Modul 117

1 Allgemeines

Dieses Dokument umfasst den grössten Teil des Lernstoffes, der im Modul 117 unterrichtet wurde. Quellen für ergänzende Informationen befinden sich im Teil Referenzen. Für die Prüfung sollte das genannte Buch **unbedingt** mitgebracht werden.

Wenn im Folgendem die Rede von „Netzwerk“ ist, so geht es um nichts anderes als um Rechnernetze.

1.1 Was ist ein Netzwerk?

Ein (Computer-)Netzwerk ist ein Verbund verschiedener (eigenständiger) elektronischer Systeme zu einem gesamten. Die Rechner im Verbund behalten dabei ihre jeweilige Eigenständigkeit, durch das Netzwerk werden aber neue Möglichkeiten und Funktionen zur Verfügung gestellt.

1.2 Wozu Netzwerke?

Ein Netzwerk dient dazu Informationen in einem gewissen Ausmass weiterzugeben und verfügbar zu machen. Dabei wird klar definiert, welche Rechner auf welche Daten welchen Zugriff haben können. Ein Netzwerk beschleunigt so den Datenaustausch und vereinfacht diesen.

Heutzutage ist beinahe jeder Computer an einem oder an mehreren Netzwerken angeschlossen, ein Betrieb ausserhalb eines Netzwerks wäre undenkbar.

2 Topologien

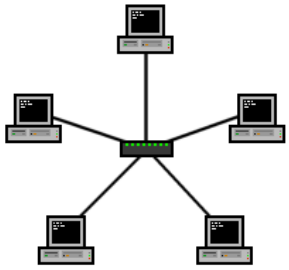
Eine Topologie bezeichnet, wie verschiedene Geräte innerhalb eines Netzwerks miteinander verbunden werden müssen, damit ein gemeinsamer Datenaustausch gewährleistet werden kann.

Die Topologie ist entscheidend für die Ausfallsicherheit des gesamten Netzwerks und über die benötigte Hardware.

Je nach Topologie gibt es für den Datenstrom Ersatzwege, damit die Kommunikation bei einem Defekt eines Netzwerkgeräts weiterhin gewährleistet ist.

2.1 Stern

Verbindet man alle Netzwerkgeräte mit einem zentralen Knoten, so ist die Rede von einer Sterntopologie. Dieser zentrale Knoten muss über keinerlei Intelligenz verfügen – es können Hubs gleichermassen wie Switches verwendet werden.



Die ganze Netzwerkkommunikation läuft über diesen zentralen Knoten ab.

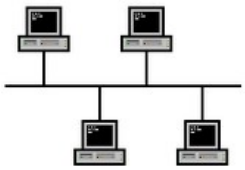
Je nach dem, ob man einen Hub oder einen Switch einsetzt werden die Datenpakete an alle oder nur an einen bestimmten Teilnehmer gesendet.

2.1.1 Bewertung

Vorteile	*Nachteile*
Bei Ausfall eines Endgeräts wird der Netzwerkverkehr nicht beeinträchtigt	Fällt hingegen der zentrale Knoten aus, so ist keine Kommunikation mehr möglich
Leicht erweiterbare und verständliche Topologie	Hoher Verkabelungsaufwand
Hohe Übertragungsraten	
Einfache Fehlersuche	

2.2 Bus

Bei einem Bus erfolgt die Kommunikation über ein Hauptkabel, das mit Endwiderständen auf beiden Seiten abgeschlossen ist.



Mit sog. T-Stücken können Endgeräte an das Hauptkabel angeschlossen werden.

Jedes Endgerät hört alle Datenpakete ab und entscheidet anhand seiner Zieladresse, ob dieses angenommen oder ignoriert werden soll.

2.2.1 Bewertung

Vorteile	*Nachteile*
Geringer Verkabelungsaufwand	Fällt das Hauptkabel aus, so ist das Netzwerk tot
Einfach erweiterbar	Jedes Paket wird an jeden Teilnehmer gesendet (Sicherheit)
Bei Ausfall eines Endgeräts wird der Datenverkehr nicht beeinträchtigt	Ein defekter Anschluss an das Hauptkabel unterbricht das Netz
	Es kann immer nur eine Station Daten senden
	Probleme mit Kollision [1]
	Geringe Performance
	Aufwändige Fehlersuche

2.2.2 CSMA/CD

CSMA/CD steht für „Carrier Sense Multiple Access / Collision Detection“ und kommt bei Bus-Netzwerken zum Einsatz.

Das Zugriffsverfahren läuft wie folgt ab:

1. Die Station überprüft ob der Übertragungsbus frei ist oder zur Zeit bereits von einer anderen Station benutzt wird (Carrier Sense). Falls auf dem Bus eine Datenbertragung festgestellt wird, führt diese eine erneute Überprüfung durch.
2. Wenn der Bus frei, startet die Station mit dem Sendevorgang. Es kann nun aber sein, dass 2 Stationen mitteinander zu senden beginnen (sei es durch Zufall, im selben Zeitraum, oder distanzbedingt). Da bei einem Bus-System die Stationen auf einem gemeinsamen Übertragungsmedium (Multiple Access) senden, kommt es zu Kollisionen. Jede Station muss solche Kollisionen entdecken können und hört deshalb seine eigene Sendung mit. Bei Kollisionen wird der Sendevorgang sofort abgebrochen (Collision Detection) und nach einer, durch den Backoff-Algorithmus bestimmten, Wartezeit versucht die Station ihre Daten erneut zu senden. Dieser Vorgang kann sich mehrere male wiederhohlen. die Wartezeit wird dabei immer grösser.
3. Dieser Mechanismus zur Kollisionserkennung muss nun aber nicht während der ganzen Übertragungszeit angewandt werden. Bei 10 bzw. 100MBit/s-Netzen muss diese Überprüfung nur für die Übertragung der ersten 576 Bits durchgeführt werden. Man spricht hier von 576 Bitzeiten. Dieser Wert berechnet sich aus den kleinstmöglichen Frames von 64 Byte = 512 Bit plus einer Sperrzeit für die Kollisionserkennung. Bei 1GB/s-Netzen ist dieser Wert so nicht mehr gültig da die resultierende maximale Buslänge damit auf ca. 20m begrenzt würde. Hier wird deshalb durch Fülldaten die minimale Framegrösse auf 512 Byte und entsprechend die Zeitspanne erhöht, während die eine Station eine Kollisionserkennung durchführen muss.

1 Mit CSMA/CD wird aber darauf reagiert

4. Nach der vorgeschriebenen Kollsionserkennung kann die Station die verbliebenen Framedaten ohne weitere Überprüfungen versenden. Sie kann hier davon ausgehen, dass nun endgültig alle Stationen im Netz erkannt haben, dass der Bus belegt ist und keine Daten mehr senden. Unter speziellen Umständen ist es möglich, wenn die maximale Ausdehnung des Busses zu gross ist oder per Repeater/Hubs zu viele Netzsegmente gekoppelt wurden, dass es zu Kollisionen kommen kann (Late Collisions). Diese Kollisionen werden dann von der Sendestation nicht mehr erkannt und können nur von höheren Protokollebenen (z.B. Schicht 4 eines verbindungsorientierten Protokolls) korrigiert werden.

Wenn der Sendevorgang eine gewisse Zeit nicht klappt, gilt dieser als gescheitert und wird nicht mehr wiederholt. In diesem Falle wird die nächst höhere Schicht darüber informiert (Fehlermeldung).

2.2.2.1 Einige Grössen

Für das CSMA/CD-Verfahren existieren einige wichtige Grössen. Wie diese berechnet werden, wird im folgenden erklärt:

- Slot Time
  Die für das Absenden eines Rahmens minimaler Länge benötigte Zeit

$$Slot\ Time = \frac{minimale\ Rahmengrösse}{Übertragungsrate} = \frac{512\ Bit}{10\ MBit/s} = 51.2\ \mu s$$

- Interframe Gap
  Die zeitliche Lücke zwischen zwei aufeinander folgenden Rahmen

$$Interframe\ Gap = \frac{96\ Bit}{10\ MBit/s} = 9.6\ \mu s$$

- Round Trip Delay
  Die Zeit die benötigt wird um ein Signal von Host A zu Host B hin und zurück zu übertragen, Host A und Host B sind dabei die am weitesten auseinanderliegenden Hosts im Netz

$$Round\ Trip\ Delay = \frac{Strecke}{Übertrgungsgeschwindigkeit} = \frac{500\ m}{231'000\ km/s} = 2.165\ \mu s$$

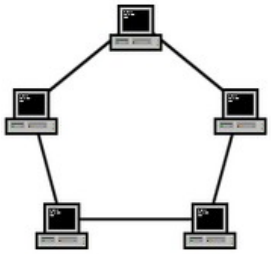
- Backoff Time
  Nach einer Kollision wird diese Zeit abgewartet, bevor erneut gesendet wird. Die Zufallszahl wird bei jedem Durchlauf aus einem grösseren Bereich gebildet.

$$Backoff\ Time = Zufallszahl \times Slot\ Time$$

2.3 Ring

Jedes Endgerät hat eine Verbindung zu zwei weiteren Endgeräten, sodass ein geschlossener Ring entsteht. Es gibt kein zentrales Netzwerkgerät.

