bridge

DIE REMOTE BRIDGE

Die Remote Bridges dienen zur Anbindung an Weitverkehrsnetze (*WAN*) und haben dazu ein oder mehrere Anschlüsse für lokale Netzwerke und ein oder mehrere für den Weitverkehr (*Remote Ports*). Mittlerweile erfolgt der Anschluß an ein WAN oder ein *Backbone*-Netz eigentlich immer über ein LAN. Deshalb treten Remote Bridges meist paarweise auf, denn für den erneuten Übergang vom Weitverkehrs- bzw. Backbone-Netz in das LAN der Empfängerstation wird abermals eine Bridge benötig.

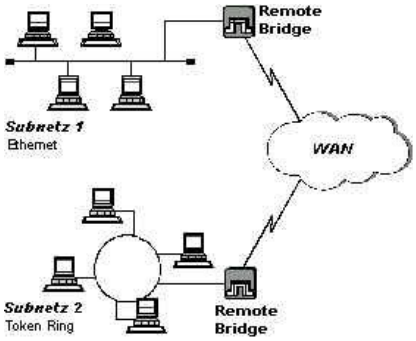


Abbildung 2.4: WAN-Anbindung zweier Subnetze über Remote Bridges

Remote Brdiges müssen besonders Leistungsfähig sein, da sie meist Netzwerke mit den verschiedensten Anforderungen koppeln müssen.

DIE MULTIPORT BRIDGE

Eine Multiport Bridge wird in erster Linie zur Strukturierung von Netzen eingesetzt. Mit ihren drei oder mehr Netzanschlüssen läßt sie sich hervorragend für eine intelligente Sternkopplung einsetzen.

Im Gegensatz zu einem Sternkoppler mit Repeater-Funktion wählt die intelligentere Bridge zum Weiterleiten der Datenpakete nur den Port aus, über den die Zielstation erreichbar ist, und trägt somit wiederum zur Lastverteilung bei.

Eine Bridge, die mindestens genauso schnell, wie das *Interface* ist, wird **wirespeed** genannt. Multiport Bridges werden auch als **Brigding-Hubs** bezeichnet und wirespeed Bridging-Hubs werden auch **Switches** genannt.

Für Multiport Bridges kommen nur Mehrprozessorsysteme in Frage, da es sonst schnell zu Engpässen in der Datenweiterleitung führen kann. Trotzdem sind sie sehr beliebt, da man z.B. ältere Netze mit neuen schnelleren Netzen verbinden kann.

DER ROUTER

Router sind Netzübergänge, die Bridges ähneln, jedoch etwas intelligenter und komplexer sind. Sie arbeiten nach der Spezifikation des OSI-Modells auf Ebene drei. Während Bridges hinsichtlich des Protokolls nach oben hin transparent sind, sind Router vom eingesetzten Netzwerkprotokoll abhängig. Sie verhalten sich viel mehr ergänzend im Hinblick auf die Protokollabhängigkeit zu Bridges, denn Router bieten den auf ihnen aufsetzenden Protokollen eine Schnittstelle nach unten, unterhalb derer verschiedene LAN relativ einfach austauschbar sind.

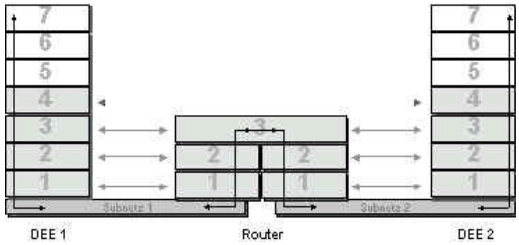


Abbildung 3.1: Router arbeiten nach der Spezifikation des OSI-Modells auf Ebene 3

Die wichtigste Funktion eines Routers ist die die Wegwahl von Sender zu Empfänger, genannt **Routing**. Hierzu gehört der Aufbau, das Aufrechterhalten und der Abbau einer geordneten Ende-zu-Ende-Verbindung. Um das Routing durchführen zu können muß der Router die eingesetzten Netzwerkprotokolle verstehen können, da die Wegwahl für ein TCP/IP-Paket anders vollzogen wird als beispielsweise für ein *IPX-Paket* eines Novell-Netzwerkes.

Router müssen alle Protokolle, die über sie geroutet werden, verarbeiten können, da sie auf der OSI-Ebene drei arbeiten. Denn eigentlich braucht jedes Protokoll seinen eigenen Router, der die spezifischen Ebenen eins bis drei des Protokolls interpretieren kann. Da vor allem in heterogenen Netzwerken meist nicht nur ein Protokoll im Einsatz ist wurden spezielle **Multiprotokoll-Router** entwickelt, die mehrere Protokolle verarbeiten können.

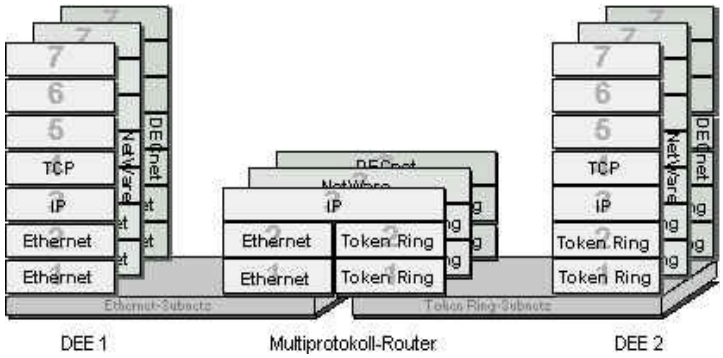


Abbildung 3.2: Multiprotokoll-Router können mehrere Protokolle verarbeiten

Damit Multiprotokoll-Router mehrere Protokolle verarbeiten können besitzen sie für jedes, welches im lokalem Netz vorkommt, einen eigenen *Protokoll-Stapel*. Auf diesen wird dann, abhängig von der Adresse des Datenpaketes, verzweigt und die entsprechende Protokollroutine aufgerufen, die das Routing vornimmt.

DIE ADRESSIERUNG BEIM EINSATZ VON ROUTERN

Ein Router stellt die Verbindung zwischen den netzabhängigen *Transport*protokollen, also der Infrastruktur, und den hostabhängigen *Anwendungs*protokollen dar. Er muß in einem Netzwerk *direkt* von den Teilnehmerstationen adressiert werden, sonst überträgt er Datenpakete nicht, denn einen grundsätzlichen Transport gibt es bei ihm nicht. Hier erkennt man den deutlichen Unterschied zur Bridge, die keine eigene Adressierung im Netz benötigt und alle ankommenden Pakete weiterleitet.

Daß die Datenpakete sicher an ihrer Zielstation ankommen, überwacht die oberhalb von Routern gelegene *Transportschicht*. Sie ist damit gleichzeitig die unterste Schicht, die eine eigene virtuelle Verbindung direkt zur Zielstation unterhält und die Ende-zu-Ende-Adressierung vornimmt.

Auf der tiefer liegenden MAC-Ebene hingegen findet immer nur eine Adressierung bis zum Nächsten Übertragungsgerät statt:

- von der Sendestation zum ersten Router, dann
- von Router zu Router und schließlich
- vom letzten Router zur Empfängerstation.

Der Router interpretiert die MAC-Adressen und setzt sie auf das neue Subnetz um. Jedoch transportiert er Pakete nur dann, wenn sie Zieladressen von Subnetzen enthalten, die er kennt. Pakete, die zwar an ihn adressiert wurden, die er aber keinem Subnetz zuordnen kann, werden von ihm entweder gelöscht oder als fehlerhaft markiert und zurückgeschickt.

Sowohl Router als auch Bridges müssen Adreßinformationen speichern, um Datenpakete weiterleiten zu können. Das Speichern erfolgt in einer Tabelle, deren Größe bei *Routern* der Anzahl der Subnetze und bei *Bridges* der Anzahl der Stationen entspricht.

Ein großer Nachteil von Routern besteht jedoch darin, daß es schwierig ist ihn in ein bestehendes Netz einzubinden. Da sie direkt adressiert werden müssen, muß in jeder einzelnen Station ein hoher Konfigurationsaufwand hingenommen werden.

MERKMALE UND EINSATZMÖGLICHKEITEN

Router besitzen die Fähigkeit, das Datenaufkommen zwischen einzelnen Netzen wirkungsvoll zu minimieren. Die Verkehrsbegrenzung erfolgt hierbei auf der Basis der logischen Netzunterteilung durch einen vollkommen adreßabhängigen Transport.

Außer durch das Entkoppeln von Subnetzen kommt es auch durch die *dynamische Wegwahl* zur Entlastung des Gesamtnetzwerkes. Denn wenn mehrere alternative Routen zu eine Zielstation zur Verfügung stehen wählt der Router den optimalen Weg abhängig von der augenblicklichen Netzauslastung und den zu erwartenden Kosten. Somit wird nicht nur die Netzwerksicherheit verbessert, sondern auch die Auslastung des Netzes verringert.

Router weisen folgende Funktionen auf:

- Anlegen und Aktualisieren einer *Routing-Tabelle* mit Informationen über Adressen, Wege, Netzauslastung und Kosten
- Informationsaufnahme zum Aktualisieren der Tabelle, sowie die Informationsweiterleitung zu anderen Routern
- Wegewahl für Datenpakete (*Routing*), worum sich nun nicht mehr die Endgeräte kümmern müssen.

Router eignen sich besonders für die Verbindung von lokalen und Weitverkehrsnetzen. Vor allem die LAN-Kopplung über WAN-Leitungen läßt sich durch den Einsatz von Routern optimieren.

DAS GATEWAY

Ein **Gateway** (*"Transitsystem"*) ist ein Rechner, meistens sogar ein Zentralrechner, welcher vollkommen unterschiedliche Netze koppeln kann. Gateways arbeiten auf

einer Ebene oberhalb der dritten OSI-Schicht, je nach Größe des Unterschieds der beiden zu koppelnden Netze (siehe Abbildung 4.1).

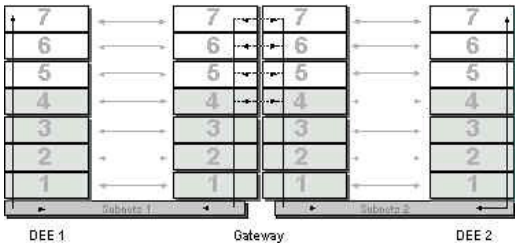


Abbildung 4.1: Gateways arbeiten in den OSI-Schichten 4, 5, 6 oder 7

Sie werden benötigt, um herstellerspezifische Protokolle ineinander umzusetzen und eine hersteller-übergreifende Kommunikation zu ermöglichen. Für die angeschlossenen Subnetze ist das Gateway ein direkt adressierbarer Rechner (*Knoten*) innerhalb des Gesamtnetzwerks, der

- die Adreß- und Formatumsetzungen,
- Konvertierungen,
- die Flußkontrolle und
- eventuell notwendige Geschwindigkeitsanpassungen für den Übergang in das jeweils andere Subnetz übernimmt.

