Skript zur Vorlesung Kommunikations- und Netzwerktechnik

3/4. Halbjahr

Günter Stagge

Einleitung: Worum geht es ?

Kommunikations- und Netzwerktechnik

Kommunikation: Wie funktioniert Kommunikation

Netzwerk: Technik zur Datenübertragung, Medium, das Kommunikation überträgt

K/N Standards und Organisationen, Normen, RFCs
OSI Schichtenmodell

N Klassifizierung von Netzen nach Ausdehnung (LAN, MAN, WAN)
N Netzwerktopologien / Architektur (Stern, Bus, Ring)
N Übertragungsmedien (Koax, TP, Glasfaser)
N Zugriffsverfahren (CSMA/CD, Token)
N Netzwerktechnologien (Ethernet, Token Ring)
N Komponenten zur Übertragung und Kopplung (Router, Hub, Switch)

K Kommunikationsmodell, Manchestercodierung
K Paketvermittlung/Leitungsvermittlung
K Übertragungskanal (Abtastung, Quantisierung, Verzerrungen, Echokompensation, Störabstand, Bitfehler, Fehlererkennung)
Modem, Multiplexverfahren
K Protokolle (Definition, Überblick)
K TCP/IP,Referenzmodell, Adressierung (Klassen, Masken, Broadcast, ARP)
K Routing
K Namensdienste (Hosts, Lmhosts, WINS, DNS)

K/N Überblick Netzwerkbetriebssysteme, Netzwerkverwaltung (TCO)

Teil 1: Netzwerktechnik

Normen, Standards

De facto Standards

Hierbei spricht man von Systemen, die sich allgemein durchgesetzt haben, ohne daß diese irgendwo offiziell definiert wären.

TCP/IP war bis Mitte der 70-er Jahre so ein De facto - Standard, das heißt, es wurde bereits vorher allgemein benutzt, aber es gab dazu kein offiziell von einer Organisation formuliertes Regelwerk.

Organisationen für Standardisierung

Wie in allen Sparten der Technik gibt es auch im Bereich Netzwerke und Kommunikation eine Vielzahl von Organisationen, die sich um die Definition von allgemein akzeptierten Spezifikationen bemühen. Wenn solche Spezifikationen zum Standard erhoben sind, ist es das Bestreben dieser Organisationen, diese zu verbreiten.

Die Vorgehensweise ist in etwa diese: Erarbeiten von Ideen und Möglichkeiten zu deren Umsetzung in Diskussionsforen. Daraus resultiert ein Entwurf, der anschließend ganz oder in Teilen zum Standard erhoben wird. Letzter Schritt ist die formelle Bekanntgabe des Standards.

Einige Organisationen

Telekommunikation, Radiokommunikation

ITU, *International Telecommunications Union.* Die Organisation, aus der die ITU hervorging, entstand bereits 1865. Schon damals, als es lediglich die Telegraphie gab, war klar, daß man sich auf einen Code (in dem Fall den Morsecode) einigen muß, wenn internationale Veständigung möglich sein sollte.

Später übernahm die ITU auch die Standardisierung von Telefonie, damit also der Telekommunikation insgesamt (ITU-T), und der Radiokommunikation (ITU-R). Seit 1947 ist sie eine Behörde der Vereinten Nationen.

Von 1956-1993 wurde die ITU-T unter dem Namen **CCITT**, *Comité Consultatif International Télégraphique et Téléphonique* geführt.

Internationale Normen

ISO, *International Organization for Standardization,* wurde 1946 gegründet. Mitglieder sind die nationalen Institute für Normung der beteiligten Länder (etwa 90). Dazu gehören DIN (Deutschland), ANSI (USA), BSI (Großbritannien), AFNOR (Frankreich).

IEEE, *Institute of Electrical and Electronics Engineers*. Im Bereich der Elektrotechnik und Informatik zu Hause, gibt es innerhalb dieser Organisation eine Standardisierungsgruppe. Von ihr stammt der wichtigste Standard für LAN' s (IEEE 802).

Internet

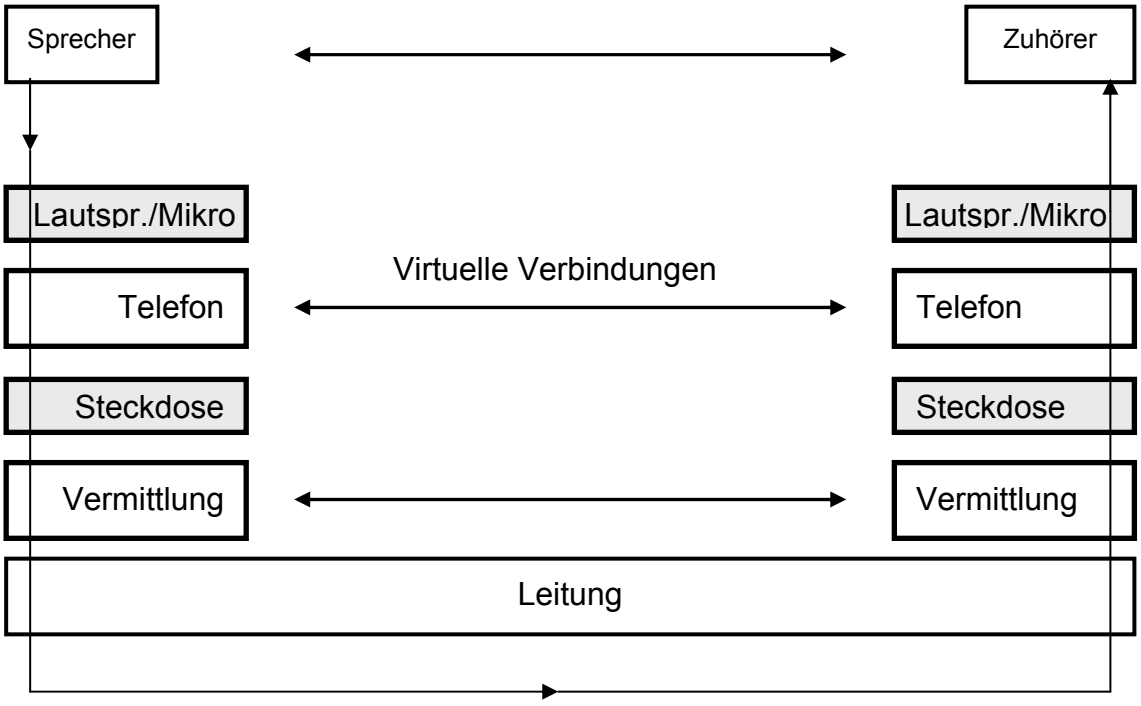
IAB, *Internet Activities Board*, gegründet 1983. Ergebnisse werden in Form technischer Berichte verbreitet, die online abrufbar sind und in der Reihenfolge ihres Entstehens sortiert werden. Diese nennt man RFC' s, *Request for Comments*.

Kommunikation im Modell

Damit sich im Kommunikationsverhalten keine Differenzen ergeben, egal wie verschieden die beteiligten Systeme in ihren sonstigen Eigenschaften auch sind, bedarf es bestimmter Festlegungen.

Einfaches Beispiel aus dem Leben: Telefonieren

Kommunikationsebenen



Das Modell ist selbstverständlich etwas vereinfacht. Aber das Wesentliche soll hier deutlich werden. Nämlich die Tatsche, daß die Kommunikation über mehrere Ebenen stattfindet. Das sind zuerst die Gesprächspartner, dann die Telefone, Vermittlungseinheiten und schließlich die Leitungsverbindungen zwischen den Vermittlungsstellen.

Technisch betrachtet sprechen nicht die Gesprächspartner miteinander, sondern der Sprecher mit seinem Telefon. Dieses wiederum mit der Vermittlungsstelle und diese kontaktiert die Übertragungsleitung. Das heißt, abgesehen von der untersten Schicht sind alle Verbindungen virtuell.

Schichten und Schnittstellen

Jede Schicht tritt in direkten Kontakt zu der unter ihr und zu der über ihr liegenden über eine Schnittstelle. Für den Sprecher besteht die Schnittstelle aus Lautsprecher und Mikrofon. Daneben kommunizert jede Ebene virtuell mit ihrem Pendant auf der Gegenseite.

Der eigentliche Informationsfluß geht also vom Sender aus von oben nach unten durch sämtliche Schichten, dann über die Leitung zum Empfänger, dessen Schichten von unten nach oben durchquert werden, bis die eigentliche Information wiederhergestellt ist (das ist in diesem Fall die Stimme des Sprechers).

Innerhalb einer Schicht wird die Information den Erfordernissen entsprechend aufbereitet und der Schnittstelle in der festgelegten Weise angeboten.

Nach der Schnittstelle Mikrofon ist die Information statt Schalldruck nun elektrische Spannung. Auf der Empfängerseite muß also in der vergleichbaren Ebene (dem Telefonapparat) wieder dieselbe (elektrische) Information vorliegen, damit die Botschaft richtig verstanden wird und in die ursprüngliche Schallinformation zurückverwandelt werden kann.

Warum ein (Schichten-) modell

Vorausgesetzt, jede Schnittstelle und jede Schicht in ihrer Funktion sind genau definiert, hat das einen Vorteil. Jede Komponente ist austauschbar.

Beispiel: So lange weiterhin als Schnittstelle zum Menschen Lautsprecher und Mikrofon benutzt werden, auf der anderen Seite die Telefondose mit ihren mechanischen und elektrischen Eigenschaften gleich bleiben, spielt es keine Rolle, wie der Telefonapparat intern arbeitet. Er kann, ohne die restliche Kommunikationskette zu stören, durch ein neueres Modell ersetzt werden.

ISO OSI Referenzmodell

In der Netzwerktechnik bedeutet das von der ISO entwickelte OSI – Modell den ersten Schritt zur internationalen Standardisierung. (1983)

OSI steht für **O**pen **S**ystems **I**nterconnection. Das Modell soll also ein offenes Kommunikationssystem definieren.

Das OSI – Referenzmodell unterteilt die für die Datekommunikation erforderlichen Funktionen in einzelne Abschnitte. Diese werden als Schichten bezeichnet.

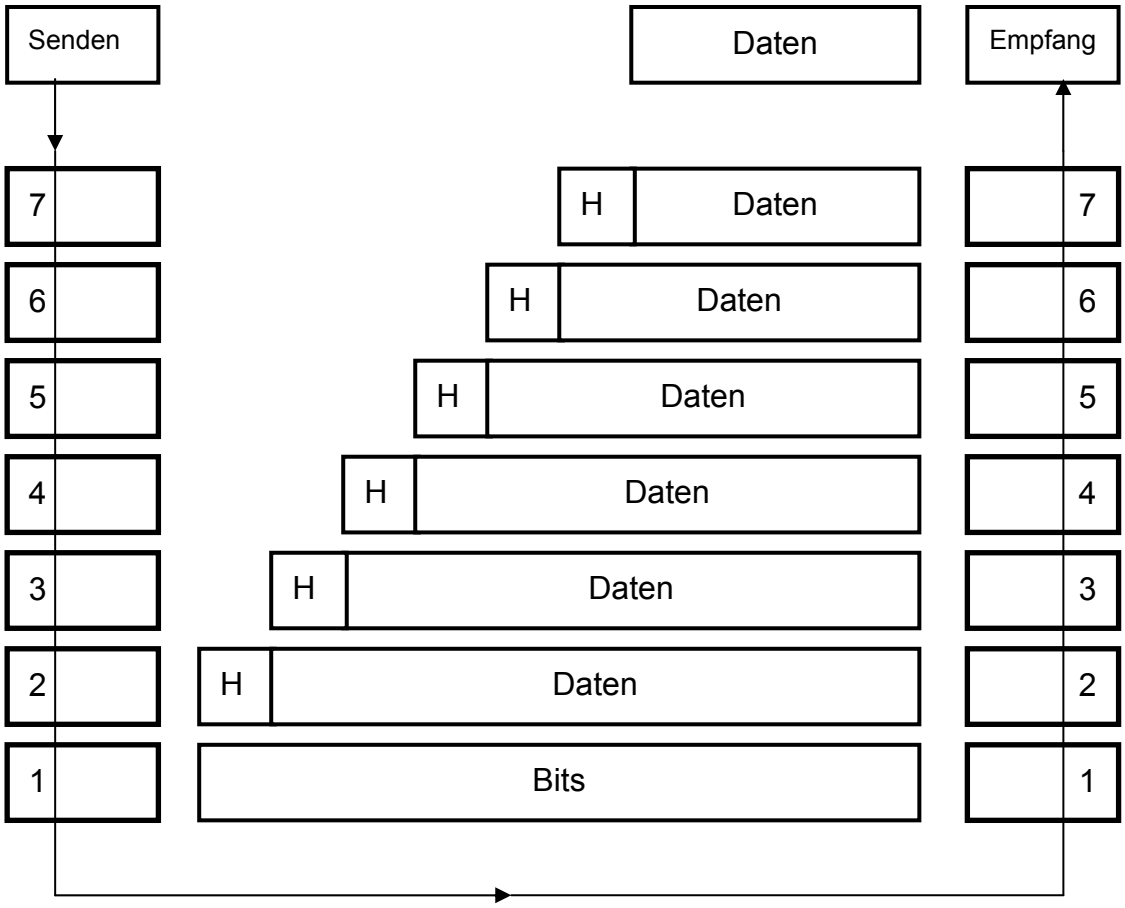
Ein wichtiger Grundsatz: Es sollte genügend Schichten geben, damit nicht mehrere Funktionen in eine gepackt werden müssen. Aber auch nicht mehr Schichten als wirklich erforderlich.

In diesem Fall hat sich auf sieben Schichten verständigt.

Eine weitere Unterscheidung besteht darin, daß die unteren Schichten 1 bis 4 transportorientiert, die oberen Schichten 5 bis 7 anwenungsorientiert sind.

7	Application Layer	Anwendungsschicht
6	Presentation Layer	Darstellungsschicht
5	Session Layer	Kommunikationsschicht
4	Transport Layer	Transportschicht
3	Network Layer	Vermittlungsschicht
2	Data Link Layer	Sicherungsschicht
1	Physical Layer	Bitübertragungsschicht

Datenübertragung im OSI – Modell



Der Sendeprozeß übergibt die Daten an die Anwendungsschicht. Diese nimmt möglicherweise Änderungen vor (es kann durchaus sein, daß auf dieser Ebene nichts geschieht). Die Anwendungsschicht auf der Empfängerseite muß die Änderungen wieder rückgängig machen können. Die dazu notwendige Information steht in einem Haeder (H), der von der Anwendungsschicht auf Senderseite angefügt wird.

Der gesamte Block, also Header und Daten, ist für die darunterliegende Darstellungsschicht der Datenstrom, den es zu bearbeiten gilt. Dort spielt es keine Rolle, was in der Anwendungsschicht Nutzdaten oder Haeder sind.

Die Information, die jede Schicht zufügt, ist also ausschließlich für das Pendant auf der anderen Seite bestimmt.

In der Bitübertragungsschicht wird natürlich kein Header, also weitere Information, zugefügt.

Der Datenstrom wird dort allerdings nicht so wie er ankommt über die Leitung zum Empfänger geschickt. Normalerweise muß er gewandelt werden in eine Form, die der Datenkanal übertragen kann. Diesen Vorgang nennt man Codierung. Dazu später mehr.

Am Empfänger angekommen erfolgt der Durchlauf in umgekehrter Reihenfolge.

Jede Schicht kommuniziert also direkt mit derselben Schicht der Gegegenseite, für die ihre Informationen (hinterlegt im Header) ja bestimmt sind.

Die drei Konzepte des OSI - Modells

Diese sind: Dienste, Schnittstellen, Protokolle

Mit **Dienst** wird festgelegt, was die Schicht macht. Jede Schicht erbringt Dienste für die darüber liegende Schicht.

Wie genau der Prozess innerhalb einer Schicht abläuft, regeln **Protokolle** (außer in der Bitübertragungsschicht). Wie die Protokolle arbeiten, spielt keine Rolle. Protokolle können beliebig verwendet und durch andere ersetzt werden, so lange sie die gestellten Aufgaben erfüllen. Durch die Anordnung in übereinander liegenden Schichten nennt man die resultierende Struktur auch **Protokollstapel**.

Ein Protokoll ist eine Festlegung, wie bestimmte Vorgänge genau ablaufen müssen. Im Netzwerkbereich bei der Datenübertragung gehört dazu neben vielen anderen Dingen die Adressierung der Netzwerkkomponenten.

Es muß lediglich gewährleistet sein, daß die **Schnittstelle** zur darüber liegenden Schicht den Vereinbarungen gemäß bedient wird. Die Schnittstelle der unteren Schicht teilt der darüberliegenden mit, wie diese auf ihre Dienste zugreifen kann.

Was passiert in den Schichten ?

Noch mal zur Erinnerung: Die Anzahl der Schichten soll im Sinne einer übersichtlichen Struktur möglichst gering sein. Andererseits ist aber zu vermeiden, daß mehrere Funktionen in eine einzige Schicht gepreßt werden.

Eines ist dabei zu beachten: Das OSI – Modell definiert keine Netzarchitektur (in Form von Diensten oder Protokollen, dazu später mehr). Es sagt nur, was die einzelnen Schichten bewirken sollen.

ISO hat selbstverständlich auch Normen für jede dieser Schichten erarbeitet und als Standards veröffentlicht. Diese finden allerdings in der Praxis eher selten Anwendung.

Im OSI – Modell sieht die Aufgabe der einzelnen Schichten folgendermaßen aus:

Bitübertragungsschicht (*Welche Form haben Bits und Hardware*)

Hier geht es um mechanische und elektrische Spezifikationen (Stecker, Kabel, Pinbelegung, Signalform, Spannungen etc).

Sicherungsschicht (*Sortierung der Bits*)

Zugriffskontrolle (wer darf wann), Flusskontrolle (Überschwemmung des Empfängers mit Daten verhindern), Aufteilung des Datenstroms in Rahmen definierter Länge, Ergänzung der Rahmen durch Bitmuster zur Erkennung von Anfang, Ende, Fehlern, Empfangsbestätigung bzw Neuanforderung eines als defekt erkannten Rahmens, Adressierung auf Hardwareebene (MAC – Adressen).

Vermittlungsschicht (*Wohin und woher*)

Logische Adressierung, Routing, aber auch Abrechnungsfunktionen (Zählung von Paketen, Bytes, Bits,), und auch hier gibt es Mechanismen zur Flusskontrolle

Transportschicht (*Das Band wird geschlossen*)

Verbindungsauf- und –abbau, Mehrfachnutzung eines Kanals (Multiplexing), parallele Nutzung mehrerer Kanäle (Multilink), Zerlegen des Datenstroms in Pakete, Sortierung in die richtige Reihenfolge

Sitzungsschicht (*Wer mit wem und wie oft*)

An/Abmelden an Remote Systemen, Handling von Netzwerksitzungen (Zugriff auf mehrere Server gleichzeitig möglich), Steuerung des Verkehrs (Voll, Halbduplex), Setzen von Fixpunkte bei Unterbrechung eines Datenstromes

Darstellungsschicht (*Umbau und Wandel*)

Zeichenkodierung (ASCII etc.. , *Tastatur, Zeichensätze*), Datenstrukturen (Gleitkomma, Ganzzahlen ...), konvertieren interner Darstellungsformen in netzkonforme, Kompression, Verschlüsselung

Anwendungschicht (*Kommunikation für alle*)

Schnittstelle zur Anwendung, wenn diese Kommunikation betreibt: Also etwa Mail (SMTP), Dateitransfer (FTP), Namensdienste (WINS, DNS), Verzeichnisdienste (NDS, ADS)

Wie war das ? Möglichst nur eine Funktion pro Schicht ?

Nun, ganz genau darf man das nicht nehmen, es ist in Wirklichkeit eher so, daß verwandte Funktionen gemeinsam auf einer Schicht residieren. Mit 50 oder mehr Schichten hätte das ganze Modell kaum noch einen Sinn.

Trotzdem gibt es hier und da schon Schwachpunkte. Wie man ziemlich schnell erkennt, gibt es die Flußkontrolle nicht nur auf einer Schicht. Auch Fehlerkontrolle und Adressierung tauchen mehrmals auf.

Mit Flußkontrolle nur auf der zweiten Schicht sowie die Fehlerkontrolle auf Schicht 7 wäre das Ganze schon wesentlich effizienter.

Nur bei der Adressierung kommt man nicht umhin, auf den Schichten 2 (Hardware) und 3 (logisch) etwas anzubieten. Der Adressraum auf Schicht 2, die sogenannten MAC – Adressen, ist völlig flach aufgebaut. Jede Adresse gibt es weltweit nur ein Mal.

Mit einem flachen Adressraum kann man keine Aufteilung in Teilnetze organisieren. Dazu bedarf es einer strukturierten Adressierung und routingfähigen Protokollen. Teilnetze wiederum werden gebraucht, damit lokaler Verkehr auch wirklich lokal bleibt.

Einteilung / Klassifizierung von Netzen

Ein weithin gängiges Kriterium der Klassifizierung ist die Reichweite bzw Ausdehnung. Aber auch die Funktionen und Organisation (privat-öffentlich) sind charakteristisch. Drei Arten werden unterschieden:

LAN = Local Area Network
MAN = Metropolitan Area Network
WAN = Wide Area Network

Die zugehörigen Bezeichnungen lassen bereits in groben Zügen die Einsatzgebiete erkennen.

LAN: Größenordnung 10m (Raum) über 100m (Gebäude) bis ungefähr 1 km (Firmengelände). LAN' s sind Broadcast – Netze (Prinzipiell ist jeder mit jedem verbunden) mit relativ hoher Bandbreite, 10/100/1000 Mbit/s (1 Mbit ist 1.000.000 Bit/s, nicht 1024x1024 bzw 2^{20} Bit/s).

Meistens Kupferkabel- Verbindungen, abgesehen von Glasfaser zwischen Gebäuden, wenn die Strcken zu lang werden oder auch bei kritischen EMV – Bedingungen.

LAN' s sind private Netze, das heißt, der Besitzer ist auch der Betreiber. Gemeinsame Nutzung und Verwaltung von Ressourcen, begrenzte Telnehmerzahl. (Noch) in der Hauptsache Datenübertragung.

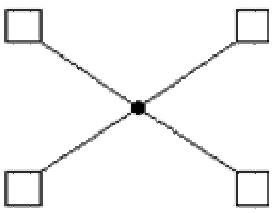
MAN: Stadtnetze, Größenordnung 10 km (z. B. MANET in MA). Übertragung mit mehr als 100 Mbit/s. Ebenfalls ein Broadcast – Netz. Funktioniert quasi als öffentliches LAN, meistens über Glasfaser. Übertragung verschiedenster Dienste (Daten, Sprache, Multimedia). Begrenzte Teilnehmerzahl.

WAN: Größenordnung ab 10 km bis Globus. Öffentlicher Charakter, geringe Bandbreiten, Wähl- oder Standleitungen sind möglich, (noch) in der Hauptsache für Datenübertragung, alternative Wegwahl beim Datenverkehr.

Netzwerk - Topologien

Auch hier sind es deren drei, nämlich Stern, Ring, Bus

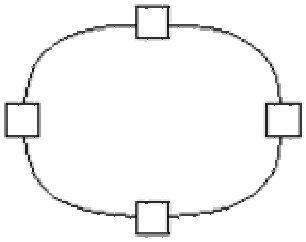
Stern:



Alle sind über einen zentralen Knoten miteinander verbunden. Nachteil: Ein Ausfall des Sternknotens – nichts geht mehr; viel Kabel ist nötig.

Vorteil: Ausfall einer Station – kein Problem für die anderen.

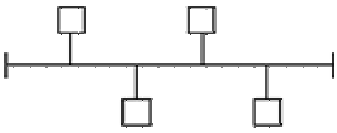
Ring:



Der Datenfluß erfolgt in einer (Umlauf-) Richtung von Knoten zu Knoten. Ausfall eines Knotens – der Ring ist tot.

In der Praxis hat man oft einen logischen Ring mit sternförmiger Verkabelung. Ausfälle einzelner Knoten werden durch Relais im Verteiler erkannt und überbrückt

Bus:



Ein durchlaufendes Zentralkabel, an dem alle Teilnehmer an Abzweigen angehängt sind. Ausfall einer Station ist ohne weitere Auswirkungen. Kabelbruch bringt allerdings den ganzen Verkehr zum Erliegen.

Die Enden müssen mit definierten Abschlußwiderständen versehen sein. An den Kabeltyp angepaßte Abschlußwiderstände verhindern Signalreflexionen an den Kabelenden. Diese würden sich mit dem Nutzsignal überlagern und es verfälschen.

Billig, einfach zu verkabeln, keine Verteiler erforderlich. Die Leitung im klassischen Busnetz schlängelt sich einfach von Rechner zu Rechner.

Übertragungsmedien

Diese gehören zur Schicht 1

Ein Medium kann man in Form von Basisband- oder Breitbandübertragung nutzen.

Basisband: Nur ein Übertragungskanal ist vorhanden, dieser nutzt den gesamten verfügbaren Frequenzbereich der Leitung.

Breitband: Die verfügbare Bandbreite wird in mehrere Kanäle/Frequenzbänder aufgeteilt.

Wird ein Kanal allerdings in Zeitfenster eingeteilt, so daß mehrere Kanäle dadurch entstehen, daß jedem ein Zeitfenster zur Verfügung steht, zwischen denen umgeschaltet wird, ist das kein Breitband.

Die Bezeichnungen Basis- und Breitband beziehen sich auf eine frequenzmäßige Aufteilung.

Die Klassifizierung / Benennung von Übertragungsmedien erfolgt in der Form XbaseY, XbroadY

X: maximale Datenübertragungsrate
Base = Basisband, Broad = Breitband
Y: Verkabelungsart oder Segmentlänge 2=200m, T= Twistet Pair, F= Fiber

Koaxialkabel:

Busnetz, Verkabelung mit definierten Endwiderständen

Thicknet (10Base5) mit externem Transceiver, der auf das Kabel gesteckt wird, Segmente bis 500 m Länge. Das Kabel ist dick und zäh, optisch ähnlich einem (gelben) Gartenschlauch.

Ein Transceiver ist die Elektronik zum Senden und Empfangen der Daten. Dieser ist bei allen anderen Techniken in der Netzwerkkarte integriert.

Thinnet (10Base2), Segmente bis 185 m, Endwiderstände (Terminatoren 50 Ω), BNC – Stecker, im Bild oben zu sehen. Dünnes, flexibles Kabel, leicht zu verlegen.

Thicknet hat nur noch wenig Bedeutung. Kleine Netze werden aber gerne mit Thinnet aufgebaut, weil keine Verteiler (Hubs oder Switches) erforderlich sind. Die Rechner werden direkt mit T-Stücken an den Bus angeschlossen.

TP, Twisted Pair

10BaseT, 100BaseT, Verdrillte Kupferkabel, solide Adern, traditionell stammt die Bauform aus der Telefonverkabelung. Verdrillt sind die Adern wegen elektromagnetischen Einstreuungen (ein längsliegendes Kabel wirkt als Antenne).

Unshielded (UTP) in verschiedenen Kategorien (1 bis 5) ist definiert

Kat 1: Trad. Telefonkabel, ein Adernpaar gedrillt, ungeeignet für Datenübertragung
Kat 2: zwei gedrillte Adernpaare, bis 4 Mbit/s
Kat 3: vier gedrillte Adernpaare, bis 10 Mbit/s
Kat 4: vier gedrillte Adernpaare, bis 16 Mbit/s
Kat 5: vier gedrillte Adernpaare, bis 100 Mbit/s
Kat 6,7: Nicht standardisiert, aber weitere Erhöhung des Frequenzbereichs und der Datenrate, für Gigabit Ethernet ist Kat 5 nicht ausreichend

Shielded (STP) gibt es auch, ist eher selten im Einsatz (IBM), die einzelnen Adern sind abgeschirmt, dazu umgibt das Ganze ein Gesamtschirm.

