# Netzwerktechnik

# 2010

**P.Wenniges**

p.wenniges@medienberufe.de

http://elearning.bildunginmedienberufen.de

# Inhalt



Ein ausführliches Inhaltsverzeichnis finden Sie am Ende des Skriptes.

## *Zweck von Computernetzwerken*

**File-Sharing**

Ein wesentlicher Vorteil eines Netzwerkes ist, dass der gesamte Datenbestand an zentraler Stelle auf einem Server gespeichert werden kann. Dies erhöht die Datensicherheit, weil Backups nur an diesem Rechner durchgeführt werden müssen. Durch die Vergabe von Zugriffsrechten auf die Daten ist auch der Datenschutz gewährleistet. Neben Nutzerdaten können auch die Anwenderprogramme zentral gespeichert und gemeinsam genutzt werden. Der Aufwand für Installation und Update der Software sinkt hierdurch beträchtlich ab.

**Resource-Sharing**

Der sicherlich bekannteste Vorteil von Datennetzen ist in der gemeinsamen Nutzung von Peripheriegeräten zu sehen. So können Sie beispielsweise Drucker oder Scanner ins Netz einbinden und damit allen Benutzern zur Verfügung stellen. Auch der Zugang ins Internet erfolgt üblicherweise an zentraler Stelle.

**Kommunikation**

Datennetze ermöglichen die firmeninterne oder globale Kommunikation, ohne dass ein ständiger Griff zum Telefon notwendig ist. Die hohen Bandbreiten moderner Netze gestatten die Durchführung von Videokonferenzen, die manche Geschäftsreise überflüssig macht.

## *Klassifikation von Netzen*

Datennetze werden hinsichtlich ihrer örtlichen Ausdehnung klassifiziert:

- LAN (local Area Network)
    - Lokale Netze stellen die mit Abstand größte Gruppe der Datennetze dar. Ihre Ausdehnung ist auf ein Gebäude oder Firmengelände beschränkt und beträgt damit etwa einen Kilometer.

- WLAN (Wireless local Area Network) Heute spielen kabellose (wireless) lokale Netze eine immer größere Rolle, weil sie flexibel und kostengünstig realisiert werden können. In vielen Netzen finden Sie eine Kombination aus LAN und WLAN, die über einen WLAN-Router problemlos möglich ist.
- MAN (Metropolitan Area Network)
    - Datennetze innerhalb von Städten werden als MAN (Metropolitan Area Network) bezeichnet. Ein Beispiel hierfür ist ein rechnergestütztes Verkehrsleitsystem innerhalb einer Stadt.
- WAN (Wide Area Network)
    - Unter WAN werden landesweite oder länderübergreifende Netze verstanden, wie sie beispielsweise für die Mobiltelefonie zur Verfügung stehen.
- GAN (Global Area Network)
    - Bei weltumspannenden Netzen wie dem Internet spricht man von GAN.

## Intranet - Internet

Da heutige Netzwerke in vielfältiger Weise miteinander verbunden sind, macht die Trennung in LAN, WAN und GAN oft keinen Sinn mehr. Denken Sie an eine Firma mit mehreren Filialen: Zur Kommunikation können diese über eine Technologie namens VPN (Virtual Private Network) miteinander verbunden werden, obwohl hardwaremäßig die Telefonleitungen genutzt werden müssen, die auch dem Internet zur Verfügung stehen. Wir können bei einem derartigen Netz also nicht mehr von einem LAN sprechen, da die örtliche Ausdehnung zu groß ist. Andererseits handelt es sich jedoch auch nicht um ein WAN oder GAN. Zur Bezeichnung von Netzen, die zur internen Kommunikation in Unternehmen oder Behörden dienen, eignet sich der Begriff Intranet besser. Ihr Merkmal ist, dass für den Zugriff auf das Netz eine Nutzungsberechtigung vorliegen muss. Diese kann hardware oder softwaremäßig realisiert werden: Im ersten Fall können nur bestimmte Rechner auf das Netz zugreifen, im zweiten Fall ist eine Einwahl über Benutzername und Passwort von einem beliebigen Rechner möglich.

Der Begriff **Internet** dient heute als Überbegriff für einen weltweiten Rechnerverbund mit mehreren Hundert Millionen Rechnern. Das Netz lässt sich für unterschiedliche Zwecke, die als **Dienste** bezeichnet werden, nutzen. Bekannte Internetdienste sind das WWW, E-Mail oder die Internettelefonie.

# *Netzwerk - Architekturen*

## Zentralrechnerkonzept (Host-Client-Architektur)

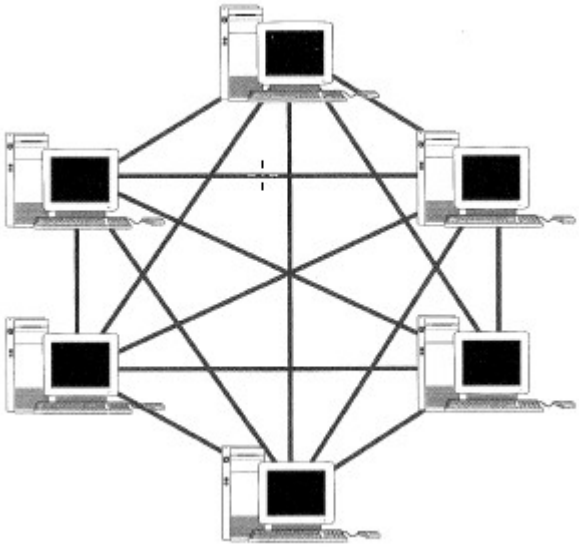
Bereits in den 70er Jahren hielten große Rechenanlagen Einzug in Industrie und Wirtschaft. Zu dieser Zeit war Rechenleistung umso preiswerter, je größer die Rechenanlage war. So entstanden Großrechner, für die spezielle Räume und eigenes Bedienpersonal (Operator) erforderlich waren. Zur Einwahl an einem Großrechner genügt der Einsatz von Terminals, bestehend aus Tastatur und Bildschirm, von denen aus ein interaktiver Dialog mit dem Großrechner möglich ist. Dieser arbeitet die Aufgaben der Teilnehmer nacheinander im Timesharing-Verfahren ab, so dass dadurch eine scheinbare Parallelverarbeitung erzielt wird.

Aufgrund der enormen technologischen Entwicklung von immer kleineren und immer leistungsfähigeren Prozessoren hat die Bedeutung der zentralen Datenverarbeitung stark abgenommen. Großrechner werden heute nur noch installiert, wenn - meist zu Forschungszwecken -

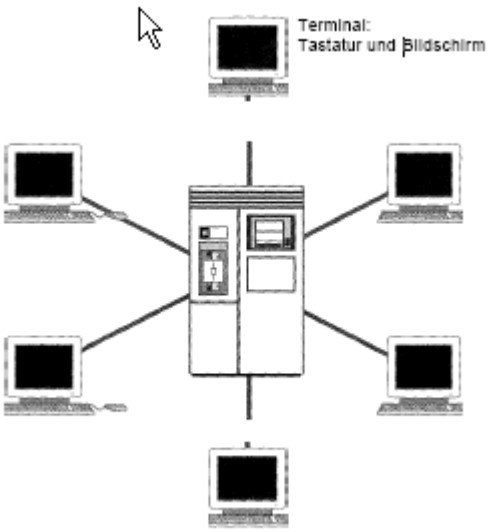
sehr hohe Rechenleistung benötigt wird. Weltweit existieren einige Hundert dieser Super-Computer: die durch Parallelbetrieb von sehr vielen Prozessoren auf enorme Rechenleistungen kommen.

## Peer-to-Peer-Konzept (P2P)

Mit der Entwicklung des PCs (Personal Computer) Anfang der 1980er Jahre wurde für die meisten Aufgaben die Nutzung eines Großrechners überflüssig. Das Verbinden gleichwertiger Computer wird als Peer-to-Peer-Netz bezeichnet, wobei der Begriff "peer" aus dem Englischen stammt und so viel wie "gleichgestellt": "ebenbürtig" bedeutet. Da alle am Netz partizipierenden Rechner also die gleiche Rechenleistung besitzen, dient die Verbindung der Rechner ausschließlich zum Datenaustausch, zur Nutzung gemeinsamer Ressourcen und/oder zur Kommunikation.
Peer-to-Peer-Netze kommen häufig im Privatbereich zum Einsatz, um zwei oder mehr (gleichwertige) Computer miteinander zu verbinden. Danach lassen sich Drucker oder der Internetzugang gemeinsam nutzen. Alle gängigen Betriebssysteme (Windows Xp, Windows Vista, Mac OS X oder Linux) lassen eine Peer-to-Peer-Vernetzung zu. Der Begriff Peer-to-Peer wird aber auch dann gebraucht, wenn Rechner über das Internet verbunden sind und lediglich einen gemeinsamen Dienst zur Verfügung stellen. Bekanntestes Beispiel sind die zahlreichen Musiktauschbörsen wie Gnutella. Das Prinzip dieser (logischen) P2P-Netze besteht darin, dass jeder Rechner seine Dateien zum Download zurVerfügung stellt und sich somit ein großer Verbund an Rechnern ergibt. Bedenken Sie aber, dass die Nutzung derartiger Dienste aus urheberrechtlichen Gründen in Deutschland teilweise illegal ist.



## Client-Server-Konzept




Die meisten lokalen Netze besitzen eine Client-Server-Architektur, bei der es zwei Arten von Rechner gibt: Clients (engl.: Kunde, Auftraggeber) erwarten bestimmte Dienste von Servern (engl.: Diener). Typische Aufgaben eines Servers sind hierbei:

- Fileserver: Server mit gemeinsam oder individuell nutzbaren Daten und gegebenenfalls auch Programmen
- Printserver: Server zur Ansteuerung gemeinsamer Drucker, oft mit RIP zur Rasterung von PostScript-Daten
- Mailserver: Server zur Verwaltung des E-Mail-Verkehrs

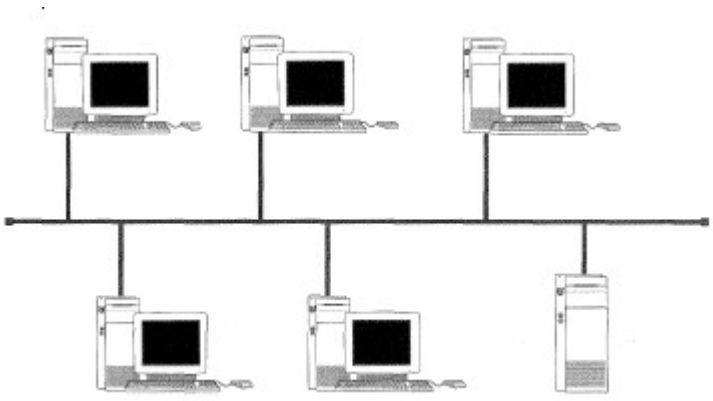
- Webserver: Server mit festem Internetzugang zurVerwaltung von Webseiten - gegebenenfalls mit Datenbankanbindung Neben der Datenverwaltung gehört zu den zentralen Aufgaben eines Servers die Benutzerverwaltung des Netzes.

So können die Zugriffsmöglichkeiten auf Daten oder Programme für jeden Benutzer individuell freigegeben oder gesperrt und damit Datenmissbrauch verhindert werden. Ein weiterer Vorteil eines Servers ist die höhere Datensicherheit, da Datenbackups zentral durchgeführt werden können und der Server über eine USV (Unterbrechungsfreie Stromversorgung) vor einem Stromausfall geschützt werden kann. Beispiele für derzeit aktuelle Server Betriebssysteme sind Windows Server 2003 und 2008, Mac OS X, Novell NetWare und Linux.

## *Netzwerk - Topologien*

Topologie ist die Lehre von der Lage und Anordnung geometrischer Gebilde im Raum. Bezogen auf die Netzwerktechnik wird unterTopologie die Art verstanden, wie die Computer physikalisch miteinander verbunden sind. Beachten Sie, dass heutige Netzwerke stern- oder baumförmig sind. Die anderen Topologien werden der Vollständigkeit halber erwähnt, weil sie in den Anfängen der Netzwerktechnik von großer Bedeutung waren.

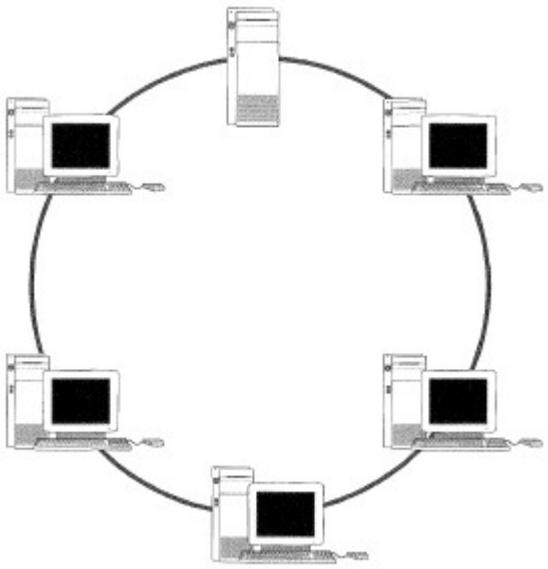
**Bus-Topologie**



| Bus-Topologie |
| --- |
| **Pro**<br>• Einfache Installation<br>• Geringer Verkabelungsaufwand<br>• Geringe Kosten |
| **Contra**<br>• Begrenzte Leitungslänge<br>• Schwierige Fehlersuche<br>• Häufige Datenkollision, da nur ein Kabel<br>• Kompletter Netzausfall bei Unterbrechung des Busses |

Bei der heute veralteten Bus-Topologie wurden alle Rechner einschließlich Server an einer zentralen Leitung - dem Bus - mittels T-Stücken angeschlossen. Damit die Datensignale an den Enden des Busses nicht reflektiert werden, mussten sich dort Abschlusswiderstände (Terminatoren) befinden. Vor allem die beiden letztgenannten Nachteile macht die Bus-Technologie zu unsicher und hat zur Ablösung des Busses durch die Stern-Technologie geführt.

## Ring-Topologie



Die Ring-Topologie wurde vorwiegend in großen Netzen (z. B. WAN) eingesetzt, spielt heute aber fast keine Rolle mehr. Sie verbindet alle Arbeitsstationen und den oder die Server ringförmig miteinander. Die Daten werden dabei vom sendenen Computer in den Ring eingespeist und 'wandern' danach von Rechner zu Rechner. Anhand ihrer Adresse werden sie schließlich vom Zielrechner erkannt.

