

1 Verteilte Systeme

Begriffe:

IEEE – Normen

IEEE = Institute of Electrical and Electronics Engineers. Aussprache : "Ei Triple-i".

Verteilte Systeme - man spricht auch vielfach von verteilter Verarbeitung (*Distributed Processing*) - werden auf vielfache Weise interpretiert.

Verschiedene *Programmmodule* eines Gesamtsystems werden auf mehreren unterschiedlichen *Rechnern*, verbunden durch ein *Kommunikationsnetz*, das den Informationsaustausch erlaubt, ausgeführt. Die Module sind hierbei weitgehend *autonom* und unterliegen keiner (oder nur einer eingeschränkten) zentralen Kontrolle. Sie sind also - genauso wie die Rechnersysteme, auf denen sie laufen - voneinander unabhängig. Bei dieser (räumlichen) Verteilung von Hard- wie auch von Software wird insbesondere eine physische Trennung der *Datenhaltungs-* und der *Verarbeitungskomponente* vorgenommen.

1.1 Die Aufgaben Verteilter Systeme

- **Datenverbund:**
Räumlich getrennte, aber logisch zusammenhängende Daten werden gemeinsam genutzt. Die Gesamtdatenmenge wird verteilt, um Daten dort zu halten, wo sie erzeugt bzw. verarbeitet werden. Als Grundvoraussetzung für das verteilte Halten von Daten müssen Instrumente zur Sicherung der *Konsistenz* und *Aktualität* vorhanden sein.
- **Lastverbund:**
Alle in einem Netz zur Verfügung stehenden Kapazitäten sollen gleichmäßig ausgenutzt werden. Bei starker Belastung einzelner Ressourcen muss eine Umverteilung anstehender Aufträge auf andere, weniger frequentierte Geräte möglich sein.
- **Funktionsverbund:**
Spezielle Rechner und Peripheriegeräte werden allen Netzteilnehmern zur Verfügung gestellt. Jede Ressource kann auf diese Weise genau für *die* Aufgabe eingesetzt werden, die sie am besten beherrscht. Besondere Funktionen (z. B. Laserdrucker oder Modems) müssen innerhalb des Netzes - je nach Anforderung - nur einmal zur Verfügung stehen und können von allen benutzt werden.
- **Verfügbarkeitsverbund:**
Das Verteilte System garantiert eine bestimmte *Mindestleistung*, die auch aufrechterhalten werden kann, falls einzelne Systemkomponenten ausfallen sollten. Dies erfordert ein gewisses Maß an Redundanz, auf die man im Fehlerfall ausweichen kann.

1.2 Ziele und Vorteile Verteilter Systeme

Verbesserte Laufzeit Eine Dezentralisierung von Daten ermöglicht deren räumliche Positionierung direkt bei den sie bearbeitenden Operationen. Daraus ergeben sich eine *bessere Laufzeit* und eine *einfachere Verwaltung*.

Parallele Verarbeitung Module - seien es nun Rechner oder Programmteile, die weitgehend autonom arbeiten - ermöglichen eine *parallele* Verarbeitung: Entkoppelte Abläufe können gleichzeitig ausgeführt werden, wodurch die Gesamtbearbeitungszeit verkürzt werden kann.

Geringe Kosten Die gemeinsame Betriebsmittel- und Ressourcennutzung, die über das Kommunikationsnetz ermöglicht wird, führt zu *Kosteneinsparungen*. Teure Geräte wie Drucker oder spezielle Speicher und komplexe Komponenten (z. B. Datenbanken) brauchen nur einmal beschafft und betrieben zu werden. Zudem führt diese Mehrfachverwendung zur besseren *Integration* aller Komponenten in das Gesamtsystem und erhöht dessen *Funktionalität*.

Verbessertes Planen und Betreiben Auch aus der Sicht des Betreuers und Betreibers lassen sich direkte Vorteile erkennen: Verteilte Systeme können besser *geplant*, *installiert* und *gewartet* werden. Ihre autonomen Subsysteme passen sich in ihrem Umfeld besser an lokale Anforderungen an und erhöhen damit die *Benutzerakzeptanz*. Darüber hinaus sind Verteilte Systeme durch ihre modulare Struktur einfacher erweiter- und änderbar. Es besteht die Möglichkeit, Hard- und Softwarekomponenten bei laufendem Betrieb auszutauschen bzw. neue Module hinzuzufügen. Bei einer Neuanschaffung kann somit zunächst mit einem kleinen System begonnen werden, das sich später schrittweise ausbauen lässt.

Leistung nur dort, wo nötig Zusammenfassend kann gesagt werden, dass Verteilte Systeme mit ihren Möglichkeiten einer wesentlichen betriebswirtschaftlichen Forderung gerecht werden: Rechenleistung wird nur dort zur Verfügung gestellt, wo sie wirklich benötigt wird. Die Systeme sind zuverlässiger, flexibler und leistungsfähiger als ihre an einem Zentrum orientierten Vorgänger.

