Grundlage von Netzwerken und Internettechnologien

US_IT-16.1

Inhaltsverzeichnis:

18.03.2015

Quelle der Präsentation:
http://www.fh-wedel.de/~si/seminare/ss04/Ausarbeitung/5.Mieling/Praesentation.pdf

Internet & Netzwerke

"(...) Aus der allgemeinen englischen Fachbezeichnung für ein *internetwork* oder *internet* verbreitete sich das Wort „Internet“ als Eigenname für das größte Netzwerk dieser Art, das aus dem Arpanet entstand. (...)"

https://de.wikipedia.org/wiki/Wikipedia:B%C3%BCcher/Internettechnologie

Entstehungsgeschichte (grob)

WWW

World Wide Web = Großes System zur gemeinsamen Ressourcennutzung durch offene Kommunikations- und Dokumentenstandards

1958	Gründung der ARPA (Advanced Research Projects Agency)
1965	Donald Davis entwirft Paketvermittlung
1966	Vernetzung der ARPA Großrechner
1969	Die ersten Großrechner über IMPs (Interface Message Processor) zusammengeschlossen ARPAnet Ab 1970 mit "normalen" Computer
1969-1971	telnet, ftp, email
1972	Öffentlichmachung con ARPANet
1983	Ablösung des Teil MILNet und des zivilen Teil ARPANet
1983	TCP/IP ersetzt NCP
1983	Gründung des NFSNet (National Science Foundation)
1989	ARPANet von DOD (Department of Defence) aufgelöst
1990	Entwicklung des erten grafischen Web-Oberflächen, http
1991	Gründung der Internet Society (ISOC), legt die RFC-Standards fest (Request for Comments)

Physikalische Netzstruktur

https://de.wikipedia.org/wiki/Internet#Infrastruktur

Telefonnetz	Modem, ISDN, DSL
Mobilnetz	GSM, GRPS, UMTS
Stromnetz	PLC (Powerline Communications)
TV-Netz	TV-Kabelmodem

Vergabe von IP-Adressen

IANA - Intermodal Association of North America

Die IANA veröffentlicht den Bestand öffentlicher IP-Adressen jeder einzelnen Regional Internet Registry.

IPv4-Adressen bestehen aus 32 Bits, also 4 Oktetten (Bytes). Damit sind 232, also 4.294.967.296 Adressen darstellbar. In der *dotted decimal notation* werden die 4 Oktetts als vier durch Punkte voneinander getrennte ganze Zahlen in Dezimaldarstellung im Bereich von 0 bis 255 geschrieben.

z.B. 203.0.113.195

https://de.wikipedia.org/wiki/IP-Adresse#IPv4

POP (Point of Presence) Zugang

Mit **Broadband Remote Access Server** (**BRAS**) oder auch **Breitband PoP** (Point of

Presence) werden Netzelemente von Breitband-Netzen wie DSL und UMTS bezeichnet. Sie sind Teil des Netzwerks eines Internet Service Providers (ISP) und speisen den Datenverkehr der Endbenutzer-Verbindungen in das Backbone-Netzwerk ein.
https://de.wikipedia.org/wiki/Breitband-Zugangsserver

Backbone

Backbone (engl. für *Rückgrat*, *Hauptstrang*, *Basisnetz*) bezeichnet einen

verbindenden Kernbereich eines Telekommunikationsnetzes mit sehr hohen Datenübertragungsraten, der meist aus einem Glasfasernetz sowie satellitengestützten Kommunikationselementen besteht.

https://de.wikipedia.org/wiki/Backbone_%28Telekommunikation%29

ISP Internet Service Provider

Internetdienstanbieter oder **Internetdienstleister** (engl. **Internet Service Provider**, abgekürzt **ISP** *oder* **Internet Access Provider**), im deutschsprachigen Raum auch oft nur **Provider**, im Sprachgebrauch meist nur *Internetanbieter* oder *Internetprovider* genannt, sind Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind.

https://de.wikipedia.org/wiki/Internetdienstanbieter

- Verwendung von http://www.ripe.net zur Nutzung des WHOIS-Dienstes

- tracert www.fbi.gov (cmd)
Zeigt die Route zu einer Adresse anhand der Hops und deren Latenz an

- pathping www.google.de (cmd)
Einfache Routenberechnung mit Verlust-Statistik

Paketvermittlung

- Daten werden in einzelne Pakete zerlegt **(MTU) 1500 bytes**
- Dem **Datenpaket** sind weitere Informationen enthalten **Header** (Herkunft, Ziel Meta)
- **Router** transportieren Pakete, **ohne feste Route**, daher können sie **verschiedene Wege** nehmen und in **unterschiedlicher Reihenfolge ankommen**

Frames zwischen Routern
Router transportieren Pakete auf **IP-Basis**
Switch stellt auf Basis von **MAC-Adressen** Verbindungen her

Routing
Geringe Wartezeit auf Pakete, weil diese klein sind, geringere Fehleranfälligkeit durch kleine Datenblöcke, die schnell ersetzt werden können

Protokolle:

TCP - Verbindungsorientierte Übertragung

Die Transportschicht (engl.: *Transport Layer*) ermöglicht eine Ende-zu-Ende-Kommunikation. Das wichtigste Protokoll dieser Schicht ist das Transmission Control Protocol (TCP), das Verbindungen zwischen jeweils zwei Netzwerkteilnehmern zum zuverlässigen Versenden von Datenströmen herstellt. Es gehören aber auch unzuverlässige Protokolle – zum Beispiel das User Datagram Protocol (UDP) – in diese Schicht. (...)

https://de.wikipedia.org/wiki/Internetprotokollfamilie#TCP.2FIP-Referenzmodell

UDP - Verbindungslose Übertragung

Das **User Datagram Protocol**, kurz **UDP**, ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.
Die Entwicklung von UDP begann 1977, als man für die Übertragung von Sprache ein einfacheres Protokoll benötigte als das bisherige verbindungsorientierte TCP. Es wurde ein Protokoll benötigt, das nur für die Adressierung zuständig war, ohne die Datenübertragung zu sichern, da dies zu Verzögerungen bei der Sprachübertragung führen würde.(...)
https://de.wikipedia.org/wiki/User_Datagram_Protocol

Routing [ˈruːtɪŋ] (BE) / [ˈruːtɪŋ], aber auch [ˈraʊtɪŋ] (AE) (engl. „Leitweglenkung“, „Streckenführung“, „Verkehrsführung“ sowie „leiten“, „senden“, „steuern“)[1][2] bezeichnet in der Telekommunikation das Festlegen von Wegen für Nachrichtenströme bei der Nachrichtenübermittlung in Rechnernetzen. Insbesondere in paketvermittelten Datennetzen ist hierbei zwischen den beiden verschiedenen Prozessen *Routing* und *Forwarding* zu unterscheiden: Das Routing bestimmt den gesamten Weg eines Nachrichtenstroms durch das Netzwerk; das Forwarding beschreibt hingegen den Entscheidungsprozess eines einzelnen Netzknotens, über welchen seiner Nachbarn er eine vorliegende Nachricht weiterleiten soll.

EGP / BGP

Interdomain-Routing verwendet sogenannte *Exterior Gateway-Protokolle* (**EGP**), und zwar (fast) immer BGP. Da Interdomain-Routing das Routing zwischen verschiedenen Providern regelt, liegt der Fokus beim Interdomain-Routing normalerweise auf einer *finanziell* effizienten (profitorientierten) Nutzung des Netzwerks. Die zugrundeliegende Idee hierbei ist die, dass ein autonomes System nicht allen seinen Nachbarn die gleichen Informationen (Routen) zukommen lässt. Welche Informationen ausgetauscht werden und welche nicht, wird zunächst in Verträgen festgelegt und dann in den Routern konfiguriert; man spricht in diesem Zusammenhang von Policy-basiertem Routing. (...)

https://de.wikipedia.org/wiki/Routing#Interdomain-Routing

HTTP

Basiert auf TCP/IP,baut zeichenorientierte zeitlich terminierte Verbindungen mittels festen Befehlssatz (get, send,...) auf

URI (Uniform Ressource Identifier) ist schematische Form der Eingabe

- t3n.de – URI
- http://t3n.de – URL (http zeigt euch wo die Ressource ist)
- ftp://t3n.de – URL (ftp zeigt euch wo die Ressource ist)
- urn:isbn:3827370191 – URN (eindeutige Identifikation des Buches „Moderne Betriebssysteme“ von Andrew S. Tanenbaum)

Ein URN (Unified Resource Name) ist ein URI (Uniform Ressource Identifier) der eine Ressource dauerhaft und ortsunabhängig bezeichnet, und das nach dem Schema urn. Das heißt: mit URN könnt ihr einer Ressource einen dauerhaft gültigen Namen zuweisen, der die Ressource damit eindeutig identifizierbar macht. Wie bereits oben im RFC von Tim Berners-Lee angesprochen, kann eine Ressource alles sein, was sich eindeutig beschreiben lässt.

Das URN-Schema sieht übrigens so aus: urn:<NID>:<NID-spezifischer Teil>

http://t3n.de/news/url-uri-unterschiede-516483/

Routing

DNS Name Space

Generic Global	com, edu, net, org, int
Generic US	gov, mil
Local Spec	de, ru

nslookup

Verwendung von http://www.denic.de , um die Verfügbarkeit einer Domäne zu prüfen.

Root-Server in der globalen Verteilung

http://www.root-servers.org/

http://de.wikipedia.org/wiki/Root-Nameserver

Browser
- Firefox
  - Einstellungen
    - Allgemein
    - Tabs
    - Suche
    - Inhalt
    - Anwendungen
    - Datenschutz
    - Sicherheit
    - Sync.
    - Ewr. Einstellungen
      - Allgemein
      - Datenübermittlungen
      - Netzwerk
      - Update
      - Zertifikate

Vereinfachte Zusammenfassung der Kommunikation im Internet:

http://www.hessen-it.de/sicherheit/Inhalte/Grundlagen/Aufbau/index.html

https://www.youtube.com/watch?v=VY_zD2840Do

Auflistung wichtiger Portnummern

https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports

OSI - Schichten Modell

7 *A*pplication File, Print, Message (Anwendung)
Übergabe der Daten an das Programm
6 *P*resentation Data Encryption (Darstellung)
Analyse der Medienformate
5 *S*ession Sitzung
Sitzungsauf- und Abbau
---
4 *T*ransport TCP / UDP (Port Steuerung)
Fehlerkorrektur, Flusskontrolle, Multiplexing
---
3 *N*etwork IP-Routing (Netzwerk)
Logische Adressierung, IP, Routing, Protokolle: ICMP IP
---
2 *D*ata-Link MAC-Adresse (Sicherung/Verknüpfung)
Physische Adressierung, Frame-Relay, PPP, Ethernet, Fehlerkennung
1 *P*hysical Kabel
Ethernet, Token-Ring

http://de.wikipedia.org/wiki/OSI-Modell

[**A**]libaba [**P**]räsentiert [**S**]ich [**T**]äglich [**N**]ackt [**D**]em [**P**]ersonal
http://alle-eselsbruecken.de/osi-schichtenmodell/

Grafik zum OSI-Modell, die wunderbar einfach die einzelnen Schichten erklärt:
http://gargasz.info/wp-content/uploads/2010/01/OSI_model_LAN.jpg

Datenkapselung

http://de.wikipedia.org/wiki/Datenkapselung_%28Netzwerktechnik%29

PDU
Protocol Data Unit

L**4**PDU | TCP | Daten | <= Segment
Quell- & Zielport

L**3**PDU | IP | TCP | Daten | <= Paket
Quell- & Ziel IP

L**2**PDU | EH | IP | TCP | Daten | ET | <= Frame
Quell- & Ziel MAC FCS
Frame Check Sequence

MTU
Max. Transfer Unit 1500bytes bei IPv4

PDUs in Beziehung zu jedem der vier ersten Schichten des OSI-Modell:

Im Layer 1 (Physical Layer) entspricht die PDU dem Bit
Im Layer 2 (Data Link Layer) entspricht die PDU dem Frame
Im Layer 3 (Network Layer) entspricht die PDU dem Paket
Im Layer 4 (Transport Layer) entspricht die PDU dem Segment

Ab Layer 5 werden übertragene Inhalte als Daten bezeichnet.

https://de.wikipedia.org/wiki/Service_Data_Unit

Das Binärsystem

Ein Block in einer IPv4 wird binär zu folgender Basis in Potenzen berechnet:

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

Beispiel: in 8 Bits:

192 = 128 + 64 +0 +0
|1|1|0|0|0|0|0|0|

Die 128 passt einmal rein, also erster Block = 1
Zum Rest Passt die 64 hinzu also zweiter Block = 1
Die Zahl ist Vollständig es folgen Nullen

Eine IPv4-Adresse besteht aus 4 Blöcke zu je 8 "Bits" also in Binär aus 32 Stellen:

Beispiel:

192.168.0.1

Wir wissen :

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

Jetzt stellen wir uns jeder dieser 8 Werte als An- und Ausschalter vor.

1= an
0= aus

192 = 128 + 64 +0 +0
| 1mal 128 | 1 mal 64 | 0 mal 32 | 0 mal 16 | 0 mal 8 | 0 mal 4 | 0 mal 2 | 0 mal 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
11000000

168 = 128 + 32 + 8

|1|0|1|0|1|0|0|0|
10101000

0 = 00000000

1 = 00000001

Dies ergibt Binär: 11000000.10101000.00000000.00000001

IPv6

Eine IPv6-Adresse besteht aus 8 Blöcken zu je 16 "Bits" also in Binär aus 128 Stellen, sie wird zur besseren Lesbarkeit hexadezimal (4 Stellen) notiert:

Beispiel:

2001:0db8:85a3:08d3:1319:8a2e:0370:7344

Um diese hexadezimale Schreibweise in die binäre Schreibweise umzuwandeln, muss man zunächst den Umweg über die dezimale Notation nehmen oder untenstehende Tabelle zur Hand nehmen. Binär notiert sieht die IPv6-Adresse dann so aus.

0001000000000001:0000110110111000:1000011010100011:0001001100011001:
1000101000101110:0000001101110000:**0111001101110111**

Nehmen wir einen Block aus einer IPv6-Adresse (:hier mal den Letzten)

| **0111 | 0011 | 0111 | 0111 |**

A	B	0	9
1010	1011	0000	1001

Übung: von Hex nach Bin anhand :

C	D	F	A	>>	1100	1101	1111	1010
9	F	A	D	>>	1001	1111	1010	1101
1	9	A	F	>>	0001	1001	1010	1111
F	E	8	0	>>	1111	1110	1000	0000
F	F	0	2	>>	1111	1111	0000	0010

Erweiterung zu einem größeren Zahlenraum: (erstmal nicht anschauen)

Dezimal DEZ	Binär BIN	Hexadezimal HEX
15	1111	F
14	1110	E
13	1101	D
12	1100	C
11	1011	B
10	1010	A
9	1001	9
8	1000	8
7	0111	7
6	0110	6
5	0101	5
4	0111	4
3	0011	3
2	0010	2
1	0001	1
0	0000	0

Dezimal zu Binär kann man auch schriftlich rechnen:
http://www.arndt-bruenner.de/mathe/scripts/Zahlensysteme.htm

Die Dezimalzahl 20 wird ins 2er-System umgewandelt

Gehe nach folgendem Verfahren vor:

- Teile die Zahl mit Rest durch 2.
- Der Divisionsrest ist die nächste Ziffer (von rechts nach links).
- Falls der (ganzzahlige) Quotient = 0 ist, bist du fertig, andernfalls nimm den (ganzzahligen) Quotienten als neue Zahl und wiederhole ab (1).

20 : 2 = 10 Rest: 0
10 : 2 = 5 Rest: 0
5 : 2 = 2 Rest: 1
2 : 2 = 1 Rest: 0
1 : 2 = 0 Rest: 1

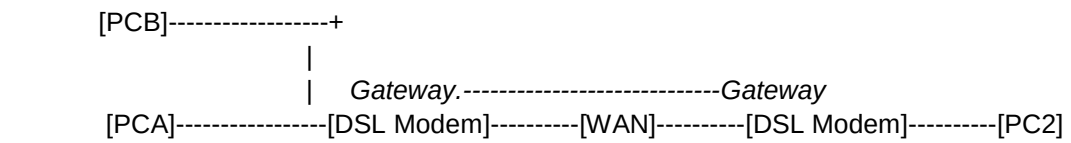
Resultat: 10100 (Wichtig: von unten nach oben!)

19.03.2015

8:00 - 8:15 Gespräch mit Herrn Rautenkranz, Frau Hergt und Herrn Ptak zur unbefriedigenden Unterrichtssituation am Vortag

Netzwerke

IP 192.168.11.11
Subnet 255.255.255.0



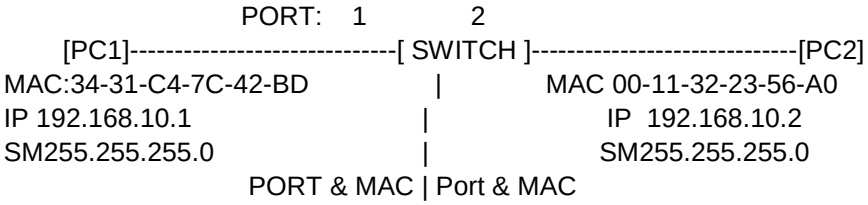
	dns	
IP	192.168.1.10	172.16.15.20
Subnet	255.255.255.0	255.255.255.0
dns	192.168.1.1	172.16.15.1
Gateway	192.168.1.1	172.15.15.1

- Ein Gateway wird in einem internem Netzwerk nicht benötigt, es wird gebraucht um einen Ort außerhalb des internen Netzwerkes anzusprechen.

*DNS= Domain Service - Übersetzt den Namen des PCs in eine IP
*LAN= Local Area Network
*WAN= Wide Area Network

>arp -a< zeigt die Übersicht aller bekannten IP-Adressen an

SWITCH



Der Kommunikationsweg in OSI-Layern gesehen:

PC1 - Layer 1 (**1** *P*hysical) Kabel zu Switch
SWITCH - Layer 2 (**2** Data-Link) L**2**PDU wird benötig, weil diese Quell- & Ziel MAC enthalten
PC2 - Layer 1 (**1** *P*hysical) Kabel zu PC2

Aufsetzen eines Servers und Zwei Clients

Virtualbox:
Netzwerk > Internes Netzwerk > Name : Schulungsnetz

Server :
Windows 2012 R2 Datacenter mit grafischer Oberfläche
Name: Server
Arbeitsgruppe: WORKGROUP (Standard)

Beide Clients:
Windows 7 Ultimate
Name: PC1 (2)
Arbeitsgruppe: WORKGROUP

*"**Nicht identifiziertes Netzwerk**" unter Windows 7 - was nun? Die lokalen Sicherheitsrichtlinien lassen sich mit **secpol.msc** konfigurieren. Unter Netzwerklisten-Manager-Richtlinien auf Eigenschaften von "Nicht identifizierte Netzwerke" gehen und dort den **Standorttyp** festlegen. Nun wird das "Nicht identifizierte Netzwerk" als Arbeitsplatznetzwerk verstanden, was als kleiner Zusatz zur Typenbezeichnung im Netzwerk- und Freigabecenter zu sehen ist.*

Apipa = Automatic Private IP Adressing

Ein Rechner versucht bei einem DHCP-Server seine TCP/IP-Adresse und andere wichtige Einstellungsparameter anzufordern.

Erreicht der Rechner jedoch keinen DHCP-Server, z.B. weil keiner im gleichen Segment aktiv und auch über DHCP-Relay nicht zu erreichen ist, so bekommt der Rechner automatisch eine zufällige Adresse aus dem Bereich 169.254.x.x.

PC1

- CMD als Admin >arp -a
- Netzwerk & Freigabecenter>LAN-Verbindung>Eigenschaften>TCP/IPv4
  IP 192.168.10.1
  SUBNET 255.255.255.0

PC2

IP 192.168.10.2
SUBNET 255.255.255.0

...

