Kommunikationstechnik:

Warum werden Computer miteinander vernetzt ?

- gemeinsame Datennutzung;
- zentrale Datensicherung;
- Ressourcenkonzentration;
- einfacher Datenaustausch;
- geringer Aufwand für Softwarepflege (Server);
- Teamarbeit: Groupware (erlaubt mehreren Benutzern an der Lösung eines Problems in Echtzeit-Dokumentenverwaltung zu arbeiten)
- Öffentliche Ordner, schwarze Bretter
- eMail;
- gemeinsame Nutzung eines Druckers;
- Skalierbarkeit durch Einbindung mehrerer Server:
  Bsp.: Anwendungsserver stellen Dienste, z.B. statistische Auswertung von Datensätzen usw., zur Verfügung. Dies reduziert den Aufwand für Hard- und Software und spart somit Kosten ein.

Zwei zentrale Netzwerkbetriebssystem-Typen

PEER TO PEER NETZWERK:
Ein Computer in einem Peer to Peer Netzwerk arbeitet sowohl als **Client** als auch als **Server**.

Ein Netzwerk - Client muß eine Softwarekomponente besitzen, die die E/A - Anforderungen überprüft und diese evtl. auf das Netzwerk umleitet. Der sogenannte REDIRECTOR bzw. REQUESTOR versetzt den Client in die Lage, folgende Aufgaben zu erfüllen:

- Anmeldung am Netz;
- Zugriff auf freigegebene Ressourcen;

- Zugriff auf und Verwendung von verteilten Anwendungen;

Ein Netzwerk - Server muß eine Softwarekomponente besitzen, die E/A -Anforderungen von Clients entgegennimmt, bearbeitet und angeforderte Daten zurück zum Client sendet.
Diese Komponente wird häufig Serverdienst genannt.

Peer to *Peer - Netze* besitzen eine **informelle** Struktur.
Bsp.:Windows 9x/NT/2000/XP, Linux,Unix uvm. unterstützen diesen Netzwerktyp standardmäßig.

SERVERBASIERTE NETZWERKE:
Dedizierte Server:
Diese Server haben "nur" die Aufgabe die Anfragen von Netzwerkclients zu beantworten.

Nicht-dedizierte Server:
Fordern und bieten Dienste an; sie sind Grundlage von Peer to Peer Strukturen (z.B. Win 95 -Maschine die Druckerzugriff erlaubt);

Vorteile von dedizierten Dateiservern

- Dateien an einem festgelegten Ort;

- Zentrale Dateiserver können effizienter verwaltet werden (Sicherheit etc.);

- Zentralisierung teurer Hard und Software auf zentralen Dateiserver;

- Bessere Skalierbarkeit

Nachteile von dedizierten Dateiservern

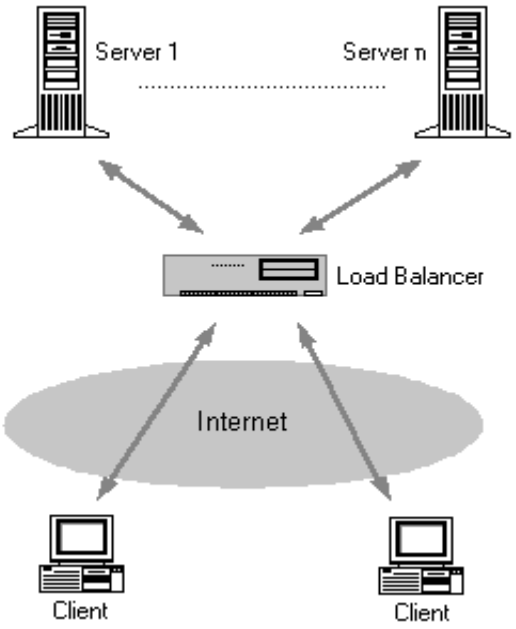
- Single Point of Failure (kompletter Datenverlust möglich !!);
- Durchschnittszugriffszeiten können sehr lang werden (Konkurrenz der Clients);

Vorteile von nicht - dedizierten Dateiservern (verteilte Datenspeicherung Peer to Peer)

- kein Single Point of Failure;
- keine spezielle, teure Server Hard- und Software;

Nachteile von nicht - dedizierten Dateiservern (verteilte Datenspeicherung Peer to Peer)

- Dateidienste schwer zu verwalten (Datenintegrität, Datenschutz, Datensicherung);
- Keine hochzuverlässige Hardware (z.B. unterbrechungsfreie Stromversorgung, Festplattenspiegelung usw.),
- Performance-Steigerung nur mit großem Kostenaufwand, da alle Clients aufgerüstet werden müssen;