Zur Ankopplung von PC's in lokalen Netzwerken (LAN) an Host-Systeme (z.B. *IBM* oder *Siemens-Mainframes*) oder öffentliche Weitverkehrsverbindungen (z.B. WAN-Verbindungen der Telekom) werden beispielsweise Gateways gebraucht.

Gateways sind also Netzübergänge, die nicht, wie Router und Bridges, primär zur Strukturierung und Lastverteilung in einem Netzwerk eingesetzt werden, vielmehr ist ihre Hauptaufgabe die Anpassung unterschiedlicher Netzwerktypen.

Hinzu kommt außerdem noch, daß mit der Hilfe von Gateways Sicherheitsfunktionen auf Applikationsebene (firewalls) implementiert werden können, was einen wichtigen Vorteil gegenüber anderen Netzübergängen darstellt.

DIE PROTOKOLLE

WIE ALLES ANFING .....

Die DARPA , eine Unterorganisation des amerikanischen Verteidigungsministeriums finanzierte in den 60er Jahren ein Forschungsprojekt mit dem Inhalt, herauszufinden, wie man Computer zur Datenübermittlung verbinden kann, um im Falle eines nuklearen Angriffs die Befehls- und Kommunikationsstrukturen aufrecht erhalten zu können.

Ein Unternehmen in Massachusetts, die Bolt Beranek&Newman Inc, installierte ein erstes Testnetzwerk, das ARPANET. Zu Beginn der 70er Jahre umfaßte das ARPANET bereits über 50 Computer in den USA und Westeropa. Bolt Beranek&Newman verwaltete das Steuerzentrum für das Netzwerk, das sogenannte NOC.

In der Mitte der 70er war das Netzwerk bereits so groß geworden, daß die DARPA anfing, nach Möglichkeiten zu suchen, wie man weitere Netzwerke bauen und miteinander verbinden kann. Der Bedarf nach höheren Netzwerkkapazitäten führte zur Entwicklung von Techniken wie Token Ring und Ethernet sowie zur Weiterentwicklung der Satelliten- und Funkkommunikation.

Mit dem Wachstum des Netzes begannen seine Benutzer das Netz auch für nicht-militärische Zwecke zu verwenden. Die Hauptbenutzer waren immer noch die Universitäten sowie das Militär und Regierungsorganisationen. Aber diese fingen an, das Netzwerk für den Austausch aller Arten von nicht-millitärischer Informationen, Dateien und Dokumente zu benutzen.

Auch wurde das Netz immer größer, der Datenverkehr nahm im Netz immer weiter zu und somit auch der Verwaltungsaufwand.
Somit wurde das ARPNET schließlich in zwei separate Netzwerke gespalten :

das MILNET für militärische Installationen
und ein neues ARPANET für zivile Einrichtungen

Beide Netze waren jedoch immer noch miteinander verbunden. Das IP lenkte den Verkehr von einem Netzwerk zum anderen und verband damit das neue ARPANET mit dem MILNET.

Im Jahre 1975 übernahm schließlich die DCA die Kontrolle über das ARPANET.

DIE GEBURT EINES PROTOKOLLS ...

DARPA finanzierte die Entwicklung einer ganzen Reihe von Protokollen für die Kommunikation im ARPANET. Das Ergebnis war ein Protokoll aus zwei Komponenten, TCP und IP, aus denen der Name TCP/IP zusammengesetzt ist. Die Protokolle wurden so entworfen, daß mit ihnen mehrere Netzwerke verbunden werden konnten, obwohl es am Anfang nur zwei Netzwerke gab - MILNET und ARPANET. IP hätte jedoch bereits Tausende von Netzwerken miteinander verbinden können. Diese Fähigkeit ist einer der Gründe dafür, daß TCP/IP heute noch so weit verbreitet ist.

Als die Entwickler des UNIX-Betriebssystem an der University of California at Berkeley TCP/IP in ihr Software-Distribution-Kit (BSD Unix) aufnahmen, begann TCP/IP - besonders in akademischen Umgebungen - sehr schnell zu wachsen. Schließlich hatten die Universitäten damit ein, zumindest softwareseitig - kostenloses Werkzeug zur Vernetzung ihrer Computer in der Hand. Die Entwicklungsgruppe in Berkeley fügte den Protokollen ein API sowie einen Satz von Werkzeugen und Utilities zur Nutzung des Internets hinzu.

In den frühen 80er Jahren schrieb das amerikanische Verteidigungsministerium vor, daß alle Computer, die mit ARPANET verbunden sind, TCP/IP einsetzen müssen.

Das war der Zeitpunkt, zu dem das Internet entstand - "und das ARPANET aufhörte, DAS NETZ zu sein, und das Internet DAS NETZ wurde."

ISO/OSI

ISO spezifiziert weltweite Standards für DV-Bereiche - unter anderem Standards für Vernetzung, den Datenbankzugriff und Zeichensätze und anderes. Neben der ISO gibt es noch viele andere Standards-Organisationen. Dazu gehört zum Beispiel das ANSI, oder das DIN.

Die Produkte der führenden Hardware- und Software-Hersteller müssen gewisse Standards erfüllen, um das Konzept der offenen Systeme zu unterstützen. Im Bereich Netzwerke und Protokolle erwartet die ISO von allen Herstellern, daß sie bei der Entwicklung ihrer Produkte eine Standardnetzwerkarchitektur zugrunde legen um beispielsweise die Kommunikation auch zwischen Usern mit unterschiedlicher Hard- oder Software zu ermöglichen.

Der bekannteste Standard der ISO, um diese Kompatibilität von Netzwerken und Protokollen zu erreichen, heißt OSI. Dieser Standard umfaßt eine Netzwerkarchitektur und einen kompletten Protokollsatz.

Doch ISO ist nicht die erste Organisation, die ein Netzwerkmodell und die zugehörigen Protokolle definiert hat. Hier sind drei alternative, herstellerspezifische Netzwerkmodelle und Protokolle :

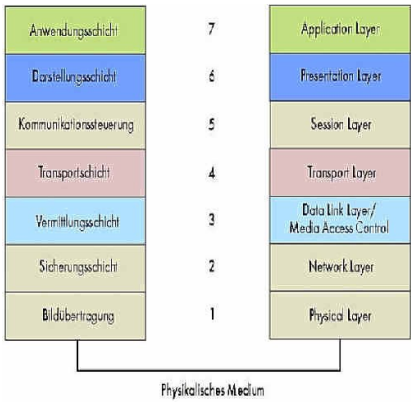
HERSTELLER	ARCHITEKTUR/PROTOKOLL
IBM	System Network Architecture (SNA)
Digital Equipment Copr.	Digital Network Architecture und DECnet
Apple Computer	AppleTalk

Der Unterschied zwischen diesen herstellerspezifischen Standards und dem ISO-Standard liegt darin, daß der ISO/OSI die Zusammenarbeit der Hardware verschiedener Hersteller ermöglicht.

Um das Ziel zu erreichen, daß alle Teile ihres Netzwerkes unabhängig von ihrem Hersteller zusammenarbeiten, gliedert OSI die Netzwerkfunktionen in Schichten und legt fest, wie die Schichten miteinander kommunizieren sollen.

DAS ISO/OSI-REFERENZMODEL

Es gibt sieben Schichten in dem Entwurf der ISO, auch als Stack bezeichnet, die jeweils eine spezielle Funktion erfüllen. Die unteren Schicht ist hardware-orientiert und beschäftigen sich unter anderem damit, wie die Übertragung stattfindet. Die oberste Schicht beschäftigt sich mit den Aufgaben des Users, wie zum Beispiel die Dateiübertragung und E-mail.



SCHICHT 1: PHYSICAL LAYER

Die erste Schicht ist die reine Hardware inklusive der Kabel, Satelliten, Netzwerkschnittstellenkarte(n) und anderer Verbindungsmedien.

SCHICHT 2: NETWORK LAYER

Die Vermittlungsschicht oder Netzwerkschicht ist die erste Schicht im OSI-Modell, zu der es eine entsprechende Schicht in den TCP/IP-Protokollen gibt. IP ist das Protokoll, das aus dieser Schicht kommt. Diese Schicht bekommt Pakete von dem Data Link (2. Schicht) und sendet sie an die korrekte Netzwerkadresse. Wenn es mehrere mögliche Übertragungswege für die Daten gibt, ermittelt diese Schicht ebenfalls den effektivsten Weg. Sie ist somit für das Ankommen der Daten am richtigen Ort verantwortlich.

SCHICHT 3: DATA LINK LAYER

Das ist die Schicht, die die Daten in Pakete zerlegt, die über das Übertragungsmedium übertragen werden sollen. Hier werden Token Ring- oder Ethernet-Verkabelungen verwaltet.Auch sie basiert auf Hardware.

SCHICHT 4: TRANSPORT LAYER

Wenn die Daten an ihren Bestimmungsort gelangen, ist es möglich, daß Paket4 eher da ist als Paket3 oder das ein Paket möglicherweise beschädigt ist. Diese Schicht hat die Aufgabe sicherzustellen, das die Pakete keine Fehler enthalten, daß alle Pakete ankommen und daß sie die richtige Reihenfolge haben. TCP beispielsweise ist ein Protokoll aus dieser Schicht; ein weiteres wäre UDP.

SCHICHT 5: SESSION LAYER

Die anderen Protokolle von TCP/IP-Protokollen sind in dieser und den darüber liegenden Schichten angesiedelt. Diese Schicht ist für die Einrichtung und Verwaltung einer Verbindung von zwei Computern (sogenannte Sessions) zuständig. Dies ist die Vorbedingung für eine Übertragung von Daten.

SCHICHT 6: PRESENTATION LAYER

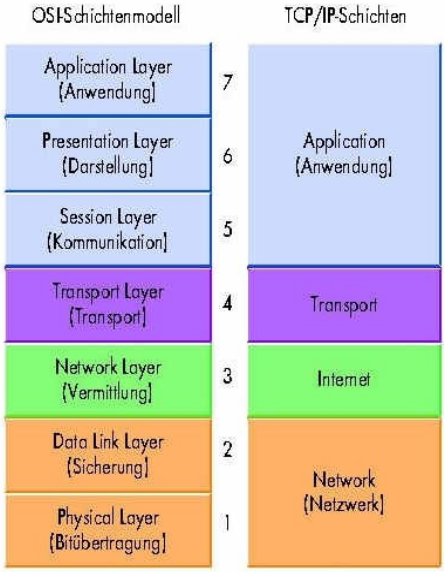
Diese Schicht arbeitet eng mit dem Betriebssystem und dem Dateisystem zusammen. Hier werden Dateien in das jeweilige Format umgewandelt, sollten Server und Client verschiedene benutzen. Somit ist der Dateitransfer zwischen Computern mit verschiedenen Dateiformaten gewährleistet.

