Netztechnik

Robin Rausch, Florian Maslowski

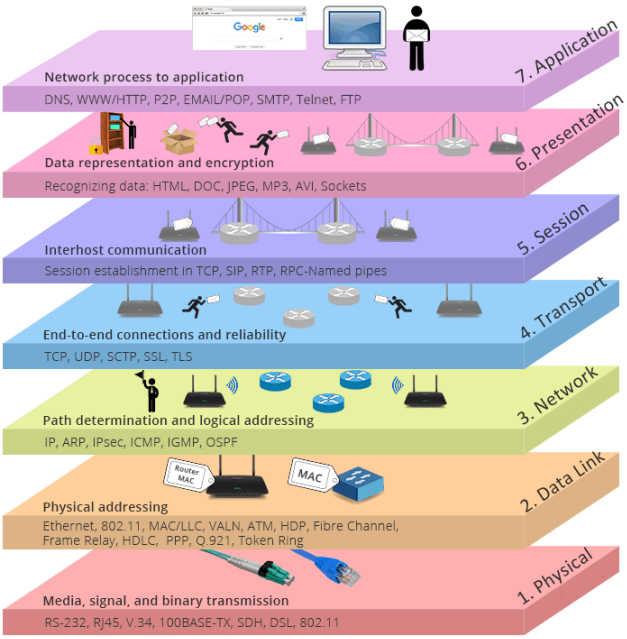
18. November 2022

Inhaltsverzeichnis

1 Grundlagen

1.1 OSI-7-Schichten-Modell

Merkhilfe: Please Do Not Throw Salami Pizza Away.
Zweck des Open-System-Interconnection-Modells ist, Kommunikation über unterschiedlichste technische Systeme hinweg zu beschreiben und die Weiterentwicklung zu begünstigen.



Hauptaufgaben der Schichten:

- Schicht 7: Anwendungen für Benutzer
- Schicht 6: Darstellung der Daten in verständliche Formate (jpg, ASCII)
- Schicht 5: Steuerung der Verbindung
- Schicht 4: Zuordnung der Datenpakete zu den Ports
- Schicht 3: Vermittelt Datenpakete
- Schicht 2: Fehlerfreie Übertragung
- Schicht 1: Bit-Übertragung

1.2 Schichten

1.2.1 Layer 1: Physical Layer - Bitübertragungsschicht

Diese Schicht beschreibt die physische Übertragung der Daten. Zusammenfassend geht es hierbei hauptsächlich um Kabel und Sender/Empfänger.

1.2.2 Layer 2: Data Link Layer - Sicherungsschicht

Hier wird der Ethernet Frame zusammengebaut und NIC und MAC-Adressen verwendet. Die MAC-Adresse fällt deshalb auch unter die Schicht 2 und wird später genauer erklärt.

1.2.3 Layer 3: Network-Layer - Vermittlungsschicht

In der 3. Schicht werden Verbindungen zu Hostsystemen (auch außerhalb des Netzes) aufgebaut. Darunter fallen beispielsweise Router.

1.2.4 Layer 4: Transport Layer - Transportschicht

Layer 4 stellt eine transparente Datenübertragung zwischen Endsystemen zur Verfügung. Darunter fallen beispielsweise TCP und UDP:

Bei TCP wird vor dem Datentransport eine Verbindung zwischen den Parteien aufgebaut und während des gesamten Datenaustausches gehalten. Nach Abschluss des Datenflusses wird die Verbindung wieder abgebaut. Verwendet werden hierbei Timer, Wiederholungen, Flusskontrolle, Windowing/Stop and Wait und Multiplexing um eine Verbindung mehrfach nutzen zu können.

Bei UDP werden die Daten in das Netzwerk in Richtung Empfänger gesendet, ohne dass der Sender weiß, ob der Empfänger empfangsbereit ist. Damit sind die oben aufgeführten Mechanismen, wie Flusskontrolle und Wiederholungen in den überlagerten Schichten zu bearbeiten.

1.2.5 Layer 5: Session Layer - Sitzungsschicht

Diese Schicht ist die erste anwendungsorientierte Schicht und behandelt Sitzungsabläufe und Synchronisationspunkte. Wenn ein Fehler auftritt, kann auf diese Synchronisationspunkte aufgesetzt werden. Ebenso fallen die Betriebsarten(Simplex, Half-Duplex und Full-Duplex) und Phasen(Verbindungsaufbau, Datenübertragung und Verbindungsaufbau) unter diese Schicht.

1.2.6 Layer 6: Presentation Layer - Darstellungsschicht

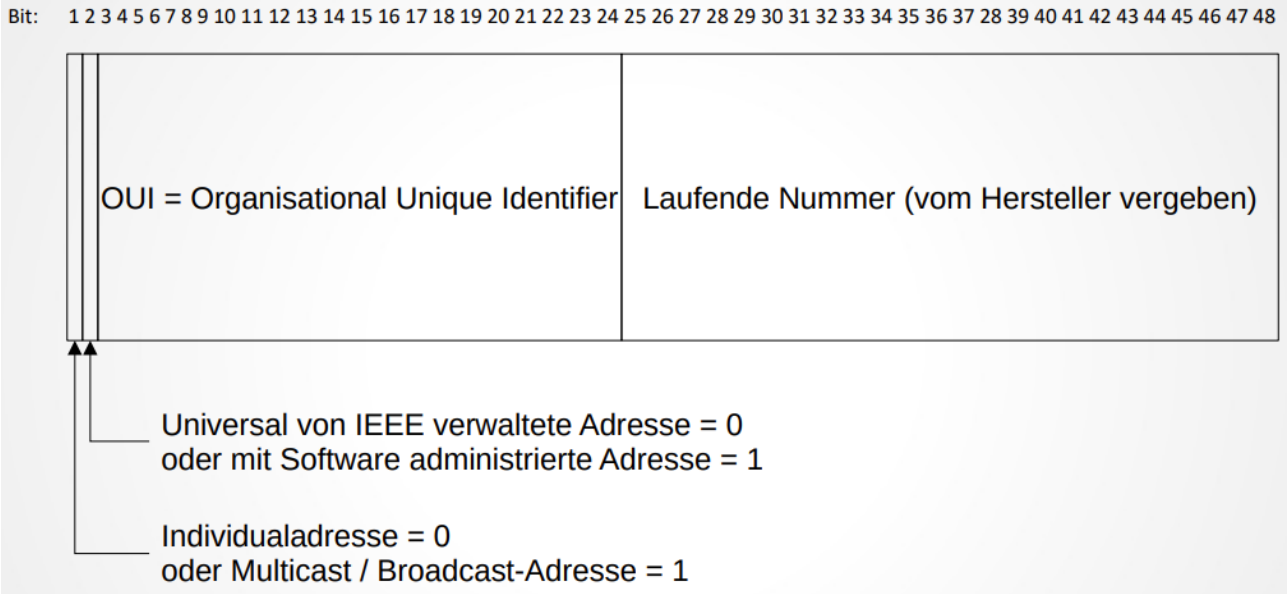
Unterschiedliche Rechner haben aufgrund unterschiedlicher Betriebssysteme unterschiedliche Darstellungsformen der Daten. Soll eine Applikation auf unterschiedlichen Betriebssystemen ablaufen können, sind Konvertierungen durchzuführen. Hier werden folgende Umsetzungen abgewickelt:
Zeichensätze (ASCII, EBCDIC), Interpretation von Bytes MSB (Most Significant Bit)/LSB (Least Significant Bit), Kompression/Dekompression und Verschlüsselung/Entschlüsselung

1.2.7 Layer 7: Application Layer - Anwendungsschicht

Diese Schicht bildet die Schnittstelle zum Anwender (User). Beispiel hierfür sind:
FTP File Transfer Protocol, SMTP Simple Mail Transfer Protocol, SNMP Simple Network Management Protocol und DNS Domain Name Service

2 MAC-Adresse

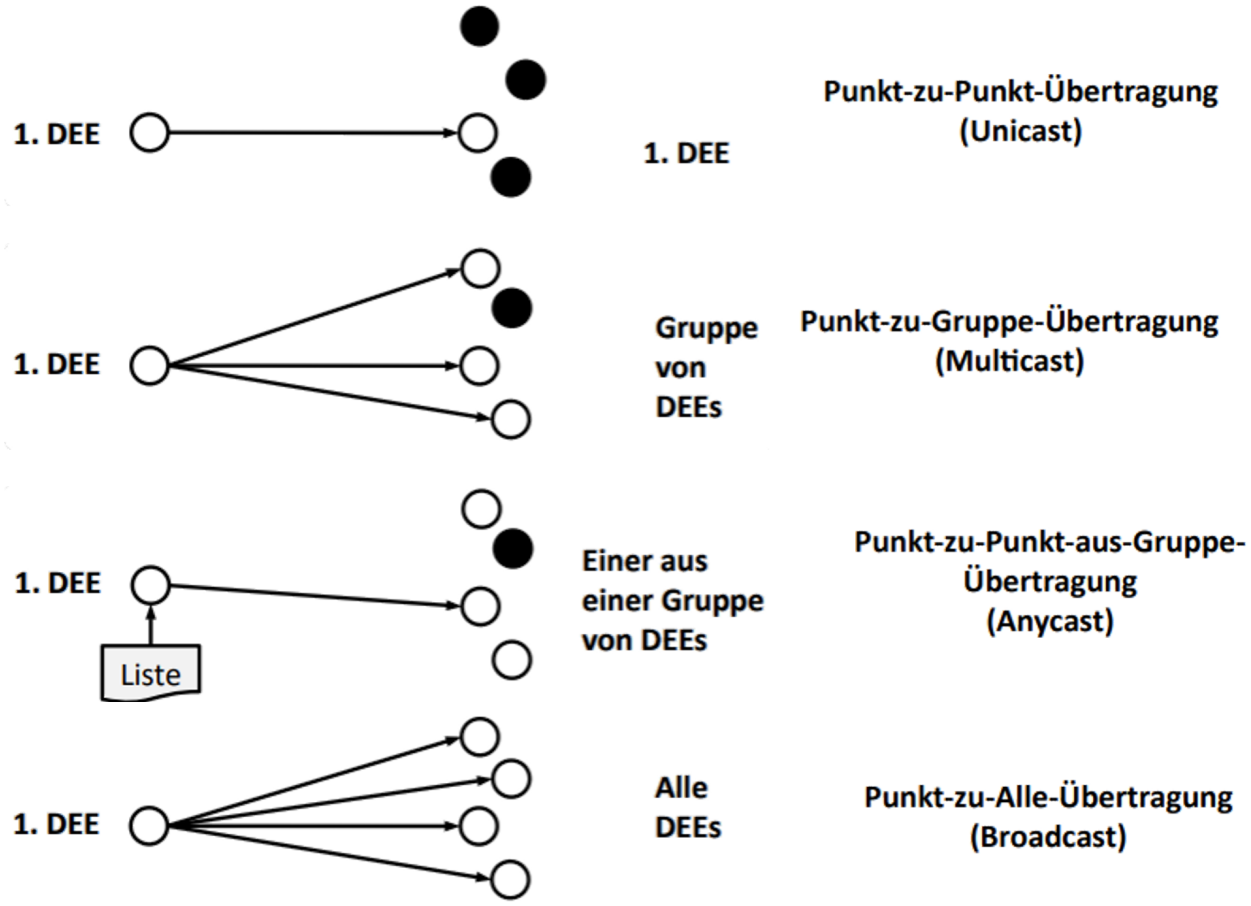
Um Informationen im Ether / Internet zuverlässig und zielgenau verschicken zu können, muss jedes Endgerät im Netz seine eigene individuelle Kennung besitzen!
⟶ *MAC Adresse*
Die MAC Adresse ist in den ROM der Network Interface Card eines jeden Gerätes eingebrannt. Die MAC ist also keine virtuelle Softwarekennung, sondern eine durchaus physisch mit dem Gerät verbundene Kennnummer. Die MAC-Adresse gehört zur OSI Schicht 2 und besteht aus 48bit welche in 4 Teile eingeteilt werden:



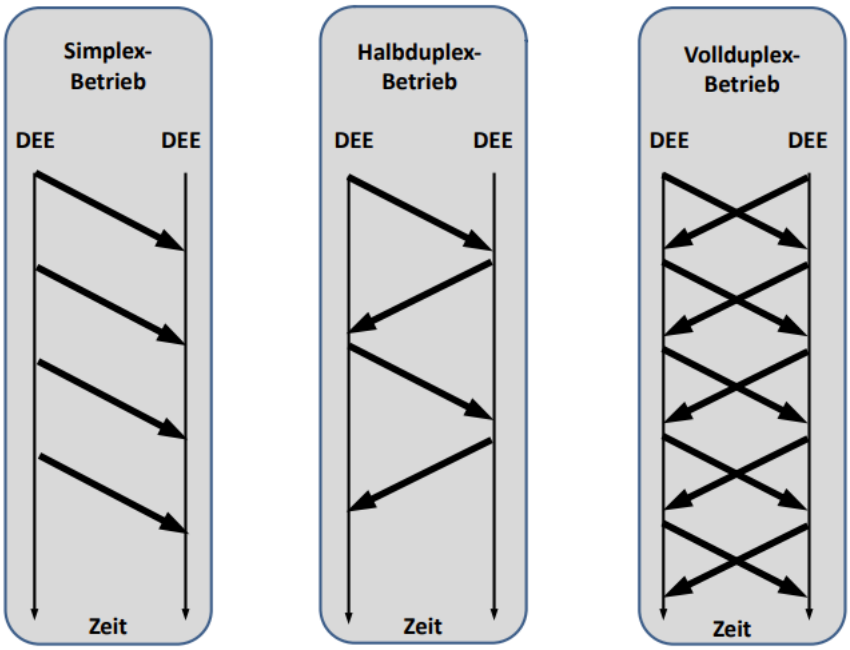
Wenn an der ersten Stelle der MAC-Adresse eine 1 steht, ist die MAC eine Broadcast oder Multicast Adresse. Wenn an der zweiten Stelle der MAC-Adresse eine 1 steht, ist die MAC eine mit Software administrierte Adresse und nicht unbedingt universell einzigartig.

3 Kabel

3.1 Verkehrsarten



3.2 Betriebsarten



3.3 Kabelarten:

Twisted-Pair: Verdrillte Paare, um geringes Nebensprechen mit hoher Übertragbarkeit zu erreichen.

LWL: Lichtwellenleiter/Glasfaserkabel hohe Geschwindigkeit, teuer, Aufwand in Spannung zurückzuwandeln. Je dünner der Faserkern (im Vergleich zum Fasermantel), desto besser ist das Ausgangssignal

3.4 Ethernet-Standards

10BaseT: 10 Mbit/s Twisted-Pair Kabel mit 100m Reichweite

10BaseF: 10 Mbit/s LWL (Fiber) mit 2000m Reichweite

100BaseTX: 100 Mbit/s Twisted-Pair Kabel, durch Vollduplex-Übertragung

100BaseFX: 100 Mbit/s LWL, durch Vollduplex-Übertragung

RJ-45-Buchsen: Port für Netzwerkkarte mit 8 Pins

3.5 Verkablungsarten:

Primarverkabelung: Für Verkabelung von Gebäuden mit LWL

Sekundärverkabelung: Für Verkabelung von Etagen mit LWL

Tertiärverkabelung: Für Verkabelung innerhalb einer Etage mit Kupferkabel

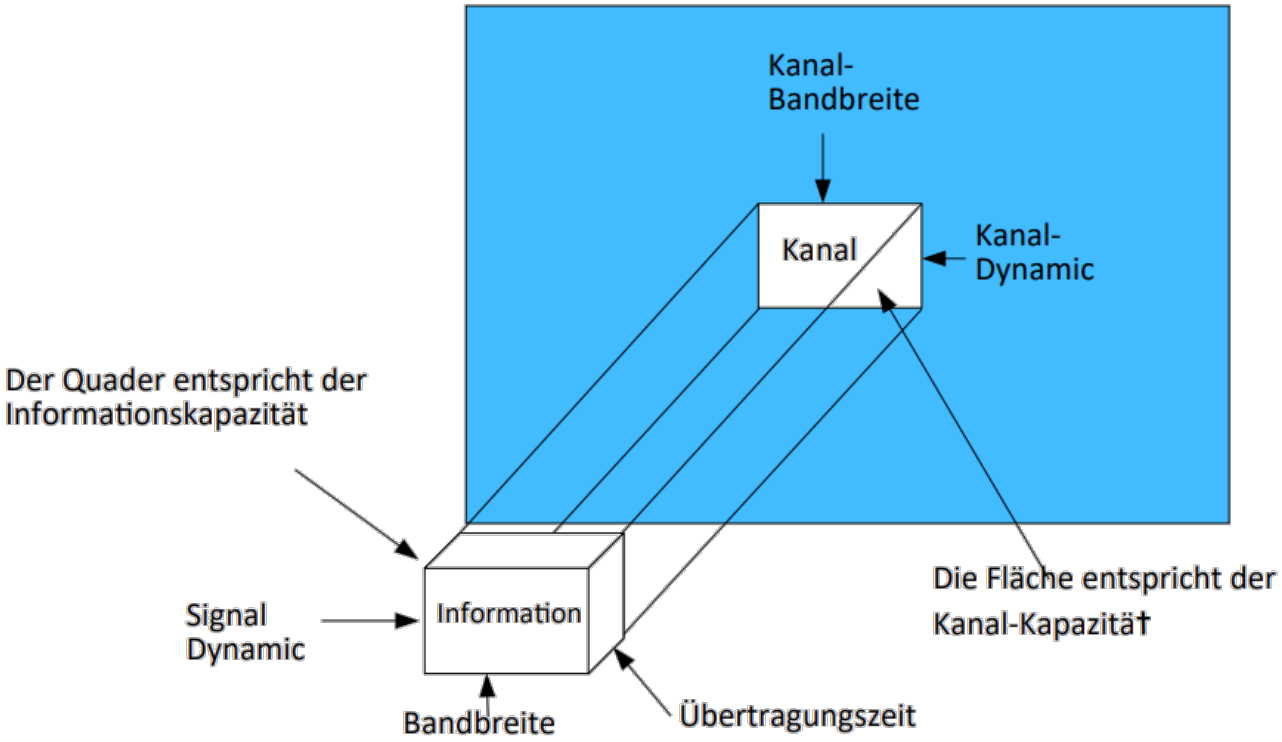
3.6 Vorteile Glasfaser statt Kupfer

- Lichtwellenleiter können beliebig mit anderen Versorgungsleitungen parallel verlegt werden. Es wirken keine elektromagnetischen Störeinflüsse.
- Wegen der optischen Übertragung existieren keine elektrischen Potentialprobleme.
- Entfernungsbedingte Verluste durch Induktivitäten, Kapazitäten und Widerständen treten nicht auf.
- Nahezu Frequenz-unabhängige Leitungsdämpfung der Signale.
- Übertragungsraten sind durch mehrere Trägerwellen mit unterschiedlichen Wellenlängen (Farbspektrum) fast unbegrenzt erhöhbar.
- Lichtwellenleiter haben eine erheblich geringere Dämpfung und eignen sich somit für weite Strecken.

3.7 Nachteile Glasfaser statt Kupfer

- Teurer als Kupfer
- Lichtimpulse lassen sich nicht zwischenspeichern. Wegen fehlender optischer Signalspeicher und Verarbeitungselementen muss eine aufwendige optisch/elektrisch und elektrisch/optische Signalumwandlung statt finden.

3.8 Informationskapazität



Kanal-Bandbreite: Die Kanalbandbreite eines drahtlosen Signals bestimmt die Datenrate dieses Signals. Je höher die Kanalbandbreite, desto schneller ist die Verbindung. Die Verwendung einer Kanalbandbreite von160 MHz ist eines der Hauptmerkmale des neuen WLAN-Standards Wi-Fi 6.

Kanal-Dynamic: Keine Ahnung? Wenn jemand weiß → bei Robin melden

3.9 NEXT - Near End Crosstalk

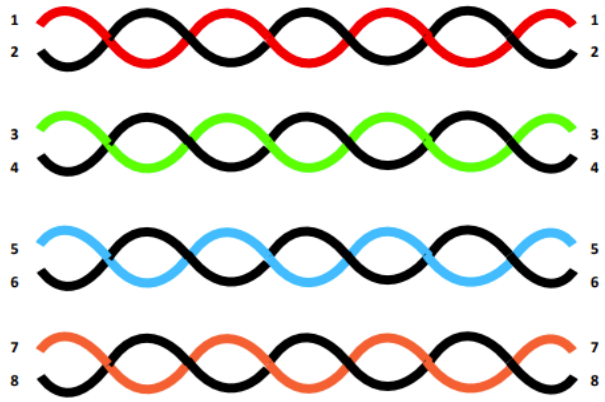
Beim Nahnebensprechen (Near End Crosstalk, NEXT) stört ein Sender einen benachbarten Empfänger. Der NEXT-Pegel ist der Signalpegel, der bei einer Signalübertragung über ein Adernpaar in einem benachbarten Adernpaar durch Induktion auftritt. Je schwächer dieses induzierte Signal ist, desto weniger Störungen gibt es.

3.10 Alien-Crosstalk

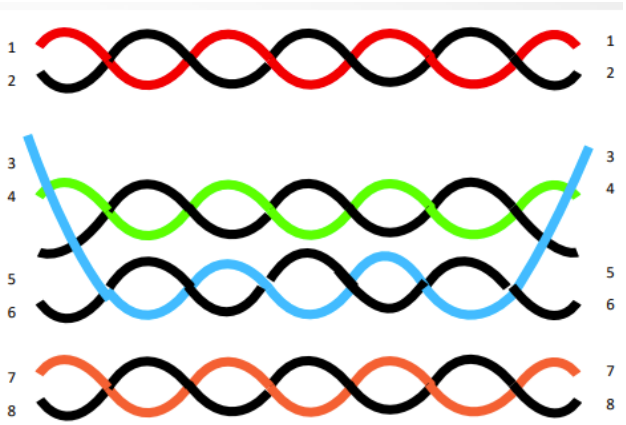
Alien Crosstalk (AXT) ist elektromagnetisches Rauschen, das in signalführenden Kabeln vorkommt, die parallel zu einem oder mehreren anderen Kabeln verlaufen.

3.11 Leitungstheorie

Um Leitungen vor elektromagnetischer Strahlung zu schützen, werden diese verdrillt. Je enger diese verdrillt werden, desto langsamer wird die Leitung(da der Weg länger wird).

