Einführung Netzwerke 06.09.99

1. Geschichtliche Entwicklung

In den 70er Jahren dominierte bei Netzwerken eine hierachische Strukur, dies resultierte aus den damals typischen „Terminalnetzen“, in denen ein HOST viele „dumme“ Terminals (in Form von Bildschirmen oder Druckern) zu bedienen hatte. Somit war die Datenverarbeitung zentral (HOST) ausgerichtet. Erst mit Aufkommen der PC`s begann ein langsamer, aber unaufhaltsamer Wandel. Zunächst wurden diese Rechner, die damals noch seht teuer waren (ca. 25000 DM) als Stand- Alone Rechner betrieben oder, als Terminals an den HOST angebunden. Diese Vernetzung lief zunächst über Koaxial- Kabel oder als Anbindung an ein WAN (Wide Area Network). Ein WAN ist ein Netzwerk, dass grössere Entfernungen mit relativ geringer Übertragungsrate überbrückt und nicht auf den privaten Bereich des Netzeigners (z.B. eine Firma) beschränkt ist. WAN`s bedienen sich somit, um die entsprechende Reichweite zu erlangen der öffentlichen Netzte (z.B. Telefon).
Infolge des Booms der PC`s begann man die alten Hierachien in peer- to- peer Verbindungen umzubauen. Die dezentralisierung der Datenverarbeitung nahm seinen Lauf. In den 80er Jahren existierte dann bereits eine grossen Menge an verschiedenen Netzen, von denen das auch heute noch gebräuchlichste das LAN (Local Area Network) ist.

2. Lokale Netzte (LAN)

Das LAN ist, wie es der Name schon sagt, ein lokales Netzwerk. Damit ist die örtliche Begrenztheit gemeint. Ein LAN ist zumeist auf ein Firmengelände (vgl. Kreishaus) beschränkt und bedient sich in der Regel keiner öffentlichen Netzte, so wie das WAN es tut. Eine Definition aus einem Fachbuch beschreibt das LAN folgendermassen :“Unter einem LAN versteht man einen bertiebsinternen Verbund mehrerer Arbeitsplatzcomputer zu einem vernetzten, kommunikationsfähigen System.“ Diese Definition ist nicht falsch, aber sicher ausbaubar, denn was dort kurz umschrieben wird besitzt noch ein paar wichtige Eigenschaften mehr, besonders wenn man das LAN mit dem WAN vergleicht.
Neben der örtlichen Begrenztheit spielt besonders die hohe Übertragungsrate (mehrere Mio. Bits/sec) eine wichtige Rolle. Durch eine hohe Überragungsrate soll gerade in der heutigen Zeit effizienteres Arbeiten gewährleistet werden.
Natürlich gibt es noch weitere Punkte, die ein LAN beziehungsweise ein Netzwerk im allgemeinen ausmacht. Um ein Netzwerk aufzubauen braucht man zunächst einmal die rein physikalische Verbindung über Kabel, Netzwerkkarten, und ähnliches. Ebensowichtig ist ein Betriebssystem, das die einzelnen Rechner im Netzwerk agieren lässt und z.B. einen Datentransfer erst möglich macht. UNIX, WINDOWS NT und NOVELL sind wohl die bekanntesten dieser sogenannten Netzbetriebssysteme.
Um jedoch nun zum Beispiel Daten über das Netzwerk zu schicken, fehlt noch eine wichtige Komponente: Das Zugriffsverfahren. Ein Zugriffsverfahren regelt, welcher Rechner wann, um bei unserem Beispiel zu bleiben, senden darf (z.B. Token Ring). Diese Zugriffsverfahren sind zumeist streng geregelt, um ein Zusammenbrechen des Netztes zu verhindern, denn wenn jeder Rechner zu jeder Zeit auf das Netzwerk zugreifen würde, käme es zum Chaos.
Als letztes Merkmal, aber nicht unwichtigstes, eines Netzes sei hier die Topologie erwähnt. Dabei werden drei Topologien unterschieden:

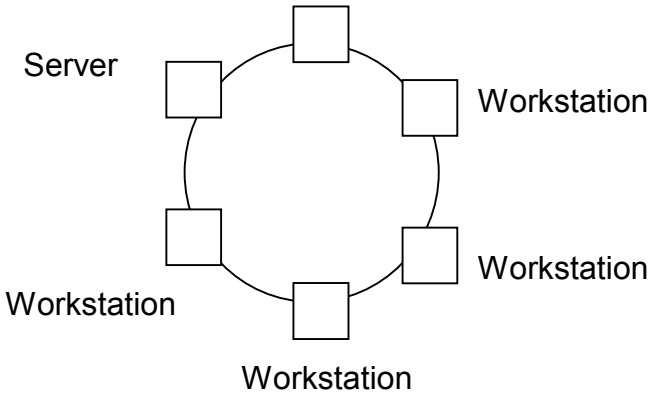
1. Ring: Bei einer Ring- Topologie sind die Rechner untereinander zu einem Ring verbunden. Das Netzwerkkabel bildet einen in sich geschlossenen Ring, wobei jeder Rechner, der an dem Ring angeschlossen ist einen eindeutigen Vorgänger und einen eindeutigen Nachfolger besitzt. Dabei werden Informationen von der sogenannten Quellstation in Richtung der Zielstation weitergeleitet.

Jeder Rechner überprüft nun, ob das Datenpaket für ihn bestimmt ist. Ist es das, so nimmt er es auf, ist es das nicht, so wird es weitergereicht. Solche eine Topologie nennt man auch Token Ring, weil der Zugriff über ein sogenanntes Token (Bitmuster) geregelt wird.

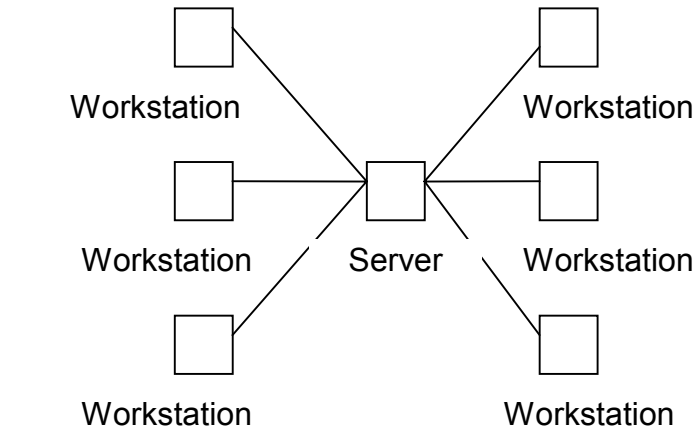
2. Stern: Die Sterntopologie wurde bereits bei Grossrechnern eingesetzt und wurde auf die heutigen PC`s übertragen. Charakteristisch ist, das alle Stationen sternförmig mit einem Netzwerkknoten (z.B. Server) verbunden sind. Somit laufen alle Informationen im Netz ausschliesslich und zentral über den Server/ Netzknoten. Die Leistung und das Verhalten eines solchen Netzwerkes hängt daher von der Anzahl der angeschlossenen Stationen und der Ausstattung (CPU, RAM, ...) des Servers ab.