1.3 Probleme Verteilter Systeme

Bei größeren Systemen ist die Kopplung und Integration der einzelnen Teilmodule nur mit großem Aufwand beherrschbar. Die Verschiedenartigkeit von Befehlssätzen, Betriebssystemen, Programmiersprachen und Kommunikationsmechanismen der verwendeten Module von meist unterschiedlichen Herstellern machen spezielle Adaptionstechniken und aufwendige Koordinierungen notwendig.

Anders als Systeme, die zentral gesteuert und überwacht werden können, sind Verteilte Systeme auch anfälliger gegen Datenmanipulation und unberechtigten Zugriff. Vor allem das Kommunikationsnetz eignet sich für Angreifer als gute Einbruchsmöglichkeit. Deshalb sind gerade in Verteilten Systemen wohldurchdachte *Schutz-* und *Sicherheitsmaßnahmen* notwendig.

Die autonome und parallele Ausführung von Teilprozessen verringert zwar im allgemeinen deren Gesamtlaufzeit, erfordert aber wegen unterschiedlicher Laufzeiten in den Modulen eine *Synchronisation* paralleler Verarbeitung. Voneinander abhängige Prozesse müssen aufeinander abgestimmt werden.

2 Einteilungen der Netze

Kommunikationsnetze bestehen aus:

- Übertragungswegen
- Übertragungseinrichtungen
- Vermittlungseinrichtungen

Unterschieden werden folgende Netze:

- Weltverkehrsnetze - WAN (Wide Area Networks)
- Regionale Netze - MAN (Metropolitan Area Networks) Ausdehnungen bis 100km
- Lokale Netze - LAN (Local Area Network) Verbindungsraum von wenigen km

2.1 Netzwerktopologien

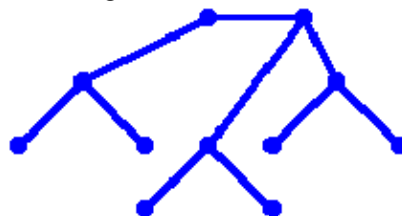
Unter dem Begriff der Topologie versteht man, wie die einzelnen Rechner logisch miteinander verbunden sind.

Stern-Topologie
Bus-Topologie,
Baum-Topologie,
Ring-Topologie.

Die **Stern**-Netze sind *zentral* gesteuert. Hier können zwar verschiedene Systeme miteinander kommunizieren, aber der Verbindungsweg geht immer über ein zentrales Vermittlungssystem.



Die **Baum**-Struktur entwickelte sich aus der Bus-Struktur, die aus verzweigten Bussen besteht, aber immer noch keine Schleifen beinhaltet. Zwischen zwei angebenen Endsystemen existiert genau ein Weg.



Bei der **Ring**-Struktur sind alle Netzknoten an einem geschlossenen Leitungsring angeschlossen. Hier muss ein gesendetes Paket explizit vom Ring genommen werden, um nicht endlos zu kreisen, da es nicht von selbst verschwindet.

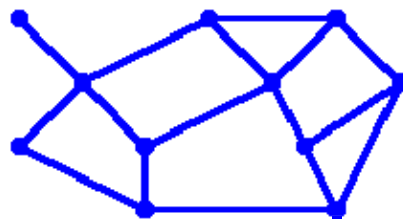


Bei **Bus**-Netzen sind alle Endgeräte mittels passive Koppler an einem einzigen Übertragungskabel (Zweidrahtleiter, Koaxialkabel oder Lichtleiter), dem "Bus" angebunden. Bekanntestes Bus-System ist zweifellos das *Ethernet*.



Das Maschennetz

Meist in WAN-Umgebungen benutzt. Router verbinden mehrere Punkte miteinander zur Erzeugung von Redundanz, und um die Möglichkeit zu bieten, die kürzeste Route zu einem Ziel zu finden.



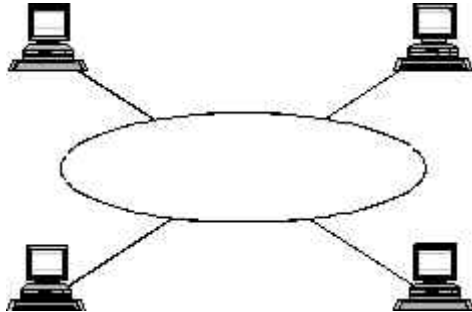
Zusammenfassung der drei wichtigsten Topologien