SCHICHT 7: APPLICATION LAYER

Mit dieser Anwendungsschicht werden beispielsweise E-mails gesendet oder Dateien über das Netzwerk übertragen. Ohne diese Schicht hätte der Computer keine Verwendung für die an sie übertragenen Daten.

TCP/IP

DAS TCP/IP-REFERENZMODELL



Hier im Vergleich das OSI-Schichtenmodell zu den TCP/IP- Schichten.

TCP/IP ist eine Sammlung von Protokollen, die nach zwei der ursprünglichen Bestandteile, TCP und IP benannt wurde. Ähnlich wie das OSI-Referenzmodell bilden die Protokolle von TCP/IP eine Abfolge von mehreren Schichten. Die Abbildung zeigt, daß das TCP/IP- Modell vier Schichten hat. Die vierte Schicht, die als Anwendungsschicht (Application Layer) bezeichnet wird, ist hier eine Kombination aus Kommunikations-, Darstellungs- und Anwendungsschicht des OSI-Modells. Die dritte Schicht von TCP/IP ist zwar die Internetschicht, entspricht aber der OSI-Vermittlungsschicht.

Die Bitübertragungsschicht und die Sicherungsschicht des OSI-Modells sind in den Schichten des TCP/IP-Modells enthalten, obwohl sie nichts mit TCP/IP zu tun haben. TCP/IP IST SOFTWARE(!), die unabhängig von der zugrundeliegenden Hardware ist. Man sollte jedoch nicht vergessen, daß die Hardware ein Teil der Gesamtlösung darstellt.

Normalerweise werden TCP/IP-Daten immer über ein vorhandenes Trägernetz wie Ethernet oder TokenRing übertragen, denn die Aufgabe von TCP/IP ist ja gerade, die Verwendung solcher Netzwerke zu vereinheitlichen. Da die Internet-Schicht die erste Abstraktionsschicht von einem konkreten Netzwerk darstellt, ist das IP somit der Kern von TCP/IP. Diese Schicht stellt nämlich den grundlegenden Dienst des Netzes zur Verfügung - den Versand von Datenpaketen, die auch Datagramme genannt werden.

Die Netzwerkschicht hat keine Informationen darüber, von welcher Art die Daten sind, die sie befördert. Für eine Ethernet-Karte sind die ankommenden Daten einfach nur Daten, die vom Netz kommen. Diese Daten eines IP- Pakets werden vom Kartentreiber als IP-Header und als Datenteil interpretiert. Auf diese Weise ist der IP-Header

innerhalb eines Ethernet-Paketes sozusagen eingewickelt. Aber auch das IP-Paket selber enthält wieder ein Datenpaket für eine höhere Protokollebene, dessen Header auf der IP-Ebene als Bestandteil der Daten (das heißt, im Datenteil) erscheint.

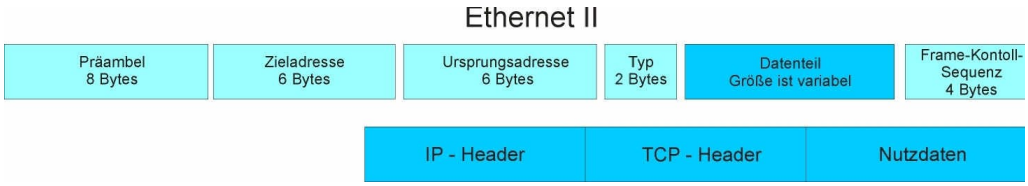
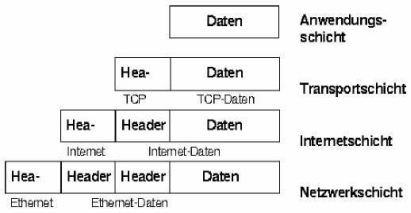


Abb.: Aufbau eines Ethernet Paketes mit der Größe der einzelnen Bestandteile und der Aufsplitung des Datenteils.

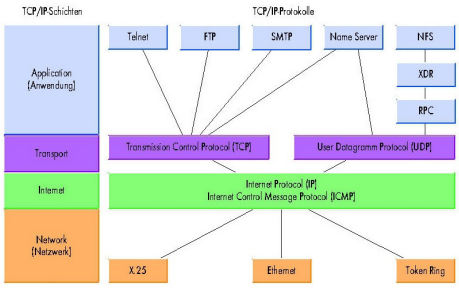


Hier ist noch einmal veranschaulicht, wie die Pakete in den einzelnen Schichten aussehen und aufgebaut sind.

Das Paket, das die Netzwerkschicht bearbeitet, besteht aus dem Ethernet-Header und einem Datenteil. Dieser Datenteil wird nun an die nächst höhere Schicht weitergereicht. Dort wird nun wieder ein Teil der Daten als Header und der Rest als Datenteil interpretiert, und weiter an die nächst höhere Schicht gereicht wird.

Das geht solange, bis alle Schichten bis zur obersten durchlaufen wurden, und diese nun die reinen Daten erhält.

PROTOKOLLE IN TCP/IP



TCP/IP enthält sehr viele Komponenten, und es kommen ständig weitere hinzu. Hier möchten wir nun einige der bekanntesten, der wichtigsten, die sichtbarsten und die am häufigsten verwendeten kurz vorstellen. Wie bereits erwähnt gibt es viele Komponenten, oder auch Protokolle für die einzelnen Schichten des TCP/IP-Modells. Diese Komponenten basieren jedoch auf den jeweils unter ihnen liegenden Schichten. Da sie auch miteinander arbeiten/kommunizieren müssen sind die einzelnen Komponenten in den sogenannten RFC genormt und offengelegt.

DAS IP PROTOKOLL

Das Internet Protocol ist für die Verbindung im Netz zuständig. Der Kern von IP arbeitet mit Internet-Adressen. Jeder Computer in einem TCP/IP-Netzwerk besitzt eine numerische Adresse. Das IP weis, wie Nachrichten zwischen diesen Adressen ausgetauscht werden. IP kümmert sich somit um die Adressierung - ob die Daten nun korrekt und in einem Stück am Ziel ankommen ist Aufgabe eines anderen Protokolls.

Dies gilt sowohl für IPv4 (IP Version 4) als auch für IPv6 (ursprünglich als IPnG bezeichnet).

DAS ICMP PROTOKOLL

Dieses Protokoll teilt Probleme mit und überträgt andere netzwerkspezifische Informationen, wie zum Beispiel den Fehlerstatus eines Netzwerkgerätes. Das IP entdeckt den Fehler und leitet ihn an das ICMP weiter. Eine gebräuchliche Verwendung von ICMP ist die Verarbeitung der Echoanforderung, die der Ping-Befehl erzeugt.

DAS TCP PROTOKOLL

TCP ist dafür verantwortlich, daß keine Daten, egal von welcher Art, verlorengehen. TCP sorgt für einen verläßlichen Datenstrom zwischen den Computern im Netzwerk und benutz IP, um Pakete an die Anwendungen der oberen Schicht zu senden. Zu den wichtigeren Funktionen von TCP gehört aber die Fehlerprüfung und die Nummerierung von Paketen, damit die richtige Reihenfolge gewährleistet wird. Ist ein Paket an der richtigen IP-Adresse angekommen, stellt TCP auf der Sende- und Empfangsseite einen Dialog her, um das Empfangen zu bestätigen oder notfalls den Host auffordert, das Paket erneut zu übertragen. Deshalb wird TCP auch verbindungsorientiert (connection oriented) bezeichnet.

DAS UDP PROTOKOLL

Dieses Protokoll sorgt ebenso wie TCP für den Reibungslosen Datenfluß und benutzt ebenfals IP, um an die oberen Schichten Pakete zu senden. Jedoch führt UDP keine Fehlerprüfung und keine Nummerierung der Datenpakete durch. Ebenfals fordert es keine erneute Sendung des Paketes im Falle eines Fehlers an. Deshalb ist UDP ein verbindungsloses (conectionless) Protokoll. Anwendungsprogrammierschnittstellen von NFS, von DNS oder von RPC arbeiten zum Beispiel mit dem UDP

DAS FTP PROTOKOLL

FTP ist eigentlich mehr als ein Protokoll, nämlich zusätzlich noch eine Anwendung und ein Dienst. Mal angenommen, sie müssen eine Datei von einem Remote-Computer kopieren. Ohne die Anwendung weiß ihr Computer nicht, daß sie kopieren wollen und ohne den Dienst erhalten sie keine Verbindung zu dem Remote-Computer,

auf dem sich die Datei befindet. Und zu guterletzt können ohne das Protokoll der Client und der Server nicht miteinander kommunizieren. Nur soviel dazu, wir beschränken uns kurz und knapp auf das Protokoll, das nämlich für das Kopieren von Dateien da ist. FTP wird von der Client- und der Serveranwendung dazu verwendet um sicherzustellen, das die Kopie und das Original Bit für Bit übereinstimmen.

Das ARP Protokoll

Das ARP ermittelt die Hardware-Adresse der Netzwerkschnittstellenkarte eines Computers, wenn von diesem nur die TCP/IP-Adresse bekannt sein sollte. Dieses Protokoll kennt die Adressen der Geräte im Netz und arbeitet eng mit dem IP zusammen.

Das RARP Protokoll

Dieses Protokoll macht das gleiche umgedreht wie das ARP - es ermittelt die TCP/IP-Adresse des Computers, wenn nur die Hardware-Adresse der Netzwerkschnittstellenkarte bekannt sein sollte.

Das SMTP Protokoll

Ein Protokoll, daß E-mails im Internet überträgt. Die Nachrichten können direkt von dem Computer des Absenders zum Computer des Empfängers übertragen werden oder über einen Zwischencomputer geleitet werden. Dieses Verfahren wird als speichern und weiterleiten (store and forward) bezeichnet.

Das POP3 Protokoll

POP3 wurde entwickelt, um Privatbenutzern die Möglichkeit zu geben, E-mails vom Computer ihres ISP herunter laden zu können.

Das HTTP Protokoll

Dieses Protokoll überträgt Dokumente, die in HTML (wie der Stuff den sie gerade lesen) geschrieben wurde, und andere Komponenten von einem Server im WWW zu seinem Browser-Client.

Das BOOTP Protokoll

Mit diesem Protokoll können sie das Betriebssystem über das Netz von einem anderen Computer laden. Dies wird beispielsweise genutzt, wenn man mit Diskless-Computern (Rechner ohne Festplatte) in einem Netzwerk arbeitet.

Das PPTP Protokoll

Dieses Protokoll wird verwendet, um im Internet ein VPN aufzubauen. Somit kann man eine sichere Verbindung (verschlüsselte Übertragung möglich) zum Netzwerk

der jeweiligen Organisation aufbauen, ohne die all die Vorteile eines globalen Privaten Netzwerkes missen zu müssen. Das Verlegen von eigenen Unterseekabeln oder das Starten von eigenen Satelliten entfällt. Die Verbindung selbst wird normal über das Internet und einem ISP hergestellt.