3. Bus: Bei der Bus- Toplologie sind Server und Workstations an einem Kabelstrang angeschlossen. Diese Art Hauptleitung wird von allen angeschlossenen Geräten zur Informationsübertragung im Netzt genutzt. Jede Workstation kann mit jeder anderen Workstation kommunizieren, ohne dass der Server unbedingt erforderlich ist (peer- to- peer). Die Informationen können hier in beide Richtungen geschickt werden, allerdings kann immer nur eine Station den Bus in Anspruch nehmen. Die Kollisionsgefahr ist gross und wächst mit der steigenden Anzahl der angeschlossenen Geräte.

RING



STERN



Einführung Netzwerke (2)

1. Allgemeine Aufgaben von (lokalen) Netzen:

Die Aufgaben von Netzen lassen sich in drei Hauptunkte fassen. Zum einen ermöglichen Netze den Zugriff auf zentrale Daten und Ressourcen (Drucker, Festplatten, Anwendungen). Dieser Zugriff ermöglicht es dem User, zum Beispiel bei einem im Netz gespeicherten Veranstaltungskalender, immer „up- to- date“ zu sein, da eine zentrale Speicherung der Daten gegeben ist.
Desweitern ermöglicht ein Netz auch den Zugriff auf zentrale Rechenleistung, so können zum Beispiel rechenintensive Arbeiten über diese, im Netz bereitgestellte, CPU schneller erledigt werden.
Die letzte Aufgabe, die hier genannt werden soll, ist, dass der Austausch von Informationen auf elektronischem Wege überhaupt erst möglich gemacht wird. Dies sieht man zum Beispiel, bei Mailing-Verfahren, mit dem der tägliche Informationsaustausch schnell und einfach vonstatten geht.

2. Sterntopologie (bei Grossrechnern)

In der Sterntopologie (Grossrechner) läuft der Zugriff auf das Netz immer über den HOST. Dabei gibt es zwei Methoden, wie verfahren werden könnte::
Zum einen wäre es denkbar, dass alle angeschlossenen Geräte im Netz immer dann senden, wenn sie was zu senden haben, und der HOST sehen muss, wie er die Datenflut verarbeitet.
Zum anderen, das benutzte Verfahren, bei dem der HOST jedes Gerät einzeln, nacheinander „fragt“ , ob es etwas zu senden hat, beziehungsweise der HOST sendet etwas an ein Gerät und „fragt“ direkt im Anschluss daran, ob etwas zurückgesendet werden möchte.

Aufbau Sterntopologie Grossrechner GKD (klassisches Bild)

(vgl. Grafiken)

1. Der HOST ist über ein Parallelkabel mit einer sogenannten Steuereinheit, oder auch Clustercontroller, verbunden. Diese Steuereinheit sammelt die gesendeten Daten der Endgeräte und leitet sie, wenn die Abfrage des HOST`s kommt, an diesen weiter. Andersherum übernimmt sie die Daten vom HOST und leitet sie an die Endgeräte weiter.

2. Anstatt einer Steuereinheit kann auch ein sogenannter Communicationcontroller, von IBM 3745 genannt, mit dem HOST verbunden sein. Dieser leitet die Daten über WAN- Verbindungen (z.B. DatexP) nach draussen (z. B. Stadt Marl) weiter oder bekommt von aussen Daten, die er zum HOST weiterleitet, wenn er durch das Zugriffsverfahren angesprochen wird. An die WAN- Verbindungen angeschlossen sein können weitere 3745er, die wiederum mit einem HOST verbunden seien können oder Steuereinheiten, die Endgeräte bedienen.

3. Ein Communicationcontroller kann aber auch einen Zugang zum LAN haben, das wiederum mit einem anderen LAN verbunden ist, welches an eine Steuereinheit angeschlossen ist. Somit kann er Daten direkt an das LAN verschicken, die von der Steuereinheit den einzelnen Endgeräten zugeordnet werden, oder die gebündelten Daten von der Steuereinheit an den Communicationcontroller schicken.
Dabei kann auch der HOST eine Verbindung zum LAN haben, wobei er sich entweder, genauso, wie der Communicationcontroller, der Steuereinheit bedienen kann, oder der im LAN befindlichen ServerGateways. Diese ServerGateways besitzen dieselbe Funktionalität wie eine Steuereinheit und können nicht nur vom Host, sondern auch von dem Communicationcontrollern oder anderen

Steuereinheiten angesprochen werden. Natürlich funktioniert diese Kommunikation auch in entgegengesetzer Richtung, von den Endgeräten über den ServerGateway zu anderen ServerGateway`s, Communicationcontrollern, Steuereinheiten oder HOST`s.

4. Die Verbindung der zwei LAN`s läuft, stark vereinfacht, über Router.

Ausnahmen: Auch normale PC`s können, in eingeschränktem Maße, die Funktionalität von ServerGateway`s übernehmen. Dies ist über die entsprechende Konfiguration der Emulation möglich.

Einführung Netzwerke (3):

1. Bustopologie

In der Bustopologie sind mehrere Geräte an ein passives Medium (z.B. Kabel) angeschlossen, wobei die jeweiligen Enden mit einem Abschlusswiderstand terminiert werden.
Der Zugriff auf das Netz wird wie folgt geregelt. Eine Nachricht wird in beide Richtungen des Netzes geschickt, da das Sendegerät nicht weiß, an welcher Stelle im Netz sich der Empfänger befindet. Er kennt nur seinen „Namen" beziehungsweise seine „Adresse". Dabei wird die Nachricht von jeder Station im Netzt empfangen, und überprüft, ob diese für sie bestimmt ist (näheres siehe Zugriffsverfahren).
Problematisch an dieser Topologie ist, daß es sich um ein „shared Lan" handelt. Das heißt, je mehr Geräte angeschlossen sind, desto geringer wird für den einzelnen die nutzbare Ressource.

