Netzwerktechnik

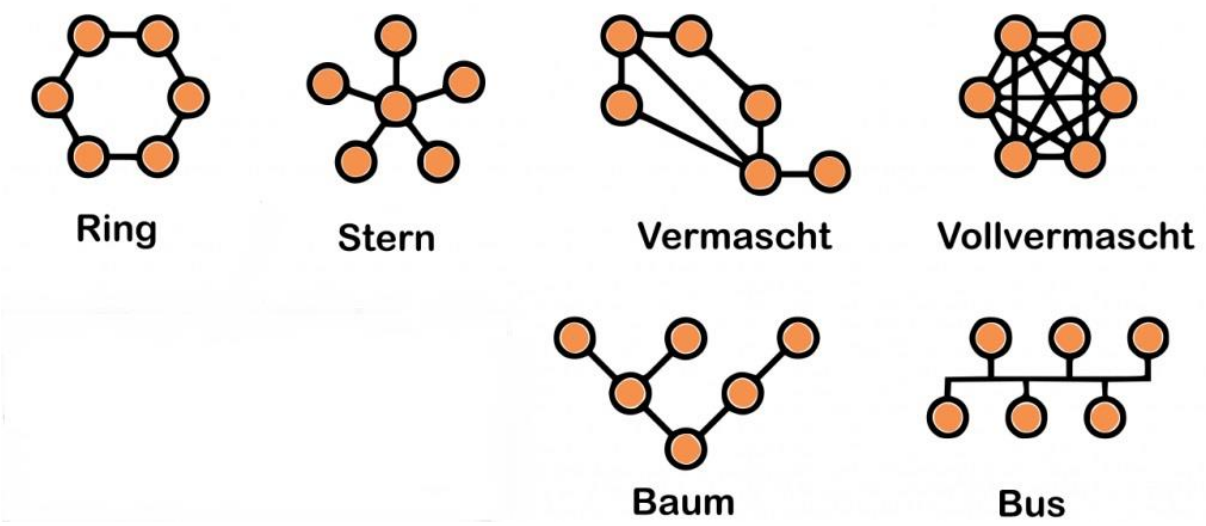
Fachbegriff Netzwerk

Ein „Netzwerk" ist eine Menge von autonomen Objekten, die miteinander auf definierte Weise verbunden sind, und so ein gemeinsames System bilden.
Ihre Verbindung zu einem System dient einem bestimmten Zweck:
Der Kommunikation oder der gemeinsamen Nutzung von Ressourcen.
Computer Netzwerk:
Ein Netzwerk welcher Computer zum Zweck der Kommunikation verbindet nennen wir ein Computer Netzwerk.
Oder…
Mehrere Geräte (PC, Handy, Server,) (min.2) die in einem Netzwerk miteinander kommunizieren und sich die Ressourcen gemeinsam teilen (z.B. einen File Server, Internet,).

Heutige Netzwerke sind in der Regel etwas komplexer und bestehen nicht einfach nur aus zwei Computern. Bei Systemen mit mehr als zehn Teilnehmern kommen standardmäßig Server-Client-Netzwerke zum Einsatz. Hierbei stellt ein Rechner als zentrale Schaltstelle (Server) seine Ressourcen den anderen Teilnehmern des Netzwerks (Clients) zur Verfügung.

Kenntnis der Netzwerktopologien wie Stern, Ring, Bus, Baum, Masche

Topologie ist die Anordnung der Rechner im Netz (Verbindungen zwischen Rechnern).



Sternstruktur:
Jedes Gerät hat eine eigene Leitung zu einem zentralen Knoten.
Die Leistungsfähigkeit des Knotens ist ausschlaggebend für die Geschwindigkeit des Netzwerkes.

Eigenschaften:
Die Zentrale (Hub, Switch) sendet die Daten weiter.
Fällt ein Rechner aus, bleibt das Netzwerk erhalten.
Nur wenn die Zentrale ausfällt kommt das Netzwerk zum Erliegen.

Ringstruktur:
Die teilnehmenden Stationen werden ringförmig über ein Kabel verbunden.
Die Datenübertragung erfolgt (meist) nur in eine Richtung (single)
Es ist auch möglich die Richtung der Übertragung im Ring zu ändern – mit zwei Leitungen (dual)
Die Station erkennt die an sie gerichtete Nachricht und nimmt sie aus dem Ring.

Eigenschaften:
keine Zentrale Einheit
Teilnehmer durch Verbindungen „aufgefädelt" - keine Anschlusswiderstände
Empfänger und Weiterleiter leiten Nachricht maximal einmal durch den Kreis

Busstruktur:
Teilnehmer hängen gemeinsam an Bus-Leitung durch T-Stück
Hauptkabel muss terminiert werden, sonst entsteht Echo (Abschlusswiderstände).

Eigenschaften:
Nur ein Rechner kann (gleichzeitig) Daten senden
Diese „wandern über die Leitung, bis die angesprochene Adresse (der Rechner) die Daten annimmt, oder das Ende der Leitung erreicht wurde (Terminierung)

Baumstruktur:
Die Knoten sind hierarchisch (nach Rangordnung gegliedert) angeordnet.
Entspricht im wesentlichem einem Netzwerk mehrerer hierarchisch angeordneten Sterntopologien

Eigenschaften:
Ausgehend von der Wurzel (root) gibt es eine Menge von Verzweigungen zu weiteren Knoten (nodes), bis zu den letzten Stufen - Blatt (leaf).
Direkte Kommunikation der Teilnehmer über den übertragenden Knoten.