Auf **PC1** : ping 192.169.10.2 >Verlust 0%

Auf **PC1** und **PC2** deaktivieren der Firewall

Auf **PC1** : ping 192.169.10.2 >Verlust 0%

Auf **PC2** : arp -a >Die IP von PC1 ist bekannt

IP Adresse:

Eine IPv4 besteht aus vier sogenannten Oktetten. Das sind vier Blöcke zu je acht An-Aus-Zuständen. Also:
▓▓▓▓▓▓▓▓ . ▓▓▓▓▓▓▓▓ . ▓▓▓▓▓▓▓▓ . ▓▓▓▓▓▓▓▓

.
/ \ 2^0 = 1
| 2^1 = 2
| 2^2 = 4
| 2^3 = 8
| 2^4 = 16
| 2^5 = 32
| 2^6 = 64
| 2^7 = 128
SUMME 255

Der maximale Wert ist 255

IP dezimal	192	168	10	1
IP binär	11000000	10101000	00001010	00000001
Subnetzmaske	255	255	255	0
SM binär	11111111	11111111	11111111	00000000
	255	128	0	0
	11111111	**1**0000000	00000000	00000000

Subnet-Bits Host-Bits

Subnet-Bit-Bereich unveränderbar - bestimmt das Subnetz (Identität)

Host-Bits : Frei vergebbar

2^Host-Bits = Anzahl IPSs

Hier 23 mal die 0 (von hinten gesehen) >> 2^23 = 8.388.608 zu vergebene IP-Adressen

2^Host-Bits - 2 = Anzahl <u>gültiger</u> IPs

z.B.
192.168.10.**0** > Reserviert für Subnet
192.168.10.**255** > Reserviert für Broadcast

Es werden zwei Hostbits reserviert.
Das Subnetz ist die erste Adresse im Netz und der Broadcast die letzte.

2^Subnet-Bits = Anzahl der Netze

Übung: 02+-+Subnettung-09-11-2009

Beispiel:

IP-Adresse : 212 15 12 120
Subnet: 255 255 255 240

IP Binär: 11010100 00001111 00001100 01111000
SNBinär: **11111111 11111111 11111111 11110000**

Die letzten vier Bits in diesem Beispiel, und im allgemeinen immer die letzten zusammenhängenden Nullen der binären Subnet-Maske nennen sich **Host-Bits**. Diese bestimmen die maximale Anzahl von IP-Adressen in einem Adressbereich, zu denen Aber auch die erste für die Subnet selbst und die letzte für den Broadcast reserviert wird, damit diese immer zu gleichen Bedingungen zu finden sind.

Die binäre Adresse des Subnetz innerhalb des Netzwerkes wird durch logische Addition der binären IP-Adresse und der Subnetzmaske gebildet und lautet also :

11010100 00001111 00001100 0111**0000**

und die binäre Adresse des Broadcasts somit, dafür werden die Bits im Netzanteil auf 1 gesetzt:

11010100 00001111 00001100 0111**1111**

Im Umkehrschluss ergeben sich darus folgende IP-Adressen

Subnet 212 15 12 **112**
Broadcast 212 15 12 **127**

Da diese beiden IP-Adressen innerhalb des Adressraumes somit vergeben sind, ist der Adressberech, welcher an Clients vergeben werden kann um zwei kleiner, also genau zwischen Subnet und Broadcast. Hier:

Von 212.15.12.**113** bis 212.15.12.**126**

20.03.2015

Aufarbeitung der Übung 02+-+Subnettung-09-11-2009

Aufgabe:	IP-Adress-Bereich
1	**212.15.12.113 - 212.15.12.122**
2	**199.1.7.17-199.1.7.22**
3	**172.16.32.56-172.16.32.94**
4	**130.198.3.193-130.198.3.254**
5	**45.67.0.1 - 45.127.254**
6	**192.168.11.121 - 192.168.11.122**
7	**178.21.45.65 - 178.21.45.95**
8	**222.34.98.1 - 222.34.98.14**
9	**10.8.0.1 - 10.15.255.254**
10	**155.23.82.1 - 155.23.83.254**

Logische Und-Adressierung von IP und Subnet

1+1=1
1+0=0
0+0=0

Die Subnetz-Adresse ist immer gerade oder 0
Die Broadcast-Adresse ist immer ungerade

11010100 00001111 00001100 01111000 IP
11111111 11111111 11111111 1111**0000** SUBNETMASKE
11010100 00001111 00001100 0100000 SUBNETZ (Adresse)
11010100 00001111 00001100 01111**1111** Broadcast (Adresse)

(=invertierte Host-Bits)

2^32	**~ 4,3 Mrd**
…	
2^24	~ 16,7 Mio
...	
2^16	= 65536
...	
2^13	= 8192
2^12	= 4096
2^11	= 2048
2^10	**= 1024**
2^9	= 512
2^8	= 256
...	

CIDR

Classless interdomain Routing

Stellt die Summe der Anzahl der Subnet-Bits dar, so
entspricht
255.255.255.0
der CIDR
11111111.11111111.11111111.00000000

8 + 8 + 8 + 0 = 24

/24 , welche so dargestellt wird

So sind in einem 32-Bit großen IPv4-Netwerk hier 24 Subnet-Bits. Es verbleiben 8 Host-bits.
So lässt sich nun rechnen :

2^(Anzahl der Host-Bits)
2^8 = 256

Aufgrund der Subnet- und Broadcast- Adresse müssen nun noch zwei Bits abgezogen werden, damit die Anzahl der zu vergebenden Adressen berechnet werden kann.

2^(Anzahl der Host-Bits) -2 = Anzahl der zu vergebenden IP-Adressen

hier: (2^8)-2 = 254

Netzwerkklassen

Klasse A Netz

16.777.214 vergebbare IP-Adressen

Beginn des Netzes bei :	1.0.0.0
Ende des Netzes:	126.0.0.0
Standard Subnet-Mask :	255.0.0.0 - /8
Privat:	10.0.0.0/8
Spezial:	0.0.0.0 (Gateway of last resort)
	127.0.0.0/8 (Local Host)

Klasse B Netz

65.534 vergebbare IP-Adressen

Beginn des Netzes bei :	128.0.0.0
Ende des Netzes:	191.255.0.0
Standard Subnet-Mask :	255.255.0.0 - /16
Privat:	172.16.0.0/12

Spezial: 169.254.0.0/16 (Apipa)

Klasse C Netz

254 vergebbare IP-Adressen

Beginn des Netzes bei : 192.0.0.
Ende des Netzes : 233.255.255.0

Standard Subnet-Mask : 255.255.255.0

Privat: 192.168.0.0/24
Spezial: -

Zeit sparen bei Subnetting Aufgaben

Bestimmen der Netzwerk-Schrittweite

- Subtrahiere von die Basis einer 32-Bit IPv4-Adresse (256) das Oktett des Umbruchs der Subnetz-Maske und erhalte die „*Magic Number*“:

Beispiel:

128.0.0.0	256 minus 128 = 128
255.**192**.0.0	256 minus 192 = 64
255.255.**224**.0	256 minus 224 = 32
255.255.255.**248**	256 minus 248 = 8

Bestimmen der Subnet-Adresse:

Beispiel:
IP 172.26.180.185
Subnet-Mask 255.255.248.0

- Wir betrachten weder 172.26. noch .185.
- Zuerst bestimmen wir die „Magic Number“

  256 minus 248 = **8**

- Jetzt teilen wir aus den Wert dem selben Oktett der IP durch unsere „Magic Number“

  180 / **8** = 22.5

  Wir benötigen nur ganze positive Zahlen, also ist das Ergebnis hier 22

- Dieses Ergebnis multiplizieren wir mit unserer „Magic Number“

  22 mal 8 = 176
  176 ist der Wert für die Subnet-Adresse – Es folgen Host-Bits

Subnet-Adresse 176.26.176.0

Ableiten der Broadcast-Adresse von der Subnet-Adresse:

IP 172.26.180.185
Subnet-Mask 255.255.248.0
Subnet-Adresse 176.26.176.0

- Wir betrachten immer noch das selbe Oktett, dismal bei unserer Subnet-Adresse, sie ist der Anfang des Adress-Raumes
- Jetzt Addieren wir zu dem Betrachteten Wert unsere „*Magic Number*“ und ziehen 1 ab (Der Basis 256 ist der Wert 0 auch enthalten,..)

176 + 8 -1 = 183

Die restlichen Host-Bits werden mit 255 (also binär mit 11111111) aufgefüllt
Broadcast-Adresse 176.26.183.255

Beispiel 2:

IP 10 . 20 . 30 . 40
SM 255 . **248** . 0 . 0
SN 10 . 16 . 0 . 0
BC 10 . 23 . 255 . 255

256-248 = **8** < Magic Number
20/8 = 2 (Ergebnis in ganzen positiven Zahlen
SN: 2*8 = 16
BC: 16 (SN)+8 (MN) -1 =23

> Subnetz(Adresse) 10.16.0.0
> Braodcast(adresse) 10.23.255.255

Man sollte nochmal erwähnen, dass die MN auch die Schrittweite ist. Deswegen wird sie ja aufaddiert. Die Verwirrung entsteht vielleicht auch durch die Tatsache, dass gewöhnlich die Netzwerkadresse bspw. 192.168.178.0 ist uns somit folglich auch die Broadcast Adresse 255(Schrittweite). Kennt jeder Fritzbox Anwender, die 1 ist die Fritzbox, Rest angedacht. Da standardmäßig immer von 255.255.255.0 als Einstellung ausgegangen wird, ist das jedem bekannt.

http://ecampus20.wbstraining.de/goto.php?target=file_272065_download&client_id=wbs20
So der Fehler ist so markiert, dass die, die schon runtergeladen hatten, den Fehler erkennen.111 statt 115(in Klammern)

23.03.2015

Subnetting
- Wiederholung & Übung
- http://www.eex-online.de/informatik/vlsm.html

24.03.2015

- Neuer Dozent - Frank Viehwegner

- Überblick über die Thematik Netzwerken und Diensten im Netzwerkumfeld

Grundlagen der Internettechnologie (ab hier, mit neuem Dozenten: Frank Viehweger)

Definition Internet (aus Anwendersicht):

"Das Internet" beschreibt eine technische Infrastruktur zum Austausch von Nachrichten.

- Zusammenschluss von vielen weltweit verteilten einzelnen Netzwerken
- Netzwerkübergreifende Kopplung dieser Art bedarf eine einheitliche Kommunikationsform
- Netzwerke werden durch Router verknüpft, welche Netzwerk-"Knoten" sind.
- Charakterisiert durch eine für jeden eingebundenen Rechner eindeutige identifizierbare ID
- die "Identifizierende Adresse" ID ist eine 32bit-Zahl (IPv4) oder 128bit-Zahl (IPv6)
- Jeder Rechner im Internet ist durch eine "Zahl zwischen 0 und ca. 4mlrd (2^32-1) abgebildet"
- Rechner A Adressiert ein Paket an die ID (IP) des Rechners B
- Router sorgen für die Zustellung, die Vermittlung
- Vergleich **Telefon**: Teilnehmer1 wählt Telefonnummer, wird vermittelt zu Teilnehmer2
  Ein Übertragungskanal - eine ganz Bestimmte Verbindungsstrecke wird für eine bestimmte Zeit hergestellt und bleibt für die gesamte Zeit des informations-Austausches bestehen : **Kanal-Orientierte Übertragung.**
  (Vorteil: Exklusiv: kein Anderer kann "stören")

- Tatsächlich funktioniert das **Internet** anders als das Telefonnetz:

Die Kommunikation im Internet erfolgt grundsätzlich Verbindungslos: Es gibt zu keinem Zeitpunkt während eines Nachrichtenaustausches eine direkte (elektrische) Verbindung zwischen Sender und Empfänger.

Zur technischen Realisierung des Internets kommen unterschiedlichste Basistechnologien zum Einsatz, z.B. analoge Übertragungstechniken (PCM, Telefonie), digitale Übertragungstechniken (ISDN, ATM, Ethernet), optische Übertragungstechniken (FDDI,..), Funktechniken (Sat-Kommunikation, WLAN, WiFi,..)

Nachricht wird von Sender bis zum ersten Router geschickt.
Wenn man von einer Verbindung sprechen kann, wird diese nur zwischen zwei "*Knoten*" hergestellt und von diesem zum nächsten *Knoten* weitergeleitet. Eine direkte Verbindung zwischen Sender und Empfänger wird **NIE** hergestellt.
Nachrichten werden als Einzelteile betrachtet, welche mit einer vollständigen Adressierung versehen und durch das Internet geleitet werden. Jeder Router entscheidet, welchen Weg das Paket weiterhin nimmt : **Paketorientierte Kommunikation**.

- Verweis auf ARPA. Ziel: Aufbau eines Kommunikationssystems, dass auch bei teilweiser Zerstörung der Infrastruktur weiter funktioniert.
- **Routing**: selbstorganisiertes zielorientiertes Versenden auch auf Umwegen

Nachrichten werden in Datensegmente (Pakete) zerlegt, adressiert und weitergeleitet Router entscheiden im klassischen Internet frei über die Auswahl der Pakete. **Jedes Paket wird** ***(Verweis auf IPv6: hier wird das Routing in Teilen anders gehandhabt)***

Die Internet-Infrastruktur kann und wird für eine Vielzahl unterschiedlicher Anwendungen (Dienste) genutzt.

- **Dienste**: Web-Seiten, Video-Streaming, Daten-Versand, E-Mails,...

  Im Internet wird klar zwischen Basistechnologien (Logisch) und darauf aufbauenden Anwendungstechnologien unterschieden.
  Unterteilung in Funktionsbereiche.
  Technische Funktionen: Adressierung, Paketierung, Nachrichtenweiterleitung, ...
  - stellt die Infrastruktur selbst bereit

  Anwendungsfunktionen: (aus Nutzersicht "eigentliche Qualität des Internets)
  - bestimmen die Art der Nutzung der Infrastruktur

- Zugangsmöglichkeiten:

  Beschreibt die strukturellen Bedingungen zur Nutzung des Internets

  grundsätzlich benötigt:
  - Endgerät (Smartphone, PC,etc)
  - Physische Verbindung (Kabel, Modem,... Router)
  - Gültige Adresse (Internetweit eindeutige gültige IP-Adresse)
  - Verbindungprogramm (Zugangssoftware: Browser, Dienste-Client)
  - logische Verbindung (Internetkommunikation : Endgerät <> Router)

  Verbindungsarten: Telefonie, Satellit, Kabel-Modem, Elektro-Netze, Mobil, usw...

- **QOS** : Quality Of Service :

Verfügbarkeit, Kapazität, Fehlerrate, Schwankungen, Zugriffszeit (Latenz), Kosten sind die Entscheidungsgrundlage für die Vermittlung von Daten durch Router
  - Teure Verbindung: niedrige Bandbreite, hohe Latenz, geringe Kapazität

- **Daten-Segmente** : Segment-Nummern.

Die Empfangsreihenfolge entspricht aufgrund des Routings nicht zwingend der Sendereihenfolge der Daten-Segmente. Durch die Nummerierung wird die Zuordnung und Wiederherstellung der Nachricht ermöglicht.

- **Netzneutralität** :
  - **IPv4** hat nur rudimentäre Vorraussetzungen zur Priorisierung
    - **TOS** (Type of service) im Header könnte die Priorität der Nachricht zuordnen
  - bei **IPv6** kann das Routing vordefiniert werden
    - gibt es bereits vordefinierte Bereiche im Header für solche Funktionen

- **Infrastruktur-Dienste** / Protokolle: DNS, DHCP, NTP, ICMP (Funktionen)

DNS : Domain Name Service (Namensauflösung
DHCP: Dynamic Host Configuration Protrocol (z.B. Zuweisen von IP-Adressen)
NPT: Network Time Control (Synchronisierung von Zeit)
ICMP: Internet Control Message Protocol (Timeout,
  Verwendet z.B. tracert bei der Verwerfung von nicht zustellbaren Paketen)

- **Anwendungsorientierte Dienste** / Protokolle: WWW (http/https), ftp, SMTP,

  POP3, IMAP,... (Nutzbare Merkmale)

Protokolle und Dienste:

Protokolle *sind Vereinbarung über die Art und Weise der Durchführung einer bestimmten Ebene der (technischen) Kommunikation.*

Dienste *sind Funktionen, die aus der Nutzung eines Kommunikationssystems heraus bereitgestellt werden können und bezieht sich dabei auf bestimmte Protokolle.*

SAP - Service-Access-Point - Stellt die Verbindung zwischen oder den Zugriff auf ein Protokoll dar - Protokollschnittstelle

Vollständige Kommunikationssysteme *sind jene, welche Anwendungs-, Netzwerk- und Übertragungsprotokolle gleichermaßen verwenden.*

Transitprotokolle *sind jene, welche nur jenen Teil der benannten Protokolle verwenden, welcher zur Übermittlung notwendig sind.*

Im Internetumfeld verfügbare Dienste:

Dienst	Protokolle
WWW	http,https, dns
eMail	pop3, smtp, imap
FTP	ftp
Usenet	nntp
Telnet	telnet
SSH	ssh
RDP	...
VNC	rfp

Jedes Protokoll (nicht jeder Dienst!) besitzt eine für das jeweilige System eindeutige ID - das ist die ***Port****nummer (max 65535 = 2^16-1)*

Anwendungsprotokolle:
DNS, DHCP, NTP Port-Adresse

http/https,pop3,smtp,imap,ftp

Netzwerkprotokolle:
IP,TCP, UDP IP-Adresse

Übertragungsprotokolle:
Ethernet, ATM, ISDN MAC-Adresse

Auf jedem Rechner existiert eine Datei mit den von der IANA empfohlenen Port-Dienst Kombinationen: Windows\System32\drivers\etc\services unter Windows. Unter Linux /etc/services.

Well known Ports: 1-1023 (<1024) Sollten bekannt sein und nicht verändert werden.

*Oberhalb von Port 1023 finde sich u.A. Unternehmens- oder Anwendungsbezogene Ports, also nicht standardisierte Ports. In den sogenannten **Hohen Ports** (high Ports) liegen dynamische Ports, welche die Steuerung von Geräten und Rechnern ermöglichen.*

Bzw. "Trojanerports"

CMD> netstat Zeigt die gegenwärtigen Verbindungen und den

diesen zugeordneten Portnummern

CMD> netstat -a ...und die lauschenden Ports *g*

Übung:

Fragestellung: Ist es sinnvoll, die regelmäßige Datensicherung auf einen externen Server ("Cloud") durchzuführen?

Fakten:
- Zu sichernder Datenbestand: 2 TB
- Täglich ändern sich max. 200GB
- Tägliche Datensicherung erforderlich, um bei Datenverlusten im Worstcase höchstens die Veränderung eines Tages zu verlieren.
- Start der Datensicherung: 22Uhr
- Netzwerkverbindung:
  20Mb/s Downstream (download)

5Mb/s Upstream (upload)
- Verfügbarkeit der oben genannten Leistungskapazitäten für den Backupprozess: 30%

Wie lange dauert eine Datensicherung?

Datenmenge:

2TB = 2 Terrabyte = 2048 GB
2TiB = 2048 GiB

Upstream:

8 bit = 1 Byte

5 Mb/s = 5 Megabit/s geteilt durch 8 Bit = 0,625 Megabyte/s
0,625 MB/s = 0,625 MB/s * **1000 *1000** = 625000 Byte/s
megabyte zu kilobyte ...kilo zu Byte
625000 Byte/s = 625000/**1024** = 610.35156 KB/s
610.35156 KB/s = 610.35156/**1024** = 0,5960464 MB /s
0,5960464 MB /s = 0,5960464 / **1024** = 0,0005821 GB/s

Verfügbarkeit der Leistungskapazität :

30% = 0,0001746 GB/s

Berechnung:

2048 GIB / 0.0001746 GB/s = 11729667,81 s
:3600s = 3258,241 h
:24h = 135,76 d

= 135 Tage 18 Stunden 14 Minuten 24 Sekunden!!!!!

Wie lange dauert die tägliche Datensicherung?

Die Datenmenge beträgt 10% des Gesamtdatenvolume.

Bei gegebener Leitungskapazität dauert die tägliche Datensicherung ca. 14 Tage

Wie lange dauert eine vollständige Rücksicherung?