Das DHCP Protokoll

Das DHCP ist eine Client/Server-Lösung für die dynamische Verteilung von IP-Adressen. Ein sogenannter DHCP-Server verwaltet einen Pool von Adressen, aus dem er dem DHCP-Client eine zuteilt, wenn dieser sich anmeldet. Diese wird nun als benutz markiert und erst wieder frei gegeben, wenn der Client seine Arbeit beendet und die Adresse wieder freigegeben hat. Man kann die Nutzung der IP-Adresse aber auch zeitlich begrenzen. Das heißt der Host muß diese vor Ablauf der Zeit verlängern lassen oder, wenn dies nicht genehmigt wird sich erneut anmelden.

TCP/IP-Adressierung

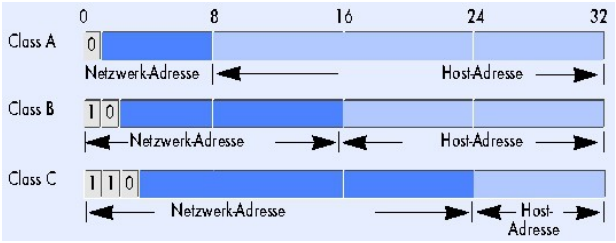
TCP/IP und das Internet verlangen, daß alle Computer im Netz (=Hosts), in der Organisation, in der ganzen Welt und im Sonnensystem sowohl durch ihren Namen als auch durch ihre Adressen eindeutig identifiziert werden.

Die IP-Adressen

Jedes IP-Paket enthält zwei Adressen in 32-Bit-Zahlen, die Absender- und Empfängeradresse. Die Internet Adresse wird in Form von vier, durch Punkte getrennte Bytes (=acht Stellen) notiert. Man spricht in diesem Fall von der 'Dotted-quad-Schreibweise'. Ein Byte entspricht einem Feld (vier pro Adresse) und kann in dezimaler Schreibweise ('Dotted Decimal Notation') eine Zahl von 0 bis 255 darstellen.

Um die Zustellung von IP-Paketen zu vereinfachen, unterteil man die Adresse in zwei Teile - den Netzwerkteil und den Rechnerteil. Ein Router muß, um ein Datenpaket zustellen zu können, nur den Netzwerkteil einer Adresse kennen. Den anderen Teil wertet erst das Zielnetzwerk des Paketes aus.

Da es jedoch verschieden große Netzwerke gibt, mit vielen oder wenigen Host, gibt es verschiedene Aufteilungen des 32-Adreßbits.



CLASS A - NETZWERKE

Theoretisch kann es nur 127 Netzwerke diesen Typs geben. Dafür kann jedes dieser Netzwerke eine riesige Anzahl von Hots umfassen: um genau zu sein 16.777.216. Es gibt nur sehr wenige Organisationen, die ein Netzwerk der Klasse A benötigen, ein typischer Vertreter ist wäre aber zum Beispiel das amerikanische Milnet. Übrigens ist das gesammte Class-A-Netzwerk mit der Nummer 127 reserviert. Somit bleiben nur 126 Netzwerke der Klasse A übrig.

CLASS B - NETZWERKE

Obwohl die Netzwerke der Klasse B nicht annähernd so riesig sind wie die Netzwerke der Klasse A, so können sie immer noch 65.536 Hosts umfassen. Solche Netzwerke werden meistens von Universitäten und großen Unternehmen benötigt. Insgesamt gibt es rund 16.384 solcher Class-B-Netzwerke.

CLASS C - NETZWERKE

Netzwerke dieser Klasse umfassen nur 256 Hosts (tatsächlich jedoch nur 254; die Nummern 0 und 256 sind reserviert), jedoch gibt es davon rund 2 Millionen (2.097.152) im Internet. Standardmäßig erhält man ein solches Class-C-Netzwerk, wenn man ein Netzwerk bei NIC anmeldet.

CLASS D - NETZWERKE

Netzwerke dieser Klassen unterscheiden sich grundlegend von den anderen Klassen - sie werden für das sogenannte Multicasting verwendet. Die Class-D-Adressen reichen von 224.0.0.0 bis 239.255.255.255.

SUBNETZE UND SUBNETZMASKEN

Subnetze zerlegen ein Netzwerk in mehrere kleinere Netzwerke. Die separaten Netzwerke sind meistens durch Netzwerkrechner, genannt Router, verbunden.

Wenn sich der Administrator einige Bits vom Host-Abschnitt der Adresse des Hauptnetzwerkes sozusagen "borgt", so muß er TCP/IP mitteilen, welche Bits des Host-Abschnitts "geborgt" wurden, um als Netzwerkadresse zu dienen. Hier kommt die Subnetmask zum Einsatz. Eine Subnetmask besteht genauso wie die IP-Adresse aus 32 Bits. Die Bits der Netzwerkadresse sind auf den Wert 1, die Bits der Hosts-Adresse sind auf 0 gesetzt (siehe Boolsche Arithmetik).

Der Netzwerknummernteil einer IP-Adresse wird nun mit Hilfe einer Subnetmask isoliert. In dem Computer werden die Felder der für sie dezimal angezeigten IP-Adresse, zum Beispiel 192.168.100.7 bereits binär in folgender Form dargestellt:

11000000 10101000 01100100 00000111

Die Felder der dezimal dargestellten Subnetzmaske 255.255.255.0 haben bereits die Form

11111111 11111111 11111111 00000000

Die AND(oder UND-)Operation ergibt die Netzwerknummer 192.168.100, und zwar so:

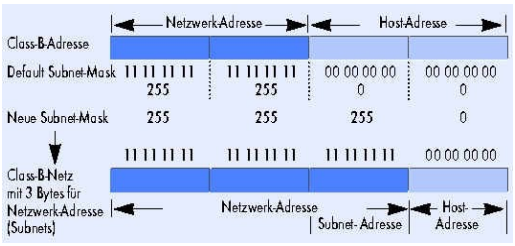
11000000 10101000 01100100 00000111	IP-Adresse: 192.168.100.7
11111111 11111111 11111111 00000000	Subnetzmaske: 255.255.255.0
11000000 10101000 01100100 00000000	Ergebnis: 192.168.100.0

Um die Host-Nummer zu ermitteln, kehrt der Computer die Bits der Subnetmaske einfach um - das heißt, jede 1 wird zur 0 und jede 0 zur einer 1 - und führt anschließend eine weitere UND-Operation aus.

11000000 10101000 01100100 00000111	IP-Adresse: 192.168.100.7
00000000 00000000 00000000 11111111	Subnetzmaske: 0.0.0.255
00000000 00000000 00000000 00000111	Ergebnis: 0.0.0.7

Hier eine Beispiel für ein Class-B-Netzwerk und die Verwendung von Subnet-Masks:

In einem Netzwerk mit beispielsweise der Nummer 192.168.100 gibt es genau 127 Adressen, bei denen das 8.Bit (high-order Bit) - bedenken sie bitte, das man von links anfängt mit zählen - im 4. Feld den Wert 0 hat und ebenso 127 Adressen, bei denen es den Wert 1 hat. Somit wäre die angepaßte Subnetmask nicht 255.255.255.1, da hier das 1. Bit des 4. Feldes geborgt wird, sondern 255.255.255.128. Somit werden alle



Host mit den Nummern 1 bis 127 den ersten Subnetz und die Host mit Nummern größer als 128 dem zweiten Subnetz zugeordnet. Am häufigsten wird die Subnetzbildung wahrscheinlich in Organisationen benutzt, die ihr Netzwerk der Klasse B in 256 Subnetze der Klasse C zerlegen. Um dies zu bewerkstelligen, setzt jeder Host seine Subnetzmaske auf 255.255.255.0.

ANMERKUNG :

Die Notwendigkeit, Subnetze zu bilden macht IPv6 mit einer erweiterten Adresse überflüssig.

Natürlich geht das ganze auch andersrum, indem man sich aus dem Netzwerknummernteil der Adresse Bits für den Host-Nummernteil leiht. Somit könnte man Beispielsweise zwei oder mehr Netzwerke der Klasse C verbinden zu einem sogenannten Supernetz, für die es dann ebenso Supernetzmasken gibt. Das würde aber hier zu weit ausschweifen. Vielleicht können wir das später ergänzen.

ZUSATZINFORMATIONEN

DIE BOOLSCHE ARITHMETIK

Das Prinzip, nachdem ein Computer arbeitet ist das Binärsystem, da es sich am einfachsten darstellen läßt. Für ihn gibt es nur zwei Zustände - AN, d.h. 1 oder AUS, d.h. 0.

DAS BINÄRSYSTEM

Eine Binärzahl besteht also nur aus Einsen und Nullen, zum Beispiel 00011011. Bei dieser Zahl besitzt jede Stelle (jedes Bit) einen bestimmten Wert.

binäre Zahl	0	0	0	1	1	0	1	1
Bit	***7***	***6***	***5***	***4***	***3***	***2***	***1***	***0***
Wert	128	64	32	16	8	4	1	0

Die Dezimale Zahl erhält man, indem man sämtliche Werte der belegten Bits (d.h. die 'AN' = 1 sind). In diesem Fall wären es 0 + 1 + 8 + 16 = 25. Ebenso könnte man die 25 aber auch in 16(32, 64, 128)Bit-Schreibweise darstellen, doch da die höheren Bits nicht belegt sind hat das wenig Sinn.

Ein Feld (von vier) einer IP-Adresse beispielsweise besteht aus 8Bit. Die größtmögliche darstellbare Zahl ist somit auf den dezimalen Wert 256 (2 hoch 8) beschränkt.

Die Umrechnung von Dezimal in Binär ist ganz ähnlich (hier am Beispiel der Zahl 187):

Dezimalzahl	durch	Ergebnis	Bit	Rest
187	128 (2 hoch 7)	1,46093	1	59
59	64 (2 hoch 6)	0,921875	0	59
59	32 (2 hoch 5)	1,84375	1	27
27	16 (2 hoch 4)	1,6875	1	11
11	8 (2 hoch 3)	1,375	1	3
3	4 (2 hoch 2)	0,75	0	3
3	2 (2 hoch 2)	1,5	1	1
1	1(2 hoch 0)	1	1	1

Das Ergebnis würde also 10111011 (=187) heißen - gar nicht so schwer, oder?

DIE BINÄRE UND-RECHENOPERATION

Die binären Rechenoperationen sind dazu da, um Ausdrücke aus "Einsen und Nullen" logisch mit einander zu verbinden. Dazu gibt es mehrere Möglichkeiten - die AND, OR, XOR und NOT Verknüpfung. Wir wollen hier aber nicht zu weit abschweifen und beschränken uns auf die erste Möglichkeit, die AND-Verknüpfung, die auch benutzt wird um aus der Subnetmask und der IP-Adresse die Netzwerknummer (oder die Host-Nummer) zu ermitteln.

Das Prinzip ist relativ einfach. Es werden zwei binäre Zahlen mit (meist) der gleichen Länge, das heißt der gleichen Bit-Zahl, miteinander verglichen. Meistens werden Daten mit Masken verknüpft. An der Stelle, wo sowohl in der Zahl als auch in der Maske eine 1 steht, ist das Ergebnis in der AND-Verknüpfung ebenfalls 1. In allen anderen Fällen gleich 0.

