Einleitung

Das Ethernet hat sich in der Automatisierungsbranche mittlerweile als Standard durchgesetzt und ist dabei, mit den mittlerweile verfügbaren Echtzeit-Varianten auch auf der Feldbusebene einen bedeutenden Marktanteil zu gewinnen. Die Modifikationen eines millionenfach bewährten Übertragungsverfahrens bietet die Gewähr, dass die physikalischen Schnittstellen wenig kosten und störungsfrei ihren Dienst versehen. Ethernet als Standard ist die Vorraussetzung dafür, dass der Informationsfluss über alle informationsverarbeitenden Systeme eines Unternehmens bis hinunter zur Feldebene reicht.

In der Festlegung auf einen Standard liegt ein erhebliches Einsparpotential. Die bisherige Vielfalt in der industriellen Kommunikation zieht erhebliche Folgekosten nach sich: aufwendiges Engineering, zusätzliche Hardware z.B. für Netzübergänge, hohe Inbetriebnahme- und Wartungskosten sowie eine kostspielige Schulung des Bedienpersonals auf den eingesetzten Systemen. Um dieses Sparpotential zu nutzen, ist das Ethernet in der industriellen Kommunikation das richtige Medium. Seine Vorzüge sprechen für sich, die Schwäche des nicht-deterministischen Zugriffsverfahren ist bei den Echtzeit-Ethernet-Varianten behoben. Es ist in allen Leistungsklassen verfügbar; längst sind optische Schnittstellen definiert, die einen Einsatz auch unter schwierigen elektromagnetischen Verhältnissen möglich machen. Und es eröffnet seit kurzem auch die Möglichkeit ohne größeren Aufwand Anlagenteile und Geräte per „Wireless-LAN“-Technik drahtlos anzubinden.

Das Vorbild für den Einsatz des Ethernet in der Automatisierung war die Bürokommunikation: Über einen Standard sind alle Rechner miteinander verbunden.

Dieses, zum Begleittext zusätzliche Skript, stellt vor allem Ethernet und die Verkabelung neben dem Protokoll-Standard TCP/IP und den Netzwerkbetriebssystemen vertiefend vor.

OSI-Modell

Ein Schichtenmodell versucht die verschiedenen Problembereiche der computervermittelten Kommunikation auf Schichten klar zu verteilen, die aufeinander aufsetzen.
Ein elementares Schichtenmodell mit zwei grundlegenden Schichten würde folgendermaßen aufgebaut sein:

- Anwendungenorientierte Schicht (Applications Oriented Layer):
  diese Schicht beinhaltet die anwendungsbezogene Bedeutung der übertragenen Daten
- Endsystem-zu-Endsystem orientierte Schicht (End-System to End-System Oriented Layer):
  diese Schicht beinhaltet die fehlerfreie und ungehinderte Datenübertragung von Computer zu Computer ohne Rücksicht auf die anwendungsbezogene Bedeutung dieser Daten

Das OSI-Modell (engl. *Open Systems Interconnection Reference Model*) ist ein offenes Schichtenmodell, das seit den 70er Jahren entwickelt und standardisiert wurde. Es teilt die verschiedenen Problembereiche der Netzwerkkommunikation in sieben Schichten auf.

Weitere Bezeichnungen für das Modell sind *ISO/OSI-Modell*, *OSI-Referenzmodell*, *OSI-Schichtenmodell* oder *7-Schichten-Modell*.

Ein Netzwerk stellt seinen Benutzern Dienste bereit. Im einfachsten Fall überträgt es Daten von A nach B. Hierzu müssen jedoch tatsächlich eine Vielzahl von Aufgaben bewältigt werden. Die Probleme, die dabei gelöst werden müssen, reichen von Fragen der elektronischen Übertragung der Signale über eine geregelte Reihenfolge in der Kommunikation (wer darf wann senden?) bis hin zu abstrakteren Aufgaben, die sich innerhalb der kommunizierenden Anwendungen ergeben. Die Vielzahl dieser Probleme und Aufgaben lässt es sinnvoll erscheinen, das Netz nicht als einen einzigen Dienstleister zu betrachten, sondern seine Dienste ganz bestimmten Kategorien zuzuordnen. Als besonders geeignet hat sich die Aufteilung in Schichten erwiesen.

Im OSI-Modell nimmt der Abstraktionsgrad der Funktionen von Schicht zu Schicht zu. Die Daten werden von einer Schicht zur nächsten weitergereicht, d.h. die Kommunikation erfolgt in vertikaler Richtung. Auf der Senderseite läuft die Kommunikation von oben nach unten und auf der Empfängerseite von unten nach oben.

Das Modell besteht aus sieben Schichten (engl. *layers*). Für jede Schicht sind die Dienste und Funktionen definiert, die auf ihr erfüllt werden sollen. Da jedoch keine Standards definiert sind, die diese Dienste und Funktionen verwirklichen, kann dies u.U. durch unterschiedliche Protokolle erfüllt werden.

- **Anwendungsschicht, Schicht 7**, die oberste der sieben hierarchischen Schichten. (engl. application layer, auch: Verarbeitungsschicht, Anwenderebene) Die Anwendungsschicht stellt den Anwendungen eine Vielzahl an Funktionalitäten zur Verfügung (z.B. Datenübertragung, E-Mail, Virtual Terminal bzw. Remote login etc.)

- **Darstellungsschicht, Schicht 6,** (engl. presentation layer, auch: Datendarstellungsschicht, Datenbereitstellungsebene) Die Darstellungsschicht standardisiert die Datenstrukturen und ermöglicht somit den semantisch korrekten Datenaustausch zwischen unterschiedlichen Systemen (u.a. Kodierung, Kompression, Kryptographie)

- **Sitzungsschicht, Schicht 5,** (engl. session layer, auch: Kommunikationssteuerungsschicht, Steuerung logischer Verbindungen, Sitzungsebene) Um Zusammenbrüche der Sitzung und ähnliche Probleme zu beheben, stellt die Sitzungsschicht Dienste für einen organisierten und synchronisierten Datenaustausch zur Verfügung. Zu diesem Zweck werden so genannte Token eingeführt.

- **Transportschicht, Schicht 4,** (engl. transport layer, auch: Ende-zu-Ende-Kontrolle, Transport-Kontrolle) Die Transportschicht ist die unterste Schicht, die eine vollständige Ende-zu-Ende Kommunikation (zwischen Sender und Empfänger) zur Verfügung stellt, d.h.

für alle Schichten oberhalb der Netzwerkschicht ist die darunter liegende Netzwerktopologie transparent. Zu den Aufgaben der Transportschicht zählt u.a. die Segmentierung von Datenpaketen und die Stauvermeidung (engl. congestion control).

- **Netzwerkschicht, Schicht 3,** (engl. network layer, auch: Vermittlungsschicht, Paketebene) Die Netzwerkschicht sorgt für die Weitervermittlung von Datenpaketen. Da nicht immer eine direkte Kommunikation zwischen Absender und Ziel möglich ist, müssen Pakete weitergeleitet werden. Weitervermittelte Pakete gelangen nicht in die höheren Schichten, sondern werden mit einem neuen Zwischenziel versehen und an den nächsten Host gesendet. Zu den Aufgaben der Netzwerkschicht zählt der Aufbau und die Aktualisierung von Routingtabellen, sowie die Flusskontrolle.

- **Sicherungsschicht, Schicht 2,** (engl. data link layer, auch: Verbindungssicherungsschicht, Verbindungsebene, Prozedurebene) Aufgabe der Sicherungsschicht ist es, eine sichere (d.h. fehlerfreie) Verbindung zu gewährleisten und den Zugriff auf das Übertragungsmedium zu regeln. Dabei teilt man die Schicht in zwei Subschichten auf: die LLC-Schicht (logical link control) und die Mediumzugriffsschicht (medium access control layer, MAC-Layer). Die Aufgaben der LLC-Schicht sind das Aufteilen des Bitdatenstromes in Datenrahmen (frames) und das Hinzufügen von Prüfsummen sowie das Verwalten von Quittungen und die Flusskontrolle. Die Mediumzugriffsschicht regelt konkurrierende Zugriffe mehrerer Stationen auf ein gemeinsames Übertragungsmedium und behandelt ggf. aufgetretene Kollisionen.

- **Physikalische Schicht, Schicht 1**, die niedrigste Schicht. (engl. physical layer, auch: Bitübertragungsschicht, physikalische Ebene) Die physikalische Schicht ist für die eigentliche Bitübertragung der Daten zuständig. Hierzu ist eine Standardisierung der Netzwerk-Leitungen und -Anschlüsse sowie ihrer physikalischen Eigenschaften nötig. Die gemeinsame Nutzung eines Übertragungsmediums kann auf dieser Schicht durch ein statisches Multiplexing erfolgen.

Das OSI-Referenzmodell wird oft herangezogen, wenn es um das Design von Netzwerkprotokollen und die theoretische Betrachtung geht. Zusammen mit diesem Modell sind Netzwerkprotokolle entwickelt worden, die jedoch heute kaum eine Bedeutung besitzen. In der Praxis wird hauptsächlich die Familie der TCP/IP-Protokolle eingesetzt. Da das TCP/IP-Referenzmodell sehr speziell auf den Zusammenschluss von Netzen (*Internetworking*) zugeschnitten ist, bietet das OSI-Referenzmodell einen umfassenderen Ansatz für die Betrachtung von Netzwerkprotokollen.

Das OSI-Modell im Überblick (im Vergleich dazu das TCP/IP-Referenzmodell):

<table>
<tr><th></th><th>OSI-Schicht</th><th>TCP/IP-Schicht</th><th>Kommunikation</th></tr>
<tr><td>7</td><td>Anwendung</td><td>Anwendung</td><td rowspan="4">Ende zu Ende (Multihop)</td></tr>
<tr><td>6</td><td>Darstellung</td><td rowspan="2">--</td></tr>
<tr><td>5</td><td>Sitzung</td></tr>
<tr><td>4</td><td>Transport</td><td>Transport</td></tr>
<tr><td>3</td><td>Netzwerk</td><td>Internet</td><td rowspan="3">Punkt zu Punkt</td></tr>
<tr><td>2</td><td>Sicherung</td><td rowspan="2">Host an Netz</td></tr>
<tr><td>1</td><td>Bitübertragung</td></tr>
</table>

Vorteile eines Schichtenmodells sind:

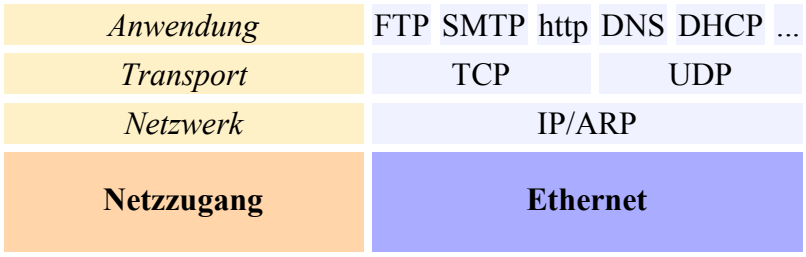
- **Spezialisierung:**
  Entwickler können sich auf die Probleme jeweils einer Schicht konzentrieren und damit mit der unterschiedlich schnellen technischen Entwicklung besser Schritt halten

- **geringere Kosten:**
  man kann die Ausrüstung (Implementierungen) für eine Schicht ändern, ohne alle anderen ändern zu müssen
- **Wahlfreiheit:**
  der Endnutzer kann durch die Wahl unterschiedlicher Implementierungen für seine Probleme maßgeschneiderte Lösungen zusammenstellen

Ethernet

Ethernet ist eine paketbasierte Computer-Vernetzungstechnologie für lokale Netzwerke (LANs). Sie definiert Kabeltypen und Signalisierung für die Bitübertragungsschicht, und Paketformate und Protokolle für die Medienzugriffskontrolle (Media Access Control, MAC)/Verbindungsschicht des OSI-Modells. Ethernet ist weitestgehend in der IEEE-Norm 802.3[1] standardisiert. Sie wurde ab den 1990ern zur meistverwendeten LAN-Technologie und hat andere LAN-Standards wie Token Ring, FDDI und ARCNET verdrängt.

