Netztechnik

Robin Rausch, Florian Maslowski

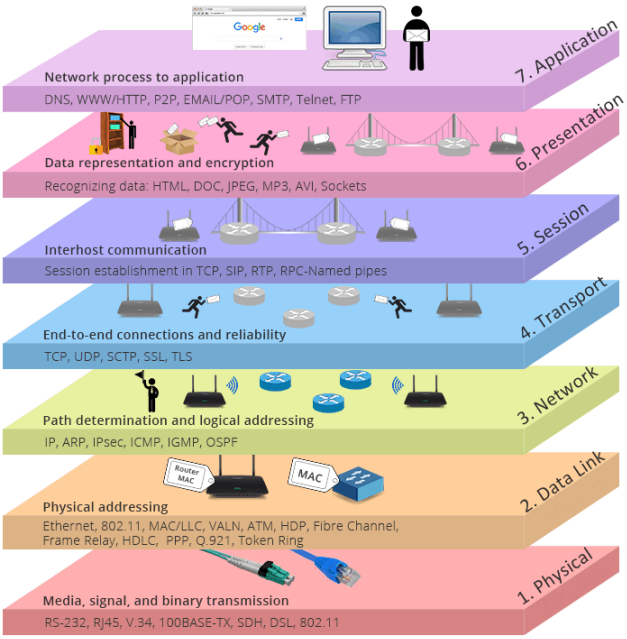
9. November 2022

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 Protokolle (+Zuordnung)

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

Die Schicht 3 beschreibt das Routing in einem Netzwerk. Darunter fallen beispielsweise Switches. ??

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

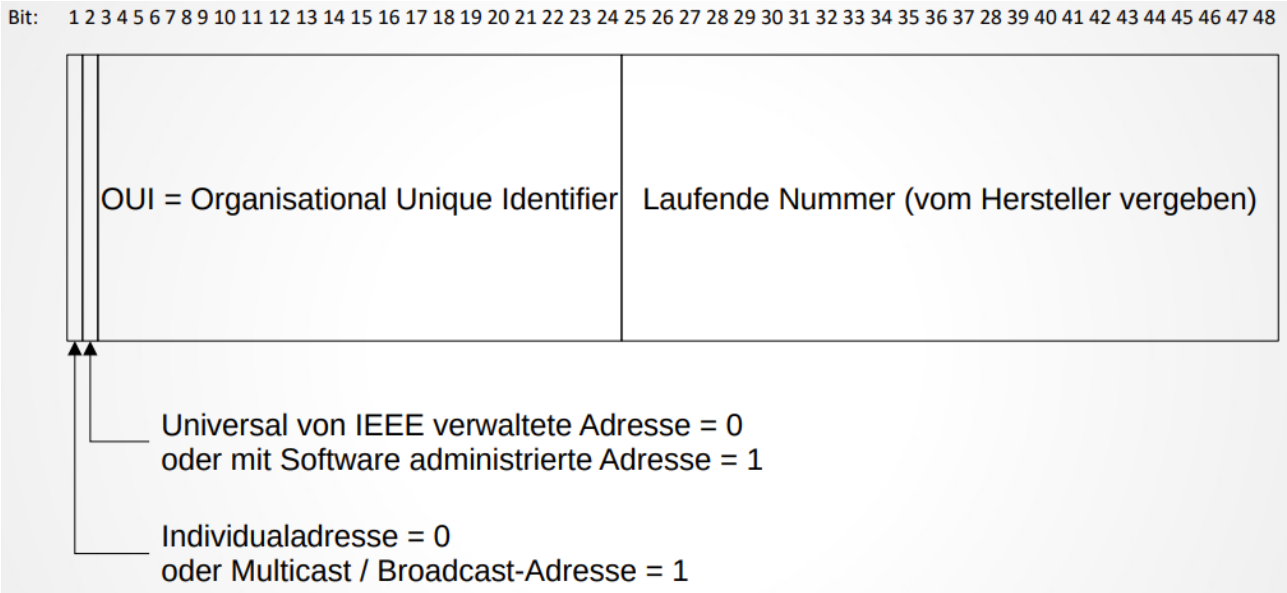
Unterschiedliche Rechner haben aufgrund unterschiedlicher Betriebssysteme unterschiedliche Darstellungsformen der Daten. Soll eine Applikation auf unterschiedlichen Betriebssystemen ablaufen können, sind Konvertierungen durchzuführen. Hier werden folgende Umsetzungen abgewickelt:
Zeichensätze (ASCII, 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