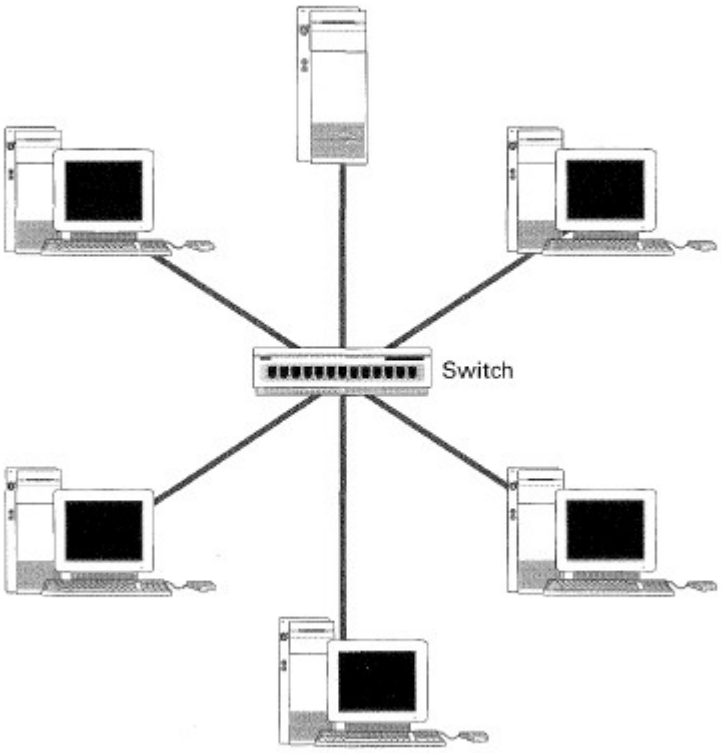
**Ring-Topologie**

**Pro**
- Hohe Ausfallsicherheit (bei Doppelring)
- Keine Datenkollisionen
- Keine Beschränkung der Gesamtlänge

**Contra**
- Hoher Verkabelungsaufwand
- Teure Komponenten
- Keine Kopplung von Telefon- und Rechnerdaten

Der Vorteil des Rings, nämlich die kollisionsfreie Datenübertragung, wird durch den Einsatz von Switches auch im Sternnetz erreicht. Die aufwändige Realisierung von Ringnetzen hat deshalb weitgehend an Bedeutung verloren.

## Stern-Topologie




Ein sternförmiges Netz lässt sich realisieren, indem jeder Computer mit einem zentralen Sternverteiler verbunden wird. Dies hat zunächst einen deutlich höheren Verkabelungaufwand zur Folge als bei der Bus- oder Ringtopologie. Dennoch sind die heutigen Rechnernetze sternförmig, oder, durch Kombination mehrerer Sternnetze, baumförmig aufgebaut. Warum konnten sich Sternnetze durchsetzen? Die Hauptursache für den durchschlagenden Erfolg dieser Technologie ist, dass der zentrale Sternpunkt heute ausschließlich durch so genannte Switches (engl.: Schalter) gebildet wird. Im Unterschied zu den früher verwendeten Hubs (engl.: Speicherrad) vermeidet ein Switch Datenkollisionen, indem er zwischen Sender und Empfänger intern eine Verbindung schaltet, die eine kollisionsfreie Datenübertragung ermöglicht.

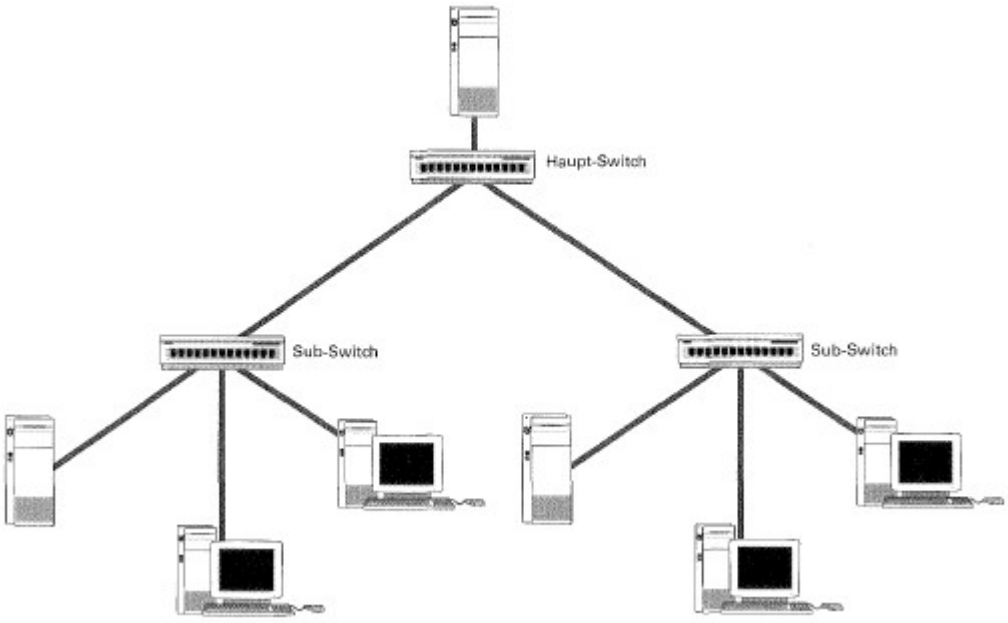
**Stern-Topologie**

**Pro**
- Keine Datenkollisionen durch Einsatz von Switches
- Netzerweiterung problemlos möglich
- Kombination mit WLAN möglich
- Kostengünstige Komponenten

**Contra**
- Netzausfall bei Ausfall des Switches
- Aufwändige Verkabelung
- Begrenzte Leitungslänge

Damit entfällt das Argument, dass Sternnetze bei hoher Belastung keine gute Performance besitzen. Auch der bisherige Nachteil des höheren Verkabelungsaufwandes kann heute umgangen werden, indem sich Computer überWLAN auch kabellos ins Netz integrieren lassen. Die Nutzung wird hierdurch flexibel, da der Zugriff nicht mehr ortsgebunden ist - denken Sie an Bahnhöfe oder Flughäfen.

## Baum-Topologie

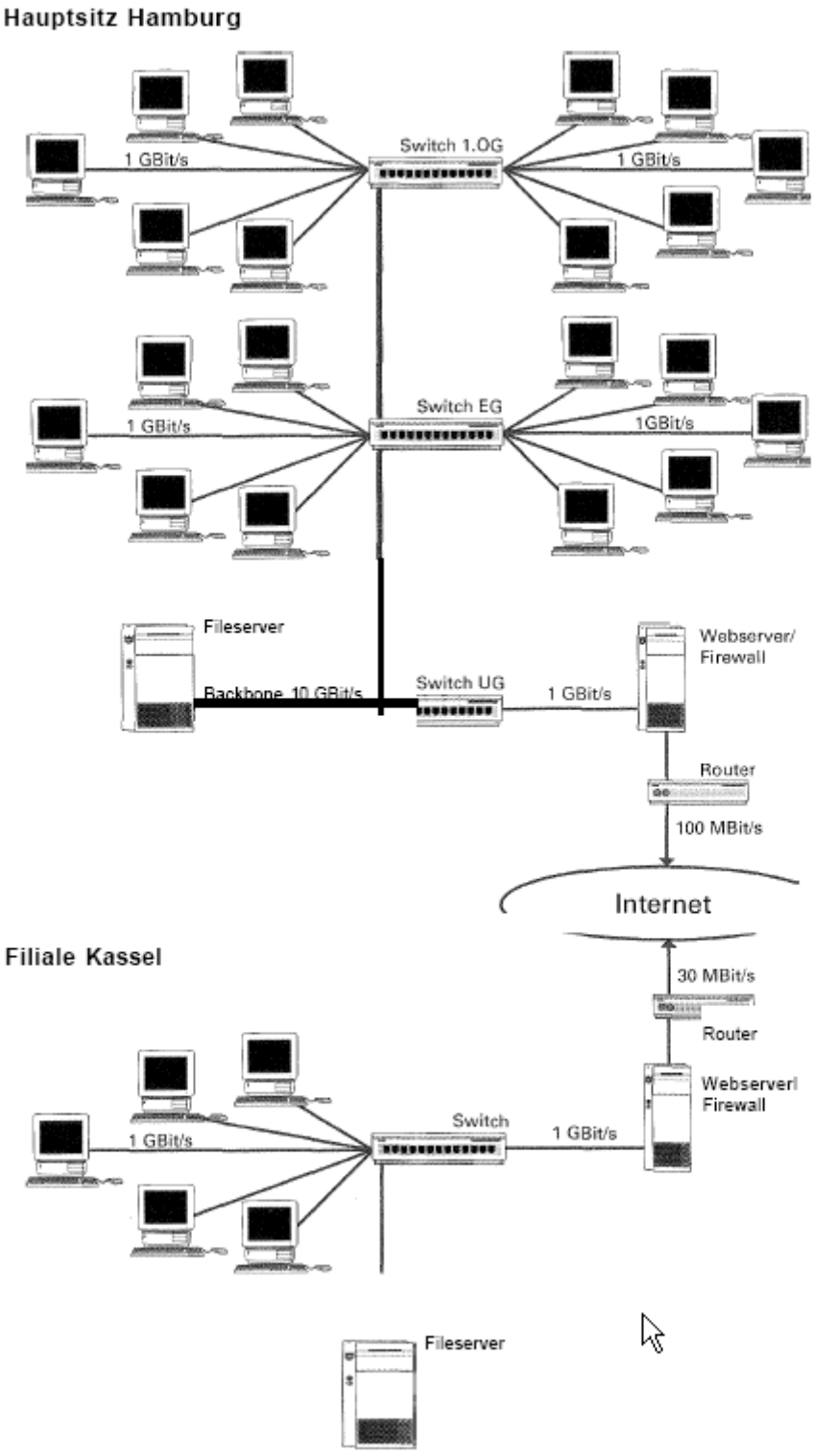



In großen Netzen wäre es unsinnig, alle Computer an einen einzigen Sternpunkt anzuschließen. Fällt dieser aus, ist das gesamte Netz lahmgelegt. Außerdem ist die Leitungslänge zwischen Computer und Switch begrenzt. In großen Netzen bietet sich deshalb die Realisierung einer Baumstruktur an: Die "Wurzel" wird durch ein oder mehrere Haupt-Switches gebildet, an die, z. B. für jedes Stockwerk, Unter-Switches angeschlossen werden. Selbst wenn ein Haupt-Switch ausfällt, bleiben die Teilnetze weiterhin nutzbar.
Neben der Ausfallsicherheit ergibt sich der Vorteil, dass Sie die Netzwerkkomponenten an die zu erwartende Datenmenge anpassen können. So kann die schnelle, aber teure Glasfaserverkabelung auf die Hauptäste beschränkt bleiben, während für die Teilnetze die günstige Kupfertechnologie zum Einsatz kommt.

## Physikalische und logische Topologie

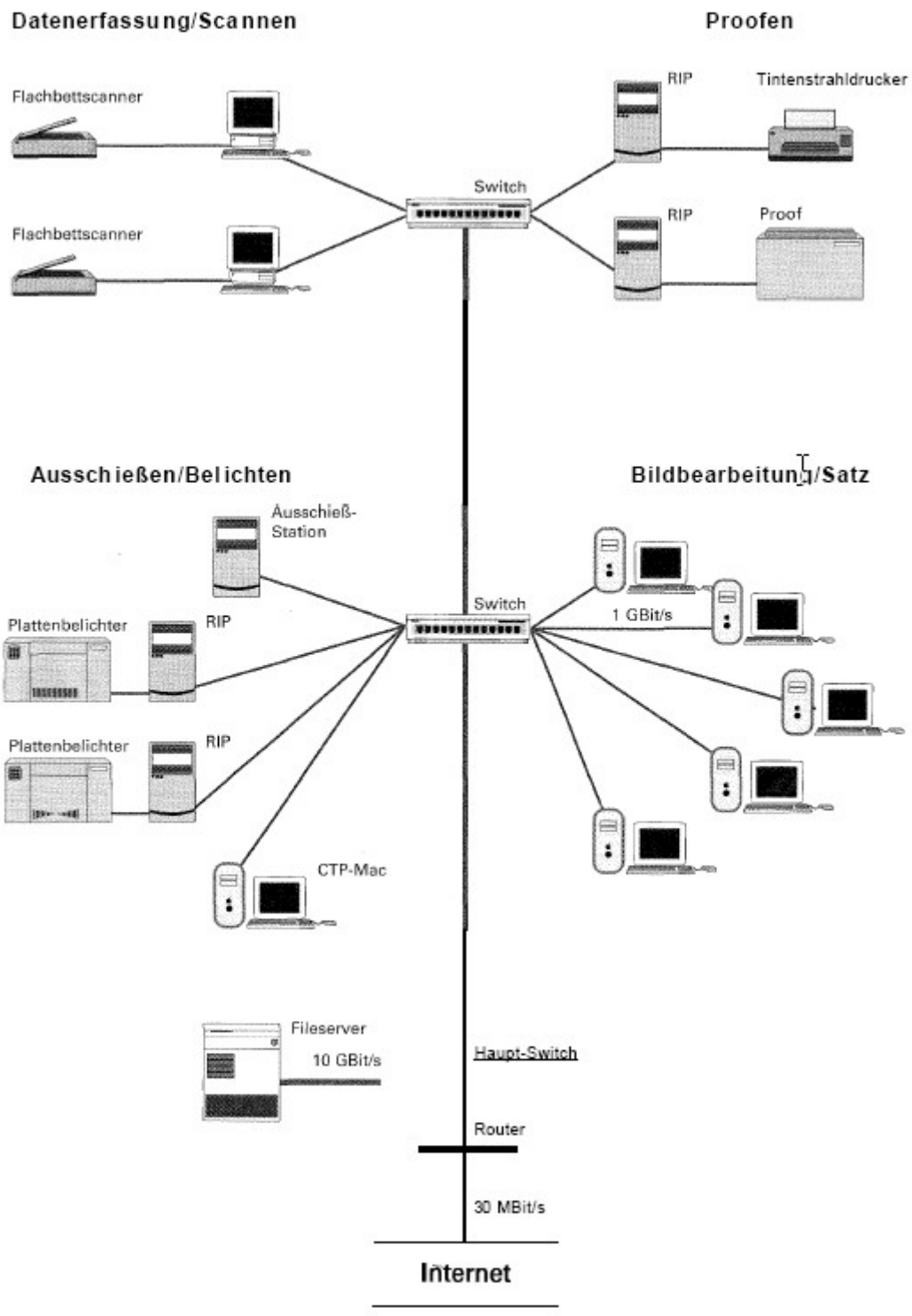
Beachten Sie den wichtigen Unterschied zwischen physikalischer und logischer Topologie. Im ersten Fall handelt es sich um die in den vorherigen Abschnitten beschriebene Art der (hardwaremäßigen) Verbindung der Rechner. Unter der logischen Topologie wird verstanden, wie das Netz durch das Betriebssystem administriert wird. Über das **Zugriffsverfahren** wird festgelegt, ob das Netz logisch als Bus betrieben wird und alle Rechner gleichzeitig Daten senden dürfen. Alternativ kann aber auch ein Senderecht vergeben werden, so dass ein logischer Ring entsteht. Die physikalische und logische Topologie eines Netzwerks müssen nicht miteinander übereinstimmen: So kann beispielsweise ein Netz physikalisch sternförmig miteinander verbunden sein und dennoch logisch als Ring betrieben werden. Die einzelnen Rechner erhalten dann vom Betriebssystem nacheinander ein Senderecht, als ob sie tatsächlich im Ring verbunden wären.