Ethernet mit TCP/IP Protokollstack



Geschichte

Ethernet wurde ursprünglich am Xerox Palo Alto Research Center (PARC) entwickelt. Eine weit verbreitete Geschichte besagt, dass Ethernet 1973 erfunden wurde, als Robert Metcalfe ein Memo über das Potenzial von Ethernet an seine Vorgesetzten schrieb. Metcalfe selbst sagt, dass Ethernet über mehrere Jahre entwickelt wurde und sich daher kein Zeitpunkt festmachen lässt. 1976 veröffentlichten Metcalfe und sein Assistent David Boggs ein Papier mit dem Titel *Ethernet: Distributed Packet-Switching For Local Computer Networks.*
Metcalfe verließ Xerox 1979, um die Benutzung von Personal Computern und LANs zu fördern und gründete die Firma 3Com. Er überzeugte erfolgreich DEC[2], Intel und Xerox zusammenzuarbeiten, um Ethernet zum Standard zu machen. Damals konkurrierende Techniken waren die proprietären Systeme Token Ring und ARCNET, die beide bald in einer wahren Flut von Ethernet-Produkten untergingen. 3Com wurde dabei ein großes Unternehmen.

Der CSMA/CD-Algorithmus

Ethernet basiert auf der Idee, dass die Teilnehmer eines Netzwerkes Nachrichten durch eine Art Funk-System versenden, allerdings nur innerhalb eines gemeinsamen Leitungsnetzes, das manchmal als Äther bezeichnet wurde (der Äther war in der Vorstellung des 19. Jahrhunderts der Stoff, durch den sich das Licht hindurch bewegte). Jeder Teilnehmer hat einen global eindeutigen 48-bit-Schlüssel, der als seine MAC-Adresse bezeichnet wird. Dies soll sicherstellen, dass alle Systeme in einem Ethernet unterschiedliche Adressen haben.

Ein Algorithmus mit dem Namen Carrier Sense Multiple Access with Collision Detection (CSMA/CD) regelt den Zugriff der Systeme auf das gemeinsame Medium. Er wurde ursprünglich in den 1960er Jahren für das ALOHAnet, ein Funknetz in Hawaii entwickelt. Das Schema ist verglichen mit Token Ring oder Master-kontrollierten Netzwerken relativ simpel. Wenn ein Gerät Daten senden möchte, hält es sich an folgenden Ablauf:

[1] http://www.ieee802.org/3/
[2] DEC: Digital Equipment Corporation, "fusioniert" mit Compaq, diese dann mit Hewlett Packard

1. Wenn die Leitung frei ist, beginne mit der Übertragung, andernfalls weiter mit Schritt 4.
2. [**Informationsübertragung**] Wenn eine Kollision entdeckt wird (Netzwerkgeräte können das Auftreten einer Kollision erkennen, da die Amplitude des Signals im Netzwerk sich erhöht), weiter übertragen (dabei wird ein so genanntes JAM-Signal als Kollisionskennung gesendet) bis die minimale Paketdauer erreicht wird (um sicherzustellen, dass alle anderen Transceiver die Kollision entdecken), dann weiter mit Schritt 4.
3. [**Übertragung erfolgreich abgeschlossen**] Erfolgsmeldung an höhere Netzwerkschichten, Übertragungsmodus verlassen.
4. [**Leitung ist belegt**] Warten, bis die Leitung wieder frei ist.
5. [**Leitung ist gerade frei geworden**] Noch eine zufällige Zeit abwarten, dann wieder bei Schritt 1 beginnen, wenn die maximale Anzahl von Übertragungsversuchen nicht überschritten wurde.
6. [**Maximale Anzahl von Übertragungsversuchen überschritten**] Fehler an höhere Netzwerkschichten melden, Übertragungsmodus verlassen.

In der Praxis funktioniert dies bildlich wie eine Dinner-Party, auf der alle Gäste ein gemeinsames Medium (die Luft) benutzen, um miteinander zu sprechen. Bevor sie sprechen, warten sie höflich darauf, dass der andere Gast geendet hat. Wenn zwei Gäste zur gleichen Zeit zu sprechen beginnen, stoppen beide und warten für eine kurze, zufällige Zeitspanne in der Hoffnung, dass beide nicht wieder zur gleichen Zeit weiter sprechen, und vermeiden so eine weitere Kollision.

Da die gesamte Kommunikation auf derselben Leitung passiert, wird jede Information, die von einem Computer gesendet wurde, von allen empfangen, selbst wenn diese Information nur für ein Ziel bestimmt ist. Die meisten Ethernet-verbundenen Geräte müssen ständig Informationen ausfiltern, die nicht für sie bestimmt sind. Dies ist eine Sicherheitslücke von Ethernet, da ein Teilnehmer mit bösen Absichten den gesamten Datenverkehr auf der Leitung mitschneiden kann, wenn er möchte. Dieser Sicherheitsmangel kann zum großen Teil durch die Einrichtung einer geswitchten Umgebung (wobei Switches anstatt Multiport-Repeater (ugs. Hub), als Verteilersysteme benutzt werden) behoben werden.

Ethernet als gemeinsames Medium funktioniert gut, solange das Verkehrsaufkommen niedrig ist. Da die Chance für Kollisionen proportional mit der Anzahl der Transmitter und der zu sendenden Datenmenge ansteigt, tritt oberhalb von 50% Auslastung vermehrt ein als „Congestion“ bekanntes Phänomen auf, wobei regelrechte Staus entstehen und eine vernünftige Arbeit mit dem Netzwerk nicht mehr möglich ist. Um dies zu lösen und die verfügbare Bandbreite zu maximieren, wurden Switches und der Full-Duplex-Modus (Daten können gleichzeitig gesendet und empfangen werden) entwickelt.

Ethernet-Frameformate und das EtherType-Feld

Historische Formate
Es gibt vier Typen von Ethernet-Frames:

- Ethernet Version I (nicht mehr benutzt)
- Der Ethernet Version 2 oder Ethernet II Frame, der sog. DIX-Frame (benannt nach DEC, Intel, und Xerox), dies ist der heute meistverwendete Typ, da er oft direkt vom Internet Protocol benutzt wird.
- IEEE 802.x LLC (Logical Link Control) Frame
- IEEE 802.x LLC/SNAP Frame

Die unterschiedlichen Frame-Typen haben unterschiedliche Formate und Paketgrößen, können aber auf demselben physischen Medium parallel verwendet werden.
Der ursprüngliche Xerox Version 1 Ethernet-Frame hatte ein 16-bit-Feld, in dem die Länge des Frames hinterlegt war, obwohl die maximale Paketlänge auf 1.500 Bytes begrenzt war.

Dieses Längen-Feld wurde in Xerox's Ethernet II-Frame als Label weiterverwendet, mit der Konvention, dass Werte zwischen 0 und 1.500 auf das originale Ethernet-Format hindeuteten, und höhere Werte den EtherType und die Verwendung des neuen Frame-Formats anzeigten. Dies wird

inzwischen in IEEE 802-Protokollen durch den SNAP Header unterstützt. Der EtherType zeigt über eine Protokollnummer das im Datenteil des Frames verwendete Protokoll an.

IEEE 802.x definierte das 16-bit-Feld nach den MAC-Adressen wieder als Längen-Feld. Da Ethernet I-Frames nicht mehr benutzt werden, erlaubt dies festzustellen, ob es sich um einen Ethernet II-Frame oder einen IEEE 802.x-Frame handelt und damit die Koexistenz beider Standards auf dem selben physischen Medium. Alle 802.x-Frames haben ein LLC-Feld. Durch Untersuchung des LLC-Feldes kann festgestellt werden, ob noch ein SNAP-Feld folgt.

Ethernet II
Die Unterschiede zwischen Ethernet (Ethernet-II) und IEEE-802.3-LANs sind subtil. Die Ethernet-Dienste werden entsprechend den Schichten 1 und 2 des OSI-Referenzmodells vermittelt; IEEE 802.3 hingegen spezifiziert die Bitübertragungsschicht (Schicht 1) und den Medienzugriff der Sicherungsschicht (Schicht 2), nicht jedoch die LLC-Funktionalität. Ethernet wie auch IEEE 802.3 werden durch Hardware implementiert. Die physikalische Komponente dieser Protokolle ist entweder eine Netzwerkkarte in einem Hostcomputer oder eine Schaltung auf einer Platine in einem Hostcomputer. Der übliche Typ ist heute der Ethernet II-Frame, wie er von den meisten Internet Protocol-basierten Netzwerken benutzt wird. Es gibt zwar Techniken, um IP-Verkehr in 802.3-Frames zu kapseln, sie werden aber kaum verwendet.

Präambel	Zieladresse	Quelladresse	Typ	Daten	Prüfsequenz
8 Byte	6 Byte	6 Byte	2 Byte	46-1500 Byte	4 Byte
aaaaaaaaaaaaaaab	8000207a3f3e	800020203aae	0x0800	IP-Paket, etc	3dae237f

Das heute fast ausschließlich verwendete Ethernet II-Frameformat (Beispiel-Werte)

Die Gesamtlänge (ohne Präambel, die zur Frame-Synchronisation benötigt wird) beträgt zwischen 64 und 1518 Bytes. Die ersten 6 Bytes enthalten die 48-Bit MAC-Adresse des Zielrechners oder die Broadcast-Adresse `ff-ff-ff-ff-ff-ff`. Darauf folgen 6 Bytes mit der MAC-Adresse des Senders. An die 2 Bytes mit dem Typfeld bei Ethernet II schließen sich die Daten an. Der gesamte Ethernetframe wird am Ende mit einer 32-Bit CRC-Prüfsumme versehen.

Typfeld	Protokoll
0x0800	IP Internet Protocol (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x8035	Reverse Address Resolution Protocol (RARP)
0x809b	Appletalk (Ethertalk)
0x80f3	Appletalk Address Resolution Protocol (AARP)
0x8137	Novell IPX (alt)
0x8138	Novell
0x86DD	Internet Protocol, Version 6 (IPv6)

Typfeld (EtherType) der wichtigsten Protokolle

Ethernet-Medientypen
Die verschiedenen Ethernet-Varianten unterscheiden sich in Geschwindigkeit und den verwendeten Kabeltypen. Der Protokoll-Stack (Software) arbeitet deshalb bei den meisten der folgenden Typen identisch.
Die folgenden Abschnitte geben einen kurzen Überblick über alle offiziellen Ethernet-Medientypen. Zusätzlich zu diesen offiziellen Standards haben viele Hersteller proprietäre Medientypen entwickelt, häufig, um mit Glasfaserkabeln höhere Reichweiten zu erzielen.

Einige frühe Varianten von Ethernet

- **Xerox Ethernet** - die ursprüngliche Ethernet-Implementation, die während ihrer Entwicklung zwei Versionen hatte. Das Frame-Format der Version 2 wird noch immer überwiegend benutzt.
- **10Broad36** - Obsolet. Ein früher Standard, der Ethernet über größere Entfernungen unterstützte. Es benutzte Breitband-Modulationstechniken ähnlich denen von Kabelmodems und arbeitete mit Koaxialkabel.
- **1Base5** - Ein früher Versuch, eine günstige LAN-Lösung zu standardisieren. Arbeitete bei 1 Mbit/s und war ein kommerzieller Fehlschlag.
- **StarLAN 1** - Die erste Ethernet-Implementation über Twisted-Pair-Kabel, entwickelt von AT&T.

10 Mbit/s Ethernet mit Koaxialkabel

- **10Base2** (bekannt als *Thinnet* oder *Cheapernet*) - 50-Ohm-Koaxialkabel verbindet die Teilnehmer miteinander, jeder benutzt ein T-Stück zur Anbindung seiner Netzwerkkarte. An den Enden der Leitung sitzen Terminatoren. Für viele Jahre war dies der dominierende Ethernet-Standard für 10 Mbit/s.
- **10Base5** (auch *Thicknet* oder *Yellow Cable*) - ein früher IEEE-Standard, der ein 10 mm-Koaxialkabel verwendete. Zum Anschluss von Geräten muss mittels einer Spezialklemme ein Loch in das Kabel gebohrt werden, durch das ein Kontakt des Transceivers geschoben und festgeklammert wird. An diesen Transreceiver wird mittels der AUI-Schnittstelle über ein Verbindungskabel die Netzwerkkarte des Computers angeschlossen. Dieser Standard bietet 10 Mbit/s Bandbreite bei Übertragung im Base-Band und 500 m Reichweite. Dieser Typ ist eigentlich obsolet, aber aufgrund seiner weiten Verbreitung in den frühen Tagen noch immer in einigen Systemen in Benutzung.