Die Leitungskapazität für den Download ist 4 mal größer und somit ist die Dauer des Transportes 4 mal kleiner:

Die Rücksicherung der Gesamtdatenmenge von 2TB dauert ca. 34 Tage

(Also im Großen und Ganzen ist dieses Beispiel in der Praxis eher nicht

umsetzbar und auch nicht Sinnvoll)

http://www.heise.de/netze/tools/bandbreitenrechner/ (Um es zu vereinfachen)

Grundlagen Webhosting

Übung:

Versetzen Sie sich bitte in das folgende Szenario:

Sie sind als Fachmann/-frau in eine Diskussion auf GF-Ebene in Ihrem Unternehmen einbezogen. Es geht um das zukünftige Hosting der Unternehmenswebsite.

Es soll ein neuer Hoster ausgewählt werden oder als Alternative das Hosting auf einem Server innerhalb der eigenen IT-Infrastruktur des Unternehmens diskutiert werden.

Welche Kriterien sind für die Hosting-Entscheidung zu berücksichtigen?

Zum Sicherheitsaspekt :

- Einerseits unerwünschte Zugriffe vermeiden
- Andererseits gewünschten Zugriffen den Zugang zu geschützten Bereich verbieten

Ziele dieser Aufgabenstellung:

- Aufführen der zu Beachtenden Merkmale für die Wahl des Web-Hosters
- Kontextbezogenheit zum Nutzungstyp der Website
- Abschätzung der Kosten/Aufwand Frage

***Unternehmenspräsentationen** und Seiten mit **Dynamischem Inhalt** werden in der Regel auf Web-Hostern (bei Providern) abgelegt, da diese "Standard-Systeme" um ein vielfaches günstiger angeboten werden, als sie selbst realisiert werden können*

*Bei **eShopsystemen** sind die Anforderungen oft so spezifisch (hoch), dass es sich als günstiger ergibt diese selbst abzubilden.*

Kriterien	Nutzungstyp		
	Unternehmens-präsentation	Dynamischer Content, CRM	eShopsystem
- Website-Charakteristik			
▪ prognostizierte Nutzungsverhalten	2	5	9
▪ Lastspitzen	2	3	8
▪ Verfügbarkeit	4	5	9
- Kosten			
▪ Hardware	3	4	8
▪ Software	1	5	7
▪ Betrieb	2	2	8
▪ Personal	3	4	8
- Fachliche Kompetenzen	3	7	7
- Quality of Service			
▪ Verfügbare Bandbreite	4	4	7
▪ Leitungsverfügbarkeit	2	3	8
▪ Verzögerungen (Delay)	2	2	8
▪ Schwankungen (Jitter)	1	3	8
▪ Bitfehlerraten	3	3	9
- Sicherheitsaspekte			
○ Firewall / DMZ	6	6	9
▪ Serversicherheit	6	6	9
▪ Updatestatus	6	6	9
- Lastenausgleich (Load Balancing)	1	3	8
- Serversynchronisation	1	3	8
- Webserver-Funktionalität			
▪ Scripting-Unterstützung	5	10	10
▪ Datenbankunterstützung	2	10	10
(MySQL, MS SQL Server, Oracle)			
▪ CMS-Unterstützung	5	7	4
(Typ3, Drupal, Wordpress)			
- FTP-Zugang	8	9	9
- ssh-Zugang	2	9	9
- Dedizierter Server	3	5	9
(Der Server bleibt ungeteilt mir anderen WS-Nutzer,			
Software kann nach belieben hinzugefügt werden)			

Sicherheitskonzept (für den Betrieb eines Web-Servers)

Welche Aspekte müssen bei der Erstellung eines Sicherheitskonzeptes im Zusammenhang mit dem Betrieb eines öffentlich erreichbaren Webservers beachtet werden?

Anwendungsbereich

(z.B.) Bereitstellung eines http/https-basierten Dienstes innerhalb der Unternehmens-IT-Struktur für Zugriffe aus dem öffentlichen Netz und dem Intranet.

Funktionsbereich

Umfasst die genaue Funktionsbeschreibung des (Web-) Dienstes.
Techn. Beschreibung der Zugriffswege und -verfahren: Ports, Adressbereiche, Schnittstellen
Definition spezieller Zugriffsverfahren (anwenderseitig, administrativ): https, ssh
Bereitstellung und Einrichtung von Verschlüsselungs- und Authentifizierungsverfahren
Zertifikats- und Schlüsselverwaltung

Zustandsdefinition

Normalbetrieb
Eingeschränkter Betrieb
Fehlerzustand
Worst Case /!\

Aspekte

- Personell
  - Verantwortlichkeit / Zuständigkeit
  - Audits (Bewertungen), Protokollierung,
  - Termine, Zyklen
  - Weiterbildung

- Strukturell
  - Standort-Sicherheit (Zugang zum Server (-raum)
  - Firewall-Konstellation (Konstellation = nicht "wie", sondern "wo")
  - DMZ (Demillitarisierte Zone)
  - Stand-Alone-Server / Virtuelle Server / Serverfarm

- Organisatorisch
  - Berechtigungen
  - Dokumentation
  - Monitoring
  - Protokollierung

- Softwareseitig
  - Betriebssystemsicherheit ("Härten")
  - Anwendungssicherheit
  - Sicherheit assoziierter Dienste
  - Update-Routinen
  - Firewall-Konfiguration
  - Antivieren- / Antitrojanersoftware
  - IDS / IPS

- Anwenderseitig
  - Nutzerschulung
  - Passwort-Regime

- Contentseitig
  - Scriptsicherheit
  - Urheberrechtsfragen

*Verweis auf die Dozentengeführte Mitschrift im Excel-Format zur Erläuterung der **DMZ***

Datensicherung und Ausfallsicherung:

Verfügbarkeit (**Hochverfügbarkeit** = 99,99% Verfügbarkeit - knapp eine Stunde Ausfall im JAHR)

http://de.wikipedia.org/wiki/Hochverf%C3%BCgbarkeit

Beschreibt die Wahrscheinlichkeit, dass ein bestimmtes System X in einem gewissen Zeitraum NICHT ausgefallen ist.

Ein **System** besteht logischerweise aus einer großen Anzahl von Einzelkomponenten, welche mit einer relativen Wahrscheinlichkeit ausfallen können.

> Dozenten-Mitschrift: Tabelle - Verfügbarkeit

Fällt also eine Komponente aus, entfällt die Verfügbarkeit des ganzen Systems.

*Die **Gesamtverfügbarkeit** des Systems ergibt sich aus der Multiplikation der **Einzelverfügbarkeiten**.*

http://upload.wikimedia.org/math/5/3/c/53c767b6f099aba0c224fd6e5e4fb01b.png

Beispiel **Webserver**:

Für Verfügbarkeit erforderliche Komponenten (Auswahl!):

- Stromversorgung
- Netzteil
- Festplatte(n) >MTBF
- Mainboard
- Lüfter
- Netzwerkanschluss
- Netzwerk-Verbindung zum Internet
  - LAN-Verkabelung
  - Switches
  - Firewall
  - Router
  - DSL-Modem

- Betriebssystem
- Webserver-Software
- Datenbank-Software
- DNS
- ...

http://upload.wikimedia.org/math/c/c/0/cc0c1d1efe12de7cafa08a9f8293fe4b.png

Redundanz

- Einsatz von Einzelkomponenten mit geringerer Ausfallwahrscheinlichkeit (z.B. 24/7 HDD's, RAID-Systeme)
  Reduntante Netzteile bestehen aus austauschbaren Modulen, die einander bei Ausfall des einen ersetzten
- Doppelte Auslegung einzelner Komponenten, welche eine unterbrechungsfreie Stromversorgung für alle Komponenten voraussetzt (USV , Netzersatzanlagen)
- Redundante (virtuelle?) Server
- Wärmelast-(Temperatur-) Puffer (Klima-Anlange, etc.)
- Redundante Netzwerk-Adapter
- Fallback-Varianten (ISDN ...)

...

- Server-Farm
- Load-Balancer
- DB-Cluster
- Multi-DNS-Server

http://de.wikipedia.org/wiki/Redundanz_%28Technik%29

Mathematische logische Rechenarten

> Verweis auf Script-Grundlagen.docx

AND > Reihenschaltung

Wahrheitstabelle:

A	B		(AND)
0	0	=>	0
0	1	=>	0
1	0	=>	0
1	1	=>	1

OR > Parallelschaltung

Wahrheitstabelle:

A	B		(OR)
0	0	=>	0
0	1	=>	1
1	0	=>	1
1	1	=>	1

NOT > Relaisschaltung

Wahrheitstabelle:

A		(NOT)
0	=>	1
1	=>	0

XOR

Wahrheitstabelle:

A	B		(XOR)
0	0	=>	0
0	1	=>	1
1	0	=>	1
1	1	=>	0

XOR Beispiel:

```
01000001  \
              >----- 00000011
01000010  /
```

RAID - Redundant Array of Independent Disks

RAID-Level:0,1,5,6,01,10,15,51,JBOD

JBOD: Just a Bunch of Disks - "Nicht-RAID"

RAID **0**: mehrere HDDs (>=2), keine Redundanz, verteiltes Schreiben und Lesen
Ziel: Performancegewinn durch Beschleunigung d. Schreib-/Lesezugriffe
Kapazität des RAID: Brutto=Netto

RAID **1**: "Mirroring", Festplattenspiegelung (>=2 HDDs), Redundantes Speichern
Ziel: Ausfallsicheres Speichern durch Redundanz.
Kapazität des RAID: Brutto=2*Netto

RAID **5**: Verteiltes Speichern über mehrere HDDs mit Redundanzinformationen, (>=3HDDs)
Ziel: Ausfallsicheres Speichern durch Redundanz (genau **1** beliebige HDD im Verbund kann ohne Datenverlust ausfallen)
Kapazität des RAID: [n Hdds im RAID]: Netto=(n-1)*(Kapazität der kl. HDD)

Übung:

ASCII:

Zeichen	Dezimal	Dual	A XOR B
A	65	01000001	00000011
B	66	01000010	
C	67	01000011	C XOR D
D	68	01000100	00000111

RAID5-Festplattenverbund:

HDD1	HDD2	HDD3	HDD4
A	B	A XOR B	
D	C XOR D		C

HDD1	HDD2	HDD3	HDD4
01000001	01000010	**00000011**	
01000100	**00000111**		01000011

Wiederherstellen der Information A durch Anwendung von XOR auf die Werte B und A XOR B, bzw. C und C XOR D

B XOR **A-XOR-B**
B 01000010 _____ 01000001 = A
A XOR B 00000011 /

C XOR **C-XOR-D**
C 01000011 _____ 01000100 = D
C XOR D 00000111 /

RAID **6**: Verteiltes Speichern über mehrere HDDs mit "doppelten" Redundanzinformationen (>=4HDDs)
Ziel: Ausfallsicher Speicherung durch 2-fache Redundanz (genau zwei beliebige Festplatten im Verbund können ohne Datenverlust ausfallen)
Kapazität: Netto=(n-2)*(Kapazität der kleinsten Festplatte)

Kombinierte RAID-Level:

*Merke: Die **erste** Ziffer steht für den inneren (Sub-RAID), die **zweite** für den äußeren RAID-Verbund.*

RAID **10**: Zwei RAID-1-Verbünde werden zu einem RAID-0-Verbund zusammengesetzt (>=4 HDDs)
Ziel: Mit "Glück" können zwei Festplatten ohne Datenverlust ausfallen
Kapazität: (n/2)*(Kapazität der kleinsten Festplatte)

RAID **01**: Zwei RAID-0-Verbünde werden zu einem RAID-1-Verbund zusammengesetzt (>=4 HDDs)
Ziel: Mit "Glück" können zwei Festplatten ohne Datenverlust ausfallen
Kapazität: (n/2)*(Kapazität der kleinsten Festplatte)

RAID **50**: Zwei RAID-5-Verbünde werden zu einem RAID-0-Verbund zusammengesetzt (>=6 HDDs)

Ziel: Ausfallsicheres Speichern durch Redundanz (genau **1** beliebige HDD im Verbund kann ohne Datenverlust ausfallen) UND beschleunigte Zugriffszeiten durch RAID 0

Kapazität: Netto=(n-1)*(Kapazität der kl. HDD)/2

Merke: RAID ist kein Backup.

Datensicherungskonzept:

Beim differenziellen Backup werden nur jene Daten gesichert, welche sich seit dem letzten Vollbackup verändert haben.
Beispiel:

MO	DI	MI	DO	FR	SA	SO
VOLL2TB	2GB	4GB	6GB	...		

Zwei Wiederherstellungsdatenträger werden gebraucht. Einen für das Vollbackup und einen für das fortlaufend, wachsende differenzielle Backup.

Beim inkrementellen Backup werden die Veränderungen seit dem letzten inkrementellen Backup gespeichert.
Beispiel:

MO	DI	MI	DO	FR	SA	SO
VOLL2TB	2GB	2GB	2GB	...		

Zur Wiederherstellung benötigt man das Vollbackup und jedes einzelne folgende inkrementelle Backup.

Übung:

Szenario: In einer Verwaltungsorganisation arbeiten ca. 300 Sachbearbeiter. Jeder Sachbearbeiter erzeugt pro Werktag im Durchschnitt 50 Seiten Text neu und bearbeitet im Durchschnitt 20 Seiten Text.

Aufgrund von automatisierten Prozessen (Datenbanken, eMail-Server,..) entstehen werktäglich zusätzlich 2 GiB Daten; 20GiB werden verändert.

Schlagen Sie unter Maßgabe folgender Bedingungen ein Speicher- und Datensicherungssystem vor.

Der Basisdatenbestand beträgt 2 TiB.

Die Speicherkapazität soll für die innerhalb der nächsten 5 Jahre zu erwartende Datenmenge ausreichend sein.

Bei einem eingetretenen Datenverlust soll maximal die Menge an einem Werktag veränderten bzw. erzeugten Daten verloren werden können. Ebenfalls soll auf jeden Datenbestand zum Ende eines Werktages der aktuellen Woche zugegriffen werden können.

Um Daten, die an bereits zurückliegenden Zeitpunkten gelöscht, beschädigt oder verändert worden sind, zu rekonstruieren, soll monatlich, quartalsweise und jährlich der gesamte Datenbestand gesichert werden. Diese Sicherungen sind jährlich umlaufend auszuführen.

Geben Sie sie erforderliche Massenspeicherkapazität an. Berechnen Sie auch den Speicherbedarf bei RAID-Systemen: 5, 6

Schlagen Sie ein geeignetes Datensicherungs- (Backup-) Regime vor. Verwenden Sie die Begriffe Vollbackup, inkrementelles Backup und differenzielles Backup.

Speicherbedarf aktiver Daten:

Für Dokumente: 1 A4 Seite Text: 50 Zeilen mit 80 Zeichen
= 50*80*1 Byte =4000 Byte -> 3.9 KiB

50 Seiten pro Person, pro Tag: ~ 200 KiB
300 Sachbearbeiter, pro Tag: ~ 60.000 KiB ~ 60 MiB
an 240 Wochentagen: ~15 GiB
in 5 Jahren: ~ 75 GiB (vernachlässigbar)

Automatisierte Prozesse: 2 GiB * 240 Tage * 5 Jahre = 2400 GiB
~ 2,5 TiB

Gesamt: 2,5 TiB (neu gewonnene Daten) + 2 TiB Basisbestand = 4,5 TiB ~ **5 TiB**

5 HDD x 1 TiB (Ohne RAID)
5 + 1 HDD x 1 TiB (RAID 5)
5 + 2 HDD x 1 TiB (RAID 6)
5 + 2 HDD + 1 HDD (HotSpare) x 1TiB (RAID 6 + 1 Hotspare HDD)

Zyklische Datensicherung:

Entscheidungsfindung: Festplatten- oder bandbasiertes Backup.

Hier: Festplattenbasiertes Sicherungssystem

Gesamtdatenmenge 3TiB (gegenwärtiger Stand + 1TB)
Tägliche Änderung: 23GiB

Werktägliche Datensicherung:

	MO	DI	MI	DO	FR	
"immer voll"	3TiB	3TiB	3TiB	3TiB	3TiB	=5 x 3TiB (+ RAID ?)
"differenziell"	3TiB	23GiB	46GiB	69GiB	92GiB	=3TiB + 250GiB(+RAID?)
"inkremtell"	3TiB	23GiB	23GiB	23GiB	23GiB	=3TiB + 92GiB (+RAID?)

Monatliche Datensicherung:

	Jan	Feb	Mär	Apr	Mai	Jun	Jul	Aug	Sep	Okt	Nov	Dez
"immer voll"	3TiB	3TiB	3TiB	3TiB	3TiB	3TiB	3TiB	3TiB	3TiB	3TiB	3TiB	3TiB
"differenziell"	3TiB	0,5TiB	1TiB	1,5TiB	2TiB	2,5TiB	3TiB	3TiB	3TiB	3TiB	3TiB	3TiB
"inkremtell"	3TiB	0,5TiB	0,5TiB	0,5TiB	0,5TiB	0,5TiB	0,5TiB	0,5TiB	0,5TiB	0,5TiB	0,5TiB	0,5TiB

Quartalssicherung:

	1.Quartal	2.Quartal	3.Quartal	4.Quartal
"immer voll"	3TiB	3TiB	3TiB	3TiB
"differenziell"	3TiB	2TiB	3TiB	3TiB
"inkrementell"	3TiB	2TiB	2TiB	2TiB

>>Generationenprinzip>https://de.wikipedia.org/wiki/Generationenprinzip

Grundlagen Dualzahlen, Hexadezimalzahlen:

Information -> Zusammenhang -> Wissen

Analoge Information <> Digitale Information / diskrete Darstellung

- bestehen aus unendlich vielen Einzelinformationen
- sind in einzelne (An-)Teile zerlegt; dazwischenliegende Werte werden verborgen

Dezimal Natürliches Zahlensystem des Menschen

Binär extrem vereinfachte Darstellung von Mengen
Natürliches Zahlensystem des Computers

Hexadezimal Transfersystem zu vereinfachen Übersetzung zwischen den ersten

Oktal Nur bei Unix-Systemen, z.B. bei chmod noch relevant

Eine Hexadezimalstelle (ein Wert zwischen 0 und F) deckt einen Wertebereich von 16 Stellen ab.

Um eine Dualzahl in Hexadezimal umzurechnen zerlegen wir die Duale in Tetraden (Vierergruppen)

Dualsystem 1001 1101
Hexadezimal 9 D

Um eine Dualzahl in Oktal umzurechnen zerlegen wir die Duale in Dreiergruppen aufgeteilt (beginnen von rechts)

Dualsystem 10 011 101

Dezimalzahl 157

Dualsystem 10011101
Anhand Dual = 2^7 + 2^4 + 2^3 + 2^2 + 2^0 = 128+16+8+4+1 = 157

Dualsystem 1001 1101
Anhand Hexadezimal = 9*16^1+9*16^0+13 = 157

Dualsystem 10 011 101
Anhand Oktal: = 2*8^2 + 3*8^1 + 5*8^0 = 128 + 24 + 5 = 157

28.03.2015

- Rückblick auf Bestimmung der Verfügbarkeit und der damit verbundenen Redundanz
- Rückblick auf Datensicherungskonzepte

ASCII - Paritätsbits: 8-Bitgruppen übertragen, eines als Paritätsbit interpretiert, um ggf. Fehler bemerkbar zu machen

Parität:

Bei der einfachen Paritätsprüfung bei einer festgelegten Bitfolge, wird 1 ein Bit als Paritäts-Bit definiert. Es dient nicht zu Informationsübertragung, sondern um die Korrektheit der Nachricht zu überprüfen. Vor der Nachrichtenübertragung wird vereinbart, ob mit gerader oder ungerader Parität geprüft wird. Das Paritätsbit sorgt

dafür, dass die Geradzahligkeit gewährleistet wird. Einfache Bitfehler werden so einfach erkannt. Ebenso bei ungerader Parität, wird geprüft, ob die Summe der Bits einen ungeraden Wert ergibt.

Es wäre auch möglich mehr als ein Bit zur Paritätsprüfung zu übertragen, moderner sind allerding z.B. CRC-Prüfungen, bei diesen 1-Bit-Fehler erkannt UND korrigiert 2-Bit-Fehler zumindest erkannt werden können. Im Rahmen der Nachrichten-Übertragung wird auf ausgefeilte Prüfverfahren, wie dem HASH-Prüfsummenverfahren zurückgegriffen.

