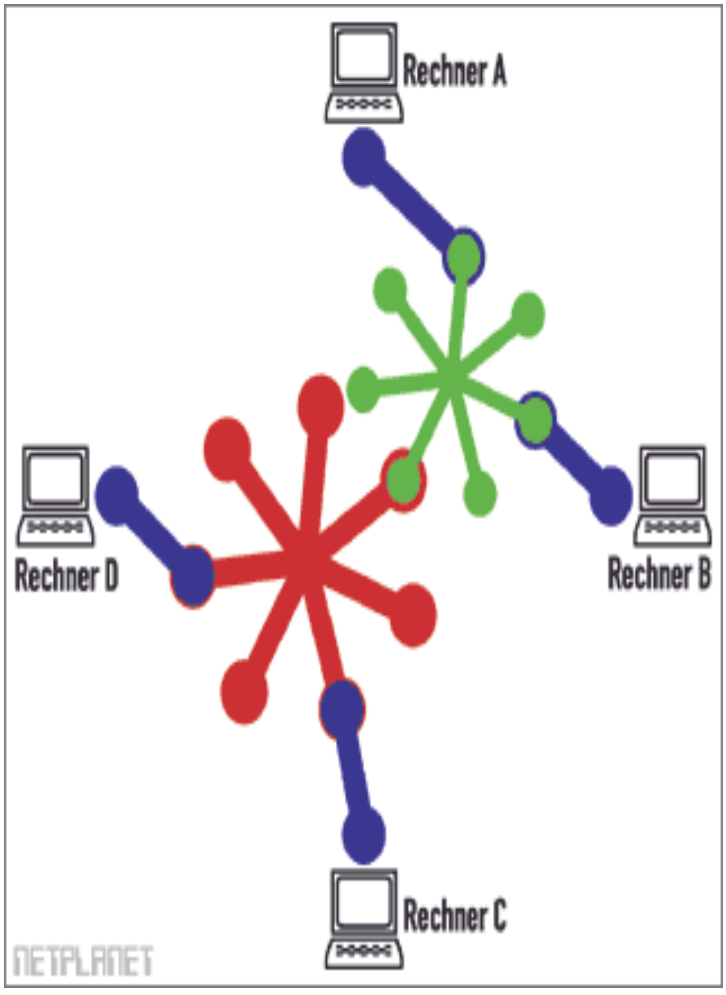
Protokolle

- Damit Computer einander "verstehen"
- Codierungsvorschriften für Daten und Ablaufbeschreibungen
- Kommunizierende Computer müssen das gleiche Protokoll anwenden



Beispiele für bekannte Netze, Dienste und Protokolle

Internet

- Das Internet ist bezüglich der Geräte und Verbindungskomponenten kein eindeutig identifizierbares Rechnernetz.
- Es ist ein weltumspannendes, offenes Netz, das auf der Verwendung der TCP/IP-Protokollen* und den dazu gehörenden Diensten basiert.
- Ein auf TCP/IP-Protokollen und Diensten aufbauendes Rechnernetz innerhalb eines Unternehmens wird Intranet genannt.

* TCP = Transmission Control Protocol
  IP = Internet Protocol

Bekannte Internetdienste und ihre Protokolle

- Die drei populärsten Dienste auf dem Internet sind: **E-Mail**, **WWW** und **File Transfer (FTP)**.
- Die dazu gehörenden Protokolle sind:

  SMTP (Simple Mail Transfer Protocol) für E-Mail.

  HTTP (Hypertext Transfer Protocol) für das World Wide Web.

  FTP (File Transfer Protocol) für das Übermitteln von Dateien.
- Moderne Browser verstehen alle drei Protokolle und können somit Mail-Server, WWW-Server und FTP-Server ansprechen.

Protokolle der verschiedenen Schichten

Schicht 7: Anwendung	Telnet, FTP, HTTP, SMTP
Schicht 6: Darstellung	Telnet, FTP, HTTP, SMTP, NetBIOS
Schicht 5: Kommunikation	TFTP, Telnet, FTP, HTTP, SMTP, NetBIOS
Schicht 4: Transport	TCP, UDP, SPX, NetBEUI
Schicht 3: Vermittlung	IP, IPX, X.25, NetBEUI, AppleTalk-over-IP
Schicht 2: Sicherung	LLC/MAC, ARP, Ethernet
Schicht 1: Übertragung	Ethernet, Token Ring, FDDI, X.25, Frame Relay.

Identifikation in der Bitübertragungsschicht : Hardwareadresse des PCs (-> MAC-Adresse)

- Jede Netzwerkkarte erhält vom Hersteller eine zwölfstellige, hexadezimale, Hardwareadresse. (Media Access Control address, z.B. 00 04 7D B5 90 F4)
- Kooperation der Hersteller stellt sicher, dass diese Adresse weltweit eindeutig ist.
- Diese Hardwareadresse ist **nicht** mit der IP-Adresse (z.B. 129.132.17.9) zu verwechseln, für deren Vergabe sie die Grundlage ist (Vermittlungsschicht).

arp –a : anzeigen des arp - caches

Ports (englisch für Anschlüsse)

Adresskomponenten, die in Netzwerkprotokollen eingesetzt werden, um Datensegmente den richtigen Diensten (Protokollen) zuzuordnen. Dieses Konzept ist z.B. in TCP und UDP implementiert.
(z. B. 216.239.33.100:80)

Kann Werte von 0 bis 65535 annehmen.

Well Known Ports

25 SMTP E-Mail-Versand

21 FTP Dateitransfer

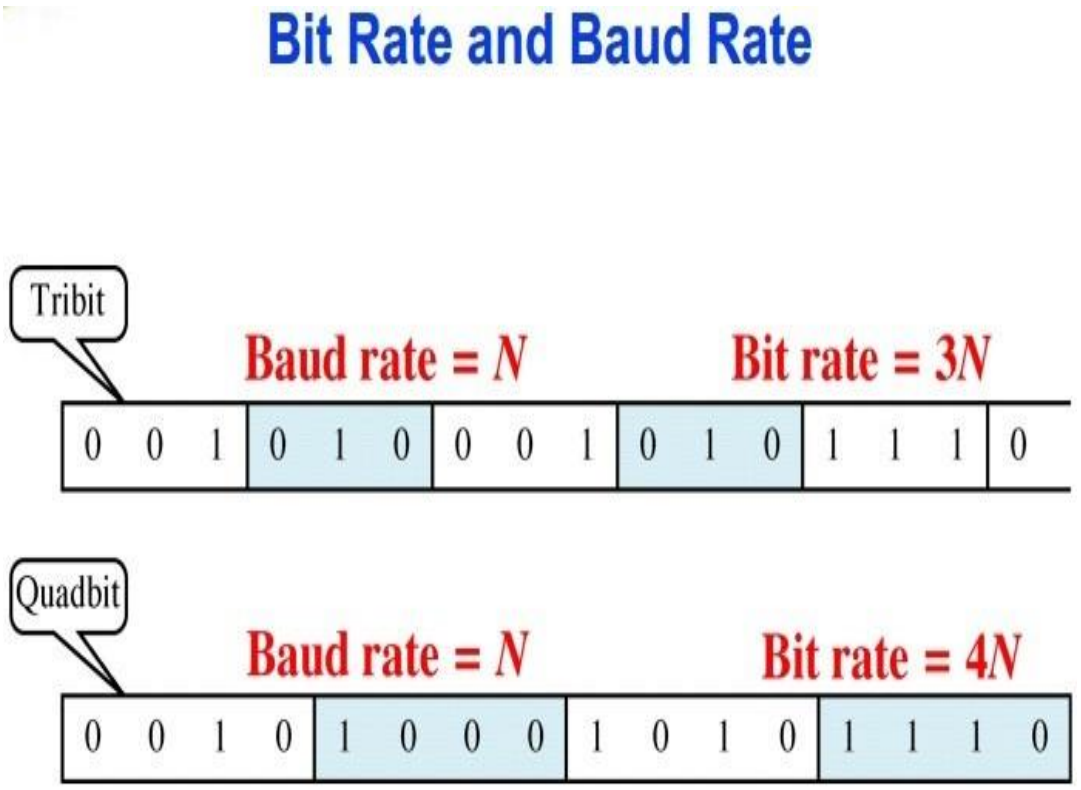
53 DNS Auflösung von Domainnamen in IP-Adressen

80 HTTP Webserver

31337 Back Orifice (Trojaner)

Bitrate und Baudrate

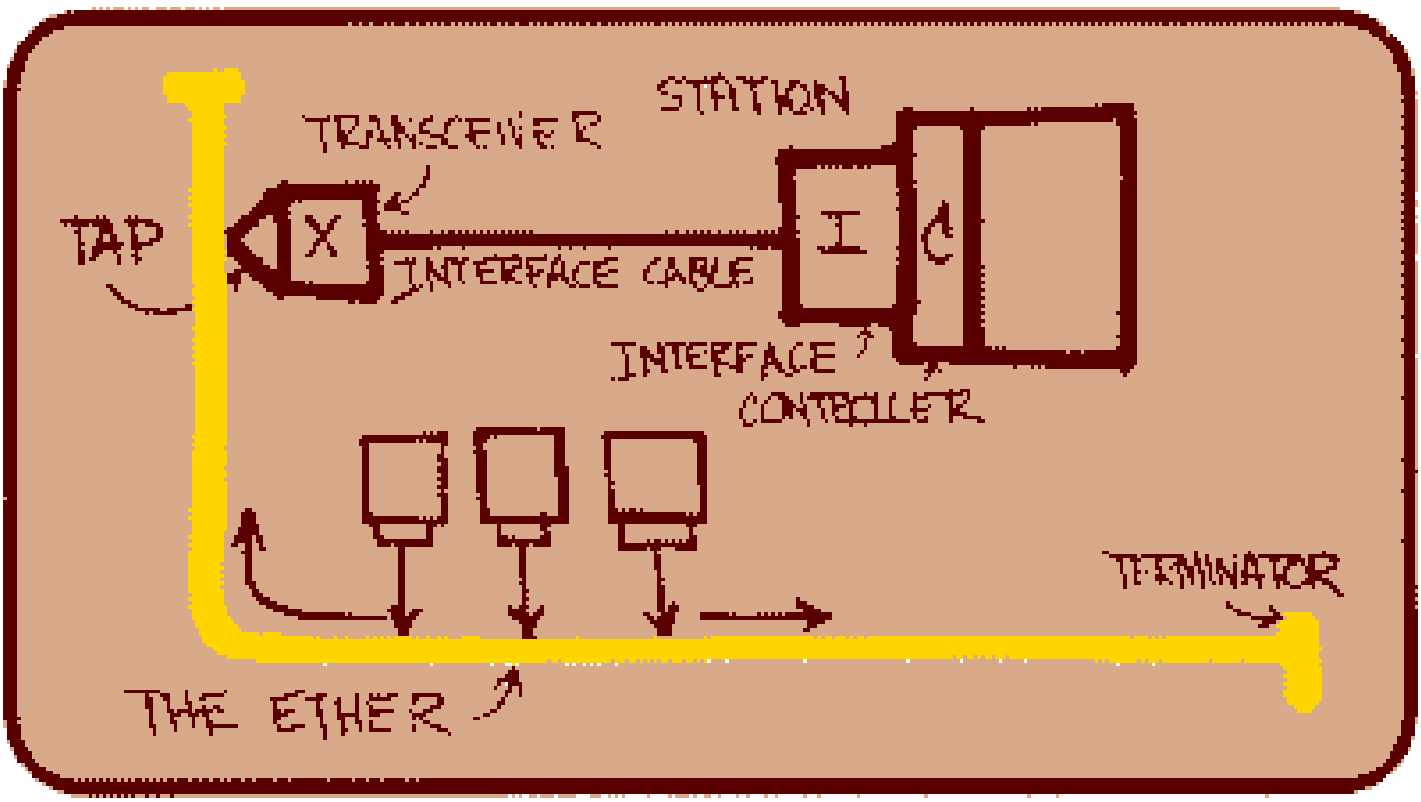
Émile Baudot



- Bitrate: Anzahl der übertragenen Nutzdaten in Bits pro Zeiteinheit. -> Datenübertragungsrate
- Typischerweise wird in Bit pro Sekunde (Bit/s) gemessen.
- Baudrate: Anzahl der übertragenen Symbole pro Sekunde.
- Baud nennt man auch Schrittgeschwindigkeit oder Symbolrate -> 1 Baud ist die Geschwindigkeit, wenn 1 Symbol pro Sekunde übertragen wird.
- Ursprünglich gab die Baudrate die Signalisierungsgeschwindigkeit beim Telegrafen an, also die Anzahl der Morsezeichen pro Sekunde.

