Netzwerke

Netzwerke ermöglichen die Verbindung unterschiedlicher Computersysteme zur Nutzung gemeinsamer Datenbestände und Geräte und dienen auch ganz allgemein der Anwenderkommunikation untereinander (E-MAIL). Ein Netzwerk kann sich in seiner Ausdehnung sowohl auf wenige Meter beschränken als auch weltumspannende Entfernungen überbrücken. In der Vergangenheit war man schon glücklich wenn man einen Computer besaß. In der Zeit, in der Computer ein immer wichtigerer Bestandteil des täglichen Lebens werden spielt die Vernetzung eine immer größere Rolle. Der erste Schritt bei der Einrichtung eines Netzwerkes ist die Entscheidung für einen Netzwerktyp. Das Übertragungsmedium ist der entscheidende Faktor über Sicherheit, Reichweite und Übertragungsgeschwindigkeit in Netzwerken. In der Regel ist die Reichweite antiproportional zur Übertragungsgeschwindigkeit, dieses bedeutet das eine Modem Verbindung mit 9600Baud (Bit/Sekunde) mehrere km überbrücken kann, im Gegensatz zu Ethernet das eine Reichweite von max. wenigen 100m hat. Welcher Netzwerktyp benutzt wird ist von der Art der Anwendung abhängig. Sowie den zur Verfügung stehenden Finanzmitteln.

Wozu brauch man Netzwerke?

Datenaustausch
Kommunikation
Ressourcenteilung
Administration

Datenaustausch

Innerhalb eines Netzwerkes werden Daten - oder Dateien - auf andere Rechner kopiert. Diese Daten stehen dann mehr als einer Person oder aber auch einem anderen PC zur Verarbeitung zur Verfügung.

Kommunikation

Informationsaustausch von PC zu PC. Bei Windows NT-Systemen ist das über ein Programm mit Telefonfunktion möglich. Bedingt aber, dass der Gegenüber an seinem PC sitzen muss um zu antworten - unpraktisch. Daher gibt es E-Mail-Programme wie z.B. Lotus Notes, Microsoft Outlook oder Netscape Communicator. Man schreibt eine Textnachricht und schickt sie ab - fertig.

Ressourcenteilung

Was sind hierbei Ressourcen? Drucker, Faxgeräte, Scanner, Internetzugänge, Speicherplatz... Warum für jeden Arbeitsplatz einen eigenen Drucker kaufen, wenn ein solches Gerät zentral zur Verfügung gestellt werden kann? Im Grunde also eine reine Sparmaßnahme.

Administration

Mit entsprechender Software kann Ihr PC über das Netzwerk durch einen Administrator gewartet werden. Hierbei ist es egal ob ein neuer Nutzer eingerichtet wird, ein neues Programm installiert oder eine Virenüberprüfung gestartet wird.

Drahtlose Netzwerke (Wireless LAN):
In Sicherheits-Relevanten Netzwerken ist das Drahtloses Netzwerk (Wireless LAN) außen vor und wird oder sollte nicht benutzt werden. In Sachen Komfort ist ein drahtloses Netzwerk die vorteilhafteste Form, vor allem, was die Installation betrifft. Ein Computer in einem drahtlosen Netzwerk verwendet einen speziellen Netzwerkadapter, der Radiowellen durch das Medium Luft aussendet. Jeder Computer im Empfangsbereich dieser Wellen, an den dieser Netzwerkadapter (Karte) angeschlossen ist, kann die Übertragung empfangen und in diesem Netz kommunizieren.

Netzwerke mit Kupfer Kabel:
Es gibt zwei Arten von Ethernetkabel, Koaxial und verdrillte Kabel (Twisted Pair UTP/STP) Die üblichste Verbindung der Netzwerkkarten erfolgt mit Twisted Pair Kabel oder mit den veralteten Koaxialkabeln (Cheapernet). Für den Einsatz von Twisted Pair Kabeln (UDP oder STP) benötigt man einen Hub oder Switch mit mehreren Ports zum Anschluss der PCs.

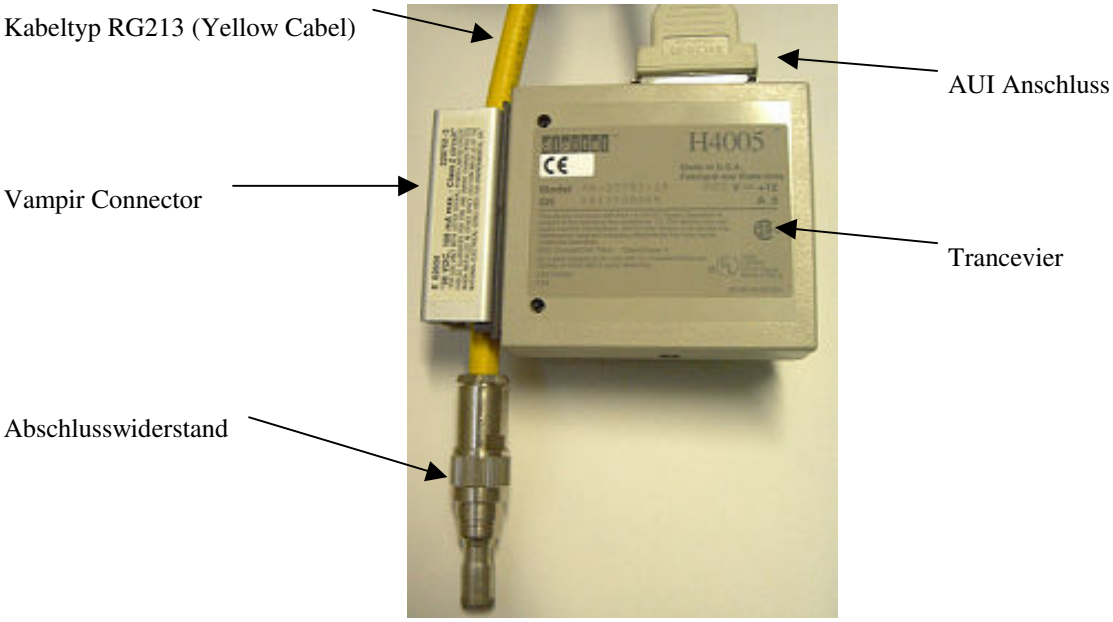
Coax-Kabel (10BASE2 oder 10BASE5)

10 BASE 2

- Kabeltyp: RG 58
- max. Länge: 185 Meter
- Geschwindigkeit: 10 Mbit/s (Mega Bits per Second)