TP – Kabel dürfen maximal 100 m lang werden

TP – Kabel wird mit RJ 45 Steckern (Bild oben) verbunden

Telefon/Modem- Kabel sehen ähnlich aus, die Stecker sind nicht ganz so breit, aber gleich hoch und heißen RJ 11.

RJ = Registered Jack (genormter Stecker)

Glasfaser, LWL

Lichtwellenleiter, bestehen aus einem Innenleiter aus Glas oder Quarz. Ummantelt wird alles mit verschiedenen Materialien, die dem mechanischen Schutz dienen.

An den Kabelenden müssen die elektrischen Signale in optische gewandelt werden und beim Empfang wieder zurück. Das erledigen Leucht – oder Laserdioden sowie Fotowiderstände.

Die Bandbreite von Glasfasern ist materialbedingt fast unendlich, aber: Dispersion erzeugt Laufzeitunterschiede, dadurch haben wir auch hier begrenzte Reichweite, allerdings wesentlich mehr als bei Kupferleitungen, möglich sind viele Kilometer

Die Begrenzung der verfügbaren Bandbreite ist oftmals aber eher durch die Umschaltgeschwindigkeit bei der Wandlung elekrisch zu optisch (1 Gbit/s) gegeben.

Vorteile von Lichtwellenleitern neben der Bandbreite: keine Abstrahlung elektromagnetischer Strahlung und nicht unterwegs anzuzapfen. Also weitgehend abhörsicher.

Auch unempfindlich gegen derartige Störungen von außen, Repeater sind nur alle 30 bis 100 km statt 5 km bei Kupfer erforderlich.

Telefongesellschaften benutzen LWL oft aus einem ganz anderen Grund: Sie sind dünn und haben vergleichsweise wenig Gewicht. Volle Kabelkanäle können oft nicht mehr durch weitere Kupferleitungen erweitert werden. Ersatz durch LWL schafft also Platz.

Tausend verdrillte Kabelpaare in 1 km Länge bringen in etwa etwa 8000 kg auf die Waage. Zwei Glasfasern mit höherer Kapazität, als diese 1000 Kupferkabel bieten, nur etwa 100 kg. Trotz hoher Kosten pro Faser ist die Verlegung von LWL also viel billiger.

Hohe Kosten hat man allerdings durch die aufwendige Verbindungstechnik, eine einzelne Faser ist natürlich auch teurer als Kupfer. Zu Glasfasern folgt im Anschluß ein eigenes Kapitel

Ein paar Grundlagen zu Glasfasern / Lichtwellenleitern

Brechung und Reflexion

Der Brechungsindex n ist eine Eigenschaft lichtdurchlässiger Stoffe.

Für die Lichtgeschwindigkeit c (n) in dem betreffenden Stoff gilt:

$c(n) = c_o / n$

(c_o = 2,9799 10^8 m/s, Lichtgeschwindigkeit im Vakuum

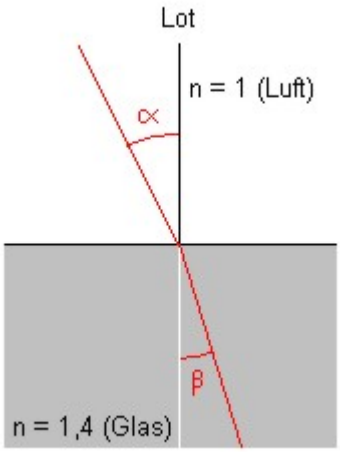
Das Vakuum hat den Brechungsindex 1 .

Einige andere Werte sind:

Stoff	Wasser	Glas	Luft
Brechungsindex n	1,33	1,4 - 1,9	1,00027

In diesem Zusammenhang spricht man von optischer Dichte. Ein Medium mit dem größeren Brechungsindex, also der kleineren Lichtgeschwindigkeit, ist das optisch dichtere Medium.

Ein schräg einfallender Lichtstrahl wird bei Passieren der Grenzschicht zum dichteren Medium zum Lot hin gebrochen, andersherum vom Lot weg, wie im Bild unten ersichtlich. Der Strahlengang an sich bleibt unabhängig von der Richtung gleich.



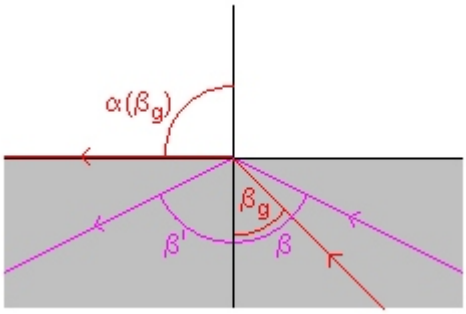
$n_{(Luft)} . \sin(\alpha) = n_{(Glas)} . \sin(\beta)$

Brechungsgesetz von Snellius
für die gewählten Medien

Für die Funktion der Glasfasern ist der Fall interessant, bei dem sich das Licht im dichten Medium ausbreitet.

Besonders zu beachten ist der Fall, wenn der Winkel β (siehe oben stehende Abbildung) so groß wird, dass sin α = 1, also α = 90° wird. Ein mit dem entsprechenden Grenzwinkel
$\beta_g = \arcsin(n_2 / n_1)$ aus dem Glas kommender Lichtstrahl würde dann nach der Brechung parallel zur Grenzfläche verlaufen, also eben $\alpha (\beta_g) = 90°$. Wird der Winkel β dann noch größer, findet keine Brechung mehr statt; der Lichtstrahl wird dann in optisch dichtere Medium zurückgeworfen. Dies bezeichnet man als Totalreflexion

Der Strahl wird mit $\beta' = \beta$ reflektiert.



Grenzwinkel und Totalreflexion

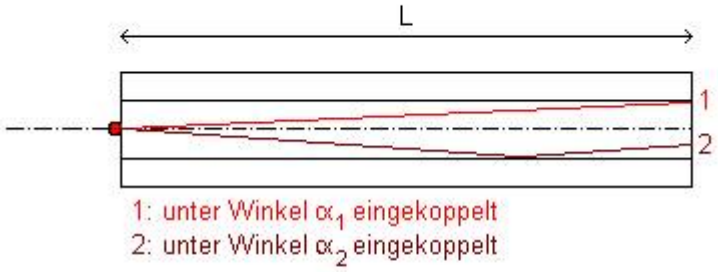
Man unterscheidet diesen Fall von der Teilreflexion: Auch bei jeder Brechung wird stets ein kleiner Teil der Lichtleistung reflektiert, nur wird dies im Zusammenhang der Brechung oft nicht erwähnt.

Signalveränderung bei Lichtwellenleitern - Dispersion

Modendispersion

Dispersion entsteht, wenn die durchlaufenden Lichtstrahlen unterschiedlich lange Wege zurücklegen können. Dadurch werden die eingekoppelten Signale mit zunehmender Leitungslänge immer mehr verfälscht.

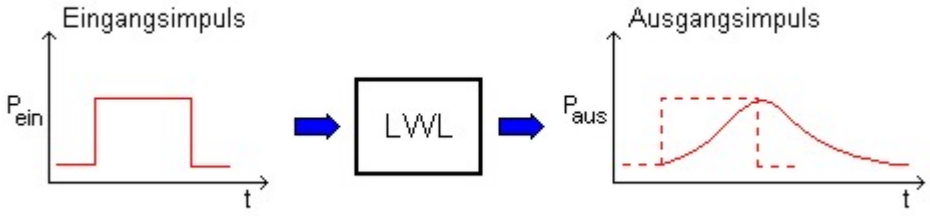
Einzelne Lichtstrahlen werden als Moden bezeichnet.



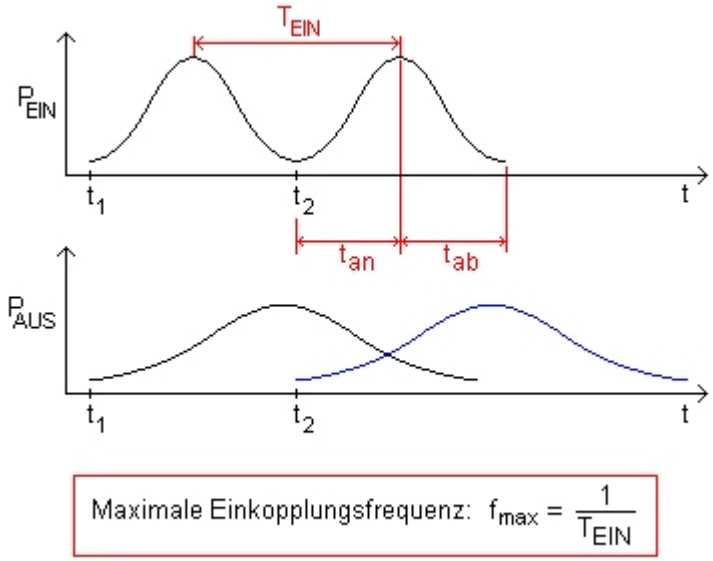
Strahlweglänge:

$$S_i = \frac{L}{\cos \alpha_i}$$

Strahlwege in Stufenprofilfaser bei verschiedenen Einkopplungswinkeln
Die Wege sind verschieden lang, während die Lichtgeschwindigkeit jeweils die gleiche ist.



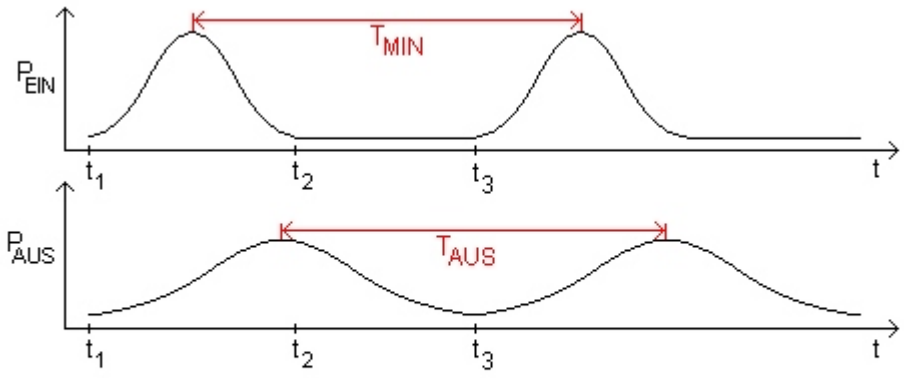
Verformung von Rechteckimpulsen aufgrund der Modendispersion



Maximale Einkopplungsfrequenz: $f_{max} = \frac{1}{T_{EIN}}$

Impulsverformung und Ineinanderfließen (Impulsnebensprechen)

Die Lösung für dieses Problems ist die Anpassung der Frequenz an die bei dem verwendeten Nachrichtenkanal (LWL) zu erwartende Signalveränderung, so dass die Signalpegel unterscheidbar bleiben:



Maximalfrequenz: $f_{max} = \frac{1}{T_{MIN}}$

An den Kanal angepasste Maximalfrequenz

Die maximal mögliche Frequenz ist diejenige, bei der wie in der oben dargestellten Abbildung kein Ineinanderfließen eintritt ($T_{min}=T_{aus}$). Die Aufweitung der Impulse ist proportional zur Länge des Leiters.

Chromatische Dispersion

Im Vakuum oder in Luft hängt die Lichtgeschwindigkeit nicht von der Lichtfrequenz ab.

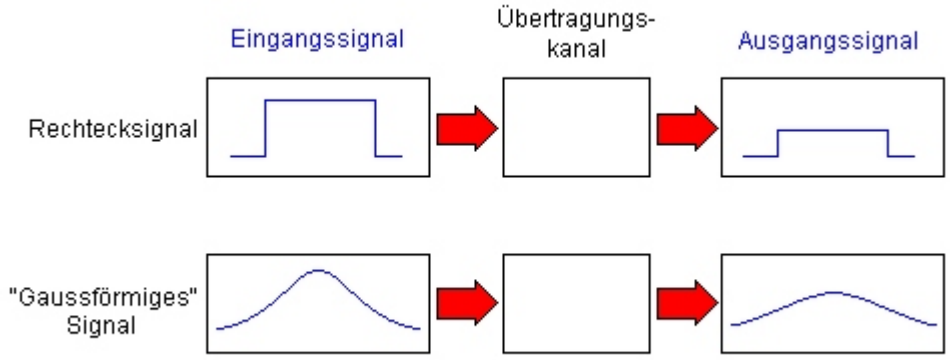
Es gibt aber Medien, in denen die Lichtgeschwindigkeit von der Frequenz abhängt; sie werden als dispergierende Medien bezeichnet. Zu ihnen gehört u. a. leider auch Glas (SiO_2).

Keine Lichtquelle erzeugt kurze Lichtimpulse genau einer Frequenz.

Chromatische Dispersion spielt deswegen auf Monomodefasern (siehe weiter unten) die entscheidende Rolle. Modendispersion hat man hier ja keine.

Dämpfung

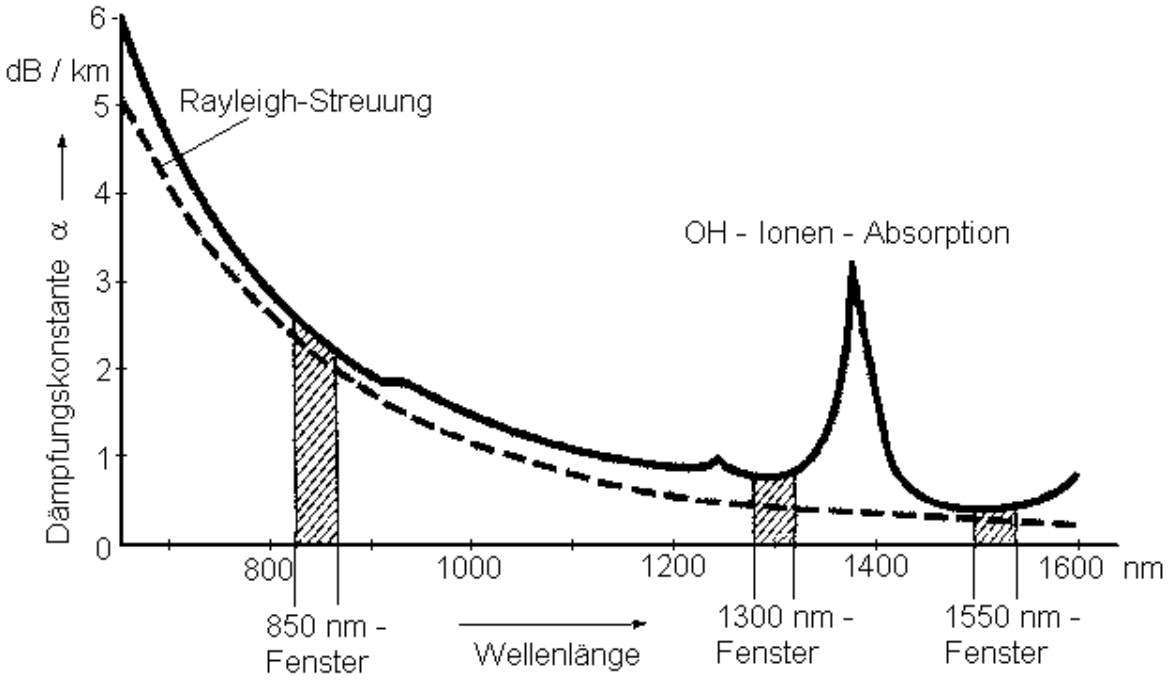
Im einfachsten Fall erfolgt lediglich eine Dämpfung des Signals, also idealerweise eine lineare Abschwächung.



Ideale Dämpfung von Signalen durch die Übertragung

Durch die Dämpfung wird die Übertragungsreichweite und gleichzeitig die Bandbreite begrenzt.

Leitermedien besitzen meist sogenannte "Transmissionsfenster" - das sind Wellenlängenbereiche mit besonders guter Durchlässigkeit. Für Glas liegt eines bei etwa 1550 nm, im Infraroten.



Qualitative Wellenlängenabhängigkeit der Dämpfungskonstante von Glas mit ungefähren Anhaltswerten

Der Betrag der Dämpfung hängt direkt von der Länge des Leiters ab.

Der Verlauf einer Dämpfung ist normalerweise nicht linear, sondern logarithmisch. Das ist leicht einzusehen, wenn man sich vorstellt, wie Dämpfung „funktioniert“.

Angenommen, von der eingehenden Leistung am Kabelanfang liegt nach 1000 m noch die Hälfte an. Von hier aus betrachtet, haben wir wieder eine Halbierung nach weiteren 1000 Metern. Also ein Viertel der Eingangsleistung.

Wäre der Verlauf linear, hätten wir dagegen nach 2000 Metern nichts mehr, wenn nach 1000 m schon die Hälfte verloren geht.

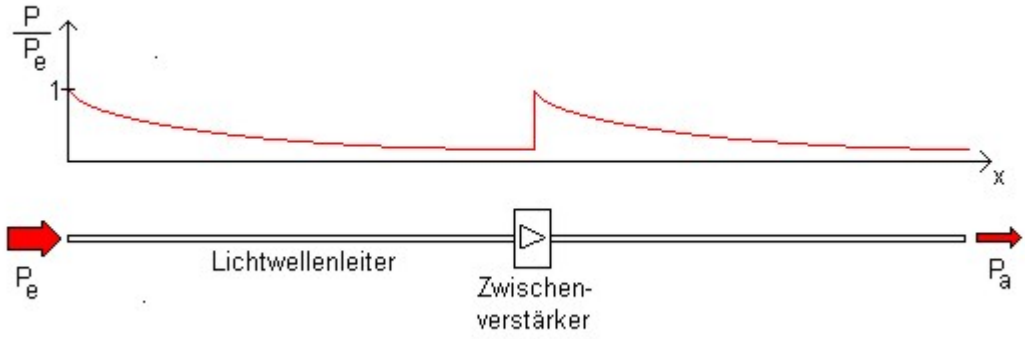
Wegen des exponentiellen Verhaltens wird die Dämpfung A logarithmisch in der "Einheit" Dezibel (dB) angegeben:

$A = 10 . \log (P_{ein} / P_{aus})$ dB

mit log als Zehnerlogarithmus und P als Lichtleistung.

Die auf die Länge L des Leiters bezogene Dämpfung heisst Dämpfungskonstante α:

$\alpha = (10 / L) . \log (P_{ein} / P_{aus})$ dB / km



Signalleistung P als Funktion der Leiterlänge x

Heutzutage (Frühjahr 2000) werden Werte für α von 0,2 dB / km erreicht.

Sensoren können mittlerweile die auf 1 % der eingekoppelten Leistung abgeschwächten Signale sicher verarbeiten. Nur noch alle 100 km ist eine Zwischenverstärkung notwendig.

Ein begrenzender Faktor war lange Zeit die Notwendigkeit, Verstärker einzusetzen, die nur elektrische Signale verarbeiten können. Das hatte zur Folge, daß bei jeder Verstärkung erst eine Umwandlung des optischen Signals in ein elektrisches stattfinden mußte. Anschließend folgte dann der umgekehrte Vorgang.

Dieses Umwandeln ist nicht beliebig schnell möglich, und so konnten die materialbedingt möglichen hohen Frequenzen gar nicht ausgenutzt werden.

Die entscheidende Verbesserung brachte ca. 1990 die Entwicklung erbiumdotierter optischer Faserverstärker , in denen tatsächlich das Lichtsignal beim Durchlaufen einer Faser verstärkt wird. Die Übertragungsgeschwindigkeit wird dabei nicht wesentlich beeinflusst.

Somit sind heutzutage Bandbreite-Länge-Produkte der Größenordnung mehrerer 100 Tbit/s) * km - also z.B. 1 TBit / s über mehrere hundert Kilometer - möglich.

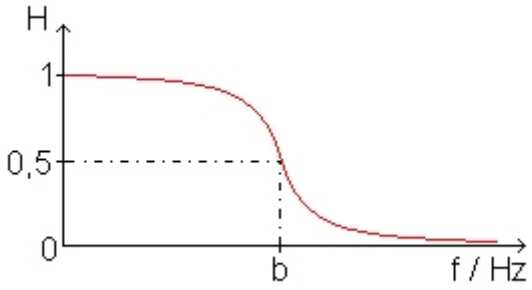
Was heißt jetzt Bandbreite-Länge – Produkt ?

Damit wird ausgedrückt, daß die übertragbare Bandbreite umgekehrt proportional zur Länge eines Lichtleiters ist. Also doppelte Länge – halbe Bandbreite usw.

Das Produkt aus Bandbreite und Länge ist bei einem bestimmten Leiter daher konstant und geeignet zu seiner Charakterisierung.

Bandbreiten und Übertragungsraten

Bandbreite



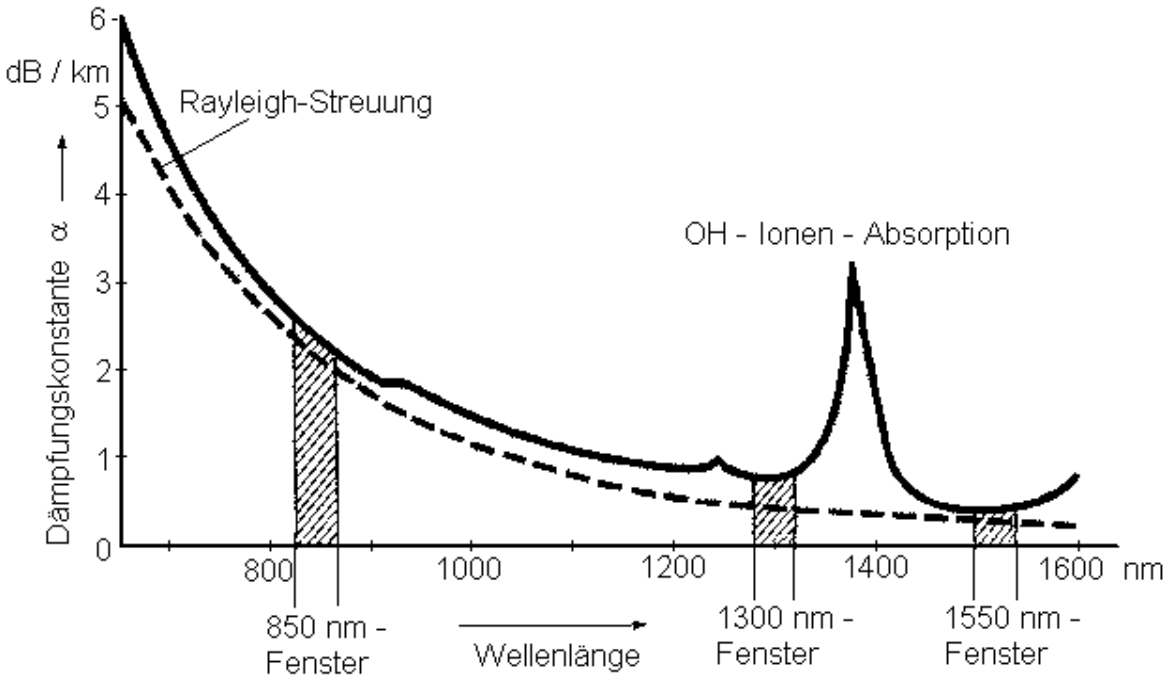
Die Bandbreite b ist diejenige Frequenz, bei der die Signalamplitude, also der Wert der Eingangsleistung, am Ausgang auf den Wert 0,5 abgefallen ist.

In diesem Zusammenhang ist oft vom – 3 dB Punkt die Rede. Ein Verhältnis Ausgangsleistung zu Eingangsleistung von 0.5 ergibt diesen Wert.

10 x log P_{aus}/P_{ein} = -3 dB

Optische Übertragungen

Auf optischen Kanälen existiert eine komplizierte, materialabhängige Dämpfung. Diese setzt sich aus Absorption und Streuung zusammen.



Qualitative Wellenlängenabhängigkeit der Dämpfungskonstante von Glas mit ungefähren Anhaltswerten

Aus der Auftragung der Dämpfung über der Wellenlänge geht hervor, dass die Wellenlängenfenster jeweils ca. 50 nm breit sind.

Die Bandbreiten dieser Fenster:

850 nm - Fenster: $\Delta\nu = 21 . 10^{12}$ Hz (21 THz)
1300 nm - Fenster: $\Delta\nu = 8{,}9 . 10^{12}$ Hz (8,9 THz)
1550 nm- Fenster: $\Delta\nu = 62 . 10^{12}$ Hz (62 THz)

Diese Werte der Bandbreiten sind um Faktoren 6200...21000 höher als bei elektrischen Kanälen (1 GHz).

Dies bedeutet allerdings nur, daß das Material diese Frequenzen prinzipiell ermöglicht.

Allerdings ist die große Bandbreite praktisch nicht ausnutzbar, da die auf optischen Kanälen auftretende Dispersion eine Herabsetzung der maximal möglichen Bandbreite zur Folge hat.

Die Bandbreite gilt also genaugenommen nur für eine Leiterlänge von Null. Das hat technisch natürlich keinen Sinn.

Mögliche Übertragungsraten und Entfernungen betragen z.B.:
(Stand Mitte 2000)

- 3,2 TBit / s über 40 km (Multiplexverfahren; s. Fibre Systems 3 (7) 9, Sept. 1999)
- 1 TBit / s über 342 km (Multiplexverfahren; s. Electronics Letters 35 (8) 648, April 1999)

- 40 GBit / s über 1000 km mit einem Kanal (s. Electronics Letters 35 (10) 823, Mai 1999) .
(Bei Multiplexverfahren werden mehrere Kanäle auf einer Übertragungsleitung genutzt.)

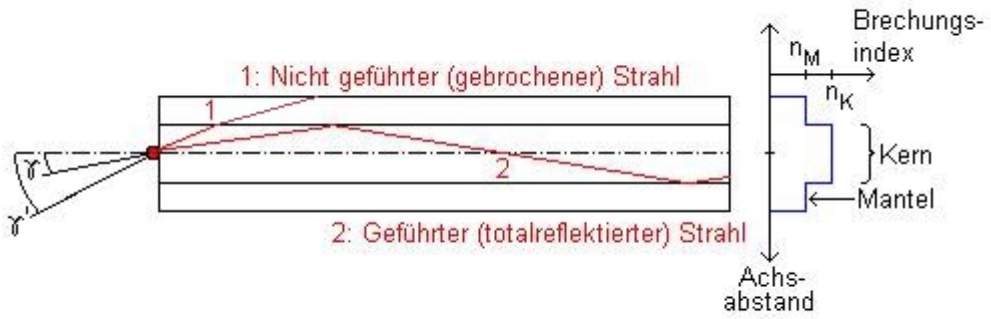
Typen und Bauformen von Lichtwellenleitern (LWL)

Multimode-LWL
- Stufenprofilfaser
- Gradientenprofilfaser

Monomode-LWL

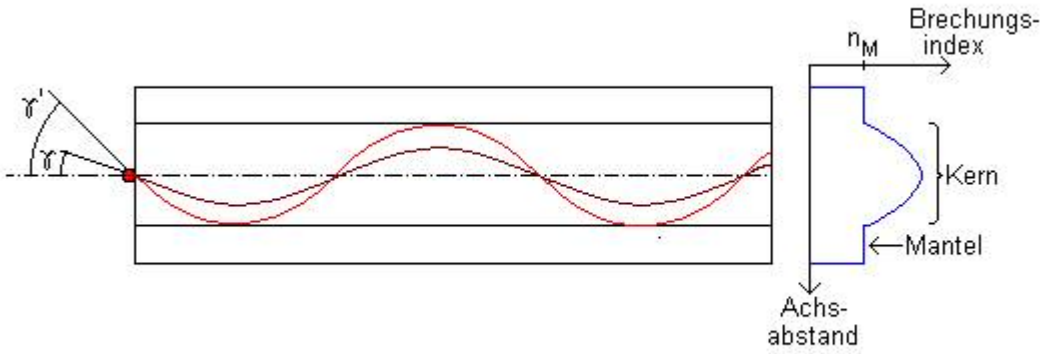
Multimode-Lichtwellenleiter

Stufenprofilfaser



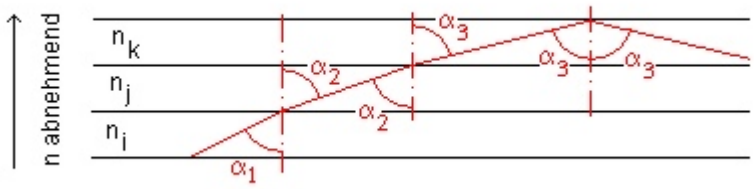
Stufenprofilfaser mit typischen Strahlen und Brechungsindexprofil.
Typische Maße sind: Kerndurchmesser 200 μm, Manteldurchmesser 280 μm

Gradientenprofilfaser



Gradientenprofilfaser mit typischen Strahlen und Brechungsindexprofil.
Typische Maße sind: Kerndurchmesser 50-62,5 μm, Manteldurchmesser 125 μm

Die gekrümmten Strahlenwege kommen zustande, weil die Strahlen beim Durchgang von einer Schicht zu nächsten - nach dem Brechungsgesetz - gebrochen werden:



Verlauf eines Lichtstrahls durch Schichten einer Gradientenfaser (qualitative Darstellung)

Von der Achse nach außen laufende Strahlen treffen auf Schichten mit geringerem Brechungsindex

Innen ist die Lichtgeschwindigkeit geringer als außen, daher ergeben sich für alle Strahlen ähnliche Laufzeiten trotz unterschiedlicher Weglängen.

