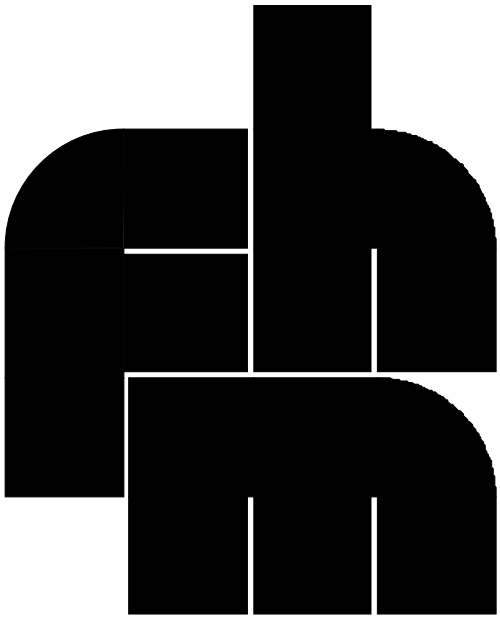


COMPUTERNETZE

Prof. Dr. Ing Manfred Paul

(Stand: WS 2001 / 02)

Inhalt

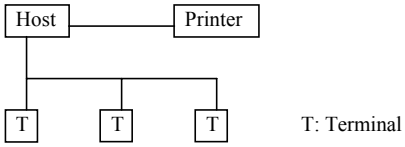
Inhalt

1. Grundlagen

1.1 Netzwerkmodelle

1.1.1 Zentralisierte Datenverarbeitung (Centralized Computing)

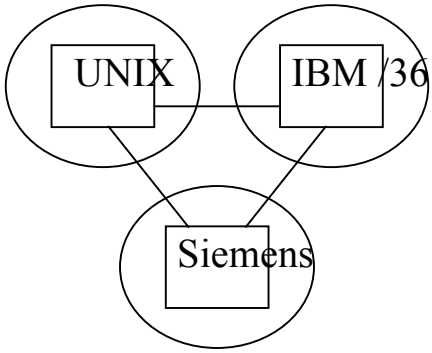
Großrechner / MDT (Mittlere Datentechnik)



Rechnerleistung zentral auf Host
RJE (Remote Job Entry)
Starten von Funktionen auf dem Host
Interaktives Arbeiten mittels Terminal

z.B. SNA = Systems Network Architecture (IBM)

1.1.2 Verteilte Datenverarbeitung (Distributed Computing)



Erstes Computernetz: ALOHANET

⇒ DARPA (Departement of Defence Advanced Research Project Agency)

⇒ ARPANET (Paketdatennetz zw. Forschungseinr. und Milit. Organisationen)

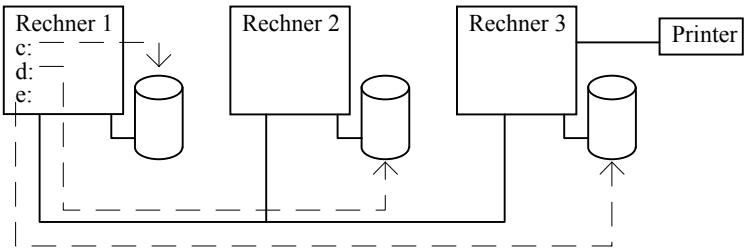
⇒ entwickelt sich zum INTERNET

Weitere Entwicklung von Rechnernetzen in mittlerer Datentechnik und auf PC-Basis

Rechnerleistung ist verteilt

1.2 Aufbau von Rechnernetzen

1.2.1 Peer to Peer Konzept



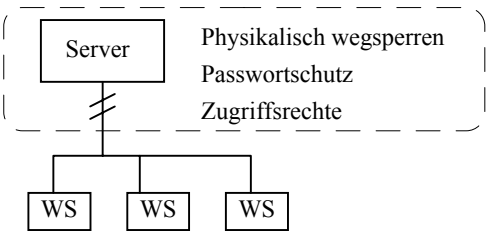
Nutzung verschiedener Recourcen (Festplatten, Drucker)

Beispiel:
Lantastic, Personal Netware, Unix - Netze, Windows for Workgroups, Windows NT Workgroupnetze, Macintosh Local Talk

Probleme:
- Sicherheit gegen unbefugten Zugriff (Ausnahme Unix, Windows NT),
  Zusätzliche Mechanismen (z.B. Bios Passwortschutz außerhalb des Betriebssystems können Sicherheit erhöhen)
- Sicherheit gegen Datenverlust

Anwendungsprogramme:
Stand Alone Applikationen (hauptsächlich)

1.2.2 Client - Server - Konzept



Server:
Zentrale Daten und Programme

Workstation / Client:
Umleiten von Eingaben / Ausgaben
Nutzung von Programmen

Aufgaben des Server Betriebssystems
Zentraler Datenbestand, Daten möglichst effizient zur Verfügung stellen
Anbieten von Dienstprogrammen (Services)
File - Locking (Kontrolle Mehrfachzugriff auf Fileebene)
Record - Locking (Kontrolle Mehrfachzugriff auf Datensatzebene)
Semaphore - Locking (Kontrolle Mehrfachzugriff auf Programme/Tasks)

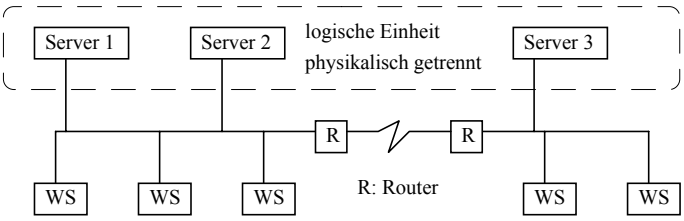
Beispiel:

Grundlagen

Novell 2.2, Novell 3.12, Windows NT, LAN-Server

Problematik:
Ausfallsicherheit
→ spez. Sicherheitsfunktionen notwendig
Zugriffsgeschwindigkeit
→ Fileserveroptimierung
→ Netzoptimierung

1.2.3 Client - Network



Gleichzeitiger Zugriff auf und gleichzeitige Administration von verschiedenen Servern

Homogenes Netz:
Gleiche Server-Bertriebssysteme
Ein Protokollstack (Eine Protokollfamilie)

Heterogenes Netz:
evtl. unterschiedliche Betriebssysteme
mehrere Protokoll - Stacks

Problematik:
Komplexität für den Benutzer und Administrator

Trends:
Verteilte Struktur = unsichtbar für den Benutzer (Banyan Vines, Novell 4.x), der Benutzer greift auf netzwerkweite, nicht nur auf serverbezogene Resourcen zu.
Intelligente Front - Ends (Clients) wie Novell Corsair (Ferret) Technologie oder Microsoft Bob, die die Komplexität vor dem Benutzer verbergen (zukünftig)
Middleware (s. später)

Applikationen:
Stand Alone
Netzwerkapplikationen
Directory Services - X.500 (Zugriff auf verteilte Recourcen log. organisiert)
Mail Services - X.400
Netzwerkbewußte Applikationen (Applikationen die transparent auf Netzwerkresourcen zugreifen können, Groupware)

Neue Trends zur Entwicklung von Netzwerkweiten Applikationen
→ z.B. Java

1.3 Begriffe

LAN: Local Area Network

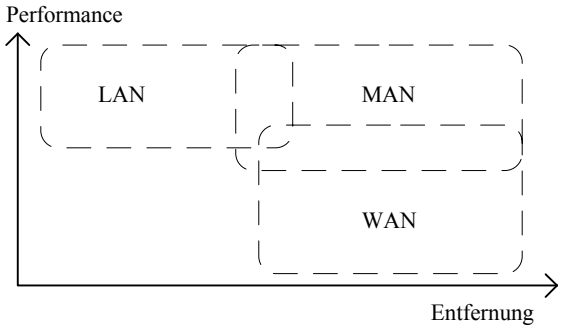
typisch:
innerhalb eines Gebäudes (Firmengelände)
Übertragungsraten: → 100 Mbit/s
Datenkommunikation mehrer *unabhängiger* Geräte

WAN: Wide Area Network

z.B. Datex-P, ISDN, Standleitungen, Modemverbindungen (Asynchron)
typisch:
Punkt zu Punkt, Punkt zu Multipunktverbindungen über *öffentl*. Leitungen
Übertragungsraten 300 Bit/s → 2 Mbit/s

MAN: Metropolitan Area Network

z.B. Datex-M, in Zukunft Breitband-ISDN
Konzept (Protokolle) erlaubt Anwendungen für Daten, Audio und Video
(Mehrdienstefähigkeit), Bandbreiten bis 155 MBit/s



2. Netzwerkdienste und Betriebssysteme

2.1 Mögliche Anwendungen in heutigen Netzen

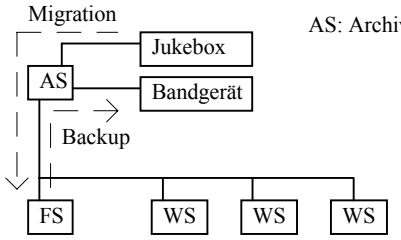
- Nachrichten versenden (Mail)
- Recourcensharing (Programme, Daten)
- Hardwaresharing (Printer, Fax, Modem, Rechner)
- zentrale Datensicherung, Datenpflege, Updates
- Ferndiagnose, Fernzugriff, Fernsteuerung
- Datensicherheit
- Videoconferencing via Network
- Netzkopplung mit Telefonanlagen
- Groupware (Mail, Terminplanung, Anrufbeantwortung, Anrufplanung)

Industrieller Bereich:
- Steuerung, Überwachung

2.2 Serverfunktionen (Services im Netz)

File Services:

Bereitstellung von Daten und Programmen, optimiert auf möglichst effizienten Zugriff
Zentraler Backup im Netz
Migration von kurzfristig nicht benötigten Daten auf 2nd-level Speicher



AS: Archivierungsserver

Print Services:

Abholung von Druckjobs vom Fileserver und Verteilung von Druckjobs im Netz (Funktion Postbote)

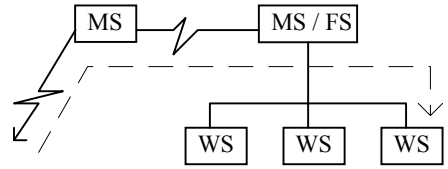
Umleitung Druckerwarteschlange Verteilung

WS: Workstation
FS: Fileserver
PS: Printserver
P: Printer

Bedienung mehrere Fileserver und mehrerer Printer, z.B. eine Printqueue für mehrere Drucker, ein Drucker für mehere Printqueues
Nutzung desselben Prozesses für netzwerkweites Fax

Message Services

Nutzung von E-mail
Store and Forward System (Speichern und Weiterleiten von Nachrichten)
Verwendung von Usern im System oder von intelligenten Anwendungsprogrammen

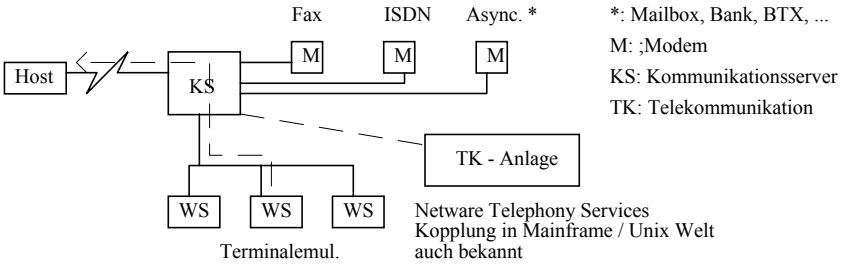


MS: Messageserver
FS: Fileserver
WS: Workstation

Mail für
User 3

Kommunikationsservice:

asynchrone Verbindungen (Modem - Sharing)
ISDN - Sharing
Mainfraimekopplung
Zugriff auf öffentliche Netze



Beispiel:

Novell Radius
zusätzlich auch Routingfunktionen und Gatewayfunktionen

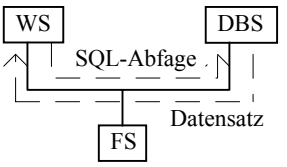
Bereitstellung von Kommunikationsdiesten im Netz

Applikationsservice:

Bereitstellung von zentralen Anwendungen im Netz (z.B. Datenbank, Telefonanlage etc.)

Datenbankserver

z.B. Gupta, Oracle, Informix, Sybase, Apple 4D-Server
Intelligentes Backend zur Datenhaltung



DBS: Datenbankserver

SQL: Structured Query Language (Datenbankabfragesprache)
Client mit Datenbank - Frontend (SQL - Windows)

ODBC: Open Database Connectivity (Schnittstelle für den Zugriff auf Datenbanken unter Windows)

Zeitserver

Festlegung und Steuerung einer netzwerkweiten Zeit
z.B. in Netware 4.x zur Sicherstellung der richtigen Reihenfolge beim Update der netzwerkweiten Resourcendatanbank (NDS)

Die Liste von Services läßt sich erweitern, grundsätzlich können alle automatisierbaren Funktionen in einem Netz als Service realisiert werden, z.B. automatische Adressvergabe über einen Adreßvergabe-Server (z.B. entsprechend DHCP Protokoll) oder ähnliches.
Üblicherweise sind mehrere Services auf einem Server realisiert, so ist häufig ein Fileserver noch mit Printservice, Faxservice, Web-Service, Routingfunktionalität usw. ausgestattet.

2.3 Zugriff auf Services

Der Zugriff auf einen Netzwerk-"Service" erfolgt von einem Netzwerk-"Client". Für Zugriff auf einen Mail-Service wird z.B. ein Mail-Client benötigt, für den Zugriff auf File-Service ein entsprechender Client. Letzterer wird im Allgemeinen auch als Netzwerkshell bezeichnet.

Client: Softwarekomponente der Workstation, ermöglicht Zugriff auf Services. Neuere Betriebssysteme wie Novell NetWare 5 oder Windows NT ermöglichen den Zugriff über einen Client direkt an der Konsole des Servers

Server: Bietet verschiedene Services an

Es gibt grundsätzlich verschiedene Verfahren, mit denen sich Clients und Services unterhalten:

- Unterbrechung von Betriebssystemaufrufen

Hier wird einfach der Aufruf von Netzwerkkommandos abgefangen und ins Netz umgeleitet. Das Betriebssystem, auf dem der Client sich befindet, ist nicht netzwerkfähig. Ältere Netzwerkbetriebssysteme (z.B. solche mit DOS Clients) arbeiten auf diesem Weg, um Abfragen nach Dateien oder Druckern einfach statt zum lokalen Betriebssystem an das Netz weiterzuleiten.

- Remote Operation

Hier ist das genaue Gegenteil der Fall. Der Client ist ein vollständiger Netzwerk-Client, der Server bzw. Service kennt das Netzwerk nicht, d.h. es ist aus seiner Sicht nicht erkennbar, ob ein Zugriff intern oder über das Netz erfolgt. Der Remote Procedure Call (RPC) Mechanismus, über den Programme ferngestartet werden können, ist ein Beispiel dafür.

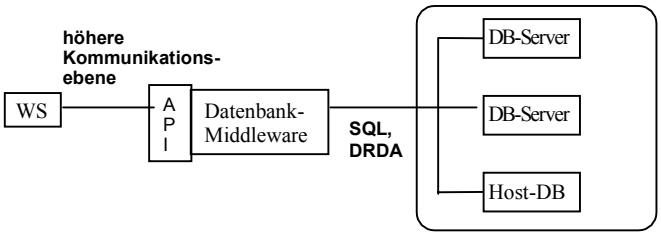
- Gemeinsamer Netzwerkzugriff

Die ist der häufigste Fall in modernen Netzwerkbetriebssystemen (Windows NT, Novell 4 mit Client32). Hier arbeiten Server und Client zusammen und koordinieren die Netzwerkkommunikation.

2.4 Netzwerk Middleware (Three Tier Computing)

Modell zur intelligenten Steuerung von Diensten im Netz

Beispiel: Steuerung der Kommunikation mit DB-Server (Datenbank Middleware)

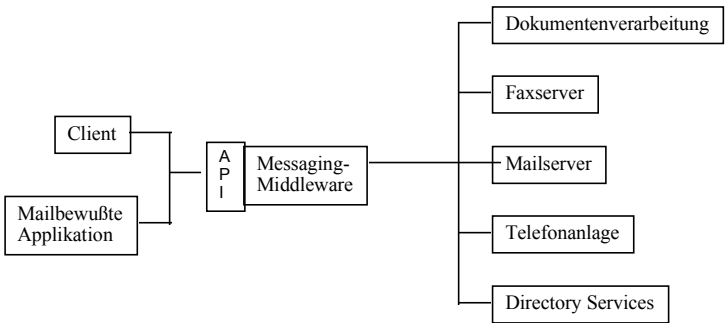


Logische Einheit

Ermöglicht den Zugriff auf verteilte Datenbanken (unsichtbar für den Benutzer)
Verlagerung der Intelligenz des Clients auf Middleware.

Novell TUXEDO
Informix online dynamic Server
Abwicklung kompletter Funktionsaufrufe (nicht nur reine Datenbankabfrage)

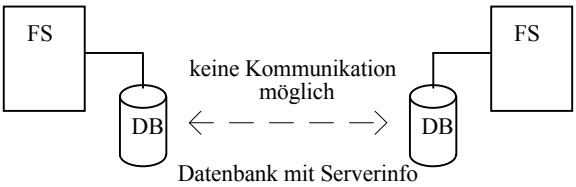
Beispiel: Messaging Middleware



Infrastruktur für Multiserverumgebung (Collaborative Computing)

2.5 Ressourcenzugriff

2.5.1 Serverkonzept



Datenbank mit Serverinfo (Novell 3: Bindery)

Objekte
- User
- Gruppen
- Zugriffsprofile für User
- Volumes (Filesystem)
- Dienste (Gateway, ...)

Information ist serverbezogen
Problematik: Abgleich der Information bei mehreren Servern muß manuell erfolgen, d.h z.B. muß ein und derselbe Benutzer auf drei verschiedenen Servern definiert werden, weil er dort auf Daten zugreifen will. NetWare 3 ist aufgrund der hohen Stabilität heute noch relativ verbreitet (vor allem bei kleineren Firmen, wo die Nachteile einer serverbezogenen Administration noch keine so große Rolle spielen).

2.5.2 Domänenkonzept

Grundsätzlich löst das Domänenkonzept das Problem, das Benutzer im Netzwerk mehr als einmal definiert werden müssen. Alle Server, für die eine zentrale Benutzerverwaltung erfolgen soll, werden in einer Domäne zusammengefaßt. An einer zentralen Stelle, dem sogenannten Domänenkontroller, wird die gesamte Benutzerverwaltung des Netzwerks zentralisiert. Als Ausfallsicherung steht noch ein Sicherungs-Domänenkontroller zur Verfügung. Microsoft Windows NT verwendet die Bezeichnungen PDC (Primary Domain Controler) und BDC (Backup Domain Controler).

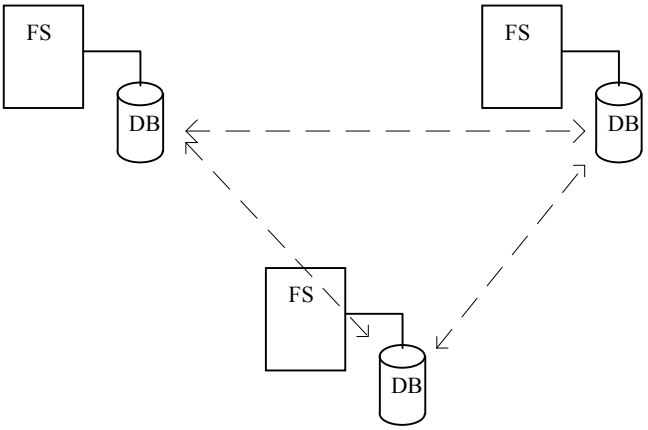
Werden mehrere Domänen zusammengefaßt, können bei Windows NT zwischen den Domänen Vertrauensstellungen definiert werden. Das führt dazu, daß eine Domäne der anderen vertraut, die Aufgabe der Authentisierung (Beglaubigung) von Benutzern im Netzwerk richtig durchzuführen. Ein Benutzer loggt sich in eine Domäne ein und kann dann auch auf Resourcen einer weiteren Domäne zugreifen, wenn diese der ersten vertraut. Vertrauensstellungen sind einseitig oder zweiseitig, aber derzeit noch nicht transitiv. D.h. das Domäne 1 der Domäne 2 vertraut und Domäne 2 der Domäne 3 heißt nicht, daß auch Domäne 1 automatisch Domäne 3 vertrauen würde.

Die Problematik besteht bei der derzeitigen Version von NT in folgenden Aspekten:
- Trustbeziehungen sind nicht transitiv, was bei mehr Domänen unübersichtlich werden kann.
- Innerhalb der Domäne gibt es keine Hierarchien von Objekten, also z.B. keine hierarchische Anordnung von Benutzern, sondern nur Listen, die entsprechend lang werden können.

Beide Nachteile werden mit Active Directory Service von Microsoft (Windows 2000) behoben.

2.5.3 Directory Service Konzept

Directory Service steuert Zugriffsrechte auf alle Ressourcen netzwerkweit.

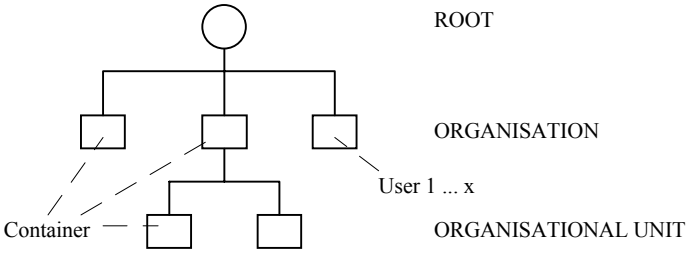


Datenbank mit Information über Netzwerk Ressourcen
- Verteilte Struktur
- Hierarchischer Aufbau

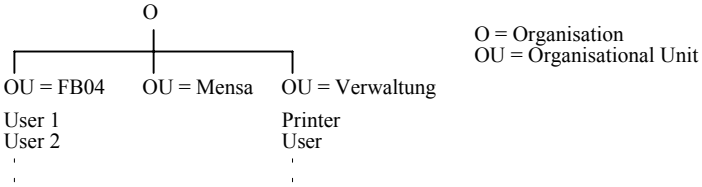
Partitionen der Datenbank und Kopien dieser Partitionen werden auf mehrere Server verteilt.
Vorteile:
- Lastverteilung bei der Authentisierung
- Backup von Netzwerkinformation verteilt

Hierarchische Organisation:
Directory Services ITU Standard: X.500.

Blattobjekte (Leaf - Objects)
Container - Objekte (Zusammenfassung mehrer Blattobjekte)



Beispiel:



Objekte in Directory Services sind netzwerkweit verwendbar, nicht mehr nur serverbezogen. Der Server, der bisher Zentrum der Administration war, wird nun ein Objekt in der Ressourcendatenbank. Neben der reinen Benutzerverwaltung ergeben sich damit neue Möglichkeiten des Einsatzes eines Directory Service. Gesteuert über entsprechende Objekte im Directory Service sind dies z.B.:
- Softwareverteilung
- Desktopmanagement (Policy Management)
- Anwendungsmanagement
- Erzeugung und Verteilung von Schlüsseln für die verschlüsselte Kommunikation
- Management von Netzwerkhardware (die auch durch entsprechende Objekte repräsentiert wird)

Näheres dazu im Kapitel Netzwerkmanagement

Problematik:
- Netzwerkverkehr (speziell WAN)
- Komplexität des Systems
  → Finden einer Ressource in verteilter Struktur
  User beim Einloggen: Wo in Directory ist User - Info gespeichert ?
  d.H. User muß seinen Kontext kennen

Realisierung in den verschiedenen Betriebssystemen:

Novell 4.x/5.x: NDS (Novell Directory Service), neu: eDirectory:
- Echte hierarchische Struktur (X.500)
- Login erfolgt über Angabe des kompletten Objektnamens in der Struktur:
  Login .CommonName**.**OrganisationalUnit**.**Organisation
  z.B. Login: .Maier.FB04.FHM
  Vereinfachung: Voreinstellung von ´.FB04.FHM´ über lokale Konfiguration der Workstation des Benutzers oder über
  Catalog Service: Vorhalten aller Benutzer in einem speziellen Katalog in der NDS
- Plattformübergreifend: Novell Netware, Windows NT (mit NDS for NT auch plattformübergreifende Benutzerverwaltung), Windows 2000, Sun Solaris, Linux, IBM OS/390 Großrechner

Microsoft Windows 2000 Active Directory:
- Keine echte hierarchische Struktur (Hierarchie nur innerhalb von Domänen)
- Speicherung der Benutzer Userverwaltung erfolgt nach wie vor in flacher Datenbankstruktur, d.h. Benutzer loggt sich nach wie vor mit einem eindeutigen Namen in die Domäne ein
- Trustbeziehungen zwischen Domänen durch Baumstruktur relisiert, Trusts sind dabei transitiv

Microsoft Exchange Directory:
- Vorläufer von Active Directory für Enterprise Mailsystem Exchange
- Adress-Verwaltung von User Mailboxen
- Exchange 2000 → Integration mit ADS

LDAP kompatible Directories (Netscape, andere)
- LDAP: Lightweight Directory Access Protokoll (Standardprotokoll zum Zugriff auf Directories)
- Verwaltung von Benutzern zur Steuerung des Zugriffs auf bestimmte Dienste im Netzwerk (z.B. Webserver)
- NDS ist vollständig LDAP v.3 kompatibel

Kopplung verschiedener Directories
- Metadirectory Konzept
- DirXML

2.5.4 Zugriffskontrolle in Netzen

Je nach verwendetem Konzept für den Ressourcenzugriff gibt es unterschiedliche Sicherheitsmechanismen für Netze.

Workstation
- Lokaler Passwortschutz (z.B. BIOS Passwort, Windows NT/2000)

Server, Netzwerk
- Passwortschutz
  - Übertragung unverschlüsselt (frühere Netzwerkbetriebssysteme, Hostsysteme)
  - Symmetrische Passwort-Verschlüsselung
  - Authentication

Netzwerkdienste, Objekte in NDS
- Rechte auf Objekte
- Rechte auf Objekteigenschaften

Filesystem (je nach verwendetem Filesystem unterschiedlich)
- Rechte auf freigegebene Verzeichnisse
- Rechte auf Directory, Files (User - bezogen), je nach Filesystem unterschiedlich
- Rechte auf Directory, Fileattribute (Filebezogen), je nach Filesystem unterschiedlich

Rechte können innerhalb des Filesystems und innerhalb der Directory Services vererbt werden.

Single Sign On:
Heute sind Netze meist heterogen realisiert, d.h. es kommen unterschiedliche Betriebssyteme und Hardwareplattformen zum Einsatz. Dies bedeutet für den Benutzer, daß er in den unterschiedlichen Systemen bekannt sein muß.
Eine gemeinsame Administration von einem zentralen Punkt ist dabei über einen plattformübergreifenden Directory Service, eine Direkte Kopplung von einzelnen Directories oder über Metadirectories zu erreichen.
Dabei ist auch ein gemeinsames Login für den Benutzer ein Ziel (Single Sign On). Durch entsprechenden Abgleich von Benutzerpasswörten zwischen den Systemen wird so der Login Vorgang vereinheitlicht. Dies stellt allerdings gleichzeitig eine Erleichterung und eine Gefahr dar.
(→ Kapitel Netzwerksicherheit).

2.6 Fehlertoleranz bei LAN Betriebssystemen

Die Grundproblematik der Zentralisierung von Daten ist wie vorher bereits beschrieben die Ausfallsicherheit des Systems. Aus diesem Grund müssen Ausfallsicherungssystem zur Verfügung stehen, um die Verfügbarkeit von Servern zu gewährleisten. Inwieweit ein solches System notwendig ist ergibt sich durch die Kosten, die bei einem Systemausfall entstehen können. Hierbei muß man durchaus unterscheiden zwischen

- ungeplantem Systemausfall und
- Wartungszeiten, für die ein System für eine gewisse Zeit heruntergefahren werden muß, um Wartungsarbeiten, Upgrades und ähnliches durchführen zu können.

Grundsätzlich muß festgestellt werden, daß eine **relativ hohe** Ausfallsicherheit durch heutige Standardsysteme gegeben ist, daß aber **sehr hohe** Ausfallsicherheit unter Umständen sehr teuer erkauft werden muß. Hier müssen die Kosten, die durch einen Systemausfall entstehen können (z.B. durch entgangene Umsätze, Kosten von Arbeit usw) gegen die Kosten der Ausfallsicherungslösung gestellt werden. Sehr viele Firmen können wahrscheinlich einen Systemausfall für mehrere Stunden oder sogar Tage verkraften, andere Firmen kann ein Systemausfall von nur einer Stunde in den Konkurs stürzen. Entsprechende Ausfallsicherungssysteme sind nötig.

