Lehrgang

WebMaster KVZ

TELEMATIK

(Grundlagen und Konzepte der Netzwerk-Kommunikation)

Version 1.0 - 01.05.1998

Konzept und Gestaltung
Barnes Enterprises
http://www.barnes.ch

Autor:

Bernhard Kreinz

System Engineer (Client/Server- Infrastruktur)
und Webmaster
der Zürich Versicherungen Schweiz

Inhaltsverzeichnis:

1.6 Standardisierungsorganisationen

Die verschiedenen Services im WWW und ihre Protokolle. Methoden des Troubleshooting im Netzbereich. Interpretieren von Fehlermeldungen. Übersicht der verschiedenen TCP/UDP -Ports.

1.7 Referenzen

Links zu allen relevanten Themenbereichen, die hier angeschnitten worden sind.

1.1 Vorwort

Im Rahmen Ihrer Ausbildung zum Webmaster werden Sie schnell begreifen lernen, dass das Internet mir seiner Vernetzung nicht nur ein Schlagwort darstellt, sondern, dass die verschiedenen Services, die Sie als Webmaster anbieten müssen oder wollen, in der Regel Netzwerkservices sind. Sie wollen Ihren Kunden (Endbenutzern am PC) Dienstleistungen wie Mail, Agenda, Publishingmöglichkeiten u.v.m zu Verfügung stellen. Das heisst aber, dass der Endbenutzer und Ihr Server (Mail, Agenda, Webserver...) miteinander kommunizieren müssen. Dies kann aber nur über eine Vernetzung von beiden Systemen erfolgreich funktionieren. Also brauchen Sie Kenntnisse über grundsätzliche Prinzipien und Konzepte im Netzwerkbereich.

Telematik versteht sich als Zwitterform zwischen Informatik und Telekommunikation. Auch hier hat die Spezialisierung voll Fuss gefasst, sodass Sie Ihre Erwartungshaltung nicht zu hoch schrauben dürfen, denn die Themen im Netzwerkbereich sind so breit gefächert, dass es kaum einen Menschen gibt, der alle Hardwarekomponenten und Protokolleigenschaften kennt. Dies hat mitunter einen historisch gewachsenen Grund: Die verschiedenen Betriebsysteme haben die Kommunikation zwischen Client (Endbenutzer) und Server auf Ihre spezifischen Bedürfnisse angepasst (proprietär). So unterscheiden sich Kommunikation (zwischen HOST und Terminal) in einer Mainframeumgebung (z.B. IBM MVS) und Kommunikation (zwischen PC und Server) in einer Client/Server - Umgebung (z.B. Windows und NT Server) grundsätzlich voneinander. Hier müssen Sie lernen, welche Kommunikationswege für Sie als Webmaster relevant sind.

Ziel dieser Vorlesung ist es also, Ihnen die Grundlagen näher zu bringen, die Sie in Ausübung des Berufes "Webmaster" im Netzwerkbereich haben müssen, sei es um eine neue Dienstleistung sinnvoll implementieren zu können, oder aber im Supportbereich, um Fehlerquellen eingrenzen zu können, und so gegebenenfalls andere zuständige Stellen (Netzwerkverantwortliche in Ihrem Betrieb; Externe Netzwerkverantwortliche- Firewallbetreuer o.a.) konkret mit Problemen anzugehen. Sie wollen doch nicht zum Telefon greifen, um dann zu hören, dass der Fehler aufgrund einer falschen Definition (Konfiguration) Ihrerseits existiert.

Schwerpunkte dieser Vorlesung sind Netzwerkservices, die für Sie als Webmaster relevant sind, d.h. verschiedene Services, welche auf der TCP/IP- Protokollfamilie aufsetzen, sowie theoretische Grundlagen der Kommunikation zwischen Client und Server.

Erste Schritte...

Warum werden Netzwerke und insbesondere das Internet von so vielen Anwendern genutzt? Die Gründe sind gerade für Firmen vielfältig:

- Teilen von Firmenressourcen
- Höhere Verfügbarkeit durch alternative Sourcen
- Sparen von Geld durch das günstigere Preis/Leistungsverhältnis von vielen kleinen Computern gegenüber Zentralrechnern

Das Internet bietet sowohl firmenintern als auch weltweit eine Reihe von Diensten, die es für Benutzer sehr attraktiv machen. Darunter gehören unter anderem folgende:

- Übertragung von Texten, Bildern, Tönen, Videos und Programmen über FTP (File Transfer)
- Internet-Telefonie und Video-Conferencing sowie Internet Chat
- Elektronische Post - Email
- Diskussionsforen - News
- Hypertextsystem - World Wide Web

Ein kleines Glossar soll helfen die gebräuchlichsten Begriffe der Internet-Technologie zu verstehen:

Bit: Kleinste Informationseinheit, bestehend aus einer 0 (Falsch) oder einer 1 (Wahr). Tausend Bits sind ein Kilobit (kbit), eine Million Bits sind ein Megabit (Mbit) und eine Milliarde Bits sind ein Gigabit (Gbit). Übertragungsleistungen werden in Bits pro Sekunde (Bit/s) gemessen.

Browser: Ein Programm zum Bewegen im WWW

***Domain-Adresse*:** Die unverwechselbare Adresse im Internet

Email: Elektronisch verschickte Nachricht

FTP: Das File Transfer Protocol für das Übertragen von Dateien zwischen verschiedenen Rechnern

Host: Ein Rechner im Internet, der Informationen bereithält (historischer Begriff)

HTTP: Protokoll für die Datenübertragung im WWW

Internet: Weltweites Netz von Computer-Netzwerken

Link: Querverweis von einer WWW-Seite zu einer anderen

Modem: Modulator/Demodulator, Gerät zur Übertragung von Comutersignalen über eine analoge Telefonleitung

Newsgroup: Diskussionsforum im Internet

***TCP/IP*:** Eine Protokoll-Suite, die die Kommunikation zwischen verschiedenen Rechnern in einem Netzwerk regelt

User: Benutzer, Teilnehmer im Internet

WWW: Das World Wide Web ist ein graphisch orientiertes hypertext-basiertes Informationssystem im Internet

Im folgenden soll das Internet als Netzwerktechnologie detailliert betrachtet werden.

Internet

Stichworte:

- DARPANET
- RFCs

Das Internet ist im Grunde ein Zusammenschluß von vielen über die ganze Welt verteilte lokale Netze, die über das UDP- oder TCP/IP-Protokoll kommunizieren. Es hat seine Ursprünge in einem Forschungsprojekt Ende der 60er Jahre, als es in den USA aus dem DARPANET (Defense Advanced Research Projects Agency Network) entstand. Heute gehören auch das Milnet, das NASA Science Internet (NSI) sowie das NSFNet (seit 1995 bei America Online) hinzu.

Jeder Standard im Internet wird durch ein Dokument gebildet, das den Titel *RFC* (Request for Comments = Aufforderung zu Anmerkungen) trägt. RFCs gibt es seit 1969, sie sind Arbeitspapiere der Forschungs- und Entwicklergruppe des Internet. Gewöhnlich ist ein RFC die Beschreibung eines Protokolls, einer Prozedur oder eines Dienstes. Es kann jedoch auch ein Statusbericht oder eine Zusammenfassung von Forschungsdaten sein. Bis Mitte 1997 gab es über 2000 veröffentlichte RFCs.

1.2 OSI – 7 Schichten-Modell

Unabhängig von der Architektur der zugrundeliegenden Rechner ist die Netzkommunikation ein sehr komplexes und abstraktes Thema. Es betrifft Hardware genauso wie Protokolle oder gar Anwendungsprogramme, die entweder das Netz ausmachen oder es benötigen. Um dieses Thema besser zu strukturieren und damit leichter auf die erhöhten Anforderungen des Marktes reagieren zu können, entwickelte die "International Standardization Organization" (ISO) 1977 ein sogenanntes Referenzmodell für "Open Systems Interconnection", das *ISO-OSI-Referenzmodell*. Hierbei handelt es sich um ein Schichtenmodell, wobei die transportorientierten Funktionen in vier und die datenverarbeitungsorientierten Funktionen in drei Schichten unterteilt sind.

Die grundlegende Idee hinter einem Schichtenmodell ist, daß jede beteiligte Schicht einer darüberliegenden Schicht bestimmte Dienste anbietet. Damit schirmt sie die höheren Schichten von Details ab, wie die betreffenden Dienste realisiert sind. Dadurch ist es möglich, daß eine Schicht n des einen Computers mit der selben Schicht n eines anderen Computers kommuniziert. Die Regeln und Konventionen dieser Kommunikation werden als das *Protokoll* der Schicht n genannt.

In der Realität kommunizieren die Schichten n nicht miteinander. Jede Schicht reicht seine Daten und zusätzliche Kontrollinformationen an die direkt darunterliegende Schicht weiter bis die tiefste Schicht erreicht ist. Unter dieser Schicht liegt das *physikalische Medium*, durch das die echte Kommunikation stattfindet.

Zwischen einem Paar übereinanderliegender Schichten besteht eine definierte Schnittstelle (*Interface*). Das Interface bestimmt die Operationen und Dienste, die die untere der oberen Schicht anbietet. Ein Satz von Schichten und Schnittstellen wird dann die *Netzwerkarchitektur* genannt. Eine Liste von Protokollen, die von einem bestimmten System genutzt werden - ein Protokoll pro Schicht - wird *Protocol Stack* genannt. Typischerweise addiert jedes Protokoll bestimmte Kontrollinformationen (*Header*) zu den Daten, wenn sie von oben nach unten durch die Schichten gereicht werden. Diese sind für den Gegenpart beim Empfänger gedacht. Diese zusätzlichen Header werden beim Empfänger dann auch auf dem Weg zur obersten Schicht wieder entfernt.

Schichten können zwei verschiedenen Arten von Diensten nach oben bereitstellen. Die eine Art ist *verbindungsorientiert* und am ehesten mit einem Telefonsystem zu vergleichen. Man wählt den Partner an, kommuniziert mit ihm und trennt die Verbindung wieder. Die zweite Art ist *verbindungslos* und

orientiert sich am Postsystem. Jede Nachricht wird mit einer vollständigen Adresse versehen und wird durch das System zum Empfänger geleitet. Hierbei kann es im Gegensatz zu verbindungsorientierten Diensten vorkommen, daß sich die Reihenfolge von verschickten Nachrichten durch unterschiedliche Verzögerungszeiten im System verändert. Jeder Dienst wird dabei durch die sogenannten *Quality of Service* charakterisiert. Diese Dienstequalität bezieht sich auf die Sicherheit der Übertragung und teilweise auch auf die Effizienz bezüglich der Geschwindigkeit.

Die sieben Schichten des im folgenden betrachteten OSI-Referenzmodells lauten von unten nach oben:

Physical Layer

(physikalische Bitübertragungsschicht): Diese Schicht definiert und beschreibt das Verfahren zur Übertragung einzelner Bits über das Übertragunsmedium (z.B. BNC-Kabel). Hierzu gehören unter anderem die Bit-Synchronisation sowie das Modulationsverfahren, das im wesentlichen die Bandbreite der Netzkommunikation bestimmt.

Data-Link Layer

(Sicherungs- oder Leitungsschicht): In dieser Schicht erfolgt die Definition des Zugriffsprotokolls (MAC = Medium Access Control) auf das physikalische Medium, die Block-Synchronisation, die Flußsteuerung, sowie die Fehlererkennung und -korrektur. Die Übertragung wird in einzelnen Datenübertragungsblöcken (Frames) sichergestellt.

Network Layer

(Vermittlungsschicht): Die Vermittlungsschicht sorgt für den Transport eines Nachrichtenblocks (Paket) von einem Endsystem zum anderen. Sie ist verantwortlich für die Adressierung, die Vermittlung, die Fehlerbehandlung und die Sequentialisierung der Datenpakete. Der Weg zwischen den Endgeräten kann hierbei sowohl physikalisch vorhanden sein oder auch nur eine logische Verbindung darstellen.

Transport Layer

(Transportschicht): Diese Schicht stellt eine Prozeß-zu-Prozeß-Verbindung zur Verfügung und trennt gleichzeitig die anwendungsbezogenen Schichten von den transportierenden. Hier werden der Datenstrom in geeignete Pakete zerlegten bzw. wieder zusammengesetzt.

Session Layer

(Verbindungs-, Kommunikationssteuerschicht): Die Sitzungsschicht ist verantwortlich für die Bereitstellung von notwendigen Sprachmittel zur Eröffnung, Durchführung, Synchronisation und zum ordnungsgemäßen Abschluß einer Sitzung zwischen den Teilnehmern. Hierbei kann zwischen verschiedenen Sitzungsarten (z.B. Punkt-zu-Punkt, Multicast) unterschieden werden.

Presentation Layer

(Datenschicht, Darstellungsschicht): Die Aufgabe dieser Schicht ist vor allem die Anpassung der auszutauschenden Daten zwischen den beiden kommunizierenden Systemen. Hier werden z.B. grundsätzlich inkompatible Datenformate von Computern verschiedener Hersteller konvertiert.

Application Layer

(Anwendungsschicht): Diese Schicht enthält alle anwendungsspezifischen Schnittstellen für die Anwendungsprogramme. Diese haben nur auf diese Schicht unmittelbaren Zugriff.

Durch dieses Modell - das sich in seiner Realisierung nicht etablieren konnte (Gründe: Timing der Einführung, Technologie mit zu vielen Schichten, Implementationsprobleme, politische Gründe) - können nun Protokolle beschrieben werden, die Standards im Netzbereich darstellen. Nicht alle Netzstandards lassen sich jedoch eindeutig auf das OSI-Referenzmodell abbilden. Dennoch hat sich durch seine klare Gliederung die Betrachtungsweise eingebürgert, Netzstandards in Relation zu diesem Modell zu sehen. Als den beiden unteren Schichten (Physical Layer, Data-Link Layer) analog können daher die *IEEE 802.X*-Standards betrachtet werden, die Kabel, physikalische Topologie, elektrische Topologie und Zugriffsschemata für verschiedene Netzprodukte beschreiben.

Layer 7	Application	Message Passing	HTTP,FTP,DNS,Telnet u.v.m
Layer 6	Presentation	Encoding	""
Layer 5	Session	Authentication & Encryption	""
Layer 4	Transport	Streams & Segments	TCP
Layer 3	Network	Datagrams	IP
Layer 2	Data Link	Frames & Packets	Ethernet Host Adapter
Layer 1	Physical Hardware	Signaling & Wiring	Ethernet Kabel

(Tabellarische Zusammenfassung)

Anwendung

Anwendung durch Endnutzer

- **Endpunkt-zu-Endpunkt-Protokolle**

Schicht 7: Application Layer -- Verarbeitungsschicht (Anwendungsschicht, Anwenderebene): File-Transfer, e-mail, Virtual Terminal (Remote login), Directory usw.

Schicht 6: Presentation Layer -- Darstellungsschicht (Datendarstellungsschicht, Datenbereitstellungsebene): Standardisiert Datenstrukturen (u.a. Kodierung, Kompression, Kryptographie)

Schicht 5: Session Layer -- Kommunikationsschicht (Kommunikationssteuerungsschicht, Steuerung logischer Verbindungen, Sitzungsebene): Hilft Zusammenbrüche der Sitzung und ähnliche Probleme zu beheben

Schicht 4: Transport Layer -- Transportschicht (Ende-zu-Ende-Kontrolle, Transport-Kontrolle):

Stellt höheren Schichten zuverlässige Ende-zu-Ende-Verbindungen (zwischen Sender und Empfänger) zur Verfügung

Protokolle für die Kommunikation zwischen unmittelbar benachbarten Einrichtungen auf der Übermittlungsstrecke

Schicht 3: Network Layer -- Vermittlungsschicht (Paketebene, Netzwerkebene): Routing der Datenpakete (OSPF, RIP als Routingprotokolle)

Schicht 2: Data Link Layer -- Sicherungsschicht (Verbindungssicherungsschicht, Verbindungsebene, Prozedurebene):

Aufteilung des Bitstromes in Einheiten (Pakete) und Austausch dieser Einheiten unter Anwendung eines Protokolls

Schicht 1: Physical Layer -- Bitübertragungsschicht (physikalische Ebene): Übertragung des Bitstromes über einen Kommunikationskanal. Standardisierung der Netzwerk-Leitungen und -Anschlüsse sowie ihrer physikalischen Eigenschaften. Vorwiegend Aufgabenbereich des Elektro-Ingenieurs: Physikalische Verbindung zu Netzwerk-Abschluß-Geräten

Netzwerk

Physisches Kommunikationsnetzwerk

Die Schichten 4 -7 betreffen Protokolle für die Kommunikation von Endpunkt zu Endpunkt (Sender zu Empfänger). Die Schichten 1 -- 3 betreffen Protokolle für die Kommunikation zwischen unmittelbar benachbarten Einrichtungen auf der Übermittlungsstrecke, also vom Sender zum ersten Vermittlungspunkt, von Vermittlungspunkt zu nächstem Vermittlungspunkt, und wieder vom Endvermittlungspunkt zum Empfänger.

Netzwerk-Stationen können nur durch den Gebrauch von Datenpaketen *(Packets)* miteinander kommunizieren. Die Art der Pakete hängt von der Technologie (Ethernet, Token Ring, FDDI) und den Software-Protokollen (z.B. TCP/IP) ab.

Jedes Datenpaket besteht aus:

- Netzwerk-Kopffelder *(Network headers)*
- Datenfeld *(Data field)*
- Netzwerk-Schlußfelder *(Network trailers)*

Datenpaket		
Netzwerk-Kopffeld	Datenfeld	Netzwerk-Schlußfeld

Netzwerk-Kopf- und -Schlußfelder enthalten Informationen, die der Netzwerk-Hardware und -Software mitteilen, wie ein Datenpaket zu behandeln ist, z.B. Netzwerk-Adresse, Fehlerkorrektur usw.

Jede im betreffenden Netzwerk verwirklichte Schicht des OSI- Referenzmodells (mit Ausnahme der Bitübertragungsschicht) fügt dem Datenpaket Information in einem Kopffeld (die Verbindungssicherungsschicht auch im Schlußfeld) hinzu.

Dies geschieht nicht dadurch, daß die in dem betreffenden Netzwerk zulässige Paketlänge vergrößert wird, sondern die Kopffelder und Schlußfelder belegen Platz innerhalb dieser Paketlänge, so daß der Platz für das Datenfeld kleiner wird. Beim Sender fügt so jede Schicht sukzessive -- angefangen bei der Anwendungsschicht -- ein entsprechendes Kopffeld mit entsprechenden Informationen hinzu. Beim Empfänger verarbeitet in umgekehrter Richtung -- beginnend mit der Datenverbindungssicherungs-Schicht -- jede Schicht den ihr entsprechenden Kopfsatz, entfernt ihn und gibt das Datenpaket an die nächsthöhere Schicht weiter.