Monomode-Lichtwellenleiter

Im Prinzip ist das auch eine Stufenindexfaser.

Der Unterschied: geringerer Kerndurchmesser: (10 μm)

Bei einer Wellenlänge des Lichts von 1550 nm = 1,55 μm beträgt der Kerndurchmesser also nur noch etwa das 6,5-fache der Wellenlänge. Das Verhältnis genügt, um das Entstehen verschiedener Moden zu unterbinden.

Die numerische Apertur von Monomodefasern ist natürlich deutlich kleiner als bei Multimodefasern: z.B. A_N = 0,12 (γ_a = 6,9°).

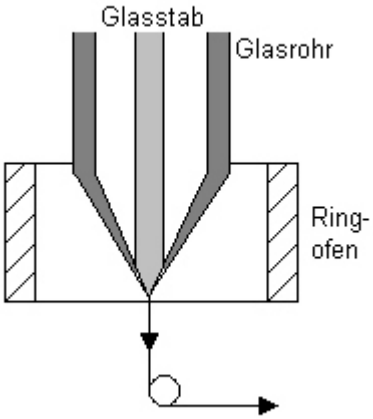
Heutzutage sind größenordnungsmäßig mehr als 100 (GBit / s)km - also beispielsweise 1 GBit/s über 100 km machbar.

Technisch möglich sind bereits mehrere (TBit/s)km, so dass in naher Zukunft die Einrichtung von Netzen dieser Kapazität erfolgen wird.

Herstellung von Lichtwellenleiterfasern

Stab-Rohr-Verfahren

Ein Glaszylinder, der innen je nach gewünschtem Brechzahlverlauf beschichtet worden ist, wird durch einen Ringofen gezogen. Dabei entsteht die Faser mit dem endgültigen Durchmesser.



Stabrohr-Verfahren

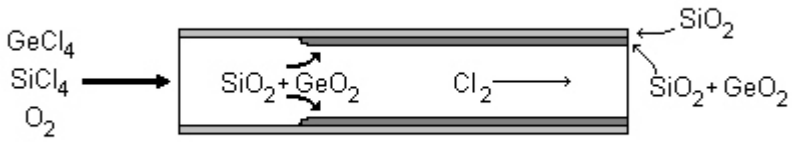
Herstellung von Gradientenfasern: Verfahren der Innenbeschichtung eines Glaszylinders. Der Zylinder wird innen mit den Schichten des gewünschten Materials bedampft.

Mittels Dotierung des Glasmaterials mit Germaniumdioxid kann der Brechungsindex des Glases (etwa 1,4) erhöht werden, bis etwa zu Werten von 1,9.

Die Herstellung der Gradientenfaser besteht aus drei Schritten:

1. Herstellung eines Hohlzylinders mit dem gewünschten Brechzahlprofil

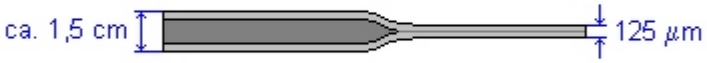
Innenbeschichtung des Hohlzylinders



2. Kollabieren des Hohlzylinders zu einem Zylinder (Vorform)

Kollabieren zur Vorform

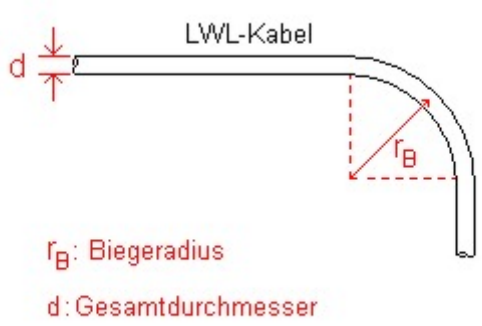
3. Ausziehen der Vorform zu einer Faser



Ausziehen zur Faser

Aus der ca. 1 m langen Vorform entsteht beim Ausziehen bei ca. 2000 °C eine Faser von mehreren Kilometern Länge. Um sie vor schädlichen Umwelteinflüssen zu schützen, wird sie sofort beim Austritt aus dem Ofen mit einer Kunststoffschicht ummantelt.

Verlegung von LWL-Kabeln



r_B: Biegeradius

d: Gesamtdurchmesser

Biegeradius von LWL-Kabeln

Typische Werte liegen bei 100 - 300 mm für die Verlegung.

Im Dauerbetrieb liegt der minimale Biegeradius etwa bei der Hälfte des jeweiligen Werts für die Verlegung eines Kabels.

LAN – Technologien

Diese spielen sich ab auf den OSI - Schichten 1, 2

Zum Einstieg ein paar Worte zu Übertragungsgeschwindigkeiten, Datenraten, Bandbreiten und der Frage, ob Bandbreite alles ist im Leben.

Übertragungsgeschwindigkeiten werden in Bits pro Sekunde angegeben. 1 Mbit/s sind übrigens 1000x1000 Bit/s, nicht 1024x1024, wie bei Speichergrößen oder Datenmengen.

1 Megabyte beispielsweise ist deshalb 1024x1024 Byte, weil in Zusammenhang mit Speichergrößen die ganze Rechnerei auf dem dualen Zahlensystem beruht. 2^{10} sind eben 1024 und nicht 1000.

1 Megabyte/s sind also, um die Verwirrung komplett zu machen, 1024x1024 (2^{20}) Byte/s. Hier ist nämlich von einer bestimmten Datenrate (Datenmenge, die pro Zeiteinheit übertragen wird) die Rede.

Die Datenrate ist nicht dasselbe wie die Übertragungsgeschwindigkeit. Abgesehen vom Unterschied zwischen Bytes und Bits ist, wie weiter unten noch gezeigt wird, nicht jedes übertragene Bit zu den Nutzdaten zu zählen.

Die verfügbare Bandbreite ist noch einmal was anderes. Sie bestimmt nichts weiter als die obere Grenzfrequenz, die höchstens übertragen werden kann. 100 MHz ist nicht etwa gleichzusetzen mit 100 Mbit/s.

Die tatsächliche Bitrate wird bei gegebener Bandbreite bestimmt durch die Codierung. Diese sieht im LAN ganz anders aus als etwa bei Modemverbindungen.

Schließlich noch eine Betrachtung zur Frage, ob höhere Übertragungsgeschwindigkeiten immer besser sind.

Nehmen wir zwei Standorte, die per WAN Standleitung verbunden sind mit 2 Mbit/s, eine Bandbreite, die verglichen mit LAN' s eher gering, aber üblich ist. Mit dem Auto erreicht man den jeweils andern Standort in einer Stunde.

An einem der Standorte haben sich durch Datensicherung 20 Terabyte Daten angesammelt, die zur Sicherheit verlagert werden sollen.

Die Übertragung via WAN – Leitung wäre möglich, dauert allerdings ein bißchen. 2 Mbit/s ergibt etwa 858 Mbyte/h. Macht für die 20 Tbyte eine Übertragungszeit von 24434 Stunden oder 1018 Tage.

Besser ist hier wohl der Transport auf Datenbändern per Auto, das dauert wie gesagt lediglich eine Stunde. 20 GB pro Band sind realistisch , 1000 Bänder werden ein einen normalen Kofferraum hineingehen.

Bei diesem Transport wird immerhin eine Datenrate von 20 TByte /h erreicht.
Statt 14,3 MByte/h sind nun also 20971520 MByte/h geboten.
Unsere WAN – Leitung müßte mit 2932031 Mbit/s (3 Mio Mbit/s) dagegen halten. Es wird sich in absehbarer Zeit wohl kein Anbieter dafür finden.

Warum aber nimmt man die langsame Leitung, wo man doch mit jedem Firmenauto eine ungleich höhere Datenrate erzielt ?

Zugriffsverfahren

Finden wir auf der OSI - Schicht 2

Mehr als einen Knoten hat man immer in einem Netz (sonst wäre es keins). Zugriffsverfahrens stellen sicher, daß sich die Daten der einzelnen Stationen auf dem Übertragungsmedium nicht überlagern.

Zugriffsverfahren können deterministisch oder nicht deterministisch (bzw stochastisch) sein.

Deterministisch. bedeutet, daß sich ein Vorgang bei Kenntnis seiner Einflußgrößen vollständig in seinem Ablauf bestimmen läßt.

Nicht deterministisch bedeutet, es sind zufallsgesteuerte Komponenten im Ablauf enthalten. Wie ein derartiger Vorgang ablaufen wird, läßt sich nicht vorhersagen

In Bezug auf Zugriffsverfahren heißt das:

Nicht deterministisch: Wer zuerst kommt, mahlt zuerst, es herrscht ein kontrolliertes Chaos. Dafür ist das Verfahren einfach, die Sendung wird bei Erkennung einer Kollision einfach wiederholt. Nachteile hat das bei vielen Stationen / hoher Auslastung, weil ab einer bestimmten Auslastung der Verkehr plötzlich so stark ansteigt, daß alles blockiert wird.

Deterministisch: Ein bestimmter Signalmechanismus sorgt dafür, daß immer nur eine Station auf Sendung geht. So gibt es auch bei hoher Auslastung keine gegenseitige Störungen. Die maximale Wartezeit, bis Senden möglich ist, kann eindeutig bestimmt werden (Umlaufzeit x (Anzahl Stationen -1)). Prioritäten für bestimmte Stationen sind möglich. Die Technik ist dafür komplizierter, der Anteil an Verwaltungsdaten größer.

Die zwei wichtigsten Zugriffsverfahren:Token Passing, CSMA/CD

Token Passing

Deterministisch. Ein definierter Datenrahmen, Token genannt, übergibt die Sendeberechtigung an eine bestimmte Station. Jede Station hat einen festgelegten Vorgänger sowie einen Nachfolger. Im Ring ist das automatisch der Fall, ansonsten erfolgt die entsprechende Regelung über Adressen.
Die sendewillige Station wartet vom Vorgänger auf das Token. Steht im Token das Besetzt- Bit auf 0, ist das ein Freitoken. Dieses wird vom Netz genommen, durch ein Token mit Besetzt Bit auf 1 ersetzt. Der Datenrahmen bekommt noch Ziel- und Absenderadresse sowie die eigentlichen Daten angehängt und wird auf die Leitung geschickt.

Alle Unbeteiligten leiten das Besetzt -Token weiter. Der, dessen Adresse drinsteht, setzt das Receive Bit, kopiert die Daten für sich und setzt dabei das Copy – Bit. Der Absender empfängt wieder sein eigenes Token mit den geänderten Bits (Receive, Copy), nimmt es vom Netz und ersetzt es durch ein neues Freitoken

Einige Regeln sind noch erforderlich:

Eine Station, die nach Datensendung ein Freitoken generiert, darf dieses nicht gleich wieder selbst nutzen. Dies ist dem Nachfolger vorbehalten. Braucht er es nicht, gibt er es seinerseits seinem Nachfolger usw.

Bestimmte Probleme erfordern eine Wächterfunktion. Hinzufügen oder Wegnahme einer Station sorgt für eine Änderung der Reihenfolge. Eine Station, die nach dem Senden ausfällt, kann kein Freitoken mehr erzeugen. Das muß nach einer gewissen Wartezeit der Wächter übernehmen, ebenso die Herausnahme von Daten für nicht erreichbare Empfänger

CSMA/CD

Nicht deterministisch. Carrier sense multiple access / collision detection

Carrier Sense: Die sendewillige Station überprüft Netzaktivität. Sie wartet, wenn Verkehr vorhanden ist.

Kein Verkehr: Nach definierter Wartezeit wid gesendet.

Anschließend erfolgt Prüfung, ob Überlagerung (collision) mit anderer zeitnaher Sendung stattfindet.

Bei Kollision erfolgt Abbruch der Sendung, Ein JAM – Signal für bestimmte Zeit als Info für andere wird generiert. (jam = blockieren)

Neue Sendung startet nach einer zufällig berechneten Zeit.

Die Kollisionserkennung geschieht über Spannungspegel. Bei Überlagerung zweier Signale ergeben sich naturgemäß doppelt so hohe Spannungswerte wie normal. Die Kollisionserkennung ist also ein rein analoges Verfahren.

Bei CSMA/CD ist keine Vorhersage möglich, wann gesendet werden kann. Viele Stationen, viel Verkehr – viele Kollisionen. Ab etwa 30 % Auslastung steigen durch überproportionale Zahl der Sende - Wiederholungen die Kollisionen so stark an, daß nichts mehr geht. Eine Priorisierung bestimmter Teilnehmer oder Daten ist allein mit diesem Verfahren nicht möglich.
CSMA/CD – Netze sind aufgrund ihrer Einfachheit stark verbreitet. Bestimmte Dienste, die doch Priorität benötigen, sind schwierig zu realisieren. Für diese Problematik hat man den Begriff QoS (Quality of Services) erfunden. Es sind in diesem Zusammenhang zusätzliche Protokolle erforderlich. Bei Token dagegen würde ein zusätzliches Bit genügen.

Ein Beispiel dafür ist Voice over IP (VoIP). Sprachverbindungen vertragen keine Verzögerungen, wenn am anderen Ende noch etwas verständlich ankommen soll. Die zugehörigen Datenpakete müssen also unter allen Umständen sofort durch das Netz geschleust werden.

LAN - Standards

Schichten 1 und 2

Hauptsächlich wird mittlerweile Ethernet eingesetzt, bei neu zu installierenden LAN' s Netzen praktisch ausschließlich.

Token Ring existiert vielfach noch, weil ein gut funktionierendes Netz natürlich ungern komplett ausgetauscht wird, nur um die Technologie zu wechseln.

Token Ring

Standardisiert als IEEE 802.5

Die Bezeichnung Token Ring ist eine Mischung aus Topologie und Zugriffsverfahren. Nämlich Token Passing und Ringtopologie.

Es stammt von IBM, die Ringleitungsverteiler werden sternförmig verkabelt, STP – Kabel kommt zur Anwendung. Das ist sonst nicht so üblich, die Masse der Verkabelung ist UTP.

Das Original arbeitet mit 4 Mbit/s, die spätere Version mit 16 Mbit/s und einer Abwandlung im Zugriffsverfahren. Sofort nach Sendung von Daten wird ein Freitoken generiert, es können also gleichzeitig mehrere Freitoken auf dem Ring existieren.

Ethernet

Standardisiert als IEEE 802.3

Xerox brachte 1976 ein System mit CSMA/CD und 2,94 Mbit/s, das Ethernet genannt wurde.

Ether ist übersetzt Äther.

Der Äther wurde in der Frühzeit der Physik als Fortpflanzungsmedium für elektromagnetische Wellen vorausgesetzt in Analogie zu Luft als Medium für Schallwellen oder Wellen im Wasser. Wellenausbreitung ohne Medium schien nicht möglich.
Bei elektromagnetischen Wellen war so ohne weiteres kein Medium zu finden. Diese konnten sich auch im Vakuum ausbreiten. Um das Paradoxon zu umgehen, griff man zu dieser Modellvorstellung eines Mediums, eben dem Äther, der alles durchdringt.

Alle Versuche, diesen Äther zu finden, scheiterten. Seit 1887 weiß man, daß es wirklich auch im puren Vakuum geht, der Äther als Modellvorstellung wurde unnötig

Hier beim Ethernet ist das Kabel das Fortpflanzungsmedium, und als solches betrachtet fand man den Äther im Namen offensichtlich sehr hübsch.

Dieses Ethernet war erfolgreich genug, daß sich Xerox, Intel und DEC später auf einen Standard für 10 Mbit Ethernet einigten. Darauf basiert 802.3.

Verschiedene Kabeltypen im Ethernet sind spezifiziert.

10Base5

Thick Ethernet. Ursprüngliche Ethernetvariante, ein gelbes Kabel (sieht ähnlich aus wie Gartenschlauch), Transceiver (Elektronik für Träger- und Kollisionserkennung) wird auf das Kabel aufgesetzt mit einer Vampirklemme, der Controller sitzt extra in Netzwerkkarte. Die Segmentlänge beträgt maximal 500m

Ganz ausgestorben ist diese Bauform nicht, Transceiver (siehe unten) kann man heute noch kaufen.

Alle heutigen Techniken vereinen Transceiver und Controller in der Netzwerkkarte.

10Base2

Thin Ethernet, dünnes Koaxkabel mit T- Stücken und BNC – Steckern. Maximale Segmentlänge 200 m

10BaseT

Das Kabel beinhaltet verdrillte Kupfer Adernpaare (Twisted Pair). Der Bus liegt innerhalb des Verteilers, dem Hub oder Switch. Die angeschlossenen Kabel sind die Bus - Abzweigungen. So sieht der Bus aus wie ein Stern. Die maximale Segmentlänge ist hier 100m.

10BaseF

Gleiche Spezifikation wie 10Base T, das Medium ist aber Glasfaser. Verwendet zur Überbrückung größerer Entfernungen bis 2000m und zur Vermeidung von Störungen durch elektromagnetische Einwirkungen.

Der Datenrahmen im Ethernet

Schicht 2 (Sicherungsschicht / Data Link Layer)

Der Bitstrom aus der Schicht 1 muß unterteilt werden in sogenannte Rahmen. Diese können in der Sicherungsschicht auf Fehler untersucht und bei Bedarf korrigiert werden

Hier spielt auch die Netzwerkkarte mit. Teure Karten machen den Rahmen selber, die Funktionalität ist dann als Hardware (eigener Prozessor) vorhanden. Billige Netzwerkkarten verlagern den Vorgang auf die Software/Treiber, belasten natürlich die CPU damit.

Netzwerkkkarten spielen also in den OSI - Schichten 1 und 2.

Wie sieht nun der Ethernet - Datenrahmen aus ?

Die gesamte Länge darf variieren von 64 bis 1518 Byte. Im einzelnen beinhaltet ein Etherntrahmen die folgenden Bestandteile:

Präambel, 7 Byte, 1/0 im Wechsel, endet mit 0. Synchronisation des Taktes.
Rahmenstart, Bitfolge 10101011, 1 Byte
Zieladresse, 6 Byte
Quelladresse, 6 Byte
Angabe der Länge der Daten, 2 Byte
Eigentliche Daten, bis 1500 Byte
Pad, 0-46 Byte, füllt das Datenfeld so weit auf, daß mindesten 64 Byte Rahmenlänge (von Zieladresse bis einschl. Prüfsumme) herauskommt.
Prüfsumme, 4 Byte

Die Rahmenlänge hängt zusammen mit der Ausbreitungsgeschwindigkeit (etwa 2/3 c_v im Kabel) und der Segmentlänge der Kabel, damit die Kollisionserkennung funktioniert. Deshalb gibt es auch eine minimale Länge, nicht nur eine maximale.

Wenn zwei kurze Rahmen auf ein Segment geschickt werden, kann es bei zu großer Entfernung der beteiligten Stationen nämlich passieren., daß beide Rahmen bereits unterwegs sind, ohne zu kollidieren, nachdem die Kollisionserkennung auf den Stationen beendet worden ist.

Fast Ethernet

Das grundlegende Konzept ist, alles vom 802.3 – Standard zu erhalten und nur die Bitzeit auf 1/10 zu reduzieren. Damit hat man 100 Mbit/s.

Das führt allerdings zwangsläufig auch zu einer Reduzierung auf 1/10 bei den Kabellängen. Die bereits vorhandenen UTP – Verkabelungen waren allerdings so verbreitet und vorteilhaft, daß es galt, diese verwendbar zu halten, und zwar mit den bisherigen Kabellängen.

Hubs (einfache Verteiler ohne Eigenintelligenz), Vampirklemmen und BNC – Kabel sind dabei nicht mehr zulässig.

Bei UTP – Kabeln der Kategorie 3 ist die Nutzung dann möglich, wenn vier statt zwei Kabelpaare für eine Verbindung genutzt werden. Meistens waren diese vorhanden, eine Hälfte für das Telefon, das andere für Netzwerk. Das Telefon mußte da dann ausweichen.

Die genaue Bezeichnung dieser Medien: 100BaseT4

Die andere Variante. Kategorie 5, da sind die Kabel eletrisch so ausgelegt, daß zwei Paare ausreichen. Diese heißen 100BaseTX, X für Vollduplex (= gleichzeitig Datenfluß in beiden Richtungen möglich)

Dann gibt es noch die Glasfaservariante 100BaseFX.

In der Regel werden alle drei Fast Ethernet – Kabelverbindungen 100BaseT genannt (auch wenn die Glasfsern natürlich nicht twisted sind).

Gigabit Ethernet

Auch hier handelt es sich um eine Erweiterung des 802.3 Standards. Bis auf die nochmals um den Faktor 10 erhöhte Bitrate bleiben die Kenngrößen also gleich.

Hohe Ansprüche werden natürlich an die Verkabelung gestellt. Kategorie 3 ist out, Kat 5 mit max 25 Metern (statt 100) sowie Nutzung aller Adern (2x4).

Hauptsächlich ist Gigabit Ethernet für Glasfaser ausgelegt. Multimodefasern reichen 500 m, Monomode 2 km. (Backbone).

Übertragungskomponenten im Netzwerk

MAC – Adressen

Schicht 2

Jede Netzwerkkarte hat eine weltweit eindeutige Hardwareadresse. Diese wird letztlich bei jeglicher Netzwerkkommunikation angesprochen. Kommt ein Paket an mit der eigenen MAC- Adresse im Header, wird es angenommen, ansonsten verworfen. Auch dieser Vorgang kostet Rechenleistung, die von besseren Netzwerkkarten in Eigenregie übernommen werden kann.

Hardwareadressen haben ein 48 Bit - Format, Die Schreibweise ist üblicherweise in 6 zweistelligen Hexadezimalzahlen, z. B. 00 2C 67 34 00 1A. Die ersten drei sind der Herstellercode. Der Rest für die interne Adresse.

Repeater

Ein Repeater wiederholt alle Signale, die er empfängt. Daher der Name. Ein wirklicher Repeater gibt sich aber nicht damit zufrieden.

Normalerweise sind auf einer physikalischen Leitung analoge, aber binär interpretierte Signale unterwegs, die empfangen werden.

Das Mindeste ist, diese zu verstärken, um die Dämpfungsverluste auf dem bisherigen Weg zu kompensieren. Das wäre bei analogen Signalen auch die sinnvolle Strategie.

Letzlich sind natürlich Signale auf einem Kabel wie gesagt immer analog. Es ist ein Verlauf von Spannung und Strom.

Allerdings wird durch simples Verstärken auch alles mitverstärkt, was sich an Störimpulsen auf dem bisherigen Weg dazugesellt hat. Ein paar Möglichkeiten hat man hier zwar durch den Einsatz von Filtern. Aber das ürsprüngliche Signal wird niemals mehr hundertprozentig wiederhergestellt.

Bei der Digitaltechnik haben wir aber (Rechteck-) signale, die als Bits interpretiert werden. Dabei gibt es bestimmte Grenzen, die vorher festgelegt sein müssen.

Entspricht beispielsweise 1 einem Pegel von 5 V, 0 einem Pegel von 0 V, so muß man lediglich definieren, in welchen Grenzen ein Pegel noch als und wann als 1 interpretiert werden soll.

Also etwa alles unter 2V = 0, über 3V = 1. Die Übertragungsleitung muß also, bevor aufgrund der Verluste das Signal nicht mehr eindeutig zu interpretieren ist, einen Repeater vorsehen oder zu Ende sein.

(Übertragen wiird nicht wirklich direkt die Bitfolge als elektrisches Signal, sondern es erfolgt eine Codierung zwecks Eindeutigkeit, genaueres dazu später)

Der Repeater kann aufgrund der digitalen Natur des Signals mehr tun als einfach verstärken: Stattet man ihn mit einer Schaltung aus, die Rechteckspannungen erzeugt, können die Signale praktisch wieder in den Originalzustand versetzt werden.

Immer wenn das ankommende Signal aufgrund der Spannung als 1 erkannt wird, kann ein Rechteck mit 5 V erzeugt werden usw. Das Eingangssignal hat dann nur noch die Funktion eines Triggers (ähnlich wie beim Oszilloskop) für den Rechteckgenerator.

Die genaue (verfälschte) Form des Eingangssignals wird also nicht weitergesendet, sondern ein komplett aufgefrisches Bit.

Das ist ein großer Vorteil digitaler Datenübertragung und eine wesentliche Triebfeder für das Bemühen, auch eigentlich analoge Dinge wie Bild- und Toninformationen zu digitalisieren, selbst wenn der Aufwand groß ist. Die Weiterverarbeitung gleich welcher Art hat keine Qualitätsverluste mehr zur Folge.

Ein Repeater ist in Ethernet – Netzen kaum noch als separates Bauteil anzutreffen. Vielmehr findet man ihn integriert in den folgenden Komponenten, die ohnehin zur Verkabelung benötigt werden.

Hub

Ursprüngliche Form des Netzwerkverteilers im Ethernet. Der Bus ist keine Leitung mehr, sondern der elekronische Kasten, aus dem die Abzweige als eigentliche Kabel sternförmig abgehen. Im Hub ist das eine reine Parallelschaltung. Ein Signal, das von einer Maschine kommt, erscheint so an allen Anschlüssen gleichermaßen. Jeder am Hub angeschlossene Partner erhält das Paket und verwirft es, nur der Empfänger

nimmt es an. Daher müssen sich alle die Bandbreite (10 oder 100 Mbit/s) teilen, die das Netz zur Verfügung stellt.

Switch

Sieht aus wie ein Hub, macht oberflächlich betrachtet auch nichts anderes. Ausnahme: Er lernt im Betrieb MAC – Adressen der angeschlossenen Geräte. Das versetzt ihn in die Lage, die Daten von vornherein nur an die richtgen Adressaten zu schicken. Es ist also auch immer nur auf der betroffenen Leitung (Port) Verkehr, was Kollisionen vermeidet und die volle Leitungskapazität (Bandbreite) jedem exklusiv zur Verfügung steht. So lange die Backplane (dahinter stehende Elektronik) genug Bandbreite bietet.

Im Prinzip läuft es darauf hinaus, daß jeder Teilnehmer sein eigenes Ethernet – Segment bekommt. Das eliminiert zwangsläufig alle Kollisionen.

CSMA-CD (Kollisionserkennung) ist deshalb auf dem Kabel gar nicht mehr nötig. So sind LWL nicht mehr auf maximal 2 km beschränkt. Im Gegensatz zu den Kupferkabeln beruht diese Grenze nämlich nicht auf Verlusten der Signalqualität durch Dämpfung und Dispersion. Vielmehr wird bei größeren Segmenten die Kollision bei kleinen Paketen nicht mehr rechtzeitig erkannt, wenn zwei Stationen nahezu gleichzeitig senden.