Topologie/Struktur	Vorteile	Nachteile
<p>Busstruktur</p>	<ul style="list-style-type: none"> • einfach installierbar • einfach erweiterbar • kurze Leitungen 	<ul style="list-style-type: none"> • Netzausdehnung begrenzt • bei Kabelbruch fällt Netz aus • aufwändige Zugriffsmethoden
<p>Sternstruktur</p>	<ul style="list-style-type: none"> • einfache Vernetzung • einfache Erweiterung • hohe Ausfallsicherheit 	<ul style="list-style-type: none"> • hoher Verkabelungsaufwand • Netzausfall bei Ausfall oder Überlastung des Hubs - das komplette Netzwerk über'n Jordan
<p>Ringstruktur</p>	<ul style="list-style-type: none"> • verteilte Steuerung • große Netzausdehnung 	<ul style="list-style-type: none"> • aufwändige Fehlersuche • bei Störungen Netzausfall • hoher Verkabelungsaufwand

2.2 Netzstrukturen

Peer-to-Peer Netzwerke

Grundzüge: Es gibt keinen dedizierten Server (Computer, der ausschließlich als Server eingesetzt wird); alle Stationen sind gleichberechtigt; jede Station kann sowohl Client als auch Server sein.



Die bekanntesten Betriebssysteme für Peer-to-peer-Netzwerke sind Windows für Workgroups und Windows 95.

Vorteile:

- unkomplizierter, schneller Aufbau
- kostengünstig

Nachteile:

- Geräte- und Verzeichnisfreigaben für jede PC lokal einrichten
- Es gibt nur wenig Zugriffs- und Datensicherheit
- Je nach eingesetztem Betriebssystem nicht sehr stabil und belastbar
- Es kann keine Client/Server-Software eingesetzt werden

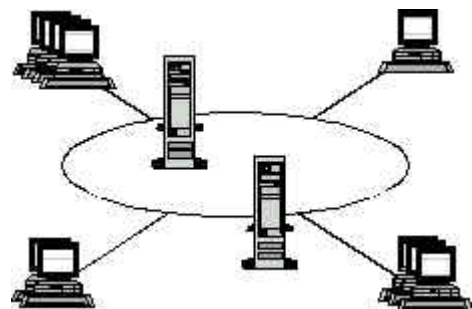
Serverbasierendes Netzwerk (Client/Server)

In einem serverbasierenden Netzwerk werden die Daten auf einem zentralen Server gespeichert und verwaltet. Man spricht von einem dedizierten Server, auf dem keine Anwendungsprogramme ausgeführt werden, sondern nur eine Server-Software.

Mögliche „Server“-Aufgaben wären :

File - Server, Print - Server, Application - Server, Mail - Server, Web - Server, Datenbank - Server

Bei den meisten Client - Server Systemen existiert auch eine zentrale Benutzerverwaltung, welche die Benutzer in verschiedene Gruppen unterteilt und diesen Gruppen dann verschiedene Rechte zuweist. Der Vorteil davon ist, dass neue Benutzer so schnell in das Netzwerk integriert werden können, da man sie einfach einer Gruppe zuweist. Der nächste Vorteil für die User (Benutzer) ist, dass sie sich von jedem Rechner im Netzwerk mit ihrem eigenen Namen am Netz anmelden können und sofort auf ihre Benutzereinstellungen und auf für sie freigegebene Ressourcen zugreifen können.



Nachteile :

Kosten für die Anschaffung von Servern + Betriebssystemen (Microsoft-Produkte),

Vorteile :

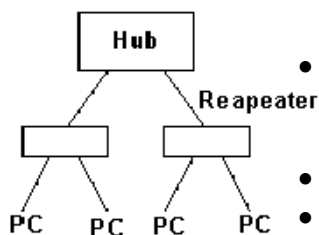
Zentrale Verwaltung aller Daten / Ressourcen, Hohe Sicherheit, bestehende Peer - to - Peer Netze können integriert werden, Bei ausreichender Skalierung sind Client - Server Netze normalerweise schneller als Peer - to - Peer Netze, Anbindungen an andere Netzwerke sind leichter möglich