	7	6	5	4	3	2	1	0	Bit
	0	1	1	0	1	0	1	1	Daten
AND	1	1	1	1	0	1	0	1	Maske
	0	1	1	0	0	0	0	1	Ergebnis

DIE ZUKUNFT

Das rasche (exponentielle Wachstum) des Internet zwingt dazu, das Internet Protokoll in der Version 4 (IPv4) durch ein Nachfolgeprotokoll zu ersetzen.

Bis vor einiger Zeit wurde das Internet größtenteils nur von Universitäten, Regierungsbehörden (dies aber auch fast nur in den USA und hier vor allem vom Verteidigungsministerium) und einigen Firmen aus der Industrie genutzt. Seit der Einführung des *World Wide Web (WWW)* ist das Internet aber auch zunehmend für Privatpersonen, kleinere Firmen etc. interessant. Das Internet wandelt sich von einem "Spielplatz für Akademiker" zu einem weltweiten Informations- und Unterhaltungssystem. Mit der ständig steigenden Anzahl von Benutzern des Internet werden sich auch die Anforderungen an das Netz ändern bzw. haben sich bereits geändert. Genannt sei hier nur als Beispiel das angestrebte Zusammenwachsen der Computer-, Unterhaltungs- und Telekommunikationsbranchen. Den Anforderungen, die z.B. *Video-on-demand* stellt, ist das Internet bzw. das Internet Protokoll in der Version 4 nicht gewachsen.

Vinton Cerf (der 'Vater' des Internet) bezeichnet in einem Interview mit der Zeitschrift c't [Kr98] das Internet *"(...) als die wichtigste Infrastruktur für alle Arten von Kommunikation."*. Auf die Frage, wie man sich die neuen Kommunikationsdienste des Internet vorstellen könne, antwortete Cerf:

> *"Am spannendsten finde ich es, die ganzen Haushaltsgeräte ans Netz anzuschließen. Ich denke dabei nicht nur daran, daß der Kühlschrank sich in Zukunft mit der Heizung austauscht, ob es in der Küche zu warm ist. Stromgesellschaften könnten beispielsweise Geräte wie Geschirrspülmaschinen kontrollieren und ihnen Strom genau dann zur Verfügung stellen, wenn gerade keine Spitzennachfrage herrscht. Derartige Anwendungen hängen allerdings davon ab, daß sie zu einem erschwinglichen Preis angeboten werden. Das ist nicht unbedingt ferne Zukunftsmusik; die Programmierer müßten eigentlich nur damit anfangen, endlich Software für intelligente Netzwerkanwendungen zu schreiben. Und natürlich muß die Sicherheit derartiger Systeme garantiert sein. Schließlich möchte ich nicht, daß die Nachbarkinder mein Haus programmieren!"*

Auf die Internet Protokolle kommen in der nächsten Zeit also völlig neue Anforderungen zu. Wie versucht wird, diese Anforderungen zu erfüllen, wird in den nächsten Abschnitten beschrieben.

CLASSLESS INTERDOMAIN ROUTING - CIDR

Der Verknappung der Internet-Adressen durch die ständig steigende Benutzerzahl wird zunächst versucht, mit dem *Classless InterDomain Routing (CIDR)* entgegen zu wirken.

Durch die Vergabe von Internet-Adressen in Klassen (Netze der Klassen A,B,C,...) wird eine große Anzahl von Adressen verschwendet. Hierbei stellt sich vor allem die Klasse B als Problem dar. Viele Firmen nehmen ein Netz der Klasse B für sich in Anspruch, da ein Klasse A Netz mit bis zu 16 Mio. Hosts selbst für eine sehr große Firma überdimensioniert scheint. Tatsächlich ist aber oft auch ein Klasse B Netz zu groß. Für viele Firmen würde ein Netz der Klasse C ausreichen. Dies wurde aber nicht verlangt, da viele Unternehmen die Befürchtung hatten, daß ein Klasse C Netz mit seinen bis zu 254 möglichen Hosts nicht ausreichen würde.

Ein größeres Hostfeld für Netze der Klasse C (z.B. 10 Bit, das entspricht 1022 Host pro Netz) hätte das Problem der knapper werdenden IP-Adressen vermutlich gemildert. Ein anderes Problem wäre dadurch allerdings entstanden: die Einträge der Routing-Tabellen wären explodiert.

Ein anderes Konzept ist das Classless InterDomain Routing (RFC 1519): die verbleibenden Netze der Klasse C werden in Blöcken variabler Größe zugewiesen. Werden beispielsweise 2000 Adressen benötigt, so können einfach acht aufeinanderfolgende Netze der Klasse C vergeben werden; das entspricht einem Block von 2048 Adressen. Zusätzlich werden die verbliebenen Klasse C Adressen restriktiver und strukturierter vergeben (RFC 1519). Die Welt ist dabei in vier Zonen, von denen jede einen Teil des verbliebenen Klasse C Adreßraums erhält, aufgeteilt:

194.0.0.0 - 195.255.255.255	Europa
198.0.0.0 - 199.255.255.255	Nordamerika
200.0.0.0 - 201.255.255.255	Mittel- und Südamerika
202.0.0.0 - 203.255.255.255	Asien und pazifischer Raum
204.0.0.0 - 223.255.255.255	Reserviert für zukünftige Nutzung

Jede der Zonen erhält dadurch in etwa 32 Millionen Adressen zugewiesen. Vorteil bei diesem Vorgehen ist, daß die 32 Millionen Adressen einer Region im Prinzip zu einem Eintrag in den Routing-Tabellen komprimiert worden sind. Der Vorteil der dadurch entsteht ist, daß z.B. jeder Router, der eine Adresse außerhalb seiner Region zugesandt bekommt...

INTERNET PROTOKOLL VERSION 6 - IPV6 (IP NEXT GENERATION)

Der vorrangige Grund für eine Änderung des IP-Protokolls ist auf den begrenzten Adreßraum zurückzuführen. CIDR schafft hier zwar wieder etwas Luft, dennoch ist klar absehbar, daß auch diese Maßnahmen nicht ausreichen, um die Verknappung der Adressen für eine längere Zeit in den Griff zu bekommen.

Weitere Gründe für eine Änderung des IP-Protokolls sind die oben schon erwähnten neuen Anforderungen an das Internet. Diesen Anforderungen ist IP in der Version 4 nicht gewachsen. Die *IETF (Internet Engineering Task Force)* begann deshalb 1990 mit der Arbeit an einer neuen Version von IP. Die wesentlichen Ziele des Projekts sind [Ta96]:

- Unterstützung von Milliarden von Hosts, auch bei ineffizienter Nutzung des Adreßraums
- Reduzierung des Umfangs der Routing-Tabellen
- Vereinfachung des Protokolls, damit Router Pakete schneller abwickeln können
- Höhere Sicherheit (Authentifikation und Datenschutz) als das heutige IP
- Mehr Gewicht auf Dienstarten, insbesondere für Echtzeitanwendungen
- Unterstützung von Multicasting durch die Möglichkeit, den Umfang zu definieren
- Möglichkeit für Hosts, ohne Adreßänderung auf Reise zu gehen
- Möglichkeit für das Protokoll, sich zukünftig weiterzuentwickeln
- Unterstützung der alten und neuen Protokolle in Koexistenz für Jahre

Im Dezember 1993 forderte die IETF mit RFC 1550 [IP: Next Generation (IPnG) White Paper Solicitation, Dec. 1993] die Internet-Gemeinde dazu auf, Vorschläge für ein neues Internet Protokoll zu machen. Auf die Anfrage wurde eine Vielzahl von Vorschlägen eingereicht. Diese reichten von nur geringfügigen Änderungen am bestehenden IPv4 bis zur vollständigen Ablösung durch ein neues Protokoll. Die drei besten Vorschläge wurden im *IEEE Network Magazine* veröffentlicht ([De93], [Fr93], [KF93]). Aus diesen Vorschlägen wurde von der IETF das *Simple Internet Protocol Plus (SIPP)* als Grundlage für die neue IP-Version ausgewählt. SIPP ist eine Kombination aus den Vorschlägen von Deering [De93] und Francis [Fr93].

Als die Entwickler mit den Arbeiten an der neuen Version des Internet Protokolls begannen, wurde natürlich auch ein Name für das Projekt bzw. das neue Protokoll benötigt. Wohl angeregt durch eine gleichnamige Fernsehsendung, wurde als Arbeitsname *IP - Next Generation (IPnG)* gewählt. Schließlich bekam das neue IP eine offi-

zielle Versionsnummer zugewiesen: IP Version 6 oder kurz IPv6. Die Protokollnummer 5 (IPv5) wurde bereits für ein experimentelles Protokoll verwendet.

Die folgende Beschreibung von IPv6 orientiert sich an RFC 2460 [Internet Protocol, Version 6 (IPv6) Specification, Dec. 1998]. Dieses Dokument gibt den neuesten Stand der Spezifikation des Internet Protokolls in der Version 6 wieder. RFC 2460 enthält einige wesentliche Änderungen der Spezifikation gegenüber RFC 1883 [Internet Protocol, Version 6 (IPv6) Specification, Dec. 1995].

DIE MERKMALE VON IPV6

Viele der als erfolgreich betrachteten Merkmale von IPv4 bleiben in IPv6 voll erhalten. Trotzdem ist IPv6 im allgemeinen nicht mit IPv4 kompatibel, wohl aber zu den weiteren Internet-Protokollen, insbesondere den Protokollen der Transportschicht (TCP, UDP); eventuell nach geringfügigen Modifikationen. Die Modifikationen betreffen im wesentlichen die erweiterte Adreßgröße (bisher 32 Bit auf nun 128 Bit).

Die wesentlichen Merkmale von IPv6 sind:

- **Adreßgröße:** Als wichtigstes Merkmal hat IPv6 gegenüber IPv4 größere Adressen. Statt bisher 32 Bit stehen nun 128 Bit für die Adressen bereit. Theoretisch lassen sich damit $2^{128} = 3.4*10^{38}$ Adressen vergeben.
- **Header-Format:** Der IPv6 (Basis)Header wurde vollständig geändert. Der Header enthält nur 7 statt bisher 13 Felder. Diese Änderung ermöglicht Routern, Pakete schneller zu verarbeiten. Im Gegensatz zu IPv4 gibt es bei IPv6 nicht mehr nur einen Header, sondern mehrere Header. Ein Datengramm besteht aus einem Basis-Header, sowie einem oder mehreren Zusatz-Headern, gefolgt von den Nutzdaten.
- **Erweiterte Unterstützung von Optionen und Erweiterungen:** Die Erweiterung der Optionen ist notwendig geworden, da einige, bei IPv4 notwendige Felder nun optional sind. Darüber hinaus unterscheidet sich auch die Art, wie die Optionen dargestellt werden. Für Router wird es damit einfacher, Optionen, die nicht für sie bestimmt sind, zu überspringen. Dies ermöglicht ebenfalls eine schnellere Verarbeitung von Paketen.
- **Dienstarten:** IPv6 legt mehr Gewicht auf die Unterstützung von Dienstarten. Damit kommt IPv6 den Forderungen nach einer verbesserten Unterstützung der Übertragung von Video- und Audiodaten entgegen. IPv6 bietet hierzu eine Option zur Echtzeitübertragung.
- **Sicherheit:** IPv6 beinhaltet nun im Protokoll selbst Mechanismen zur sicheren Datenübertragung. Wichtige neue Merkmale von IPv6 sind hier

Authentifikation (authentication), Datenintegrität (data integrity) und Datenverlässlichkeit (data confidentiality).