Aber auch Kupferleitungen profitieren. Wegen der zwei Adernpaare, die standardmäßig in einem Kabel enthalten sind, kann der Datenverkehr im Vollduplexmodus (beide Richtungen zugleich) stattfinden. Im herkömmlichen Ethernet wurde das zweite Adernpaar für die Zwecke der Kollisionserkennung gebraucht.

Patchpanel, Patchfeld

To patch: flicken

Das Patchfeld vereinfacht die Organisation (neudeutsch das Handling) der Netzverkabelung. Es befindet sich im Schaltschrank, wo auch der Hub / Switch eingebaut ist.

In den Wänden irgendwo im Gebäude sind Netzwerkbuchsen eingelassen, an denen die Benutzer ihre Rechner anstöpseln.

Die Wanddosen sehen etwa so aus wie in der obigen Abbildung. Jeder Anschluß hat eine eindeutige Nummer. Das hier angeschlossene Kabel geht von der Buchse aus durch das Gebäude und endet an einem der Anschlüsse im Patchfeld. Dieser Port des Patchfeldes hat dieselbe Nummer wie der Port in der Wandsteckdose.

Jetzt kann bei Bedarf der Anschluß im Patchfeld mit irgendeinem Port des Switches verbunden werden, und die zugehörige Wanddose hat Verbindung zu allen anderen Rechnern, die ebenfalls am Switch angeschlossen sind.

Router

Schicht 3

Router haben nichts zu tun mit MAC – Adressen. Sie arbeiten auf der Ebene der logischen Adressen. Auf dieser Ebene werden Segmente/Subnetze gebildet. Die Weiterleitung bzw Wegfindung im Verbund mehrerer Subnetze ist die Aufgabe der Router.

Genaueres dazu folgt später noch bei TCP/IP

LAN Switching

Geräte, die heutzutage als Switches bezeichnet werden, sind in Wirklichkeit oft viel mehr. Der Trend zu wenig Nutzern pro Segment ist mittlerweile so weit gediehen, daß nur noch ein einziger Benutzer pro Segment existiert.

Obwohl Switches prinzipiell auf der Schicht 2 zu Hause sind, verfügen viele auch über Funktionalitäten auf Layer (gleichbedeutend mit Schicht) 3.

Jeder Nutzer hat damit unmittelbaren Zugriff auf die volle Bandbreite, diese muß nicht mehr wie beim Hub mit allen Beteiligten geteilt werden.

Ein 24 – Port Switch bildet also 24 Ethernet – Segmente, die intern miteinander verbunden sind. Das verhindert vollständig Kollisionen, die normalerweise auf gemeinsam genutzten Medien auftreten.

Ein gemeinsam benutztes Medium gibt es praktisch nicht mehr.

Intern wird eine Switching – Tabelle angelegt, so daß mit deren Angaben die Rahmen am richtigen Port (mit der passenden MAC – Adresse) ausgegeben werden.

Die Switching Methode mit Speichern und Weiterleiten kopiert den gesamten Datenrahmen in einen internen Pufferspeicher und berechnet eine zyklische Blocksicherung (CRC). Bei Fehler oder wenn der Rahmen zu groß (> 1518 Byte) bzw zu klein (< 64 Byte) ist, wird der Frame abgelehnt.

Die durchgehende Switching Methode ist schneller, weil nur die Zieladresse kopiert wird. Dann wird sofort der Ausgangsport mittels Weiterleitungstabelle bestimmt und der Rahmen durchgegeben.

Die Layer 3 – Funktionen, die angeboten werden, ermöglichen das Segmentieren von Netzen ähnlich wie bein klassischen Routing, das auf der Ebene der logischen Adressen (IP) arbeitet.

Zunächst konfiguriert man sogenannte virtuelle LAN' s (VLAN). Das bedeutet, daß der Netzverkehr für unterschiedliche Aufgaben aufgeteilt wird. Bestimmte Ports aller beteiligten Switches gehören zu einem VLAN, in dem sich vielleicht nur die Druckdienste bewegen. Zwischen VLAN' s gibt es erst einmal keine Kommunikationsmöglichkeit.

Wer zu welchem VLAN zählt, wird auf der Schicht 2 geregelt. Soll von einem VLAN zum anderen Verkehr möglich sein, muß das durch Routing geschehen. Das heißt aber, daß Mitglieder unterschiedlicher VLAN' s auch unterschiedlichen Subnetzen der Schicht 3 (logische Adressierung, siehe Kapitel TCP/IP) angehören müssen.

Dann kann das Routing auch im Switch integriert sein

Switches, die auf mehreren Ebenen arbeiten, sind Multilayer Switches.

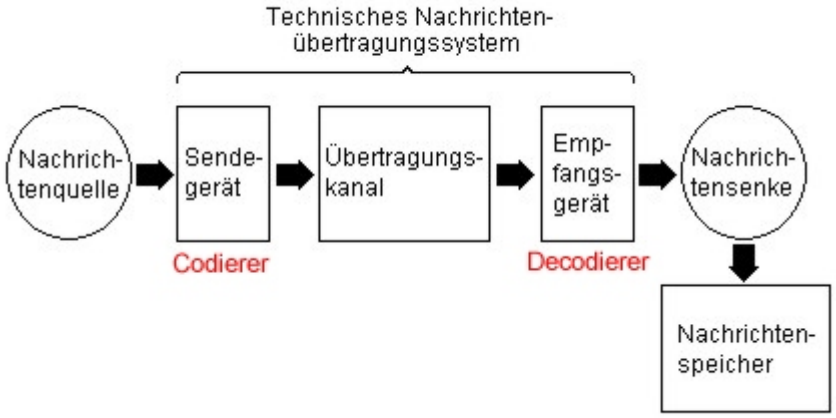
Teil 2: Kommunikationstechnik

Der Übertragungskanal

Technisches Kommunikationsmodell

Die Übertragung einer Nachricht erfordert in aller Regel eine Anpassung an den verwendeten Übertragungskanal. Also die Umformung in Signale, die der Übertragungskanal transportieren kann.

Den Vorgang der Umformung nennt man Codierung. Die Rückwandlung in die Form, die der Empfänger versteht, ist demzufolge die Decodierung.



Einige Begriffe zum Übertragungskanal

Vielfach werden für die Datenübertragung Leitungen verwendet, die ursprünglich für analoge Signale konzipiert waren (vor allem Telefonnetze).

Auch wenn wir immer von digitalen Daten reden, sind letztlich alle Übertragungen analoger Natur und unterliegen den daraus resultierenden Einschränkungen.

Digital werden die Signale erst durch die entsprechende Interpretation.

Um Datenverluste auf dem Übertragungsweg zu verhindern, müssen die Eigenschaften des Kanals und mögliche Übertragungsstörungen berücksichtigt werden.

Dies geschieht beim Sendegerät durch die Codierung.

CRC

CRC heißt zyklische Blocksicherung, cyclic redundancy check.

Eine mathematische Funktion wird dabei auf eine größere Anzahl Bits angewendet, das Ergebnis ist eine Prüfsumme.

In der Regel werden 16 oder 32 Bit – Blöcke verwendet.

Diese Prüfsumme wird an die Daten (also den Block aus 16 oder 32 bit) angehängt. Der Empfänger benutzt im Prinzip dieselbe Berechnung auf den Datenteil, also die ersten 16/32 Bit des Gesamtpakets, ohne die Prüfsumme.

In Wirklichkeit handelt es sich um komplizierte Polynomberechnungen. Das genaue Verfahren resultiert aus mathematischen Überlegungen, da letztlich eine genau definierte Sicherheit erforderlich ist, daß die Ergebnisse auch wirklich Fehler anzeigen und nicht selber irreführend sind.

Das Grundprinzip ist aber einfach: Der Datenblock bzw dessen Wert wird multipliziert. Das Ergebnis ergibt die angehängte Prüfsumme. Empfängerseitig dividiert man den Wert der Prüfsumme durch den Wert der Daten. Bleibt ein Rest, war die Übertragung falsch.

Beispiel:

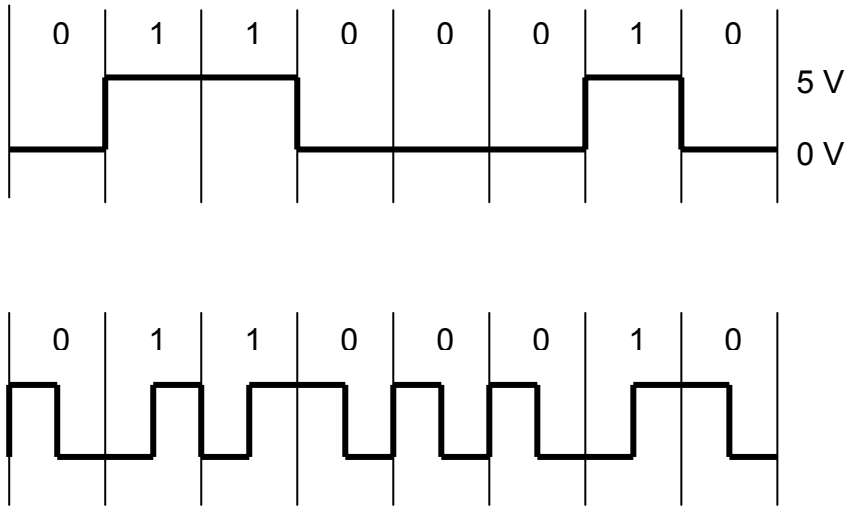
Sender:
12 wird losgeschickt, multpliziert mit 3, ergibt 36. 36 wird als Prüfsumme angehängt.

Empfänger:
36:12 ergibt 3 ohne Rest. Okay.
35:12 (falsche Prüfsumme), 36:11 (falscher Datenblock) oder 35:11 (beides falsch) ergibt einen Rest ungleich 0. Fehler

Codierung beim Ethernet

Manchester – Codierung

Um empfangsseitig bei einer Datenübertragung die eindeutige Erkennbarkeit der einzelnen Bits sicherzustellen, auch wenn mehrere gleiche Bits aufeinanderfolgen, ist die Definition der Zustände 0 und 1 über Spannungspegel nicht sehr geeignet.



Eine Aufeinanderfolge von gleichen Bits bedeutet eine konstante Spannung, hier entweder 0 oder 0,7 V .

Konstant 0 V hätte man aber auch bei Ausfall der Datenübertragung.

Sicherer wird die Erkennung, wenn jedes Bit durch einen Spannungswechsel definiert ist. Beispielsweise eine ansteigende Flanke für 1 und eine fallende für 0. Dies realisiert die Manchestercodierung. Der Wechsel zwischen den Pegeln erfolgt wenn notwendig zwischen den Taktzyklen, wo keine Auswertung erfolgt

Der Takt bestimmt den Zeitpunkt, wie lange ein Bit „dauert". In der Mitte dieser Periode wird die Flanke als Bit ausgewertet..

Der Takt muß deshalb in aller Regel „mitgeliefert" werden. (siehe Präambel beim Ethernetrahmen). Im Ethernet haben wir auch nicht mehr die 5V der „klassischen" Digitaltechnik, sondern Pegel von ± 0,7 V.

Baudrate versus Bitrate

Beide werden oft gleichgesetzt, was selten stimmt.

Baud: Beschreibt die reine Signalgeschwindigkeit = wie oft das Signal pro Sekunde seinen Spannungswert ändert. Nur abhängig von der oberen Grenzfrequenz, die man übertragen kann.

Bit/s = Baud gilt dann, wenn pro Signalwechsel nur ein Bit übertragen würde. So wie im Bild oben bei der Manchestercodierung. Es gibt lediglich zwei verschiedene Spannungswerte, und ebenso zwei digitale Zustände 0 und 1.

Üblich ist diese Einfachheit nicht immer. Normalerweise wird versucht, möglichst viele eindeutig unterscheidbare Zustände im analogen Signal zu definieren. Jedem Zustand kann dann ein Zahlenwert zugeordnet sein.

Je langsamer die Verbindung, umso größer sind natürlich derartige Bemühungen.

Ein Beispiel: Mit acht Spannungsstufen (bzw 0,1 ...7 V) wären beispielsweise 3 Bit pro Signalwechsel bzw Takt möglich. Warum 3 Bit ?

Drei Bits sind erforderlich, um bis 7 zu zählen. 7V wäre dann dezimal 7, binär 111, 6 entspricht 110 usw. Das heißt, damit kann man den Bereich einer dreistelligen Dualzahl (macht also 3 Bit) genau abbilden.

Modulation

Eine angewandte Methode bei analogen Verbindungen ist die Modulation. Telefonleitungen z.B. sind nicht in der Lage, Gleichspannungen zu übertragen. Daher sind einfache Spannungsstufen für die Darstellung digitaler Zustände hier ungeeignet.

Die digitalen Werte müssen mit Signalen definiert sein, die der Kanal verträgt. Das sind etwa bestimmte Frequenzen oder Phasensprünge.

Modulationsverfahren

Auch bei der Datenübertragung bedient man sich oft wie gesagt aus technischer Notwendigkeit analoger Signale. Beispielsweise, indem die Zustände 0 und 1 durch zwei verschiedene (Ton-) Freqenzen dargestellt werden.

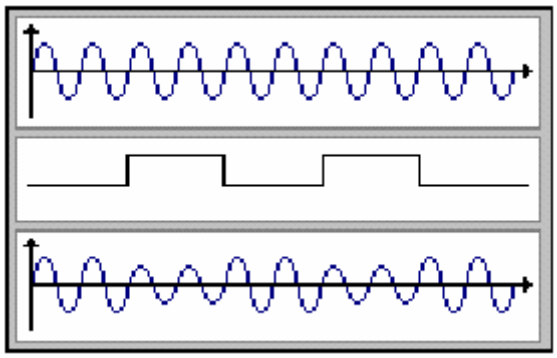
Ein Sinuston konstanter Frequenz, der Träger, wird moduliert in Abhängigkeit einer Signalspannung. Moduliert, also verändert werden können hierbei Frequenz, Amplitude und Phasenlage.

Bei der klassischen Modulation wird der Träger innerhalb eines bestimmten Bereiches, dem Amplituden-, Frequenz-, oder Phasenhub, kontinuierlich verändert in Abhängigkeit eines analogen Eingangssignals. Das ist das verwendete Verfahren beim AM- (Lang-, Mittel-, Kurzwelle) bzw FM (UKW) – Rundfunk.

In der digitalen Welt ist der Frequenz- oder Phasenhub sozusagen der Abstand zwischen zwei Eckwerten, etwa Frequenzen bei FM. Deshalb ist hier eher die Rede von Umschalten / Shifting. 0 wäre also beispielsweise der untere Wert, 1 der obere und es gibt keinen kontinuierlichen Hub, keine Zwischenwerte.

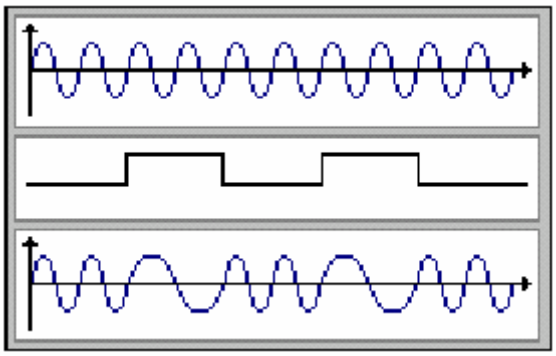
In den Bilddarstellungen sind jeweils drei Signale abgebildet. Oben der Träger, in der Mitte das Signal, unten der modulierte Träger.

AM, Amplitudenmodulation



Sehr störanfällig, wie man leicht beim Mittlewellen- und Kurzwellenrundfunk hören kann. Jede Störung ändert ja die Amplitude. Für Datenübertragung deswegen wenig brauchbar

Frequenzmodulation, FM, eigentlich FSK (frequency shift keying)



FSK ist wie gesagt eine Sonderform der Frequenzmodulation.

Störungsanfälligkeit gering. Störungen der Amplitude werden ja nicht ausgewertet, falsche Frequenzen können ausgefiltert werden. Gut hörbar an der Qualität beim UKW – Rundfunk.

Den beiden binären Zuständen werden zwei verschiedene Frequenzen (1000, 2000 Hz, Sinuswellenträger) zugeordnet, die innerhalb der Bandbreite des Kanals (3000 Hz) liegen.

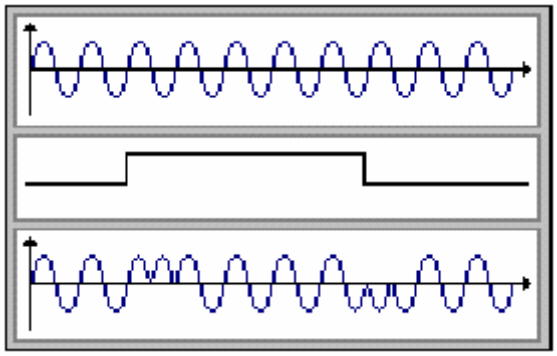
Zwischen diesen beiden Frequenzen wird umgeschaltet, je öfter, umso höher natürlich die mögliche Bitrate.

Aber auch hier ist die Übertragungsrate bestimmt durch die maximale Grenzfrequenz. Diese sorgt dafür, daß nicht beliebig oft umgeschaltet werden kann, obwohl beide Frequenzen eindeutig innerhalb der Bandbreite liegen.

Schalten heißt ja Signalwechsel, und wenn Frequenzen > 3000 Hz mangels Bandbreite ausgefiltert werden, heißt das nichts anderes als daß bei 3000 Hz nur noch ein Sinus auf der Leitung existieren kann. Egal, wie die Signalform am Eingang auch aussieht.

In der Praxis ergibt das eine Schaltfrequenz von 2400 Hz, entsprechend 2400 Baud, die bei reinem FSK auch 2400 Bit/s sind.

Phasenmodulation, PM, PSK (phase shift keying).



Statt Frequenzen werden Phasenverschiebungen zur Unterscheidung der binären Zustände verwendet. Bietet von allen drei Verfahren die größte Bitrate. Üblich sind Phasenwechsel von 45, 135.225 und 315 Grad. 4 Werte sind also gegeben, damit kann man zwei Bit darstellen.

Im Bild oben sind, um es deutlich sichtbar zu machen, Phasensprünge von +180°=1 sowie -180°=0 gezeichnet. Daß es immer zwei Sprünge nacheinander sind, macht die korrekte Erkennung einfacher.

Nutzung der Kanalkapazität

Simplex:

Daten können nur in eine Richtung übertragen werden.

Halbduplex:

Beide Richtungen sind möglich, aber nicht gleichzeitig.

Vollduplex:

In beiden Richtungen kann gleichzeitig übertragen werden.

Frequenzmultiplex:

Signale werden mittels Träger und Modulation in ihrer Frequenzlage (zu höheren Frequenzen hin) verschoben. Mehrere Trägerfrequenzen erlauben gleichzeitig unterschiedliche Signale auf einem Kanal. Dieser muß selbstverständlich die entsprechende Bandbreite zur Verfügung stellen.

Der Empfänger sortiert durch Filterung die Frequenzbänder wieder auseinander und demoduliert dann die Signale. Angewandt zum Beispiel in Telefonnetzen dort, wo analoge Übertragung stattfindet.

Zeitmultiplex:

Die Nutzung des Kanals wird in gleiche Zeitabschnitte unterteilt. Für digitale Daten gut geeignet. Zeitscheiben – Prinzip, ähnlich Multitasking.

Die Leitung steht einem Nutzer für eine bestimmte Zeitspanne zur Verfügung. Danach kommt der nächste an die Reihe. Die Schaltfrequenz ist so hoch, daß dem Nutzer die Unterbrechung nicht auffällt. Die Datenrate der Leitung teilt sich durch die Zahl der Nutzer. Das gilt aber nicht für die Bandbreite ! Jeder hat ja innerhalb seines Zeitfensters die ganze Leitung.

Echokompensation

Diese verhindert auf Telefonleitungen störende Echos bem Sprechen über große Entfernungen. Reflexionen gibt es besonders an Schaltstellen, wo Leitungen enden. Der Sprecher hört sozusagen sein Echo, da ein Teil der ausgesendeten Signale reflektiert wird.

Ähnliches beobachtet man zum Beispiel mit Licht, wenn mit einer Taschenlampe durchs Fenster geleuchtet wird. Ein kleiner Teil des Lichts wird reflektiert. Man sieht ein Spiegelbild der Lampe.

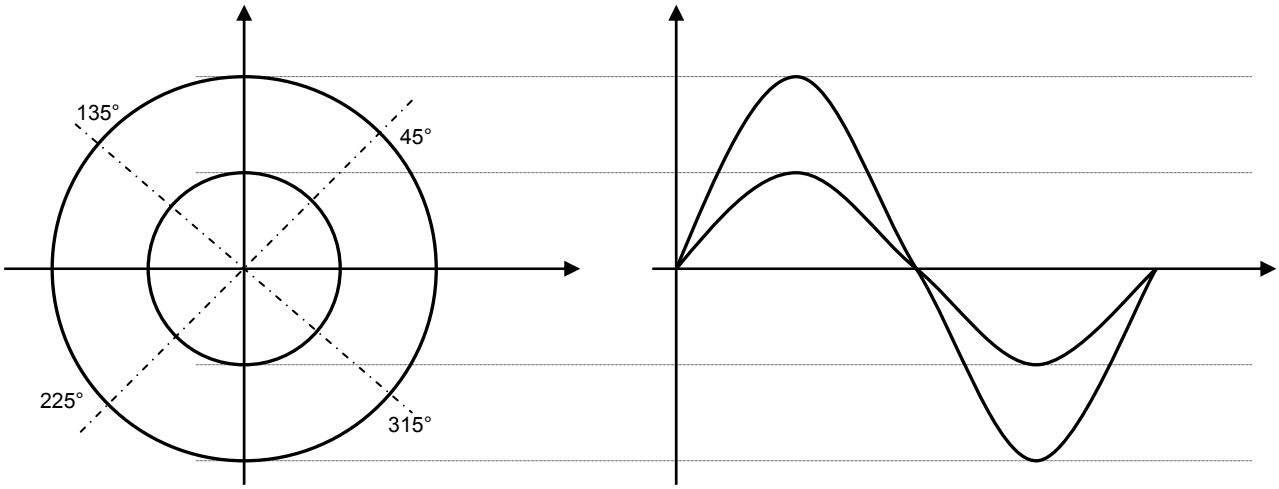
Die Kompensationsschaltung kann man sich wie eine antiparallele Diodenschaltung vorstellen. Je nachdem welche Seite spricht, wird die passende Übertragungs-richtung geschaltet und die andere gesperrt.

In Wirklichkeit sind das natürlich Verstärker, einer für jede Richtung. Die typische Umschaltzeit beträgt 2 bis 5 ms

Schlecht ist das Verfahren für Datenübertragung. Kein Vollduplex ist möglich. Deswegen gibt es in der Echokompensation eine Trägererkennung (FSK). Es erfolgt so die Abschaltung der Echokompensation, wenn anstelle von Sprache eine Trägerfrequenz erkannt wird.

Modem (Modulator - Demodulator)

Modems bedienen sich der Modulationsarten AM, PSK, FSK gleichzeitig, um innerhalb des vorhandenen Frequenzbereichs möglichst viele Bits pro Baud zu übertragen. Das folgende Bild soll das verständlich machen.



Nicht nur zwischen zwei Frequenzen wird hin und her geschaltet. Es werden außerdem zwei unterschiedliche Amplituden sowie vier verschiedene Phasensprünge angewandt.

2 x 2 x 4 Zustände ergibt 16, also 4 Bit / Baud (2^4 = 16).

In der Wirklichkeit sind noch etliche Phasen mehr im Spiel. Die hier gezeigte Konstellation ergibt ja auch erst 9600 Bit/s (4x2400). Aber mehr würde die Zeichnung hoffnungslos überfrachten.

Was möglich ist, hängt von der Leitungsqualität ab. Modems handeln beim Verbindungsaufbau aus, welche Geschwindigkeit sie benutzen. Wobei neben den Fähigkeiten der Leitung natürlich auch die der beteiligten Modems einkalkuliert wird. Aus dem Grund ist es möglich, auch mit alten Modellen noch am Verkehr teilzunehmen.

Dennoch: Alle Modulationstricks reichen nicht, um auf die bislang erreichten 56 k zu kommen. Zusätzlich kommen auch Kompressionsverfahren zur Anwendung.

Verbindungarten und Netzvermittlung

Verbindungslos:

Zugriff auf ein Netz, bei dem Informationen unmittelbar übertragen werden. Das heißt, der Sender schießt die Daten sozusagen einfach ins Netz.

Der Weg der Übertragung ist nicht vorher festgelegt oder bekannt. Die zu übertragenden Daten werden in Blöcke / Pakete unterteilt. Jedes Paket muß also die Absender- und Empfängeradressen beinhalten.

Die Wege der einzelnen Pakete zudem können verschieden sein. Sie müssen dann beim Empfänger gegebenenfalls wieder in der richtigen Reihenfolge zusammengesetzt werden.

Beispiel: Briefpost; Mail, Datenübertragung, auch das UDP – Protokoll (Schicht 4), es wird benutzt, wenn Schnelligkeit wichtiger ist als Genauigkeit, etwa bei der Übertragung von Sprache, Video.

Verbindungsorientiert:

Vor der Übermittlung von Daten muß eine logische Verbindung aufgebaut werden. Dies geschieht in drei Phasen:

Verbindungsaufbau
Datenübertragung
Verbindungsabbau

Der Sender schickt eine Nachricht an den Empfänger mit der Bitte um Verbindungsaufbau. Darin muß also die Netzadresse des Empfängers sowie die Absenderadresse enthalten sein.

Der Empfänger schickt die Bestätigung, dann beginnt die Datenübertragung. Dabei bleibt die Reihenfolge erhalten. Der Weg ändert sich ja nicht.

Sind alle Daten gesendet, initiiert der Sender durch eine entsprechende Anforderung an den Empfänger den Abbau der Verbindung. Bestätigt wird der Abbau nicht.

Beispiel:Telefon, X25, Frame Relay

Paketvermittlung:

Basiert auf Zerlegung der Nachrichten in kleine Datenpakete. Die Möglichkeit der Pakete, unterschiedliche Wege zu nehmen, führt zu einer effektiven Netzauslastung. Dafür muß der Empfänger mehr Intelligenz aufweisen, um alles wieder richtig zusammenzusetzen.

Die alternative Wegführung macht das System relativ ausfallsicher. Es funktioniert auch bei Ausfall eines Knotens, da dieser dann umgangen wird. Hinzu kommt die Möglichkeit, ankommende Pakete auf einem Knoten zwischenzuspeichern, bis die Weiterleitung möglich wird.

Paketvermittlung ist natürlich nur wirklich sinnvoll in Verbindung mit verbindungslosen Verbindungsformen

Leitungsvermittlung:

Basiert auf einer physikalischen Ende-zu-Ende Verbindung zwischen Sender und Empfänger. Zuerst wird eine Verbindung auf Anforderung des Senders durchgeschaltet, die während der gesamten Übertragungszeit bestehen bleibt.

Die Datenübertragung kann in beiden Richtungen ablaufen. Der Verbindungsabbau kann von jedem der Partner eingeleitet werden.

Nachteile sind hier das Warten auf den Verbindungsaufbau bzw auf eine freie Leitung, Die Verbindung bleibt auch in Pausen belegt, wenn keine Daten fließen, und die Leitung kann in den Pausen nicht von anderen genutzt werden.

TCP/IP

TCP steht für Transmission Control Protocol.
IP bedeutet schlicht und ergreifend Internet Protocol.

Ein Protokoll im Netzwerkbereich ist eine Festlegung, wie bestimmte Abläufe bei der Datenübertragung zu behandeln sind.

Die heute und vermutlich auch noch viele Jahre benutzte Version ist Ipv4. In der Zukunft wird es wohl eine Version geben, die Ipv6 genannt wird.

Ursprünglich waren in den USA Universitäten und Regierungsbehörden über das ARPANET verbunden. Dieses Forschungsnetz wurde vom Verteidigungsministerium gefördert. Schwierigkeiten gab es, als völlig andersartige Funk- und Satellitennetze dazukamen.