Ethernet

Robert Metcalfe im Juni 1976
am Xerox Palo Alto Research Center:
Funktionsprinzip von Ethernet



Bei **Ethernet** spricht man von einer paketvermittelnden Netzwerktechnik, deren Standards auf den Schichten 1 und 2 des OSI-Schichtenmodells die Adressierung und die Zugriffskontrolle auf unterschiedliche Übertragungsmedien definieren.

IEEE Normen auf Layer 1 und 2 :

<table>
<tr><td rowspan="2">2</td><td rowspan="3">802.1
Internet-Working</td><td colspan="4">802.2
Logical Link Control (LLC)</td></tr>
<tr><td colspan="4">802.1
Media Access Control (MAC)</td></tr>
<tr><td>1</td><td>802.3
Ethernet</td><td>802.4
Token-Bus</td><td>802.5
Token-Ring</td><td>802.11
Wireless LAN</td></tr>
</table>

- Es existieren zahlreiche Ethernet-Standards
- Diese unterscheiden sich u.a. in der **Übertragungsrate** und dem **Übertragungsmedium.**
- Es existieren Versionen für Koaxialkabel, Twisted-Pair-Kabel und Glasfaser-Kabel bis maximal 10 Gbit/s (100 Gbit/s in Planung).

2 Übertragungsverfahren existieren:

- **Basisband** (BASE)
- **Breitband** (BROAD)

Standard	MBit/s	Übertragungsmedium
10BASE2/5	10	Koaxialkabel (50 Ohm Wellenwiderstand)
10BROAD36	10	Koaxialkabel (75 Ohm Wellenwiderstand)
10BASE-F	10	Glasfaserkabel
10BASE-T	10	Twisted-Pair-Kabel
100BASE-FX	100	Glasfaserkabel
100BASE-T4	100	Twisted-Pair-Kabel (Cat 3)
100BASE-TX	100	Twisted-Pair-Kabel (Cat 5)
1000BASE-LX	1.000	Glasfaserkabel
1000BASE-SX	1.000	Glasfaserkabel (Multimodefasern)
1000BASE-ZX	1.000	Glasfaserkabel (Singlemodefasern)
1000BASE-CX	1.000	Doppelt-twinaxiale Kupferkabel
1000BASE-T	1.000	Twisted-Pair-Kabel (Cat 5)
1000BASE-TX	1.000	Twisted-Pair-Kabel (Cat 6)
10GBASE-SR	10.000	Glasfaserkabel (Multimodefasern)
10GBASE-LR	10.000	Glasfaserkabel (Singlemodefasern)
10GBASE-CX4	10.000	Doppelt-twinaxiale Kupferkabel
10GBASE-T	10.000	Twisted-Pair-Kabel (Cat 6e)

10BASE5 z.B. bedeutet. . .

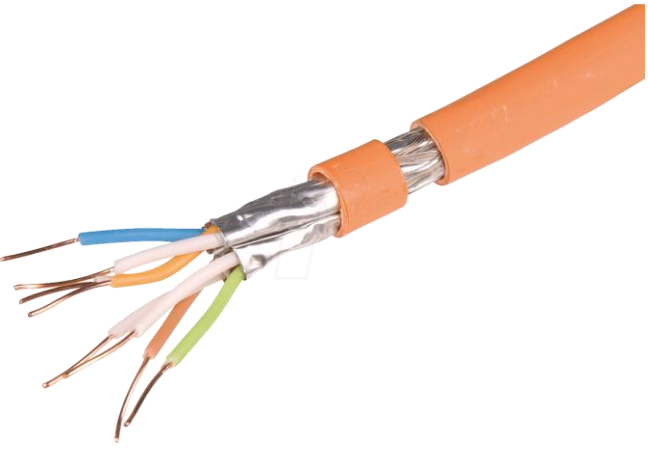
- Übertragungsrate: 10 MBit/s
- Übertragungsverfahren:
- Basisband
- Maximale Segmentlänge:
- 5 * 100m = 500m

Protokolle beim Ethernet

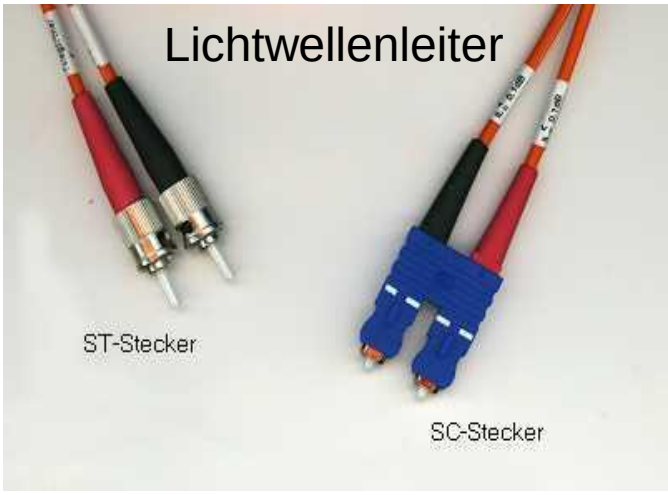
- Ethernet verwendet das **Address Resolution Protocol** (ARP) um die logischen Adressen der Vermittlungsschicht (IPv4-Adressen) in MAC-Adressen aufzulösen
- Bei IPv6 wird das **Neighbor Discovery Protocol** (NDP) verwendet, dessen Funktionalität identisch ist und das ähnlich arbeitet

Bei Ethernet verwendete Medientypen

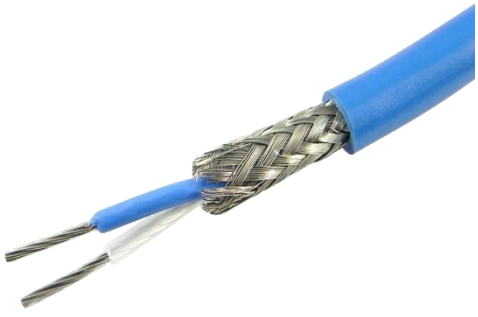
Twisted Pair



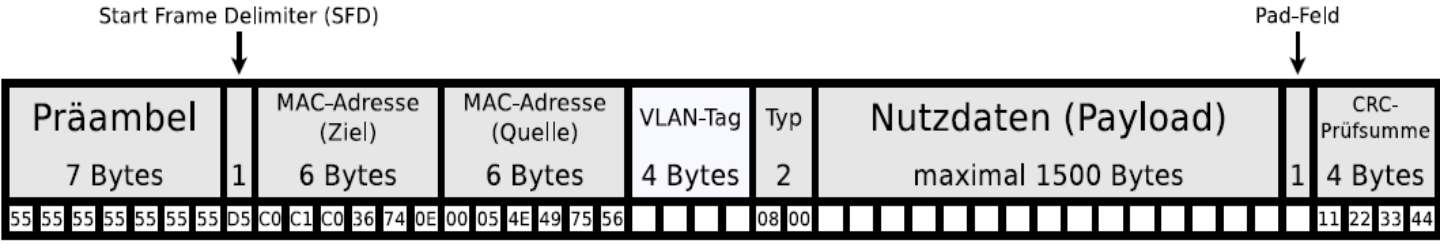
Lichtwellenleiter



Twinaxial mit Stecker

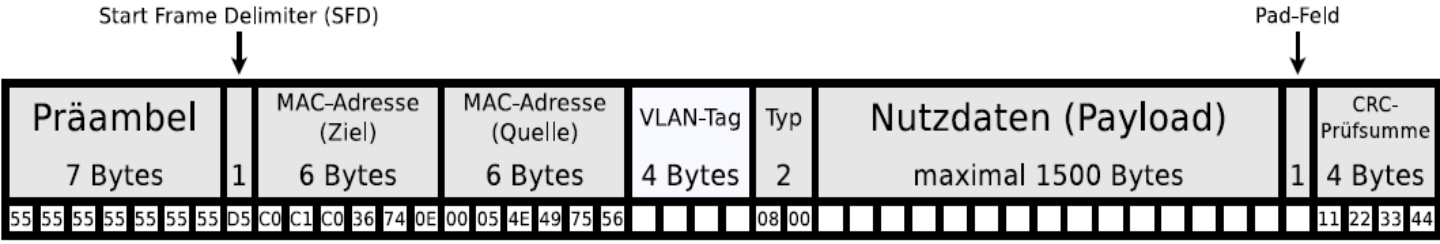


Ethernet Rahmenformat



- Die Präambel besteht aus der 7 Bytes langen Bitfolge 101010...1010 :
- Synchronisiert bei Bus-Topologien den Empfänger auf die Bit-Abstände.
- Darauf folgt der 1 Byte große SFD mit der Bitfolge 10101011.

- Die Datenfelder für die physischen Adressen (MAC-Adressen) von Sender und Ziel sind jeweils 6 Bytes lang.
- Der 4 Bytes lange optionale VLAN-Tag (VLAN -> Virtual LAN) enthält unter anderem :
- eine 12 Bits lange VLAN-ID und ein 3 Bits großes Feld zur Priorisierung.



- Das Datenfeld Typ enthält das verwendete Protokoll der nächsthöheren Schicht.

- Bei IPv4 hat das Datenfeld Typ den Wert 0x0800
- Bei IPv6 hat das Datenfeld Typ den Wert 0x86DD
- Enthalten die Nutzdaten eine ARP-Nachricht, hat das Datenfeld Typ den Wert 0x0806

- Mindestgröße eines Ethernet-Rahmens: 72 Bytes, Maximale Größe: 1526 Bytes.
- Der VLAN-Tag vergrößert die maximale Größe um 4 Bytes.
- Jeder Rahmen kann maximal 1500 Bytes Nutzdaten enthalten.
- Mit dem Datenfeld Pad werden Rahmen bei Bedarf auf die erforderliche Mindestgröße von 72 Bytes gebracht -> das ist nötig, damit die Kollisionserkennung via CSMA/CD funktioniert
- Abschließend folgt eine 32 Bits lange Prüfsumme, die aber nicht die Präambel und den SFD einschließt.