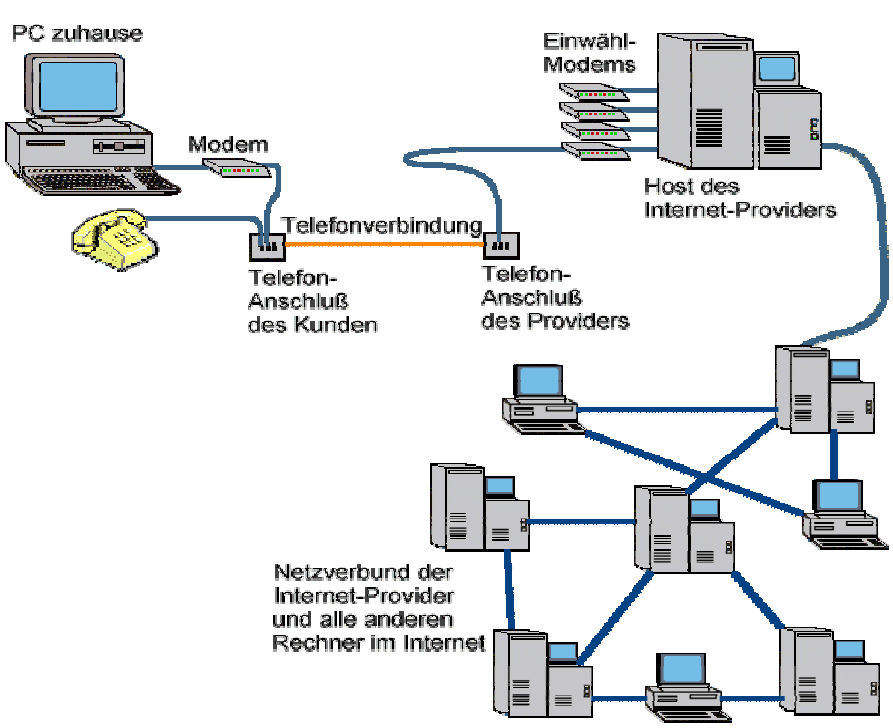


Klassen von Netzwerken

Local Area Network:
Was sind **LAN** ?
Gruppe von Computern, die innerhalb einer geographisch begrenzten Ausdehnung, z.B. Gebäude oder Campus, vernetzt sind.

Wide Area Network:
Was sind WAN ?
Ein Weitverkehrsnetz verbindet LAN's miteinander. Ein WAN ist in seiner Ausdehnung nicht begrenzt. Ein Beispiel für ein globales WAN ist das Internet.

Anmerkung :
In der Literatur findet man auch die Unterscheidung in MAN (Metropolitan Area Network: auf Stadtgebiete begrenzt), WAN (auf Kontinente begrenzt) und GAN (Global Area Network: weltumspannend).



Netzwerkstandards:

Warum werden Netzwerkstandards definiert ?
Bevor Server ihre Dienste Clients zur Verfügung stellen können, müssen beide Einheiten miteinander kommunizieren können. Damit diese Prozesse reibungslos im Hintergrund funktionieren, haben sich Computerfirmen auf Standards und Spezifikationen geeinigt.

Standardisierungsarten:

De-facto-Standars

entstehen durch weite Verbreitung im kommerziellen und universitären Bereich; sie können auch proprietär (Eigentümer; Entwicklung einer Firma) und u. U. nicht veröffentlicht sein;

D**e Jure -Standards**

wurden nicht von einer einzelnen Firma entwickelt und somit besitzt auch niemand die Rechte an ihnen; werden mit der Absicht entwickelt die Conectivity ("verbindbarkeit") und die Interoperabilität (Zusammenarbeit / Funktion) zu verbessern;

Standars für offene und geschlossene Systeme:
Unveröffentlichte und nicht verfügbare Standards heißen *Standars für geschlossene Systeme;*
Beispiele: Novell Netware (**ODI** *Open Data -Link Interface*)
Microsoft / 3COM (**NDIS** Network Driver Interface Specification)

Veröffentlichte und zugängliche Standards nennt man *Standards für offene Systeme*;
Beispiele: **OSI** Open Systems Interconnections (-Referenzmodell)
IEEE 802.X Standards (Institute of Electrical and Eletronic Engeneers)

ISO: International Standard Organisation
Die ISO iniziierte die formulierung eines Standards, der als Basis für Computernetze dient à das OSI Referenzmodell;
damit in Netzwerken einInformationsaustausch stattfinden kann werden eine Reihe von Regeln benötigt, die die Kommunikationsprozesse in einem relativ engen Rahmen festlegen.
Da die Kommunikation zwischen Computern ein extrem komplexer Prozeß ist, muß dieser in Teilprozesse / Teilprobleme untergliedert werden. Im OSI - Referenzmodell wird der Kommunikationsprozeß in ein siebenschichtiges Kommunikationsprotokoll aufgeteilt.