10 Mbit/s Ethernet mit Twisted-Pair-Kabel

- **StarLAN 10** - Die erste Ethernet-Implementation über Twisted-Pair-Kabel mit 10 Mbit/s, ebenfalls von AT&T. Wurde später zu 10Base-T weiterentwickelt.
- **10Base-T** - läuft über 4 Adern (2 Paare) eines Cat 3 oder Cat 5 Kabels. Ein Hub oder Switch sitzt in der Mitte und hat für jeden Teilnehmer einen Port. Diese Konfiguration wird auch für 100Base-T und Gigabit-Ethernet benutzt.
- **FOIRL** - Fiber-optic inter-repeater link. Der ursprüngliche Standard für Ethernet über Glasfaserkabel.
- **10Base-F** - Allgemeiner Ausdruck für die neue Familie von 10 Mbit/s Ethernet-Standards: 10Base-FL, 10Base-FB und 10Base-FP. Der einzig weiter verbreitete davon ist 10Base-FL.
- **10Base-FL** - Eine revidierte Version des FOIRL-Standards.
- **10Base-FB** - Gedacht für Backbones, die mehrere Hubs oder Switches verbinden. Ist inzwischen technisch überholt.
- **10Base-FP** - Ein passives sternförmiges Netzwerk, das keinen Repeater brauchte. Es gibt keine Implementationen.

Fast Ethernet

- **100Base-T** - Allgemeine Bezeichnung für die drei 100 Mbit/s-Ethernetstandards über Twisted-Pair-Kabel, 100Base-TX, 100Base-T4 und 100Base-T2.
- **100Base-TX** - Benutzt wie 10Base-T zwei Adernpaare, benötigt allerdings Cat 5 Kabel. Mit 100 Mbit/s ist 100Base-TX heute die Standard-Ethernet-Implementation.
- **100Base-T4** - 100 Mbit/s Ethernet über Category 3 Kabel (wie es in 10Base-T-Installationen genutzt wird). Nutzt alle vier Adernpaare des Kabels. Es ist inzwischen obsolet, da Category 5-Verkabelung inzwischen die Norm darstellt. Es ist darüber hinaus auf halbduplexe Übertragung begrenzt.

- **100Base-T2** - Es existieren keine Produkte. Bietet 100 Mbit/s Bandbreite über Cat 3-Kabel. Unterstützt den Full-Duplex-Modus und benutzt nur zwei Paare. Es ist damit funktionell äquivalent zu 100Base-TX, unterstützt aber alte Kabel.
- **100Base-FX** - 100 Mbit/s Ethernet über Glasfaser.

Gigabit Ethernet

- **1000Base-T** - 1 Gbit/s über Kupferkabel der Kategorie 5. Benutzt alle verfügbaren 4 Adernpaare.
- **1000Base-SX** - 1 Gbit/s über Glasfaser.
- **1000Base-LX** - 1 Gbit/s über Glasfaser. Optimiert für längere Distanzen unter Verwendung von Single-Mode-Fasern.
- **1000Base-CX** - Der Vorgänger von 1000Base-T mit einer maximalen Reichweite von 25 m.

10 Gigabit Ethernet
Der neue 10-Gigabit Ethernet-Standard bringt sieben unterschiedliche Medientypen für LAN, MAN und WAN mit sich. Der Standard heißt IEEE 802.3ae, ist aber noch nicht endgültig verabschiedet.

- **10GBase-SR** - entwickelt um kurze Strecken mit vorhandenen Multimode-Fasern zu überbrücken. Hat abhängig vom Kabeltyp eine Reichweite zwischen 26 und 82 m. Außerdem unterstützt es 300 m Reichweite über eine neue 2000 MHz/km Multimode-Faser.
- **10GBase-LX4** - nutzt Wavelength Division Multiplexing um Reichweiten zwischen 240 und 300 m über vorhandene Multimode-Fasern zu ermöglichen. Unterstützt außerdem 10 km über Single-Mode-Fasern.
- **10GBase-LR** und **10GBASE-ER** - diese Standards ermöglichen 10 bzw. 40 km über Single-Mode-Fasern.
- **10GBase-SW**, **10GBase-LW** and **10GBase-EW** - Diese Varianten benutzen einen zusätzlichen WAN PHY, um mit OC-192 / STM-64 SONET/SDH-Equipment zusammenarbeiten zu können. Der Physical Layer entspricht 10GBase-SR bzw. 10GBase-LR und 10GBase-ER, sie benutzen daher auch die gleichen Fasertypen und erreichen dieselben Reichweiten (zu 10GBase-LX4 gibt es keine entsprechende Variante mit WAN PHY).

10 Gigabit Ethernet ist noch sehr neu, welche Standards kommerziell erfolgreich werden, muss abgewartet werden.

Power over Ethernet
Ebenfalls zur Familie der Ethernet-Standards gehört IEEE 802.3af, der Verfahren beschreibt, mit denen sich Ethernet-fähige Geräte über die freien Adern eines Twisted-Pair-Kabels mit Energie versorgen lassen.

Verwandte Standards
Folgende Netzwerk-Standards gehören nicht zum IEEE 802.3 Ethernet-Standard, unterstützen aber das Ethernet-Frameformat und können mit Ethernet zusammenarbeiten:

- **Wireless LAN** (IEEE 802.11) - Drahtlose Vernetzung im Geschwindigkeitsbereich zwischen 2 und 54 Mbit/s.
- **100BaseVG** - Ein früher Konkurrent zu 100 Mbit/s Ethernet. Läuft über Category 3-Kabel, nutzt 4 Adernpaare und war ein kommerzieller Fehlschlag.
- **TIA 100Base-SX** - Von der Telecommunications Industry Association promoteter Standard. 100BASE-SX ist eine alternative Implementation von 100 Mbit/s Ethernet über Glasfaser; ist inkompatibel mit dem offiziellen 100Base-FX-Standard. Sein Haupt-Feature ist die mögliche Interoperabilität mit 10Base-FL, da es Autonegotiation zwischen 10 oder 100 Mbit/s beherrscht. Die offiziellen Standards können dies auf Grund unterschiedlicher Wellenlängen der verwendeten LEDs nicht. Zielgruppe sind Organisationen mit einer bereits installierten 10 Mbit/s Glasfaser-Basis.

- **TIA 1000Base-TX** - Stammt ebenfalls von der Telecommunications Industry Association. War ein kommerzieller Fehlschlag, und es existieren keine Produkte. 1000Base-TX benutzt ein einfacheres Protokoll als der offizielle 1000Base-T-Standard, benötigt aber Cat 6 Kabel.

Strukturierte Verkabelung

Bei einer „strukturierten Verkabelung" handelt es sich um eine Verkabelung, deren Struktur in der Europäischen Norm EN 50173 beschrieben ist und ihren Ursprung in der ISO 11801 hat. Dort wird erklärt, wie ein passives Netzwerk aufgebaut werden muss, um das Ziel der Anwendungsunabhängigkeit zu erreichen.
Es wird ein hierarchisches System von Verteilern beschrieben, die über so genannte Primär- und Sekundärkabel miteinander verbunden werden. Ein dritter Kabelbereich, die Tertiärverkabelung, verbindet die Teilnehmeranschlüsse mit den Verteilerstrukturen. Die Anzahl der Teilnehmeranschlüsse wird so festgelegt, dass eine spätere Nachverkabelung nicht mehr notwendig wird.
Mit dem Begriff der „strukturierten Verkabelung" sind Leistungsmerkmale verbunden, die die Nutzung eines beliebigen Datendienstes erlauben. Die übertragungstechnischen Eigenschaften aller Komponenten müssen bestimmten Anforderungen genügen, die in der EN 50173 aufgenommen worden sind.
Leider werden häufig Problemthemen wie Brandschutz, Sicherheit gegen aktive und passive Angriffe, elektromagnetische Verträglichkeit oder die eng mit der Verkabelung verbundenen Erdungs- und Massekonzepte ausgegrenzt.
Diese Bereiche kann man auf keinen Fall unbeachtet lassen. Der Begriff eines „modernen Netzwerkes" beinhaltet also eine strukturierte Verkabelung, die durch weitere Eigenschaften ergänzt werden muss.

Primärverkabelung

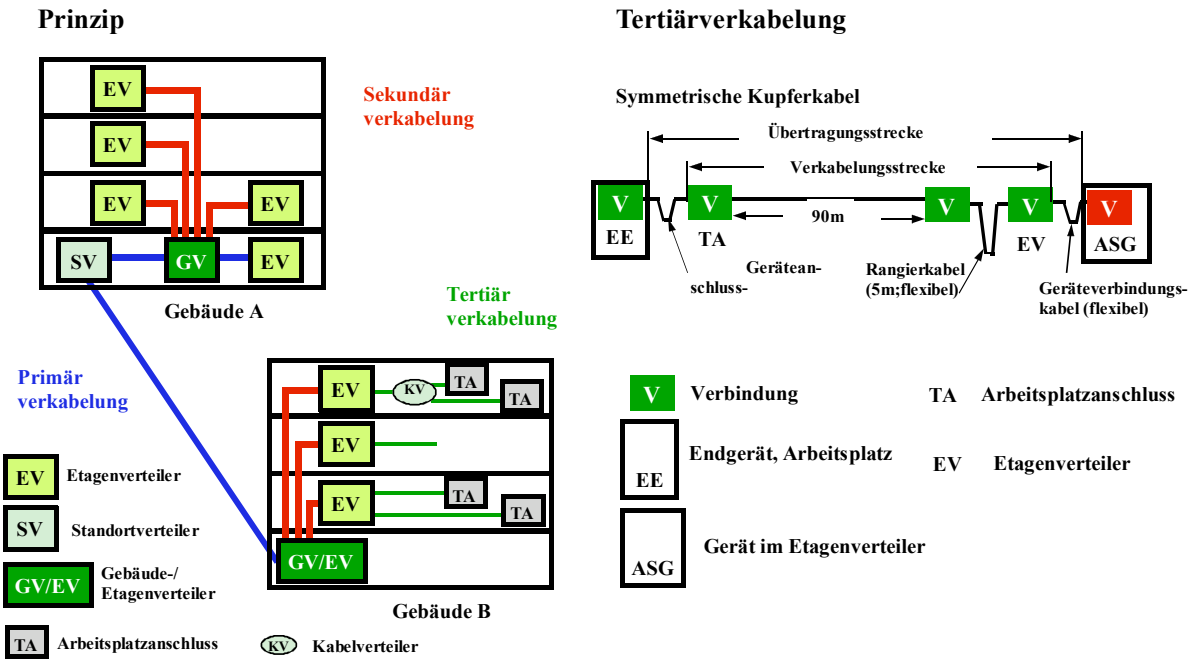
Gebäudeübergreifende, campusweite Standortverkabelung zur Verbindung der Standort- bzw. Gebäudeverteiler. Wird die Verbindung zwischen Standort und Etagenverteiler mit Multimodelichtwellenleitern realisiert, beträgt die maximale Entfernung 2.000 m. Der Einsatz von Monomodefasern ermöglicht zwar weitaus größere Reichweiten (bis 60 km), Längen mit mehr als 3.000 m zwischen Standort und Etagenverteiler liegen außerhalb des Anwendungsbereiches der EN 50173.

Sekundärverkabelung

Gebäudeinterne Verkabelung zur Verbindung der Etagenverteiler mit dem Gebäudeverteiler. Der Gebäudebackbone zwischen Gebäude- und Etagenverteiler darf 500 m nicht überschreiten.

Tertiärverkabelung

Etagen- bzw. Raumverkabelung zur Verbindung der Etagenverteiler mit den Anschlussdosen am Arbeitsplatz. Die Länge der Tertiärverkabelung darf, unabhängig von der Kabelart, 90 m Installationsstrecke nicht überschreiten. Das ist die Kabellänge vom mechanischen Anschluss des Kabels im Etagenverteiler bis zum Anschluss am Arbeitsplatz. Die maximale Länge von Patchkabeln im Etagenverteiler und Geräteanschlusskabel am Arbeitsplatz darf in Summe 10 m nicht überschreiten, wenn kein zusätzlicher Rangierverteiler vorhanden ist, sonst gilt eine Länge von 9 m.



Verkabelungsstrecken

Das Leistungsvermögen einer symmetrischen Übertragungsstrecke wird an und zwischen den Schnittstellen zu aktiven Geräten festgelegt. Die Verkabelung umfasst nur passive Abschnitte von Kabeln, Verbindungskomponenten, Geräteanschlusskabeln, Geräteverbindungskabeln und Rangierkabeln.