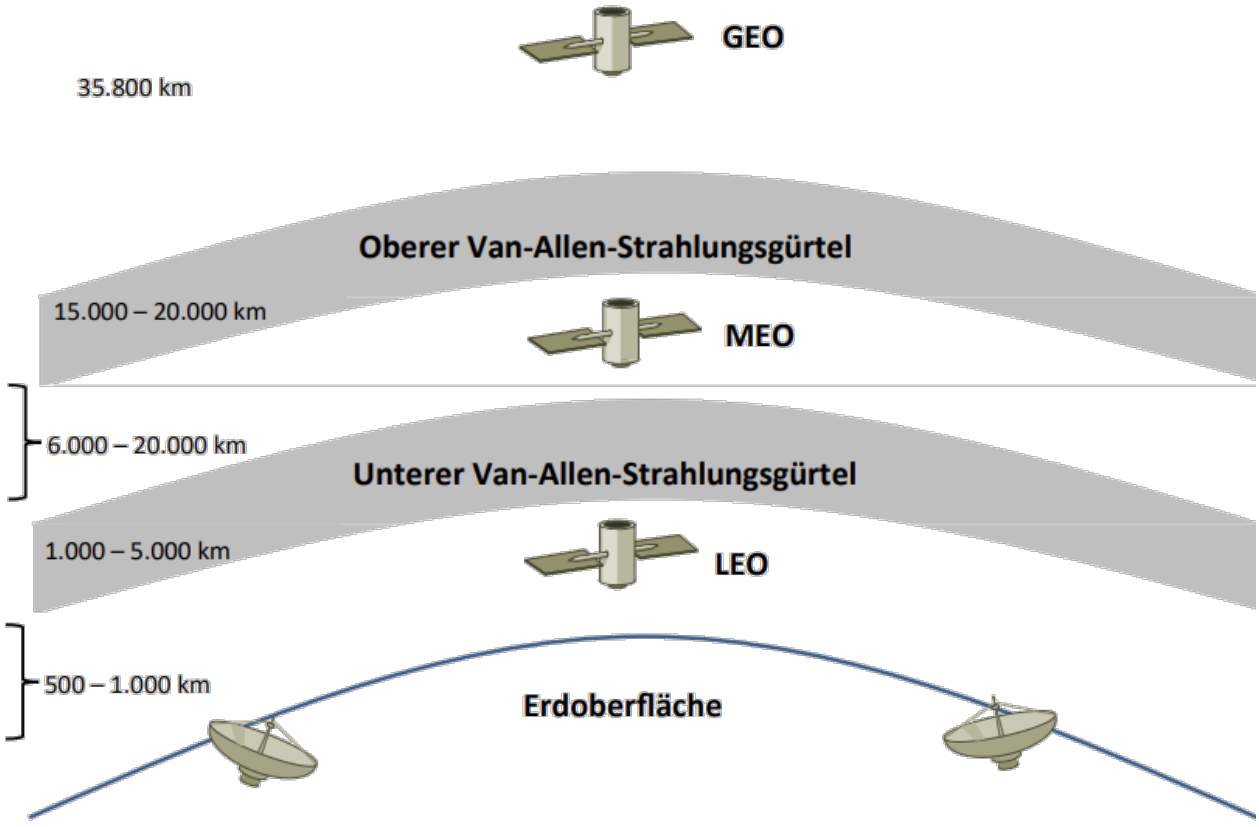


Split Pairs



Richtige Verdrahtung

4 Satelliten



5 Netze

5.1 Netzwerk-Technologien

Repeater Verstärkt Eingangssignal auf Ausgang, OSI-Schicht 1

Hub Multiport Repeater, OSI-Schicht 1

Bridge Verbindet 2 Netze, arbeitet mit MAC-Adressen, OSI-Schicht 2

Switch Schlauer Hub. Verstärkt nur an richtigen Port. Arbeitet mit MAC-Adressen, OSI-Schicht 2

Router Verbindet Netze, arbeitet mit IP-Adressen, OSI-Schicht 3

Gateway Verbindet Netze, arbeitet auf allen OSI-Schichten, Protokollunabhängig

5.2 Switch

5.2.1 Spanning Tree

Switche haben eine Hierarchie beim Weiterleiten von Paketen. Kleine Priorität ist besser. Falls Priorität gleich, entscheidet die MAC-Adresse über den bevorzugte Switch. Hierbei ist ebenfalls der Switch mit der geringsten MAC-Adresse der Root Switch.
Switche geben Pakete nur an Switche mit geringerer Priorität und niedrigerer MAC-Adresse weiter. Beste Switch in der Vernetzung wird zum Root.
Es gibt dabei 3 Arten von Ports an den Switches:

Root-Port Zur Root-Switch

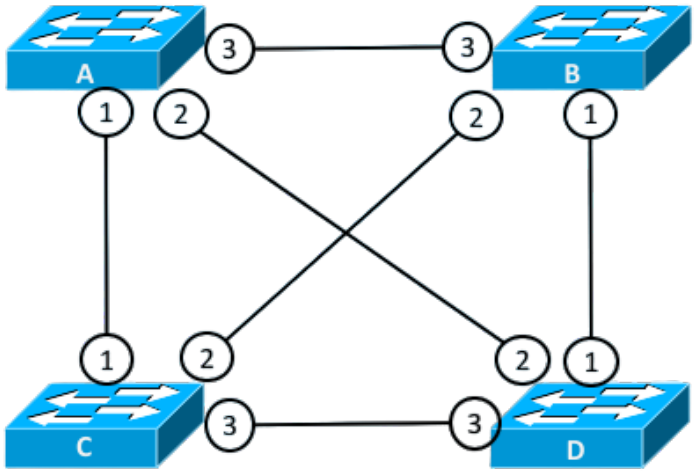
Designated-Port Zu Switch mit besserer Priorität oder höherer MAC-Adresse als die eigene

Blocking-Port Zu Switches, welche weniger bevorzugt sind als sie selbst

In Untenstehender Skizze ist Switch B die Root-Switch und alle Ports, die zu ihr führen, sind Root-Ports.
Da die restlichen Switche die gleiche Priorität haben, wird die höchste MAC-Adresse bevorzugt.
Dadurch sind die Ports zu Switch A die Blocking-Ports und die von D zu A und C ebenfalls.
Ports an Root-Switch sind alle designated.

Prio:
32768
MAC:
08-00-0C-00-00-0A

Prio:
1000
MAC:
08-00-0C-00-00-0B

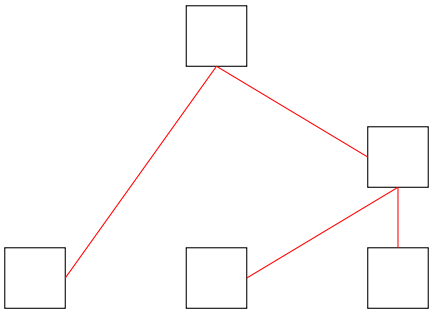


Prio:
32768
MAC:
08-00-0C-00-00-0C

Prio:
32768
MAC:
08-00-0C-00-00-0D

5.3 Netz Topologien

Baum Topologie



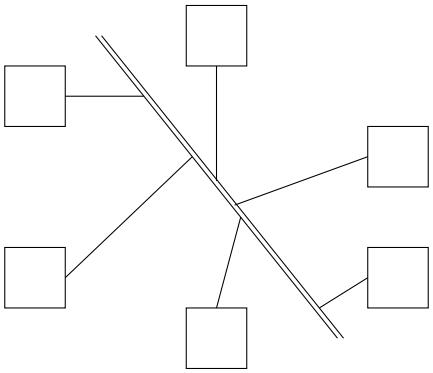
Vorteile:

- Bei Ausfall einer Komponente bricht nur ein Teil des Netzes zusammen
- leichte Skalierbarkeit

Nachteile:

- Durchsatzproblem an der Wurzel / jeder Netzkomponente $\longrightarrow$ höhere Laufzeiten

Bus-Topologie



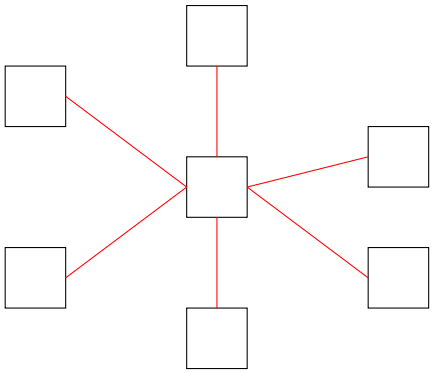
Vorteile:

- hohe Ausfallsicherheit
- leichte Skalierbarkeit

Nachteile:

- Ausfall der Hauptleitung $\longrightarrow$ Totalausfall
- Hauptleitung benötigt hohe Bandbreite

Stern Topologie



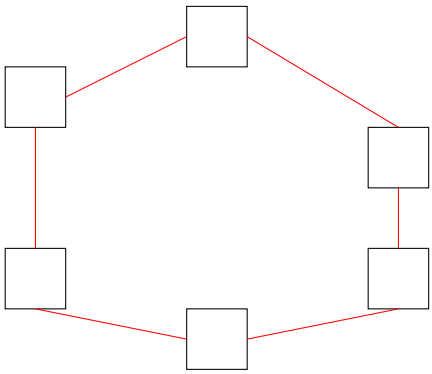
Vorteile:

- Leicht umsetzbar / skalierbar
- sehr schnell
- Beim Ausfall einer Komponente ist *nur* diese betroffen

Nachteile:

- Beim Ausfall der zentralen Wurzel $\longrightarrow$ Totalausfall
- Clients müssen immer über zentrale Wurzel kommunizieren.

Ring-Tropologie



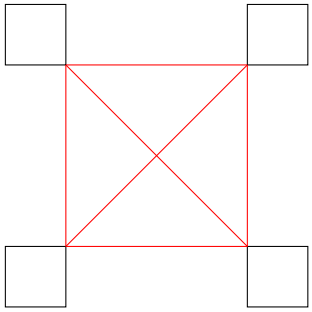
Vorteile:

- simpler Aufbau
- leichte Skalierbarkeit

Nachteile:

- Unterbrechung des Rings $\longrightarrow$ Totalausfall

Vermascht



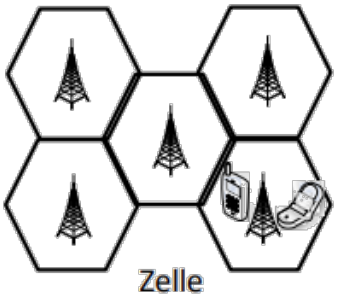
Vorteile:

- Bei Ausfall einer Komponente ist egal
- schneller Zugriff

Nachteile:

- Viele Verbindungen $\longrightarrow$ teuer und aufwendig

Zelle



Vorteile:

- sehr effiziente Kosten-Nutzen verteilung
- leichte Skalierbarkeit

Nachteile:

- Interferenzen
- Bei Ausfall einer Zelle ist halt doof für die in der Zelle
- Zwischen Zellen ist auch doof/ineffizient

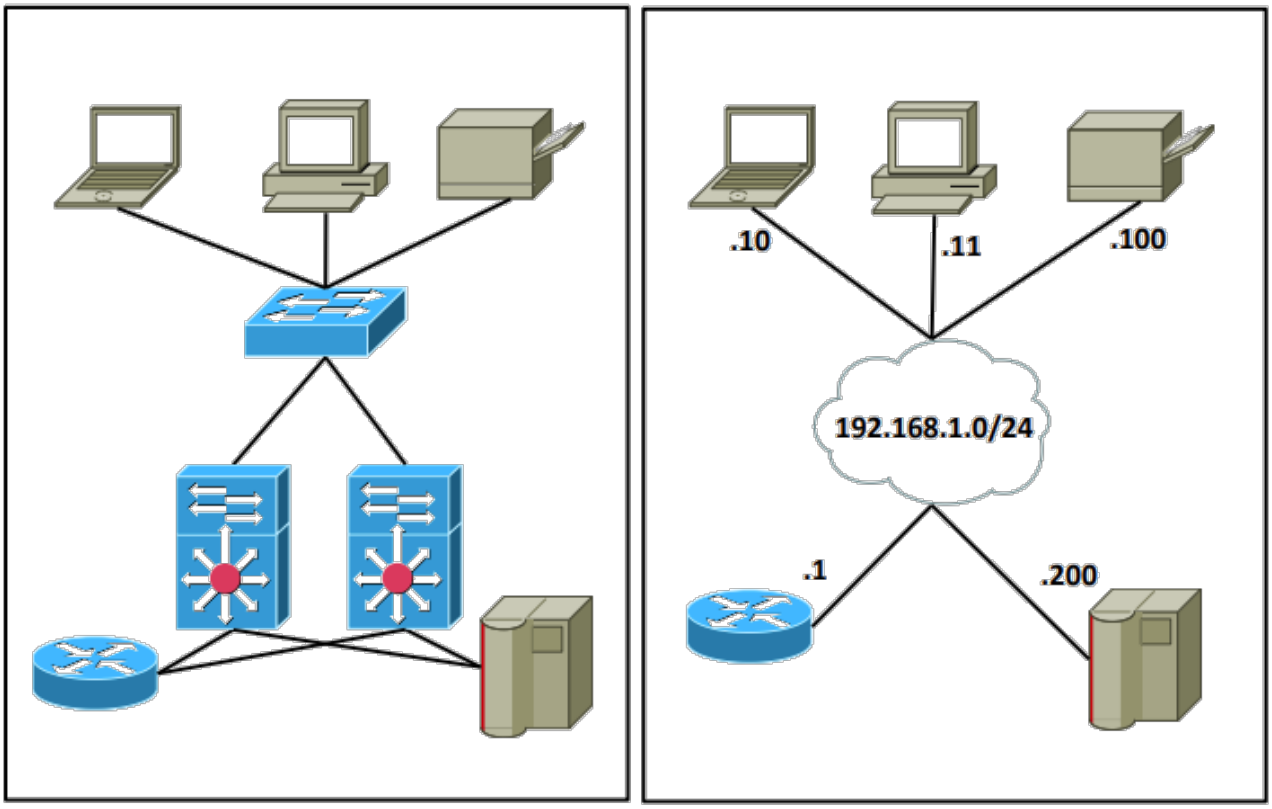
5.3.1 Netze in Unternehmen

Das Verwenden eines Netzes hat signifikante Vorteile für ein Unternehmen / Betrieb. Ressourcen und Betriebsmittel können gemeinsam genutzt werden (Zentral-Drucker). Dadurch können Kosten eingespart werden. Die Kommunikation innerhalb des Unternehmens wird durch verschiedene Netze (internes Telefon, Kommunikation zwischen den Systemen) um ein vielfaches erleichtert. Sollte das Unternehmen im Laufe der Zeit an Größe zulegen, ist die Skalierbarkeit des Systems im Allgemeinen unbegrenzt. Zusätzliche Systeme oder Server können problemlos hinzugefügt werden. Die Systemleistung eines einzelnen Computers kann außerdem gesteigert werden. Aufwendige Anwendungen können auf einem leistungsstarken Server ausgeführt werden, sind also nicht an die locale Leistung eines einzelnen Computers gebunden. Die Komponente der Teamarbeit im globalen Sinne wird durch ein globales Netzwerk zwischen Unternehmen außerdem vereinfacht.