Ein Datenpaket wird von Teilnehmer zu Teilnehmer weitergeleitet, bis es seinen Bestimmungsort erreicht hat.



2.3.1 Bewertung

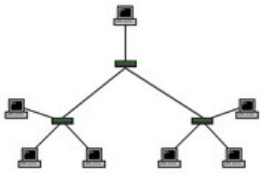
Vorteile	*Nachteile*
Geringer Verkabelungsaufwand	Fällt ein Teilnehmer aus, so ist keine Kommunikation mehr möglich [2]

2 Neue Karten verfügen über eine Protection-Umschaltung, wodurch der Datenstrom einfach über die andere Richtung umgeleitet wird

Vorteile	*Nachteile*
Alle Teilnehmer sind gleichberechtigt	Geringe Geschwindigkeit
Kollisionsfreie Übertragung	Aufwändige Erweiterung
Signal wird bei jedem Teilnehmer verstärkt	Jedes Paket wird an jeden Teilnehmer gesendet (Sicherheit)
Grosse Netzausdehnung	Aufwändige Fehlersuche

2.4 Baum

Mehrere Sternförmige Netzwerke können zu einem baumförmigen Netzwerk verbunden werden.



Dafür werden die zentralen Knoten der Sterne mit einem Uplink verbunden. Es entsteht ein hierarchisches Netzwerk.

Diese Topologie wird vor allem in grossen Gebäuden verwendet um mehrere Sterne miteinander zu verbinden.

2.4.1 Bewertung

Vorteile	*Nachteile*
Leicht erweiterbar	Wenn ein Uplink ausfällt, sind alle untergeordneten Äste tot
Es können riesige Gebiete erschlossen werden	Hohe Kosten durch Verkabelungsaufwand
Siehe Stern-Topologie	Siehe Stern-Topologie

2.5 Vermaschtes Netz

In einem vermaschtem Netz ist jedes Endgerät mit einem oder mehreren anderen Endgeräten verbunden. Fällt ein Knoten aus, so besteht in den meisten Fällen ein alternativer Weg für die Datenpakete. Um diese Wege finden zu können, werden komplizierte Routing-Mechanismen eingesetzt.

In einem vermaschtem Netz werden oftmals Netze mit verschiedenen Topologien zusammengeschlossen, das Internet ist beispielsweise auch ein vermaschtes Netz.

2.5.1 Bewertung

Vorteile	*Nachteile*
Hohe Ausfallsicherheit durch alternative Wege	Hoher Verkabelungsaufwand
	Schwer verständlich durch Komplexe Routingmechanismen

2.6 Zelltopologie

Bei drahtlosen Netzen wird ein bestimmtes erschlossenes Gebiet als „Zelle“ bezeichnet. Eine Zelle ist ein Bereich, in welchem eine drahtlose Kommunikation verschiedener Geräte über verschiedene Frequenzbereiche (WLAN, Bluetooth, Infrarot, ...) möglich ist.

Zellen können sich dabei überschneiden oder weit voneinander entfernt sein.

Da die Zelltopologie nur bei drahtlosen Netzwerken anzutreffen ist, kann diese nicht mit anderen Topologien wie z.B. Stern oder Ring verglichen werden.

3 Netze

Netzwerke können nicht nur nach ihrer Topologie, sondern auch nach ihrer räumlichen Ausdehnung klassifiziert werden.

Werden zwei oder mehrere Netzwerke der selben Stufe zusammengeschlossen, so entsteht ein Netzwerk der nächst höheren Stufe.

3.1 PAN

Unter einem Personal Area Network (Abkürzung: PAN) versteht man ein Netz, welches aus Kleingeräten wie z.B. PDAs oder Mobiltelefonen aufgebaut werden kann.

PANs können daher mittels verschiedener drahtgebundenen Übertragungstechniken, wie USB oder FireWire wie auch mittels drahtlosen Techniken, wie IrDA oder Bluetooth aufgebaut werden (WPAN). Die Reichweite beträgt gewöhnlich nur wenige Meter, womit die PANs die kleinsten Netze der Netzhierarchie darstellen.

3.2 LAN

Unter einem Local Area Network (LAN) versteht man ein Computernetz innerhalb eines räumlich begrenzten Gebiets, wie z.B. ein Gebäude oder ein Stockwerk.

Ein LAN kann mittels verschiedenster Technologien aufgebaut werden. Ethernet per Twisted-Pair-Kabel, speziell Fast Ethernet mit bis zu 1000 MBit/s (125 MByte/s) Datendurchsatz pro Sekunde (Gigabit-LAN), ist der am weitesten verbreitete Standard. Zunehmend unbedeutender sind Token Ring, FDDI und ARCNET.

In der Regel stellt ein LAN genau eine Broadcast-Domäne dar, also den Bereich eines Rechnernetzes, in dem alle angeschlossenen Geräte mit ihrer Hardware-Adresse (MAC-Adresse) auf Schicht 2 des ISO/OSI-Referenzmodells (data link layer - der Sicherungsschicht) direkt miteinander kommunizieren können.

3.3 MAN

Ein Metropolitan Area Network oder kurz MAN ist ein Netzwerk, das sich über ein Gebiet in der Grössenordnung einer Grossstadt, einem grossen Industriegebiet oder einer Agglomeration erstrecken kann.

MANs werden oft von international tätigen Telekommunikationsfirmen aufgebaut, die dann auf diese Weise verkabelte Metropolen wiederum in einem Wide Area Network (WAN) national oder sogar international Global Area Network (GAN) wieder vernetzen.

3.4 WAN

WAN ist die Abkürzung für Wide Area Network, deutsch: grossräumiges Netz.

WAN ist ein Computernetz, das sich im Gegensatz zu LANs oder MANs über einen sehr grossen geographischen Bereich erstreckt. Die Anzahl der angeschlossenen Rechner ist auf keine bestimmte Zahl begrenzt. WANs erstrecken sich über Länder oder sogar Kontinente. WANs werden benutzt, um verschiedene LANs, aber auch einzelne Computer miteinander zu verbinden.

Wegen der grossen Anzahl der angeschlossenen Rechner ist das unadressierte Senden von Informationen (Broadcasting) an alle Rechner sehr ineffizient. Deshalb werden Daten nur an bestimmte Empfänger gesendet.

3.5 GAN

GAN ist eine Abkürzung für Global Area Network.

Unter einem GAN versteht man ein Netz das weltweit mehrere WANs verbindet. Dies kann zum Beispiel die Vernetzung weltweiter Standorte einer internationalen Firma sein. Oft wird bei einem GAN Satellitenübertragung eingesetzt.

3.6 Architekturen

Mit dem Begriff IT-Architektur wird häufig der konzeptionelle Aufbau der Informationssysteme einer Organisation/eines Unternehmens bezeichnet.

Zwei Netzwerkarchitekturen haben sich im Laufe der Zeit durchgesetzt. Das Client/Server-Architektur und das Peer to Peer Netz.

3.6.1 Client/Server

Bei einer Client/Server-Architektur werden gemeinsam genutzte Informationen auf einem zentralen System, dem Server, gespeichert. Einem Server sind meistens mehrere Clients untergeordnet. Durch die zentrale Speicherung und die zentrale Verwaltung von Rechten kann so nicht nur die Sicherheit erhöht, sondern auch der Aufwand verringert werden. So wird z.B. eine Datensicherung stark erleichtert.

Ein Server ist im Prinzip kein anderes Gerät als ein normaler PC, nur dass noch einige zusätzliche Dienste auf ihm laufen. In der Praxis wird aber für einen Server oftmals teurere Hardware verbaut und ein anderes Betriebssystem als auf den Clients installiert.

Mit der Verbreitung der Personal-Computern wurde immer mehr Rechenkapazität auf die Clients ausgelagert. Der Server in einem solchen Umfeld bietet meist nur noch die Daten an. Eine häufige Form ist z.B. ein zentraler Datenbankserver.

3.6.2 Peer to Peer

Bei einem Peer to Peer Netzwerk wird nicht zwischen Server und Client unterschieden; jeder Computer dient gleichermassen als Server wie auch als Client. Jeder Computer kann dabei gewisse Dienste zur Verfügung stellen und die Dienste anderer, sich im Netzwerk befindlichen, Computer nutzen.

3.6.3 Vergleich der Architekturen

Die beiden Architekturen bieten gewisse Vor- und Nachteile, hier eine Übersicht:

Architektur	***Client/Server***	***Peer to Peer***
Kosten	Durch einen zusätzlichen Server werden hohe Kosten verursacht. Mit der Zeit spart man jedoch durch den geringeren Verwaltungsaufwand einiges an Geld.	Es wird kein zusätzlicher Server benötigt. Die Verwaltungskosten können jedoch bei steigenden Anforderungen stark zunehmen.
Installation	Das einrichten eines Servers und der Zusammenschluss mit den Clients erfordert grosses Wissen und auch Erfahrung. Die korrekte Konfiguration des Netzes kann je nach Netzwerkgrösse Tage bis sogar Jahre dauern.	Die Installation ist relativ simpel und erfordert eher wenig Aufwand. Da aber Dienste auf verschiedene Computer aufgeteilt werden, muss man in der Planung sehr vorsichtig sein. Ansonsten könnte eine Arbeitsstation überlastet werden.