MAC-Broadcast-Adresse

- Möchte ein Netzwerkgerät einen Rahmen explizit an alle anderen Geräte im gleichen physischen Netz senden, fügt es im Rahmen in das Feld der Zieladresse die Broadcast-Adresse ein.
- Bei dieser MAC-Adresse haben alle 48 Bits den Wert 1 -> Hexadezimale Schreibweise:

  FF-FF-FF-FF-FF-FF
- Rahmen, die im Zielfeld die Broadcast-Adresse tragen, werden von Bridges und Switches nicht in andere physische Netze übertragen.

Umwandlung in einen Datenstrom auf Layer 1

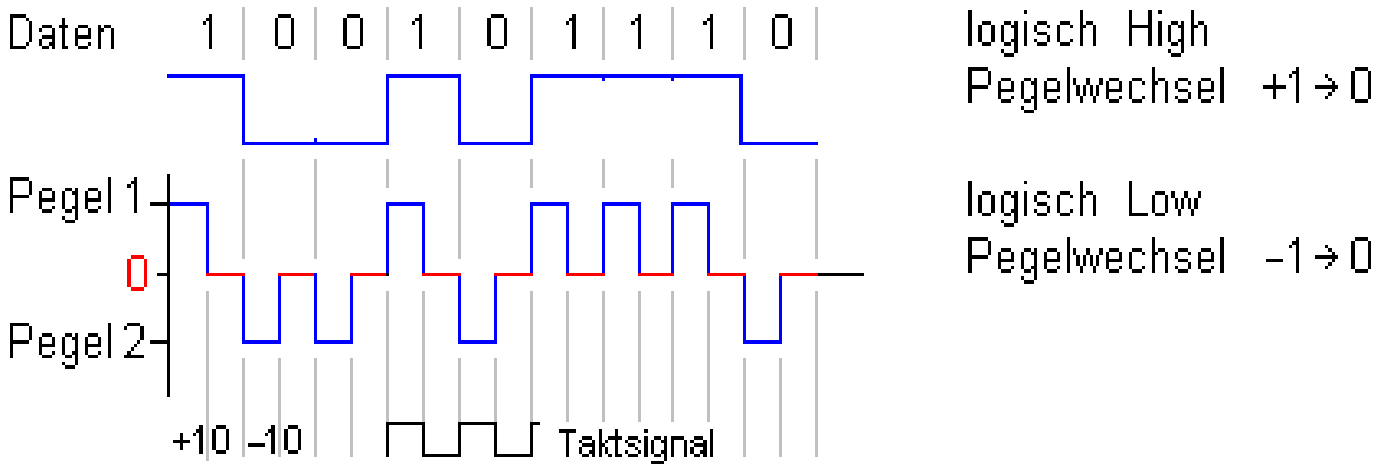
Nachdem der Datenstrom als Folge von Bytes bereitgestellt wurde, werden nun abhängig vom physischen Medium und der Übertragungsrate ein oder mehrere Bits in einen Leitungscode kodiert, um einerseits die physischen Eigenschaften des Mediums zu berücksichtigen und andererseits dem Empfänger eine Taktrückgewinnung zu ermöglichen.

Leitungscode :

- legt bei der digitalen Telekommunikation fest, wie die zur Informationsübertragung genutzten Symbole auf der physischen Ebene übertragen werden.
- dabei werden bestimmte Pegelfolgen, etwa Lichtintensitäten auf Glasfasern oder Spannungen oder Ströme auf elektrischen Leitungen, binären Bitsequenzen im Datenstrom zugeordnet.

Beispiele für Leitungscodes :

- Non Return to Zero (NRZ) (RS-232)
- Return to Zero (RZ) (IrDA -> *Infrarot*)
- Manchesterkodierung (IEEE 802.3)
- 8b10b (Gigabit-Ethernet, PCIe, USB 3.0, HDMI)
- 64b66b (10-Gigabit-Ethernet)



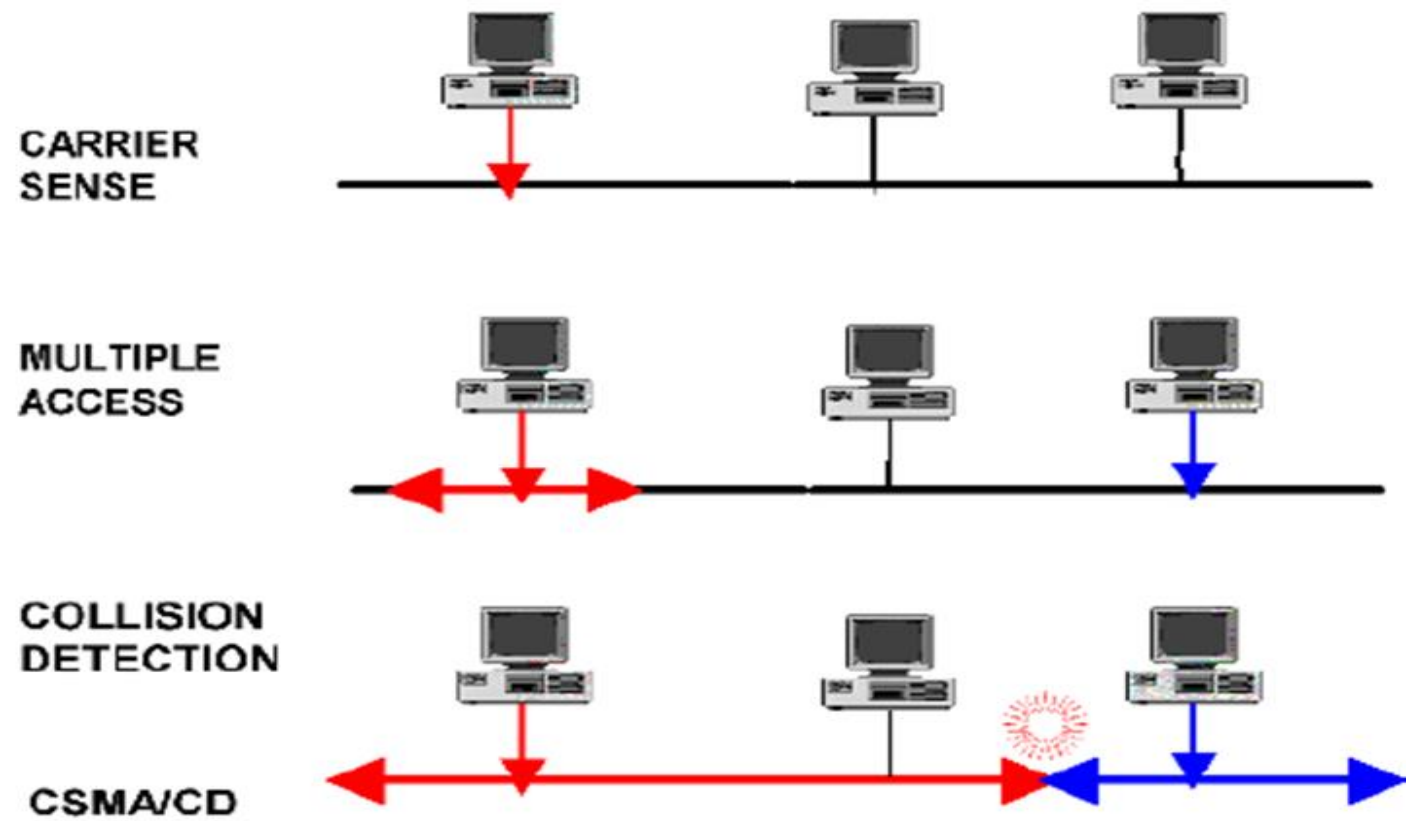
Return-to-Zero-Leitungscode

CSMA/CD

In Busnetzen gilt grundsätzlich :

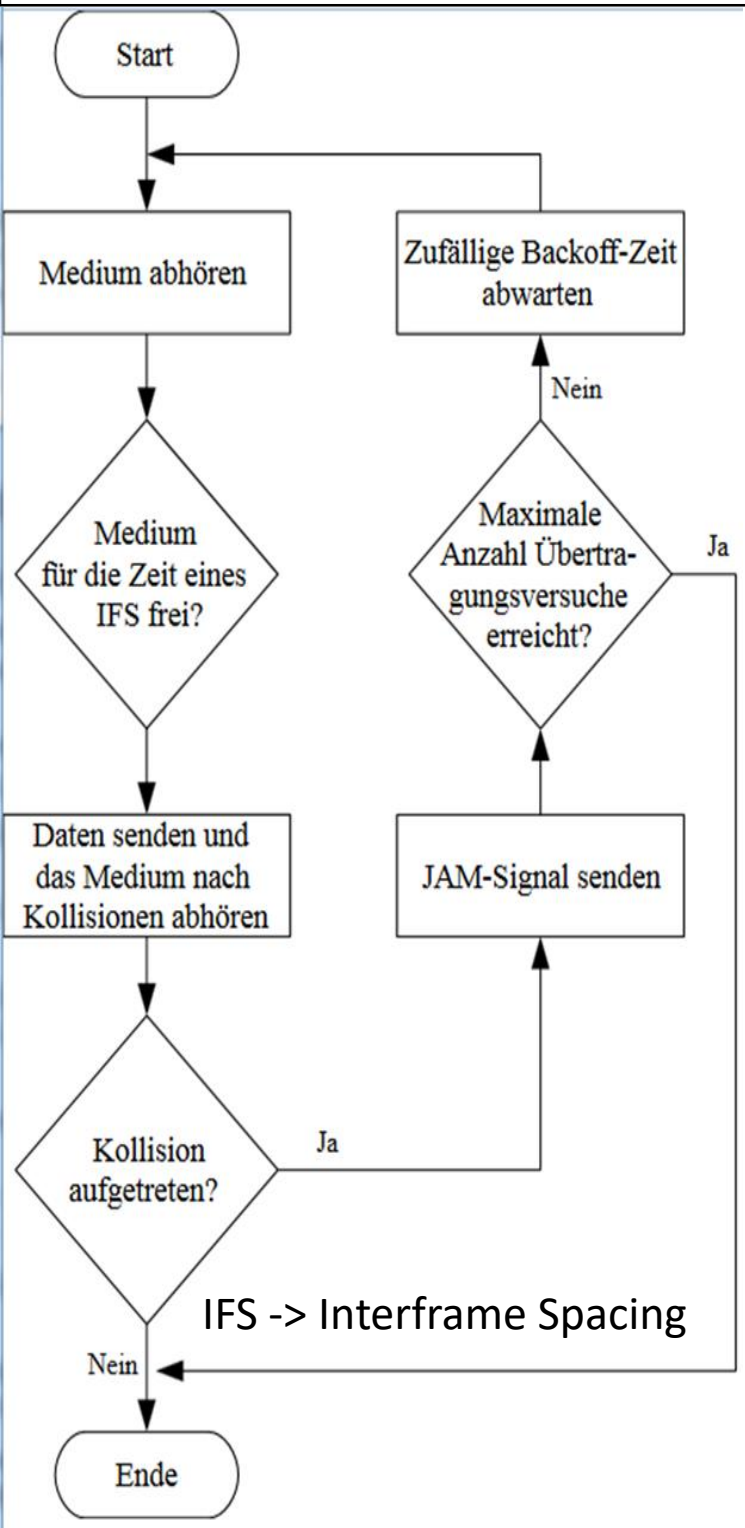
- Wartezeit und übertragbare Datenmenge sind nicht eindeutig vorhersagbar.
- Alle Teilnehmer stehen in Bezug auf den Medienzugriff im direktem Wettbewerb.