Vermaschte Struktur:
Direkte Verbindung von einem Rechner zu mehreren anderen (mehrere Verbindungswege).
Es muss nicht jeder Rechner mit jedem verbunden sein (=Vollvermascht).

Kenntnis der Vor- und Nachteile der jeweils eingesetzten Netzwerktopologien

Sternstruktur:
Vorteile:
Ausfall eines Gerätes (ausgenommen Zentrale) betrifft nur dieses Gerät.
Fehler leicht zu lokalisieren.
Nachteile:
Höherer Verkabelungsaufwand (gegenüber Bustopologie).
Fällt Zentrale aus > fällt das Netzwerk aus.
Übertragungsrate von Zentrale abhängig (z.B. Hub niedrig, Switch hoch).
Sicherheit und Vertraulichkeit von der Konfiguration der Zentrale abhängig.

Ringstruktur:
Vorteile:
Keine Kollisionen (siehe auch Zugriffsverfahren).

Dual beide Richtungen möglich, wenn ein Ring ausfällt, wird zweite Leitung verwendet.
Nachteile:
Bei Ausfall eines Rechners, fällt das Netz aus.
Höherer Verkabelungsaufwand

Busstruktur:
Vorteile:
Geringer Kabelaufwand
Leichte Erweiterbarkeit
Ausfall eines Rechners betrifft nicht das gesamte Netzwerk
Nachteile:
Bei defektem Bus kommt das gesamte Netzwerk zum Erliegen
Schwierige Fehlersuche
Sicherheit und Vertraulichkeit (Sniffer)

Baumstruktur:
Vorteile:
Ausfall eines Gerätes hat keine Auswirkung auf das Netzwerk
Nachteile:
Ausfall einer Sterntopologie führt zum Ausfall des nachfolgenden Baums (Sternstrukturen)

Vermaschte Struktur:
Vorteile:
Ausfallsicher, da mehrere Verbindungswege möglich sind.
Ausfall eines Rechners führt nicht zum Ausfall des Netzwerkes.
Nachteile:
Hoher Verkabelungsaufwand
Komplexes Routing

Funktionsprinzip eines Routers, Switches

Funktionsprinzip eines Routers:
Können mehrere Netzwerke mit unterschiedlichen Protokollen und Architekturen miteinander verbinden.
Arbeitet auf der Vermittlungsschicht (Schicht 3) des OSI-Schichtmodells.
Ein gemeinsames Protokoll in der Schicht 3 ist notwendig (z.B. IP)
Er filtert defekte Pakete.
Ein Router hat mindestens zwei Netzwerkanschlüsse.
Jede Schnittstelle hängt auf Schicht 1+2 in einem anderen Netz.
Auf Schicht 3 werden die Datenpakete von Router zu Router in das Ziel-Netz weitergeleitet.
Der Sender braucht zur Verbindung mit seinem Ziel nur dessen IP-Adresse kennen. Ziel-MAC ist die MAC-Adresse des Gateways (= Router Schnittstelle)
Er besitzt eine Routing Tabelle, die angibt, über welchen Anschluss des Routers ein Netz erreichbar ist.
Routingtabelle setzt sich zusammen aus:
Ein Ziel, bestehend aus Adresse und Subnetmaske.
Ein Gateway, die nächste Station zum Ziel.
Ein Interface, über welches das Paket versendet werden soll.
Die Metrik (Um Routen zu bevorzugen, wenn es mehrere Routen für ein Ziel gibt).
Es handelt sich hierbei um ein dynamisches Verfahren, das Ausfälle und Engpässe ohne Eingreifen eines Administrators berücksichtigen kann.

Die Aufgabe eines Routers:

Ermittlung der verfügbaren Routen
Auswahl der geeignetsten Route
Herstellen der Verbindung
Anpassen der Datenpakete an die Übertragungstechnik (Fragmentierung)

Router-Varianten:

Backbone-Router
Hardware-Router
Layer-3 Switch (Switches, VLAN, Routing-Funktion)
Software-Routing (2 NW-Karten)
DSL-Router, WLAN-Router (Eingeschränkte Funktionalität, NAT/PAT (Access Points sind keine Router - OSI-2)

Routingverfahren:

Next Hop-Routing: Was ist die nächste Station zum Ziel
Source Routing: Die gesamte Route ist bekannt.

Funktionsprinzip eines Switches:

Ein Switch ist ein Kopplungselement (Verteiler), das mehrere Stationen in einem Netzwerk miteinander verbindet.
In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Switch als Verteiler für die Datenpakete.
Arbeitet auf Schicht 2 des OSI Layer (Data Link Layer).
Ist schneller und sicher als ein Hub.
Benötigt kein CSMA/CD Verfahren.
Full Duplex Betrieb ist möglich.
Frames werden anhand der MAC-Adresse übermittelt.
Er untersucht die Zieladresse (MAC Adresse) jedes eingehenden Frames, und sendet diesen dann an den Port, laut Switching-Tabelle, weiter.
Er merkt sich die MAC-Adresse und den dazugehörigen Port.
Switching-Tabelle beinhaltet die MAC-Adresse und den Physische Port.
Im Unterschied zum Hub werden Frames nur an den Port weitergeleitet, der für die entsprechende Zieladresse in der Switching-Tabelle gelistet ist.
Ist der Port nicht bekannt, dann sendet der Switch die Frames an alle Ports. (Broadcast)
Ein Hub limitiert die Bandbreite des Netzwerks, beim Switch steht die volle Bandbreite für die Verbindung zwischen zwei Stationen zur Verfügung.