Das OSI - Referenzmodell (Schichten / der Protokollstapel):

Schicht 1: Die physikalische Schicht (**physical Layer**): besteht aus Protokollen zur Kontrolle der Kommunikation auf dem Übertragungsmedium, Bit Übertragung (Handshakes etc.);

Schicht 2: Verbindungsschicht (Sicherungsschicht, **data link**) muß Nachrichten, sogenannte Rahmen (frames), zum Senden in Bits zerlegen und aus empfangenen Bits wiederum Rahmen rekonstruieren; (Gerätekommunikation)

Schicht 3: Netzwerkschicht (**network**) bearbeitet die Kommunikation der Pakete von Geräten auf *logisch voneinander getrennten Netzwerken (Netzadresse usw.).*

Schicht 4: Transportschicht (**transport**) sorgt für zuverlässige Zustellung der Nachrichten (Segments) an die Zielgeräte. Bei Datenverlust muß die Transportschicht eine erneute Zusendung des entsprechenden Datenpaketes anfordern.

Schicht 5: Sitzungsschicht (**session)** verwaltet Dialoge zwischen Computern, d.h. sie startet, überwacht und beendet Kommunikationen
(Simplex: nur eine Richtung, Halbduplex: Daten in beide Richtungen aber pro Zeiteinheit nur in eine Richtung, Vollduplex: z.B. Sprachübertragung beim Telefon)

Schicht 6: Darstellungsschicht (**presentation**) liefert an die Anwendungsschicht ein einheitliches Datenformat deshalb DARSTELLUNGSSCHICHT. Sie befasst sich also mit der Syntax und mit Grammatikregeln für die Kommunikation zwischen zwei Computern.

Schicht 7: Anwendungsschicht (**application**) bildet die Schnittstelle der Netzwerkdienste mit den Anwendungen auf dem Computer;

Ethernet

Das als Ethernet bezeichnete Netzwerk zeichnet sich zunächst durch die Medienzugriffskontrolle CSMA/ CD aus. Im Gegensatz hierzu benutzen Token Ring Netzwerke das Token Passing verfahren. Die Standardisierung und die vorwiegenden Arbeitsbezeichnungen sind z.T historisch zu begründen.