Beispiel:

Sender A: "A" ----------> "A" :Empfänger B

Bitfolge: 1000001 ----------> 1000011 (Nachricht verfälscht)

gerade Parität: 01000001 (Paritätsbit muss 0 sein, damit 1+1=gerade Zahl ergibt)

Bei 01000011 wird erkennbar, dass die Quersumme nicht gerade ist und die Verfälschung wurde erkannt.

ASCII -Tabelle

Dez	Hex	Zeichen	Dez	Hex	Zeichen	Dez	Hex	Zeichen	Dez	Hex	Zeichen
0	0	NUL	32	20	<LEER>	64	40	@	96	60	`
1	1	SOH	33	21	!	65	41	A	97	61	a
2	2	STX	34	22	"	66	42	B	98	62	b
3	3	ETX	35	23	#	67	43	C	99	63	c
4	4	EOT	36	24	$	68	44	D	100	64	d
5	5	ENQ	37	25	%	69	45	E	101	65	e
6	6	ACK	38	26	&	70	46	F	102	66	f
7	7	BEL	39	27	'	71	47	G	103	67	g
8	8	BS	40	28	(	72	48	H	104	68	h
9	9	TAB	41	29	)	73	49	I	105	69	i
10	A	LF	42	2A	*	74	4A	J	106	6A	j
11	B	VT	43	2B	+	75	4B	K	107	6B	k
12	C	FF	44	2C	,	76	4C	L	108	6C	l
13	D	CR	45	2D	-	77	4D	M	109	6D	m
14	E	SO	46	2E	.	78	4E	N	110	6E	n
15	F	SI	47	2F	/	79	4F	O	111	6F	o
16	10	DLE	48	30	0	80	50	P	112	70	p
17	11	DC1	49	31	1	81	51	Q	113	71	q
18	12	DC2	50	32	2	82	52	R	114	72	r
19	13	DC3	51	33	3	83	53	S	115	73	s
20	14	DC4	52	34	4	84	54	T	116	74	t
21	15	NAK	53	35	5	85	55	U	117	75	u
22	16	SYN	54	36	6	86	56	V	118	76	v
23	17	ETB	55	37	7	87	57	W	119	77	w
24	18	CAN	56	38	8	88	58	X	120	78	x
25	19	EM	57	39	9	89	59	Y	121	79	y
26	1A	SUB	58	3A	:	90	5A	Z	122	7A	z
27	1B	ESC	59	3B	;	91	5B	[	123	7B	{
28	1C	FS	60	3C	<	92	5C	\	124	7C	|
29	1D	GS	61	3D	=	93	5D	]	125	7D	}
30	1E	RS	62	3E	>	94	5E	^	126	7E	~
31	1F	US	63	3F	?	95	5F	_	127	7F	DEL□
Dez	Hex	Zeichen	Dez	Hex	Zeichen	Dez	Hex	Zeichen	Dez	Hex	Zeichen

Erweiterter ASCII

Dieser wird zur Darstellung zur nicht im ASCII enthaltenden Zeichen verwendet. Er umfasst 256 Zeichen, also ASCII und die weiteren. Oftmals haben allerdings viele Hersteller ihre eigene Vorstellung gehabt, welche Zeichen in der Erweiterung enthalten sein sollen.

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	Σ
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	ø
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	░	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	│	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	█	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	₧	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	

Unicode

Unicode ist ein 32-Bit Standard. Unternehmensübergreifende Vereinbarung über gemeinsame Zeichensätze. Ziel ist es alle weltweit genutzten Zeichen abzubilden.

Durch UTF (Unicode Transfer Format) wird der Zeichensatz wieder von den 32-Bit Unicode-Format auf 8-Bit runtergerechnet.

Im Unicode ist immer der ASCII an bekannter Stelle in bekannten Umfang enthalten.

Die Codecharts bei http://www.unicode.org/charts geben eine ausführliche Beschreibung der jeweiligen Zeichentabelle an.

Die sicherste, weil am meisten verbreitere Weg zur Verbreitung von Informationen ist ASCII (mit dem Makel, der begrenzten Anzahl der Zeichen).

Ein schlechter Kompromiss waren die ASCII-Erweiterungen, welche oft in Eigen-Regie der Unternehmen angelegt wurde.

Als Übergreifend und kompatibel zu bisherigen Standard wird beim Unicode der ASCII eingeschlossen und er verfügt über Umrechnungs- und Anpassungsformen, welcher die Abbildung in kleineren Bit-Räumen ermöglicht -16 -8-Bit > UTF (UTF Unicode Tranfer Format).

Darstellung von negativen Werten im Dualen System:

>> Script-Grundlagen.docx Seite 18

2er-Komplement Die duale Betragszahl wird bitweise invertiert (1er-Komplement).
Anschließend wird die Zahl 1 dual addiert. Das Ergebnis ist die duale Darstellung des negativen Werts der Betragszahl im 2er-Komplement.

Betragszahl 17: 0001 0001

```
  1110 1110   < bitweise invertiert
+ 0000 0001   < dual 1 wird addiert
  1110 1111   =                  - 17 (Dezimal)
```

>> Script-Grundlagen.docx Seite 17, 18

Vorzeichenbit: Eine einfache Methode besteht darin, in der Bitfolge einer Binärzahl ein Bit als Vorzeichenbit zu definieren: dieses Bit entspricht dem kleinen Minus-Symbol, mit dem in der dezimalen Schreibweise eine Zahl als negativ markiert wird. Genau wie wir es gewohnt sind, steht das Vorzeichen(-bit) links vor der Zahl, das heißt, es wird das am weitesten „links“ stehende Bit belegt.

Der Dezimalzahl -7 entspricht die

Binärdarstellung (8 Bit)	**1**000 0111.
in 16-Bit-Schreibweise	**1**000 0000 0000 0111. und
in 32-Bit-Schreibweise	**1**000 0000 0000 0000 0000 0000 0000 0111.

Darstellung von gebrochenen Zahlen

Festkommazahlen

Beispiel

Wertigkeit:	2^3	2^2	2^1	2^0	|	2^-1	2^-2	2^-3	2^-4
Binär:	1	1	0	0	|	0	1	0	0
Dezimal:		12			|		25		

Die Genauigkeit ist binär wie auch bei dezimalen Rechenmethoden abhängig von der Anzahl der Stellen. Hier : In dieser 8-Bit-Darstellung wird der Wertebereich verkleinert. Nicht alle Zahlen sind auf diese Art darstellbar.

Die Genauigkeit der Annäherung ist binär abhängig von der Anzahl der Nachkommastellen.

z.B. Dezimal: 12.3

Wertigkeit:	2^3	2^2	2^1	2^0	|	2^-1	2^-2	2^-3	2^-4
Binär:	1	1	0	0	|	0	1	0	1
Dezimal:		12			|		3125		

Übung: Wie groß muss eine binäre Festkommazahl mindestens sein, wenn links vom Komma 12, rechts vom Komma 4 Dezimalstellen abgebildet werden sollen?

40 vor dem Komma
10 danach

Beispiel zur Darstellung von gebr. Zahlenwerten im dualen Festkommaformat:

Dezimal:	17,625	=	2^4 + 2^0	,	2^-1 + 2^-3
		=	16 + 1	,	0,5 + 0,125
Dual			10001	,	0 1 1 0

Der Nachteil besteht nicht in der nicht exakten Darstellung von Zahlenwerten, sondern bereits für mittelgroße dezimale Darstellungen einen großen Aufwand an Dualstellen betreiben müssen.

Gleitkommazahlen

Umrechnen einer Gleitkommazahl in die Gleitkommadarstellung

Die Dezimalzahl **18,4** soll in die binäre Gleitkommadarstellung umgerechnet werden. Der Ablauf besteht in der Regel aus 6 Schritten. Die Reihenfolge der einzelnen Schritte oder gesonderten Teilschritte kann auch anders erfolgen.

Prinzipiell besteht der Ablauf daraus, die Zahl umzurechnen, zu normalisieren, den neuen Exponenten zu ermitteln, das Vorzeichen zu bilden und anschließend die Werte Vorzeichen, Charakteristik (Exponent) und Mantisse zusammen zu setzen.

1. Vorkommazahl umrechnen

Im ersten Schritt wird für die Vorkommazahl 18 die Dualzahl ermittelt. Hier wird das Teiler- bzw. Divisions-Verfahren angewendet.

$$
\begin{array}{rcrcrcll}
18 & : & 2 & = & 9 & \rightarrow & 0 & (letztes\ Bit) \\
9 & : & 2 & = & 4,5 & \rightarrow & 1 & \\
4 & : & 2 & = & 2 & \rightarrow & 0 & \\
2 & : & 2 & = & 1 & \rightarrow & 0 & \\
1 & : & 2 & = & 0,5 & \rightarrow & 1 & \rightarrow 10010
\end{array}
$$

2. Nachkommazahl umrechnen

Im zweiten Schritt wird für die Nachkommazahl 0,4 die Dualzahl ermittelt. Dabei wird die Multiplikationsmethode angewendet.
Als Zwischenergebnis entsteht eine duale gebrochene Zahl.

$$
\begin{array}{rcrcrcll}
0,4 & \cdot & 2 & = & 0,8 & \rightarrow & 0 & (erstes\ Bit) \\
0,8 & \cdot & 2 & = & 1,6 & \rightarrow & 1 & \\
0,6 & \cdot & 2 & = & 1,2 & \rightarrow & 1 & \\
0,2 & \cdot & 2 & = & 0,4 & \rightarrow & 0 & \\
0,4 & \cdot & 2 & = & 0,8 & \rightarrow & 0 & \\
0,8 & \cdot & 2 & = & 1,6 & \rightarrow & 1 & \\
\ldots & & & & & & & \\
0,6 & \cdot & 2 & = & 1,2 & \rightarrow & 1 & \rightarrow 0,01100110011...
\end{array}
$$

Ergebnis aus Schritt 1 und 2: 18,4 = 10010,01100110011001100110110100100...

3. Normieren bzw. Normalisieren (Mantisse ermitteln)

Bei der Normalisierung verschiebt man das Komma so, das man eine normalisierte Zahl erhält. Zum Beispiel 1,0101 (2) oder 0,123 (10). Dabei greift man auf die Exponentialdarstellung zurück, damit die Zahl ihren Wert behält.

10010,01100110011... * 2^0
1,001001100110011... * 2^4 (Normalisierung)

Bei der Normalisierung geht es darum, dass man nur die Nachkommastellen speichern möchte. Bei der binären Darstellung von Zahlen steht vorne immer eine Eins (1). Diese Vorkomma-Eins kann man beim Speichern bzw. bei der Darstellung weglassen (hidden bit), weil hier immer eine Eins steht. Dafür hat man hinten eine Stelle mehr für die Genauigkeit.

4. Exponent umrechnen (Charakteristik ermitteln)

Der Exponent wird auch als Charakteristik bezeichnet, weil sein Wertebereich verschoben ist (Bias). Das macht man deshalb, damit der Exponent immer positiv oder mindestens Null ist. Dadurch spart man sich ein Bit für Darstellung des Vorzeichens des Exponenten. Die Bias-Darstellung erleichtert auch den Größenvergleich. Nachteil, es gibt eine positive Null (+0) und eine negative Null (-0). Seltene Alternativen sind auch das Zweierkomplement und das Einerkomplement.

Der Bias oder Exzess hängt von der gewählten Genauigkeit (Anzahl der Bits) ab.

- Einfach Genauigkeit (32 Bit) bedeutet einen Bias von 127.
- Doppelte Genauigkeit (64 Bit) bedeutet einen Bias von 1023.

Da wir mit einer einfachen Genauigkeit (32 Bit) arbeiten entspricht das einem Bias von 127.

Charakteristik (neuer Exponent) = Exponent + Bias = 4 + 127 = 131

$$
\begin{array}{rcrcrcl}
131 & : & 2 & = & 65,5 & \rightarrow & 1 \quad (letztes\ Bit) \\
65 & : & 2 & = & 32,5 & \rightarrow & 1 \\
32 & : & 2 & = & 16 & \rightarrow & 0 \\
16 & : & 2 & = & 8 & \rightarrow & 0 \\
8 & : & 2 & = & 4 & \rightarrow & 0 \\
4 & : & 2 & = & 2 & \rightarrow & 0 \\
2 & : & 2 & = & 1 & \rightarrow & 0 \\
1 & : & 2 & = & 0,5 & \rightarrow & 1 \quad \rightarrow 10000011
\end{array}
$$

5. Vorzeichen bestimmen

- Positiv = 0
- Negativ = 1

6. Gleitkommazahl bilden (mit einfacher Genauigkeit)

$1\,V$	$8\,E$	$23\,M$
0	10000011	00100110011001100110011

>> Script-Grundlagen.docx Seiten 26 -28
>>http://www.vlsi.informatik.tu-darmstadt.de/student_area/tgdi/folien/Kapitel08v5.pdf
>>https://www.youtube.com/watch?v=QiZu_JRr5vE

Das duale Gleitkommaformat ist ein "Standard", entwickelt mit dem Ziel sehr große oder sehr kleine Zahlenwerte in dualer Form darstellen zu können.

Beispiel:

454334523523523456 >> 4543 * 10^14

0,0000001234 >> 1234*10^-7

Hierdurch ergibt sich allerdings immer eine Ungenauigkeit.

Es gibt zwei Darstellungsformen.

Einfach genaue Gleitkommazahl:
Länge 32bit
Bias 127

Doppelt genaue Gleitkommazahl:
Länge 64bit
Bias 1023

- Im Gleitkommazahl bedeutet eine duale 1 an der höchstwertigen Stelle eine negative Zahl. Es ist Das Vorzeichenbit (v)

0 Positiv
1 Negativ

- Es folgt die Exponentialzahl, bestehend aus Exponent und Mantisse
- Die Mantisse gibt den dazustellenden Wert an
- Der Exponent beschreibt den Wertebereich

Beispiel
4543 * 10^**14**
Mantisse Exponent

- Im Dualsystem ist logischerweise Die Basis zum Exponenten nicht 10, sondern **immer** 2

Weil das Format keine Möglichkeit zu Verfügung stellt für den Exponenten negative Werte darzustellen, bedient man sich eines Tricks. Man addiert zu jeder Exponentenstelle eine feste Zahl und erreicht damit, dass der Exponent in den positiven Bereich geschoben wird.

Beispiel:

In Dezimal: 5

5>0 Ist eine positive Zahl, somit ist das Vorzeichenbit 0

0 | _____ | _____ |

5 in binär: 0101

Jetzt gleitet das Komma nach vorne, bis nur noch eine 1 alleine am Anfang steht

01**01**, *2^0 = 1,**01** *2^**2**

Mantisse: 01
(den Rest der 23 Stellen auffüllen)
01000000000000000000000

0 | _____ | 01000000000000000000000 |

Exponent: Zum Exponenten 2 wird der Bias 127 (bei 32Bit) addiert

2+127 = **129 > binär : 10000001**

0 | 10000001 | 01000000000000000000000 |

Beispiel 2

Dez. -3

-3<0 Vorzeichen 1

in binär: 11
Komma 1,1 *2^1

Mantisse : 10000000000000000000000

Exponent: 1+127=128
binär: 10000000

>single 1 10000000 10000000000000000000000

Beispiel 3

0,05078125

Rechenbeispiel : Modulo Multiplikation:

0,05078125 * 2 = 0,1015625	| 0	erstes bit
0,1015625 * 2 = 0,203125	| 0	
0,203125 * 2 = 0,40625	| 0	
0,40625 * 2 = 0,8125	| 0	
0,8125 * 2 = 1,625	| 1	
0,625 * 2 =1,25	| 1	
0,25 * 2 = 0,5	| 0	
0,5 * 2 = 1	| 1	

>> 00001101

>0 Vorzeichenbit:0

In binär: 0,00001101 * 2^0

Komma: 1,101 * 2^-5

Beispiel 4

-17 <= V-Bit 1
in Binär: 10001
Komma: 1,0001 * 2^4 >Mantisse> 0001
Exponent 4+127 = 131 >binär> 10000011

1 10000011 00010000000000000000000

Beispiel 5

67,15625 >0 VBit 0
In Binär:

67,0 >>

67 : 2 =33.5 | 1 letztes Bit
33 : 2 = 16,5 | 1
16 : 2 = 8 | 0
8 : 2 = 4 | 0
4: 2 = 2 | 0
2:2 = 1 | 0
1:2 = 0,5 | 1

67 ^= 1000011

0,15625 >>

0,15625 * 2 = 0,3125 | 0 erstes Bit der nachkommazahl
0,3125 * 2 = 0,625 | 0
0,625 * 2 = 1,25 | 1
0,25 * 2 = 0,5 | 0
0,5 * 2 = 1 | 1

>> 1000011,00101
>Komma> 1,00001100101 * 2^6 >Mantisse: 00001100101
>Exponent> 6+127 = 133 >binär> 10000011

0 10000011 00001100101000000000000

Beispiel 6

-0,0078125
<0 VBit = 1

0,0078125 * 2 = 0,015625 | 0 *erstes Bit nach dem Komma
0,015625 * 2 = 0,03125 | 0
0,03125 * 2 = 0,0625 | 0
0,0625 * 2 = 0,125 | 0
0,125 * 2 = 0,25 | 0
0,25 * 2 = 0,5 | 0

0,5 * 2 = 1 | 1

>> 0,0000001
>Komma> 1,0 * 2^-7 > Mantisse 0
>Exponent> -7 + 127 = 120 >binär>01111000

1 01111000 00000000000000000000000

Montag, 30.03.2015

Grundlagen Computernetzwerke

>>TCP_IP.doc
>>Uebertreagungstechnik.doc
>>Ethernet 802.3.doc
>>Grundlagen Netzwerktechnik.doc

LAN und WAN unterlagen ursprünglich einer logischen Trennung, welche nun aufgrund vergleichbarer Infratrukturen nicht mehr so existiert.

Entwicklung der Computervernetzung

50er - 70er Jahre

Großrechensysteme (Mainframes) [Rechenzentren, mit hoch spezialisiertem Personal ohne signifikante Vereinheitlichung der Hardware- und Software-Komponenten]. Um Anwendern Zugang zu ermöglichen wurden bereits verfügbare Verbindungen (z.B Telefonleitungen) genutzt. Die dafür genutzte Schnittstelle bezeichnet man als **Terminal** (welche Fernschreiber sehr ähnelten)

TTY (***T**ele**ty**pe* - *Fernschreiber*) ~ Kommandozeilenorientierte Verbindung zwischen einem Großrechensystem und der Benutzerschnittstelle. ("dumme Terminals" ~ haben keinerlei eigene Verarbeitungs- und Speicherfunktion)

80er - 90er Jahre

Massenhafte Verbreitung von **Personal Computer**(n), welche ursprünglich **NICHT** auf Vernetzung ausgelegt und für die autarke Nutzung gedacht waren. Aufgrund der gewerblichen Nutzung wurde die Erweiterung dieser Geräte nötig (Speicher, Festplatten,...). Auch Programme wurden komplexer und somit anspruchsvoller. Die Funktionalität und die Leistungsfähigkeit (allerdings auch die Kosten) stiegen in diesem Rahmen > Steigende **TCO** ~ Total Cost of Ownership ~ Gesamtkosten [Betriebs- Energie- Lizenzkosten, Aufwand an User-Service, Arbeitsausfallzeiten bei Nicht-Funktion, Datenverlust und -verfälschung durch unsachgemäßen Umgang]

Peripheriegeräte benötigten zunehmend Zugriff auf das WAN, welcher nicht "verteilt" werden konnte, folglich entstanden die Anforderungen :

- **"Ressourcesharing"** ~ Gemeinsame Nutzung von Peripherie-Geräten (Drucker, Scanner, Massenspeicher, WAN-Zugänge...)