Erstes Designziel war demzufolge, mehrere Netze nahtlos zusammenschließen zu können. Die zwei primär verwendeten Protokolle, also TCP und IP, gaben dieser Architektur den Namen.

Weiter sollte maximale Ausfallsicherheit gewährleistet sein. Das heißt, viele Wege führen vom Sender zum Empfänger, so daß bei Ausfall eines Knotens noch Alternativen zur Verfügung stehen.

Das bedeutet, man benötigt eine verbindungslose Vernetzungsschicht mit Paketvermittlung. Das ist die Internetschicht, (Vermittlungsschicht nach OSI). So ermöglicht dies den angeschlossenen Partnern, ihre Datenpakete sozusagen einfach in ihr Netz zu schießen. Sie kommen richtig an.

Die Reihenfolge kann beim Empfänger durchaus anders sein, weil die Pakete möglicherweise verschieden lange Wege nehmen .

Auf der Empfängerseite ist es Sache der höheren Schichten, es wieder zu richten.

Vergleichbar funktioniert die Post. Wir übergeben die Sendung dem Netz via Briefkasten. Der Vorgang der Weiterleitung spielt für uns keine Rolle. Lediglich die Zieladresse muß richtig sein.

Die erste Beschreibung des Referenzmodells stammt aus dem Jahre 1974. TCP/IP ist allerdings nicht allgemein gehalten wie OSI, so daß es zur Beschreibung anderer Netzarchitekturen nicht taugt.

Aber immerhin gibt es auch für TCP/IP ein Referenzmodell.

	TCP/IP	OSI
7	Anwendungsschicht	Anwendungsschicht
6		Darstellungsschicht
5		Sitzungsschicht
4	Transportschicht	Transportschicht
3	Internet- / Vermittlungsschicht	Vermittlungsschicht
2		Sicherungsschicht
1		Bitübertragungsschicht

Dieses Modell enthält lediglich drei Schichten, die den Schichten 3, 4 und 7 des OSI – Modells entsprechen.

Das bedeutet nicht, daß ein TCP/IP – Netz allein damit auskommt. Ohne eine Bitübertragungsschicht beispielsweise könnte ja niemals eine Verbindung zustande kommen. TCP/IP sagt bloß nichts dazu.

Auf diesen drei Schichten allerdings tut sich eine ganze Menge mehr als nur TCP und IP.

Zu den zwei untersten Schichten gibt es wie gesagt keine Festlegungen seitens TCP/IP, dort finden wir die verschiedenen Netzwerktechnologien.

Die wichtigsten hier benutzten Protokolle zeigt das folgende Bild:

7	TELNET FTP SMTP, HTTP DNS	Anwendungsschicht
6		
5		
4	TCP UDP	Transportschicht
3	IP ICMP ARP, DHCP	Vermittlungsschicht
2	Ethernet, Token Ring, PPP	
1	Ethernet, Token Ring, PPP	

Eine kurze Beschreibung der Funktionen dieser Protokolle:

Telnet: Baut eine Terminalsitzung zu einem Server auf. Ohne grafische Oberfläche, vorwiegend genutzt zum Arbeiten auf Unix – Servern, aber auch zur Remote- Konfiguration von Netzwerkkomponenten wie Routern und Switches.

FTP: File Transfer Protocol, zum Austausch von Dateien zwischen zwei Rechnern. Zugriffskontrolle per Benutzer/Passwort möglich, wird aber bei Verbreitung von Software (Download) nicht benutzt bzw es wird automatisch Benutzername und Passwort „anonymous“ vorausgesetzt.

SMTP: Simple Mail Transfer Protocol, zur Übermittlung von Email - Dateien zwischen Computern. SMTP benutzt TCP. Es arbeitet mit ASCII – Dateien (7 Bit). Aus diesem Grund müssen Anhänge in einem anderen Format immer erst entsprechend codiert werden.

HTTP: Hyper Text Transport Protocol, Standardprotokoll zum Austausch von Dokumenten im world wide web.

DNS: Domain Name System, hauptsächlicher Nutzen ist die Übersetzung eines Hostnamens in seine IP – Adresse. Aber auch der umgekehrte Weg ist vorgesehen.

TCP: Transmission Control Protocol, zuverlässiges verbindungsorientiertes Protokoll. Ein Bitstrom wird fehlerfrei einer anderen Maschine zugestellt. Es erfolgt Zerlegung in einzelnene Nachrichten, die an die Internetschicht weitergereicht wird. Die Empfängermaschine setzt diese Einzelblöcke via TCP wieder korrekt zusammen.

UDP: User Datagramm Protocol, verbindungsloses Protokoll für Anwendungen, die Paketreihenfolge und/oder Verbindungsaufbau lieber selbst erledigen, anstatt dies TCP zu überlassen. Kommt auch zur Anwendung, wenn es auf Genauigkeit nicht ankommt. Das ist etwa bei Video oder Sprache so, es geht außerdem bei der TCP- Verwaltung für derartige Anwendungen zu viel Datendurchsatz verloren.

IP: Internet Protocol, übernimmt die Datenpakete von den darüberliegenden Schichten. Hauptaufgabe ist das Routing, also das Finden des besten Weges zwischen Quelle und Ziel, sofern sich beide in verschiedenen Netzen befinden. Die logische Adressierung mit IP – Adressen findet hier statt.

DHCP: Dynamic Host Configuration Protocol, automatische Vergabe von IP – Adressen. Ein DHCP – Server ist ein Dienst, der einen IP - Adresspool verwaltet. Das Protokoll ermöglicht es einem Client, beim Start eine Anfrage nach einer freien Adresse ins Netz zu schicken, die vom DHCP Server beantwortet wird.

Das heißt, der Rechner muß in seiner Netzwerkeinstellung auf die Benutzung von DHCP eingerichtet sein. Damit ist er in der Lage, einen genau definierten Broadcast, die DHCP – Anfrage, ins Netz zu schicken, wenn er hochfährt, obwohl er ja eigentlich noch gar keine gültige Adresse besitzt.

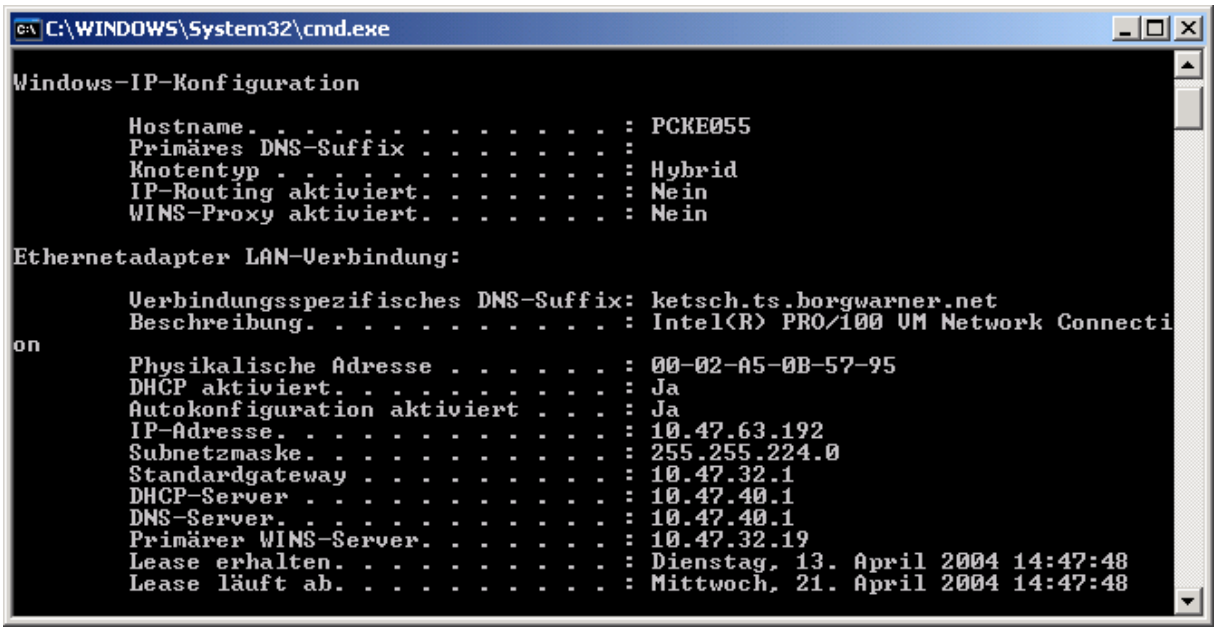
Der DHCP – Server ist der einzige im Netz, der sich davon angesprochen fühlt. Er sucht sich eine freie Adresse aus seinem Pool und sendet diese als DHCP – Angebot zurück, auch als Broadcast. Eine direkte Adressierung ist ja hier noch nicht möglich.

Dem Client wird eine freie Adresse aus dem Pool zugewiesen. Die Verwaltung dieses Adresspools erledigt der Dienst ohne weiteres Zutun. Es wird sichergestellt, daß keine Adresse doppelt vergeben wird

Der Client akzeptiert das erste Angebot, die sogenannte Adress-Lease. (Es könnten mehrere kommen, wenn mehr als ein DHCP-Server vorhanden ist). Damit hat er nun die gewünschte Adresse und sendet eine Nachricht, Angebot angenommen. Auch dies als Broadcast. Würde dem DHCP – Server direkt diese Nachricht zugestellt, was in diesem Stadium bereits möglich wäre, bekäme ein anderer, der vielleicht auch ein Leaseangebot verschickt hat, nämlich nicht mit, daß die Sache erledigt ist.

Eine Lease besteht aus eine Zuordnung von einer IP –Adresse zu einer bestimmten MAC – Adresse in der DHCP – Datenbank.

Das bisher beschriebene Verfahren ergibt die dynamischen Adressen. Das bedeutet, eine Maschine kann durchaus verschiedene Adressen bekommen. Die Lease wird für eine bestimmte Zeit ausgestellt. Beispielsweise 3 Tage, 8 Tage. Das sind typische Werte.



Hier im Bild wird die IP-Konfiguration eines Rechners angezeigt. Die letzten zwei Zeilen informieren über die Zeiten der Lease. Wann sie erhalten wurde und wann sie abläuft.

Eine endliche Leasedauer hat den Vorteil, daß Adressen von Maschinen, die länger ausgeschaltet oder aus anderen Gründen nicht im Netz bleiben, wieder freiwerden. Hat man beispielsweise 254 Adressen, können durchaus mehr als 254 Rechner versorgt werden, so lange nicht alle gleichzeitig am Verkehr teilhaben wollen.

Dazu gibt es noch ein paar Regeln. Hat die Maschine erst einmal eine Adresse, behält sie diese erst einmal. Auch wenn die Lease abgelaufen ist. Vor Ende der halben Leasedauer passiert erst einmal gar nichts. Danach wird beim DHCP-Server angefragt, ob man die Adresse denn weiterhin behalten darf. Normalerweise darf man.

Es könnte natürlich auch mal sein, daß der DHCP – Dienst gerade nicht antworten kann. So lange das der Fall ist, erfolgen Anfragen in immer kürzeren Abständen. Diese Zeitabstände halbieren sich jeweils. Bei einer Leasedauer von acht Tagen wie gesagt nach vier Tagen das erste Mal. Dann wieder nach der Hälfte der verbleibenden Lease, also nach weiteren zwei Tagen, dann wieder einen Tag später. Bis dahin sollte der Administrator den Dienst eigentlich wieder zum Laufen gekriegt haben.

Auf jeden Fall ist gewährleistet, daß ein Client mit seiner Adresse weitermachen kann, auch wenn der DHCP- Dienst mal unpäßlich ist.

Der andere Fall ist der, daß die Adresse einer Maschine nach längerer Abwesenheit anderweitig vergeben ist. Auch dann fragt diese Maschine beim Start, ob die bisherige Adresse weiterhin verwendet werden darf. Das wird aber abgelehnt und stattdessen eine neue, noch freie, Adresse angeboten.

Nachteil der dynamischen Adressierung ist natürlich der zusätzlich erforderliche Netzwerkverkehr. Es ist also ein guter Kompromiß zu finden. Eine sehr kurze Leasedauer ermöglicht mehr Teilnehmer, eine lange verringert die Netzwerklast.

Auf jeden Fall sollte man periodisch wiederkehrende Lastspitzen umgehen. Beispielsweise eine Leasedauer von sieben Tagen. Da hätte man womöglich immer Montag Morgen zum einsetzenden Anmeldeverkehr auch noch die Adressvergabe am Hals. Eine zu kurze Leasedauer (< 3 Tage) würde ähnlich wirken, weil dann am Wochenende immer alle Leases ablaufen würden.

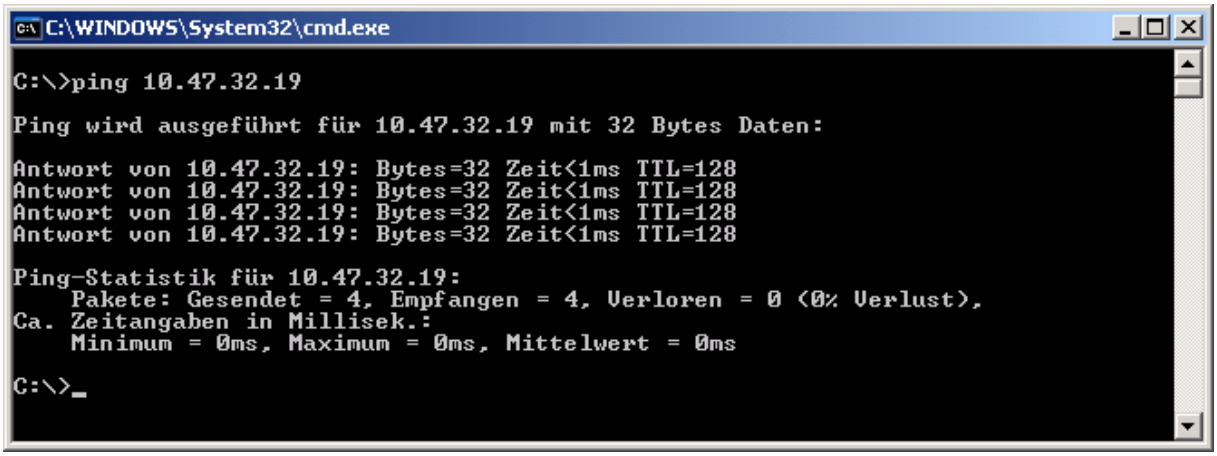
Auch feste Adressen mit unbegrenzter Dauer können vergeben werden. Das sieht so aus, daß man am DHCP – Server einer Mac – Adresse manuell eine eindeutige IP-Adresse zuweist. Kommt die Maschine mit der betroffenen MAC – Adresse ins Netz, bekommt sie auf jeden Fall genau diese IP – Adresse, wenn sie auf DHCP eingestellt ist. So etwas nennt man Reservierung.

Was aber soll ein DHCP – Dienst, wenn doch mit festen Adressen gearbeitet wird ? Nun, es gibt Netzkomponenten, die ständig im Netz verfügbar sein müssen. Etwa Netzwerkdrucker. In den meisten Fällen sind solche Geräte vom Hersteller auf die Nutzung von DHCP konfiguriert, damit auch wenig versierte Anwender das Teil erfolgreich einsetzen können.

Optimal ist das nicht. Erstens werden unnötig Adressen aus dem Pool belegt. Außerdem gibt es Anwender, die solche Geräte ausschalten und etwa nach dem Wochenende wieder einschalten. Dann kann es vorkommen, daß sich die Adresse ändert und nichts mehr geht.

Normalerweise ist es möglich, am Gerät selbst eine feste Adresse einzustellen und kein DHCP zu benutzen. Aber per Reservierung hat man all diese Adressen an einer zentralen Stelle verwaltet. Und sollte mal der Adressbereich im Netzwerk geändert werden, genügt es, die Reservierung anzupassen. Anschließend kann der Anwender das Gerät aus- und wieder einschalten und die neue Adresse ist angekommen.

ICMP: Internet Control Message Protocol, Steuerprotokoll, sorgt für den Austausch von Servicemeldungen im Netz. Eine solche Meldung wäre zum Beispiel die, daß ein Zielhost nicht erreichbar ist.



Hier wurde der Rechner mit der Adresse 10.47.32.19 „angepingt“. Dieser Ping – Befehl ermöglicht das Testen von IP – Verbindungen. Daß man die Antwort mit den verschiedenen Informationen erhält, ist dem ICMP – Protokoll zu verdanken.

ARP: Address Resolution Protocol, Steuerprotokoll, übersetzt IP- Adressen in MAC – Adressen. So lange ein Paket via Router durch verschiedene Netze zum Ziel geleitet wird, greift die logische Adressierung (IP). Im Zielnetz angekommen, gilt es, die Hardwareadresse des Empfängers ausfindig zu machen, danach kann die Nachricht zugestellt werden.

Nur Hardwareadressen sind weltweit einzigartig, und deshalb ohne weitere Strukturierung. Damit können auf dieser Ebene keine Subnetze gebildet werden. So ist immer eine logische Adressierung erforderlich, sobald mehr als ein Netz im Spiel ist.

Alle routingfähigen Netzwerk – Protokollstapel (etwa IPX/SPX oder AppleTalk) haben deswegen einen dem ARP – Protokoll vergleichbaren Mechanismus.

Ein paar Worte zu Novell / IPX

Bis zur Version Intranetware 4.11 war IPX/SPX der Standard – Protokollstapel bei Novell – Netzwerken. Andere waren optional. Erst ab der Version Netware 5 ist auch hier TCP/IP Standard.

IPX – Netzwerke haben von der Adressierung her den Anschein, als wären hier tatsächlich reine MAC – Adressen im Spiel. Das ist aber nicht der Fall. Sowie Routing bzw Subnetze erforderlich sind, müssen Subnetze in irgendeiner Form mit logischen Adressen unterschieden werden.

Eine IPX – Adresse besteht also aus mehreren Komponenten, insgesamt drei, und sieht etwa so aus:

B0519923 **:** 00A024704C05 **:** 4014

Die Schreibweise ist hexadezimal. Eine Stelle hexadezimal entspricht bekanntlich 4 Bit dual.

Teil 1 ist die achtstellige Netzwerkadresse, die aus 4 Byte/32 Bit besteht. Daran schließt sich die Knotenadresse mit 48 Bit an, die eigentliche Adresse des Rechners im Netz.. Der letzte Teil bezeichnet die Portnummer, die zusammen mit der Knotenadresse die Socketnummer bildet.

Sockets definieren eine Knotennummer in Kombination mit einem bestimmten Port. Ports sind neben Adressen eindeutige Identifikatoren für bestimmte Dienste. Ports und Sockets gibt es analog auch bei TCP/IP. Dort sind viele Ports definiert, etwa 21 für FTP, 80 für http und einige andere. Mehr dazu weiter unten.

Alle Clients haben also ihre eigene individuelle Knotennummer, aber dieselbe Netzwerknummer, so lange sie dem selben Subnetz angehören.

Die Knotennummer ist hier identisch mit der MAC – Adresse. Die Netzadresse zeigt an, ob ein Knoten im selben Netz gemeint ist, oder nicht. Wenn nicht, geht das Paket an den nächsten Router, der es weiterleitet.

Erst wenn das Zielnetz erreicht ist, wird die Zieladresse (= Knotennummer) adressiert.

IP – Adressierung

Jeder Host hat eine 32 Bit – Adresse. Diese wird in der Regel nicht als Dual -, sondern als Dezimalzahl mit 4 Blöcken dargestellt. Jeder Block enthält 8 Bit.

Theoretisch sind damit maximal etwa 4,2 Mrd. Adressen (2^{32}) möglich, durch Unterteilungen und Reservierungen sind es aber weit weniger .

Zu einer IP - Adresse gehört immer auch eine Subnetmask, in den meisten Fällen auch ein Standardgateway

Eine IP - Adresse wäre beispielsweise 168.89.34.12

Jede dieser dreistelligen, durch Punkt getrennte Zahlen steht für die jeweils entsprechende Dualzahl.

Bitmuster:	10101000	01011001	00100010	00001100
Dezimal	168	89	34	12

IP Adressen werden in Klassen eingeteilt.

Adress – Klassen:	A	`0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx`
	B	`10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx`
	C	`110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx`

Die Klasse ist am ersten Oktett zu erkennen, an den ersten Stellen.

A: $\geq$ 1 – 126 . x . x . x
B $\geq$ 128 – 191 . x . x . x
C $\geq$ 192 – 223 . x . x .x

0, 127, ab 224 sind zahlenmäßig in den Wertebereichen enthalten, aber für bestimmte Zwecke reserviert

Beispiel Klasse A: Weil das erste Bit auf 0 festgelegt ist, bleiben noch die restlichen 7 Bit als Wertebereich im ersten Block. Das ermöglicht Werte von 0 bis 127.

Die Beispieladresse 168.89.64.12 gehört also in die Klasse B.

Aufteilung in Teilnetze

Ohne eine Segmentierung würde jedes größere Netz, auf jeden Fall ein weltweites, zusammenbrechen. Gäbe es keine sinnvolle Aufteilung, würde nämlich jedes gesendete Paket auf allen Leitungen im gesamten Netz auftauchen und diese unnötig belegen, auch wenn nur ein bestimmter, einzelner Adressat irgendwo in der Welt gemeint ist.

Alle, für die das Paket nicht bestimmt ist, checken dessen Adressinformation und verwerfen es anschließend. Besser für die Netzbelastung wäre es, wenn diese Pakete erst gar nicht so weit kämen.

Verschiedene Teil - Netzwerke sind also nowendig, um den Netzwerkverkehr innerhalb lokaler Segmente zu halten und damit die Verkehrsdichte auf ein vertretbares Maß zu bringen. Mit Hilfe der Segmentierung können zudem gleiche Adressen mehrmals verwendet werden, wenn das System entsprechend organisiert ist.

Entsprechend organisiert heißt hier, daß es Adressbereiche gibt, die im öffentlichen Bereich nicht auftauchen. Dazu gehören alle Adressen, die mit 10 (Klasse A) beginnen, alle mit 192.168...(Klasse C)

Verwendet man eine derartige Adresse im Internet, das heißt man schickt etwa ein Paket mit der Zieladresse 10.47.32 25 auf die Reise, würde der nächste Router dies verwerfen.

Die internen Adressbereiche werden also für LAN' s benutzt. Und weil die Adressen eines LAN' s nie im Internet auftauchen, können sie in einem andere LAN genauso gut wieder verwendet werden.

Zur Einteilung der Netze definiert man eine Subnetmask, dadurch erfolgt die Aufteilung der IP – Adresse in zwei Anteile. Einer davon definiert die Adresse des Teilnetzes (Netzadresse), der andere die Adresse des Gerätes/Hosts innerhalb dieses Teilnetzes.

Die Bezeichnung Gerät oder Host deutet darauf hin, daß es sich ja nicht immer um Rechner handeln muß.

Über die gesamte Adresse wird hierbei eine gleichgroße (32 bittige) Maske gesetzt. Mit deren Hilfe definiert man, welcher Anteil der IP – Adresse zum Gerät (Rechner oder andere Netzwerkkomponente) gehört und welcher Anteil zur ID (Adresse) des jeweiligen Netzes.

Beispiel:

IP - Adresse	195.89.34.12	11000011 01011001 00100010|00001100
Subnetmask	255.255.255.0	11111111 11111111 11111111|00000000
Netzadresse	195.89.34.0	11000011 01011001 00100010|00000000

Die Stelle, an der die Subnetmask eine 1 aufweist, zählt zur Netzadresse. Wo eine Null in der Subnetmask steht, zählt die Stelle zur Geräteaddresse.

Die Null ist demzufolge reserviert für die Netzadresse selbst, es darf also in diesem Netz kein Gerät mit der Nummer 195.89.34.0 adressiert werden.

Jede der drei Adressklassen hat ihre Standard - Subnetmask.

A: 255.0.0.0
B: 255.255.0.0
C: 255.255.255.0

Die oben gewählte Subnetmask der Adresse 195.89.34.12 ist also entsprechend der Klasse C konfiguriert, zu der die Adresse gehört.

Für die einzelnen Klassen ergibt sich so eine bestimmte Anzahl Netzwerke und Anzahl Geräte

Zur Erinnerung:

```
A     0xxxxxxx|xxxxxxxx.xxxxxxxx.xxxxxxxx
      11111111|00000000.00000000.00000000

B     10xxxxxx.xxxxxxxx|xxxxxxxx.xxxxxxxx
      11111111.11111111|00000000.00000000

C     110xxxxx.xxxxxxxx.xxxxxxxx|xxxxxxxx
      11111111.11111111.11111111|00000000
```

Die ersten Bits sind charakteristisch für die Klasse und können nicht frei gewählt werden. Deshalb verringert sich die Zahl der möglichen Subnetze.

A: 2^7 Subnetze, (2^{24}) –2 Adressen
B: 2^{14} Subnetze. (2^{16}) –2 Adressen
C: 2^{21} Subnetze, (2^8) –2 Adressen

In der Klasse A ist also nur das erste Oktett für die Netzwerkadresse zuständig. Das ergibt zunächst eine Zahl von 2^8 = 256 Subnetzen mit jeweils 2^{24} Geräte - Adressen. Da das erste Bit jedoch fest auf 0 gesetzt ist, bleiben lediglich 7 Bit übrig, die für die Netzadresse variiert werden können.

Es kann demzufolge weltweit nur 127 Netze der Klasse A geben.

Die Anzahl der Adressen in einem Netz reduziert sich deswegen immer um zwei, weil die Null für die eigentliche Netzadresse steht und die 255 für die Broadcastadresse (Sendung an alle).

Haben wir also beispielsweise eine C- Adresse 192.168.10.24, ist die zugehörige Netzadresse 192.168.10.0 und die Broadcastadresse 192.168.10.255. Gültige Rechneradressen sind also in diesem Netz alle von 192.168.10.1 bis 192.168.10.254.

Technisch notwendig ist diese Einteilung übrigens nicht. Sie dient nur dazu, Ordnung ins System zu bringen.

Technisch würden auch C - Adressen mit A – Subnetmasks funktionieren. Es wäre nicht einmal nötig, die Subnetmask mit zwei zusammenhängenden Blöcken aus Nullen und Einsen zu bilden. Bei einem Durcheinander wäre allerdings besonders aus der Dezimalschreibweise kaum noch erkennbar, wer mit wem im selben Netz sitzt.

Nachteile hat eine solche Segmentierung leider auch. Sie besteht in einer erheblichen Verschwendung von Adressen. Besonders die B – Netze tragen dazu bei.

Da ein C – Netz nur 254 Adressen erlaubt, erwerben viele Firmen B – Netze, die bis zu 65534 Hosts vertragen. Diese Zahl ist aber so groß, daß sie selten genutzt wird. Hat jemand etwa Bedarf für 2000 Adressen, reicht ein C – Netz nicht. Also hat man ein B – Netz. Das verschwendet dann aber gleich 63534 Adressen.

Als die IP – Adressierung erdacht worden ist, hatte man nicht die Vorstellung, daß mal 100000 Netze am Geschehen beteiligt sein würden, und deswegen werden öffentliche IP – Adressen allmählich knapp.

Subnetze haben nur dann einen Sinn, wenn sie durch spezielle Komponenten getrennt sind.

Wenn mehrere Teil- (Sub-) netze existieren, muß bei der Netzwerkkommunikation erkannt werden, ob sich die Zieladresse im selben Netzwerk befindet oder nicht, damit die Anfrage gegebenenfalls aus dem eigenen Subnetz heraus weitergeleitet werden kann.

Dieser Vorgang des Weiterleitens wird Routing genannt, wenn die Weiterleitung mittels IP- Adressen erfolgt. Die entsprechenden Geräte sind demzufolge Router.

Ob das Ziel „außerhalb“ liegt oder nicht, errechnet sich durch das so genannte „Anding“. Das erste Bit der Adresse wird UND – verknüpft mit dem ersten Bit der Subnetmask, das zweite Bit hier mit dem zweiten dort usw. Der Vorgang wird mit der Quell- sowie der Ziel – Adresse durchgeführt.