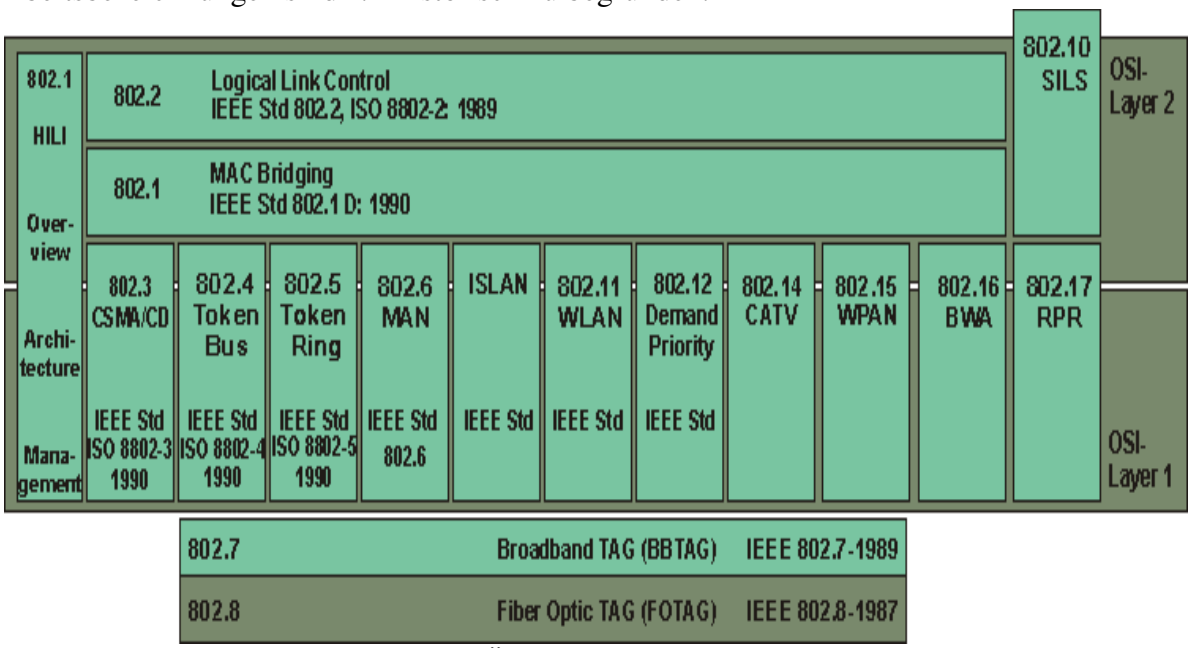


Abb: Osi-Schichten und IEEE 802 im Überblick

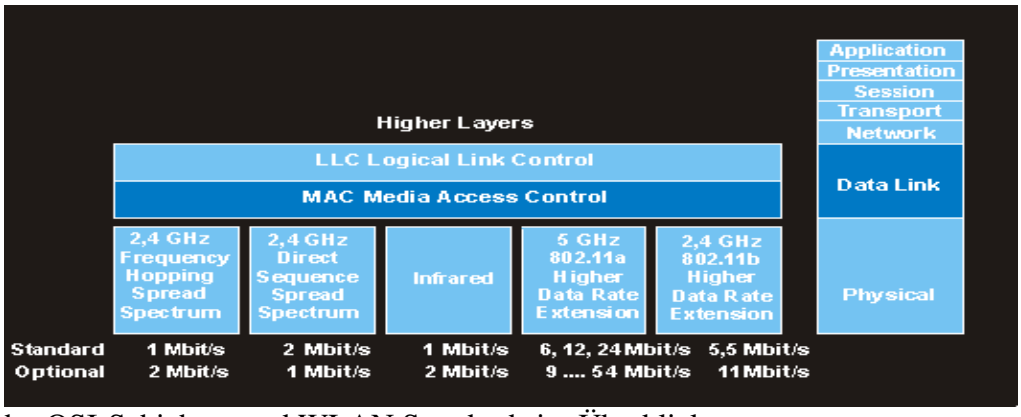


Abb: OSI-Schichten und WLAN Standards im Überblick

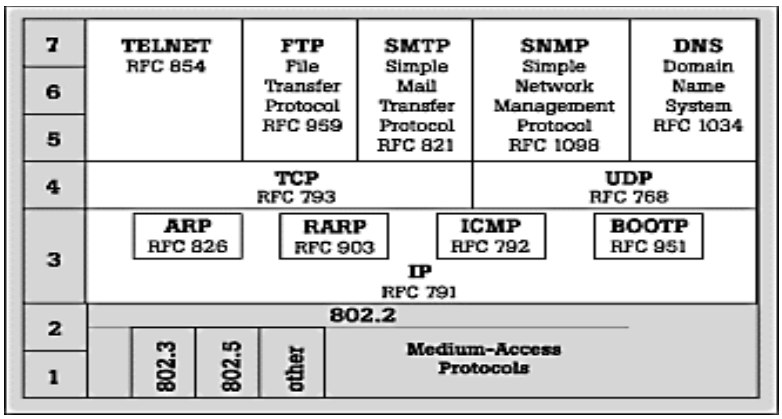
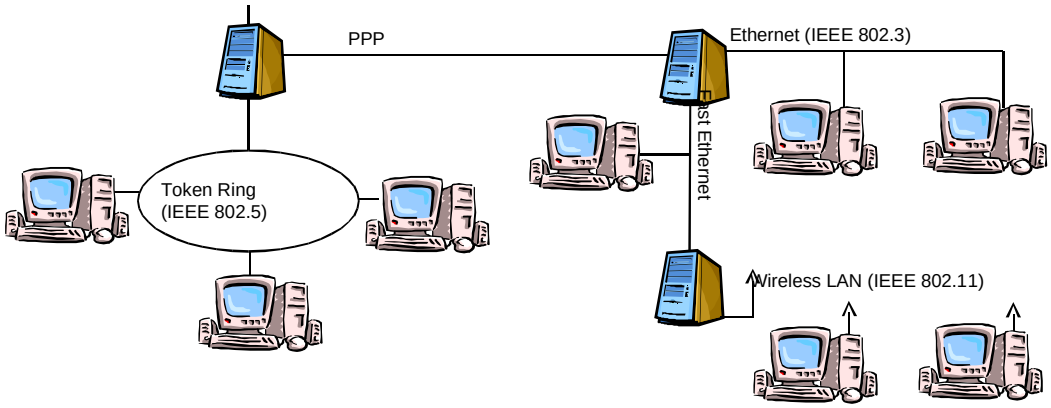


Abb: OSI-Schichten und die Einordnung einiger Protokolle sowie IEEE 802

Überblick zur Anbindung verschiedener Netzwerke:



Fragen zum Ethernet

1 Welche Bedeutung hat IEEE und IEEE 802 ?

2 Was wird in IEEE 802 definiert (ganz allgemein) und in welchem Bereich des OSI-Modells ist dies einzuordnen ?

3 Wer oder was hat den Namen Ethernet festgelegt und welche Besonderheiten bzw. Merkmale zeichnen ein Ethernet - Netzwerk aus ?