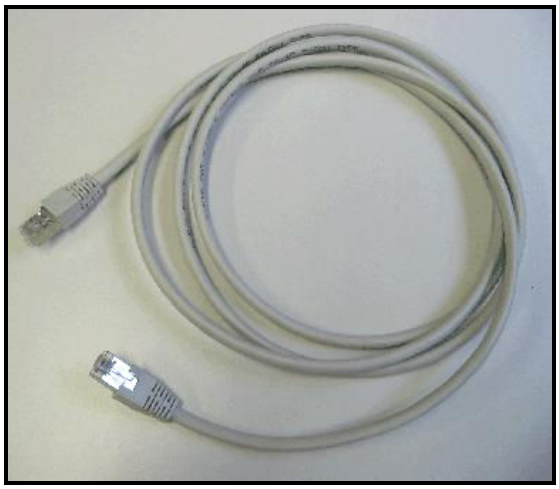
10 BASE 5

- Kabeltyp: RG 213
- max. Länge: 500 Meter
- Geschwindigkeit: 10 Mbit/s



Kat-5-Kabel (10BASE-T oder 100BASE-T)

- Kabeltyp: Kat-5 oder Kat-5e, auch TP / Twisted Pair
- max. Länge: 100 Meter
- Geschwindigkeit: 10 Mbit/s oder 100 Mbit/s

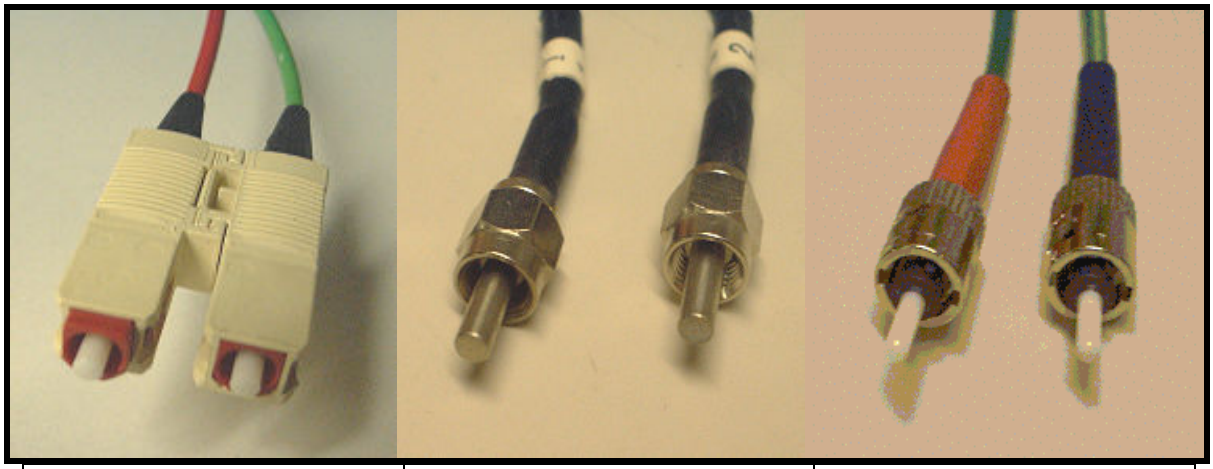


Netzwerke mit Lichtwellenleiter:

Netzwerke auf der Basis von Lichtwellenleitern, die anders als Kupferverbindungen störunempfindlich und abhörsicher sind sowie generell eine niedrige Fehlerrate aufweisen, bieten den einfachsten Weg zu höheren Datenübertragungsraten, somit gibt es auch kein Kabel-Kategorien-Wirrwarr wie etwa bei UTP/STP. Für Fiber Optik Verbindungen, die sternförmig ausgeführt werden, kommen zwei Leitungen zum Einsatz, die oftmals mit ST-Steckern oder SC Steckern versehen sind.
Bei Lichtwellenleiter unterscheidet man zwischen Mono- und Multimode Leiter. Multimode Faserl verwenden mehrere Wellenbereiche bei der Signalübertragung, während eine Monomode-Faser das Licht nur in einem Mode überträgt, was im üblichen zu geringeren Dämpfungswerten und höheren Bandbreiten führt.
Des weiteren unterscheidet man noch den Durchmesser von Fiber Optik Kabeln, die Faserstärke von Multimode liegt bei 62,5 µm und bei Monomode bei 8-10 µm. Die gebräuchlichste Form aber ist das Multimode Kabel.

Lichtwellenleiter

- Kabeltyp: Monomode oder Multimode
- max. Länge: 2-10 km
- Geschwindigkeit: 100 Mbit/s - 1 Gbit/s



SC – Stecker	**SMA** – Stecker	**ST** - Stecker

LAN-Standards

IEEE Standard für Netzwerke	
Standard	**Bedeutung**
IEEE 802.1	Definition, Architektur, Management, Internetworking
IEEE 802.2	Protokollfestlegung und Definition von Datenformatpaketen (Frames) zwischen Logical-Link-Controls (LLCs)
IEEE 802.3	CSMA/CD für Busnetz, MAP-Standard
IEEE 802.4	Token Passing für Busnetz, MAP-Standard
IEEE 802.5	Token Passing für Ringnetz, Token-Ring-Standard
IEEE 802.6	Metropolitan Area Network (MAN)
IEEE 802.7	Broadband Media, Breitbandnetzwerke
IEEE 802.8	Fiber Optic Media, Lichtwellenleiter
IEEE 802.9	Integrated Voice and Data Line, Sprachkommunikation
IEEE 802.10	Secure Data Interchange, Sicherheits- und Geheimhaltungsmechanismen
IEEE 802.11	Wireless LANs, drahtlose LANs
IEEE 802.12	100VG-AnyLAN, Fast Ethernet
IEEE 802.14	CAT-TV-Netze, Kabelfernsehen im Netzwerk
IEEE 802.30	100 Base-X, 100 Base-T, Fast Ethernet

IEEE = Institute of Electrical and Electronic Engineers

Ethernet Standards

Standard	**Bedeutung**	
10Base 2	Cheapernet oder Thin Wire (Koaxialkabel, RG58) mit 185m maximaler Kabelsegmentlänge und 30 Stationen.	
10Base 3	Breitband Ethernet mit 3600m maximaler Kabelsegmentlänge.	
10Base 5	Thick-Ethernet mit Koaxialkabel (Yellow Cable) und 500m Kabelsegmentlänge.	
10Base F	Ethernet mit Lichtwellenleiter – Fiber Optic Verbindungen.	
	10Base-FP	enthält Richtlinien für passive LWL-Hubs
	10Base-FB	für die Verwendung von LWL als Backbone,max 2 km.
	10Base-FL	entspricht quasi dem FORIL-Standart (Fiber Optic Repeater Inter Link), maximales Kabelsegment 1 km.
100BaseFX	Fiber Optic Verbindungen mit 100MBit/s (fast Ethernet,CSMA/CD)	
10Base T	Ethernet auf Twisted-Pair-Kabeln mit maximal 100m Kabelsegmentlänge	
100Base T	Fast-Ethernet mit CSMA/CD-Verfahren auf Twisted-Pair-Kabel	
	100Base TX	verwendet UTP/STP-Kabel der Kategorie 5 und ist Vollduplex-fähig, gilt als Standart für Fast-Ethernet
	100Base T4	kann bereits mit Kabeln der Kategorie 3 verwendet werden, wofür dann drei Datenleitungen und eine für die Kollisionserkennung zum Einsatz kommen, daher ist kein Vollduplex-Betrieb möglich.
100Base VG-AnyLAN	Fast Ethernet mit DPMA-Verfahren (Demand Priority Medium Access) auf Twisted-Pair oder LWL-Kabeln, sternförmige Topologie. Zusammenführung von Ethernet mit Token Ring	
1000Base T	Gigabit Ethernet (IEEE 802.3z), 1000 MBit/s auf Twisted-Pair-Kabeln ab der Kabel-Kategorie 6 oder mit Lichtwellenleiter.	