Klassifizierung der Verkabelungsstrecken

Die universelle Verkabelung umfasst mehrere Installations- und Übertragungsstrecken, die in fünf Klassen definiert werden:

- Klasse A bis 100 kHz
- Klasse B bis 1 MHz
- Klasse C bis 16 MHz
- Klasse D bis 100 MHz
- LWL-Klasse für die Unterstützung von Netzanwendungen oberhalb von 10 MHz

Folgende Parameter müssen bei der Festlegung der Übertragungsklassen beachtet werden:

- Nenn- Wellenwiderstand (Impedanz)
- Rückflussdämpfung (Return loss)
- Dämpfung
- Nahnebensprechdämpfung (NEXT)
- Dämpfungs- Nebensprechdämpfungsverhältnis (ACR)
- Fernnebensprechdämpfung (ELFEXT)
- Gleichstrom – Schleifenwiderstand
- Laufzeitunterschied
- Erdungsysmmetriedämpfung
- Kopplungswiderstand von Schirmen

Verkabelungsstrecken mit Lichtwellenleiter

Definiert wird das Leistungsvermögen einer Übertragungsstrecke mit Lichtwellenleitern mit der Annahme, dass nur eine einzige optische Wellenlänge in einem Übertragungsfenster verwendet wird. Normen für die Anwendung des Wellenlängen – Multiplexings sind noch nicht verfügbar.

Das Hauptkriterium einer Verkabelungsstrecke mit Lichtwellenleitern ist die Dämpfung. Die Dämpfung einer Übertragungsstrecke ist von der Netzanwendung abhängig.

Hierfür gelten folgende Werte:

Teilsystem	**Länge der Installationsstrecke in m**		**Dämpfung**	**in dB**	
		Einmoden		Mehrmoden	
		1.310 nm	1.550 nm	850 nm	1.300 nm
Tertiärverkabelung	90	2,2	2,2	2,5	2,2
Sekundärverkabelung	500	2,7	2,7	3,9	2,6
Primärverkabelung	1.500	3,6	3,6	7,4	3,6

Normergänzungen zu EN 50173 (IEC 61 873)

Kaum hat die EN 50173 im Netzwerkbereich Einzug gehalten, da deutete sich schon eine Ergänzung an. Der Grund hierfür liegt in der Entwicklungsgeschichte der EN 50173.
In der Norm werden passive Komponenten bis zu einer Frequenz von 100 MHz spezifiziert. Durch das Mitwirken vieler Firmen und Organisationen, die sich in vielen Fällen auf den kleinsten gemeinsamen Nenner geeinigt haben, ist vom Entwurf bis zur Veröffentlichung eine lange Zeit vergangen. Dieser Tatsache ist es zuzuschreiben, dass die EN 50173 in fast allen Teilbereichen nicht mehr den heutigen Möglichkeiten und Anforderungen entspricht.
Die in der aktuellen Norm festgeschriebenen Dämpfungs-, NEXT- und ACR – Werte sind so schlecht, dass damit ein Investitionsschutz von 10 bis 15 Jahren nur schwer zu realisieren ist.
Im neuen Normenentwurf werden zwei neue Netzanwendungsklassen definiert:
Zum einen wird eine **Klasse E** für Übertragungen bis zu 200 MHz (Messung bis 250 MHz) definiert, die die Verwendung von hochwertigen S/UTP bzw. S/STP-Kabeln mit entsprechenden Systemreserven erlaubt. Als Verbindungssystem soll das weit verbreitete RJ45-System verwendet werden.
Zum anderen wird eine **Klasse F** für einen Frequenzbereich bis 600 MHz definiert. Basis für diese Normerweiterung ist der deutsche Normenentwurf E DIN 44312-5. Die geforderten Übertragungswerte können nur noch mit hochwertigen S/STP-Kabeln (auch mittlerweile spezielle S/UTP-Kabel von ATßT) und neu entwickelte Steckervarianten erreicht werden.
Neben den neuen Klassen wird auch die Definition der Übertragungsstrecke neu festgelegt. Der Kabelverzweiger wird entfallen, dafür sollen die flexiblen Anschlussleitungen in eine zusätzliche Spezifikation mit aufgenommen werden.
Neben diesen Vorgaben wurden noch weitere Vorgaben in die neue Norm aufgenommen:
Die maximalen Laufzeiten bei hohen Frequenzen sowie die Laufzeitunterschiede zwischen den verschiedenen Paaren eines Kabels werden festgeschrieben.
Eine neue Meßmethode mit dem Namen Power SumNEXT wird in die Norm integriert. Bei der Messung werden Daten gleichzeitig über drei Adernpaare gesendet und beim vierten Adernpaar die eingekoppelte Störung gemessen.
Eine weitere Meßmethode sieht vor, dass das Nahnebensprechen auch am entfernten Ende bestimmt wird, da bei einer Full Duplex – Übertragung gleichzeitig gesendet und empfangen wird.

Digital Subscriber Line

Digital Subscriber Line (DSL) bezeichnet die digitale Teilnehmeranschlussleitung in öffentlichen Kommunikationsnetzen. Streng genommen vom physikalischen Medium unabhängig, bezeichnet DSL doch meist das Übertragungsverfahren über ein doppeladriges Kupferkabel.

Nach einer Bitkom-Studie vom Anfang Februar 2003 gibt es 3,2 Millionen DSL-Anschlüsse und 25 Millionen ISDN-Kanäle in Deutschland; jeder fünfte ISDN-Kanal der Welt liegt in Deutschland.

Beispiele

- ISDN - *Integrated Services Digital Network*, unterschieden in

    - *ISDN-Basisanschluss* mit 2 B-Kanälen (Nutzkanälen) zu je 64 kbit/s und einen D-Kanal (Signalisierkanal) mit 16 kbit/s
    - *ISDN-Primärmultiplexanschluss* mit 30 B-Kanälen und einem D-Kanal mit 64 kbit/s;

- ADSL - *Asymmetric Digital Subscriber Line*, eine asymmetrische Datenübertragungstechnologie mit Bitraten bis 8 Mbit/s zum Teilnehmer (*downstream*) und 1 Mbit/s in der Gegenrichtung (*upstream*);
- HDSL - *High Data Rate Digital Subscriber Line*, eine asymmetrische Datenübertragungstechnologie mit Datenraten zwischen 1,54 und 2,04 Mbps;
- SDSL - *Symmetrical Digital Subscriber Line*, eine symmetrische Datenübertragungstechnologie mit Bitraten von bis zu 2,3 Mbit/s symmetrisch;
- VDSL - *Very High Speed Digital Subscriber Line*, eine asymmetrische Datenübertragungstechnologie mit Bitraten von 12,9 bis 51,8 Mbps (*downstream*) bzw. 1,6 bis 2,3 Mbps (*upstream*);
- RADSL - *Rate Adaptive Digital Subscriber Line* eine asymmetrische Datenübertragungstechnologie mit Bitraten von 6MBit/s (*downstream*) bzw. 640 KBit/s (*upstream*).

xDSL bezeichnet eine der Varianten der DSL-Technologie wie ADSL, SDSL, HDSL oder VDSL.

Reichweite
xDSL ist aufgrund der physikalischen Eigenschaften der Leitung in der Reichweite begrenzt. Generell gilt: Je höher die Bitrate, umso geringer die Reichweite. Für alle xDSL-Varianten sind daher Modi definiert, mit denen durch Verringerung der Bitrate - teilweise sogar dynamisch adaptiv - die Reichweite erhöht werden kann.

Anwendungen
Während ISDN in erster Linie für die Telefonie mit zwei Amtsleitungen genutzt wird, ist ADSL die erste Technologie, die Netzbetreiber für den schnellen Internet-Zugang von Privatkunden installiert haben. SDSL ist für beide Bereiche geeignet und kommt hauptsächlich für Geschäftskunden zum Einsatz.

Die Tendenz geht dahin, mehrere Dienste über eine einzige Doppelader übertragen zu können – idealer weise das "Triple Play" aus Telefonie, Internet-Zugang und Video.

DSL-Hardware
Für den DSL-Zugang werden (sowohl auf Kunden- als auch auf Seite der Telefongesellschaft) folgende Hardwarebauteile benötigt:

- **DSL-Modem** oder **ATU-R** (**A**DSL **T**ransceiver **U**nit - **R**emote)
- **DSLAM** (**D**igital **S**ubscriber **L**ine **A**ccess **M**ultiplexer) oder **ATU-C** (**A**DSL **T**ransceiver **U**nit - **C**entral Office)
- **DSL-AC** (**D**igital **S**ubscriber **L**ine **A**ccess **C**oncentrator) oder auch **Breitband-PoP**

Dazu kann je nach technischer Realisierung weiteres Equipment wie ein RADIUS-Server für die Benutzeranmeldung, -Verwaltung und Billing (Verbrauchsdatenspeicherung zum Zwecke der Rechnungserstellung) oder Splitter zur Abtrennung von ISDN/POTS-Signalen benötigt werden. Im erweiterten Sinne gehört auch noch der PC/Router des Kunden zur DSL-Ausrüstung, weil dort die PPPoE-Strecke vom DSL-AC terminiert.

Schnittstellen und Spezifikationen

Schnittstellen und Spezifikationen für xDSL-Technologien (einschliesslich ISDN) sind beispielsweise:

- 1TR111 - Technische Beschreibung der digitalen Wählanschluesse ;
- 1TR236 - Spezifikation für die Schnittstelle S0 zwischen ISDN-Endeinrichtung und Netzabschluß des Basisanschluß (NTBA);
- 1TR237 - Spezifikationen der Schnittstelle S2M zwischen Endeinrichtungen und Netzabschluss beim Primärmultiplexanschluß im EURO-ISDN;
- 1TR6 - ISDN-D-Kanal-Protokoll (national, heute nicht mehr angeboten);
- 1TR67 - Nationale Festlegungen der Deutschen Telekom AG zum DSS 1-Protokoll;
- U-R2 - Ende 2001 von der Telekom definierte Schnittstelle für die Interoperabilität von ADSL-Endgeräten.

Protokolle

Protokolle für xDSL-Technologien sind beispielsweise:

- PPPoE (*PPP over Ethernet*) - Protokoll, das die Kapselung von PPP-Paketen in Ethernet-Frames regelt; PPPoE wird u.a. von der Telekom für T-DSL verwendet.
- PPPoA (*PPP over ATM*) - Protokoll, das die Kapselung von PPP-Paketen in ATM-Zellen regelt.

Internet Protocol (IP)

Internet Protokolle im TCP/IP-Protokollstapel

Anwendung	FTP	SMTP	HTTP	DNS	...
Transport	TCP			UDP	
Netzwerk	**IP** *(IPv4, IPv6)*				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Das Internet Protocol **(IP)** (auch *Internetprotokoll*) ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll. Es ist eine (bzw. *die*) Implementation der *Internet*-Schicht des TCP/IP-Modells bzw. der *Netzwerk*-Schicht des OSI-Modells. Es bildet damit die erste medium-unabhängige Schicht der Internet-Protokollfamilie. Im Gegensatz zu der physischen Adressierung der darunter liegenden Schicht, bietet IP *logische* Adressierung. Das bedeutet, dass mittels IP-Adressen und Subnetzmaske (*subnet masks*) Computer innerhalb des Netzwerkes in logische Einheiten, so genannten Subnetze, gruppiert werden können. Auf dieser Basis ist es möglich, Computer in größeren Netzwerken zu adressieren und Verbindungen zu ihnen aufzubauen, da logische Addressierung die Grundlage für Routing (Wegewahl und Weiterleitung von Netzwerk-Paketen) ist. IP stellt also die Grundlage des Internets dar.

IP-Adresse

IP-Adressen erlauben eine logische Adressierung von Computern in IP-Netzwerken (z.B. dem Internet). Ein Host besitzt dabei mindestens eine eindeutige IP-Adresse pro Netzwerkschnittstelle. IP-Adressen der IP Version 4 erscheinen normalerweise als Folgen von vier Zahlen, die durch einen Punkt getrennt werden, z.B. 192.168.0.34 oder 127.0.0.1.

Grundlagen

IP-Adressen werden in jedes IP-Paket in die Quell- und Zieladressfelder eingetragen. Jedes IP-Paket enthält damit sowohl die Adresse des Senders als auch die des Empfängers.

Aufbau

Die seit der Einführung der Version 4 des Internet Protocols überwiegend verwendeten IPv4-Adressen bestehen aus 32 Bits, also 4 Bytes. In der *dotted decimal notation* werden sie als 4 durch Punkte voneinander getrennte Dezimalzahlen geschrieben,
Beispiel: 141.14.128.16
Jede Zahl kann dabei Werte von 0 bis 255 annehmen. Die oben stehende Adresse entspricht der vorzeichenlosen 32-Bit Zahl $141*256^3+14*256^2+128*256+16=2.366.537.744$. Manchmal trifft man auch auf die hexadezimale Darstellung (8D0E8010). Ein Rechner sieht die Binärdarstellung $10001101000011101000000000010000_2$. Es sind maximal 2^{32}, also etwa 4.000.000.000 Adressen möglich.