- **Erweiterbarkeit:** IPv6 ist ein erweiterbares Protokoll. Bei der Spezifikation des Protokolls wurde nicht versucht alle potentiell möglichen Einsatzfelder für das Protokoll in die Spezifikation zu integrieren. Vielmehr bietet IPv6 die Möglichkeit über Erweiterungs-Header (s.u.) das Protokoll zu erweitern. Damit ist das Protokoll offen für zukünftige Verbesserungen.

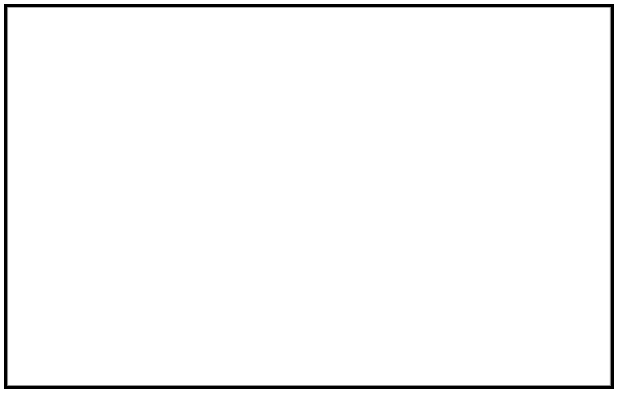
DAS IPV6 DATENGRAMMFORMAT

Ein IPv6-Datengramm besteht aus dem *Basis-Header* (s.u. Der IPv6-Basis-Header), gefolgt von den optionalen *Zusatz-Headern* (s.u. Erweiterungs-Header) und den Nutzdaten.

Allgemeine Form eines IPv6-Datengramms.

DER IPV6-BASIS-HEADER

Der IPv6-Basis-Header ist doppelt so groß wie der IPv4-Header. Der IPv6-Basis-Header enthält weniger Felder als der IPv4-Header, dafür ist aber die Adreßgröße für die Quell- und Zieladresse von bisher 32-Bit auf nunmehr 128-Bit erweitert worden.



IPv6 Basis-Header.

Version:

Mit dem Feld *Version* können Router überprüfen, um welche Version des Protokolls

es sich handelt. Für ein IPv6-Datengramm ist dieses Feld immer 6 und für ein IPv4-Datengramm dementsprechend immer 4. Mit diesem Feld ist es möglich für eine lange Zeit die unterschiedlichen Protokollversionen IPv4 und IPv6 nebeneinander zu verwenden. Über die Prüfung des Feldes Version können die Daten an das jeweils richtige "Verarbeitungsprogramm" weitergeleitet werden.

Priority:

Das Feld *Priority* (oder *Traffic Class*) ...

Flow Label

Das Feld *Flow Label*...

Payload Length

Das Feld *Payload Length (Nutzdatenlänge)* gibt an, wie viele Bytes dem IPv6-Basis-Header folgen, der IPv6-Basis-Header ist ausgeschlossen. Die Erweiterungs-Header werden bei der Berechnung der Nutzdatenlänge mit einbezogen. Das entsprechende Feld wird in der Protokollversion 4 mit *Total Length* bezeichnet. Allerdings bezieht IPv4 den 20 Byte großen Header auch mit in die Berechnung ein, wodurch die Bezeichnung "total length" gerechtfertigt ist.

Next Header

Das Feld *Next Header* gibt an, welcher Erweiterungs-Header dem IPv6-Basis-Header folgt. Jeder folgende Erweiterungs-Header beinhaltet ebenfalls ein Feld Next Header, das auf den nachfolgenden Header verweist. Ist dies der letzte zu IPv6 zugehörige Header, so gibt das Feld an, welches Transportprotokoll (z.B. TCP oder UDP) folgt. Eine genauere Beschreibung des Konzepts mehrerer Header folgt im Abschnitt Erweiterungs-Header.

Hop Limit

> Mit dem Feld *Hop Limit* wird festgelegt, wie lange ein Paket überleben darf. Der Wert des Feldes wird nach jeder Teilstrecke gesenkt. Ein Datengramm wird dann verworfen, wenn das Feld Hop Limit auf Null herunter gezählt ist, bevor das Datengramm sein Ziel erreicht hat. IPv4 verwendet hierzu das Feld *Time to Live*, welches die Zeit in Sekunden angibt, die ein Paket überleben darf. Allerdings wird dieses Feld von den meisten Routern nicht so interpretiert. In IPv6 wurde das Feld deshalb umbenannt, um die tatsächliche Nutzung

wiederzugeben.

Source Address, Destination Address

Die beiden Felder *Quell-* und *Zieladresse* dienen zur Identifizierung des Senders und Empfängers eines IP-Datengramms. IPv6 verwendet zur Adressierung 4 mal so große Adressen wie IPv4: 128 Bit statt 32 Bit. Eine genaue Beschreibung der IPv6-Adressen folgt im Abschnitt IPv6-Adressierung.

Ein Vergleich des IPv4-Headers mit dem IPv6-Basis-Header veranschaulicht, welche Felder bei IPv6 weggelassen wurden:

- Das Feld *Length (Internet Header Length - IHL)* ist nicht mehr vorhanden, da der IPv6-Basis-Header eine feste Länge von 40 Byte hat. Bei IPv4 ist dieses Feld notwendig, da der Header aufgrund der Optionen eine variable Länge hat.
- Das Feld *Protocol* wird nicht mehr benötigt, da das Feld *Next Header* angibt, was nach dem letzten IP-Header folgt (z.B. TCP oder UDP).
- Alle Felder die bisher zur Fragmentierung eines IP-Datengramms benötigt wurden (*Identification, Flags, Fragment Offset*), sind im IPv6-Basis-Header nicht mehr vorhanden, da die Fragmentierung in IPv6 gegenüber IPv4 anders gehandhabt wird. Alle IPv6 kompatiblen Hosts und Router müssen Pakete mit einer Größe von 1280 Byte (RFC 1883 legte diese Größe noch auf 576 Byte fest) unterstützen. Durch diese Regel wird eine Fragmentierung im Prinzip nicht notwendig. Empfängt ein Router ein zu großes Paket, so führt er keine Fragmentierung mehr durch, sondern sendet eine Nachricht an den Absender des Pakets zurück. In dieser Nachricht wird der sendende Host angewiesen, alle weiteren Pakete zu diesem Ziel aufzuteilen. Das bedeutet, daß von den Hosts "erwartet" wird, daß sie von vornherein eine Datengrammgröße wählen, die keine Fragmentierung voraussetzt. Dadurch wird eine größere Effizienz bei der Übertragung erreicht, als wenn Pakete von Routern auf dem Weg fragmentiert werden müssen. Die Steuerung der Fragmentierung erfolgt bei IPv6 über den *Fragment Header*.
- Das Feld *Checksum* ist nicht mehr vorhanden, da die Berechnung der Prüfsumme sich nachteilig auf die Leistung der Datenübertragung ausgewirkt hat. Das entfernen der Prüfsumme aus dem Internet Protokoll hat zu heftigen Diskussionen geführt [Ta96]. Die eine Seite kritisierte heftig das entfernen der Prüfsumme, während die andere Seite argumentierte, daß Prüfsummen etwas sind, das auch von Anwendungen übernommen werden kann, sofern sich die Anwendung tatsächlich um Datenintegrität kümmert. Ein weiteres Gegenargument war, daß eine Prüfsumme auf der Transportschicht bereits

vorhanden ist, weshalb innerhalb der Vermittlungsschicht keine weitere Prüfsumme notwendig sei. Letztendlich fiel die Entscheidung, daß IPv6 keine Prüfsumme enthält.

ERWEITERUNGS-HEADER

IPv6 nutzt das Konzept der Erweiterungs-Header, um a) eine effiziente Datenübertragung und b) eine Erweiterung des Protokolls zu ermöglichen. Der erste Punkt ist leicht ersichtlich: Der Basis-Header enthält nur Felder, die unbedingt für die Übermittlung eines Datengramms notwendig sind, erfordert die Übertragung weitere Optionen, so können diese über einen Erweiterungs-Header angegeben werden. IPv6 sieht vor, das einige Merkmale des Protokolls nur gezielt benutzt werden. Ein gutes Beispiel ist hier die Fragmentierung von Datengrammen. Obwohl viele IPv4-Datengramme nicht fragmentiert werden müssen, enthält der IPv4-Header Felder, für die Fragmentierung. IPv6 gliedert die Felder für die Fragmentierung in einen separaten Header aus, der wirklich nur dann verwendet werden muß, wenn das Datengramm tatsächlich fragmentiert werden muß. Ein weiterer wesentlicher Vorteil des Konzepts der Erweiterungs-Header ist, daß das Protokoll um neue Funktionen erweitert werden kann. Es genügt, für das Feld *Next Header* einen neuen Typ und ein neues Header-Format zu definieren. IPv4 erfordert hierzu eine vollständige Änderung des Headers.

Derzeit sind 6 Erweiterungs-Header definiert. Alle Erweiterungs-Header sind optional. Werden mehrere Erweiterungs-Header verwendet, so ist es erforderlich, sie in einer festen Reihenfolge anzugeben.

Header	***Beschreibung***
IPv6-Basis-Header	Zwingend erforderlicher IPv6-Basis-Header
Optionen für Teilstrecken (Hop-by-Hop Options Header)	Verschiedene Informationen für Router
Optionen für Ziele (Destination Options Header)	Zusätzliche Informationen für das Ziel
Routing (Routing Header)	Definition einer vollständigen oder teilweisen Route
Fragmentierung (Fragment Header)	Verwaltung von Datengrammfragmenten
Authentifikation (Authentication Header)	Echtheitsüberprüfung des Senders

Verschlüsselte Sicherheitsdaten (Encapsulating Security Payload Header)	Informationen über den verschlüsselten Inhalt
Optionen für Ziele (Destination Options Header)	Zusätzliche Informationen für das Ziel (für Optionen, die nur vom endgültigen Ziel des Paketes verarbeitet werden müssen)
Header der höheren Schichten (Upper Layer Header)	Header der höheren Protokollschichten (TCP, UDP, ...)

