Vorlesungsreihe
Entwicklung webbasierter Anwendungen

Technische Grundlagen und Protokolle

Prof. Dr.-Ing. Thomas Wiedemann
email: wiedem@informatik.htw-dresden.de

HOCHSCHULE FÜR TECHNIK UND WIRTSCHAFT DRESDEN (FH)
Fachbereich Informatik/Mathematik

Einordnung in die inhaltliche Thematik

Schwerpunkte

- Wiederholung und Vertiefung zu den notwendigen Basistechnologien aus den Bereichen Netzwerktechnik, Verteilte Informationssysteme, Programmierung und Datenbanken
  - Netzwerkgrundlagen (Wiederholung OSI-Referenzmodell)
  - Protokolle (TCP/IP , IP6, http, ...)
- Technologien und Werkzeuge zur Entwicklung webbasierter Anwendungen
- Webbasierte Anwendungen im realen Einsatz (Dimensionierung und Sicherheit)

Internet - Technische Grundlagen

- Kurze Historie
- Netzwerktechnologien
- OSI-Referenzmodell
- Vergleich OSI – Internet
- Basisprotokolle (IPv4, TCP/IP, UDP, SMTP, HTTP)
- Typische Konfigurationsparameter
- IPv6

Historische Entwicklung des Internet

- als heterogenes Netz ab 1969 durch das amerikanische Verteidigungsministerium entwickelt
- wesentliche Ziele:
  - **Ausfallsicherheit auch bei Verlust einzelner Knoten**
  - **Verzicht auf zentrale Steuerung**
- zu Beginn unter dem Namen Arpanet (Kopplung von 4 verschiedenen Rechnern) bereits unter der Nutzung des Basisprotokolls TCP/IP
- wachsende Bedeutung auch im außermilitärischem Bereich
- um 1982 Kopplung verschiedener Regierungsnetzwerke
- endgültiger Durchbruch mit dem Einsatz in Universitäten und Hochgeschwindigkeitskopplungen zwischen Rechenzentren (UNIX-Basisnetzprotokoll)
- von 1969 bis Anfang der 80er Jahr ständige Weiterentwicklung der Protokolle zur Standardisierung des Datenaustauschs
- Die rasante Entwicklung des Internet in den 90er Jahren war untrennbar mit der Entwicklung allgemeinen Netzwerktechnik verbunden.

Wiederholung zur OSI-Referenzstruktur

OSI-Schichten

7 Application	Anwendungsschicht zur Definition anwendungsspezifischer Regeln (wie z.B. prinzipieller Aufbau einer Email (CC /BC / Subject ...)
6 Presentation	Darstellungsschicht zur Wandlung der anwendungsspezifischen Daten (Zahlen/Text/...) in oder aus den Bitmustern
5 Session	Sitzungsschicht zum geordneten Aufbau und Abbau von Verbindungen
4 Transport	Transportschicht zum Aufbau einer Verbindung zwischen den eigentlichen Nachrichtenempfängern (Applikationen)
3 Network	Vermittlungsschicht zur Koordinierung der Kommunikation mit einer größeren Anzahl von Rechnern
2 Logical	Sicherungsschicht für eine erste Steuerung und Kontrolle des Informationsflusses (bei intakten Netzen häufig schon sehr sicher)
1 Physical	Bitübertragungsschicht zum eigentlichen Transport der Informationen, hauptsächlich Definition der Hardware und Signalpegel