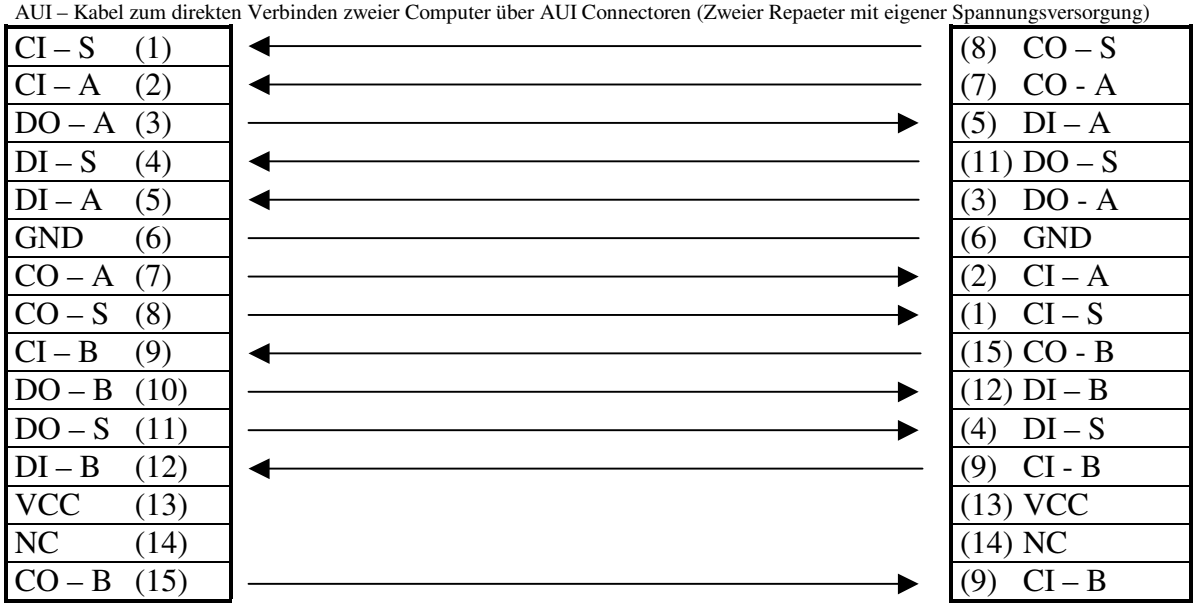
AUI - Kabel und Anschlüsse

(Attachement Unit Interface)

AUI Stecker Belegung

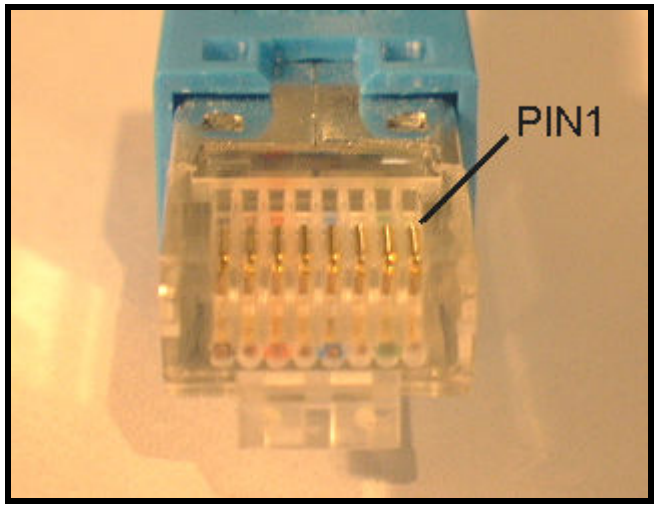
PIN Nr.	Signal	Bedeutung
1	Control In Shield,CI-S oder NC	Abschirmung der Signalleitungen oder auch nicht belegt
2	Control IN, CI-A	Steuerinformation zur Kollisionserkennung
3	Data Out A, DO-A	Datenübertragung, senden
4	Data In Shield, DI–S	Abschirmung der Empfangsleitungen
5	Data In A, DI–A	Datenübertragung, empfangen
6	GND	Masseleitung
7	Control Out, CO-A oder NC	Signalisierung des Betriebszustandes oder nicht belegt
8	Control Out Shield, CO-S oder NC	Abschirmung der Signalleitungen oder auch nicht belegt
9	Control In B, CI–B	Steuerinformationen zur Kollisionserkennung
10	Data Out B, DO-B	Datenübertragung, senden
11	Data Out Shield, DO-S oder NC	Abschirmung der Sendeleitungen oder auch nicht belegt
12	Data In B, DI-B	Datenübertragung, empfangen
13	VCC	Spannung 5V
14	NC	nicht belegt
15	Control Out, CO-B oder NC	Signalisierung des Betriebszustandes oder auch nicht belegt

AUI – Kabel zum direkten Verbinden zweier Computer über AUI Connectoren (Zweier Repaeter mit eigener Spannungsversorgung)



Stecker SubD15 Stecker SubD15

Twisted – Pair - Kabel und Anschlüsse



Die Standart Farben bei der Verkabelung eines Ethernet ist die Farbgebung nach EIA/TIA 56813

Pin Nr.	4 adrige Belegung	Farben: EIA/TIA 56813	DIN - 47100	IEC
1	TXD +	weiß / orange	grau	schwarz
2	TXD -	Orange	rosa	grün
3	RXD +	weiß / grün	grün	rot
4	NC	Blau	weiß	weiß
5	NC	weiß / blau	braun	blau
6	RXD -	Grün	gelb	orange
7	NC	weiß / braun	blau	gelb
8	NC	Braun	rot	braun

Einfache UTP Kopplung zweier PCs:

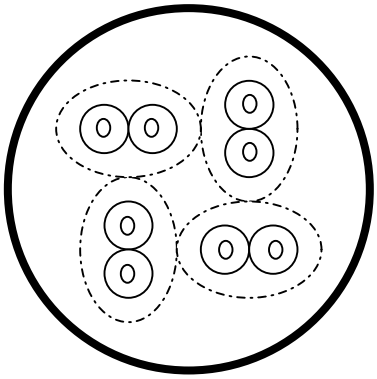
Kabelbelegung zum Koppeln von zwei PCs ohne Switch oder Hub, oder zum kaskadieren von mehreren Switch bzw. Hubs untereinander.