IPv6 Erweiterungs-Header.

Die ersten 5 Header sind in RFC 2460 (bzw. RFC 1883). Der Authentifikations--Header sowie der Header für Sicherheitsdaten werden in RFC 2402 (RFC 1826) und RFC 2406 (RFC 1827) beschrieben.

IPv6 Datengramme. (a) IPv6-Basis-Header und Nutzdaten; (b) IPv6-Basis-Header mit einem Zusatz-Header für Routing-Informationen, gefolgt von Nutzdaten.

GLOSSAR

Dieser selbst zusammengestellte Glossar erhebt keinerlei Anspruch auf Vollständigkeit.

ANSI

***A**merican **N**ational **S**tandards **I**nstitute*; Amerikanischer Normungsausschuß und Mitglied der ISO, bekannt z.B. für Schnittstellenempfehlungen und Normung von Programmiersprachen. http://www.ansi.org/

AppleTalk

LAN-Vermittlungs-Protokoll, das von der Firma *Apple* entwickelt wurde. Es ist unabhängig von der Netzwerkschicht implementiert. So existieren Implementationen für *LocalTalk* und *EtherTalk*.

ARPA

***A**dvanced **R**esearch **P**rojects **A**gency*; Agentur des Verteidigungsministeriums der USA. Sie ist verantwortlich für die Entwicklung neuer Technologien zur militärischen Nutzung. Die ARPA hat das erste Datennetz, das *ARPANet*, ins Leben gerufen. Aus dem ARPANet ist das heutige *Internet* entstanden.

ARPAnet

*ARPA**Net**work* in den USA. Es begann 1968 zu arbeiten und war damit die Keimzelle des *Internet*. Seine Backbone-Funktionalität hat heute das *NSFNet* übernommen.

ASCII

***A**merican **S**tandard **C**ode for **I**nformation **I**nterchange*; Ein 7-Bit-Code für alphanumerische und einige andere Steuerzeichen.

Backbone

Kernstück (*Rückgrat*) eines Netzwerkes; Netzwerk mit meist höherer Geschwindigkeit, mit dem lokale Netze verbunden werden.

Bridge

Netzübergang auf *OSI-Ebene* 2. Eine Bridge kann Netze mit unterschiedlichen Übertragungsmedien und unterschiedlichen Übertragungsgeschwindigkeiten koppeln.

Brouter

LAN-WAN-Verbindungsgerät mit kombinierten *Bridge*- (Filtern und Übertragen von Datenpaketen) und *Router*funktionen (Protokoll-Routing, Wegwahl).

Browser

Programm zum Lesen von Hypertext. Der Browser ermöglicht das Betrachten der verschiedenen Dokumente im Hypertext und die Navigation zwischen den Dokumenten, z.B. WWW-Browser.

Bus-Topologie

Bus-*Topologie* ist eine LAN-Topologie zur seriellen Datenübertragung, bei der alle Netzstationen an einem linienförmigen Kabelstrang angeschlossen sind. Die Enden des Kabels sind mit Abschlußwiderständen versehen.

Client

Systemteil einer *Client-Server-Architektur*, die einen Dienst initiiert. Er fordert (*Requesting*) den Dienst vom *Server* an. Dieser gibt die Daten nach der Bearbeitung an den Client zurück. Die Art der angeforderten Dienste kann sehr unterschiedlich sein.

Client-Server-Architektur

Die C/S-Architektur bezeichnet ein Systemdesign bei dem die Verarbeitung einer Anwendung in zwei separate Teile aufgespaltet wird. Ein Teil läuft auf dem *Server* (*Backend-Komponente*), der andere Teil auf einer Workstation (*Client* oder *Front-End*). Beide Teile werden über Netzwerke zu einem System zusammengefügt. Der Client gibt auf dem Server die Bearbeitung von Daten in Auftrag und nimmt die Leistungen des Servers in Anspruch. Im Gegensatz zu *Host*-basierten Architekturen sind die Server heute nicht mehr mit der gesamten Datenverarbeitung beschäftigt, sondern geben die Daten zur weiteren Aufbereitung an den Client zurück.

CSMA/CD

***C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection*; Ist ein Zugriffsverfahren in LANs, bei dem die teilnehmenden *Stationen* physikalisch den Verkehr auf der Leitung abhören. Findet gerade keine Übertragung statt, so kann die jeweilige Station senden. Versuchen zwei Stationen gleichzeitig zu senden, so kommt es zu einer *Kollision*, die von allen beteiligten Stationen erkannt wird. Nach einem zufälligen Zeitraum versuchen die kollidierten Teilnehmer erneut zu übertragen. Kommt es erneut zu einer Kollision, so werden die Zeitspannen, aus denen die zufällige Wartezeit ausgewählt wird, schrittweise vergrößert.

DARPA

*U.S. Department of **D**efense **A**dvanced **R**esearch **P**rojects **A**gency*; Staatliche Einrichtung des amerikanischen Verteidigungsministeriums, die das ARPAnet und später das Internet gegründet hat.

Datagramm

In Übertragungsnetzen ist ein Datagramm ein Datenpaket, das ohne Quittierungsmechanismus vom Sender zum Empfänger übermittelt wird. Dazu muß es die vollständige Empfängeradresse und Absenderangaben enthalten.

DECnet

Routingfähiges Kommunikationsprotokoll von ***D**igital **E**quipment **C**orp.* (DEC).

DE-NIC

DE**utsches **NIC; Ist das *NIC* der *Top-Level-Domain .de* des Internet mit Sitz in Karlsruhe. Es ist für die Vergabe von *IP-Adressen* und *Domains* innerhalb und für den Betrieb des primären Nameservers der Domain .de verantwortlich. http://www.de-nic.de/

DNS

***D**omain **N**ame **S**ervice* / ***D**omain **N**ame **S**erver*; Hierarchisch aufgebauter Dienst im Internet und anderen *TCP/IP*-Netzen, der für einen kryptischen Hostnamen die entsprechende IP-Adresse zurückgibt.

Domain

Allgemein ein eigenständiger Verwaltungsbezirk in einem Netzwerk. Im Internet wird unter Domain eine Gruppe von Computern verstanden, deren Hostnamen das gleiche Suffix, den Domainnamen, besitzen.
Einige der wichtigsten Domains sind:

xxx.com (commercial)
xxx.edu (Universitäten besonders in USA)
xxx.net (Netzorganisationen)
xxx.gov (Regierung der USA)
xxx.mil (Militär USA zum Teil NATO)

xxx.uk (United Kingdom)
xxx.de (Deutschland)

Ethernet

Weit verbreitetes Produkt für LAN mit dem Zugriffsverfahren *CSMA/CD*. Ethernet ermöglicht Übertragungsgeschwindigkeiten bis zu 10 Mbit/s.

Ethernet-Switch

Gerät (*Switch*), das statisches und/oder dynamisches LAN-Switching auf Basis der Ethernet-Technologie durchführt. Er kann entweder zwischen Einzelgeräten (*Port-Switching*) oder Segmenten (*Segment-Switching*) vermitteln.

FAQ

***F**requently **A**sked **Q**uestions*; Fragen, die zu einem Thema häufig gestellt werden, werden in Frage-Antwort-Form als Text zusammengestellt.

FDDI

***F**iber **D**istributed **D**ata **I**nterface*; Auf Glasfaserkabel basierende Hochgeschwindigkeitstechnologie (bis zu 100 Mbit/s) für den Backbone-Bereich. Mittlerweile auch auf Kupfer- (CDDI) und Twisted-Pair-Verkabelung (SDDI) möglich.

Fiber Optic Cable

Auch *Lichtwellenleiter*, *Glasfaserkabel*. Übertragungsmedium, das aus einem Innenleiter aus Glas oder Kunststoff und mehreren Ummantelungen zum Schutz vor mechanischer Belastung besteht.

Firewall

Sammelbezeichnung für Lösungen, die versuchen LANs, welche ans Internet angeschlossen sind, vor unberechtigtem Zugriff aus diesem zu schützen. Außerdem sind sie in der Lage, auch den Verkehr aus dem LAN ins Internet zu kontrollieren und reglementieren.

FTP

***F**ile **T**ransfer **P**rotocol*; Eine Standardanwendung für *TCP/IP*, die nur die Fileübertragung und keinen Filezugriff beinhaltet.

Gateway

Netzübergang auf den *OSI-Schichten* 4 bis 7. Mit einem Gateway können verschiedenartige Netzwerke miteinander verbunden werden, weil eine Umsetzung von Protokoll, Namen und Adressen vorgenommen werden kann.

Handshake

Synchronisationsmethode, die in unterschiedlichsten Ausprägungen in der Kommunikationstechnik (z.B. beim Verbindungsaufbau oder Datenübertragung) als Hard- oder Softwarelösung eingesetzt wird. Handshake ist eine Form des Quittungsbetriebes. Quittiert werden unterschiedlichste Informationen wie der Wunsch zur Datenübertragung, Kommunikationsbedingungen oder Datenpakete.

Header

Teil eines Nachrichtenpaketes, der die Absender- und Empfängeradresse und weitere Zusatzinformationen enthält.

Host

Ein zentraler Großrechner, auf den von anderen Systemen aus zugegriffen wird. Die vom Host bereitgestellten Dienstleistungen können über *Lokal-* und *Fernabfrage* abgerufen werden. Die Verbindung zum Host wird über *Terminals* aufgebaut: Daten können an den Host gesendet und vom Host empfangen werden.

HTML

***H**yper**T**ext **M**arkup **L**anguage*; Dokumentenbeschreibungssprache, die im *World Wide Web* verwendet und von allen WWW-*Browsern* verstanden wird.

HTTP

***H**yper**T**ext **T**ransmission **P**rotocol*; Das Protokoll, daß die Übertragung von *HTML*-Seiten im Internet regelt.

Hub

Konzentrator; Ein Gerät, das die Anschlußbündelung verschiedener Netzgeräte über einem zentralen Punkt an das Verkabelungssystem erlaubt.

IEEE

***I**nstitute of **E**lectrical and **E**lectronic **E**ngineers*; Führendes amerikanisches Standardisierungsgremium. Für lokale Netzwerke sind die verschiedenen IEEE 802-Spezifikationen von Bedeutung. http://www.ieee.org/

Internet

Das weltweit größte Verbundnetz heterogener Netzwerke. Das Internet basiert auf *TCP/IP*.

IP

***I**nternet **P**rotokoll*; Sorgt vor allem dafür, daß *Datagramme* von *Routern* an ihr Ziel transportiert werden.

IP-Adresse

Auch Punkt-Adresse genannt. Eine 32-Bit Zahl, die für jeden Computer im Internet einmalig ist. Sie wird z.B. so geschrieben: 128.11.3.31.

IP-Netzklasse

Art der Unterteilung einer *IP-Adresse* in einen Netz- und einen Host-Anteil. Die Netzklasse ist abhängig von der Anzahl der in einer Firma an das Internet anzuschließenden Computer. In der Praxis werden heute die Klassen A, B und C verwendet.