Architektur	*Client/Server*	*Peer to Peer*
Performance	Da Netzwerkspezifische Aufgaben vom Server übernommen werden, haben die Clients eine kleinere Last zu tragen.	Je nach dem, welche Dienste auf einem Computer laufen, kann dieser erheblich verlangsamt werden.
Sicherheit	Da die gesamte Kommunikation gegen aussen (Internet) über den Server läuft und die Rechte zentral verwaltet werden, kann eine hohe Sicherheit erreicht werden.	Durch Sicherheitsdefizite an einem Rechner kann ein potentieller Angreifer auf das gesamte Netz gelangen. Da die Rechner nicht permanent laufen sind diese möglicherweise auch nicht immer auf dem neuesten Sicherheitsstand.
Updates	Software kann bequem über den Server aktualisiert werden, Updates können von den Clients über den Server bezogen werden.	Software muss auf jedem Rechner separat aktualisiert werden.
Backup	Gemeinsam genutzte Dateien werden auf dem Server abgelegt. Dies erleichtert ein Backup stark.	Wichtige Daten müssen von jedem Rechner einzeln gesichert werden.
Erweiterung	Kleinere Erweiterungen stellen kein Problem dar, bei Grösseren hingegen muss man möglicherweise einen weiteren Server in das Netz miteinbeziehen und die Aufgaben neu auf die Server verteilen.	Eine Erweiterung ist eher mühsam, da auf dem neuen Rechner wieder sämtliche Zugriffe auf die anderen Rechner konfiguriert werden müssen. Grössere Erweiterungen sind nur schlecht möglich, ein Peer to Peer Netzwerk macht nur bei wenigen Clients Sinn – man müsste auf die Client/Server Architektur ausweichen.

3.6.3.1 Fazit

Ein Client/Server-Netzwerk ist zwar am Anfang mit etwas höheren Kosten verbunden, auf die Dauer ist diese Architektur jedoch sehr viel komfortabler und in manchen Fällen auch günstiger, als ein Peer to Peer Netzwerk.

4 OSI-Referenzmodell

Das OSI-Referenzmodell ist ein offener Standard, der die Kommunikation zwischen verschiedenen informationsverarbeitenden Geräten beschreibt und ist die Grundlage für die meisten herstellerunabhängigen Protokolle.

Die Kommunikation wird auf sieben Schichten aufgeteilt. Jede dieser Schichten hat eine klare Aufgabe und funktioniert unabhängig von höheren oder tieferen Schichten. Eine Schicht bietet den anderen Schichten gewisse Dienstleistungen und bezieht ihrerseits auch Dienstleistungen anderer Schichten.

Die Kommunikation läuft beim Sender von der obersten Schicht (der Anwendung) zur untersten Schicht (der physikalischen Übertragung) und schliesslich zum Empfänger. Beim Empfänger läuft die Kommunikation genau umgekehrt ab; von der untersten Schicht wieder zur obersten Schicht. Logisch gesehen sieht es so aus, als ob jeweils die gleichen Schichten miteinander kommunizieren würden, jedoch erfolgt eine Kommunikation immer nur auf der untersten Schicht.

Hier eine Übersicht über die einzelnen Schichten:

#	Schicht	English	Einordnung	Einheiten
7	Anwendung	Application	Anwendung	Daten
6	Darstellung	Presentation		
5	Sitzung	Session		
4	Transport	Transport	Transport	Segmente
3	Vermittlung	Network		Pakete
2	Sicherung	Data Link		Frames
1	Datenübertragung	Physical		Bits

4.1 Schicht 1 (Physical)

Bei der ersten Schicht handelt es sich um die rein physikalische Übertragung der Daten, es kommt also keinerlei Software zum Einsatz.

Die Übertragung findet dabei auf Lichtwellenleitern, Kupferdräten oder sonstigen Medien statt. Es werden dabei nur Bit-Folgen übertragen, die physikalische Schicht kennt keinerlei Logik.

Bestimmte Hardware (neben Antennen oder Übertragungskabel) funktionieren auch auf der untersten Schicht, wie z.B. der Hub oder der Repeater.

4.2 Schicht 2 (Data-Link)

Die Sicherungsschicht hat die Aufgabe, den Zugriff auf die physische Schicht zu regeln und die Korrektheit der Datenübertragung zu gewährleisten. Weiter wird der Bit-Datenstrom in Rahmen umgewandelt (und umgekehrt) und die Daten werden mit Prüfsummen versehen und kontrolliert. Verlorengegangene und fehlerhafte Pakete können erneut angefordert werden.

Hardware, wie z.B. multiport Bridges oder Switches funktionieren auf der zweiten Schicht.

4.3 Schicht 3 (Network)

Die Vermittlungsschicht schaltet die notwendigen Verbindungen für die Datenübertragung und leitet Datenpakete an deren jeweiliges Ziel weiter, auf diese Weise wird netzwerkübergreifende Kommunikation möglich.

Die Aufgabe der dritten Schicht ist grob gesagt das ganze Routing, was auch das Aufbauen und das Aktualisieren von Routingtabellen umfasst. Ein Router ist also klar auf der Vermittlungsschicht einzuordnen.

4.4 Schicht 4 (Transport)

Die Transportschicht segmentiert die Datenpakete und ist dafür verantwortlich, dass es auf den tieferen Schichten keinen Stau an Datenpaketen geben kann. Sie ist die oberste Schicht, die sich um die Übertragung der Daten kümmert und soll den Schichten 5 bis 7 einen einheitlichen Zugriff bieten, sodass die oberen Schichten sich nicht weiter um die Eigenheiten des Netzwerks kümmern müssen.

4.5 Schicht 5 (Session)

Auf der Sitzungsschicht wird die logische Verbindung hergestellt und verwaltet. So ist z.B. der synchronisierte Datenaustausch eine Aufgabe dieser Schicht. Bei Übertragungsausfällen kann mit Fixpunkten die Verbindung erneut erstellt werden, die Datenübertragung kann so fortgesetzt werden.

4.6 Schicht 6 (Presentation)

Die Darstellungsschicht führt die übertragenen Daten in ein bestimmtes Format, wie z.B. ASCII oder Unicode, über. Hier wird auch die Kompression/Dekompression sowie die Ver- und Entschlüsselung vorgenommen.

4.7 Schicht 7 (Application)

In der obersten Ebene werden die zu senden Daten zusammengestellt oder ausgegeben. Beispiele dafür sind das Verfassen/Anzeigen einer E-Mail oder einer Kurznachricht.

5 TCP/IP

Die Internetprotokollfamilie TCP/IP umfasst über 500 Protokolle, welche die Basis für die gesamte Internetkommunikation bilden. Da sich die einzelnen Protokolle nicht eindeutig einer OSI-Schicht zuordnen lassen können, greift man auf ein eigenes Modell, das TCP/IP-Modell, zurück.

Im Gegensatz zum OSI-Modell ist der Zugriff auf eine Schicht aus einer beliebigen Schicht möglich, die Unterteilung verläuft etwas weniger strikt. Ausserdem existieren beim TCP/IP-Modell nur vier Schichten, man hat die Aufgaben gegenüber OSI etwas zusammengefasst.

Hier ein Überblick über das TCP/IP-Modell im Bezug auf das OSI-Referenzmodell.

#	*TCP/IP-Schicht*	*Zugehörige OSI-Schicht*	*Protokolle*
4	Anwendung	Application, Presentation, Session	HTTP, FTP, SMTP, POP3
3	Transport	Transport	TCP, UDP
2	Netz/Internet	Network	IP (v4, v6), ARP
1	Netzzugang	Data Link, Physical	Ethernet, WLAN

5.1 TCP/IP Verbindung

TCP/IP arbeitet verbindungsorientiert. Dabei muss der Sender zuerst wissen, ob der Empfänger auch wirklich erreichbar ist und so eine Verbindung erstellt werden kann. Der Verbindungsaufbau funktioniert dabei nach dem Drei-Wege-Handshake, welcher (stark vereinfacht) etwa so aussieht:

1. Station A sendet Station B ein bestimmtes Signal
2. Station B erhält das Signal von Station A und schickt eine Bestätigung an Station A
3. Station A erhält diese Bestätigung, die Verbindung steht

Wenn Station A nun nach Schritt 3 die Bestätigung erhalten sollte, so ist die Warscheinlichkeit gross, dass eine Übertragung gut verlaufen kann. Eine absolute Sicherheit existiert nicht, da Station A das Bestätigungssignal von Station B seinerseits auch bestätigen müsste – dies müsste unendlich fortgesetzt werden.

5.2 IP (v4)

Das IP-Protokoll arbeitet auf der Netzwerk-Schicht des TCP/IP-Modells und ist das tiefste Protokoll, das nicht an das Übertragungsmedium gebunden ist. Mit der IP-Adresse lässt sich ein Host in einem Netzwerk identifizieren, mithilfe der Subnet-Mask kann festgestellt werden, in welchem Teilnetz sich ein Host befindet.