1.3 Netzwerktopologien (Komponenten)

Stichworte:

- LANs, MANs und WANs
- Ethernet - Fast Ethernet
- Repeaters, Bridges, Hubs, Routers, Gateways
- Netzwerk-Topologien
- Konzepte: Point-to-Point, Store-and-Forward und Packet-Swiched

Institute, Behörden und Firmen vernetzen in immer stärkerem Maße ihre verwendeten Rechnerplattformen. Dies dient im wesentlichen zum leichteren Austausch wichtiger Daten und Information, der Nutzung von netzweiten Ressourcen (Drucker, Massenspeicher etc.) sowie der einfacheren Wartbarkeit von einer entfernten Konsole oder gar zur multimedialen Kommunikation. Die physikalische Ausdehnung dieser lokalen Netze (*LAN*s = Local Area Networks) beschränkt sich in der Regel auf ein oder mehrere Gebäude in relativer Nähe (< 10 km, siehe auch Tabelle 1.1).

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

Tabelle 1.1: Klassifizierung verbundener Prozessoren nach ihrer Entfernung

Die Unterscheidungskriterien von LANs sind

- ihre Größe
- ihre Übertragungstechnologie
- ihre Topologie

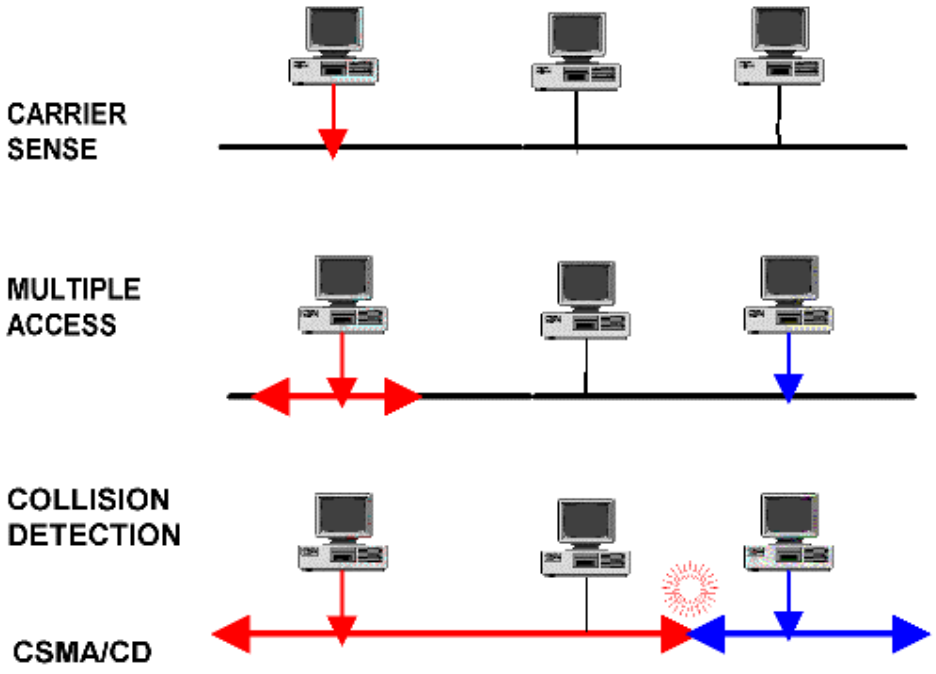
Die Größe von LANs ist beschränkt. Die Beschränkung ist bekannt und wird durch maximal erlaubte Verzögerungszeiten innerhalb des Netzwerks bestimmt. Typische Verzögerungszeiten liegen im Bereich von 10 Mikrosekunden.

Die Übertragungstechnologie gängiger LANs besteht zumeist aus einem Kabel, das alle Maschinen verbindet. Als Topologie ist daher entweder ein Bus oder ein Ring vorgegeben. Neuere Technologien fordern ein eigenes Kabel für jeden angeschlossenen Rechner, was zu einer Sterntopologie mit einem zentralen Sternverteiler (Hub) führt.

Die verbreitetsten LANs sind *Ethernet* (Bus: 10 Mbit/s, 100 Mbit/s und 1 Gbit/s) und *Token-Ring* (Ring: 4 bzw. 16 Mbit/s).

Diese Standards spezifizieren verschiedene Netzkabeltypen, -topologien und -zugriffe. Bei Ethernet (= IEEE 802.3) kann jeder Rechner als Master zu jeder Zeit auf das Netzwerk senden. Gibt es hierbei einen Konflikt zwischen zwei gleichzeitig sendenden Rechnern, wartet jeder Rechner für eine über Zufallsgeneratoren bestimmte Zeit um dann wieder einen Sendeversuch zu starten. Bei Token Ring (= IEEE 802.5) bestimmt ein im Netzwerk umlaufendes "Token" den sendenden Zugriff jedes Rechners.

Insbesondere das Ethernet spielt im Internet-Umfeld eine wichtige Rolle (wobei der Name von Xerox stammt und an den "Äther" - dem Kabel - erinnert, der nach der Lehrmeinung vor 1887 nötig war um Strahlung zu transportieren). Wesentlich ist beim Ethernet die Art zur Vermeidung von Kollisionen, was im MAC-Sub-Layer der Data-Link-Schicht geschieht. Es handelt sich dabei um das Protokoll *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD). Es sorgt dafür, daß bei einer Kollision beim Senden von Daten von zwei Rechnern die Transmission sofort unterbrochen wird. Die korrumpierten Daten werden verworfen und nach Zeiten, die von Zufallsgeneratoren bestimmt werden, beginnen die Rechner wieder aufs neue ihre Daten zu senden.



(Beispiel für das CSMA/CD Protokoll)

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

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

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

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

Die gängigen Kabelstandards für die Übertragung von 100 MBit/s sind daher wie in der folgenden Tabelle aufgeführt:

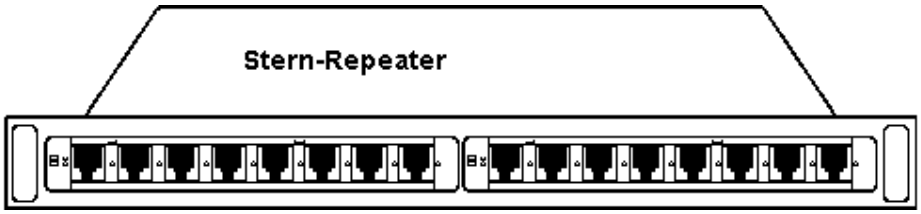
Name	Kabel	Maximale Segmentlänge	Vorteile
100Base-T4	Twisted Pair (Cat. 3)	100 m	Alter Kabeltyp, aber nur unidirektional
100Base-TX	Twisted Pair (Cat. 5)	100 m	Full Duplex bei 100 Mbps
100Base-FX	Fibre Optics	2000 m	Full Duplex bei 100 Mbps

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

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

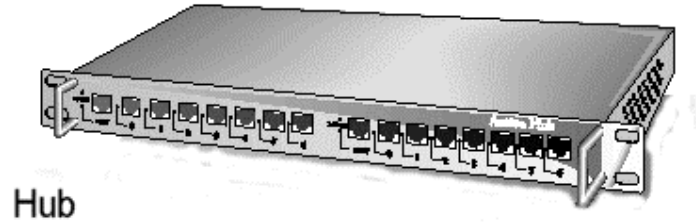
Die elektrische Signale können auf den physikalischen Leitungen nur eine begrenzte Distanz zurücklegen, ohne Leistung in einem gewissen Rahmen zu verlieren. In LANs werden daher Repeater, Bridges, Hubs, Routers und Gateways genutzt, um die Signale zu regenerieren und mit anderen LANs oder Wide Area Networks (*WAN*s) zu kommunizieren.

Repeaters: Sie wiederholen elektrische Signale und frischen sie damit auf. Damit erlauben sie die Verbindung zweier Kabelabschnitte zur Verlängerung des Netzstrangs.



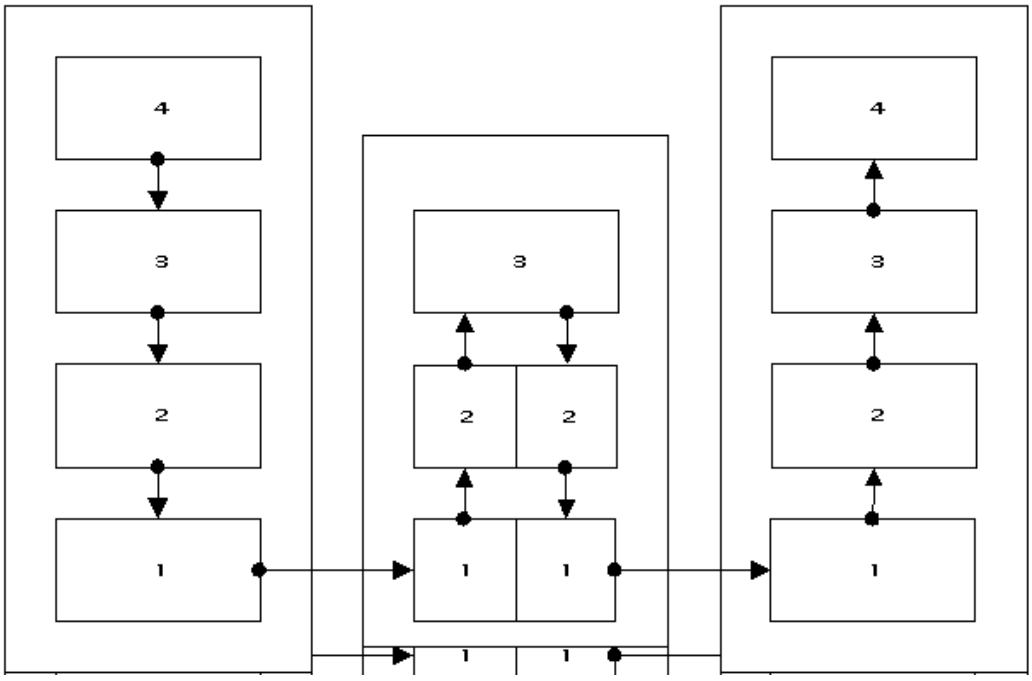
Bridges: Sie erlauben die Verbindung zweier LANs. Jede Station im jeweiligen LAN kann damit auf Ressourcen des anderen LANs zugreifen. Bridges verbinden die OSI Sicherungsschicht des einen LANs mit der Sicherungsschicht eines anderen LANs und erlauben daher die Kombination verschiedener Netzkabeltypen. An dieser Schnittstelle werden Protokolltypen übersetzt.

Hubs: Sie arbeiten wie die Bridges zumeist in der OSI-Sicherungsschicht, haben jedoch zumeist noch einige Funktionalitäten aus dem Network Layer. Sie sind für sternförmige Netzwerktopologien gedacht und leistungsmäßig oftmals am oberen Ende des Spektrums angesiedelt.


Hub

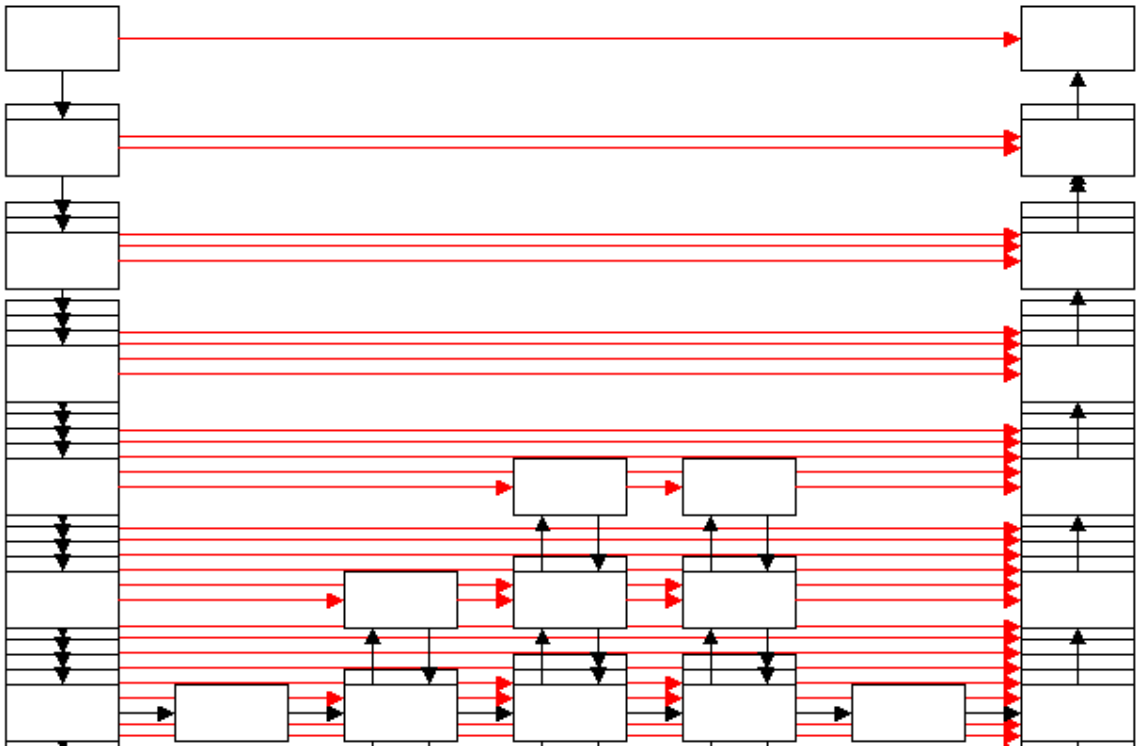
Switches: Arbeiten wie Hubs, lassen aber komplexe Designmöglichkeiten im Network Layer (2) zu. Hier können logische LAN's die traditionellen physischen Lan's ablösen. Starke Backbones möglich.

Routers: Sie arbeiten im OSI Network Layer (2) und können je nach Adresse eines Datenpakets dessen Weiterleitung oder die Zurückweisung bewirken. Dies kann helfen (unnötigen) Netzverkehr in LANs drastisch zu reduzieren, da Datenpakete nur durchgelassen werden, wenn die Zieladresse "jenseits" des Routers liegt.



(Diese Abbildung verdeutlicht die Funktionsweise eines Routers - hier in der Mitte abgebildet)

Gateways: Sie arbeiten in der OSI Transportschicht (oder höher) und erlauben es Netzen, die auf völlig unterschiedlichen Protokollen basieren, miteinander zu kommunizieren.



(Diese Abbildung veranschaulicht die Kommunikation zwischen einem Sender (ganz links) und einem Empfänger (ganz rechts). Dazwischen ist (von links nach rechts) ein Repeater, dann eine Bridge, ein Router, noch ein Router, ein Repeater und schliesslich der Empfänger.)

Wie schon beim OSI-Modell festgestellt wurde, muß bei der Netzwerktechnologie zwischen Diensten (wie X.25, Frame Relay, ATM oder B-ISDN) und Protokollen (wie z.B. TCP/IP) unterschieden werden. Im folgenden soll ein näherer Blick auf die Internet-relevanten Dienste und Protokolle geworfen werden.

Die gesamte Kommunikation im Internet basiert auf dem TCP/IP-Protokoll und dem Socket-Mechanismus (= bidirektionale Verbindung zwischen zwei Computern). Sowohl unter UNIX als auch unter Windows NT bzw. Windows 95 sind die TCP/IP-Funktionalitäten schon im Betriebssystem enthalten. Für andere Betriebssysteme gibt es entsprechende Protokoll-Stacks.

Relevante Netzwerkdienste

Stichworte:

- X.25
- Frame Relay
- Breitband-ISDN und ATM

Insbesondere die nationalen Telekommunikationsbetreiber bieten eine Reihe von Netzwerkdiensten für ihre Kunden an. Die wichtigsten sollen im folgenden kurz vorgestellt werden.

X.25

Viele ältere Netzwerke - insbesondere in Europa - folgen einem Standard, der X.25 genannt wird. Dieser wurde in den 70er Jahren von der CCITT entwickelt, um eine Schnittstelle zwischen öffentlichen Netzwerken und ihren Kunden bereitzustellen. Technisch gesehen läßt sich X.25 in einem Schichtenmodell mit Physical Layer (Protokoll: X.21), Data Link Layer und Network Layer darstellen. Diese sorgen für eine sehr sichere Verbindung auch über Telefonleitungen.

Die Hauptaufgabe vom verbindungsorientierten X.25 ist die Anbindung von Terminals an ihre Hosts. Die dabei erreichte Datenrate liegt bei 64 kBit/s, was für aktuelle Anforderungen oftmals nicht mehr ausreichend ist. Die Paketgröße beträgt dabei bis zu 128 Bytes.

Frame Relay

Frame Relay bietet einen grundlegenden verbindungsorientierten Dienst an. Dieser transportiert Daten zu günstigen Kosten von A nach B ohne komplexe Protokolle zur Fehlerkorrektur einzusetzen. Durch die immer besseren (digitalen) Telefonleitungen und die ausreichende Leistungsfähigkeit der Endgeräte für eigenen Fehlerkorrektur-Algorithmen gewinnt Frame Raley an Bedeutung.

Ein Frame (= Paket) besteht aus bis zu 1600 Bytes und wird typischerweise über eine gemietet Leitung verschickt. Eine 10-Bit Zahl definiert dabei ein virtuelles Gerät, das angesprochen wird. Die Übertragungsgeschwindigkeit erreicht bis zu 1,5 MBit/s.

Breitband-ISDN und ATM

Eine recht neuer Dienst ist das Breitband-ISDN (Integrated Services Digital Network). Es wurde für Anwendungen wie Video-on-Demand, multimediale Email, Musik in CD-Qualität, LAN-zu-LAN-Verbindungen usw. geschaffen. Dies alles basiert dabei auf normalen (digitalen) Telefonleitungen.

Die darunterliegende Technologie wird ATM (Asynchronous Transfer Mode) genannt, da sie nicht mehr synchron, d.h. an einen systemweiten Zeitgeber gebunden ist. Hierbei transportiert ATM alle Informationen in kleinen Paketen (genannt Zellen), die eine fixe Länge haben. Jede Zelle ist 53 Bytes lang, wobei 5 Bytes für den Header und die restlichen 48 Bytes für die Nutzdaten sind.

Der Vorteil bei der Übertragung von Zellen ist, daß im Gegensatz zur traditionellen Technologie die Datenrate sowohl konstant (für Audio und Video) als auch variabel (für Daten) sein kann. Die typischen Geschwindigkeiten liegen hierbei bei 155 und 622 MBit/s.

Um nun die Ethernet-Standards und TCP/IP auch über ATM verwenden zu können, muß eine spezielle Anpassungskomponente eingeführt werden: die LAN-Emulation. Nur mit ihrer Hilfe ist es möglich eine kostengünstige Migration von Ethernet-basierten Computern in Richtung ATM ohne Austausch aller Netzwerkkomponenten (Netzwerkkarten, Routers, Hubs usw.) durchzuführen.

Topologien und Architekturen

Um den Datenverkehr zwischen Firmen oder Filialen innerhalb von Städtegrenzen zu ermöglichen, wurden *MANs* (Metropolitan Area Networks) als die vergrößerte Ausgabe von LANs installiert. Ihre wichtigsten Vertreter sind *FDDI* (Fibre Distributed Data Interface) mit Transferleistungen von 100 Mbit/s und *DQDB* (Distributed Queue Dual Bus = IEEE 802.6) mit skalierbaren Übertragungsraten von 34, 45 oder 140 Mbit/s.