- **Datenaustausch** zwischen den PCs
- **Zentrale Administration**

1. Lösungsansatz: **Lokale Vernetzung**

- Punkt-zu-Punkt-Verbindung
- Arbeitsgruppenvernetzung (Workgroups) /

Peer-to-Peer-Vernetzung (Gleiche mit Gleichen)

- Arbeitsgruppenvernetzung im Client-Server-Modus

Zentrale Vorgaben für:
- Verfügbarkeit aller an den Server angeschlossenen Geräte
- Ressourcennutzung wird server-seitig gesteuert

- Client-Server-Model mit eingeschlossenem modernen Terminal-Betrieb, ggf. Systemvirtualisierung (intelligente Terminals, Thin-Clients)

90er - 2000er

In logischer Folge wurden Netzwerke zur gemeinsam Ressourcen-Nutzung zusammengeschlossen.

Netzwerk-Kategorien/Begriffe:

LAN	Local Area Network	(private, örtlich beschränkte, NW-Infrastruktur, typische Ausdehnung: **100m**)
MAN	Metropolitan Area Network	(über eine größere Fläche, mehrere Gebäude,... ausgedehnte NW-Infrastruktur, typische Ausdehnung 10km)
WAN	Wide Area Network	(überregionale Netzwerke mit unter einheitl. Verwaltung, typische Ausdehnung >100km)
GAN	Global Area Network	(weltumspannende Netzwerke, ...)

Unterscheidung durch Eigentumsverhältnisse und Topologien:

Netzwerk-Topologien:

Terminal-Verbindung
klassisch: entfernte I/O-Schnittstelle zu einer zentralen Verarbeitungs- und Speichereinheit

Punkt-zu-Punkt-Verbindung
Direktverbindung zwischen zwei Endgeräten

Bus-Topologie
Zentrales "Verbindungskabel" an das mehrere Endgeräte angeschlossen sind.

*Über 15 Jahre die bestimmende Topologie von Netzwerken, weil sie "**einfach**" aufgebaut ist, da sie nur ein Verbindungskabel und keine zentrale Verarbeitungseinheit braucht. Nachteilig ist, dass sich **alle Endgeräte ein Medium** teilen; je mehr Geräte den Bus nutzen, desto schwieriger ist die Verteilung von Prioritäten. Darüber hinaus kann ein Fehler im Netzwerk das ganze Netzwerk unterbinden. Sie arbeiten selbstorganisierend, typischerweise kann nur einer von vielen Daten senden. >Nicht determiniertes*

Zugriffsverfahren

Ringförmige-Topologie

Das Verbindungskabel ist in sich geschlossen "ringförmig"

*Hier wird die Datensende-Berechtigung **ringförmig** weitergegeben an den nächsten. Ein von Endgerät zu Endgerät weitergereichtes **Signal** bestimmt die Sendeberechtigung, dieses nennt sich **Token**; Daraus abgeleitet ist das verbreitete Token-Ring-Netzwerk. >Deterministisches Zugriffsverfahren*

Stern-Topologie

Zentraler Netzwerkknoten als zentrales Verbindungsgerät (Hub), sternförmig ausgehende Verbindungen

*Stellt eine **Misch-Topologie** dar, da keine übergeordnete Instanz die Freigabe verwaltet und darüber hinaus die sternförmige Anordnung einen Ausfall des gesamten Netzes verhindert bei einem Fehler. Benötigt einen **Hub** in der Mitte, der Verkabelungsaufwand ist ebenfalls größer. (physisch=Stern; logisch=BUS)*

Unterschied Hub <> Switch
*Ein **Hub** stellt nichts anderes als einen verkapselten BUS dar. Im Gegensatz hierzu besteht ein **Switch** aus mehreren BUSsen, welche geschaltet werden können.*

Baum-Topologien

Mehrere miteinander schleifenfrei verbundene "Sterne"

*Stellt die oftmals organisch gewachsenen Verbindung **zwischen** den einzelnen Stern-Topologien dar. Dies ermöglicht einer **flexiblere** Strukturierung, da einzelne Sterne auch gehäuft vorkommen können. **Schleifen** sind auch hier **nicht** erlaubt.*

Maschen-Topologie

Zwischen Netzwerkknoten (Router) netzförmig hergestellte Verbindungen

Matrix-, Vollvermaschte-Topologie, etc. ...

*Im Gegensatz zur Bus-, Stern- und Baumtechnologie sind **Schleifen** gewünscht und **Router** die Stelle von Hubs und Switches einnehmen, wodurch redundante Verbindungen ermöglicht werden.*

Netzwerkkomponenten:

Passive Komponenten

tragen zur Signalübertragung (optisch, elektrisch,

elektromagnetisch) bei,

Aktive Komponenten

Steuernde und Signalumwandelnde Funktion

Protokolle

Verarbeitungs-, kodierungs- und Adressierungsfunktionen im Netzwerk

Passive Komponenten:

Übertragungsmedien:

- Kabel (elektrische Medien)
- Lichtwellenleiter (optische Medien)
- "Luftschnittstelle" (elektromagnet. / opt. Übertragung)
- Stecker, Buchsen, Anschlussdosen (Konfektion der Medien)
- Patchfeld
- Spleißbox

Link: Vollständige Verbindungsstrecke zwischen Endgeräten (Clients, Server).

(Arbeitsplatz-PC)
Endgerätepatchkabel
Anschlussdose RJ45
Verlegekabel (Im Kabelkanal) z.B.
Patchfeld
Patchkabel
(Switch)

Metallische Leiter:

Koaxialkabel (Buch S.34)

- Typ: **RG58**/U kam in BUS-Förmigen Netzwerken zum Einsatz (Ethernet)

- Asymmetrischer Leiter - Schirmung wird als Antwort-Schicht genutzt

http://info.electronicwerkstatt.de/bereiche/stecker/kabellaengen.html

>Kabeltypen Tabellen> Mitschrift.xlsx

Twisted Pair Kabel (**TP**) (Buch S. 36 ff)

- Paarweise verdrillte (Kupfer-) Adern ohne Abschirmung! (schwer zu finden)
- S/UTP (Unshielded Twisted Pair) (Standard) besitzen eine Gesamtschirmung
- S/FTP, F/FTP oder SF/FTP besitzen eine Gesamt und eine Paarschirmung
  Form: (Schirm gesamt / Schirm Adernpaar) TP

Merke: *Wichtig ist beim Ab-Isolieren, die Verdrillung nur so weit wie nötig aufzuheben, um die Funktion der Phasenverschiebung (= Kohärenz http://www.abi-physik.de/buch/wellen/kohaerenz/) nicht aufzuheben.*

>Kabeltypen Tabellen> Mitschrift.xlsx

Lichtwellenleiter (**LWL**) (Buch Seite 58 ff)

- "Mode" beschreibt den tatsächen Weg, den die Lichtwelle durch das Medium nimmt:
  - Multimode (mit Kollisionen)
  - Singlemode (Kollisionsfrei)

Nutzen:
- Übertragung großer Datenmengen bei hohen Geschwindigkeiten > Hohe Bandbreiten
- lange Übertragungsstrecken
- bei starken äußeren elektromagnetischen Einflüssen

Multimode-Glasfaser mit Stufenindex-Profil (wirschaftlich):

- Zu verwenden bei kurzen Distanzen (<1KM)
- Die Übertragungsfrequenzen liegen nicht über 1GHz, daher liegt Kupfer als Medium ebenfalls nahe

Multimode-Glasfaser mit Gradientenindex-Profil:

- Guter Erhaltungssatz durch graduelle Ablenkung des Signals bei Kollision mit den Außenwänden

Singlemode-Glasfaser:

- Kollisionsfreie Signalübertragung für hohe Distanzen (<100km) einsetzbar.

>**Wichtig**: Auswahlkriterien für jeweilige Verkabelung
Metallische Leiter / LWL / Kabellos aus "Leitungen und Kabel.doc"

Kriterien für die Wahl einer Verkabelungstechnik im LAN:

(1=blöd 5 =voll toll)

Kriterium	Kupferleiter	LWL	"Luftschnittstelle"
Bandbreite	3	5	1
Reichweite	2	4	2
Wirtschaftlichkeit	3	2	4
Abhörsicherheit	3	5	2
Zuverlässigkeit	4	4	2
Montageaufwand	3	1	4
Haltbarkeit	3	4	Endgeräte bedingt
Vielseitigkeit	3	4	2
Redundanz	2	3	<4
Kompatibilität	4	2	3
Flexibilität	4	2	4
EMV	3	5	2

>Mitschrift.xlsx
>Leitungen und Kabel.doc

31.03.2015

- Überblick über die Bezugsquellen von Kabel- und Steckverbindungen deren Eigenschaften und Verfügbarkeit unter Berücksichtigung der relativen Notwendigkeiten, z.B. Brandschutzbestimmungen, am Einsatzort.
  http://www.glasfaserinfo.de/

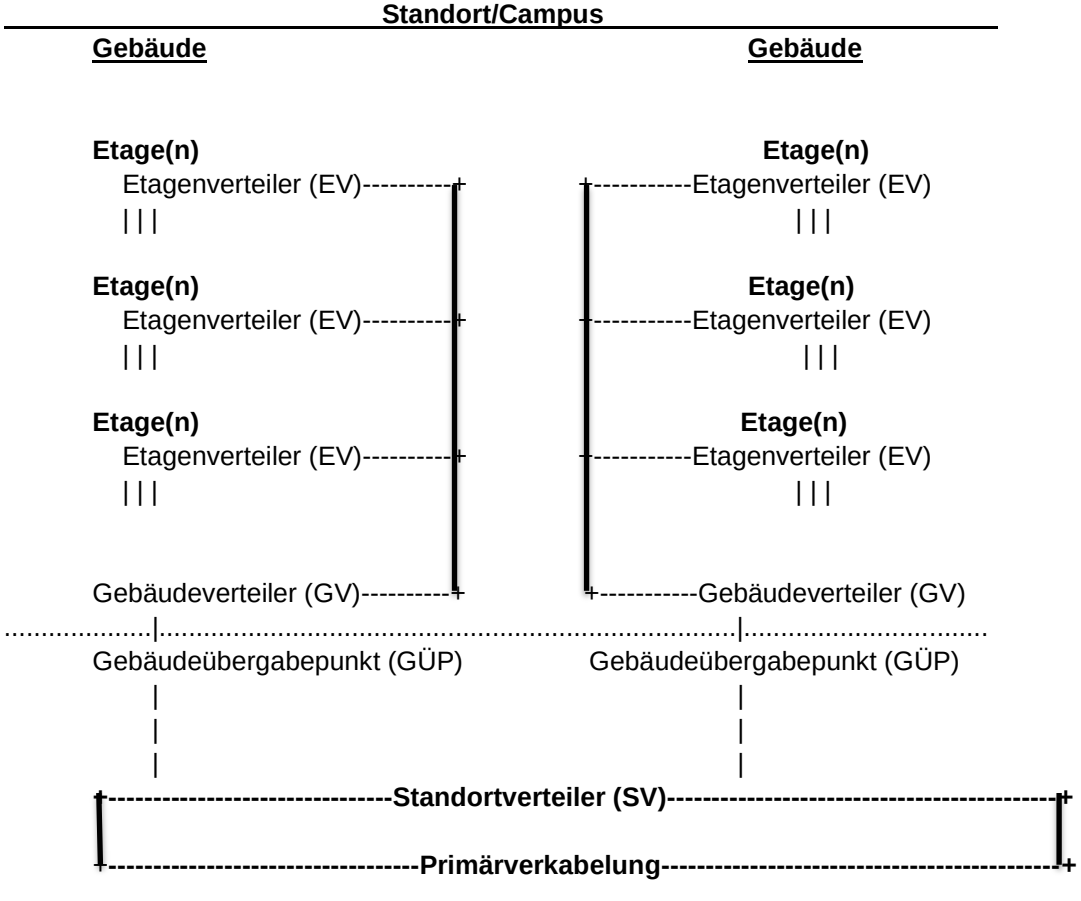
Strukturierte anwendungsneutrale Gebäudeverkabelung (DIN EN 50173)

http://de.wikipedia.org/wiki/Strukturierte_Verkabelung

>>**BAUSTEINTEST** (Struktur, Bezeichnungen, GÜP [Medienwandler], Ziel der Norm: Unterverteilungen innerhalb der Etagen zu vermeiden.)

Prüfungsrelevant

- Verkabelung basierend auf drei Zonen (primär / sekundär / tertiär)



Primärverkabelung: (Standortverkabelung)

Ring-Topologie (FDDI) zur Verbindung der Gebäude

Sekundärverkabelung: Vertikalverkabelung |

Tertiärverkabelung: Horizontalverkabelung (Etagenverkabelung) --

FDDI >10KM, Doppel-Ring (>2 Faserpaare), Beide Ringe werden für die Kommunikation genutzt, im Fehlerfall Notbetrieb durch den verbliebenen

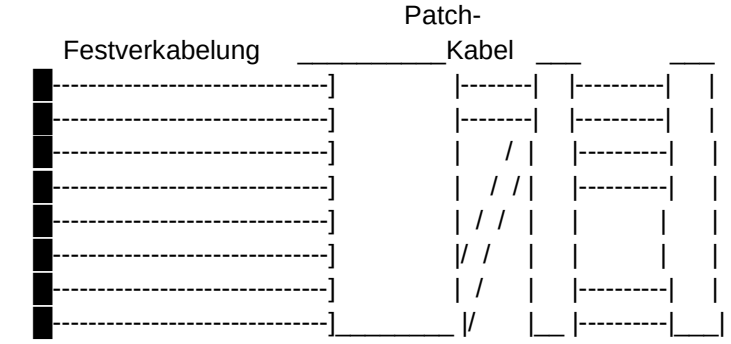
GÜP - Gebäude-Übergabe-Punkt - zur Medienwandlung (Außenkabel <-> Innenkabel)

SV Standortverteiler (Campus Distributor)

GV Gebäudeverteiler ~ Switch für die Verteilung zu den Etagen (Building Distributor)

EV Etagenverteiler ~ Switch für die Verteilung auf der jeweiligen Etage (Floor Distributor)

Konformität besteht, wenn Mindest-Bedingungen zur Entsprechung zur Norm gegeben sind.



Netzwerkkomponenten:

Aktive Komponenten

OSI 7	Gateway
OSI 6	Gateway
OSI 5	Gateway
OSI 4	Gateway
OSI 3	Router, (Switch)
OSI 2	Switch, Bridge
OSI 1	Network Interface Connector (NIC), Repeater, Hub

LEVEL 1 (eine Adressierung der Informationen findet NICHT statt)

- **Network Interface Connector** (z.B. Netzwerkkarte)

-Stellt die physische Verbindung zwischen einem Endgerät (PC) und dem Netzwerk her.
- Arbeitet in Abhängigkeit von dem Übertragungsmedium (TP, Koaxialkabel, LWL, Luftschnittstelle) und Übertragungsstandard (z.B.Ethernet, FDDI, ATM,...)

- **Repeater**
  - Erweitert ein Netzwerksegment
  - Verstärkt und filtert die Netzwerksignale
  - Typischerweise werden Repeater in **bus**förmigen Topologien verwendet
  - In WLAN-Umgebungen dienen sie zur Vergrößerung des Sende- und Empfangsbereiches
- **Hub**
  - Überträgt die Funktion des Repeaters auf eine Stern-Topologie

LEVEL2 (Hardware-Adressierung)

- **Switch**
  - erweitert die Funktion des Hubs (Sternkoppler) um das aktive und bedarfsweise Schalten von Verbindungen zwischen den angeschlossenen Endgeräten.
  - Nutzt zur Zustellung von Nachrichten die Geräte-Adressen (MAC-Adressen) der Endgeräte
  - Besitzt als zentrale Netzwerkkomponente im LAN eine Vielzahl weiterer Funktionalitäten (s.u.)

- **Bridge**
  - Verbindet Netzwerke durch selektive Nachrichtenweiterleitung. Dazu werden die MAC-Adressen in den Nachrichten ausgewertet.

LEVEL3 (IP-Basierte Adressierung)

- **Level-3-Switch**
  -Erweitert die Grundfunktion des Switchs (s.o.) um Funktionen aus OSI3, speziell um die Auswertung logischer Netzwerkadressen: IP-Adressen.

- **Router**
  - Leitet Nachrichten auf Grund ihrer (IP-) Adressierung und unter Berücksichtigung der Verfügbarkeit und des Zustandes alternativer Verbindungswege weiter.

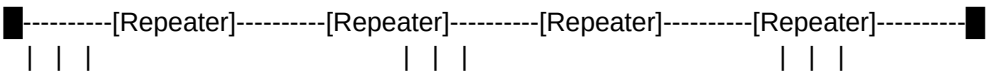
LEVEL4-7

- **Gateway**
  - Ein Netzwerkgerät, mit über den eigentlichen Nachrichtentransport- und die Weiterleitung hinausgehenden Verarbeitungsfunktionen
  - *VPN-Gateway (Überbrückung externer Netzwerke, Nachrichtenverschlüsselung* und Authentifizierung)
  - *Proxy*
  - *Firewall*

Repeater

Repeater-Regel (5-4-3)

Segment | Segment | **Segment** | Segment | **Segment**



Stationen Stationen Stationen

Es dürfen nicht mehr als fünf (5) Kabelsegmente verbunden werden. Dafür werden vier (4) Repeater eingesetzt. An nur drei (3) Segmenten dürfen Endstationen angeschlossen werden.

5-4-3

Bridge

```
[ LAN1 ]----------[ BRIDGE ]-----------[ LAN2 ]
[      ]                               [      ]
[-PC1  ]                               [-PC7  ]
[-PC2  ]                               [-PC8  ]
[ ...  ]                               [ ...  ]
```

Die Bridge "lauscht" im Lernmodus die MAC-Adressen der jeweiligen Netzwerke aus, um im Arbeitsmodus eine Nachricht deren Ziel im jeweils anderen Netzwerk zu finden ist, weiterzuleiten.

Switch

- Ein Switch schaltet dynamisch Netzwerksegmente.

- **Bauform** : Stapelbar (Office) / 19"-Einbau

- **Übertragungsmodi**:

Simplex

Halbduplex

Duplex

- **Switching-Funktionen**:

Spanning Tree Protocol

Trotz grundlegend "verbotener" Schleifen-Konfiguration wird eine Redundanz erstellt, welche inaktiv bleibt. Bei einer Störung wird die Alternativ-Strecke aktiviert, die gestörte deaktiviert. Es wird immer eine eindeutig schleifenfreie Verbindung unter Verwendung der Schleifen-Erkennung (loop detection) verwendet.

Link Aggregation

Beschreibt das Zusammenfassen mehrerer physischen zu einer logischen Verbindungen.

Backplane-Kopplung

Direkte Verbindung zwischen zwei Switches, nicht mittels Link Aggregation, sondern spezielle Verbindungen mit höherer Bandbreite nutzt

VLAN (Virtual LAN)

Statisch: Port-Basiertes VLAN (auch Switch-Übergreifend)
Zusammengehörigkeit nach Port-Gruppe
z.B. 1, 6 ,8 ,22

Dynamisch : nach oder IP-Adresse

VLAN Tags: Markierungen eines Frames zur Zuordnung zu einem bestimmten VLAN (über einen oder mehrere Switche hinweg)

PoE: (Power Over Ethernet) ~ 48V bei 350mA > ~ 15W pro Leitung

Übung:

>>Übung1.pdf

Erarbeiten Sie Ansatzpunkte für die Entwurfsplanung eines IT/TK-Netzwerkes unter dem Gesichtspunkt "Konvergenz der Netze". Gehen Sie von einer umfassenden Planung aus, die passive und aktive Netzwerkkomponenten sowie zentrale dienstorientierte Elemente ("Server") umfassen sollte.

Formulieren Sie Unklarheiten der Aufgabenstellung als Fragen an den Auftraggeber.

Der Planungsgegenstand ist eine kardiologische Praxisklinik. Es handelt sich um ein Gebäude der Größe 50x20m: Kellergeschoss, Erdgeschoss und Obergeschoss. Dir grobe funktionale Aufteilung entnehmen Sie bitte der folgenden Gebäudeskizze.

Hinweis: Die Aufgabe umfasst lediglich die Ansatzpunkte für den Grobentwurf zur Planung:

- Was ist planungstechnisch zu berücksichtigen?
- Welche offenen Fragen müssen geklärt werden?
- Was umfasst der Entwurfvorschlag?
- Welche Merkmale sollten passive, aktive und Serverkomponenten für diese
- konkrete Planungsaufgabe erfüllen?