5.2.1 IP-Adresse

Eine IP-Adresse (v4) setzt sich aus 4 Zahlen zusammen, die jeweils 1 Byte gross sind. D.h. ein Segment (= 1 Byte der Adresse) kann Werte von 0 bis 255 einnehmen, die einzelnen Segmente werden durch einen Punkt voneinander getrennt. Beispiele für IP-Adressen:

```
192.168.0.1
10.92.210.95
```

Aus vier Bytes können bekanntlich mehr als 4.3 Milliarden Zahlen gebildet werden.

5.2.2 Spezielle IP-Adressen

Pro Netzwerk gibt es zwei spezielle IP-Adressen, welche nicht an Hosts vergeben werden dürfen.

5.2.2.1 Die Netzadresse

Diese Adresse gibt an, in welchem Netzwerk sich ein Host befindet. Die Netzwerkadresse ist das Ergebnis einer bitweisen UND-Verknüpfung aus einer Hostadresse mit der dazugehörigen Subnetmask:

Adresse	*dezimal*	*binär*
Host	192.168.0.129	11000000.10101000.00000000.10000001
Subnet	255.255.255.0	11111111.11111111.11111111.00000000
Netz	**192.168.0.0**	**11000000.10101000.00000000.00000000**

5.2.2.2 Die Broadcast-Adresse

Die Broadcast-Adresse ist die höchste IP-Adresse in einem Netzwerk. Im Netz 192.168.15.0/24 wäre die Broadcast-Adresse z.B. 192.168.15.255. Sie wird dazu verwendet um alle Hosts in einem Netz anzusprechen. Datenpakete die von einem Host an die Broadcast-Adresse versendet werden, gelangen an alle Hosts.

5.2.3 Subnetzmaske

Die Subnetzmaske (oder Subnetmask) gibt Auskunft darüber, in welchem Netzwerk sich ein Host befindet. Jede Subnetmask ist in zwei Teile unterteilt; in einen Netz- und einen Hostteil. Der Netzteil besteht aus positiven Bits (1), der Hostteil aus negativen (0). Damit die Funktionsweise einer Subnetmask klar wird, sollte diese binär und nicht dezimal dargestellt werden:

```
255.255.255.0 = 11111111.11111111.11111111.00000000
```

Bei dieser Subnetmask sind 24 Bit für den Netzteil und 8 für den Hostteil reserviert. Die Reihe von positiven Bits darf nie durch negative Bits unterbrochen werden! Sobald ein negative Bit auftritt müssen alle weiteren Bits ebenfalls negativ sein. Ein Byte einer Subnetmask kann also nur folgende Werte annehmen:

- `128 (10000000)`
- `192 (11000000)`
- `224 (11100000)`
- `240 (11110000)`
- `248 (11111000)`
- `252 (11111100)`

- 254 (11111110)
- 255 (11111111)

Wie man herausfinden kann, ob eine Kommunikation zwischen zwei Hosts (A und B) möglich ist, findet man wie folgt heraus:

- Man ermittelt die Netzadresse des ersten Hosts (A) anhand der oben gezeigten Vorgehensweise (siehe Netzadresse ermitteln)
- Mit dem zweiten Host (B) geht man nun genau gleich vor
- Sind die beiden Netzadressen gleich, so ist eine Kommunikation ohne weiteres möglich. Sind die Adressen jedoch unterschiedlich, so wird für die Kommunikation ein Router benötigt.

5.2.3.1 Die CIDR-Schreibweise

Eine Subnetmask muss nicht unbedingt mit 4 Bytes dargestellt werden, es geht auch kürzer. So reicht es, wenn man an eine IP-Hostadresse einfach, getrennt durch einen Schrägstrich, die Anzahl der Netzbits anhängt:

`IP: 192.168.0.0, Subnetmask: 255.255.255.0 --> 192.168.0.0/24`

Die Eindeutigkeit bleibt dabei aber trotzdem vorhanden.

5.3 Netzwerkklassen

In der Entstehungszeit des Internets hat man sogenannte Adressklassen definiert um die IP-Adressen besser verteilen zu können:

Netzklasse	*Adressbereich*	*Subnetmask*
Klasse A	0.0.0.0 - 127.255.255.255	255.0.0.0
Klasse B	128.0.0.0 - 191.255.255.255	255.255.0.0
Klasse C	192.0.0.0 - 223.255.255.255	255.255.255.0
Klasse D	224.0.0.0 - 239.255.255.255	-
Klasse E	240.0.0.0 - 255.255.255.255	-

Die Klasse A ist ausschliesslich für nordamerikanische Grossfirmen (General Electrics, Apple, IBM) und für ein paar grössere Hochschulen (z.B. MIT) reserviert. Da aber selbst diese grossen Firmen niemals 16 Millionen Hosts benötigen, werden sehr viele IP-Adressen verschwendet. Damit man dieser Verschwendung entgehen konnte wurde das Classless Inter Domain Routing (CIDR) eingeführt.

Auf diese Weise können Subnetmasken (wie bereits beschrieben) nicht mehr nur die Werte 0 oder 255 einnehmen und es werden nicht mehr ganz so viele IP-Adressen verschwendet, jedoch kann noch lange nicht jede IP-Adresse genutzt werden!

5.4 Subnetting

Oftmals ist es nötig, ein grosses Netzwerk in einige kleinere zu unterteilen. Dies tut man weil manche Arbeitsstationen sich physisch an einem anderen Ort befinden als eine andere Gruppe oder wenn man zwei Teilen (auch mit unterschiedlicher Anzahl an Hosts) die gleiche Bandbreite zusichern will.

Damit man Subnetze (Unternetze) bilden kann, sind zwei Angaben notwendig. Die Netzadresse mitsamt der Subnetmask und die Anzahl der zu bildenden Teilnetze. Aus diesen Daten sollen folgende Informationen errechnet werden:

- Die Subnetmask
- Die IP-Adressbereiche der einzelnen Subnetze

Für das Berechnungsbeispiel wird mit folgenden Daten gearbeitet:

- Netzwerkadresse: 10.35.0.0
- Subnetmask: 255.255.0.0
- Anzahl zu bildender Teilnetze: 3

Die Teilnetze werden dann wie folgt gebildet:

5.4.1 Anzahl Teilnetze berechnen

Die Anzahl der zu erstellenden Teilnetze ist zwar schon gegeben, in der Praxis lässt sich jedoch längst nicht jede Anzahl realisieren. Die Anzahl der Teilnetze muss immer einer Zweierpotenz entsprechen und wird wie folgt berechnet:

$Anzahl = 2^x$ dabei gilt: $128 > Anzahl \geq Anzahl\ zu\ bildender\ Teilnetze$

Zwar lassen sich pro Netz 128 Teilnetze erstellen, dies macht jedoch keinen Sinn, da dann sämtliche Adressen für das Netz bzw. für das Broadcasting verwendet würden – Hosts könnten dabei nicht adressiert werden und müssten über Broadcast-Meldungen angesprochen werden. Dies macht nur wenig Sinn.

Auf die gegebenen Daten bezogen ergibt sich folgende Rechnung:

$$\underline{Anzahl} = 2^2 = \underline{4}$$

Es müssen in Tat und Wahrheit also **vier** Teilnetze gebildet werden.

5.4.2 Bildung der Subnetmask

Nun gilt es, die Subnetmask zu bilden. Anhand dieser kann man danach die Subnetze bestimmen. Dazu teilen wir die Anzahl möglicher IP-Adressen durch die Anzahl der zu erstellenden Teilnetze. Das Ergebnis aus dieser Rechnung wird von der Anzahl möglicher IP-Adressen abgezogen:

$$Subnetmask = 256 - (\frac{256}{Anzahl\ Subnetze})$$

Auf unser Beispiel bezogen erhält man folgende Rechnung:

$$\underline{Subnetmask} = 256 - (\frac{256}{4}) = \underline{192}$$

Durch diese Berechnung erhält man natürlich nicht die ganze Subnetmask, sondern nur noch den Teil, den wir an die Subnetmask anhängen müssen. Aus der Maske 255.255.0.0 wird also 255.255.192.0.

Unsere Subnetmask lautet also: **255.255.192.0**

5.4.3 Netze bilden

Der Rest ist reine Fleissarbeit. Man beginnt mit der ursprünglichen Netzadresse (10.35.0.0) und sucht nun die darauf folgende Netzadresse. Da die Subnetmask angibt, dass die Grenze zwischen Host- und Netzteil im dritten Segment liegt, muss auch dieses Segment hochgezählt werden und zwar mit folgendem Wert:

$$Wert = \frac{256}{Anzahl\ Subnetze}$$

Für unser Beispiel ergibt dies folgende Rechnung:

$$Wert = \frac{256}{4} = \underline{64}$$

Das dritte Segment muss also jeweils mit dem Wert 64 erhöht werden um das nächste Netzadresse zu errechnen. Die Broadcast-Adressen sind auch einfach zu errechnen, man nimmt immer die nächstkleinere Adresse des Netzes mit der nächsthöheren Adresse. Die Hosts liegen dann zwischen Netz- und Broadcastadresse.