Ethernet verwendet das Medienzugriffsverfahren Carrier Sense Multiple Access / Collision Detection (CSMA/CD)



Carrier Sense (CS) heißt:

- Jedes Netzwerkgerät hört vor dem Senden den Kanal ab, und sendet nur dann, wenn der Kanal frei ist.
- Die Netzwerkgeräte können also zwischen einer freien und einer besetzten Verbindungsleitung unterscheiden.



Multiple Access (MA) heißt:

Alle Netzwerkgeräte greifen auf dasselbe Übertragungsmedium konkurrierend zu.

Collision Detection (CD) heißt:

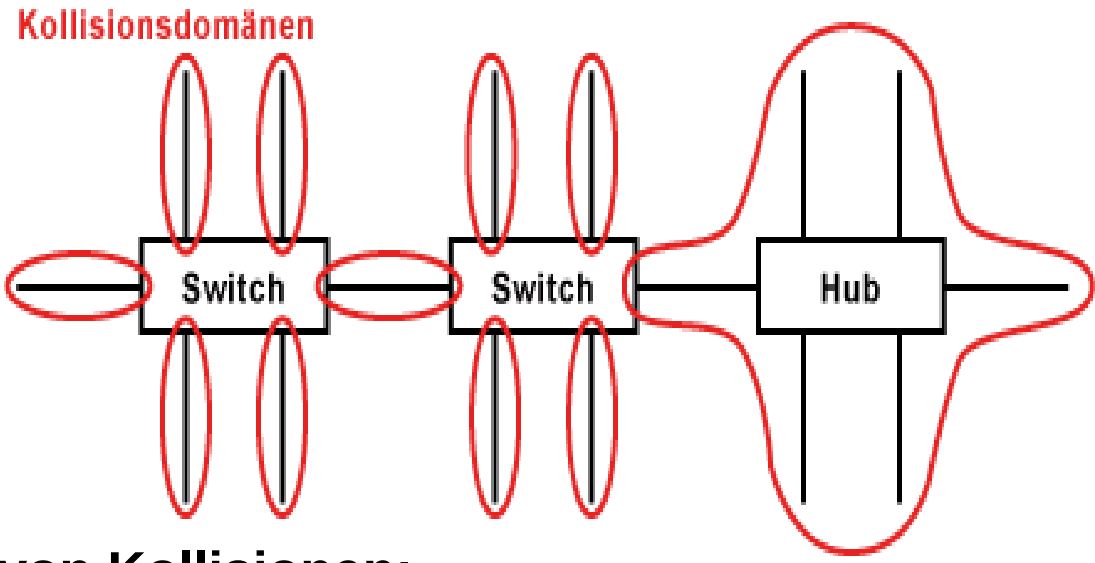
Jedes Netzwerkgerät hört auch während des Sendens den Kanal ab, um auftretende Kollisionen zu entdecken und wenn nötig eine Fehlerbehandlung durchzuführen.

Kollisionsdomäne

- Der Bereich, in dem sich Kollisionen ausdehnen können.
- Eine Kollisionsdomäne ist ein Netzwerk oder ein Teil eines Netzwerks, in dem mehrere Netzwerkgeräte ein gemeinsames Übertragungsmedium nutzen.
- Sie umfasst alle Netzwerkgeräte, die gemeinsam um den Zugriff auf ein Übertragungsmedium konkurrieren.

Kollisionsdomänen entsprechen Netzwerksegmenten.

- Repeater und Hubs vergrößern die Kollisionsdomäne.
- Bridges, Switches und Router teilen die Kollisionsdomäne.
- Zur Kollisionserkennung verwendet der kabelgebundene Netzwerkstandard Ethernet das Medienzugriffsverfahren CSMA/CD.
- Bei Funknetzen ist eine sichere Kollisionserkennung unmöglich.
- Aus diesem Grund verwendet WLAN zur Kollisionsvermeidung das Medienzugriffsverfahren CSMA/CA.



Behandlung von Kollisionen:
Kollisionserkennung
Carrier **S**ense **M**ultiple
Access/**C**ollision **D**etection
Ethernet

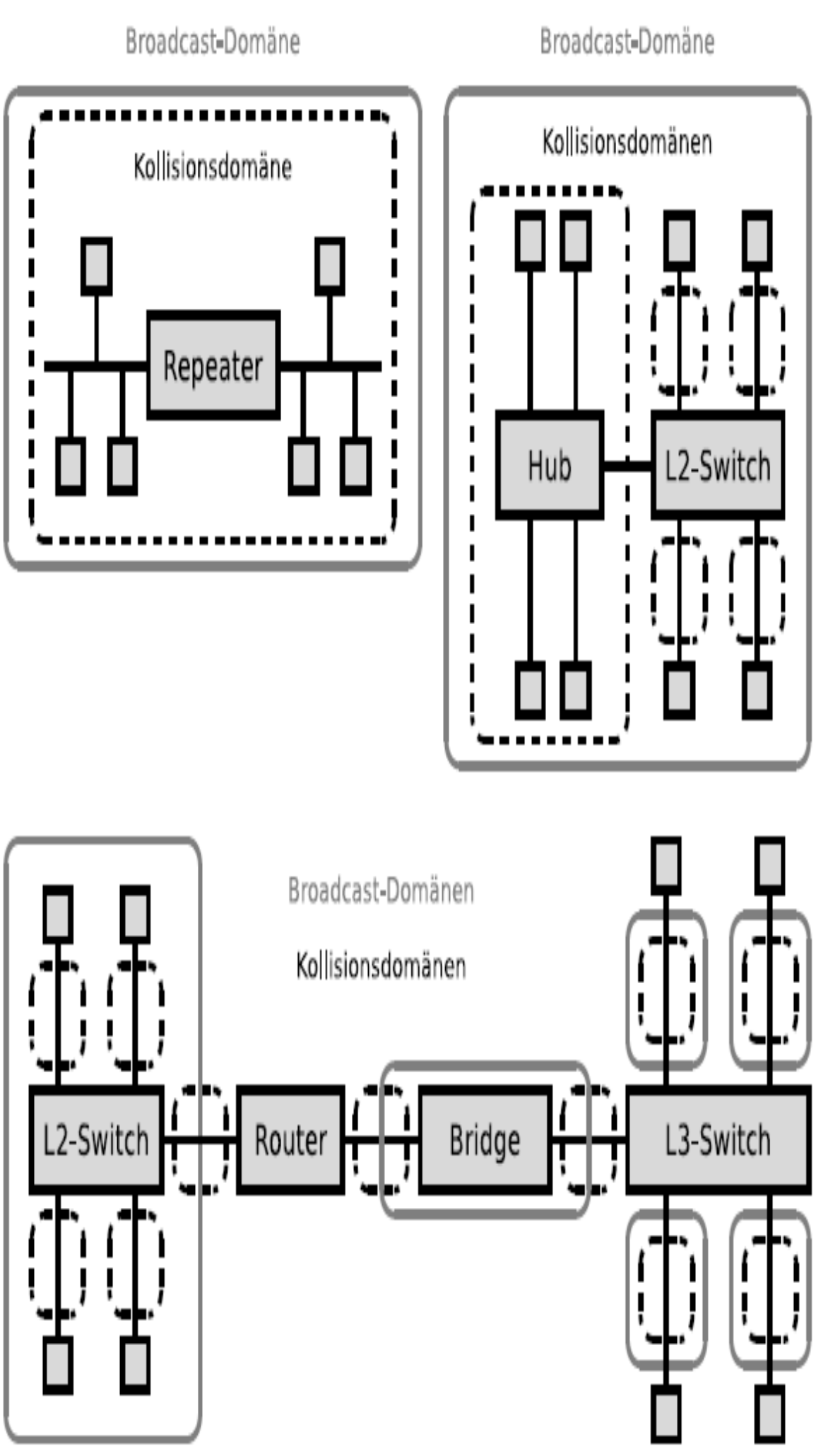
Kollisionsvermeidung
Carrier **S**ense **M**ultiple
Access/**C**ollision **A**voidance
WLAN

Broadcast-Domänen

- Logischer Verbund von Netzwerkgeräten, bei dem ein Broadcast alle Teilnehmer der Domäne erreicht.
- Geräte aus Schicht 3 (**Router**,**Layer-3-Switche**) teilen die Broadcast-Domäne
- Geräte aus Schicht 1 und 2 (**Repeater**, **Hubs**, **Bridges**, **Layer-2-Switche**) unterbrechen sie nicht.

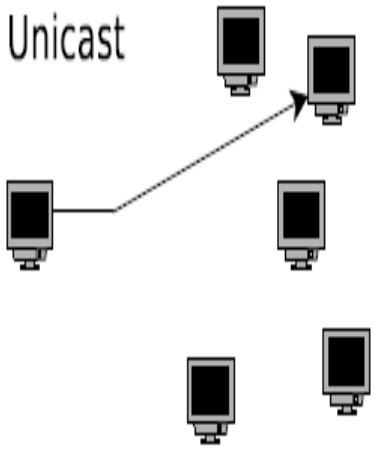
- Broadcast-Domänen bestehen aus einer oder mehreren Kollisionsdomänen.
- Die Geräte aus Schicht 1 (**Repeater**, **Hubs**) unterbrechen die Kollisionsdomäne nicht.
- Die Geräte aus Schicht 2 und 3 (**Bridges**, **Layer-2-Switche**, **Router**, **Layer-3-Switche**) unterbrechen die Kollisionsdomäne.

Broadcast-Domänen entsprechen Netzen.

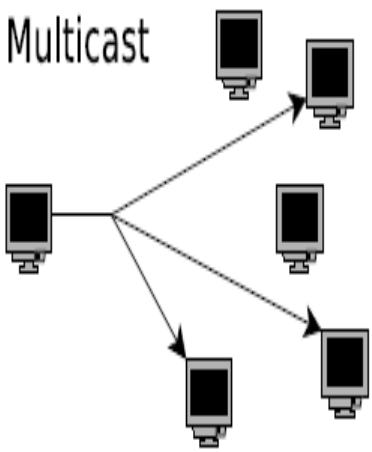

Broadcast-Domäne
Broadcast-Domäne
Kollisionsdomäne
Repeater
Kollisionsdomänen
Hub
L2-Switch
Broadcast-Domänen
Kollisionsdomänen
L2-Switch
Router
Bridge
L3-Switch

Unicast, **Multicast, Broadcast und Anycast**

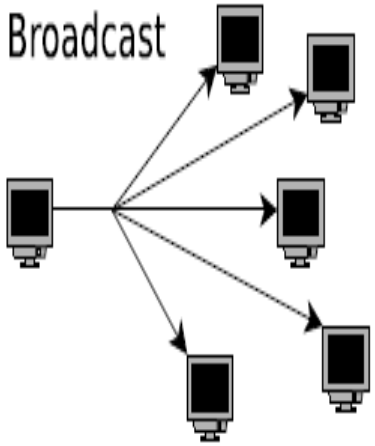
Unicast -> Eine IP-Adresse hat einen einzelnen Empfänger.