3 Netzknoten

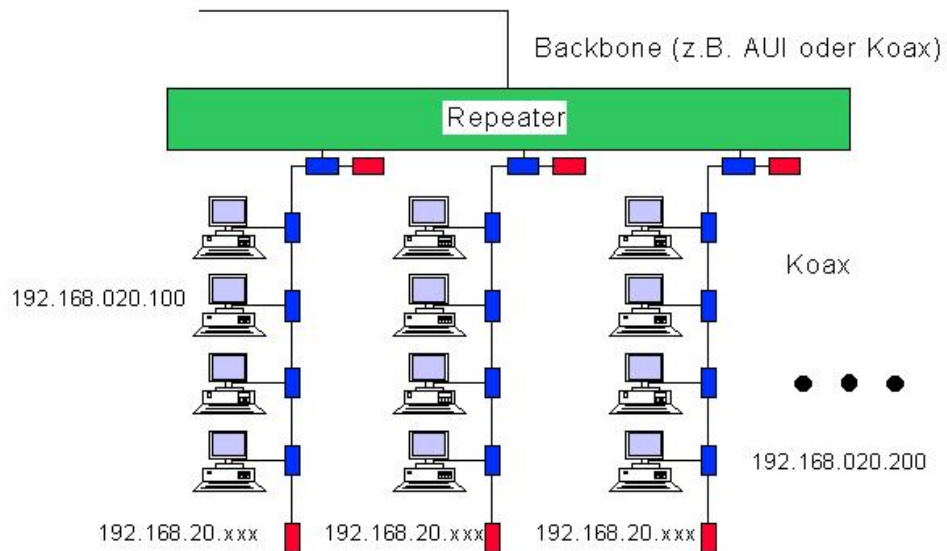
(auch Kopplungselemente)

Repeater

- Koppeln zwei gleiche LAN-Segmente miteinander.
 - sind Signalregeneratoren, die mehrere (mindestens zwei) Netzwerkanschlüsse haben
 - werden eingesetzt, wenn Segmente das Limit ihrer physikalisch erlaubten Ausdehnung (z.B. 500 m 10BASE5, 185 m 10BASE2) erreicht haben, aber erweitert werden sollen
 - teilen ein Netz in mehrere Segmente um die Verfügbarkeit des Netzes zu erhöhen, da Repeater verhindern, dass fehlerhafte elektrische Signale von einem Segment auf ein anderes übertragen werden (?)
 - Er hat nur die Funktion Signale zu verstärken und sie neu zu übertragen. Dadurch ist es möglich lange Kabelstrecken zu überbrücken.
 - arbeiten auf der **Schicht 1** des OSI-Modells
 - Sobald sie auf einem ihrer Eingänge die ersten Bits eines übertragenen Pakets empfangen, schicken sie es auf allen Ausgängen fast ohne Zeitverzögerung weiter.
 - Eine Modifikation der Daten erfolgt nicht.
 - Ein Netz darf maximal vier Repeater enthalten (laut IEEE 802.3).
 - Ein Repeater übernimmt keinerlei regulierende Funktion in einem Netzwerk, und kann nicht dazu verwendet werden, um ein Netzwerk zu entlasten.
- Für angeschlossene Geräte ist nicht erkennbar, ob sie an einem

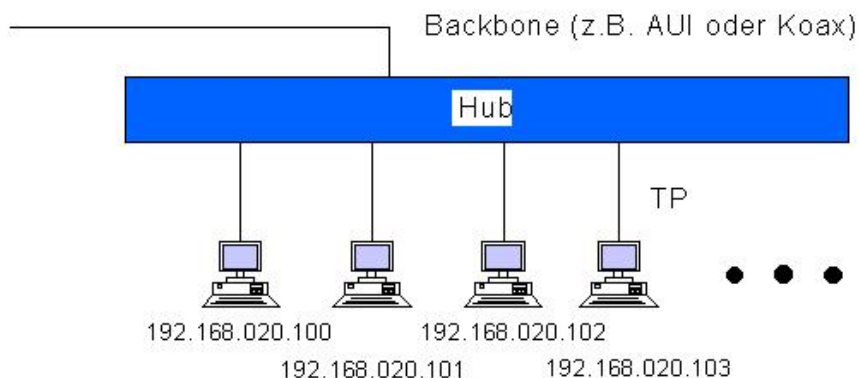
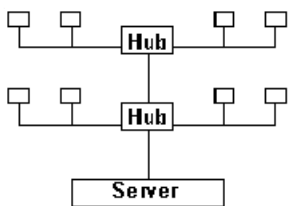


Repeater angeschlossen sind. Er verhält sich völlig transparent.



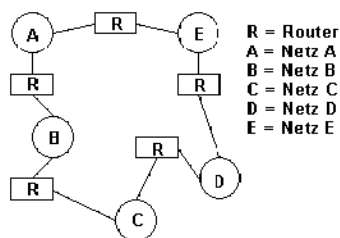
Hub

- spezielle Form von Repeatern (Multiport Repeater für 10Base-T)
- Netzwerkgerät, das die zentrale Vermittlungsstelle für ein sternförmig verkabeltes Netzwerk bildet.
- Hubs arbeiten auf der Bitübertragungsschicht (**Schicht 1**) des OSI-Modells. Sie haben reine Verteilfunktion.
- Alle Stationen die an einem Hub angeschlossen sind, teilen sich die gesamte Bandbreite mit der der Hub an ein Netzwerk angeschlossen ist. Nur die Verbindung vom Computer zum Hub verfügt über die gesamte Bandbreite. Durch die Verbindung mehrerer Hubs lassen sich die Anzahl der möglichen Stationen erhöhen.
- Ein Hub nimmt ein Datenpaket an und sendet es an alle anderen Ports. Dadurch sind alle Ports belegt. Diese Technik ist nicht besonders effektiv. Es hat aber den Vorteil, das solch ein Hub einfach und kostengünstig zu bauen ist.