2.6.1 Kosten eines Systemausfalls

Die folgende Tabelle zeigt das Ergebnis einer Kostenanalyse, die bei ausgewählten Firmen in verschiedenen industriellen Bereichen durchgeführt wurde (Quelle: Novell Brainshare 98 aus Dataquest Contingency Planning Research):

Industriebereich	Geschäftsbereich	Kostenbereich pro Std. in US$	Durchschnittl. Kosten pro Std. in US$
Finanzen	Wertpapierhandel	5 600 000 – 7 300 000	6 450 000
Finanzen	Kreditkartenorganisation	2 200 000 – 3 100 000	2 600 000
Medien	Pay-TV	67 000 – 233 000	150 000
Handel	Radio/TV/Hifi	87 000 – 140 000	113 000
Handel	Kataloganbieter	60 000 – 120 000	90 000
Transport	Fluglinie (Reservierung)	67 000 – 112 000	89 000
Medien	Ticketverkauf	56 000 – 82 000	69 000
Transport	Paketdienst	24 000 – 32 000	28 000
Finanzen	Bankautomatengebühren	12 000 – 17 000	14 000

Auch eine sehr hohe Verfügbarkeit schließt einen kurzeitigen Systemausfall nicht aus. Die folgenden Zahlen verdeutlichen dies:

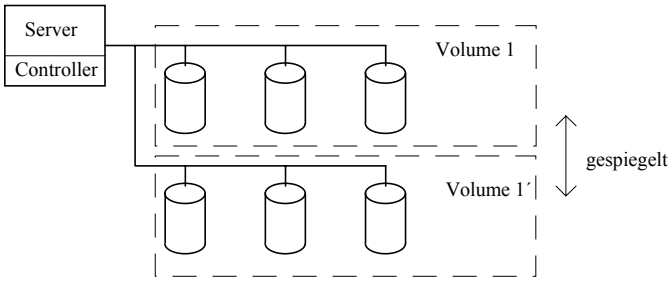
Verfügbarkeit	Ausfallzeit pro Jahr
96 %	350,4 Std.
98 %	175,2 Std
99 %	87,6 Std
99,9 %	8,7 Std
99,99 %	52,5 min
99,999 %	5,2 min

2.6.2 Realisierung von Ausfallsicherungssystemen

- Redundanz der FAT, DET (Tabellen)
- Festplattenspiegelung (1 Controller, mehrere Disks)
- Festplattenduplexing (2 Controller, mehrere Disk)

Festplattenspiegelung und Duplexing wird oft kombiniert mit sogenanntem Disk-Striping

(bei Novell: Volume Spanning)
Realisierung: Eine Partition wird über mehrere Platten verteilt. Dadurch überlappender Zugriff (quasi-parallel) möglich mit entsprechender Steigerung der Zugriffsgeschwindigkeit.

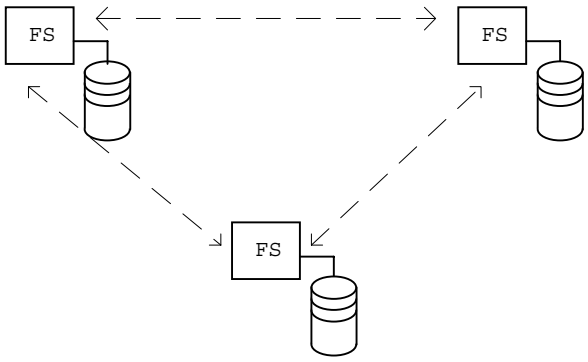


- RAID

  Verlegung des Disk Striping / Volume Spanning auf HW-Ebene
  Erhöhung der Verfügbarkeit von Festplatten durch Verteilung auf möglichst viele Festplatten und Wiederherstellung von Daten bei Plattenausfall. Man unterscheidet verschiedene sog. RAID Level:
  Level 1: Block Striping
  Level 2: Bitstriping mit ECC
  Level 3: Bitstriping mit Paritätsplatte
  Level 4: Blockstriping mit separater Paritätsplatte
  Level 5: Blockstriping mit verteilter Paritätssicherung

- Datenspiegelung über verschiedene Server, eigentlich Shadowing bzw. Replication.

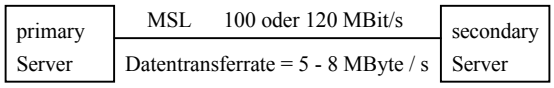
z.B. Replizierung von verteilten Datenbanken (z.B. Directory Services), Replizierung von Datenbereichen auf Festplatten (z.B. Novell Replication Service)



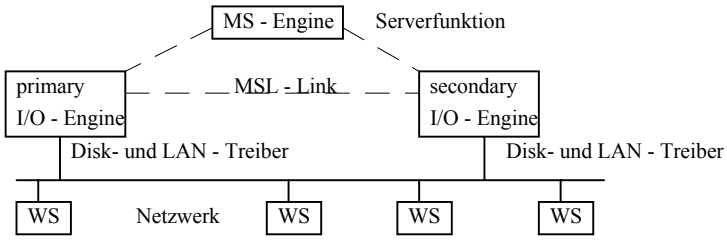
■ Server Spiegelung (derzeit nur Novell 3.11 SFT III bzw. 4.2 - SFT III)

SFT III = System Fault Tolerance III:
Komplette Spiegelung zweier Server mit großen Teilen Ihrer Hauptspeicherbereiche, die Server präsentieren sich nach aussen als ein System. Die beiden Server sind über das LAN sowie eine dedizierte Verbindung (MSL: Mirrored Server Link) miteinander verbunden).

physikalischer Aufbau



logischer Aufbau



Kommunikation vom Client findet nur über die Primary I/O-Engine mit der MS-Engine statt, die Secondary I/O Engine wird über das MSL Link auf dem Laufenden gehalten. Im Fehlerfall des Primary Servers kann die Secondary Server die Verbindung zur MS-Engine herstellen. Um sicherzustellen, daß der Secondary Server unterscheiden kann, ob wirklich ein Ausfall des Primary Servers vorliegt oder ein Ausfall der MSL Verbindung, tauschen beide Server ständig über das LAN sogenannte I'm Alive Pakete aus.
Ausfallzeit: Konfigurierbar von 1s bis 10s.

■ Standby Server (Vinca, Novell)
Ähnliches Konzept wie SFT III aber ohne Spiegelung der Speicherbereiche der Server. Stattdessen wird lediglich eine Festplattenspiegelung über eine dedizierte Verbindung zwischen den Serven durchgeführt. Bei Serverausfall wird der Standby Server automatisch aktiviert und übernimmt (transparent für die Benutzer) die Rolle des ersten Servers.
Hierbei kann ein einziger Standby Server die Backupfunktion für mehrere Server übernehmen.
Ausfallzeit: Gegeben durch Neustart des Standby Servers und Laden der Volumes einige Minuten)

■ Cluster

Ein Cluster ist eine lose Kopplung von Servern über schnelle Netzwerkverbindungen (SAN: Storage Area Network)mit gemeinsamem Speichersystem. Im Gegensatz zu den vorhergehenden Konzepten sind alle im Cluster beteiligten Server aktiv, fällt ein Server aus, übernimmt ein anderer Server aus dem Cluster die Funktionen des ersteren mit. Hierbei wird der Cluster dem Benutzer als ein einziger Server präsentiert „Single System Image“. Dies beinhaltet den Datenaustausch von Information im RAM der Server. Dadurch können Anwendungen (die für den Einsatz im Cluster entwickelt wurden) im Cluster sowie der Zugriff auf verschiedene Server verteilt werden (Load Balancing).

Ziele die durch Clustering erreicht werden sollen, sind:
- Erhöhung der Verfügbarkeit
- Erhöhung der Systemperformance
- Darstellung des Clusters von Servern als ein System (Single System Image)
- Skalierbarkeit
- Lastverteilung

Die Realisierung eines SANs kann bei heutigen Systemen erfolgen über:
- SCSI Verbindungen
- Fast Ethernet / Gigabit Ethernet (über Switch), ATM, FDDI (über eigenes Clustering Interconnect Protocol CICP)
- SCI (Scalable Coherent Interface, 200MB/s)
- Fibre Channel
- SSA (Serial Storage Architecture) (IBM)

Es gibt verschiedene Clusterkonzepte:
- Clustering von einzelnen Servern zur Realisierung einer gegenseitigen Ausfallsicherung von zwei Servern (Microsoft MS Cluster Server).

- Verteilter Cluster: (Novell Cluster Services) Hier ist eine Ausfallsicherung eines Servers durch mehrere Server im Cluster möglich (Novell Terminologie: Fan-Out Failover). Damit bietet dieser Cluster nicht nur Ausfallsicherung sondern gleichzeitig die Skalierbarkeit des Gesamtsystems.

- MultiSite Cluster: Cluster über mehrere Standorte hinweg

3. Übertragungsmedien für Netze

3.1 Leitungsgebundene Medien

- Koax - Verkabelung
  50 Ω - Ethernet, Thickwire - Yellow Cable
  50 Ω - Cheapernet, Thinnet, Thinwire Ethernet

- Twisted Pair

			Wellenwiderstand	Leitungswiderstand
IBM	Typ 1	STP	150 Ω / 4 MHz	50 mΩ / m
Kabelkanal	Typ 2	STP	150 Ω / 4 MHz	120 mΩ / m
Patchkabel	Typ 3	UTP	84 - 113 Ω / 1 MHz	85 mΩ / m

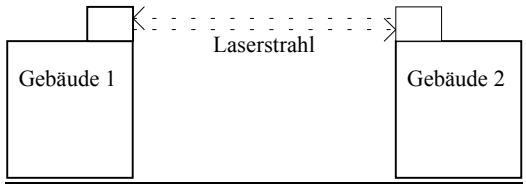
UTP Kategorien (Levels)

Cat 1	Telefonkabel	< 1 MHz
Cat 2	Datenkommunikation	< 4 MHz
Cat 3	Datenkommunikation	< 16 MHz
Cat 4	Datenkommunikation	< 20 MHz
Cat 5	Datenkommunikation	< 100 MHz
Cat 6	Datenkommunikation	< 300 MHz

- Glasfaser (Monomode-, Multimodefasern)
  Einsatz bei:FDDI, auch Ethernet, Token Ring

3.2 Nicht Leitungsgebundene Medien

- Richtfunk
- Satellitenübertragung
- Funkübertragung (LAN)
- Infrarotübertragung
- Laserstrecke

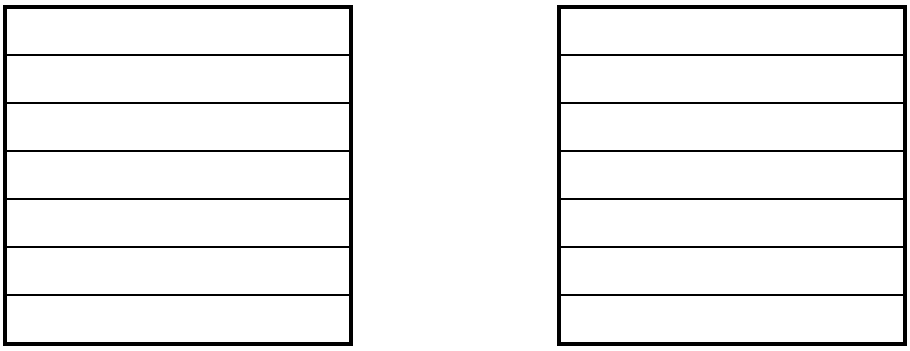


4. Protokolle und Standards

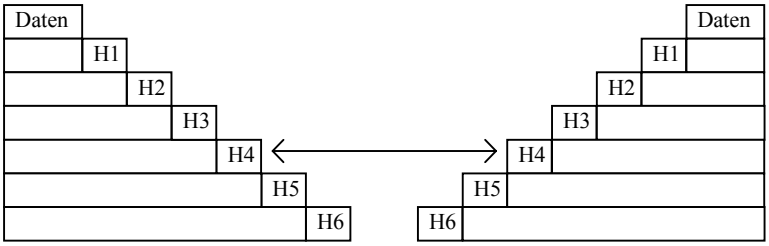
Um Daten zwischen zwei Rechnern übertragen zu können, müssen zunächst einige Grundbedingungen erfüllt sein. Das beginnt damit, welcher Rechner unter welchen Bedingungen was senden darf. Es geht weiter über die Adressierung, die durchaus verschiedensten Anforderungen gerecht werden muß. Die meisten Protokolle erlauben eine Gruppierung von Adressen, um die Verteilung (das Routing) von Paketen im Netz einfacher gestalten zu können, zudem müssen auch Mechanismen zur Adressierung von Diensten vorhanden sein, da ja mehrere Dienste auf einer physikalischen Maschine koexistieren können. Eine weitere Aufgabe ist die Flußkontrolle, über die gesteuert wird, daß ein Sender einem Empfänger genau soviele Daten pro Zeiteinheit schickt, wie dieser verarbeiten kann und die Kontrolle der Gesamtübertragung durch das Senden von Bestätigungspaketen. Pakete sind Teil einer Kommunikationsbeziehung, die irgendwann einmal anfängt und wieder aufhört, parallele Kommunikation zu einem Dienst und die nötigen Codeumsetzung sind weitere Themen, schließlich endet das ganze damit, daß die Dienste, auf die zugegriffen werden soll, ja auch irgendwie im Netzwerk gefunden werden sollen.

Dieser Aufgabenberg ist gewaltig, und nun könnte ein Hersteller eines Rechners natürlich auf die Idee kommen, diese Aufgabe für sich und seine Rechnerfamilie proprietär zu lösen. Diesen Ansatz verfolgten die Hersteller tatsächlich in den 70er Jahren, inzwischen ist man zu einem modularen Ansatz übergegangen. Jede diese Aufgabe wird unabhängig von anderen gelöst. Diesen Ansatz soll folgendes Kommunikationsmodell verdeutlichen.

4.1 Kommunikationsmodell



Modell zur Beschreibung von Kommunikation
- Schnittstellen klar definiert
- Jede Ebene fügt Information hinzu, die auf der Empfängerseite auf der gleichen Ebene ausgewertet wird
- Aufgabe jeder Ebene klar definiert, austauschbare Funktionsblöcke bei Kommunikation
- Ebenen werden auch als Schichten bezeichnet, jede Schicht setzt auf der nächstniedrigeren auf.



Anwendung auf Rechnerkommunikation

- Es gibt Standards für Funktion jeder Ebene
- Es gibt Standards für die Schnittstellen zwischen Ebenen

Ein übertragenes Datenpaket zwischen zwei Rechnern enthält also zunächst Header, dann nochmals Header usw. Er sieht also in etwa folgendermaßen aus:

Header 1	Header 2	Header 3	Header 4	Header 5	Header 6	Header 7	Daten

Jeder Header enthält spezielle Information zur Übertragung, entsprechend der verschiedenen Aufgaben, die bei der Übertragung gelöst werden müssen. Typischerweise verweist jeder Header auf seinen Datenbereich, in dem sich tatsächlich dann der nächstfolgende Header befindet. Der Headeraufbau wird durch das verwendete Übertragungsprotokoll bestimmt, nachdem die Header aufeinander abgestimmt sind, also durch eine ganze Protokollfamilie (Protokollsuite, Protokollstack, Protokollstapel). Jeder Header, d.h. jedes Protokoll übernimmt dann ganz bestimmte Aufgaben zur Übertragung. Eine allgemeine Beschreibung dessen, was da alles festgelegt wird, liefert das sog. OSI Referenzmodell.

4.2 OSI Referenzmodell

Das OSI Referenzmodell ist ein Modell zur Beschreibung von Kommunikation. Es beschreibt die Teilaufgaben, die in einer Kommunikationsbeziehung zwischen Rechnern zu erledigen sind, ohne sich auf eine bestimmte Implementation festzulegen.

OSI: Open Systems Interconnection
Von der ISO (International Standards Organisation) entwickelt; seit 1983 Standard.

Ebenen des OSI - Modells

7	Application layer	Anwendungsschicht
6	Presentation layer	Darstellungsschicht
5	Session layer	Kommunikationssteuerungsschicht
4	Transport layer	Transportschicht
3	Network layer	Netzwerkschicht
2	Data Link layer	Sicherungsschicht
1	Physical layer	Bitübertragungsschicht

Jede Schicht stellt der darüberliegenden einen Dienst mit bestimmten Funktionen zur Verfügung, der von dieser genutzt werden kann. Der Dienst ist über einen Dienstzugangspunkt (Service Access Point) erreichbar, die einzelnen Nachrichten zwischen den Schichten werden als Diensteprimitive (Service Primitives) bezeichnet.

Typische Aufgaben:

1. Physical Layer:

Aufgaben:
- Physikalische Schnittstellen (V24, RS232) (Spannungswerte, Impedanzen)
- Übertragungsverfahren
- Übertragungsparameter (Übertragungsgeschwindigkeit, Pulsformen, Leitungscodes)
- Prozedurale Anschlußbedingungen (Signalfolgen usw.)
- Dienste (Synchronisationsverfahren, Natzanschlußstruktur)
- Dienstequalität (Übertragungsfehlerrate, Verzögerung, Durchsatz, Verfügbarkeit)

Informationseinheit: Bit

2. Data Link Layer:

MAC - Teilschicht (**M**edia **A**ccess **C**ontrol)

Aufgaben:
- Medienzugriff
- physikalische Adressierung

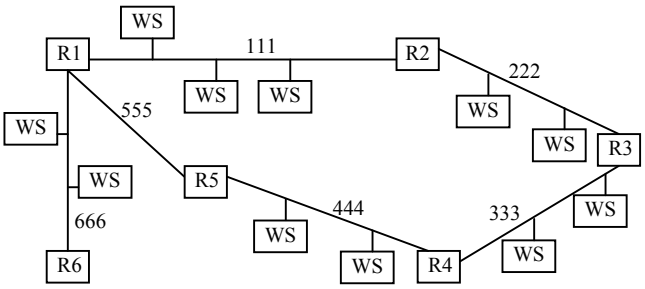
z.B. Ethernet IEEE 802.3
z.B. Token Ring IEEE 802.5

LLC - Teilschicht (**L**ogical **L**ink **C**ontrol)

Aufgaben:
Fehlerkontrolle
Sicherung der Übertragung
LLC IEEE 802.2
SDLC HDLC

Infomationseinheit: Frame, Paket

3. Network Layer:



Aufgaben:
- logische Adressierung in Netzen
- Paketvermittlung → Routing
- Flußkontrolle (teilweise)
- Kontrolle der Paketreihenfolge

Informationseinheit: Datagramm

4. Transport Layer

Aufgaben:
- Zerlegung und Zusammenfügung von Paketen (Segmentierung)
- Adressierung von logischen Übertragungskanälen
- Adressierung von Diensten
- Adreß- / Namensauflösung
- Flußkontrolle
- Fehlersicherung

Informationseinheit: Segment

5. Session Layer:

Aufgaben:
Management von Sitzungen (Dialogkontrolle)
Informationseinheit: Nachricht

6. Presentation Layer:
Aufgaben:
Formatierung der Daten
Verschlüsselung
Informationseinheit: Nachricht

7. Application Layer
Aufgaben
Bereitstellung einer lokalen Benutzeroberfläche
Netzwerkservices (FTP, Directory services, Mail, MHS, SMTP)
Informationseinheit: Nachricht

4.3 Protokolle und Standards

Nun gibt es immer noch sehr viele Hersteller und damit eben auch verschiedene Ansätze für eine gelungene Aufteilung. Ergebnis sind die vielen Protokollfamilien, die heute im Markt nebeneinander her existieren. So gibt es z.B. die Internet Protokoll-Suite, die NetWare Protokollsuite, usw. Zudem ist es so, daß sich im Vergleich zum OSI Referenzmodell die Aufgaben des einen oder andereren Protokolls nicht unbedingt eindeutig einer bestimmten Schicht zuordnen lassen. Manche erstrecken sich von ihrem Aufgabengebiet her über mehrere Ebenen, andere füllen vielleicht nicht alle Teilaufgaben, die in einer bestimmten Schicht festgelegt sind.

Wer macht nun Protokolle? Es gibt:
De-Facto Standards: Standards/Protokolle, die sich am Markt entwickeln und oft aus herstellerspezifischen Entwicklungen hervorgehen
De-jure Standards: Standards/Protokolle, die von Standardisierungsgremien verabschiedet werden

Standardisierungsgremien:
CCITT: Consultative Commitee for International Telegraphy and Telephony (X, V- Standards), heute ITU (International Telecomunication Union)
ISO: (1946 gegründet) 89 Staaten; Mitglied bei CCITT
ANSI: Amerikanischer Repräsentant der ISO
IEEE: Institute of Electrical and Electronical Engineers

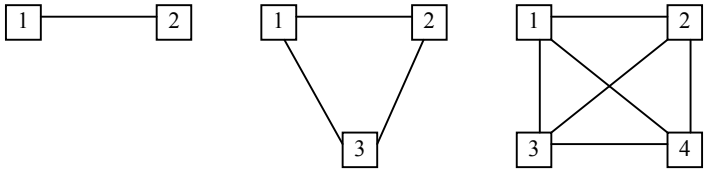
Nachfolgende Tabelle zeigt eine ungefähhre Zuordnung gängiger Protokollstacks zum OSI-Referenzmodell.

<table>
<tr><td>7</td><td>Application layer</td><td rowspan="7">IBM
SNA</td><td rowspan="7">DEC
DNA</td><td>NFS</td><td>Novell
NCP</td><td rowspan="4">OSI</td><td rowspan="7">Apple-
talk</td></tr>
<tr><td>6</td><td>Presentation layer</td></tr>
<tr><td>5</td><td>Session layer</td></tr>
<tr><td>4</td><td>Transport layer</td><td>TCP</td><td>SPX</td></tr>
<tr><td>3</td><td>Network layer</td><td>IP</td><td>IPX</td></tr>
<tr><td>2</td><td>Data Link layer</td><td colspan="2" rowspan="2">Ethernet, Arcnet,
Token Ring, FDDI</td></tr>
<tr><td>1</td><td>Physical layer</td></tr>
</table>

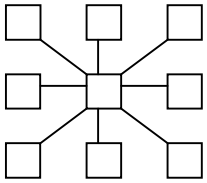
5. Physical Layer

5.1 Physikalische Netztopologien

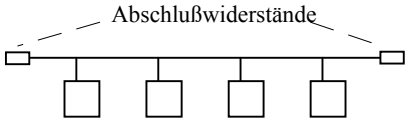
- Maschentopologie (In öffentlichen Netzen verwendet)
  Punkt zu Punkt Verbindungen zwischen Rechnern bzw.
  zwischen Rechnern und Peripherie



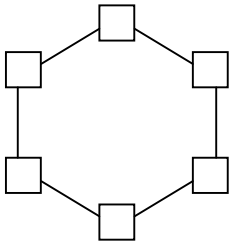
- Sterntopologie (Basis für eine sog. Strukturierte Verkabelung, heute sehr häufig in LANs verwendet)
  Punkt zu Punkt Verbindungen mit einem zentralen Punkt
  (HUB, Repeater, Concentrator, MSAU)
  MSAU - Multiple Station Access Unit - Ringleitungsverteiler (Token Ring)



- Bustopologie
  Multipunktverbindung zwischen verschiedenen Knoten



- Ringtopologie
  Punkt zu Punkt Verbindungen zwischen Knoten, die als Zwischenverstärker das Signal regenerieren können (Repeater).



- Hybridtechnologie (Mischtopologie)
  LANs unterschiedlicher Topologien werden verbunden

Meistens findet man in heutigen Netzen verschiedene der vorgestellten Topologien gleichzeitig. Mit den verschiedenen Topologien sind auch die Protokolle der MAC Teilschicht festgelegt bzw. umgekehrt. Die typischen Konfigurationsregeln (z.B. Längen) sind durch die entsprechenden Protokolle vorgegeben.

Zudem wird häufig eine hierarchische Struktur von Netzen aufgebaut, bestehend aus zwei oder auch drei Ebenen:

Ebene 1: Backbone (Firmenweites Netzwerksegment). Hier wird eine häufig Netzwerktopologien verwendet, die hohe Übertragungsraten erlauben (z.B. Token Ring, FDDI, zunehmend auch Switches (s. später)).
Ebene 2: Stockwerksverkabelung (fällt manchmal mit dem Backbone zusammen)
Ebene 3: Abteilungsverkabelung (getrennter Aufbau von Netzwerksegmenten abteilungsweit. Trennung von der Stockwerkssegmenten oder Backbone durch Geräte zur Lasttrennung (Router, Bridges/Switches s. später).

	Maschen	Stern	Bus	Ring
Verlegung				
Ausfallsicherheit				
Fehlersuche				
Eignung für kleine Netze				
Eignung für große Netze				
wesentlicher Nachteil				
Wesentlicher Vorteil				

5.2 Übertragungsverfahren

5.2.1 Grundlagen

- Breitbandübertragung
  auf verschiedenen Frequenzen verschiedene Infomation übertragen
- Basisbandübertragung
  ohne Träger - Signal benötigt die gesamte Bandbreite

Übertragung mehrer Kanäle im
Zeitmultiplex - Time Division Multiplex – TDM
  Zeitliche Verschachtelung digitaler Signale auf einem Übetragungsmedium
  - Synchron: feste zeitliche Zuordnung von Kanälen (z.B. im ISDN verwendet)
  - Asynchron: Variable Aufteilung, Verwendung von Zellen (z.B. ATM)

Frequenzmultiplex - Frequency Division Multiplex – FDM
  Übertragung mehrere analoger Signale auf einem Übertragungsmedium in versch. Frequenzlagen

Wellenlängenmultiplex – Wavelength Division Multiplex – WDM
  Übertragung versch. Informationskanäle bei verschiedenen Wellenlängen gleichzeitig in einem Lichtwellenleiter.
  Typische Bandbreiten: 96 Kanäle a 10Gbit/s, Nortel Networks: 160 Kanäle a 10Gbit/s, Testphase: 40Gbit/s pro Wellenlänge, Labor: 80Gbit/s(Stand April 2000)

5.2.2 Asynchrone Übertragung

Zeichenweise Informationsübertragung (Start - Stop Verfahren). Kein kontinuierlicher Datenstrom zwischen Sender und Empfänger.

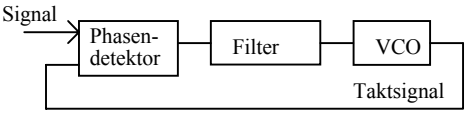
V.24

Start	Zeichen	Parity	Stop

Problematik: 20% - 30% Overhead

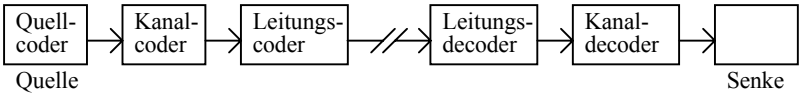
5.2.3 Synchrone Übertragung

Kontinunierlicher Datenstrom zwischen Sender und Empfänger.
Zeichenorientierte Übertragung (verwendet z.B. bei BSC - Binary Synchronous Control)
ältere Host Systeme - heute kaum mehr
Bitorientierte Übertragung (verwendet bei SDLC, HDLC, LAP-B)
Synchronisierung Sender / Empfänger durch ein Taktsignal im Datenstrom
Empfänger: Taktrückgewinnung - Prinzip PLL

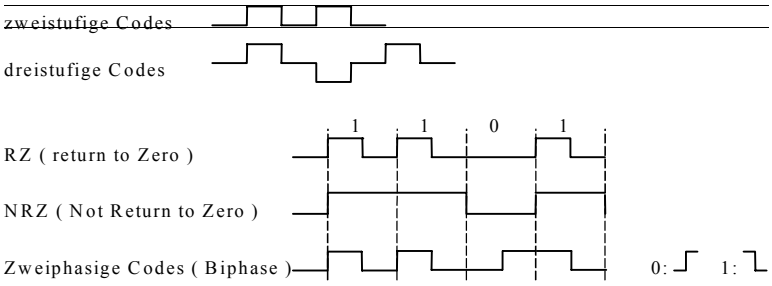


Notwendig zur Taktrückgewinnung:
genügend Flanken im Signal → Leitungs - Code

5.2.4 Leitungscodierung:



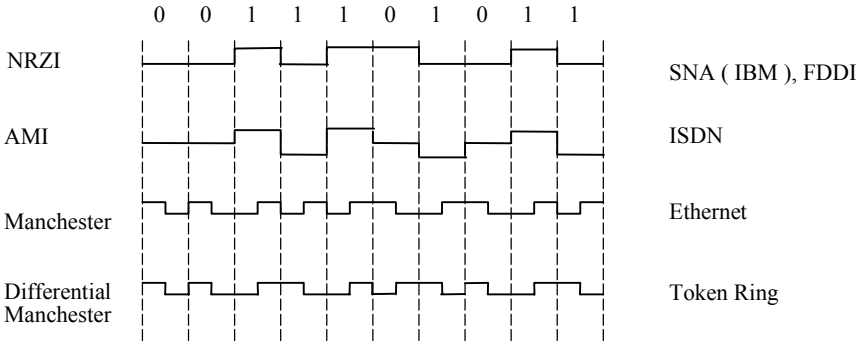
Zur Übertragung digitaler Signale ist eine Leitungscodierung notwendig, die festlegt, wie bestimmte Folgen von 0 und 1 physikalisch durch bestimmte Spannungspegel repräsentiert werden. Dabei unterscheidet man:



Es gibt zwei grundsätzlich unterschiedliche Arten der Leitungscodierung
- Codierung der einzelnen Bits
Hierbei wird jedes Bit codiert, z.B. NRZ: 0=0v, 1= 5V
- Codierung der Übergänge zweier aufeinanderfolgender Bits

Hierbei wird z.B. eine 0 durch Wiederverwendung des vorangegangenen Symbols, eine 1 als Umkehrung des vorangegangenen Symbols codiert, z.B NRZI: 0 Signal bleibt konstant, 1: Signal ändert sich

Die meisten der gängigen Leitungscodes sind aus Kombinationen dieser grundsäzlichen Verfahren entstanden. Speziell im Netzwerkbereich verwendete Leitungscodes sind z.B:



NRZ z.B. 0 = 0V1 = 5V
NRZI z.B. 0 = konst. 1 = Pegeländerung

Bewertungskriterien für Leitungscodes:
- Synchronisierbarkeit
- Bandbreitenausnutzung
- Gleichspannungsfreiheit
- Störempfindlichkeit
- Implementierungsaufwand

Anpassung des Kanalcodes an den Leitungscode
Gerade bei Verwendung von Codes, die eine geringe Bandbreiteausnutzung haben, aber damit evtl. auch bei langen Folgen von gleichen Bits nicht genügend Flanken im Signal zur Taktrückgewinnung bereitstellen (wie z.B. NRZ, NRZI oder andere) wird häufig die zu übertragende Bitfolge umcodiert, um ein Signal mit genügend Flanken zu erhalten.