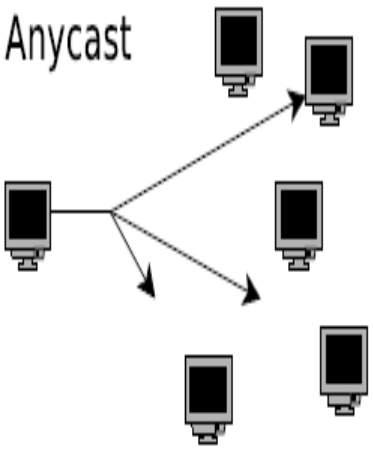
Multicast -> Eine IP-Adresse kann eine Gruppe von Empfängern bezeichnen. Einem Netzwerkgerät können
auch mehrere IP-Adressen zugeordnet sein.



Broadcast (engl.; Rundruf)
-> eine Nachricht, bei der Datenpakete von einem Punkt aus an alle Teilnehmer eines Nachrichtennetzes übertragen werden.



Bei **Anycast** erreicht man über eine Adresse einen einzelnen Empfänger aus einer Gruppe
Es antwortet der Empfänger, der über die kürzeste Route erreichbar ist.



Zusammenhang zwischen MAC-Adressen und IP-Adressen

Ausschließlich physische Adressierung via MAC-Adressen ist in Computernetzen mit eventuell globalen Ausmaßen nicht sinnvoll.
-> Grund: Wartbarkeit (und Kollisionsdomänen)

Es sind logische Adressen nötig, die von der konkreten Hardware unabhängig sind
-> **IP-Adressen**

MAC Address	IP Address
00-16-E6-42-C4-33	192.168.1.100

3 - Network		Configures packets for intra-subnet and inter-subnet communications	IPv4, IPv6 , IPX
2 – Data Link	LLC	Applies physical addresses to the data creating a switchable frame.	MAC addresses
	MAC		
1 - Physical		Converts the data into the format appropriate for the associated media.	Hubs, fiber optics, copper, electricity, RF

Aufbau von IP-Adressen

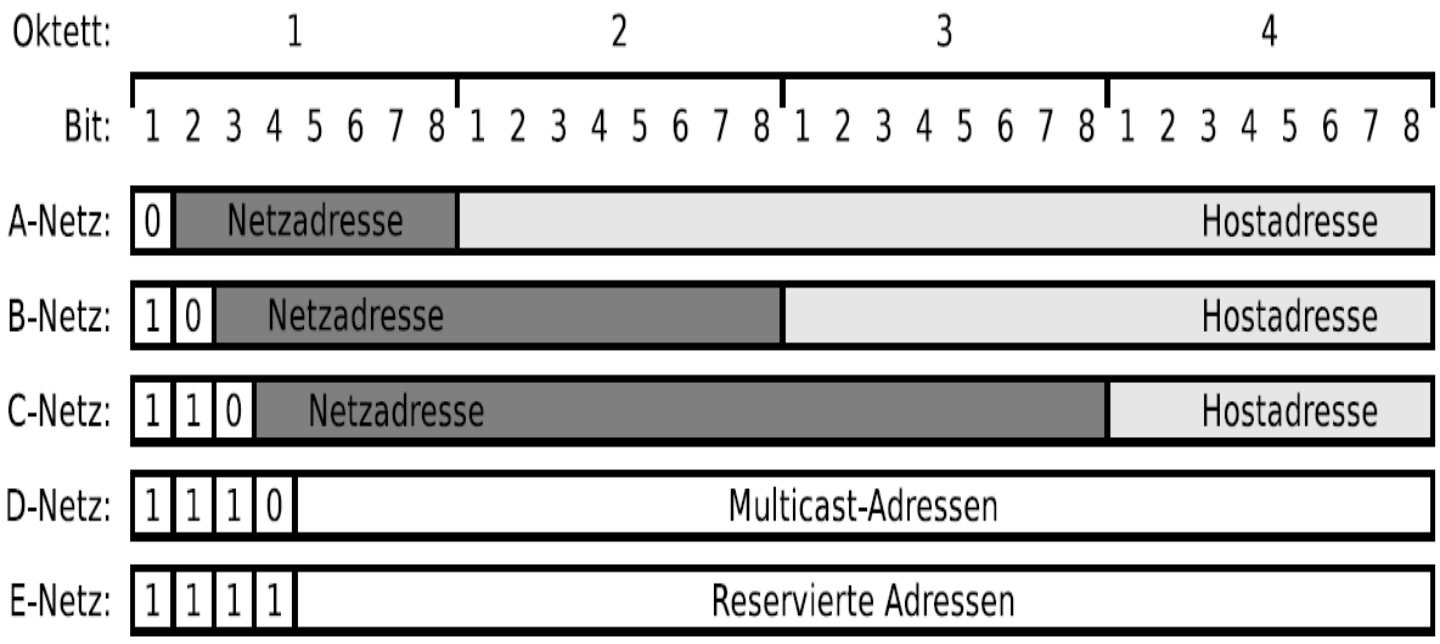
- IPv4-Adressen sind 32 Bits (4 Bytes) lang.
- Daher können 2^{32} = 4.294.967.296 Adressen dargestellt werden.
- Üblich ist die Darstellung in der sogenannten Dotted decimal notation.
- Die 4 Oktette werden als vier durch Punkte voneinander getrennte ganze Zahlen in Dezimaldarstellung im Bereich von 0 bis 255 geschrieben.
- Beispiel: **141.52.166.25**

Adressraum = Menge aller gültigen Netzadressen

Kennt sich das ZDF mit IP-Adressierung aus ?

- Die 32 Bits einer IPv4-Adresse bestehen aus den beiden Feldern:
- **Netzadresse** (Network Identifier bzw. Netzwerk-ID)
- **Hostadresse** (Host Identifier bzw. Host-ID)

Klassen für IP-Adressen (Classful network**):**
Klasse A: 7 Bits für Netzadresse und
24 Bits für Hostadresse
Klasse B: 14 Bits für Netzadresse und
16 Bits für Hostadresse
Klasse C: 21 Bits für Netzadresse und
8 Bits für Hostadresse



- Ursprünglich wurden IPv4-Adressen in Klassen von A bis C eingeteilt
- Klassen D und E für spezielle Aufgaben.

Präfixe und Hostadressen bei IP-Adressklassen

- Die Präfixe legen die Netzklassen und ihre Adressbereiche fest.
- $2^7 = 128$ **Klasse A**-Netze mit jeweils maximal $2^{24} = 16.777.216$ Hostadressen.
- $2^{14} = 16.384$ **Klasse B**-Netze mit jeweils maximal $2^{16} = 65.536$ Hostadressen.
- $2^{21} = 2.097.152$ **Klasse C**-Netze mit jeweils maximal $2^8 = 256$ Hostadressen.
- Klasse D enthält Multicast-Adressen (zum Beispiel für IPTV).
- Klasse E ist für Experimente reserviert.

Klasse	Präfix	Adressbereich	Netzteil	Hostteil
A	0	0.0.0.0 - 127.255.255.255	7 Bits	24 Bits
B	10	128.0.0.0 - 191.255.255.255	14 Bits	16 Bits
C	110	192.0.0.0 - 223.255.255.255	21 Bits	8 Bits
D	1110	224.0.0.0 - 239.255.255.255	—	—
E	1111	240.0.0.0 - 255.255.255.255	—	—

Beispiele Class-A-Netze :

- General Electric 3.0.0.0
- IBM 9.0.0.0
- Columbia University 15.0.0.0
- Hewlett Packard 16.0.0.0
- Apple 17.0.0.0
- M.I.T 18.0.0.0

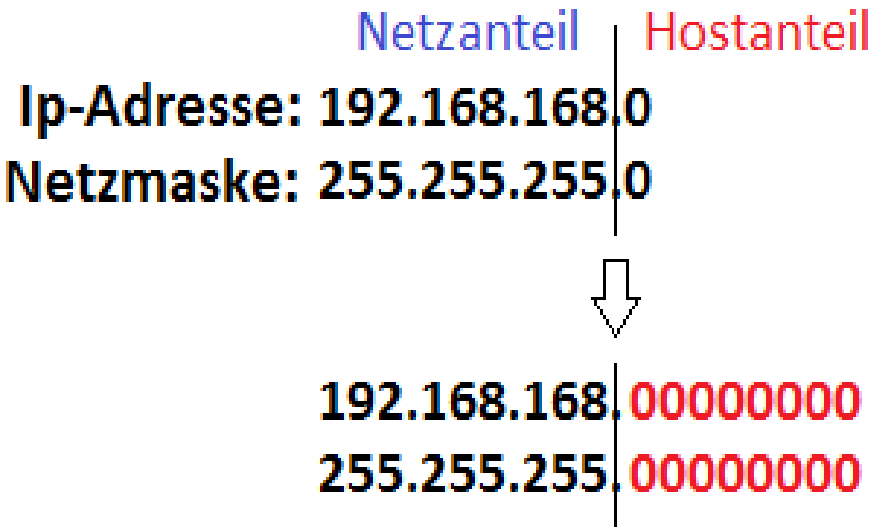
Probleme der Netzklassen:

- Sie können nicht dynamisch an Veränderungen angepasst werden.
- Sie verschwenden viele Adressen.

Lösung:

- 1993: Einführung des klassenlosen Routings – Classless Interdomain Routing (CIDR).
- Subnetting -> Unterteilung logischer Netze in Teilnetze (Subnetze).
- Supernetting -> Zusammenfassen von mehreren Netzen mit teilweise gleichem Netzwerkanteil.

Die Netzmaske (netmask)



- Alle Knoten in einem Netzwerk bekommen eine Netzmaske zugewiesen.
- Länge: 32 Bits (4 Bytes).
- Mit ihr wird die Anzahl der Subnetze und Hosts festgelegt.
- Die Netzmaske unterteilt die Hostadresse der IP-Adresse in **Netznummer** und **Hostadresse.**

	IPv4-Adresse	11000000 10101000 00000001 10000001	192.168.1.129
UND	Netzmaske	11111111 11111111 11111111 00000000	255.255.255.0
=	Netzwerkteil	11000000 10101000 00000001 00000000	192.168.1.0

	IPv4-Adresse	11000000 10101000 00000001 10000001
UND	NOT Netzmaske	00000000 00000000 00000000 11111111
=	Geräteteil	00000000 00000000 00000000 10000001

CIDR
Classless Interdomain Routing

Seit Einführung des CIDR 1993 werden IP-Adressbereiche in der Notation :

- Anfangsadresse/Netzbits vergeben.
- Die Netzbits sind die Anzahl der Einsen im Netzwerkteil der Netzmaske.

Schreibweise mit Subnetzmaske	Binäre Schreibweise	Verkürzte Schreibweise mit CIDR-Suffix
10.0.0.1/255.0.0.0	11111111.00000000.00000000.000000	10.0.0.1/8
192.168.0.1/255.255.255.0	11111111.11111111.11111111.00000000	192.168.0.1/24

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Subnetting

- wird dafür genutzt, um große aber auch kleinere physikalische Netzwerke in logische Teilnetze zu unterteilen.
- Ein Subnet, Subnetz bzw. Teilnetz ist ein physikalisches Segment eines Netzwerks, in dem IP-Adressen mit der gleichen Netzwerkadresse benutzt werden.
- Diese Teilnetze können über Router miteinander verbunden werden und bilden dann ein großes zusammenhängendes Netzwerk.