Router

- Ein Router ermöglicht es mehrere Netzwerke mit unterschiedlichen Protokollen und Architekturen zu verbinden.
- verbindet zwei oder mehrere Netze, die lokal oder entfernt sein können
- Empfängt ein Router ein Datenpaket, so leitet er es aufgrund der darin enthaltenen Adressierungsinformation an den gewünschten Empfänger weiter (für das Netzprotokoll nicht transparent).
- Ein Router kann auch Daten zwischen verschiedenen Übertragungsmedien weiterleiten (z. B. von Ethernet auf eine serielle Verbindung).
- Zwischenspeicherung der Daten wird durch die Umsetzung bei verschiedenen Übertragungsgeschwindigkeiten notwendig
- Router kann verschiedene alternative Wege zur Auswahl haben, auf die er den Datenfluss verteilen kann
- leitet Datenpakete durch das Netzwerk, allerdings nicht mehr aufgrund der physikalischen Adresse der Frames der MAC-Schicht sondern auf der Basis der Adresse der **Schicht 3** (im Internet ist dies die IP-Adresse)
- Anhand von Routing-Tabellen können die Wege der Datenpakete festgelegt und gesteuert werden. Die Routing-Tabelle sagt ihnen nicht nur, wie viele Hops (zu passierende Zwischen-Stationen) für ein Paket nötig sind, damit es sein Ziel erreicht, sondern auch welche dazwischenliegenden Netzwerke es meiden muss, da sie stärker belastet sind als andere.

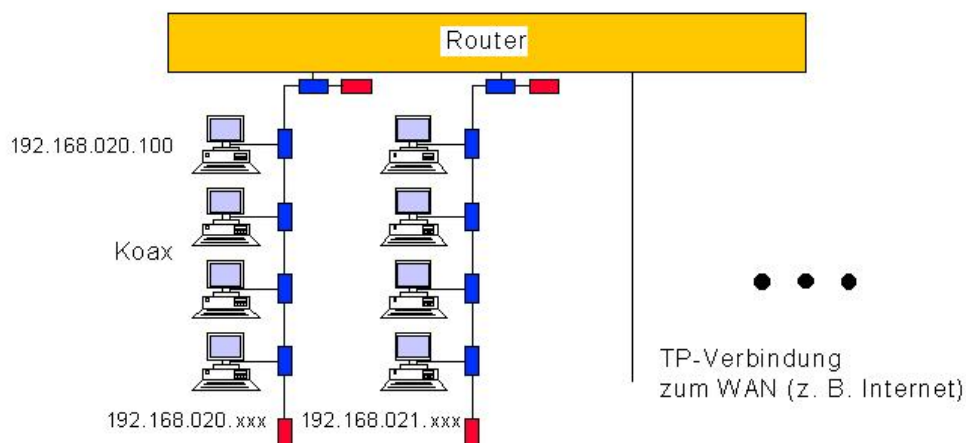


Die Routingtabelle enthält folgende Angaben:

- alle bekannten Netzwerkadressen
- Verbindungsarten in andere Netzwerke
- Weginformationen zu anderen Routern
- Verbindungskosten

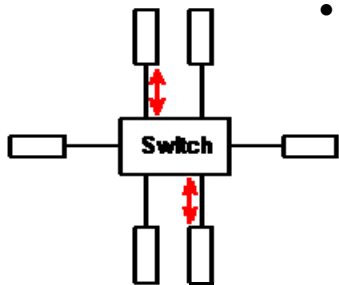
Anhand dieser Informationen entscheidet ein Router über den Weg, den ein Datenpaket nimmt.

In der Routingtabelle werden auch die Anzahl der Zwischenstationen für ein Datenpaket gespeichert, das es für das Erreichen des Ziels benötigt.