Switches unterscheidet man hinsichtlich ihrer Leistungsfähigkeit mit folgenden

Eigenschaften:

Anzahl der speicherbaren MAC-Adressen für die Quell- und Zielport Verfahren.
Wann ein empfangenes Datenpaket weitervermittelt wird (Switching-Verfahren).
Latenz (Verzögerungszeit) der vermittelten Datenpakete.
Die Anzahl der Adressen, die ein Switch aufnehmen kann, hängt von seinem internen Speicher ab. Ein Qualitätsmerkmal eines Switches ist, wie viele Adressen er insgesamt und pro Port speichern kann.

Unicast: An ein Endgerät Adressieren
Multicast: An mehrere Geräte oder eine Gruppe Adressieren
Broadcast: An alle Geräte im Netzwerk Adressieren

Kenntnis des Fachbegriffes Subnetzmaske u. deren technischen Zusammenhänge

Ein Subnetz bzw. Teilnetz ist ein physikalisches Segment eines Netzwerks, in dem IP-Adressen mit der gleichen Netzwerkadresse benutzt werden. Diese Teilnetze können über Router miteinander verbunden werden.
Subnetting bedeutet die Aufteilung eines zusammenhängenden Adressraums von IP-Adressen in mehrere kleinere Adressräume.
Jede IP-Adresse besteht aus einem Netzwerkteil und Hostteil.
Die Subnetzmaske bestimmt, wo sich die IP-Adresse teilt.
Gibt an, wie viele Bits am Anfang der IP-Adresse der Netzwerkteil ist.
Der Netzwerkteil muss bei allen Geräten des jeweiligen Netzes gleich sein.
32 Bit Länge (bei IPv4 in 4 x 8 Bit unterteilt).
Binäre Darstellung ist wichtig, um den Aufbau und die Berechnung zu verstehen.
Im Netzwerkteil sind lauter 1, im Hostteil lauter 0.

Zwei Darstellungsarten:

Dezimal
212.124.128.44
255.255.255.0

Längenschreibweise / Suffix
212.124.128.44 /24

Kenntnisse über das OSI-Modell

Die IOS (ISO) International Organisation for Standardisation versucht weltweit gemeinsame Standards zu schaffen.

OSI = Open Systems Interconnection
Definition der Netzwerkkommunikation in 7 Schichten
Universell für verschiedene Systeme anwendbar
Jede Schicht hat spezifische Aufgaben und Funktionen

	ISO/OSI Schicht	TCP/IP Schicht	Protokolle
7	Application Layer (Anwendungsschicht)	Application Layer	HTTP, SMTP, FTP, DHCP, Telnet
6	Presentation Layer (Darstellungsschicht)		
5	Session Layer (Sitzungsschicht)		
4	Transport Layer (Transportschicht)	Transport Layer	TCP, UDP
3	Network Layer (Vermittlungsschicht)	Internet Layer	IP, IPsec, IPv6, ICMP
2	Data Layer (Sicherungsschicht)	Network Access Layer	Ethernet
1	Physical Layer (Bitübertragungsschicht)		

Das 7 Schichten Modell:

7. Application Layer (Anwendungsschicht)
   Beschreibt die Anwendung selbst.

6. Presentation Layer (Darstellungsschicht)
   Beschreibt das Format der Daten, die übertragen werden.

5. Session Layer (Kommunikationssteuerschicht)
   Beschreibt den Ablauf der Kommunikationssitzungen.

4. Transport Layer (Transportschicht)
   Beschreibt die Übertragung von Daten zwischen Prozessen.

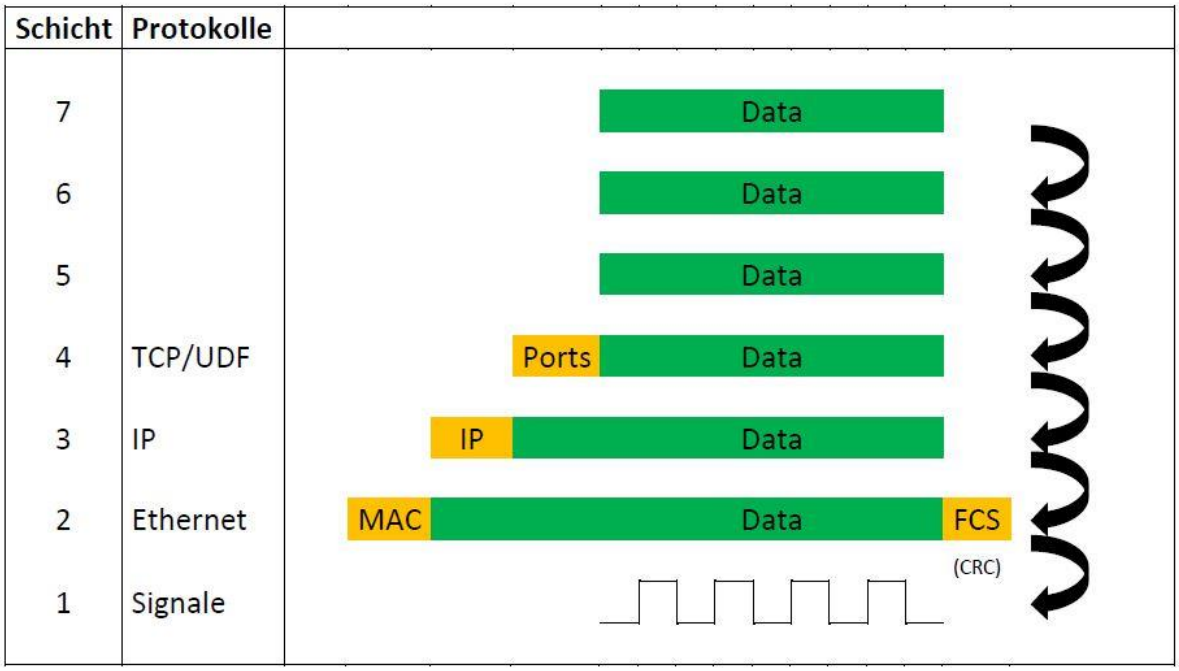
3. Network Layer (Vermittlungsschicht)
   Beschreibt die Übertragung von Daten zwischen unterschiedlichen Netzen.