Eine große Bedeutung auf dem Netzmarkt besitzen weltumspannende *WANs* (Wide Area Networks). Sie basieren in der Regel auf den physikalischen Leitungen, die von den nationalen Telekom-Unternehmen betrieben werden. Ein prominenter Vertreter einer physikalischen Netztechnologie ist *ISDN* (Integrated Service Digital Network, 128 kBit/s bis 2 Mbit/s). Eine neue Technologie für WANs, die jedoch auch für LANs und MANs eingesetzt werden kann, ist *ATM* (Asynchronous Transfer Mode), die Datentransferraten von 25, 50, 155 oder 622 Mbit/s erlaubt und speziell für zeit- und synchronisationskritische multimediale Datentypen geeignet ist.

Die Datentransmission über WANs basiert sehr stark auf dem Einsatz von Switching-Elementen bzw. Routing-Komponenten, die die Daten von einem Endsystem über Kontinente zu einem anderen Endsystem leiten können. Die Prinzipien wie dieses Weiterleiten geschehen kann, werden *Point-to-Point*, *Store-and-Forward* oder *Packet-Switched* genannt. Die Daten werden dabei in

Paketen über das Netz geschickt. Werden die Pakete sehr klein und haben immer eine konstante Größe, werden sie *Zellen* (Cells) genannt.

Die Topologie der zugrundeliegenden WANs kann sehr unterschiedlich aussehen. Die Möglichkeiten reichen von einem Stern über einen Ring, einen Baum, einem Komplettverbund (n-zu-n) und gekoppelten Ringen bis hin zu vollkommen irregulären Netzen. Besonders komplex wird die Topologie dann, wenn auch kabellose Netzwerkteile durch Funkstrecken und Satelliten einbezogen werden.

Die Verbindung sehr vieler WANs über Gateways ergibt dann das *Internetwork* oder einfacher das *Internet*!

Achtung ! Alle hier gemachten Angaben über maximale Leistungsfähigkeit sind spätestens nächste Woche wieder überholt ! Diese Aussage soll ediglich verdeutlichen, dass speziell in den Layern 1 und 2, das Breitband-Problem gelöst werden soll. Daher sind hier Aussagen über Leistungsfähigkeit mit Sorgfalt zu geniessen !

Client/Server-Architektur

Stichworte:

Peer-to-Peer- und Client/Server-Netze

(näheres dazu erfahren Sie in der Vorlesung über Systemtechnik)

Internet - Intranet - Extranet

Stichworte:

Unterscheidung von Internet, Intranet und Extranet

Pluspunkte für ein Intranet

- ASCII-Text
- Internet, Intranet und Extranet definieren sich wie folgt:

Internet: Netzwerktechnologie auf der Basis von TCP/IP (WWW, Email, FTP, ...)

Intranet: Internet-Technologie eingesetzt in firmeninternen Netzen - auch über Ortsgrenzen hinaus (Virtuelles LAN)

Extranet: Kommunikationstechnologie des Firmennetzes mit der Außenwelt (Stichwort: Firewall)

Pluspunkte für ein Intranet mit Internet-Technologie:

- Vereinfacht das interne Informationsmanagement und die Kommunikation
- Integriert das interne Netzwerk in das Internet. Dadurch Erleichterung der Kommunikation mit Kunden und Partnern
- Integriert neue Technologien in bestehende Systeme
- Vereinfacht Anwendungsentwicklung und Systemadministration
- Für den Endanwender einfach zu bedienen, schnell und relativ zuverlässig
- Sicher, kosteneffizient und skalierbar

1.4 Protokollverhalten in unterschiedlichen Topologien

Microsoft Windows Protocol Layering

Diese Protokollpalette stammt noch vom "alten" Lan Manager her. Was Sie also unten lesen, kann in modernen Netzwerken in dieser Form nicht mehr angewendet werden. Da NetBeui nicht routbar ist, kann es im Internet keine Verwendung finden. Als Transport Layer für Netbios kann aber sowohl, IP als auch IPX verwendet werden.

Näheres dazu erfahren Sie in der Vorlesung über Systemtechnik.

Network Interface

Like the other network protocols, the Microsoft Windows protocols can be based on a variety of network interface types. Interestingly, though, it often does this by having its datagrams placed inside the datagrams from another network protocol suite such as IPX or IP. This techniques is referred to variously as piggybacking or tunneling depending on the situation.

NetBEUI

The lowest level software in the Microsoft Windows protocol suite is NetBEUI. It fills the same role as IP and IPX, but is not "routable." That is, there is no provision for sending NetBEUI datagrams trough routers to create an internetwork of NetBEUI-based networks. NetBEUI is really just a thin layer to hide the details of the network interface layer from NetBIOS. It is sometimes called NBF, the NetBIOS Frame format.

NetBIOS

NetBIOS is the name of the middle layer in the Microsoft Windows protocol suite. Typically, current systems using NetBIOS piggyback the datagrams from this layer on top of IPX (via a software product called "NWLink NetBIOS") or IP. The software for layering NetBIOS over IP is called by different names. The user interface seems to refer to it as the "WINS Client," technical folks tend to refer to it as "NBT" (for "NetBIOS over TCP/IP"), and the Windows NT documentation refers to it as NetBT. All of these names refer to the use of RFC1001 and RFC1002 which leads yet others to refer to this practice as RFCNB.

SMB

SMB, the Server Message Block protocol is used by the Microsoft Windows as a transport layer protocol. Like NetBIOS, SMB can be layered over either NetBIOS or IPX to promote maximum marketability. The best reference for SMB is found in the SAMBA documentation. At the Ball State Computer Science Department we

use SAMBA to supply SMB services on our Sun Solaris (Unix) timesharing machine. This allows our Microsoft Windows PCs to avail themselves of the services of the Sun for file-sharing and print-sharing in a very simple way without buying any software for the many PCs.

Novell Netware Protocol Layering

The protocol suite developed by Novell for use with its NetWare LAN system is extremely popular. Upon close examination it is clearly an outgrowth of the Xerox Networking System (XNS) developed at the Xerox Palo Alto Research Center (PARC). Xerox PARC was the center of many popular developments in the field of computer science including Ethernet and the graphical user interface (GUI). XNS included the precursors to several of the protocols we will be studying including ARP and RIP. It also included the first popular remote procedure call (RPC) system: we will be studying the Sun RPC system as well.

Network Interface

The IPX protocol can be layered on a variety of data link layer protocols. As a proprietary protocol, Novell controls the standards and standardization process for doing so. Hence, the set of such protocols is limited in comparison to the more open IP protocol suite. On the other hand, Novell provides commercial-grade support for its implementations of IPX on network protocols and network interface hardware vendors can have their products certified by Novell for compatibility. Just because an IP standard exists for a given data link layer protocol, doesn't mean it is possible to go out and buy an implementation that has commercial-grade support.

The Novell system is marketed as a LAN system and hence supports popular LAN data link protocols but has much less support for WAN data link protocols. However, it has many different ways of interfacing with the data link protocols based on the popular Ethernet wiring systems.

IPX

IPX provides essentially the same level of functionality as IP and clearly fits at layer 3 of the ISO reference model. However, a machine that functions as an IP router might not also function as an IPX router and vice versa. Devices that provide routing for both protocols are known as multiprotocol routers and tend to be expensive.

Since WAN routers for IP became popular, it has become standard for IPX datagrams to be placed inside IP datagrams for WAN delivery. This kind of creativity will be discussed in greater detail in the later section on network protocol encapsulation techniques.

SPX & NCP

The Novell protocol suite includes several protocols that utilize IPX directly and hence might be considered transport layer protocols. Notably, the sequenced packet exchange (SPX) protocol, which is a direct descendent of the XNS protocol by the same name, provides a reliable datagram stream service. SPX can be compared to TCP in that they both are transport layer protocols that offer a good measure of reliability. However, TCP presents itself to higher layers as a stream of individual bytes whereas SPX provides group of bytes bundled together and delivered to the higher layer as a single package. SPX typically takes less CPU processing to manage this lesser abstraction but does not use the network as efficiently as a good TCP implementation.

The NetWare Core Protocol (NCP) is used to provide file sharing. Since file sharing is one of the primary features of the suite, it may be much more common than SPX. NCP is comparable to NFS in the TCP/IP suite and should probably be considered an application layer protocol despite the fact that it does not have an underlying transport protocol to support it.

1.5 Die TCP/IP Protokollfamilie

Stichworte:

- Internet Protocol
- Transmission Control Protocol
- TCP/IP über Modems
- Die TCP/IP Protokollfamilie

IP: Das Network Layer im Internet

Auf der Network-Schicht kann man das Internet als eine Sammlung von Subnetzen oder Autonomen Systemen betrachten, die miteinander verbunden sind. Der Klebstoff, der alles zusammenhält ist IP, das *Internet Protocol*.

Grundsätzlich funktioniert die Kommunikation im Internet wie folgt: Das Transport Layer nimmt die Datenströme und bricht sie in *Datagramme* auf. Theoretisch können Datagramme bis zu 64 kBytes groß sein, in Wirklichkeit sind sie selten größer als 1500 Bytes. Jedes Datagramm wird über das Internet transportiert und dabei möglicherweise sogar noch in kleiner Fragmente zerteilt. Wenn die Bruchstücke dann an ihrem Ziel angelangen, werden sie von der dortigen Network-Schicht wieder zu den originalen Datagrammen zusammengesetzt. Diese werden dann an den Transport Layer weitergereicht, von wo sie dem Eingangsdatenstrom des empfangenden Prozesses zugeleitet werden.

Das IP-Datagramm besteht aus dem Header und dem Datenteil. Der Header unterteilt sich in einen 20 Bytes langen statischen Teil und einen optionalen Teil variabler Länge.

Die Übertragung geschieht in der Big-Endian-Reihenfolge, d.h. von links nach rechts mit dem High-Order-Bit des Versionsfeld als erstes (SPARC ist Big-Endian, Pentium ist Little-Endian). Auf Little-Endian-Maschinen muß die Konversion sowohl beim Sender als auch beim Empfänger in Software durchgeführt werden.

Die einzelnen Felder des IP-Headers haben folgende Bedeutung:

Feldname	Beschreibung
Version (4 Bit)	Versionsinformation des Datagramm-Protokolls
IHL (4 Bit)	Länge des IP-Headers in 32-Bit-Worten (Minimum ist 5, Maximum ist 15)
Type of Service (8 Bit)	Hier kann die spezielle Behandlung der Daten im Bezug auf Zuverlässigkeit und Geschwindigkeit (z.B. für Sprachdaten) bestimmt werden
Total Length (16 Bit)	Diese Gesamtlänge beinhaltet sowohl den Header als auch die Nutzdaten (Maximum 65.535 Bytes)
Identification (16 Bit)	Bei fragmentierten Datagrammen dient dieses Feld der Zuordnung
DF, MF (je 1 Bit)	*Don't Fragment* und *More Fragment* Flags zur Behandlung der Fragmentierung bei einzelnen Datagrammen
Fragment Offset (13 Bit)	Bestimmt die Position der Daten eines Fragments innerhalb des originalen Datagramms
Time to Live (8 Bit)	Bestimmt die Lebenszeit eines Pakets in Sekunden bzw. "Router Hops", um Endlosschleifen zu verhindern (Maximum ist 255)
Protocol (8 Bit)	Bestimmung des Transportprozeßes (TCP oder UDP)
Header Checksum (16 Bit)	Prüfsumme des Headers zur Vermeidung von Übertragungsfehlern
Source Address (32 Bit)	Adresse des Quell-Computers
Destination Address (32 Bit)	Adresse des Ziel-Computers
Options	Zusätzliches Feld variabler Länge mit fünf Optionen: - Security (Sicherheit) - Strict Source Routing (Angabe des kompletten Übertragungspfads) - Loose Source Routing (Liste von zu verwendenden Routers) - Record Route (Protokollieren des Übertragungspfads) - Timestamp (Protokollieren des Übertragungspfads und der Zeit)

Tabelle 3.1: Die Felder des IP-Headers

Die Konvention für die IP-Adressen basiert auf einem 32-Bit-Wert, wobei die Darstellung im Dezimalsystem erfolgt. Jeder 8-Bit-Dezimalwert wird durch einen Punkt von seinem Nachbarn getrennt (z.B. 192.44.32.1). Der 32-Bit-Wert kodiert die Netzwerk- und die Host-Nummer der zugrundeliegenden Adresse.

Hierbei sind die Netzwerke in verschiedene Klassen eingeteilt:

Klasse	ID	Adresse	Adressraum
A	1 Bit (0)	7 Bits (Network) + 24 Bits (Host)	1.0.0.0 bis 127.255.255.255
B	2 Bits (10)	14 Bits (Network) + 16 Bits (Host)	128.0.0.0 bis 191.255.255.255
C	3 Bits (110)	21 Bits (Network) + 8 Bits (Host)	192.0.0.0 bis 223.255.255.255
D	4 Bits (1110)	28 Bits Multicast-Adresse	224.0.0.0 bis 239.255.255.255
E	5 Bits (11110)	27 Bits Reserviert für die Zukunft	240.0.0.0 bis 247.255.255.255

Tabelle 3.2: IP-Adressenformat

Besondere IP-Adressen sind hierbei die folgenden:

127.xxx.yyy.zzz: Loopback (Rückkopplung auf sich selbst)

255.255.255.255: Broadcast auf dem lokalen Netzwerk

Network.255.255.255: Broadcast auf einem entfernten Netzwerk

Das Netzwerk einer bestimmten Klasse kann für interne Unterteilungszwecke (weniger Belastung des Backbones, Aufteilung in Abteilungen) in Subnetze eingeteilt werden. Die Rechner innerhalb des Subnetzes werden dabei direkt angesprochen, alle anderen über ein *Default Gateway* d.h. typischerweise einen Router. Eine Subnetzmaske für beispielsweise 256 Rechner lautet 255.255.255.0. Diese Maske wird über bool'sche Operationen mit der Rechneradresse verknüpft und gibt darüber Auskunft, ob ein anderer Rechner zum selben Subnetz gehört oder nicht.

Die Tage des heutigen Adreßschemas von IP sind gezählt, denn die gültigen Adressen werden durch die enorme Ausbreitung des Internets knapp. Sollen jedoch wie geplant Millionen neuer Maschinen in das Internet aufgenommen werden, muß dieser Zustand verbessert werden. Seit 1990 wurde daher die Arbeit an einer neuen IP-Konvention begonnen (IP Version 6, genannt IPv6). Die **Hauptziele von IPv6 waren dabei:**

- Unterstützung von Milliarden von Rechnern mit einer effizienten Methode zur Adreßraumbelegung
- Reduktion der Größe der Routing-Tabellen
- Vereinfachung des Protokolls, damit Router die Pakete schneller bearbeiten können
- Bessere Sicherheit (Authentifikation und Eigentumsrechte)
- Bessere Beachtung des Servicetyps (speziell für Echtzeitdaten)
- Erweiterbarkeit des Protokolls für die Zukunft
- Möglichkeit des neuen und des alten Protokolls über längere Zeit zu koexistieren

Die endgültige Spezifikation von IPv6 wurde 1993 in den RFCs 1883 bis 1887 festgelegt. Die Adreßfelder wurden dabei von 4 Bytes auf 16 Bytes erweitert. Dies ergibt 2^{128} = 3 x 10^{38} Adressen. Wäre die gesamte Erde (Land *und* Wasser) mit Computern bedeckt, würde IPv6 7 x 10^{23} IP-Adressen pro Quadratmeter erlauben. Dies liegt schon im Bereich der Anzahl der Moleküle auf dieser Fläche. Bei einer pessimistischen Abschätzung der effektiven Verteilung von Adressen kann noch immer mit etwa 1000 Adressen pro Quadratmeter gerechnet werden.

Die anderen Änderungen betreffen Priorität des Datenstroms (z.B. für Echtzeit-Multimedia), spezielle Mechanismen für Pakete, die einem führenden Paket folgen, maximale Lebenszeit des Pakets und limitierte Anzahl der zu durchlaufenden Netzwerkkomponenten (Hop Limit). Die Kompatibilität mit dem alten IP-Standard wird durch Vereinbarungen gewährleistet, die spezielle Bitfolgen zur Erkennung der Konvention umfassen.

Da IP in der Regel segmentiert wird (anhand der verschiedenen Adressklassen, und dann in Subnetze) muss es um Traffic-Overhead zu vermeiden geroutet werden. Router benötigen als Orientierung dazu sogenannte Routingprotokolle um zu wissen, welche Destination Address wohin geroutet werden soll. Solche Routingprotokolle sind RIP und OSPF.

TCP und UDP:

Das Internet besitzt zwei Hauptprotokolle im Transport Layer, wobei das eine verbindungsorientiert (TCP) und das andere verbindungslos (UDP) (RFC 768) ist. Hierbei ist UDP grundsätzlich identisch mit IP bis auf einen sehr kleinen Header. TCP (Transmission Control Protocol) wurde speziell dafür designed einen verläßlichen Punkt-zu-Punkt Byte-Strom über ein unzuverläßiges internationales Netzwerk zu ermöglichen. Ein solches Netzwerk unterscheidet sich von einem Intranet, da es unterschiedlich aus Sicht der Topologie, der Bandbreite, der Verzögerungen, der Paketgrößen und vieler anderer Parametern sein kann. TCP wurde so ausgerichtet, um sich dynamisch auf diese Eckdaten einstellen zu können.

TCP wurde zunächst über den RFC 793 definiert. Nach einiger Zeit wurden Fehler und Inkonsistenzien verbessert sowie Erweiterungen spezifiziert (RFCs 1122 und 1323). TCP sorgt im Gegensatz zu IP für die Garantie, daß Pakete korrekt übertragen und in der richtigen Reihenfolge wieder zusammengesetzt wurden.

TCP ist vom OSI-Modell her gesehen die unterste Schicht bei der zwei über mehrere Netzwerkknoten getrennte Systeme in Verbindung stehen. IP vermittelt ja nur zwischen jeweils zwei benachbarten Knoten. Die Kommunikation über TCP vermittelt dem Benutzer das Gefühl, dass die zwei entfernten Rechner wie in einem LAN miteinander verbunden sind, obwohl noch drei Schichten darunter "weitergearbeitet" wird.

Die verschiedenen TCP-Services werden dadurch bereitgestellt, daß sowohl Sender als auch Empfänger Kommunikationsendpunkte erzeugen, die *Sockets* genannt werden. Jeder Socket hat eine *Socket-Nummer* (Adresse), die aus der IP-Adresse des Rechners und einer lokalen 16-Bit-Zahl (dem *Port*) besteht. Um einen TCP-Service zu erhalten muß die Verbindung explizit zwischen dem Socket der sendenden und dem Socket der empfangenden Maschine etabliert werden. Die Verbindung einer IP Adresse mit einer Portnummer nennt man Socket. Ein Socket identifiziert einen Anwendungsprozess eindeutig. Standardports müssen einer Applikation nicht speziell mitgegeben werden, wenn diese schon dafür vorgesehen ist. Mann kann diese Ports dementsprechend aber auch ausnützen. Versuchen Sie doch mal eine Telnetsitzung mit Port 25 und schauen dann, was passiert !

Port-Nummern unter 256 werden *Well-known Ports* genannt und sind für Standard-Services reserviert. Möchte ein Prozeß beispielsweise eine Verbindung zu einem Rechner aufnehmen, um einen Datentransfer über FTP zu starten, so benutzt er den Port 21. Die Liste der Well-known Ports steht im RFC 1700.