**Netzstruktur einer Internetagentur**




Beispiel für die Netzstruktur einer Internetagentur mit Hauptsitz und Filialen.

**Netzstruktur eines Reprobetriebs**



# *Netzwerkgeräte*

Ob Netzwerkkabel, Modem oder Router: ohne Netzwerkgeräte läuft's nicht. Hier werden die verschiedenen Netzwerkgeräte vorgestellt.

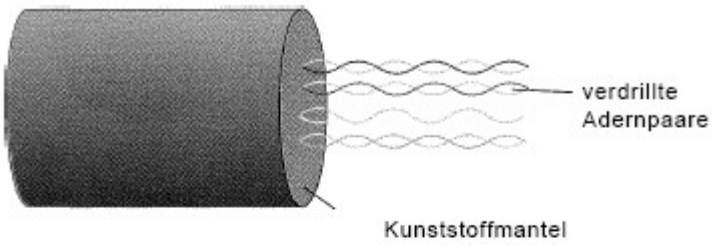
## Netzwerkverbindungen mittels Kabel

Die Auswahl des richtigen Kabels hängt von der gewünschten Übertragungsrate, der Netztopologie und nicht zuletzt von den Kosten des Kabels ab. Für drahtgebundene Verbindungen kommen hierbei zwei Medien in Frage: Twisted-Pair-Kabel oder Lichtwellenleiter.

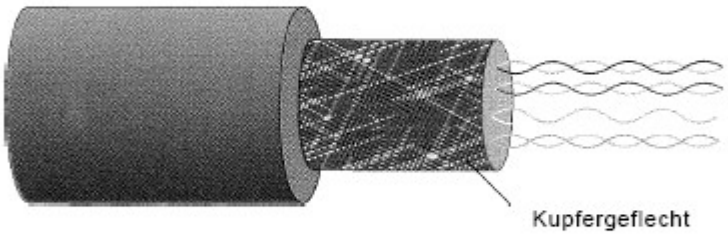
### Twisted Pair

Das Twisted-Pair-Kabel, das in den USA auch als Telefonkabel verwendet wird, besteht im einfachsten Fall aus verdrillten Kupferleiter-Doppeladern (UTP). Um äußere Störeinflüsse zu reduzieren, werden Twisted-Pair-Kabel mit einer metallischen Abschirmung um die Adernpaare (S/UTP) sowie mit zusätzlicher Aluminiumfolie um jedes Adernpaar (S/FTP) angeboten. Die Verkabelung mit Twisted Pair wird bei sternförmig vernetztem Ethernet eingesetzt. Die Verbindung von TwistedPair-Kabel und Switch erfolgt mittels RJ-45-Stecker bzw. -Buchse, ebenso die Verbindung des Kabels mit der Netzwerkkarte des Computers.

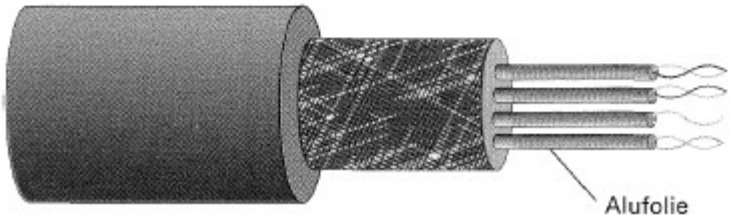
UTP-Kabel (Unshielded Twisted Pair)




S/UTP-Kabel (Screened Unshielded Twisted Pair)




S/FTP-Kabel (Screened Foiled Twisted Pair)



Der große Vorteil einer Twisted-Pair Verkabelung liegt in den niedrigen Kosten und der einfachen Installation. Die zulässige Kabellänge sowie die maximale Taktung des Netzes muss bei der Auswahl des Kabels beachtet werden. Twisted-Pair-Kabel werden hierzu in Kategorien von 1 bis 7 eingeteilt:

| Kategorie | max. Takt | Einsatzgebiet |
|---|---|---|
| CAT 1 | k.A. | Telefon |
| CAT 2 | 1 MHz | Telefon (ISDN) |
| CAT 3 | 16 MHz | 10-MBit-Ethernet |
| CAT 4 | 20 MHz | unbedeutend |
| CAT 5 | 100 MHz | 100-MBit-Ethernet |
| CAT 5e | 100 MHz | 1000-MBit-Ethernet |
| CAT 6 | 250 MHz | divers, z. B. ATM-Netze |
| CAT 7 | 600 MHz | 10-GBit-Ethernet |

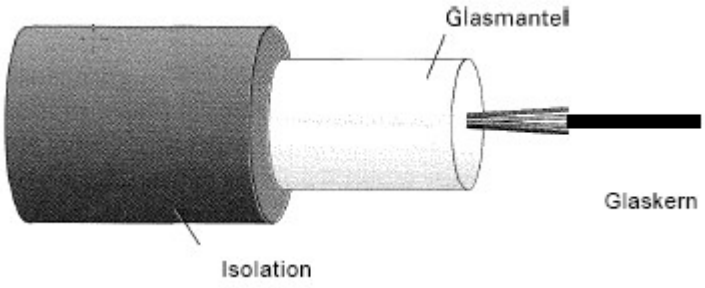
Für die heute üblichen 100-MBit/s- oder 1-GBit/s-Netze werden Kabel der Kategorie 5 bzw. 5e verwendet. Beachten Sie weiterhin, dass zur direkten Verbindung zweier Rechner (ohne Switch) ein gekreuztes (crossover) Twisted-PairKabel benutzt werden muss.

**Koaxialkabel**

Koaxialkabel kennen Sie vielleicht vom Antennenanschluss Ihres Fernsehers. Es besteht aus einer inneren Kupferader, die von einer Isolationsschicht, gefolgt von einem Kupferdrahtnetz, umgeben ist. Im Bereich der Netzwerktechnik haben Koaxialkabel keine Bedeutung mehr.

**Lichtwellenleiter**

Licht bewegt sich mit Lichtgeschwindigkeit (ca. 300.000 km/s) und damit deutlich schneller als Elektronen. Lichtwellenleiter (LWL), umgangssprachlich als Glasfaser bezeichnet, ermöglichen Übertragungsraten von derzeit 10 GBit/s.




LWL bestehen aus etwa 0,05 mm dünnen Glasfasern, die von einem äußeren Glasmantel mit einem anderen Brechungsindex umhüllt sind. Dadurch werden die Lichtimpulse am äußeren Mantel vollständig reflektiert und bewegen sich entlang der inneren Fasern. Abgesehen von der hohen Übertragungsrate bieten Lichtwellenleiter den Vorteil, dass sie völlig unempfindlich gegenüber elektrischen oder elektromagnetischen Störeinflüssen sind. Ein weiteres Argument für die Glasfasertechnologie betrifft die Abhörsicherheit: Das Anzapfen eines Lichtwellenleiters ist nach derzeitigem Stand der Technik nicht möglich. Den obigen Vorteilen stehen im Wesentlichen die höheren Kosten für Installation und Komponenten gegenüber. Da mittlerweile sogar 10-GBit-Netzwerke mit Kupferkabel betrieben werden können, müssen Sie sich bei der Planung die Frage stellen, ob die Investition in die teurere LWL-Technologie gerechtfertigt ist.

**WLAN**

Kommunikation und Information an jedem Ort und zu jeder Zeit - dies scheint der Trend des 21. Jahrhunderts zu sein. Was mit einer explosionsartigen Verbreitung der Mobiltelefone begonnen hat, setzt sich jetzt mit der sprunghaften Zunahme an mobilen Computern (Laptop, Notebook, Palmtop, ... ) fort. Da liegt der Wunsch nahe, auch mit diesen mobilen Geräten im Internet surfen, E-Mails empfangen oder einfach nur einen Abgleich seiner Daten mit dem Desktop-PC vornehmen zu können. Mit WLAN kein Problem!

**Standards**

| IEEE | Frequenz | Max. Datenrate |
|---|---|---|
| 802.11 | 2,4 GHz | 1 bis 2 MBit/s |
| 802.11a | 5 GHz | 54 MBit/s |
| 802.11b | 2,4 GHz | 11 MBit/s |
| 802.11g | 2,4 GHz | 54 MBit/s |
| 802.11n | 2,4/5 GHz | 300 MBit/s |

Wie der Name sagt, ist WLAN für "lokale" Netze vorgesehen - die Reichweiten der Sender betragen in Gebäuden bis zu 50, im Freien bis zu 500 Meter. In der Tabelle sind die wichtigsten Standards des "Institute of Electrical and Electronics Engineers': kurz IEEE, zusammengestellt: Zurzeit erfolgt die Umstellung auf die neue Spezifikation 802.11 n, die eine deutlich höhere Datenrate als die bisherige Grenze von 54 MBit/s ermöglicht.

Beachten Sie jedoch, dass die genannten Datenraten Bruttoangaben sind. Die tatsächlich übertragbare (Netto-) Datenrate beträgt etwa die Hälfte. Hinzu kommt, dass die Datenrate weiter sinkt, wenn mehrere Geräte am WLAN partizipieren. DieTrägerfrequenzen von 2,4 bzw. 5 GHz liegen zwischen den Frequenzen der Mobiltelefonie und infrarotem Licht. Natürlich stellt sich hierbei die Frage, inwieweit eine derartige Strahlung gesundheitsschädlich sein kann oder sogar ist. Allerdings wird die gepulste Strahlung der schnurlosen DECT-Telefone als weitaus riskanter eingeschätzt.

## *Netzwerkkabel*

Netzwerkkabel gibt es in verschiedenen Bauweisen. Sie werden in Bus-, Stern- oder Ring-Topologien verwendet.

- **10Base2**: Ethernet mit 10 MBit/s auf einem dünnen Coax-Kabel (RG-58), auch Cheapernet genannt. Beide Enden des Kabels müssen mit einem Abschlusswiderstand von 50 Ohm terminiert sein. Bei 10Base2 befinden sich AUI* und MAU* auf der Netzwerkkarte, die über ein T-Stück an das Kabel angeschlossen wird.
  Ein Segment darf maximal 185 Meter lang sein, maximal sind vier Repeater, also fünf Segmente möglich.
- **10Base5**: Ethernet mit 10 MBit/s auf dickem Coax-Kabel (RG-8A/U, Yellow Cable), auch Thick Ethernet genannt. AUI und MAU sind getrennt ausgeführt.
- **10BaseFL**: Ethernet mit 10 MBit/s über eine sternförmige Glasfaserverkabelung. Die maximale Ausdehnung beträgt bei Multimode-Faser und einer Wellenlänge von 850 nm zwei Kilometer und bei einer Wellenlänge von 1300 nm fünf Kilometer, mit Monomode-Faser bei einer Wellenlänge von 1300 nm schafft man sogar bis zu 20 Kilometer.
- **10BaseT**: Ethernet mit 10 MBit/s über eine sternförmige Twisted-Pair-Verkabelung. Die Stationen sind jeweils über ein eigenes Kabel von maximal 100 Meter Länge an einen zentralen Verteiler (Hub oder Switch) angeschlossen.
- **100BaseFx**: Ethernet mit 100 MBit/s (Fast Ethernet) über eine sternförmige Glasfaserverkabelung (Multi- oder Monomode-Faser). Die maximale Kabellänge zwischen Station und zentralem Verteiler beträgt 400 Meter.

Zwischen zwei Verteilern oder Medien-Konvertern lassen sich mit Multimode-Faser bis zu 2 Kilometer, mit Monomode-Faser zwischen 20 und 40 Kilometer überbrücken (jeweils bei einer Wellenlänge von 1300 nm).

- **100BaseSx**: entspricht 100BaseFx mit einer Wellenlänge von 850 nm. Die maximale Kabellänge beträgt 300 Meter. Dieser Standard entstand im Gefolge der Definition von 1000BaseSx: Die geringere Wellenlänge wurde dort erstmals eingeführt, da die Komponenten für diese Technik weit günstiger sind als bei den klassischen Ethernet-Standards über Glasfaser und einer Wellenlänge von 1300 nm.
- **100BaseTx**: Ethernet mit 100 MBit/s (Fast Ethernet) über eine sternförmige Twisted-Pair-Verkabelung mit vier Adern. Die maximale Kabellänge zwischen Station und zentralem Verteiler beträgt 100 Meter.
- **1000BaseSX**: Ethernet mit 1000 MBit/s (Gigabit Ethernet) über eine Multimode-Glasfaser bei einer Wellenlänge von 850 nm. Die maximale Kabellänge liegt je nach Fasertyp und -qualität zwischen 220 und 550 Metern.
- **1000BaseLX**: Ethernet mit 1000 MBit/s (Gigabit Ethernet) über eine Multi- oder Monomode-Glasfaser bei einer Wellenlänge von 1270 nm. Die maximale Kabellänge liegt je nach Fasertyp und -qualität zwischen 550 und 5000 Metern.
- **1000BaseT**: Gigabit-Ethernet mit 1000 MBit/s über eine sternförmige Twisted-Pair-Verkabelung mit vier Adern. Die maximale Kabellänge zwischen Station und zentralem Verteiler beträgt 100 Meter.