2. Data Link Layer (Sicherungsschicht)
   Beschreibt die Übertragung von Daten in einem abgeschlossenen Netzwerk.

1. Physical Layer (Bitübertragungsschicht)
   Beschreibt die Übertragung von Bits in der Form von Signalen auf einem Medium.

Einordnung:
Schicht 5-7: Anwendungsorientiert
Schicht 1-4: Transportoriendiert

Datenverkapselung



Der PC, der sendet, beginnt bei Schicht 7. Die Verarbeitung des Pakets läuft bis Schicht 1.
Der empfangende PC beginnt bei Schicht 1. Die Verarbeitung des Pakets läuft bis Schicht 7.

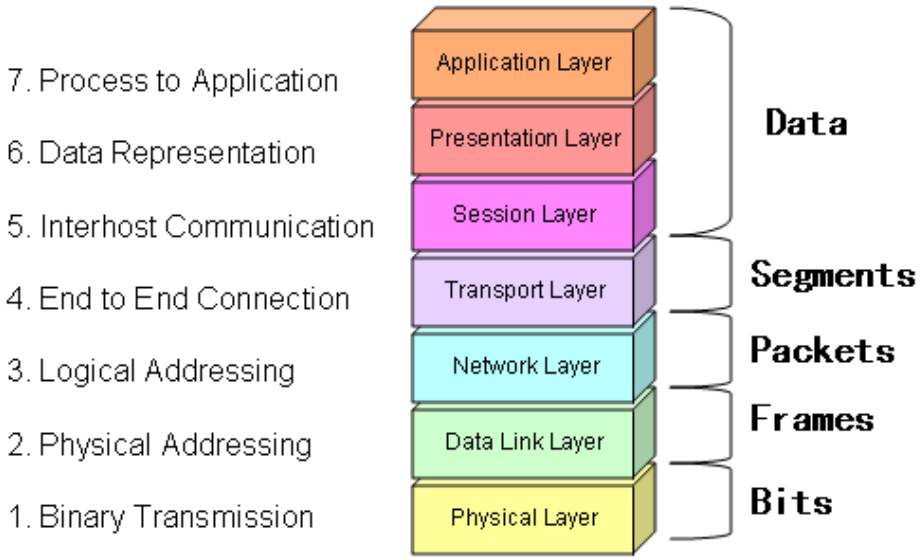
Einordnung von Protokollen in das OSI-Modell

Protokolle in den jeweiligen Schichten!

Application Layer: HTTP, HTTPS, SMTP, FTP, LDAP, NCP
Presentation Layer: HTTP, HTTPS, SMTP, FTP, LDAP, NCP
Session Layer: HTTP, HTTPS, SMTP, FTP, LDAP, NCP

Transport Layer: TCP, UDP, Port, SPX, SCTP
Network Layer: IP, IPX, ICMP, IGMP
Data Link Layer: ARP, MAC, FDDI
Physical Layer: Ethernet, Token Ring

Einheiten:
Schicht 5-7: Daten
Schicht 4: Segmente
Schicht 3: Pakete
Schicht 2: Rahmen (Frames)
Schicht 1: Bits



Einordnung von Netzwerk- und Hardwaregeräten in das OSI-Modell

Application Layer: Gateway, Switch
Presentation Layer: Gateway, Switch
Session Layer: Gateway, Switch

Transport Layer: Content Switch
Network Layer: Router, Layer 3 Switch
Data Link Layer: Layer 2 Switch, Bridge
Physical Layer: Ethernet Kabel, Hub, Repeater

Kenntnisse über die Protokollfamilie TCP/IP

Transmission Control Protocol / Internet Protocol
IP ist auf der Vermittlungsschicht (Schicht 3) des OSI-Schichtenmodells angeordnet.
TCP ist auf der Transportschicht (Schicht 4) des OSI-Schichtenmodells angeordnet.
Wird für den Transport von Datenpaketen in einem Netzwerk verwendet.
Wird im LAN und WAN verwendet.
Grundlage, um im Internet zu kommunizieren.
Universell und unabhängig für alle gängigen Betriebssysteme.