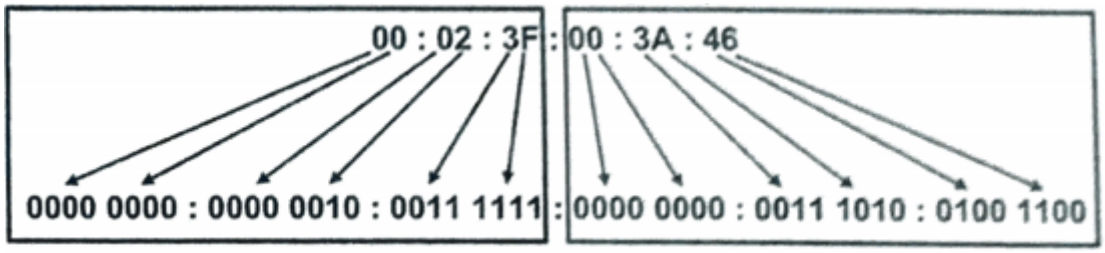
Diese Schicht bildet die Schnittstelle zum Anwender (User). Beispiel hierfür sind:
FTP File Transfer Protocol, SMTP Simple Mail Transfer Protocol, SNMP Simple Network Management Protocol und DNS Domain Name Service

2 MAC-Adresse

Um Informationen im Ether / Internet zuverlässig und zielgenau verschicken zu können, muss jedes Endgerät im Netz seine eigene individuelle Kennung besitzen!
$\longrightarrow$ *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:



3 Byte OUI (Herstellerkennung) 3Byte Gerät-Seriennummer

3 Netze

3.1 Netzwerk-Topologien

3.2 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

3.3 Subnetting

3.4 Switch

3.4.1 Spanning Tree

Switche haben Hierarchie beim Weiterleiten von Paketen. Kleine Priorität ist besser. Falls Priorität gleich, entscheidet höhere MAC-Adresse die bevorzugte Switch
Switche geben Pakete nur an Switche mit geringerer Priorität oder höherer 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

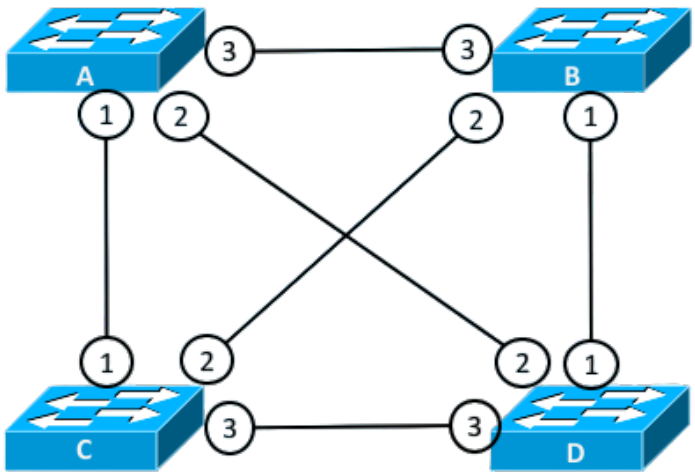
Designated-Port Zu Switch mit besserer Priorität oder höherer MAC-Adresse als die eigene