2. Ringtopologie

Auch diese Topologie wird als „shared LAN" bezeichnet, wobei sich der negative Effekt, der Ressourcenteilung, natürlich auch hier feststellen läßt. Bei der Ringtopologie bilden die Geräte, an das passive Medium angeschlossen, einen Kreis. Wird hier eine Nachricht versendet bekommt jeder die Nachricht und überprüft ob sie für ihn bestimmt ist.

Zusammenfassung:

Die bei einem großen Netzwerk benutzte Verkabelung entspricht mittlerweile fast immer einer Sterntopologie, die zwar aufwendig zu verlegen, dafür aber sehr flexibel ist. Logisch wird eine Ringtopologie meist durch die Hub`s abgebildet (vgl. hausinterne Topologie).

3. Hub

LAN- Verteilungen und LAN- Konzentrationen unterschiedlicher Topologien aufzubauen, ist die generelle Aufgabe von Hub`s. Dabei belegt man in der Regel einen Hub nie voll, denn der Hub ist eine intelligente Maschine, die viele Aufgaben übernimmt und bei voller Belegung steigt das Risiko eines Ausfalls. Desweitern bilden Hub`s die Topologie des Netztes logisch ab.

4. Übertragungsmedien

Bei Netztwerken werden zwei verschiedene Übertragungsmedien benutzt. Zum einen Kupfer, mit elektrischer Datenübertragung, zum anderen Glasfaser, mit optischer Datenübertragung. Die Vor- und Nachteile der beiden Medien werden im folgenden näher erläutert.

4.1. Kupfer

Bei Kupfer werden zwei verschiedene Kabelarten unterschieden: Koaxialkabel und Twisted-Pair-Kabel.

a. Koaxialkabel

Koaxialkabel sind wie folgt aufgebaut (von innen nach aussen): Kupferleiter➔ Isolator➔ Kupferleiter➔ Isolator➔ Gummimantel. Das Problem ist, daß es beim Koaxialkabel unterschiedliche

Endwiderstände benutzt werden. So wird für ein Koaxialkabel eines Fernsehers (75 Ω) z. B. ein anderer Widerstand benutzt, als bei einem Koaxialkabel für die Datenübertragung (50 Ω).

b. Das Twisted- Pair- Kabel besteht aus 4 verdrillten Kupferadernpaaren. Es gibt zwei Arten von Twisted- Pair- Kabeln, die unterschieden werden:

a.a. UTP (Unshielded Twisted Pair) ist die Form, bei der die einzelnen Kupferadern nicht gegeneinander abgeschirmt sind. Dabei können durch die entstehenden elektromagnetsichen Felder Störungen auftreten. Kurios ist jedoch, daß telefonieren nur mit UTP möglich ist. UTP sind billig und leicht zu verlegen, dazu kommt, daß die Qualität inzwischen so gut ist, daß kaum noch Störungen auftreten.

a.b. STP (Shielded Twisted Pair): Hierbei sind die verdrillten Kupferadern gegeneinander abgeschirmt, so daß eine fast störungsfreie Übertragung möglich ist. Diese Kabel sind dementsprechend teurer, als UTP- Kabel.

4. 2. Lichtwelle (Glasfaserkabel)

Glasfaserkabel sind deutlich teurer als Kupferkabel. Hinzu kommt die absolute elektische Störungsfreiheit, weil bei einer optischen Übertragung elektromagnetische Störungen (z. B. Gewitter) keine Rolle spielen. Auch muß das optische Signal nur ungefähr alle 30 km (bei Single Mode) „aufgefrischt“ werden und die Übertragungsgeschwindigkeiten sind extrem hoch (Standard: 625 Mbit/s).

5. Wo setze ich welches Medium ein?

Bei der Frage , wo ich am besten welches Medium einsetze sollte man sich zunächst die Aufteilung des Geländes, in Primär-, Sekundär- und Tertiärbereich verdeutlichen. Der Primärbereich bezeichnet das Gelände zwischen Gebäuden, hier werden Glasfaserkabel verlegt, um nicht durch elektromagnetische Störungen beeinträchtigt zu werden. Der Sekundärbereich bezeichnet die Steigleitungen (von Etage zu Etage) auch hier werden Glasfaserkabel verlegt, um den elektromagnetischen Störungen, die z.B. durch Stromleitungen enstehen können, entgegenzuwirken. Im Tertiärbereich werden die Kabel vom Etagenverteiler zu den Büros verlegt. Hierbei werden alternativ Glasfaserkabel oder Kupferkabel verlegt. Welches Kabel genau verlegt wird, ist abhängig davon, welche Anforderungen an das Netz gestellt werden und welche Ergebnisse die Kosten-Nutzen- Analyse liefert.

6. Zugriffsverfahren

Es gibt eine Vielzahl von Zugriffsverfahren für Netzwerke. Hier sollen jedoch nur die beiden wichtigsten, Token Ring (Token Passing) und Ethernet, und noch ein weiteres, ATM (Asynchonious Transfer Mode), erläutert werden.

6.1. Ethernet (CSMA/CD- carrier sense multiple access/ collision detection)

Das Ethernet entspricht in seinem Verfahren der Norm IEEE 802.3 ist aber nicht damit gleichzusetzen. Ethernet wird in Bustopologien eingesetzt.

Das Verfahren arbeitet wie folgt: Wenn eine Station etwas senden möchte „horcht“ sie, ob Traffic auf der Leitung ist. Ist dem so, so wartet die Station, bis kein Traffic mehr ist und sendet dann ihre Nachricht in beide Richtungen des Busses. Ist kein Traffic auf der Leitung, sendet sie sofort. Beim Empfangen bekommt jede Station das Datenpaket und entscheidet, ob es für sie bestimmt ist. Probleme entstehen, wenn zwei oder mehrere Stationen senden wollen und dann, wenn kein Traffic ist, gleichzeitig ihre Nachrichten abschicken. Hierbei kommt es zur Kollision. Die Stationen bemerken die Kollision und zählen dann ,nach einem speziellen Algorhitmus, einen Countdown ab. der jeweils unterschiedlich ist, und senden dann.
Je mehr Geräte jedoch angeschlossen sind, desto mehr Traffic und desto mehr Kollisionen gibt es, so ist es nicht ersichtlich, wann man seine Nachricht senden kann, und wann sie ankommt. Dies ist vollkommen vom Zufall abhängig. Da Ethernet jedoch im Gegensatz zu Token Ring wesentlich billiger ist (z.B. Adapterkarte Ethernet: ca.100 DM/ Token Ring ca. 600 DM), wird es hauptsächlich eingesetzt. Dabei umgeht man die Kollisionsgefahr dadurch, daß pro Bus nur noch ein Gerät angeschlossen ist. Die einzelnen Segmente werden dabei über Switches verbunden.