Gründe für Subnetting:

- Trennen von Netzwerken unterschiedlicher Topologie.
- Trennen von Netzwerken nach Standorten, Gebäuden und Etagen.
- Trennen von Netzwerken nach Abteilungen und Bereichen.
- Trennen des Netzwerks zur Reduzierung des Verkehrsaufkommens.

Wichtige Wiederholung!

Jeweils die **erste** und **letzte** IP-Adresse eines IP-Adressbereichs (z. B. 192.168.0.0 bis 192.168.0.255) kennzeichnen die **Netzwerk-Adresse** (192.168.0.0) und die **Broadcast-Adresse** (192.168.0.255).
Diese Adressen können an keinen Host vergeben werden. Deshalb muss die Anzahl der IP-Adressen um zwei reduziert werden, damit man auf die richtige Anzahl nutzbarer IP-Adressen kommt.

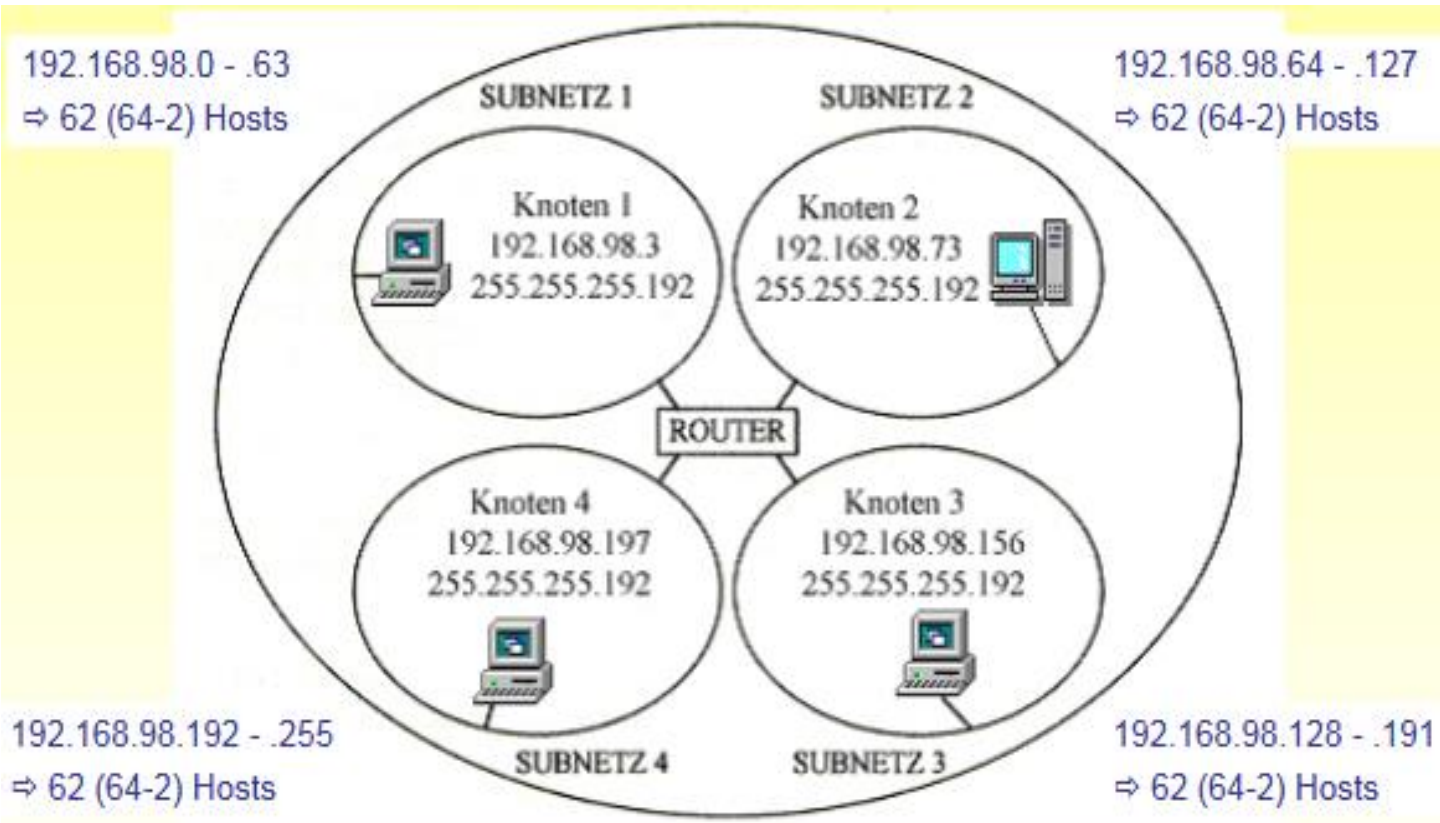
VLSM (Variable Length Subnet Mask):
VLSM bedeutet übersetzt soviel wie Subnetzmaske mit variabler Länge. VLSM ermöglicht einem Netz, mehr als eine Teilnetzmaske zuzuweisen.

Wiederholung : Wie errechnet der Computer die Subnetzadresse und die Hostadresse ?

IP-Adresse AND Netzmaske = Subnetzadresse

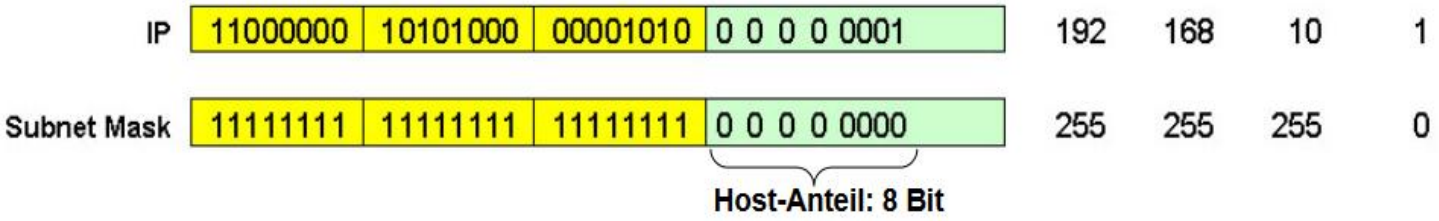
IP-Adresse AND (NOT Netzmaske) = Hostadresse

Beispiel für ein Subnet :

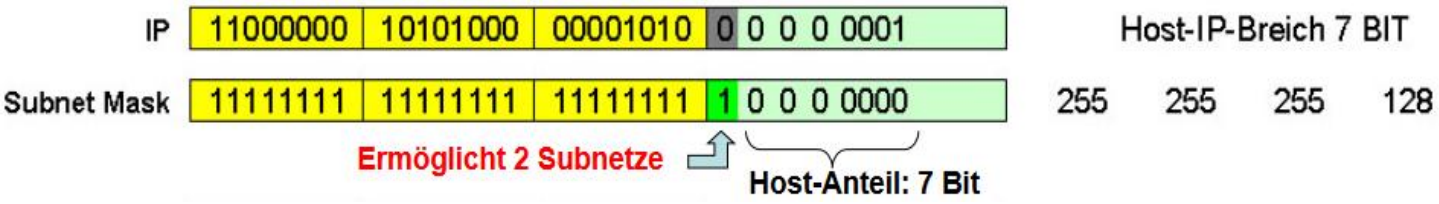


Beispiele für mögliche Subnets:

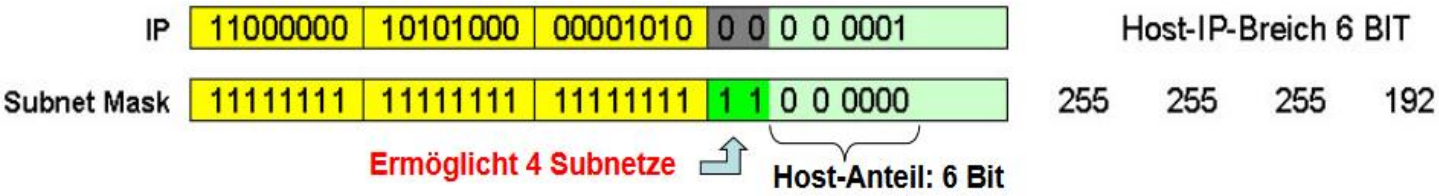
Netz ohne Subnetze :



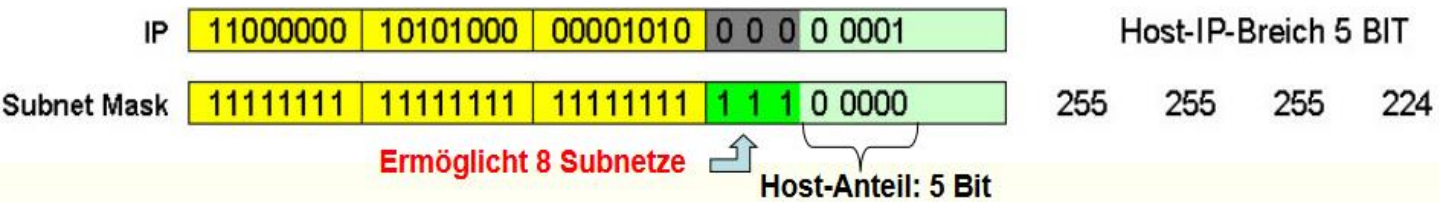
Netz mit 2 Subnetzen :



Netz mit 4 Subnetzen :



Netz mit 8 Subnetzen :



Die Tabelle zeigt die möglichen Aufteilungen eines Klasse C-Netzes in Subnetze.

Netzbits	/24	/25	/26	/27	/28	/29	/30	/31	/32
Netzmaske	0	128	192	224	240	248	252	254	255
Subnetzbits	0	1	2	3	4	5	6	7	8
Subnetze	1	2	4	8	16	32	64	128	256
Hostbits	8	7	6	5	4	3	2	1	0
Hostadressen	256	128	64	32	16	8	4	2	—
Hosts	254	126	62	30	14	6	2	0	—

Aufteilen eine Klasse-C-Netzes mithilfe dieser Tabelle :

Beispiel 1 : Ein Klasse C-Netz soll in 5 Subnetze mit jeweils maximal 25 Hosts aufgeteilt werden:

- Jedes Subnetz benötigt eine Subnetznummer.
- Für 5 Subnetze sind 3 Subnetzbits nötig.
- Mit Hilfe der restlichen 5 Bits im Hostteil können in jedem Subnetz bis zu 32 − 2 = 30 Hosts adressiert werden.
- Somit ist die Schrägstrichdarstellung /27 geeignet.

Beispiel 2 :

Gegeben : Ein Netz: IP: 192.168.168.0
Netzmaske: 255.255.255.0
(Oder anders geschrieben: 192.168.168.0/24)

Aufgabe :
Das vorhandene Netz ist in 4 Subnetze zu unterteilen.

Vorgehensweise : Damit ein Netz in kleinere Subnetze unterteilt werden kann, muss der Netzanteil um eine entsprechende Anzahl von Bits in der Netzmaske erweitert werden.