## Tabellarische Übersicht

**Ethernet 10 MBit/s**

| Art | Modus | Medium | max. Länge |
|---|---|---|---|
| 10Base-2 | Halb-Duplex | Koax (BNC) | 185 m |
| 10Base-5 | Halb-Duplex | Koax (Yellow) | 250 m |
| 10Base-T | Halb-Duplex | Twisted Pair | 100 m |
| 10Base-FL | Halb-Duplex | Multimode LWL | 2000 m |

**Fast-Ethernet 100 MBit/s**

| Art | Modus | Medium | max. Länge |
|---|---|---|---|
| 100Base-TX | Halb-Duplex | Twisted Pair | 100 m |
| 100Base-TX | Voll-Duplex | Twisted Pair | 100 m |
| 100Base-FX | Halb-Duplex | Multimode LWL | 400 m |
| 100Base-FX | Voll-Duplex | Multimode LWL | 2000 m |

**Gigabit-Ethernet 1000 MBit/s**

| Art | Modus | Medium | max. Länge |
|---|---|---|---|
| 1000Base-TX | Voll-Duplex | Twisted Pair (8 Adern) | 100 m |
| 1000Base-SX | Voll-Duplex | Multimode LWL | 500 m |
| 1000Base-LX | Voll-Duplex | Monomode LWL | 10 km |
| 1000Base-ZX | Voll-Duplex | Monomode LWL | 70 km |

**10 Gigabit-Ethernet 10 GBit/s**

| Art | Modus | Medium | max. Länge |
|---|---|---|---|
| 10GBase-LX4 | LAN Voll-Duplex | Multimode LWL 1310 nm | 300 m |
| 10GBase-LX4 | LAN Voll-Duplex | Monomode LWL 1310 nm | 2-10 km |
| 10GBase-SR | LAN Voll-Duplex | Multimode LWL 850 nm | 300 m |
| 10GBase-LR | LAN Voll-Duplex | Monomode LWL 1310 nm | 10 km |
| 10GBase-ER | LAN Voll-Duplex | Monomode LWL 1550 nm | 40 km |
| 10GBase-SW | WAN Voll-Duplex | Multimode LWL 850 nm | 300 m |
| 10GBase-LW | WAN Voll-Duplex | Monomode LWL 1310 nm | 10 km |
| 10GBase-LW4 | WAN Voll-Duplex | Monomode LWL 1310 nm | 40 km |
| 10GBase-EW | WAN Voll-Duplex | Monomode LWL 1550 nm | 40 km |

## WLAN-Adapter und Access-Point

Damit ein Computer am Funknetz partizipieren kann, benötigt er einen WLAN-Apapter. In heutigen mobilen Computern sind diese bereits integriert, in Desktop-PCs genügt das Einstecken eines WLAN-USB-Sticks. Mehrere Computer mitWLAN-Adapter können ohne weitere Hardware zu einem Ad-hoc-Netz zusammengeschlossen werden. Meistens kommt jedoch eine als Access-Point bezeichnete Vermittlungsstation zum Einsatz: Diese bietet den Vorteil, dass sie gleichzeitig eine Schnittstelle zum verkabelten LAN bereitstellt. Somit können mobile Computer in bestehende kabelgebundene Netze eingebunden werden.

Bei heutigen WLAN-Access-Points handelt es sich oft um Gerätekombinationen, die zusätzlich einen DSL-Router und eine Telefonanlage enthalten. Mehrere Access-Points können ihrerseits zu Funkzellennetzwerken (wireless bridges) verbunden werden, innerhalb derer sich der Nutzer frei bewegen kann. DerWechsel von einem AccessPoint zum nächsten erfolgt hierbei - wie beim Mobiltelefon - automatisch. DieTechnik ermöglicht also eine flächendeckende Funkvernetzung. In vielen öffentlichen Einrichtungen wie z. B. auf Flughäfen, in Bahnhöfen oder in Zügen wird dieser Service mittlerweile angeboten.

## Bluetooth

Auch bei Bluetooth handelt es sich um eine Funkverbindung, deren Reichweite vor allem für den Nahbereich von 10 bis 30 m gedacht ist und die vor allem zur kabellosen Anbindung von Peripheriegeräten (Drucker, Tastatur, Maus) an den PC dient. Sie können Bluetooth auch dazu nutzen, um Daten zwischen Mobiltelefonen auszutauschen.

Die Nutzung von Bluetooth zur Vernetzung von PCs ist zwar möglich, empfiehlt sich aber nicht, weil die Übertragungsrate mit maximal 2,1 MBit/s hinter den Möglichkeiten von WLAN weit zurückbleibt. Zum Anschluss Bluetooth-fähiger Geräte an einen PC benötigt dieser lediglich einen USB-Adpater. Auch für Bluetooth stehen Access-Points zur Verfügung, die beispielsweise einen ISDN- oder DSL-Zugang ins Internet ermöglichen. Problematisch ist, dass Bluetooth dasselbe Frequenzband von 2.400 bis 2.438 GHz verwendet und somit Störungen mit WLAN-Geräten nicht auszuschließen sind. Sie sollten sich also für die eine oder andere Technik entscheiden.

## Netzwerkkarte

Zur Einbindung eines Rechners in ein Netzwerk benötigt dieser eine Adapterkarte mit einem Netzwerkcontroller, der im Wesentlichen zwei Funktionen erfüllen muss:

- Physikalischer Netzzugang (Schicht 1 des OSI-Referenzmodells):
    - Twisted Pair, Glasfaserkabel oder drahtlose Funkverbindung
- Regelung des Netzzugriffsverfahrens (Schicht 2 des OSI-Referenzmodells):
    - CSMA/CD (Ethernet) oder CSMA/CA (WLAN)

Die Höhere Ebenen des Referenzmodells werden nicht softwaremäßig bearbeitet. DieseTreibersoftware ist der Karte beigefügt oder bereits Bestandteil des Betriebssystems.

## MAC-Adresse

Zur Identifikation besitzt jede Netzwerkkarte eine weltweit einmalige Netzwerkadresse. Diese wird als MAC-Adresse (Media Access Control) bezeichnet und besteht aus einer 48 Bit langen Zahl, gegliedert in sechs Blöcke. Sie wird auch Burnt-in-Adresse genannt, weil sie in einen eigenen ROM-Speicher des Netzwerkcontrollers "eingebrannt" ist.

### Ethernetkarten

Da es sich bei lokalen Netzen in der Regel um ein Ethernet handelt, werden Netzwerkkarten auch als Ethernetkarten oder -adapter bezeichnet. Noch immer weit verbreitet ist das Fast Ethernet mit einer Übertragungsrate von 100 MBit/s, so dass Sie hierfür 100-MBit-Ethernet-Karten benötigen. Die Ablösung durch das Gigabit-Ethernet ist in vollem Gange, die zugehörigen Gigabit-Ethernet-Adapter sind in ähnlicher Preisklasse erhältlich und stehen wahlweise fürTwisted Pair oder Glasfaserkabel zur Verfügung. GigabitKarten sind abwärtskompatibel, d. h., sie können auch in 100-MBit-Ethernet eingesetzt werden.

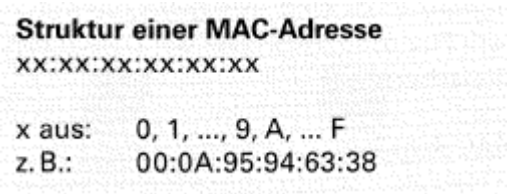
Für Hochgeschwindigkeitsnetze gibt es 10-GBit-Ethernet-Karten, die allerdings sehr teuer sind und allenfalls im Backbone-Bereich zur Verbindung von Servern oder mit Haupt-Switches in Frage kommen. Zur Realisierung eines WLAN-Funknetzes müssen WLAN-Adapterkarten oder ein WLAN-USB-Stick verwendet werden. Diese unterscheiden sich äußerlich dadurch, dass sie statt Anschlussbuchsen eine kleine Antenne besitzen.

## MAC-Adressierung

Ein entscheidendes Kriterium für den Betrieb eines Netzes ist, dass alle beteiligten Komponenten eindeutig identifizierbar sind - vergleichbar mit dem Fingerabdruck oder der DNA eines Menschen.

### MAC-Adresse

In Netzwerken wird diese Identifikation über die MAC-Adresse gewährleistet, wobei MAC für "Media Access Control" steht und nichts mit dem gleichnamigen Betriebssystem zu tun hat. Die MAC-Adresse befindet sich -fest einprogrammiert- auf der Netzwerkkarte und besteht aus einer 48-Bit-Zahl, gegliedert in sechs Blöcke mit je einem Byte (6 x 8 Bit = 48 Bit). Sie wird üblicherweise in hexadezimaler Schreibweise notiert, wobei eine Hexadezimalzahl bekanntlich vier Bit repräsentiert:




Mit 48 Bit lassen sich $2^{48}$ (~281 Billionen) unterschiedliche Zahlen speichern, so dass der Vorrat an weltweit einmalig vorkommenden Zahlen so schnell nicht erschöpft sein wird.

## Repeater

Die maximal zulässige Kabellänge ist begrenzt und vom Kabeltyp abhängig. Werden längere Kabelstrecken benötigt, ist die Verstärkung des Signals erforderlich. Repeater sind Zwischenverstärker zur Verbindung von Kabelsegmenten desselben Kabel- und Netzwerktyps. Die Verbindung erfolgt auf Schicht 1 des OSI-Referenzmodells. Müssen mehrere Segmente miteinander verbunden werden, dann können MultiportRepeater eingesetzt werden.

## Hub

Hubs (ausgesprochen: arbeiten, wie Repeater, auf der Schicht 1 des OSI-Referenzmodells, haben die gleiche Funktionalität, bieten aber die Vervielfachung des Signals und dienen daher als Sternverteiler im Computernetzwerk. Sie werden heute kaum noch gebraucht und zunehmend durch Switches ersetzt.

> Bei Einsatz eines Hubs im Netz wird durch die Verkabelung im physikalischem Sinne eine Stern-Topologie realisiert. Der logische Aufbau ähnelt dem einer Bus-Topologie, weil jede gesendete Information alle Teilnehmer erreicht. Alle Teilnehmer in einem Netzwerk, die an einen Hub angeschlossen sind, befinden sich in derselben Kollisionsdomäne. Durch einen Hub wird die Ausfallsicherheit gegenüber einem Bus-Netz erhöht. Die Störung eines Kabels legt hier nicht das gesamte Netz lahm, sondern beeinträchtigt lediglich einen einzelnen Teilnehmer, der dann nicht mehr erreichbar ist. Außerdem ist der Fehler einfacher zu lokalisieren.
>
> *(Quelle: Wikipedia.de, 09.2009)*

## Switch

Switches sind Komponenten, die für sternförmige Netze konzipiert wurden. Sie besitzen 8, 16 oder mehr Ausgänge {Ports} mit RJ-45-Buchsen zum Anschluss der Rechner. Ein Switch {eng!.: Schalter} verbindet die Computer des Netzes also an einer zentralen Stelle und dient zusätzlich als Signalverstärker.

Ein Switch besitzt also gleichzeitig auch die Funktion eines Repeaters. Darüber hinaus ist ein Switch in der Lage, die eintreffenden Datenpakete (Ethernet-Frames) zu analysieren und eine Punkt-zu-Punkt-Verbindung zwischen Sender und Empfänger herzustellen. Auf diese Weise werden Datenkollisionen ausgeschlossen.

Switches arbeiten aus diesem Grund mindestens auf Schicht 2 des OSI-Modells (Sicherungsschicht). Mittlerweile gibt es auch Switches, die eine weitere Schicht des OSI Modells, Schicht 3, integrieren. Damit übernimmt das Switch gleichzeitig die Funktion eines Routers, ist also in der Lage, die Pakete auf "intelligente" Weise im Netz weiterzuleiten.


## Bridge

Eine Bridge (eng!.: Brücke) besitzt starke Ähnlichkeit mit einem Switch, besitzt aber weniger Ports und ist vor allem zur kollisionsfreien Verbindung zweierTeilnetze gedacht. Wie Switches arbeitet die Bridge auf Schicht 2 des OSI-Modells. Mit Hilfe von Bridges können Netze auf mehrere Kilometer Länge ausgebaut und damit beispielsweise mehrere Firmengebäude verbunden werden. Die Verstärkungsfunktion des Repeaters ist in der Bridge enthalten.

## Router

Ein Router (route, eng!.: Strecke) kümmert sich um die Verbindung von Netzwerken auf der Vermittlungsebene (Schicht 3) des OSI-Referenzmodells. Router sind als eigenständige Geräte erhältlich - alternativ kann auch ein Computer zum "Routing" genutzt werden.

Spezielle Formen wie ISDNoder DSL-Router übernehmen zusätzlich die Anbindung an das Telefonnetz. Häufig integrieren Router eine Hardware- Firewall zum Schutz des lokalen Netzes vor äußeren Angriffen. In lokalen Netzen werden Router überwiegend zur Verbindung des Netzes mit dem Internet genutzt. Von "außen" ist nur die IP-Adresse des Routers sichtbar. Damit das Internet von allen Hosts genutzt werden kann, muss sich der Router um die Weiterleitung der Daten kümmern. Hierzu besitzt er eine Routing-Tabelle mit den IP-Adressen aller Arbeitsstationen.

Handelt es sich um einen statischen Router, dann müssen diese manuell durch den Netzwerk-Administrator einprogrammiert werden. Bei größeren Netzen kommen dynamische Router zum Einsatz, die sich automatisch um die Verwaltung und (dynamische) Zuteilung der Netzadressen kümmern. Ohne Router wäre aber auch das Internet selbst undenkbar: In einem Netzverbund mit mehreren Millionen Computern ist eine effiziente Wegvermittlung durch Router unerlässlich. Sie sorgen dafür, dass in Abhängigkeit von der aktuellen Netzauslastung optimale Verbindungswege für die zu übertragenden Daten gefunden werden.

## Gateway

Ein Gateway (engl.:Tor) kann Netze bis zur Schicht 7 des OSI-Modells miteinander verbinden. Diese Netze müssen demnach überhaupt keine Gemeinsamkeiten mehr besitzen und können sich beispielsweise im Zugriffsverfahren, den Übertragungsprotokollen und der Codekonvertierung voneinander unterscheiden. Ein Gateway schließt logischerweise die Funktionen von Router, Bridge und Repeater mit ein. In reinen TCP/IP-Netzen kann die Funktion des Gateways durch einen Router übernommen werden. Ein Gateway ist jedoch beispielsweise notwendig, um ein TCP/IP-Netz mit einem IPXI SPX-Netz von Novell zu verbinden.

## *Zugriffsverfahren*

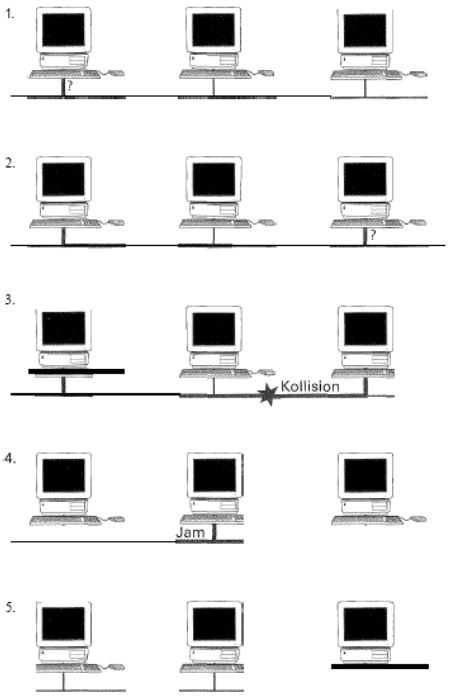
Zugriffsverfahren machen den Datenaustausch im Netzwerk auf Hardwareebene überhaupt erst möglich. Die Verwendung verschiedener Zugriffsverfahren kann ein Computernetzwerk beschleunigen oder verlangsamen.

### Ethernet

Ethernet ist fast schon zum Synonym für kabelgebundene lokale Netze geworden. Das Verfahren ist unter IEEE 802.3 standardisiert und wird ständig weiterentwickelt. Die Bezeichnung "Ethernet" umfasst die Beschreibung

- der benötigten Stecker und Kabel für die Integration eines Computers in ein LAN,
- das Zugriffsverfahren (CSMA/CD),
- die Protokolle zur Regelung des Datenverkehrs,
- die Art der Datenübertragung in Datenpaketen (Frames).