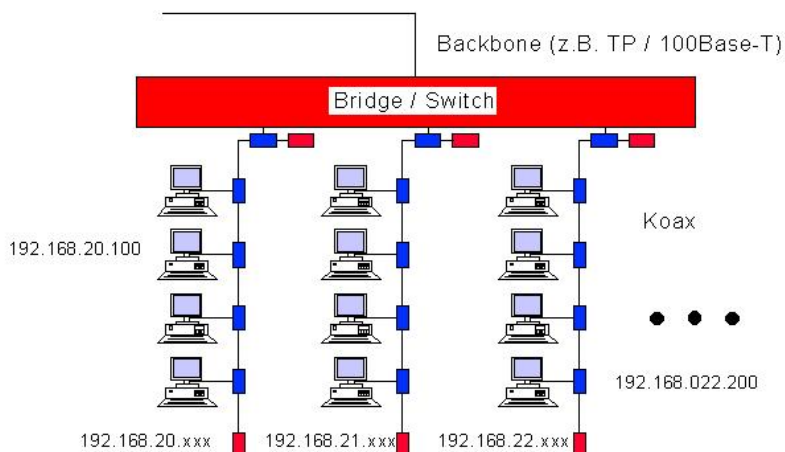
Bridge / Switch

- Bridges und Switches arbeiten auf der **Schicht 2** des OSI-Modells
- Sie verbinden verschiedene physikalische Netzwerktypen miteinander (beispielsweise kann mit einer Bridge ein Ethernet-Segment an einen FDDI-Ring angeschlossen werden)
- Bridges nehmen nicht wie Repeater einzelne Bits, sondern komplette Rahmen entgegen.
- Sie überprüfen Prüfsummen und wandeln die Rahmen gegebenenfalls in das Format des Ausgangsnetzwerkes um.
- Bridges ermöglichen es, einzelne LANs zu einem praktisch unbegrenzt großen Netzwerk zusammenzufassen.
- Um die Belastung der einzelnen LANs zu begrenzen, sind Bridges mit einer gewissen Lernfähigkeit ausgestattet.
- Sie lernen mit der Zeit, welche Station in welchem Teilnetz angeschlossen ist. Legt eine Datenbank aller Stationsadressen an (Routing-Tabelle).
- Dadurch können sie Rahmen gezielt nur in die Teilnetze weiterleiten, in der sich der Zielrechner befindet.
- Bridges und Switches sind eigentlich gleichwertige Bezeichnungen. Handelt es sich um ein Gerät mit sehr vielen Ports, so spricht man in der Regel von Switches.
- Empfängt ein Switch ein Datenpaket, so sucht er in seinem Speicher nach **der Zieladresse(MAC)**, und schickt dann das Datenpaket nur an diesen Port. Während zwei Ports miteinander kommunizieren können zwei Ports parallel Daten austauschen. Im Idealfall kann ein n-Port-Switch $n/2$ Datenpakete(Frames) gleichzeitig vermitteln. Die MAC-Adresse lernt ein Switch mit der Zeit kennen. Die Anzahl der Adressen, die ein Switch aufnehmen kann, hängt ab von seinem Speicherplatz.



Switches/Bridges unterscheidet man hinsichtlich ihrer Leistungsfähigkeit mit folgenden Eigenschaften:

- Anzahl der speicherbaren MAC-Adressen
- Verfahren, wann ein empfangenes Datenpaket weitervermittelt wird
- Latenz der vermittelten Datenpakete



Gateway

Gateways zählen nicht zu den Kopplungselementen. Ihre Hauptfunktion besteht nicht darin, die Reichweite eines Netzwerks zu erweitern.

Ein Gateway verbindet zwei Netzwerke miteinander, die zueinander inkompatibel sind (verschiedenen Netzwerk-Welten).

Ein Gateway setzt die Protokolle und die Adressierung in das jeweilige Ziel-Netzwerk um. Dabei kann es vorkommen, dass es je nach Anforderung speziell konfiguriert oder neu entwickelt werden muss.

NIC(Network Interface Card)

Ein NIC ist ein Netzwerkadapter. In einem Computer handelt es sich um eine Netzwerkkarte, die es ermöglicht auf ein Netzwerk zuzugreifen.

Ein NIC arbeitet auf der Bitübertragungsschicht(Schicht 1) des OSI-Modells. Jeder NIC hat eine Hardware-Adresse, die es auf der Welt nur einmal gibt (MAC). Anhand dieser Adresse lässt sich der Netzwerkadapter zweifelsfrei identifizieren.



4 Zugriffsmethoden

CSMA/CD

Carrier Sense Multiple Access with Collision Detection

Überprüft vor dem Senden, ob das Kabel frei ist, und nach dem Senden, ob eine Kollision mit einem anderen Datenpaket stattgefunden hat. Verwendet beim "Ethernet" und das in der Praxis am häufigsten verwendete Verfahren.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance

Überprüft vor dem Senden, ob das Kabel frei ist, und sendet zunächst einen Rundspruch in das Netzwerksegment um das Senden der Daten anzukündigen. Verwendet bei "AppleTalk". Verhindert Kollisionen, ist aber langsamer als CSMA/CD.

Token-Passing

Ein Token wird durch den Ring gesendet. Nur ein Computer, welcher ein leeres Token erhalten hat darf Daten durch das Netzwerk schicken. Sobald eine Empfangs-Bestätigung eingetroffen ist, sendet er ein leeres Token zum nächsten Computer im Ring. Verwendet im TokenRing, keine Kollisionen.