Bezeichnung	Anschluß	Anschluß	Bezeichnung
TD+	1	3	RD+
TD-	2	6	RD-
RD+	3	1	TD+
RD -	6	2	TD-

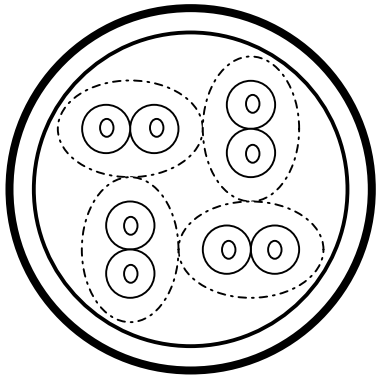
Kategorietypen bei Twisted Pair Kabel:

Kategorie	Bedeutung/Daten	Datenrate
1	Leistung eines konventionellen Telefonkabels. Für Alarmsysteme und analoge Sprachübertragung.	bis 1 MBit/s
2	Kabel zum Ersatz des Kategorie-1-Kabels. Wird auch für ISDN eingesetzt.	bis 4 MBit/s
3	UTP- oder STP-Kabel, Unshielded Twisted Pair (ohne Schirmung) oder Shielded Twisted Pair (mit Schirmung). Wird z.B. für Ethernet (10Base-T) verwendet.	bis 10 MBit/s bei 100m
4	UTP/STP – Kabel für größere Entfernungen als mit Kategorie-3-Kabeln. Wird für Ethernet und Token Ring eingesetzt.	bis 20 MBit/s
5	Erweiterter Frequenzbereich. Gilt als Standart-Kabel und wird beispielsweise für FDDI und Fast Ethernet verwendet.	bis 100 MBit/s
6	Ist bereits für ATM verwendbar.(Asynchron Transfer Mode)	bis 200 MBit/s
7	Geringes Nebensprechen und geringere Dämpfung als Kategorie-6-Kabel.	bis 600 MBit/s
8	*Noch nicht verabschiedet.*	bis 1200 MBit/s bei 50m

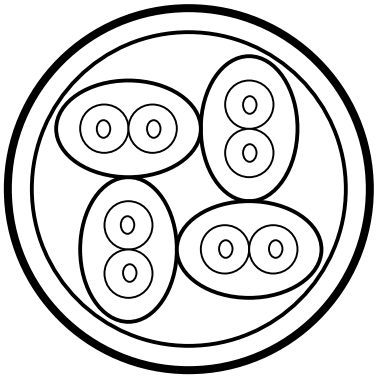
Bauart bei Twisted Pair Kabel:



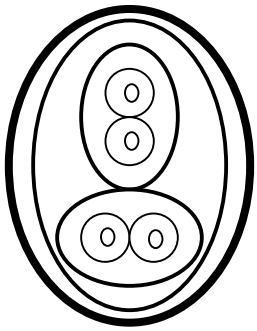
UTP



S/UTP



S/STP



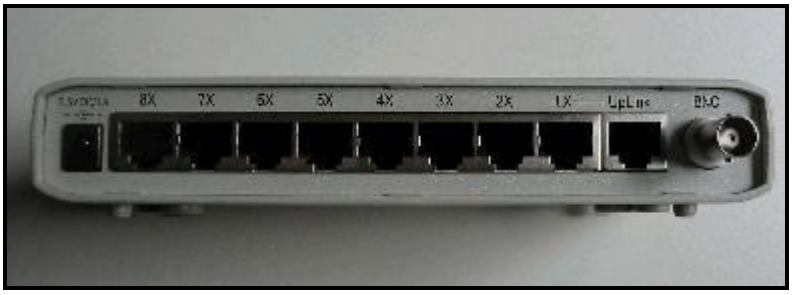
ITP

Internetworking

Netzwerke oder Netzwerksegmente der gleichen oder auch unterschiedlicher Art können über verschiedene (Internetworking-) Elemente miteinander verbunden werden. Je nach Anwendungsbereich verwenden diese Elemente unterschiedliche Schichten des OSI-Modells (Open Systems Interconnection), und je unterschiedlicher die zu koppelnden Netze und Anwendungen arbeiten, umso komplexer müssen diese Elemente werden, damit die gewünschte Übertragung und Datenumsetzung vorgenommen werden kann.

Repeater:
Ein Repeater ist das einfachste Koppelelement in einem Netzwerk. Dieser verbindet Segmente auf der untersten Schicht des OSI Models und dient nur zur Verstärkung von Signalen.

Hubs:
Ein Hub arbeitet wie ein Repeater auf der 1. Schicht des OSI Models, hat aber im Gegensatz zum Repeater mehrere Anschlüsse. Kollisionen werden im Netzwerk weitergegeben. Computer werden Sternförmig angeschlossen.



Bridges:
Eine Bridges trennt mehrere Netzwerke Kollisionen werden aber nicht durchgelassen. Da die Bridges auf der 2. Schicht des OSI Modells arbeiten kann sich auch die Physikalische Schicht der zu koppelnden Netzwerke unterscheiden. Die Bridges speichern die Adresse der Segmente, Anfragen von einem Rechner zu einen Rechner im eigenen Netz werden nicht an ein anderes Segment weitergegeben.

Switches:
Der Switch ist wie eine Bridge ein Gerät des OSI – Layers 2, d.h. er kann LANs mit verschiedenen physikalischen Eigenschaften verbinden, z.B. Lichtwellenleiter und Twisted-Pair-Netzwerke. Allerdings müssen, ebenso wie bei der Bridge, alle Protokolle höherer Ebenen 3 bis 7 identisch sein. Ein Switch ist somit protokolltransparent. Jedem Netzwerksegment steht die volle Bandbreite zur Verfügung. Dadurch erhöht der Switch die Netzwerk-Performance wie eine Bridge im Gesamtnetz, sowie auch in jedem einzelnen Segment.

Router:
Die Router arbeiten auf der 3. Schicht des OSI Modells, und demnach dürfen sich die 1. und 2. Schicht der zu koppelnden Netze voneinander unterscheiden. Sie haben die Fähigkeit, unterschiedliche Netzwerktypen als auch unterschiedliche Protokolle verarbeiten zu können. Ein Router ist in einigen Fällen für ein bestimmtes Netzwerkprotokoll (z.B. TCP/IP, ISDN) ausgelegt. Es existieren jedoch auch Router, die multiprotokollfähig sind und verschiedene Protokolle unterstützen. Die logischen Adressen in einem Netzwerk können von Routern ausgewertet werden, und mit Hilfe anzulegender Routing-Tabellen werden daraufhin die optimalen Wege vom Sender zum Empfänger ermittelt. Router besitzen intern einen relativ großen Speicher, da sie die Paketlänge verändern, beispielsweise Übergang von Ethernet auf Token Ring oder ISDN.