Beispiel: Verwendung 4B/5B Codierung mit NRZI bei FDDI:
Hier werden jeweils Halbbytes durch 5 bit Worte ersetzt und zwar so, daß den 16 möglichen Halbbytes 16 geeignete 5bit Codeworte (aus 32 Möglichkeiten) zugeordnet werden. Geeignete Codeworte sind solche, die bei der Leitungscodierung genügend viele Signalflanken beinhalten.

Ein anderes Beispiel ist die Verwendung eines 3B/4B Codes beim ISDN.

6. Data Link Layer

Die Sicherungsschicht (Data Link Layer) unterteilt sich in 2 Bereiche:
- MAC Teilschicht (Media Access Control)
- LLC Teilschicht (Logical Link Control)

6.1 LAN Zugriffsverfahren

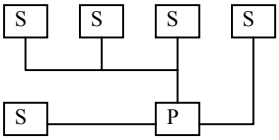
6.1.1 Logische Topologien

Unabhängig von der physikalischen Topologie eines Netzes gibt es verschiedene Zugriffsverfahren, um zu steuern, wie Informationen auf das Medium gebracht werden können. Hierbei gibt es im Grunde drei Möglichkeiten:

- Steuerung des Medienzugriffs von einem zentralen Punkt (Polling). Nachdem hier ein zentraler Kontrollpunkt existiert, der logische Verbindungen zu jedem Teilnehmer aufbauen muß, um den Medienzugriff zu regeln, spricht man hier von einer logischen Sterntopologie.
- Konkurrenz der Teilnehmer untereinander um den Medienzugriff (Konkurrenzverfahren). Hier ist jeder Teilnehmer gleichberechtigt, man spricht von einer logischen Bustopologie.
- Steuerung des Medienzugriffs durch Weitergabe einer Sendeberechtigung von Teilnehmer zu Teilnehmer, d.h. in einem logischen Ring.

Es ist damit möglich, ein Netzwerk in physikalischer Sterntopologie aufzubauen (heute häufig eine sternförmige Verkabelung mit UTP Cat. 5 oder 6), und dann je nach verwendetem Zugriffsprotokoll ein logisches Busnetz (z.B. Ethernet) oder ein logisches Ringnetz (z.B. Token Ring) zu implementieren. Allerdings muß dann die Verkabelung hinsichtlich physikalischer Voraussetzungen (z.B. Leitungslängen) für die entsprechenden Zugriffsprotokolle verwendbar sein.

6.1.2 Polling (Logische Sterntopologie)



zentrale Zugriffssteuerung
Vorteil: Deterministisches Verfahren (Zeitscheibenverfahren)
Nachteil: Overhead
Anwendung: Host - Umgebung z.B. IBM

6.1.3 Konkurrenzsystem (Contention, logische Bustopologie)

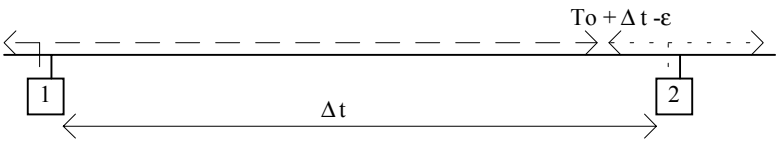
Grundregel: Teilnehmer können bei Bedarf Daten sofort senden → Kollisionen
Abhilfe gegen Kollisionen:
- Trägererkennung CSMA (Carrier Sense Multiple Access
- Kollisionserkennung CD (Collision Detection)
  → CSMA / CD
  Nach Kollision wird eine zufällige Zeitspanne gewartet
  abhängig von Anzahl bisher erfolgloser Versuche
  Kollisionserkennung durch Spannungsüberhöhung auf der Leitung (analoger Prozess)
- Kollisionsvermeidung CA (Collision Avoidance)

→ CSMA / CA
kurzes RTS (Request to Send) Paket wird zum Empfänger geschickt und quittiert
dann erst Datenübertragung

Vorteile: Einfaches Protokoll, geringer Overhead
Nachteile: nicht deterministisch (Antwortzeiten nicht kalkulierbar, keine Prioritäten möglich)

Anwendung:
CSMA / CD → Ethernet, IEEE802.3
CSMA / CA → LocalTalk (Apple)

Problematik Kollisionserkennung



To: Station 1 sendet
To + Δt - ε: Station 2 sieht das Paket gerade noch nicht und sendet ebenfalls
→ Kollision
To + 2Δt: Sender erfährt von Kollision

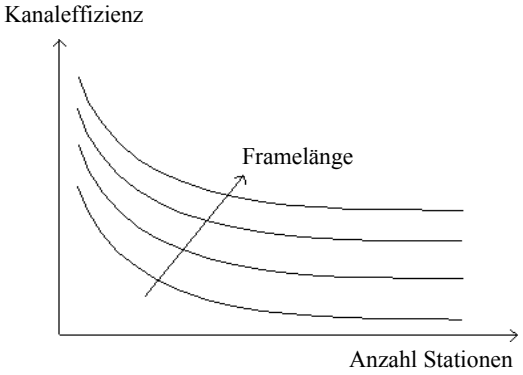
2Δt = Konkurrenzperiode
erst nach dieser Zeit kann der Sender sicher sein, daß keine Kollision erfolgt ist
Ausbreitungsgeschwindigkeit typ. 200m / µs
Bei 500 m Länge: 2Δt = 5µs

Sender sendet in 2Δt: ΔB = 50 Bit
ΔB↑ bei größeren Leitungslängen
ΔB↑ bei größeren Übertragungsraten

Kanaleffizienz: [Tannenbaum, Kap. 3.4]
Vorraussetzung: konst. Wahrscheinlichkeit für nochmalige Übertragung

$$K_{eff} = \frac{1}{1+2\frac{Ble}{cF}}$$

B = Bandbreite
c = Ausbreitungsgeschwindigkeit
l = Länge der Leitung
e = nat. Zahl
F = Framelänge



Das CSMA Verfahren ist skalierbar, d.h. bei höheren Datenraten kann man durch Verringerung der Leitungslänge oder durch Erhöhung der minimalen Paketgröße die Konkurrenzperiode konstant halten.

6.1.4 Token Passing (logische Ringtopologie)

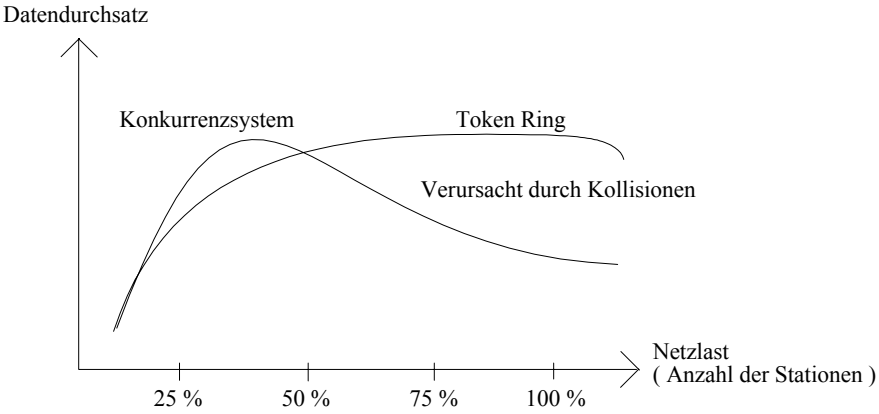
Ein spezielles Bitmuster (Token) wird als Sendeberechtigung von Station zu Station weitergereicht. Das Token kann von jeder Station durch einen Frame ersetzt werden. Der Frame wird durch das Netz zum Empfänger geschickt, dieser quittiert den Erhalt und sendet den Frame zurück zum Empfänger. Dieser nimmt den Frame vom Netz. Der Sender kann nun ein weiteres Paket senden, oder er gibt den Token wieder frei. Eine Station behält den Token, d.h. die Sendeberechtigung nur für eine bestimmte Zeit, die Tokenhaltezeit, danach muß sie den Token auf jeden Fall weitergeben..

Vorteile:
- Deterministisches Verfahren (d.h. Antwortzeiten kalkulierbar),
- Eine Prioritätensteuerung ist möglich, d.h. es können wichtigere und unwichtigere Stationen definiert werden.

Nachteil:
- Protokollaufwand hoch, z.B. muß eine Station im Netz Aufgaben der Ringwartung übernehmen (wie Erzeugung von Tokens, Verhinderung endlos kreisender Pakete, Neustart wenn Token verlorengeht usw.)

Anwendung: Token Ring, Arcnet, Token Bus (IEEE 802.4), FDDI

6.1.5 Vergleich Token Passing / Konkurrenzsystem



Konkurrenzsystem: Protokoll-Limitierung
Token Passing: Limitierung durch evtl. Netzwerkhardware
Token Passing verträgt höhere Netzlast

6.2 IEEE Projektgruppen

Network	IEEE 802.1 Internetworking		
LLC	802.2 LLC		
MAC	802.3 CSMA/CD	802.4 Token Bus	802.5 Token Ring
PHYS.	Basisband Breitband	Breitband	Basisband

802.6	MAN
802.7	Breitbandtechnologie
802.8	Fiber Optics
802.9	Integration Sprache - Daten
802.10	LAN Sicherheit
802.11	Wireless
802.12	High - Speed - Netze

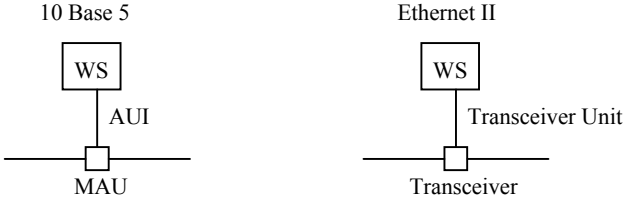
6.3 Protokolle der MAC Teilschicht
6.3.1 IEEE 802.3 und Ethernet

Beide Verfahren verwenden CSMA/CD Zugriffsprotokoll, Ethernet ist sich zunächst die klassische Variante eines physikalischen Busnetzes, unter IEEE 802.3 werden eine ganze Reihe von Varianten von CSMA/CD Netzen unter dem auch dafür üblicherweise verwendeten Begriff "Ethernet" zusammengefaßt. Diese Varianten unterstützen verschiedene physikalische Topologien und Übertragungsraten. Die gängigsten sind:

10 Base 5	Koaxverkabelung mit 500 m Segmentlänge (Thickwire)
10 Base 2	Koaxverkabelung mit 185 m Segmentlänge (Thinwire)
10 Base T	Twisted Pair
10 Base F	Fiber Optic 2 strangig (FB = synchron, FL = asynchron)
100 Base TX	Twisted Pair bidirektional, 4 adrig, UTP Cat5, STP Typ 1
100 Base T4	Twisted Pair 8 adrig (2x4), UTP Cat 3 und höher
1000 Base TX	Twisted Pair bidirektional , 4 adrig

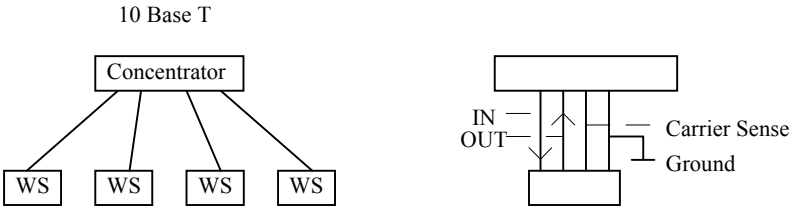
Bezeichnungen:
- 10, 100, 1000: Übertragungsrate in Mbit/s
- Base: Basisbandübertragung

Die klassische Ethernet Spezifikation und die IEEE 802.3 Standards unterscheiden sich zudem bei üblichen Bezeichnungen für die Geräte:



AUI = Attachement Unit Interface
MAU = Medium Attachement Unit

Nachfolgendes Bild zeigt eine typ. 10 Base T Verkabelung mit 4 adrigen Leitungen



Ein sehr weitgehender weiterer Unterschied ist die Verwendung unterschiedlicher Frameformate. IEEE 802.3 kennt neben dem im klassischen Ethernet verwendeten Frameformat Ethernet_II noch drei weitere verschiedene Frameformate. Im folgenden sind die Formate gegenübergestellt:

Ethernt_II

Präambel	Ziel-adresse	Quell-adresse	Typ	Daten	CRC

Ethernet_802.3 Rohformat

Präambel	Ziel-adresse	Quell-adresse	Länge	Daten	CRC

Ethernet 802.2 (eigentlich IEEE802.3 und IEEE802.2)

Präambel	Ziel-adresse	Quell-adresse	Länge	LLC	Daten	CRC

Ethernet_SNAP (Subnetwork Adressing Protocol)

Präambel	Ziel-adresse	Quell-adresse	Länge	LLC	Typ	Daten	CRC

Die verschiedenen Frameformate können jeweils für unterschiedliche Netzwerkprotokolle verwendet werden, da die Netzwerkprotokolle unterschiedliche Adressierungsarten von der Data Link Layer her unterstützen. Die nachfolgende Tabelle zeigt, welche Frameformate für welche gängigen Netzwerkprotokolle verwendet werden können.

Frameformate	Gängigste Netzwerkprotokolle
Ethernet_II	IPX, TCP/IP, NetBeui
Ethernet_802.3	IPX, NetBeui
Ethernet_802.2	IPX, SNA, NetBeui
Ethernet_SNAP	IPX, TCP/IP, AppleTalk, NetBeui

6.3.2 IEEE 802.5 und Token Ring

	802.5	Token Ring
max. Stationen	250	260 / 72
Datenrate	1 MBit/s - 4 MBit/s	4 MBit/s - 16 MBit/s
Medium	not specified	TP
Topologie	not specified	Stern

Token Ring Verkabelung: Star-wired Ring

Token Ring Frame Formate:
- Token_Ring
- Token_Ring SNAP (vgl. Ethernet)

Frameaufbau Token Ring
- AC = Access Control
- FC = Frame Control
- FS = Frame Status
- DA = Destination Address
- SA = Source Address

AC - Byte:

P	P	P	T	F	R	R	R

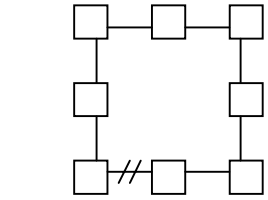
P = Prioritätsbits
R = Reserviert für Priorität
T = Token Bit; (0 = Token; 1 = Frame)
M = Monitorbit
- sendende Station setzt M = 0
- active Monitor setzt M = 1
- wenn ein Frame bei dem M = 1 am Active Monitor vorbeikommt
- → Frame wird vernichtet (endlos kreisend)

FC - Byte:
Datenfeld enthält Daten oder Control Informationen

FS - Byte
- 2 Bit - Address Resolution Bits
  - Empfänger sagt: habe an mich adressierte Nachricht gefunden
- 2 Bit - Frame Copied Bits
  - Empfänger sagt: habe Nachricht erfolgreich in meinen Speicher kopiert

Protokollaufgaben:
zentrale Ringwartung → Überwachungsstation (Active Monitor)
- steuert die Erzeugung eines Tokens (Claim Token Process)
- bei Verlust des Tokens → Ring leeren → neues Token erzeugen
- Vernichten endlos kreisender Pakete (M- Bit)
- Erkennen verstümmelter Frames
- Ringzusammenbruch
- einfügen von 24 Zusatzbits
- Erzeugen eines Taktsignals (Ringtakt)

Mechanismus zur Fehlersuche im Token Ring:
Jede Station überprüft dauernd ob sie vom vorherigen Knoten (NAUN= Nearest Active Upstream Neighbour) Datenpakete erhält. Bei Leitungsunterbrechungen (Unterbrechung des Rings), sendet sie ein Dauersignal (Beacon Frame). Mit Hilfe eines Netzwerkanalysetools kann dann festgestellt werden, welche Station die meisten Beacon Frames gesendet hat, die damit am nächsten an der Fehlerstelle positioniert ist.



Physikalische Länge eines Bits:
Datenübertragungsrate 4 MBit/s
Ausbreitungsgeschwindigkeit ca. 200 m/µs
→ Bitlänge = (200 m/µs) / (4 MBit/s) = 50 m

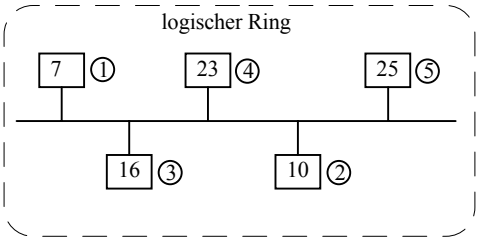
Datenübertragungsrate 16 MBit/s
→ Bitlänge = (200 m/µs) / (16 MBit/s) = 12,5 m

Das bedeutet z.B., daß ein 4kByte großer Frame im 4Mbit/s Token Ring eine physikalische Länge von 820km besitzt. Bei Ringdurchmessern, die kleiner sind (und das sind sie typischerweise), bedeutet das, daß eine sendende Station quasi gleichzeitig senden und empfangen muß.

Damit dies nicht eventuell auch bei Token selbst geschieht, fügt der active Monitor eine Verzögerung von 24 bit (entspricht der Länge des Tokens selbst) ein.

6.3.3 Token Bus

Dezentrale Ringwartung und kein active Monitor



- Automatische Tokenerzeugung wenn bestimmte Zeit kein Token gesehen wurde
- Jede Station merkt sich den log. Vorgänger und Nachfolger
- beim Einschalten einer Station → Folgeadressuche
- beim Verlassen meldet die Station dem Vorgänger die log. Adresse des Nachfolgers
  (Set Successor Frame)

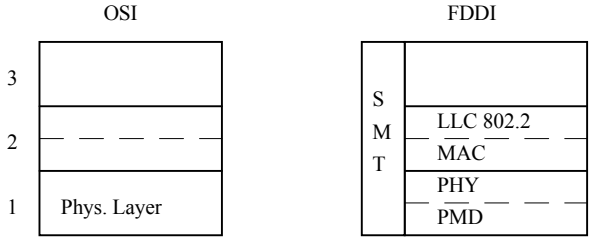
Einsatz in 802.4 Netzen
MAP = Manufacturing Automation Protocol
und in Arcnet Netzen in vereinfachter Form

6.3.4 FDDI (Fiber Distributed Data Interface)

ANSI - Standard seit 1986
Erster 100 Mbit/s LAN-Standard überhaupt, ursprünglich konzipiert für Glasfaser-Übertragung

Multimodefaser: max Entfernung = 2 km zwischen 2 Stationen
Monomodefaser: max Entfernung = 60 km zwischen 2 Stationen
Max. Anzahl der Stationen = 1000 (effektiv nur 500 → Doppelring)
Max. Ringdurchmesser = 200 km (effektiv 100 km)

Leitungscodierung:
Token Ring Diff. Manchester
FDDI NRZI 4B / 5B
Umcodierung: Halbbytes werden ersetzt durch 5 Bit - Worte
z.B. 0000 → 11110 [Rechnernetze nach OSI, Kap. 13.6.3]



PHY = Physical Layer Protocol (Kodierung, Synchronisation)
PMD = Physical Medium Dependend (Zugriff auf optisches Medium)
SMT = Station Management (Asynchrone und / oder synchrone Bandbreite)

FDDI:
Jede Station ist active Monitor
Beaconing wie bei 802.5
Framelänge max. 4500 Byte

Varianten bzw. Weiterentwicklungen:

FDDI-2
Token Passing wird ersetzt durch echte synchrone Übertragung, dabei Aufteilung der Bandbreite in feste Slots mit ca 6MB/s Übertragungsrate pro Kanal, Rahmenlänge 12500 bit mit Taktrate 8kHz. Synchrone Übertragung über feste Kanäle, restliche frei Slots im Rahmen können für Paketverkehr verwendet werden.

FDDI auf Twisted Pair 100 MBit/s
Green Book Vorschlag 1991
Weiterentwickelt SDDI
auf STP 150Ohm mit NRZI

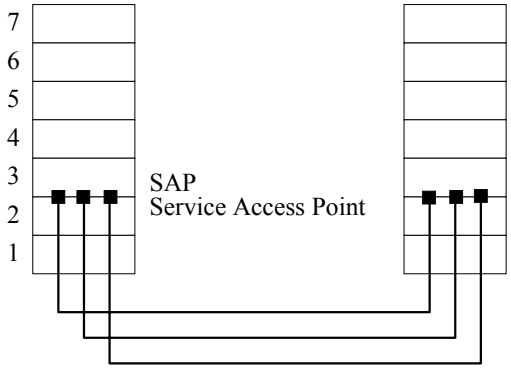
CDDI Copper DDI 1990
Umkodierung auf UTP Cat 5

TP-PMD (TP-Physical Medium Dependet -FDDI)
→UTP Cat 5
→ STP 150 Ohm IBM Typ 1
Umkodierung auf MLT - 3 (;Multilevel3)

6.4 IEEE 802.2 LLC

LLC - Frame:

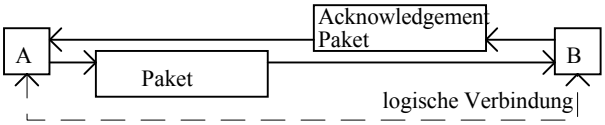
Header	DSAP Adresse	SSAP Adresse	Control	Information	CRC



LLC
Typ 1

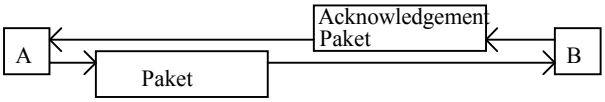
Unacknowledged - Connectionless Service
Verbindungslose Übertragung

Typ 2



Connection Oriented Service (Verbindungsorientierte Übertragung)

Typ 3



Acknowledged Connectionless Service

7. Network Layer

Typische Aufgaben von Protokollen der Netzwerkschicht sind folgende:
- Netzwerkweite Adressierung
- Verhinderung endlos kreisender Pakte in Netzen
- Übertragungsfehlerkontrolle (i.A. bei WAN Protokollen)
- Routing (Routenfindung und Abgleich von Routinginformation in Netzen)

7.1 Netzwerkweite Adressierung

Eine der wesentlichen Aufgaben von Protokollen der Netzwerkschicht ist eine netzwerkweite Adressierung. Jedem Rechner, d.h. jeder Netzwerkkarte mit einer Hardwareadresse wird nochmal eine Netzwerkadresse zugeordnet.

Damit stellt sich zunächst die Frage, warum die bereits vorhandenen Hardwareadressen nicht ausreichen, die von den Netzwerkkartenherstellern sowieso weltweit eindeutig vergeben werden. Damit wäre ja auch in einem weltweiten Netz wie z.B. dem Internet jeder Rechner eindeutig identifizierbar. Die Antwort zu dieser Frage liegt unter anderem in der Verwaltbarkeit von Adressen auch im Hinblick auf Unterstützung von Routing. Netzwerkadressen können nach logischen Gesichtspunkten organisiert werden, Hardwareadressen sind durch die Hersteller der Netzwerkkarten vorgegeben. Wollte man eine Liste von allen Teilnehmern im Internet machen, wäre diese Liste relativ unübersichtlich. Sie wäre ungefähr genauso unübersichtlich wie ein Telefonbuch mit allen Telefonteilnehmern in Deutschland, wenn die Telefonnummern in der Reihenfolge der Anmeldung der Teilnehmer am Netz der Telekom eingetragen würden. Wie sieht die Abhilfe der Telekom aus? Nun, es werden Ortkennzahlen verwendet, unter anderem werden auch die Telefonnummern selbst nach Stadtteilen organisiert.

Eine solche Organisation findet auch bei der Verwendung von Netzwerkadressen statt. Die Adressen werden nicht Rechner für Rechner vergeben, sondern netzwerkweise, wobei ein Netzwerk unterschiedlich viele Rechner enthalten kann.

Eine Netzwerkadresse besteht grundsätzlich aus zwei Teilen:
- Netzwerkanteil (entspricht im obigen Beispiel einer Vorwahl)
- Hostanteil (entspicht der individuellen Nummer des Teilnehmers)

Damit wird eine Zuordnung des Netzwerkanteils einer Netzwerkadresse pro Netzwerksegment ermöglicht, die Unterscheidung der einzelnen Rechner erfolgt über den Hostanteil.

Das Adressformat ist je nach verwendetem Netzwerkprotokoll unterschiedlich.

Beispiele:

Novell IPX Protokoll
Das IPX Protokoll verwendet 20 stellig hexadezimale Adressen, aufgeteilt in einen festen Netzwerkanteil (8-stellig bzw. 32bit) und einen Hostanteil (12stellig bzw. 48bit). Letzterer ist identisch mit der Hardwareadresse des jeweiligen Rechners und wird daher nicht individuell konfiguriert. Damit wird eine Zuordnung einer Netzwerkadresse pro Netzwerksegment ermöglicht, die Unterscheidung der einzelnen Rechner erfolgt dann ausschließlich über die Hardwareadresse.

Internet Protokoll (IP):
Hier werden 32bit Netzwerkadressen verwendet. Die Aufteilung in einen Netzwerk und Hostanteil ist variabel, die möglichen Adressen werden in verschiedene Adressbereiche (sogenannte Klassen) aufgeteilt, die eine unterschiedliche Aufteilung in Netzwerk und Hostanteil vorgeben. Zur Unterscheidung werden die ersten Bits der IP Adresse harangezogen.

Das folgende Bild zeigt eine Aufteilung der Klassen, der Netzwerkanteil ist jeweils mit x, der Hostanteil mit y markiert.

Klasse	32 bit Adresse	Dezimale	Anzahl mögl.	Anzahl mögl.

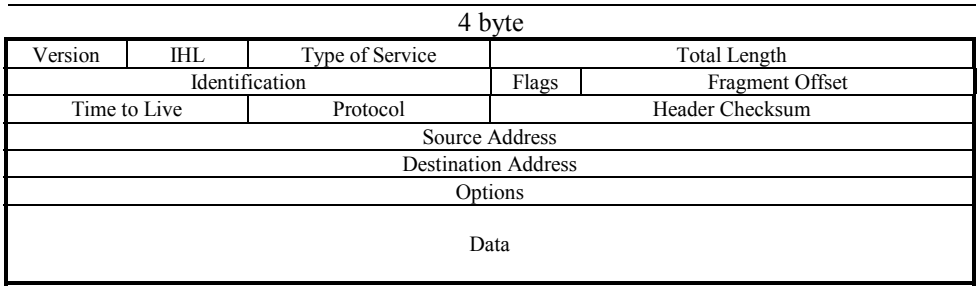
		Adresse	Netzwerke	Hosts
Class A	0xxxxxxx.yyyyyyyy.yyyyyyyy.yyyyyyyy	1-126	126	16.777.214
Class B	10xxxxxx.xxxxxxxx.yyyyyyyy.yyyyyyyy	128-191	16.384	65.534
Class C	110xxxxx.xxxxxxxx.xxxxxxxx.yyyyyyyy	192-223	2.097.152	254

Class A bedeutet nun, daß das erste Byte als Netzwerkadresse und die übrigen als Hostadresse interpretiert wird, bei Class B sind es die ersten beiden Bytes, bei Class C die ersten drei Bytes. Die restlichen möglichen Adressen sind für besondere Aufgaben reserviert. Die IP Adressen jedes einzelnen Rechners sind individuell festzulegen. Sie können entweder für jede Station einzeln konfiguriert werden, die andere Möglichkeit ist, daß die einzelnen Rechner ihre IP Adressen bei Bedarf von einem zentralen Rechner über ein spezielles Protokoll (überwiegend DHCP) abfragen. Auf dem DHCP Server wird dann ein bestimmter Adressbereich zur dynamischen Vergabe bereitgehalten.