### CSMA/CD




Zum Betrieb eines Netzwerkes muss eindeutig festgelegt sein, wie der Datenaustausch zwischen den einzelnen Rechnern im Netz erfolgen soll.
Diese: als Zugangs- oder Zugriffsverfahren bezeichnete Festlegung besitzt bei Ethernet die komplizierte Bezeichnung CSMA/CD (Carrier Sense Multiple Access/Collision Detection):

1. Alle Rechner "hören" permanent das Netz ab (Carrier Sense), um festzustellen, ob Daten zu empfangen sind oder ob das Medium zum Senden eigener Daten frei ist.
2. Ein Rechner beginnt zu senden, wenn das Netz frei ist, andernfalls wird nach einer kurzen Wartezeit ein erneuter Versuch gestartet (Multiple Access).
3. Wenn zufällig ein zweiter Rechner gleichzeitig zu senden beginnt, kommt es zur Datenkollision.
4. Der Rechner, der die Kollision zuerst entdeckt (Collision Detection), sendet ein Störsignal (Jamming-Signal) aus. Damit erfahren alle Rechner, dass eine Störung vorliegt und somit das Senden momentan nicht möglich ist.
5. Nach einer kurzen Zufallszeit versucht der sendewillige Rechher erneut zu senden. Die Wahrscheinlichkeit, dass es wieder zu einer Kollision kommt, ist nun gering, sollte es dennoch dazu kommen, wiederholen sich 4 und 5.

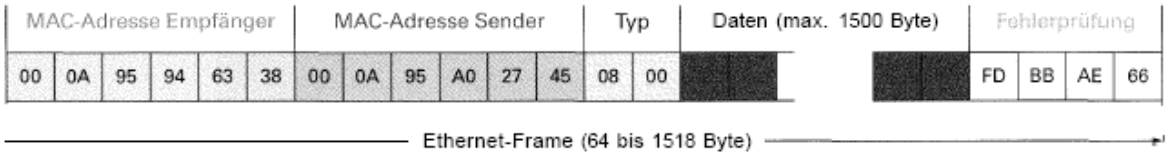
In der Grafik ist das Zugriffsverfahren am Beispiel der heute veralteten Bus-Topologie dargestellt. Als Ethernet vor etwa dreißig Jahren entwickelt wurde, war dieseTopologie jedoch weit verbreitet. Dies erklärt, weshalb ein Verfahren zur Kollisionserkennung eingesetzt werden musste. Die Situation heute ist eine andere: Lokale Netze werden fast ausschließlich sternförmig aufgebaut. Als Sternverteiler kommen Switches zum Einsatz, die eine "Intelligenz" besitzen und für die Datenübertragung immer eine direkte Verbindung zwischen Sender und Empfänger herstellen -

daher auch die Bezeichnung "Switch" (eng!.: Schalter). Ein "Switched Ethernet" arbeitet damit kollisionsfrei, so dass CSMA/CD nicht benötigt würde. Dennoch hat man es dabei belassen, auch um Kompatibilität zu Netzen mit Kollisionen zu erreichen. Durch die Kollisionsfreiheit steigert sich natürlich die Performance im Netz, da alle Daten nur einmal gesendet werden müssen.

## Ethernet-Frame

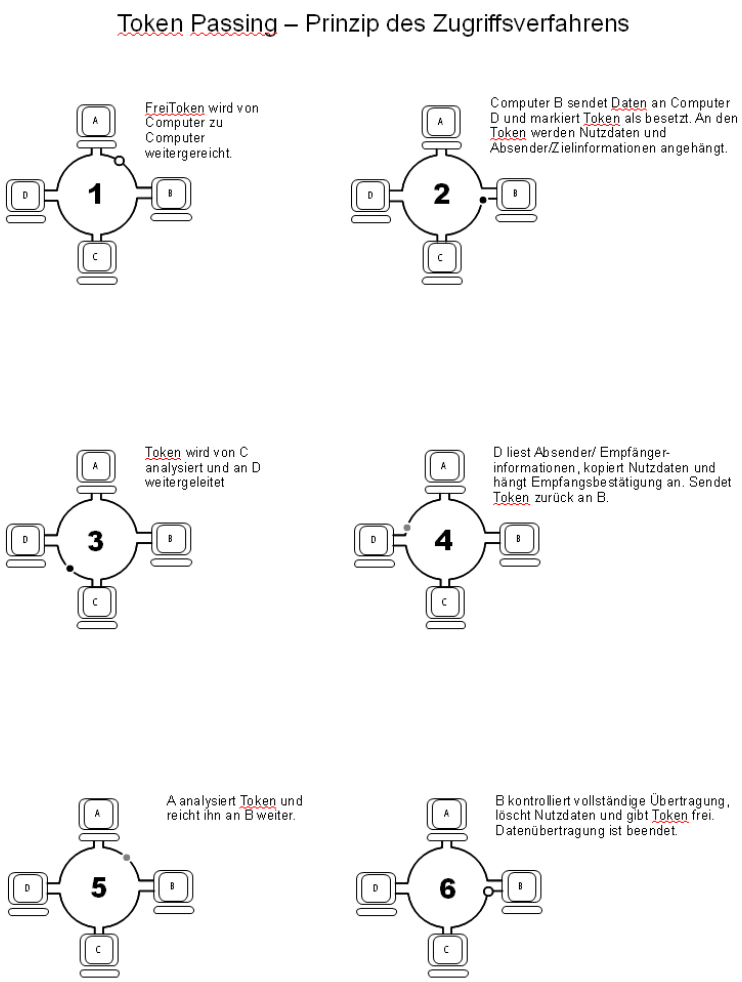
Vor der Datenübertragung "schnürt" der Sender ein "Datenpaket', das als Ethernet-Frame bezeichnet wird. In der Grafik unten ist eine mögliche Spezifikation eines Ethernet-Frames dargestellt. Es aber darauf hingewiesen, dass es noch andere Spezifikationen gibt. Der Ethernet-Frame setzt sich aus folgenden Teilen zusammen:

- MAC-Adresse des Empfängers
- MAC-Adresse des Senders
- Zusatzinformation über das NetzwerkprotokoII
- Die eigentlichen Nutzdaten, wobei maximal 1500 Byte möglich sind
- Prüfsumme zur Fehlererkennung bei der Datenübertragung




Die in der Grafik eingetragenen Zahlen sind lediglich Beispiele. Trifft ein gesendetes Paket im Switch ein, kann dieser mit Hilfe der beiden MAC-Adressen eine direkte Verbindung zwischen Sender und Empfänger herstellen. Wie bereits erläutert sind Datenkollisionen hierdurch unmöglich. Nun haben Sie sicherlich schon gehört, dass in Netzwerken (wie auch im Internet) eine weitere Adresse, die IP-Adresse, eine wichtige Rolle spielt. Worin liegt der Unterschied zwischen MAC- und IP-Adresse? Die MACAdresse ist hardwaremäßig festgelegt und nicht veränderlich. IP-Adressen hingegen können dynamisch zugeteilt werden, z. B. wenn Sie sich mit einem Computer am Netz anmelden. Nach Abschalten des Computers wird die IP-Adresse wieder frei. Auf diese Weise wird die Verwaltung von Netzen wesentlich flexibler.

## Token Ring (Token Passing)




Der Token Ring kann mit Geschwindigkeiten von 4 oder 16 MBit/s, als HighSpeedToken Ring (HSTR) mit 100MBit/ betrieben werden. Als Übertragungsmedium ist Twisted Pair vorgesehen. Der wichtigste Unterschied zu Ethernet ist, dass bei Token Ring ein als TokenPassing bezeichnetes Zugriffsverfahren verwendet wird, das Datenkollisionen verhindert:

Im Leerlauf kreist ein bestimmtes Bitmuster mit drei Byte Länge, das **FreiToken** genannt wird. Wenn ein Rechner Daten senden will, muss er auf das Frei-Token warten und wandelt dieses dann in ein Belegt-Token um. Die Daten werden gesendet, indem sie an das Belegt-Token angehängt werden. Der empfangende Rechner kopiert die Daten in seinen Speicher und gibt sie danach im Ring weiter. Im letzten Byte setzt der Empfänger zusätzlich ein Bestätigungsbit.

Wenn die Daten den Sender wieder erreichen, nimmt dieser sie aus dem Netz. Anhand des Bestätigungsbits erkennt er, dass der Empfänger die Daten übernommen hat.

Der Sender wandelt abschließend das Belegt- wieder in ein Frei-Token um. Danach kann der nächste Rechner zum Sender werden.

## *Dienste und Protokolle im Computernetzwerk*

Das, was wir so als das Internet bezeichnen, ist in der Regel eine sehr verschiedenartige Sammlung von Diensten, die über das Netzwerk in Anspruch genommen wird. Hier soll einmal die Begrifflichkeit und das Zusammenspiel von Diensten und Protokollen erklärt werden.

### Dienste im Computernetzwerk

- WWW
    - World Wide Web
        - Stellt HTML - Dateien zum Abruf zur Verfügung
- POP3/SMTP/IMAP
    - Post Office Protocol,
        - Sammelt E-Mails und stellt sie zum Abruf bereit

    - Simple Mail Transfer Protocol
        - Nimmt E-Mails vom Client entgegen und leitet sie weiter
    - Internet Message Access Protocol
        - Dienst zum Verwalten von E-Mails auf dem Server
- DHCP
    - Dynamic Host Configuration Protocol
        - Stellt den anfragenden Clients Netzwerk - Konfigurationsdaten zur Verfügung, z.B. IP-Adresse, Subnetzmaske, DNS, etc.
- DNS
    - Domain Name System/Server/Service
        - Dienst zum Verwalten und Koordinieren von IP-Adressen und Namen
- FTP
    - File Transfer Protocol
        - Stellt Speicherplatz zur Verfügung und liefert / empfängt Daten
- NTP
    - Network Time Protocol
        - Übermittelt ein Zeitsignal
- IRC
    - Internet Relay Chat
        - Ermöglicht Echtzeit - Kommunikation
- NNTP (Usenet)
    - Network News Transfer Protocol
        - Stellt Möglichkeiten der Kommunikation zu verschiedenen Themen bereit.
- SSH
    - Secure Shell
        - Ermöglicht die Fernsteuerung von Computern

Surftipp: Netmafia - Internet und Dienste

### Serverarten

- Application Server
    - Stellt Anwendungsprogramme für Clients bereit
- Compute Server
    - Rechenserver für hochkomplexe Aufgaben, z.B. Berechnung von Klima-Modellen
- Datenbank Server
    - Stellt strukturierte Daten bereit
- File Server
    - Stellt Speicherplatz zur Verfügung und liefert Daten aus
- Internet Server
    - Diverse Dienste: E – Mail, Webserver, IRC - Server

## *Protokolle und Modelle*

Das OSI-Referenzmodell bildet die (theoretische) Basis für Computernetzwerke. Mit diesem abstrakten Modell ist es möglich, dass unterschiedlichste Dienste, Geräte und Sprachen miteinander arbeiten können.

## Schichtenmodelle

Jede Technik oder jeder Vorgang, der zur Datenübertragung genutzt wird, lässt sich in drei Bereiche aufteilen:

- Anwendung
- Protokoll
- Übertragungsweg

Die Anwendung ist der eigentliche Grund, warum eine Datenübertragung überhaupt stattfindet. Sie stellt die Daten bereit und nimmt sie auch wieder entgegen.

Das Protokoll klärt die Nutzung des Übertragungswegs zwischen zwei oder mehr Stationen.

Der Übertragungsweg ist das Medium, welches zur Datenübertragung genutzt wird. Z. B. Kabel oder Funk.

### Proprietäre Systeme

Kommen Übertragungsweg, Protokoll und Anwendung von einem einzigen Hersteller, muss sich niemand Gedanken über die Technik machen und fragen, wie sie funktioniert. Alles spielt sich in einem abgeschlossenen System ab, das selten Probleme macht, allerdings auch wenig flexibel und transparent ist. Der Nutzer ist in diesem Fall an den Hersteller gebunden.

### Offene Systeme

In offenen Systemen sind Übertragungsweg, Protokoll und Anwendung genormt, spezifiziert und offengelegt. Das bedeutet: Jeder kann sich einen Teil heraussuchen und dazu eine Technik entwickeln, die sich dann auf dem Markt als Produkt behaupten muss und auch jederzeit austauschbar ist. Hier ist es auch möglich, dass Produkte unterschiedlicher Hersteller zusammenarbeiten und jederzeit gewechselt und erweitert werden können.

In der hochspezialisierten Computer- und Netzwerkwelt haben sich schnell Schichtenmodelle etabliert, in denen komplexe Vorgänge in einzelne Schritte aufgegliedert werden. Jeder Schritt wird als Schicht dargestellt, die übereinander gestapelt sind. Jede Schicht sorgt dafür, dass an den Schnittpunkten zur anderen Schicht Schnittstellen zur erfolgreichen Kommunikation enthalten sind.

Im Gegensatz zu hochintegrierten Systemen sind Schichtenmodelle nicht für hohe Geschwindigkeit oder Leistung ausgelegt. Es geht um eine hohe Flexibilität der einzelnen Schichten, damit diese leichter angepasst und ausgetauscht werden können.

## Das OSI - Referenzmodell

Das ISO-genormte OSI-Modell ist ein allgemeines, herstellerunabhängiges Referenzmodell für die Kommunikation in Netzwerken (OSI = Open Systems Interconnection). Es legt Standards und Spezifikationen für sieben Funktionsschichten fest. Die unteren vier bilden das Transportsystem, die oberen drei das Anwendungssystem. Diese Funktionsaufteilung ist aus zwei Gründen sinnvoll:

- Sie fördert system- und programmübergreifenden Datenaustausch. Unterschiedliche Systeme könnendas gleiche Transportsystem benutzen und sich nur im Anwendungssystem unterscheiden. Ein populäres
  Beispiel ist das Internet, in dem die verschiedensten
  Computer kommunizieren.

- Das Schichtmodell bietet Flexibilität beim Einsatz neuer Hard- und Softwaretechniken, denn Änderungen in einer bestimmten Schicht ziehen nicht zwangsläufig Änderungen anderer Schichten nach sich. Beispielsweise können schnellere Netzkarten und Verkabelung (Schicht 1) ein Netz erheblich beschleunigen, auch wenn die darüber liegenden Schichten nicht oder nur teilweise geändert werden. Verbesserungen der Datenkompression oder Verschlüsselung bleiben auf die zugehörige Schicht 6 beschränkt usw.

Die eigentliche physikalische Datenübertragung findet nur auf der untersten Bitübertragungsschicht statt; darüber liegen sechs protokollgesteuerte Softwareschichten mit diversen Funktionen zur Organisation, Absicherung und Steuerung der Übertragung. Das Übertragungsmedium (Kabel, Funk usw.) ist im OSI-Modell nicht festgelegt.