Gateways:
Gateways können völlig unterschiedliche (heterogene) Netze miteinander koppeln. Sie stellen einen gemeinsam (virtuellen) Knoten dar, der zu beiden Netzen gehört und den netzübergreifenden Datenverkehr abwickelt. Gateways werden einerseits für die LAN-WAN Kopplung (oder die LAN-WAN-LAN Kopplung) andererseits für den Übergang zwischen unterschiedlichen Diensten verwendet (z.B. das Absetzen von Fax-Nachrichten aus einen LAN).

Netzwerktopologien

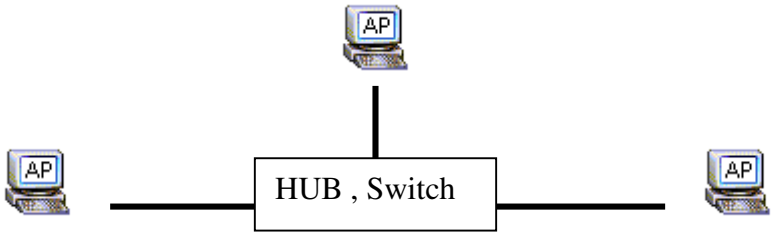
Busnetz:

Die Bustopologie wird bei kleinen Netzwerken verwendet. Alle Stationen inklusive Server werden über ein Kabel, dem Bus angeschlossen der an beiden Enden mit Abschlusswiderständen versehen sein muss. Hier wird meist Koaxialkabel verwendet. Das verwendete Koaxialkabel wird mit Hilfe von T Stücken zu einen Bus verbunden.

Vorteil:
- Einfache Installation und Erweiterung
- Kurze Leitungen daher geringe Verkabelungskosten
- Der Ausfall eines Rechners führt zu keiner Störung

Nachteil:
- Begrenzte Netzausdehnung
- Hoher Netzwerktraffic
- Ausfall des gesamten Netzes bei defektem Kabel

Sternnetz:

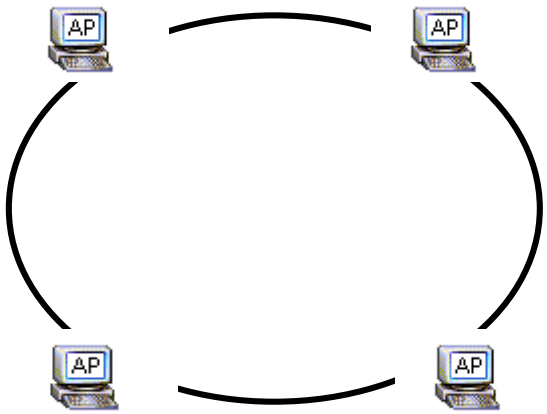


Die klassische und älteste Netzwerkstruktur ist der Stern. Das Zentrum des Sterns bildet der Server oder ein zentraler Großrechner, heute verwendet man in Netzwerken einen Switch oder Hub an denen alle Arbeitsstationen und Server angeschlossen werden. Zur Erweiterung des Systems um weitere Arbeitsstationen ist häufig ein größerer Hub oder Switch erforderlich.

Vorteile:
- Einfache Vernetzung
- Keine Störung des Netzwerkes bei Ausfall eines beteiligten Rechners

Nachteile:
- Hoher Verkabelungsaufwand, höhere Verkabelungskosten
- Netzausfall bei defektem Switch oder Hub

Ringnetz:

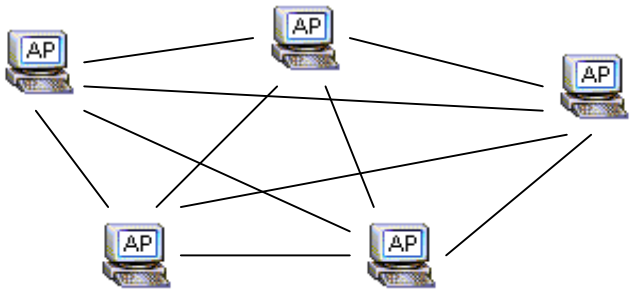


Die einzelnen Stationen werden zu einen Ring angeordnet und die Nachrichten werden von einer zur nächsten weitergegeben, bis der Zielrechner das Packet empfängt.
Wird der Ring unterbrochen fällt das Netzwerk aus. Um dieses Problem entgegen zu wirken wird ein weiterer Ring verwendet (aktiver Ring und ein Stand-By-Ring).

Vorteile:
- Grosse Netzausdehnung theoretisch unbegrenzt
- Signalregeneration
- keine Datenkollision

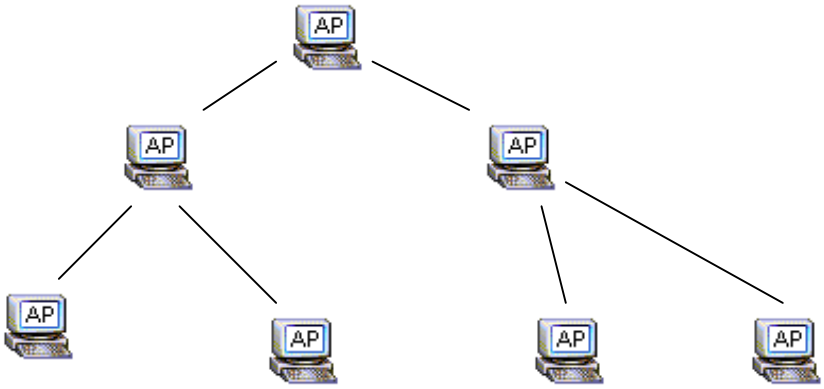
Nachteile:
- Aufwendige Fehlersuche
- Hoher Kabelaufwand
- Die Reaktionszeit kann sehr lang sein (je größer das Netz)

Vermaschtes Netz:



Jeder Netzwerkteilnehmer ist untereinander verbunden. Alle Netzwerkteilnehmer haben eine ständige Verbindung zu jedem anderen Netzwerkteilnehmer. Die vermaschte Topologie kommt dann zum Einsatz, wenn zum Beispiel aus Redundanzgründen von einem Knoten eines Netzwerks mehr als zwei Gegenstationen direkt erreichbar sind. Heutige Netzwerke die ein größeres geographisches Gebiet erschließen sind in der Regel in dieser Art aufgebaut. Wichtige Areale sind meistens auf zwei oder mehr Wegen erreichbar. Es ist dann die Aufgabe von intelligenten Verbindungsknoten, den optimalen aber auch offenen Pfad (Route) für die Daten zu wählen.