5.4.4 Lösung

Durch obige Berechnungen kann das ursprüngliche Netz in folgende Teilnetze gegliedert werden:

Subnet	*Netzadresse*	*Broadcastadresse*	*Erster Host*	*Letzter Host*
1	10.35.0.0	10.35.63.255	10.35.0.1	10.35.63.254
2	10.35.64.0	10.35.127.255	10.35.64.1	10.35.127.254
3	10.35.128.0	10.35.191.255	10.35.128.1	10.35.191.254
4	10.35.192.0	10.35.255.255	10.35.192.1	10.35.255.254

Subnetmask: `255.255.192.0`

5.4.5 Rückwärtsrechnung

Manchmal muss man herausfinden, in welchem Subnet sich ein bestimmter Host befindet. Folgende Informationen sind gegeben:

- Subnetmask: `255.255.248.0`
- Host-Adresse: `58.63.97.15`

Da die Grenze zwischen dem Netz- und dem Hostteil in der Subnetmask im dritten Segment liegt, ist auch nur dieses für unsere Berechnung relevant.

Als erstes muss dieses dritte Segment der Subnetmask von der maximalen Anzahl an Adressen pro Byte abgezogen werden:

$$256 - 248 = \underline{8}$$

Nun können wir das Subnet ganz bequem mit folgender Rechnung herausfinden, auch hier interessiert uns nur das dritte Segment, diesmal aber das der Host-IP:

$$Teilnetz = \frac{97}{8} = \underline{12}$$

Der Rest interessiert uns nicht weiter.

Der Host mit der IP-Adresse 58.63.97.15 befindet sich also im zwölften Teilnetz.

5.5 Supernetting

Supernetting ist das Gegenteil von Subnetting.

Dieses Verfahren beschreibt die Einteilung des IP-Adress-Raumes in mehrere Klassen (A, B, C und auch D und E). Die Anzahl der verfügbaren Netzwerke und Hosts ist je nach Klasse fest vorgegeben. So stehen für ein Netz der Klasse C mit der Subnetmask 255.255.255.0 nur 254 verfügbare Hostadressen bereit. Falls mehr Adressen in einem Netz benötigt werden, müsste ein Netz der Klasse B (Subnetmask 255.255.0.0) mit dann 65534 möglichen Adressen verwenden. Um die Verschwendung von ungenutzten IP-Adressen zu verkleinern, wird mit Supernetting eine feinere Unterteilung ermöglicht.

Supernetting fasst durch Verkürzung der Netzmaske Netze der gleichen Klasse zu einem Netz zusammen. Mit der Netzmaske 255.255.252.0 sind somit 1022 Hosts in einem Netz adressierbar.

Die Netze 193.10.4.0/24, 193.10.5.0/24, 193.10.6.0/24 und 193.10.7.0/24 befinden sich alle an einem Standort. Durch Supernetting kann man diese vier Netze zu dem Netz 193.10.4.0 mit der Netzmaske 255.255.252.0 zusammenfassen.

Dies macht beispielsweise auch das Routing über die genannten Netze überflüssig, da jetzt nur noch ein Netz vorhanden ist.

Mit dem Entstehen des klassenlosen Verfahren CIDR hat der Begriff Supernetting seine Bedeutung verloren.

5.6 Ports

Ein Port ist eine Adresskomponente mit der die Zuordnung von Datenpaketen an ein bestimmtes Protokoll erleichtert wird. Eine Portnummer ist eine 16 Bit/2 Byte Zahl, die Werte von 0 bis 65'535 einnehmen kann. Ports sind in TCP/IP implementiert und können für eigene Protokolle registriert bzw. gemietet werden. Damit TCP/IP die zu sendenden Datenpakete an das Protokoll SMPT übergibt, wird folgende Schreibweise verwendet:

```
10.69.18.155:25
```

Wobei 10.69.18.155 die IP-Adresse des Servers und 25 die registrierte Portnummer für das SMTP-Protokoll ist.

Einige wichtige Portnummern sind:

- 24 = FTP für den Dateitransfer
- 25 = SMTP für das Versenden von E-Mails
- 53 = DNS für die Auflösung von Domänennamen
- 80 = HTTP für Webserver
- 110 = POP3 für das Empfangen von E-Mails

5.7 UDP

Das User Datagramm Protocoll (UDP) ist ein verbindungsloses Protokoll das auf der Transportebene des TCP/IP-Modells einzuordnen ist. Da das Protokoll verbindungsunabhängig operiert, ist der Empfang der Datenpakete nicht gewährleistet. Ein Paket wird einfach an einen bestimmten Zielhost gesendet, was mit dem Paket weiter passiert spielt für UDP keine weitere Rolle. Solche Korrekturmassnahmen müssen auf der Anwendungsebene getroffen werden.

Bei kleinen Datenmengen kann die Geschwindigkeit so enorm erhöht werden, da keine Verbindung auf- und abgebaut werden muss. Bei grösseren Datenmengen empfiehlt sich jedoch eine TCP/IP-Verbindung mit Handshake.

6 Protokollle

Ein Protokoll ist eine klare Abmachungen zwischen zwei Parteien, welche Struktur die Daten haben müssen, damit sie zwischen diesen beiden Parteien ausgetauscht werden können. Für einen Datenaustausch werden meistens mehrere Protokolle benötigt, für das Abrufen einer Homepage aus einem Webbrowser wird neben HTTP beispielsweise auch noch TCP/IP verwendet, welches sich aus mehreren Protokollen zusammensetzt.

Im folgenden werden einige wichtige Protokolle kurz erläutert:

6.1 HTTP

Das Hypertext Transfer Protocol (HTTP) ist ein zustandsloses Protokoll zur Übertragung von Daten.

HTTP ist ein Kommunikationsschema, um Webseiten (oder Bilder oder prinzipiell jede andere beliebige Datei) von einem entfernten Computer auf den eigenen zu übertragen.

Wenn auf einer Webseite der Link zur URL http://www.example.net/infotext.html aktiviert wird, so wird an den Computer mit dem Namen www.example.net die Anfrage gerichtet, die Datei infotext.html zurückzusenden. Der Name www.example.net wird dabei zuerst über das DNS-Protokoll in eine IP-Adresse umgesetzt. Zur Übertragung wird über das TCP-Protokoll auf Port 80 eine HTTP-GET-Anforderung gesendet.

Zusätzliche Informationen wie Angaben über den Browser, zur gewünschten Sprache etc. können über einen Header (Kopfzeilen) in jeder HTTP-Kommunikation übertragen werden. Sobald der Header mit einer Leerzeile abgeschlossen wird, sendet dann der Computer, der einen Web-Server (an Port 80) betreibt, seinerseits eine HTTP-Antwort zurück. Diese besteht aus Header-Informationen des Servers, einer Leerzeile und dem Inhalt der Datei infotext.html. Die Datei ist normalerweise im Hypertext-Format HTML, das vom Browser in eine lesbare Darstellung gebracht wird. Es kann jedoch jede andere Datei in jedem beliebigen Format sein, zum Beispiel Bilder, Audio- und Videodateien. Die Informationen können auch dynamisch generiert werden und braucht auf dem Server nicht als Datei abgelegt zu sein.

Der Server sendet eine Fehlermeldung zurück, wenn die Information aus irgendeinem Grund nicht gesendet werden kann. Der genaue Ablauf dieses Vorgangs (Anfrage und Antwort) ist in der HTTP-Spezifikation festgelegt.

6.2 FTP

Das File Transfer Protocol (FTP), ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP ist in der Anwendungsschicht von TCP/IP angesiedelt. Es wird benutzt, um Dateien vom Server zum Client (Download), vom Client zum Server (Upload) oder clientgesteuert zwischen zwei Servern zu übertragen.

Viele FTP-Server bieten sog. Anonymous FTP an. Hier ist zum Einloggen neben den realen Benutzerkonten ein spezielles Benutzerkonto, typischerweise "anonymous" vorgesehen, für das kein Passwort angegeben werden muss. Zum "guten Ton" gehört jedoch, bei anonymem FTP seine eigene, gültige E-Mail-Adresse als Passwort anzugeben.

6.3 SMTP

Die Abkürzung SMTP steht für Simple Mail Transfer Protocol (Einfaches E-Mail-Übertragungsverfahren). SMTP ist ein Protokoll der TCP/IP-Protokollfamilie, das den Versand von E-Mails in Computer-Netzwerken regelt. Ein SMTP-Server belegt in der Regel den Port 25.

Ein Benutzer wird zumeist vom Ablauf des SMTP-Protokolls nichts mitbekommen, da dies sein Mailprogramm im Hintergrund für ihn erledigt. Dieses Programm verbindet sich zu einem SMTP-Server, der die Mail zum Empfänger weiterleitet.