Aufgaben von TCP:

- Nachrichtensegmentierung: Zerlegung längerer Datenblöcke in mehrer Pakete (jeweils versehen mit einer Paket ID), die dann in einer gemeinsamen Paketsequenz über einen logischen Kanal gesendet werden.
- Adressbildung
- Fehlererkennung
- Sequenzbildung: (three-way-handshake)
  Anforderung der Transportverbindung - Annahme der Transportverbindung - Start der Datenübertragung
- Zustellung zu benannten Prozessen (Ports)
- End to End Control (Flusskontrolle)

Zusammengefasst:

- IP Adresse des Servers identifiziert Computer (genauer: Schnittstelle)
- Portnummer des Server spezifiziert einen Service auf diesem Computer
- Die Kombination von Adresse und Portnummer identifiziert eine Anwendung, and die ein Datenpaket übermittelt werden soll eindeutig.
- IP Adresse des Clients + dynamisch zugeteilte Portnummer (bleibt während einer Session dieselbe) identifiziert Client b.z.w. Session als eindeutig.

Die SERVICES-Datei von Windows NT 4.0 sieht beispielsweise folgendermaßen aus:

```
echo                7/tcp
echo                7/udp
discard             9/tcp    sink null
discard             9/udp    sink null
systat             11/tcp
systat             11/tcp    users
daytime            13/tcp
daytime            13/udp
netstat            15/tcp
qotd               17/tcp    quote
qotd               17/udp    quote
chargen            19/tcp    ttytst source
chargen            19/udp    ttytst source
ftp-data           20/tcp
ftp                21/tcp
telnet             23/tcp
smtp               25/tcp    mail
time               37/tcp     timserver
time               37/udp    timserver
rlp                39/udp    resource      # resource location
name               42/tcp    nameserver
name               42/udp    nameserver
whois              43/tcp    nicname       # usually to sri  -nic
domain             53/tcp    nameserver    # name  -domain server
domain             53/udp    nameserver
nameserver         53/tcp    domain        # name  -domain server
nameserver         53/udp    domain
mtp                57/tcp                  # depre  cated
bootp              67/udp                  # boot program server
tftp               69/udp
rje                77/tcp    netrjs
finger             79/tcp
link               87/tcp    ttylink
supdup             95/tcp
hostnames         101/tcp    hostn ame      # usually from sri -nic
iso-tsap          102/tcp
dictionary        103/tcp    webster
x400              103/tcp                  # ISO Mail
x400-snd          104/tcp
csnet-ns          105/tcp
pop               109/tcp    postoffice
pop2               109/tcp                  # Post Office
pop3              110/tcp    postoffice
portmap           111/tcp
portmap           111/udp
sunrpc            111/tcp
sunrpc            111/udp
auth              113/tcp    authentication
sftp              115/tcp
path              117/tcp
uucp-path         117/tcp
nntp              119/tcp    usenet        # Network News Transfer
ntp               123/udp    ntpd ntp      # network time protocol (exp)
nbname            137/udp
nbdatagram        138/udp
```

```
nbsession          139/tcp
NeWS               144/tcp    news
sgmp               153/udp    sgmp
tcprepo            158/tcp    repository    # PCMAIL
snmp               161/udp    snmp
snmp-trap          162/udp    snmp
print-srv          170/tcp                  # netw ork PostScript
vmnet              175/tcp
```

Alle TCP-Verbindungen sind Full-Duplex und Punkt-zu-Punkt. Full-Duplex bedeutet, daß der Datenverkehr gleichzeitig in beide Richtungen erfolgen kann. Punkt-zu-Punkt bedeutet, daß jede Verbindung exakt zwei Endpunkte besitzt. TCP unterstützt kein Multicast oder Broadcast.

TCP/IP über Modems oder das Data Link Layer im Internet

Layer 4	TCP
Layer 3	IP
Layer 2	SLIP, PPP

Werden zwei Firmen-Router an unterschiedlichen Standorten miteinander verbunden oder wollen sich Benutzer von zu Hause über ihre Telefonanlage an das Internet anbinden, so wird eine Punkt-zu-Punkt-Verbindung benötigt. Zwei Protokolle werden dafür zumeist verwendet: *SLIP* (Serial Line IP) und *PPP* (Point-to-Point Protocol).

SLIP ist das ältere der beiden Protokolle und wurde 1984 entwickelt um Sun Workstations über Modems mit dem Internet zu verbinden. SLIP wird im RFC 1055 beschrieben und ist sehr einfach. Die Workstation sendet rohe IP-Pakete über die (serielle) Leitung, wobei ein spezielles Flag-Byte (0xC0) das Ende des Frames anzeigt.

SLIP besitzt jedoch keine Fehlerkorrektur, jede der beteiligten Endpunkte muß die IP-Adresse des Gegenübers wissen, es besitzt keine Methode zur Authentifikation der Kommunikationspartner und nicht zuletzt ist SLIP kein Internet-Standard. Aus diesem Grund gibt es verschiedene, inkompatible Versionen.

PPP (RFC 1661, RFC 1662, RFC 1663) wurde daher entwickelt, um die obengenannten Probleme von SLIP zu lösen. PPP unterstützt Fehlerkorrektur, verschiedene Protokolle, den Austausch von IP-Adressen zur Laufzeit, sichere Authentifizierung und andere verbesserte Eigenschaften.

Das PPP-Protokoll ist ein wenig komplizierter als das SLIP-Protokoll.

Länge in Bytes	Name	Inhalt
1	Flag	01111110
1	Adresse	11111111
1	Control	00000011
1 oder 2	Protokoll	(Auswahl unter LCP, NCP, IP, IPX, AppleTalk)
Variabel	Daten	(Standardlänge: 1500 Bytes)
2 oder 4	Check-Summe	./.
1	Flag	01111110

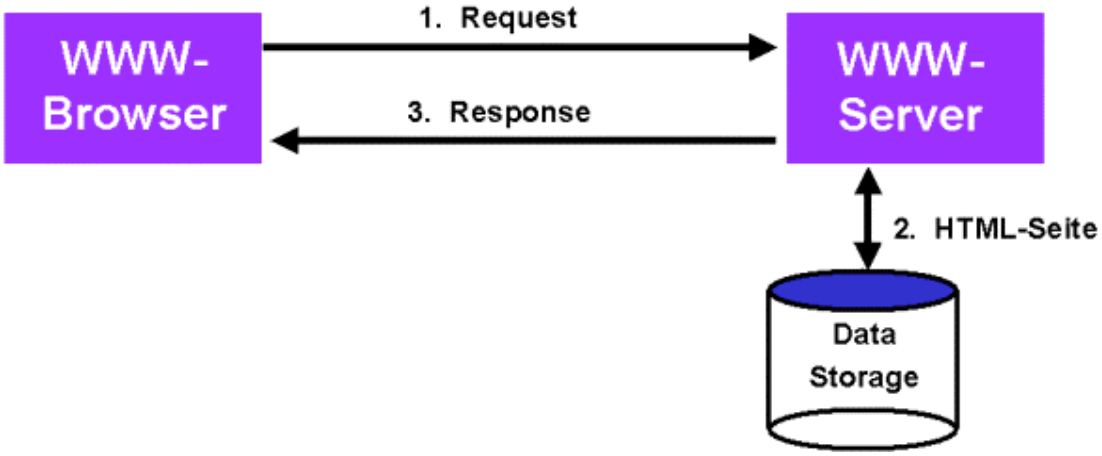
Tabelle 3.3: Der Datenstrom beim PPP-Protokoll

HTTP - HyperText Transfer Protocol

Layer 7	HTTP
Layer 4	TCP
Layer 3	IP

Stichworte

- HTTP-Konzepte
- Requests: Anfragen beim Server
- Responses: Antworten des Servers
- Methoden



Das Standard-Transferprotokoll im WWW ist HTTP (HyperText Transfer Protocol). Jede Interaktion auf dem Web besteht aus einer ASCII-Anfrage, der eine multimediale, RFC 822-konforme (MIME) Antwort folgt. Obwohl die Verwendung von TCP für die Transportverbindung sehr gängig ist, könnte auch ein anderer Standard (z.B. ATM AAL 5) die Basis sein.

HTTP verändert sich ständig. Verschiedene Versionen sind in Gebrauch und weitere sind in der Entwicklungsphase. Das hier aufgeführte Material ist sehr grundlegend und sollte daher Allgemeingültigkeit haben.

Das HTTP-Protokoll besteht aus zwei recht unterschiedlichen Komponenten: Einen Satz an Anfragen vom Client (dem Browser) zum Server und einen Satz an Antworten in die andere Richtung. Alle neueren Versionen von HTTP unterstützen zwei verschiedene Arten von Anfragen: *Simple Requests* und *Full Requests*. Der erste Fall ist eine einfache *GET*-Zeile, die die gwünschte Seite benennt, ohne zusätzliche Informationen über die Protokollversion. Die Antwort ist eine "rohe" Seite, ohne Header-Informationen, ohne MIME und ohne Kodierung. Die Anfragezeile (z.B. über TELNET, Port 80) könnte folgendermaßen aussehen:

GET /hypertext/WWW/MyText.html

Die Seite würde zurückgeschickt ohne daß die *Content*-Typen angezeigt werden. Dieser Mechanismus wird für Rückwärtskompatibilität benötigt. Er wird zusehends überflüssig werden, da immer mehr Browser und Server auf der Verarbeitung von Full Requests basieren. Full Requests werden durch die Verwendung einer Protokollversion in der GET-Zeile angezeigt.

GET /hypertext/WWW/MyText.html HTTP/1.0

Requests können auch aus mehreren Zeilen bestehen. Eine leere Zeile zeigt das Ende der Anfrage an. Die erste Zeile eines Full Requests beinhaltet das Kommando (z.B. GET), die gewünschte Seite und das Protokoll mit dessen Version.

Obwohl HTTP für die Verwendung im WWW entwickelt wurde, sind mehr generische Funktionalitäten für zukünftige objektorientierte Applikationen enthalten. Aus diesem Grund ist das erste Wort in einem Full Request der Name der Methode (Kommando), die auf einer WWW-Seite ausgeführt werden soll. Die eingebauten Methoden sind *case-sensitiv* (d.h. "GET" ist nicht gleich "get") und werden in der folgenden Tabelle aufgelistet:

Methode	Beschreibung
GET	Anfrage um eine Web-Seite zu lesen
HEAD	Anfrage den Header einer Web-Seite zu lesen
PUT	Anfrage eine Web-Seite zu speichern
POST	Anhang zu einer benannten Ressource (z.B. eine Web-Seite)
DELETE	Lösche eine Web-Seite
LINK	Verbindet zwei existierende Ressourcen

UNLINK	Beendet eine Verbindung zwischen zwei Ressourcen

Tabelle 3.4: Die HTTP-Request-Methoden

Die GET-Methode veranlaßt den Server eine Seite zu schicken. Wenn der GET-Request jedoch von einem *If-Modified-Since*-Header gefolgt wird, schickt der Server nur die Daten, wenn sie seit dem angegebenen Datum modifiziert wurden. Durch diesen Mechanismus kann ein Browser eine Ressource abfragen, die über Caching-Mechanismen zwischengespeichert wurden und dennoch immer eine aktuelle Information erhalten. Ist die Seite im Cache noch immer gültig, schickt der Server eine entsprechende Statuszeile zurück. Auf diese Art verhindert man den unnötigen Transfer der Seite.

Die HEAD-Methode fragt nach dem Header einer Web-Seite. Die PUT-Methode ist die Umkehrung von GET. Ähnlich wie PUT ist die POST-Methode. Statt existierende Daten zu ersetzen, werden die neuen Daten in einer generalisierten Weise an die vorhandenen Daten angehängt. DELETE entfernt die Seite, wie man bei diesem Befehl auch vermuten könnte. Die LINK- und UNLINK-Methoden erlauben es Verbindungen zwischen existierenden Seiten zu beeinflussen.

Jeder Request erhält eine Response in Form einer Statuszeile und möglichen zusätzlichen Informationen. Die Statuszeile kann unter anderem folgende Codes enthalten:

200: OK

304: not modified

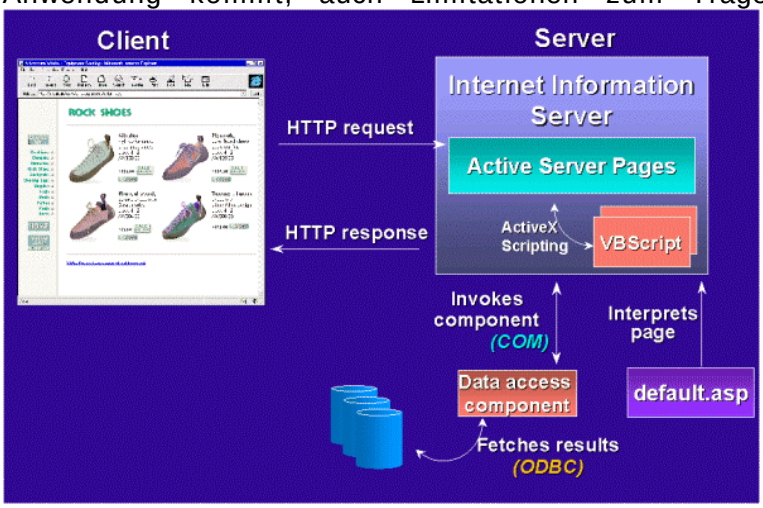
400: bad request

403: forbidden

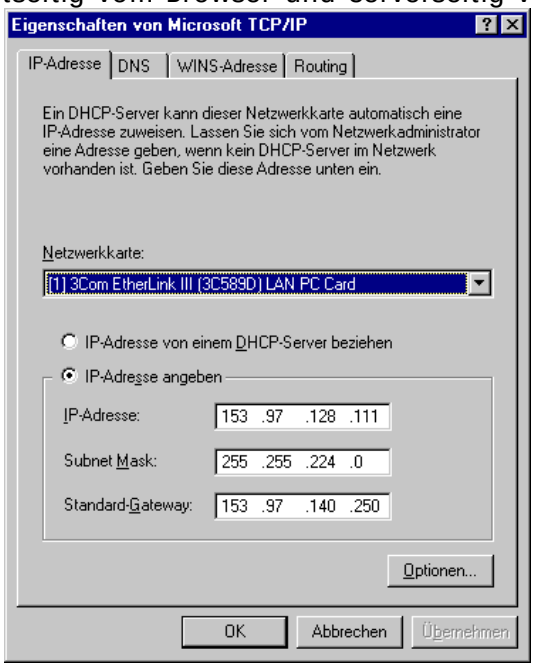
404: File not found

Es sind Ihnen sicher noch weitere Fehlermeldungen bekannt. Sie werden diese später im Kapitel Webserver Serverkonfiguration kennenlernen - Vortag über Systemtechnik)

(Wenn Sie vielleicht schon als Webpublisher, oder als Webprogrammierer gearbeitet haben, dann wissen Sie, dass spätestens wenn der Browser zur Anwendung kommt, auch Limitationen zum Tragen kommen, die vom Protokollverhalten von http 1.0 herrühren - Dies ist mit ein Grund, dass die Version 1.1 vor der Haustüre steht)



Die HTTP-Möglichkeiten hängen Clientseitig vom Browser und Serverseitig von einem HTTP-Interface (sprich Webserver) ab. In diesem Sinn ist HTTP als Applikation plattformunabhängig - Das Betriebssystem ist egal) (Sie sehen links in der TCP/IP Konfiguration eines Windows NT Clients nirgends einen Tab für HTTP !!!!)



HTTP Version 1.1:

Gilt als neuer Standard und wird im RFC 2068 definiert. Wird mittlerweile von allen gängigen Serversystemen der neuen Generation unterstützt (IIS4.0 Netscape Fasttrack, Apache u.s.w. –Browserseitig wirken die Neuerungen erst ab 4. Generation Clients (Netscape, IE)

HTTP 1.1 ist voll kompatibel zu HTTP 1.0 und seine Neuerungen lassen sich mehr oder weniger an einer Hand abzählen.

Hier eine kurze Liste der wichtigsten Neuerungen:

- Persistent Connections:
  Neuerdings wird nicht für jedes einzelen Element einer HTML-Seite eine eigene TCP-Session aufgebaut. Gerade bei kleinen Dateien und einfachen Anforderungen, wie conditional GET mit if-modified-since Header, hatt dieses Vorgehen erheblichen Overhead zur Folge. Eine Verbindung bleibt nach einem erfolgreichen Request solange offen bis eine der beiden Stationen (Server oder Client) im Connection-Header Field einen close Befehl überträgt. Ausserdem wird für die ASCII-Übertragung noch eine Komprimierung angewendet. Dies bedeutet alles in allem eine erhebliche Performance-Steigerung.
- Pipelining:
  Zusaätzlich zu Persistent Connection tritt neu ein Verfahre, das als Pipelining bezeichnet wird in Aktion. Dies bedeutet, dass meherer requests oder responses gesendet werden können, ohne dass auf eine Antwort der Gegenstelle gewartet werden muss. Die Pipeline wird sequentiell abgearbeitet (FIFO - first in first out).
- Authentizierung schon im HTTP-Header erhalten. :
  Möglichkeit einer sogenannten „Challenge-Response-Authentication“, d.h. der verschlüsselten Passwortübergabe. (MD5 Verschlüsselung)
- Verbessertes Caching:
  Selektives Downloaden von Komponenten (das expire-Attribut kann auf jedes Objekt einer HTML/ASP Datei angewendet werden).
  (neue Chaching Funktionen Clientseitig und Serverseitig). Im Request-Header wird in Verbindung mit:
  Request Header = Range : ranges-specifier
  durch einen GET-Request nur noch über den im ranges-spezifier angegebenen Teil des Dokumentes übertragen. Dies hat zu Folge, dass bei einem Unterbruch in der GET-Phase nicht mehr das ganze Dokument oder Element runtergeldaen werden muss, sondern an der Stelle aufgexsetzt werden kann, wo der Unterbruch stattfand.

So kann zum Beispiel auch folgende Eigenschaft in Verbindung mit dem Range verwendet werden:
Request Header = if-Range : (entity tag | HTTP date)
Nur ein bestimmter Bereich eines Dokumentes wird übertragen, falls nicht das ganze Dokument geändert wurde.

- Virtuelle Server jetzt über HOST-Header ansprechbar, das heisst, dass jetzt auf eine einzige IP-Adresse mehrere virtuelle Webserver definiert werden können. Dies kann als eine sinnvolle Schonung der Infrastruktur-Resourcen gesehen werden. Noch sind wir ja von einer IPv6 Implementation weit entfernt, sodass IP-Adressen immer noch kanppes Gut darstellen. (Sie werden die Art und Weise wie man virtuelle Webserver definiert noch in der Vorlesung über Systemtechnik kennenlernen)

Wenn Sie den aktuellen RFC zum HTTP1.1 studieren wollen, besuchen Sie doch bitte die Website des W3C Consortiums unter : www.w3.org/protocols

Zur TCP/IP-Architektur gehört ein Satz standardisierter Applikationsprotokolle. Auch wenn diese in jünster Zeit durch modernere und den gewachsenen Ansprüchen mehr entsprechende Dienste ersetzt worden sind, lohnt es sich, mehr über sie zu erfahren.