Beispiel, Quell – und Zieladresse im selben Subnetz:

Eigene Adresse	168.89.34.12
Subnetmask	255.255.255.0
Netzadresse	168.89.34.0
Zieladresse	168.89.34.13

Eigene Adresse	10101000 01011001 00100010 00001100
Zieladresse	10101000 01011001 00100010 00001101
Subnetmask	11111111 11111111 11111111 00000000
Ergebnis	10101000 01011001 00100010 00000000

Nach dem Anding bleibt die Netz – ID 168.89.34.0 übrig.
0 UND X ergibt immer 0, 1 UND X immer X. Deshalb werden alle Bits im Bereich der Geräteadresse beim Anding immer zu Null.

Für Quell- und Zieladresse kommt hier dieselbe Netzwerkadresse heraus, die Zieladresse gehört demnach ins eigene Subnetz und kann direkt angesprochen werden.

Beispiel, Quell – und Zieladresse nicht im selben Subnetz:

Eigene Adresse	168.89.34.12
Subnetmask	255.255.255.0
Zieladresse	168.89.33.12

Eigene Adresse	10101000 01011001 00100010 00001100
Subnetmask	11111111 11111111 11111111 00000000
Ergebnis 1	10101000 01011001 00100010 00000000
Zieladresse	10101000 01011001 00100001 00001100
Subnetmask	11111111 11111111 11111111 00000000
Ergebnis 2	10101000 01011001 00100001 00000000

Vergleich der Ergebnisse:

Ergebnis 1	10101000 01011001 **00100010** 00000000
Ergebnis 2	10101000 01011001 **00100001** 00000000
Subnetmask	11111111 11111111 **11111111** 00000000

Nach dem Anding bleiben hier verschiedene Netz – ID übrig, weil die Adressen sich an einer Stelle unterscheiden, an der die Subnetmask den Wert 1 hat.

In diesem Fall wird sofort der Router adressiert. Es ist nicht notwendig, die Subnetzmaske des Zielnetzes zu wissen. Wenn beim Anding (mit der eigenen Maske) nicht die eigene Netzwerkadresse herauskommt, liegt das Ziel auf jeden Fall außerhalb.

Daß hier B – Adressen mit C – Subnetmasks zusammenkommen, ist wie schon gesagt aus technischer Sicht vollkommen unproblematisch. Im eigenen Netz, das eine geschlossene Einheit bildet, kann das ohne weiteres konfiguriert werden.

In internen Netzen ist das oft sogar sehr sinnvoll. A- Netze wie zum Beispiel 10.47.32.0 sind mit der Subnetzmaske 255.0.0.0 kaum brauchbar, weil niemand ein einziges Netz mit 16 Millionen Rechnern installiert.

Hat man allerdings eine Komponente, die direkt im Internet steht, muß man sich natürlich bei der öffentlichen Adresse dieser Komponente an die Regeln halten.

Kommunikation über Grenzen von Subnetzen

Das Standardgateway ist die dritte Komponente bei der Konfiguration einer IP – Adresse.

Ein Router, der zwischen zwei Netzen steht, muß zwei Netzwerkanschlüsse besitzen, für jedes Subnetz einen mit passender Adresse.

In der Regel wird für den Router die erste mögliche Adresse im Netz (1) gewählt. Technisch notwendig ist das aber nicht.

Beispiel:

NETZ 1	**ROUTER**		**NETZ 2**
168.89.34.0	168.89.34.1	168.89.33.1	168.89.33.0

Da nach wie vor die Subnetmask 255.255.255.0 gilt, zählen die 33 bzw 34 noch zur Netzwerkadresse. Es handelt sich demnach wirklich um verschiedene Netze

Die Adresse des Standardgateway ist immer diejenige des Routers, die im eigenen Subnetz steht und wird dann zur Zieladresse, wenn die eigentliche Zieladresse im anderen Netz liegt.

In der Netzwerkkonfiguration eines PC im Netz 1, der mit TCP/IP als Netzwerkprotokoll arbeitet , müßte also beispielsweise stehen:

IP – Adresse	168.89.34.12
Subnetmask	255.255.255.0
Standardgateway	168.89.34.1

Der Router dient zur logischen Trennung. Er sorgt dafür, daß Verkehr innerhalb eines Subnetzes bleibt, wenn er nur dessen Mitglieder betrifft. Pakete, die an Mitglieder des eigenen Netzes adressiert sind, läßt der Router nicht passieren.

Alle Pakete, deren Zieladresse im eigenen Subnetz liegen, werden also nicht über einen Router hinweg gelangen. Zusätzlich gibt es noch einige andere. Prinzipiell alles, was per Broadcast übermittelt wird. Dazu gehören etwa Namensanfragen, wenn im Netz kein Namensdienst existiert oder DHCP – Anforderungen.

Ausnahmen, gibt es aber auch hier. Freigegebene Verzeichnisse beispielsweise. Diese sollen im gesamten Netz sichtbar sein, damit ein Server auch entfernte Clients bedienen kann. Das Sichtbar- bzw Bekanntmachen einer Freigabe heißt ja auch, daß bestimmte Datenrahmen zu diesem Zweck an alle verschickt werden müssen.

In einem physikalischen Netz kann man mittels Adressierung verschiedene Teilnetze auch ohne Router konfigurieren (indem man also die Adressen entsprechend vergibt). Damit erreicht man keine Entzerrung des Verkehrs, die Unterteilung wäre nur eine logische.

Wie funktioniert Routing ?

Jede Maschine in einem IP - Netzwerk, ob Router oder nicht, unterhält eine Routingtabelle. Diese enthält die notwendigen Informationen zur Wegfindung. Diese sind: Zielnetz, Zielnetzmaske, Gateway, Schnittstelle.

Jeder Eintrag besteht aus diesen vier Komponenten.

Ein Rechner im Netz 1 aus dem obigen Beispiel für das eigene Netz folgenden Eintrag:

Zielnetz: 168.89.34.0
Maske: 255.255.255.0
Gateway 168.89.34.1 (Router, Standardgateway)
Schnittstelle: 168.89.34.12 (eigene Netzwerkkarte)

Auch wenn nur ein Netz existiert, ist eine Routingtabelle vorhanden. Es gibt dann kein Gateway, bzw dieses ist identisch mit der eigenen Netzwerkadresse.

Interessanter wird die Sache am Router. Der muß genau wissen, wohin die an ihn adressierten Pakete geschickt werden sollen. In dieser Konfiguration mit zwei Netzen ist das ganze allerdings noch ziemlich übersichtlich. Im Prinzip gilt es lediglich, alle an einer Seite ankommenden Pakete auf die andere Seite weiterzureichen.

Der Router hat in jedem Netzwerk eine Schnittstelle, und er benötigt daher zwei Einträge.

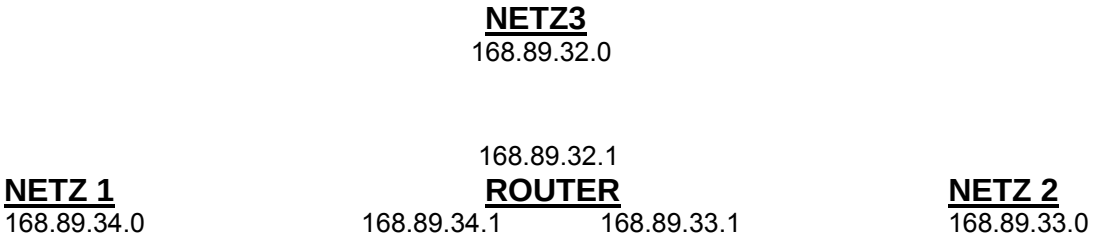
Zielnetz: 168.89.34.0
Maske: 255.255.255.0
Gateway 168.89.34.1 (Router, Standardgateway)
Schnittstelle: 168.89.34.1 (eigene Netzwerkkarte)

Zielnetz: 168.89.33.0
Maske: 255.255.255.0
Gateway 168.89.33.1 (Router, Standardgateway)
Schnittstelle: 168.89.33.1 (eigene Netzwerkkarte)

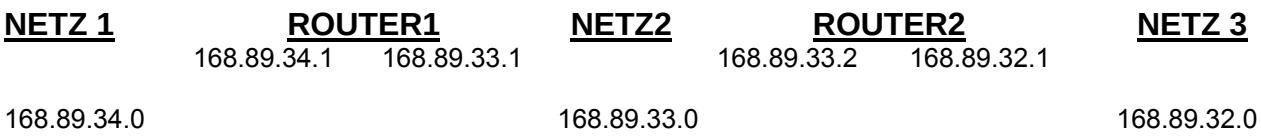
Der Weg in eines der Netze ist logischerweise immer auch die Schnittstelle, die in dem jeweiligen Netz platziert ist.
Für jedes Teilnetz gibt es nur eine Schnittstelle nach außen, so daß alle Hosts in einem Netz dasselbe eindeutige Standardgateway besitzen.

Auch in der folgenden Konfiguration bleibt alles eindeutig. Der Router bekommt eine dritte Schnittstelle mit dem entsprechenden Tabelleneintrag:

Zielnetz: 168.89.32.0
Maske: 255.255.255.0
Gateway 168.89.32.1 (Router, Standardgateway)
Schnittstelle: 168.89.32.1 (eigene Netzwerkkarte)



Meistens sind Netzwerke, die man koppeln möchte, räumlich so angelegt, daß nicht alle wie oben an einem Router hängen können. Mehrere Router sind also im Spiel, und da kann es Netze geben, die kein eindeutiges Standardgateway aufweisen.



Jeder Router ist direkt mit zwei der drei Netze verbunden, das dritte kennt er sozusagen nur vom Hörensagen. Dieses Hörensagen besteht wiederum in einem weiteren Eintrag in der Routingtabelle, durch den das entfernte Netz bekannt gemacht wird.

Router1:

Zielnetz: 168.89.32.0
Maske: 255.255.255.0
Gateway 168.89.33.2 (Router, Standardgateway)
Schnittstelle: 168.89.33.1 (eigene Netzwerkkarte)

Das Gateway ist jetzt nicht mehr die eigene Netzadresse im Netz 2, sondern die erreichbare des gegenüberliegenden Routers, ebenfalls im Netz 2.

Das Paket kann also direkt an die Schnittstelle von Router2 gereicht, werden, wenn es weder für Netz 1 noch für Netz 2 bestimmt ist. Router 2 weiß, was damit zu tun ist.

Weil am Netz 2 beide Router beteiligt sind, gibt es dort auch kein eindeutiges Standardgateway mehr für die dort angesiedelten Hosts. Sinnvollerweise wählt man den Router, über den das größere Verkehrsaufkommen zu erwarten ist, und gibt dem die Nummer 1.

Es kommt oft vor, daß in einer Anordnung wie oben zwischen zwei Routern gar kein Netz existiert. Wenn zwei entfernte LAN' s miteinander gekoppelt werden, etwa über eine ISDN - Leitung, dann benötigt man die Router nur zur Anbindung an die WAN – Leitung.

Natürlich will man hin und wieder von einem LAN aus ins Internet. Im LAN werden ja wie gesagt Adressen benutzt, die im Internet ignoriert werden. Um dennoch eine Kommunikation möglich zu machen, hat man einen Router, der mit einer Adresse im LAN und mit einer öffentlichen, internetkonformen Adresse im Internet steht.

Die LAN – Clients kommunizieren also nicht direkt im Internet. Sendet ein solcher Rechner etwas an eine Adresse im Internet, werden diese Pakete mit der Quelladresse des Routers (dessen Adresse auf der Internetseite) versehen und verschickt. Die Antwort darauf enthält demzufolge als Zieladresse die öffentliche des Routers. Der wiederum muß die ankommenden Sendungen übersetzen in die zugehörigen internen Adressen, um sie zustellen zu können.

Dieser Mechanismus heißt Network Adress Translation (NAT), siehe unten.

Statisches und dynamisches Routing

In kleinen Netzen mit einem oder wenigen Routern, in denen kaum Änderungen vorkommen, sind feste Tabellen gut und üblich. Das heißt dann statisches Routing.

In großen Netzen, wenn viele Router beteiligt sind, vor allem im Internet, werden sogenannte Routingprotokolle eingesetzt, die im wesentlichen für drei Dinge zuständig sind:

Aktualisierung der Routingtabellen bei Änderungen
Finden des kürzesten Weges
Vermeiden von Endlosschleifen

Router kommunizieren miteinander, indem sie sich gegenseitig eine Vielzahl von Nachrichten senden. Fällt einer aus oder kommt ein neuer hinzu, müssen die Tabellen aktualisiert werden.

Zum Zwecke dieser Kommunikation gibt es, wie könnte es anders sein, spezielle Protokolle. Einige davon, die in IP – Netzen zur Anwendung kommen, sind:

RIP – Routing Information Protocol
BGP – Border Gateway Protocol
OSPF – Open Shortest Path First

OSPF ist der Nachfolger von RIP im Internet. Beide sind dazu gedacht, die optimale Route für ein Paket zu finden. OSPF tut das sehr viel effektiver. RIP in der Ursprungsversion übermittelt immer komplette Routingtabellen, und auch sonst sorgt es für viel Netzwerkverkehr. Für große Netzwerke ist RIP ungeeignet.

Die schnellste Route ist nicht unbedingt die beste. Im Sinne der Netzauslastung ist es sogar sehr sinnvoll, auch alternative Wege parallel zu nutzen, also nicht einfach alle Pakete nacheinander auf den besten Weg zu schicken. Genau das kann OSPF gut.

BGP hat andere Zielsetzungen. Während OSPF in autonomen Systemen ausschließlich dafür sorgt, die Paketzustellung so effizient wie möglich zu machen, ist BGP dafür gedacht, zusätzliche Regeln zu verarbeiten.

Es geht beispielsweise darum, bestimmte Vorschriften in einem Land einzuhalten. Verkehr innerhalb von Kanada darf nicht über Systeme der USA geleitet werden, auch wenn die physikalisch beste Route das nahelegen würde. OSPF würde sich dafür nicht interessieren.

Das Ganze nennt sich dynamische Routing. Die Software in den Routern berechnet in regelmäßigen Abständen die Leitwege automatisch neu.

Sind viele Wege möglich, kann ein Paket im Prinzip endlos im Kreis laufen. Um das zu verhindern, gibt es entsprechende Algorithmen, ebenso für das Erkennen des kürzesten Weges.

Falls trotzdem mal was schiefgeht, gibt es in den IP-Paketen einen Zähler (TTL, Time to live), der mit jedem „Hop“ (=Router), der durchlaufen wird, heruntergezählt wird. Maximal 128 Hops sind möglich, dann ist der Zähler auf 0 und das Paket wird verworfen.

Mit dem ping – Kommando (ping <Adresse>) kann man die Anzahl der Hops zu einem Ziel leicht feststellen. Die Antwort zeigt diese mit TTL an, im eigenen Netz also 128. Führt der Weg zu Zieladresse über einen Router, steht dort 127 usw…

Sockets und Ports

Das Thema, in Zusammenhang mit IPX/SPX schon mal erwähnt, sei hier noch einmal aufgegriffen.

Es sind diverse, sogenannte „well known“ Ports festgelegt für verschiedene Dienste im Protokollstapel von TCP/IP.

Einige sind:

FTP Datentransfer:	20
FTP Steuerkommandos	21
Telnet:	23
SMTP:	25
DNS:	53
DHCP:	67
http::	80
https:	443
Proxy:	8080

Ein Port zusammen mit einer Hostadresse bildet ein Socket.

Insgesamt gibt es 65536, also 2^{16} Ports (Port 0 bis 65535), davon sind die meisten frei nutzbar.

Das Ganze hat folgenden Sinn: Ein Client kann mehrere Verbindungen zu einem anderen Client oder vor allem zu einem Server haben. Eine Verbindung zwischen zwei Partnern beinhaltet zunächst deren IP – Adressen und Namen zur Identifikation einer Session.

Nun ist es aber nicht ungewöhnlich, daß ein Server mehrere Dienste anbietet und daß ein Client auch einige davon gleichzeitig nutzt. Die verschiedenen Sitzungen werden dann eindeutig durch die zugrundeliegenden Ports definiert. IP- Adresse und Namen sind dafür ungeeignet weil für jede Sitzung identisch.

Ports sind auch geeignet, um einem Router zu veranlassen, bestimmte Broadcast – Pakete gegen seine sonstige Gewohnheit doch durchzulassen.

Falls also etwa ein DHCP – Server ein anderes Subnetz mitversorgen soll, müßte der Port 67 entsprechend konfiguriert, also durchgelassen werden. Dieser Port wird benutzt in Zusammenhang mit dem DHCP Relay Agent. Dieser sammelt DHCP – Requests ein und sendet diese an den DHCP – Server (im anderen Netz). Das ginge noch ohne weiteres.

Die Antwort, also das Angebot einer Adresse, ist aber auch noch ein Broadcast, weil der Client in dem Moment ja noch keine Adresse hat. Dieser muß also auch den Router passieren können.

NAT

Noch etwas anderes wird mittels Ports geregelt, das NAT, Networt Adress Translation. Dieser Mechanismus übersetzt, wie der Name schon sagt, Adressen. Und zwar interne IP – Adressen in öffentliche und umgekehrt.

Es ist ja so, daß man in einem LAN oft mehreren oder allen Teilnehmern Internetzugang einrichtet. Das tut man nicht, indem jeder eine öffentliche IP – Adresse bekommt (was technisch natürlich auch möglich wäre). Öffentliche Adressen sind aber knapp, müssen beantragt werden und kosten demzufolge Geld.

Was also macht man ? Ein Router mit der NAT – Fähigkeit bekommt einen Anschluß im LAN und einen weiteren in öffentlichen Internet.

Ein Client, der nun einen Host irgendwo im Internet adressiert, sendet das entsprechende Paket an sein Standardgateway, also die interne Routeradresse, weil es sich nicht um ein internes Ziel handelt.

Der Router ersetzt nun die Quelladresse durch seine eigene (die öffentliche). Im Internet erscheint also der NAT – Router als Absender. Zusätzlich gibt der Router dieser Sendung noch eine Portnummer mit.

Wenn mehrere Clients Internetverkehr unterhalten, haben alle Pakete, sobald sie im Internet sind, dieselbe Quelladresse. Das bedeutet, daß alle Antworten auch an diese Adresse geschickt werden. Unser Router muß nun dafür sorgen, daß jedes Paket intern richtig zugestellt wird.

Das tut er, indem jeder Internetsitzung ein eigener Port zugeordnet wird. Diese sind eindeutig und anhand der Portnummer einer ankommenden Sendung kann der zugehörige interne Host identifiziert werden.

CIDR

Trotz vieler Versuche, die bisherige IP – Version auch bei immer knapper werdenden Adressen funktionsfähig zu halten, wird man in absehbarer Zeit an einer Ablösung nicht vorbeikommen.

Ein aktueller Versuch, Ipv4 das Leben noch etwas zu verlängern besteht darin, statt uneffektiver B – Netze einem Kunden stattdessen mehrere C – Netze zur Verfügung zu stellen. Das Ganze läuft unter dem Namen CIDR, Classless InterDomain Routing.

Der Name sagt es schon. Man will sich lösen von der starren Einteilung der Klassen. Im Rückblick ist klar, daß man besser daran getan hätte, die C – Klasse mit 10 statt 8 Bit für die Hostadresse auszustatten. Das wären 1022 Rechner pro Netz, was in vielen Fällen ausreichend wäre, und es stünden rund eine halbe Million Netze zur Verfügung.

Bei B – Netzen hat man nur 16384 Netze.

Die noch vorhandenen C – Netze liegen zahlenmäßig bei rund zwei Millionen. Diese werden in Blöcken variabler Länge vergeben. Benötigt jemand zum Beispiel 2000 Adressen, bekommt er dann acht aufeinander folgende C – Netze (je 254 Adressen) anstelle eines vollen B – Netzes.

Zusätzlich wird der Adressraum in vier geographische Zonen aufgeteilt. Asien/Pazifikraum, Europa, Mittel-/Südamerika und Nordamerika.

Die regionale Zuordnung vereinfacht das Routing erheblich, weil ein Paket, das von Europa aus zu einem außereuropäischen Ziel gehen soll, einfach an ein europäisches Standardgateway geschickt werden kann.

Aber trotz dieser Klimmzüge rechnet niemand ernsthaft damit, daß Ipv4 noch eine große Zukunft hat.

Ipv6

Damit dieser neuen Version von IP die Zukunft nicht so schnell ausgeht, hat man zunächst einmal festgelegt, was denn überhaupt an Eigenschaften vorhanden sein soll.

Die wesentlichen seien hier aufgezählt:

1) Angebot von Milliarden Adressen, die auf jeden Fall für alle Zukunft ausreichen müssen

2) Reduzierung des Umfanges von Routingtabellen

3) Vereinfachung der Protokolle, damit die Weiterleitung schneller möglich ist

4) Mehr integrierte Sicherheit, Authentifizierung und Datenschutz

5) Mehr Gewicht auf Dienstarten (Quality of Service)

6) Möglichkeit, mobile Hosts ortsunabhängig ohne Adressänderung zu betreiben

7) Künftige Weiterentwicklung

8) Koexistenz der alten und neuen Protokolle für die Übergangszeit

Logischerweise sind alle bisherigen Protokolle nicht kompatibel, die mit der Adressierung zu tun haben. Das sind demzufolge TCP, UDP, ICMP, OSPF, BGP, DNS.

Die Adressen sind ja der Hauptgrund, warum Ipv6 entwickelt wurde. Eine Adresse umfaßt 16 Byte, geschrieben hexadezimal in acht Blöcken zu je zwei Byte (16 Bit).

Beispielsweise: 8000:0000:0000:0000:0123:4567:89AB:CDEF

Um das etwas abzukürzen und weil oftmals viele Nullen vorkommen, gibt es ein paar Schreiboptimierungen. Führende Nullen weglassen etwa, also statt 0123 nur 123, und komplette Nullblöcke durch zwei Doppelpunkte ersetzen.

Damit sieht die Beispieladresse so aus: 8000::123:4567:89AB:CDEF

Es ist also nicht so, daß pro Nullgruppe ein Doppelpunkt steht, sondern immer zwei Doppelpunkte für eine oder mehrere aufeinanderfolgende Nullgruppen.

Wäre nun vor allem die Frage zu klären, ob denn Ipv6 genug Adressen bietet. Schließlich ist das ja der eigentliche Anlaß für die Neuerung.

16 Byte hat eine Adresse, das heißt wir haben eine Dualzahl mit 128 Stellen. Es sind demzufolge 2^{128} Adressen möglich. Reicht das ?

2^{128} sind rund $3{,}4 \times 10^{38}$. Da die Oberfläche der Erde (alles zusammen, also Wasser und Land) in etwa 511 Millionen Quadratmeter aufweist, haben wir für jeden Quadratmeter $6{,}6 \times 10^{23}$ Adressen zur Verfügung.

Das ist mehr als die Zahl von Avogadro ($6{,}023 \times 10^{23}$ Atome). Im Chemieunterricht erfährt man dazu, daß diese Zahl der Molekülmasse eines Stoffes in Gramm entspricht. Für Luft bedeutet das etwas mehr als 14 Gramm.

Die Anzahl der Luftmoleküle in einem cm^3 Luft in Bodennähe ist lediglich 1/10000 davon (die Luftdichte bei 1013 mbar ist 1,29 mg / cm^3).

Das heißt wir könnten jedem Luftmolekül auf dem Globus bis 100 Meter Höhe eine eigene IP – Adresse geben.

Das ist natürlich nicht die ganze Wahrheit, auch bei Ipv6 hat man bestimmte Bereiche definiert. Dadurch kommt es zwangsläufig zu Ineffizienz.

Ein Vergleich mit dem System der Telefonnumern macht diese Art „Verschwendung“ schnell deutlich: Ein Bereich definiert sich durch seine Vorwahl, und darin wiederum gibt es beispielsweise sechsstellige Telefonnummern. Damit könnten also 999999 Teilnehmer erreicht werden. Hat der Bereich nur 15000 Teilnehmer, sind die restlichen 984999 ungenutzt.

So ein Problem haben ja auch die schon genannten B – Netzadressen bei Ipv4, wo selten alle 16384 Adressen genutzt sind.

Ein schlauer Mensch hat jedenfalls ausgerechnet, daß auch bei schlechtester Ausnutzung der festgelegten Strukturierung von Ipv6 immer nochmehr als1000 Adressen pro Quadratmeter auf der Erde geboten sind (RFC 1715).

Im Moment sind knapp 30 % des verfügbaren Adressraums verplant. Ein paar Bereiche sollen hier erwähnt sein:

Ganz wichtig in der Übergangsphase: Adressen mit 80 Nullen zu Beginn stehen für die alten IPV4 – Adressen, die so durch den neuen Adressraum geschleust werden können. Alte IP-Adressen können wie folgt geschrieben sein:

::192.31.20.46

Andere Bereiche (natürlich gibt es noch mehr ...):

`010x xxxx xxxx`	Service Provider
`100x xxxx xxxx`	Geographische Bereiche
`1111 1110 11xx`	Lokale Adressen

Namensauflösung

Seit Computer vernetzt werden, gibt man ihnen Namen. Abgesehen davon, daß die Benutzer mit Namen mehr anfangen können, als mit mehr oder weniger kryptischen Adressen, auch Programme greifen auf Netzwerkressourcen via Namen in Form von ASCII – Zeichenketten zu.

ASCII ist kurz gesagt, ein Code, bei dem in einer Tabelle 256 alphanumerischen Zeichen und anderen Symbolen je ein 8-Bit – Wert zugeordnet ist.

Frühzeitigen Ansätze in Sachen Namensgebung sind NetBIOS und DNS. Beide haben es bis heute geschafft zu überleben.

NetBIOS, (NetBEUI)

Beides ist von IBM entwickelt, NetBIOS war ursprünglich gedacht als Protokoll zur Kommuniktion zwischen Mainframe (Hauptrechner) und daran angeschlossenen Terminals.

NetBIOS steht für Network Input Output System.

Es deckt von sich aus die OSI – Schichten 3 bis 5 ab. NetBIOS nutzt keine Adressen, sondern Rechnernamen für die Kommunikation mit anderen Stationen im Netzwerk. Die Rechnernamen werden in entsprechenden NetBIOS-Tabellen gehalten.

Der formale Begriff für die Verbindung zweier Stationen miteinander ist die Sitzung/Session . Eine Station kann zur gleichen Zeit mehrere Sitzungen mit mehreren oder nur einer Station haben

Die Kommunikation startet zunächst immer als Broadcast (Sendung an alle). Der Angesprochene (der mit dem gewünschten Namen) antwortet, alle anderen verwerfen die Anfrage.

Es ist möglich, mit NetBIOS unterschiedliche Topologien und Übertragungsprotokolle auf Ebene 2 zu verwenden. Das läuft am Ende darauf hinaus, NetBIOS – Namen mit Hardware (MAC-) Adressen zu verknüpfen.

Für Routing auf der Schicht 3 (Vermittlungsschicht) bietet NetBIOS keine Funktionen an. Deshalb hat man es so gestaltet, daß es quasi in Huckepack – Manier auf andere, routingfähige Protokolle, etwa TCP/IP, aufgesetzt werden kann. Dann arbeitet es nur noch auf der Schicht 5 bzw 4 und 5, wenn TCP nicht benutzt wird.

Oft wird allerdings NetBIOS zusammen mit einem anderen, nicht routingfähigen Protokoll eingesetzt. NetBEUI stammt auch von IBM, findet sich aber ebenso in den Microsoft Windows Betrriebssystemen, was ihm zu großer Verbreitung verholfen hat.

NetBEUI hat einige zusätzliche Funktionen, etwa die Suche nach einem Server oder die Anpassung der Größe von Datenpaketen nach Erfordernissen, das seinen Einsatz in kleinen Netzen mit wenigen Rechnern sinnvoll macht. Es hat dort eine höhere Effizienz als die routingfähigen Protokolle und deshalb durchaus seine Berechtigung.