Baumnetz:



Netzwerke sind nicht auf eine bestimmte Topologie begrenzt und je größer das Netzwerk ist, desto größer ist die Wahrscheinlichkeit, dass mehrere Topologien zum Einsatz kommen, was sich dann als Mischform – als Baum – darstellen kann. Dabei findet eine Kaskadierung des Gesamtnetzes mittels Kabelkonzentratoren, Hubs und Switches statt.

Vorteile:
- Gesamte Leitungslänge, sowie Komplexität der Schaltzentralen vermindert.

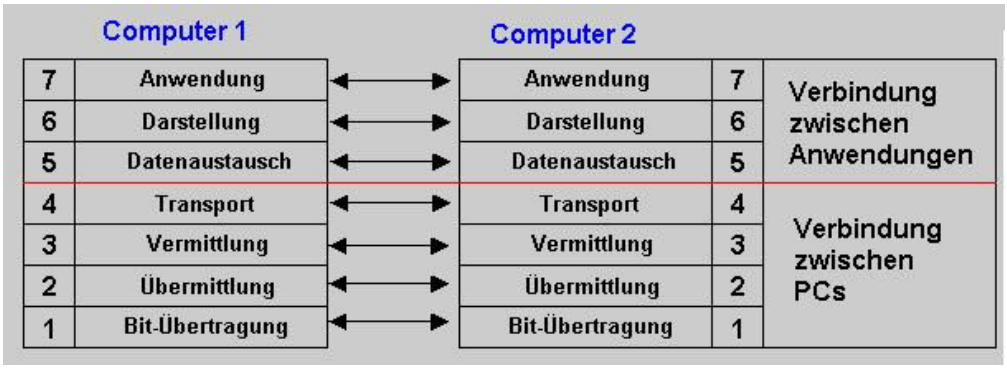
Nachteile:
- Ein Ausfall eines Netzes betrifft ganze Äste

OSI-7-Schichtenmodell (ISO 7498)

Die Netzwerkkommunikation innerhalb eines PCs ist in 7 Schichten aufgeteilt:

- Schicht 7 (Application Layer) ist das Benutzerprogramm - die Anwendungsschicht.
- Schicht 6 (Presentation Layer) ist der Übersetzer für Eingabe, Austausch und Darstellung von Daten.
- Schicht 5 (Session Layer) synchronisiert den Datenaustausch zwischen Anwendungen (z.B. LotusNotes zu Lotus Notes).
- Schicht 4 (Transport Layer) ist zuständig für direkte Punkt-zu-Punkt-Verbindungen und Software-Fehlerkorrektur.
- Schicht 3 (Network Layer) legt den Weg innerhalb des Netzwerkes fest.
- Schicht 2 (Data Link Layer) sorgt für einen fehlerfreien Zugriff auf die Hardware.
- Schicht 1 (Physical Layer) sind Kabel, Strom, Daten....

Unterhalten sich zwei Rechner, muss auf jedem Rechner dieses Schichtenmodell abgebildet sein, damit die Daten korrekt übertragen werden.



Dieses Schichtenmodell, auch OSI-Referenzmodell genannt, haben verschiedene Hersteller in Protokolle umgesetzt.

Netzwerkprotokolle

Apple Talk
Apple Talk ist ein spezifisches Protokoll der Firma Apple für die Kommunikation zwischen Macintosh-Computern und hierfür geeigneter Peripherie.

APPC
Advanced Program to Program Communikation ist eine Entwicklung von IBM und Bestandteil der System Network Architecture (SNA), welches die Kommunikation mit jedem IBM-Computer unterstützt. APPC wird vorwiegend im IBM-Token-Ring verwendet und ist nicht auf LANs beschränkt.

DECnet
DECnet stammt von der Firma Digital und stellt prinzipiell eine Familie von Soft- und Hardwareprodukten dar. Das Protokoll ist aber nicht auf DEC-Computer beschränkt, sondern auch für PCs nutzbar. DECnet ist routbar und somit auch für die Verbindung zu öffentlichen Netze geeignet. Von der Leistungsfähigkeit her ist es am ehesten mit TCP/IP zu vergleichen und kann verschiedene Verbindungen wie Ethernet oder X.25 nutzen.

IPX/SPX
Internet Packet Exchange/Sequenced Packet Exchange ist das klassische Netzwerkprotokoll der Firma Novell, wie es in Novell Netware implementiert ist. Durch IPX werden die Anwendungen mit Netzwerktreibern ausgestattet und die Datenpakete über das Netzwerk transportiert, während das darüberliegende SPX die Steuerung und Überwachung der Operationen übernimmt. Ab Novell Netware 4.x vollzieht die Abkehr von diesem Protokoll hin zu IP.

NetBEUI
NetBIOS Enhanced User Interface ist ein Standartprotokoll von Microsoft und ab Windows for Workgroups implementiert. Es ist wie NetBIOS für ein Peer-to-Peer-Konfiguration ausgelegt und führt zu einem erheblichen administrativen Aufwand, denn jeder PC muss individuell betreffs der Freigabe bzw. der Nutzung von Zugriffsrechten und Diensten konfiguriert werden. Es ist keine Verwendung des DNS (Domain Name Service) möglich, und auch von daher ist für größere Netze TCP/IP besser geeignet, welches ebenfalls von Windows standardmäßig zur Verfügung gestellt wird.

NetBIOS
NetBIOS stammt von IBM und ist für Peer-to-Peer-Kommunikation zwischen PCs vorgesehen. Der OS/2-LAN-Server unterstützt dieses Protokoll beispielsweise. Es kann im Gegensatz zu IPX/SPX und TCP/IP nicht geroutet werden und eignet sich nur für relativ kleine Netze, da es bei einer Vielzahl von PCs nicht mehr einfach zu managen ist.

NPMS
Named Pipes/Mail Slots wurde von Microsoft entwickelt und dient der Kommunikation zwischen unterschiedlichen Netzen. Es hat sich jedoch nicht am Markt durchgesetzt.

OSI
Das Protokoll Open System Interconnection gilt als Alternative zu TCP/IP ist jedoch nicht sehr verbreitet, da TCP/IP weitaus akzeptierter ist. Einige Teile des OSI-Protokolls wie X.400-Mailing oder X.500 Directory Services gelten zwar als Standart, werden jedoch mit TCP/IP kombiniert.

TCP/IP
Transmission Control Protocol/Internet Protocol ist eine Protokoll Familie für die Kommunikation zwischen unterschiedlichen Computersystemen und Bestandteil des UNIX-Betriebssystems. TCP ist auf der 4. OSI-Schicht lokalisiert und baut die Verbindungen zwischen den Stationen auf und wieder ab. In der darunterliegenden Schicht ist das IP Protokoll für die Adressierung und Versendung der Datenpakete verantwortlich. TCP/IP betrifft darüber hinaus die OSI-Schichten 5-7, die solche Dienste wie die Übertragung von Dateien zwischen unterschiedlichen Computersystemen (FTP, File Transfer Protokoll), die einfache Terminal zu Terminal Verbindung (Telnet) und für die Nachrichtenübermittlung (SMTP, Simple Mail Transfer Protokoll) zur Verfügung stellen. TCP/IP stellt einen Industriestandart dar, wird von den meisten Computerplattformen unterstützt und stellt in vielen Fällen die einzige praktische Lösung zur Kommunikation zwischen heterogenen Systemen dar. Bei Aufbau und Verwaltung von TCP/IP-Netzen gibt es die zwei Bereiche Adressverwaltung und Namensauswertung.