7.2 Das Internet Protokoll (IP)

IP ist als Übertragungsprotokoll das Basisprotokoll für die Internet Protokollwelt. Es wird der dritten Schicht (Netzwerkschicht) des OSI Referenzmodells zugeordnet und setzt damit auf den Protokollen der Data-Link Layer (z.B. Ethernet) auf, die den Zugriff auf das Übertragungsmedium steuern. Im OSI Referenzmodell nach oben gesehen stellt es die Basis für die Transprotprotokolle TCP oder UDP (Ebene 4 des OSI Modells) dar.

Das folgende Bild zeigt den Aufbau eines IP Frames:



Die einzelnen Felder haben folgende Bedeutung:

- Version: Die Version des IP Protokolls, die aktuelle Version ist 4.
- IHL: IP-Header Länge in 32bit Worte
- Type of Service: Angabe für die Upper Layer Protokolle, wie ein spezielles IP-Paket zu handhaben ist. Festgelegt werden:
  - die Wichtigkeit Pakets in Werten von 0 bis 7 und
  - Je ein Bit für Festlegung auf
    - niedrige Verzögerungszeit
    - hohe Übertragungsgeschwindigkeit
    - hohe Zuverlässigkeit
    - bei der Übertragung
- Total Length: Gesamtlänge des IP-Pakets in Bytes, inklusive Daten und Header
- Identification: Eindeutige Identifizierung eines einzelnen Pakets
- Flags: Zwei der drei Bits legen fest, wie und ob ein Paket von der Transportschicht in mehrere IP-Fragmente unterteilt wurde.
- Time to Live: Dieses 8 bit Feld legt fest, über wieviele Router das Paket mmaximal weitergereicht werden darf, bis es vernichtet wird. Jeder Router dekrementiert den Wert um 1.
- Protocol: Legt fest, welches Transportprotokoll (z.B. TCP oder UDP) verwendet wird.
- Header Checksum: Fehlerkontrolle des IP Headers
- Source und Destination Address: 32bit Quell- und Zielnetzwerkadressen (siehe später)
- Options: Dieses Feld kann unterschiedliche Längen aufweisen. Wird für zusätzliche Daten verwendet wie z.B. für Source Routing, Zeitinformation, aber auch zum Auffüllen mit Bits (Padding) um z.B. die minimale Paketlänge im Ethernet garantieren zu können.

7.3 IP-Adressierung

Als Protokoll der Netzwerkschicht erlaubt IP eine reine Netzwerkadressierung, d.h. Sende und Empfangsadressen sind hardwareunabhängig und damit in einem abgeschlossenen Netz frei wählbar. Bei Anschluß an das Internet erhält man eine oder mehrere Adressen von einem sogenannten Service Provider, also einer Firma, die einem eine physikalische Verbindung ins Internet zur Verfügung stellt.

Der Adressraum umfaßt dabei 32 Bit, wobei jeder Host (Rechner mit IP-Nummer) eine eindeutige IP Nummer zur Kommunikation benötigt. Dies schränkt die Menge der weltweit eindeutig verfügbaren Adressen deutlich ein. Je nach Klasse wird nun ein unterschiedlicher Anteil von Bytes jeweils als Netzwerkadresse und Hostadresse interpretiert. Darüberhinaus gibt es aber auch die Möglichkeit, diese feste Zuordnung zu verlassen, und eine andere individuellere Aufteilung von Hostanteil und Netzwerkanteil festzulegen. Um dies bei der Konfiguration zu können, wird neben der reinen IP Adresse eine Angabe benötigt, wie diese Adresse jeweils zu interpretieren ist. Dazu wird jedem Rechner neben der IP Adresse auch noch eine sogenannte Netzwerkmaske zugeteilt, anhand derer die Aufteilung zu erkennen ist. Die Netzwerkmaske wird dabei so definiert, daß der Netzwerkanteil einer Adresse mit 1-bits, der Hostanteil mit 0-bits dargestellt wird.

Natürlich werden hier nicht die einzelnen Bits dargestellt, sondern die Bites werden zu Bytes zusammengefaßt und wie die Adressen selbst mit einem „ . “ getrennt. Die einzelnen Bytes werden nun in dezimaler oder, bei Netzwerkmasken, in hexadezimaler Schreibweise dargestellt. Ein Beispiel für eine typische Netzwerkadresse wäre damit:

Adresse:	183. 94. 51. 45	bzw.	183. 94. 51. 45
Netzwerkmaske:	255.255. 0. 0	bzw.	FF. FF. 0 . 0

Die Netzwerkmaske definiert für die ersten beiden Bytes lauter 1-Bits, für den Hostanteil lauter 0-Bits. Diese Vorgehensweise erlaubt es einem Rechner, durch eine einfache bitweise UND-Verknüpfung aus einer beliebigen Adresse den Netzwerkanteil festzustellen. Dies würde sich wie folgt darstellen:

Adresse:	10110111 . 01011110 . 00110011 . 01001101
Maske:	11111111 . 11111111 . 00000000 . 00000000
Netzwerkanteil:	10110111 . 01011110 . 00000000 . 00000000 , festgestellt durch UND Verknüpfung

Einige Konventionen, die es bei der Vergabe von IP-Adressen zu beachten gilt, sind:

Netzwerkadressen:
Adressen mit Hostanteil 0 repräsentieren nicht eine einzelne Station, sondern einen ganzen Netzwerkstrang, z.B. repräsentiert die Adresse 162.120.0.0 eine Class B Netzwerkadresse, die Hosts in diesem Netzwerk besitzen Adressen von 162.120.0.1 bis 162.120.255.254.

Broadcast:
Adressen mit einem Host- oder Netzwerkanteil, der nur aus 1-Bits besteht, sind nicht erlaubt, da diese Adressen für Broadcasts, also Pakete an alle Hosts eines Netzwerks, reserviert sind. Nach obigem Beispiel wäre also die Class B Adresse 162.120.255.255 verboten.

Loopback (bzw. Localhost):
Die Adresse 127 ist eine spezielle Adresse, die Funktionalitätstests zum Netzwerk erlaubt. Sie erlaubt die Kommunikation eines Clients und eines Hosts auf demselben Rechner via TCP/IP, ohne Daten tatsächlich auf das Netzwerk zu senden. Auch bei Broadcasts sorgt das Loopback-Interface in einem Rechner dafür, daß Daten die auf das Netz gesendet werden auch die eigene Station mit einschließen. Meistens wird 127.0.0.1 als Loopback-Adresse verwendet.

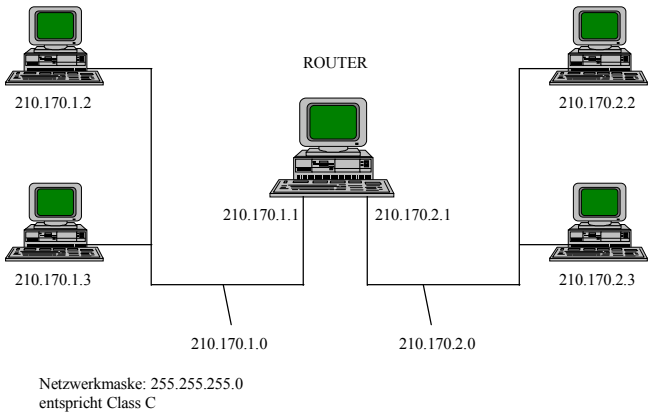
7.4 Paketzustellung im IP-Netz

7.4.1 Das ARP Protokoll

Im folgenden ist nun zu klären, wie ein Datenpaket von einer Station zur nächsten gelangt. Die Kenntnis der (logischen) Netzwerkadresse einer Zielstation reicht nicht aus, um z.B. einen Ethernet Frame zu bauen, in dem die Hardwareadresse der Zielstation enthalten sein soll. Hierzu ist ein Adressauflösung nötig, d.h. um einer IP Station ein Paket senden zu können, muß aus der IP Zieladresse erst die entsprechende Hardwareadresse der Netzwerkkarte der Zielstation ernmittelt werden.. Diese Aufgabe übernimmt das ARP Protocol (Adress Resolution Protocol). Die sendende Station sendet einen Broadcast mit der Nachricht “Ich habe hier ein Paket für die Netzwerkadresse soundso, wer ist das ?”. Die Zielstation antwortet an die Hardwareadresse des Senders mit ihrer Netzwerk- und Hardwareadresse. Daraufhin kann das Paket an die Station mit der richtigen Hardwareadresse zugestellt werden.

7.4.2 Routing im IP Netz

Wir haben nun die Begriffe Netzwerk und Host eingeführt. Im folgenden wird ein Netzwerksegment als eine Verbindung zwischen mehreren Hosts betrachtet, die vom nächsten Netzwerk durch einen Router getrennt ist. Ein Router wird verwendet, um unterschiedliche Netzwerksegmente in einem Netzwerk zu verbinden (siehe auch später). Insofern muß auch ein IP-Router Netzwerkadressen nach Netzwerk und Hostanteil unterscheiden können. Die folgende Abbildung zeigt ein IP-Netzwerk mit zwei Class C Netzwerksegmenten.



Jeder Netzwerkkarte in jedem Host wird eine eigene IP Nummer zugeteilt, die beiden Teilnetze erhalten z.B. die Nummern 210.170.1.0 bzw 210.170.2.0. Die 0 kennzeichnet das jeweilige Netzwerksegment, die Nummer 1 bis 254 sind für die Rechner im jeweiligen Segment vorgesehen.

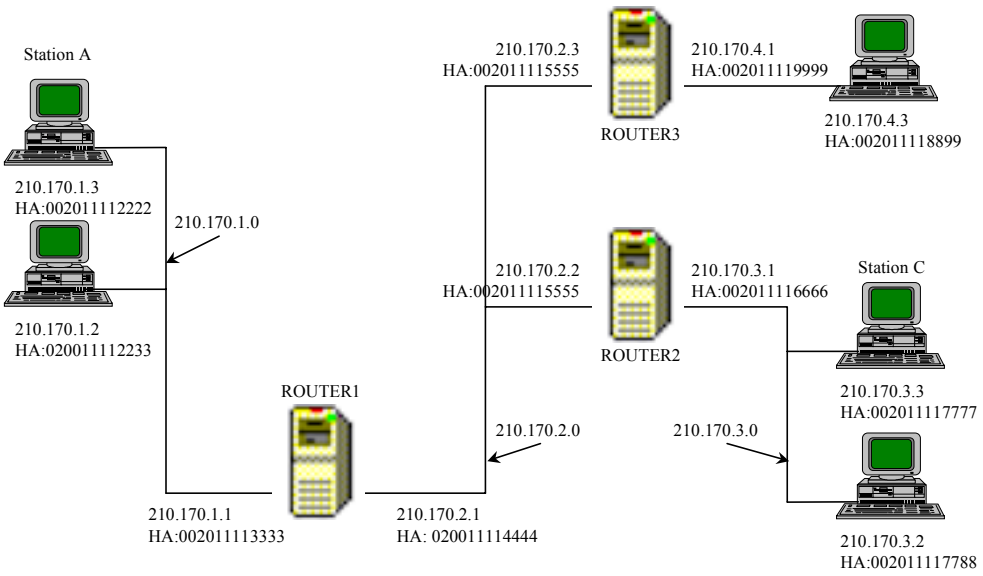
Wie funktioniert nun hier der Sendevorgang von Paketen?
Je nachdem, ob sich die Zielstation im gleichen Netzwerksegment befindet oder in einem anderen, ergeben sich zwei Möglichkeiten:

1. Die Zielstation befindet sich im gleichen Teilnetzwerk:
Die Zielhardwareadresse wird mittels ARP ermittelt und das Paket im lokalen Segment zugestellt.
2. Die Zielstation befindet sich in einem anderen Netzwerk:
Die Station stellt dies aufgrund einer anderslautenden Netzwerkadresse der Zielstation fest, sie sendet das Paket an den Router. Dieser hat dann die Aufgabe, das Paket an die entsprechende Station im anderen Segment zuzustellen. Damit das Paket dem Router zugestellt werden kann, muß der sendenden

Station natürlich auch die IP-Adresse des Routers bekannt sein, die entsprechende Hardwareadresse wird dann ebenfalls wieder über ARP ermittelt.

Damit muß die Konfiguration einer IP Station in einem Netzwerk mit Routern also folgende drei Angaben enthalten:
1. Netzwerkadresse des Hosts
2. Netzwerkmaske für diese Segment
3. Netzwerkadresse des nächsten Routers.

Nehmen wir ein Beispiel, wie ein Datenpaket in einem Netzwerk mit vier Teilnetzen weitergeleitet wird:



Netzwerkmaske: 255.255.255.0

Die Station A sendet ein Paket zur Station C. Dazu vergleicht sie zunächst die Netzwerkzieladresse mit ihrer eigenen Netzwerkadresse, um festzustellen, ob sich die Zielstation im gleichen Netzwerk befindet wie sie selbst oder in einem anderen Segment. In unserem Fall ist sie über zwei Router hinweg erreichbar.

Nachdem sich die Zielstation in einem anderen Netzwerksegment befindet, sendet die Station das Paket an den nächsten Router. Dessen Hardwareadresse wird über ARP ermittelt. Es wird also ein Frame mit folgenden Adreßfeldern erzeugt:

Ethernet Adressen:
Hardwarequelladresse: Adresse der Netzwerkkarte in der Sendestation
Hardwarezieladresse: Adresse der Netzwerkkarte im Router

IP Adressen:
Netzwerkquelladresse: 210.170.1.3
Netzwerkzieladresse: 210.170.3.3

Insgesamt wird also folgender Frame im Netzwerk 210.170.1.0 an den Router geschickt:

Ziel HW-Aresse	Quell HW-Adresse	Ziel IP-Adresse	Quell IP-Adresse	Daten
002011113333	002011112222	210.170.3.3	210.170.1.3	110110101110101

Das Paket wird zunächst an den nächsten Router gesandt. Dieser ersieht in seiner internen Routingtabelle, auf welchen Netzwerkstrang und zu welcher Zielstation das Paket weitergeleitet werden muß. Die internen Routingtabellen der drei Router sind in nachfolgender Tabelle zusamengestellt. In unserem Fall wird das Paket zum nächsten Router am Netzwerkstrang 210.170.2.0 weitergeleitet. Das Paket sieht nun wie folgt aus:

Ziel HW-Aresse	Quell HW-Adresse	Ziel IP-Adresse	Quell IP-Adresse	Daten
002011115555	002011114444	210.170.3.3	210.170.1.3	110110101110101

Dieser schaut wiederum in seine Routing Tabelle, stellt fest, daß die Empfangsstation im angrenzenden Segment 210.170.3.0 zu finden ist. Er führt einen ARP Request durch , um die Hardwareadresse zu ermitteln und stellt das Paket zu. Dies ist dann das zugestellte Paket:

Ziel HW-Aresse	Quell HW-Adresse	Ziel IP-Adresse	Quell IP-Adresse	Daten
002011117777	002011116666	210.170.3.3	210.170.1.3	110110101110101

Beim Routing werden also Pakete von einem Router zum jeweils nächsten weitergegeben, bis das Netzwerksegment mit der Zielstation erreicht ist. Dabei ändern sich jeweils die Hardwareadressen, die Netzwerkadressen bleiben konstant. Dieses Verfahren wird auch als Hop by Hop Routing bezeichnet. Jeder Router im Pfad analysiert die IP Adresse der Zielstation und legt aufgrund der Einträge in seiner Routingtabelle fest, an welche Zielstation das Paket gesandt wird. Im Netzwerksegment mit der Zielstation wird ebenfalls wieder über ARP die entsprechende Hardwareadresse ermittelt.

Routingtabellen:
In unserem Beispiel sehen die Routingtabellen der drei Router etwa wie folgt aus:

Router 1:

Ziel Netzwerk	Next Hop	Interface	
210.170.1.0	210.170.1.1	210.170.1.1	lokal
210.170.2.0	210.170.2.1	210.170.2.1	lokal
210.170.3.0	210.170.2.2	210.170.2.1	remote
210.170.4.0	210.170.2.3	210.170.2.1	remote

Router 2:

Ziel Netzwerk	Next Hop	Interface	
210.170.1.0	210.170.2.1	210.170.2.2	remote
210.170.2.0	210.170.2.2	210.170.2.2	lokal
210.170.3.0	210.170.3.1	210.170.3.1	lokal
210.170.4.0	210.170.2.3	210.170.2.2	remote

Router 3:

Ziel Netzwerk	Next Hop	Interface	
210.170.1.0	210.170.2.1	210.170.2.3	remote
210.170.2.0	210.170.2.3	210.170.2.3	lokal
210.170.3.0	210.170.2.2	210.170.2.3	remote
210.170.4.0	210.170.4.1	210.170.4.1	lokal

7.4.3 Subnetting

Obiges Beispiel zeigt, daß für getrennte Segmente auch getrennte Netzwerknummern nötig sind. Daher ist es z.B. schon aus administrativen Gesichtspunkten heraus sinnvoll, eine weitere Unterteilung einer Netzwerkadresse in weitere Teilnetze, sogenannte Subnetze, durchzuführen. Dies kann für Class A oder Class B Adressen z.B. so erfolgen, daß jeweils ein oder auch zwei Bytes zur Unterscheidung der Teilnetze herangezogen werden. Obiges Beispiel wäre also auch mit der Class B Adresse 162.170.0.0 möglich, wobei die Teilnetze 162.170.1.0, 162.170.2.0 und 162.170.3.0 heißen könnten.
Definiert würde das dann über eine Netzwerkmaske 255.255.255.0

Die Adresse 162 würde zunächst auf ein Class B Netz hindeuten, die Netzwerkmaske legt aber noch ein drittes Byte als Netzwerkadresse fest, diese dritte Byte wird dementsprechend zur Unterteilung der Subnetze herangezogen. Insgesamt könnten so 254 Subnetze in diesem Class B Netz gebildet werden.

Die Aufteilung der Adresse ergibt sich damit zu

	Binär:	Dezimal
Adresse:	10xxxxxx.xxxxxxxx.|xxxxxxxx.|xxxxxxxx	128-191.xxx.xxx.xxx
Netzwerkmaske:	11111111.11111111.|11111111.|00000000	255.255.255.0

Netzwerk Subnet Host

Grundsätzlich ist aber auch eine andere Netzwerkmaske möglich. Folgendes Beispiel zeigt Subnetting in einem Class C Netz:

	Binär:	Dezimal
Adresse:	110xxxxx.xxxxxxxx.xxxxxxxx.|xxx|xxxxx	192-224.xxx.xxx.xxx
Netzwerkmaske:	11111111.11111111.11111111.|111|00000	255.255.255.224

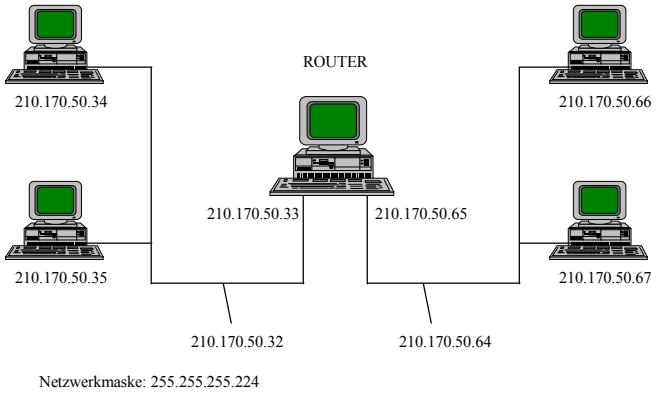
Netzwerk Subnet Host

Die ersten 3 bit des letzten Byte stehen nun zur Unterscheidung der verschiedenen Subnetze zur Verfügung. Damit können 6 (2^3-2) Subnetze gebildet werden, jedes dieser Subnetze kann 30 (2^5-2) Hosts enthalten. Adressen, bei denen alle Bits 1 oder 0 sind, werden häufig nicht verwendet, da eine Adresse mit 1-Bits auch als Broadcast und eine Subnetz-Adresse mit 0-Bits auch als das “Hauptnetz” interpretiert werden kann. Dies hängt weitestgehend von den verwendeten Routern und Routingprotokollen ab (so überträgt RIP z.B. nur Netzwerkadressen ohne dazugehörige Netzwerkmasken, OSPF oder andere Routingprotokolle (oft Routerherstellerspezifische) dagegen übertragen beides, so daß man hier flexibler wird). Durch Subnetting gehen also eventuell Adressen verloren, und zwar umso mehr, je weniger Bits die Subnetzmaske umfaßt. Dies muß dann aber in Kauf genommen werden , wenn eine logische Trennung in Subnetze durch die Verwendung von bestimmten Routern bzw. Routingprotokollen erfolgen soll.

Die Nummern der Subnetze lauten nun am Beispiel der Class C Adresse 210.170.50.0:

Binär (letztes Byte)	Dezimal (vollständ. Adresse)	Mögliche Hostadressen
000|00000	210.170.50.0	i.A nicht verwendet
001|00000	210.170.50.32	210.170.50.33-62
010|00000	210.170.50.64	210.170.50.65-94
011|00000	210.170.50.96	210.170.50.97-126
100|00000	210.170.50.128	210.170.50.129-158
101|00000	210.170.50.160	210.170.50.161-190
110|00000	210.170.50.192	210.170.50.193-222
111|00000	210.170.50.224	i.A. nicht verwendet

Die folgende Abbildung zeigt nochmals unser erstes Beispiel, nun aber mit Subnetting.

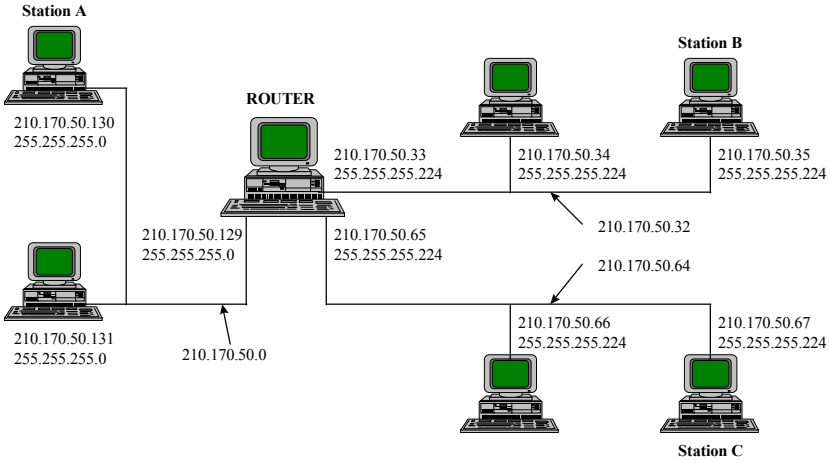


Auch hier kann aus einer gegebenen IP Adresse der Netzwerkanteil wieder durch bitweise UND Verknüpfung gewonnen werden, wie folgendes Beispiel zeigt:

Adresse:	10110111 . 01011110 . 00110011 . 01001101	183. 94. 51. 45
Maske:	11111111 . 11111111 . 11111111 . 11100000	255.255.255.224
Netzwerkanteil:	10110111 . 01011110 . 00110011 . 01000000	183. 94. 51. 32

7.4.4 Proxy ARP

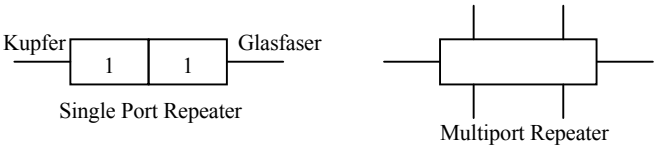
Generell ist es auch möglich, den verschiedenen Netzwerksträngen unterschiedliche Netzwerkmasken zuzuteilen. So ist z.B. eine Aufteilung wie im folgenden Bild möglich. Hier werden die Subnetze 32 und 64 verwendet, alle anderen werden in einem Netzwerksegment zusammengefaßt.
Allerdings besteht hier die Problematik, daß Sender und Empfänger unterschiedliche Subnetzmasken besitzen. Damit gehen sie bei der Kommunikation von unterschiedlichen Voraussetzungen aus, was die Frage betrifft, ob sich ein Kommunikationspartner im lokalen oder einem entfernten Netzwerksegment befindet.
Station B geht davon aus, daß sich Station A mit Adresse 130 im letzten Byte in einem anderen Subnetz als 64 befindet und schickt daher alle Pakete folgerichtig an den Router. Nur, Antwortpakete werden zunächst nicht empfangen. Station A geht nämlich aufgrund seiner Netzwerkmaske davon aus, daß sich alle Hosts mit den Adressen 1 bis 254 im letzten Byte im eigenen Segment befinden. Ein ARP Request für Station B oder C würde also zunächst keine Hardwareadresse liefern, womit diese Stationen zunächst unerreichbar wären.



Abhilfe schafft hier die Fähigkeit mancher Router, sogenanntes Proxy-ARP zu unterstützen. Ein Router, der Proxy-ARP unterstützt, ist in der Lage für alle Hosts in den angeschlossenen Subnetzen stellvertretend für diese Stationen ARP-Requests zu beantworten. Im konkreten Fall würde also der Router für Station B oder C seine eigene Hardwareadresse als die richtige angeben und sich dann um die Weiterleitung des entsprechenden Pakets kümmern. Proxy ARP wird von manchen UNIX-Routern, Hardwareroutern und Novell NetWare 4 Routern unterstützt, nicht jedoch von NetWare 3.

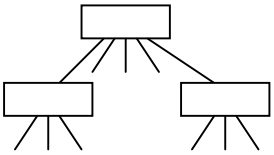
8. Internetworking

8.1 Repeater

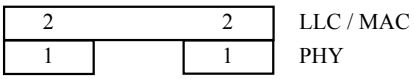


Ethernet: 4 Repeater in Serie

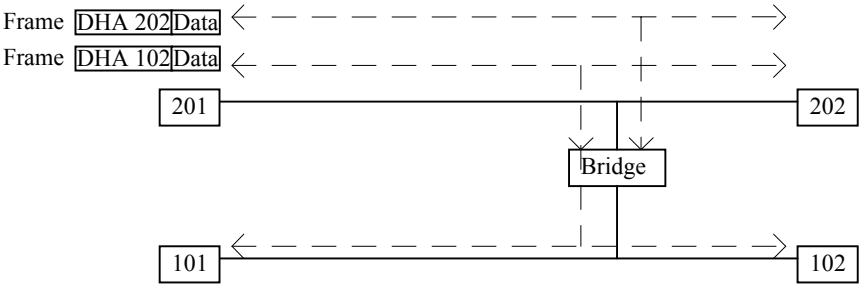
Heute: Concentrator z.B. 10 Base T /100 Base T
Ein Concentrator (Ethernet Hub) kann auch als Multiportrepeater betrachtet werden, auch hier gilt, daß nicht mehr als 4 Ethernet Hubs in Serie geschaltet werden können.



8.2 Bridge / Switch



Aufgabe: Lastverteilung durch Trennung von Stationsadressen



DHA = Destination Hardware Address

Hardwareanforderungen hoch, da jedes Paket gelesen werden muß
Brücke ist gekennzeichnet durch die sog.
- Filtering Rate (Pakete/s die ausgewertet werden)
- Forwarding Rate (Pakete/s die weitergeleitet werden)

durchschnittl. Werte: Filt.R. =12000 Pakete/s
For.R. = 8000 Pakete/s

Verbindung der Netzwerksegmente durch
MAC - Ebene: MAC - Layer - Bridge eine Topologie auf beiden Seiten
(LLC - Ebene:)

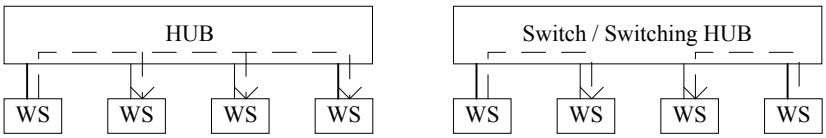
8.2.1 Transparente Brücken (selbstlernende Brücken)

spez. IEEE 802.1 d
Bridge lernt selbstständig durch Lesen von Quelladressen in Paketen und bildet dann interne Tabellen
Möglichkeiten:

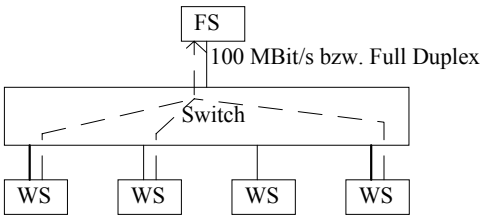
- Zieladresse bekannt:	weiterleiten oder vernichten des Pakets, je nach dem, ob DHA vor oder hinter der Bridge
- Zieladresse nicht bekannt:	weiterleiten und lernen aus der Sourceadresse des Antwortpaketes

Nach Erreichen einer max. Anzahl von Einträgen, löschen dieser nach Alter der Einträge (streichen der am längsten nicht benutzten)

8.2.2 Frame Switching



Punkt zu Punkt Verbindung; jede WS erhält die volle Bandbreite
- Vorhandene Verkabelung Nutzbar

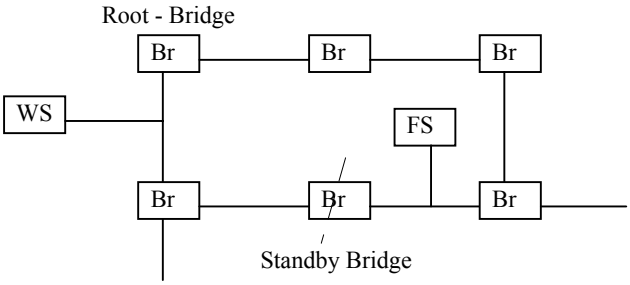


Funktionsweise Layer 2 Switching:
Switching auf Ziel-Hardwareadressen.
Damit kann ein Layer 2 Switch als Äquivalent zu einer Bridge betrachtet werden.
lesen Zieladresse - schalten auf Zielport ohne Zwischenspeicherung (anders als bei einer Bridge, die zum Lesen der Pakete die Pakete zwischenspeichert).