Demand-Priority

Entwickelt für 100VG-AnyLAN Ethernet (IEEE 802.12).

Das Netz besteht aus Hubs (Repeater) und Endknoten (Computer, Bridge oder Router). Die Hubs steuern den Netzwerk-Zugriff mit Round-Robin und verbinden den Quell- direkt mit dem Zielcomputer. Bei Konflikten zählt die Priorität des Zugriffs.

5 Bezeichnungen der Netzwerktechniken

10Base5

10Base5 ist eine Methode, Ethernet mit einer Bandbreite von 10 Mbit/s über Koax-Kabel zu betreiben(Thick Ethernet).

Die maximale Kabellänge eines Segments beträgt 500 Meter. Die beiden Kabelenden müssen mit Endwiderständen von 50 Ohm abgeschlossen werden.

Pro Segment dürfen 100 Endgeräte angeschlossen werden. Die jeweiligen Stickleitungen dürfen dabei nicht länger als 50 Meter lang sein.

10Base2 (IEEE 802.3)

10Base2 ist eine Methode Ethernet mit einer Bandbreite von 10 MBit/s über Koax-Kabel zu betreiben(Thin Ethernet).

Die Maximale Kabellänge eines Segmentes beträgt 185 Meter. Die beiden Kabelenden müssen mit Endwiderständen von 50 Ohm abgeschlossen werden.

Das Netzwerkkabel wird direkt von Workstation zu Workstation geführt.

Stickleitungen von der Netzwerkkarte zum Kabelstrang sind nicht zulässig.

Das nachträgliche Anfügen zusätzlicher Workstations erfordert die kurzzeitige Unterbrechung des Netzwerks.

Pro Segment können maximal 30 Geräte angeschlossen werden.

10BaseT (IEEE 802.3)

10BaseT ist ein Ethernet-Netzwerk(mit 10 MHz) in dem alle Stationen über UTP-Kabel(Twisted Pair) stern- oder baumförmig an einem zentralen Hub angeschlossen sind. Über Crossover-Kabel ist es möglich zwei Stationen oder Hubs direkt miteinander zu verbinden. Bei mehr als zwei Stationen ist jedoch zwingend ein Hub notwendig.

Die maximale Kabellänge zwischen Station und Hub beträgt maximal 100 Meter.

Als Anschlußtechnik kommt die RJ45-Technik(breite Western-Stecker, 8polig) zum Einsatz. Der Standard ist im IEEE 802.3i festgelegt.

FOIRL

FOIRL(Fiber Optic Inter-Repeater Link) ist eine Methode, um Ethernet-Repeater mit 10 Mbit/s Bandbreite mit Glasfaserkabel zu verbinden.

Dabei nutzt man die Vorteile der Glasfaser hinsichtlich Störanfälligkeit und EMV.

Die maximale Länge der Verbindung beträgt 1 Kilometer.

10BaseFB

Diese Verkabelung ermöglicht eine effizientere Kommunikation der Repeater(über 4) untereinander auf normalen FOIRL-Kabel.

10BaseFB ist unter IEEE 802.3.17 beschrieben.

10BaseFL

10BaseFL definiert den Anschluss einer Workstation an einen Hub über Glasfaserkabel mit 10 MBit/s. Die maximale Länge des Kabels beträgt 2 Kilometer.

10BaseFL ist unter IEEE 802.3.18 beschrieben.

10BaseFB

10BaseFB ermöglicht den Anschluss mehrerer Geräte über Glasfaserkabel an einen passiven Hub.

10BaseFB ist unter IEEE 802.3.16 beschrieben.

100BaseT (IEEE 802.3u)

100BaseT ist die allgemeine Bezeichnung für Ethernet mit 100 MBit/s. Die Stationen sind über UTP-Kabel der Kategorie 5 sternförmig an einen Hub angeschlossen.

Die maximale Länge der Kabel beträgt 100 Meter.

100BaseT4

100BaseT4 ermöglicht Ethernet mit einer Bandbreite von 100 MBit/s über UTP-Kabel der Kategorie 3 zu betreiben. Der Unterschied zur normalen Ethernet-Verkabelung, ist die Verwendung aller Adernpaare.

100BaseFx

100BaseFx ist eine Methode für den Einsatz von Ethernet mit 100 MBit/s über Multimode-Glasfaserkabel.

Diese Methode ist ähnlich wie FDDI spezifiziert.