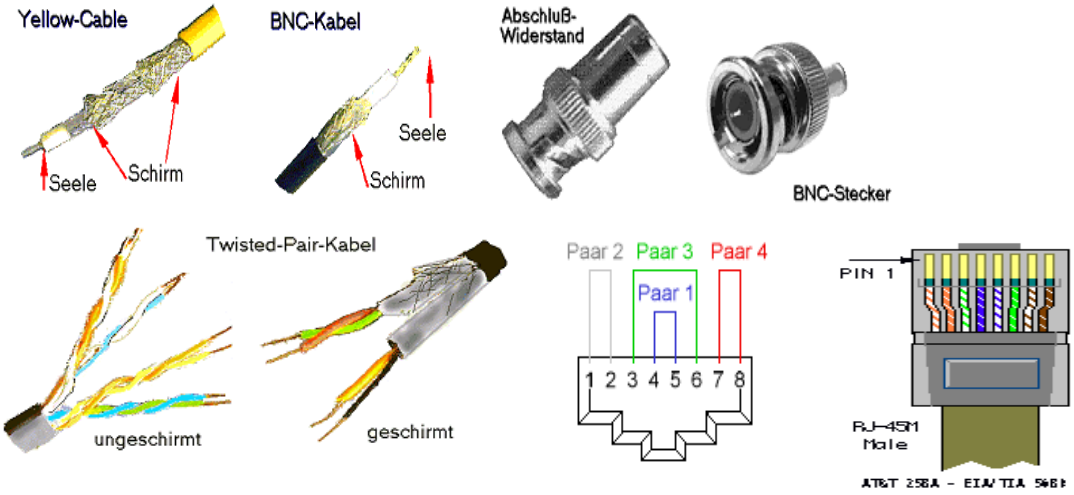
4 Wie funktioniert die Kommunikationskontrolle in einem Ethernet (kurz, eigene Worte)

5 Welche vier wichtigsten Elemente beinhaltet IEEE 802.3 ?

6 Was ist das Besondere bzw. Neue im IEEE 802.2 bzw. was ist der Unterschied zu IEEE 802.3 und welche Vorteile ergeben sich daraus ?

7 Beschreiben Sie bitte die wichtigsten features von:
1 BASE 5, 10 BASE 2, 10 BASE 5

8 Beschreiben Sie bitte die wichtigsten features von:
BASE F, 10 BROAD 36, 10 BASE T, 100 BASE X



EIA/TIA 568A/568B and AT&T 258A define the wiring standards and allow for two different wiring color codes.

Pin #	EIA/TIA 568A	AT&T 258A, or EIA/TIA 568B	Ethernet 10BASE-T	Token Ring	FDDI, ATM, and TP-PMD
1	White/Green	White/Orange	X		X
2	Green/White	Orange/White	X		X
3	White/Orange	White/Green	X	X	
4	Blue/White	Blue/White		X	
5	White/Blue	White/Blue		X	
6	Orange/White	Green/White	X	X	
7	White/Brown	White/Brown			X
8	Brown/White	Brown/White			X

- Pairs may be solid colors and not have the stripe.
- Category 5 cable must use Category 5 rated connectors.

Straight Through - Verdrahtung

Netzwerkprotokolle

Der Zweck eines Netzwerkes besteht im Austausch von Daten zwischen Computern. Die Protokolle stellen dabei die Kommunikationsregeln dar. Genau wie Menschen könne auch Computer Nachrichten auf verschiedene Weise austauschen, solange gewährleistet ist, dass Sender und Empfänger die gleichen (oder kompatiblen) Regeln befolgen (PROTOKOLLE).

Bsp.:
IPX ist das Netzwerkprotokoll, welches auf dem Data-Link-Layer aufsetzt;
SPX ist das Transportprotokoll, welches auf dem Network-Layer (hier IPX) aufsetzt
(NWLINK ist die Microsoft - Version von IPX/SPX)

NetWare IPX/SPX

Die Modularität von IPX/SPX vereinfacht die Aufgabe NetWare-Protokolle auf unterschiedliche Hardware adaptierbar zu machen
(es könne auch Teile/Module der Protokolle isoliert verwendet werden).

IPX (Internetwork Packet Protokol)

- Protokoll der Netzwerkschicht;
- liefert Datagramm (Header, Daten, CRC);
- ist für Routing und logische Adressierung zuständig (...RIP-Protokoll);
- verwendet physikalische Adressen von niedrigen Schichten um Geräte zu adressieren;
- verwendet Sockets, d.h. Adressen von höheren Schichten um Pakete an ihre Endadresse weiterzuleiten;
- IPX ist in den DOS NetWare Requestor integriert;

(RIP Router Information Protocol: führt Funktionen der Netzwerkschicht aus)

SPX (Sequence Packet Exchange)