6.2 Token Ring/ Token Passing

Dieses Verfahren entspricht der Norm IEEE 802.5.

Dieses Verfahren wird, wie der Name schon sagt, bei Ringtopologien eingesetzt. Die Station, die sich als erste im Netz anmeldet wird zur Monitorstation, die für die Überwachung des Tokens (Bitmuster) zuständig ist. Sie schickt das erste Token los. Wenn ein Token verschwindet, was schon mal vorkommt, so bemerkt die Monitorstation das Verschwinden, weil das Token nach einem bestimmten Zeitintervall wieder „vorbeikommen“ müsste. Dann sendet sie ein neues Token. Taucht einmal ein Token mehr auf, so wird dieses von der Monitorstation „gefressen“.
Das Token wandert so im Ring von einer Station zur nächsten. Will eine Station etwas senden, so „schnappt“ sie sich das Token, markiert es als „besetzt“ und hängt seine Nachricht daran. Dann schickt sie es weiter. Gelangt das Token mit der Nachricht zum Empfänger, nimmt dieser die Nachricht entgegen und schaltet es zusätzlich noch auf „empfangen“. Der eigentliche Sender der Nachricht setzt es dann wieder auf „frei“ und schickt es weiter. Ist kein „empfangen“ gesetzt, so schickt er die Nachricht erneut.
Desweiteren gibt es noch ein sogenanntes Prioritäts- Token. Hierbei kann ein besetztes Token „reserviert“ werden. Ist es dann wieder beim Sender, wird es nicht auf frei gesetzt, sondern sofort an die entsprechende Station gesendet. Diese Funktion ist den Administratoren vorbehalten.

Der Vorteil dieses Verfahrens ist, daß es zu keinen Kollisionen kommt, jeder nacheinander einmal drankommt und somit weiß, wann er senden kann bzw., wann seine Nachricht ankommt. Ausserdem kann das Netz zu 80- 90% ausgelastet sein, während ein Ethernet ab 50- 60% Belastung zumeist zusammenbricht, d.h. daß
keine ordentliche Datenübertragung mehr möglich ist.

Einführung Netze (3.1)

Exkurs: Kabel

Die Verkabelung von Netzwerken richtet sich nach der Norm EN 50173. Sie beschäftigt sich mit der „Strukturierten Verkabelung“ von Netzen, um so effizient wie möglich zu verkabeln.

Bei der Verkabelung ist immer auch die maximale Wegstrecke zu beachten, die mit dem Kabel überbrückt werden soll. Diese bezeichnet die technische Grenze des Kabels, nämlich die Strecke, über die es verlegt werden kann, ohne das ein Verstärker das Signal „auffrischen“ muss. Hierbei gilt bei einem Glasfaserkabel Single Mode 30 km, einem Glasfaserkabel Multiple Mode 2- 3 km und bei einem Twisted- Pair- Kabel 100 m. Wobei man bei einem TP immer sagt, daß die Entfernung zwischen Patchfeld und Anschlussdose maximal 90 m sein darf, damit für die Restverkabelung zu Hub/ PC genügend Kabellänge überbleibt.

Die meisten Netze werden, im Tertiärbereich) Sternförmig verkabelt, weil diese Verkabelung sehr flexibel ist. So kann in einem Büro zum Beispiel gleichzeitig ein Token Ring und ein Ethernet angeschlossen sein. Auch die Verlegung des Kabels vom Patchfeld zur Anschlussdose ist sehr aufwendig, dafür aber extrem flexibel.

Unterschieden werden die TP- Kabel in UTP und STP, wobei sie unterschiedliche Wellenwiderstände (elektrische Kenngrösse) besitzen. So liegt der Wellenwiderstand bei einem UTP bei 100 Ω +/– 15% und bei einem STP bei 150 Ω +/– 15%.

Dabei werden die Kabel, um sie besser zu kategorisieren, in verschiedene Klassen und Kategorien eingeteilt. Die wichtigsten sind die Linkklassen, die die Frequenz der Übertragung bestimmen, und zum anderen die Kategorien, in denen die Kabel über bestimmte elektrische Eigenschaften eingeordnet sind. Zu diesen Eigenschaften zählen: die maximale Frequenz, der Wellenwiderstand, die maximale Dämpfung und die Nebensprechdämpfung. Dieser Standard ist besonders wichtig für die Hardwarehersteller, die sich bei der Entwicklung von z.B. Hub`s an diesem Standard orientieren können, um die Einstellungen der Hub`s zu optimieren.
Der benutze Standard ist im Moment Kat. 5, bei dem die Frequenz <= 100MHz ist. Ein neuer Normentwurf beschäftigt sich mit Kategorie 6 Kabeln, die bis zu 600 MHz schaffen (z.B. für ATM 622 MBit /s).
Diese Kategorie 6 Kabel werden schon heute bei Neuverkabelungen benutzt, um die zukünftigen Entwicklungen (z.B. GigaBit- Ethernet) schnell und problemlos einführen zu können.

Als Anschlusskomponenten sind hier noch kurz das Patchfeld und die RJ45 (Anschlussdose) genannt, die vollabgeschirmt sind.

Einführung Netze (4):

1. ATM (Asynchonous Transfer Mode)

Für das ziemlich neue Übertragungsverfahren ATM gibt es noch keine Normen. Die Möglichkeit die ATM eröffnet ist, Daten, Sprache (z.B. Telefon) und Bilder (z.B. TV) über dieselbe Leitung zu transportieren.
ATM ist ein verbindungsorientiertes, vermittendes Verfahren. Es funktioniert folgendermaßen:
Der Sender „klopft“ beim gewünschten Empfänger an. Hier gibt es jetzt drei Möglichkeiten: Entweder „steht schon jemand in der Tür“ und überträgt Daten an den Empfänger, oder der Empfänger „öffnet“ nicht oder, der Empfänger „öffnet“. Ist die „Tür offen“, das heißt, die Verbindung hergestellt, so fragt der Sender, ob der Empfänger der richtige ist, den es könnten ja auch mehrere Empfänger „in dem Haus wohnen“, stimmt der Empfänger, so wird er „gefragt“, ob er das (Daten-) Paket haben will. Der Empfänger will, und der Datentransfer kann beginnen.
Dieses Verfahren hat den Vorteil, daß nur Sender und Empfänger um die Kommunikation wissen und diese die Leitung dann für sich alleine haben.
Dem Benutzer wird eine dedizierte Verbindung mit garantiert hoher Bandbreite zur Verfügung gestellt (bis zu 625 MBit/s). Damit gibt es kein Shared- Lan mehr und die Ressource ist voll nutzbar.
Das Verfahren transportiert die Daten in Zellen mit einer festen Größe (48 Byte Netzdaten, 6 Byte Header) und ist sowohl im LAN, als auch im WAN einsetzbar. Die Übertragungsgeschwindigkeiten sind flexibel gehalten.
Protokolle wie TCP/ IP und IPX, entwickelt für Ethernet beziehungsweise Token Ring- Verfahren, können über einen sogenannten LAN- Emulator auch für ATM genutzt werden.