Anzahl von bits:	1	2	3	4	5	6	7	8	...
Anzahl der Subnetze:	2	4	8	16	32	64	128	256	...

Mit 1 bit können 2^1 = 2 Subnetze aufgebaut werden.
Es sind aber 4 Subnetze notwendig.

Mit 2 bits können 2^2 = 4 Subnetze aufgebaut werden.

-> Wir brauchen 4 Subnetze.

Netzanteil	Hostanteil	
192.168.168.	00000000	
255.255.255.	00000000	Vorher

Wir “klauen“ dem Hostanteil 2 Bits :

Netzanteil		Hostanteil	
192.168.168.00		000000	
255.255.255.11		000000	Nachher

-> Der Hostanteil besteht nun aus 6 Bits

Jedem Subnetz stehen deshalb $2^6 = 64$ IP-Adressen zur Verfügung :

- **Eine IP-Adresse für die Netzadresse des Subnets.**
- **Eine IP-Adresse für den Broadcast.**
- **62 IP-Adressen für die Hosts.**

Nun haben wir automatisch die Netzadresse vom 1. Subnetz :

192.168.168.00000000
255.255.255.11000000

Oder komplett in dezimaler Schreibweise :

192.168.168.0
255.255.255.192

Hilfsmittel

Dezimalzahl	Binärzahl
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

Beim Broadcast werden alle Hostbits auf “1“ gesetzt.

→ Broadcast: **192.168.168.00111111**

Und wieder in dezimaler Schreibweise :

192.168.168.63

Was wir bisher haben :

1 IP	62 IPs	1 IP
Subnetzadresse	Host-IP-Range	Broadcast
192.168.168.0		192.168.168.63

Der Host-IP-Range ist der IP-Adress-Bereich zwischen der Subnetzadresse und der Broadcastadresse :

Subnetzadresse	Host-IP-Range	Broadcast
192.168.168.0	192.168.168.1 - 192.168.168.62	192.168.168.63

Das ist das **1. Subnetz**.

Wenn man nun die Broadcastadresse des **1. Subnetzes** um 1 erhöht, bekommt man die Subnetzadresse des **2. Subnetzes** :

Subnetzadresse	Host-IP-Range	Broadcast
192.168.168.0	192.168.168.1 - 192.168.168.62	192.168.168.63
192.168.168.64		

Wenn man nun zur Adresse des **2. Subnetzes** 62 (-> 62 IPs) hinzuaddiert haben wir den Host-IP-Range.

Wenn ich dazu noch eine 1 hinzuaddiere haben wir die Broadcastadresse des **2. Subnetzes:**

Subnetzadresse	Host-IP-Range	Broadcast
192.168.168.0	192.168.168.1 - 192.168.168.62	192.168.168.63
192.168.168.64	192.168.168.65 - 192.168.168.126	192.168.168.127

Für die zwei weiteren Subnetze sind die gerade gezeigten Schritte zu wiederholen.

-> Nun haben wir eine Tabelle mit allen möglichen Subnetzen, den Host-IPs und den Broadcastadressen :

1 IP	62 IPs	1 IP
Subnetzadresse	Host-IP-Range	Broadcast
192.168.168.0	192.168.168.1 - 192.168.168.62	192.168.168.63
192.168.168.64	192.168.168.65 - 192.168.168.126	192.168.168.127
192.168.168.128	192.168.168. 129 - 192.168.168. 190	192.168.168.191
192.168.168.192	192.168.168. 193 - 192.168.168. 254	192.168.168.255

Aufgabe :

Ein Netz mit der Netzwerkadresse 172.96.0.0 soll in vier Teilnetze aufgeteilt werden.

a) Zu welcher Adressklasse gehört dieses Netz ?
b) Welche Netzmaske gehört dazu ?
c) Erstellen sie eine Tabelle mit Subnetzmaske(n), Netzwerkadressen, Broadcastadressen und den Bereichen für die verfügbaren Hosts.
Verwenden sie die Dezimal- und die Binärschreibweise.

IPv4-Adressbereiche zur besonderen Nutzung

IANA (Internet Assigned Numbers Authority)
-> Für Europa -> RIPE (Réseaux IP Européens)

- Sind für die Vergabe von IP-Nummern zuständig.

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

- Adressbereich für private Netze, der ohne Registrierung der Adresse benutzt werden darf.
- Adressen aus diesem Bereich dürfen allerdings im öffentlichen Internet nicht auftreten.

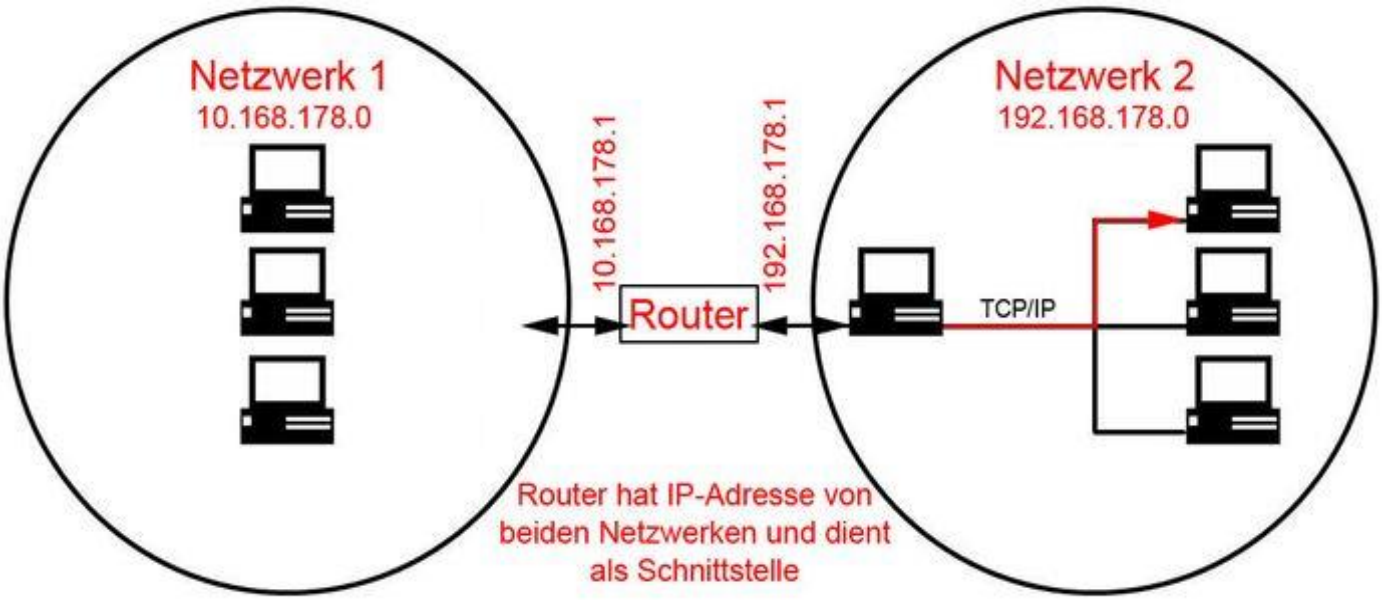
Spezielle IP-Adressen

127.0.0.0 - 127.255.255.255
Loopback-Adressen: Jedes an eine dieser Adressen geschickte Paket soll den Host nicht verlassen, sondern intern zurückgeschickt werden.

224.0.0.0 sind Netzwerke für Multicastsendungen.
255.255.255.255 für Broadcastsendungen für die jeweiligen Netzwerke. "Limited Broadcast"

Router Teil 2

Primäre Aufgabe:
Weiterleitung (Forwarding) der IP-Pakete.
Um diese Aufgabe zu erfüllen, müssen die Router für jedes eintreffende Paket die korrekte Schnittstelle (Port) ermitteln.



Die Aufgabe eines Routers ist ein komplexer Vorgang, der sich in 4 Schritte einteilen lässt:

1. Ermittlung der verfügbaren Routen.
2. Auswahl der geeignetsten Route unter Berücksichtigung verschiedener Kriterien.
3. Herstellen einer physikalischen Verbindung zu anderen Netzwerken.
4. Anpassen der Datenpakete an die Übertragungstechnik (Fragmentierung).

Arbeitsweise der Netzwerkgeräte auf Layer 3

1. Wird ein Datenpaket in das Netzwerk gesendet, prüft das IP-Protokoll des sendenden Rechners, ob das Datenpaket für das eigene Netzwerk bestimmt ist.
2. Dabei wird die eigene IP-Adresse und die Subnetzmaske mit der IP-Adresse und Subnetzmaske des Ziels verglichen und so die Netzwerk-IP ermittelt.
3. Befindet sich das Ziel im eigenen Netzwerk, wird das Datenpaket direkt an die Zieladresse geleitet.
4. Sind die beiden Netzwerk-IPs unterschiedlich, wird das Datenpaket an den Router geschickt.
5. Der Router hat für beide Netzwerke eine IP-Adresse, besitzt somit eine Schnittstelle zu beiden Netzwerken und prüft anhand der *Routingtabelle*, ob es möglich ist, das Datenpaket an das andere Netzwerk weiter zu leiten.
6. Ist es möglich, schickt der Router die Daten in das andere Netzwerk.

Jeder Router verwaltet eine lokale **Routing-Tabelle.**

Die Routing-Tabelle enthält :

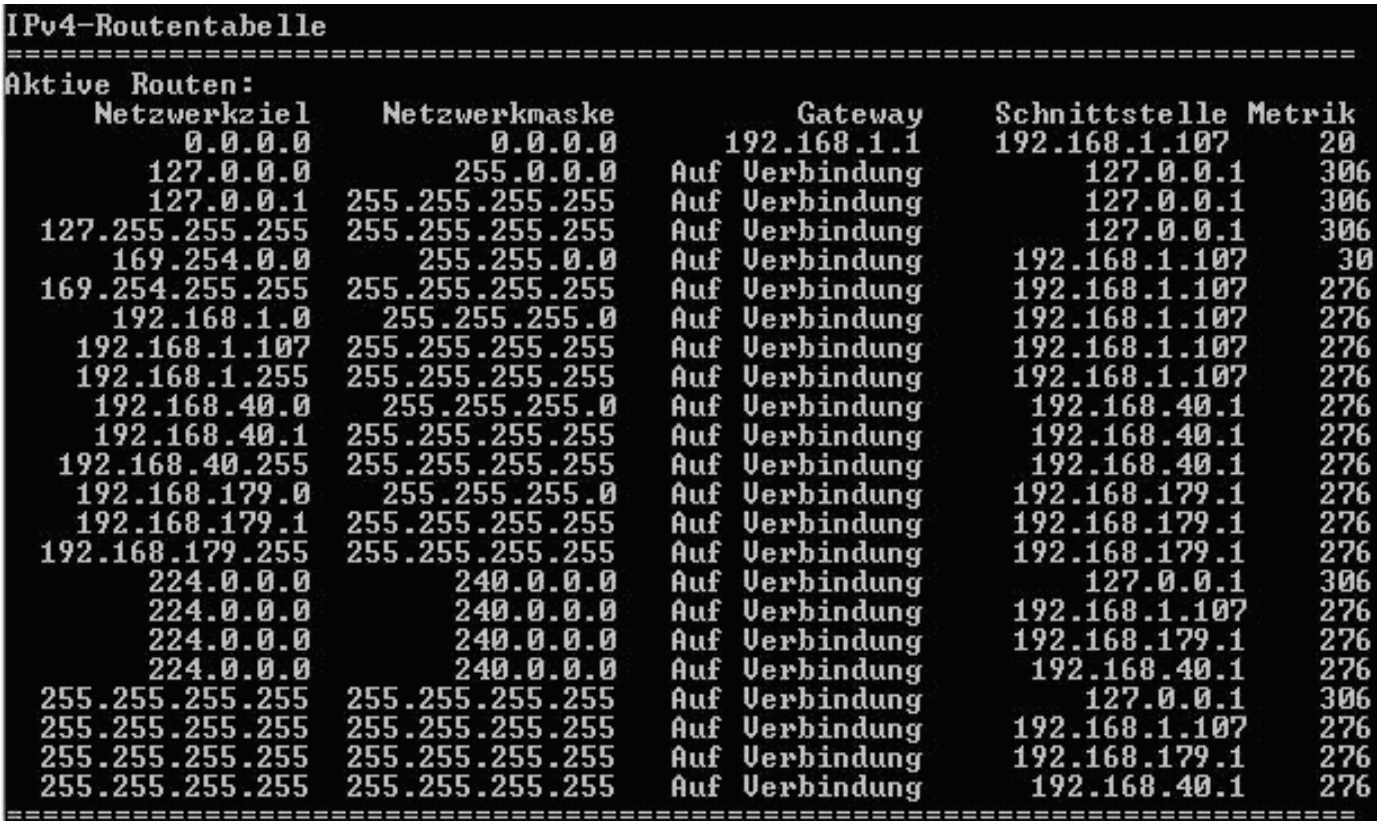
- die dem Router bekannten **logischen Netze.**
- die Information, welches logische Netz über welchen **Port** (-> Hardware) erreichbar ist.