Es ist keine Detailierung erforderlich!

*"Daumenzahl" *g* pro 10m² Nutzfläche = 2 Netzwerkanschlüsse*

Antworten & Fragen:

01.04.2015

Erforderliche Komponenten-Kategorien:

- Switches (4xEV, 1xGV)
- Patchfelder (evtl. Spleißboxen) 5 (4xEV, 1xGV)
- Verlegekabel nach Bedarf
- Wand-Dosen
- Patchkabel (kurz & lang) nach Bedarf

Fläche ges.: 50m x 20m x 3 Etagen=3000m²
Raumhöhe: 2,5m
Etagenhöhe: 3m

Untergeschoss: ~ 40% relevant für Verkabelung ~ 400m²

Erdgeschoss: ~ 50% relevant für Verkabelung ~ 500m²

Obergeschoss: ~ 60% relevant für Verkabelung ~ 600m²

Bei Zugrundelegung von zwei Endgeräteanschlüssen auf 10m² relevante Nutzfläche:

Untergeschoss: ~ 80 Anschlüsse

Erdgeschoss: ~ 100 Anschlüsse

Obergeschoss: ~ 120 Anschlüsse

Abschätzung der maximalen Kabellängen in der tertiären Ebene:

Basis: Verlegung entlang der Gebäudewände in ggf. noch zu installierenden Kanälen

Nordseite: 45m
Westseite: 20m
Südseite: 35m
100m

Ergebnis: Bei einer zulässigen maximallänge der fest verlegten Etagenverkabelung von **90m** (+10m Patchkabel) sind **zwei** Etagenverteiler zwingend erforderlich.

Alternative: Kabelführung in zwei Zügen, um beide "kurzen" Gebäudeseiten (West+ Ost).

Nachteil: Durchführung durch öffentlich zugänglichen Bereich (Treppenaufgang) in dieser Variante erforderlich.

Vorschlag: Platzieren der Etagenverteiler am Westende des Gebäudes (Gangende)
Für UG: Zusätzlicher Etagenverteiler im IT-Raum (Anschlüsse der dort platzierten Server (...) sowie der Anschlüsse im benachbarten Archiv und Personalbereich).

Als maximale Länge dre festen Verkabelung ergibt sich nun:
1x Gebäudelänge = 50m

Bedarfsabschätzung:

Verlegekabel (TP, Cat7)

Untergeschoss:
80 Anschlüsse:
25 EV-Tech. * ø 5 m = 125m
15EV-Zentr. Nord * ø 15m = 225m
40EV-Zentr. Süd* ø 25m = 1000m = 1km >> 1350m
Erdgeschoss:
100 Anschlüsse * ø 25m Kabellänge >> 2500m
Obergeschoss:
120 Anschlüsse * ø 25m Kabellänge >> 3000m
Gesamt: **6850m**

Produktbeispiel: "Datalink Installationskabel Cat7 u900 duplex 100m" ~190€
~ 6500€

Verlegekabel (LWL, 4-8 Fasern)

Untergeschoss:	50m
Erdgeschoss:	100m
Obergeschoss:	100m
Gesamt:	**250m**

Produktbeispiel: "LWL Universalkabel 8 Fasern ~ 1,50€/m
375€

Patchfelder: (TP, Cat 7)

Untergeschoss:	4 Stück
Erdgeschoss:	4 Stück
Obergeschoss:	5 Stück
	13 Stück

Produktbeispiel: "Digitus Patchpanel DN-91624S ~ 40€
~520€

Switche: (TP[1000Gb/s] + LWL[1000Gb/s])

Untergeschoss:	(42 + 24 + 24 + 24)	4 Stück
Erdgeschoss:	(42 + 24 + 24)	3 Stück
Obergeschoss:	(42 + 42 + 42)	3 Stück
		10 Stück

Produktbeispiel: Cisco 200 Series Switch SG200-50 ~ 500€
Cisco SG200-26 Switch ~ 250€
~4000€

Datendosen: (Doppeldose 2xRJ45, Cat7)

Untergeschoss:	40 Stück
Erdgeschoss:	50 Stück
Obergeschoss:	60 Stück
	150 Stück

Produktbeispiel: "diverse" ca. 10€
~ 1500€

Patchkabel: (Verbindung: Patchfeld-Switch 1,5m Cat7)

300 Stück

Produktbeispiel: "RJ45 Patchkabel Cat6a TM31 02m" ~ 8€
~ 2400€

Produktbeispiel: "Rital 19" Netzwerkschrank 24HE, 600x600mm, grau"
~ 550€

Produktbeispiel: "Riello 19" USV, SDL 6000-7 Sentinel Dual
6000VA/4200W
~ 2000€

Unterbrechungsfrei Stromversorgung:

Offline USV - startet erst bei festgestellter Unterbrechung ~ Geräte stürzen ab

Line Interactive USV - startet bei festgestellter Unterbrechung mit in der Regel tollerierbarer Unterbrechung

Online USV - ist permanent Versorger für Verbraucher und Empfänger angelegter Stromversorgung - empfohlen

>>**BAUSTEINTEST**

Übliche Strecke:
PC1 - Patchkabel - Dose - Verlegekabel - Patchfeld - Patchkabel - Switch (Aktiv) - Patchkabel - Patchfeld - Velegekabel - Dose - Patchkabel - PC2

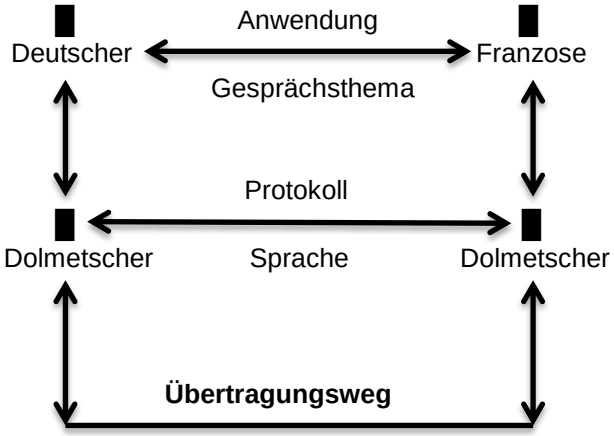
07.04.2015

>> BAUSPEINPRÜFUNG : OFFEN (Kein Questionmark)
Switching: VLAN, POE, Link Aggregation

Protokolle im Netzwerk

Allgemeines (menschliches) Kommunikationsmodell

- horizontal : logischer Informationsfluss
- vertikal: physischer Nachrichtenfluss



Technische Kommunikationsmodelle:

- OSI-Referenzmodell
- DoD-Schichtenmodell (Department-of-Defense)

>>**BAUSTEINPRÜFUNG**

OSI-Referenzmodell:

Layer 7 : *application layer* Anwendungsschicht

Komponenten:	Gateway (VPN-GW,...)
Protokolle:	http, https, ftp, smtp, pop3, nntp, snmt,...
Adresse:	**URL**

Layer 6 : *presentation layer* Darstellungsschicht

Komponenten:	Gateway
Protokolle:	(Keine Protokolle, sondern Zeichenkodierung: ASCII, MIME)
Adresse:	URL

Layer 5 : *session layer* Sitzungsschicht

Komponenten:	Gateway
Protokolle:	ssl
Adresse:	URL

Layer 4 : *transport layer* Transportschicht

Komponenten:	Gateway
Protokolle:	TCP, UDP, SPX, SCTP
Adresse:	**Port**

Layer 3 : *network layer* Vermittlungsschicht

Komponenten:	Router (Layer-3-Switch)
Protokolle:	Internetprotokoll (IP), ICMP, IPX, NetBios
Adresse:	**IP**

Layer 2 : *data-link layer* Sicherungsschicht

Komponenten:	Bridge, Switch

Protokolle: Ethernet, ARP
Adresse: **MAC**

Layer 1 : *physical layer* Bitübertragungsschicht
Komponenten: NIC, Repeater, Hub
Protokolle: Ethernet (IEEE 802.3)
Token-Ring, FDDI, ATM

[redacted] Medium (LWL, TP, "Luft",...) [redacted]
.-.-. .-.-..-.-. .-.-..-.-. .-.-..-.-. .-.-..-.-. .-.-..-.-. .-.-..-.-. .-.-..-.-. .-.-.-. .-.-.-..

Übertragungsprotokolle im LAN*: Ethernet

- **Ethernet** findet zunehmend Anwendung auch im WAN-Bereich

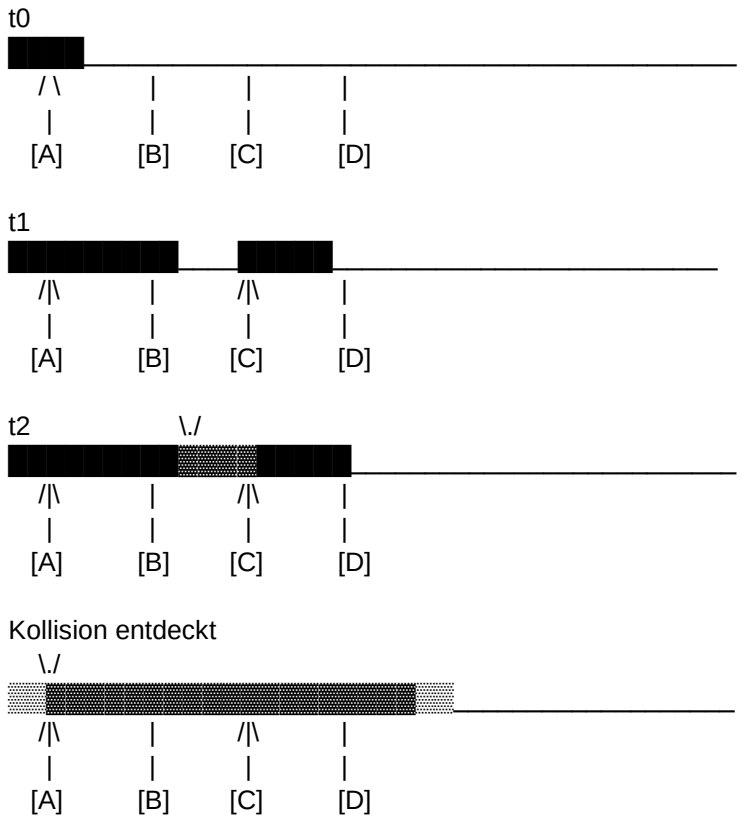
("Ethernet ist ein eher umgangssprachlicher Sammelbegriff für eine ganze Protokollfamile)

- Standardisiert als **IEEE 802.3**

- Gemeinsames Merkmal aller Ethernet-Varianten ist die Art des Medienzugriffverfahrens **CSMA/CD**

(nichtdeterministisch, dezentrales Verfahren : unbestimmter Nutzungszeitpunkt, keine zentrale Festlegung)

CSMA/CD
Carrier **S**ense **M**ultible **A**ccess / **C**ollision **D**etection ~ Kollisionserkennung
https://de.wikipedia.org/wiki/Carrier_Sense_Multiple_Access/Collision_Detection



- **Mindestlänge** einer Ethernet-Nachricht :

64byte (14 byte header, 46Byte Daten, 4Byte CRC)

- **Längenbeschränkung**:
100m (200m) im Stern (**TP**)
185m (4 x 185m) im **BUS** (Koaxialk.)
2500m (Maximalausdehnung einer Kollisions-Domäne [s.u.])

- Ein Bereich, in dem mehrere Endgeräte physisch miteinander verbunden sind, nennt sich auch *Kollisions-Domäne* **(802.3**)

- Der Einsatz von Switches (im Gegensatz zu Hubs) sorgt für minimale Kollisions-Domänen

- Maximal empfohlene **Anzahl von Endgeräten** je Kollisions-Domäne: **30**

- Ursprünglich für BUS-förmige Netzwerke entwickelt

- **Codierungsverfahren**:

- Ethernet adressiert Endgeräte anhand ihrer MAC-Adresse
- Daten werden in Frames zusammengefasst
- Der Inhalt einzelner Frames werden dem Übertragungs-Medium entsprechend codiert (Verfahren: Manchester Code)

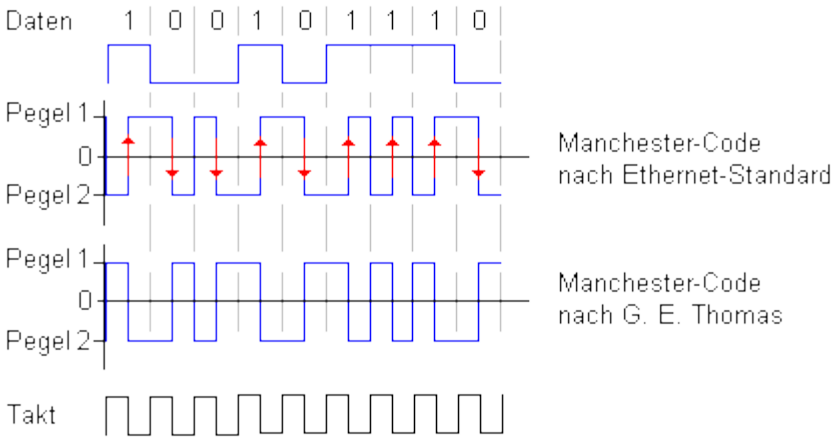
*Beim **Manchester Code** werden Nullen mit einem Spannungsanstieg und Einsen mit einem Spannungsabfall dargestellt. Die separate Übertragung eines Taktes ist nicht nötig, da MC diesen durch die stetigen Flankenwechsel bereits mitbringt.*

- Flankengesteuert, nicht pegelgesteuert (Spannungsanstieg & -abfall)

Beispiel:

Hallo
1001000 1100001 1101100 1101100 1101111

\/\



http://de.wikipedia.org/wiki/Ethernet#CSMA.2FCD-Algorithmus

http://elektroniktutor.oszkim.de/internet/codes.html

Einige Ethernet-Protokolle

>>Übertragungstechnik.doc

10Base2 10MHz-Basisband-200yd Segmentlänge 10Mbit/s
(Koax., RG58, 185m,BUS)
"Thin Ethernet / Cheapernet"

10Base5 10MHz-Basisband-500yd Segmentlänge
(Koax., 450m, BUS)
"Thick Ethernet"

10BaseT 10MHz-Basisband-100m Segmentlänge (TP, Stern)
"Twisted Pair"

10BaseF 10MHz-Basisband-100m Segmentlänge (LWL, Stern)
"Fibre-Optics"

100Base ... 100MHz-Basisband-100m Segmentlänge (TP/LWL, Stern)

1000Base ... 1000MHz-Basisband-100m Segmentlänge (TP / LWL)
"Gigabit-Ethernet"

http://www.elektronik-kompendium.de/sites/net/1406171.htm

***Basisband**: Zur Übertragung wird nur eine Frequenz verwendet*
***Breitband**: Verschiedene Frequenzbereiche werden mit einem Medium übertragen*

Zusammenfassung Ethernet:

- Angesiedelt auf OSI-Layer 1, verwendet Layer 2 zwecks MAC-Adressierung.
- Es verwendet ein nichtdeterministisch, dezentrales Verfahren mit unbestimmtem Nutzungszeitpunkt, ohne zentrale Festlegung.
- Basisband: Zur Übertragung wird nur eine Frequenz verwendet
- Flankengesteuert, nicht pegelgesteuert (Spannungsanstieg & -abfall) mittels des taktintegrierten Manchester-Verfahrens.
*- Überführt die Nachrichten in eine verarbeitbare Struktur : **Frame**.*

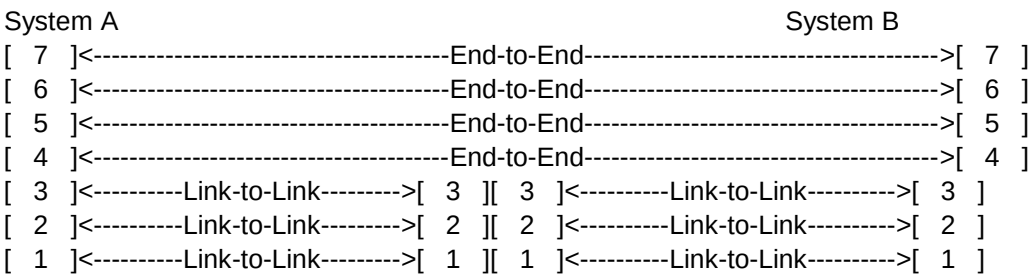
Frames**:**

Aufbau:
- Präambel 8 Byte
- Zieladresse 6 Byte
- Quelladresse 6 Byte
- Typfeld 2 Byte
- Datenfeld 46 - 1500 Byte
- Prüffeld 4 Byte

insg. mind. 64 Byte

- Exemplarische Verwendung von Wireshark zur Darstellung von Frames unter Bezug auf die Kommunikationswege zwischen den physisch verbundenen Geräten

Signifikanz einer Kommunikationsbeziehung:



Im Bezug auf Etherlink bedeutet die obige Darstellung:

Eine Frame-basierte Verbindung (Ethernet) wird immer nur zwischen zwei Geräten hergestellt, die eine direkte physische Verbindung zueinander besitzen, d.h. sich im selben Netzwerksegment ("am selben Draht") befinden.

Zwischen diesen Geräten wird eine sogenannte Link-to-Link - Verbunding hergestellt.

Die Adressierung erfolgt mittels fester (...() gerätespezifischer Adressen:
MAC-Adressen.

Die MAC-Adressen in Bezug auf Netzwerke unstrukturiert sind, können Verbindungen über Ethernet nicht geroutet werden.

Routing heißt eine Nachricht über mehrere Stufen zuzustellen, was nur möglich ist, wenn eine Netzwerkinformation mit-transportiert wird. MAC-Adressen enthalten keine NW-Informationen.

Ethernet ist ein nicht-routingfähiges Protokoll.

Ethernet ist ein verbindungslos arbeitendes Protokoll.

ARP: (Address Resolution Protocol)

Funktion: Ermittelt zu einer (gegebenen) logischen Adresse (IP-Adresse) die MAC-Adresse der / einer zugehörigen Netzwerkschnittstelle.

Zu diesem Zweck werden sogenannte "Who is / Who has" - Abfragen im Netzwerk generiert. Der fragende Host übermittelt dabei die IP-Adresse des Ziel-Hosts. Befindet sich der Ziel-Host im selben Netzwerksegment (und ist aktiv, bzw. erreichbar), antwortet er mit seiner MAC-Adresse.

Windows-CMD-Tool :
>arp<
>arp -a< Auflisten bekannter IP-MAC-Assoziationen
>arp -s IP MAC< Zuordnen einer neuen MAC-Adresse

Artikel zu Arp-Spoofing
http://www.linux-magazin.de/Ausgaben/2004/06/Interner-Zugriff

>IHK-Prüfung
Paketlaufzeit-Analyse > Schlussfolgerung > Man-In-The-Middle-Attacke (MitM)
Arp Flooding: Zwingt durch fluten der Arp-Tabelle mit Anfragen einen Switch zu nächst niedrigeren Funktionalität herunter > Hub

Internet Protokoll - IP

Funktion: Stellt die Ende-zu-Ende-Verbindung innerhalb einer Kommunikations-Beziehung her; die Adressierung erfolgt über logisch strukturierte Adressen (Netzwerkanteil+Hostanteil)

Fragen zu IP: Welche IP-Adressen benötigen keine Subnetzmaske?
Antwort: Klassenbezogene Adressen (Nicht CIDR).

z.B. 191.33.14.11

192 entspricht 10111111, also Klasse B

Private IP-Bereiche

Kasse A	10	0	0	0
	0 0001010			
Klasse B				
	172	16	0	0
	1**0** 101100			
Klasse C	192	168	0	0
	11**0** 00000			
_____				
Multicast				
Klasse D	224	0	0	0
	111**0** 0000			

Ist keine Netzwerkmaske angegeben, lässt sich anhand der ersten 4 Bit die Netzwerkklasse ablesen:

- Jede IP-Adresse, die mit einer 0 beginnt, gehört zu einem Klasse A-Netzwerk,
- Jede IP-Adresse, deren erste Null an der zweiten Stelle steht, gehört zu einem Klasse B-Netzwerk.
- Jede IP-Adresse, deren erste Null an der dritten Stelle steht, gehört zu einem Klasse C-Netzwerk.
- Jede IP-Adresse, deren erste Null an der vierten Stelle steht, gehört zu einem Klasse D-Netzwerk.