Netzklassen

Ursprünglich wurden die IP-Adressen in Netzklassen von A bis C mit verschiedenen Netzmasken eingeteilt. Klasse D und E waren für spezielle Aufgaben vorgesehen. Aufgrund der immer größer werdenden Routing-Tabellen, wurde 1996 CIDR (*Classless Interdomain Routing*) eingeführt. Damit spielt es keine Rolle mehr, welcher Netzklasse eine IP-Adresse angehört.

Netzwerk- und Geräteteil

Jede 32-Bit IP-Adresse wird in einen Netzwerk- und einen Geräteteil (Hostteil) getrennt. Im Fall einer sogenannten B-Netzklasse (beim *classful routing*) geben die oberen (vorderen) 16 Bits den Netzwerkteil wieder, die hinteren 16 Bits den Geräteteil. Die Adresse kann beim „*classless routing*" auch 141.14.128.16/16 geschrieben werden.
Der Netzwerkteil, im oben stehenden Beispiel 141.14.0.0, muss dann für alle Geräte im Netzwerk gleich sein. Der Geräteteil wird für jedes Gerät und jede Schnittstelle (Netzwerkkarte) individuell vergeben. Im 16/16 Bit-Fall sind dann noch 2^{16}=65.536 Geräte möglich. Die Nummer 0 wird nicht vergeben, sie bezeichnet das Netzwerk selbst. Als Konvention wird die höchste Geräteadresse für Nachrichten an alle Geräte (Broadcasts) verwendet, die maximale Gerätezahl reduziert sich also um zwei auf 65.534. Die erste Adresse ist 141.14.0.1, die letzte 141.14.255.254 und die Broadcast-Adresse 141.14.255.255.
Statt der 16/16-Bit Aufteilung ist beim „*classless routing*" auch jede andere Aufteilung möglich. Verbreitet ist durch die frühere Einteilung in Netzklassen die Verwendung von 24-Bit Netzwerkteil und 8 Bit Hostteil, z. B. 192.168.42.3/24. Hier ist der Netzwerkteil 192.168.42.0, die Geräteadresse ist 3. Jedes Geräte (bzw. Schnittstelle) verwendet eine Adresse der Form 192.168.42.x, wobei Geräteadressen von 1 bis 254 möglich sind. Die Adresse 192.168.42.255 wird für Broadcasts verwendet.

Netzmasken

Statt der Darstellung 192.168.42.3/24 verwendete man früher beim „*classful routing*" die Kombination der IP-Adresse und Netzmaske. Dies ist auch bei der Konfiguration von Schnittstellen noch üblich. Die Netzmaske ist dabei die 32-Bit-Darstellung, bei der alle Bits des Netzwerkteils auf 1 und alle Bits des Geräteteils auf 0 gesetzt sind. Bei .../16 ist die Netzmaske daher 11111111 11111111 00000000 000000000, also 255.255.0.0.

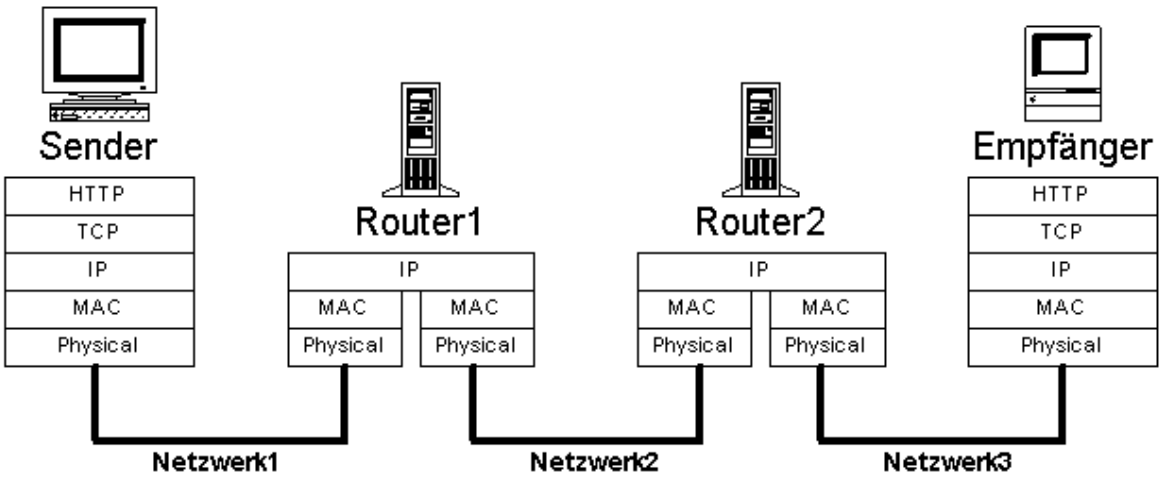
IP-Adresse/Netzwerk	Adresse	Netzmaske	Adressen im Netzwerk	Broadcast
10.0.0.44/8	10.0.0.44	255.0.0.0	10.0.0.1 bis 10.255.255.254	10.255.255.255
134.60.1.111/16	134.60.1.111	255.255.0.0	134.60.0.1 bis 134.60.255.254	134.60.255.255
192.168.0.1/24	192.168.0.1	255.255.255.0	192.168.0.1 bis 192.168.0.254	192.168.0.255
192.168.10.23/32	192.168.10.23	255.255.255.255	192.168.10.23	-
0.0.0.0/0	-	0.0.0.0	alle	-

Beispiele für Adressen, Netzwerke und Netzmasken

IP-Adressen, Netzwerkteil und Routing

Will ein Gerät ein IP-Paket versenden, werden die Netzwerkteile der Quell-IP-Adresse und Ziel-IP-Adresse verglichen. Stimmen sie überein (d.h. Ziel und Quelle sind am gleichen Netzwerk

angeschlossen), wird das Paket direkt an den Empfänger gesendet. Im Falle von Ethernet-Netzwerken dient das ARP-Protokoll zum Auffinden der Hardwareadresse (MAC-Adresse).
Stimmen die Netzwerkteile dagegen nicht überein, so wird über eine Routingtabelle die IP-Adresse für das nächste *„gateway"* gesucht und das Paket auf dem lokalen Netzwerk dann an dieses Gerät gesendet. Es hat über mehrere Schnittstellen Zugriff auf andere Netzwerke und *routet* das Paket ins nächste Netzwerk (Router). Dazu konsultiert der Router seinerseits seine eigene Routingtabelle und sendet das Paket gegebenfalls an den nächsten Router oder an das Ziel. Bis zum Endgerät kann das Paket viele Netzwerke und Router durchlaufen. Das Durchlaufen eines Routers wird auch *Hop* (Sprung) genannt.



Routing einer HTTP/TCP Verbindung über drei Netzwerke

Ein Router hat dabei für jede seiner Schnittstellen eine eigene IP-Adresse und Netzmaske, die zum jeweiligen Netzwerk gehört. Jedes IP-Paket wird einzeln geroutet. Die Quell- und Zieladresse im IP-Header werden vom Sender gesetzt und bleiben während des gesamten Wegs unverändert.

Spezielle IP-Adressen
Das Netz 127.0.0.1/8 bezeichnet immer den lokalen Computer (*loopback address*). Es dient dazu, dass Client und Server-Prozesse am selben Computer miteinander kommunizieren können.
Die spezielle Adresse 255.255.255.255 kann neben der höchsten Geräteadresse im Netz ebenfalls als Broadcastadresse verwendet werden. Dadurch ist das Versenden von Broadcasts ohne Kenntnis weitere Netzwerkparameter möglich. Dies ist für Protokolle wie BOOTP und DHCP wichtig.
Der Adressbereich 224.0.0.0/4 (Adressen 224.0.0.0 bis 239.255.255.255) ist für Multicast-Adressen reserviert. Damit gibt es drei IP-Adress-Typen:

- Unicast - Senden an einen bestimmten Empfänger im Internet (normale Adressierung)
- Broadcast - Senden an alle Geräte im selben Netzwerk (Subnetz)
- Multicast - Senden an einige Geräte im selben Netzwerk (oder Geräte im MBone-Netzwerk)

Die RFC 3330 gibt Auskunft über die derzeit definierten speziellen IP-Adressen.

DNS - Übersetzung von Rechnernamen in IP-Adressen
Über das weltweit verfügbare Domain Name System DNS können Namen in IP-Adressen (und umgekehrt) verwandelt werden. Der Name *www.fhi-berlin.mpg.de* ergibt zum Beispiel 141.14.141.241.

IPv6 - neue Version mit größerem Adressraum
Die aktuelle IP Version (IPv4) stellt über 4 Milliarden eindeutige Adressen bereit. Große Bereiche des Adressraumes sind durch das „classful routing" stark fragmentiert. Auch sind einige Bereiche des gesamten IP Adressraums für besondere Anwendungen reserviert sind (z.B. private Netze). Dadurch stehen weniger Adressen zur Verfügung, als theoretisch möglich sind.

In Zukunft werden immer mehr Geräte (z.B. Telefone, Organizer, Haushaltsgeräte) vernetzt, so dass der Bedarf an eindeutigen IP-Adressen ständig zunimmt. Für eine Erweiterung des möglichen

Adressraumes wurde IPv6 entwickelt. Es verwendet 128-Bit Adressen, so dass auch in weitere Zukunft keine Adressraumprobleme bei Verwendung von IPv6 auftreten können (mit 128-Bit Adressen lässt sich theoretisch jedes Atom der Erde adressieren).
Neben den größeren Adressen bietet IPv6 noch weitere interessante Neuerungen:

- Autokonfiguration (ähnlich DHCP), Mobile IP und automatisches Renumbering
- Services wie IPsec, QoS und Multicast serienmäßig
- Vereinfachung und Verbesserung der Header (wichtig für Router)

Vergabe von IP-Adressen und Netzbereichen

IANA - Internet Assigned Numbers Authority
Die Vergabe von IP-Netzen im Internet wird von der IANA geregelt. Die daraus verfügbaren IP-Adressen werden ggf. vom Administrator in Subnetze unterteilt und an die Computer vergeben. Die Subnetze selber sind untereinander mit Routern verbunden. Die IANA vergibt Adressbereiche an Organisationen wie größere Firmen oder Universitäten. Beispielsweise wurde der Bereich 13.0.0.0/8 der Xerox Corporation zugeteilt. Die Organisationen können *ihre* Adressen dann den Geräten in ihrem Netzwerk frei zuweisen.
Firmen wie die Deutsche Telekom unterteilen den ihnen zugewiesenen Adressbereich weiter und teilen ihren Kunden Adressen im Rahmen ihrer Dienste zu. Sie sind damit so genannte Internet Provider. Kunden können dann entweder Endkunden oder weitere (Sub-)Provider sein. Die Adressen können dabei entweder permanent zugewiesen werden oder über eine Einwahlmöglichkeit dynamisch zugeteilt werden. Bei permanenten Adressen kann das Internet die Funktion einer Standleitung übernehmen. Auch Server-Dienste können dann angeboten werden. Bei privaten Kunden ist die dynamische Zuteilung üblich.

Private Netze
Für private Netzwerke kann man die Adressen selbst zuteilen. Dafür sollte man die Adressen aus den Bereichen für private Netze verwenden (z. B. 192.168.1.1, 192.168.1.2 ...). Diese Adressen werden von der IANA nicht weiter vergeben und im Internet nicht geroutet. Eine Verbindung aller Rechner im privaten Netzwerk mit Rechnern im Internet - auch in anderen privaten Netzen - ist über NAT (Network Address Translation) trotzdem möglich.

Gerätekonfiguration

Manuelle Konfiguration
Für Benutzer oder Administratoren gibt es Programme, um die IP-Adresse anzuzeigen und zu konfigurieren. Unter Dos oder Windows steht im Kommandomode *ipconfig* und unter Unix *ifconfig* zur Verfügung. Bei manueller Konfiguration wird in der Regel die individuelle Adresse, die Netzmaske und ein Gatewayrechner über den Befehl *route* eingetragen.