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

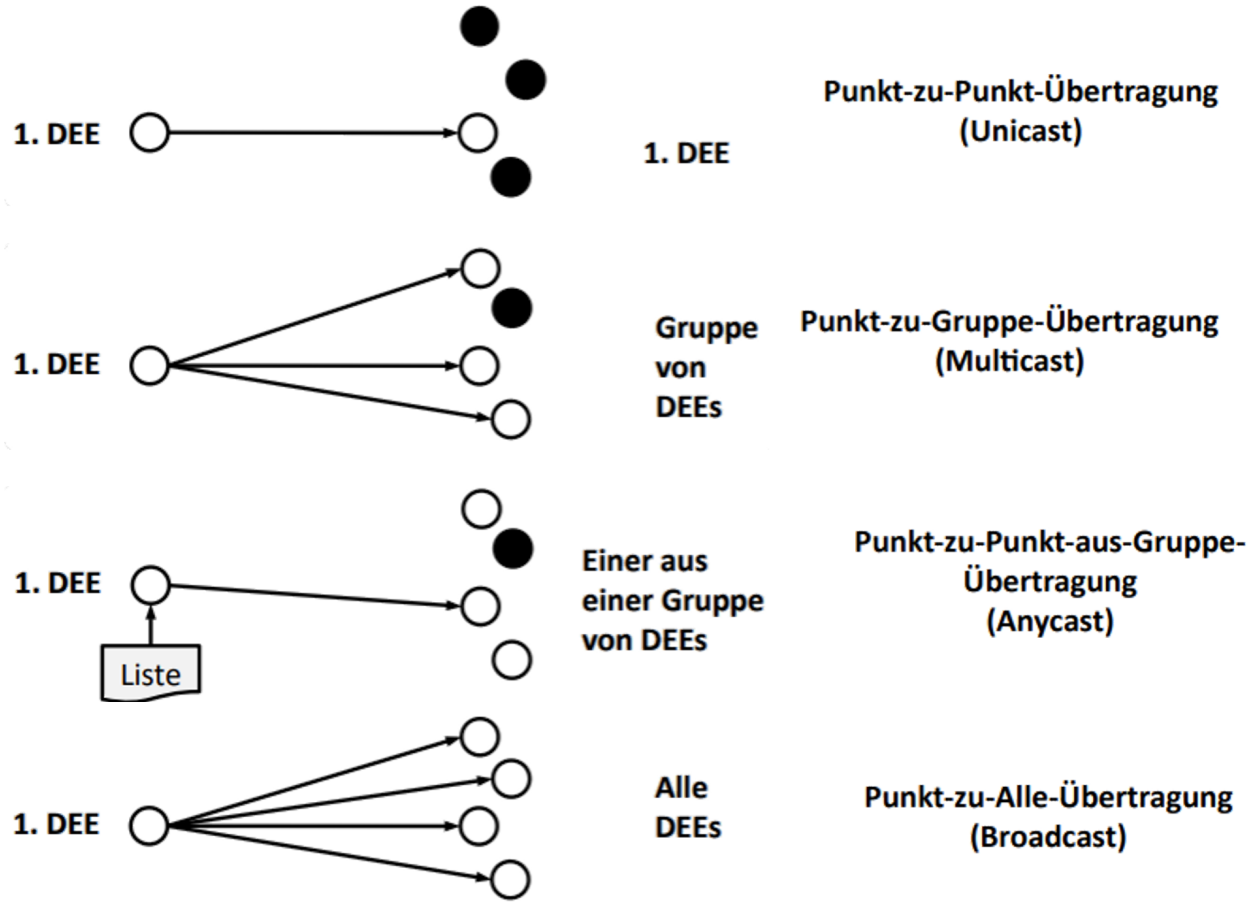


Prio:
32768
MAC:
08-00-0C-00-00-0C

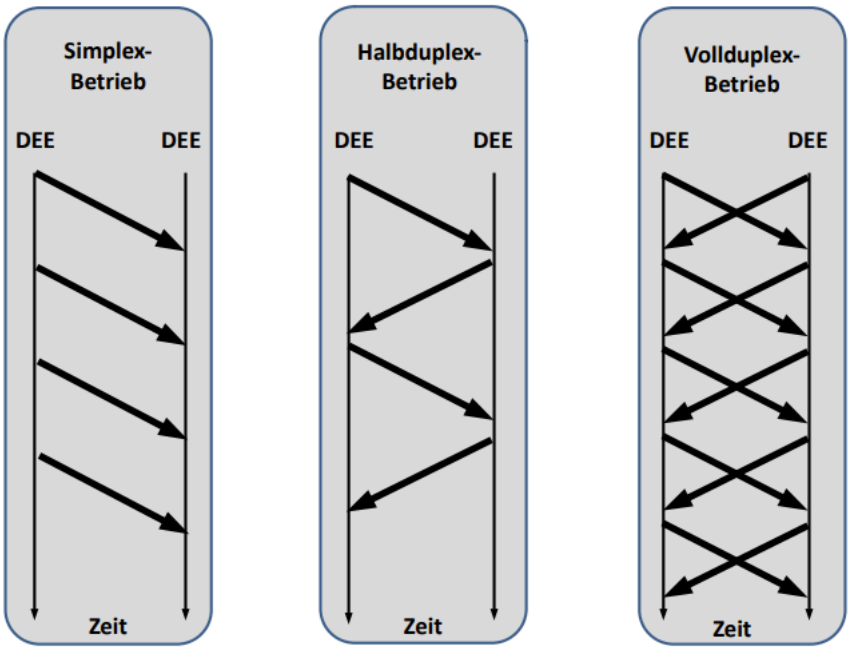
Prio:
32768
MAC:
08-00-0C-00-00-0D

4 Kabel

4.1 Verkehrsarten



4.2 Betriebsarten



4.3 Kabelarten:

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

LWL Lichtwellenleiter/Glasfaserkabel hohe Geschwindigkeit, teuer, Aufwand in Spannung zurückzuwandeln.