Telnet

Layer 7	Telnet
Layer 4	TCP
Layer 3	IP

Stichworte:

- Terminalsitzung
- Client- und Server-Seite
- Eine Telnet-Sitzung

Telnet dient dem Zugriff auf einen am Netz angeschlossenen Rechner in Form einer Termalsitzung und ist im RFC 854 spezifiziert. Die Client-Seite wird über das Kommando *telnet* angesprochen. Auf der Server-Seite, d.h. auf dem über telnet angesprochenen Rechner, läuft ein sogenannter *Daemon* oder *Server*, der entsprechend reagiert. Der Telnet Server-Prozeß liegt standardmäßig auf dem TCP-Port 23.

Der Aufruf von *telnet* erfolgt in der Regel mit der Angabe eines Rechnernamens. Zusätzlich kann eine Portnummer angegeben werden. Auf diese Weise läßt sich ein Dialog mit anderen Diensten wie z.B. SMTP manuell abwickeln. Wird kein Rechnername angegeben, geht *telnet* in einen Kommandomodus und liefert eine Eingabeaufforderung. In diesem Kommandomodus lassen sich Verbindungen zu Rechnern aufbauen und abbrechen, die Betriebsparameter beeinflussen und vieles mehr. Durch ein "Fluchtzeichen" - standardmäßig ^[(d.h. gleichzeitiges Drücken von Ctrl und []) kann man jederzeit in diesen Modus zurückwechseln.

Durch den Start von Telnet wird eine TCP/IP-Verbindung zum Zielrechner und dem entsprechenden Server-Prozeß aufgebaut. Dieser arrangiert dann den weiteren Ablauf derart, daß das Login, so wie man es normalerweise über ein lokales Terminal gewöhnt ist, nun über die gerade entstandene Verbindung vonstatten geht. Dies ist sozusagen ein "künstliches" Terminal. Das Ergebnis ist ein Fenster zum Server-Rechner, in dem eine Shell läuft, über die man dann Programme starten kann.

FTP

Layer 7	FTP
Layer 4	TCP
Layer 3	IP

Stichworte:

- FTP-Konzept
- Übertragung und Rückmeldungen
- Übertragungsmodi

Das File Transfer Protocol ist im RFC 959 spezifiziert. Es legt TCP-Port 21 als Kommandokanal und TCP-Port 20 als Datenkanal fest.

FTP unterscheidet sich in mancher Hinsicht von anderen Dateitransfer-Programmen. Zu den herausragensten Unterschieden zählen die Verwendung von getrennten Kanälen für Kontrollinformationen und Daten sowie der Umstand, daß FTP-Datentransfers nicht im Hintergrund ablaufen, d.h. ohne einen Spooler arbeiten.

FTP verwendet als Protokoll-Elemente durch Newline-Zeichen terminierten ASCII-Text, der aus einem vier Zeichen langen Kommandowort mit optionalen Parametern besteht. Rückmeldungen beinhalten einen dreistelligen Zifferncode und einen erklärenden Text, der eine Erklärung zum Erfolg oder Mißerfolg der Aktion gibt. Die FTP-Protokollkommandos erlauben das Senden, Empfangen, Löschen oder Umbenennen von Dateien, das Einrichten, Löschen und Wechseln von Dateiverzeichnissen, das Anfügen von Dateien sowie das versenden von elektronischer Post.

Für jeden Datentransfer wird eine TCP-Verbindung zwischen Client und Server eröffnet und nach der Übertragung wieder geschlossen. Auf diese Art und Weise verwendet FTP die Sicherheitsfunktionen von TCP, das ja bereits alle nötigen Vorkehrungen zur fehlerlosen Übertragung trifft. FTP muß darüberhinaus keine eigenen Sicherheitsfunktionen anwenden.

Obwohl mehrere Übertragungsmodi wie z.B. die Komprimierung von Daten spezifiziert sind, werden auf gängigen Systemen nur zwei Modi implementiert: Text- und Binärmodus. Im Textmodus werden Textdateien als durch "Carriage-Return" und "Newline" getrennte ASCII-Zeilen versendet und lassen sich somit zwischen unterschiedlichen Systemen transferieren. Im Binärmodus wird eine Datei ohne jegliche Umwandlung als eine Folge von Bytes übertragen, was natürlich schneller geht.

TFTP

Layer 7	TFTP
Layer 4	UDP
Layer 3	IP

Stichworte:

- UDP-Protokoll
- TFTP-Protokoll-Codes
- Anwendungsgebiete

Das *Trivial File Transfer Protocol* ist ein Dateitransfer-Protokoll für Minimalanforderungen und im RFC 783 spezifiziert. Es verwendet den UDP-Port 69. Wie FTP unterstützt auch TFTP einen Text- und einen Binärübertragungsmodus. Hauptmerkmal gegenüber FTP ist aber die Verwendung eines verbindungslosen Transport-Protokolls, hier also UDP. Für die Gestaltung des Protokolls hat das mehrere Konsequenzen: Zunächst muß TFTP selbst die Sicherung der Übertragung durch Algorithmen wie Zeitüberwachung und Paket-Wiederholung vornehmen. Außerdem wird kein ""Einloggen" auf dem Server-Rechner durchgeführt. Der TFTP-Server ersetzt die fehlende Autorisierung durch restriktive Zugriffsbeschränkungen. In welcher Weise sich ein System gegen unberechtigte Zugriffe über TFTP schützt, ist allerdings in der Protokollspezifikation nicht festgelegt und deshalb implementierungsabhängig.

Die TFTP-Protokoll-Codes sind:

- Lesanforderung
- Schreibanforderung
- Daten senden
- Quittung
- Fehler

Die Vorteile von TFTP liegen nicht unbedingt im regelmäßigen Dateitransfer zwischen Systemen. Vielmehr liegt das Hauptanwendungsgebiet dieses Protokolls heutzutage vor allem im Laden von Server-Programmen sowie zum Starten von plattenlosen Rechnern. Im letzten Fall wird TFTP für den Transfer des Systemprogramms in den Hauptspeicher verwendet. Grund dafür sind die geringen Voraussetzungen für den Betrieb von TFTP, außer dem Protokoll selbst benötigt man lediglich Basisfunktionen von IP, das sehr einfache UDP-Protokoll

sowie einen Treiber für den Zugang zum Netzwerk. Ein solcher minimaler Protokoll-Stack ist mit geringem Aufwand zu implementieren. Das Resultat hat in wenigen Kilobytes Speicher platz, z.B. in einem EPROM.

Aktuelle Vertreter einer Netzwerkkonzepts, das u.a. TFTP verwendet, sind Java-Stations und NetPCs.

Berkeley-Utilities: rlogin, rsh, rcp und rexec

Stichworte:

- rlogin: Remote Login
- rsh: Remote Shell
- rcp: Remote Copy
- rexec: Remote Execute

Layer 7	rlogin,rsh,rcp,rexec
Layer 4	Tcp
Layer 3	Ip

Die Universität von Kalifornien in Berkeley hat durch die Integration von TCP/IP in UNIX entscheidend zum Erfolg der TCP/IP-Architektur beigetragen. Dabei haben sich die Entwickler nicht auf die Implementierung bestehender Protokolle und Dienste wie Telnet und FTP beschränkt, sondern auch eigene Kommandos entwickelt. Die r-Utilities dienen hierbei der Kommunikation mit entfernten Rechnern. Der Name dieser Werkzeuge stammt von der Tatsache, daß alle Kommandos mit einem "r" für den Begriff *remote* beginnen.

Das Kommando *rlogin* steht für "Remote Login", d.h. es erlaubt ein Anmelden auf einem anderen Rechner. Der dazugehörige Server wartet auf TCP-Port 513 auf Verbindungsanforderungen. Wie bei Telnet wird auch hier im Server-Rechner ein Login-Prozeß gestartet und ein Pseudoterminal eingerichtet. Auch sonst sind nur wenig funktionelle Unterschiede zu Telnet festzustellen.

Die "Remote Shell" *rsh* und der zugehörige Server (TCP-Port 514) ermöglichen dem Benutzer, Kommandos auf einem anderen Rechnern auszuführen. *rsh* ist keine Shell im eigentlichen Sinne, d.h. interpretiert selbst keine Kommandoaufrufe. Die als Parameter angegebene Kommandozeile wird zum Server geschickt, wobei *rsh* die Standardein- und ausgabekanäle des dadurch gestarteten Kommandos mittels zweier TCP-Verbindungen mit dem lokal ablaufenden Prozeß verknüpft.

rcp ist das Dateitransfer-Kommando der Berkeley-Utilities und arbeitet wie eine Erweiterung des *copy*-Kommandos im Netz. Alle im Netz sinnvollen Varianten der Verwendung von copy (oder cp unter UNIX) werden auch von rcp implementiert, wie z.B. das Kopieren von lokalen Dateien auf entfernte Rechner und umgekehrt sowie das Kopieren zwischen Drittrechnern und lokales Kopieren. Auch das rekursive Kopieren ganzer Dateibäume wird ermöglicht - eine Funktion, die FTP nicht beherrscht, die aber in der Praxix sehr häufig benötigt wird.

Eine Möglichkeit zum Starten von Kommandos auf anderen Rechnern wird durch *rexec* angeboten. Es verwendet TCP-Port 512. Das von *rexec* verwendete Protokoll ähnelt stark dem von *rsh*, mit dem wesentlichen Unterschied, daß mit dem Auftrag ein verschlüsselte Paßwort gesendet wird und somit eine normale Aithentifizierung wie beim Login zustandekommt.

Gopher

Layer 7	Gopher
Layer 4	Tcp
Layer 3	Ip

Stichworte:

- Historie und Konzepte
- Verwendung von Gopher

Das *gopher*-Protokoll wird vom Gopher-System verwendet, das an der Universität von Minnesota entwickelt wurde. Der Name stammt historisch gesehen von einer Sportmannschaft der Universität ab, den "Golden Gophers". Zudem ist eine Verwandschaft zum umgangssprachlichen "go for" (= hol es dir) zu erkennen.

Gopher ist ein Vorläufer des World Wide Web, wobei seine Entwicklung einige Jahre vor dem WWW stattgefunden hat. Es ist ein Informationsabrufsystem, das konzeptionell sehr ähnlich zum WWW ist, jedoch nur Text und keine Bilder unterstützt. Meldet sich ein Benutzer bei einem Gopher-Server an, wird ein Menü mit Dateien und Verzeichnissen angezeigt. Hierbei kann jedes dieser beiden mit einem anderen Gopher-Menü irgendwo auf der Welt verbunden sein.

Der große Vorteil von Gopher im Bezug auf das WWW liegt in der Tatsache, daß es auch auf 25 x 80 ASCII-Terminals lauffähig ist (wovon es noch eine große Menge zu finden gibt). Weiterhin ist Gopher aufgrund seiner Basierung auf Text extrem schnell. Daher gibt es noch immer tausende von Gopher-Servern auf der

ganzen Welt. Indem das *gopher*-Protokoll verwendet wird, haben auch WWW-Benutzer die Möglichkeit Gopher zu verwenden. Hierzu wird dann das Gopher-Menü als anklickbare Web-Seite angezeigt.

Eine weitere Funktionalität von Gopher wird über das *gopher+*-Protokoll realisiert: Es ist damit möglich eine komplette Recherche-Anfrage an einen Gopher-Server zu schicken. Das Ergebnis repräsentiert die gefundenen Themengebiete auf dem entfernten Gopher-Server. Dies ist insbesondere für Literatur-Recherche eine äußerst wichtige technische Anwendung.

News

Layer 7	nntp
Layer 4	Tcp
Layer 3	Ip

Stichworte:

- net news - USENET
- Konzepte der News-Verteilung
- Themenhierarchie
- News-Readers
- Subscribe - Unsubscribe
- Posting - Crossposting
- Flamewars
- Killfiles
- Moderierte News-Gruppe
- FAQ
- Smileys oder Emoticons
- Anonyme Remailer
- NNTP

Eine der populärsten Anwendungen von Computer-Netzwerken ist das weltweite System von News-Gruppen, genannt *net news*. Oftmals werden die *net news* als USENET bezeichnet, obwohl zwei verschiedene Mechanismen dahinterstecken. Das erstere ist Internet-basiert, das zweitere nicht.

Eine News-Gruppe ist ein weltweites Diskussionsforum über ein spezifisches Thema. Menschen, die an dem Thema interessiert sind, können sich für die

betreffende News-Gruppe "einschreiben". Eingeschriebene Benutzer verwenden eine spezielle Art von Programm - einen News-Reader - um alle Artikel zu lesen, die an eine bestimmt News-Gruppe gerichtet wurden. Benutzer von News-Readern können auch Beiträge an eine News-Gruppe abschicken. Jeder Artikel, der abgeschickt an eine News-Gruppe abgeschickt wurde, wird automatisch an alle Teilnehmer (Subscribers) verteilt, wo auch immer sie sich befinden. Die gängigen Verteilzeiten liegen zwischen wenigen Sekunden bis hin zu ein paar Stunden, je nach Entfernung zwischen Sender und Empfänger.

Die Anzahl der News-Gruppen ist so groß (aktuell über 10.000), daß sie in einer Hierarchie angeordnet sind um überhaupt noch einen gewissen Überblick zu gestatten. Hierbei gibt es jedoch auch regionale oder nationale Unterschiede. Die "offizielle" weltweite Hierarchie folgt in der untenstehenden Tabelle:

Name	**Themengebiete**
Comp	Computer, Informatik und die Computer-Industrie
Sci	Natur- und Ingenieurwissenschaften
Humanities	Literatur und Geisteswissenschaften
News	Diskussion über das USENET selbst
Rec	Freizeitaktivitäten inklusive Sport und Musik
Misc	Alles, was in keine andere Kategorie paßt
Soc	Kontakte und soziale Belange
Talk	Debatten, Argumentationen und Polemik
Alt	Alternativer Baum über grundsätzlich jedes Themengebiet

Tabelle 4.1: USENET-Hierarchie in absteigender Signal-zu-Rauschen-Rate

Die *Comp*-Gruppe war die originale USENET-Gruppe, die von Informatikern, Computer-Profis und Computer-Fans benutzt wird. Technische Diskussionen stehen dabei im Vordergrund. Die *Sci*- und *Humanities*-Gruppen werden von Naturwissenschaftlern, Schülern und Amateuren genutzt, die sich für Physik, Chemie, Biologie oder auch Shakespeare interessieren. Nicht völlig überraschend ist es, daß die *Sci*-Gruppe deutlich größer als die *Humanities*-Gruppe ist. Dies scheint daran zu liegen, daß das Konzept der direkten elektronischen Kommunikation mit Gleichgesinnten sehr beliebt bei Naturwissenschaftlern ist. Die meisten Geisteswissenschaftler sind dagegen sehr skeptisch gegenüber dieser Art der Kommunikation.

Der *News*-Zweig der Hierarchie wird genutzt, um das News-System zu administrieren und entsprechende Informationen zu verbreiten. Die Diskussionen über neu einzurichtende News-Gruppen findet hier statt. Dies geschieht über eine Diskussion der neu zu erzeugenden News-Gruppe über einen bestimmten Zeitraum. Danach kommt es zu einer Abstimmung über die News-Gruppe. Ist das Ergebnis mit 2:1 auf der Ja-Seite und sind es mindestens 100 mehr Ja-Stimmen als Nein-Stimmen, wird die neue Gruppe eingerichtet. Einzig für die *Alt*-Gruppe ist das Vorgehen weniger formal.

Die bisherigen News-Gruppen haben einen professionellen oder akademischen Hintergrund. Dies ändert sich mit der *Rec*-Gruppe, die sich mit der Freizeigestaltung und verschiedenen Hobbies beschäftigt. Dies setzt sich in der *Soc*-Gruppe fort, wo Diskussionen über Religion, Politik, Kultur usw. geführt werden. Die *Talk*-Gruppe ist die Heimat sehr kontroverser Themen und wird von Benutzern bevölkert, die oftmals ausgeprägte Meinungen jedoch nur wenige Fakten vorzuweisen haben. Die *Alt*-Gruppe ist ein kompett alternativer Baum und besitzt seine ganz eigenen Regeln. Er ist so etwas wie der rechtsfreie und anarchistische Raum der News-Hierarchie.

Jede der oben aufgeführten Kategorien wird in Unterkategorien aufgeteilt. So ist z.B. *rec.sport* über Sport, *rec.sport.basketball* über Basketball und *rec.sport.basketball.women* über Damen-Basketball. Zu fortlaufenden Diskussionen in den Medien führt naturgemäß die News-Hierarchie ab *Alt.sex*, da dort fast jede noch so absurde Spielart menschlicher Lust zu finden ist. Gruppen mit Kinderpornographie oder Vergewaltigung als Thema haben jedoch durch gewisse Selbstreinigungsmechanismen kaum lange Überlebenschancen.

Es existieren viele verschiedenen *News-Reader*, d.h. Programme mit denen man News lesen kann. Zum Teil sind sie Tastatur-basiert, zum Teil über ein Maus steuerbar. In fast allen Fällen überprüft der News-Reader sobald er gestartet ist eine Datei mit der Liste der News-Gruppen, bei denen sich der Benutzer eingeschrieben (subscribed) hat. Er stellt dann typischerweise eine Zusammenfassung der bisher ungelesenen Artikel der ersten News-Gruppe auf und wartet auf die Auswahl des Benutzers eine oder mehrere zu lesen. Nachdem eine News gelesen wurde, kann sie gelöscht, gesichert, gedruckt usw. werden.

Eine weitere Funktionalität von News-Readern ist das Abonieren (subscribe) und Kündigen (unsubscribe) von News-Gruppen. Eine entsprechende Änderung schlägt sich in einer Datei nieder, die alle abonierten News-Gruppen enthält. Weiterhin sind News-Reader in der Lage, neue News-Artikel abzuschicken (posting). Der Benutzer erzeugt dabei den Artikel und schickt ihn an die gewünschte Gruppe. Dabei ist auch ein sogenanntes *Crossposting* möglich, d.h.

ein Artikel wird an mehrere News-Gruppen geschickt. Artikel können auch auf bestimmte regionale Gebiete beschränkt werden.

Die Soziologie des News-Welt ist einzigartig. Niemals zuvor war es möglich, daß tausende von Menschen, die sich nicht kennen, eine weltweite Diskussion über die unterschiedlichsten Themen führen können. Unglücklicherweise mißbrauchen einige Menschen die Möglichkeit zu einer großen Gruppe anderer Menschen sprechen zu können. Schickt jemand eine Meldung an eine News-Gruppe ab, die zum Inhalt hat "Leute wie ihr sollten erschossen werden", dann werden starke emotionale Reaktionen erzeugt. Diese zeigen sich oft in einem sogenannten *Flamewar*, der dann folgt. Beleidigende Nachrichten (Flames) gehen dabei von einer Seite zur anderen. Diese Situation kann auf zwei Arten angegangen werden, wobei die eine individuell und die andere kollektiv ist. Individuelle Benutzer können ein sogenanntes *Killfile* installieren, das Artikel nach bestimmten Themengebieten oder Personen spezifiziert, so daß sie vom News-Reader sofort nach der Ankunft automatisch gelöscht werden. Die meisten News-Reader sind sogar in der Lage eine gesamte Diskussionsfolge auszublenden. Dies ist dann sinnvoll, wenn man das Gefühl hat, daß eine Diskussion anfängt in eine Endlosschleife einzutreten.