Automatische Konfiguration über Server
Über Protokolle wie BOOTP oder DHCP können IP-Adressen beim Hochfahren des Rechners über einen entsprechenden Server zugewiesen werden. Auf dem Server wird dazu vom Administrator ein Bereich von IP-Adressen definiert, aus dem sich weitere Rechner beim Hochfahren eine Adresse entnehmen können. Diese Adresse wird an den Rechner *geleast*. Rechner, die feste Adressen benötigen, können im Ethernet-Netzwerk über ihre MAC-Adresse identifiziert werden und eine dauerhafte Adresse erhalten.
Vorteil hierbei ist die zentrale Verwaltung der Adressen. Ist nach der Installation des Betriebssystems die automatische Konfiguration vorgesehen, müssen keine weiteren Einstellungen für den Netzwerkzugriff mehr vorgenommen werden. Mobile Geräte wie Laptops können sich Adressen teilen, wenn nicht alle Geräte gleichzeitig ans Netz angeschlossen werden. Daneben können sie ohne Änderung der Konfiguration bei Bedarf in verschiedene Netzwerke (z. B. Firma, Kundennetzwerk, Heimnetz) integriert werden.

Dynamische Addressierung

Insbesondere Internet Service Provider, die Internet-Zugänge über Wählleitungen anbieten, nutzen die dynamische Adressierung via PPP oder PPPoE, da sie so mit weniger für sie kostenpflichtigen IP-Adressen auskommen. Es werden so viele Adressen bereitgestellt, wie Einwahlleitungen verfügbar sind. Erwischt ein Kunde keine freie Leitung, benötigt er auch keine IP-Adresse (AOL verwendet beispielsweise zur Berechnung der Anschlusskapazität einen Schlüssel von einer Leitung je 15 Kunden). Durch zeitlich versetzte Nutzung der Kapazitäten können sich mehrere Kunden eine IP-Adresse teilen. Somit bekommt das Endgerät (Arbeitsplatz-Rechner) bei jeder Einwahl ins Internet eine andere, momentan freie Adresse. Als Nebeneffekt ist der Rechner weniger anfällig gegen *gezielte* Angriffe aus dem Netzwerk. *Nicht geschützt* ist der Rechner jedoch gegen Denial of Service-Angriffe, die nur kurzfristig zum Zeitpunkt der Attacke die IP-Adresse des Zielrechners benötigen.

Statische Adressierung
Größere Firmen haben meist eine eigene Standleitung zum Internet und verwenden einen fest zugewiesenen Adressbereich (**statische Adressierung**). Bei der Nutzung von Gateways wird der Datenaustausch zwischen den Netzen entweder von dedizierten Rechnern (Proxies) stellvertretend für den anfragenden Arbeitsplatz übernommen oder durch NAT eine Adressumsetzung zwischen interner IP-Adresse und Gateway-IP-Adresse vorgenommen. Dadurch ist es möglich, dass mehrere Endgeräte gleichzeitig dieselbe (Gateway-)IP-Adresse verwenden.

Sonstiges

IP Aliasing - Mehrere Adressen auf einer Netzwerkkarte
Normalerweise wird jedem Rechner eine IP-Adresse für jede Schnittstelle (Netzwerkkarte etc.) zugewiesen. Ein normaler Rechner mit einer Schnittstelle hat damit genau eine IP-Adresse. Router mit mehreren Schnittstellen haben entsprechend mehrere IP-Adressen, für jede Schnittstelle eine. Dies ist jedoch nicht zwingend. Moderne Implementierungen erlauben die Zuordnung von mehreren IP-Adressen zu einer Schnittstelle, so genanntes IP-Aliasing.
Dies wird verwendet, wenn ein Serverrechner verschiedene Services anbietet. Jedem Service wird dann eine eigene IP-Adresse zugewiesen. Der Service wird damit Rechner-unabhängig. Falls ein anderer Rechner den Service anbieten soll, kann die IP-Adresse einfach auf die Schnittstelle im neuen Rechner übernommen werden. Der Umzug ist damit für die Clients nicht sichtbar.

Unterschiedliche Netzwerke auf einem physikalischen Netzwerk
Auf einem physikalischen Netzwerk (z. B. Ethernet-Netzwerk) können unterschiedliche logische Netzwerke (mit unterschiedlichem Netzwerk-Adressteil) aufgesetzt werden und gleichzeitig verwendet werden. Dies wird unter anderem eingesetzt, wenn später das Netzwerk wirklich aufgeteilt werden soll.

Transmission Conrol Protocol (TCP)

TCP im TCP/IP-Protokollstapel

Anwendung	FTP	SMTP	http	...
Transport	**TCP**			
Netzwerk	IP			
Netzzugang	Ethernet	Token Ring	FDDI	...

Das *Transmission Control Protocol* (**TCP**) ist ein zuverlässiges, verbindungsorientiertes Netzwerkprotokoll. Es ist Teil der TCP/IP-Protokollfamilie.

TCP stellt einen virtuellen Kanal zwischen zwei Rechnern (genauer: Endpunkten) her. Auf diesem Kanal kann in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP-Protokoll auf. Es ist in Schicht 4 des OSI-Netzwerkschichenmodells angesiedelt.

Verbindungsauf- und -abbau

Ein Endpunkt stellt eine Rechneradresse gemeinsam mit einem so genannten Port dar. Ports sind 16-bit Zahlen und reichen von 1 bis 65535. Ports unterhalb von 1024 sind für Standard-Anwendungen reserviert (englisch: *well known ports*) und werden von der IANA vergeben, z. B. ist Port 25 für das SMTP Protokoll für elektronische Post reserviert.

Ein Server-Rechner, der einen Dienst wie beispielsweise elektronische Post anbietet, generiert normalerweise einen Endpunkt mit dem Port und seiner Adresse. Dies wird als *„passive open"* bezeichnet.

Will ein Client eine Verbindung aufbauen, generiert er einen eigenen Endpunkt aus seiner Rechneradresse und einer noch freien Portnummer. Mit Hilfe eines ihm bekannten Ports und der Adresse des Servers kann dann eine Verbindung aufgebaut werden. Für den Aufbau der Verbindung sind drei Pakete erforderlich (3- Wege-*Handshake*).

Während der Datenübertragungsphase (*„active open"*) sind die Rollen von Client und Server (aus **TCP**-Sicht) vollkommen symmetrisch. Insbesondere kann jeder der beiden beteiligten Rechner einen Verbindungsabbau einleiten. Während des Abbaus kann die Gegenseite noch Daten übertragen, die Verbindung kann also *halb*-offen sein. Ein 4-Wege-*Handshake* wird benutzt, um die Verbindung abzubauen.

Datenintegrität und Zuverlässigkeit

Im Gegensatz zum paketorientieren UDP implementiert **TCP** einen bidirektionalen, byte-orientierten, zuverlässigen Datenstrom zwischen zwei Endpunkten. Das darunter liegende Protokoll (meist IP) ist paketorientiert, wobei Datenpakete verloren gehen können, in verkehrter Reihenfolge ankommen dürfen und sogar doppelt empfangen werden können. TCP prüft die Integrität der Daten mittels einer Prüfsumme. Der Sender wiederholt das Senden von Paketen falls keine Bestätigung innerhalb einer bestimmten Zeitspanne eintrifft. Die Daten der Pakete werden im Empfänger in einem Puffer zu einem Datenstrom zusammengefügt und doppelte Pakete verworfen.

Bestätigungen

Die jeweilige Länge des Puffers, bis zu der keine Lücke im Datenstrom existiert, wird bestätigt (*„Windowing"*). Dadurch ist die Ausnutzung der Netzwerk-Bandbreite auch bei großen Strecken möglich. Bei einer Übersee- oder Satellitenverbindung dauert das Eintreffen des ersten *„Acknowledges"* (ACK) aus technischen Gründen mehrere 100 ms, in dieser Zeit können unter Umständen mehrere hundert Pakete gesendet werden. Der Sender kann den Empfängerpuffer füllen bevor die erste Bestätigung eintrifft. Alle Pakete im Puffer können gemeinsam bestätigt werden. Bestätigungen werden zusätzlich zu den Daten in die Paket-Header im entgegengesetzen Datenstrom eingefügt (*„Piggybacking"*).

Weitere Protokolleigenschaften

Über ein Dringlichkeitsbit (*„Urgent"*) können Daten als vorrangig gekennzeichnet werden. Dadurch ist beispielsweise die bevorzugte Behandlung von CTRL-C (Abbruch) bei einer Terminalverbindung (TELNET) möglich.

Um Bandbreite zu sparen, wird auf der TCP Ebene meistens der Nagle-Algorithmus eingesetzt, der zu kleine Pakete verhindern soll.

Problematik der Datenwiederholung

Die Wiederholung von Daten für die noch keine Bestätigung empfangen wurde, ist nicht unproblematisch. Im Internet, in dem viele Netzwerke mit unterschiedlichen Eigenschaften verbunden werden, ist Datenverlust einzelner Pakete durchaus normal. Die Verlustrate nimmt zu, falls bestimmte Netzwerke innerhalb der Verbindung an ihre Auslastungsgrenze kommen. Eine naive Implementierung von TCP/IP würde die verlorenen Pakete einfach wiederholen, was zu noch größerer Auslastung führen würde und unter Umständen zum Zusammenbruch des Neztwerks führen könnte. TCP/IP Implementierungen verwenden daher Algorithmen, die dies verhindern. Normalerweise wird langsam gestartet („*Slow Start*“) und die Senderate dann bis zum Datenverlust erhöht. Jeder Datenverlust verringert die Senderate, insgesamt nähert sich die Datenrate dem jeweiligen zur Verfügung stehenden Maximum.

Protokolle, die in der Regel auf TCP aufsetzen

HTTP, HTTPS, FTP, Telnet, SSL, SSH, SMTP, NNTP, UUCP, POP3, IMAP4, SMB, rsync, DNS, RSH, Gopher, finger, auth, IRC

User Datagram Protocol (UDP)

UDP im TCP/IP-Protokollstapel

Anwendung	DNS	DHCP	NTP	...
Transport	**UDP**			
Netzwerk	IP			
Netzzugang	Ethernet	Token Ring	FDDI	...

Das *User Datagram Protocol* (**UDP**) ist ein nicht zuverlässiges, verbindungsloses Protokoll. Es gehört zur Transportschicht der TCP/IP-Protokollfamilie.

Header Format

0	8	16	24	32
Quell-Port		Ziel-Port		
Länge		Prüfsumme		
Daten				

Der UDP Header besteht aus 4 Header Feldern, von denen zwei optional sind. Die Quell- und Ziel-Port Felder sind 16 Bit groß und identifizieren den sendenden und empfangenden Prozess. Da UDP verbindungslos ist, ist der Quell Port optional. Er wird dann „*0*“ gesetzt. Den Port Feldern folgt das verbindliche Längen Feld, das die Größe der Daten des UDP-Datagramms in Oktetten enthält. Der kleinstmögliche Wert ist 8 Oktette. Das letzte Header Feld ist eine 16 Bit große Prüfsumme über den Header und die Daten. Die Prüfsumme ist auch optional, wird aber in der Praxis fast immer benutzt (falls nicht, wird sie ebenfalls „*0*“ gesetzt). Dem Header folgen anschließend die Daten.

Eigenschaften

Verbindungslos heißt, es wird nicht erst eine Verbindung zum Gegenüber aufgebaut (*Handshaking* wie bei TCP) sondern man schickt "auf gut Glück" eine Anfrage. Es ist also nicht garantiert, dass das Paket überhaupt ankommt.

Aufgrund dieser Tatsache können zwischen zwei Hosts relativ schnell Datenpakete ausgetauscht werden. Es wird deshalb dort eingesetzt, wo die schnelle Übermittlung wichtiger ist, als die **Zuverlässigkeit**, also die Gewissheit, dass die Daten korrekt und vollständig angekommen sind. In der Praxis sind das Übertragungen von Multimedia oder bei Online-Spielen. Auch ein sehr wichtiger Dienst im Internet, das Domain Name System, setzt auf UDP auf.

Zeitlicher Versatz der Pakete (engl. jitter) kann bei UDP nicht erkannt werden.

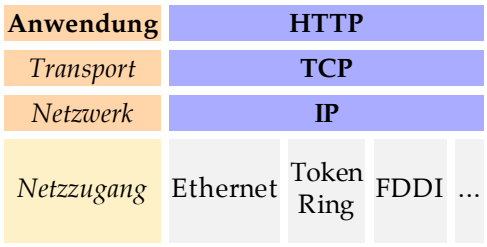
Protokolle, die auf UDP aufsetzen
UDP wird unter anderem von folgenden Protokollen verwendet:

DNS, NFS, TFTP, SNMP

UDP selber verwendet meistens das IP-Protokoll.

Hypertext Transfer Protocol (HTTP) auf TCP aufbauend

HTTP im TCP/IP-Protokollstapel



Das **Hypertext Transfer Protocol** (HTTP) ist ein zustandsloses Protokoll in der Anwendungsschicht. Es dient zur Übertragung von Hypermedia-Informationen. Durch Erweiterung seiner Anfragemethoden, Headerinformationen und Fehlercodes ist es nicht auf Hypertext beschränkt. Es wird von Web-Browsern verwendet um auf Web-Server zuzugreifen.