4.4 Verkablungsarten:

Primarverkabelung: Für Verkabelung von Gebäuden mit LWL

Sekundärverkabelung: Für Verkabelung von Etagen mit LWL

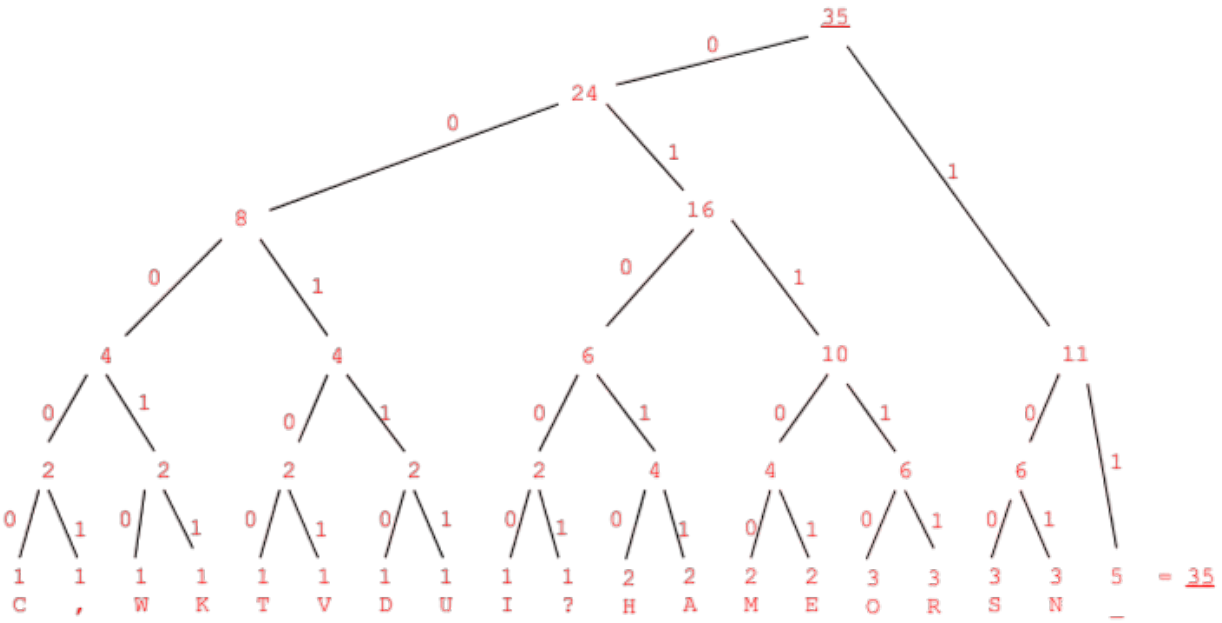
Tertiärverkabelung: Für Verkabelung innerhalb einer Etage mit Kupferkabel

5 Codierung

5.1 Huffmann-Codierung

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

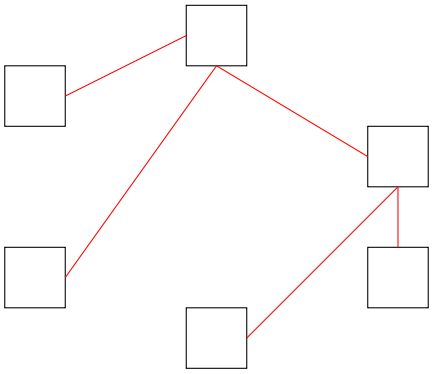
1. **Tabelle** mit vorkommenden Zeichen und deren Häuffigkeit erstellen
2. **Binärbaum** mit Zeichen erstellen. Zeichen nach Häufigkeit sortiert. Zeichen mit geringster Häufigkeit zusammenfassen. Zusammengefasste zeichen weiter vereinen bis Baum vollständig ist
3. **Codierung** der Zeichen aus Binärbaum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


35
24
11
8
16
4
4
6
10
2
2
2
2
2
4
4
6
6
1 C
1 ,
1 W
1 K
1 T
1 V
1 D
1 U
1 I
1 ?
2 H
2 A
2 M
2 E
3 O
3 R
3 S
3 N
5 _
= 35

6 Netze

6.0.1 Netz Topologien

Baum Topologie



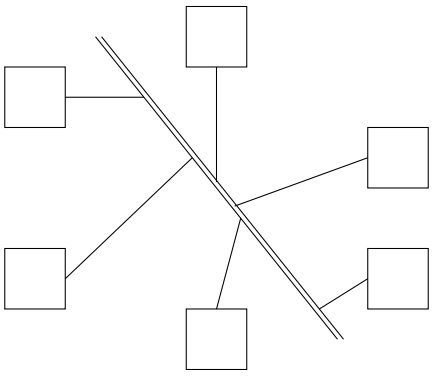
Vorteile:

- 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



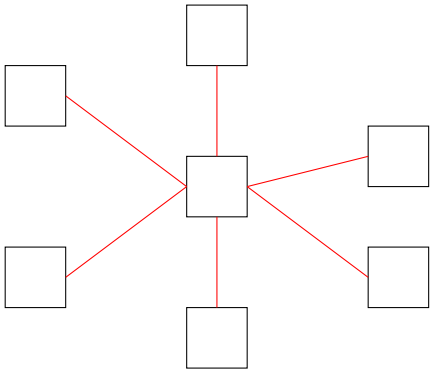
Vorteile:

- hohe Ausfallsicherheit
- leichte Skalierbarkeit

Nachteile:

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

Stern Topologie



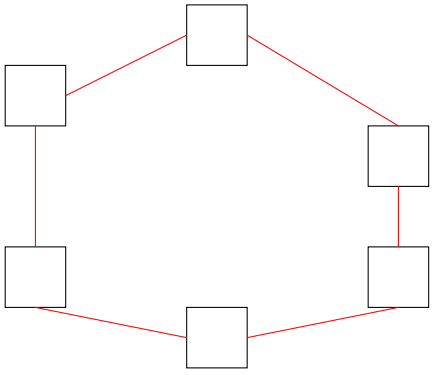
Vorteile:

- 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

6.0.2 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.