Typische Verzögerungszeiten:
Switch: 20 .. 40 ns
Bridge: 1200 ns
Router: 1600 ns
Kosten: 300 - 1000 DM/Port

8.2.3 Spanning Tree Protocol

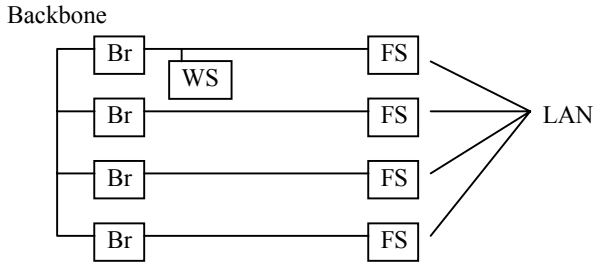
Nutzung mehrer Bridges/Switches im LAN



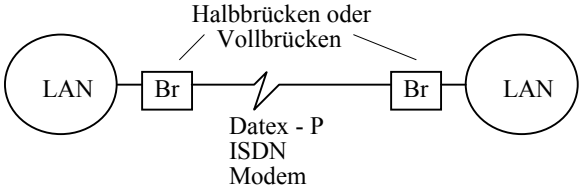
- Root Bridge (Hauptbrücke)
- Standby - Modus einzelnder Brücken

Dynamische Verbindung zwischen allen Stationen
Automatische Rekonfiguration nach Bridgeausfall
Tabellenabgleich über spezielle Pakete → BPDUs (Bridge Protocol Data Units)

Lokale Bridge



Remote Bridge

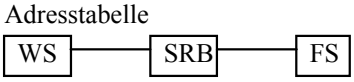


Aufgaben einer Bridge gemäß IEEE 802.1 d
- Untersuchung jedes Pakets auf phys. Empfängeradresse (ggf. Weiterleitung)
- Bildung und Pflege von internen Adresstabellen
- Managementfunktionen (Spanning Tree)

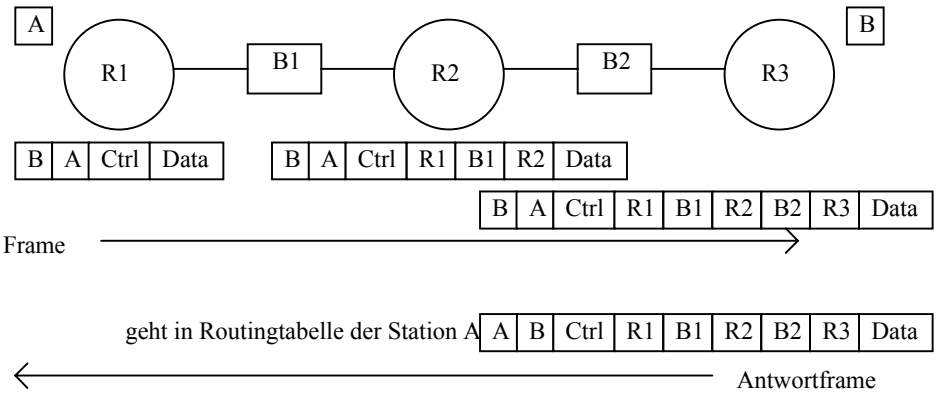
8.2.4 Source Routing Bridge (IBM)

- nicht intelligent
- keine Adresstabellen

Adresstabelle



WS sendet Discovery - Pakete zur Zielstation
durchlaufen gesamtes Netz
jede SRB ergänzt das Datenpaket (hier warst du)
→ ergibt Bridgereihenfolge von Quelle zum Ziel



Problematik:
Mehr Stationen → mehr Discovery - Pakete →mehr Netzlast

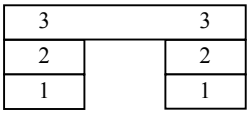
Auch SRBs sind Protokollunabhängig

8.2.5 SRT Bridge

Transparent und Source Routing

8.3 Router
8.3.1 Funktionsweise eines Routers

Wie bereits im vorangegangenen Kapitel gezeigt wurde, läßt sich die Funktionsweise eines Routers nur mit Netzwerkadressen beschreiben, damit wird Routing als generelle Aufgabe an sich der Schicht 3 des OSI Referenzmodells zugewiesen. Dies stellt sich ungefähr wie folgt dar:



Routing setzt also eine logische Trennung von Netzen in Subnetze voraus. Datenpakete werden einem Router zugestellt, dieser hat dann die Aufgabe, die Pakete basierend auf Informationen in seiner Routingtabelle weiterzuleiten.

Wie entstehen nun Routingtabellen? Hier gibt es folgende Möglichkeiten:
- Statisches Routing: Abgleich per Hand
- Dynamisches Routing: Verwendung von Routingprotokollen

Aufgabe von Routingprotokollen:
- Auffinden der besten Route durchs Netz
- Routinginformation verwalten
- gegenseitige Meldungen über Routenänderung
- Anzeigen / Berücksichtigen von Pfadkosten (in lokalere Routerdatenbank)

Routing Protokolle:

RIP I und RIP II (IP)	Routing Information Protocol für IP Umgebungen
R IP (IPX)	Routing Information Protocol für IPX Umgebungen
OSPF (IP, WAN)	Open Shortest Path first
NLSP (WAN)	Netware Link State Protokol
IS - IS	OSI Routing Protokol

Was ist die beste Route?
- Geringste Anzahl von Routern im Pfad
- evtl. WAN - Verbindung berücksichtigen (Zeit / Kosten)

Routertypen
- Ein- / Multiprotokoll - Router
- Multiport - Router

Typische routbare Protokolle:
- TCP/IP, IPX/SPX, OSI, Apple Talk, DECNET

Nicht routbare Protokolle:
- SNA (IBM,LLC), LAT (DEC), NETBIOS

8.3.2 Sonderformen von Routern

Brouter
- Router, der alles was er nicht routen kann, bridged

Switching & Routing
- Layer - 2 Switch: Weiterleitung von Paketen innerhalb eines HUBs
- Routing Layer 3: Weiterleiten in andere Netzwerksegmente

Routing Bridge

Bridge mit zusätzlichen Funktionen z.B. zur Pfadselection, Sicherheitsfunktion

Remote Router ermöglicht Kopplung über WAN´s

Routingprotokolle:
Distance Vector → LAN
Link - State → WAN

Funktionalität von Routern / Remote Routern
- Filtern bestimmte Pakete (log. Adr.) (RIP, SAP) Service Advertising Protocol
- Priority Queuing (Weiterleitung von Information nach Priorität)
- Dial on demand Routing (Physikalischer Verbindungsaufbau nur bei Bedarf)
- Spoofing Vorgaukeln der Verbindung bei connection oriented Protokollen z.B. SPX, obwohl physikalische Verbindung abgebaut ist.
- Dial Backup Backup Konfiguration bei Leitungsaufall (automatisch)
- Netzwerkmanagementunterstützung

8.3.3 Vergleich: Bridge - Router

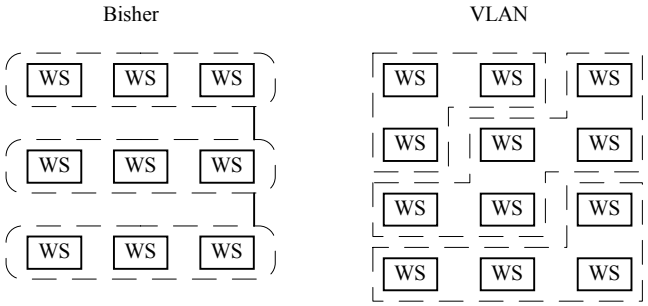
Router	Bridge
begrenzung auf bestimmte Protokolle (Network-Layer) evtl. zusätzliche Bridgefunktion	Protokolltransparenz
Wird aktiv wenn Paket an Router adressiert	ließt jedes Paket
Erkennung fehlerhafter Pakete	Vernichtung fehlerhafter Pakete
Wegwahlfunktion	-
Zusatzfunktion	-
Trennung eines Netzes in log. Subnetze	1 logisches Netz

8.3.4 Layer 3 Switching

Auswerten der NW-Adresse und weiterleiten in ein anderes Teil-NW
Multilayer Switch, Routing Switch

Damit werden aus LANs “virtuelle LANs” (VLAN, VAN)

→ Neue Organisationsform von Netzen
bisher: logische = physikalische Netzstruktur



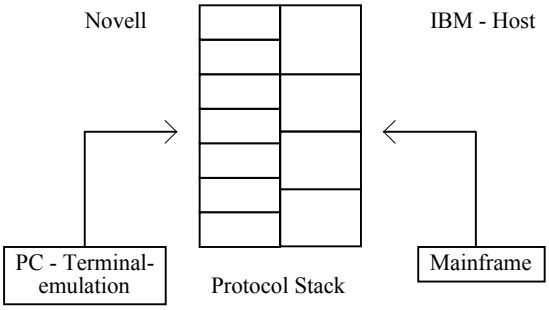
VLAN: Logische Ebene von physikalischer Ebene völlig getrennt. Bisher war die Voraussetzung einer logischen Trennung von Netzen (via Router) zwangsläufig eine physikalische Trennung von Netzen (über eben diese Router). Durch Level-3 Switching können innerhalb eines Switches mehrere log. Netze koexistieren. Damit sind z.B. physikalische Änderungen des Netzes bei Änderung der Arbeitsgruppen innerhalb eines Netzes nicht mehr nötig.

Interner Aufbau z.B. Cisco Routing Switch
1 Prozessor Routing
1 Prozesor Switching Layer 2+3
mehrere I/O Prozessoren
Problematik Level 2 Token Switch:
Token zur Empfangsstation
zwischenspeicherung notwendig

Grundproblematik bei Switchingtechnologie: Unterschiedliche Framelänge der einzelnen Pakete
Antwort auf diese Problematik: --> ATM

8.4 Gateway

Gateways dienen zur Protokollumsetzung zwischen zwei Netzen. Dies kann eine einfache Protokollumsetzung zwischen zwei gleichen Protokollstacks zum Zweck der Zugriffsicherung sein (z.B. eine IP/IP Gateway in einem Firewall), eine Protokollumsetzung bestimmter einzelner Protokolle (z.B. IPX/IP-Gateway) bis hin zu einer Umsetzung eines Protokollstacks (z.B. Umsetzung der Protokolle der OSI-Ebenen 1-5 bei einem Gateway in die IBM SNA-Welt).



Weitere Beispiele sind Protokollgateways, wie z.B. IPX/IP Gateways oder IP/IP Gateways, wie sie z.B. in Firewalls verwendet werden.

9. OSI Transport Layer

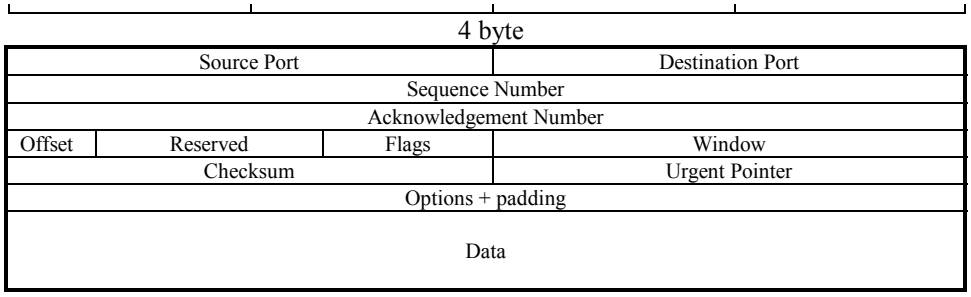
Zum Datentransfer zwischen zwei Rechnern sind grundsätzlich folgende Aufgaben zu lösen:
- Segmentierung von Pakaten
- Steuerung der Übertragungsmenge (Flußkontrolle)
- Senden von Bestätigungen, wenn Pakete empfangen wurden
- Fehlersicherung
- Bereitstellung verschiedener Übertragungskanäle
- Adressierung von Diensten

Findet der Datentransfer nur zwischen zwei Rechnern statt, die direkt im selben Segement des Netzes miteinander verbunden sind, läßt sich ein Teil dieser Aufgaben auch von Protokollen erledigen, die direkt auf ein Zugriffsprotokoll wie Token Ring oder Ethernet aufsetzen, erledigen. Ein Beispiel hierfür ist z.B. das aus dem SDLC hervorgegangene LLC Protokoll.

In einem größeren Netz mit netzwerkweiter Adressierung findet die Lösung dieser Aufgaben allerdings durch eigene Transportprotokolle statt, die man im Allgemeinen der Ebene 4 des OSI Referenzmodells zuordnet.

9.1 Transportprotokolle im Internet

In der Internet Protokollwelt stehen zwei alternative Transportprotokolle zur Verfügung. Eines davon, TCP (Transport Control Protocol) ist verbindungsorientiert (connection oriented), das andere ist das verbindungslose UDP (User Datagramm Protocol).
Aufgaben, die durch TCP realisiert werden, sind:
- Festlegung eines Übertragungsfensters (Window-Feld), um die Übertragungsmenge festzulegen
- Segmentierung und Nummerierung von Paketen (Sequence Number)
- Bestätigungen (Acknowledgement Number)
- Adressierung von Diensten (über Source Port, Destination Port)



Das User Datagram Protocol übernimmt lediglich die Aufgabe der Adressierung der Upper Layer Prozesse. Aufgaben der Flußkontrolle sowie Transportkontrolle müssen dann von den oberen Schichten übernommen werden. Entsprechend einfach sieht der Frame auch aus.

UDP-Frame:

Source Port	Dest Port	Länge	CRC

Beispiele für Upper Layer Protokolle, die auf einem der beiden Transportprotokolle aufsetzen, sind:
UDP: NFS, TFTP, SNMP
TCP: FTP, Telnet, SMTP

9.2 Sockets

Um zu verstehen, wie in der Internet Protokollwelt Verbindungen aufgebaut werden, muß zunächst der Begriff Socket erklärt werden.

Sockets stellen eine Programmierschnittstelle zu TCP bzw. UDP dar (der Begriff und die Implementation kommt aus dem Berkley UNIX). Sockets funktionieren ähnlich wie ein Dateihandling. So liefert eine Funktion zum Öffnen einer Datei als Rückgabewert einen sog. Dateihandle. Weitere Zugriffe auf diese Datei, z.B. zum Schreiben oder Lesen, finden dann über dieses Dateihandle statt. Ähnlich funktioniert der Zugriff auf TCP. Hier ist der Rückgabewert beim Öffnen einer Verbindung ein Socket, über den dann der Datenaustausch über normale Schreib/Lese Funktionen abläuft. Der Socket ergibt sich über die Kombination der IP-Adresse mit einer Port Nummer, also z.B. 192.168.5.31:1677

Eine Verbindung kommt nun wie folgt zustande:
Ein Dienst wartet auf einem Server mit einer bestimmten IP Adresse unter einer bestimmten Port Nummer auf eine Verbindung. Dies wird als ein sogenannter „Listen Socket“ bezeichnet. Der Client Prozeß macht nun Service Anfragen über Aufrufe zu diesem Socket. Dies geschieht wie folgt:

1. Der Client macht einen Request für eine Verbindung (SYN Paket) mit den gewünschten Übertragungsparametern
2. Der Server beantwortet den Request (SYN ACK) und macht nun seinerseits einen Request mit seinerseits gewünschten Parametern
3. Der Client bestätigt den Erhalt des Pakets vom Server und baut dann seinerseits die Verbindung zum Server auf (verwendet wird der kleinste gemeinsame Nenner bezüglich der Übertragungsparameter).

Der ganze Prozeß wird als 3-way-handshake bezeichnet.

9.3 NetWare Transport-Protokolle

NCP (NetWare Core Protocol)
In der NetWare Welt wird für die normale Kommunikation zwischen Client und Server das NCP (NetWare Core Protokoll) verwendet. Dieses Protokoll repräsentiert die Kommunikation zwischen dem Novell File-Server Prozeß und der NetWare Client Shell. Man kann es den Ebenen 4-7 zuordnen. Der Ebene 4 wird es deswegen mit zugeordnet, da es viele Transportprotokoll Aufgaben mit übernimmt.

SPX (Sequenced Packet Exchange)
Für besondere Anwendungen wie z.B. Printing und die Fernsteuerung von Servern steht mit SPX (Sequenced Paket Exchange) ein eigenes verbindungsorientiertes Protokoll zur Verfügung.

10. Internet Diensteprotokolle

Die Internet Protokollwelt ist eine gewachsene Protokollwelt mit Protokollen für verschiedenste Aufgaben. Zunächst standen dabei Protokolle für sehr einfache Aufgaben wie Filetransfer, Terminalemulation und Electronic Mail im Vordergrund, so daß sich die Anforderungen zunächst grundlegend von denen in heutigen LANs unterschieden.

Die Entwicklung begann ca. 1970 mit einer Studie der DARPA (Department of Defense Advanced Research Projects Agency) zur Entwicklung von Protokollen zur Datenkomunikation. Der Schwerpunkt lag dabei auf obigen Anforderungen, erst sehr viel später kamen Protokollezum transparenten Zugriff auf Filesysteme, also eine Umgebung die vergleichbar mit dem Zugriff auf Fileserver in Netzen ist, hinzu.
Die folgende Aufstellung zeigt die Entwicklung:

1972	Beginn Internet Protokollentwicklung
1978	Internet Protokollstack weitgehend vollständig
1980	Verwendung im ARPA-Net (heute noch Teil des Internet)
1982	Verwendung der Internet Protokolle im BSD-Unix
1986	SUN entwickelt NFS (Network Filing System)*

Die Internet Protokollentwicklung und Standardisierung wird von mehreren Organisationen verantwortet:
- Internet Society (ISOC): Besitzt die Zielsetzung, das Internet als globale Kommunikationsplattform zu etablieren.
- Internet Architecture Board (IAB): Technische Organisation der Internetentwicklung. Das IAB ist eine Unterorganisation der ISOC.
- Internet Engineering Task Force (IETF): Standardisierungsgremium, aufgeteilt in neun Bereiche. Die IETF entwickelt Spezifikationen, die später zu Internet Standards werden. Unterorganisation der IAB.
- Internet Research Task Force (IRTF): Langfristige Forschungsprojekte, Unterorganisation der IAB.

Die meisten der Protokolle und Anwendungen sind in sogenannten RFCs (Request for Comment) veröffentlicht. Diese sind im Internet verfügbar, die Pflege der RFCs wirdvom SRI Network Information Center (NIC) in Menlo Park, Kalifornien, übernommen. RFCs werden bei Weiterentwicklungen von Protokollen nicht geändert, sondern es werden neue RFCs erstellt, die den geänderten Stand wiederspiegeln. Insofern findet man sehr häufig mehrere RFCs zu einem bestimmten Thema. Die RFCs sind aufsteigend nummeriert, so daß höhere Nummern neuere Veröffentlichungen widerspiegeln.

Im folgenden eine Aufstellung der wichtigsten Internet Protokolle

Telnet	Terminal Emulation
FTP	File Transfer Protocol
TFTP	Trivial File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
RIP	Routing Information Protocol
ICMP	Internet Control Message Protocol
NFS	Network File System *
XDR	External Data Representation *
RPC	Remote Procedure Call *
IP	Internet Protocol
TCP	Transport Control Protocol
UDP	User Datagram Protocol

Die verschiedenen Diensteprotokolle setzen entweder auf UDP oder TCP auf werden durch bestimmte TCP bzw. UDP ports adressiert. Im folgenden werden die wichtigsten Diensteprotokolle kurz beschrieben.

10.1 Domain Name System (DNS)

Bisher haben wir uns mit netzwerkweiter Adressierung beschäftigt. Allerdings ist unpraktisch, Server oder andere Kommunikationspartner im Netz anhand einer Adresse finden zu müssen, insofern ist es sinnvoll, Rechnern Namen zu geben, um mit ihnen zu kommunizieren.
Hierfür gibt es im wesentlichen zwei Möglichkeiten:
- Führen von lokalen Tabellen, die Namen bestimmten Adressen zuordnen (Host Tabelle)
- Zentralisierung der Adress/Namensauflösung mit Hilfe einer zentralen Datenbank

Letzteres wird durch DNS realisiert. So kann ein zentraler DNS Server von Rechnern befragt werden, unter welcher Adresse ein Rechner mit bestimmtem Namen zu finden ist. Darüberhinausgehend ist DNS ein weltweites System von Rechnern mit Adressinformation, hierbei wird eine Aufteilung des Internets in sog. Domänen vorgenommen. Innerhalb dieser Domänen werden dann die einzelnen Hosts zusammengefaßt. Die Domänenstruktur ist hierarchisch, beginnend von einer [Root] wird ein DNS Baum gebildet. Für jede Domäne sind bestimmte DNS Server verantwortlich,die entsprechenden DNS Server für darunterliegende Domänen werden dann logisch mit den DNS Servern der „höheren“ Domänen verbunden. Auf diese Weise kann die Namensauflösung eines Rechner oder einer Domäne hierarchisch durchgeführt werden.

Wir innerhalb eines Netzes nach einem bestimmten Namen gefragt, versucht zunächst der lokale DNS Server die Namensauflösung. Besitzt er keine entsprechenden Einträge in seiner Datenbank, wird die Namensauflösung zunächst an einen Root Server und dann an jeweils darunterliegende Server weitergeleitet.

10.2 Telnet

Telnet ist ein einfaches Protokoll, um eine Terminalemulation auf einem entfernten Rechner zu realisieren. Im einfachsten Fall wird ein zeilenorientierter Zugriff durchgeführt (VT100/VT200). Übertragen werden im wesentlichen Tastatureingaben und Bildschirmausgaben. Es wird heute hauptsächlich noch im Bereich der Hostkommunikation verwendet, wobei das TN3270 Protokoll (für Mainframezugriff) bzw. TN5250 Protokoll (für IBM As/400 Zugriff) auf Telnet aufsetzen.

10.3 FTP

FTP, das File Transfer Protocol wurde entwickelt um einen Filetransfer zwischen zwei Rechnern, einem FTP Client und einem FTP Server, zu ermöglichen. Zunächst wird eine Verbindung zu einem

entfernten Server aufgebaut, für den Dateitransfer ist dann ein Login nötig, häufig gestatten FTP Server den Datenzugriff über ein „anonymous“ Login.

Für einen FTP Filetransfer werden zwei unterschiedliche Ports verwendet, auf Client Seite Ports über 1023, auf Serverseite ein Command Channel auf Port 21 und ein Data Channel auf Port 20. Der Aufbau des Command Channels erfolgt beim klassischen FTP Zugriff von der Clientseite aus, der des Datenkanals von der Serverseite aus. Dies stellt speziell Internet Firewalls vor Probleme (siehe dort).

Ein FTP Zugriff ist allerdings nicht nur über einen speziellen FTP Client möglich, er kann auch aus einem Internet Browser wie z.B. Netscape erfolgen. Allerdings wird hier häufig sog. Passive Mode FTP verwendet. Hier werden beide Übertragungskanäle nur von Clientseite aus aufgebaut.

10.4 HTTP

Http (Hypertext Transfer Protocol) wird verwendet um im WWW (World Wide Web oder einfach Web) auf Information zuzugreifen. WWW integriert viele der anderen Internet Dienste und ermöglicht den Zugriff auf Information über ein einziges Benutzerinterface, des sog. Internet Browser. In diesem kann auf WWW Server genauso zugegriffen werden wie auf FTP Server, News Server, oder andere. Auf WWW Servern wird die Information in Form von HTML Seiten dargestellt. HTML (HyperText Markup Language) ist ein Datenformat, das über Schlüsselwörter (Links) auf andere Seiten im World Wide Web verweist und damit eine Verknüpfung von Information ermöglicht. Die Adressierung der entsprechenden Web Standorte erfolgt über sogenannte URLs (Uniform Resource Locator), deren Grundlage wiederum DNS ist. So wird eine typische Adresse z.B. wie folgt angegeben:
http://www.e-technik.fh-muenchen.de

Es hat sich sehr weitgehend eingebürgert, die Web Server mit www zu kennzeichnen, allerdings ist dies kein muß, der Name kann völlig beliebig gewählt werden.

Die Seiten können Text in HTML format enthalten, zusätzlich können jedoch Graphiken und Programme als CGI oder Java Applets integriert sein.

10.5 SMTP

SMTP ist das Simple Mail Transfer Protocol. Hier können Nachrichten (Mails) von einer Station zur anderen geschickt werden. Dabei werden sogenannte Mailserver definiert, auf denen die Mails für die Benutzer gespeichert werden und dann von einem zum nächsten Mailserver weitergeleitet werden. Damit liegt SMTP ein sog. Store and Forward Mechanismus zugrunde.

10.6 Usenet News (NNTP)

NNTP (Network News Transfer Protocol) wird für spezielle News Server (Usenet) verwendet. News ist ein Kommunikationsmedium zum Austausch öffentlicher Information mit weltweit etwa 4000 Themenbereichen (News Gruppen). Die Beiträge können von allen Benutzern gelesen werden, in den

meisten Newsgruppen kann man auch eigene Artikel plazieren. Auch bei den Newsgruppen gibt es einen hierarchischen Aufbau. Man kann bestimmte Newsgruppen zu verschiedensten Themen „abonnieren“, d.h. man erhält regelmäßig neueste Informationen zu bestimmten Themen.

10.7 NFS

NFS, das Network File System wurde Anfang der achtziger Jahre von SUN entwickelt. Es ermöglicht das Einbinden von Dateisystemen fremder Server in den Dateibaum eines Clients, um auf diese Daten genauso zugreifen zu können, wie auf eigene.

10.8 Verwendete Ports

Die für die verschiedenen Dienste verwendeten Ports für den jeweiligen Service Prozeß sind in folgender Tabelle zusammengestellt. Die ports zwischen 0 und 1023 werden teilweise auch als sog. Trusted Ports oder privilegierte Ports bezeichnet, bei Zugriff innerhalb eines UNIX Systems benötigt man zum Öffnen dieser Ports eine sog. Root Berechtigung. Die Zuordnung der Dienste zu den jeweiligen Ports ist eine Konvention aus dem UNIX Bereich, RFC 1700 zeigt eine Liste reservierter Ports.
Clientseitig werden i.A. Adressen oberhalb 1023 verwendet. Eine Ausnahme stellt hier DNS dar, hier wird für die Kommunikation zwischen zwei DNS Servern Port 53 verwendet.

Diensteprotokoll	TCP Server Port
DNS	53
Telnet	23
FTP	Data Channel: 20 Command Channel: 21
SMTP	25 (Receiver)
POP 3	110
NNTP	119
HTTP	80

Auch im UDP Protokoll gibt es Ports, die von TCP Ports völlig unabhängig sind. D.h., bei gleichzeitigem Einsatz beider Protokolle TCP und UDP können durchaus gleiche Portnummern beider Protokolle unterschiedliche Dienste adressieren.

11. Firewalls und Netzwerksicherheit

Gerade beim Anschluß ans Internet müssen Schutzmechanismen gegen unbefugtes Eindringen in ein firmeninternes Netz von außen vorgesehen werden. Grundsätzlich gibt es hier zwei Möglichkeiten:
- Sichern jedes firmeninternen Rechners (der Aufwand steigt natürlich mit der Zahl der Rechner, so daß dies kaum mehr sinnvoll realisierbar ist.
- Zentralisierung der Sicherheitsproblematik eines Netzzugriffs von außen auf einen einzigen Punkt. Dieser Punkt wird dann speziell abgesichert (sog. Firewall)

11.1 Angriffsmöglichkeiten

Die folgende Liste zeigt eine (nicht vollständige) Auswahl an Angriffsmöglichkeiten für Netze:
- Ausspionieren von Daten auf Systemen durch Einbruch in diese Systeme
- Ausspionieren bei der Übertragung zwischen Systemen (Mitlesen)
- Manipulation von Daten auf Systemen (z.B. durch Hacken, Viren, Java Applets, Active X Controls), im Prinzip werden hier Programme durch irgendeinen Mechanismus auf einen Client übertragen und dort ausgeführt.
- Manipulation von Verbindungen (Übernehmen einer Verbindung mit Hilfe gefälschter Adressen)
- Verhindern der normalen Funktion eines Rechners (Denial of Service Attack). Beispiele hierfür sind: Ping of Death oder Syn Flooding

Was sind Möglichkeiten, die ein Hacker nutzen kann, um in ein Netzwerk einzubrechen:
- Paßwortattacken (Hacken)
- Social Engineering
- Fehler und Hintertüren in Programmen oder Protokollen
- Informationslecks in Firmen
- Versagen der Authentisierungsmechanismen

11.2 Funktion und Komponenten von Firewalls

11.2.1 Paketfilter

Eine sehr einfache Möglichkeit ist, Kommunikationsbeziehungen zu filtern. Hier können ICMP, IP, UDP bzw TCP Filter implementiert werden. Damit ist diese Firewall lediglich ein Router, der abhängig von bestimmten Adressen routen kann.