Das Protokoll wurde 1989 von Tim Berners-Lee am CERN zusammen mit dem URL und HTML erfunden; das World Wide Web (WWW) wurde geboren.

HTTP ist ein Kommunikationsschema, um Webseiten (oder Bilder oder prinzipiell jede andere beliebige Datei) von einem entfernten Computer auf den eigenen zu übertragen. Wenn auf einer Webseite der Link *www.example.net:80/infotext.html* angeklickt wird, so wird an den Computer mit dem Namen *www.example.net* die Anfrage gerichtet, die Datei *infotext.html* zurückzusenden. Der Name *www.example.net* wird dabei zuerst über das DNS-Protokoll in eine Adresse umgesetzt. Zur Übertragung wird über das TCP-Protokoll auf Port 80 eine HTTP-GET Anforderung gesendet. Zusätzliche Informationen wie Angaben über den Browser, gewünschte Sprache etc. können über einen Header in jeder HTTP-Kommunikation übertragen werden.

Der Computer, der diesen Web-Server (an Port 80) betreibt, sendet dann seinerseits eine HTTP-Antwort zurück. Diese besteht aus Headerinformationen des Servers, einer Leerzeile und dem Inhalt der Datei *infotext.html*. Die Datei ist normalerweise im Hypertext-Format HTML, das vom Browser in eine lesbare und ansprechende Darstellung gebracht wird. Es kann jedoch jede andere Datei in jedem beliebigen Format sein, zum Beispiel Bildinformationen, Audio- und Videodateien.

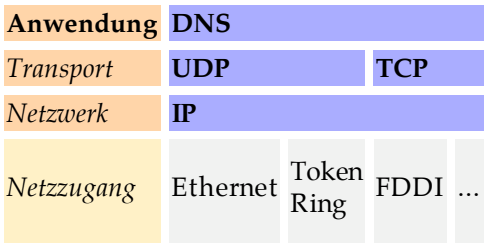
Die Information kann auch dynamisch generiert werden und braucht auf dem Server nicht als Datei abgelegt sein. Der Server sendet eine Fehlermeldung zurück, wenn die Information aus irgendeinem Grund nicht gesendet werden kann. Der genaue Ablauf dieses Vorgangs (Anfrage und Antwort) ist in der HTTP-Spezifikation festgelegt.

Vor jeder HTTP-Anfrage wird eine neue TCP-Verbindung aufgebaut, nach Übertragung der Antwort wieder geschlossen. Enthält eine HTML-Datei Verweise auf zehn Bilder, so werden insgesamt elf TCP-Verbindungen benötigt, um die Seite auf einem grafikfähigen Browser aufzubauen. Informationen aus früheren Anforderungen gehen verloren (zustandsloses Protokoll). Über „*Cookies*" in den Headerinformationen können aber Anwendungen realisiert werden, die Statusinformationen (Benutzereinträge, Warenkörbe) zuordnen können. Dadurch können Anwendungen die Status- bzw. Sitzungseigenschaften erfordern, realisiert werden. Auch eine Benutzerauthentifizierung ist möglich.

Normalerweise kann die Information, die über HTTP übertragen wird, auf allen Rechnern und Routern, die im Netzwerk durchlaufen werden, gelesen werden. Über HTTPS kann die Übertragung verschlüsselt erfolgen.
Die neueste Version von HTTP ist 1.1, sie erlaubt dem Browser viele einzelne Daten auf einmal zu übertragen (Geschwindigkeitsvorteil), abgebrochene Downloads fortzusetzen usw.

Domain Name System (DNS) auf UDP und TCP **aufbauend**

DNS im TCP/IP-Protokollstapel



Das **Domain Name System** (DNS) ist einer der wichtigsten Dienste im Internet. Das DNS ist eine verteilte Datenbank, die den Namensraum im Internet verwaltet. Das geschieht im Wesentlichen durch die Umsetzung von Namen in Adressen. Das Ganze ist vergleichbar mit einem Telefonbuch, das die Namen der Teilnehmer in ihre Telefonnummer auflöst. Das DNS ist notwendig, weil Menschen sich Namen weitaus einfacher merken können als Zahlenkolonnen. So kann man sich den Namen *www.tfh-berlin.de* sehr einfach merken, die dazugehörende IP-Adresse *164.64.226.10* dagegen nicht ganz so einfach.

Das DNS wurde 1983 von Paul Mockapetris entworfen und im RFC 882 beschrieben. Der RFC 882 wurde inzwischen von den RFCs 1034 und 1035 abgelöst.
Das DNS löste die *hosts*-Dateien ab, die nun nur noch für die statische Namensauflösung zuständig sind.
Das DNS zeichnet sich aus durch

- dezentrale Verwaltung
- hierarchische Strukturierung des Namensraums in Baumform
- Eindeutigkeit der Namen
- Erweiterbarkeit

Komponenten des DNS
Das DNS besteht aus drei Hauptkomponenten

- Domänennamensraum und den Resource Records (RR)
- Nameservern
- Resolver

Domänennamensraum
Der Domänennamensraum hat eine baumförmige Struktur. Die Blätter und Knoten des Baumes werden als **Labels** bezeichnet. Ein kompletter Domänenname eines Objektes besteht aus der Verkettung aller Labels.

Label sind Zeichenketten (alphanumerisch, als einziges Sonderzeichen ist das '-' erlaubt) die mindestens ein Zeichen und maximal 63 Zeichen lang sind. Die einzelnen Label werden durch Punkte voneinander getrennt. Ein Domänenname wird mit einem Punkt abgeschlossen (Der hinterste Punkt wird normalerweise weg gelassen, gehört rein formal aber zu einem vollständigen Domänennamen dazu).
Ein korrekter, vollständiger Domänenname lautet z. B. *www.fhi-berlin.mpg.de.* (der Punkt gehört zum Domänennamen).
Ein Domänenname darf inklusive aller Punkte maximal 255 Zeichen lang sein.
Ein Domänenname wird immer von rechts nach links delegiert und aufgelöst, d.h. je weiter rechts ein Label steht, umso höher steht es im Baum. Der Punkt ganz rechts wird auch als *„root"* (Wurzel) im Namensraum bezeichnet.
Das erste Label (das, das ganz rechts steht) wird im Allgemeinen auch als Top Level Domain (TLD) bezeichnet.

Resource Records (RR)
Daten, die ein Objekt im DNS beschreiben, werden als Satz von Resource Records dargestellt. Alle Resource Records eines Objektes werden als **Zone** bezeichnet.

Ein Resource Record ist immer folgendermaßen aufgebaut:

<name> [<ttl>] [<class>] <type> <rdata>

- **<name>** Der Domänenname des Objekts zu dem der Resource Record gehört
- **<ttl>** *time to live* Gültigkeit des Resource Records (in Sekunden)
- **<class>** Protokollgruppe zu der der Resource Record gehört. Üblicherweise wird **IN** (Internet) verwendet. Es sind aber auch die Klassen **CH** (Chaosnet) oder **HS** (Hesiod) sowie **CS** (CSNET, wird nicht mehr verwendet und wird lediglich noch als Beispiel in einigen obsoleten RFCs genannt) möglich.
- **<type>** beschreibt den Typ des Resource Records. Im DNS mögliche Typen sind:

  A IP-Adresse eines Hosts
  CNAME Alias name für einen Host
  HINFO Host information
  MB Mailbox domain name (*Experimentell*)
  MD Mail destination (nicht mehr in Gebrauch - heutzutage wird MX verwendet)
  MF Mail forwarder (nicht mehr in Gebrauch - heutzutage wird MX verwendet)
  MG Mail group member (*Experimentell*)
  MINFO Mailbox oder *mail list information*
  MR Mail rename domain name (*Experimentell*)
  MX Mail Exchange
  NULL Null Resource Record (*Experimentell*)
  NS Hostname eines autoritativen Nameservers
  PTR Domain Name Pointer (für das Reversemapping um IP Adressen Namen zuzuweisen)
  SOA Start of Authority
  TXT Text
  WKS *Well known service description*

- **<rdata>** (resource data) Daten die den Resource Record näher beschreiben (z.B. eine IP Adresse für einen A-RR, oder einen Hostnamen für einen NS-RR)

Nameserver
Nameserver sind Programme die einen oder mehrere Teile des Namensraumes autoritativ kennen, und diese auf Anfrage weitergeben. Nameserver werden von der höheren Ebene im Baum delegiert und sind dann für den Teilnamensraum unterhalb der delegierten Ebene zuständig (und können u.U. weitere Teilnamensräume unterhalb dieser Ebene delegieren). Die Baumstruktur stellt die eindeutige Zuordnung eines Nameservers zu einem Teil des Namensraum sicher.

Normale Anfragen werden auf Port 53 UDP beantwortet. Transfers kompletter Zonen werden auf Port 53 TCP durchgeführt.

Früher sprach man von *primary* und *secondary* Nameserver, heute spricht man von **autoritativen** Nameservern. Ein autoritativer Nameserver ist ein Nameserver, der gesicherte Informationen über eine Zone hat. Dem gegenüber steht ein **nicht-autoritativer** Nameserver der Informationen über eine Zone sozusagen aus zweiter oder dritter Hand hat, also nicht sicher sagen kann, dass die Information korrekt ist (da sie sich z.B. schon geändert haben kann).
Nameserver können auch als **caching Nameserver** agieren. Dabei speichern sie die einmal von einem Resolver angefragten Informationen zwischen, damit diese bei einer erneuten Anfrage schneller vorliegt. Dies ist meistens sinnvoll, da sich die Informationen im DNS nicht sehr schnell ändern. Die Daten im Cache des Nameservers verfallen nach der TTL (*time to live*). Das kann u.U. aber auch bedeuten, dass der Nameserver in dieser Zeit falsche Informationen liefern kann, wenn sich die Daten zwischenzeitlich geändert haben.
Damit ein Nameserver Informationen über andere Teile des Namensraumes finden kann, werden ihm Informationen über die sog. Root-Server in Form einer statischen Datei hinterlegt. Diese Datei enthält die Namen und IP Adressen der Root-Server. Derzeit gibt es 13 Root-Server (Server A bis M).

Nameserversoftware

- BIND (Berkeley Internet Name Domain) ist der Ur-Nameserver und heute noch die meistgenutzte Nameserversoftware. BIND ist Open Source Software.
- djbdns (entwickelt von Dan Bernstein) gilt als sehr sicher und erfreut sich steigender Beliebtheit.
- PowerDNS ist eine Implementierung, die vor allem für das direkte Betreiben von Zonen aus SQL-Datenbanken bekannt ist.
- NSD ist optimiert für Server die ausschließlich autoritative Antworten liefern sollen.

Resolver
Resolver sind Programme die Informationen aus den Nameservern abrufen können. Sie bilden die Schnittstelle zum Nameserverdienst. Resolver sind entweder eigene Programme, oder sie sind in Applikationen (z.B. einen Browser) eingebunden.

Ein Resolver arbeitet entweder **iterativ** oder **rekursiv**.

Bei einer rekursiven Anfrage schickt der Resolver eine Anfrage an einen ihm bekannten Nameserver und gibt als Antwort entweder den gewünschten Resource Record (wenn der befragte Nameserver selber rekursiv arbeitet) oder "gibt es nicht". Rekursiv arbeitende Resolver überlassen also die Arbeit anderen und funktionieren so wie manches andere im Internet: *Ich weiß ein bisschen was und ich kenne jemanden der mehr weiß.*

Bei einer iterativen Anfrage bekommt der Resolver entweder den gewünschten Resource Record oder einen weiteren Namserver, den er als nächsten fragt. Der Resolver hangelt sich so von Nameserver zu Nameserver bis er bei einem autoritativen Nameserver landet. Die so gewonnene Antwort gibt der Resolver dann weiter.

Die Root-Server arbeiten ausschließlich iterativ. Sie wären sonst mit der Anzahl der Anfragen schlicht überlastet.

Bekannte Resolver sind die Programme *nslookup* und *dig*.