6.0.3 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.

6.1 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)

6.2 Kommunikationsarten

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

6.3 Netzwerkkomponenten

6.3.1 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.

6.3.2 Client

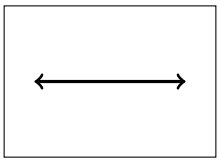
Der Client stellt einen Rechner im Netz dar. Er simuliert einen Computer an einem gewissen Standpunkt. Der Client besitzt eine Network-Interface-Card.

6.3.3 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.

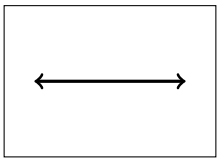
6.3.4 Repeater

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.



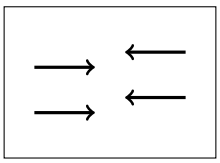
6.3.5 HUB

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



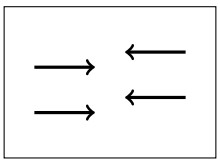
6.3.6 Bridge

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



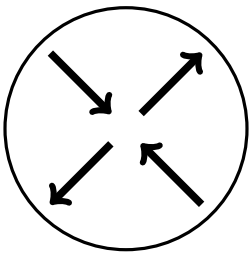
6.3.7 Switch

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.



6.3.8 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.



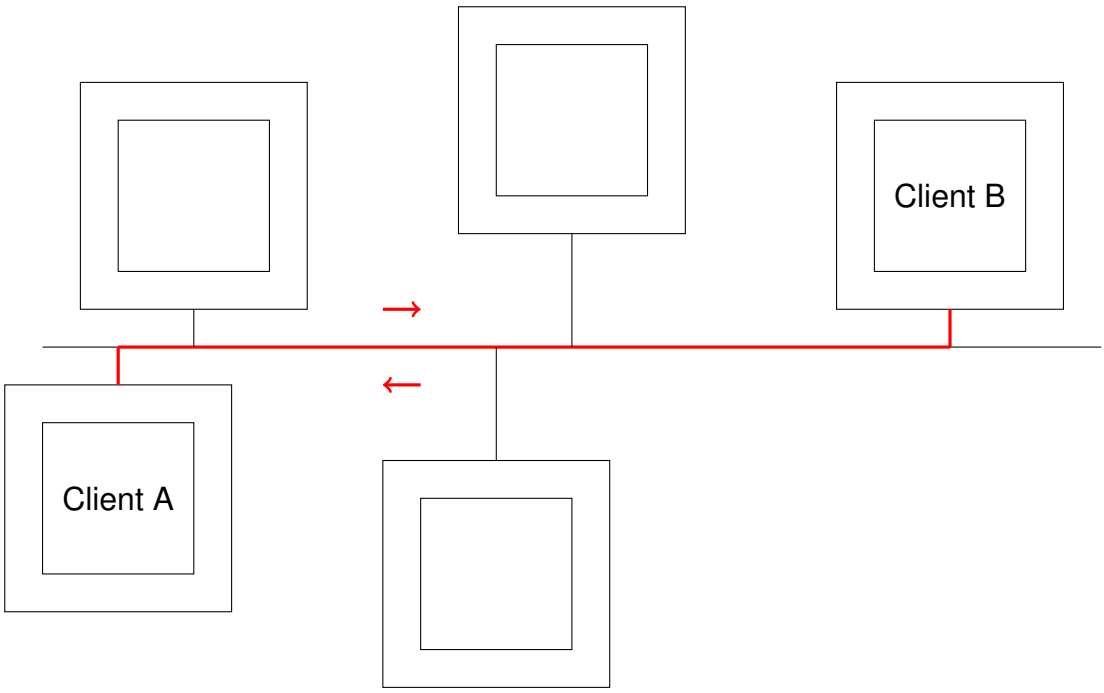
6.3.9 Einordnung der Komponenten ins OSI-Modell

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

6.4 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.