5.3.2 Private Netze

Besitzt ein Haushalt einen Home Server mit Internetanbindung, so ist es Privatpersonen möglich, von nahezu überall auf der Welt auf ihre persönlichen Daten zugreifen zu können. Diese Option steht Privatpersonen außerdem durch Cloud Services zur Verfügung. Nachteil: Die Daten werden externen Firmen zur Verfügung gestellt, diese Option ist mit Vorsicht zu genießen. Privatpersonen können durch das Internet außerdem auf, generell betrachtet, Online Services zugreifen (Online Banking, Online Shopping). Die Kommunikation wird auch für Privatpersonen erheblich erleichtert. Durch Chat, Voice Chat oder sogar Video Chat Anwendungen ist die Kommunikation nahezu an jedem Ort der Erde möglich. Auch das Unterhaltungsprogramm profitiert vom Internet. Dienste wie YouTube oder Netflix wären ohne das Internet undenkbar.

5.3.3 Logische und Physikalische Netze



5.4 Servermodelle

Art	Beschreibung
Ein-Server-Modell	Ein Computer/Server übernimmt alle zentralen Dienste
Mulit-Server-Modell	Mehrere Computer/Server teilen sich die Verwaltung (für große Netze)

5.5 Kommunikationsarten

Art	Beschreibung
Simplex	Einer spricht, der Rest hört zu
Halbduplex	Wechselseitiges Sprechen und Hören
Vollduplex	Jeder spricht und hört gleichzeitig

5.6 Netzwerkkomponenten

5.6.1 Port

Ein Port ist der Teil einer Netzwerk-Adresse, der die Zuordnung von TCP- und UDP-Verbindungen und -Datenpaketen zu Server- und Client-Programmen durch Betriebssysteme bewirkt. Zu jeder Verbindung dieser beiden Protokolle gehören zwei Ports, je einer auf Seiten des Clients und des Servers.

5.6.2 Client

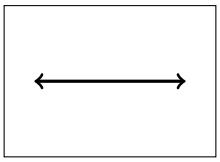
Der Client stellt einen Rechner im Netz dar. Er simuliert einen Computer an einem gewissen Standpunkt. Der Client besitzt eine Network-Interface-Card.

5.6.3 Netzwerkkarte

Eine Netzwerkkarte besitzt eine individuelle MAC-Adresse und befindet sich in eigentlich jedem Rechner. Sie stellt die Verbindung zwischen dem Rechner und dem Netzwerkmedium dar. Außerdem verfügt sie über eine Netzwerk-Schnittstelle.

5.6.4 Repeater

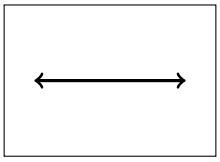
Der Repeater hat jeweils einen Eingang und einen Ausgang. Er verstärkt Signale durch regenerieren/synchronisieren des Taktes. Dazu arbeitet er auf Bitebene und verursacht eine kleine Latenz.



- Es können nur sehr wenige Repeater in folge geschalten werden
- Es gibt keine Begrenzung von Kollisionsdomänen $\rightarrow$ Kollisionen werden einfach weitergeleitet
- Repeater können verwendet werden um Längenbegrenzungen einzuführen oder um die Anzahl von Teilnehmern in einem Netz zu erhöhen
- gehört zur OSI Schicht 1

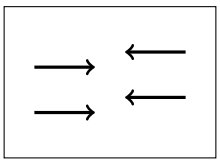
5.6.5 HUB

Der HUB ist ein Multiport Repeater. D.h. er hat mehrere Ein- und Ausgänge und arbeitet auch auf Bitebene.



5.6.6 Bridge

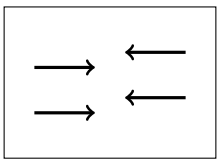
Die Bridgefungiert als Brücke zwischen zwei LAN-Netzwerken. Sie kennt die relevanten MAC-Adressen in beiden Netzen und verbindet so die Netze miteinander.



- Bridges begrenzen eine Kollisionsdomäne, da sie die Kollisionen abfangen
- Prüft bei jedem Frame die Ziel-MAC und schaut in eigener Tabelle nach ob die MAC im Netz vorhanden ist, aus dem der Frame kam. Falls dies der Fall ist wird der Frame verworfen. Andernfalls prüft die Bridge mithilfe der Tabelle an welchen Port/in welches Netz der Frame weitergeleitet werden soll
- gehört zur OSI Schicht 2 (da Bridge mit MAC Adressen arbeitet)
- In einem Netz dürfen maximal 7 Bridges verbaut sein
- Bridges werden bei Längenbegrenzungen, Anzahl der Teilnehmer erhöhen, Ausbreitung fehlerhafter Packete vermeiden, Kollisionen begrenzen und Verringerung der Netzlast eingesetzt

5.6.7 Switch

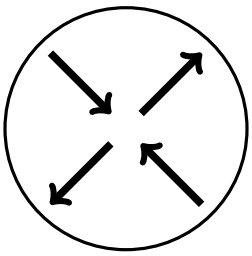
Der Switch ist eine Multiport-Bridge. D.h. er hat mehrere Ein- und Ausgänge und verbindet so mehrere Netzwerke miteinander. Er verwendet Filtertabellen um den schnellsten Weg für Signale zu finden. Er arbeitet ebenso mit MAC-Adressen.



- Der Switch kann Store & Foreward betreiben. D.h. er untersucht und speichert Frames bevor er sie weiterleitet. Dadurch können fehlerhafte Frames direkt aussortiert werden. Dadurch leidet jedoch die Leistung.
- Oder der Switch betreibt Cut Through, wobei er einfach die Frames an die Zieladresse weiterleitet ohne den Frame zu prüfen.
- Oder der Switch betreibt Cut Through Collision Free. D.h. Frames werden nur auf die ersten 64 Byte untersucht, falls bis dahin kein Fehler auftritt, wird dieser weitergeleitet.
- Kollisionen bleiben auf ein Netzwerk-Segment begrenzt. Dadurch werden Kollisionsdomänen gebildet.

5.6.8 Router

Der Router verbindet Netzwerke indem er Datenpackete weiterleitet oder blockiert. Er arbeitet mit IP-Adressen und wird oft auch als intelligenter Switch bezeichnet. Der Router wird für das gesamte Netz verwendet.



- gehören zur OSI Schicht 3
- Verbinden zwei separate Netzwerke miteinander
- Broadcasts werden auf Ebene 2 behandelt und Kollisionen auf Ebene 1
- Router begrenzen somit Broadcast- und Kollisionsdomänen
- Router haben für jedes Netz eine andere Subnetmaske, IP-Adresse und sogar MAC-Adresse

5.6.9 Einordnung der Komponenten ins OSI-Modell

Die Netzwerkkomponenten lassen sich in die Schichten 1 bis 4 einordnen. Die Schicht 1 beinhaltet alle Kabel(Kupferkabel, Ethernetkabel, Glasfaserkabel) und den Repeater. Zu Schicht 2 gehören Switches und Bridges. In Schicht 3 ist der Router und in Schicht 4 handelt es sich um die Netzwerkkarte und die Ports.

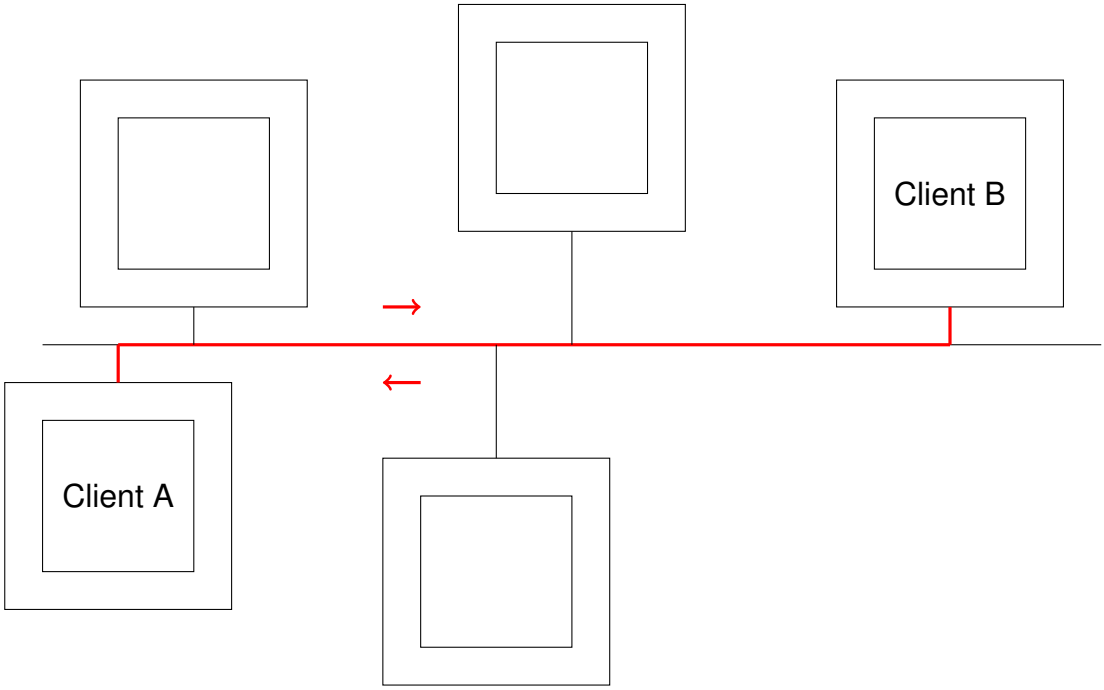
Nummer	Bezeichnung	Komponenten
1	Bitübertragungsschicht	Repeater, Kabel
2	Sicherungsschicht	Switches, Bridges
3	Vermittlungsschicht	Router
4	Transportschicht	Netzwerkkarte, Ports

5.6.10 HSRP und VRRP

Wenn, um die Verfügbarkeit eines Netzwerkes zu steigern, zwei Router verwendet werden, muss das Protokoll HSRP oder VRRP verwendet werden.
HSRP funktioniert mithilfe einem dritten virtuellen Default-Gateway und MAC-Adresse. Diese vergibt dann möglichst effizient die Packete and den Router mit höherer Priorität.
VRRP ist das Akronym für Virtual Router Redundancy Protocol. Es handelt sich dabei um ein Internet-Protokoll, womit sich ein oder mehrere Backup-Router betreiben lassen, wenn Sie einen statisch konfigurierten Router in einem LAN (Local Area Network) einsetzen. Somit dient der zweite Router nur als Backup, falls der erste ausfällt oder *nicht mehr klar kommt*.

5.7 Round Trip Delay Time - RTDT

Die Paketumlaufzeit bzw. Round Trip Time gibt die Zeit an, die ein Datenpaket in einem Rechnernetz benötigt, um von der weitesten entfernten Quelle zum Ziel und zurück zu reisen. Es handelt sich also um die Summe aus Laufzeit von Punkt A nach Punkt B und der Laufzeit von Punkt B nach Punkt A.