6.4 weitere Protokolle

Weitere wichtige Protokolle:

Protokoll	*Erklärung*
Telnet	Telnet ist der Name eines im Internet weit verbreiteten Protokolls. Es wird dazu verwendet, Benutzern den Zugang zu Internetrechnern über die Kommandozeile zu bieten. Aufgrund der fehlenden Verschlüsselung wird es mehr und mehr durch andere Protokolle wie SSH verdrängt.
POP3	POP3 (Post Office Protocol Version 3) ist ein Übertragungsprotokoll, über welches ein Client E-Mails von einem E-Mail-Server abholen kann.
SSH	SSH (Secure shell) ist sowohl ein Programm als auch ein Netzwerkprotokoll, mit dessen Hilfe man sich z.B. über das Internet auf einem entfernten Computer einloggen und dort Programme ausführen kann. Es ermöglicht eine sichere authentifizierte und verschlüsselte Verbindung zwischen zwei Rechnern über ein unsicheres Netzwerk.

Protokoll	*Erklärung*
SNMP	Das Simple Network Management Protocol (SNMP) ist Teil der Internet Protokolle. SNMP hat sich aufgrund seines simplen Aufbaus zum Standard-Protokoll für Netzwerkmanagement, der Verwaltung und Überwachung von Netzelementen (Router, Server, Switches etc.) entwickelt.
RIP	Das Routing Information Protocol (RIP) ist ein Routing-Protokoll. Es dient der dynamischen Erstellung der Routingtabelle von Routern. RIP wird in den Protokollen IP und IPX benutzt.

7 Adressierung

In einem TCP/IP-Rechnernetz verfügen Computer nicht nur über eine IP-Adresse, sie haben auch einen Namen. Dies kommt daher, dass sich Menschen einen Namen besser als eine lange Zahl merken können.

In den folgenden Abschnitten werden die Möglichkeiten erläutert, wie man von einem Hostnamen auf dessen IP schliessen kann.

7.1 DNS

Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Das DNS ist eine verteilte Datenbank, die den Namensraum im Internet verwaltet.

Hauptsächlich wird das DNS zur Umsetzung von Namen in Adressen (forward lookup) benutzt. Dies ist vergleichbar mit einem Telefonbuch, das die Namen der Teilnehmer in ihre Telefonnummer auflöst.

Mit dem DNS ist auch eine umgekehrte Auflösung von IP-Adressen in Namen (reverse lookup) möglich. In Analogie zum Telefonbuch entspricht dies einer Suche nach dem Namen eines Teilnehmers zu einer bekannten Rufnummer.

Um DNS-Namen im Internet bekannt machen zu können, muss der Besitzer die Domain, die diese Namen enthält, registrieren. Durch eine Registrierung wird sichergestellt, dass bestimmte formale Regeln eingehalten werden und dass Domain-Namen weltweit eindeutig sind. Registrierungen sind gebührenpflichtig.

7.2 DHCP

Das DHCP (Dynamic Host Configuration Protocol) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter an Computer in einem Netzwerk (z.B. Internet oder LAN).

Durch DHCP ist die Einbindung eines neuen Computers in ein bestehendes Netzwerk ohne weitere Konfiguration möglich. Es muss lediglich der automatische Bezug der IP-Adresse am Client eingestellt werden. Ohne DHCP ist ein relativ aufwendiges Setup nötig, das neben der IP-Adresse die Eingabe weiterer Parameter wie Subnetmask, Gateway, DNS-Server, WINS-Server usw. verlangt. Per DHCP kann ein DHCP-Server diese Parameter beim Starten eines neuen Rechners (DHCP-Client) automatisch vergeben.

In grossen Netzwerken bietet DHCP den Vorteil, dass bei Topologieänderungen nicht mehr alle betroffenen Workstations per Hand umkonfiguriert werden müssen, sondern die entsprechenden Vorgaben vom Administrator nur einmal in der Konfigurationsdatei des DHCP-Servers gemacht werden müssen. Auch für Rechner mit häufig wechselndem Standort (z.B. Notebooks) entfällt die fehleranfällige Konfiguration - der Rechner wird einfach ans Netzwerk gesteckt und erfragt alle relevanten Parameter vom DHCP-Server.

7.2.1 DHCP-Server

Der DHCP-Server läuft im Hintergrund und tritt nur in Erscheinung, wenn ein Client eine Anfrage an ihn sendet.

Es gibt verschiedene Betriebsmodi eines DHCP-Servers:

1. Manuelle Zuordnung
   Hier wird der MAC-Adresse des Clients innerhalb der Konfigurationsdatei eine IP-Adresse fest zugeordnet.
2. Automatische Zuordnung
   In diesem Modus wird jedem Client eine IP-Adresse fest und auf unbestimmte Zeit zugeordnet. Das Problem an diesem Modus ist, dass die IP-Adresse an die MAC-Adresse des Clients gebunden ist. Sobald aber die Anzahl der Rechner im Netz die Anzahl an freien IP-Adressen überschreitet, können keine weiteren Adressen mehr vergeben werde - der DHCP-Cache muss geleert werden.
3. Dynamische Zuordnung
   Dieses Verfahren gleicht der automatischen Zuordnung, allerdings hat der Server hier in seiner Konfigurationsdatei eine Angabe, wie lange eine bestimmte IP-Adresse an einen Client vermietet werden darf, bevor der Client sich erneut beim Server melden und eine Verlängerung beantragen sollte. Diese Zeit, die vom Administrator bestimmt werden kann, heisst Lease-Zeit.

7.3 ARP

ARP (Address Resolution Protocol) ist ein Netzwerkprotokoll, das die Zuordnung von Internetadressen zu Hardwareadressen (MAC-Adressen) ermöglicht. Obwohl es nicht auf Ethernet- und IP-Protokolle beschränkt ist, wird es fast ausschliesslich im Zusammenhang mit IP-Adressierung auf Ethernet-Netzen verwendet. ARP gehört zur Internetschicht der TCP/IP-Protokollfamilie.

Will ein Rechner in einem Ethernet an einen Rechner im selben Netz ein IP-Paket senden, muss er die Information in einem Ethernetframe verpacken. Jeder Frame enthält eine Ethernetquell- und eine Ethernetzieladresse. Zunächst kennt ein Rechner nur die eigene Adresse, die er in das Feld für die Quelladresse einfügt. Mit Hilfe des ARP-Protokolls kann jeder Rechner die Ethernet-Zieladresse der anderen Rechner ermitteln. ARP wird also verwendet, wenn einem Computer die MAC-Adresse eines anderen Computers nicht bekannt ist und sie somit nicht adressiert werden kann.

7.3.1 ARP-Funktionsweise im Ethernet

Es wird eine ARP-Anforderung (ARP Request-Broadcast) mit der IP-Adresse des anderen Computers gesendet. Bei Broadcasts ist das Erzeugen eines Ethernetframes kein Problem, da als MAC-Zieladresse die Broadcast-Adresse ff-ff-ff-ff-ff-ff (Hexadezimal) verwendet werden kann. Ein Host, der diese IP-Adresse kennt, antwortet mit dem Zurücksenden der passenden MAC-Adresse (ARP-Reply).

Der antwortende Host muss nicht unbedingt der gesuchte Host sein, da jeder teilnehmende Host über einen Cache von MAC- und IP-Adressen verfügt. Dies wird jedoch üblicherweise nicht implementiert, das sonst in einem grösseren Netz eine ARP-Anfrage von vielen Hosts beantwortet würde.

Empfängt ein Host eine ARP-Anforderung oder ARP-Antwort, aktualisiert er seinen so genannten ARP-Cache. Dazu trägt er die Quell-IP-Adresse und Quell-MAC-Adresse bzw. die entsprechenden Zieladressen in die ARP-Tabelle ein. Jeder Eintrag läuft normalerweise nach 20 Minuten aus. Sobald ein Eintrag in der Tabelle genutzt wird, wird dessen Ablaufzeit verlängert.

8 Übertragung

Die folgenden Abschnitte gehen auf die Datenübertragung in den unteren OSI- bzw. TCP/IP-Schichten ein.

Es gibt drei verschiedene Möglichkeiten, wie eine Datenübertragung funktionieren kann:

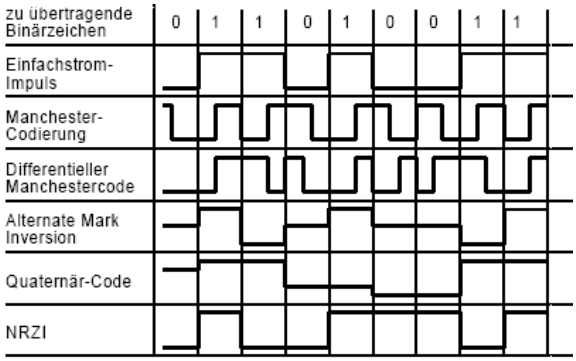
1. Simplex
   Eine Datenübertragung ist nur in eine Richtung möglich. D.h. Sender und Empfänger sind klar definiert, der Sender nimmt niemals die Rolle des Empfängers oder umgekehrt ein.

2. Halbduplex
   Eine Datenübertragung kann in beide Richtungen stattfinden, Sender und Empfänger können ihre Rollen ändern. Die Kommunikation kann aber niemals gleichzeitig in beide Richtungen laufen, sondern nur nacheinander.
3. Vollduplex
   Die Kommunikation kann gleichzeitig in beide Richtungen laufen.