- erweitert IPX um einen Dienst, der eine garantiert richtige Auslieferung der Daten realisiert (im Fehlerfall werden die Pakete erneut gesendet);
- SPX etabliert virtuelle Leitungen, die man Verbindungen nennt;
- SPX versieht Datenpakete mit Sequenznummern, so dass umgehend entschieden werden kann, ob Daten verloren oder fehlgeleitet wurden;

NCP (Netware Core Protocol)

- beinhaltet Prozeduraufrufe für Netzwerkdienste: Dateidienst, Druckdienst usw.
- die NetWare Client Software hat eine Schnittstelle um auf NCP-dienste zuzugreifen;
- NCP ist ein Protokoll der höheren Schichten, welches Bestandteil des Betriebssystemkernels ist. NCP hat Funktionalitäten der Sitzungs-, Darstellungs- und Anwendungsschichtten des OSI Modells und verfügt über eine eigene Programmiersprache, die Softwareentwickler zur Programmierung von NetWare Applikationen verwenden können.
  Anmerkung: siehe Linux: modprobe ncpfs

Vorteil von TCP / IP (Details siehe Netzwerkgrundlagen II) gegenüber IPX/SPX
ist, dass es keinem Hersteller gehört und somit für jedermann frei verfügbar ist.
TCP/IP ist ein de facto Standard !
TCP / IP ist in allen UNIX - Varianten enthalten;
TCP(Transmission Control Protocol) entspricht SPX in der NetWare "Welt";
IP(Internet Protocol) entspricht IPX in der NetWare-Umgebung;

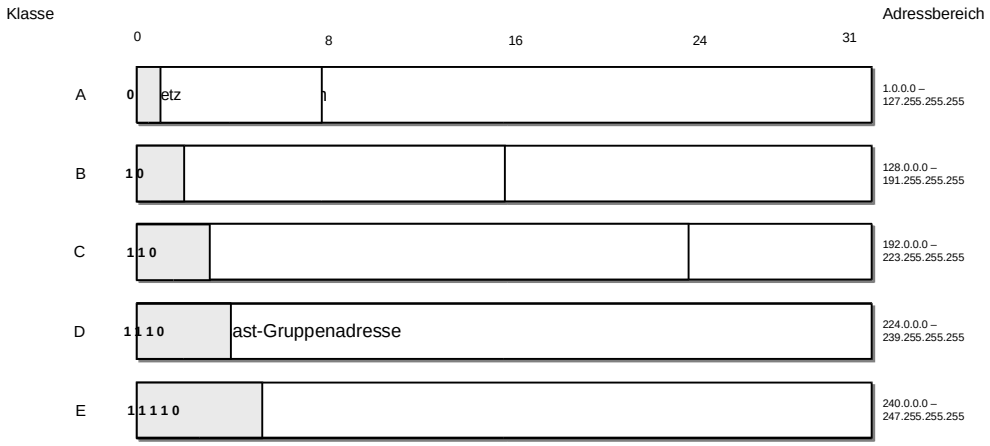
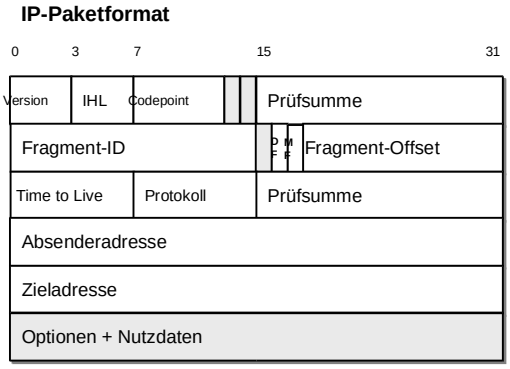


Abb: IP-Adressklassen



Source Port			Destination Port
Sequence Number			
Acknowledgement Number			
Length	reserved	Control Flags	Window Size
Checksum			Urgent Pointer
Options (optional)			
Data (optional)			