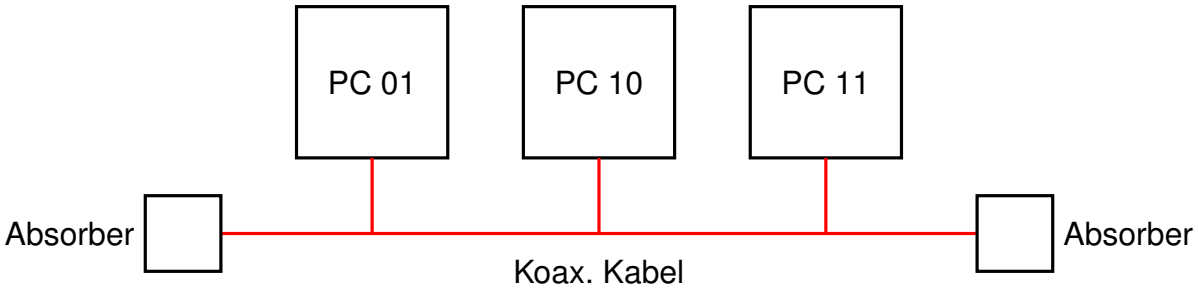


5.8 Bezeichnungen von Netzen

Abkürzung	Beschreibung	Ausdehnung	Anwendungen
BAN	Body Area Network	1m	Wearable Computers
PAN	Personal Area Network	10m	Bluetooth
LAN	Local Area Network	10km	LAN/WLAN
SAN	Storage Area Network	10km	für Datenspeicherung/-sicherung
MAN	Metropolitan Area Network	100km	Stadtgebiet
WAN	Wide Area Network	mehrere 1.000km	Öffentliche Netze(LTE, 5G, ...)
GAN	Global Area Network	mehrere 10.000km	Erdumspannende Netze die WAN's über Satelliten und Seekabel miteinander verbinden

6 Ethernet

Mit der Erfindung des Ethernets wollte man individuellen Stationen / Systemen den Zugriff auf ein gemeinsames Medium zur Datenübertragung ermöglichen. Die Netzwerktechnologie verwendet das CSMA/CD Verfahren und eignet sich primär für lokale Netze.



Soll ein Datenpaket verschickt werden (z.B. ein Zahlenwert), so muss der Sender das Ziel des Paketes kennen, um die Information zum korrekten Empfänger schicken zu können. Will *PC 01* die Zahl *5d* an *PC 10* senden, ergibt sich folgender Rahmen:

0010 *(Kennung des Ziels, 4Bit)*	0101 *(Daten, 4Bit)*

Damit der Empfänger den Erhalt der Daten quittieren kann, muss jedoch auch die Kennung des Senders im Rahmen enthalten sein:

0010 *(Kennung des Ziels)*	0001 *(Kennung der Quelle)*	0101 *(Daten)*

Der verschickte Rahmen lautet demnach:

0010 0001 0101

Um zu wissen, ob es sich bei den empfangenen Impulsen tatsächlich um eine gesendete Information handelt, wird ein Datenrahmen immer durch eine Präambel angekündigt. Es könnten sonst Missverständnisse durch Signalrauschen oder Störungen auftreten. Die endgültige Struktur eines Datenrahmens:

Präambel (7Byte)	SFD (1Byte)	Ziel (MAC)	Quelle (MAC)	Nutzdaten

6.1 Vollständiges Ethernet-Paket

Präambel 7	SFD 1	Ziel-Mac 6	Quell-MAC 6	Typ 2	Nutzdaten 46-1500	CRC 4

Zahlenwert im Feld = Bytegröße des Feldes.

6.2 Ethernet-Synchronisation

Um das Signal bei einer Übertragung zu synchronisieren wird vor jedem Ethernetframe eine Präambel und ein SFD(Start Frame Delimiter) gepackt. Die Präambel lautet *1010101010...* für 7 Byte und der SFD ist 1 Byte groß: *10101011*.

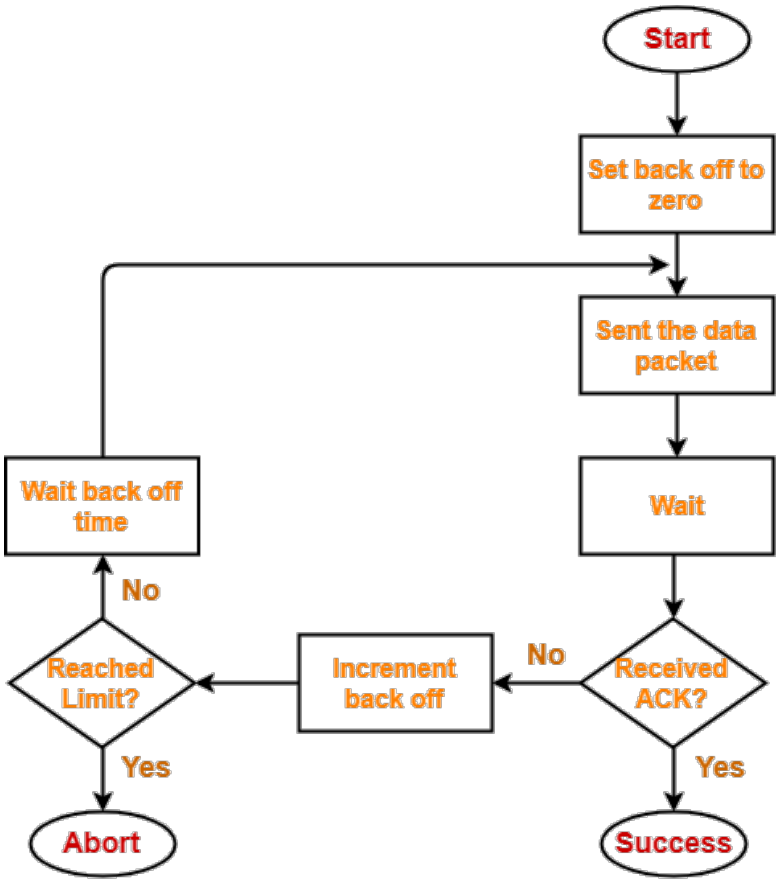
6.3 Power over Ethernet

Bei PoE werden netzwerkfähige Geräte über das achtadrige Ethernet-Kabel mit Strom versorgt.
Hauptvorteil von PoE ist, dass man ein Stromversorgungskabel einsparen kann und so auch an schwer zugänglichen Stellen oder in Bereichen, in denen viele Kabel stören würden, Ethernet-angebundene Geräte installieren kann. Die Stromversorgung zum Gerät muss nicht separat mit einem Stromkabel und Netzgerät zugeführt oder mit einer Batterie gelöst werden. Das Gerät bezieht die Energie stattdessen über das Datennetz. Dazu muss – meist an zentraler Stelle, im Netzwerkverteiler – neben den Datensignalen zusätzlich Strom in die Datenleitung eingespeist werden. Somit lassen sich einerseits zum Teil Installationskosten einsparen, andererseits kann der damit einfach zu realisierende Einsatz einer zentralen unterbrechungsfreien Stromversorgung (USV) die Ausfallsicherheit der angeschlossenen Geräte erhöhen.

7 Zugriffsverfahren

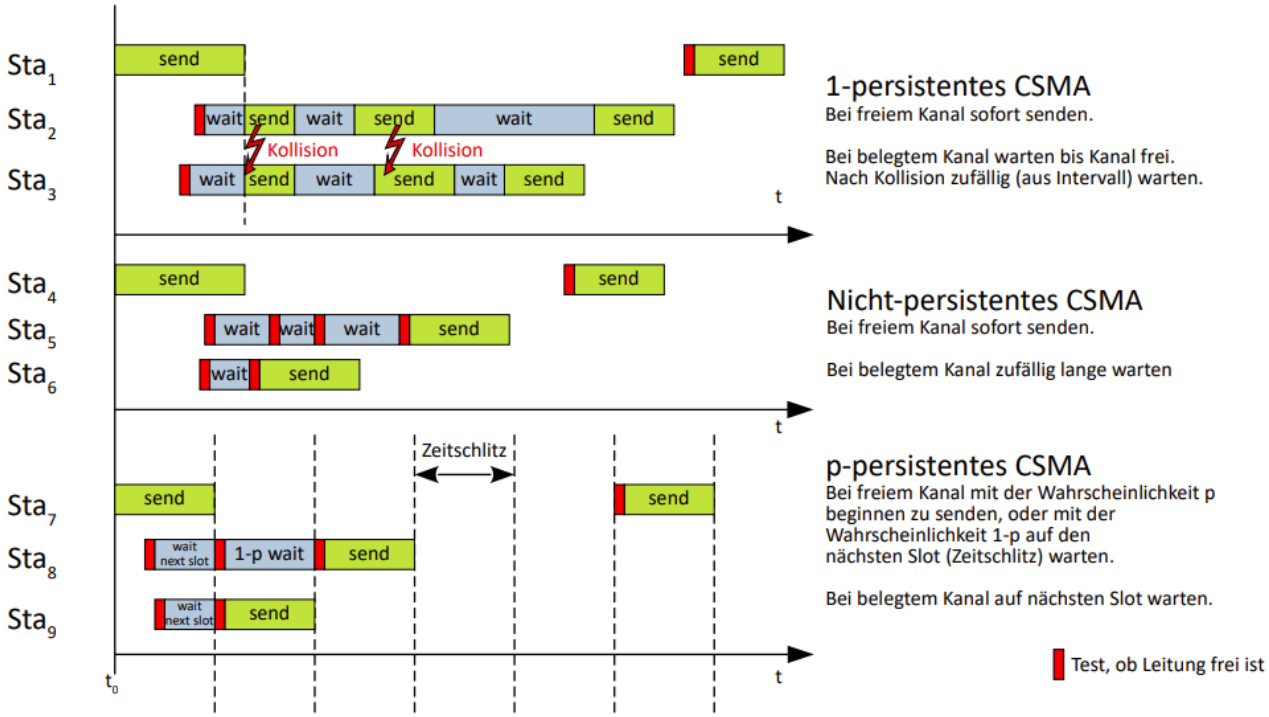
Bei geteilten Medium wird ein Zugriffsverfahren benötigt(außer Switch). Folgende Zugriffsverfahren stehen zur Auswahl:

7.1 ALOHA

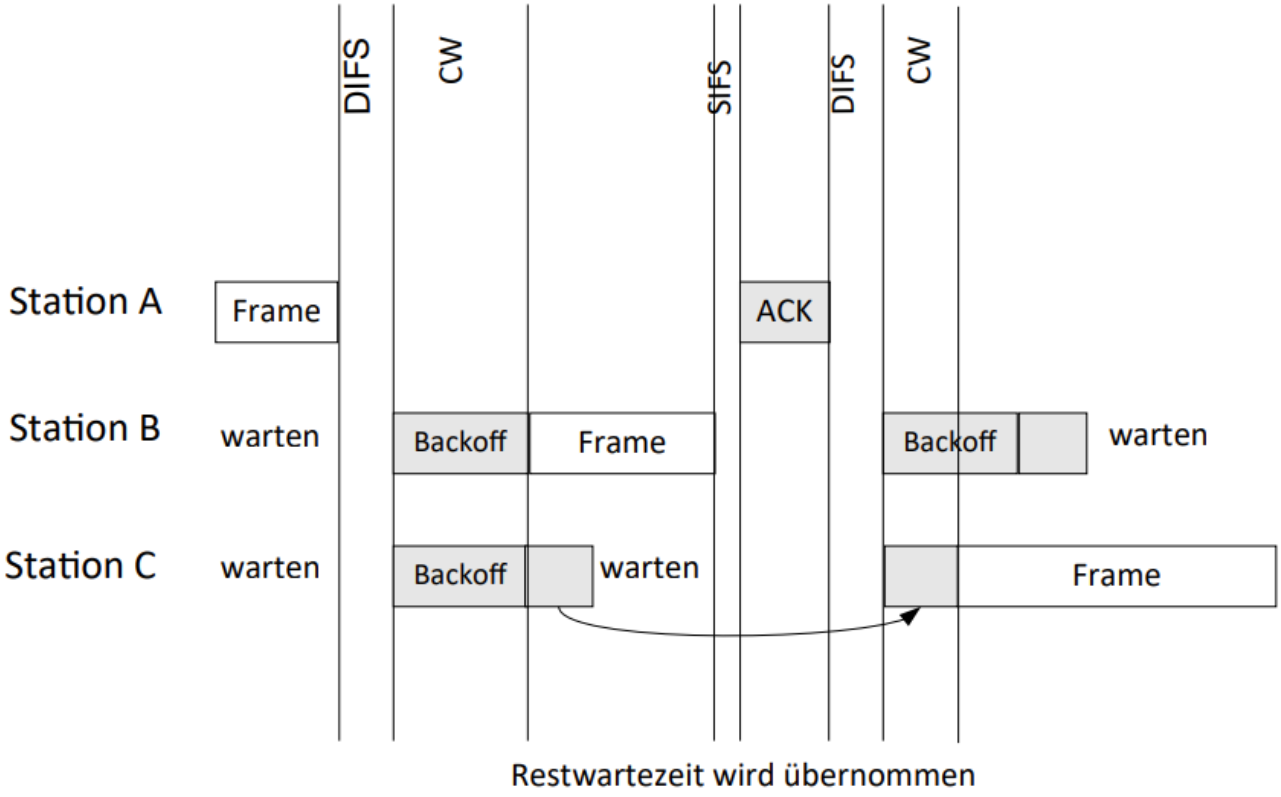


Flowchart for Pure Aloha

7.2 CSMA

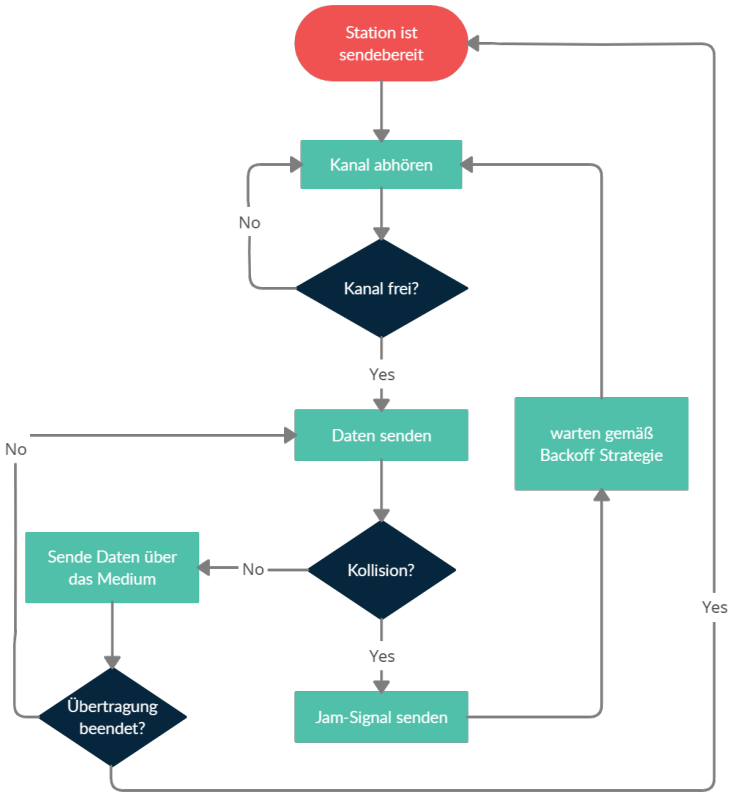


7.3 CSMA/CA



7.4 CSMA/CD - Verfahren

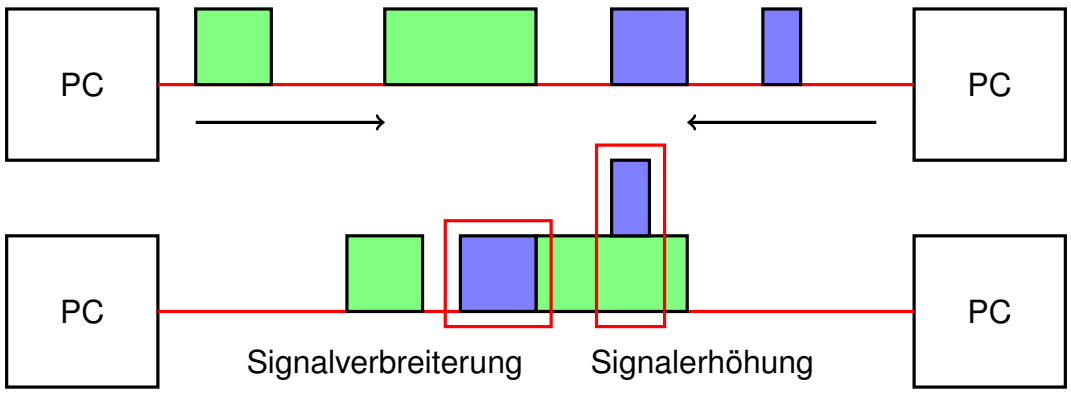
Programmablaufplan des CSMA/CD Verfahrens:



7.4.1 Kollision

Problem:
Da Alle Systeme mit nur einem Übertragungsmedium vernetzt sind, um Materialkosten zu sparen, und Skalierbarkeit zu erhalten, muss der Leiter bidirektional verwendet werden. Dadurch kann es zu Kollisionen von Impulsen kommen.
$\longrightarrow$ Es kommt zu einer Signalerhöhung / Signalverbreiterung und damit zu einer fehlerhaften Übertragung.

Lösung:
CSMA/CD Verfahren - Jam Signal **Situation:**



Das sendende System vergleicht ständig das gesendete Signal mit dem Signal auf der Leitung. Kommt es zu Abweichungen bricht das System die Übertragung ab und sendet ein

Jam-Signal welches andere Systeme im Netz über die Kollision informiert. Alle Systeme unterbrechen die Übertragung.
Ab wann dürfen die einzelnen Systeme wieder anfangen Daten zu senden?

Jedes Signal auf der Leitung braucht eine bestimmte Zeit, um zwischen den beiden entferntesten Systemen im Netz einmal hin, und wieder zurück zu laufen. Diese Zeit wird mit RTDT bezeichnet. Ist die RTDT abgelaufen, befinden sich keine Signale mehr im Netz, es kann neu gesendet werden.

Nach dem Ethernet-Standard 802.3 ist die RTDT auf 51,2 Mikrosekunden festgelegt.

Kommt es nach dem Warten der RTDT dennoch zu einer weiteren Kollision, variieren die Systeme ihre Wartezeit indem sie ein vielfaches der RTDT warten. Als Vielfaches können die Faktoren 0,1,2 und 3 gewählt werden.
$\longrightarrow$ Es wird unterschiedlich lang gewartet.

Kommt es erneut zu einer Kollision, wird der Bereich der Vorfaktoren von 0 bis 7 erweitert.

$$\text{Wartezeit} = k \cdot \text{RTDT}$$

k = 0 bis 2^i-1 i = Anzahl Versuche

Nach 10 Versuchen wird i nicht mehr erhöht, nach 16 erfolglosen Versuchen wird der Sendeversuch abgebrochen.

7.5 Token Ring

Bei Token Ring wird ein sog. Token im Kreis gelassen. An diesen heftet jeder Client seine Nachrichten an und und liest die für ihn vorgesehene Nachrichten. Der Token durchläuft hierbei die Staten *frei*, *belegt* und *gelesen*. Somit wird der Token erst wieder freigegeben, wenn der Sender die Rückmeldung gelesen erhalten. Wenn der Token nicht gelesen wurde und der Sender die Nachricht ungelesen zurück bekommt, setzt dieser den Token wieder frei.

8 Netzwerkprotokolle

Hat die Netzwerkkarte einen Datenrahmen empfangen, muss ermittelt werden, welches Protokoll zur Weiterverarbeitung verwendet werden soll. Innerhalb des Datenrahmens muss also der Typ und das Ziel der Daten festgelegt sein. Diese Informationen stehen in einem 2Byte großem Typenfeld. Für jedes Protokoll existiert eine eigene Kennung:

ARP	0x0806
IPv4	0x0800
IPv6	0x86DD

Allerdings kommt dem Typenfeld eine weitere Bedeutung:

Wert kleiner als 0x0600	Länge des Datenrahmens
Wert größer als 0x0600	Protokollkennung

Alle Protokollkennungen müssen also größer als 1536d oder 0x0600h sein!

Achtung:
Das ICMP Netzwerkprotokoll ist ein Protokoll der IP-Familie und folgt somit dem IPv4-Protokoll!
Ebenso gehört das ICMPv6 Netzwerkprotokoll zur IPv6 Familie und folgt somit auch dem IPv6 Protokoll!

8.1 Datenübertragung

Um sicher zu gehen, dass alle Informationen fehlerfrei übertragen wurden, wird dem Datenrahmen ein 4Byte großes Prüffeld (CRC) angehängt. Dieses Prüffeld ergibt sich aus einer Polynomdivision.

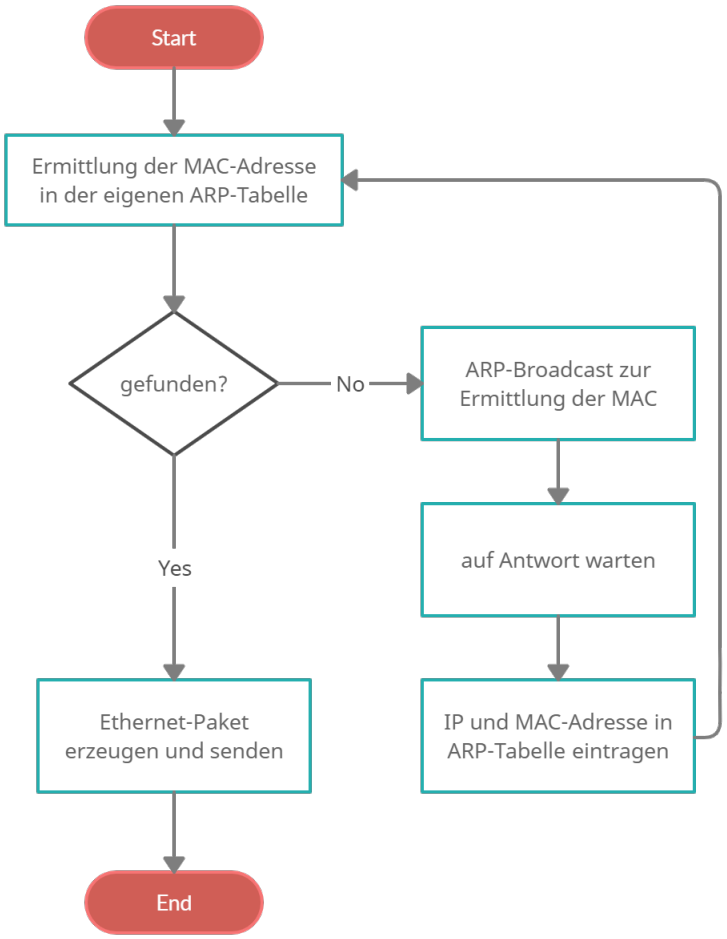
Präambel	SFD	Ziel-Mac	Quell-MAC	Typ	Nutzdaten	CRC

Unterschreitet der Anteil der Nutzdaten 46Byte, wird durch Padding aufgefüllt.

Min: 64Byte - Max: 1518Byte

9 ARP-Protokoll

Programmablaufplan des ARP Verfahrens:



10 DHCP

DHCP ist das Protokoll zur Vergabe der IP-Adressen an Router. Die meisten privat genutzten Router sind an einen DHCP Server gebunden der Ihnen jeden Tag eine neue IP-Adresse vergibt.

11 DNS - Domain Name System

DNS verwandelt URL's in IP-Adressen. Es funktioniert wie eine risige Tabelle in welches die URL's mit zugehöriger IP-Adresse gespeichert sind.

12 ICMP

Das Internet Control Message Protocol (ICMP) dient in Rechnernetzwerken dem Austausch von Informations- und Fehlermeldungen über das Internet-Protokoll in der Version 4 (IPv4). Für IPv6 existiert ein ähnliches Protokoll mit dem Namen ICMPv6.
ICMP ist Bestandteil von IPv4, wird aber wie ein eigenständiges Protokoll behandelt. Es wird von jedem Router und jedem Rechner erwartet, dass sie ICMP „verstehen“. Die meisten ICMP-Pakete enthalten Diagnose-Informationen: Sie werden vom Router zur Quelle zurückgeschickt, wenn der Router Pakete verwirft, etwa weil beispielsweise das Ziel nicht erreichbar ist oder die TTL abgelaufen ist.

13 VLANs

VLANs (Virtual Local Area Networks) unterteilen ein bestehendes einzelnes physisches Netzwerk in mehrere logische Netzwerke. Jedes VLAN bildet dabei eine eigene Broadcast-Domain. Eine Kommunikation zwischen zwei unterschiedlichen VLANs ist nur über einen Router möglich, der an beide VLANs angeschlossen ist.