Zum reibungslosen Netzbetrieb gehören neben der Zugriffsregelung wie CSMA oder TokenPassing weitere Vereinbarungen zur Fehlerüberprüfung, Paketgröße, Verschlüsselung usw.

Zusammenfassend wird von Netzwerk-Protokollen gesprochen. Netzwerke mit TCP/IP-Protokoll, also Inter- und Intranets sowie ATM-Netze arbeiten mit fünf statt sieben Schichten, denn Schicht 5, 6 und 7 sind zu einer Anwendungsschicht zusammengefasst. HTTP, das grundlegende Protokoll des World Wide Web, FTP (Datentransfer), IRC (Chat) und SMTP, MIME und POP (E-Mail) gehören zur Anwendungsschicht. Im lnter- und Intranet ist der Internetbrowser das zentrale Programm, das einen Großteil dieser Schicht abdeckt.

## OSI - Referenzmodell (Open Systems Interconnection)

### Schicht 7 – Anwendungsschicht

(engl. **application layer**, auch: Verarbeitungsschicht, Anwenderebene) Die Verarbeitungsschicht ist die oberste der sieben hierarchischen Schichten. Sie stellt den Anwendungen eine Vielzahl an Funktionalitäten zur Verfügung (zum Beispiel Datenübertragung, E-Mail, Virtual Terminal, Remote login etc.). Der eigentliche Anwendungsprozess liegt oberhalb der Schicht und wird nicht vom OSI-Modell erfasst.
Protokolle und Normen: X.400, X.500, ISO 8571 (FTAM), ISO 9040/9041 (VT), ISO 9506 (MMS), MHS, VTP, FTP, NFS, Telnet, SMTP, HTTP, LDAP

### Schicht 6 – Darstellungsschicht

(engl. **presentation layer**, auch: Datendarstellungsschicht, Datenbereitstellungsebene) Die Darstellungsschicht setzt die systemabhängige Darstellung der Daten (zum Beispiel ASCII, EBCDIC) in eine unabhängige Form um und ermöglicht somit den syntaktisch korrekten Datenaustausch zwischen unterschiedlichen Systemen. Auch Aufgaben wie die Datenkompression und die Verschlüsselung gehören zur Schicht 6. Die Darstellungsschicht gewährleistet, dass Daten, die von der Anwendungsschicht eines Systems gesendet werden, von der Anwendungsschicht eines anderen Systems gelesen werden können. Falls erforderlich, agiert die Darstellungsschicht als Übersetzer zwischen verschiedenen Datenformaten, indem sie ein für beide Systeme verständliches Datenformat, die ASN.1 (Abstract Syntax Notation One ), verwendet.
Protokolle und Normen: ISO 8822 / X.216 (Presentation Service), ISO 8823 / X.226 (Connection-Oriented Presentation Protocol), ISO 9576 (Connectionless Presentation Protocol)

**Schicht 5 – Sitzungsschicht**

(engl. **session layer**, auch: Kommunikationssteuerungsschicht, Steuerung logischer Verbindungen, Sitzungsebene) Die Schicht 5 sorgt für die Prozesskommunikation zwischen zwei Systemen. Hier findet sich unter anderem das Protokoll RPC (Remote Procedure Call). Um Zusammenbrüche der Sitzung und ähnliche Probleme zu beheben, stellt die Sitzungsschicht Dienste für einen organisierten und synchronisierten Datenaustausch zur Verfügung. Zu diesem Zweck werden Wiederaufsetzpunkte, so genannte Fixpunkte (Check Points) eingeführt, an denen die Sitzung nach einem Ausfall einer Transportverbindung wieder synchronisiert werden kann, ohne dass die Übertragung wieder von vorne beginnen muss.
Protokolle und Normen: ISO 8306 / X.215 (Session Service), ISO 8327 / X.225 (Connection-Oriented Session Protocol), ISO 9548 (Connectionless Session Protocol)

**Schicht 4 – Transportschicht**

(engl. **transport layer**, auch: Ende-zu-Ende-Kontrolle, Transport-Kontrolle) Zu den Aufgaben der Transportschicht zählen die Segmentierung von Datenpaketen und die Stauvermeidung (engl. congestion avoidance). Die Transportschicht ist die unterste Schicht, die eine vollständige Ende-zu-Ende Kommunikation zwischen Sender und Empfänger zur Verfügung stellt. Sie bietet den anwendungsorientierten Schichten 5-7 einen einheitlichen Zugriff, sodass diese die Eigenschaften des Kommunikationsnetzes nicht zu berücksichtigen brauchen.
Fünf verschiedene Dienstklassen unterschiedlicher Güte sind in Schicht 4 definiert und können von den oberen Schichten benutzt werden, vom einfachsten bis zum komfortabelsten Dienst mit Multiplexmechanismen, Fehlersicherungs- und Fehlerbehebungsverfahren.
Protokolle und Normen: ISO 8073/X.224, ISO 8602, TCP, UDP, SCTP

**Schicht 3 – Vermittlungsschicht**

(engl. **network layer**, auch: Paketebene) Die Vermittlungsschicht sorgt bei leitungsorientierten Diensten für das Schalten von Verbindungen und bei paketorientierten Diensten für die Weitervermittlung von Datenpaketen. Die Datenübertragung geht in beiden Fällen jeweils über das gesamte Kommunikationsnetz hinweg und schließt die Wegesuche (Routing) zwischen den Netzknoten mit ein. Da nicht immer eine direkte Kommunikation zwischen Absender und Ziel möglich ist, müssen Pakete von Knoten, die auf dem Weg liegen, weitergeleitet werden. Weitervermittelte Pakete gelangen nicht in die höheren Schichten, sondern werden mit einem neuen Zwischenziel versehen und an den nächsten Knoten gesendet.
Zu den wichtigsten Aufgaben der Vermittlungsschicht zählen der Aufbau und die Aktualisierung von Routingtabellen sowie die Flusskontrolle. Auch die Netzadressen gehören zu dieser Schicht. Da ein Kommunikationsnetz aus mehreren Teilnetzen unterschiedlicher Technologien bestehen kann, sind in dieser Schicht auch die Umsetzungsfunktionen angesiedelt, die für eine Weiterleitung zwischen den Teilnetzen notwendig sind.
Hardware auf dieser Schicht: Router, Layer-3-Switches (BRouter)
Protokolle und Normen: X.25, ISO 8208, ISO 8473 (CLNP), ISO 9542 (ESIS), IP, IPsec, ARP, ICMP

**Schicht 2 – Sicherungsschicht**

(engl. **data link layer**, auch: Abschnittssicherungsschicht, Verbindungssicherungsschicht, Verbindungsebene, Prozedurebene) Aufgabe der Sicherungsschicht ist es, eine zuverlässige, das heißt weitgehend fehlerfreie Übertragung zu gewährleisten und den Zugriff auf das Übertragungsmedium zu regeln. Dazu dient das Aufteilen des Bitdatenstromes in Blöcke und das

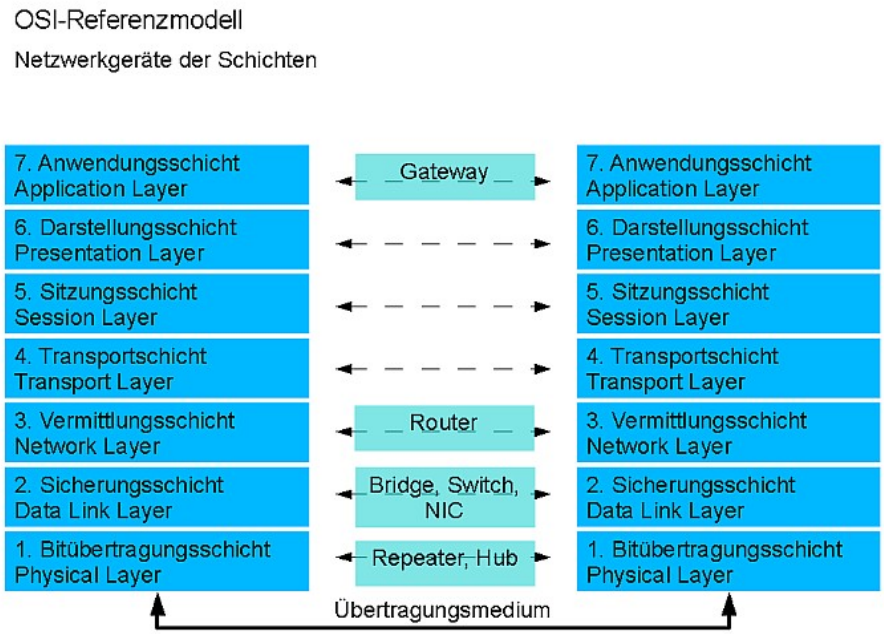
Hinzufügen von Folgenummern und Prüfsummen. Fehlerhafte, verfälschte oder verloren gegangene Blöcke können vom Empfänger durch Quittungs- und Wiederholungsmechanismen erneut angefordert werden. Die Blöcke werden auch als Frames oder Rahmen bezeichnet.
Eine so genannte Flusskontrolle macht es möglich, dass ein Empfänger dynamisch steuert, mit welcher Geschwindigkeit die Gegenseite Blöcke senden darf. Die internationale Ingenieursorganisation IEEE sah die Notwendigkeit, für lokale Netze auch den konkurrierenden Zugriff auf ein Übertragungsmedium zu regeln, was im OSI-Modell nicht vorgesehen ist.
*Nach IEEE ist Layer 2 in zwei Sub-Layers unterteilt: LLC (Logical Link Control) und MAC (Media Access Control).*
Hardware auf dieser Schicht: Bridge, Switch (Multiport-Bridge)
Protokolle und Normen: HDLC, SDLC, DDCMP, IEEE 802.2 (LLC), IEEE 802.3 (CSMA/CD), IEEE 802.11 (WLAN), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring)

### Schicht 1 – Bitübertragungsschicht

Die Bitübertragungsschicht (engl. **physical layer**) ist die unterste Schicht. Diese Schicht stellt mechanische, elektrische und weitere funktionale Hilfsmittel zur Verfügung, um physikalische Verbindungen zu aktivieren bzw. deaktivieren, sie aufrechtzuerhalten und Bits darüber zu übertragen. Das können zum Beispiel elektrische Signale, optische Signale (Lichtleiter, Laser), elektromagnetische Wellen (drahtlose Netze) oder Schall sein. Die für sie verwendeten Verfahren bezeichnet man als übertragungstechnische Verfahren. Geräte und Netzkomponenten, die der Bitübertragungsschicht zugeordnet werden, sind zum Beispiel die Antenne und der Verstärker, Stecker und Buchse für das Netzkabel, der Repeater, der Hub, der Transceiver, das T-Stück und der Endwiderstand (Terminator). Auf der Bitübertragungsschicht wird die digitale Bitübertragung auf einer leitungsgebundenen oder leitungslosen Übertragungsstrecke bewerkstelligt. Die gemeinsame Nutzung eines Übertragungsmediums kann auf dieser Schicht durch statisches Multiplexen oder dynamisches Multiplexen erfolgen. Dies erfordert neben den Spezifikationen bestimmter Übertragungsmedien (zum Beispiel Kupferkabel, Lichtwellenleiter, Stromnetz) und der Definition von Steckverbindungen noch weitere Elemente. Darüber hinaus muss auf dieser Ebene gelöst werden, auf welche Art und Weise überhaupt ein einzelnes Bit übertragen werden soll.
Damit ist Folgendes gemeint: In Rechnernetzen wird heute Information zumeist in Form von Bitfolgen übertragen. Selbstverständlich sind der physikalischen Übertragungsart selbst, zum Beispiel Spannungspulse in einem Kupferkabel im Falle elektrischer Übertragung, oder Frequenzen und Amplituden elektromagnetischer Wellen im Falle von Funkübertragung, die Werte 0 und 1 unbekannt. Für jedes Medium muss daher eine Codierung dieser Werte gefunden werden, beispielsweise ein Spannungsimpuls von bestimmter Höhe oder eine Funkwelle mit bestimmter Frequenz, jeweils bezogen auf eine bestimmte Dauer. Für ein spezifisches Netz müssen diese Aspekte präzise definiert werden. Dies geschieht mit Hilfe der Spezifikation der Bitübertragungsschicht eines Netzes.
Hardware auf dieser Schicht: Modem, Hub, Repeater
Protokolle und Normen: V.24, V.28, X.21, RS 232, RS 422, RS 423, RS 499

## Netzwerkgeräte im OSI-Referenzmodell

Netzwerkgeräte lassen sich z.T. den einzelnen Schichten des OSI-Modells zuordnen. Viele Geräte heutiger Bauart stellen allerdings verschiedene Funktionen zur Verfügung, die auf verschiedenen Ebenen des OSI-Modells arbeiten. Die Einordnung solcher Multifunktionsgeräte kann daher nur über die einzelnen Funktionen erfolgen.




## *Das Internet Protokoll*

Das IP ist zum meistgenutzten Protokoll im Computernetzwerk geworden. Selbst die Computer - interne Datenkommunikation wird teilweise über dieses Protokoll geführt.

## IPv4-Adresse

### IPv4

Eine IPv4-Adresse („v4" steht für Version 4) besteht aus einer 32-Bit-Zahl, die sich in 4 X 8 Bit, also vier Byte, gliedert: In einem Byte lassen sich 256 Zahlen von 0 bis 255 speichern. Bei vier Byte ergeben sich somit $256^4$ oder 4,29 Milliarden unterschiedliche Adressen. Trotz dieser scheinbar großen Zahl gehen die IPv4-Adressen so langsam aus. Ursache hierfür ist, dass durch die Bildung von Netzklassen große Adressbereiche reserviert sind. Bedenken Sie auch, dass nicht nur Computer eine eindeutige IP-Adresse benötigen, sondern prinzipiell alle Geräte, die am Internet teilnehmen könn(t)en, also z.B. Mobiltelefone.

### IPv6

Schon vor etlichen Jahren wurde aus oben genannten Gründen die Arbeit an einem neuen IP-Adress-Standard begonnen. IPv6 (Version 6, Version 5 wurde verworfen) erweitert IPv4 um 96 auf 128 Bit. Mit dieser unvorstellbar großen Zahl ($2^{128}$ = 3,4 x $10^{38}$ Adressen) ließe sich locker jedes Reiskorn dieser Erde mit einer IP-Adresse versehen. IPv6 besteht aus acht Blöcken mit je zwei Byte. Achtung: Wie bei MAC-Adressen erfolgt die Schreibweise hexadezimal, wobei für jeden Block vier Hexadezimalziffern benötigt werden:
`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`

Es wird noch einige Jahre dauern, bis alle Betriebssysteme und Geräte auf IPv6 umgestellt worden sind. Der Umstieg soll möglichst „sanft" erfolgen, so dass übergangsweise eine gemischte Verwendung von IPv4- und IPv6- Adressen möglich sein wird.