IP Filter: Hier werden im wesentlichen Absender und Ziel-IP-Adressen gefiltert. Die Firewall routet dann nur Pakete von und zu bestimmten Ziel bzw. Quelladressen.

Hierzu wird im Router/Firewall eine Adressliste mit diesen Adressen geführt. Es gibt bei den meisten Produkten die Möglichkeit, entweder aufzuführen, zu welchen Adressen Kommunikationsbeziehungen erlaubt sind (Pass List) oder verboten sind (No-Pass List). Normalerweise ist die gängige Vorgehensweise, daß zunächst jeder Paketverkehr über die Firewall verboten wird, und dann notwendige Ausnahmen von dieser Grundregel gemacht werden.

Die meisten Paketfilter sind nicht nur in der Lage, nach IP-Adressen zu filtern, sondern dies auch noch abhängig von Quell und Zielports durchzuführen. Problematisch ist der Einsatz speziell von Port-Filtern dann, wenn Protokolle mit mehreren logischen Verbindungen wie z.B. FTP, bestimmte Protokolle im Multimediabereich gefiltert werden sollen. So müssen z.B. für FTP Übertragungen ganze Bereiche möglicher Portnummern geöffnet werden, um Kommunikation zu ermöglichen. Diese Ports sind dann natürlich wieder als Angriffspunkte offen.

Man unterscheidet statische und dynamische Paketfilterung. Bei dynamischen Paketfiltern wird der Status jeder Verbindung mit in einer Tabelle gespeichert, die dann Grundlage zur Filterung ist. Antwortpakete, die zu bestimmten ausgehenden Verbindungen gehören, werden durchgelassen, auch wenn entsprechende Filterregeln das für andere eingehende Pakete verhindern würden. Die Filterregeln werden dabei dyamisch angepaßt, was die Konfiguration solcher Problemstellungen erheblich erleichtert. Diese Art der Paketfilterung wird häufig als Stateful Inspection oder Stateful Filtering bezeichnet. Sie wird vor allem für Protokolle eingesetzt, die mehrere Verbindungen benötigen (z.B. FTP) .

11.2.2 IP Adressumsetzung (NAT)

Hier werden den Rechnern innerhalb eines Intranets inoffizielle Adressen gegeben, diese werden dann bei Kommunikation ins Internet dynamisch auf die gültige Adresse des Routers/Firewalls gesetzt. Aus dem Internet betrachtet beginnt und endet damit jede Kommunikation mit dem Router, der Router selbst sorgt dann für die „Verlängerung“ der Verbindung zum jeweiligen Client im Netz.
Als inoffizielle Adressen können natürlich beliebige Adressen gewählt werden, es empfiehlt sich jedoch aus Sicherheitsgründen einen der reservierten Adressbereiche zu verwenden.

Als reservierte Adressbereiche stehen folgende Adressen zur Verfügung:

192.168.0.0	...	192.168.255.255
172.16.0.0	...	172.31.255.255
10.0.0.0	...	10.255.255.255

Man unterscheidet statisches und dynamisches NAT:

Dynamisches NAT
Beim dynamischen NAT werden private Adressen eines ganzen Subnetzes in eine offizielle Adresse umgesetzt (dies ist die öffentliche Seite des NAT Routers, d.h., die Seite, von der aus die Verbindung ins Internet besteht.
Der Vorteil ist, daß für Kommunikationsbeziehungen, die aus dem Intranet heraus gestartet werden, die ursprüngliche Quelladresse einer Station im Internet nicht sichtbar wird. Aus der Sicht des Clients ist die Verbindung transparent ins Internet, d.h. dem Client ist die Adreßumsetzung nicht bewußt, er denkt, er hängt direkt am Internet. Ob die internen Rechner von außen erreichbar sind, wenn die internen Adressen außen bekannt sind, ist abhängig von der Konfiguration der jeweiligen Firewall.

Statisches NAT
Statisches NAT kann dazu verwendet werden, einzelne interne Rechner mit bestimmten internen IP-Adressen, auf entsprechende offizielle IP Adressen der Firewall umzusetzen. Hier erhält jeder intere

Rechner eine entsprechende offizielle Adresse auf der öffentlichen Seite des NAT Routers. Damit ist der interne Rechner aus dem Internet über diese offizielle IP-Adresse erreichbar.

Wird statisches und dynamisches NAT parallel eingesetzt, muß die Firewall auf der öffentlichen Seite mehrere IP Adressen parallel erhalten (Multihoming), eine für die dynamische Komponente und je eine für jede statische Verbindung ins interne Netz.

Einen absoluten Schutz vor dem Eindringen von außen bietet diese Lösung nicht. Sind die im internen Netz verwendeten Adressen im außen bekannt, könnten Sie auch erreicht werden (zumindest wenn es sich nicht um die oben angegebenen Adressen aus den privaten Adressbereichen handelt, die im Internet nicht geroutet werden). Aus diesem Grunde sollte durch entsprechende Filterung der Routingprotokolle zusätzlich dafür gesorgt werden, daß der NAT Router die Routing Information über die internen Netze nicht nach außen weitergibt.

11.2.3 TCP/UDP Relay

Hier findet auf der Ebene 4 eine Portumsetzung innerhalb von Kommunikationsbeziehungen statt. Das Gateway wartet auf einem vordefinierten Port auf eine Verbindung, diese wird dann über einen anderen Port weitergeleitet.

Logisch wird dadurch eine Verbindung zwischen Client und Firewall und davon getrennt eine zweite Verbindung von der Firewall zum entsprechenden Host im Internet aufgebaut.

Da hier kein Routing verwendet wird, das IP-Paket also nicht weitergeleitet wird sondern tatsächlich neu aufgebaut wird, spricht man in diesem Zusammenhang auch von einem sogenannten Dual Homed Gateway, also einem Gateway mit zwei physikalisch getrennten Netzwerkverbindungen.

Die Anwendung dieser Gateways ist durch die feste Zuordnung von Zielsystemen mit bestimmten Zielports begrenzt. Dies kann z.B. bei Nutzung verschiedener Server problematisch werden, die denselben Dienst über unterschiedliche Ports anbieten.

Ähnlich funktionieren auch Protokollumsetzer wie IP/IP Gateways oder auch IPX/IP Gateways. Letztere wickeln dann eben die Verbindung innerhalb des Intranets bis zum Gateway über Novell's IPX Protokoll ab.

11.2.4 Application Layer Gateway (Proxy)

Hier findet eine vollständige Trennung der Kommunikation innerhalb eines Intranets mit dem Internet statt. Die Firewall wird ist damit ein Dual Homed Gateway mit einer Überwachung der Verbindungen auf der Applikationsschicht. Dies wird im allgemeinen mit einer IP Adreßumsetzung (NAT) kombiniert (s.o.).

Möchte ein Benutzer z.B. eine bestimmte Seite auf einem WWW Server im Internet lesen, wird zum Proxy Server eine Verbindung aufgebaut. Der Proxyserver baut nun seinerseits anstelle des Clients die Verbindung zur gewünschten Web Site auf und liest sie. Von dort wird sie dann dem Client zur Verfügung gestellt.
Der Proxy Server besitzt einen Cache der für manche Diensteprotokolle die am häufigsten gelesenen Seiten zwischenspeichert. Bei einem erneuten Zugriff kann dann die Nachfrage direkt aus dem Cache befriedigt werden. (z.B. HTTP Proxy Cache).

Protokolle, für die häufig Proxy Server eingesetzt werden, sind:
- HTTP
- SMTP
- FTP
- NNTP

Die Firewall muß natürlich die entsprechenden Protokolle verstehen, um protokollspezifisch eingreifen zu können. Dies erhöht zunächst den Aufwand solcher Gateways ganz gewaltig. Zudem besteht hier das Risiko, daß Angriffe, die das Gateway nicht selbst betreffen, auch nicht mitprotokoliert werden können.

Proxy Server können auf verschiedene Weisen eingesetzt werden:

Proxy Cache

Dies ist die Standardkonfiguration

Hierarchischer Proxy Cache

Hier werden mehrere Proxy Server zu einer Hierarchie zusammengestellt, daß heißt, wenn ein Proxy Server eine Seite benötigt, holt er Sie wiederum aus einem übergeordneten Cache. Zur Kommunikation der Caches unterienander wird hierbei das Internet Cache Protokoll (ICP) eingesetzt.

Transparent Proxy

Auf Client Seite (im Netscape oder In ternet Explorer muß normalerweise eingestellt werden, daß ein Proxy verwendet wird). Ein Transparenter Proxy steuert dies automatisch (transparent für den Benutzer)

Revers Proxy (Web Accelerator)

Der wesentliche Aspekt ist bei Proxy und Proxy Cache Servern natürlich die Performance des entsprechenden Servers, des verwendeten Betriebssystems sowie des Proxy Servers selbst. So gibt es inzwischen allerdings so schnelle Proxy Server (z.B. Novell Bordermanager), die als Web Accelerator dienen können. Hier wird einem Webserver, auf dem aus dem Internet viele Anfragen eintreffen, einfach ein Web Accelerator vorgeschaltet, der die am häufigsten gewünschten Seiten aus dem Cache ohne der Notwendigkeit des Plattenzugriffs liefern kann.

11.3 Firewallarchitekturen

Grundsätzlich ist es möglich Firewalls als fertige Produkte zu kaufen, oder aber sie selbst mit Hilfe von Standardhardware und Firewall-Softwarekomponenten selbst aufzubauen. Hierbei gibt es verschiedene Möglichkeiten, wie eine Anordnung von Komponenten zu einer Firewall erfolgen kann.

Grundsätzlich muß beim Aufbau einer Firewall bedacht werden daß sich folgende drei Komponenten in etwa die Waage halten müssen:
- Aufwand
- Kontrolle
- Performance

Grundsatz ist: *Die sicherste Firewall ist die, die keinen Verkehr mit der Außenwelt zuläßt!*

Im folgenden werden die gängigsten Konzepte kurz vorgestellt:

Dual Homed Host

Screened Host Architektur

Screened Subnet Architektur

Aufgaben:
Ext: Verhindern von Adressfälschungen
DMZ: Hier würde eine Paketüberwachung (Snooping, Herumschnüffeln) nur Informationen von und zum Bastion Host liefern, aber keine Information über das interne Netz
Int. Dieser Router hat die Aufgabe , das Intranet vor der DMZ und vorm Internet zu schützen

Problematik: Mehrere Router liefern natürlich auch mehrere Angriffspunkte

Im folgenden werden einige Variationen gegenübergestellt:

Wie können jetzt die gängisten Protokolle am besten gefiltert werden:

DNS:
DNS benötigt Port 53 für die Kommunikation mit anderen DNS Servern, hier ist ein Portfilter einsetzbar. Allerdings muß hier unterschieden werden, ob ein DNS Request eines Clients oder eines Servers erfolgt.

Telnet:
Telnet ist ein sehr einfaches Protokoll, innerhalb einer Telnetverbindung werden z.B. Paßwörter unverschlüsselt übertragen. Eingehende Telnetsessions sollte man über IP-und Portfilterung soweit wie möglich beschränken, zusätzlich sollten nur einmal benutzbare Paßwörter verwendet werden. Ausgehende Telnet Sessions sollten über Paketfilter und/oder Proxy Server abgewickelt werden

FTP:
Bei klassischem FTP kann eigentlich fast nur ein Proxy Server verwendet werden, bei passive Mode FTP ist ein einfacher Paketfilter ausreichend, wobei hier auch wieder der gesamte eingehende Datenverkehr über einen Gesicherten Host zu übertragen sind.

HTTP:
Für ausgehendes HTTP empfielt sich der Einsatz von Proxy Servern. Problemtisch ist dann aber die Verwendung dynamischer HTML Seiten und CGI Scripts. Zudem werden Informationen wie auch Paßworte unverschlüsselt übertragen. Abhilfe bietet hier das SSL (Secure Socket Layer) Protokoll. Für eingehendes HTTP empfiehlt sich eine genaue Zugriffsüberwachung sowie der Einsatz spezieller Programme zum Upload auf einen internen Server, wenn dies überhaupt notwendig ist.

SMTP/NNTP:
SMTP ist als Store and Forward Protokoll sehr gut für den Einsatz eines Proxy Servers geeigent. Zudem ist es sinnvoll alle Verbindungen per Paketfolter auf einen bestimmten Bastion Host zu lenken. Ähnliches gilt für NNTP.

11.4 Sicherheit von Netzen

Grundsätzlich sind Firewalls nur eine Möglichkeit, Netze zu sichern. Diese ist auch nur für Angriffe aus dem Internet erfolgreich. Aus diesem Grund gibt es Firmen, die auch zwischen Abteilungen Firewalls einsetzen.

Zudem müssen neben Firewalls aber auch andere Mechanismen zum Schutz vorhanden sein. Folgende Mechanismen geben eine Übersicht:

- Physikalischer Zugriffsschutz auf bestimmte Rechner (insbesondere Server)
- Geheimhaltung, Integrität und Verfügbarkeit
- Identifikation und Beglaubigung
- Überwachung des Netzes auf Eindringlinge
- Maßnahmen zur Geheimhaltung von Paßworten (physikalisch und elektronisch)
- Verwenden von Verschlüsselung (Beim Netzzugriff und bei der Informationsübertragung durch ungesicherte Netze)
- Überwachung der Netzwerkaktivität (Auditing)
- Zugriffskontrolle auf Ressourcen

Die gesicherte Übertragung von Information wird mit der zunehmenden Nutzung des Internets immer wichtiger. Anwendungen sind z.B. ein Aufbau von gesicherten verschlüsselten Kanälen durch das Internet zwischen verschiedenen Standorten einer Firma (Virtual Private Networks VPN) oder auch die Identifikation von Benutzern im Internet für Anwendungen wie Electronic Banking oder E-Commerce. Man unterscheidet im Allgemeinen folgende Anwendungsgebiete bei der Herstellung einer gewissen Netzwerksicherheit:

- Verschlüsselung von Nachrichten
- Identification (elektronische Signatur): Hier wird durch Übertragung von bestimmten Prüfsummen bewiesen, daß eine Nachricht von einem bestimmten Benutzer kommt
- Authentication (Beglaubigung): Hier sendet eine Benutzer private Information, die beweist, daß er der ist, für den er sich ausgibt.

11.5 Verschlüsselung

Es gibt bei der Verschlüsselung zwei grundsätzlich unterschiedliche Ansätze:

- symmetrische Verschlüsselung (Secret Key Encryption) und
- asymmetrische Verschlüsselung (Public Key Encryption).

11.5.1 Symmetrische Verschlüsselung

Das wesentliche Kennzeichen ist, daß zum Verschlüsseln wie zum Entschlüsseln derselbe Schlüssel verwendet wird. Dieser muß vor einer Kommunikationsbeziehung zwischen beiden Kommunikationspartnern über einen getrennten Übertragungskanal ausgetauscht werden.

Zur Verschlüsselung gibt es u.A. folgende Verfahren:

- Verschiebung von Alphabeten
- Ersatz von Zeichen (Substitution)
- Vertauschen von Bits (Permutation)
- Algebraische Methoden

Eines der bekanntesten Verfahren ist der DES Algorithmus (Data Encryption Standard), der bei der ISO als DEA-1 bezeichnet wird. Hier wird ein Text in Blöcke von 64bit-Binärworten eingeteilt und blockweise mit einem 56 byte Schlüssel verschlüsselt. Dazu wird auf den Klartext 16mal eine Kombination von Substitution und Permutation angewandt.

Der Algorithmus wurde später weiterentwickelt zu 3-fach DES, hier wird mit zwei Schlüsseln gearbeitet. Der Test wird mit Schlüssel 1 verschlüsselt, mit Schlüssel 2 entschlüsselt und wieder mit Schlüssel 1 verschlüsselt.

RC2 und RC4 sind Verschlüsselungsalgorithmen mit variabler Schlüssellänge. Die Algorithmen sind in einer Reihe kommerzieller Produkte verfügbar (Netscape, Novell Netware, Lotus Oracle ...). Die Verschlüsselungsgeschwindigkeit hängt nicht von der Schlüssellänge ab. Üblicherweise wird eine Schlüssellänge von 128bit verwendet, für den Export wird die Schlüssellänge auf 40bit beschränkt. Damit sind nur noch 2^{40} (=ca $1*10^{12}$) verschiedene Schlüssel realisierbar.

Ein weiteres bekanntes Verfahren ist der 1990 entwickelte IDEA Algorithmus. Mit einer Schlüssellänge von 128bit werden Blocks von 64bit Länge verschlüsselt. Hierbei wird durch bitweises Exclusiv oder, durch Addition mod 2^{16} (65536) sowie Multiplikation modulo $2^{16}+1$ (65537) ein verschlüsselter Text erzeugt. IDEA gilt als sicherer als DES oder sogar 3-fach DES.

11.5.2 Asymmetrische Verschlüsselung

Hier werden jeweils zwei Schlüssel berechnet, ein sogenannter Public Key und ein sogenannter Private Key. Beide Schlüssel stehen in einem komplexen mathematischen Zusammenhang. Zur Verschlüsselung von Nachrichten wird der Public Key verwendet, zum Entschlüsseln ein Private Key, der nur dem Empfänger bekannt ist. Dabei kann der Public Key jedermann bekannt sein. Solange der Private Key geheimgehalten wird, ist die Verschlüsselung sicher.

Im wesentlichen basieren diese Berechnungen auf Verwendung von Methoden der Restklassenalgebra. Dadurch sind die Verschlüsselungsalgorithmen wesentlich langsamer als symmetrische Verschlüsselungsverfahren, dies wird heute durch die ständig steigende Rechenleistung von Computersystemen aufgefangen. Eines der bekanntesten asymmetrischen Verfahren ist die sog. RSA (Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman) Public Key Encryption. Ein anderes Verfahren ist DSA (Digital Signature Algorithm). Während RSA universell einsetzbar ist, ist DSA nur für digitale Signaturen einsetzbar.

Es gibt zwei wesentliche Anwendungen:

- Verschlüsselung: Hier wird eine Nachricht mit einem public key verschlüsselt, sie kann dann mit Hilfe eines nur dem Empfänger bekannten private keys nur von diesem Empfänger gelesen werden.
- Elektronische Signatur (z.B. in Mailsystemen): Hier kann eine Nachricht mit Hilfe eines nur dem Sender bekannten private keys signieren. Jeder mögliche Empfänger kann dann mit Hilfe des Public Keys überprüfen, ob die Nachricht auch wirklich authentisch ist, d.h. ob sie wirklich vom angegebenen Sender stammt.

In einer bestehenden Verbindung können auch beide Verfahren gleichzeitig zur Anwendung kommen, dann benötigen Sender und Empfänger zwei entsprechende Schlüsselpaare.

Basis für die Berechnung von Schlüsseln sind möglichst große Primzahlen (100 bis über 200 bits) , wobei das Produkt dieser Primzahlen Teil der Schlüssel ist. Es wird vorausgesetzt, daß es genauso schwierig ist, einen mit einem Public Key verschlüsselten Text mit demselben Schlüssel wieder zu entschlüsseln, wie die Zerlegung des Produkts zweier Primzahlen zu finden.

Im folgenden wird gezeigt, wie man prinzipiell die Schlüssel berechnen kann:

Beispiel: Primzahlen p=13 und q=19,
Damit ergibt sich das Produkt n =p*q zu 247.
Zur Findung des public keys wird noch die Funktion s=(p-1)*(q-1) benötigt, hier ergibt sich s zu 216.

Nun wählt man einen public key (e,n) so, daß e und s keinen anderen gemeinsamen Teiler besitzen als die Zahl 1. Hier könnte z.B. e=5 zufällig gewählt werden (üblich sind 3, 17 oder 65537 $=2^{16}+1$).
Der public key ist in diesem Beispiel damit (5,247).

Ein private key (d,n) wird nun so gewählt, daß der Rest der ganzzahligen Division von d*e/s 1 ergibt. Hier kann z.B. d=173 gewählt werden. Damit ist der private key (173,247).

Sind die Schlüssel generiert, werden p und q vernichtet

Verschlüsselt wird nun die Nachricht im Klartext: „12“

Verschlüsselung:
$12^5/247=248832/247=1007$ Rest 103, damit ist „103“ nun der verschlüsselte Text

Entschlüsselung:
$103^{173}/247=1{,}663*10^{349}/247$ =xxxx Rest 12, damit ist der entschlüsselte Text „12“

11.5.3 Digitale Signaturen

Zur Verwendung für Signaturen besteht das Problem, daß ein großer Aufwand getrieben wird, wenn die gesamte Nachricht verschlüsselt werden muß. Abhilfe schafft die Verwendung sogenannter Einweg-Prüfsummen (oder Message Digests bzw. One Way Hash-Funktionen) h=H(M), wobei M die Nachricht ist (M für Message).

Ein solcher Message Digest besitzt (unabhängig vom Umfang der zu sichernden Nachricht) eine feste Länge m (wie z.B. 64 oder 128 bit, das National Institute of Standards and Technology NIST empfiehlt 160 bit für Hashfunktionen). Damit werden die Verschlüsselungs- und Entschlüsselungszeiten gegenüber der Zeit zur Verschlüsselung der ganzen Nachricht erheblich verkürzt.

Um fälschungssichere Nachrichten zu senden, muß ein Message Digest so generiert werden, daß folgende Eigenschaften erfüllt sind:
- Mit vorgegebenem M kann man h leicht berechnen
- Mit vorgegebenem h kann man M kaum berechnen
- Mit gegebenem M kann man kaum einen andere Nachricht N mit Message Digest H(N) = H(M) finden.

Sehr oft ist auch noch eine weitere Eigenschaft, die sogenannte Kollisionsresistenz erforderlich:
- Es ist schwierig, zwei beliebige Nachrichten M und N zu finden mit H(M)=H(N)

Der entsprechende Message Digest identifiziert damit eindeutig eine bestimmte Nachricht, er liefert sozusagen einen eindeutigen Fingerabdruck.

Das folgende Beispiel zeigt, was geschieht, wenn die Kollisionsresistenz nicht erfüllt ist:
- Cäsar bereitet zwei Versionen eines Vertrags vor. Eine begünstigt Vertingetorix, die andere benachteiligt ihn.
- Cäsar bringt an jedem Dokument einige kleine Änderungen an und berechnet für jede Version den Hashwert. Nehmen wir an, er erzeugt so 2^{32} Dokumente.

- Er vergleicht danach die Hashwerte aller Versionen der beiden Dokumente und sucht übereinstimmende Paare. Er rekonstruiert die beiden Dokumente, die denselben Hashwert liefern.
- Cäsar läßt Vertingetorix die Vertragsversion unterzeichnen, die ihn begünstigt. Er benutzt dabei aber ein Protokoll, bei dem nur der Hashwert unterzeichnet wird.
- Später ersetzt Cäsar den von Vertingetorix unterschriebenen Vertrag durch die Version mit dem gleichen Hashwert, die Vertigetorix nicht unterschrieben hat und das Schlamassel ist perfekt.

Es gibt verschiedene Einweg Hashfunktionen. Die bekanntesten sind:
- Snefru (128 bzw. 256 bit)
- N-Hash (128 bit)
- MD2, MD4 und MD5 (MD steht für Message Digest) (128bit)
- SHA (Secure Hash Algorithm) (160bit)

Digitale Signatur und Public Key Verfahren werden häufig kombiniert und gewährleisten damit Sicherheit und Authentizität.

11.6 Beglaubigung (Authentication)

Verschlüsselung kann eine sichere Übertragung von Information gewährleisten. Was allerdings vorausgesetzt werden muß, ist, daß die beiden Kommunikationspartner auch die richtigen sind. Dies sicherzustellen, kann natürlich auf einem separaten Weg erfolgen, schwierig wird das Unterfangen allerdings, wenn zunächst eine Verbindung zu einem Kommunikationspartner aufgebaut werden soll, und in derselben Session eine gesicherte Verbindung hergestellt werden soll. So ist z.B. beim Einloggen in EDV-Systeme aber auch im Bereich des E-Commerce ist eine einwandfreie Identifikation eines Nutzers des Systems bzw. eines Kunden erforderlich. Hierzu werden häufig symmetrische und asymmetrische Verschlüsselung kombiniert.
Um diese Identifikation sicherzustellen, kann zunächst eine Beglaubigung erfolgen. Hier gibt es grundsätzlich mehrere Möglichkeiten:
- Eingabe eines geheimen Passworts (Hier kann ein System überprüfen, ob ein Nutzer das richtige Passwort hat)
- Überprüfung ob ein eingegebenes Passwort gültig ist (durch Anwendung einer Einweg-Hash-Funktionen auf das Paßwort und Vergleich dieser Funktion mit dem früher gespeichertem Wert)

Bei der zweiten Möglichkeit sind die Paßworte selbst nicht mehr im System gespeichert, dies erhöht die Sicherheit. Allerdings ist auch eine Datei mit Hash-Funktionen von Paßwörtern durch Vergleiche mit einer zweiten Datei mit Hashfunktionen gängiger Paßworte zu knacken. (z.B. über Angriff mit einem Wörterbuch).

Dies läßt sich durch Anwendung von Zufallssequenzen (Salt), die auf die Paßworte angewandt werden, bevor die Hashfunktion gebildet wird, erschweren, wenn auch nicht verhindern. Zusätzlich zu den Hash-Funktionen werden dann die Salt-Werte in der Datenbank gespeichert.

Beispiel: User Login bei Novell Netware
Zunächst hat der Server folgende Information über den Benutzer gespeichert:
- User Name
- Eine Userspezifische Zufallszahl (Salt)
- Eine Hash Funktion (Message Digest) HSP=H1(Salt,Passwort)
- Public RSA Key des Users
- Private Key in verschlüsselter Form (verschlüsselt mit Hash Funktion HSP)

Die Authentisierung läuft nun in folgenden Schritten ab:

<u>Erstellen der Verbindung:</u>
Schritt 1: Der User verbindet sich mit dem Server
Schritt 2: Server überprüft, ob der User in der NDS existiert

Beginn des Logins:
Schritt 3: Server sendet den userspezifischen Salt Wert und eine allg. Zufallszahl (R1) (Nachricht A, Rätsel)
Berechnungen am Client:
Schritt 4: Client berechnet eine Hashfunktion HSP=H1(Salt,Passwort) selbst da diese nicht vom Server gesendet wird
Schritt 5: Client berechnet eine Zahl Y durch Verschlüsselung der Zufallszahl R1 mit HSP als Schlüssel (RC2 Verschlüsselung)
Schritt 6: Client erzeugt eine Zufallszahl R2 und einen Block von Zufallsdaten S
Schritt 7: Client erfragt den Public Key des Servers
Beenden des Logins:
Schritt 8: Verschlüsselung von R2, S, Y mit dem Public Key des Servers und Übertragung zum Server (Nachricht B, des Rätsels Lösung)
Schritt 9: Server entschlüsselt Y aus der ihm vorliegenden Hashfunktion HSP und Zufallszahl R1
Schritt 10: Server berechnet ebenfalls H2(HSP,R1) und vergleicht den Wert mit Y → entspricht Passwortcheck
Schritt 11: Server verschlüsselt R2, den Private Key des Users und S mit Y als Schlüssel und sendet diese Nachricht zum Client (Nachricht C, Bestätigung des Zugriffs)

Client erhält Private Key vom Server:
Schritt 12: Client entschlüsselt die Nachricht und erhält den Private Key des Benutzers, dazu muß HSP von vorher verwendet werden
Schritt 13: Client checkt über R2, das die Nachricht vom richtigen Server kam, nur der konnte R2 aus der Nachricht B entschlüsseln

Durch diese Kombination aus symmetrischer und asymmetrischer Verschlüsselung wird nachgeprüft, ob der Benutzer das richtige Passwort besitzt ohne daß das Passwort wirklich über die Leitung geschickt wird.

An weiteren Verfahren der Beglaubigung wie Smart Cards oder biometrische Verfahren (Fingerabdruck, Augenscan, usw.) wird gearbeitet.