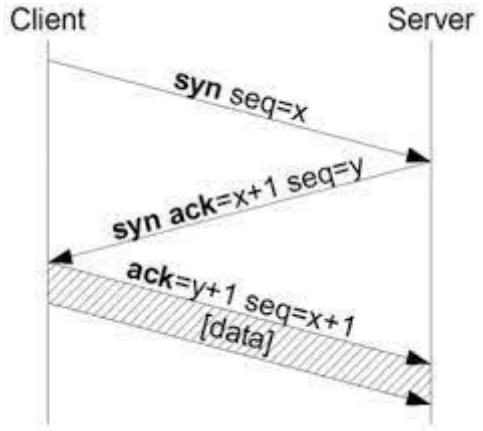
Hauptmerkmale TCP:
TCP - Ist eine gesicherte Verbindung.
Die dafür sorgt das Datenpakete…
vollständig
unverändert
und in der richtigen Reihenfolge beim Empfänger ankommen.
Ist ein Protokoll der OSI Schicht 4
Voll-Duplex Verbindung
Fehlererkennung
Flusssteuerung
Verhindert, dass ein langsamer Empfänger von einem schnellen Sender mehr Pakete bekommt, als er verarbeiten kann.
Staukontrolle
Ähnlich wie Adaptive-Cut-Through (Bei zu vielen Fehlern Datenrate drosseln)
Verbindungsorientiertes Protokoll
Pakete werden in der richtigen Reihenfolge gesendet

Lokaler PC kann 2 Verbindungen mit gleicher IP und Port herstellen, sofern der gegenüberliegende PC andere Ports benützt.
Verbindung 1: (Lokaler Rechner, Port x, Entfernter Rechner, Port y)
Verbindung 2: (Lokaler Rechner, Port x, Entfernter Rechner, Port z)

Eine TCP-Verbindung ist durch folgende 4 Werte eindeutig identifiziert:
Quell-IP-Adresse
Quell-Port
Ziel-IP-Adresse
Ziel-Port

3 Way Handshake Verbindungsaufbau:
Client sendet Paket (SYN)
Server bestätigt, dass er das Paket erhalten hat (SYN ACK)
Client bestätigt, dass er das Bestätigungspaket des Servers erhalten hat (ACK)
Senden der Daten

3 Way Handshake Verbindungsaufbau



Funktionen:

Logische Adressierung / Logical Adressing (IP)

Sorgt dafür, dass ein großes Netzwerk in Segmente geteilt wird. IP übernimmt die logische Adressierung so das Datenpakete nur in das Netz gelangen, in das sie gehören.

Wegfindung /Routing (IP)

Dient zu Wegfindung, dass ein Datenpaket sein Ziel erreicht.

Fehlerbehandlung und Flussteuerung / Error Control and Flow Control (TCP)

Durch TCP stehen Sender und Empfänger ständig in Kontakt zueinander, und tauschen Kontrollmeldungen aus. Tritt ein Fehler auf, wird das Datenpaket erneut übertragen. Zusätzlich wird eine Daten-Flusssteuerung verwendet, um die verfügbare Übertragungsgeschwindigkeit auszunutzen.

Anwendungsunterstützung / Application Support (TCP)

Dient dazu, um die Kommunikationsverbindungen zwischen spezifischen Anwendungen zu unterscheiden. TCP- und UDP-Ports dienen dazu, um diese voneinander unterscheiden zu können.

Namensauflösung / Domain Name System (DNS)

Um eine Verbindung auf IP-Ebene möglich zu machen, ist eine Namensauflösung notwendig. Das heißt, dass zu einem Computer oder Domain-Namen eine zugehörige IP-Adresse ermittelt wird.

Vorteile von TCP/IP:

Jede Anwendung ist mit TCP/IP in der Lage über jedes Netzwerk Daten zu übertragen und auszutauschen.

Fachbegriff IPv4-Adresse und deren Aufbau

Ist eine Adresse in Computernetzen, die auf dem Internetprotocol (IP) basiert.
Sie wird Geräten in einem Netz zugewiesen, damit sie erreichbar sind und dass Daten zwischen Absender und Empfänger transportiert werden können.
Kann einen einzelnen Empfänger oder eine Gruppe von Empfängern bezeichnen (Multicast, Broadcast)
Ein Computer kann auch mehrere IP-Adressen haben. - (2. Netzwerkkarte)
Besteht aus Netz- und Hostteil der mit der Subnetmaske unterteilt wird.

Unterteilt in 4 Oktetten (Bytes), 1 Oktett besteht aus 8 bit,
Gesamt: 4x8 bit= 32 bit, 32-stellig (binär)
Damit sind 2 hoch 32, also 4.294.967.296 Adressen möglich.
Darstellung in Dezimalzahlen, Werte 0-255.

Statische IP-Adresse:
Fixe IP-Adresse, die sich nicht ändert.

Dynamische IP-Adresse:
Wird dynamisch mittels DHCP (Dynamic Host Configuration Protocol) vergeben.

Kenntnisse über IPv6-Adressierung

IPv6-Adressen sind 128 Bit lang.
Ist der direkte Nachfolger von IPv4 und Teil der Protokollfamilie TCP/IP.
Wegen Adressknappheit eingeführt (4 Milliarden IPv4 Adressen reichen nicht mehr aus)
Aufbau in 8 Blöcke mit jeweils 16Bit = 128bit, also 2 hoch 128 -IP-Adressen möglich.
Hexadezimale Darstellung der Adresse
Zur Verkürzung können Nullen am Beginn eines Blocks, oder wenn ein Block nur Nullen hat, weggelassen werden.
Die Adresse wird durch eine Präfixlänge in einen Netzwerkteil und Geräteteil getrennt.
Die ersten 64 Bit bilden das Präfix, die letzten 64 Bit bilden bis auf Sonderfälle einen für die Netzwerkschnittstelle eindeutigen Interface-Identifier.
Durch Nutzung des Dual-Stack Verfahren werden allen Schnittstellen neben der IPv4-Adresse zusätzlich mindestens eine IPv6-Adresse und die notwendigen Routinginformationen zugewiesen. Rechner kann dann über beide Protokolle unabhängig kommunizieren.