>IHK-Prüfung-Beispiel:

Ein PC kann kein Netzwerk aufbauen. Beim Überprüfen finden Sie die IP-Adresse 169.254.0.17. Was ist die wahrscheinliche Fehlerursache?
> PC ist automatische IP-Konfiguration über DHCP vorbereitet. Es kann jedoch keine Verbindung zu einem DHCP-Server hergestellt werden.

Fragen zu IP: Was ist eine **Unicast**adresse?

Antwort: Eine Adresse, die **einen** (1) Empfänger eindeutig identifiziert.

Fragen zu IP: Was ist eine **Broadcast**adresse?
Antwort: (Numerisch) letzte Adresse im Netzwerk und ist eine Adresse, von der aus **alle** erreichbaren Hosts aus angesprochen werden

Fragen zu IP: Was ist eine **Multicast**adresse?
Antwort: Eine Gruppenadresse. Alle Mitglieder erhalten diese Nachricht. (Mitglieder von Multicast-Gruppen sind z.B. Router, DHCP-Server,..)

Fragen zu IP: Was ist eine **Anycast**adresse?
Antwort: Adressiert den nächstliegenden Host als Mitglied einer Gruppe. Der nächstliegende Router, DHCP-Server,... Nur für IPv6 verfügbar.

https://de.wikipedia.org/wiki/Unicast

Fragen zu IPv4: Was ist symmetrisches Subnetting?
Antwort: Aufteilen eines vorgegebenen Netzwerkes ("Basisnetz") in mehrere jeweils gleich große Teilnetze (Standardverfahren).

Symmetrische Teilnetze:

Beispiel: Erzeugen Sie aus dem Basisnetzwerk 10.240.192.0 /18 fünf symmetrische Teilnetze.

Geben Sie für jedes Teilnetz an:

- 5 Subnetze: 2^2 < 5 < 2^3 >> 3 Subnetz-Bits
- Anzahl Hosts je Subnet 2^(32-21)-2 = 2^11 -2 = 2046
- Neue Subnet-Mask 18+3 = 21

Basisnetz 10.240.192.0 /18
00001010.11110000.11000000.00000000

Basis SNM 255.255.192.0 /18
11111111.11111111.11000000.00000000

Neue SNM 255.255.248.0 /21
11111111.11111111.11111000.00000000

- 1.SN 10.240.192.0 /21
00001010.11110000.11000000.00000000

1. Host 10.240.192.1
00001010.11110000.11000000.00000001 +1

letzt. Host	10.240.199.254 00001010.11110000.11000111.11111110	+2046-1
BC	10.240.199.255 00001010.11110000.11000111.11111111	+1
2.SN	10.240.200.0 00001010.11110000.11001000.00000000	
1.Host	10.240.200.1 00001010.11110000.11001000.00000001	
l. Host	10.240.207.254 00001010.11110000.11001111.11111110	
BC	10.240.207.255 00001010.11110000.11001111.11111111	
3.SN	10.240.208.0 00001010.11110000.11010000.00000000	
1H	10.240.208.1 00001010.11110000.11010000.00000001	
l. Host	10.240.215.254 00001010.11110000.11010111.11111110	
BC	10.240.215.255 00001010.11110000.11010111.11111111	
4.SN	10.240.216.0 00001010.11110000.11011000.00000000	
1Host	10.240.216.1 00001010.11110000.11011000.00000001	
lHost	10.240.223.254 00001010.11110000.11011111.11111110	
BC	10.240.223.255 00001010.11110000.11011111.11111111	
5.SN	10.240.224.0 00001010.11110000.11100000.00000000	
1Host	10.240.224.1 00001010.11110000.11100000.00000001	
lHost	10.240.231.254 00001010.11110000.11100111.11111110	
BC	10.240.231.255 00001010.11110000.11100111.11111111	

http://www.itslot.de/2013/12/ipv4-subnetting-berechnen-schritt-fur_22.html

08.04.2015

Aufgabenstellung:

Bilden Sie im Netzwerk 192.168.1.0/24 fünf Subnetze.

Ermitteln Sie für jedes Subnetz:

- Netzwerkadresse
- Subnetzmaske
- Broadcastadresse
- 1. Hostadresse
- größte / letzte Hostadresse
- Hostanzahl

Lösung:

1.) : Ermittlung der neuen Subnetzmaske.
1.1) Ermittlung der erforderlichen Subnetz-ID-Länge

5 Subnetze gefordert:
2^2 < **5** <=2^3 => 3 Subnetz-Bits erforderlich
4 < **5** < 8

Neue Subnetzmaske:

Alte Subnetzmaske + Neue Subnetz-Bits
24 + 3 = 27

in Dezimal : 255.255.255.224

2.) : Ermittlung der Host-Anzahl je Subnetz.

Berechnung:
2^(32- Länge der neuen Subnetzmaske) - 2

2^(32-27) -2
= 2^5 -2
= 32 - 2
= 30

3.) : Berechnung der Subnetze.

1. Subnetz: 192 . 168 . 1 . 0 /27
11000000 10101000 00000001 00000000 *=Basisnetz-Adresse*

1. Host 192 . 168 . 1 . 1
11000000 10101000 00000001 00000001 *+1*

Letzter Host: 192 . 168 . 1 . 30 *+Hostanzahl-1 (29)*
11000000 10101000 00000001 00011110 *=1+30-1*

Broadcast: 192 . 168 . 1 . 31 *+1*
11000000 10101000 00000001 00011111

2. Subnetz: 192 . 168 . 1 . 32 /27
11000000 10101000 00000001 00100000

1. Host 192 . 168 . 1 . 33
11000000 10101000 00000001 00010001

Letzter Host: 192 . 168 . 1 . 62
11000000 10101000 00000001 00111110

Broadcast: 192 . 168 . 1 . 63
11000000 10101000 00000001 00111111

3. Subnetz: 192 . 168 . 1 . 64 /27
11000000 10101000 00000001 01000000

1. Host 192 . 168 . 1 . 65
11000000 10101000 00000001 01000001

Letzter Host: 192 . 168 . 1 . 94
11000000 10101000 00000001 01011110

Broadcast: 192 . 168 . 1 . 95
11000000 10101000 00000001 01011111

4. Subnetz: 192 . 168 . 1 . 96 /27
11000000 10101000 00000001 01100000

1. Host 192 . 168 . 1 . 97
11000000 10101000 00000001 01100001

Letzter Host: 192 . 168 . 1 . 126
11000000 10101000 00000001 01111110

Broadcast: 192 . 168 . 1 . 127
11000000 10101000 00000001 01111111

5. Subnetz: 192 . 168 . 1 . 128 /27
11000000 10101000 00000001 10000000

1. Host 192 . 168 . 1 . 129
11000000 10101000 00000001 10000001

Letzter Host: 192 . 168 . 1 . 158
11000000 10101000 00000001 10011110

Broadcast: 192 . 168 . 1 . 159
11000000 10101000 00000001 10011111

Erläuterungen:

1 Subnet-Bit: 128	5 Subnet-Bits: 248
2.Subnet-Bits: 192	6 Subnet-Bits 252
3 Subnet-Bits: 224	7 Subnet-Bits 254
4 Subnet-Bits: 240	8 Subnet-Bits 255

Subnetzanzahl (Aufgabenstellung)	Länge der Subnetz-ID (Anzahl Subnet-Bits)	Neue Subnetzmaske auf Basis: /16 255.255.0.0	/24 255.255.255.0	/20 255.255.240.0
3	2	/18 255.255.192.0	/26 255.255.255.192	/22 255.255.252.0
8	3	/19 255.255.224.0	/27 255.255.255.224	/23 255.255.254.0
11	4	/20 255.255.240.0	/28 255.255.255.240	/24 255.255.255.0
29	5	/21 255.255.248.0	/29 255.255.255.248	/25 255.255.255.128
41	6	/22 255.255.252.0	/30 255.255.255.252	/26 255.255.255.192
64	6	/22 255.255.252.0	/30 255.255.255.252	/26 255.255.255.192

VLSM - Variable Length Subnet Mask (asymmetrische Teilnetze)

Übung: **Aufgabe:**

Von der ICANN wurde Ihnen folgendes Class-C Netz zugewiesen: **192.152.226.0/24**

Entwerfen Sie ein möglichst effizientes Adressierungsschema mit VLSM für Ihre Niederlassungen. Entwerfen Sie Ihre Subnetze so, dass die geforderte Anzahl an IP-Adressen gerade so zugewiesen werden kann und noch möglichst viel Platz im C-Netz übrig bleibt für weitere Subnetze.

Niederlassung	**Benötigte Hosts**	Subnetzgröße	Länge Hostbereich	Länge SNM
Köln	12	12+2<2^**4** =>> 16	**4**	32-4=28
Mönchengladbach	26	32	**5**	27
Saarbrücken	29	32	**5**	27
Salzgitter	124	128	**7**	25

	Subnetzmaske	
Köln	255.255.255.240	11111111.11111111.11111111.1111**0000**
Mönchengladbach	255.255.255.224	11111111.11111111.11111111.111**00000**
Saarbrücken	255.255.255.224	11111111.11111111.11111111.111**00000**
Salzgitter	255.255.255.128	11111111.11111111.11111111.1**0000000**

Basisnetz

192 . 152 . 226 . 0 /24

Vorgehensweise

Die Anzahl der Host die in einem Subnet adressierbar sind entspricht immer der Potenz zur Basis zwei minus zwei (Netzwerk-Adresse + Broadcast-Adresse)

1.) Erforderliche Größe für jedes Subnetz ermitteln (2er-Potenzregel!)
(---> Subnetzgröße)

2.) Subnetze nach Größe ordnen:
Salzgitter, Saarbrücken, Mönchengladbach, Köln

3.) Subnetting nach Standardmethode für das (oder die) größte(n) Netz(e) durchführen.

Salzgitter:

Subnetzmaske:	255.255.255.128	/25
	11111111.11111111.11111111.10000000	
Netzwerk-Adresse	192.152.226.0	/25
	11000000.10011000.11100010.00000000	
Erster Host	192.152.226.1	/25
	11000000.10011000.11100010.00000001	
Letzter Host	192.152.226.126	/25
	11000000.10011000.11100010.01111110	
Broadcast	192.152.226.127	/25
	11000000.10011000.11100010.01111111	

4.) Subnetting nach Standardmethode für das nächst kleine Netz durchführen.
Basisnetz ist das nächste "freie" Subnet aus dem vorherigen Schritt.

Saarbrücken:

Basis-Netz:	192.152.226.128	/25
Subnetzmaske:	255.255.255.224	/27
Netzwerk-Adresse:	192.152.226.128	/27
	11000000.10011000.11100010.10000000	
Erster Host:	192.152.226.129	/27
Letzter Host:	192.152.226.158	/27
Broadcast:	192.152.226.159	/27
	11000000.10011000.11100010.10011111	
	(Netzwerkadresse+Subnetzgröße-1)	

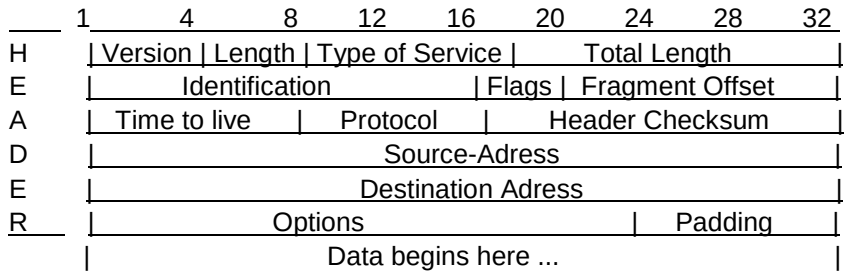
'Gladbach:

Basis-Netz:	192.152.226.160	/27
Subnetzmaske:	255.255.255.224	/27
Netzwerk-Adresse:	192.152.226.160	/27
Erster HoRst:	192.152.226.161	/27
Letzter HoRst:	192.152.226.190	/27
Broadcast:	192.152.226.191	/27

Kölle:

Basis-Netz:	192.152.226.192	/27
Subnetzmaske:	255.255.255.240	/28
Netzwerk-Adresse:	192.152.226.192	/28
Erster Horst:	192.152.226.193	/28
Letzter Horst:	192.152.226.206	/28
Broadcast:	192.152.226.207	/28

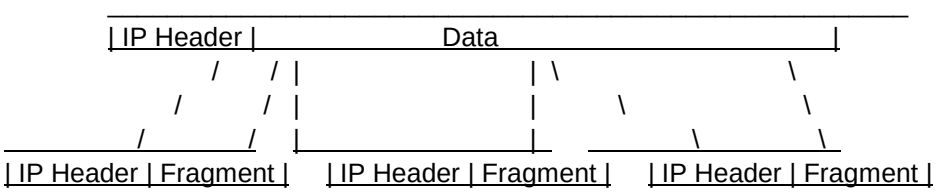
IPv4-Headerformat:



Total Length: 64bit? <> 64KiB

2^16 -1 ist die maximale Länge der im "Total Length"-Bereich darstellbaren Größe

Prinzip der Fragmentierung:



- Ein IPv4 Paket kann in mehrere Einzelpakete zerlegt werden. Dabei erhält jedes Fragment eine Kopie des Original-Headers und einen sequenziellen Anteil des ursprünglichen Datenvolumens (payloads).
- Die einzelnen Fragmente unterscheiden sich nur im Header
  - die Gesamtlänge (diese Bezieht sich auf das Segment) ,
  - das Fragment-Offset (gibt die Position des Fragmentes innerhalb eines Fragmentstroms wieder) und ggf.
  - das Frag-More-Flag bei Erwartung von noch weiteren Fragmenten.
- Die Identifikationsnummer ist bei allen gleich.
- "Time to live" (TTL) gibt die Lebenserwartung eines Paketes an. Jeder Router dekrementiert diesen Wert beim Weitertransport, wird 0 erreicht, wird das Paket gelöscht, um "Rundläufer" ohne erreichen des Ziels zu verhindern.

>tracert< (Windows)

Traceroute sendet mehrfach IP-Datenpakete vom Typ ICMP Echo Request an den

Ziel-Host, beginnend mit einer *Time to Live* (TTL) von 1. Der erste Router, der das Datenpaket weiterleiten soll, zählt den Wert der TTL um eins herunter auf 0, woraufhin er es nicht weiterleitet, sondern verwirft. Dabei sendet er die ICMP-Antwort Typ 11: *Time exceeded* mit Code 0: *Time to live exceeded in transit* an den Absender.

>TCP/IP.doc

IPv6

rfc2460: Beschreibung der Header-Struktur aus Rfc zu entnehmen.
http://tools.ietf.org/html/rfc2460,

rfc3513: Adressarchitektur und Adressierung
http://tools.ietf.org/html/rfc2513

RFC-Primärquelle: https://www.rfc-editor.org/

https://www.youtube.com/watch?v=lCtht37clfA

Warum?
- Adressknappheit in IPv4
- Starres und z.T. überladenes Headerformat
- Broadcastproblem!
- Fehlende Autokonfiguration in IPv4
- ...

Was ist neu?
- 128 Bit Adresslänge (2^128 ~ 3,4 * 10^38 Adressen)
- Konzept der Extensions-Header (eingebaute Erweiterungsmöglichkeit)
- Autokonfiguration (Nachbarerkennung) für lokale Umgebungen.
- Es gibt keine Broadcastadressen mehr!
- Neue Adressierungsart: Anycast.
- Nutzung fester Routen (optional)
- Priorisierung von Paketen
- Spezielle Headerformate für Routingoption, Verschlüsselung, Authentifizierung

>MITSCHRIFT.XLSX
>TCP_IP.DOC

Selbststudium: "nur schauen" :Mitschrift > IPV6 > Beispiel_IP_V6_a.xfsx / .._b.xfsx /...Loesung.xfsx

09.04.2015

IPv6

Headerformat

| Basis-Header | Extended Header? | Extended Header? | ... | Payload |

Der Extended Header kann anwendungsspezifische Einträge enthalten und wird im BasisHeader ggf. benannt. Er enthält aber auch vorgegebene Einträge:

Hop-by-Hop-Options
Routing
Fragment

Destination Options
Authentification
Encapsulating Security Payload (->IPSec) [EH,...]

IPv6-Adressen/Adressierung

Die Notation erfolgt acht von : getrennten Tetraden in hexadezimaler Schreibweise.

Eine Tetrade entspricht 2 Byte, also 16 Bit - eine Adresse somit 128 Bit

2001:A321:00C7:0000:0000:0A51:0000:023F

Aneinanderhängende mit Null gesetzte Tetraden können mit **::** genau EIN mal gekürzt werden:
Führende Nullen in Tetraden können immer mit weg gekürzt werden.

2001:A321:C7**::**A51:0:23F

Präfix

Der Präfix entspricht in der Schreibweise und Bedeutung der IPv4-Subnetzmaske
in CIDR-Schreibweise.

2001:A321:C7**::**A51:0:23F /**16**

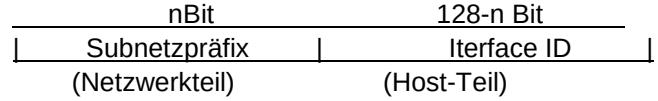
Adresstypen

00...0	::/128	unspezifische Adresse
00...1	::1/128	Loopback-Adresse
11111111	FF00::/8	Multicast-Adresse
1111111010(000000)	FF80::/10	Link-local-Unicastadresse
1111111011	FFC0::/10	Site-local-Unicastadresse

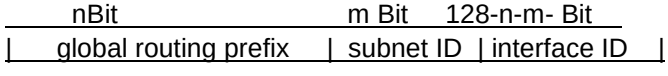
alles andere: ... Global Unicastadressen
gegenwärtig (fast)immer 2001: ...

Struktur

allgemein:



global unicast:



>**IHK-PRÜFUNG**>!! n + m =64!!!!

Dual Stack: beschreibt das gleicheizige Betreiben einer IPv4 und IPv6 Architektur auf einer Schnittstelle

Beispiel IPv6 Adressierung:

Unternehmensnetz: 2001:0000:9D38::/48

(ausführlich) 2001:0000:9D38:**0000**:0000:0000:0000:0000 /48

Standorte: /55 max. Standorte 128
Standortnetze: /63 max. Standortnetze 256

Die Differenz zwischen der Netz-ID und Standort ID bildet die max Anzahl der Netzwerke: 55- 48 = 7 2^7= 128

Standorte binär (von 49 bis 64 Bit)

0000 0000 0000 0000

z.B. Standort 13 :

Binär **0001 1010 0000 0000**
Hex 2001:0000:9D38:**1a00**:: /55

z.B. Standort 13, Netz 12:

Binär: **0001 1010 0001 1000**
Hex: 2001:0000:9D38:**1A18**::/63

Anzahl der Host-Adressen:

/128 - /63 (Unternehmensnetzte und Standortnetze) = 65 (Host-Bits)
>> 2^65 ~ 3,7 * 10^19 Hosts

Erste Host-Adresse:

2001:0000:9D38:**1A18**::1 /63

Letzte Host-Adresse:

2001:0000:9D38:**1A1**9:FFFF:FFFF:FFFF:FFFE /63

Gateway-Adresse:

2001:0000:9D38:**1A19**:FFFF:FFFF:FFFF:FFFF /63

Übung zur IPv6 Adressierung:

2001:00C7:7214:0561:**0000**:**0000**:**0000:0000**

(Bit) 16 32 48 64

Unternehmen: 2001 : 00C7 : 7214 : 0561 :: /64

500 Länder [DE=49, FR33, BR=55] +9 Bit = /73

200 Regionen [Sachs=35, Südwest=5,Manaus=92] +8 Bit = /81

1000 Orte [leipzig=3,Pau=22, Manaus=1] +10Bit = /91

100 Abteilungen [Verwaltung=56,Einkauf=18, Vertreib=61] +7 Bit = /98

Aufgabenstellung:

Bitte ermitteln Sie gemäß der oben angegebenen Vorgaben und der drei Beispiele die IPv6-Netzwerkadressen für:

1. Netz: Deutschland-Sachsen-Leipzig-Verwaltung
2. Netz: Frankreich-Südwest-Pau-Einkauf
3. Netz: Brasilien-Manaus-Manaus-Vertrieb

1.Netz:

(Bit)16 32 48 64 80 96 112 128

2001:00C7:7214:0561:**0000**:**0000**:**0000:0000**

0000

00011000 10000000 << Länder ID in **Dual** (DE=dez 49) 9 Bit!!!