Um sich die Routingtabelle des eigenen Rechners anzusehen gibt man **route print** auf der Kommandozeile ein.

Beispiel für eine IPv4 Routingtabelle :

```
Active Routes:

  Network Address          Netmask  Gateway Address       Interface  Metric
        0.0.0.0          0.0.0.0      172.16.1.9    172.16.2.128       1
        0.0.0.0          0.0.0.0      172.16.2.1    172.16.2.128       1
      127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
    172.16.2.0    255.255.255.0    172.16.2.128    172.16.2.128       1
  172.16.2.128  255.255.255.255        127.0.0.1       127.0.0.1       1
172.16.255.255  255.255.255.255    172.16.2.128    172.16.2.128       1
    192.1.3.0    225.255.255.0     220.1.3.118     220.1.3.118       1
  220.1.3.118  255.255.255.255        127.0.0.1       127.0.0.1       1
    224.0.0.0        224.0.0.0     220.1.3.118     220.1.3.118       1
    224.0.0.0        224.0.0.0    172.16.2.128    172.16.2.128       1
255.255.255.255  255.255.255.255    172.16.2.128    172.16.2.128       1
```



```
IPv4-Routentabelle
===========================================================================
Aktive Routen:
    Netzwerkziel    Netzwerkmaske          Gateway    Schnittstelle Metrik
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.107     20
        127.0.0.0        255.0.0.0   Auf Verbindung        127.0.0.1    306
        127.0.0.1  255.255.255.255   Auf Verbindung        127.0.0.1    306
  127.255.255.255  255.255.255.255   Auf Verbindung        127.0.0.1    306
      169.254.0.0      255.255.0.0   Auf Verbindung    192.168.1.107     30
  169.254.255.255  255.255.255.255   Auf Verbindung    192.168.1.107    276
      192.168.1.0    255.255.255.0   Auf Verbindung    192.168.1.107    276
    192.168.1.107  255.255.255.255   Auf Verbindung    192.168.1.107    276
    192.168.1.255  255.255.255.255   Auf Verbindung    192.168.1.107    276
     192.168.40.0    255.255.255.0   Auf Verbindung     192.168.40.1    276
     192.168.40.1  255.255.255.255   Auf Verbindung     192.168.40.1    276
   192.168.40.255  255.255.255.255   Auf Verbindung     192.168.40.1    276
    192.168.179.0    255.255.255.0   Auf Verbindung    192.168.179.1    276
    192.168.179.1  255.255.255.255   Auf Verbindung    192.168.179.1    276
  192.168.179.255  255.255.255.255   Auf Verbindung    192.168.179.1    276
        224.0.0.0        240.0.0.0   Auf Verbindung        127.0.0.1    306
        224.0.0.0        240.0.0.0   Auf Verbindung    192.168.1.107    276
        224.0.0.0        240.0.0.0   Auf Verbindung    192.168.179.1    276
        224.0.0.0        240.0.0.0   Auf Verbindung     192.168.40.1    276
  255.255.255.255  255.255.255.255   Auf Verbindung        127.0.0.1    306
  255.255.255.255  255.255.255.255   Auf Verbindung    192.168.1.107    276
  255.255.255.255  255.255.255.255   Auf Verbindung    192.168.179.1    276
  255.255.255.255  255.255.255.255   Auf Verbindung     192.168.40.1    276
===========================================================================
```

- **Netzwerkziel:** Hier sind die Netzwerk-IPs der Zielnetze aufgelistet.
- **Netzwerkmaske:** Die zugehörige Subnetzmaske für das Zielnetz.
- **Gateway:** Das Gateway gibt an, wohin das Datenpaket geschickt wird, um das Netzwerkziel zu erreichen. Ist man bereits direkt an das Netzwerk angeschlossen, steht in der Spalte **Auf Verbindung**. Ansonsten die IP-Adresse des Routers, der die Weiterleitung übernimmt.
- **Schnittstelle:** Die Schnittstelle ist die IP-Adresse der Netzwerkkarte, über die das Datenpaket an das Ziel geschickt wird.
- **Metrik:** Jede Route wird anhand von "Kosten" ermittelt. Je niedriger die Kosten sind, umso schneller gelangt man an das Ziel. Wenn für ein Zielnetzwerk mehrere Routen vorhanden sind, wird automatisch die Route mit den niedrigsten Kosten genommen. Je mehr Router zwischengeschaltet sind, umso höher sind die Kosten.

Statisches und dynamisches Routing

Statisches Routing

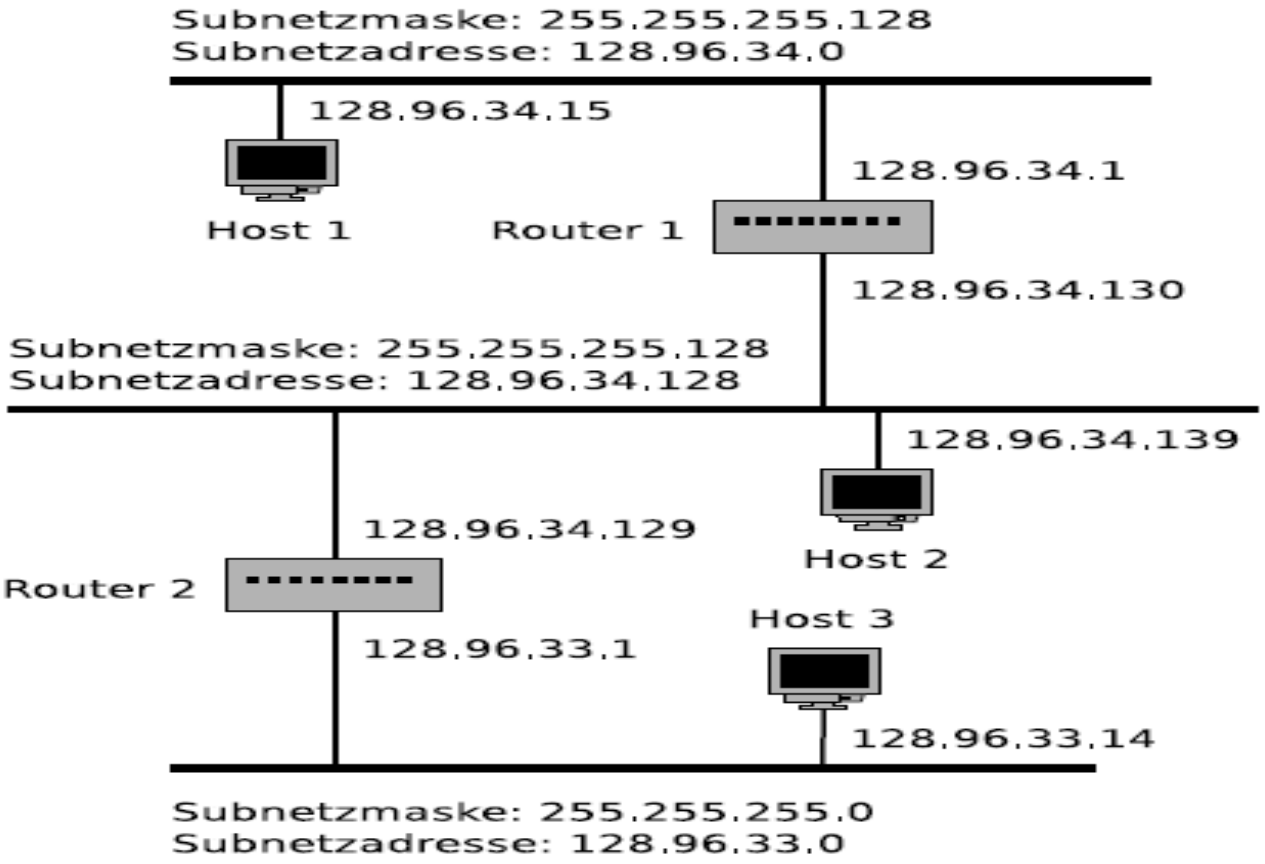
-> ein fester durch einen Administrator vorgegebener Weg.

Dynamisches Routing

-> ein durch ein Routingprotokoll, das automatisch Topologieänderungen berücksichtigt, ermittelter Weg.

Routingfähige Protokolle und Routing-Protokolle

- Man unterscheidet grundsätzlich routingfähige Protokolle (z.B. TCP/IP) und Routing-Protokolle (z.B. RIP).
- Die Wegbestimmung (Routing) ist der Prozess, bei dem die Weiterleitungstabellen (Routing-Tabellen) mit Hilfe von Routing-Protokollen erstellt werden.
- Die Weiterleitungstabellen sind nötig, damit die Bestimmung des besten Weges, also zu den niedrigsten Kosten, zum Ziel möglich ist.
- Diese Routing-Protokolle werden zwischen den Routern ausgeführt.



Hauptklassen von Routing-Protokollen :

- Distanzvektor-Routing-Protokolle
  Beispiel: Routing Information Protocol (RIP)

- Link-State-Routing-Protokolle
  Beispiele: Border Gateway Protocol (BGP) und Open Shortest Path First (OSPF)

Router sind in **autonomen Systemen** (AS) organisiert.

Jedes AS besteht aus einer Gruppe von logischen Netzen, die :

- das Internet Protocol verwenden.
- von der gleichen Organisation (z.B. einem Internet Service Provider, einem Unternehmen oder einer Universität) betrieben und verwaltet werden.
- das gleiche Routing-Protokoll verwenden.
- Die miteinander verbundenen AS bilden in ihrer Gesamtheit das **Internet**.