2. Koppelelemente

A. Repeater:

Der Repeater wird vorallem im Ethernet eingesetzt. Seine Aufgabe besteht darin die Signale „aufzufrischen“, wenn sie die maximale Wegstrecke zurückgelegt haben. So kann man zum die Kabellänge und damit die Übertragungsstrecke erhöhen.

B. Bridge:

Eine Bridge verbindet zwei gleichartige Netze (z.B. Ethernet- Ethernet). Hierbei gibt es einmal Local Bridges, die an beiden Seiten direkt mit dem LAN verbunden sind, und Remote Bridges, die auf der einen Seite direkt mit dem LAN verbunden sind, und auf der anderen Seite über z.B. eine WAN-Verbindung mit einer anderen Bridge, die ebnfalls an ein LAN angeschlossen ist. Dabei wandelt sie das LAN- zugriffsverfahren in ein WAN- Zugriffsverfahren und auf der anderen Seite wider in ein Lan-Zugriffsverfahren.
Bridges arbeiten auf der Grundlage von MAC- Adressen (Medium Access Control). Jede Netzwerkkarte besitzt eine weltweit eindeutige Adresse, die man (bei Token Ring- Adapterkarten) auch überschreiben kann. Zu beachten ist jedoch: Die Adressen in einem Netzwerk müssen eindeutig sein!!!
Die meisten Protokolle haben ihre eigene interne Adresse (z.B. IP), eine Ausnahme wäre zum Beispiel SNA.

Die Bridge arbeitet folgendermaßen:

Alle Informationen, die über das Netz laufen, werden von der Bridge gesammelt und daraufhin überprüft, ob sie weitergeleitet (an das andere Netz) werden, oder nicht. Dazu muss die Bridge die Empfängeradresse kennen, das heißt, wissen in welchem Netz der Empfänger sitzt. Hierbei gibt es zwei Verfahren: transparent Brigde und source Routing.
Beim „transparent Bridge“ merkt sich die Bridge, wer wo sitzt. Kennt sie den Empfänger einmal nicht, dann wird die Nachricht auf jeden Fall sicherheitshalber übertragen. Ansonsten wird nur das gesendet, was an einen Empfänger auf der anderen Seite geht.
Beim source Routing sagt der Absender, wohin die Nachricht geht. Dabei schickt er ein „Find“ los. Das Find wird in alle angeschlossenen Netze gesendet. Landet es beim gesuchten Empfänger, so wird es auf dem Weg, das es gekommen ist zurückgeschickt. Dieser Weg wird als der kürzeste zwischen diesen beiden Stationen behalten und ab dann immer für die Kommunikation der beiden Geräte benutzt.
Bei beiden Verfahren gilt jedoch: Keine Nachricht darf über mehr als sieben Bridges gehen, sonst verschwindet sie.
Bei einer Bridge sind die verbundenen Netze nicht logisch voneinander getrennt.

C. Router:

Ein Router arbeitet im Gegensatz zur Bridge auf der Ebene der Protokolladressen. Daher müssen sie alle im Netz verwendeten Protokolle im Netz kennen. Diese Eigenschaft nennt man auch „Protokollabhängigkeit“. Auch ist hier das Verbinden von unterschiedlichen Netzen (Token Ring-Ethernet) möglich. Router kommunizieren in der Regel über eigene Protokolle untereinander und tauschen sogenannte „Routing Tables“ aus. In diesen Routing Tables stehen im Grunde genommen „Wegbeschreibungen“, wie man am schnellsten die Daten von A nach B schickt. Router untersuchen jedoch nicht jede Nachricht, die im Netz gesendet wird. Der Absender muss dem Router mitteilen, das er etwas zu übertragen hat. Damit landet nur das beim Router, was wirklich weitergeleitet werden muss. Ein weiterer Unterschied zur Bridge ist, daß der Router die verbundenen Netze logisch trennt und in Sub- Netze unterteilt.
Wie schon beschrieben verwendet der Router die protokolleigenen Adressen. Bei SNA ist dies nicht möglich. Daher kann man hier keinen Router einsetzen. Stattdessen kann ein Brouter, ein intelligentes Gerät oder Programm, benutzt werden, das die Daten in ein IP- Protokoll „verpackt“ und dann sendet. Auf der anderen Seite wird das Paket dann wider „entpackt“.

D. Gateway:

Ein Gateway kann im Gegensatz zum Router Protokollübergänge realisieren. Dabei fungiert es praktisch als Übersetzer.