Unterscheidung von public /private IP-Adressen

Public IP-Adressen:
Sind IP-Adressen, die nur einmal vergeben werden, nur von einem Gerät verwendet werden.
Werden vom Provider vergeben.
Können statisch oder dynamisch sein.
Kann nicht in einem privaten Netzwerk verwendet werden.
Kein direkter Zugriff auf private Adressen möglich.

Private IP-Adresse:
Sind bestimmte IP-Adressbereiche, die im Internet nicht verwendet und nicht geroutet werden.
Werden ausschließlich in privaten Netzen verwendet.
Sind nach außen ins Internet nicht sichtbar, - bringt Verschleierung und Anonymität bei Internetzugriffe nach außen.
Können im privaten Netz ohne administrativen Aufwand verwendet werden
Der private Adressbereich ist immer nur innerhalb des privaten Netzes sichtbar, und kann somit auch in anderen privaten Netzen verwendet werden.
Dient zur Einsparung von IP-Adressen.
Wenn das private Netz einen Router (NAT) hat, der eine private und
eine öffentlich IP-Adresse hat, dann kann dieser einen Internetzugang herstellen.

Kenntnis der privaten IP-Adress-Bereiche

Private IP-Adressbereiche – RFC 1918
Festgelegt von der IANA (Internet Assigned Numbers Authority)

Klasse A 10.0.0.0 /8 10.0.0.0 - 127.255.255.255 = 16,7 Mio. Adressen (224)
Klasse B 172.16.0.0 /12 172.16.0.0 - 172.31.255.255 = 1 Mio. Adressen (220)
Klasse C 192.168.0.0 /16 192.168.0.0 - 192.168.255.255 = 65.635 Adressen (216)

Fachbegriff MAC-Adresse und deren Aufbau

MAC (Media Access Control):
Die MAC-Adresse (Media Access Control) stellt die physikalische Adresse einer Netzwerkschnittstelle dar. Sie ist eindeutig und besitzt eine Länge von 48 Bit.
MAC-Adressen kommen beispielsweise im Ethernet und Token Ring aber auch bei Bluetooth und WLAN zum Einsatz.
Dient zur eindeutigen Kennzeichnung eines Gerätes im LAN. (OSI Schicht 2)
Fix im ROM der Netzwerkkarte.
Aufbau:
48 Bit Adressen, verkürzte Schreibweise als 12-stellige Hexadezimalzahl)
> 00-00-5E-00-01-ID
Getrennt durch Doppelpunkte (00:80) oder Minus (00-80)
Die ersten 24 Bit > Herstellerkennung (Organisation Unique Identifier= OUI).
Die hinteren 24 Bit > Laufende Nummer des Herstellers des Netzwerkgeräts.

Fachbegriff Ethernet

Meist verbreitete LAN-Technologie
Ist eine Hardware und Softwaretechnologie zum Datenaustausch in Form von Frames in einem LAN.
Ethernet wurde als Konzept für lokale Netzwerks und die damit verbundene gemeinsame Nutzung eines Datenmediums entwickelt
Basiert auf dem Standard IEEE 802.3 (Institute of Electrical and Electronics Engineers)
Ursprünglich wurde eine Bustopologie (Thick Ethernet) mit CSMA/CD-Verfahren genutzt (10Mbit/s)
Ständige Weiterentwicklung -10 Mbit/s, 100 MBit/s, 1 GBit/s, 10 GBit/s, 40 GBit/s, 100GBit/s
Definiert auf OSI Schicht 2 die Adressierung und Zugriffskontrolle auf unterschiedlichen Übertragungsmedien.
Zugriff auf das Medium mit dem CSMA/CD-Verfahren (Carrier Sense Multiple Access and Collision Detection).

Zentrale Komponenten:
Ethernet Frame
CSMA/CD Verfahren
Ethernet-Standards
Ethernet transportiert Daten paketweise. Als sogenannte FRAMES.
Ethernet überträgt die Daten ohne Garantie das diese innerhalb einer bestimmten Zeit den Empfänger erreichen. Deswegen verwerfen Ethernet Komponenten Datenpakete, wenn nicht genügend Bandbreite verfügbar ist. Wegen der unzuverlässigen Übertragungstechnik ist Ethernet auf die Intelligenz höherer Protokolle angewiesen.

Erweiterungen:

Ermöglicht den Geräten die bestmöglichen Übertragungseigenschaften automatisch zu erkennen und zu konfigurieren
10 oder 100 Mbit/s, Halb- oder Vollduplex
Überprüfung auf Optimum

CSMA/CD- Carrier Sense Multiple Access / Collission Detection:

ist ein System entwickelt um bei gemeinsamer Nutzung eines Übertragungsmediums (Kabel), Informationsverlust vermeiden, und durch Collission Detection ggf. Pakete erneut senden.