6.5 Bezeichnungen von Netzen

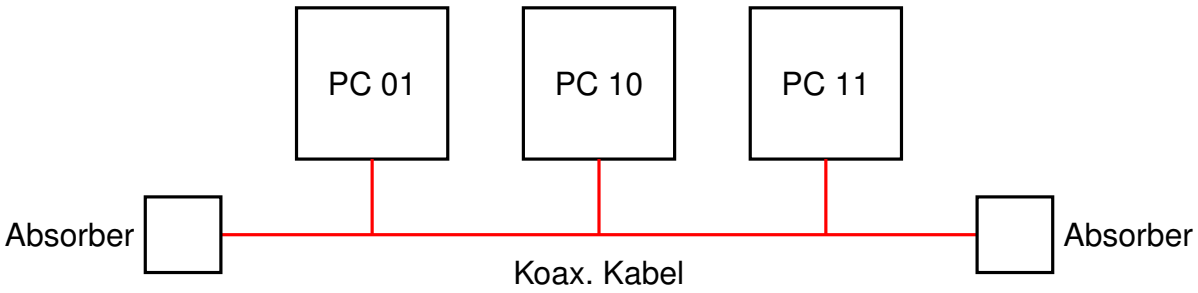
Tabelle 1: Bezeichnungen von Netzen

Abkürzung	Beschreibung	Kabellänge	Anwendungen
CAN	Control Area Network	5km	Steuerungstechnik
PAN	Personal Area Network	100m	Handynetz
LAN	Local Area Network	100m	Home Netz
MAN	Metropolitan Area Network	100km	Unternehmen mit mehreren Standorten
WAN	Worldwide Area Network	Weltweit	Internet, Telefon

7 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

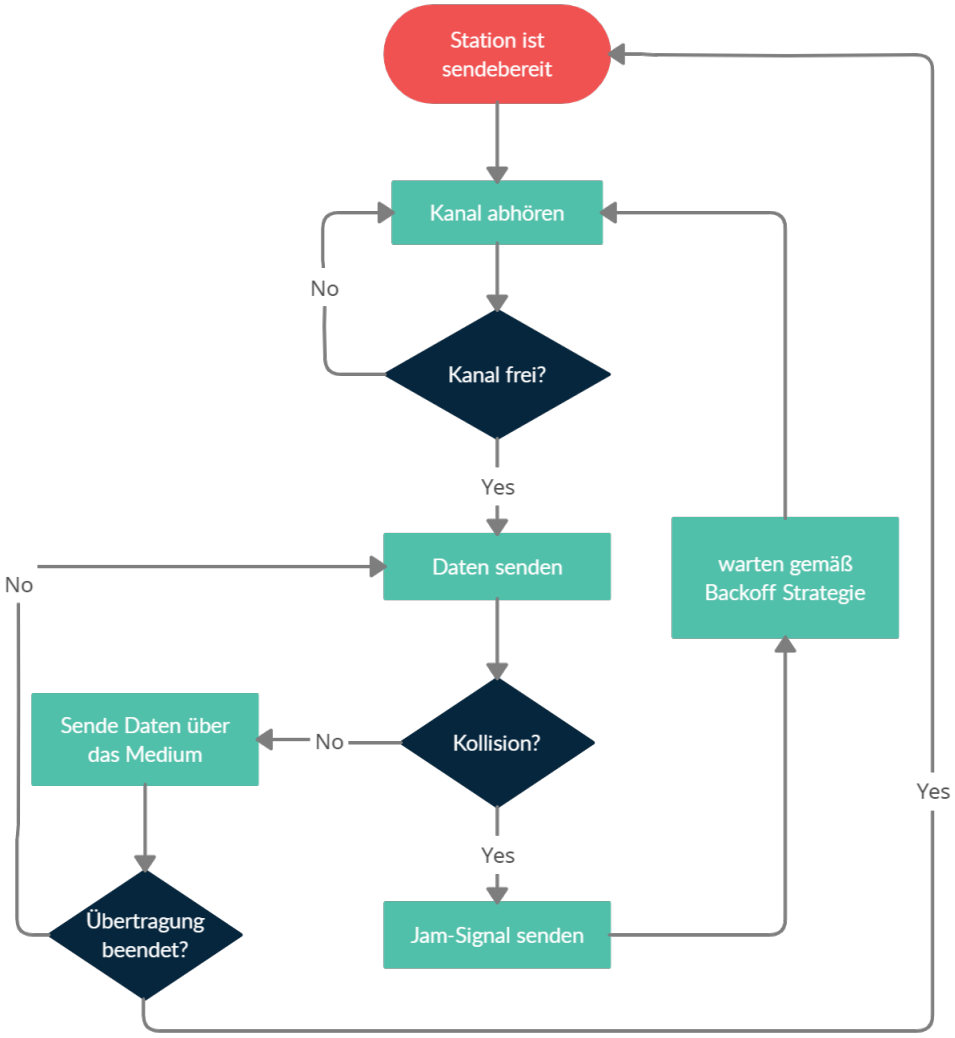
7.1 Vollständiges Ethernet-Paket

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

Zahlenwert im Feld = Bytegröße des Feldes.