14 Subnetting

Subnetting ermöglicht es Netzwerkadministratoren beispielsweise, das eigene Firmennetzwerk in Subnetze aufzuteilen, ohne dies im Internet bekannt zu machen. Das heißt, der Router, der schließlich das Netzwerk mit dem Internet verbindet, wird weiterhin als einfache Adresse angegeben.

Alle Subnetze eines Netzes funktionieren unabhängig voneinander und die Datenvermittlung läuft schneller. Warum ist das so? Subnetting macht das Netzwerk überschaubarer. Ein Broadcast, bei dem ein Teilnehmer Daten an das gesamte Netz sendet, verläuft ohne Ordnung durch Subnetze relativ unkontrolliert.

Durch Subnets werden Datenpakete durch den Router viel gezielter an die Empfänger geleitet. Befinden sich Sender und Empfänger im gleichen Subnetz, können die Informationen direkt zugestellt und müssen nicht umgeleitet werden.

14.1 Die IP Adresse

Bei dem Netzwerkprotokoll IPv4 (heute aktuell: IPv6) besteht eine IP-Adresse aus 32 Bit. Diese sind in vier Abschnitte mit je einem Oktett aufgeteilt.
Beispiel IP Adresse:

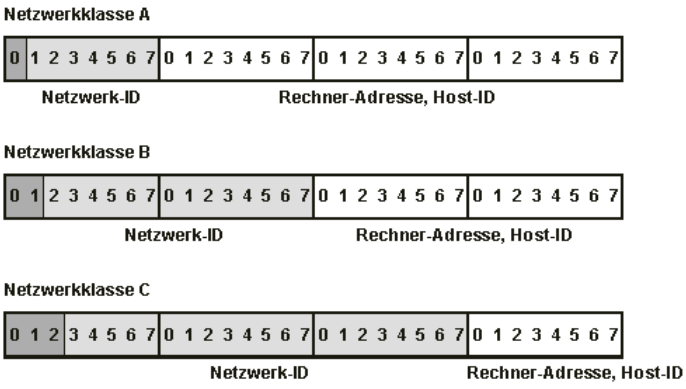
dezimal	192.168.0.1
binär	11000000.10101000.0000000.00000001

Zu beachten ist dabei, dass jedes Oktett als eigenständig bei der Berechnung der Wertigkeit angesehen wird.
Der höchste darstellbare Wert eines Oktettes beläuft sich demnach auf 255.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

14.2 Netzwerkklassen

Eine IP Adresse ist immer einem bestimmten System, welches sich in einem bestimmten Netz befindet zuzuordnen. Demnach besitzt eine IP Adresse einen Netzwerk und einen Hostbereich. Die IP Adresse muss dazu nicht in der Mitte geteilt sein (2 Oktette Netzwerk, 2 Oktette Hostbereich), sondern kann dazu beliebig zwischen jedem Bit geteilt werden. Netzen, mit 1 Oktett, 2 Oktetten und 3 Oktetten Netzwerkbereich wurden besondere Bezeichnungen zugewiesen:



14.3 Subnetzmaske

Um ein bestehendes Computernetz zur besseren Übersicht und Verwaltung in mehrere kleine Netze aufteilen zu können, bedarf es einer Subnetzmaske. Diese gibt den Netzwerkbereich einer IP Adresse an. Mit Hilfe der Subnetzmaske kann außerdem überprüft werden, ob sich zwei Geräte im gleichen Subnetz befinden oder nicht. Verknüpft man IP Adresse und Subnetzmaske durch eine AND Verknüpfung, erhält man die Netzwerkkennung des Subnetzes, indem sich die IP Adresse befindet. Stimmen die Netzwerkkennungen zweier Systeme überein, befinden sie sich im selben Subnetz.

14.4 CIDR

Die CIDR ist eine vereinfachte Schreibweise für die Subnetzmaske. Da eine Subnetzmaske dadurch definiert wird, dass sie in binär Schreibweise eine fortlaufende Kette von gesetzten

Bits haben muss, die nicht durch ein nicht gesetztes Bit unterbrochen werden darf, kann man die Schreibweise dahingehend vereinfachen, dass einfach die gesetzten Bits gezählt werden:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

In diesem Falle wäre die CIDR /17

14.5 VLSM bzw. Supernetting

VLSM ist ein erweitertes Subnetting. Hierzu wird die Subnetmaske in eine variable Länge gebracht um das Subnetz in mehrere verschieden große Teile zu unterteilen und sie hierarchisch nach ihrer Größe sortiert. Somit ist es möglich, Subnetze mit einer jeweils verschiedenen Anzahl an Hosts zu erschaffen, ohne dass dafür eine große Menge an IP-Adressen verschwendet werden muss.

Aufgabenstellung:

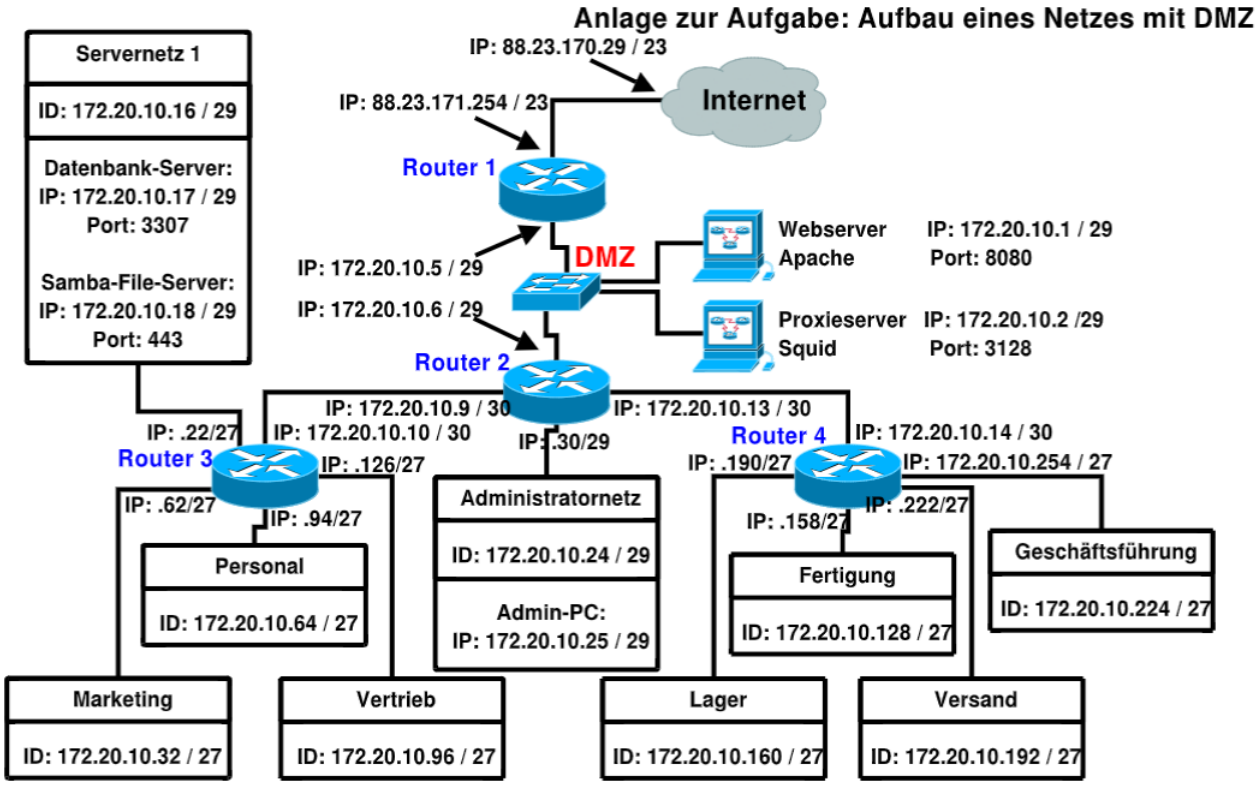
Es wird ein neues Gebäude gebaut. Dafür steht der IP-Bereich 11.137.4.0 /23 zur Verfügung. Die ersten 2 von den 6 Etagen sollen jeweils 100 IP-Adressen haben und die restlichen 4 jeweils 50 IP-Adressen. Gib die IP-Range jeder Etage ohne die jeweiligen Default Gateway- und Broadcast-Adressen an!

Lösung:

Etage	IP-Range
1	11.137.4.1 - 11.137.4.126
2	11.137.4.129 - 11.137.4.254
3	11.137.5.1 - 11.137.5.62
4	11.137.5.65 - 11.137.5.126
5	11.137.5.129 - 11.137.5.190
6	11.137.5.193 - 11.137.5.254

14.6 DMZ - Demilitarisierte Zone

Eine Demilitarisierte Zone bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server. Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze abgeschirmt.



15 IPv6

IPv6 ist die Fortsetzung von IPv4. Grund für die Einführung war, dass IPv4 zu wenige IP-Adressen vergeben konnte. Bei IPv6 sind die Adressen 128 bit lang und somit mehr als ausreichend. Bei IPv6 gibt es keine Checksumme mehr, da diese sowieso durch CRC schon kontrolliert wird. Ebenso können Packete nichtmehr fragmentiert werden und müssen beim Versenden schon in der richtigen Größe gewählt werden.
IPv6 Adressen besitzen einen Scope. Der Scope Link Local zum Beispiel stellt den Bereich von der Adresse bis zum Router dar, wobei der Scope Global Unique den gesamten Bereich bis zum externen Server/Host (mit Internet) darstellt. Außerdem gibt es keine Broadcast-Adressen mehr! Hierzu gibt es allerdings einen Ersatz. In IPv6 sind All-0 = All Zeros und All-1 = All Ones zunächst zulässige Werte für Adressen. Die vollständige All-0 und All-1 über alle Felder sind nach wie vor ungültig!
Eine unspezifizierte IPv6 Adresse sieht folgendermaßen aus:
:: bzw. ::/128

15.1 IPv6 und IPv4 im Vergleich

Vorteile und Nachteile von IPv6 zu IPv4:

Vorteile	Nachteile
128 Bit = 2^{128} Adressen	Wenn jedes Gerät eine feste, statische Adresse bekommt, kommt es evtl. zu Sicherheitsrisiken
NAT wird nichtmehr gebraucht	
Broadcast-Adressen werden nichtmehr gebraucht	
ARP wird nichtmehr gebraucht	
bis zu 4GiB Datenversandt	
verbessertes Multicast	

15.2 IPv4 Adresse im IPv6 Format

Unter IPv6 genutzte IPv4 -Adressen
x:x:x:x:x:d.d.d.d
x entspricht einem 16-Bit-Hexadezimalwert (0 – FFFF) auf der höherwertigen Seite der Adresse.
d entspricht einem 8-Bit-Dezimalwert (0 – 255) auf der niederwertigen Seite der Adresse.
Diese Schreibweise dient nur der internen Darstellung und wird nie als Quell- oder Zieladresse versendet!