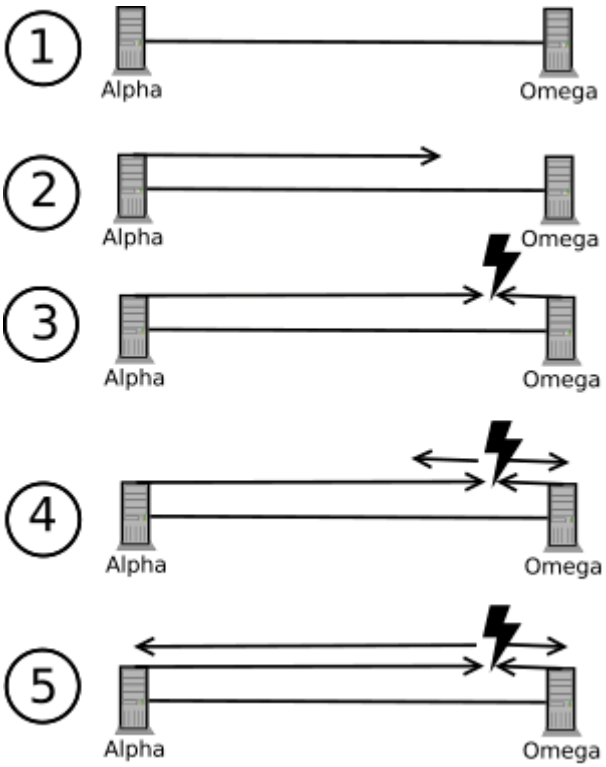
1. Station Alpha hat einen Rahmen an Station Omega gesendet, die Entfernung der beiden Stationen voneinander entspricht der maximal möglichen Ausdehnung des Ethernets.

2. Kurz bevor der Rahmen die Station Omega erreicht, sendet auch diese Station einen Rahmen, da zu diesem Augenblick die Leitung an ihrer Stelle noch nicht belegt ist.

3. Die beiden Ethernet-Rahmen kollidieren, die Kollision wird zuerst von Station Omega bemerkt.

4. Station Omega sendet das Jamming-Signal. Da der Beginn des Rahmens von Station Omega noch auf dem Netz ist, läuft die Kollision vor dem Jamming-Signal in die Richtung von Station Alpha. Diese Station darf die Übertragung des Rahmens noch nicht beendet haben, da sie sonst die Kollision nicht bemerken würde.

5. Die Kollision hat auch Station Alpha erreicht, die ebenfalls das Jamming-Signal sendet. So liegt für einen kurzen Augenblick auf dem gesamten Netz dieses Signal. Nach der Backoff-Zeit versuchen beide Stationen Alpha und Omega, erneut ihre Rahmen zu senden.



Flow Control (Flussteuerung):
Wenn ein Host zu viele Datenpakete bekommt und mit der Verarbeitung nicht mehr nachkommt, besteht die Gefahr das die Datenpakete teilweise verworfen werden. Mit der Flussteuerung signalisiert der Host (Pause Paket) der Gegenstelle eine Sendepause einzulegen.

Broadcastdomäne:
Ein Switch bekommt ein Datenpaket das er keinem Empfänger (Port) zuordnen kann
Der Switch sendet dann das Datenpaket an alle Ports. Er sendet also einen Broadcast.
In der Regel kommt dann auf einem Port das Antwortpaket, und der Switch weiß dann, an welchen Port er alle weiteren Pakete schicken soll.
Die Reichweite des Broadcasting nennt man Broadcastdomäne. Sie umfasst alle Host, die auf Schicht 1 und 2 erreichbar sind. Die Broadcastdomäne endet dort, wo der Übergang in ein anderes Netzwerk über ein anderes Protokoll erfolgt. In der Regel an einem Router.

Fachbegriff xDSL

DSL (Digital Subscriber Line):
xDSL = x..Platzhalter für A, S oder V

Unterscheidung zwischen ADSL (asymmetrisch) und SDSL (symmetrisch)
ADSL Up- und Downloadgeschwindigkeit unterschiedlich
SDSL Up und Downloadgeschwindigkeit gleich
Leistungsgebunde Breitbandtechnologie
Nutzt vorhandene Kupfer Telefonkabel
Max. Dämpfung 5km vom Knoten weg
Teilnehmer benötigt Splitter und Modem
Splitter teilt die Leitung in Daten und Telefonie auf – Frequenzweiche.
Über analogen Telefonanschluss (POTS) oder digitalen Telefonanschluss (ISDN = Integrated Services Digital Network)
ASDL über ISDN -> 8 Mbit/s down 1 Mbit/s up
Ständige Erhöhung der Geschwindigkeiten.

VDSL (Very High Speed Digital Subscriber Line) Der wichtigste Unterschied zum DSL:
VDSL ermöglicht Übertragungsraten mit einer Download-Geschwindigkeit von bis zu 50 MBit/s und eine Upload-Geschwindigkeit von bis zu 10 MBit/s.

Unterscheidung der Fachbegriffe Upload, Download

Upload:
Geschwindigkeit, mit der man Informationen ins Internet versenden kann.
Hochladen oder Hinaufladen bezeichnet einen Datenfluss vom lokalen Rechner oder einem lokalen Speichermedium zu einem entfernten Rechner

Download:
Geschwindigkeit, mit der man Informationen vom Internet empfangen kann.
Herunterladen bezeichnet man das Empfangen von Daten auf dem eigenen Computer.

Fachbegriff WLAN

WLAN (Wireles Local Area Network):

Ist ein lokales drahtloses Netzwerk/Funknetz.
Übertragung per Funk
Standard IEEE 802.11
Wird ständig erweitert um Datendurchsatz, Effizienz, Reichweite und Datensicherheit zu erhöhen.