## IP - Organisation

Im Falle des Internets bilden viele Millionen Rechner einen riesigen Rechnerverbund. Um nicht nach der berühmten Nadel im Heuhaufen suchen zu müssen, ist es sinnvoll, die IPAdresse in zwei Teilbereich zu gliedern, einen Netz- und einen Host-Teil: 192.168.1.15

Die Trennung zwischen Netz- und Hostteil geschieht mittels der sogenannten Subnetzmaske.

## *Subnetting / IP-Berechnung*

## Grundlegendes zum Verständnis von Subnetting

Rechner im Internet werden über IP-Adressen angesprochen, die eindeutig sind. Eine IP-Adresse (IP) ist eine 32-bit-Zahl und enthält sowohl die Netzkennung als auch die Hostkennung eines Rechners. In der kürzeren Dezimalschreibweise sieht eine IP zum Beispiel aus wie "192.168.0.1", jede der 4 durch Punkte getrennten Zahlen repräsentiert eine 8bit-Binärzahl. Sie wird auch als Oktett bezeichnet und kann Werte zwischen 0 (binär 00000000) und 255 (binär 11111111) annehmen. Die zur IP gehörende Subnetmaske (ebenfalls 32bit) gibt an, welcher Teil der IP Hostkennung und welcher Netzkennung ist. Sie ermöglicht die Teilung eines Gesamtnetzes in mehrere kleinere Teilnetze.

Am besten ist dies in der Binärdarstellung der Netmask zu sehen : Die Netzkennung ist (von links nach rechts betrachtet) der Teil der IP, bei dem die Bits der Netmask 1 sind.

Als Beispiel betrachten wir die häufig in privaten LANs genutzte IP 192.168.0.1 mit einer typischen Subnetzmaske von 255.255.255.0.

**Darstellung 1 : Dezimal- und Binärschreibweise von Subnetzmasken (siehe auch zur Hilfe Anhang A)**

| IP - Dezimal | 192 | 168 | 0 | 1 |
|---|---|---|---|---|
| SM | 255 | 255 | 255 | 0 |
| SM binär | 11111111 | 11111111 | 11111111 | 00000000 |
| | Netzkennung | | | Hostkennung |

Wie anhand der Darstellung zu sehen ist, befindet sich der Host im Subnetz 192.168.0. und ist hat die erste Hostadresse in diesem Netz.

Da eine Subnetzmaske definiert, wie viele Bits zur Adressierung des Hosts, und wieviel zur Adressierung des Netzes zur Verfügung stehen, legt sie die maximale Anzahl der Hosts und Netze fest - je mehr Bits für die Hostkennung verwendet werden, desto weniger stehen für die Netzkennung zur Verfügung. Der gesamte IP4-Adressraum ist zwar relativ gross, aber begrenzt.

Auch die CIDR-Darstellung der Netzwerkmaske lässt sich an obiger Darstellung gut illustrieren. Es handelt sich hierbei um eine Kurzdarstellung der Netzmaske, die die Anzahl der auf 1 gesetzten Bits in der Subnetzmaske angibt. Ihr wird meist ein Slash ("/") vorangesetzt, so dass man an Stelle unserer Darstellung

"IP : 192.168.0.1, SNM : 255.255.255.0" in CIDR-Schreibweise auch "192.168.0.1/24" schreiben kann. Dies gibt an, das die Subnetzmaske 24 Bits hat, die auf 1 gesetzt sind (siehe Darstellung 1).

Früher teilte man die IP-Adressen in Klassen ein, je nach Subnetzmaske. Gebräuchlich waren die Subnetzmasken 255.0.0.0 ("Klasse-A-Netze"), 255.255.0.0 ("Klasse-B-Netze") und 255.255.255.0 ("Klasse-C-Netze"). Unsere IP 192.168.0.1/24 wäre also ein Rechner in einem Klasse-C-Netz.

Man beachte : Es spricht nichts dagegen, Subnetzmasken wie /21 oder /7 zu benutzen, bei denen die Trennung von Host- und Netzteil in dezimaler Schreibweise nicht zwischen den einzelnen Oktetten liegt. Dies war aber damals nicht notwendig und daher nicht vorgesehen. Lediglich /8, /16 und /24 Netze (also Klasse A,B, und C) waren in Benutzung, man spricht daher von diesem Schema als klassenbasierte IP-Adressierung.

Man teile die das Internets also in Klasse A, B, und C-Netze auf und definierte Adressbereiche für die einzelnen Netztypen :

**Tabelle 1 : klassenbasierte IP-Adressierung**

| Adressklasse | Netzbits | Hostbits | Adressbereich * | Anzahl Netze | Anzahl Hosts | Subnetzmaske |
|---|---|---|---|---|---|---|
| A | 8 | 24 | 0-126 | 126 | 16777216 | 255.0.0.0 |
| B | 16 | 16 | 128-191 | 16384 | 65536 | 255.255.0.0 |
| C | 24 | 8 | 192-223 | 2097152 | 256 | 255.255.255.0 |

* erstes Oktett der IP in Dezimalschreibweise

Man Beachte : Es spricht ebenfalls nichts dagegen, dass ein Rechner die Adresse IP : 10.11.12.12 SNM : 255.255.255.0 besitzt, obwohl das erste Oktett der Definition nach ein Klasse A Netz sein sollte und somit eine SNM von 255.0.0.0 habe sollte. Dies widerspricht lediglich der damaligen Definition, ist aber möglich.

Beim Betrachten von Tabelle 1 ist auffällig, das einige Adressbereiche nicht aufgeführt sind. Diese Bereiche sind für besondere Aufgaben reserviert. Siehe dazu Anhang B.

Jeder, der öffentliche IP-Adressen benötigte, bekam ein (oder auch mehrere) Adressbereiche zugeteilt - je nach Bedarf an IP-Adressen ein Class-A, -B oder -C-Netz. Bald wurden die ~ 4 Milliarden IP-Adressen knapp, und es wurden Massnahmen zur Bekämpfung des Mangels eingeführt. NAT (network address translation, Nutzung einer gemeinsamen öffentlichen IP durch viele Rechner mit privaten IPs hinter einem Router) und die klassenlose IP-Adressierung das Ergebnis. Man bezeichnet häufig Subnetze, die keine der SNMs von /8, /16 oder /24 haben, als klassenlose Subnetze. Durch klassenlose Adressierung lässt sich die Anzahl der maximalen Hosts pro Subnetz besser dosieren, weniger IP-Verschwendung ist die Folge.

Hinweis : Eine längerfristige Lösung ist die Einführung von IPv6, das die Adresslänge von 32 auf 128 Bit erhöht, und damit natürlich die Anzahl der zur Verfügung stehenden IP-Adressen dramatisch erhöht. Bis heute ist aber IPv4 die mit Abstand am weitesten verbreitete Adressierungsmethode, IPv6-Testnetze existieren aber seit geraumer Zeit, erste Produktionsumgebungen mit IPv6 bestehen ebenfalls.

# Berechnen von Subnetzeigenschaften - kommentierte Beispiele

**Beispiel 1 :**

## Aufgabe :

Gegeben ist eine IP und die zugehörige Subnetzmaske in Dezimalschreibweise. Berechnen Sie die Netzwerkadresse des zugehörigen Subnetzes, dessen Broadcast-Adresse und die Anzahl der Hosts, die maximal in diesem Subnetz untergebracht werden können.

```
Gegeben : IP 113.8.66.42, Netmask 255.255.255.240
```

## Rechnung :

*Schritt 1* - Umwandlung der dezimalen Netmask in CIDR-Schreibweise

Die dezimale Darstellung der Netmask ( hier z.B. 255.255.255.240) ist dem Verständnis der CIDR-Schreibweise eher hinderlich. Also wird die SNM zu erst in binary umgewandelt, daraus kann man die CIDR einfach ablesen :

```
dezimal 255 255 255 240
bin 11111111 11111111 11111111 11110000

Anzahl Bits 1 : 8 + 8 + 8 + 4 = 28

CIDR /28
```

Die CIDR ist folglich 28.

*Schritt 2* - maximale Anzahl Hosts pro Subnetz bestimmen

Mit Hilfe der CIDR kann die maximale Anzahl von Hosts berechnet werden, die in jedem einzelnen der entstehenden Subnetzte untergebracht werden können :

Eine IP-Adresse hat 32 Bit, eine CIDR von 28 bedeutet, dass 28 Bit davon Netzkennung sind. Folglich bleiben 4 Bit für die Hostkennung übrig. Wir könnten also theoretisch 2^4 Hosts pro Subnetz unterbringen. Die erste IP des Subnetzes ist jedoch als Netzwerkadresse des Subnetzes selbst reserviert, die letzte IP eines Subnetzes dient den Hosts des Subnetztes als Broadcast-Adresse. Daher müssen diese beiden Adressen von der theoretisch maximalen Anzahl subtrahiert werden. Es ergibt sich in unserem Fall :

32 - 28 = 4

/* (Anzahl der Bits der IP-Adresse) - (CIDR) = (Anzahl Bits der Hostkennung) */
2^4 = 16

/* 2 hoch (Anzahl Bits der Hostkennung) = theoretische Maximalanzahl der Hosts */
16 - 2 = 14

/* 2 subtrahieren wegen Netzkennung und Broadcast */

Man kann folglich 14 Hosts pro Subnetz adressieren.

*Schritt 3* - Netzadresse des Gesamtnetzes bestimmen, in dem sich die IP befindet.

Die in Schritt 1 bestimmte CIDR zeigt, dass die von links gesehen ersten 28 Bit der IP-Adresse die Netzkennung sind und die von rechts gesehen ersten 4 Bit die Hostkennunng. Das Umwandeln der IP in das Binärsystem ergibt folgendes :

```
IP (dezimal): 113. 8. 66. 42
IP (binary) : 01110001 00001000 01000010 00101010
```

Um die Netzwerkadresse zu bestimmen, beachten wir nur den Teil der IP, bei dem die SNM auf 1 gesetzt ist :

```
SNM (binary) : 11111111 11111111 11111111 11110000
```

Die Netzkennung lautet folglich in binary :

```
01110001 00001000 01000010 00100000
```

Beachten Sie, das die letzten 4 Bits Null sind, da die Subnetzmaske an diesen Stellen 0 ist, und diese Zahlen folglich nicht zur Netzkennung, sondern zur Hostkennung gehören!

Das Umwandeln ins Dezimalsystem ergibt :

```
113. 8. 66. 32
```

Folglich ist die Netzkennung 113.8.66.32

*Schritt 4* - Bestimmen der Schrittweite der einzelnen Subnetze

Zuerst ist das erste Oktett der Subnetzmaske zu bestimmen, dass nicht komplett aus Bits besteht, die auf 1 gesetzt sind. In der Dezimalschreibweise also von links nach rechts das erste Oktett, das nicht 255 lautet.

In unserem Fall ist es das vierte Oktett, es lautet '240'.

```
256 - 240 = 16
```

Die Schrittweite ist also 16.

*Schritt 5* - Bestimmen der Start- und End-IP-Adressen der einzelnen Subnetze sowie von deren Broadcastadressen

Die Netzkennung des ersten Subnetzes lautet 113.8.66.32 (siehe Schritt 3). Es wird nun das erste Oktett der IP benötigt, in dem die Hostkennung beginnt (also das von links gesehen erste, in dem die Subnetzmaske nicht 255 lautet). Dies ist in unserem Fall das vierte Oktett. Nur dieses betrachten wir im Folgenden :

Die Netzkennung des ersten Subnetztes lautet im vierten Oktett 32, da die Schrittweite 16 beträgt (siehe Schritt 4), beginnt das nächste Subnetz bei 48, das darauf folgende bei 64, und so weiter. Daraus ergeben sich die IP-Adressen in den jeweiligen Subnetzen - sie liegen zwischen den Netzkennungen der Subnetze. Die Broadcastadresse ist jeweils die letzte IP vor der Netzkennung des nächsten Subnetztes. Es ergibt sich in unserem Fall :

Subnetz 1
Netzkennung 113.8.66.32
IP-Bereich : 113.8.66.33 - 113.8.66.46
Broadcastadresse : 113.8.66.47

Subnetz 2

Netzkennung 113.8.66.48
IP-Bereich : 113.8.66.49 - 113.8.66.62
Broadcastadresse : 113.8.66.63

Subnetz 3
Netzkennung 113.8.66.64
IP-Bereich : 113.8.66.65 - 113.8.66.78
Broadcastadresse : 113.8.66.79

.
.
.
und so weiter

Der Host mit der IP 113.8.66.42 liegt im Subnetz 1, die weiteren Subnetze hätte man nicht berechnen müssen, zur Verdeutlichung ist es hier aber geschehen.

## Anhang

Anhang A - Potenzen von 2 in dezimal und binary

Das flüssige Rechnen mit Potenzen von 2 im binären Zahlensystem ist für IP- und Subnetzberechnungen sehr hilfreich. Die folgenden Werte sollten bekannt sein.

| Potenz | $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
|---|---|---|---|---|---|---|---|---|
| Dezimal | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Binär | 10000000 | 01000000 | 00100000 | 00010000 | 00001000 | 00000100 | 00000010 | 00000001 |
| addiert | 128 | 192 | 224 | 240 | 248 | 252 | 245 | 255 |
| addiert | 10000000 | 11000000 | 11100000 | 11110000 | 11111000 | 11111100 | 11111110 | 11111111 |

**Anhang B - für besondere Aufgaben reservierte Adressbereiche**

1. loopback - 127.0.0.1

Das gesamte Netz mit der Kennung 127.0.0.0 ist nicht verfügbar, da 127.0.0.1 als sogenannte Loopback-Adresse definiert ist - jeder Rechner kann sich selbst unter dieser Adresse ansprechen und löst diese meist in den DNS-Namen 'localhost' auf.

Dies ist einfach in jeder Shell nachzuvollziehen :

```
root@threat # ping localhost
PING localhost (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=10.5 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=12.1 ms
```

```
 --- localhost ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 17.1/22.3/27.5 ms
```

2. private IP-Bereiche

Als privat definierte Adressbereiche werden im Internet nicht geroutet und können somit problemlos von jedem in privaten Netzwerken verwendet werden, ohne sich um die Beschaffung einer öffentlichen IP kümmern zu müssen.

Hinweis : Rechner mit IPs aus diesen Adressbereichen können nur über Router, die NAT ausführen, ans Internet angeschlossen werden. Bei der Einwahl zu Ihrem Internetprovider über Modem / ISDN wird Ihrem Rechner eine öffentliche IP aus dessen Pool zugewiesen, sie verwenden in diesem Fall keine private IP. Bei einem Rechner, der über eine mit einer privaten IP belegten Ethernet-Karte über einen DSL-Router ans Internet angeschlossen ist, führt dieser Router NAT aus und verfügt auf dem zum Internet gerichteten Anschluss ebenfalls über eine öffentliche IP.