Wenn sich eine größere Anzahl von Benutzern einer News-Gruppe durch Informationsmüll genervt fühlt, kann eine News-Gruppe auch *moderiert* werden. In einer solchen Gruppe liest der Moderator alle an die Gruppe gerichteten Artikel bevor sie für die Allgemeinheit zugänglich sind. Der Moderator läßt nur die "guten" Artikel zu und löscht die "schlechten". Zu einigen Themengebieten gibt es sowohl moderierte als auch unmoderierte News-Gruppen.

Da sich jeden Tag einige tausend Menschen zum ersten mal in der Welt der News bewegen, werden bestimmt Anfängerfragen immer und immer wieder gestellt. Um den Netzwerkverkehr und den Overhead, den solche Fragen erzeugen, zu reduzieren, gibt es für viele News-Gruppen ein *FAQ*-Dokument (Frequently Asked Questions = häufig gestellte Fragen). Dieses Dokument versucht möglichst alle Anfängerfragen zu beantworten.

Durch die News-Benutzer hat sich im Internet ein bestimmter Jargon eingebürgert, der auch von anderen Diensten übernommen wurde. So sind die Begriffe BTW (By The Way = Übrigens), ROFL (Rolling On the Floor Laughing = Ich rolle mich vor Lachen auf dem Boden), IMHO (In My Humble Opinion = Nach meiner persönlichen Meinung) oder RTFM (Read The Fucking Manual = Lies die verdammte Gebrauchsanweisung) sehr gebräuchlich. Um Gefühle auszudrücken, haben sich kleine ASCII-Symbole etabliert, die *Smileys* oder *Emoticons*. Durch eine 90-Grad-Drehung kann ihre Bedeutung oftmals schnell erkannt werden. Die gebräuchlichsten Beispiele sind in der untenstehenden Tabelle aufgeführt.

Smiley	Bedeutung
:-)	Ich bin glücklich
:-)))))	Ich lache stark
:-|	Ich bin apatisch
:-(	Ich bin traurig/sauer
;-)	Ich zwinkere/bin ironisch
:-(0)	Ich schreie
:-(*)	Ich übergebe mich
8-)	Trägt eine Brille
C:-)	Hat ein großes Gehirn
:+)	Hat eine große Nase
:-{)	Hat einen Schnurrbart

Tabelle 4.2: Einige Smileys und ihre Bedeutung

Obwohl die meisten Menschen ihren echten Namen in Postings benutzen, möchten manche vollkommen anonym bleiben. Dies trifft vor allen Dingen bei kontroversen Diskussionsgruppen oder bei News-Gruppen für die Partnerschaftssuche zu. Dieser Wunsch hat zu den *Anonymen Remailern* geführt. Die zugehörigen Server akzeptieren Nachrichten und verändern die entsprechenden persönlichen Adreßfelder. Eine mögliche Antwort wird dadurch an den Remailer geschickt, der in einer Tabelle den richtigen Adressaten findet und ihm die Nachricht zukommen läßt. Problematisch wird dieser Mechansimen bei Rechtsbrüchen, wenn die Polizei den Zugriff auf die wahre Identität der Remailer-Nutzer verlangt.

Nachdem bisher eher der organisatorische und soziologische Aspekt der News betrachtet wurde, soll jetzt die Technik noch ein wenig beleuchtet werden. Um News zu empfangen muß News-Knoten eine periodische Verbindung zu einem anderen News-Knoten haben, den man dann *Newsfeed* nennt. Im empfangenden News-Knoten werden die eintreffenden News in einer Verzeichnishierarchie gespeichert. Dort greifen die Benutzer über ihre News-Reader zu.

Durch den gegenseitigen periodischen Zugriff der News-Knoten aufeinander verteilen sich die News über die Welt. Nicht jeder News-Knoten empfängt jedoch alle News. Hierfür gibt es mehrere Gründe. Zunächst ist die tägliche Menge an News größer als 500 MBytes und wächst noch immer stark. Alles zu speichern

erfordert einen großen Plattenplatz. Auch sind Übertragungszeiten und Kosten Gründe. Bei 28,8 kbps (Modem) und einer zugehörigen Telefonleitung dauert es 39 Stunden um die News von 24 Stunden zu übertragen. Bei 56 kbps dauert es noch immer 20 Stunden. Weiterhin ist nicht jeder News-Knoten an allen News-Gruppen interessiert. Zuletzt werden nicht alle News-Gruppen von allen Systemadministratoren toleriert. Im Dezember 1995 wurde temporär im weltweiten CompuServe-Netzwerk die Verteilung aller News-Gruppen mit dem Wort "Sex" im Namen gestoppt. Dies wurde durch deutsche Behörden verursacht, die glaubten dadurch die Verbreitung von Pornographie verhindern zu können. Der folgende weltweite Protest war vorhersehbar, direkt, sehr laut und schmerzhaft für Deutschland.

Die News-Artikel haben das selbe Format wie RFC 822-kompatible Email, jedoch mit der Erweiterung um einige Header. Diese Eigenschaften machen News einfach zu transportieren und kompatibel mit den meisten Email-Systemen. Die News-Header wurden im RFC 1036 definiert.

Das gängige News-Protokoll ist das *Network News Transfer Protocol* (NNTP), das im RFC 977 definiert wurde. Es ist vor allem für den Einsatz auf dem Internet geeignet. NNTP nutzt hierbei den TCP-Port 119 für den Transport der News-Artikel.

Email und Messaging

Layer 7	SMTP
Layer 4	TCP
Layer 3	IP

Stichworte:

- Historische Email-Systeme
- ARPANET-Email und X.400
- User Agent und Message Tranfer Agent
- Basisfunktionalitäten
- Mailboxen und Mailing-Listen
- Umschlag - Inhalt
- Header - Body
- Email-Reader
- MIME
- SMTP
- Email-Gateway
- POP3 und IMAP
- Spamming

Nachdem in den vorangehenden Kapiteln sehr viel über Protokolle und Dienste im Internet gesprochen wurde, kommen wir jetzt zu einer "echten" Anwendung. Denn wenn man jemanden fragt, was er jetzt gleich machen wird, so antwortet er wohl selten: "Ich gehe jetzt ein paar Rechnernamen im DNS nachschauen". Vielmehr wird die Antwort sein, daß Leute im "Web surfen" oder ihre Email lesen.

Architektur und Dienste

Electronic Mail oder kürzer *Email* ist inzwischen recht verbreitet. Es ist doch immerhin seit fast zwei Jahrzehnten in Gebrauch. Die ersten Email-Systeme bestanden einfach aus Dateitransfer-Protokollen mit der Konvention, daß die erste Zeile der Nachricht (Message) die Empfängeradresse enthielt. Mit der Zeit wurden jedoch Schwachstellen dieser Technik offensichtlich:

Das Versenden von Nachrichten an eine Gruppe von Empfängern war sehr unbequem

Die Nachrichten hatten keine interne Struktur. So war beim Weiterleiten einer Nachricht nicht zu erkennen, was die originale Nachricht war und was durch die weiterleitenden Person hinzugefügte Informationen.

Der Absender wußte nie genau, ob die Nachricht angekommen war oder nicht

War jemand nicht an seinem Arbeitsplatz und wollte, daß alle eintreffenden Nachrichten von einem Stellvertreter bearbeitet werden, war dies schwer zu realisieren

Die Benutzerschnittstelle war zu roh. Zunächst mußte eine Datei in einem Editor erstellt werden und nach dem Abspeichern mit einem speziellen Transferprogramm abgeschickt werden.

Es war nicht möglich Nachrichten zu erzeugen, die aus einer Mixtur aus Text, Graphiken und gesprochener Sprache besteht

Aus diesen Gründen wurden mit der Zeit bessere Vorschläge für Email-Systeme gemacht. 1982 wurde der ARPANET Email-Vorschlag als RFC 821 (Übertragungsprotokoll) und RFC 822 (Nachrichtenformat) veröffentlicht. Diese wurden seither de facto Internet-Standards. Zwei Jahre später wurde der CCITT-Standard *X.400* verabschieded, der sich jedoch nie etablieren konnte.

Obwohl X.400 von einem offiziellen internationalen Standard, allen Telekombetrieben, vielen Regierungen und einem substantiellen Teil der Computer-Industrie unterstützt wurde, konnte eine handvoll Informatiker mit einem "Hack" ihr System weltweit durchsetzen. Dies lag weniger an der guten Qualität des ARPANET-Vorschlags als vielmehr an dem sehr schlechten und komplexen Design von X.400. Die Wahl zwischen einem einfachen und funktionierenden System gegenüber einem mächtigen aber nicht operablen System fiel der Netzwerkgemeinde nicht schwer.

Im folgenden soll ein Überblick über die Organisation von Email-Systemen gegeben werden. Sie bestehen normalerweise aus zwei Subsystemen: Der *User Agent*, der das Lesen und Verschicken von Email erlaubt und der *Message Transfer Agent*, der die Nachricht von Sender zu Empfänger bewegt. Der User Agent ist hierbei ein lokales Programm, das kommandobasierte, menübasierte oder graphische Methoden der Interaktion mit einem Email-System bereitstellt. Die Message Transfer Agents sind oftmals Hintergrundprozesse, die Email-Nachrichten durch das System transportieren.

Typischerweise unterstützen Email-Systeme fünf Basisfunktionalitäten, wie sie im folgenden beschrieben werden:

Die *Komposition* betrifft den Prozeß der Erzeugung von Nachrichten und Antworten. Obwohl ein einfacher Texteditor verwendet werden kann, bietet das

System Hilfe bei der Erstellung der zahlreichen Email-spezifischen Informationsfeldern, die jede Nachricht beinhaltet.

Der *Transfer* referenziert auf die Bewegung der Nachricht von Sender zu Empfänger. Hauptsächlich erfordert dies den Aufbau einer Verbindung zu einem Zielrechner oder einem Zwischenrechner, das Abschicken der Nachricht und das Lösen der Verbindung. Das Email-System sollte diese Arbeit automatisch durchführen.

Das *Reporting* hat die Aufgabe dem Sender mitzuteilen, was mit der Nachricht geschehen ist. Wurde sie ausgeliefert, wurde sie abgelehnt, ging sie verloren? In vielen Fällen ist eine Rückbestätigung der Auslieferung einer Nachricht essentiell.

Das *Anzeigen* erlaubt es den Benutzern, die eintreffenden Nachrichten zu lesen. Manchmal werden hierzu spezielle Konversionsschritte oder Präsentationskomponenten (z.B. für Graphiken) benötigt.

Die *Disposition* ist der letzte Schritt und betrifft die Otionen, die ein Benutzer nach dem Empfang der Nachricht hat. Die Möglichkeiten reichen von Wegwerfen vor dem Lesen über Abspeichern bis hin zum Antworten. Weiterhin sollten Mechanismen zum Weiterleiten gegeben sein.

Die meisten Email-Systeme erlauben die Einrichtung von *Mailboxen* zum Abspeichern eintreffender Nachrichten. Hierzu werden Kommandos benötigt, die das Erzeugen und Löschen von Mailboxen, das Inspizieren des Inhalts sowie das Einfügen und Löschen einzelner Nachrichten betreffen.

Eine weitere Funktionalität, die oftmals gefordert wird, sind *Mailing-Listen*, die es erlauben eine Nachricht an eine ganze Gruppe von Benutzern zu schicken. Eine andere Option, die manchmal gewünscht wird, ist die *Registrierung* von Email. Damit erfährt der Absender, wann seine Nachricht beim Empfänger angekommen ist. Weitere Optionen sind Durchschläge, hoch priorisierte Email, sichere (verschlüsselte) Nachrichten, alternative Empfänger falls der erste nicht verfügbar ist und die Möglichkeit daß Sekretariate die Emails ihrer Chefs bearbeiten.

Ein Schlüsselkonzept moderner Email-Systeme ist die Unterscheidung zwischen dem *Umschlag* und dem *Inhalt*. Der Umschlag umschleßt den Inhalt und enthält alle Informationen, um den Inhalt zu transportieren. Der Message Transport Agent nutzt diese Informationen für die Auslieferung der Nachricht. Die Nachricht in einem Umschlag besteht zumeist aus zwei Teilen, den *Kopf* (Header) und den *Körper* (Body). Der Header enthält dabei Kontrollinformationen für den User Agent. Der Body ist ausschließlich für den menschlichen Benutzer gedacht.

Der User Agent

Der User Agent - auch *Email Reader* genannt - akzeptiert normalerweise eine Reihe von Kommandos für die Komposition, dem Empfang und die Beantwortung von Nachrichten sowie für die Manipulation von Mailboxen. Einige User Agents haben aufwendige Menü- oder Graphik-basierte Benutzerschnittstellen für die man eine Maus benötigt, während andere einfache Tastatureingaben erwarten. Funktional gesehen sind sie meist identisch.

Startet man einen Email Reader, so wird er typischerweise zuerst in die Eingangs-Mailbox (Incoming) des Benutzers schauen ob für ihn eine Nachricht angekommen ist. Dann wird er die Anzahl der eingetroffenen Nachrichten oder einzeilige Zusammenfassungen aller Nachrichten anzeigen. Weitere Angaben können dabei zusätzlich auf dem Bildschirm erscheinen: Die Nachricht ist neu, die Nachricht ist nicht neu wurde aber in der Mailbox belassen, auf die Nachricht wurde schon geantwortet, die Nachricht wurde an jemanden "geforwarded", usw.Weitere Angaben können die Größe der Nachricht in Bytes sein, der Absender und ein sogenanntes *Subject*. Das Subject-Feld ist eine Analogie zu der Betreff-Zeile in einem Brief und wird in Email-Readern zumeist als Zusammenfassung angezeigt. Daher ist es in Emails recht wichtig ein aussagekräftiges Subject zu formulieren.

Eine Sammlung häufig implementierter Kommandos auf einem Email Reader zeigt die folgende Liste:

- Anzeigen der Subjects einer Mailbox
- Anzeigen der ersten Zeilen mehrerer Nachrichten als Liste
- Senden einer Nachricht
- Forwarden einer Nachricht
- Eine Nachricht beantworten
- Eine Nachricht löschen
- Eine Undelete-Operation auf gelöschte Nachrichten anwenden
- Eine Nachricht in einer anderen Mailbox speichern
- Die Nachrichten nach Beendigung des Mail Readers in der Eingangs-Mailbox behalten
- Eine andere Mailbox lesen
- Zur nächsten oder vorhergehenden Nachricht gehen und sie anzeigen
- Zu einer speziellen Nachricht gehen und sie anzeigen

Um eine Email abzuschicken, muß der Benutzer zunächst die Nachricht formulieren, die Zieladresse angeben und möglicherweise weitere Parameter zur Verfügung stellen. Insbesondere die Zieladresse muß in einem Format angegeben werden, die der User Agent versteht. Viele User Agents akzeptieren DNS-Adressen in der Form *mailbox@location*, z.B. "bk@barnes.ch". Aber auch die X.400-Adressen lohnen einen Blick. Sie sehen viel anders aus als die DNS-Adressen. Sie werden aus *Attribut* = *Wert*-Paaren gebildet:

/C=US/SP=MASSACHUSETTS/L=CAMBRIDGE/PA=360 MEMORIAL DR./CN=KEN SMITH/

Diese Adresse spezifiziert Land, Staat, Ort, persönliche Adresse und einen Namen. Viele andere Attribute sind möglich. Daher kann man eine Email an jemanden schicken, dessen Namen man nicht kennt, über den man aber viele andere Informationen besitzt. Typischerweise würde man jedoch zumeist *Aliase* (benutzerspezifische Kurzbezeichnungen) verwenden, auch bei den DNS-Adressen.

Nachrichtenformate

Wie schon weiter oben gesagt bestehen Emails aus einem primitven Umschlag (RFC 821), einigen Header-Feldern, einer leeren Zeile zur Abtrennung und einem Nachrichtenkörper. Jedes Header-Feld besteht aus einem ASCII-String, der einen Feldnamen, einen Doppelpunkt und einem Wert besteht. Die grundlegenden Header-Felder wie sie im RFC 822 definiert sind, sind in der nachstehenden Tabelle aufgelistet:

Header	Bedeutung
To:	Email-Adressen der primären Empfänger
Cc:	Email-Adressen weiterer Empfänger
Bcc:	Email-Adressen für Durchschläge
From:	Person, die die Nachricht erstellte
Sender:	Email-Adresse des Absenders
Received:	Eine Zeile wird hier von jedem Transfer Agent auf dem Weg zum Ziel hinzugefügt
Return-Path:	Kann genutzt werden um einen Weg zurück zum Absender zu identifizieren

Tabelle 5.1: RFC 822 Header-Felder

Zusätzlich zu den RFC 822 Feldern können noch eine Reihe von anderen Feldern genutzt werden. Die gebräuchlichsten listet die folgende Tabelle auf:

Header	Bedeutung
Date:	Datum und Zeit wann die Nachricht abgeschickt wurde (mit Zeitzone)
Reply-To:	Email-Adresse an wen Antworten geschickt werden sollen
Message-Id:	Einzigartige Nummer, mit der die Nachricht später referenziert werden kann
In-Reply-To:	Message-Id der Nachricht zu der diese Nachricht eine Antwort ist
Reference:	Andere relevante Message-Ids
Keywords:	Benutzerspezifische Schlüsselworte
Subject:	Kurze Zusammenfassung der Nachricht (Betreff-Zeile)

Tabelle 5.2: Zusätzlich Header-Felder

Nach dem Header kommt der Nachrichtenkörper. Ein Benutzer kann dort jedes gültige Zeichen hineinschreiben. Einige Leute beenden ihre Nachrichten mit einer Signatur mit Namen und Adresse, kleinen ASCII-Cartoons und Anmerkungen von sehr unterschiedlicher Phantasie und Wichtigkeit.

In den frühen Tagen von ARPANET beinhalteten Emails ausschließlich textuelle Nachrichten in Englisch und im ASCII-Standard. Heute beinhalten Nachrichten spezielle Buchstaben verschiedener Sprachen, z.B. Umlaute oder Buchstaben mit Akzenten Buchstaben aus einem nicht-lateinischen Alphabet, z.B. Hebräisch oder Russisch Elemente aus Sprachen ohne Alphabet, z.B. Chinesisch oder Japanisch nichttextuelle Elemente, z.B. Bilder, Video oder Audio

Als Lösung für solche Nachrichten wurde in RFC 1341 und RFC 1521 die *Multipurpose Internet Mail Extension* (MIME) vorgeschlagen, das inzwischen weltweit genutzt wird. Grundsätzlich wird bei MIME eine Struktur zum Message-Körper hinzugefügt, die die Kodierungsregeln für Nicht-ASCII-Nachrichten definiert. Alles was dann nuch getan werden muß, ist das absendende und das empfangende Programm zu ändern. Diese MIME-fähigen Programme kodieren/dekodieren alle Nicht-ASCII-Elemente in einer speziellen Art, daß sie auf ASCII-Basis übertragen werden können.