NetBIOS ist auch in Verbindung mit NetBEUI auf Schicht 5 reduziert. Beide werden oft wegen ihres gemeinsamen Auftretens und der Namensähnlichkeit fälschlicherweise gleichgesetzt oder verwechselt.

Namensdienste

Routingfähige Protokolle müssen auf der Schicht 3 mit logischen Adressen arbeiten. Bei TCP/IP sind das die IP – Adressen. Da auf Anwendungsebene normalerweise Rechnernamen verwendet werden, müssen diese bei der Netzwerkkommunikation in zugehörige IP – Adressen gewandelt werden. Diese Adressen sind die Grundlage der Kommunikation über verschiedene Teilnetze.

Erst im Zielnetz angekommen kann mittels ARP – Protokoll auf die Ebene der MAC – Adressen heruntergegangen werden, um ein Paket zuzustellen.

Die Notwendigkeit dieser Zuordnung, Rechnernamen zu IP – Adressen, hat die Namensdienste WINS (Windows Internet Name System) und DNS (Domain Name System) hervorgebracht. Diese finden wir übrigens auf der Schicht 7 des OSI – Modells.

Ein Server, der diese Namensdienste bereitstellt, heißt demzufolge DNS – Server beziehungsweise WINS - Server

Groß in Fahrt gekommen ist NetBIOS in Verbindung mit TCP/IP (oft als NetBIOS over IP) bezeichnet. Hier sind ja nun wie gesagt logiche (IP-) Adressen im Spiel, es müssen also die NetBIOS – Namen nicht mehr direkt den Hardwarwadressen zugeordnet werden. Dies ist auch gar nicht möglich, da NetBIOS in Verbindung mit anderen Netzwerkprotokollen nicht mehr direkt mit der Schicht 2 kommuniziert, sondern eben mit Schicht 3 oder 4.

Beide genannten Namensdienste haben sozusagen klein angefangen. Ursprünglich bestand die ganze Zuordnungstabelle (Namen zu IP- Adressen) in einer Textdatei, die auf jedem Rechner (Host) an einer bestimmten Stelle des Verzeichnisbaums innerhalb des Betriebssystems liegt.

Für DNS heißt diese Datei einfach HOSTS, bei WINS hat man daraus LMHOSTS gemacht. Die Dateinamen sind ohne Endung (.txt oder dergleichen ...).

Beispieleinträge einer hosts

```
102.54.94.97     rhino.acme.com          # Quellserver
38.25.63.10      x.acme.com              # x-Clienthost
127.0.0.1        localhost
```

Beispieleinträge einer lmhosts

```
102.54.94.97   maestro         #PRE #DOM:technik
102.54.94.102     PC001
102.54.94.123  nordpol         #PRE
```

Beide Dateien sind nach wie vor auf allen Rechnern, die TCP/IP installiert haben, vorhanden (LMHOSTS aber nur auf Windows – Maschinen, andere Betriebssysteme kennen NetBIOS, aber kein WINS).

Selbstverständlich funktionieren diese Dateien auch nach wie vor, wenn man sie mit den entsprechenden Daten füllt. Dabei muß man sogar aufpassen, denn die Auswertung der hier definierten Zuordnung hat Priorität vor der Abfrage irgendwelcher Namensserver.

Die Abfrage bricht ab, wenn ein Eintrag zum gesuchten Namen gefunden ist. Ist dies ein fehlerhafter Eintrag in der HOSTS, wird kein Namensserver mehr abgefragt. Die Tatsache, daß in dem Fall keine Verbindung zustande kommt, wird als Nicht – Erreichbarkeit des Adressaten gewertet und nicht als falsche Adresszuordnung.

Das Unterhalten der Dateien HOSTS und LMHOSTS ist bei einer großen Zahl beteiligter Stationen natürlich extrem aufwendig und im Internet wäre das Verfahren wohl kaum noch praktikabel.

Aus diesem Grund ist man dazu übergegangen, in Netzwerken Dienste zu unterhalten, die an zentraler Stelle eine Datenbank mit allen Namen und Adressen führen. Ein derartiger Dienst läuft auf einem Server.

Clients haben in ihrer Konfiguration diesen Namensserver eingetragen und sind so in der Lage, bei Beginn der Kommunikation diesen direkt nach der gewünschten Adresse zu fragen.

Nebenbei haben Namensdienste noch einen positiven Effekt. Sie reduzieren, egal ob mit Textdatei oder zentraler Datenbank, den Netzwerkverkehr. NetBIOS – Namensanfragen werden standardmäßig an alle im Netz geschickt (Broadcast). In der Hoffnung, daß auch der Angesprochene die Anfrage mitbekommt.

Fragt man stattdessen gleich einen, der sich auskennt, also in unserem Fall den Namensserver oder die HOSTS/LMHOSTS, braucht man die Unbeteiligten gar nicht behelligen. Also spart man viel Broadcastverkehr im Netz.

WINS (Windows Internet Name System)

Microsoft hat WINS in Zusammenhang mit Windows NT als Netzwerkdienst eingeführt. Er funktioniert, einmal gestartet, weitgehend automatisch.

WINS – Clients sind so konfiguriert, daß sie die Adresse des WINS – Servers kennen. Stimmt alles, tragen sie sich selbst in die Datenbank ein. Diese Datenbank ist flach, hat also keinerlei hierarchische Strukturen. Fährt ein WINS – Client herunter, meldet er sich auch selbst wieder ab.. Auch dann, wenn er immer an bleibt, wird sein Datenbankeintrag periodisch erneuert.

Nicht nur Rechner-, sondern auch Benutzer- und (NT-) – Domänennamen finden sich im WINS – Dienst.

Der Abfragevorgang kann mittels Knotentypen eingestellt werden. Davon gibt es vier.

B-Knoten: Nur Broadcast
P-Knoten: (Peer) Nur direkte Abfrage des Namensservers
M-Knoten: (Mixed) Erst Broadcast, dann Abfrage des Namensservers
H-Knoten: Erst Abfrage des Namensservers, dann Broadcast

Das Ganze funktioniert auch über Router hinweg. Es muß also nicht in jedem Subnetz ein WINS – Server laufen. Clients stellen ja ihre Anfragen an eine bestimmte Adresse (eben die des WINS – Servers), also nicht via Broadcast.

Hat man mehrere WINS – Server (einen pro Subnetz), tauschen diese ihre Informationen untereinander aus. Dazu muß man sie vorher gegenseitig als Replikationspartner einrichten. Das passiert nicht automatisch.

So ist gewährleistet, daß alle Namensanfragen im jeweiligen Subnetz bleiben. Außerdem wissen alle auch über die Namen der anderen Netze Bescheid. Das heißt, Clients erfahren von „Ihrem“ Server auch die Namen der Systeme in den anderen Netzen.

Die Replikation der WINS – Server untereinander (wann und mit wem) kann auch in weiten Bereichen eingestellt werden. Mehrere WINS – Server in einem Subnetz sollte man keinesfalls vorsehen.

Da auch andere Betriebssysteme NetBIOS können, aber kein WINS, gibt es da noch ein Hintertürchen, um auch diese in die WINS – Datenbank zu bekommen.

Ein Windows PC ab Wndow 95 – Client (oder Server) kann als WINS – Proxy eingerichtet werden. Der fängt die NetBIOS – Aufrufe (Broadcasts) beispielsweise von Unix – oder Novell – Maschinen auf und leitet sie an den WINS – Server weiter (und beantwortet sie dann). Der WINS – Proxy muß dazu natürlich im selben Subnetz stehen wie die Clients, die selber nur NetBIOS, aber kein WINS kennen.

Der WINS – Proxy ermöglicht so auch Nicht-WINS Clients die Abfrage des WINS – Servers. Diese Clients können also auch auf Rechner in anderen Subnetzen zugreifen, wenn diese in der WINS – Datenbank stehen.

Sollen WINS – Clients, also Microsoft – Maschinen, mit einer nicht WINS – fähigen Maschine im anderen als ihrem eigenen Subnetz kommunizieren, dann muß der WINS – Server einen statischen Eintrag für diesen Host enthalten.

Der WINS – Proxy übernimmt die Namensauflösung für die Clients, die kein WINS beherrschen. Er trägt deren Adressinformationen allerdings nicht in die WINS – Datenbank ein. Selbsttätig registrieren sich dort nur WINS – Clients.

Neuere Microsoft – Betriebssysteme, ab Windows 2000, sind nicht mehr auf WINS und NetBIOS – Namen angewiesen. Hier ist man, wie in der Unix – Welt schon lange, zu DNS übergegangen.

Dennoch wird WINS noch lange benutzt werden, da viele Netze darauf basieren, die nicht einfach von heute auf morgen abgelöst werden. In kleinen Netzen spricht ohnehin nichts dagegen, wenn nur Microsoft – Betriebssysteme beteiligt sind. WINS erfordert so gut wie keine Konfiguration, was man von DNS nicht gerade behaupten kann.

Ähnlich wie bei der TCP/IP – Konfiguration ist ab Windows 2000 mittlerweile auch das Einrichten eines DNS – Servers fast automatisch. (Dennoch schadet es nicht, zu wissen, was da passiert).

Allerdings unterstützt mittlerweile auch DNS die dynamische Registrierung. Das bedeutet, ein Rechner, entsprechend konfiguriert, kann seinen Eintrag in der DNS – Datenbank selbst vornehmen.

Man wird auch in Zukunft noch viele PC' s unter Windows 2000 oder XP als WINS – Clients einrichten.

Daß WINS, vor allem aufgrund fehlender Strukturierung, nicht unbedingt für große Netze gedacht ist, schon gar nicht für weltweite Dimensionen, hat wie gesagt, selbst Microsoft dazu veranlaßt, seine Basis auf DNS umzustellen.

DNS (Domain Name System)

1983 eingeführt, etwa ab 1986 gibt es die heutige Version

So lange nicht mehr als einige hundert Rechner im Internet waren, konnte die hosts – Datei ihre Dienste tun. Automatisiert wurde das Verfahren noch dadurch, daß sich alle Beteiligten nachts die aktuelle Version von der Stelle, wo sie gepflegt wurde, abgeholt haben.

Nachdem die Zahl der Stationen immer mehr in die Tausende ging, war klar, daß diese Methode der Namensauflösung nicht beizubehalten ist.

Eine einzige zentrale Verwaltung ist bei den Dimensionen des Internet völlig unmöglich. Eine hierarchische Organisationsstruktur, die die Verwaltung auf viele Stellen aufteilt, ist deswegen angestrebt worden. Abgesehen davon wäre die hosts-Datei mittlerweile viel zu groß.

DNS ist demzufolge aufgebaut als hierarchisches Benennungsschema, das auf den sogenannten Dömänen basiert. Des weiteren ist die Datenbank, die dieses Schema enthält, auf viele Server verteilt.

Die grundsätzliche Funktion ist wie gesagt Namen (also ASCII – Zeichenketten) in IP – Adressen umzuwandeln. Dazu ruft ein Anwendungsprogramm eine Prozedur auf, die Resolver genannt wird. Der Resolver sendet die Anfrage in Form eines UDP – Paketes an den lokalen DNS – Server. Der sucht den Namen aus seiner Datenbank und gibt dem Resolver die zugehörige IP – Adresse aus. Der Resolver gibt dann die IP – Adresse an das Anwendungsprogramm aus, so daß dieses eine TCP – Verbindung zum Ziel aufbauen oder UDP – Pakete dorthin versenden kann.

Zur Erinnerung: Ob UDP oder TCP hängt davon ab., ob das Anwendungsprogramm die Abfolge der Pakete oder Flußkontrolle lieber selbst übernimmt oder dies eben TCP überläßt.

Auch der DNS – Dienst benutzt für seine Daten eine ganz normale Textdatei.

Die hierarchische Struktur von DNS kann man vergleichen mit der des Postsystems. Hier geschieht die Verwaltung der Namen durch eine Angabe von Land, Stadt, Straße, Hausnummer und Namen des Adressaten. Es gibt also keine Verwechslung zwischen einem Günter Stagge in der Karlstraße in Karlsruhe und einem in der Uhlandstraße in Köln.

DNS funktioniert genauso. Anstelle von Städten hat man hier die Domänen. Analog zu Hauptstädten, Landeshauptstädten, Regierungsbezirken, Kreisstädten usw gibt es im DNS verschiedene Ebenen.

Ganz oben steht die Rootdomäne, durch einen Punkt (.) dargestellt, der aber in den Namen nie aufgeführt wird.

Die obere Ebene (die unter der Root) ist in zwei Bereiche unterteilt: Allgemein und Länder.

Allgemeine Domänen sind:

com (commercial)
edu (educational)
gov (US Bundesregierung)
int (internationale Organisationen)
mil (US Streitkräfte)
net (Netzbetreiber und –Anbieter)
org (nicht gewinnorientierte Organisationen, etwa Universitäten)

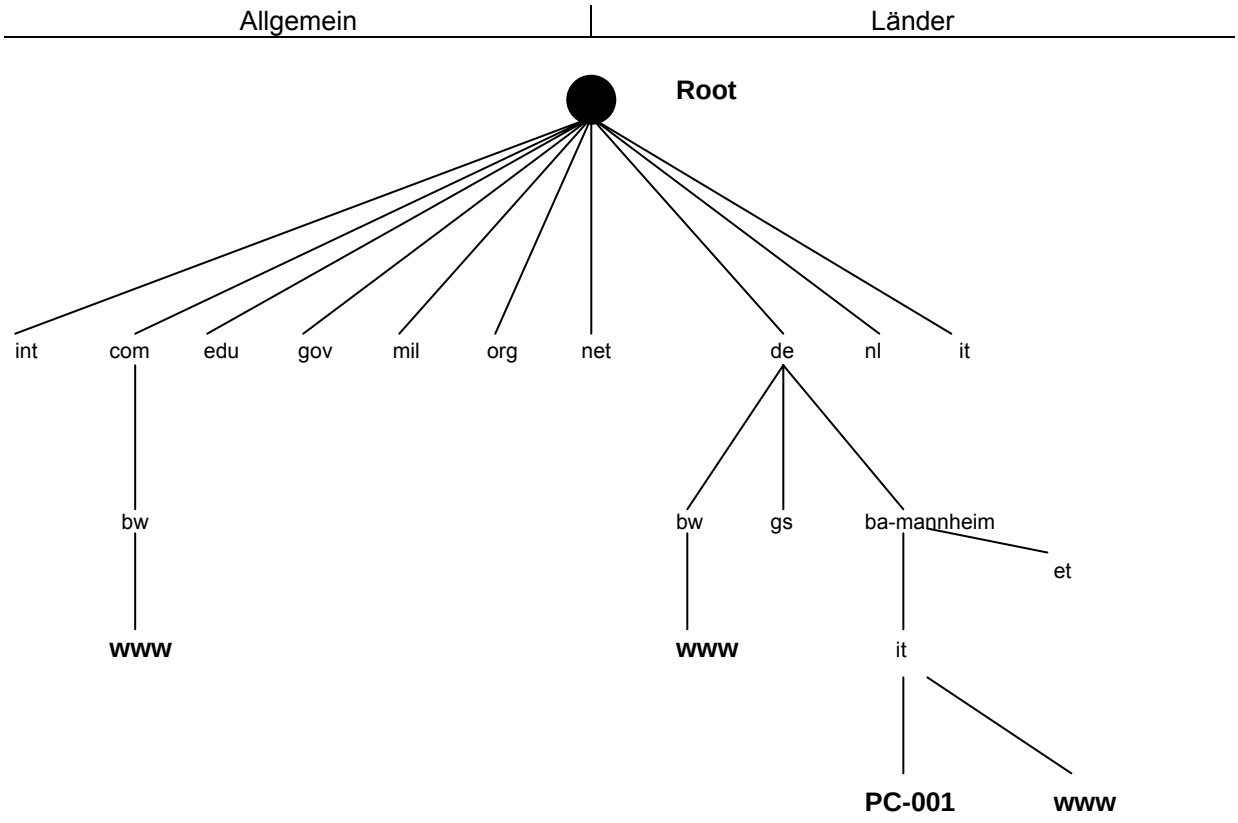
Die Länder – Domänen umfassen einen Eintrag für jedes Land. Auch hierfür gibt es übrigens eine ISO – Definition, die ISO 3166. Deutschland ist hier beispielsweise unter de geführt, die Niederlande unter nl, Italien unter it und so weiter...

Jede Domäne ist in Unterdomänen unterteilt, die Unterdomänen wiederum in Unterdomänen. Das ergibt eine Baumstuktur.

In jeder dieser Ebenen steht normalerweise eine mehr oder weniger große Zahl von Rechnern.

Die Bezeichnung einer Domäne geschieht von ihrem Pfad aus nach oben bis zur Wurzel (die allerdings normalerweise unbenannt bleibt, siehe oben).

Groß- und Kleinschreibung spielen hier keine Rolle. Ein zusammengesetzter (Domänen-) Name darf maximal 63 Zeichen lang sein. Der gesamte Pfad ist auf 255 Zeichen begrenzt. Ein kompletter Name wird als FQDN (Fully Qualified Domain Name) bezeichnet.



Die Dezentralisierung bei der Verwaltung erreicht man, indem jede Domäne die unter ihr liegenden Domänen verwaltet. Um eine neue Domäne anzulegen, ist die Genehmigung der übergeordneten Domäne erforderlich.

Den Vorgang nennt man Delegieren. Das heißt, die (nach der Delegation) übergeordnete Domäne, welche alles ab ihrer Ebene abwärts verwaltet, delegiert die Zuständigkeit bestimmter Hosts an eine Unterdomäne.

Die in Deutschland ansässige Domäne bw im Bild oben könnte sich entweder unter com oder de registrieren lassen. Denkbar wäre auch, daß es zwei Domänen bw in Deutschland gibt. Die erste wurde unter de registriert, die zweite hatte dann nur die Möglichkeit, einen anderen Namen zu wählen, oder sich eben beispielsweise unter com einzuklinken, wenn dahinter ein kommerzielles Untenehmen steht. Ein Netzanbieter würde eher net wählen.

Beide können www anbieten und sind dennoch eindeutig zu unterscheiden.
Am Beispiel der Domäne it.ba-mannheim.de sollen weitere Details erklärt werden.

Möchte der Fachbereich Informationstechnik in der BA Mannheim die Domäne it.ba-mannheim.de gründen, muß sie den fragen, der ba-mannheim.de verwaltet. Die Einrichtung von ba-mannheim selber hingegen wurde bei de beantragt.

Die Unterteilung in Domänen ist rein organisatorisch und hat mit physikalischen Netzstrukturen nichts zu tun. Eine zweite Domäne in ba-mannheim könnte also durchaus im selben LAN beheimatet sein. Ebenso wäre es denkbar, Teile von it ganz woanders in einen getrennten Standort zu betreiben.

Der Rechner PC-001 oben im Bild würde mit vollem Namen pc-001.it.ba-mannheim.de heißen.

Hier wird auch ein weiterer Effekt der Hierarchie deutlich. (Der erste war ja die dezentrale Verwaltung). Der Name PC-001 könnte in jeder Domäne benutzt werden. Das ist ja ein relativer Name, das heißt, er muß in einem Zusammenhang interpretiert werden. Innerhalb des Fachbereichs Informationstechnik wird auch bestimmt jeder nur diesen Namen verwenden, da der Zusammenhang (Mitglied von it ...) jedem dort klar ist.

Absolute Namen (FQDN) enden hingegen ganz oben bei der Rootdomäne, also in der Schreibweise müßte genaugenommen sogar immer noch ein Punkt am Ende stehen.

Damit wird jetzt auch die Geschichte mit dem world wide web deutlich. Jeder, der eine Domäne betreibt und einen www – Dienst anbietet, braucht nichts weiter zu tun als einen entsprechenden Server aufzustellen und diesen www zu nennen. Dabei muß der Server im internen Netz noch nicht einmal so heißen. Der DNS – Server, der für die Domäne zuständig ist und bei www – Anfragen dessen Adresse herausgibt, muß diesen Server natürlich unter dem Namen www führen.

Zunächst wirkt der Ansatz mit verschiedenen Namen intern und extern vielleicht etwas weit hergeholt. Sinn hat diese Konstruktion aber durchaus. Ein Fachbereich mag ja mit einem Server für seine Dienste gut auskommen.

Handelt es sich aber um ein größeres Angebot, das entsprechend viele Anfragen generiert, muß die Last eventuell auf mehrere Schultern, sprich Server aufgeteilt werden. Dazu muß man selbstverständlich auch mehrere (inhaltlich identische) Server in meinem Netz aufstellen.

Nun gilt in jedem Netz erst einmal, daß Namen und IP – Adressen nicht mehrfach vorkommen dürfen. Drei Server, auch wenn sie, wie in unserem Fall, genau dasselbe tun, treten demzufolge mit drei verschiedenen Namen (und Adressen) in Erscheinung.

Der DNS – Server kann hingegen für alle drei IP – Adressen denselben Namen in seiner Tabelle vorhalten. Das geschieht in einer speziellen Anordnung, die Namen stehen untereinander und werden der Reihenfolge nach abgearbeitet.

Das Verfahren heißt Round Robin und verteilt die Last, indem die Anfragen herumgereicht werden. Die erste Anfrage an Server 1 , die zweite an Server 2, die dritte an Server 3, die vierte wieder an Server 1 ...

Im Bild oben gibt es in der BA Mannheim aber nur einen www – Server, der folgerichtig www.it.ba-mannheim.de heißt.

Jeder, der im Internet surft, stellt früher oder später fest, daß es auch Namen ohne www gibt.

Das kann zum einen deshalb der Fall sein, weil es sich um einen Dienst handelt, der unter anderem Namen bekannt ist , etwa ftp. Auf viele Downloadseiten trifft das zu.

Aber auch dann, wenn unsere Domäne it.ba-mannheim.de einen weiteren Webserver, der andere Inhalte als der erste bereitstellt, installiert, kann der ja nicht auch www heißen. Dazu müßte dann eine zusätzliche Domäne aufgemacht werden.

Denkbar wäre hier, daß die Hauptseite auf dem Server www liegt, viele Links, die dort angeboten werden, aber auf den zweiten Server zeigen, auf dem sich die dahinterliegenden Inhalte befinden. Die Namen der Seiten auf dem zweiten Server enthalten dann logischerweise kein www.

Namensserver und Zonen

DNS - Namensserver sind fast immer Unix oder Linux – Maschinen. Die dort verwendete Technik wird BIND genannt. BIND steht für Berkeley Internet Name Domain.

Wie schon erwähnt ist ja die Berkeley University die Wurzel (nicht allen Übels), aber quasi der Geburtsort von TCP/IP und auch der Vorgänger des Internet (ARPANET) und DNS (HOSTS).

Mit der Einführung von Windows 2000 hat sich nun auch Microsoft DNS verschrieben. Interessant ist, daß DNS nach wie vor seine Zoneninformationen in Textdateien ablegt. Diese Zonendateien haben allerdings unterschiedliche Namen bei BIND und Microsoft.

BIND:	db.*domäne* db.w.x.y
Windows 2000:	*domäne*.dns y.x.w-in-addr.arpa.dns

w.x.y stehen für die zugehörigen Netzwerkadressen. Domäne ist der Name der verwalteten Domäne, für die der Namensserver (autorativ) zuständig ist.

Ein Netz mit der Adresse 192.168.1.0 hätte den Dateinamen db.192.168.1 bzw 1.168.192-in-addr.arpa.dns für die Zonendatei der Reverse – Lookupzone.

Die zwei Dateien haben auch wieder, wie könnte es anders sein, ihre Ursache in der Existenz zweier verschiedener Zonen.

Die Aufgabe, die ein DNS – Server hat, wird Lookup genannt.

Dabei gibt es die Forward – Lookup – Zone, die für die übliche Auflösung von Namen in IP – Adressen verantwortlich ist.

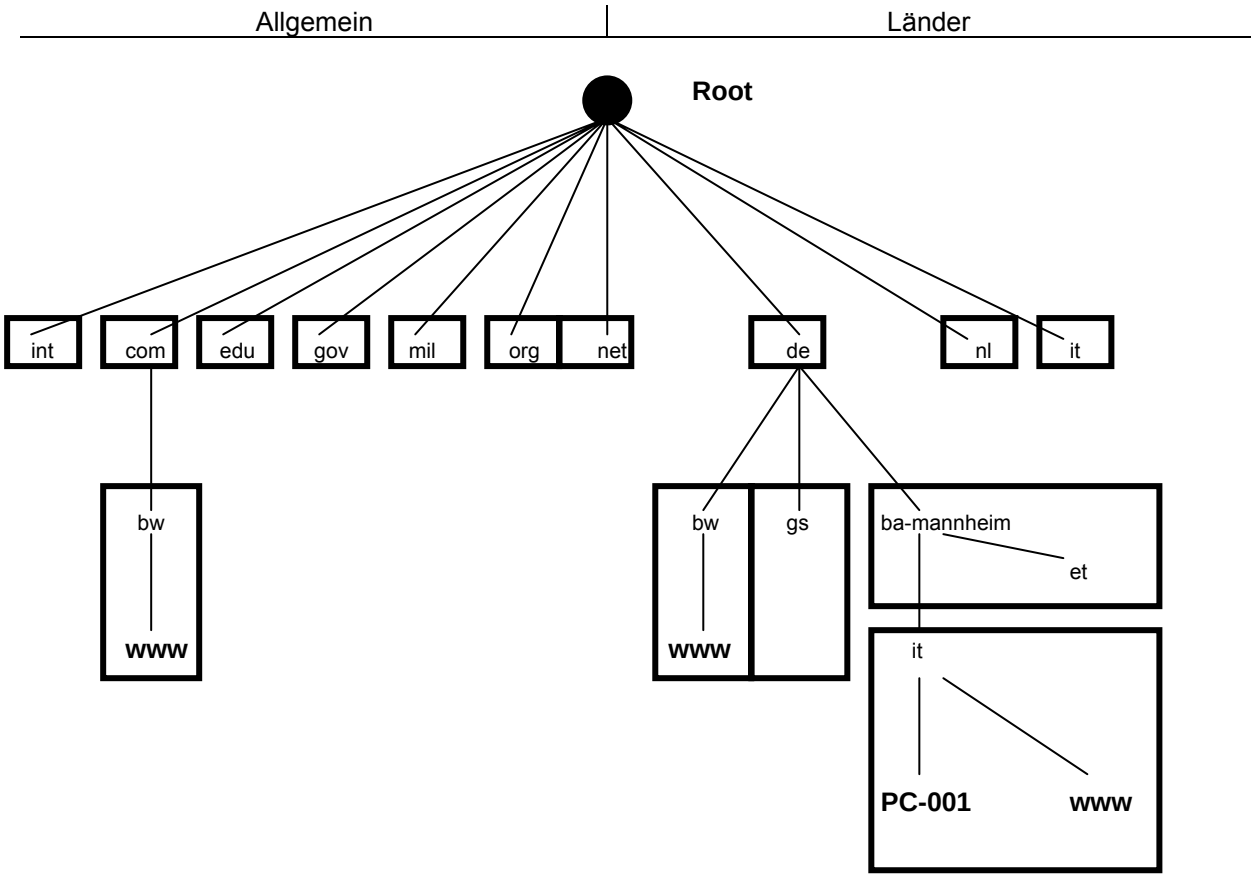
Auch der umgekehrte Vorgang, also die Suche nach einem Namen zu einer gegebenen IP – Adresse, ist bei DNS vorgesehen. Die dafür eigens eingerichtete Zone ist die Reverse – Lookup – Zone.

Für Reverse – Lookup wurde eigens eine Domäne im DNS – Namensraum (auf der obersten Root-Ebene) eingerichtet. Sie heißt in-addr.arpa.

In-addr.arpa untergeordnete Domänen bildet man durch Umkehren der Netzadresse mit Anhängen des Namens. Ein Netz mit der Adresse 172.16.0.0 (B-Netz) bildet die (Reverse-Lookup-) Unterdomäne 16.172.in-addr.arpa.