0000:0000

00011000 10010001 10000000 << Bundesland in **Dual** (SA=35) 8 Bit!!!

0000:0000:0000

00011000 10010001 10000000 01100000 <<Stadt in Dual (L=3) 10 Bit!!

0000:0000:0000:0000

00011000 10010001 10000000 01101110 00000000 <<Abt. in Dual (Verw.=56) 7Bit!!

Bin : 0001 1000 1001 0001 1000 0000 0110 1110 0000 0000

Hex: 1 8 9 1 : 8 0 6 E : 0 0

>> 2001:00C7:7214:0561:1891:806E:0000:0000 /98

2.Netz:

2001:00C7:7214:0561:**0000**:**0000**:**0000:0000 /48**

9 Länder-Bits (Fr=33) > dez 33 > bin 0001 0000 1

8 Regional-Bits (Südwest = 5) > dez 5 > bin 0000 0101

10 Städte-Bits (Pau=22) > dez 22 > bin 0000 0101 10

7 Abteilungs-Bits (Einkauf=18) > dez 18 > bin 0010 010

...0001 0000 1000 0010 1000 0010 1100 0100 1000

1 0 8 2 : 8 2 C 4 : 8

2001:00C7:7214:0561:1082:82C4:8000::/96

Übung 2

Ermitteln Sie für das IPv6-Netzwerk

2001:A3:C46::/48

und eine **16**-Bit-Subnetz-ID folgende Angaben:

Subnetz-ID: 62

Netzwerkadresse

1. Host-Adresse

größte Host-Adresse

Gateway-Adresse

2001:00A3:0C46:0000:0000:0000:0000:0000 /48

62 = 0000 0000 0011 1110 (16bit, s.o.)

0 0 3 E

2001:00A3:0C46:**003E**:0000:0000:0000:0000 /64 Netzwerkadresse

2001:00A3:0C46:**003E**:0000:0000:0000:0001 /64 erste Hostadresse im Subnetz

2001:00A3:0C46:**003E**:FFFF:FFFF:FFFF:FFFE /64 letzte Hostadresse

2001:00A3:0C46:**003E**:FFFF:FFFF:FFFF:FFFF /64 Gatewayadresse

Hilfstabellen

Dez	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*A*	*B*	*C*	*D*	*E*	*F*
Hex	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
Bin	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
1	2	4	8	16	32	64	128	256

2^9	2^10	2^11	2^12	2^13	2^14	2^15	2^16
512	1024	2048	4096	8192	16384	32768	65536

Wenn's schnell gehen muss:

http://www.arndt-bruenner.de/mathe/scripts/Zahlensysteme.htm

Transportschichtprotokolle

TCP Transmission Control Protocol (OSI Layer 4)

UDP User Datagram Protocol (OSI Layer 4)

Hier findet eine direkte Anwendungskommunikation statt, z.B. zwischen Web-Server und Browser über eine Port-Adresse.

TCP wird eingesetzt, wenn die Sicherheit (im Sinne unbeschädigt) der Nachricht sichergestellt werden soll.

Im Flags- Feld wird der Zustand der Nachricht festgehalten und mitgeteilt.

Flag: 1 Bit 1/0 gesetzt / nicht gesetzt

TCP Flags

URG	Urgent = Dringend
ACK	Acknowledge = Bestätigung
PSH	Push = Weiterleitung
RST	Reset = Rücksetzung
SYN	Synchronize
FIN	Final = Ende

Phase: Verbindungsaufbau:

HostA ▉ >>> (Flags=SYN), (Seq=x) >>>>>> ▉ Host B
HostA ▉ <<<< (Flags=SYN,ACK), (Seq=x+1) (ACK=x+1)>>>>>> ▉ Host B
HostA ▉ >>>> (Flags=ACK), (Seq=x+1) (ACK=y+1) >>>>>> ▉ Host B

Phase: Nachrichtenaustausch

Phase: Verbindungsabbau (TCP Flags)

HostA ▉ >>> TCP-FIN
TCP-FIN-ACK <<<<< ▉ Host B

Ablauf analog des Verbindungsaufbaus;
Anstelle SYN-Flags ist das FIN-Flag gesetzt.

http://www.syn-wiki.de/LAN-WAN-Analysis/htm/ger/_0/TCP_Flags.htm

Das UDP-Protokoll ist das einfacherer Protokoll , während das TCP über mehr Header-Informationen verfügt.

UDP wird eingesetzt, wenn zeitkritisch Nachrichten zugestellt werden sollen, bzw. wenn diese keinen großen Verarbeitungsaufwand darstellen (z.B. DNS-Abfragen)

Sicherheit in Netzwerken

- Sicherheitsstandards festlegen
- Vermittlung von Sicherheitsstandards

- Programme(Websites) mit Blick auf sicherheitskritischen Features
- Kommunikation zu anderen Anwendungen / Datenbanken

- Berücksichtigung von Sicherheitsaspekten bei Kundenberatung und Planung

Grundziele (cryptographische) der IT-Sicherheit

= Netzwerksicherheit + Anwendungssicherheit + Systemsicherheit + Anwender

1.) Vertraulichkeit -> Verschlüsselung
2.) Authentizität -> Authentifizierung/Anmeldung/Accounting/Certs
3.) Integrität -> Prüfsummenverfahren/Zertifikate (Hashing)
4.) Verbindlichkeit -> Timestamp (Protokollverfahren)

1.) Verhinderung unerwünschter Einsichtnahme in Nachrichten
2.) Eindeutige Feststellung der Identität eines Kommunikationspartners
3.) Verhinderung oder Erkennbarmachung von Manipulationen an Dokumenten
4.) Rechtssicheres Nachweisen einer dedizierten Aktivität eines dedizierten Handlungstragenden zu einem bestimmten Zeitpunkt

>PP-Präsentation>

Ein Verschlüsselungssystem muss so gut sein, dass es den Wert der verschlüsselten Nachricht übersteigt, damit das "Knacken" unrentabel wird. ("unbegrenzte" finanzielle Mittel besitzen nur Staaten oder Geheimdienste)

Wenn man die Vigenère-Chiffre so verwendet, dass der Schlüssel möglichst lang ist und deren Werte wirklich zufällig gewählt wurde, entsteht eine uneingeschränkt sichere Chiffre. Jeder Schlüssel darf dafür nur ein mal verwendet werden. Dieses Verfahren wird One-Time-Pad genannt.

Für die binäre Verschlüsselung gilt demnach:

Ein Klartextbit z wird mit dem Zufallsbit r chiffriert durch die Vorschrift:
$Z = (z + r) \bmod 2 = z \text{ XOR } r.$

Es bleibt das Schlüsselaustauschproblem. Verweis: -> Michael Rabin

Moderne kryptografische Algorithmen

Es gibt generell zwei Kategorien: symmetrische & asymmetrische Verfahren

Symmetrische Verfahren nutzen zum Chiffrieren und Dechiffrieren immer gleiche Schlüssel.

Asymmetrische Verfahren verwenden zum Chiffrieren und Dechiffrieren unterschiedliche Schlüssel (public und private keys). Der öffentliche Schlüssel dient zum Verschlüsseln, nur der private Schlüssel ermöglicht das Entschlüsseln.

Symmetrische Algorithmen:

- Data-Encryption-Standard (DES)/3DES - unsicher
  - Advanced-Encryption-Standard (AES)
  - International-Data-Encryption-Algorithm (IDEA, ETH)
  - Blowfish, Twofish (Bruce Schneier)
  - RC2/RC3 (Ron Rivest, MIT)

Beispiel **DES**:
Das Prinzip: Ein 64-Bit-Klartextblock wird beim Durchlauf von ingesamt 16 Runden jeweils mit unterschiedlichen Teilen eines 128-Bit-Schlüssels durch Permutation und Substitution verknüpft.

Wichtig: DES wird seit 1994 mit stark fallendem Aufwand an Rechenzeit gebrochen und gilt als nicht mehr zuverlässiges Verfahren.

Vorteile:

- Sie sind schnell, d.h. sie haben einen hohen Datendurchsatz.
- Die Sicherheit ist im wesentlichen durch die Schlüssellänge festgelegt, d.h. bei guten symmetrischen Verfahren sollte es keine Attacken geben, die wesentlich besser sind als das Durchprobieren aller Schlüssel (Brute-Force-Attacken).
- Sie bieten hohe Sicherheit bei relativ kurzem Schlüssel.
- Die Schlüsselerzeugung ist einfach, da gewöhnlich als Schlüssel jede Bitfolge einer festen Länge erlaubt ist und als Schlüssel eine Zufallszahl gewählt werden kann.

Nachteile:

- Jeder Teilnehmer muss sämtliche Schlüssel seiner Kommunikationspartner geheim halten
- Zur Schlüsselverteilung sind sie weniger gut geeignet als asymmetrische Verfahren, insbesondere bei einer großen Anzahl von Kommunikationspartnern
- Für Verbindlichkeitszwecke sind sie weniger praktikabel als asymmetrische Verfahren, da bei der Verwendung symmetrischer chlüssel nicht ohne weiteres erkannt werden kann, welcher der beiden Kommunikationspartner die Nachricht verschlüsselt hat. Dies lässt sich nur die zwischengeschaltete dritte Partei sicherstellen, die über entsprechende kryptographische Protokolle in den Nachrichtenfluss eingebunden wird.

Public-Key-Verfahren

- RSA (R. Rivest, A. Shamir, L. Adlam)
- Diffie-Hellman-Algorithmus
- ElGamal-Algorithmus

Beispiel RSA

Das Verfahren nutzt die Schwierigkeit, große Zahlen in Primfaktoren zu zerlegen in Verbindung mit der Modulo-Arithmetik. Vereinfacht: es ist mathematisch problemlos, zwei große (Prim-) Zahlen zu multiplizieren. Es ist aber sehr aufwändig, aus dem Produkt die Faktoren zu ermitteln.

Der Ablauf:

Schlüsselerzeugung:

1.) Wähle zufällig zwei große Primzahlen p und q. Die Länge der Zahlen sollte mindestens 512 Bit betragen.
2.) Berechne n = pq (n hat eine Länge von mindestens 1024 Bit)
3.) Wähle eine kleine ungerade natürliche Zahl e, die zu phi(n) = (p-1)(q-1) relativ prim ist, d.h. es gilt ggT (e,phi(n))=1 (alles klar?)
4.) Berechne d als Lösung der Gleichung ed mod phi (n)=1
5.) Gib das Paar P = (e,n) bekannt als öffentlichen Schlüssel
6.) Halte das Paar S = (d,n) geheim als geheimen Schlüssel

Verschlüsseln: Die Nachricht M wird codiert als E(M) = M^e mod n

Entschlüsseln: Der Chiffretext C wird decodiert durch D(C) = C^d mod n

Ablauf eines asymmetrisch verschlüsselten Nachrichtenaustausches:

Protagonisten:

Alice	Sender der gesicherten Nachricht
Bob	Empfänger der gesicherten Nachricht
Eve	Mitleser einer gesicherten Nachricht
Mallory	"man in the middle"

1. Alice und Bob Installieren jeweils auf ihren Rechnern eine Sicherheitssoftware (z.B. GnuPG)

2. Alice und Bob erzeugen mit Hilfe der Software jeweils unabhängig voneinander ein Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel.

3. Alice und Bob tauschen ihre jeweiligen öffentlichen Schlüssel untereinander aus.

4. Alice verfasst in ihrem Mailprogramm eine Nachricht an Bob, verschlüsselt sie mit Hilfe der Sicherheitssoftware und des integrierten asymmetrischen Algorithmus (z.B. RSA) und unter Nutzung des öffentlichen Schlüssels von Bob.

5. Die verschlüsselte Nachricht wird an Bob übertragen.

6. Bob entschlüsselt die Nachricht mit Hilfe seiner Sicherheitssoftware und des integrierten asymmetrischen Algorithmus (...) und unter Verwendung seines privaten Schlüssels.

7. Die Nachricht liegt in entschlüsselter Form bei Bob vor.

Vorteile (guter) asymmetrischer Verfahren:

- Jeder Teilnehmer einer vertraulichen Kommunikation muss nur seinen eigenen privaten Schlüssel geheim halten.
- Sie lassen sich einfach für digitale Signaturen benutzen.

- Sie bieten elegante Lösungen für die Schlüsselverteilung in Netzen, die die öffentlichen Schlüssel bzw. Schlüsselzertifikate frei zugänglich auf zentralen Servern gespeichert werden können, ohne die Sicherheit des Verfahrens zu beeinträchtigen.
- Sie sind gut geeignet für Nicht-Abstreitbarkeitszwecke.

Nachteile asymmetrischer Verfahren:

- Sie sind langsam, d.h. sie haben im allgemeinen einen geringen Datendurchsatz.
- Sicherheit: für alle bekannten Public-Key-Verfahren gilt: Es gibt wesentlich bessere Attacken als das Durchprobieren aller Schlüssel, deshalb werden (im Verglaich zu symmetrischen Verfahren) relativ lange Schlüssel benötigt, um ein gleich hohes Maß an Sicherheit zu erreichen.
- Die Sicherheit beruht "nur" auf der vermuteten, aber von der Fachwelt anerkannten, algorithmischen Schwierigkeit eines mathematischen Problems (zum Beispiel die Zerlegung einer großen Zahl in die Primfaktoren).
- Die Schlüsselerzeugung ist i.a. komplex und aufwändig, da die Erzeugung "schwacher" Schlüsselpaare vermieden werden muss. Hybride Verfahren versuchen, die Vorteile beider Arten von Verschlüsselung zu kombinieren: sie benutzen asymmetrische Verschlüsselung, um einen Sitzungsschlüssel (Sessionkey) für ein symmetrisches Verfahren zu übermitteln, und verschlüsseln die Massendaten mit dem symmetrischen Verfahren. Der Sessionkey wird gewöhnlich nur für eine Sitzung (Übertragung) verwendet und dann vernichtet. Das asymmetrische Schlüsselpaar wird je nach Umständen für einen langen Zeitraum verwendet.

Anwendungsbeispiele:

- PGP - RSA zum Schlüsselaustausch, IDEA zum Verschlüsseln, MD5 + RSA zur Signatur
- SSH - RSA zur Identifikation und Schlüsselaustausch, IDEA, Blowfish oder 3DES zum Verschlüsseln
- SSL - RSA zur Authentifikation, DES, 3DES, IDEA... zum Verschlüsseln, MD5 als Einweg-Hash

Hybrides Verschlüsselungsverfahren:

(Verwendung bei SSL-gesicherten Protokollen, wie ssh, https, pop3s,...,
VPN-Verbindungen)

Beispielhafter Ablauf für eine gesicherte https-Verbindung:

- Client stellt eine https-Verbindungsanfrage an den Webserver
- Der Webserver bestätigt die Verbindungsanfrage und schlägt dem Client eine Liste von Verschlüsselungsverfahren vor.
- Der Webserver überträgt ein Zertifikat an den Client. Der Client prüft dieses durch Einreichung bei einem sog. "Trust Center" (vertrauenswürdige dritte Stelle)
- Client und Server handeln untereinander die beidseitig verfügbaren und damit nutzbaren Algorithmen aus.
- Der Webserver sendet seinen öffentlichen Schlüssel an den Client.
- Der Client erzeugt eine große Zufallszahl(!), verschlüsselt dies über ein asymmetrisches Verfahren und mit dem öffentlichen Schlüssel des Webservers.
- Der Client überträgt die verschlüsselte Nachricht an den Webserver.
- Der Webserver entschlüsselt die übertragene Zufallszahl mit Hilfe seines privaten Schlüssels.
- Damit besitzen Client und Webserver ein "gemeinsames Geheimnis";die Zufallszahl. Diese wird für die Dauer des folgenden Nachrichtenaustausches als gemeinsamer

Schlüssel innerhalb eines symmetrischen Verfahrens verwendet.

Da dieser Schlüssel für jede erneute Verbindungzwischen den Kommunikations-partnern wiederholt ausgehandelt wird, spricht man hier vom sog. **Session Key.**

Vorteile:

- Das rechenaufwendige asymmetrische Verfahren wird nur beim Verbindungsaufbau benötigt, um einen gemeinsamen Schlüssel zu erzeugen.
- In folge kann das effiziente symmetrische Verfahren bei bestehender Verbindung genutzt werden.
- Die integrierte Authentifizierung (Überprüfung des Zertifikates) ermöglicht die Überprüfung der vorgegebenen Identität

---

Akronym-Übersicht

Protokolle:

ATM	Asynchronous Transfer Protocol (OSI Layer 2)
ARP	Address Resolution Protocol (OSI Layer 2)
DHCP	Dynamic Host Configuration Protocol (OSI Layer 5-7, nutzt TCP)
DNS	Domain Name Service (OSI Layer 5-7, nutzt UDP/TCP/IP)
FTP	File Transfer Protocol (OSI Layer 5-7, nutzt TCP/IP)
ICMP	Internet Control Message Protocol (OSI Layer 3)
IMAP	Internet Mail Access Protocol (OSI Layer 5-7)
IP	Internet Protocol (OSI Layer 3)
IPX	**I**nternetwork **P**acket e**X**change (Novell Netware) (OSI Layer 3)
NetBIOS	Network Basic Input Output System (Microsoft) (OSI Layer 3)
NNTP	Network News Transfer Protocol (OSI Layer 5-7, nutzt TCP/IP)
NTP	Network Time Protocol (OSI Layer 5-7, nutzt UDP)
POP3	Post Office Protocol V.3 (OSI Layer 5-7, nutzt TCP/IP)
RDP	Remote Desktop Protocol (OSI Layer 5-7, nutzt TCP/IP)
RFB	Remote Framebuffer Protocol (OSI Layer 5-7, nutzt TCP/IP)
SMTP	Simple Mail Transfer Protocol (OSI Layer 5-7, nutzt TCP/IP)
SPX	**S**equenced **P**acket **E**xchange (OSI Layer 4)
SSL	Secure Session Layer (OSI Layer 5-7, nutzt TCP/IP)
TCP	Transmission Control Protocol (OSI Layer 4)
UDP	User Datagram Protocol (OSI Layer 4)

CSMA/CD	**C**arrier **S**ense **M**ultible **A**ccess / **C**ollision **D**etection
FDDI	Fibre Distributed Data Interface
MIME	**M**ultipurpose **I**nternet **M**ail **E**xtension

Netzwerke & Zonen:

DMZ	Demilitarized Zone (http://de.wikipedia.org/wiki/Demilitarized_Zone)
VLAN	Virtual LAN

LAN	Local Area Network

MAN	Metropolitan Area Network
WAN	Wide Area Network
Telnet	Teletype Network

Standards:

ASCII	**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange
DENIC	DE Network information Center
IEEE	Institute of Electrical and Electronics Engineers
ISDN	Integrated Service Digital Network
ISO	International Organization for Standardization

Hardware:

AWG	American Wire Gauge (http://de.wikipedia.org/wiki/American_Wire_Gauge)
BNC	British Naval Connector (Koaxial-Kabel)
NIC	Network Interface Connector
RAID	Redundant Array of Independent Disks
RJ45	**Registered Jack** - Netzwerk Anschluss
TTY	Teletype
UTP	Unshielded Twisted Pair (NW-Kabel)

Sonstige:

CRC	Cyclic Redundancy Check
CMS	Content Management Sytem
EMV	Elektromagnetische Verträglichkeit
LSB	Least significant bit
MAU	Media Access Unit (>Token-Ring)
MTBF	Mean Time Between Failures
MSB	Most Significant Bit(s)
SSH	Secure Shell
TCO	Total Cost of Ownership
VLSM	Variable Length Subnet Mask
VNC	Virtual Network Computing
XOR	e**X**clusive **OR >** Entweder/Oder