8.1 Codierungsarten

Die rein physikalische Bitübertragung auf der untersten Ebene kann mit unterschiedlichen Codierungen erfolgen. Man unterscheidet dabei zwischen synchronisierenden- und nicht synchronisierenden Codierungen. Hier eine Übersicht der gängigsten:

- Einfachstromimpuls
  Bei einer logischen 0 wird kein Strom übertragen, bei einer logischen 1 wird Strom übertragen.
- Manchestercodierung
  Für eine 0 wird eine senkende Flanke, für eine 1 eine steigende Flanke übertragen. Auf diese Weise erfolgt auch gleich die Synchronisation.
- Differenzielle Manchestercodierung
  Eine 1 wird mit einem Flankenwechsel dargestellt, eine 0 mit zwei bzw. keinem Flankenwechsel. Synchronisierend.



- AMI
  Eine 1 wird mit einer positiven Spannung, eine 0 wird mit einer negativen Spannung dargestellt. Diese Codierung ist nicht wirklich binär, sondern ternär, da drei Zustände verwendet werden.
- Quaternär-Code
  Pro Signalwechsel werden zwei Bits übertragen. Es wird mit 4 Signalpegeln gearbeitet:
  11 = 3, 10 = 2, 01 = 1, 00 = 0
  Diese Codierung ist auch nicht binär!
- NRZI
  Bei einer logischen 1 ändert sich der Signalzustand, bei einer logischen 0 nicht.

8.2 Ethernet II Frame

Ethernet-basierende Netzwerke verwenden heutzutage zur Datenübertragung fast ausschliesslich den Ethernet II Frame. Dieser setzt sich aus den folgenden sieben Teilen zusammen:

Gruppe	Element	Funktion	Bytes
Datenkopf	Präambel	Aufbau der Datenübertragung	7
	Starting Frame Delimiter	Kennzeichnet den Beginn des auswertbaren Teils des Datenpakets	1
	Empfänger	MAC-Adresse des Empfängers, wird vor dem Absenden ermittelt (ARP)	6
	Absender	MAC-Adresse des Absenders	6
	Typfeld	Länge des Datenblocks	2

Gruppe	Element	Funktion	Bytes
Datenblock	Daten	Die eigentlichen Nutzdaten	46-1500
Prüfsumme	CRC	Die Prüfsumme (durch den Cyclic Redundancy Check berechnet)	4

8.3 Kabel

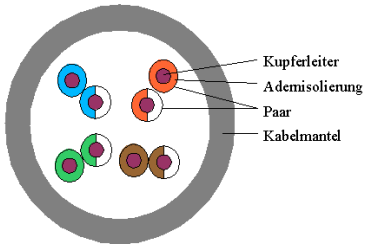
Eine Datenübertragung läuft in den meisten Fällen über Kabel ab, es sei denn, man verwendet die Luft als Übertragungsmedium (WLAN). In den folgenden Abschnitten werden die wichtigsten Kabeltypen kurz erläutert.

8.3.1 twisted pair

Das twisted pair-Kabel (tp) ist die heutzutage wohl am meisten eingesetzte Kabelart für Netzwerke. Es besteht aus 8 Drähten, die jeweils in 2er-Gruppen miteinander verdrillt sind. Je nach Abschirmung können tp-Kabel in verschiedene Kategorien eingeteilt werden. Für die Verwendung in Computernetzen sollten dabei nur noch die Kategorien fünf, sechs und in Zukunft auch sieben eine Rolle spielen. Bei tp-Kabeln wird auch zwischen verschiedenen Bauarten unterschieden, hier eine Übersicht:

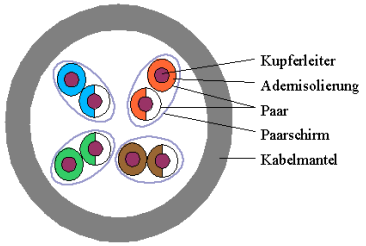
8.3.1.1 UTP

Beim Unshielded Twisted Pair Kabel (UTP) sind weder die verdrillten Paare, noch das Gesamtkabel abgeschirmt. Signale auf den einzelnen Aderpaaren beinflussen sich so gegenseitig, an einen Betrieb im Computernetzwerk ist gar nicht zu denken, dafür können UTP-Kabel sehr einfach verarbeitet werden und sind sehr kostengünstig.



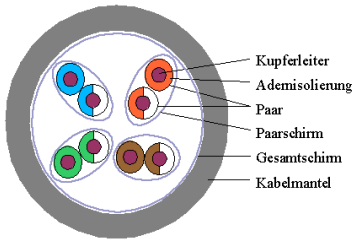
8.3.1.2 STP

Beim Shielded Twisted Pair Kabel (STP) sind die Adernpaare von einer dünnen metallischen Schicht umgeben. Durch die zusätzliche Schirmung wird das Kabel minimal dicker und ist so etwas weniger gut zum Biegen geeignet.



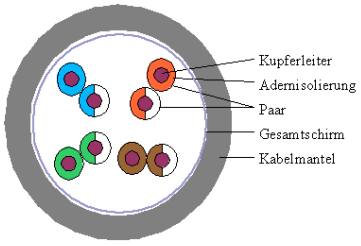
8.3.1.3 S/STP

Ein Screened Shielded Twisted Pair Kabel verfügt wie das normale STP-Kabel auch über eine Schirmung der Adernpaare, dazu kommt noch eine Gesamtschirmung (metallische Schicht) um alle Adernpaare herum.



8.3.1.4 S/UTP

Das Screened Unshielded Twisted Pair Kabel ist gleich aufgebaut wie das UTP-Kabel, also ohne Schirmung der Adernpaare. Dafür verfügt das S/UTP-Kabel über eine Gesamtschirmung, wie es beim S/FTP-Kabel der Fall ist.



Bei den Kategorien eins und zwei verwendet man ungeschirmte Kabel. Für die Kategorien drei bis fünf kann man wahlweise ein

ungeschirmtes oder ein geschirmtes Kabel benutzen. Ab CAT-6 ist ein geschirmtes Kabel aber zwingend vorgeschrieben.

Generell lohnt es sich etwas mehr Geld für ein gut geschirmtes Kabel auszugeben, dies kann einem viel Ärger und so auch zusätzliche Kosten ersparen.

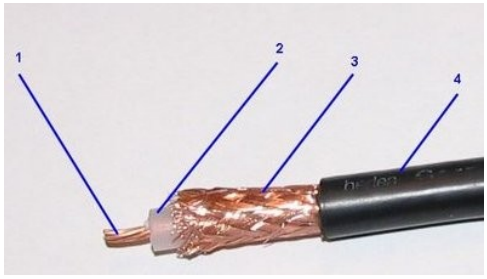
8.3.1.5 Stecker

Für tp-Kabel wird ein sog. RJ45 Stecker verwendet, welcher rein äusserlich dem Telefonstecker RJ11 sehr ähnlich sieht, jedoch etwas breiter ist und acht statt vier Drähte zusammenfasst.

8.3.2 Koaxialkabel

Ein Koaxialkabel besteht aus 4 Schichten:

1. Dem Innenleiter, der sog. „Seele“, über welchen die Spannungspegel übertragen werden, dieser besteht aus Kupfer
2. Einer Isolation, welche aus einem nicht-leitendem Material besteht
3. Einem Aussenleiter, bzw. der Schirmung, welche aus einem Kupfergeflecht besteht
4. und dem Schutzmantel aus einem harten Gummimaterial



Koaxialkabel werden heutzutage für Netzwerke immer weniger eingesetzt, da sie mit einem einzigen Leiter nur halbduplex funktionieren und nur bis zu einer Übertragungsgeschwindigkeit von bis zu 10 Mbit/s standardisiert wurden.

8.3.2.1 Stecker

Koaxialkabel werden mit einem sog. Bayonet Neill Concelman (BNC) Stecker angeschlossen, diese werden eingestöpselt und um 90° gedreht, so entsteht eine relativ starke Verbindung, die rein mechanisch wesentlich stärker ist als eine Verbindung zwischen RJ45-Steckdose und -Stecker. Dafür hat der BNC-Stecker jedoch relativ schlechte elektrische Eigenschaften, was auch dazu beigetragen hat, dass BNC-Kabel heute kaum noch verwendet werden.

8.3.3 Lichtwellenleiter

Beim Lichtwellenleitern (auch Glasfaserkabel) werden nicht elektrische Impulse, sondern optische Signale übertragen. Dieser Kabeltyp ist weniger störungsanfällig als Koax und tp, da optische Signale in einem Glasfaserkabel so gut wie gar nicht beeinflusst werden können. Mit Glasfaserkabel sind enorme Geschwindigkeiten möglich, jedoch sind sie gegenwärtig noch sehr teuer.

9 Geräte

Ein Netzwerk besteht nicht nur aus Protokollen und Kabeln, sondern vor allem aus bestimmter Netzwekhardware, ohne die eine Kommunikation nicht möglich wäre.

9.1 Hub

Ein Hub ist die einfachste Möglichkeit, ein Sternförmiges Netzwerk zu erstellen. Dieser verfügt über mehrere Ports (Steckplätze). Dabei werden alle Endgeräte an den Hub angeschlossen.