MIME-Elemente werden mit einem speziellen Header gekennzeichnet. Die gängigsten MIME-Typen zeigt die folgende Tabelle auf.

Typ	Untertyp	Beschreibung
Text	Plain	Unformatierter Text
Text	Richtext	Text mit einfachen Formatierungskommandos
Bild	Gif	Bild im GIF-Format
Bild	Jpeg	Bild im JPEG-Format
Audio	Basic	Wiedergabefähiger Sound
Video	Mpeg	Video im MPEG-Format
Applikation	Octet-stream	Eine uninterpretierte Byte-Sequenz
Applikation	Postscript	Ein druckbares Dokument im Postscript-Format

Tabelle 5.3: MIME-Typen und -Untertypen wie sie in RFC 1521 definert werden.

Nachrichtenübertragung

Im Internet wird eine Email von einer Quelle verschickt, indem die zugehörige Maschine eine TCP-Verbindung auf Port 25 zu einer Zielmaschine etabliert. An diesem Port lauscht auf der Empfängerseite ein Hintergrundprozeß (Daemon), der das *Simple Mail Transfer Protocol* (SMTP) versteht. Der Daemon akzeptiert eintreffende Verbindungen und kopiert Nachrichten zu ihren zugehörigen Mailboxen. Kann eine Nachricht nicht ausgeliefert werden, wird eine Fehlermeldung zurückgeschickt. SMTP ist ein einfaches ASCII-Protokoll. Nach Aufbau der TCP-Verbindung über Port 25 agiert die sendende Maschine als Client und die empfangende Maschine als Server. Die Größe der Nachricht sollte jedoch in vielen Fällen 64 kBytes nicht übersteigen. Der Server schickt die Nachricht mit Hilfe von DNS weiter, bis der engültige Empfänger erreicht ist.

Email über SMTP funktioniert am besten, wenn sich sowohl Sender als auch Empfänger auf dem Internet befinden und TCP-Verbindungen aufnehmen können. Jedoch sind nicht alle Maschinen, die Email schicken oder empfangen wollen, auf dem Internet. In diesem Falle existieren *Email Gateways*, die von einer Email-Konvention zur anderen übersetzen können, z.B. von SMTP nach X.400.

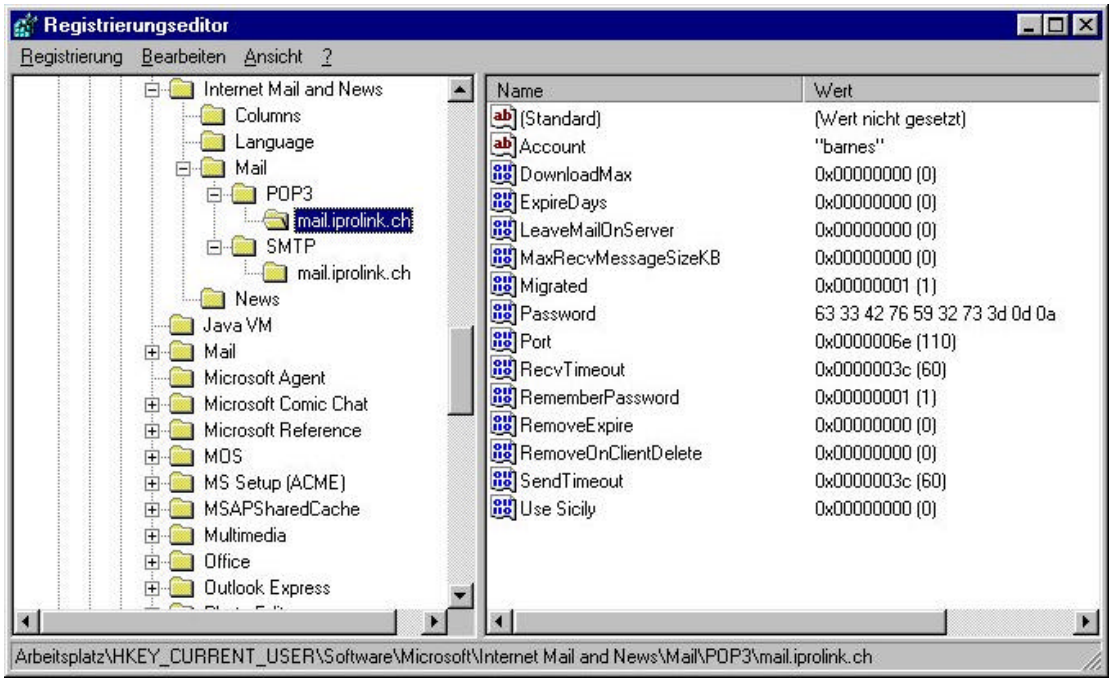
Bisher sind wir von der Situation ausgegangen, daß eine Maschine direkt aus dem Internet Email empfangen kann. Jedoch ist es in vielen Firmen die Email-

Infrastruktur auf der Basis eines zentralen Email-Servers aufgebaut. Die Benutzer holen sich auf diesem Server mit Hilfe von Client-Rechnern ihre Emails ab.

POP3

Layer 7	POP3
Layer 4	TCP
Layer 3	IP

Das gebräuchlichste Protokoll hierfür ist das *Post Office Protocol 3* (POP3), wie es in RFC 1225 definiert ist. Eine Client-Software mit diesem Protokoll hat Kommandos um sich beim Server einzuloggen, Nachrichten abzuholen und Nachrichten zu löschen. Das Protokoll selbst sieht dabei ähnlich wie SMTP aus. Die grundlegende Idee bei POP3 ist, daß alle Email-Nachrichten vom Server auf den Client kopiert werden und die lokalen Nachrichten dort verarbeitet werden.



(Beispiel einer POP3 Konfiguration anhand Win95/NT)

IMAP

Layer 7	IMAP
Layer 4	TCP
Layer 3	IP

Ein etwas weitergehendes und moderneres Protokoll ist das *Interactive Mail Access Protocol* (IMAP), das in RFC 1064 definiert wird. Es wurde entwickelt, um mehrere Client-Rechner zu unterstützen zwischen denen sich der Benutzer bewegt. Daher ist die Grundidee von IMAP, die Email-Nachrichten immer an einem zentralen Ort vorzuhalten.

Spamming

Kaum ein Thema sorgt in letzter Zeit für soviel Gesprächsstoff in der Internet-Gemeinde wie die steigende Zahl unerwünschter Emails. "Werden Sie Millionär in 30 Tagen" oder " Bei uns bekommen Sie den besten Rechner des Universums" sind Botschaften, die zuhauf in den Mailboxen eintreffen.

Dieses sogenannte *Spamming* - benannt nach einem amerikanischen Büchsenfleisch zweifelhafter Qualität - geht inzwischen über das Ärgernis hinaus. Firmen verlieren beträchtliche Geldsummen durch Spamming-Angriffe auf den Email-Server. Internet-Provider müssen immer öfter Kundenbeschwerden wegen Spam-Mails bearbeiten. So sind dies beispielsweise bei Earthlink, Pasadena inzwischen 1000 bis 3000 Beschwerden pro Tag!

Bei einer Umfrage im April 1997 sagten über 15% der Benutzer, daß sie sehr viel Spam-Mail erhalten, ca. 24% viel, ca. 28% wenig, ca. 20% wenige und nur ca. 12% keine. War vor noch nicht allzu langer Zeit die Antwort der Internet-Gemeinde auf Spamming das sogenannte *Mail-Bombing*, d.h. das Überfluten des Absenders mit Antworten, so wird dies immer schwieriger. Kommerzielle Spam-Versender nutzen spezielle Internet-Technologien, um ihre Absenderadresse zu verbergen.

Das Domain-Konzept im Internet

Stichworte:

- Domain Name System
- Der Namensraum
- Top Level Domains

Programme referenzieren Rechner und andere Ressourcen äußerst selten über über binäre Netzwerkadressen. Statt dessen finden ASCII-Zeichenketten viel öfters Verwendung, wie z.B. "barnes.ch". Dennoch versteht ein Netzwerk im allgemeinen und das Internet im speziellen ausschließlich binäre Adressen wie "192.44.32.1". Daher werden Mechanismen zur Konvertierung der einen Konvention in die andere benötigt.

Ganz zu Anfang des DARPANET genügte dafür eine einfache ASCII-Datei, die alle Rechnernamen und IP-Adressen auflistete. Jede Nacht holten alle angeschlossenen Rechner diese Datei von der Originalquelle ab. Für ein Netzwerk mit nur einigen hundert Maschinen war dies ein adäquates Vorgehen. Nachdem jedoch zigtausend Maschinen im Internet miteinander verbunden waren, erwies sich dieses Vorgehen als nicht weiter tragfähig. Insbesondere die wachsende Größe der Datei und die Namenskonflikte bei der Einbindung neuer Rechner erforderte die Entwicklung eines neuen Konzepts - des *Domain Name Systems* (DNS). Die Essenz von DNS ist die Einführung eines hierarchischen, domänebasierten Namensschemas und eines verteilten Datenbanksystems für die Implementierung dieses Namensschemas. Es wird primär für die Abbildung (Mapping) von Rechnernamen auf IP-Adressen verwendet und ist in den RFCs 1034 und 1035 spezifiziert.

Eine große und sich ständig ändernde Datenbank mit Rechnernamen ist ein nicht-triviales Problem. Beim normalen Postsystem wird das Management von Namen durch die Zuordnung von Zeichenketten für das Land, den Ort, die Straße und den Adressaten geregelt. Bie dieser Art der hierarchischen Adressierung gibt es keine Konfusion zwischen einem Bernhard Tritsch in Darmstadt und einem Bernhard Tritsch in Freiburg. Das Domain Name System funktioniert auf die selbe Weise.

Konzeptionell ist das Internet in mehrere hundert *Top Level Domains* aufgeteilt, wobei jede Domain viele Rechner umfaßt. Jede Domäne ist aufgeteilt in Subdomänen, die sich wiederum in Subdomänen verzweigen. Alle diese Domänen können in einer Baumstruktur dargestellt werden. Die Blätter der Bäume repräsentieren Subdomänen, die keine weiteren Subdomänen (aber

natürlich Rechner) beinhalten. Ein Blatt kann eine einzelne Maschine aber auch eine Firma mit tausenden von Einzelrechnern umfassen.

Die Top Level Domains bestehen aus zwei Gruppen: generische und länderspezifische. Die generischen Domänen sind

com (Commercial)

edu (Educational Institutions)

gov (US Federal Government)

int (bestimmte internationale Firmen)

mil (US Armed Forces)

net (Network Providers) und

org (Nonprofit Organizations).

Die länderspezifischen Domänen wie *de* umfassen einen Eintrag für jedes Land, wie es in ISO 3166 definiert ist.

Momentan besteht eine teilweise sehr kontrovers geführte Diskussion um die Erweiterung der generischen Top Level Domains. Wesentliche Einflußnahme nimmt dabei das *Interim Policy Oversight Committee* (IOPC). Das IOPC setzt sich aus Vertretern verschiedener Web-Organisationen zusammen und hat sich die Erörterung politischer Fragen rund ums Interent auf die Fahnen geschrieben. Ein Vorschlag des IOPC besteht darin, die Top Level Domains

firm (Kommerzielle Firmen)

store (Online-Geschäfte)

web (WWW-spezifische Sites)

arts (Kunst)

rec (Freizeitangebote)

info (Informationsforen) und

nom (persönliche Eigennamen)

in die bestehende Liste aufzunehmen. Zum Schutz von Minderjährigen wurde kurzzeitig sogar die Einführung einer Rotlichtzone im Internet (Endung *xxx*) erörtert.

Jede Domäne wird durch den aufsteigenden Pfad bis hin zur (unbenannten) Wurzel des Baumes benannt. Die Komponenten werden durch einen Punkt voneinander getrennt. Daher kann eine Abteilung (GRZ) innerhalb des Instituts für Graphische Datenverarbeitung (IGD) in der Fraunhofer-Gesellschaft (FHG)

folgendermaßen heißen: "GRZ.IGD.FHG.DE". Dieser Name steht dabei in keinerlei Konflikt mit einer Abteilung GRZ am MIT in den USA: "GRZ.MIT.EDU". Solche Namen werden als *Fully Qualified Domain Name* bezeichnet.

Domänenamen sind unabhängig von der Groß- und Kleinschreibung, daher bedeuten *edu* und *EDU* das selbe. Komponentennamen können bis zu 63 Buchstaben lang sein, der gesamte Pfad bis zu 255 Buchstaben.

Domain Name Service - DNS

Layer 7	DNS
Layer 4	UDP
Layer 3	IP

Stichworte:

- Domänen und Zonen
- NIC
- Primäre und sekundäre Name Server
- Die Namensauflösung
- Forwarder
- Rekursives Name Mapping
- DNS-Spoofing

Für das Verständnis der DNS-Namenskonventionen ist insbesondere der Begriffe *Domäne* wichtig. Die Domäne taucht bereits im Zusammenhang mit den bekannten Internet-Namen auf, z.B. "IGD.FHG.DE" oder "ZGDV.DE". Domänen sind weltweit strukturiert und werden momentan vom *Network Information Center* (NIC) sowie seinen nationalen Ablegern (z.B. DeNIC) vergeben und verwaltet.

Eine Domäne kennzeichnet eine logische Struktur von Rechnern. Innerhalb einer Domäne kann es also wie weiter oben schon beschrieben Subdomänen geben. Diese dienen einer weiteren Strukturierung umfangreicherer Netzwerke. Beim Betrieb einer eigenen Domäne ist ihr Besitzer auch für deren Verwaltung über einen *Domain Name Server* verantwortlich.

Der Domain Name Server (oder einfacher Name Server) speichert Informationen über die Domäne sowie die darin enthaltenen Systeme. Bei diesen lassen sich drei Rollen unterscheiden:

Auf primären Name Servern wird das Original der DNS verwaltet. Dort werden alle Änderungen vorgenommen.

Sekundäre Name Server bekommen ihre Daten von anderen Name Servern über das Netzwerk.

Ein Master Name Server ist der Server, von dem ein sekundärer Name Server seine Informationen erhält. Ein sekundärer Name Server kann seine Daten sowohl von einem primären Name Server als auch von einem sekundären Name Server erhalten.

Sekundäre Name Server sind aus dreierlei Gründen erforderlich:

Durch sie wird Redundanz und damit eie höhere Verfügbarkeit geschaffen: Beim Ausfall eines Name Servers steht immer noch ein zweiter Server für Anfragen zur Auflösung eines Internet-Namens in eine IP-Adresse zur Verfügung.

An Standorten, die mit schmalbandigen Leitungen verbunden sind, ist es effizienter einmal die Information zu übermitteln und dann auf einen lokalen DNS-Server zuzugreifen, als jedesmal den primären Name Server zu belasten.

Durch den Einsatz mehrerer DNS-Server kann die Last auf dem primären Server reduziert werden.

Wenn ein Client nun auf einen DNS-Server zugreift, versucht dieser die angeforderte Information bereitzustellen. In kleineren und mittleren lokalen Netzen, in denen die gesamten Informationen auf allen DNS-Servern verfügbar sind, ist dies kein Problem. In großen Netzwerken und bei einem Zugriff auf das Internet ist die Information aber sehr häufig nicht lokal verfügbar. DNS kennt für solch einen Fall das Konzept des *Forwarder*. Ausgewählte DNS-Server können als Forwarder eingerichtet werden. Nur diese Systeme können auf weitere DNS-Server - vor allem im Internet - zugreifen. Solch eine Beschränkung ist sowohl aus Gründen der Lastverteilung als auch der Sicherheit nötig. Allein dadurch kann bei einer *Firewall* gezielt eingeschränkt werden welche Systeme mit dem Internet kommunizieren dürfen und welche nicht.

Die übrigen DNS-Server werden so eingerichtet, daß sie die Forwarder verwenden. Diese Konfiguration erfolgt auf der Ebene des DNS-Servers und nicht auf der Ebene der Domänen. Wenn ein Client nun eine Anfrage an seinen DNS-Server sendet, versucht dieser zunächst die Anfrage mit Hilfe seiner Informationsdatei zu beantworten. Falls das nicht klappt, leitet er die Frage an einen der angegeben Forwarder weiter. Dieser kümmert sich um die Anfrage (ggf. durch den Zugriff auf weiter DNS-Server) und gibt das Ergebnis an den ersten DNS-Server zurück. Dieser liefert dann die erfragte IP-Adresse an den Client.

Neben den klassischen Anfragen, bei denen auf Basis eines Internet-Namens eine IP-Adresse erfragt wird, kann auch eine IP-Adresse an den DNS-Server gesendet werden, um den zugehörigen Internet-Namen zu erhalten. Diese Anfragen werden als rekursiv (oder invers) bezeichnet. Ihr Zweck liegt darin zu überprüfen, ob ein Server tatsächlich der ist, der er zu sein vorgibt - oder ob er womöglich einen falschen Namen zu einer IP-Adresse angibt.

Hier ergibt sich ein Hauptangriffspunkt kommerzieller Anbieter sicherheitskritischer Dienste, wie z.B. Banken mit Online-Anschluß. Das *DNS-Spoofing* entspricht der gezielten Manipulation der Zuordnung zwischen logischem Namen und IP-Adresse eines Servers. Es wird dabei vorgegaukelt, daß sich über den logischen Namen zu einem bestimmten Rechner verbunden wurde. Dies ist dann jedoch ein Rechner der Angreifer, der damit auch möglicherweise sicherheitskritische Informationen des Benutzers erhält.

"Yellow Pages" bzw. NIS

Stichworte:

- NIS und NIS+
- NIS Namespace
- NIS-Datenbank

Die Firma Sun Microsystems entwickelte das vormals "Yellow Pages" genannte verteilte System zur zentralen Administration von Benutzern und Computern. Die Realisierungsgrundlage ist eine Art "Nachschlage-Service", der insbesondere System-Administratoren entlasten soll.

Der Name "Yellow Pages" wurde dann in "Network Information System" geändert. Es gibt auch ein erweitertes NIS+, das erweiterte Funktionalitäten bereitstellt. NIS+ konnte sich bisher jedoch im Gegensatz zu NIS nicht als Standard durchsetzen.

Eine NIS-Domäne ist eine Gruppe von Computern, die sich eine Reihe von gemeinsamen Daten teilen:

- Passworte
- Gruppen
- Hosts, Server
- Services
- Aliase

Der NIS-Namensraum (Name Space) besteht dabei aus folgenden Informationen:

- Workstation-Name und -Adresse
- Benutzer
- Netzwerk
- Netzwerkdienste

Die grundlegende Architektur von NIS baut dabei auf eine Architektur mit Master Servers und Slave Servers (Replicators). Der NIS-Namensraum ist hierbei flach, d.h. er ist nicht hierarchisch. Die Informationen werden in einem Satz von Dateien gespeichert, die "Maps" oder "Databases" genannt werden.

NIS repräsentiert in vielen Umgebungen eine umfangreiche Datenbank. Diese ersetzt viele Informationen, die unter UNIX normalerweise in /etc-Dateien oder anderen Konfigurationsdateien verwaltet werden.