11.7 Schlüsseltausch

Es wurde bisher gezeigt, daß asymmetrische Verschlüsselung auf einen sicheren Übertragungskanal zum Austausch von Schlüsseln verzichten kann. Auf der anderen Seite aber sind asymmetrische Verschlüsselungsverfahren wesentlich aufwendiger als symmetrische. Daher werden gerade zur Verschlüsselung langer Nachrichten nach wie vor gerne symmetrische Verschlüsselungsverfahren bevorzugt. Hier stellt sich aber, wie bereits gesagt, das Problem des Schlüsseltausches vor der eigentlichen Nachrichtenübertragung.

Der häufigste Weg, eine gesicherte Verbindung aufzubauen, ist, daß einer der Kommunikationspartner (z.B. Asterix) einen secret key an den anderen Kommunikationspartner (Obelix) überträgt, in dem er ihn mit dem public key von Obelix verschlüsselt. Für die eigentliche Dauer der Kommunikationsbeziehung wird nun als Sitzungsschlüssel der secret key verwendet (Dieses Verfahren wurde in obigem Beispiel eines Logins in ein Novell System bereits demonstriert).

Hier ist allerdings noch zu klären:
1. Wie der Sitzungsschlüssel generiert wird
2. Wie Asterix den public key von Obelix erhält
3. Wie Asterix sicher sein kann, daß er überhaupt mit Obelix kommuniziert

Zu 1. Generieren des Sitzungsschlüssels
Der Sitzungsschlüssel kann entweder durch Asterix selbst erfolgen und dann auf geeignetem Weg zu Obelix transportiert werden (z.B. verschlüsselt mit dem public key von Obelix) oder aber durch das Einschalten einer neutralen Stelle, mit der beide Kommunikationspartner vorab einen Schlüssel vereinbart haben.

Zu 2. Erhalt des public keys von Obelix
Asterix kann den public key wie folgt erhalten haben:
- von Obelix selbst oder
- aus einer Datenbank für public keys eines Dritten (eines sog. Trust Centers)

  Die letztere Variante hat den Vorteil, daß eine Kommunikation auch mit einem anderen (auch bisher unbekanntem) Gesprächspartner erfolgen kann, wenn derjenige einen public key besitzt, der dem Trust Center bekannt ist.

Zu 3: Gegenseitige Authentizität der Kommunikationspartner:
Hier müssen entsprechende Verfahren zur Verteilung öffentlicher Schlüssel zum Einsatz kommen oder einen Mechanismus geben, mit dem nachgewiesen werden kann, dass die Verteilung richtig erfolgt ist.

11.7.1 Diffie Hellman Methode

Eine mögliche Variante des Schlüsseltauschs für symmetrische Schlüssel ist das Diffie Hellmann Verfahren. Es funktioniert wie folgt:
Asterix und Obelix müssen sich auf zwei große Primzahlen n (so daß (n-1)/2 muß auch eine Primzahl ist) und g einigen, diese können auch öffentlich bekannt sein. Asterix wählt nun eine große Zahl (512bit) x, Obelix entsprechend y. Diese Zahlen werden geheimgehalten.

Beispiel: n=47 und g=3
Astrix wählt x=8, Obelix y=10
Asterix sendet: (n, g, g^x mod n) entspricht: (47,3,28) mit 3^8mod47 =28
Obelix sendet : g^y mod n = 3^{10}mod 47 = 17
Astrix berechnet: $(g^y \text{ mod } n)^x = 17^8 \text{ mod } 47 = 4$
Obelix berechnet: $(g^x \text{ mod } n)^y = 28^{10} \text{ mod } 47 = 4$
Nach den Gesetzen der modularen Arithmetik ergeben beide Berechnungen ($g^{x\,y}$ mod n) =4 als Schlüssel.

Trotz der Eleganz dieses Verfahrens ist es angreifbar, und zwar durch eine sogenannte Man-In-The-Middle Attack. Der Man-In-The-Middle nimmt einfach am Verfahren teil in dem er sich eine Zahl z überlegt und damit sowohl Asterix als auch Obelix täuscht.

11.7.2 Schlüsseltausch über Dritte

Statt einer direkten Kommunikation gibt es die Möglichkeit für den Generation oder aber auch nur den Austausch von Schlüsseln eine dritte Stelle einzuschalten, der beide vertrauen. Diese Stelle wird als Schlüsselverteilungszentrum (Key Distribution Center KDC), Trusted Authority (TA) oder Trust Center bezeichnet. Beispielsweise kann sich nun einer der Kommunikationspartner (Asterix) an das Trust Center wenden, um einen Sitzungsschlüssel für die Kommunikation mit einem anderen Teilnehmer (Obelix) zu erhalten. Dieser wird vom Trust Center generiert und in zwei Versionen (jeweils verschlüsselt mit secret keys von Asterix und Obelix) an Asterix gesandt. Asterix decodiert seinen Sitzungsschlüssel und sendet die zweite Version an Obelix, der seine Version des Sitzungsschlüssels ebenfalls dekodiert. Damit kann der Sitzungsschlüssel für die nachfolgende Kommunikationsbeziehung verwendet werden.

11.7.3 Kerberos Protokoll

Es gibt verschiedene Standardprotokolle für Beglaubigung und Schlüsseltausch, wie Wide-Mouth Frog,Yahalom, Needham-Schroeder, Otway-Rees, Dass oder Woo-Lam. Eines der bekannten ist Kerberos, das am MIT (Massachusetts Institute of Technology) entwickelt wurde. Es wird im wesentlchen als verteilter Dienst verwendet, der es einem Client ermöglicht, sich bei einem oder mehreren Servern zu beglaubigen. Optional kann eine Verschlüsselung der Komunikation erfolgen.

Ein Kerberos Key Distribution Center besteht aus zwei Services, dem Authentication Service und dem sogenannten Ticket Granting Service (TGS). Der Authentication Service kennt alle secret keys aller Teilnehmer

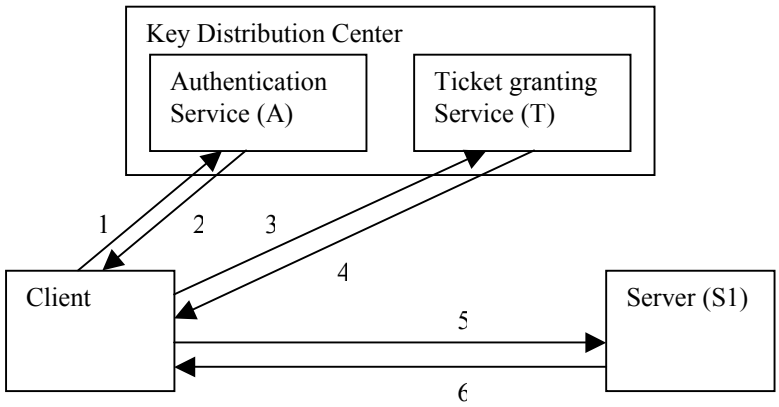
Kerberos verwendet drei Sicherheitsobjekte:

Kerberos Ticket: Für den Zugriff auf den Server werden sogenannte Kerberos Tickets erzeugt. Ein Ticket enthält folgende Informationen:
- den Namen des Clients
- die Identification des Servers
- ein Zeitintervall für die Gültigkeit des Tickets
- einen Sitzungsschlüssel für den Zugriff auf den Server

Authenticator: sichert die Identität des Clients gegenüber dem Server. Er wird vom Client erzeugt und mit einem Sitzungsschlüssel verschlüsselt, er enthält die aktuelle Uhrzeit und eine Prüfsumme

Sitzungsschlüssel: Dient der verschlüsselten Kommunikation zwischen Client und Server

Ein Beglaubigungsvorgang bei einem Server läuft wie folgt ab:



1. Der Client fordert ein Ticket für den Zugriff auf den Ticket Granting Service vom Kerberos Authentication Service an und sendet dazu
   - Seine eigene Identität
   - Die Identität des Servers T
   - Eine Zufallszahl (engl. Nonce)
2. Der Authentication Service sendet
   - einen Sitzunsschlüssel K_{CT} für den Zugriff auf den Service T sowie die Nonce, verschlüsselt mit dem Clientschlüssel (der aus dem Passwort des Nutzers gebildet wurde)
   - ein Ticket, um sich beim Server T auszuweisen, verschlüsselt mit dem Schlüssel des Servers T

3. Der Client möchte mit dem Server S1 kommunizieren und sendet
   - das von A erhaltene Ticket zum Server T
   - seinen Authenticator
   - die Identification für S1
   - eine Nonce (Zufallszahl)

   Nachdem Authenticator und Ticket beide mit dem Sitzungsschlüssel K_{Ct} verschlüsselt sind, dieser aber nur dem Client und dem Authentication Service bekannt sind, ist hierdurch die Beglaubigung erfolgt.
4. Der Ticket Granting Server prüft das Ticket und sendet
   - einen Sitzunsschlüssel K_{CS1} für den Zugriff auf Server S1 und die Nonce des Clients, verschlüsselt mit dem aktuellen Sitzungsschlüssel K_{CT} sowie
   - ein Ticket für S1

5. Für jede Nutzung des Servers S1 (d.h. für jeden Request) sendet der Client
   - seinen Authenticator und
   - das Ticket für S1.
6. Optional sendet der Server selbst die Nonce zurück an den Client, um sich selbst zu authentisieren.

Auf diese Weise werden Sitzunsschlüssel generiert und eine gegenseitige Beglaubigung durchgeführt.

11.8 Zertifizierung

Bei Anforderung eines Schlüssels aus einer zentralen Datenbank könnte es evtl. geschehen, daß die Datenbankabfrage nach dem public key von Obelix abgehört wird und Asterix einen anderen Schlüssel als den von Obelix erhält, ohne es zu bemerken. Auf der anderen Seite könnte auch Obelix seinen public key an Asterix schicken, jemand könnte ihn abfangen und statt dessen seinen eigenen Public key senden. Wie können nun Asterix und Obelix verifizieren, daß sie tatsächlich miteinander und nicht mit einem dritten kommunizieren.

Dieses Problems läßt sich durch die Verwendung von Zertifikaten, die von einem Trust Center (in diesem Fall auch als Certificate Authority (CA) bezeichnet) lösen. Diese Organisation überprüft z.B. die wirklichen Identitäten dieser beiden Kommunikationspartner und stellt hierüber ein elektronisches Zertifikat aus, das dann für die Kommunikation verwendet werden kann. Damit entspricht die Funktion einer solchen Organisation in etwa der eines Notars. Erhält Vertingetorix von Cäsar ein beglaubigtes Dokument, so kann Vertingetorix davon ausgehen, daß Cäsar das Dokument wirklich eigenhändig unterschrieben hat, der Notar könnte dies gegebenenfalls auch bezeugen.

Der wichtigste Standard für digtale Zertifikate ist der X.509 Standard. Ein X.509 Zertifikat, das Obelix nun an Asterix schicken kann, muß folgende Informationen enthalten:
- Den Namen des Eigentümers des Zertifikats (Asterix)
- Einen seiner öffentlichen Schlüssel (public key)
- Den Namen der CA
- Eine digitale Signatur der CA

Nachdem verschiedene Algorithmen für digitale Signaturen verwendet werden können, muß der benutzte Algorithmus ebenfalls angegeben werden. Zudem haben Zertifikate oft eine begrenzte Gültigkeit. Zertifikate können bei Mißbrauch von der austellenden CA widerrufen werden. Sie veröffentlich dazu eine sogenannte Certificate Revocation List (CRL), die periodisch aktualisiert wird. Jeder Teilnehmer einer Kommunikation, der ein Zertifikat erhält kann anhand dieser Liste überprüfen, ob es noch gültig ist.

Für jedes Schlüsselpaar (private und public key) wird ein eigenes Zertifikat ausgestellt. Wenn genügend Personen einer bestimmten Certificate Authority vertrauen, läßt sich so eine ganze Hierarchie von gesicherten Verbindungen realisieren.

Wichtig zu wissen ist, dass nicht der Besitz eines Zertifikats ausschlaggebend für den Nachweis einer Identität ist (Zertifikate sollen ja frei verteilt werden können), sondern der Nachweis, dass man im Besitz des private keys ist, der zum im Zertifikat genannten public key gehört.

11.9 Anwendungsbeispiele

In der Internet Protokollwelt gibt es heute folgende wesentliche Verfahren zum Aufbau verschlüsselter Verbindungen

- Verschlüsselung der Diensteprotokolle: Die wird über eine eigene Schicht oberhalb des Transportprotokolls, die sogenannte Secure Socket Layer (SSL) erreicht, auf die dann beispielsweise http aufsetzen kann (wird dann als secure http bzw. https bezeichnet)
- Verschlüsselung auf der IP-Schicht über IPSEC

Auch im Bereich eMail spielen die vorgestellten Mechanismen heute eine große Rolle zur Bereitstellung von Verschlüsselungs- und Beglaubigungsmechanismen. Die wesentlichen sind S/MIME, PEM und PGP.

11.9.1 Secure Socket layer (SSL)

SSL wurde 1995 von Netscape als Sicherungsprotokoll für die Transportschicht in die IETF eingebracht und ist die Grundlage für das weiterentwickelte TLS (ransport Layer Security Protocol). Ursprünglich wurde es zur Absicherung einer http Kommunikation entwickelt, ist inzwischen auch für andere Diensteprotokolle verfügbar (siehe nachfolgende Portliste). Im Internet Modell sitzt SSL sitzt sozusagen zwischen der Transportschicht und der darüberliegenden Diensteprotokollschicht (bzw. Session Layer im OSI Modell).

Folgende well known ports werden für SSL verwendet:

Port	Protokoll	Bedeutung
443	https	http over SSL
465	ssmtp	smtp over SSL
563	snntp	nntp over SSL
992	telnets	telnet over SSL
995	spop3	pop3 over SSL

Beim Aufbau einer SSL Verbindung wird zuächst ein Handshake durchgeführt:
Eim Verbindungsaufbau eines Clients zu einem Server erfolgt wie folgt:

1. Client Hello: Client teilt dem Server mit:
   - welche kryptographischen Verfahren er unterstützt.

2. Server Hello: Übermittelt werden:
   - Das kryptographische Verfahren
   - Ein Serverzertifikat (optional)
   - Parameter für einen Schlüsseltausch (optional)
   - Eine Zertifikatsanforderung zur Beglaubigung des Clients (optional)

3. vom Client zum Server: übermittelt werden:
   - das Clientzertifikat (wenn angefordert)
   - Parameter für Sitzungsschlüssel, verschlüsselt mit dem public key des Serves
   - Digitale Signatur zur Überprüfung des Client Zertifikats (optional)

11.9.2 IP Security (IPSEC)

IPSEC stellt nicht ein einziges Protokoll dar, sondern eine Architektur zum Aufbau verschlüsselter Kommunikationsbeziehungen IPSEC ermöglicht den Einsatz

- verschiedener Verschlüsselungsalgorithmen

- verschiedener Sicherheitsdienste (Zugangskontrolle, Beglaubigung, Integrität, Vertraulichkeit)
- Kontrolle, wie detailliert die Sicherheitsdienste angewandt werden.

IPSEC ermöglicht den Aufbau von verschlüsselten Kanälen zwischen Routern oder von Clients zu Routern und ist damit eine Schlüsseltechnologie für den Aufbau von VPNs (Virtual Private Networks).

IPSEC besteht im wesentlichen aus zwei Teilen:
Teil 1: Protokolle zur Implemenation der Sicherheitsdienste:
AH (Authentication Header) und ESP (Encapsulating Security Payload)
Teil 2: Schlüsselmanagement:
ISAKMP Protokoll (Internet Security Association and Key Management Protocol)

11.9.3 PGP (Pretty Good Privacy)

Eines der grundsätzlichen Probleme bei der Verteilung von public keys ist das Problem, eine Vetrauenskette zu bilden. PGP geht davon aus, dass jeder Benutzer seine eigenen Kriterien hat, nach denen er anderen zertifizierten Schlüsseln vertraut (z.B. vertraut er evtl. Schlüsseln, die er direkt von ihm bekannten Personen erhalten hat) und wie weit er diesen Zertifikaten vertraut. PGP erlaubt daher eine beliebige Verflechtung von Zertifikaten. Ein Benutzer signiert nun zunächst seinen public key selbst und kann nun seinen Schlüssel mit beliebigen anderen e-Mail Teilnehmern austauschen und deren Schlüssel ebenfalls signieren. Im Lauf der Zeit ergibt sich eine Sammlung unterschiedlichster Schlüssel und Zertifikate die als Key Ring bzw. Schlüsselbund bezeichnet wird. Zu jedem Schlüssel wird gespeichert ein Zertifikat gespeichert, das festhält, mit welchem Algorithmus der Schlüssel erzeugt wurde (RSA, DSS etc.) und welcher Vertrauensumfang diesem Zertifikat entgegengebracht wird. Über den Vertrauensumfang wird sozusagen festgelegt, ob man einer estimmten Person zutraut, das Verfahren zur Zertifizierung von Schlüsseln zu beherrschen oder nicht.
Je nach Version von pgp werden unterschiedliche Verschlüsselungsverfahren und Algorithmen verwendet.

Das Beglaubigen von Nachrichten wird wie folgt durchgeführt:
Der Sender erzeugt aus dem Rumpf der Nachricht eine Einwegprüfsumme und verschlüsselt diese mit seinem privaten Schlüssel. Welches Verfahren zur Bildung der Prüfsumme herangezogen wurde (z.B. MD5) wird in der Nachricht spezifiziert.
Der Empfänger durchsucht bei Erhalt der Nachricht seinen key-Ring nach dem öffentlichen Schlüssel von A, berechnet ebenfalls die Prüfsumme aus der Nachricht und vergleicht diese mit der erhaltenen Prüfsumme. Zudem teilt PGP dem Empfänger mit, welches Vertrauensmaß der Empfänger dem öffentlichen Schlüssel des Senders entgegenbringt, und zwar auf der Grundlage der vorhandenen Zertifikate, die im Key Ring für den Sender enthalten sind.

Nachrichtenverschlüsselung wird wie folgt durchgeführt:
Der Sender verschlüsselt die Nachricht mit einem Einmalschlüssel auf Basis eines symmetrischen Algorithmus (z.B. DES). Dieser Einmalschlüssel wird mit dem public key des Empfängers verschlüsselt. Die Nachricht wird in ASCII kodiert und zusammen mit dem Schlüssel übertragen. Der Empfänger dekodiert zunächst den Schlüssel und damit dann die eigentliche Nachricht.

11.10 Sicherheitspolicen

Um ein Netzwerk sicher zu machen, muß für jedes Netz eine eigener Sicherheitsstandard festgelegt werden, der folgende Punkte berücksichtigt:

- Welche Netzwerkverbindungen werden genutzt und sind insofern angreifbar
- Risikoanalyse
- Untersuchung der möglichen Angriffsarten auf das Netz
- Check und Einführung von Schutzmechanismen
- Unabhängige Evaluierung

Es gibt unabhängige Organisationen, die für Betriebssystem und Netze Sicherheitszertifikate vergeben. Das vielleicht bekannteste ist in USA das NCSC (National Computer Security Center). Hier werden Systeme nach Klassen eingeteilt, das zugrundelegende Konzept heißt TCSEC (Trusted Computer System Evaluation Criteria)
Class D (Minimaler Schutz)
Class C1 (vorhandene Zugriffssicherheit)
Class C2 (Kontrollierte Zugriffsicherheit)
Class B1 (Bestätigte Zugriffsicherheit)
Class B2 (Strukturierter Schutz)
Class B3 (Sicherheitsdomänen)
Class A1 (Verifiziertes Design)
In Europa werden Produkte gegen die ITSEC (Information Technology Security Evaluation Criteria) Kriterien getestet. Hier werden dann von europäischen Organisationen Zertifikate für die Integrität und die Effektivität von Systemen vergeben. Typische Zertifikate sind E2-Level für Effektivität und F-C2 für Funktionalität.
E2 kombiniert mit F-C2 entspricht dannetwa wieder der C2 Zertifizierung der NCSC.
Betriebssystem wie Windows NT und NetWare sind z.B. C2 zertifiziert, allerdings mit einem sehr großen Unterschied: Bei Novell Netware gilt C2 für ein komplettes Netzwerk, bei Windows NT nur für den Rechner mit dem lokalen Betriebssystem an sich.

12. Netzwerkmanagement

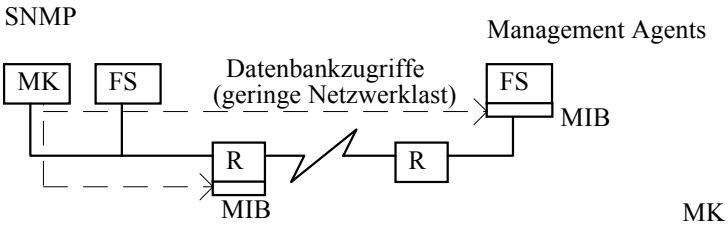
Man unterscheidet:
- Netzwerkmanagement
- Desktopmanagement

12.1 Netzwerkmanagement:

Standardmanagement Modell der ISO:

5 funktionale Bereiche:
- Fault Management
  Fehlerbenachrichtigung, Fehler erkennung, Fehlervoraussage, (Proaktives Management)
- Performance Management
  Überwachung der Performance (Leistungsfähigkeit) von Netzkomponenten der Netzverbindungen
- Configuration Management
  Netzwerkübersicht (Map), Überwachung und Fernsteuerung von Netzwerkkomponenten, Fernkonfiguration
- Security Management
  Recourcenverwaltung, Schutz vor unerlaubten Zugriff, Benutzerverwaltung
- Accounting Management
  Berechnung oder Abrechnung von Services

Aufbau eines Managementsystems:
Im Allgemeinen besteht ein Netzwerkmanagementsystem aus zwei Komponenten, einer Managementstation und einem überwachten Rechner. Der Rechner wird durch eine spezielle Schnittstelle, dem sogenannten Management-Agent, managebar. Der Agent ist als Software auf dem zu überwachenden Rechner installiert.



MK = Managementkonsole
MIB = Management Information Base

In Band Management: Management über das LAN
Out Band Management: Management über redundanten Weg (Dedizierte Leitung / Modem)

Management Agents:
Die Agents haben unterschiedliche Funktionalität, z.B.:

Serverüberwachung:
- Server-Agent: z.B. Überwachung bestimmter Server-Hardware (z.B. Compaq)
- Agents zur Überwachung von Zusatzfunktionen wie z.. USV (Unterbrechungsfreie Stromversorgung)

Netzwerküberwachung:
- Überwachung der angeschlossenen Netzwerke von den Servern aus (Managewise LANalyzer Agent, Problematisch bei Switches)
- Agents zur Überwachung von Hubs, Bridges, Switches, Routern (Herstellergebunden)

Standards:
ISO: CMIP (Common Management Information Protocol)
CMOT (CMIP over TCP/IP)
IETF: SNMP (Simple Network Management Protocol)
SNMP II

SNMP:
Jeder Agent stellt eine Datenbank (MIB=Management Information Base) zur Verfügung, in der spezifische Daten des überwachten Gerätes festgehalten sind. Die Kommunikation zwischen Netzwerkmanagementstation und den Agents (genauer mit der MIB der Agents) erfolgt im Allgemeine über das Protokoll SNMP (Simple Network Management Protocol).
SNMP erlaubt die Fernsteuerung der überwachten Geräte (Veränderung der Werte in der MIB) sowie das Versenden von Fehlermeldungen (sogenannte Traps) vom Agent zur Managementstation. SNMP kann, auch wenn es aus der IP Welt kommt, in verschiedenen Protokollwelten verwendet werden, es kann insbesondere auch auf das Novell IPX Protokoll aufsetzen.

SNMP kennt 5 Befehle: Get Request, Get Response, Get Next, Set, Trap
(Objekt lesen, Tabellen lesen, Schreiben von Information, Alarmmeldung)

Beispiel für eine Kommunikation zwischen Konsole und Agent:
Get Request: Kosten Routerverbindung
Get Response: Kosten = 12
Set: Setze Kosten = 15

Aufbau der MIBs
Die Agents enthalten Information über das zu überwachende Gerät in Form sogenannter MIBs. Es gibt zwei verschiedene Typen von MIBs:
Standard MIBs (Internet MIBs): standardisierte MIBs, hier ist der Aufbau der MIB sowie der Parameter innerhalb der MIB genau festgelegt.
Enterprise MIBs: Hier kann jeder Hersteller für sein Gerät (z.B. ein Routerhersteller für seine Router) genau festlegen, welche Parameter des Geräts überwacht werden sollen, und welche Traps (Fehlermeldungen) in welchen Fällen an eine Management Station geschickt werden.

Die MIBs folgen einer einheitlichen, hierarchischen Struktur
(SMI: Structure and Identification of Management Information)

Generell muß natürlich auch die Managementstation über die Informationen der einzelnen Parameter der MIBs aller Agents verfügen, sonst könnten unter Umständen Traps, die ankommen, nicht richtig interpretiert werden. Speziell bei nicht standardisierten MIBs z.B. bestimmten Enterprise MIBs muß eventuell die MIB an der Managementstation entsprechend compiliert werden, damit die entsprechende Information hier vorliegen kann. Bei NMS erfolgt dies über einen speziellen MIB Compiler,der innerhalb der Management Konsole gestartet werden kann.

Wesentliche Unterschiede zu anderen Netzwerkmanagementprotokollen:
SNMP am weitesten verbreitet
CMIP ist komplexer; wesentlich: abwärtskompatibel zu SNMP

CMIP Mangementstation kann auf SNMP Komponenten zugreifen

SNMP II
Weiterentwicklung für erweiterte Funktionalität
Kommunikation zwischen Managementkonsolen
Erweiterte Sicherheitsfunktionen
Get Bulk: lesen kompletter Tabellen in einem Befehl → Performancegewinn

Beispiele für Netzwerk-Management Software

Firewalls und Netzwerksicherheit

- Novell anageWise	LAN, WAN
- IBM Tivoli	LAN, WAN
- HP Openview	LAN, WAN

Alarm-Management:
Für das Alarmmanagement müssen die entsprechenden Agents konfiguriert werden:
- Schwellwerte für Alarmmeldungen bei Überlastung
- Fehlerzustände

Damit dann entsprechende Trap-Meldungen bei einer Management Konsole auch ankommen, muß die Adresse dieser für jeden Agent konfiguriert werden (z.B. Traptarg.cfg bei Novell). Da nicht unbedingt gewährleistet ist, daß bei Ausfall einer Komponente überhaupt noch eine Fehlermeldung geschickt werden kann, macht es unter Umständen Sinn, zumindest Kritische Systeme dauerzuüberwachen (z.B. über Ping).

Zusätzlich können die Agents konfiguriert werden, so daß nicht alle möglichen Störfälle automatisch zum Senden eines Traps führen, sondern nur ganz bestimmte. Dazu kann normalerweise jeder einzelne Trap festgelegt werden, alternaiv, sind die möglichen Störfälle in Klassen eingeteilt (Severity Levels, typisch Level 1 bis 7) und es kann festgelegt werden, daß zB. nur Störfälle ab einem bestimmten Level wie Severity Level 6 geschickt werden. Auf diese Weise kann der durch die Managementfunktionaliät verursachte Netzwerkverkehr reduziert werden, was sich speziell bei WAN Verbindungen auszahlt.

12.2 Desktopmanagement

Hier können die Clients eines Netzes überwacht werden. Dazu wird allerdings nicht auf SNMP aufgesetzt, sondern über ein eigenes Protokoll auf den Client zugegriffen.

Typische Aufgaben umfassen:
- Softwareverteilung und File-Transfer
- Inventarisierung
- Remote Control

Hier geht es also nicht um Alarmmanagement, sondern um Fernkonfiguration und Benutzerunterstützung. Aufgrund der zunehmenden Komplexität heutiger Netze und Workstationbetriebssysteme kommt dem Desktopmanagement eine immer größer werdende Bedeutung zu.

Beispiele für Desktopmanagementsysteme:
- Novell Z.E.N.Works
- Microsoft Systems Management Server (SMS)

13. Neue Entwicklungen

13.1 Ipng (IP next generation, Ipv6)

Die größten Probleme des IP Protokolls in der derzeitigen Version 4 sind der begrenzte Adressraum und, für die Verwendung im Internet, das Fehlen von Verschlüsselungsalgorithmen. Beide Probleme werden in der nächsten Version IP Version 6 bzw. Ipng adressiert. Ipng wurde als Nachfolger des jetzigen IP von der IETF im Juli 1994 verabschiedet.
Der Adressraum von Ipng ist 16Byte. Die Schreibweise wird von einer byteweise Schreibweise mit . Trennung in eine wortweise Schreibweise mit : Trennung verändert.

Beispiel für eine IPnG Adresse:
FE00:0:0:0:0:0:0:1

Ipng soll neben dem IP verwendet werden, insofern muß eine Kompatibilität der beiden gewährleistet sein.
Dies wird dadurch erreicht, daß für die Codierung der alten IP Adressen im Ipng die ersten 12 Byte der 16Byte mit Nullen aufgefüllt werden.
Aus 210.170.50.33 wird 0:0:0:0:0:0:210.170.50.33

Folgende Erweiterungen sollen in Ipng implementiert werden:
- 16 Byte Adressraum
- Autokonfiguration von Adressen
- Einfacherer IP-Header
- Zusätzliche Header und Optionen für Sonderfunktionen
- Unterstützung von Verschlüsselung
- Source Routing Unterstützung

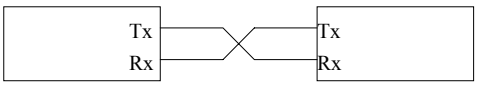
Weitere Details findet man in RFC 1752: Recommendation for Ipng.