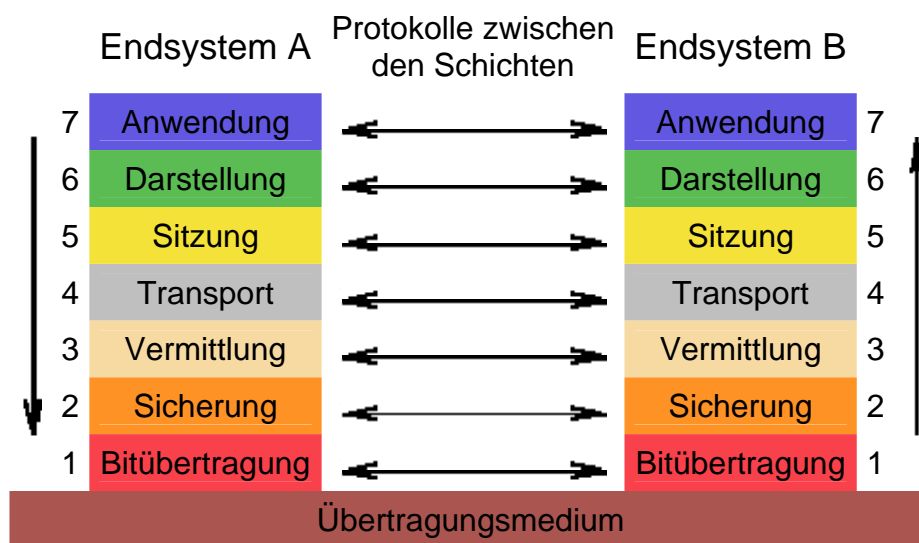
100BaseVG

100VG-AnyLAN ist die Bezeichnung einer Entwicklung von IBM und HP. In dieser Technik ist die Token-Ring-Technologie für ein 100 MBit-Netzwerk vereint.

VG-AnyLAN ist unter IEEE 802.12 beschrieben.

6 OSI-7-Schichtmodell

OSI = Open System Interconnection (Offenes System für Kommunikationsverbindungen)



Das OSI-7-Schichtmodell ist ein Referenzmodell für herstellerunabhängige Kommunikationssysteme.

- Die Schichteneinteilung erfolgt mit definierten Schnittstellen.
- Einzelne Schichten können angepaßt oder ausgetauscht werden.
- Die Schichten 1..4 sind transportorientierte Schichten.
- Die Schichten 5..7 sind anwendungsorientierte Schichten.
- Das Übertragungsmedium ist nicht festgelegt.

Bitübertragungsschicht	
Schicht 1 Physical	Diese Schicht ist verantwortlich für den physikalischen Transport der Informationen oder Daten. Sie ist die elektrische, mechanische und funktionale Schnittstelle zum Übertragungsmedium. Das Übertragungsmedium ist jedoch kein Bestandteil der Schicht 1.
Sicherungsschicht	
Schicht 2 Link	Die Schicht 2 enthält Prozeduren zur Fehlererkennung, Fehlerbehebung und Datenflusskontrolle.
Vermittlungsschicht	
Schicht 3 Network	Diese Schicht steuert die zeitliche und logische getrennte Kommunikation zwischen den verschiedenen Endgeräten, unabhängig von Medium und Topologie.
Transportschicht	
Schicht 4 Transport	Diese Schicht stellt die Verbindung dar, zwischen den anwendungsorientierten Schichten und den transportorientierten Schichten.
Sitzungsschicht	
Schicht 5 Session	Diese Schicht organisiert den Dialog zwischen den Endsystemen. Sie enthält Steuerungsmechanismen für den Datenaustausch.
Darstellungsschicht	
Schicht 6 Representation	Diese Schicht wandelt die Daten für die Anwendungsschicht in ein geeignetes Format um. Diese Schicht wandelt die Daten von der Anwendungsschicht in ein geeignetes Format um.
Anwendungsschicht	
Schicht 7 Application	Diese Schicht stellt die Verbindung zu den unteren Schichten her. Auf dieser Ebene findet die Dateneingabe und -ausgabe statt.

Zusammenfassung Netzknoten und OSI-Modell:

1. *Repeater* arbeiten gemäß OSI-Schicht 1,
2. *Bridges* gemäß Schicht 2,
3. *Router* gemäß Schicht 3 und
4. *Gateways* gemäß einer Schicht zwischen 4 und 7.

Netzwerkmanagement - Prüfungsvorbereitung

Aus 7 werden 4 Schichten(TCP/IP-Protokollstruktur)

(Hierfür gibt es auch andere Bezeichnungen)

Schicht 7	Anwendung	Process/ Application Layer	WWW, SMTP, Telnet, FTP, E-Mail, Networkmanagement
Schicht 6	Darstellung		
Schicht 5	Sitzung		
Schicht 4	Transport	Host-to-Host Layer	TCP, UDP
Schicht 3	Netzwerk, Vermittlung	Internet Layer	IP
Schicht 2	Sicherung	Local Network Layer	Ethernet IEEE 802 SNAP- Sub-Network-Access- Protokoll IEEE 802.3 Ethernet (CSMA/CD) FDDI (Fiber ...)
Schicht 1	Physikalischer Anschluss		