Abb: TCP-Paketformat

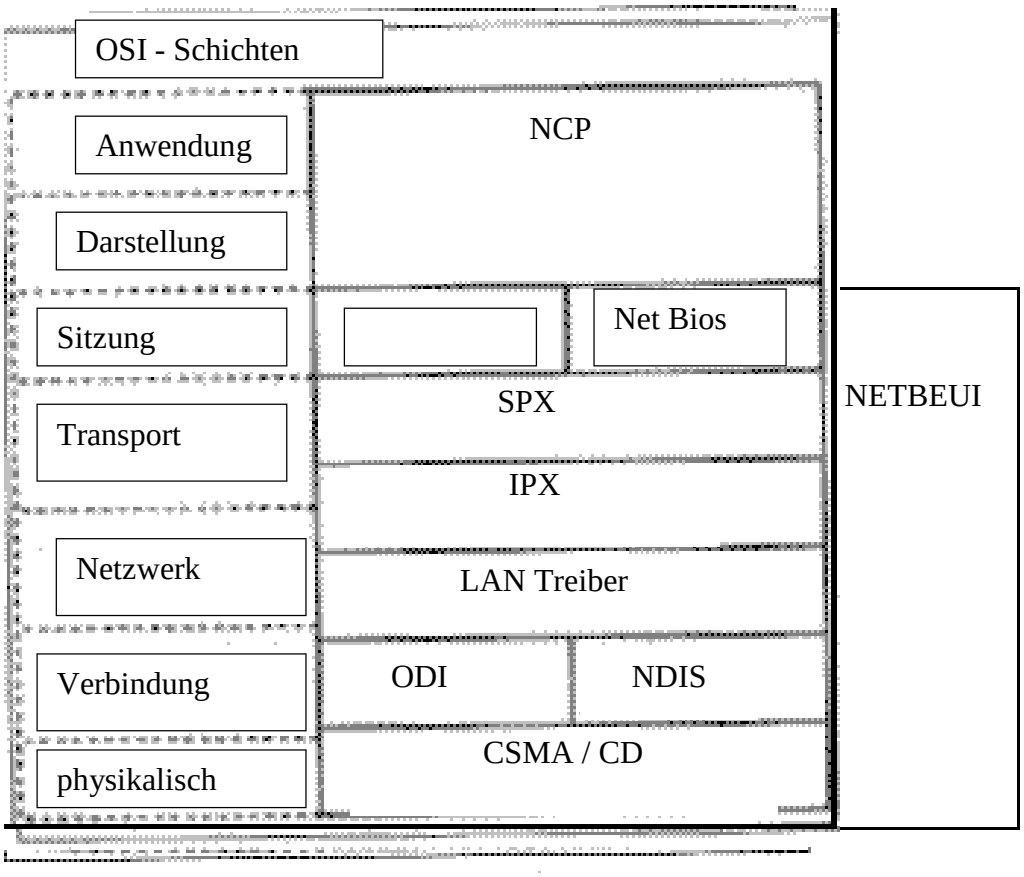
NetBEUI:
Erweiterung von Microsofts "Network Basic Input/output System (Net-BIOS);
schnell aber nicht Routingfähig; kann mit NDIS-Standard koexistieren (je nach Erfordernis)

NDIS (Network Driver Interface Specification)
Ist ein von Microsoft und 3COM entwickelter Standard, der eine Schnittstelle zwischen Netzwerk- Transportprotokoll und der Verbindungsschicht definiert:

- herstellerunabhängige Schicht zwischen NDIS Protokoll und Netzwerkkartentreiber;
- Methode um mehrere (Netzwerk-) Protokolle an einen einzelnen (Karten-) Treiber zu binden;
- umgekehrt kann durch NDIS ein Protokoll an mehrere Adapter (Netzwerkkarten) gebunden werden;

ODI (Open Data Link Interface)

- von Apple und Novell entwickelt (Pedant zu NDIS);
- ursprünglich für Macintosh und NetWare, liefert ebenfalls herstellerunabhängige Schnittstelle um Protokolle an Adapter zu binden;#