7.2 CSMA/CD - Verfahren

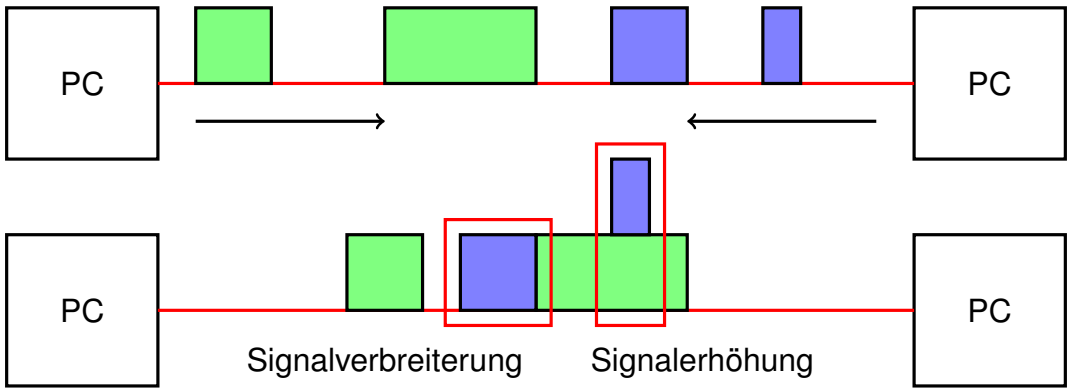
Programmablaufplan des CSMA/CD Verfahrens:



7.2.1 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 RTT bezeichnet. Ist die RTT abgelaufen, befinden sich keine Signale mehr im Netz, es kann neu gesendet werden.

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

Kommt es nach dem Warten der RTT dennoch zu einer weiteren Kollision, variieren die Systeme ihre Wartezeit indem sie ein vielfaches der RTT 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.

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

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.

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:

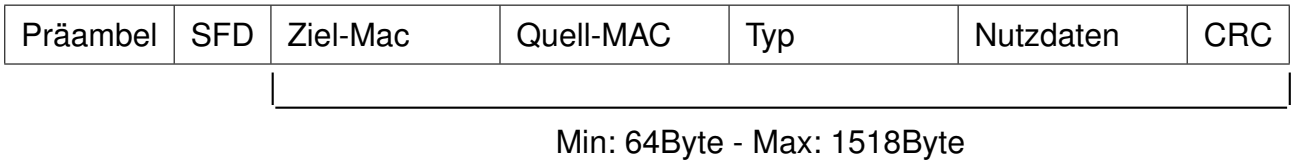
Wert kleiner als 0x0600	Länge des Datenrahmens
Wert größer als 0x0600	Protokollkennung

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

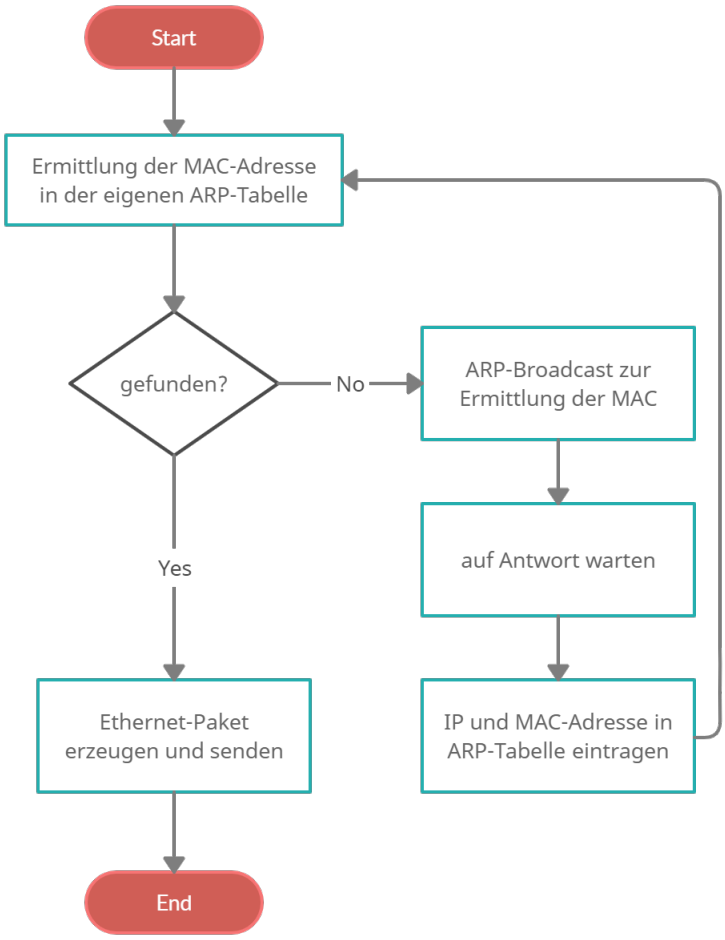
Um sicher zu gehen, dass alle Informationen fehlerfrei übertragen wurden, wird dem Datenrahmen ein 4Byte großes Prüffeld (CRC) angehängt. Dieses Prüffeld ergibt sich aus einer Polynomdivision.