Unten das bereits bekannte Bild, ergänzt durch Zonengrenzen, also Bereiche, die von einem bestimmten Namensserver verwaltet werden.

Innerhalb jeder dieser Zonen wird es sicherlich auch sekundäre Zonen geben. Reverse – Lookup – Zonen sind aber durchaus entbehrlich und könnten hier und da durchaus weggelassen auch werden.



Zonen sind im Gegensatz zu Domänen also Bereiche, die von einem Namensserver versorgt werden. Im Bild oben sind das die rechteckig umrandeten Gebiete. Ein Namensserver kann durchaus für mehr als eine Domäne zuständig sein. Wirklich machen wird man das aber kaum.

Zonen sind also nicht zwangsläufig identisch mit Domänen.

Theoretisch wäre es zwar möglich, die gesamten DNS – Namensdienste auf einem einzigen Namensserver laufen zu lassen. Sinnvoll ist das natürlich nicht. Auch hier ist Dezentralisierung zwecks Ausfallsicherung der Weg zum Ziel.

Zonen überlappen sich nicht. Jede Zone enthält einen bestimmen Teil des Domänen – Namensraumes und den/die Namensserver, die dort zuständig sind.

Überhaupt ist bei DNS bei fast allen Strukturierungen von Zonen die Rede.

Jede Zone enthält in der Regel einen primären Namensserver, der sie sogenannten autorativen Datensätze dieser Zone enthält. Die gesamten Sätze stehen in der sogenannten Zonendatei. Die Zonendatei ist vom Dateiformat her eine Standard – Textdatei, genau wie die gute alte HOSTS.

Autorative Datensätze stammen von der Stelle, die sie verwaltet, und sind demnach richtig.

Normalerweise gibt es innerhalb einer Zone immer noch sekundäre Namensserver zur Lastverteilung. Diese erhalten in regelmäßigen eine Kopie der Zonendatei des primären Servers. Inzwischen gibt es auch die Variante des inkrementiellen Updates. Das heißt, es muß nicht mehr wie früher üblich die gesamte Zonendatei übertragen werden.

Die Daten der sekundären Server werden nicht direkt geändert, sind also nur zum Auslesen gedacht.

Auch hier redet man wieder von Zonen, hier aus gegebenem Anlaß von primärer und sekundärer Zone. Diese beiden liegen innerhalb der Zone, die den Verwaltungsbereich des primären Namensservers darstellt.

Darüber hinaus unterscheidet man zwischen Master- und sekundären DNS – Servern.

Masterserver ist immer ein Server, von dem ein anderer seine Zoneninformation erhält. Auch ein sekundärer Server kann einen weiteren mit Informationen versorgen und ist für diesen wiederum der Masterserver.

Wo die Grenzen von Zonen liegen, hängt im wesentlichen davon ab, wo und wie viele (eigenes verwaltete bzw autorative) Namensserver gewünscht sind.

In der BA Mannheim oben im Bild hat die BA einen Namensserver für ba-mannheim.de, der aber nicht it.ba-mannheim.de bedient. Hier möchte der Fachbereich Informationstechnik einen eigenen Namensserver unterhalten, während die andern Fachbereiche, etwa Elektrotechnik (et) darauf keinen Wert legen.

It bildet also eine separate Zone, weil man dort einen eigenen Namensserver verwaltet.

Auch die Root ganz oben hat ihre Namensserver. Diese müssen im wesentlichen die zuständigen Server der darunterliegenden Domänen kennen. Die Rootserver kennt übrigens jeder DNS – Server automatisch, ohne daß er dafür extra eingerichtet werden müßte. Siehe dazu die Zonendatei Cache.dns am Ende dieses Kapitels.

Namensanfragen

Die Aufgabe, die ein DNS – Server hat, nennt man Lookup. Zwei Typen werden unterschieden.

Forward – Lookup:
Der häufigste Fall. Auflösung von Namen in Adressen

Reverse Lookup:
Auflösung von Adressen in Namen

Hat nun ein Resolver (DNS – Client) eine Anfrage zu einem bestimmten Domänennamen vorliegen, schickt er diese an den lokalen Namensserver weiter. Ist die gesuchte Domäne unter der Verwaltung des lokalen Namensservers, gibt der den autorativen Datensatz aus.

Es kann aber sein, daß sich die Anfrage auf ein entferntes Ziel bezieht. Nehmen wir an, der Resolver des PC-001 in it.ba-mannheim.de fragt nach der IP – Adresse von www.bw.com.

Der lokale Namensserver it.ba-mannheim.de wird gefragt, weiß aber nichts darüber, weil die Frage bislang noch nie gestellt worden ist.

Unser Resolver könnte noch bei ba-mannheim und bei de anfragen, und wenn die alle nichts wissen, com befragen.

Der für com zuständige DNS – Server wiederum fragt bei bw (bw.com, nicht bw.de !). Dort müssen ja die gesuchten autorativen Datensätze liegen.

Genau genommen fragt der DNS – Client (irgendein PC) nur den DNS – Server, der in seiner Konfiguration eingetragen ist (rekursiv), die weitere Abfragerei bis zum Ziel (iterativ) erledigt dann der DNS – Server. Erst wenn der die gewünschte Adresse in Erfahrung gebracht hat, gibt er sie an den Client zurück. Dazu weiter unten noch etwas mehr.

Jeder Server, der die gesuchten Informationen nicht hat und deshalb woanders suchen muß, berichtet zurück an seinen Vorgänger. Das ist wichtig, damit derjenige, der gefragt hat, nicht „ungeduldig“ wird, während die Abfragen sich durch den DNS – Baum hangeln. So kommt die gewünschte Information irgendwann bei it.ba-mannheim an und wird dort eine Weile zwischengespeichert, falls weitere Anfragen kommen.

Die zwischengespeicherte Information ist nicht autorativ, weil Änderungen in irgendeiner Zone natürlich nicht in alle Zwischenspeicher (Caches) der Welt gestellt werden.

Jeder Datensatz hat deshalb auch eine TTL -Angabe (Time to live). Damit wissen entfernte Namensserver, die Einträge zwischenspeichern, wie lange diese aufgehoben werden sollen.

Das kann von Sekunden bis zu einem Tag dauern. Diese Zeitspanne legt natürlich der Verwalter fest, sie wird also vom autorativen Datensatz bestimmt.

Die ganze Abfragekette endet, wenn einer der Befragten die Information hat. Nur wenn alle Caches diesbezüglich leer sind (oder die dort gespeicherten Informationen mittlerweile falsch sind), geht die Anfrage wirklich bis zu den autorativen Datensätzen.

Hat man einen DNS – Server, der schon einige Zeit seinen Cache gefüllt hat, kann dieser die meisten Anfragen direkt beantworten. Deshalb ist das Neustarten eines solchen Servers oft dafür verantwortlich, daß das Internet in Firmennetzten erstmal zäh wirkt. Die ganze Sucherei bis zu den autorativen Daten geht für jeden Internetzugriff wieder von vorne los.

Es ist auch möglich, DNS – Server zu unterhalten, ohne eine eigene Zone zu verwalten. Dies sind dann reine Cacheserver, die alle Adresszuordnungen entsprechend ihrer TTL zwischenspeichern. Clients werden also bereits hier in der Regel für häufig benutzte Adressen die Adressinformation bekommen.

Damit kann beispielsweise eine WAN – Leitung zu einem Außenbüro entlastet werden, ohne daß man gleich eine neue Zone erfinden muß.

Normalerweise hat jeder DNS – Server einen anderen konfiguriert, an den er Namensanfragen richten kann, die er selber nicht beantworten kann. Versäumt man dies, funktioniert die Sache trotzdem, da ja wie erwähnt die Rootserver auf jeden Fall bekannt sind.

Noch mal ein genauerer Blick auf die beiden Abfragetypen

Rekursiv: Ein Clientcomputer fragt seinen lokalen DNS – Server nach der Adresse, die hinter einem Namen steht. Anschließend wartet er auf dessen Antwort. Egal, was dieser DNS – Server alles noch anstellen muß, um an die gewünschte Information zu kommen. Dieser DNS –Server ist derjenige, der in der Client – Netzwerkkonfiguration eingetragen ist.

Iterativ: Wird von DNS – Servern benutzt, um an Adressinformationen zu kommen.

1 Der Client PC001 generiert seine (rekursive) Abfrage nach der Adresse von www.bw.com.

2 Der lokale DNS – Server it.ba-mannheim.de weiß die Adresse nicht. Er fragt bei ba-mannheim.de.

3 ba-mannheim.de hat auch keinen Eintrag. Als Antwort schickt er daher nicht die gewünschte Adresse, sondern eine Liste von Adressen der Server, die für de zuständig sind (autorativ).

4 Mit dieser Information ist it.ba.mannheim.de in der Lage, einen DNS – Server zu befragen, der de versorgt.

5 Auch dort ist die Adresse nicht verfügbar. Es wird nun deswegen eine Liste der com – DNS – Server an it.ba-mannheim zurückgelierfert.

6 Unser it – DNS – Server kann nun also bei com weiterfragen. Der Befragte hat auch keine Kenntnis, hat aber wiederum die Information, wer für bw.com zuständig ist. Das erfährt nun also unser it – DNS – Server.

7 it.ba-mannheim.com fragt also einen DNS – Server, der bw.com verwaltet und bekommt dort endlich die gewünschte Antwort. Dort sollte sich ja der autorative Datensatz für www.bw.com finden.

8 Der lokale DNS – Server bekommt also die Adresse und gibt sie an den fragenden Client weiter. Nebenbei speichert er die Namenszuordnung entsprechend der TTL und kann weitere gleichartige Anfragen direkt beantworten.

Informationen in einer Zonendatei

Eine DNS – Zonendatei enthält so allerlei verschiedene Dinge. Diese unterscheiden sich in ihrer Bezeichnung und Funktion. Die wichtigsten Eintragstypen (A, NS, CNAME, MX seien hier mal erwähnt.

A: Der wichtigste. Bildet Namen auf IP – Adressen ab.

NS: Nameserver. Definiert die für eine Zone autorisierenden Nameserver.

CNAME: Weiterer Name für einen Host, der schon einen A – Eintrag hat. Etwa dann, wenn man intern einen Servernamen anders haben möchte als extern. Also beispielsweise Server01 als interner Name und www extern.

MX: Mail Exchanger. Der Server, an den sich Mail – Anwendungen halten.

Beispiel hier: Mailserver BWC01, BWC02, die in der Domäne bw.com den Mailaustausch bewerkstelligen. BWC01 ist auch noch Webserver (www).

Bwc01.bw.com	86400	A		10.47.32.21	
Bwc02.bw.com	86400	A		10.47.64.15	
Bw.com	86400	MX	1	bwc01.bw.com	
Bw.com	86400	MX	2	bwc02.bw.com	
www.bw.com	86400	CNAME		bwc01.bw.com	

Man erkennt: Nur A – Einträge bilden IP – Adressen auf Namen ab. Diese A – Einträge benötigt jeder Host. Ganz egal, ob er noch weitere Einträge bekommt.

Alle weiteren Einträge (nicht A) bilden Namen auf andere Namen ab.

Im Beispiel oben sind die Server BWC01 und BWC02 erst einmal durch ihre A – Einträge bestimmten IP – Adressen zugeordnet.

Ihre Funktion als Mailserver bekommen sie durch die MX – Einträge. Hiermit wird klargestellt, daß alle Mails mit den Adressen *benutzername*@bw.com an die Server BWC01 und BWC02 gehen sollen.

Durch den CNAME – Eintrag ist sichergestellt, daß der Server bwc01.bw.com auch unter dem Namen www.bw.com ansprechbar ist. Damit wird der Webdienst angeboten.

Die Zahl 86400 bezeichnet die TTL dieser Einträge in Sekunden. Die Lebensdauer dieser Einträge in einem DNS – Cache beträgt also 24 Stunden.

Der Schluß dieses Kapitels gibt noch einen Blick auf die Zonendatei, die jeder DNS – Server automatisch mitbekommt und in denen die Rootserver der Root- bzw Stammdomäne eingetragen sind.

```
cache.dns -- DNS-ZWISCHENSPEICHERDATEI
;
;   Anfangs-Zwischenspeicherdaten für Stammdomänen-Server
;
;   FOLGENDES SOLLTE GEÄNDERT WERDEN:
;   ->  Ändern Sie nichts, wenn Sie mit dem Internet verbunden sind.
;       Bearbeiten Sie diese Datei nur, wenn die Liste der Stammnamens-
;       Server aktualisiert wurde.
;           ODER
;   ->  Entfernen Sie diese Einträge, und ersetzen Sie sie mit NS- und
;       A-Einträgen für den DNS-Server, der für die Stammdomäne Ihrer
;       Site autorisierend ist, wenn Sie NICHT mit dem Internet
;       verbunden sind.
;
;   Anmerkung: Wenn dies ein Stammdomänenserver ist, ist für Ihr
;   privates Intranet kein Zwischenspeicher erforderlich. Sie können
;   Ihre Boot-Datei bearbeiten, um ihn zu löschen.
;


;
;       Diese Datei enthält Informationen über Stammnamenserver, die
;       zum Initialisieren von Cache auf Internetdomänen-Namenserver
;       erforderlich sind (z. B. Verwenden Sie diese Datei als
;       Referenz in der Konfigurationsdatei "cache  .  <Datei>" der
;       BIND-Domänennamenerver).
;
;       Diese Datei wird von InterNIC-Registrierungsdienste unter
;       anonymen FTP zur Verfügung gestellt als:
;           Datei               /domain/named.root
;           auf Server          FTP.RS.INTERNIC.NET
;       -ODER- unter Gopher auf  RS.INTERNIC.NET
;           unter Menü          InterNIC-Registrierungsdienste (NSI)
;              Untermenü        InterNIC-Registrierungsarchive
;           Datei               named.root
;
;       Zuletzt aktualisiert:    22. August 1997
;       Verwandte Version der Stammzone:   1997082200
;


;
; formerly NS.INTERNIC.NET
;
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
;
```

```
; formerly AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
;
; temporarily housed at NSI (InterNIC)
;
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     198.41.0.10
;
; housed in LINX, operated by RIPE NCC
;
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
;
; temporarily housed at ISI (IANA)
;
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     198.32.64.12
;
; housed in Japan, operated by WIDE
;
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
; End of File
```

Netzwerkbetriebssysteme (ein Überblick ohne Anspruch auf Vollständigkeit, total subjektiv)

Verglichen mit Großrechnern waren und sind PC' s billig. Dieser Umstand hat zu ihrer schnellen Verbreitung geführt.

Als man anfing, anstelle von Großrechnern PC' s in Unternehmen einzusetzen, stellte sich leider bald ein Problem ein. Auf jedem dieser PC' s wurden Daten erzeugt, bearbeitet und gespeichert.

Das hatte zur Folge, daß praktisch alles mehrfach vorhanden war und Dateien in den unterschiedlichsten Versionen kursierten.

Der Austausch von Daten von PC zu PC ging mühsam mit Disketten vonstatten. Dieser Mühe mochte sich kaum jemand unterziehen, und deshalb wuchs das Chaos.

Um in einem solchen Umfeld eine vernünftige Datenhaltung zu gewährleisten, geht der Aufwand an Zeit und Personal gegen unendlich, wenn die Zahl der PC' s einmal zweistellige Dimensionen angenommen hat.

Der erste Ansatz zur Verbesserung hieß Vernetzung. In den Achtziger Jahren war allerdings eines schon weit gediehen: Die Vorherrschaft von Microsoft. Das Betriebssystem MS-DOS war auf praktisch jedem PC zu finden, und das war durchaus nicht netzwerkfähig.

Außerdem ist DOS ein 16 Bit – System, es konnte nur mit viel List und Tücke dazu überredet werden, überhaupt bis zu 1 MB Arbeitsspeicher zu adressieren. Genaugenommen läßt ich mit 16 Bit nämlich nur bis 64 k zählen.

1 MB war bald auch zu wenig, und so gibt es für DOS etliche Speichermanager, die mit noch mehr Tricks auch diese Speichergrenze umgehen.

Netzwerkbetriebssysteme sollten neben der eigentlichen Vernetzung zumindest zwei Dinge können:

1. Daten an einem zentralen Ort bereitstellen
2. Regeln, wer auf welche Daten zugreifen darf

Es kam die große Zeit der Firma Novell. Dort konzentrierte man sich darauf, ein Betriebssystem zu entwickeln, das Serverdienste und eine Zugriffskontrolle bereitstellen konnte. Die Clients liefen wie bisher unter DOS, das allerdings mit Netzwerksoftware und –Treibern von Novell aufgerüstet wurde.

Damit konnten DOS – PC' s via Netzwerk einen Server erreichen, auf dem Novell lief.

Als Netzwerk - Protololstapel nutzte man nicht etwa TCP/IP, sondern eine Eigenentwicklung, die den Namen IPX/SPX bekam.

Nun hatte man zwei Dinge: vernetzte Computer und die Möglichkeit der zentralen Datenhaltung und Zugriffskontrolle. Zusätzlich konnten auch Druckdienste zentral auf einem Novell – Server eingerichtet werden.

Ein anderes Betriebssystem, das von vornherein für die Vernetzung ausgelegt war, ist Unix. Es spielte eine große Rolle bei der Vernetzung der amerikanischen Universitäten, und in diesem Zusammenhang steht auch die Verbreitung von TCP/IP.

Es ist, (wie später das davon abgeleitete Linux) von Programmierern entwickelt, die selbst auch die Benutzer sind. Dementsprechend unübersichtlich ist alles aufgebaut. Das macht die Verbreitung auf Benutzer – PC' s so zäh.

Derartige Systeme in der EDV haben eine erstaunliche Überlebenskraft. Natürlich funktionieren Unix und Linux sehr gut, wenn man damit umgehen kann.

Programmierer, die für mehr oder weniger gleichgesinnte arbeiten, haben logischereweise überhaupt keine Vorstellung davon, was ein Anwender für Anforderungen stellt. Auf der anderen Seite stellt man fest, daß diejenigen, die so etwas gut beherrschen, gar kein Interesse an einer einfacheren Bedienung haben.

Genau danach sieht Unix aus.

Besonders ohne graphische Oberflächen sind unter Unix selbst einfache Editoren mit den absurdesten Tastenkombinationen zu bedienen, und wer so etwas beherrscht, ist verständlicherweise stolz darauf und mag diesen Vorsprung nicht unbedingt gern abgeben.

Nichts desto trotz gilt Unix als stabile Serverplattform und ist es wohl auch. Es arbeitet mit 32 Bit und kann den gesamten installierten Arbeitsspeicher auch benutzen.

Die Philosophie, jeder Mausklick ein Neustart wie etwa bei Windows NT gilt hier außerdem nicht.

Ferner gibt es Unix für die verschiedendsten Hardwareplattformen, es muß also nicht ein Intel – kompatibler Server sein.

Noch etwas sei zur Ehrenrettung von Unix gesagt. Jemand , der 10 Jahre Windows hinter sich hat, muß Windows gut beherrschen, wenn man ihm eine normale Intelligenz unterstellt. Mit dieser Intelligenz wäre das aber wohl auch mit Unix möglich gewesen, selbst wenn der Einstieg dort wirklich ungleich schwieriger ist.

Viele Softwareprodukte sind außerdem sehr geeignet zu beweisen, daß eine graphische Oberfläche allein keine Benutzerfreundlichkeit garantiert. Auch unter Windows.

Man vergleiche nur einmal verschiedene Programme zur Videoverarbeitung...

Die Verbreitung von PC' s und MS-DOS veranlaßte damals IBM und Microsoft, gemeinsam ein neues Betriebssystem für diese Plattform zu entwickeln. Daraus wurde OS/2.

Das war ein sehr leistungsfähiges und gut durchdachtes Betriebssystem.

OS/2 hatte alles, was heute noch üblich und gut ist. 32 Bit System, multitaskingfähig, aller Arbeitsspeicher konnte genutzt werden, und Netzwerkfunktionalität war voll integriert. Es gab auch bald eine eigene Serverversion. Graphische Oberfläche war ebenfalls dabei. Es fehlte auch nicht an einem passenden Dateisystem, das praktisch beliebig große Festplatten bedienen konnte und lange Dateinamen ermöglichte.

Leider waren zu der Zeit, als OS/2 auf dem Markt erschien, schon 2 MB RAM astronomisch viel und teuer, und all die DOS – Rechner konnten weit weniger anbieten. Aber DOS hätte den Speicher ohnehin nicht nutzen können, nicht mal geschenkt.

Mit 1 MB und weniger war OS/2 kaum wirklich zu gebrauchen, so daß sich seine Verbreitung stark in Grenzen hielt.

Nicht zuletzt dieser zähe Start von OS/2 veranlaßte Microsoft, eine graphische Oberfläche zu entwickeln, die auf MS-DOS aufsetzt. Sozusagen zur Überbrückung. Der Erfolg war ab der Version 3 allerdings weit größer als gedacht, und zudem kriselte es irgendwann zwischen Microsoft und IBM. So stieg Microsoft aus dem OS/2 – Zug aus.

Es kann sein, daß OS/2 das beste aller PC – Betriebssysteme war, aber es sollte nicht sein.

Als IBM Mitte der Neunziger Jahre einen großen Werbefeldzug für die OS/2- Version 3 mit dem Beinamen Warp startete, war dasRennen schon gelaufen.

Microsoft machte für Heimuser weiter mit Windows 3.1 und 3.11, letzteres mit Netzwerkfähigket und deshalb als Windows for Workgroups bekannt. Aber das waren im Grunde immer noch keine Betriebssysteme, denn das Ganze lief nicht ohne DOS als Unterbau.

Parallel dazu kam Windows NT, das zunächst dieselbe Oberfläche aufweist, wie Windows 3x. Der Unterbau allerdings war völlig unabhängig von DOS, im Grunde die Fortführung von OS/2 mit Microsoft – Mitteln.

Ende 1995 kam schließlich Windows 95, dessen graphische Oberfläche bis heute existiert und die auch für NT und später 2000 nicht wesentlich geändert worden ist.

Seit Windows 95 gibt es auch bei Microsoft nichts mehr ohne Netzwerk.

TCO (Total Cost of Ownership)

Über die Heim – PC' s fand Windows seinen Weg auch zu den Büro – Arbeitsplätzen, und auf Workstations und PC' s findet sich kaum noch etwas anderes. Der Vorteil, daß sich so jeder recht schnell zurechtfindet, ist auch gleichzeitig der Nachteil.

Für Maschinen in der Fertigung oder sonstwo in einem Unternehmen werden Anschaffung und Betrieb nach technischen und wirtschaftlichen Erfordernissen abgewickelt. Der Benutzer wird bestimmt nicht gefragt, welche Farbe er gern etwa für eine Rasterpresse hätte oder ob er diese gar wöchentlich ändern könnte.

Völlig anders bei PC' s. Diese sind zwar auch nichts anderes als Mittel zum Arbeiten, die vom Unternehmen bereitgestellt werden. Trotzdem kann jeder Benutzer frei daran herumkonfigurieren und installieren. Egal wie viele It – Mitarbeiter vorhanden sind, fast alle machen in der Hauptsache PC – Support.

Das verschwendet derart viel Arbeitszeit, auf Seiten der IT genauso wie bei den PC – Benutzern, daß mittlerweile eine Unmenge von Werkzeugen dagegen existieren. Etwa Softwareverteilung über das Netz, vorgefertigte Standardinstallationen oder Netzwerkverwaltungen.

Teilweise gibt es sogar Ansätze, so etwas wie die alte Welt des Großrechners quasi wiederzubeleben, indem PC' s nur noch ein Betriebssystem enthalten, auf dem ein sogenannter Terminalclient läuft.

Die Programme laufen dabei auf einem Terminalserver, es wird nur noch die graphische Oberfläche zum Client projiziert. Das kann sogar so weit gehen, daß beim Start des PC auch das Betriebssystem von einem zentralen Server geladen wird und dieses lokal gar nicht installiert ist.

Das, was ein PC beim Kauf kostet, ist jedenfalls völlig vernachlässigbar gegenüber den Kosten, die er im Betrieb verursacht. Diese Gesamtkosten, eben die Total Cost of Ownership, tauchen aber in keiner Finanzrechnung auf. Daher erlebt man selten irgendwo eine wirklich effizente IT – Infrastruktur.

Netzwerkverwaltung, Verzeichnisdienste

Ein Netzwerk soll Ressourcen anbieten und den Zugriff auf diese regeln. Mechanismen dazu bieten alle Netzwerkbetriebssysteme in irgendeiner Form an.

Das Sammelsurium dieser Mechanismen nennt man Verzeichnisdienst. Einfache Systeme bilden logische Einheiten, etwa Domänen (diese haben nichts mit Domänen im DNS zu tun), in denen Benutzer in einer zentralen Datenbank definiert werden. Ein solches Benutzerkonto enthält die ensprechenden Anmeldeinformationen und kann dann auf verschiedene Ressourcen, etwa Verzeichnisse, Dateien oder Drucker, Berechtigungen erhalten.

Benutzerkonten sind immer Dreh – und Angelpunkt, allerdings sind viele Dinge dazugekommen. Etwa Postfächer für Email, die Möglichkeit, viele Standorte zu vernetzen, Intranet- und Internetzugänge und mittlerweile wird versucht, die komplette Struktur eines Unternehmens im Verzeichnisdienst abzubilden.

Bekommt ein Benutzer beispielsweise ein Emailkonto, ist es nicht mehr so, daß der Mailserver ein eigenes Verzeichnis hat, das dann den entsprechenden Eintrag enthält. Vielmehr ist alles in einem Datensatz enthalten, die eigenschaften des Benutzers bekommen einfach ein paar zusätzliche Registerkarten.

Die Sache mit der Abbildung der Unternehmensstruktur wird aber wohl immer ein Traum bleiben, da Strukturen und Namen eines Unternehmens heute schneller wechseln als daß Netzwerkplanung und Umsetzung dieser Pläne da folgen könnten.

Die Verwaltung dieser modernen Instrumente geschieht über ein Werkzeug ähnlich dem Windows – Explorer, der die angelegte Struktur mit Containern darstellt. Diese Container können beispielsweise die Abteilungen sein, dann sind möglicherweise alle Benutzer, Rechner, Drucker, die dazu gehören, im Container dieser Abteilung versammelt.

Genauso könnte aber auch ein Container „Drucker“ existieren, der dann alle Drucker gleich welcher Abteilung beinhaltet. Die Organisation ist dann letztlich der zugrunde liegenden Philosophie anzupassen.

Die erste richtige Umsetzung eines solchen Verzeichnisdienstes dürfte die NDS (Novell Directory Structure) von Novell sein. (Ja, die Firma gibt es noch).

NDS ist eine echte hierarchische Datenbank, in der ähnlich wie im DNS gleiche Namen vorkommen können. Der Max Müller in der Buchhaltung ist dann ein anderer als der max Müller im Einkauf, da nur die relativen Namen gleich sind.

Die absoluten Namen wären ja bespielsweise

Max.mueller.buchhaltung@firma.com

Max.mueller.einkauf@firma.com

Vollständig integriert könnte so eine Organisation dazu führen, daß der Anmeldename eines Benutzers gleich der Emailadresse ist.

Im Rahmen der Einführung von Windows 2000 hat Microsoft etwas Vergleichbares eingeführt und Active Directory genannt. Es sieht optisch sehr ähnlich aus, hat aber eine Einschränkung:

Die Strukturierung ist wirklich rein optisch, in Wirklichkeit ist die Datenbank flach und nicht hierarchisch.

Das ist nötig, um kompatibel zu sein mit den bisherigen Verzeichnissen von Windors NT. Diese führen nämlich nach wie vor nur den alten NetBIOS – Namen, alles, was dahinter hängt, kennen NT – Systeme nicht.

Trotz verschiedener Abteilungs – Container müssen alle Namen eindeutig sein. Egal ob Benutzer, Drucker, Computer, Server oder was auch immer.