IPX

***I**nternetwork **P**acket **Ex**change*; Schicht 3-Protokoll der Firma *Novell*, das in *Netware* eingesetzt wird.

ISDN

***I**ntegrated **S**ervices **D**igital **N**etwork*; Standardisierte Technologie, mit der verschiedene Kommunikationsdienste (Übermittlung von Sprache, Daten, Bildern ...) über ein Medium realisiert werden.

ISP

***I**nternet **S**ervice **P**rovider*; Firmen oder Institutionen, die Teilnetze des Internet betreiben. Das Internet besteht in Summe aus den Teilnetzen der ISP, die untereinander mehr oder weniger gut verbunden sind.

Knoten (node)

Ein an ein Netzwerk angeschlossenes Gerät, das Daten abgibt oder empfängt, wird als Knoten dieses Netzes bezeichnet. Das können sowohl einzelne Rechner, *Server* als auch Drucker sein, die von mehreren Netzteilnehmer angesprochen werden.

Koxialkabel

Kabel auf Kupferbasis mit einem Kupferleitungsdraht. Der Draht ist in Kunststoff eingegossen, dieser von einem Drahtgeflecht zur Abschirmung umgeben. Das Abschirmungsgeflecht ist von einem Mantel umgeben, meist aus flexiblem Kunststoff, der vor mechanischen Belastungen und vor Witterungseinflüssen schützt.

LAN

***L**ocal **A**rea **N**etwork*; Netzwerke, in denen sich die Netzgeräte in einem Bereich von wenigen Quadratkilometern (meist weniger) befinden.

Layer / Schicht

Netzwerke werden in der Regel als ein Satz von mehr oder weniger unabhängigen Protokollen realisiert. Jedes davon implementiert eine spezielle Schicht (Layer). Die unterste Schicht regelt die direkte Hardware-Verbindung. Die höchste besteht aus Anwendungsprogrammen. Jede Schicht dazwischen stellt Dienste für die nächst höhere Schicht zur Verfügung. Dazu bedient sie sich Protokollen, die mit der jeweiligen Schicht der Gegenseite kommunizieren.

MAC

***M**edia **A**ccess **C**ontrol*; MAC ist die erste Unterebene der *Data Link Ebene* im *OSI-Modell*. In der MAC-Ebene werden die Zugriffsverfahren (z.B. *CSMA/CD* oder *Token-Passing*) der LANs implementiert.

MAN

***M**etropolitan **A**rea **N**etwork*; Auf ein Stadtgebiet oder einen Ballungsraum beschränktes Netz, das hohe Übertragungsgeschwindigkeiten ermöglicht.

MILNet

***MIL**itary **Net**work*; Organisatorisch abgetrennter Teil des Internet, der von militärischen Institutionen der USA betrieben wird.

Modem

***Mo**dulator/**Dem**odulator*; Ist ein Gerät zur Umwandlung digitaler Signale in Tonfrequenzsignale zur Übertragung auf einer analogen Leitung.

NetBEUI

***NetB**IOS **E**xtended **U**ser **I**nterface*; Nicht routingfähiges Standard-*Protokoll* im *LAN-Manager* und *Microsoft*-Netzwerklösungen.

Netzwerk

auch Netz, Network oder Net; Ein Telekommunikationsnetz umfaßt die Gesamtheit der netz-, vermittlungs- und übertragungstechnischen Einrichtungen sowie die Verbindungsmöglichkeiten zwischen diesen Systemelementen.

NSFNet

***N**ational **S**cience **F**oundation **Net**work*; Hochgeschwindigkeits-Wissenschaftsnetz der USA, das von der *NSF* getragen wird. Ist ein Backbone-Verbund von Netzwerken, der die gesamten USA überspannt und Verbindungen in alle Regionen der Welt unterhält.

OSI-Modell

Referenzmodell der ***O**pen **S**ystems **I**nterconnection*, das in sieben Schichten wesentliche Details zur Rechnerkommunikation zusammenfaßt.

Patch-Kabel

Kabel, das benutzt wird, um fest verlegte Kabelstränge variabel zu verbinden.

Peer-to-Peer-Net

Netzwerk, bei dem mehrere Netzknoten direkt kommunizieren, um gemeinsam Ressourcen zu nutzen. Solche Netze benötigen keinen dedizierten *Fileserver*.

physical layer

Bitübertragungsschicht; Unterste (Schicht 1) des *ISO/OSI-Modells*. Beschäftigt sich mit der Übertragung roher Bits in einem Übertragungskanal.

Port

Hardware-Ein-/Ausgang, z.B. Ein-/Ausgang an Netzwerkgeräten wie *LAN-Switches*, *Bridges* oder *Routern*.

PPP

***P**oint to **P**oint **P**rotocol*; PPP ist ein *Protokoll* zur LAN-Kopplung über *WAN*s.

presentation layer

Darstellungsschicht; Ebene 6 des *ISO/OSI-Modells* der offenen Kommunikation beschäftigt sich mit Funktionen, die durch ihr häufiges Auftreten eine allgemeine Lösung rechtfertigen, statt sie jedem Anwender erneut zur Lösung zu überlassen.

Protokoll

Sammlung von Regeln über den Aufbau, die Überwachung und den Abbau von Verbindungen, sowie für die Übertragung von Daten.

Proxy-Server

Ein Proxy-Server arbeitet ähnlich wie ein Festplatten-Cache. Er speichert öfters sich wiederholende Programmaufrufe zwischen. Wenn in einem Netzwerk öfters von anderen Teilnehmern auf entfernte *WWW-Seiten* zugegriffen wird, so ist es sinnvoll, daß der *Provider* diese Seiten "zwischenlagert". Bei einer erneuten Anfrage dieser Seite braucht nun nicht mehr auf den entfernten *Server* zugegriffen zu werden, sondern die Daten werden aus dem heimischen Proxy-Server geliefert. Das spart Zeit und Geld. *Das Problem:* Datenaktualität.

Repeater

Netzübergang auf *OSI-Ebene* 1 zum Verstärken und Regenerieren von Signalen in Netzen.

Router

Netzübergang auf *OSI-Ebene* 3. Ein Router dient zur Strukturierung von Netzwerken. Er schafft Verbindungen zwischen Netzwerken mit verschiedenen Übertragungsprotokollen. Die Hauptfunktion eines Routers ist die Wegwahl (*Routing*).

Schnittstelle

Definierte Grenze zwischen zwei Hardware-, zwei Software- oder zwischen Hard- und Softwarekomponenten. Beispiele für Schnittstellen sind die Übergänge von Computer zu Datenübertragungseinrichtungen oder von Kommunikationsgeräten untereinander.

Segment

Zusammenhängendes Kabelstück eines LANs, an das die LAN-Stationen angeschlossen sind. Die mögliche Länge eines Segments richtet sich nach der Signalausdehnung, die ohne Einsatz von *Repeatern* möglich ist. Segmente werden durch *Repeater*, *Bridges*, *Switches* oder *Router* miteinander verbunden.

Segmentierung

Aufteilung (Strukturierung) einer LAN-Verkabelung in einzelne *Segmente*, die durch Bridges, Router oder *LAN-Switching-Hubs* verbunden werden. Ziel der Segmentierung ist die Bereitstellung einer höheren *Bandbreite* durch Lokalisierung des Datenverkehrs.

Server

In der *Client-Server-Architektur* ist der Server der Softwareteil, der bestimmte Dienste im Auftrag des *Clients* ausführt, d.h. über definierte *Schnittstellen* zur Verfügung stellt. Die Serversoftware läuft dabei natürlich oft auf dedizierten Server-Rechnern.

Subnetz

Netzabschnitt, der physikalisch vom restlichen Netzwerk getrennt ist (z.B. durch einen Netzübergang).

Supervisor

Netzwerkverwalter mit bestimmten Rechten um die Netzpflege und -verwaltung durchführen zu können.

Switching

Schalten, Vermitteln; Switching ist in der Kommunikationstechnik einer der am häufigsten gebrauchten Begriffe. Da alle mögliche Dinge geschaltet, umgesteckt oder vermittelt werden können, herrscht auch eine gewisse Konfusion bei der Verwendung dieses Begriffes.

TCP

T*ransmission* ***C****ontrol* ***P****rotocol* = Übermittlungs-Kontroll-Protokoll; Packt die Daten, die eine Anwendung senden möchte in *Datagramme*, überwacht ihre fehlerfreie Übermittlung und packt sie beim Empfänger wieder aus.

TCP/IP

Die Protokollfamilie, die ursprünglich für *UNIX* entwickelt wurde, heute jedoch verschiedenste Rechnerwelten miteinander verbindet. Weil die Protokolle *TCP* und *IP* eine zentrale Rolle im Internet haben, spricht man manchmal vom weltweiten TCP/IP-Netz, von TCP/IP *Clients* etc.

Token Ring

LAN-Technologie für ringförmig angeordnete Netzwerke, die hauptsächlich im *IBM*-Umfeld eingesetzt wird.

Topologie

Die Anordnung, wie Rechner beim Aufbau eines LANs miteinander verbunden werden: Es gibt Bus-, Ring-, Sterntopologie beziehungsweise Mischformen.

transport layer

Transportschicht; Schicht 4 nach dem *ISO/OSI-Modell* der offenen Kommunikation. Aufgabe der Transportschicht ist es, die Daten von der Sitzungsschicht zu übernehmen, sie wenn nötig in kleinere Einheiten zu zerlegen, sie dann an die Vermittlungsschicht zu geben und dafür zu sorgen, daß alle Teile richtig am anderen Ende ankommen.

Twisted Pair

Kabeltyp, bei dem die einzelnen Adernpaare miteinander verdrillt sind, um die elektromagnetische Abstrahlung so gering wie möglich zu halten.

WAN

***W**ide **A**rea **N**etwork*; WANs bestehen aus mehreren LANs, die über Fernleitungen miteinander gekoppelt sind.

Workgroup

Als Workgroup bezeichnet man LAN-Teilnehmer, die sich zu Arbeitsgruppen zusammenschließen und die für ihre Arbeitserfordernisse bestimmte Rechte erhalten.

WWW

***W**orld **W**ide **W**eb*; sehr flexibles, erweitertes Informationssystem auf der Basis von Hypertext-Verbindungen.

W3C

W**orld **W**ide **W**eb **C**onsortium*; Industrie-Consortium unter Leitung des *MITs* (M**assachusetts **I**nstitute of **T**echnology*; amerikanisches Forschungsinstitut) und *INRIA* (***In**stitut de **R**echerche en **I**nformatique et en **A**utomatique*). Es beschäftigt sich u.a. mit der Weiterentwicklung von Standards für das WWW (z.B. *HTML*, *HTTP* und *MIME*). Derzeit läuft der Standardisierungsprozeß ständig den Entwicklungen hinterher, welche unter anderem die Unternehmen *Netscape* und *Microsoft* in ihre *Browser* implementieren. http://www.w3.org/