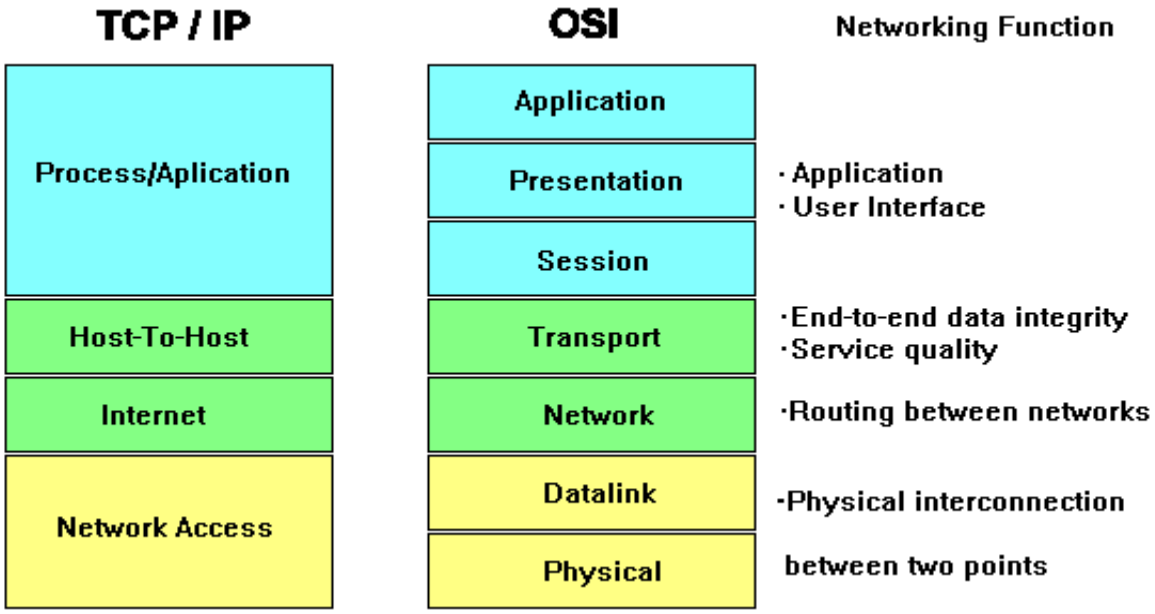


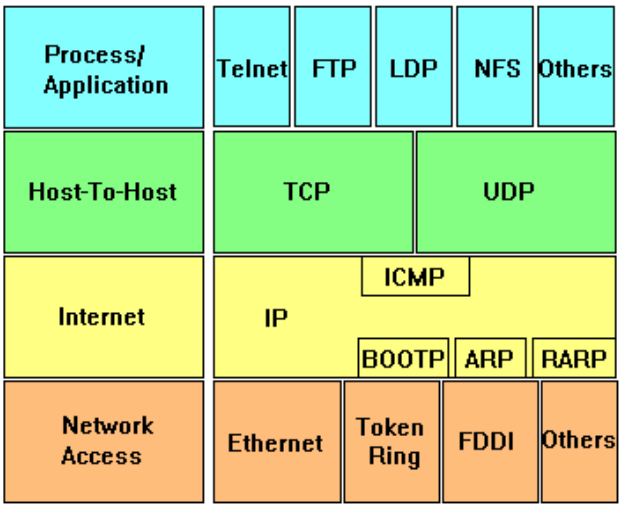
NetBios (Network Basic Input /Output System)

- ist Applikationsschnittstelle für **PC-basierte** (MS) Anwendungen mit unteren Protokollschichten;
- ist nicht routingfähig;

NetBEUI (MS-Netze):

- NetBios Extended User Interface
- NetBEUI ist ein Transportprotokoll welches eine Erweiterung von NetBios darstellt;
- ist nicht routingfähig;
- für kleine isolierte LAN vorgesehen, Datenaustausch unter WINDOWS xx





Kommunikationsgeräte
Die Datenpakete eines Netzwerkes werden von verschiedener Hardware weiter geleitet, um an ihren Zielort zu gelangen. Dadurch werden Netze, wie z.B. das Internet, wie von einer Art Klebstoff zusammen gehalten. Die wichtigsten heißen HUBs, Bridges, Gateways, Repeater und Router.

Repeater
Daten werden oft über lange Strecken übertragen. Auf ihrem Weg werden die physikalischen Signale, welche die Daten repräsentieren, immer kleiner. Damit sie nicht ganz verloren gehen müssen ***Repeater*** die Signale verstärken.

HUBs verbinden Gruppen von Computern. Hubs mit eigener Stromversorgung nennt man *aktive Hubs.* Ein Hub ist ein Multiport Repeater.

Bridges verbinden örtliche Netzwerke veranlassen die Weiterleitung von Daten in ein anderes Netzwerk. Bridges verbinden Kollisionsdomänen - oder umgekehrt- Bridges unterteilen LAN in Kollisionsdomänen. Die Frames werden anhand der MAC-Adresse (Media Access Control) geswitched.

Switches:
Ein Switch ist eine Multiport-Bridge
Switches können mittlerweile Brücken und Router ersetzen. Switches können Daten u. a. nur zu dem Port weiter leiten, der zum Empfangscomputer führt (Routerfunktion). Moderne Switches sind VLAN (virtuall LAN) fähig, d.h sie können auch Broadcastdomänen unterteilen)

Router sorgen dafür, dass die Datenpakete ihren Weg zum Zielort finden. Dabei bevorzugen Router Wege, die schnell oder wenig ausgelastet sind. Router kommen üblicherweise nur zum Einsatz, wenn Daten zwischen verschiedenen Netzwerken zu verschicken sind
(siehe IP-Adressierung, VLAN)

Brouter (Bridge + Router) routet routingfähige Protokolle und agiert als Bridge für nicht routingfähige Protokolle;

Gateways arbeiten ähnlich wie Bridges, nur dass sie auch Daten von anderen Netzwerktypen empfangen können (durch Protokollübersetzung), d.h. ein Gateway kann über alle sieben OSI-Schichten hinweg arbeiten !!

==========
Repeater, HUBs arbeiten auf der physikalischen Schicht;
Brücken arbeiten auf der Sicherungsschicht;
Router und Brouter arbeiten auf der Netzwerkschicht;
Gateways arbeiten i.a. auf der Anwendungsschicht;