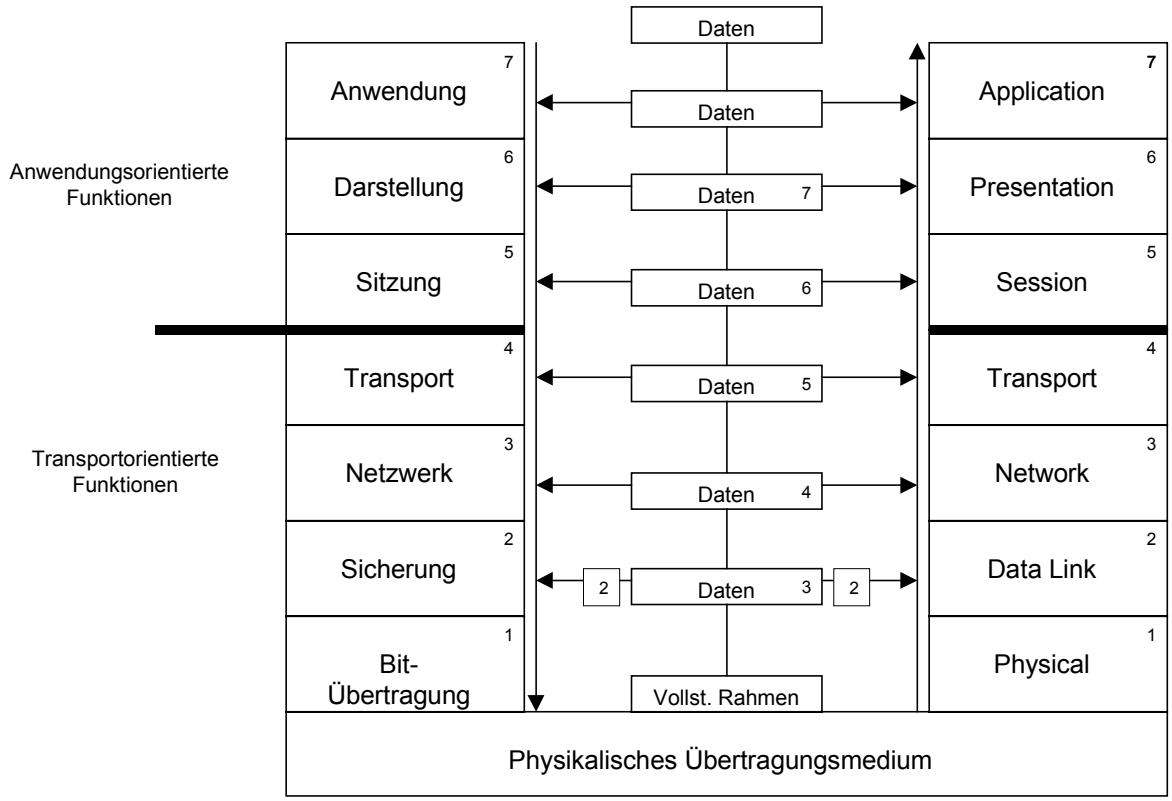
E. Switch:
Ein Switch besitzt die gleiche Funktionalität wie ein Router und eine Bridge, jedoch ist ein Switch nicht auf Softwarebasis realisiert, wie die beiden anderen, sondern hardwaremäßig. Damit ist ein Switch viel schneller und die Kosten (pro Port) billiger.
Ausserdem besitzt es Error Decovery.

Einführung Netzwerke (5):

1. Protokolle

Sender und Empfänger in einem Netzwerk müssen über eine gemeinsame Sprache verfügen, um kommunizieren zu können. Diese „Sprache“ nennt man auch Protokoll. Besitzen die Kommunikationspartner unterschiedliche Protokolle, so muss von einem Gateway oder Router das Protokoll des jeweiligen anderen „übersetzt“ werden. Möglich wäre auch, das die Kommunikationspartner jeweils über eine dritte, gemeinsame Sprache miteinander kommunizieren.
Aus dieser Problematik heraus wurde die Schaffung eines enheitlichen Protokoll- Standards gefordert. Die ISO (International Standardisation Organisation) entwickelte daraufhin das OSI (Open System Interconnection) Protokoll und das OSI Referenzmodell. Da das OSI- Protokoll sich jedoch als sehr komplex und zu teuer herausstellte, konnte es sich nicht als Standard durchsetzen, heute gilt als Standard das TCP/ IP. Das OSI- Referenzmodell bleibt jedoch von grosser Bedeutung.
Bei diesem Referenzmodell wird der Kommunikationsprozess in 7 Schichten unterteilt.

2. OSI Referenzmodell



Die hereinkommenden Daten werden von der siebten Schicht entgegengenommen und von Schicht zu Schicht „gereicht“. Dabei hängt jede Schicht spezifische Informationen an das Datenpacket. Die zweite Schicht hängt sowohl etwas dahinter (Trailer), als auch davor (Header). Was für Informationen das sind, und welche Aufgaben die Schichten im einzelnen übernehmen wird im folgenden erklärt.

a. Die Schichten

a.a. 1.Schicht: Physical Layer:

Der Physical Layer überträgt Bitströme über die Datenverbindung. Geregelt werden dabei die mechsnische Definition (z.B. welches Kabel), die elektrische Definition (z.B. welche Spannung ist 0, welche 1) und die funktionale Definition (z. B. Vollduplex).

a.b. 2.Schicht: Data Link Layer:

Der Data Link Layer ist für die zuverlässige Übertragung der Daten zuständig. Dazu gehören unter anderem das Bilden einer Prüfsumme, mit der Übertragungsfehler festgestellt werden können, sowie das Erkennen und Beseitigen von Übertragungsfehlern. Desweitern werden von dieser Ebene aus die Verbindungen aktiviert, überwacht und deaktiviert.
Die zu übertragenen Daten werden zu Frames verpackt. Dazu werden die Daten je nach Grösse entweder zusammengepackt oder unterteilt; auf der Empfängerseite werden sie dann wieder „entpackt“. Damit bei diesem Pakettransport nicht ein späteres Paket zuerst ankommt wird von diesem Layer auch noch die Steuerung der Reihenfolge der Datenpakete und die Synchronisation der verbundenen Einheiten übernommen.

a.c. 3.Schicht: Network Layer:

Dieses Layer tritt nur dann in Aktion, wenn ein Netzwerk existiert. Hierbei wird der Austausch von Datenpaketen zwischen nicht direkt verbundenen Stationen gesteuert. Dabei gibt es drei Möglichkeiten:
1. Die Leitung wird durchgeschaltet (z.B. Wählen) , dies ist jedoch nicht im OSI verankert.
2. ein virtueller Kanal wird geöffnet (vgl. ATM)
oder
3. die Daten werden einfach losgeschickt (verbindungslose Kommunikation)

Die beiden letzen Verfahren arbeiten nach dem „Store & Foreward“- Prinzip. Dabei werden die Daten auf jeder passierten Bridge/ Gateway/ Router gespeichert und dann weitergeleitet.
Zu den weiteren Aufgaben des Network Layers gehören die Identifizierung der Knoten(z.B. über die IP- Adressen), der Auf-/ Abbau der logischen Verbindung, die Wegsteuerung (Routing) und die Flußsteuerung („Staumelder“).

Einführung Netzwerke (5.1)

1. Das OSI- Referenzmodell:

1.1 Transportorientierte Schichten

a. vierte Schicht: Transport Layer:

Das Transport Layer bildet die Nahtstelle zwischen den transportorientierten und den anwendungsorientierten Schichten des OSI . Ihre Aufgabe besteht darin, den höheren Schichten die Möglichkeit zu bieten, Nachrichten zwischen logischen Benutzern zu übertragen. Dabei werden mit "logischen Benutzern" alle kommunikationsfähigen Einheiten bezeichnet. Gekennzeichnet werden logische Benutzer durch Transportadressen.
Des weiteren findet eine "Vorverpackung" der Daten statt und auf der Gegenseite das Zusammensetzen dieser gepackten Daten, sofern dieses noch nicht geschehen ist. Auch die Steuerung des Datenflusses findet als Vorstufe in dieser Schicht statt.