NIS basiert auf einer tabellarischen Informationsaufbereitung. Die zwei Spalten der Tabelle haben hierbei folgende Bedeutung:

- Einen "Schlüssel"
- Informationen über den Schlüssel

Einige der Informationen sind in mehreren Datenbank-Dateien gespeichert. So gibt es z.B. für die Benennung von Workstations die Dateien "host.byname" und "host.byaddr".

Network File System - NFS

Das Network File System wurde von der Firma Sun Microsystems, Inc. entwickelt und auf den Markt gebracht. Sun hat sich der Philosophie der verteilten und offenen Systeme verschrieben. Daher wurde NFS von Anfang an so konzipiert, daß es die Kopplung von Rechnern verschiedener Hersteller mit den unterschiedlichsten darauf ablaufenden Betriebssystemen erlaubt.

Die Spezifikation der NFS-Protokolle wurde von Sun veröffentlicht, eine Referenzimplementation für UNIX ist allen interessierten Parteien für einen günstigen Preis zugänglich. Die meisten Hersteller von UNIX- und PC-Systemen haben haben diese Referenzimplementation oder eine Variante davon auf ihre Rechner portiert und führen dafür Lizenzgebühren an Sun ab. Damit wurde NFS (zumindest für die UNIX-Welt) zum de-facto Standard für den verteilten Dateizugriff.

Die Nutzung im Internet-Umfeld ist evident: NFS erlaubt die Kopplung von Rechnern an einem Standort und damit die Verbindung ihrer Dateisysteme.

Dadurch lassen sich vorher getrennte Rechner, die verschiedene Internet-Dienste zur Verfügung stellen, als eine logische Einheit betrachten.

NFS erlaubt Programmen, auf Dateien in NFS-Server-Rechnern schreibend und lesend zuzugreifen. Der Zugriff geschieht für diese Programme transparent: sie müssen für den Betrieb mit NFS weder abgeändert, noch speziell vorbereitet oder mit zusätzlichen Parametern aufgerufen werden. Die Dateien im NFS-Server werden zugänglich gemacht, indem sie zunächst exportiert werden. Die NFS-Clients greifen auf diese exportierten Dateisysteme oder Ausschnitte aus Dateisystemen zu, indem sie sie in das eigenen Dateisystem einhängen. Dies wird im Netzwerkjargon "mounten" genannt. Die Bereitstellung der Zugriffsmöglichkeit erfolgt also nicht auf Veranlassung des zugreifenden Programms, sondern muß bereits vor dem Zeitpunkt des Zugriffs für lokale Systeme geschehen sein.

Ein Teilaspekt der Transparenz ist die Geschwindigkeit des Dateizugriffs über das Netz. Diese muß so hoch sein, daß kein merklicher Unterschied zu einem lokalen Plattenzugriff bemerkbar ist.

Das LDAP-Protokoll

Das *Ligthweight Directory Access Protocol* dient dem Internet-weiten Zugriff auf Verzeichnisse. Ein Verzeichnisdienst übernimmt die Verwaltung und Bereitstellung von Informationen - typischerweise über Benutzer, Benutzergruppen und andere Objekte im System. Hierdurch können einige interessante Eigenschaften ergeben:

Zentrale Verzeichnisdienste im Internet, z.B. für Email-Adressen

Einheitliche Schnittstelle für den Zugriff auf unterschiedliche Verzeichnisdienste (z.B. NFS oder NT-Filesystem)

Möglichkeit der Sicherung (Replikation) einzelner Verzeichnisinformationen

(LDAP wird nur von Browsern der 4ten Generation unterstützt und natürlich von verschiedenen E-Mail und Kalendersystemen proprietärer Hersteller wie Lotus, Microsoft oder anderen Verzeichnisdiensten wie der NDS von Novell.)

1.6 Standardisierungs-Organisationen

ITU-T -- International Telecommunication Union -- Telecommunication

Der Vorläufer der ITU-T wurde schon 1865 gegründet, um den internationalen Telegraphenverkehr zu normieren. 1947 wurde es eine Behörde der UNO.

1956 bis Februar 1993 war der Name des heutigen ITU-T: **CCITT** -- *Comité Consultatif de Télegraphique et Téléphonique = Consultative Committee for International Telegraph and Telephone*

ITU-T (bis Februar 1993: CCITT) ist ein Commitee der UN Organisation *International Telecommunications Union (ITU)*.

International Telecommunications Union (ITU) hat drei Hauptsektoren:

- *ITU-R* für Radiokommunikation: teilt weltweit die Radiofrequenzen zu
- *ITU-T* für Telekommunikation
- *ITU-D* für technische Entwicklungen

Mitglieder der ITU-T sind:

- ca. 200 Staatliche Verwaltungen und Ministerien (staatliche PTTs): sind als einzige stimmberechtigt, alle anderen haben Beobachter- und Beraterstatus
- ca. 100 anerkannte private Betreiber (z.B: AT&T, MCI, British Telecom)
- regionale Telekommunikationsorganisationen (z.B. europäische ETSI)
- andere interessierte Organisationen (z.B. Bankinstitute, Fluggesellschaften)

Offiziell veröffentlicht ITU-T (CCITT) nur Empfehlungen, während ISO (s.u.) Standards publiziert. Da ITU-T aber eine UNO-Organisation ist, sind ihre "Empfehlungen" viel verbindlicher als ISO-"Standards". Wer international Telekommunikationsdienste anbieten will, muß sich an ITU-T-Empfehlungen halten. Die Übernahme von ISO-Standards unterliegt dagegen der Freiwilligkeit der Betroffenen.

Standards und Empfehlungen des ITU-T/CCITT haben die Form Buchstabe [Punkt] Zahl (z.B. V.34). Die Buchstaben geben das Gebiet des Standards an. Für uns wichtig sind die Gruppen:

I: Diensteintegrierende Netze -- Integrated Services Digital Network (ISDN) [Datenbank der I-Empfehlungen: URL: http://www.itu.ch/itudoc/itu-t/rec/i.html. -- Zugriff am 18. 4. 1997]

V: Datenkommunikation über Telephonnetze: [Datenbank der V-Empfehlungen: URL: http://www.itu.ch/itudoc/itu-t/rec/v.html. -- Zugriff am 18. 4. 1997]

V.1 ff.: Grundlagen und allgemeine Festlegungen

V.10 ff.: Schnittstellen für Modems im Fernsprechband

V.35 ff.: Breitbandmodems

V.40 ff.: Fehlersicherung

V.50 ff.: Übertragungsqualität und Unterhalt

V.100: Verknüpfung von öffentlichen Daten- und Telefonnetzen -- V.110: Unterstützung von Datenendeinrichtungen mit V-Schnittstellen durch ein ISD

X: Öffentliche Datenkommunikationsnetzwerke: [Datenbank der X-Empfehlungen: URL: http://www.itu.ch/itudoc/itu-t/rec/x.html. -- Zugriff am 18. 4. 1997]

- X.1 ff.: Dienste und Leistungen in Datennetzen
- X.20 ff.: Schnittstellen in Datennetzen
- X.40 ff.: Übertragung, Kennzeichengabe und Vermittlung in Datennetzen
- X.92 ff.: Netzaspekte in Datennetzen
- X.200 ff.: OSI-Modell, Dienste und Protokolle
- X.300 ff.: Zusammenarbeit von verschiedenen Netzen
- X.400 ff.: Nachrichten-Behandlungs-Systeme

Alle vier Jahre gibt CCIT/ITU-T einen Satz von Standards heraus. Jeder Jahrgang hat eine bestimmte Farbe, deshalb spricht man z.B. von *Blue Books*:

- red: 1960, 1984
- blue: 1964, 1988
- white: 1968, 1992
- green: 1972
- orange: 1976
- yellow: 1980

Seit 1988 werden Standards auch außerhalb dieses Vierjahreszyklus veröffentlicht. (Pro Jahr veröffentlicht ITU-T ca. 5000 Seiten Empfehlungen).

Weiterführende Ressourcen:

Web-Page von ITU: URL: http://info.itu.ch.

ISO -- International Organization for Standardization

ISO wurde 1946 gegründet und ist eine freiwillige (nicht per Staatsvertrag geregelte) Organisation mit Sitz in Genf, deren Beschlüsse nicht den Charakter international verbindlicher Verträge haben. Sie hat als Ziel, internationale Standards zu schaffen. Stimmberechtigte Mitglieder sind fast alle nationalen normgebenden Institutionen der 89 beteiligten Staaten. Daneben gibt es noch andere Mitglieder mit Beobachter- und Beraterstatus. ISO ist Mitglied der ITU-T. Im Bereich der Telekommunikation ist ISO für die Entwicklung von OSI verantwortlich.

Mitglieder von ISO sind z.B.:

- ***ANSI*** -- *American National Standards Institute*: [WWW-Page: http://www.ansi.org. -- Zugriff am 18. 4. 1997]. ANSI ist die Standardisierungsorganisation der USA (entspricht dem deutschen DIN). ANSI entwirft die Standards nicht selbst, sondern publiziert und verbreitet Standardentwürfe und Standards. Ein für Bibliotheken wichtiger ANSI Standard ist Z39.50 *"Information Retrieval Service Definition and Protocol Specification for Library Applications Standard".*
- ***BSI*** -- *British Standard Institute* [WWW-Page: http://www.bsi.org.uk/. -- Zugriff am 18. 4. 1997]
- ***DIN*** -- *Deutsches Institut für Normung* [WWW-Page: http://www.din.de. -- Zugriff am 18.4. 1997]
- ***SNV*** -- *Schweizerische Normenvereinigung*
- ***AFNOR*** -- *Association Francaise de Normalisation* [WWW-Page: http://www.afnor.fr. -- Zugriff am 18. 4. 1997]
- ***NNI*** -- *Nederlands Normallisatie-Instituut* [WWW-Page: http://www.nni.nl/. -- Zugriff am 18.4. 1997]
- ***JISC*** -- *Japanese Industrial Standards Committee* [Über JISC: http://www.hike.te.chiba-u.ac.jp/ikeda/JIS/. -- Zugriff am 18. 4. 1997]

Die Aktivitäten von ISO werden gegliedert in:

- *TC* -- Technical Commitee: z.B. TC97 behandelt Computer and Information Processing
- *SC* -- Subcommittee eines Technical Commitee: z.B: TC97/SC15 behandelt Datenstrukturen und Kennsätze und wird bei der Schweizer Normenvereinigung geführt
- *WG* -- Working Group eines Subcommitee: z.B. TC97/SC15/WG1 behandelt Disketten

Ein ISO Standard durchläuft eine Reihe von teils lange dauernden Zuständen:

- *WD*: Working Document
- *CD*: Commitee Document, erstellt von einer Working Group (WG). Bis vor kurzem als DP - - Draft Proposal bezeichnet
- *DIS*: Draft International Standard, hat Zustimmung des Subcommitee (SC)
- *IS*: International Standard, hat Zustimmung des Council

Wird nach Fertigstellung eines Standards eine Erweiterung geschaffen, so erhält diese den Zusatz *AMD* (früher *ADD*)

Neben Standards gibt es noch Technical Reports (*TR*). Sie kommentieren Standards, haben aber nicht Standardcharakter.

Weiterführende Ressourcen:

WWW-Page der ISO: http://www.iso.ch.

IEEE -- Institute of Electrical and Electronic Engineers

IEEE ist eine Organisation in den USA, die auch Standards für die Datenkommunikation entwickelt. Diese Standards werden dem ANSI zur Billigung und Erhebung zum US-Standard vorgelegt. Auch dem ISO werden die Standardentwürfe vorgelegt. Die Committees von *Project 802* entwerfen vor allem Standards für den Physical und den Data Link Layer des OSI. Viele der IEEE 802 Standards sind auch ISO 8802 Standards (z.B. IEEE 802.3 = ISO 8802.3).

Weiterführende Ressourcen

WWW-Page des IEEE: http://www.ieee.org .

1.7 Referenzen

- **RFC-Archiv** / INTERNIC. -- URL: http://ds.internic.net/ds/dspg1intdoc.html .
- **RFC Web** / Ohio State Univ. -- URL: http://www.cis.ohio-state.edu/hypertext/information/rfc.html
- **Internet Society**: (eine private non-profit organization): entwickelt die Netzwerktechnologie weiter, achtet auf das Einhalten der Protokolle, unterstützt das IAB. URL: http://info.isoc.org/.
- **Internet Architecture Board (IAB)**: ist zuständig für die Standards, u.a. für die Internet Assigned Numbers Authority, die für die Adressen zuständig ist. URL: http://www.iab.org/iab/.
- **Internet Engineering Task Force (IETF)**: IETF ist eine Expertengruppe, die Probleme der Technik und der Standards des Internet behandelt. URL: http://www.ietf.org.
- **Internet Research Task Force.** URL: http://www.irtf.org/irtf/.

Protokolle zur Verbindung lokaler Rechner über Modems [bzw. ISDN-Wählverbindung] mit dem Internet:

- **PPP -- *Point-to-Point Protocol*: RFC 1661**. -- URL: http://ds.internic.net/rfc/rfc1661.txt.
- **SLIP** -- *A Nonstandard for transmission of IP datagrams over serial lines*: **RFC 1055**. -- URL: http://ds.internic.net/rfc/rfc1055.txt.

Transport-Protokolle (Transport Layer)

- **TCP** -- ***Transmission Control Protocol*: RFC 793**. -- URL: http://ds.internic.net/rfc/rfc793.txt.
- **UDP** -- ***User Datagram Protokoll*: RFC 768**. -- URL: http://ds.internic.net/rfc/rfc768.txt.

Routing-Protokolle (Network Layer)

- **IP(v4)** -- ***Internet Protocol (Version 4)***: : für die eigentliche Datenübertragung: **RFC 791**. -- URL: http://ds.internic.net/rfc/rfc791.txt.
- **ICMP** -- ***Internet Control Message Protocol***: für status messages für IP, wie Error-Meldungen und Veränderungen in der Hardware des Netzwerkes, die das Routing beeinflussen: **RFC 792**. -- URL: http://ds.internic.net/rfc/rfc792.txt.
- **RIP** -- ***Routing Information Protocol***: zur Bestimmung des besten Routing
- **OSPF** -- ***Open Shortest Path First***: eine Alternative zu RIP

Adreß-Protokolle (Application Layer)

- **ARP** -- ***Address Resolution Protocol***: für IP-Adressen: **RFC 826**. -- URL: http://ds.internic.net/rfc/rfc826.txt .
- **RARP** -- ***Reverse Address Resolution Protocol***: wie ARP aber in umgekehrter Reihenfolge: **RFC 903**. -- URL: http://ds.internic.net/rfc/rfc903.txt.
- **DNS** -- ***Domain Name System***: **RFC 1034, 1035**. -- URLs: http://ds.internic.net/rfc/rfc1034.txt, http://ds.internic.net/rfc/rfc1035.txt.

User-Services-Protokolle (Application Layer)

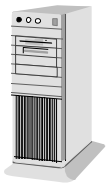
- **FTP -- *File Transfer Protocol*: RFC 959**. -- URL: http://ds.internic.net/rfc/rfc959.txt.
- **TFTP -- *Trivial File Transfer Protocol*: RFC 783**. -- URL: http://ds.internic.net/rfc/rfc783.txt.
- **TELNET** für remote logins: **RFC 854**. -- URL: http://ds.internic.net/rfc/rfc854.txt. -- **RFC 855**. -- URL: http://ds.internic.net/rfc/rfc855.txt.
- **SMTP -- *Simple Mail Transfer Protocol*: RFC 821**. -- URL: http://ds.internic.net/rfc/rfc821.txt.
- zu den User-Services-Protokollen kommen noch die Berkeley **r-utilities** hinzu (sie beginnen alle mit r = remote), wie rlogin (remote login), rshell (remote shell), rcp (remote copy)
- **Gopher: RFC 1436.** -- URL: http://ds.internic.net/rfc/rfc1436.txt.

- **HTTP -- *Hypertext Transfer Protocol* --** URL: www.w3.org/Protocols
- **HTTP 1.1 RFC 2068 URL:** www.w3.org/Protocols

Andere Protokolle (Netzwerkverwaltung)

- **SNMP -- *Simple Network Management Protocol*** für die Systemüberwachung :**RFC 1157**. -- URL: http://ds.internic.net/rfc/rfc1157.txt.
- **SNMPv2 -- *Simple Network Management Protocol version 2*** für die Systemüberwachung: **RFC 1441 - 1450**. -- URL: http://ds.internic.net/rfc/rfc1441.txt.

HTML Seite wird in Paketform (fragmentiert) übertragen



<table>
<tr><td rowspan="3">Der Benutzer sendet eine Anfrage über eine URL, welche mit protocol://server/filename
Wobei als Protokoll http verwendet wird. Der Client erhält jetzt die Anwort für jedes einzelne Element, welches in der Datei (htm(l)) beschrieben wurde. Also wird für jedes html-dokument, sowie für jedes Bild, Applet u.s.w. eine eigene TCP Anfrage gestartet.
HTTP:
Sendet eine Anfrage nach einer Datei auf dem Server und übernimmt die Datei (zusammengesetzt von TCP) und interpretiert Sie.
Im Falle von HTTP übernimmt dieses die Aufgaben von:
Applikation Layer
Presentation Layer
Session Layer</td><td>Applikation Layer</td><td></td></tr>
<tr><td>Presentation Layer</td><td></td></tr>
<tr><td>Session Layer</td><td></td></tr>
<tr><td colspan="2">TCP:
Dieses Protokoll regelt, unter anderem die Zusammensetzung der fragmentierten Pakete und setzt sie in der richtigen Reihenfolge wieder zusammen. Aussderdem steht in diesem Header der Serviceport von http (Port 80) an den die Pakete dann übergeben werden.</td><td>Transport Layer</td><td></td></tr>
<tr><td colspan="2">IP:
Hier werde u.a. Absender-IP Adresse und Ziel-IP Adresse eingetragen. Anhand der Zieladresse und dessen Netzteil muss gegebenenfalls ein Router entscheiden, welchen Weg das „Routing“ nimmt.
Wichtig ist noch, dass hier auch der ServicePort für den Transport eingetragen ist TCP (Port 6) UDP (Port10)</td><td>Network Layer</td><td></td></tr>
<tr><td rowspan="2">Pakete, die, diese Schicht überqueren wollen, müssen mit einem Ethernet Header
(nach 802.2 oder 802.3(Frame Typ)) versehen werden oder von diesem befreit werden.
Diese Schicht „horcht“ auf dem Netzwerksegement, ob ein „vorbeiflitzendes Element“ (Paket) für diese Station bestimmt ist. Auf der anderen Seite sendet es Pakete an eine bestimmte MAC Adresse. In unserem Fall an den Default-Gateway, sofern die Zielstation in im eigenen LAN ist.(Wenn 802.3, d.h mit CSMA/CD)</td><td>LLC:
Logical Link Control:
Ermöglicht Peer-to-Peer Kommunikation auf einem LAN</td><td rowspan="2">Data Link Layer</td><td rowspan="2"></td></tr>
<tr><td>MAC:
Medium Access Control Sublayer (MAC Adresse)
Hardwareadresse von Computer im LAN
• MAC Adresse wird über einen ARP-Request ermittelt.</td></tr>
<tr><td colspan="2">Übertragungsmedium (Kabel) muss den Spezifikationen von 802.3 genügen.</td><td>Physical Layer</td><td></td></tr>
</table>