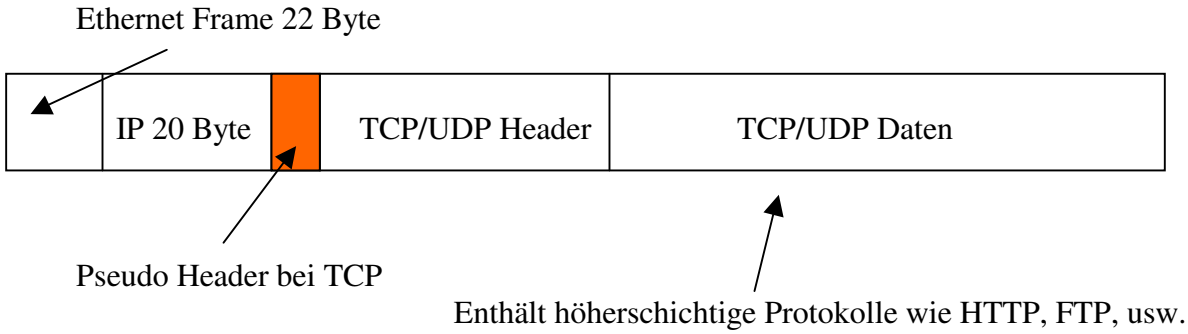
1. Adressverwaltung
Für jedes in einem TCP/IP-Netzwerkverbund vorhandene Gerät muss ein eindeutiger Name sowie eine IP-Adresse angegeben werden. Durch die Kombination von IP-Adresse & Subnetmask wird sowohl der Computer selbst, als auch das Teilnetz (Subnet) identifiziert, in dem er eingebunden ist. Wird der Computer in ein anderes Subnet verschoben, so muß die IP-Adresse bzw. die Subnetmask angepaßt werden.

2. Namensauswertung / -auflösung
Während Benutzer für die Computer, mit denen sie sich verbinden möchten, eingängige Namen verwenden, identifizieren Programme einen Computer anhand seiner IP-Adresse. Folglich ist ein Dienst erforderlich, der die Umsetzung von Name auf IP-Adresse (und umgekehrt) organisiert und zwar netzwerkweit.
Zur Namensauswertung gibt es mehrere Möglichkeiten:
- Hosts-Tabellen (auf NT-Rechnern im Ordner %systemroot%\system32\drivers\etc)
- Domain Name Service (DNS)
- Windows Internet Naming Service (WINS, MS-spezifisches Produkt)

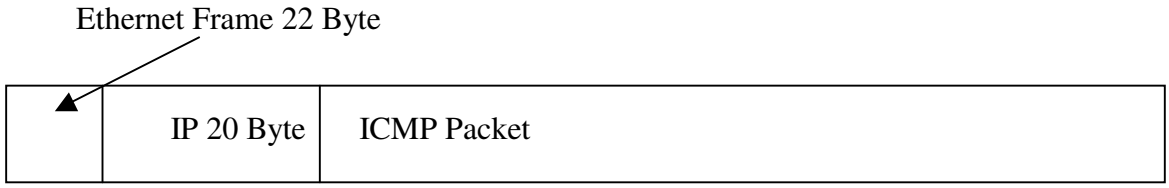
Wird auf einem Rechner TCP/IP installiert, so sind dabei sowohl Adressinformationen als auch Angaben zur Namensauflösung einzutragen.

Übersicht der wichtigsten Protokolle im Ethernet

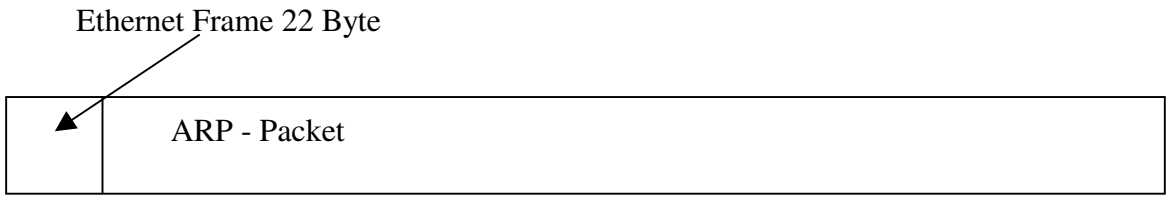
TCP oder UDP Packet im Ethernet bei IP v4



ICMP Packet im Ethernet



ARP Packet im Ethernet



Der Aufbau eines Ethernet II Frame:

Präambel:	7 Byte	
Frame Delimiter:–	1 Byte	
Zieladresse:–	6 Byte	(Destination Addresse)
Quelladresse:–	6 Byte	(Source Addresse)
Typfeld:	2 Byte	
Nutzlast: (ARP, ICMP, UDP, TCP)	46 bis 1500 Byte	
Frame Check Sequence / Cyclic Redundancy Check: 4 Byte		

Präambel: wird zur Synchronisation benutzt und enthält abwechselnd 7*10101010, wird durch die Netzwerkkarte generiert.

Frame Delimitter: enthält das Bitmuster 10101011 und signalisiert damit dass ab jetzt das eigentliche Frame beginnt, wird durch die Netzwerkkarte generiert.

Zieladresse: enthält die 6 Byte lange MAC Adresse. Sollen alle physikalisch angeschlossenen Stationen angesprochen werden so enthält die MAC Adresse FF-FF-FF-FF-FF-FF (alle Bits auf logisch high).

Quelladresse: enthält die 6 Byte lange MAC Adresse des Absenders

Typ-Feld: enthält Informationen darüber was im Nutzlastbereich transportiert wird, 0x0800 für ein IP Datagramm oder 0x0806 ist der Code für ein ARP Anfrage.

Nutzlastbereich: Sollte min. 46 Bytes und max. 1500 Bytes enthalten (MTU bei Ethernet II)

Frame Check Sequence / Cyclic Redundancy Check: Prüfsumme wird durch die Netzwerkkarte generiert.

Der Aufbau eines IP Datagrammes:
(Internet Protokoll)

4 Bit	4 Bit	4 Bit	4 Bit	4 Bit	4 Bit	4 Bit	4 Bit
Version	Header-länge	Type of Service		Komplette Länge in Bytes			
16 Bit Identifikation				Schalter	Fragmentierungsposition		
Time to Live		Protokoll		Header Prüfsumme			
IP Quelladresse							
IP Zieladresse							
Nutzlast							

Version - 4Bit: Die Versionsnummer von IP, meistens 4 neuerdings auch 6.