Hubs sind primitive Geräte mit keinerlei Intelligenz. Der Hub empfängt ein Datenpaket an einem Port und sendet dieses Packet dann an alle anderen Ports. Jeder Client erhält nun alle Pakete und muss selber (anhand der Ziel-Adresse) entscheiden, ob das Paket angenommen oder ignoriert werden soll.

Ein Hub funktioniert auf dem 1. OSI-Layer, sprich der physischen Bit-Übertragung.

9.2 Switch

Ein Switch hat grundsätzlich dieselbe Aufgabe wie ein Hub, verfügt aber über eine gewisse Intelligenz und wird daher auch als „intelligenter Hub“ bezeichnet. Er arbeitet nicht auf dem 1. OSI-Layer sondern auf dem 2. – der sog. Sicherungsschicht.

Der wichtigste Unterschied zwischen einem Switch und einem Hub ist folgender:

Erhält ein Switch ein Datenpaket durch einen Port, so wird in diesem zuerst nach der Ziel-Adresse gesucht. Kann der Switch die Ziel-Adresse einem Endgerät zuordnen, wird das Datenpaket durch den entsprechenden Port gesendet.

Da Pakete nicht einfach weitergeleitet werden können, sondern vorher noch überprüft werden müssen, treten Verzögerungen auf. Dafür wurde ein spezieller Buffer geschaffen, in welchem sich zu verarbeitende Pakete einreihen können. Auf diese Weise gehen keine Pakete verloren.

Durch den Switch wird den Netzwerkkarten der Clients einiger Aufwand erspart, dafür ist der Switch nicht ganz so schnell wie ein Hub. Die Fehlersuche wird durch einen Switch erschwert, da nicht mehr alle Pakete von allen Ports aus sichtbar sind. Unterm Strich entlastet der Switch ein Netzwerk aber stark und erhöht ausserdem dessen Sicherheit.

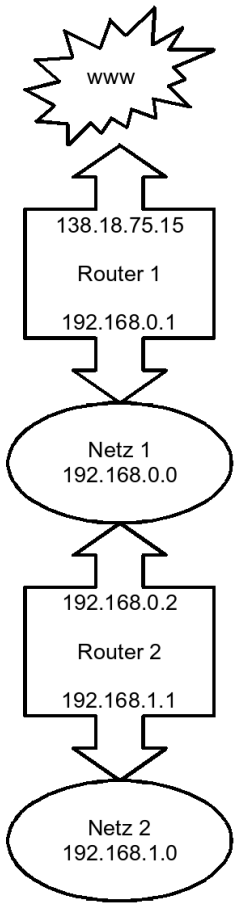
9.3 Repeater

Ein Repeater hat die Aufgabe, ein eingehendes Signal zu regenerieren und zu verstärken. Das Signal wird dabei nicht verändert, es soll nur wieder exakt das Signal erstellt werden, welches der ursprüngliche Sender abgeschickt hat. Dieses Gerät arbeitet rein physikalisch und ist so auf dem ersten OSI-Layer einzuordnen.

Erweiterte Repeater können zusätzlich noch die Bitsequenzen neu synchronisieren.

9.4 Router

Ein Router ist ein relativ komplexes Gerät, welches auf der dritten Schicht des OSI-Layers (der Netzwerk-Schicht) arbeitet. Grob gesagt hat er die Aufgabe, Datenpakete von einem Subnet in ein anderes weiterzuleiten. Dazu greift der Router auf eigens angelegte Routingtabellen zurück und kann so entscheiden, wohin das Paket weitergeleitet werden soll. Es ist auch möglich mehrere mögliche Routingwege zu definieren, so kann die Ausfallsicherheit eines Netzwerks stark erhöht werden.



9.4.1 Der Routing-Vorgang

Es gibt sehr viele unterschiedliche Möglichkeiten des Routings welche je nach Netzgrösse enorm komplex werden können. Dies würde jedoch den Rahmen dieses Dokuments sprengen. Darum hier ein Beispiel für einen einfachen Routingvorgang zwischen zwei privaten Netzen und dem Internet.

In der Abbildung rechts sind zwei Router, zwei private Netze und das Internet dargestellt. Jeder dieser beiden Router hat eine interne Routingtabelle, für dieses Beispiel sehen diese wie folgt aus:

Router 1:

Ziel	*Gateway*	*Hop-Count*
192.168.0.0/24	*	0
192.168.1.0/24	192.168.0.2	1
0.0.0.0/0	*	10

Router 2:

Ziel	*Gateway*	*Hop-Count*
192.168.0.0/24	*	0
192.168.1.0/24	*	0
0.0.0.0/0	192.168.0.1	10

Zu diesem Routingbeispiel sind einige Erklärungen notwendig:

- Erhält ein Router ein Paket durch den Port 1, so ist es klar, dass er dieses Paket durch Port 2 weiterschicken wird, alles andere wäre sinnlos.
- Befindet sich ein Router im selben Netz wie das Ziel, wird als Gateway * angegeben.
- 0.0.0.0 ist die sog. Default-Route. Kann ein Paket keinem bestimmten Netzwerk zugeordnet werden, gehört dieses bei diesem Beispiel wohl ins Internet. Das Paket wird also an den Router weitergesendet, der das Paket dann zum Internet weiterleiten kann.
- Der Hop-Count macht eine Aussage darüber, wie viele Router das Ziel noch entfernt ist. Dieser Wert wird bei jedem Routingvorgang reduziert damit der Sendevorgang auch irgendwann mal abgeschlossen werden kann.
- Im Falle der Default-Route 0.0.0.0 ist die Anzahl der Router nicht bekannt, darum wird ein hoher Wert angegeben (hier 10). Das hat damit zu tun, dass für ein Ziel mehrere Gateways existieren können – alternative Routen sozusagen. Der Router versucht immer, ein Paket an die Route mit dem tiefsten Hop-Count zu senden, da so am wenigsten Zeit verloren geht. Damit aber ein Paket nicht automatisch zum www gesendet wird, wird dieser für die Standardroute möglichst hoch gewählt.

9.5 Gateway

Ein Gateway dient dazu, die Netzwerkkommunikation zwischen zwei verschiedenen Protokollen zu gewährleisten. Dazu wandelt er die Datenpakete so um, dass sie den Anforderungen des Ziel-Protokolls entsprechen. Dieser kann auf jeder beliebigen Schicht im OSI-Modell implementiert werden.

Router werden oft mit Gateways gleichgesetzt. Dies ist aber falsch, da ein Router auf dem dritten OSI-Layer implementiert ist und keine Protokollübersetzung vornehmen kann. Ein Gateway implementiert aber gleichzeitig einen Router und kann so auch zwei Netzwerke verbinden.

9.6 Bridge

Eine Bridge ist ein Gerät, das Datenpakete von einem Netzwerksegment zum anderen überträgt. Die Unterteilung eines Netzwerks in mehrere Segmente wird erforderlich, wenn ein Netzwerk an seine Kapazitätsgrenzen stösst.

9.7 Firewall

Eine Firewall kann auf Soft- oder Hardwareebene implementiert sein. Sie wird in den meisten Fällen dazu eingesetzt, das Internet von einem LAN zu trennen und lässt nur Datenpakete durch, die über einen bestimmten Port gesendet werden. So kann man z.B. den Port 110 (POP3) sperren, damit man vom lokalen Netz aus keine E-Mail-Nachrichten empfangen kann.

9.8 Netzwerkkarte

Damit eine Arbeitsstation oder ein Peripheriegerät an ein Netzwerk angeschlossen werden kann, wird eine Netzwerkkarte benötigt. Diese stellt die Schnittstelle zwischen Endgerät und Netzwerk dar. Diese

Karten werden häufig per PCI (PC) bzw. PCMCIA (Notebook) an die Arbeitsstation angeschlossen, neuere Mainboards enthalten meistens bereits eine Netzwerkkarte.

9.8.1 MAC-Adresse

Eine Netzwerkkarte wird durch ihre MAC-Adresse eindeutig identifiziert. Die MAC-Adresse setzt sich aus 6 Bytes zusammen und wird generell hexadezimal ausgeschrieben. Sie ist auf der Netzwerkkarte meistens aufgedruckt, man kann sie jedoch auch per Software ermitteln.

Die MAC-Adresse besteht aus zwei Teilen, die ersten 3 Bytes identifizieren den Hersteller, die zweiten 3 Bytes identifizieren die Karte innerhalb des Herstellers eindeutig.

MAC-Nummernkreise werden durch IEEE vergeben und sind kostenpflichtig.

10 Referenzen

Für die Erstellung dieses Dokuments haben folgende Bücher als Referenz gedient:

Titel	*Verlag*	*ISBN*
Informatik- und Netzinfrastruktur für ein kleines Unternehmen realisieren (117)	compendio	3-7155-9056-4

Viele Informationen wurden Wikipedia (www.wikipedia.de) und den Schulunterlagen entnommen. Weiter wurde das Dokument „Datenkommunikation und Rechnernetze“ von Rolf Lanz und Adrian Moning verwendet.