13.2 IEEE 802.12 100 Base VG - Anylan

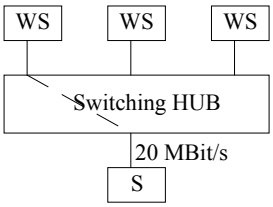
Entwickelt von HP, Apple, anfangs auch IBM
VG: Voice Grade (UTP Cat 3-5)
Zugriffsverfahren DPA: Demand Priortiy Access
Punkt zu Punkt Verbindungen d.h.
Sender schickt direkt an Empfänger (geregelt über Switching Hub, Prioritätssteuerung)
→ andere Stationen sehen Pakete nicht → Sicherheit
Switching HUB bedient Anfragen nach Priorität → keine Kollisionen
4 Adern mit je 25 MBit/s (Quartet Signaling / Parallele Übertragung)
5B/6B Code → effektive Bandbreite 30 MHz

13.3 Full Duplex Übertragung

Full Duplex Ethernet



10 MBit/s Ein- und Ausgang parallel → 20Mbit/s,
inzwischen ist auch 100 Mbit/s Full-Duplex Ethernet verfügbar

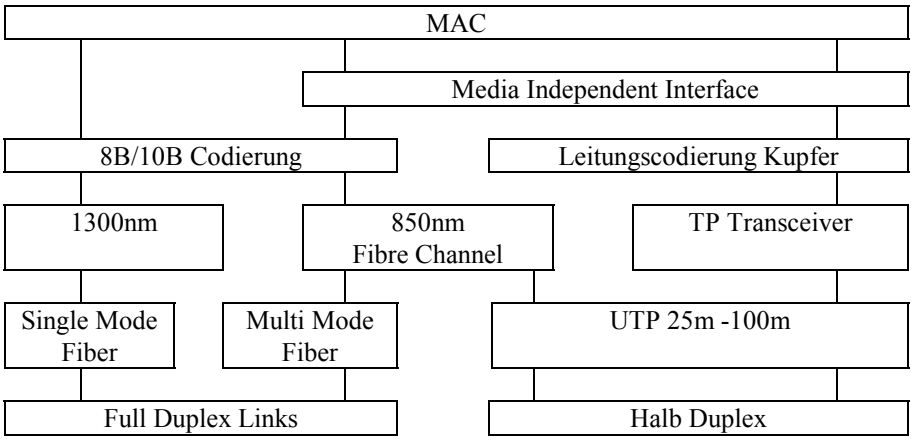


Für Full Duplex Token Ring und Full Duplex FDDI haben sich ebenfalls Standards verabschiedet. Auch hier ist das grundsätzliche Verfahren das Abschalten der entsprechenden Zugriffskontrolle.

13.4 Gigabit Ethernet (IEEE 802.3z, 802.3ab)

1000 Base T Cat 5 UTP
1000 Base CX STP/Twinax
1000 Base SX Multimode Fiber (850nm)
1000 Base LX Monomode Fiber oder Multimode (1300nm)

STP und Fiber Standards sind verabschiedet, zur Festlegung des UTP Standards wurde ein eigenes IEEE 802.3ab Subkommitee gebildet. Dieses hat das Ziel, einen Standard für eine Reichweite von 100m auf UTP Cat. 5 Kabeln zu erzielen.



Zugriffsverfahren: CSMA/CD
Problematik: Bei Erhöhung der Übertragungsrate auf 1Gbit/s möchte man auf die vorhandenen Verkabelungsstrukturen aufsetzen, d.h. die Leitungslängen sollen gleich sein wie bei 100 Base T. Daher muß bei gleicher Leitungslänge die minimale Paketgröße vergrößert werden.
Minimale Paketlänge: 512 Byte
Da hierdurch ein Nachteil bei kleinen Paketen besteht (die auf die 512 Byte aufgefüllt werden müssen), wird auf der anderen Seite ein Burst Modus eingeführt, der es erlaubt, mehrere Pakete bis auf eine Gesamtlänge von 1500 Byte bis 8kByte zusammenzufassen.
Es soll ebenfalls ein Full Duplex Ethernet (2Gbit/s) geben (Gigabuffer Repeater).

Für die Optik Version bestehen folgende Randbedingungen:

Bezeichnung	Realisierung	Medium	Max. Länge
1000 Base SX	Multimode Fiber (850nm)	62,5µm	260m
1000 Base SX	Multimode Fiber (850nm)	50µm	550m
1000 Base LX	Multimode Fiber (850nm)	62,5µm	440m
1000 Base LX	Multimode Fiber	50µm	550m

	(850nm)		
1000 Base LX	Monomode Fiber	8,3 µm	3km

1000 Base T auf UTP Kabeln:

- Verwendung einer 5 Level Codierung
- gleichzeitig Verwendung von 4 Adernpaaren
- Vollduplex Betrieb auf allen 4 Paaren
- Trellis Codierung (nicht 8B10B) (Verteilung der 8 Datenbits und 1 Paritybit auf verschiedene Level der 4 Kanäle

13.5 Fibre Channel

Ursprünglich entwickelt von HP, IBM, Sun als Möglichkeit einer Hochgeschwindigkeitsanbindung von Rechnern zu Peripheriegeräten. Fibre Channel ist allerdings auch als LAN Technologie denkbar. Die entsprechenden Standards (ANSI-T11) sind bereits verabschiedet. Fibre Channel definiert die Schichten 1 und 2 des OSI Modells.

Übertragungsraten:
1 Gbit/s heute verfügbar (2Gbit/s als Dual Channel)
4 Gbit/s in Entwicklung
8 Gbit/s geplant
Vorteile: Ausfallsicherheit bei Verwendung eines Dual Channel
geringer Protokoll Overhead
gesicherte Übertragung (keine Zellverluste wie bei ATM)
Länge: bis 10km
Adressraum: 16 Mio Adressen im lokalen Fibre Channel Netz, damit mit klass. LAN Technologien vergelichbar

Funktionsweise:
geswitchte Netze: Fibre Channel Fabric
Bus-Netze: Fibre Channel Arbitrated Loop

Bildet die Grundlage für andere Technologien:
ATM over Fibre Channel
Gigabit Ethernet auf Fibre Channel

13.6 ATM (Asynchronous Transfer Mode)

13.6.1 Grundlagen

ATM wurde als Hochgeschwindigkeits-Vermittlungstechnik für Daten, Sprache und Video entwickelt.
Datenkommunikation: Kurzfristiger, nicht vorhersehbarer Datenaustausch "bursty traffic"
Sprache / Video: längere Dauer, vorherbrestimmte Bandbreite, synchron (konstante / variable Bitrate)

Es ist im WAN Bereich (z.B. Breitband ISDN), dem MAN wie auch für den LAN Bereich geeignet. Damit besteht einer der wesentlichen Vorteile dieser Technologie in der Tatsache, daß die herkömmlichen Grenzen zwischen WAN, MAN, und LAN verschwinden können. Allerdings hat ATM gerade für den Einsatz in LANs mit reiner Datenübertragung auch Nachteile.

ATM basiert auf Paketvermittlung von kleinen Paketen, sog. Zellen (Größe: 53byte), die in virtuellen Datenkanälen (Virtual Channel) ähnlich wie bei der klassischen Paketvermittlung zum Empfänger gesendet (besser: geschaltet) werden. Diese Kanäle müssen vor dem Senden aufgebaut und hinterher wieder abgebaut werden, die Datenübertragung erfolgt also verbindungsorientiert. Damit unterscheidet sich dieses Verfahren völlig von der in LANs überwiegend verwendeten verbindungslosen Übertragung. Herkömmliche Aufgaben typischer LAN Protokolle wie Flußkontrolle, Fehlerkontrolle und Bestätigungskontrolle werden abgelöst durch Aufgaben wie Verkehrskontrolle, Überlastkontrolle und Überwachung der Übertragungskapazität.

Der ATM Standard wird vom ATM Forum, einem Zusammenschluß verschiedener Hersteller, definiert.

Übertrragungsraten
LANs: 25,6 MBit/s (IBM), 100 Mbit/s, 155,52 MBit/s,
öffentliche Netze: 34,368 MBit/s, 44,736 Mbit/s, 155,52 Mbit/s
langfristig im Breitband ISDN: 622,08 MBit/s, bis 2.488,32 MBit/s

13.6.2 ATM Schichtenmodell

ATM Adaption Layer (AAL)	Segmentierung von Paketen in Zellen
ATM Layer	Paketübertragung in Virtuellen Verbindungen / Virtuellen Pfaden, Zellheadererzeugung, Flußkontrolle, Zellmultiplex
Physical Layer	Transmission Control Sublayer: Fehlerkontrolle, Entkopplung Zellrate, Physical Medium Sublayer: Bit timing

Unterteilung des ATM Modells in 3 Ebenen:

Benutzerebene: Beschreibt die Kommunikation zwischen Benutzern
Kontrollebene: Beschreibt die Kommunikation von Benutzern mit dem Netzwerk, die sog. UNI Schnittstelle (User to Network Interface).
Managementebene: Beschreibt die Kommunikation im Netzwerk, die sog. NNI Schnittstelle (Network to Network Interface manchmal auch als Edge to Edge Interface bezeichnet).

13.6.3 ATM Layer

ATM erlaubt Übertragung durch Virtuelle Verbindungen, die zwischen Benutzern im Netz aufgebaut werden. Punkt zu Punkt und Punkt zu Multipunkt-Übertragung ist möglich. Diese virtuelle Verbindung wird realisiert durch eine Folge von unidirektionalen Verbindungsabschnitten, sog. virtuellen Kanälen (Virtual Channel, VC) zwischen ATM Switches.
Mehrere Känäle zwischen den Komponenten (Switches) im Netz werden zu virtuellen Pfaden (Virtual Path, VP) gebündelt, um Kontrollaufgaben zu vereinheitlichen und den Overhead für jede einzelne Verbindung zu senken. (siehe Beiblatt). Für die Teilnehmerschnittstelle bedeutet dies, daß der gesamte Datenverkehr eines Teilnehmers in einem virtuellen Pfad zusammengefaßt wird.

Konsequenterweise gibt es zwei Arten von ATM Switches:
VP Switches: Kanäle bleiben den virtuellen Pfaden fest zugeordnet, der komplette Pfad wird geschaltet, Virtual Channel Identifiers bleiben unverändert)
VC Switches: Virtuelle Pfade und einzelne virtuelle Kanäle werden (auch über verschiedene Pfade) geschaltet.

ATM Zelle:
Zellgröße: 48bit (ursprünglicher Vorschlag: USA und Japan: 32bit, Europa 64bit)
zuzüglich 5 Byte Header
Felder des Headers:
GFC: Generic Flow Control (verwendet zur Ende zu Ende Flußkontrolle)
VPI: Virtual Path Identifier
VCI: Virtual Channel Identifier
PT: Payload Type: (Typ der gesendeten Information: z.B. User Daten, Management Information etc.)
CLP: Cell Loss Priority (Zellpriorität zur Steuerung der Vernichtung von Paketen bei Überlast im Netz)

Es gibt zwei unterschiedliche Zelltypen, entsprechend der verschiedenen Schnittstellen im ATM Netz:
- UNI (User Network Interface), Zellen werden zur Kommunikation zwischen Benutzern und dem Netzwerk verwendet und
- NNI (Network Network Interface), Zellen zur Kommunikation zwischen den Netzwerkknoten

Einziger Unterschied zwischen beiden ist, daß bei UNI Zellen ein 4-bit Feld für die Ende zu Ende Flußkontrolle zur Kommunikation zwischen den Benutzern vorgesehen ist, das bei NNI Zellen fehlt. In NNI Zzellen sind 12bit für die Angabe des VPI (Virtual Path Identifier) reserviert, bei UNI Zellen entsprechend nur 8bit.

13.6.4 AAL Layer:

Generelle Aufgabe ist die Umsetzung von Daten höherer Schichten in ATM Zellen: Generell können unterschiedliche Informationstypen mit unterschiedlichen Geschwindigkeiten übertragen werden Hierzu werden vier verschiedene Serviceklassen definiert:

	Klasse A	Klasse B	Klasse C	Klasse D
Zeitliche Relation zwischen Quelle und Ziel	benötigt	benötigt	nicht benötigt	nicht benötigt
Bitrate	konstant	variabel	variabel	variabel
Verbindungsart	verbindungsorientiert	verbindungsorientiert	verbindungsorientiert	verbindungslos

Steuerung der Übertragungsbandbreite:
Die Übertragungsbandbreite kann einem Endgerät im ATM Netz flexibel zugeordnet werden, dies geschieht statisch oder dynamisch. Folgende Möglichkeiten werden heute von ATM Switches unterstützt (wobei es Unterschiede gibt, welche Konzepte bei welchen Switches auf welche Weise implementiert sind):

- CBR: Constant Bit Rate:

Echtzeitanwendungen wie Voice/Video, virtuelle feste Bandbreite
- VBR: Variable Bit Rate:

Verkehr bei einer Basisrate, die während der Kommunikation verändert werden kann
- UBR: Unspecified Bit Rate:

Keine feste Bandbreite reserviert, Applikationen senden Daten wenn Bandbreite verfügbar, für klass. Datenkommunikation in LANs geeignet.
- ABR: Available Bit Rate:

flexiblestes Konzept, eigener Steuermechanismus zur maximalen Ausnutzung der gerade verfügbaren Bandbreite. Geeignet für klass. Datenkommunikation in LANs.

13.6.5 Einsatz von ATM in LANs

Damit ATM in LANs eingesetzt werden kann, wird ein Standard für die LAN Emulation benötigt (LAN-E). Hier wird das klassische Verhalten von Shared LANs mit Komponenten, die sich einen gemeinsamen Übertragungskanal teilen, emuliert. Beispielsweise wird hier festgelegt, wie ein Broadcast (Rundruf) an alle Teilnehmer weitergeleitet wird. Damit wird den Teilnehmern ein LAN vorgegaukelt. LANE arbeitet auf Schicht 2 des OSI Modells, d.h. es können klassische routbare wie auch nichtroutbare Protokolle hierauf aufsetzen.

ATM im LAN wird häufig als eine Backbone Technologie betrachtet, d.h. für den Einsatz als schnelles Rückrat in einem klassischen LAN mit Ethernet, Token Ring oder auch FDDI Segmenten unter Verwendung klassischer Netzwerkprotokolle wie TCP/IP.

Hierfür gibt es schnelle Switches, die IP-Subnetze oder VLANs auf emulierte LANs (ELANs) umsetzen. Ein weiterer Standard ist Multiprotocol over ATM (MPOA). Dieser Standard legt fest, wie

klassische Protokolle der Ebene 3 wie IP oder IPX über ein ATM Netzwerk kommunizieren können. Er setzt auf den sogenannten ELANs auf und sorgt für kurze Wege über die ELANs.

Hier kommt allerdings einer der Nachteile von ATM zum Tragen. Der Verlust von Zellen ist per Design in diese Technologie integriert. Über die Cell Loss Priority in einer ATM Zelle wird gesteuert, welche Zellen im Fall einer Netzwerküberlastung vernichtet werden können. Das heißt, wenn im Fall der Übertragung eines größeren TCP Pakets in verschiedenen Zellen nur eine Zelle verloren geht, muß das gesamte Paket, d.h. alle anderen erfolgreich übertragenen Zellen ebenfalls neu übertragen werden. Dies reduziert jedoch die maximal zu erwartenden Datentransferraten auf Größenordnungen, wie sie auch mit anderen Technologien wie z.B. FDDI zu erreichen sind.

Kosten ATM-Switch für den Einsatz in LANs:
Ca 10000 - 20000 DM für 16 Port Switch
Adapter ca 2000 DM

Optisches Interface
Zur optischen Übertragung kann ATM auf SONET (bzw. SDH) aufsetzen.
SONET: Synchronous Optical NET
SDH: Synchrone Digitale Hirarchie (Europäische Norm)
Durch diese Standards werden weltweit gültige Übertragungsraten festgelegt:
51MBit/s / 155MBit/s / 622MBit/s / 1,2GBit/s / 2,4GBit/s

Größere ATM Netze:
Deutsches Forschungsnetz DFN
- 30 Cisco 7000 Router
- 12 ATM Switdches

DARPA Testprojekt
- 6 ATM Switches über 2,4 GBit/s SONET
- Desktop 155 - 1,2 GBit/s

14. Anhang

14.1 Verwendete Abkürzungen

ABR	Available Bit Rate (ATM)
ACK	Acknowledgement Paket
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1 (Maschinenunabhängige Darstellung von Information, OSI Protokoll)
ATM	Asynchronous Transfer Mode
AMI	Alternate Mark Inversion (Code)
ANSI	American National Standards Institute
APPC	IBM Advanced Program to Program Communication
APPN	IBM Advanced Peer to Peer Networking
AUI	Attachment Unit Interface
BPDU	Bridge Protocol Data Unit
CAT	Category (Kabelkategorie)
CBR	Constant Bit Rate
CCITT	Consultative Committee for International Telegraphy and Telephony
CDDI	Copper Distributed Data Interface
CLNP	Conectionless Network Protocol (OSI Layer 3)
CMI	Coded Mark Inversion (Code)
CMIP	Common Management Information Protocol (OSI)
CMOT	CMIP over TCP/IP (OSI)
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
DARPA	Department of Defense Advanced Research Projects Agency
DAS	Dual Attachment Station
DIX	Digital-Intel-Xerox
DoD	Department of Defense (USA)
DNA	Digital Network Architecture (DEC)
DS	Directory Services (OSI Protokoll)
EBCDIC	Extended Binary Coded Decimal Interchange Code (IBM)
ES-IS	End System-Intermediate System (OSI Routing Protocol)
FAT	File Allocation Table
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FDM	Frequency Division Multiplexing
FTAM	File Transfer, Access and Management (OSI-Protokoll)
FTP	File Transfer Protocol (Internet Protokoll)
HPFS	High Performance Filing System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronical Engineers
IETF	Internet Engineering Task Force
IP	Internet Packet

IPng	IP Next Generation
IPX	Internet Packet Exchange (Novell)
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System-Intermediate System (OSI Routing)
ISO	International Standards Organisation
ITU	International Telecom Union
LAN	Local Are Network
LAN-E	LAN Emulation (ATM)
LAT	Local Area Transport (DEC- Terminalserver- Protokoll)
LLC	Logical Link Control
LSP	Link State Protocol
LU	Logical Unit (IBM-Welt)
LU6.2	IBM Peer to Peer Protokoll
MAC	Media Access Control
MacOS	Macintosh Operating System
MAN	Metropolitan Area Network
MAU	Medium Attachment Unit (Transceiver)
MDT	Mittlere Datentechnik
MIB	Management Information Base
MHS	Message Handling System
MPOA	Multiprotocol over ATM
MSAU	Multiple Station Access Unit (Ringleitungsverteiler)
NAK	Negative Acknowledgement Paket
NAU	Network Adressable Unit (z.B. PU, LU, SSCP)
NCP	NetWare Core Protocol
NDS	Netware Directory Services
NFS	Network File System
NLSP	Netware Link State Protocol
NNTP	Network News Transfer Protocol
NRZ	Non Return to Zero
NRZI	Non Return to Zero Inverted
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First (Routing)
PHY	Physical Layer Protocol (FDDI)
PMD	Physical Layer edium Dependent (FDDI)
POP	Post Office Protocol
PU	Physical Unit (IBM-Welt)
PUCP	Peripheral Unit Control Point (Lokaler SSCP in Cluster Controller, IBM-Großrechnerwelt)
RAID	Redundant Array of Inexpensive Disks
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RS	Return to Zero
SAP	Service Advertising Protocol (Novell)
SAP	Service Access Point
SAS	Single Attachment Station
SSCP	System Services Control Point (Steuert Session-Aufbau in IBM Großrechnern)
SDDI	Shielded Distributed Data Interface
SDH	Synhronous Digital Hierarchy (Eoropäisches Equivalent zu SONET)
SFD	Start of Frame Delimiter (Frame-Anfangsfeld)
SMI	Structure and Identification of Management Information

SMT	Station Management (FDDI)
SMTP	Simple Mail Transfer Protocol (Internet Protokoll)
SNA	Systems Network Architecture (IBM)
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network (High Speed Standard bis 2.4GBit/s)
SPX	Sequenced Packet Exchange (Novell)
SUTP	Screened Unshielded Twisted Pair
STMP	Simple Mail Transfer Protocol
STP	Shielded Twisted Pair
TCP	Transport Control Protocol
TDM	Time Division Multiplexing
TELNET	Protokoll zur Terminal Emulation (Internet Protokoll)
TPDU	Transport Protocol Data Unit (Internet Protokollwelt)
TP4	Transport Protocol 4 (eines der OSI Transport Protokolle)
TP-PMD	Twisted Pair-Physical Medium Dependent (Norm für FDDI über Twisted Pair)
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol (Internet Protokoll)
UTP	Unshielded Twisted Pair
VBR	Variable Bit Rate
VLAN	Virtual LAN
VLM	Virtual Loadable Module
VC	Virtual Channel
VCI	Virtual Channel Identifier
VP	Virtual Path
VPI	Virtual Path Identifier
VT	Virtual Terminal (OSI-Protokoll)
VTAM	Virtual Telecommunications Access Method („Netzwerkbetriebssystem“ der IBM Großrechnerwelt)
WAN	Wide Area Network
XDR	External Data Representation (Internet Protokoll)

14.2 Fragen zum Inhalt

Fragen zur Prüfungsvorbereitung:
Die folgenden Fragen sollen vor allem einen Überblick über den möglichen Fragestil geben, nicht so sehr einen vollständigen Katalog für eine Prüfung. Es sind Beispielfragen enthalten, die aus Praktikumsversuchen stammen, die in Ihrem Semester evtl gar nicht durchgeführt wurden.

Grundsätzlich müssen nicht alle Fragen beantwortet werden, um die volle Punktzahl zu erhalten, die Prüfung wird einen Fragenüberhang von ca 10% beinhalten.

OSI Referenzmodell
Vervollständigen Sie das folgende Bild des OSI-Referenzmodells. Sie können dabei die deutschen oder englischen Begriffe verwenden

Application Layer
Data Link Layer

In welche beiden Teilschichten kann man die Data Link Layer unterteilen?

Codierung
Was ist das wesentliche Kennzeichen von Codierungsverfahren wie Manchester bzw. Diff. Manchester?

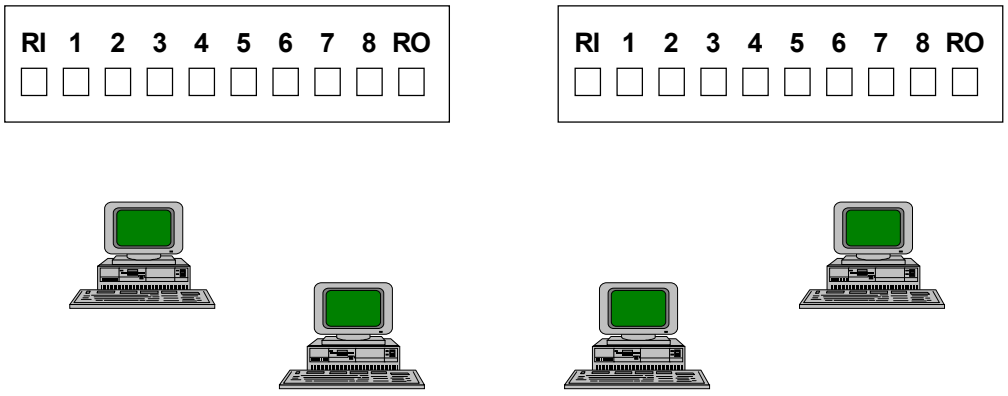
Bei FDDI wird eine andere Art der Codierung verwendet. Welche? Was ist der wesentliche Unterschied zu Manchester bzw. Diff. Manchester Code?

Performance
Mit welchem Programm/Tool kann man die Auslastung/Utilization eines Netzwerksegments messen bzw. anzeigen lassen.

Directory Services
Welches sind die beiden wesentlichen Unterschiede einer Bindery eines Fileservers und Directory Services?
Welcher grundsätzliche Unterschied besteht für den Benutzer beim Einloggen in einen einzelnen Fileserver gegenüber einem Netzwerk mit Directory Services?
Nennen Sie 5 verschiedene Blattobjekte (leaf objects) in der Novell NDS.

Standardprotokolle
Wieviele Subnetze kann man in einem Netz mit einer Class C Adresse maximal bilden, wenn an allen Stationen die Subnetzmaske FF.FF.FF.F0 verwendet wird.
Erklären Sie kurz den Verwendungszweck des ARP Protokolls.

Token Ring
4a. Vervollständigen Sie in nachfolgender Skizze den Aufbau eines Token Ring Netzes mit zwei Ringleitungsverteilern und vier Netzwerkstationen:



LAN Zugriffsverfahren
Beschreiben Sie in drei Schritten die Funktionsweise des CSMA/CD Zugriffsverfahrens beim Senden.
Ordnen Sie die folgenden Merkmale und Begriffe den Zugriffsverfahren Ethernet (802.3), Token Ring (802.5) und FDDI zu. Kreuzen Sie dazu entsprechend an (Mehrfachnennungen sind möglich):

	Ethernet	Token Ring	FDDI/CDDI
Deterministisches Verfahren			
Class A (bzw. DAS) -Station			
Eine Station als Active Monitor			
Manchester Codierung			
Twisted Pair Verkabelung möglich			
Ringleitungsverteiler			
Transceiver bzw. Medium Attachment Unit			
Kollisionserkennung			

Router
Welche der folgenden Protokolle werden zwischen Routern verwendet, um interne Routingtabellen abzugleichen: IPX, IP, RIP, OSPF, SNA, Netbios, TCP?
Welcher Ebene des OSI Modells sind diese Routingprotokolle am ehesten zuzuordnen?

Printing
Mit welchem Dienstprogramm/Utility wird im Novell Netz ein Printserver definiert?
Welchen Weg nimmt ein Druckjob von einer Workstation aus in einem Novellnetz bis zum Ausdruck.

Workstation → _____ -→ _____ -→ Drucker

Welches Protokoll wird in einem Novell Netz zur Kommunikation zwischen Printserver und Remote Drucker verwendet?

Weitere Fragen:

Neue Entwicklungen

1. Was ist der wesentliche Unterschied zwischen den Novell Protokollen IPX und SPX?

2. Wofür steht der Begriff MAN?

3. Welcher Ebene im OSI Referenzmodell könnte das TCP Protokoll am ehesten zugeordnet werden?

4.Welches sind die wichtigsten, typischen Aufgaben von Protokollen der Netzwerkschicht?

5. Nenne Sie zwei wichtige Kriterein zur Bewertung von Leitungscodes zur Datenübertragung

6. Was versteht man unter dem Begriff "selbsttaktender Code"

7. In welchen Topologien können Ethernet Netze verkabelt werden?

8. Wie hängt die Transferrate in Ethernet und Token Ring-Netzen von der Paketgröße ab?

9. Wofür steht der Begriff "10 Base 5" und wofür stehen die 10, das Base und die 5?

10. Wodurch unterscheiden sich Ethernet 802.3 und 802.2 Frame Formate?

11. Wie groß (Wieviele Byte) ist ein Token im 802.5 Token Ring?

12. Erklären Sie kurz die Funktionsweise der Datenübertragung im 802.5 Token Ring

13. Erklären Sie den Begriff "Early Token Release"

14. Durch welches Protokoll wir bei transparenten Brücken verhindert, daß im Netz redundante Wege entstehen

15. Welches der genannten Protokolle ist nicht routbar: IP, IPX, SNA, DECNET

16. Wodurch unterscheiden sin in der Funktionsweise Transparente und Source-Routing Brücken?

17. Nennen Sie mindestens drei typische Funktion von Servern in Netzen

18. Wodurch unterscheidet sich Directory Services von einer einzelnen serverbezogenen Bindery?

19. Wie kann die Ausfallsicherheit von Servern im Hinblick auf Festplattenausfall verbessert werden? Nenne Sie 3 Möglichkeiten

20. Was ist ein Alias in Directory Services

21. Über welches Protokoll erfolgt in Novell Netzen die Steuerung von Remote Printern

22. Das Standardmanagement Modell der ISO sieht fünf funktionale Bereiche für Netzwerkmanagementaufgaben vor. Nenne Sie drei davon.

23. Wodurch unterscheidet sich im wesentlichen die Netzwerkadressierung in IPX bzw. TCP/IP Netzen.

24. Wie wird in IP und IPX Netzen verhindert, daß sich Pakete endlos im Netz befinden können

25. Wodurch unterscheidet sich die Kommunikation in SNA Netzen grundlegend von der in PC-Netzen

26. Erklären Sie die Funktionsweise eines Ethernet Switches.