1.2 Anwendungsorientierte Schichten:

a. fünfte Schicht: Session Layer:
Die Aufgabe des Session Layers ist die Aufrechterhaltung eines Dialoges beziehungsweise einer Sitzung , selbst, wenn mal vorübergehend das Transportsystem ausfällt. Dabei ist mit Dialog/ Sitzung die Verbindung von zwei Anwendungen, die miteinander, in einem Netzwerk, kommunizieren.
Das Session Layer besitzt dabei mehrere Kommunikationsformen:

- Two- way Simultaneous Interaction (entspricht Duplex)
- Two- way Alternate Interaction (entspricht Halbduplex)
- One- way Interaction (entspricht Simplex)

b. sechste Schicht: Presentation Layer:
Das Presentation Layer ist zuständig für die Darstellung der Nachrichtenform.. Dabei müssen die Nachrichten in ein gemeinsame bekannte Darstellungsart umgesetzt werden. Typische Funktionen der sechsten Ebene sind dabei Remote Job Entry Funktion, Terminalemulation oder Datenübertragung.

c. siebte Schicht: Application Layer:
Das Application Layer ist das Bindeglied zur eigentlichen Anwendung. Diese Ebene ist aus einer Reihe von Protokollen zusammengesetzt, die sich ständig erweitern. Wichtige Netzwerkanwendungen, die in dieser Schicht ablaufen sind zum Beispiel FTAM (File Transfer Access and Management), JTM (Job Transfer and Manipulation), Virtual Terminal, X400 und X500.

Aufbauend auf dem OSI- Referenzmodell wurde von der IEEE- Organisation ein Standard entwickelt, der die unteren drei Schichten des OSI- Modells abdeckt. Dabei entsprechen:
Network Layer - Higher Layer Interface (IEEE 802.1)
Data Link Layer- Logical Link Control, Medium Access Control
Physical Layer- Physical Layer

2. File Transfer
Es gibt unterschiedliche Formate beziehungsweise Codierungen von Zeichen. Darunter fallen zum Beispiel ASCII (unter UNIX, DOS und WIN X, dabei ist WIN X nicht identisch mit dem DOS-Zeichensatz) und EBCDIC (unter MVS, OS/ 400).
Das Problem, das sich beim File Transfer ergibt ist, dass die Zeichen umgestellt werden müssen. Das ist besonders bei den Sonderzeichen nicht ganz einfach.

a. Filetransfer mit dem HOST:

In der GKD werden drei verschiedene Verfahren für den File Transfer mit dem HOST benutzt.

- TSO (IND$FILE): Dieses Verfahren kann nur vom PC (Client) aus angestoßen werden. Der Nachteil ist, das man eine relativ ungesicherte Übertragung hat, entweder der Transfer funktioniert, oder er funktioniert nicht.
- FTP: Der Transfer kann von beiden HOST und Client angestoßen werden. Es gibt von FTP eine Client und eine Server- Variante, wobei der HOST beide hat. FTP hat den Vorteil, das es schneller ist als TSO.
- XCOM: ist ein File- Transfer- Produkt, das hauptsächlich für UNIX- Maschinen genutzt wird. Auch hier können beide Parteien den Transfer einleiten. Vorteilhaft ist die bessere Steuerung (z.B. wann übertrage ich) und die gute Überwachung des Transfers. Dabei werden die Daten (die in Paketen geschickt werden) bei einem gestörten Transfer nicht noch mal vollständig übertragen, sondern nur die Pakete, aber dem gestörten.

3. Betriebssysteme

Betriebssysteme verwalten Ressourcen. Sie sind die Basis für Anwendungen und machen die Hardware für die Anwendungen transparent. Außerdem vermitteln sie zwischen Hardware und der Anwendung.

Hardwareelemente	**Betriebssystemaufgabe**
CPU	Verteilung der Leistungen Konfliktfreier Ablauf
Netzwerk	Bereitstellung der Schnittstelle Bereitstellung der Netzdienste
Speicher (RAM)	Auslagerungsdatei Verteilung der Leistung Konfliktfreier Ablauf
I/ O	Spooling
HD	Bereitstellung Dateisystem

a. Betriebssysteme im Vergleich:

System	**Stabilität**	**Client-Server**	**Multitasking**	**Multiuser**	**Benutzer/ Sicherheit**	**Bemerkung (GKD bez.)**
Win 3.x/ 95/ 98		C	-	∅	+/ -	
UNIX	X	C/ S	+		+/ +	Für GTIS
OS/ 2	X	C	-/ +	∅	+/+	
WIN NT	X	C/ S	+	∅	+/ +	Flexibel
Novell Netware	X	S	+ ~	∅	∅	Noch eingesetzt
OS/ 390	X	S	+	+	+/ +	

Einführung Netzwerke (7):

1. Firewall (allgemein):

Firewalls sind Netzwerkkomponenten, die ein internes Netzwerk eines Betriebes (Intranet) mit einem öffentlichem Netz verbinden. Dabei wird ein gesichertes Netzwerk (Intranet) mit einem ungesicherten Netzwerk (z. B. Internet) verbunden.
Der Begriff Firewall wird primär in Verbindung mit dem Internet verwendet. Die Aufgabe von Firewalls ist es, die Sicherheit im internen Netz zu erhöhen. Dazu gehören: ein möglichst ungestörter Zugriff auf das öffentliche Netzwerk, die Verhinderung eines unberechtigten Zugriff auf das eigene Netzwerk, die Authentifizierung und Identifikation sowie die Datenverschlüsselung . Eine Firewall stellt daher den einzigen gesicherten Zugang des eigenen Netzes zum öffentlichen Netzwerk dar.
Sie besteht in der Regel aus mehreren Hard- und Softwarekomponenten, die individuell konfiguriert werden können. Durch die Konzentration des Zugangs auf eine einzelne Komponente werden die Überwachungs- und Kontrollfunktionen vereinfacht.
Prinzipiell unterscheidet man drei Arten des Zugangs: die Packet -Filterung, das Circuit Relay und den Application Gateway . Die Packet- Filterung ist die einfachste Firewall- Konfiguration bei der die Datenpakete anhand einer vorhandenen Tabelle analysiert und transferiert werden. Das Circuit-Relay- Konzept arbeitet mit einem Subnetz und zwei Routern , einem externen und einem internen Router und einem Host als Verbindungspartner über den die Kommunikation abläuft. Die sicherste aber auch aufwendigste Alternative eines Firewalls stellt der Application Gateway dar, der hinreichende Sicherheitsmechanismen realisiert.
Firewall- Systeme arbeiten auf den Schichten 2 bis 7 des OSI- Referenzmodells. Im Internet wird diese Technik in Form von Security- Firewalls eingesetzt; zum Schutz eines firmeneigenen Netzwerks, einem Intranet , gegen unberechtigtem Zugriff. Ein möglicher Zugang kann von der entsprechenden Firma durch einen Proxy- Server bereitgestellt werden. Bei den Zugriffskontrollsystemen von Firewalls unterscheidet man den Verfahren nach die Datenpaket-Filterung, das Circuit- Relay und den Application- Gateway. Alle drei Funktionalitäten setzen auf unterschiedlichen Schichten auf und verbinden das Internet mit dem firmeneigenen Netzwerk. So ist die Paketfilterung eine Funktion der Vermittlungsschicht , das Circuit- Relay eine Funktion der Transportschicht und das Application- Gateway umfaßt alle Schichten und setzt auf der Anwendungsschicht auf.