0:0:0:0:0:0:d.d.d.d

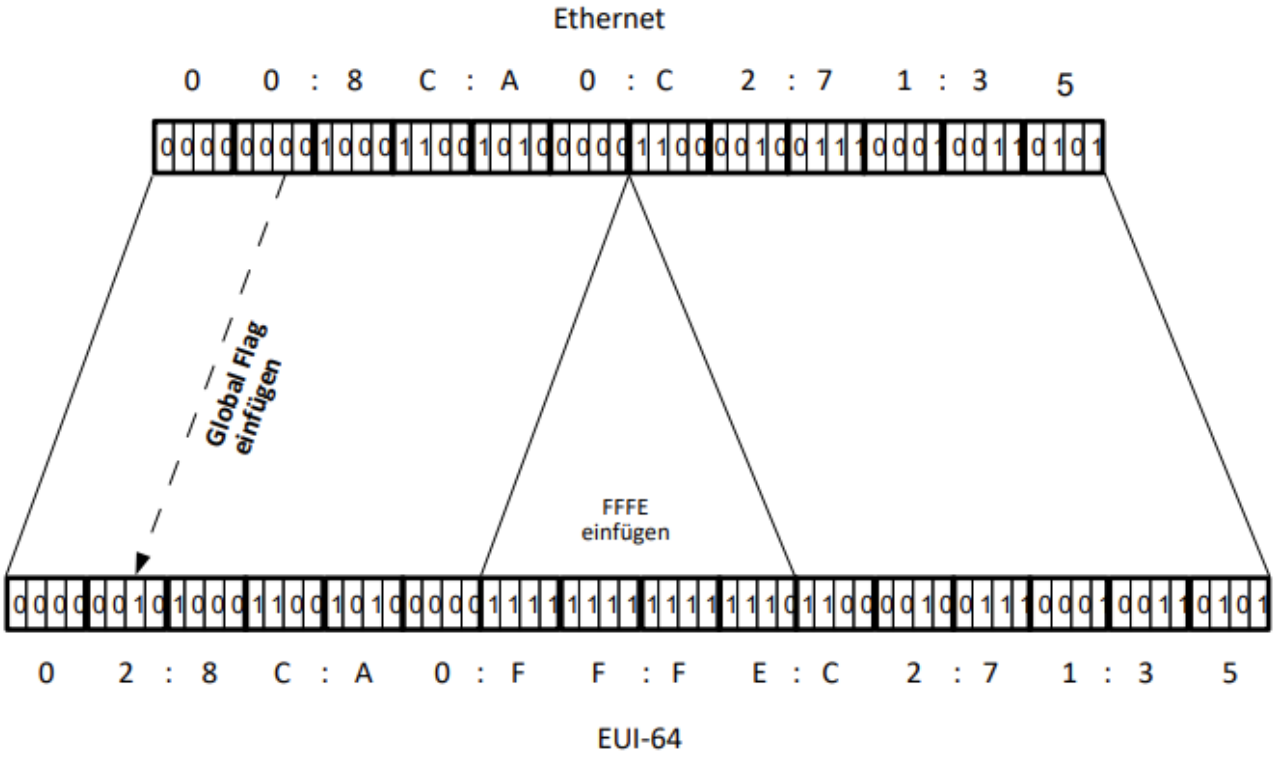
Beispiel:
::abba:815 = 0:0:0:0:0:0:171.186.8.21 = ::171.186.8.21

IPv4-mapped IPv6-Adresse
Hierbei sind die ersten 80 Bits auf 0 gesetzt.
Danach werden die nächsten 16 Bits auf 1 gesetzt.

Beispiel:

Ausgeschriebene Form	Komprimierte Form
0:0:0:0:0:ffff.129.144.52.38	::ffff.129.144.52.38

15.3 IPv6: EUI-64-MAC-Adressen

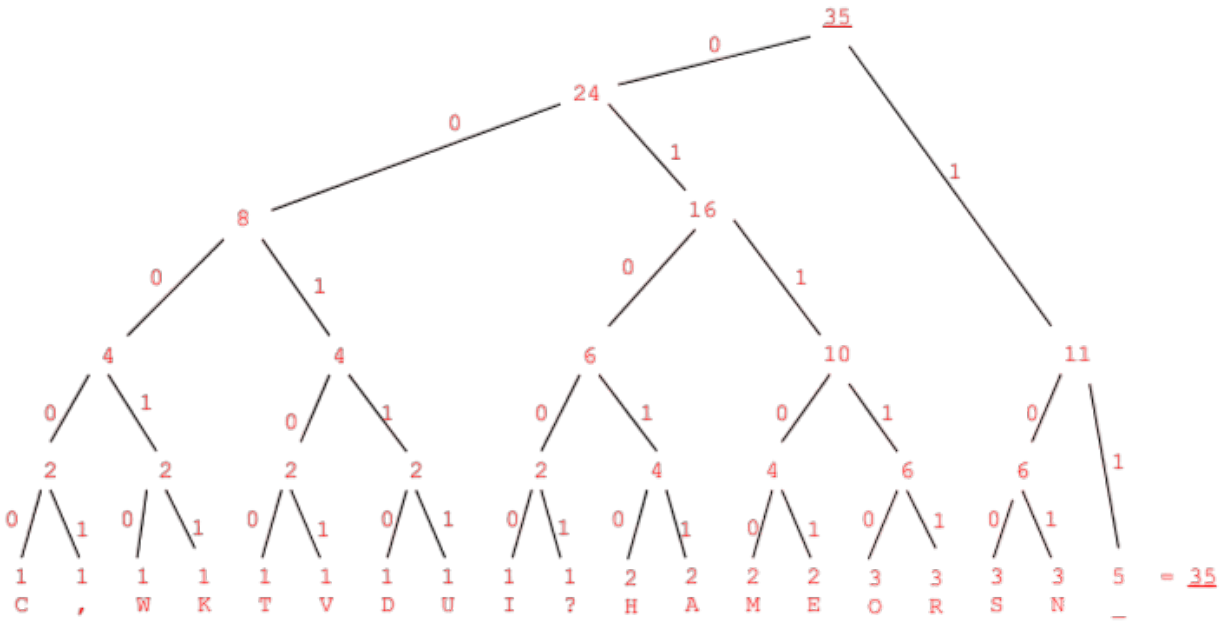


16 Codierung

16.1 Huffmann-Codierung

Algorithmus zum **Komprimieren** von Dateien.
Idee: Häufige Zeichen kurze Bit-Codierung, sodass Binär-Codierung möglichst kurz ist.

1. **Tabelle** mit vorkommenden Zeichen und deren Häuffigkeit erstellen
2. **Binärbaum** mit Zeichen erstellen. Zeichen nach Häufigkeit sortiert. Zeichen mit geringster Häufigkeit zusammenfassen. Zusammengefasste zeichen weiter vereinen bis Baum vollständig ist
3. **Codierung** der Zeichen aus Binärbaum lesen und in Tabelle schreiben



16.2 Channel Coding

16.2.1 Fehlererkennung mit Paritätsbits

Code ohne Parität		Code mit Parität	
Hexadezimal-Darstellung	Binär-Darstellung	Gerade Parität	Ungerade Parität
0	0000	00000	00001
1	0001	00011	00010
2	0010	00101	00100
3	0011	00110	00111
4	0100	01001	01000
5	0101	01010	01011
6	0110	01100	01101
7	0111	01111	01110
8	1000	10001	10000
9	1001	10010	10011
A	1010	10100	10101
B	1011	10111	10110
C	1100	11000	11001
D	1101	11011	11010
E	1110	11101	11100
F	1111	11110	11111

16.2.2 Fehlererkennung mit Hamming Distanz

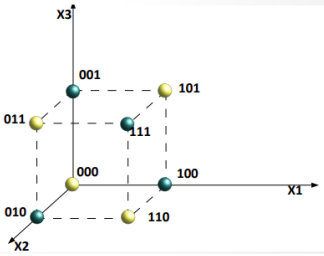
Die Distanz zweier Codewörter ist die Anzahl der Bits in denen sich die beiden Codewörter unterscheiden.
So haben die Codewörter 0000 und 1111 die Distanz 4.
Die Codewörter 0000 und 0001 haben die Distanz 1.
Die Hamming-Distanz ist der minimale Abstand aller möglichen Codewörter eines Codes.

Allgemein gilt:
Die Fehlererkennungs- und -korrektureigenschaften eines Codes hängen von seinem Hamming Abstand ab.

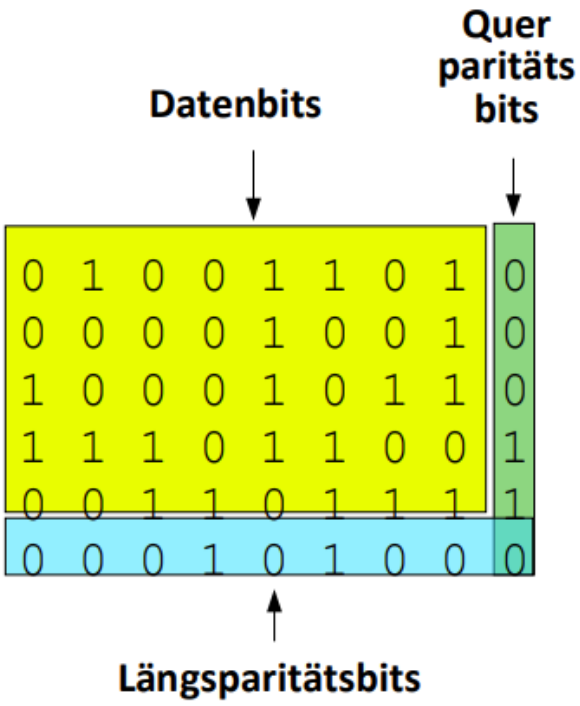
Zum Auffinden von d Fehlern benötigt man einen Hamming-Abstand von d + 1.
Zur Korrektur von d Fehlern braucht man einen Hamming-Abstand von 2d + 1.

Wird ein 2 Bit-Binärcode um ein Prüfbit erweitert, entsteht folgende Zuordnung:
2 Bit-Binärcode + Parity-Bit -> 3 Bit-Binärcode

00	0	000 \	
01	1	011 |	gültige Codes
10	1	101 |	
11	0	110 /	
		001 \	
		010 |	ungültige Codes
		100 |	
		111 /	



16.2.3 Fehlererkennung mit 2-dimensionaler Parität



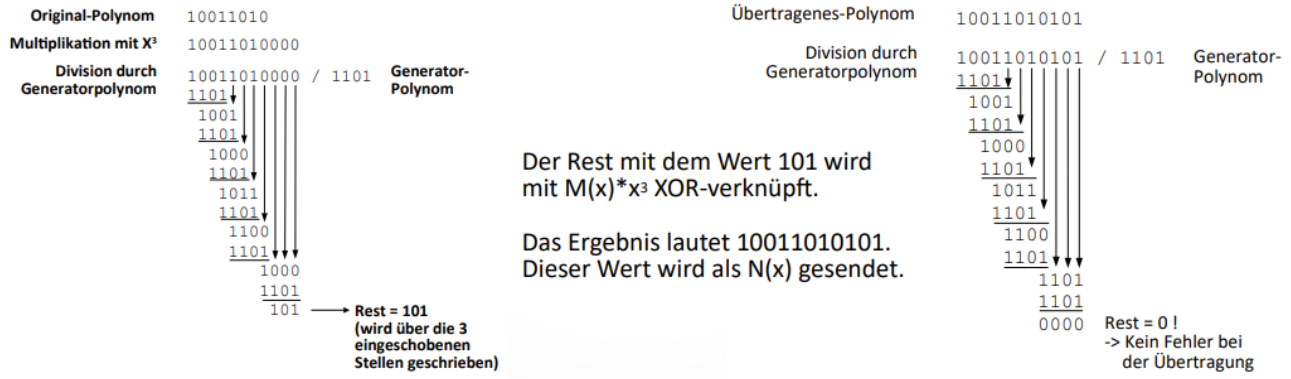
16.2.4 Fehlererkennung mit CRC(Cyclic Redundancy Check)

Beispiel

Wir haben eine 8-Bit-Nachricht M. Ihr wert sei 10011010.
Das entspricht folgendem Polynom.
$M(x)= 1*x^7 + 0*x^6 + 0*x^5 + 1*x^4 + 1*x^3 + 0*x^2 + 1*x^1 + 0*x^0 = x^7 + x^4 + x^3 + x^1$

Das Generatorpolynom G sei vom Grad 3.
$G(x) = x^3 + x^2 + x^0$ In diesem Beispiel sei G(x) = 1101.

Da das Generatorpolynom vom Grad 3 ist, wird M(x) zuerst mit x^3 multipliziert denn .
Dies entspricht einer Verschiebung um 3 Stellen nach links.
Damit wird aus :10011010 der Wert 10011010000.
Danach wird M(x) durch G(x) dividiert, was einer blockweisen XOR-Operation entspricht.



Der Rest mit dem Wert 101 wird mit $M(x)*x^3$ XOR-verknüpft.

Das Ergebnis lautet 10011010101.
Dieser Wert wird als N(x) gesendet.

Übliche CRC-Generatorpolynome sind:

CRC	C(x) Generatorpolynom
CRC-8	$X^8 + X^2 + X^1 + 1$
CRC-10	$X^{10} + X^9 + X^5 + X^4 + X + 1$
CRC-12	$X^{12} + X^{11} + X^3 + X^2 + 1$
CRC-16	$X^{16} + X^{15} + X^2 + 1$
CRC-CCITT	$X^{16} + X^{15} + X^5 + 1$