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

9 ARP-Protokoll

Programmablaufplan des ARP Verfahrens:



10 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.

10.1 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:

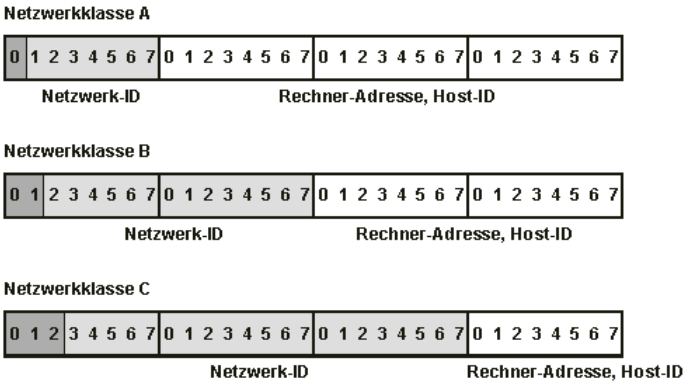
dezimal	192.168.0.1
binär	11000000.10101000.0000000.00000001

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

10.2 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:



10.3 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.

10.4 CIDAR

Die CIDAR 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 CIDAR /17

10.5 VLSM

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:

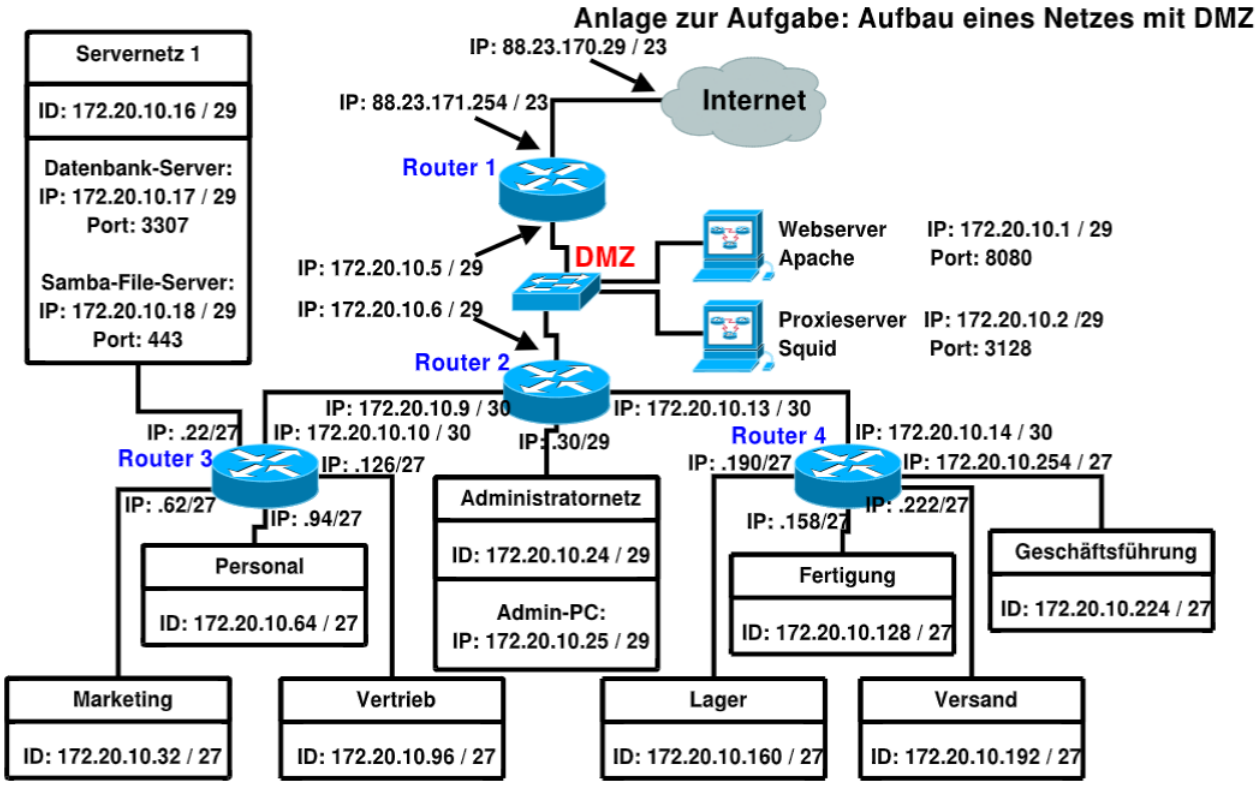
Es wird ein neues Gebäude gebaut. Dafür steht der IP-Bereich 11.137.4.0 /23 zur Verfügung. Die ersten 2 von den 6 Etagen sollen jeweils 100 IP-Adressen haben und die restlichen 4 jeweils 50 IP-Adressen. Gib die IP-Range jeder Etage an!

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

10.6 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.



10.7 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	