Standard (IEEE)	Frequenz	Streams	Datenrate bei Kanalbreite			
			20 MHz	40 MHz	80 MHz	160 MHz
802.11	2,4 GHz	1	2 MBit/s			
802.11b	2,4 GHz	1	11 MBit/s			
802.11a/h/j	5 GHz	1	54 MBit/s			
802.11g	2,4 GHz	1	54 MBit/s			
802.11n	2,4 GHz 5 GHz	1 2 3 4	75 MBit/s 150 MBit/s 225 MBit/s 300 MBit/s	150 MBit/s 300 MBit/s 450 MBit/s 600 MBit/s		
802.11ac	5 GHz	1 2 3 4 5...8			433 MBit/s 867 MBit/s 1.300 MBit/s 1.733 MBit/s 3.400 MBit/s	867 MBit/s 1.733 MBit/s 2.300 MBit/s 3.500 MBit/s 6.936 MBit/s
802.11ax	2,4 GHz 5 GHz	1 2 3 4 5...8	144 MBit/s 287 MBit/s 432 MBit/s 574 MBit/s	287 MBit/s 574 MBit/s 861 MBit/s 1.144 MBit/s	600 MBit/s 1.201 MBit/s 1.801 MBit/s 2.402 MBit/s bis 4.804 MBit/s	1.201 MBit/s 2.402 MBit/s 3.603 MBit/s 4.804 MBit/s bis 9.608 MBit/s

Erweiterungen des IEEE 802.11 Standards:

a (54 Mbit/s)
b (11 Mbit/s)
h (54 Mbit/s)
g (54 Mbit/s)
n (600 Mbit/s)
ac (6,9 Gbit/s)
ax (6,7 Gbit/s)

Ist besonders dort interessant wo die Kosten für die Verlegung von Kabeln zu hoch ist, oder die Verkabelung unmöglich ist.

Verschlüsselungen:

WPA, WPA2, WEP, IPSEC

Frequenzbereich:

Bei modernen Routern kann man zwischen 2,4 und 5 Ghz Bereich wählen. Sämtliche eingesetzte Geräte und Stationen müssen den gewählten Frequenzbereich unterstützen.

WLAN 2,4 GHz:

In 14 Kanäle aufgeteilt (die ersten 13 verwendbar).
Weitverbreitester eingesetzter Frequenzbereich.

Max. 100mW Sendeleistung.
Kompatibilität mit älteren Endgeräten.

WLAN 5 Ghz:
Bietet höhere Bandbreiten.
Ist nicht so anfällig für Störungen.
Hat aber eine kürzere Reichweite als 2,4 GHz.
Höhere Sendeleistung bis zu 1000mW.
Nicht kompatibel mit älteren Access Points.
Verwendet MIMO (multiple Input, multiple Output) > mehrere Verbindungen gleichzeitig.

Richtfunk:
Dient zum Überbrücken von Entfernungen über mehrere Kilometer (Sichtverbindung!) durch spezielle Antennen.
Einsatz bei:
Schwieriger bzw. unmöglicher Kabelverlegung, wenn Mobilität wichtig ist.

Fachbegriff Access-Point

Ist ein Zugangspunkt zu einem Netzwerk.
Ermöglicht die Verbindung von einem WLAN zu drahtgebundenen LAN.
Um Mobilen Endgeräten die Ressourcen im lokalen Netz zugänglich zu machen.
Um die Reichweite zu erhöhen.
Meist in Kombination mit einem DSL-Router (Für Internet und WLAN)

Verbindungsarten/Betriebsarten:

AdHoc – Modus (direkte Verbindung, 2 oder mehr Clients)
Alle Stationen sind gleichwertig
Alle Stationen können untereinander eine Verbindung aufbauen
Alle Stationen benutzen denselben Netzwerknamen (SSID) und die festgelegte Verschlüsselung.
Da aber kein Access Point benutzt wird übernehmen die Stationen selbst die Koordination.
Es gibt keine Weiterleitung von Daten, sondern immer nur eine direkte Kommunikation zwischen den Stationen.
Abhilfe wäre die Ausstattung einer Routing-Fähigkeit der teilnehmenden Stationen.
Durch die direkte Kommunikation der Stationen ist die Reichweite sehr begrenzt, da sich die Stationen sehr nahe sein müssen.
Einsatz bei Notebooks, Smartphones, Sensoren und Aktoren.

Infrastruktur - Modus (mit Access Point)
Ähnlich wie Mobilfunk, nutzt er einen Wireless Access Point (oft ein Router), der kleine Datenpakete an alle Stationen im Empfangsbereich sendet. (Beacons).
Beacons enthalten den Netzwerknamen (SSID- Service Set Identifier), Liste unterstützter Übertragungsraten, Art der Verschlüsselung
Access Point ist der zentrale Punkt, über den sich alle Stationen am Netzwerk anmelden.
Es wird eine Verbindung zu anderen Netzen bzw. Internet hergestellt.

Wireless Distribution System (WDS) und Repeating:
Dienst zur Reichweitenerhöhung bestehender Funknetze bzw. Verbindung kabelgebundener Netze via Funk.

Client Modus:
Access Point verhält sich zu übergeordneten Access Points als Wireless Adapter (Rechner oder Netzwerke können an übergeordnete Netze angebunden werden)

Ethernet Bridge Modus:
Access Point bietet zusätzlich eine RJ45 Netzwerkschnittstelle an.
Vermittelt die Daten zwischen Ethernet und WLAN.

Bridge Modus:
Dient zur Verbindung von räumlich entfernten Netzwerken.
Access Point besitzen wetterfeste Außenantennen mit Richt- und Rundstrahlfunktion > Sichtkontakt zwischen den Access Points ist wichtig.

Repeater Modus:
Dient, um die Reichweite zwischen Access Point oder Router und den Stationen zu vergrößern.
Der Access Point dient nur zur Weiterleitung von Daten.