Headerlänge - 4Bit: Größe des Headers inklusive aller eventuellen Optionen.

Type of Service - 8Bit: Beeinflusst die weiterleitenden Router in ihre Entscheidung, auf welcher Route das Datagramm gesendet werden soll.

Komplette Länge in Bytes - 16Bit: Die Größe des gesamten Datagramms. Hieraus ergibt sich eine Maximalgröße von 64KBytes für ein Datagramm, bei Ethernet II 1500 Bytes.

Identifikation - 16Bit: Dieses Feld wird vom IP Stack nach jedem gesendeten Datagramm um eins erhöht. Somit bekommt jedes Paket eine eigene ID, die z.B. bei Fragmentierung und Reassemblierung wichtig ist.

Schalter - 3Bit: Bit 1: ist immer 0.
Bit 2: das Paket darf nicht fragmentiert werden.
Bit 3: weitere Fragmente folgen.

Fragmentierungsposition - 13Bit: Wird benutzt, um ein fragmentiertes IP Paket wieder korrekt zusammenzusetzen.

Time to Live - 8Bit: Die Lebenszeit eines Datagramms, wird bei jedem Routing vom Router um 1 dekrementiert.

Protokoll - 8Bit: Sagt aus, welches höherschichtige Protokoll sich im IP Datagramm befindet.

Wert	Protokoll
1	ICMP
2	IGMP
6	TCP
17	UDP

Headerprüfsumme - 16Bit: Enthält die Prüfsumme vom IP Header.

Quell/Zieladresse je - 32Bit: Diese Felder enthalten die IP Adresse des Absenders und Empfängers.

Der Aufbau einer ICMP Nachricht:
(Internet Control Message Protokoll)

8Bit	8Bit	8Bit	8Bit
Typ	Code	Prüfsumme (Checksum)	
Je nach Typ und Nachricht unterschiedlich			
Testdaten			

Typ - 8Bit: Identifiziert die Aufgabe der Nachricht.

Wert	Aufgabe
0	Echo reply
1	
2	
3	Destination unreachable
4	Source quench
5	Redirect (Change Route)
6	
7	
8	Echo request
9	
10	
11	Time exceedet for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp request
14	Timestamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

Code - 8Bit: Enthält Detailangaben zu bestimmten Typen.

Prüfsumme - 16Bit: Enthält Prüfsumme (Checksumme) der ICMP Nachricht.

Der Aufbau einer ARP Anfrage:
(Address Resolution Protokoll)

2 Byte Hardware Typ	2 Byte Protokoll Typ
1 Byte Länge der Hardwareadresse	1 Byte Länge der Protokolladresse
2 Byte Operation	
6 Byte MAC Adresse Absender	4 Byte IP Adresse Absender
6 Byte MAC Adresse Ziel	4 Byte IP Adresse Ziel

Hardware Typ - 2Byte: Enthält den Code für Ethernet oder andere Link Layer.

Protokoll Typ - 2Byte: Enthält den Code für IP oder anderes Übertragungsprotokoll.

Länge der Hardwareadresse - 1Byte: Enthält 6 für 6 Byte MAC Adresse.

Länge der Protokolladresse - 1Byte: Enthält 4 für 4 Byte IP Adressen.

Operation - 2Byte: Enthält den Code der signalisiert ob es sich um eine Anfrage oder Antwort handelt.

MAC Adresse Absender - 6Byte: Enthält 6 Byte MAC Adresse des Anfragenden.

IP Adresse Absender - 4Byte: Enthält 4 Byte IP Adresse des Absenders.

MAC Adresse Ziel - 6Byte: Enthält 6 Byte MAC Adresse des Empfänger.

IP Adresse Ziel - 4Byte: Enthält 4 Byte IP Adresse des Empfängers.

Der Aufbau des TCP Protokoll:
(Transmission Control Protokoll)

4Bit	4Bit	4Bit	4Bit	4Bit	4Bit	4Bit	4 Bit
Quellport				Zielport			
Sequenznummer							
Bestätigungsnummer							
Header-länge	Reserviert	Schalter		Fenstergröße			
TCP Prüfsumme				Anzeige für dringende Übertragung			
DATEN							

Quellport - 2Byte: Quell Port für die Verbindung.

Zielport - 2Byte: Der Zielport für die Verbindung bei HTTP z.b. 0080.

Sequenznummer - 4Byte: TCP nummerierter Bytestrom von den eingetroffenen Segmenten.

Bestätigungsnummer - 4Byte: TCP nummerierter Bytestrom von den ausgehenden Segmenten.

Headerlänge - 4Bit: Da der TCP – Header Optionen enthalten kann, wird hier die Länge des Headers in 32 Bit-Schritten angegeben

Schalter - 6Bit: Angabe der Funktion des Segments.

BIT	Bedeutung
URG Bit	Datenübertragung dringend (urgent)
ACK Bit	Datenübertragung bestätigen (acknowledged)
PSH Bit	Datenübergabe an die Anwendung (push)
RST Bit	Verbindung neu initialisieren (reset)
SYN Bit	Verbindung aufbauen (synchronize)
FIN Bit	Datenübertragung beenden (finished)

TCP Prüfsumme - 16Bit: Enthält Prüfsumme über Header und Pseudoheader sowie Datenbereich.

Anzeige für dringende Übertragung – 2Byte: Markierung eines Bereiches des Datenteils als dringend.

Beispiel eines Verbindungsaufbaus bei TCP:

Richtung	SEQ Counter	ACK Counter	Flags	Daten
A >> B	1023	0	SYN	keine
A << B	1	1023	SYN,ACK	keine
A >> B	1024	1	ACK	keine

Datenübertragung bei TCP

Richtung	SEQ Counter	ACK Counter	Flags	Daten
A >> B	1024	1	PSH	100 Byte inc Header
A << B	1	1124	ACK	keine
A << B	1	1124	PSH	100 Byte inc Header
A >> B	1124	101	ACK	keine

Verbindungsabbau bei TCP

Richtung	SEQ Counter	ACK Counter	Flags	Daten
A << B	101	1124	FIN	keine
A << B	1124	102	ACK	keine

Der Aufbau eines UDP Datagrammes:
(User Datagram Protokoll)

16 Bit Quellport	16 Bit Zielport
16 Bit Länge des Datagrams	16 Bit Optionale Prüfsumme
DATEN	

Quellport - 16Bit: Der Quellport der Verbindung.

Zielport - 16Bit: Der Zielport der Verbindung.

Länge des Datagramm - 16Bit: Enthält die Länge des UDP Headers und Datenbereich

Optionale Prüfsumme - 16Bit: Kann eine Prüfsumme über Header und Daten enthalten. Befindet sich in diesem Feld eine 0, so wurde beim Absender keine Prüfsumme erzeugt.