2. Firewall (GKD):

In der GKD ist die Firewall hardwaremässig realisiert. Dabei sichern zwei "Paketfilter" und ein Proxy-Server das Intranet gegen das Internet ab.

3. SSL (SecuritySoketLevel):

Trotz der Firewall gibt es noch weitere Sicherheitsrisiken, bei der Anbindung des Intranets an das Internet. Hierbei ist besonderes Augenmerk auf die Übertragung von Dokumenten zu richten. Eine Email zum Beispiel kann von jedem im Internet angesehen werden, der über die entsprechenden Kenntnisse verfügt. Um hierbei die Übertragung gegen Angriffe abzusichern, wird SSL eingesetzt. Dabei werden die Daten vom Internetanwender über einen gemeinsam bekannten Schlüssel kodiert und vom WWW- Server der GKD dekodiert und im Intranet an den Empfänger verschickt. Diese Methode ist sicherer als die unverschlüsselte Übertragung, aber schützt noch nicht vor angriffen an sich. Da die Dokumente unverschlüsselt auf dem WWW- Server liegen, kann durch einen Angriff auf den WWW- Server dessen Sicherheit überwunden werden, und der Angreifer hat zugriff auf alle Daten.

4. Digitale Signatur:

Um das Sicherheitsrisiko bei der Datenübertragung zwischen Internet und Intranet weiter zu minimieren wird eine Digitale Signatur eingesetzt, die eine sogenannte "Ende zu Ende Sicherheit" besitzt. Hierbei hat jeder Anwender einen eigenen Schlüssel. Dieser Schlüssel liegt sowohl beim Empfänger, als auch beim Sender vor. Werden Daten verschickt, so werden sie mit dem Schlüssel des Empfängers kodiert, damit nur dieser die Daten nutzen/lesen kann. Dabei werden die Datenpakete zwar auch auf dem WWW- Server zwischengespeichert, liegen dort jedoch verschlüsselt vor.

Einführung Netzwerke (8):

1. Netzwerkmanagement:

Die Aufgabe des Netzwerkmanagements ist es, die Netzwerkkomponenten zu überwachen, um früh auftretende Probleme zu erkennen und ihnen vorzubeugen und längerfristig gesehen, eine hohe Verfügbarkeit der Komponenten zu garantieren.
Als Netzwerkkomponenten gelten hier: Übertragungswege (Verbindungen), Router, Switch- Systeme, Hub`s, Server und Workstations.

Zur Überwachung werden dabei drei Verfahren eingesetzt:
A. SNMP- Management
B. RMON- System
C. LAN- Analyse

Zu A.
SNMP (Simple Network Management Protokoll)
Dieses Verfahren hat sich seit seiner Entwicklung (ende der 80er) als Standard etabliert. Es basiert auf dem Übertragungsprotokoll UDP, um die Netzlast nicht zu erhöhen.
In der Praxis gibt es eine sogenannte Netzwerkmanagement- Station und auf den überwachten Geräten den sogenannten SNMP- Agent, der installiert werden muss. Die Station kommuniziert mit diesem SNMP- Agent über bestimmte Befehle, die in konfigurierbaren Zeitabständen abgesetzt werden.
Es gibt dabei drei Basisbefehle, die von der Management- Station ausgehen:
1. "get", holt Informationen vom SNMP- Agent
2. "get next", holt Informationsketten vom SNMP- Agent
3. "set", verändert die Parameter

Des weiteren gibt es noch einen Befehl, der vom SNMP- Agent aus gesendet werden kann:
1. "trap", wird bei auftretenden Störungen sofort abgesetzt, um die Management- Station zu informieren

Für die Kommunikation greift das Verfahren auf die sogenannte Management Information Base (MIB) zu. Hierbei gibt es eine Standard MIB (MIB II), die für die Grundabfragen zuständig ist und eine private MIB, die für die gerätespezifischen Einstellungen zuständig ist.
Die MIB ist hierarchisch aufgebaut. Die benutze Sprache ist ASN.1. Die Abfragen orientieren sich hierbei an der Baumstruktur und liefern Dezimalketten, die diesen Weg beschreiben, zurück.
Das heizt, das die Dezimalketten die Baumstrukur wiedergeben.

Zu B.
RMON (Remote MONitoring)
RMON ist eine SMNP- Erweiterung. Hierbei gibt es, ähnlich der Management- Station, einen RMON-Manager und einen RMON- Probe (Hardware oder Software), vergleichbar mit dem SNMP- Agent.
Dabei liest der Probe alle Datenpakete im Netz mit und schickt die Analyse an den RMON- Manager.

Beim RMON unterscheidet man zwei Typen.
RMON1 analysiert die zweite Ebene des OSI- Referenzmodells und ist in Form von MIB`s organisiert. Diese sind wiederum in Gruppen unterteilt.

RMON- Gruppen:
a) Statistik, beinhaltet allgemeine Auswertungen, wie z.B. die Auslastung

b) History, gibt Trends an
c) Alarm, hier sind die Schwellwerte definiert
d) Host, Statistiken für bestimmte Geräte
e) Host Top N, die 10 Geräte mit z.B. der höchsten Auslastung
f) Matrix, Verkehrsbeziehungen
g) Filter
h) Data Pacture
i) Event
j) [Token Ring]

RMON2 analysiert die Ebene 3- 7 des OSI- Referenzmodells.

Zu C:
LAN- Analyse
Die LAN- Analyse bietet die Möglichkeit die Datenpakete mitzulesen. Dies schafft einen großen Vorteil bei konkreten Problemen. Der LAN- Analyzer ist eine Kombination aus PC und Software und wird für diese Aufgabe eingesetzt.