Folgende Adressbereiche sind als privat definiert :

```
10.0.0.0 bis 10.255.255.255 ( Class A )

172.16.0.0 bis 172.31.255.255 ( Class B )

192.168.0.0 bis 192.168.255.255 ( Class C )
```

3. diverse für Testzwecke reservierte Adressbereiche
--

a.) CIDR: Classless Inter-Domain Routing

Zitiert nach: http://www.sp1r1t.org/networks/subnetting/subnetting.txt

## *Sicherheit im Netzwerk*

Die Sicherheit spielt in Computernetzwerken eine immer größere Rolle. Neben sensiblen Daten, wie Bankdaten und Kennwörtern, deren Missbrauch größeren finanziellen Schaden bedeuten kann, sind wertvolle persönliche Daten gefährdet.

Verschiedene Maßnahmen können helfen, Computernetzwerke vor unbefugtem Zugriff und Missbrauch zu schützen.

## W-LAN - Sicherheit

Dass Daten im drahtlosen Netzwerk einigermaßen einfach 'abgehört' werden können, ist schon problematisch. Noch problematischer kann es sein, wenn das eigene Netzwerk als Plattform für Datenklau missbraucht wird.

Interessant dazu ist ein Urteil des Landgerichts Hamburg.

Demnach sind alle "Betreiber" von Computernetzwerken verantwortlich für eventuellen Missbrauch. Es gilt also, sich davor durch diverse Maßnahmen zu schützen.

# WEP - Wired Equivalent Privacy

WEP ist ein Verschlüsselungsverfahren für WLANs, die dem Standard IEEE 802.11 entsprechen. Dazu wird in jedem WLAN-Endgerät Schlüssel (Passwort) hinterlegt, dem niemand bekannt ist und auch nicht nachvollziehbar sein sollte.
Trotz des offenen Übertragungsmediums Funk soll WEP ein Funknetzwerk genauso abhörsicher machen, wie es ein kabelgebundenes Netzwerk ist. Dazu stellt WEP Funktionen für die Paketverschlüsselung und zur Authentifizierung zur Verfügung.

**Hinweis: WEP gilt als veraltet und sollte nicht mehr verwendet werden. Ein WLAN sollte immer mit WPA2 (IEEE 802.11i) abgesichert werden. WLAN-Geräte, die WPA2 nicht unterstützen, sollten dringend ausgetauscht und nicht mehr eingesetzt werden.**
**Die folgende Beschreibung zu WEP, soll dokumentieren, warum WEP nicht mehr eingesetzt werden sollte.**

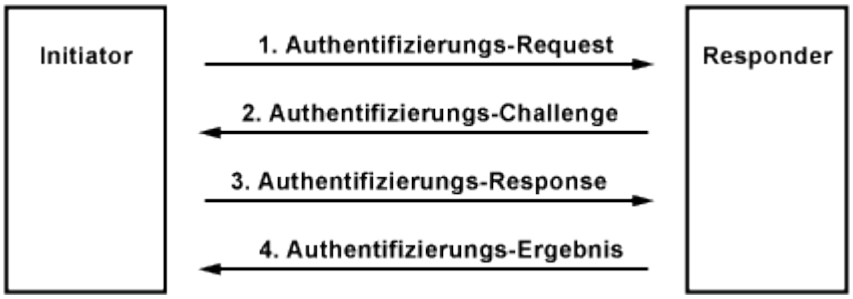
## WEP-Konfiguration

Bei der Konfiguration von WEP gibt es in der Regel 3 Varianten zum Einstellen bzw. Konfigurieren.

1. **WEP ist deaktiviert.**
   Eine Verschlüsselung der Daten findet nicht statt. Zur Authentifizierung wird das Verfahren "Open System" verwendet.
2. **WEP ist aktiviert und wird zur Verschlüsselung verwendet.**
   Die mobilen Stationen und der Access Point verschlüsseln und entschlüsseln die Daten mit dem hinterlegten WEP-Code. Zur Authentifizierung wird das Verfahren "Open System" verwendet.
3. **WEP ist aktiviert und wird zur Verschlüsselung und Authentifizierung verwendet.**
   Die mobilen Stationen müssen sich über das Verfahren "Shared Key" vom Access Point authentifizieren lassen. Zusätzlich werden alle Daten verschlüsselt übertragen.

## Authentifizierung

Die Authentifizierung unterscheidet zwei Verfahren. Das Open System Authentication ist die Standard-Authentifikation. Sie schaltet für ein WLAN alle Clients frei. Es findet praktisch keine Authentifizierung statt.
Shared Key Authentication ist die sichere Variante mittels einem Challenge-Response-Verfahren mit einem geheimen Schlüssel zur Authentifizierung. Das Challenge-Response-Verfahren basiert auf dem Austausch von 4 Nachrichten zwischen einem Initiator und einem Responder.




1. Die mobile Station schickt eine Authentifizierungsanforderung an den Access-Point.
2. Der Access-Point schickt einen Zufallstext (Challenge) an die mobile Station.

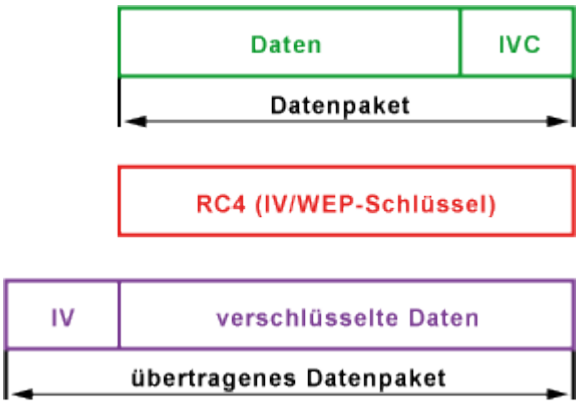
3. Die Station verschlüsselt den Text mit dem vorkonfigurierten 64- oder 128-Bit WEP-Code und sendet ihn an den Access-Point.
4. Der Access-Point entschlüsselt den Text mit dem eigenen bekannten WEP-Code. Wenn der verschickte Text mit dem erzeugten Zufallstext übereinstimmt, dann ist auch der WEP-Code identisch. Der Access-Point bestätigt die Identität der Station.
5. Die mobile Station stellt eine Verbindung zum Access-Point her.

Die 4 Nachrichten der WEP-Authentifikation sollen sicherstellen, dass der Initiator zugriffsberechtigt ist. In der Regel ist das WLAN-Endgerät der Initiator und der Access Point (AP) der Responder. Eine gegenseitige Authentifizierung lässt sich durch das Vertauschen der beiden Stationen und Wiederholen des Challenge-Response-Verfahrens erreichen.
Der Haken an WEP ist die manuelle Konfiguration des Schlüssels auf allen WLAN-Endgeräten. Dazu ist eine Person nötig, die sich um die Verwaltung der geheimen WEP-Schlüssel kümmert. Dynamische Sitzungsschlüssel oder Schlüsselzertifizierung ist in WEP nicht vorgesehen.

**Verschlüsselung**

Die Verschlüsselung erfolgt mit dem Verschlüsselungsverfahren RC4. Es handelt sich dabei um eine Datenstromchiffrierung von RSA Data Security.
Das mit WEP verschlüsselte WLAN-Datenpaket besteht aus mehreren Teilen:

- geheimer WEP-Schlüssel mit 40 (WEP40/WEP64) oder 104 (WEP104/WEP128) Bit
- 32-Bit-Prüfsumme der unverschlüsselten Daten (Integrity Check Value, ICV)
- 24-Bit Initialisierungsvektor (IV) der den WEP-Schlüssel zum Gesamtschlüssel mit 64 Bit oder 128 Bit macht und einmal pro Datenpaket inkrementiert (-1) wird




Das Datenpaket setzt sich aus den Daten und der 32-Bit-Prüfsumme der Daten zusammen. Dieses Datenpaket wird mit der IV-WEP-Schlüssel-Kombination verschlüsselt. Den verschlüsselten Daten wird der IV vorangestellt, damit der Empfänger den RC4-Schlüssel aus IV- und WEP-Schlüssel zusammensetzen und die verschlüsselten Daten entschlüsseln kann. Da der IV in Klartext übertragen wird, erfolgt die effektive Verschlüsselung nur mit 40 bzw. 104 Bit, obwohl gerne von 64 bzw. 128 Bit gesprochen wird.

**Sicherheitsprobleme**

WEP ist ein Verfahren um ein WLAN zu verschlüsseln. Trotzdem ist es möglich den Schlüssel zu knacken. Dazu muss die ablaufende WLAN-Kommunikation abgehört werden. Dazu ist nur eine handelsübliche Hardware nötig, die mit modifizierter Firmware oder auch nur mit entsprechenden Treibereinstellungen zu passiven Attacken geeignet ist.
Bis zum Herausfinden des WEP-Schlüssels reicht es, den in Klartext vorliegenden IV-Schlüssel

mitzuprotokolieren. Insgesamt gibt es nur 16.777.216 ($2^{24}$) Schlüsselmöglichkeiten, die aufgrund der inkrementierenden Zählweise irgendwann wiederholt werden müssen. Ein durchschnittlich belasteter 11-MBit-Access-Point würde diesen Zahlenraum in ca. einer Stunde wiederholen.
Mit relativ einfachen Mitteln lässt sich dann der WEP-Schlüssel zurückberechnen. Die verschlüsselten Datenpakete können dann entschlüsselt werden.

## WPA - WiFi Protected Access

Noch vor der offiziellen Verabschiedung von IEEE 802.11i, brachte die Herstellervereinigung Wi-Fi Alliance auf Basis eines Entwurfes von IEEE 802.11i ein eigenes Verfahren mit der Bezeichnung "WiFi Protected Access" (WPA) heraus. Damit sollte Schaden und Imageverlust der WLAN-Technik verhindert werden, der durch die fehlenden Sicherheitsfunktionen entstanden war. Der entstehende Markt für kabellosen Netzwerke und die damit verbundenen Einnahmen sollten nicht gefährdet werden.
In WPA kommt TKIP (Temporal Key Integrity Protocol) als Verschlüsselungsmethode zum Einsatz. TKIP setzt auf den RC4-Algorithmus mit einer verbesserten Schlüsselberechnung (Fast Packet Keying, FPK).

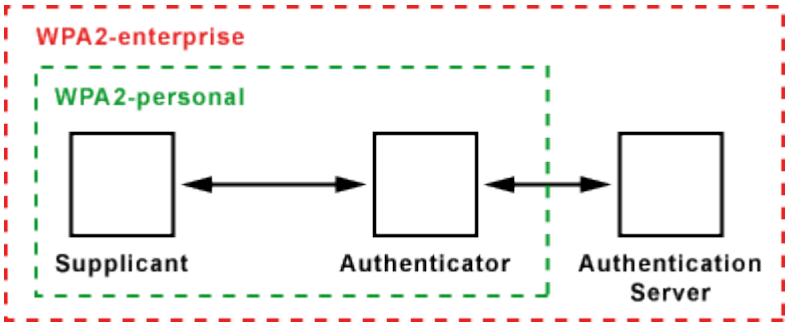
## WPA2 - WiFi Protected Access

Nach der Verabschiedung von IEEE 802.11i erweiterte die Herstellervereinigung Wi-Fi Alliance WPA um eine zweite Version. Damit basiert WPA2 auf dem Standard IEEE 802.11i. Zu beachten ist, dass WPA2 nicht gleich IEEE 802.11i ist. WPA2 gibt es in zwei Varianten, die beide nicht identisch mit IEEE 802.11i sind.

| **WPA-Variante** | | **WPA** | **WPA2** |
|---|---|---|---|
| **Personal Mode** | Authentifizierung | PSK | PSK |
| | Verschlüsselung | TKIP/MIC | AES-CCMP |
| **Enterprise Mode** | Authentifizierung | 802.1x/EAP | 802.1.x/EAP |
| | Verschlüsselung | TKIP/MIC | AES-CCMP |

Der wesentliche Unterschied zwischen WPA und WPA2 ist die Verschlüsselungsmethode. Während WPA das weniger sichere TKIP verwendet, kommt in WPA2 das sichere AES zum Einsatz.
AES (Advanced Encryption Standard) ist der Nachfolger des veralteten DES (Data Encryption Standard). In der Regel bringt AES mehr Datendurchsatz als TKIP. Moderne WLAN-Chipsätze enthalten einen Hardware-Beschleuniger für AES. Bei TKIP muss in der Regel der interne Prozessor die Arbeit erledigen.

**Funktionsweise von IEEE 802.11i und WPA/WPA2**




Bei der WPA-Schlüsselverhandlung bekommen die Stationen Rollen zugewiesen. Der Access Point ist der Authenticator (Beglaubigter) und der Client der Supplicant (Antragsteller/Bittsteller). Dabei ist genau festgelegt, welche Seite welches Paket zu welchem Zeitpunkt verschickt und wie darauf reagiert werden muss.

Bei WPA erfolgt die Netzwerk-Authentifizierung mit einem Pre-Shared-Key (PSK) oder alternativ über einen zentralen 802.1x/Radius-Server. Dabei wird ein Passwort mit 8 bis 63 Zeichen Länge verwendet. Das Passwort ist Teil eines 128 Bit langen individuellen Schlüssels, der zwischen WLAN-Client und dem Access Point ausgehandelt wird. Der Schlüssel wird zusätzlich mit einem 48 Bit langen Initialization Vector (IV) berechnet. Dadurch wird die Berechnung des WPA-Schlüssels für den Angreifer enorm erschwert.

Die Wiederholung des aus IV und WPA-Schlüssel bestehenden echten Schlüssels erfolgt erst nach 16 Millionen Paketen (2-24). In stark genutzten WLANs wiederholt sich der Schlüssel also erst alle paar Stunden. Um die Wiederholung zu verhindern, sieht WPA eine automatische Neuaushandlung des Schlüssels in regelmäßigen Abständen vor. Damit wird der Wiederholung des echten Schlüssels vorgegriffen. Aus diesem Grund lohnt es sich für den Angreifer kaum den Datenverkehr zwischen Access Point und WLAN-Clients abzuhören.

**Schwachstellen von WPA2**

Die Schwachstelle von WPA2 ist der Schlüssel, der bei Broadcasts und Multicasts die Datenpakete verschlüsselt (Groupkey). Dieser Schlüssel ist allen Stationen bekannt. Bekommt eine nicht autorisierte Person diesen Schlüssel heraus, ist sie in der Lage den anfänglichen Schlüsselaustausch zwischen Client und Access Point zu belauschen. Die Aushandlung dieses Schlüssels ist zumindest bei IEEE 802.11i täglich vorgesehen (86400 Sekunden).
Eine weitere Schwachstelle ist das Passwort (PSK). Je kürzer oder simpler diese Phrase ist, desto schneller bekommt ein Hacker Zugriff auf das geschützte Netzwerk. Eine lange Phrase mit zufälligen Buchstaben, Zeichen und Zahlen, dürfte zumindest nicht zu erraten sein.

# Inhaltsverzeichnis