Erweiterung des DNS
Bisher sind die Label auf alphanumerische Zeichen und das Zeichen '-' eingeschränkt. Dies hängt vor allem damit zusammen, dass das DNS (wie auch das Internet ursprünglich) in den USA entwickelt wurde. Allerdings gibt es in vielen Ländern Zeichen, die nicht in einem Label verwendet

werden dürfen (in Deutschland zum Beispiel die Umlaute), bzw. es gibt komplett andere Schriftsysteme (z.B. Chinesisch). Namen mit diesen Zeichen sind bisher nicht möglich.
Dies soll sich aber in naher Zukunft durch die Einführung von IDN (RFC 3490) ändern. Um das neue System mit dem bisherigen kompatibel zu halten, werden die erweiterten Zeichensätze mit erlaubten Zeichen kodiert, also auf derzeit gültige Namen abgebildet. Die erweiterten Zeichensätze werden dabei zunächst gemäß dem nameprep-Algorithmus (RFC 3491) normalisiert, und anschließend per punycode (RFC 3492) auf den für DNS verwendbaren Zeichensatz abgebildet. Das Voransetzen des durch die IANA festgelegten IDNA-Prefix *xn--* vor das Ergebnis der Kodierung ergibt das vollständige IDN-Label.
Eine weitere aktuelle Erweiterung des DNS stellt ENUM (RFC 2916) dar. Diese Anwendung ermöglicht die Adressierung von Internet-Diensten über Telefonnummern, also das "Anwählen" von per Internet erreichbaren Geräten mit dem aus dem Telefonnetz bekannten Adressschema. Aus dem breiten Spektrum der Einsatzmöglichkeiten bietet sich insbesondere die Verwendung für Voice over IP Services an.

DynDNS
Es kann nur Rechnern mit fester, sich also nur sehr selten ändernden IP-Adresse ein fester Rechnername zugeordnet werden. Da jedoch sehr viele Nutzer mit Heimrechnern eine variable IP-Adresse haben (mit jeder Einwahl in das Internet wird eine andere IP-Adresse aus einem Pool zugeteilt), gibt es inzwischen DynDNS-Betreiber, die dafür sorgen, dass man auch mit solch rasch ändernden Adressen möglichst immer über den selben Rechnernamen erreichbar ist.

Netzwerkbetriebssysteme

Die ursprüngliche und wohl immer noch wichtigste Aufgabe von Netzwerkbetriebssystemen ist die Nutzung von Ressourcen wie Drucker, Plotter, Festplatten, CD-ROMs usw. sowie eine sichere und zentrale Speicherung der Daten. Die Kommunikation der Nutzer im internen Netz (Intranet), aber auch in weltweiten Datennetzen (z. B. E-Mail, Internetzugang, WWW, Groupware usw.), gehört heute ebenso zu den Standardaufgaben, wie die Integration von Internet-Protokollen und -Diensten in die PC-Betriebssysteme Novell Netware und Windows zeigen. Auch die Anbindung an Großrechner sowie die Integration von spezifischen Applikationsservern sind wesentliche Aufgaben. An Bedeutung gewinnt insbesondere aus Kostengründen immer mehr die zentrale und einfache Konfiguration und Administration der Rechner im Netz.
In den 90er Jahren war verstärkt die Tendenz festzustellen, dass Systeme der mittleren Datentechnik (Minicomputer), in zunehmendem Maße die Mainframes verdrängten. Insbesondere UNIX- und Linux-Systeme haben hier an Bedeutung gewonnen. Aus der ursprünglich Host-zentrierten DV fand eine Verlagerung der EDV auf dezentrale Systeme in den Abteilungen statt. Merkmale sind u. a.:

- Verarbeitung am Arbeitsplatz
- verteilte Verarbeitung
- Verarbeitung auf Abteilungsebene
- Gleichrangige Netzwerkverarbeitung
- Individuelle Datenverarbeitung

Zu den Ursachen hierfür zählten die großen Fortschritte in den Entwicklungen lokaler Netze, z. B.:

- Festplatten-Verwaltung in Servern
- Multi-User-Software
- Datenverarbeitung in Netzen, Hosts usw.
- Fehlertoleranz
- Datenschutz und -sicherheit

Es setzte sich durch, dass Mainframes, Minis und PC-basierte LANs nicht gegeneinander antraten, sondern sich zunehmend ergänzten. Im Mittelpunkt sollte die Anwendung stehen, das heißt die zu erledigenden Aufgaben.

Merkmale von Netzwerkbetriebssystemen

Es lassen sind zwei Typen von Servern für Netzwerkbetriebssysteme unterscheiden:

- dedizierte Server (z. B. Novell): der Server ist nicht gleichzeitig als Arbeitsstation einsetzbar.
- nicht-dedizierte Server (z. B. UNIX, Windows 2000): der Server ist gleichzeitig auch als Arbeitsstation nutzbar (Client-Server-Prinzip), obwohl sie meist als „reine" Server betrieben werden.

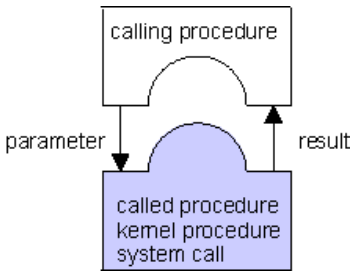
Wichtige Merkmale von Netzwerkbetriebssystemen sind:

- Architektur des Betriebssystems
  - Server-Platform als Kernstück des Betriebssystems, das alle Netzfunktionen bereitstellt, darunter Dateisysteme und Festplatten, Memory-Management, Prozeß- und Taskscheduling, File-, Print- und Backupdienste, File- und Recordlocking usw.
  - Redirection-Software auf den Clients, um den Zugriff auf Netzlaufwerke und -ressourcen möglichst transparent zu erlauben
  - unterstützte Netzwerkdienste
  - Kommunikationssoftware
  - Unterstützung verschiedener Client- und Server-Platformen (z. B. Linux mit NFS für die UNIX-Umgebung und "Samba" für Windows-Clients)
- Leistungsfähigkeit und Zuverlässigkeit
  - Datendurchsatz
  - Verkabelung des Netzes
  - Netz-Komponenten (Repeater, Switches, Router)
  - kritische Anwendungen
  - Abhängigkeit des Betreibers vom Funktionieren des Netzes
- Sicherheit
  - Accounting- und Passwort-Sicherheit
  - Datei- und Directory-Sicherheit
  - Internetwork-Sicherheit
  - Fileserver-Sicherheit
- Standards
  - genormte Standards (ISO, IEEE, DIN, ANSI usw.)
  - Industriestandards
  - Anwendungsstandards, z.B. für serverbasierende Applikationen, clientbasierende Applikationen, verteilte Applikationen,
  - Protokollstandards, z.B. Medien-Protokolle (Ethernet, ATM, FDDI usw.), Transport-Protokolle (IP, IPX usw.), Client-Server-Protokolle
  - Standards der Interprozeß-Kommunikation, z.B. Sockets, TLI, Corba usw.

Die meisten Netzwerksysteme arbeiten nach dem **Client-Server-Prinzip**. Abhängig von der Arbeitsweise im Netzwerk sind zu unterscheiden LAN und Single-User-Anwendungen, wo über das Netz meist nur ein Dateisystem zur Verfügung gestellt wird oder LAN und netzwerkfähige Software, mit Ausnutzen von File-Sharing sowie File- und Record-Locking (mehrere Nutzer arbeiten mit gemeinsamen Daten).

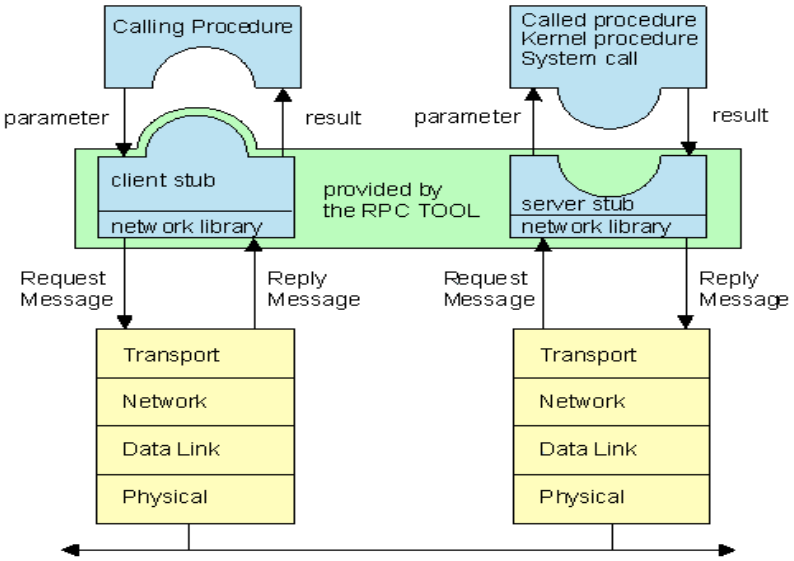
Remote Procedure Call (RPC)

Das Verfahren der Remote Procedure Calls wurde Anfang der 80er Jahre vom Sun Microsoystems für ihr Network File System (NFS) entwickelt. Es ist derzeit das wesentliche Element in Netzwerkbetriebssystemen, um Serverdienste für Clients zur Verfügung zu stellen. Ein lokaler Prozeduraufruf kann folgendermaßen skizziert werden:

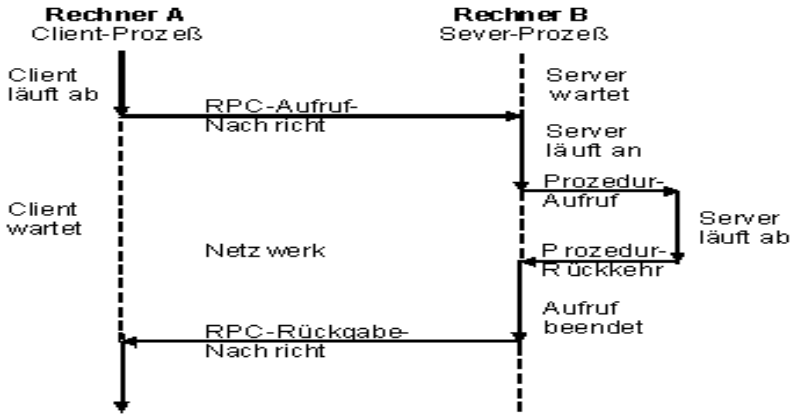


Eine Prozedur oder Funktion wird mit den entsprechenden Parametern aufgerufen, und kehrt nach erledigter Arbeit mit einem Resultat zurück. Für Dienste des Betriebssystems werden i.d.R. sog. System Calls, also Aufrufe von Prozeduren des Systems genutzt.

Nach diesem Schema arbeiten auch RPCs:



Eine Anwendung ruft einen Netzwerkdienst auf wie eine lokale Prozedur mit Übergabe von Parametern auf. Der Aufruf wird von der RPC-Library in ein RPC-Paket verpackt und über das Netz an den Server gesendet, der den Dienst ausführt und das Resultat liefert. Dieses wiederum wird an die Anwendung zurückgegeben.
Damit kann der zeitliche Ablauf eines RPC so skizziert werden:



Literaturverzeichnis und Weblinks

Schawohl, Ernst [Compos.]. Alkemper, Christian [Transl..]
Cisco Networking Academy Program : Lehrbuch 1. und 2. Semester
- (Cisco Networking Academy Program, first-year companion guide [Orig. Title])
München, 2002, Markt + Technik Verl., 595 S. : Ill., graph. Darst.
ISBN: 3-8272-6263-1

Tanenbaum, Andrew S. [Auth.]
Computernetzwerke
- (Computer networks [Orig. Title])
3., rev. Aufl, München [u.a], 2000, Pearson Studium, 873 S. : Ill., graph. Darst.
ISBN: 3-8273-7011-6

Tanenbaum, Andrew S. [Auth.]. Baumgarten, Uwe [Transl..]
Moderne Betriebssysteme
- (Modern operating systems [Orig. Title])
2., ueberarb. Aufl, Muenchen [u.a.], 2002, Pearson Studium, 1021 S. : Ill., graph. Darst.
ISBN: 3-8273-7019-1

Badach, Anatol [Auth.]. Hoffmann, Erwin [Auth.]. Knauer, Olaf [Auth.]
High speed internetworking : Grundlagen und Konzepte für den Einsatz von FDDI und ATM
1. korr. Nachdruck, Bonn [u.a.], 1995, Addison-Wesley, 596 S. : Ill.
ISBN: 3-89319-713-3

DIN EN 50173 : Informationstechnik, anwendungsneutrale Verkabelungssysteme ;
deutsche Fassung EN 50173:1995 + A1:2000, Berlin, 2000, Beuth, 80 S.

IANA - Internet Assigned Numbers Authority http://www.iana.org

RFC - Datenbank : http://www.faqs.org/rfcs/

The Free Encyclopedia : http://en.wikipedia.org/

Cisco Tech Paper, Example TCP/IP: http://www.cisco.com/en/US/products/sw/secursw/ps743/
products_user_guide_chapter09186a008007f2df.html