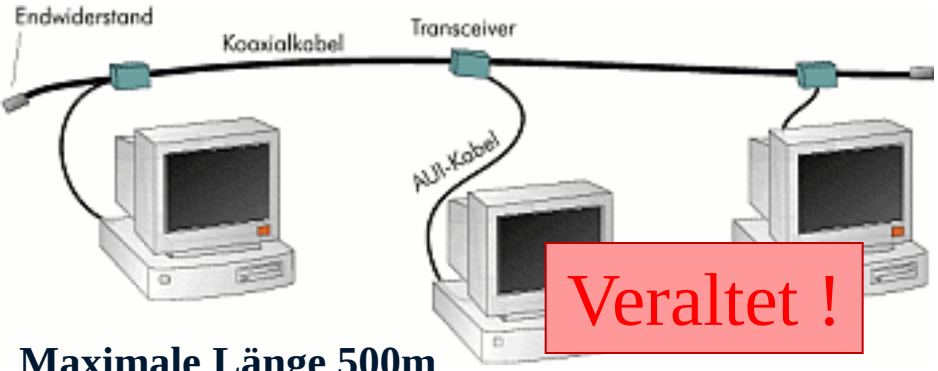
Schicht 1 – Bitübertragung : Verfügbare Optionen

- **Prinzipiell stark durch Entwicklung der Mikroelektronik geprägt** (Taktraten, Verarbeitungsgeschwindigkeit, Kosten der Hardware)

ETHERNET

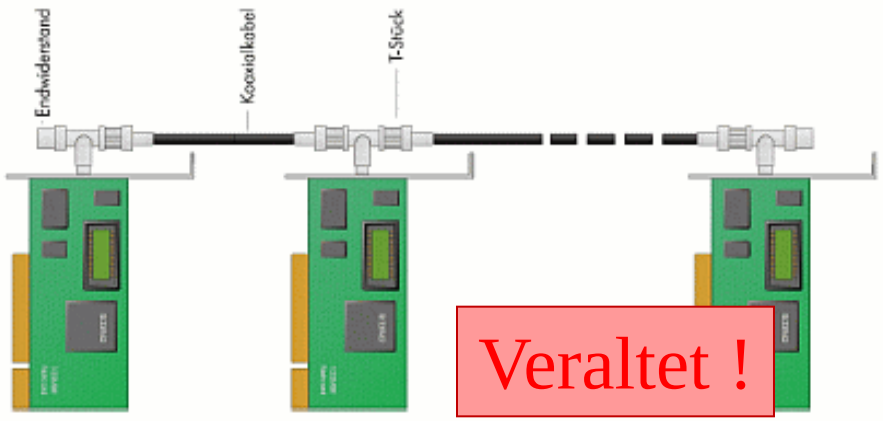
- 1973 am Xerox PARC für verteilte Systeme entwickelt
- niedrige Fehlerraten und einfach realisierbar
- auch heute noch sehr stark verbreitet
- mehrere Geschwindigkeitsvarianten (10 entspricht 10 Mbps = Mega bit per second)

Thick Ethernet mit Halbzoll-Kabel (10Base5)



Maximale Länge 500m

Thin-Ethernet mit dünnerem Kabel (10Base2)



Maximale Länge 185 m

Abb. Quelle(n): [SelfLinux]

Schicht 1 – Bitübertragung : Verfügbare Optionen II

Ethernet mit Sternstruktur (10BaseT)

- vom zentralen Verteiler, dem "Hub", führen Twisted-Pair-Kabel zu den einzelnen Rechnern
- Anschluss mit RJ45-Steckern (wie bei Telefonen)

Vorteile:

- Im Gegensatz zur sehr empfindlichen Busstruktur (ein Defekt legt das gesamte Netz lahm) kommt es bei der Sternstruktur nur zum Ausfall des einen Segmentes
- trotz höherer Kosten infolge größeren Verkabelungsaufwandes heute die am häufigsten verwendete Technologie für lokale Netze (falls nicht Glasfaser oder neuere Verfahren)
- höhere Übertragungsraten 100BaseT und 1000BaseT mit speziell geschirmten Kabeln und entsprechenden Karten (1000BaseT = 125 Mbyte/s meist für Netz-Backbones)

Maximal 100 m pro Kabel

Abb. Quelle(n): [SelfLinux]

Schicht 1 – Bitübertragung : Lastverhalten von ETHERNET

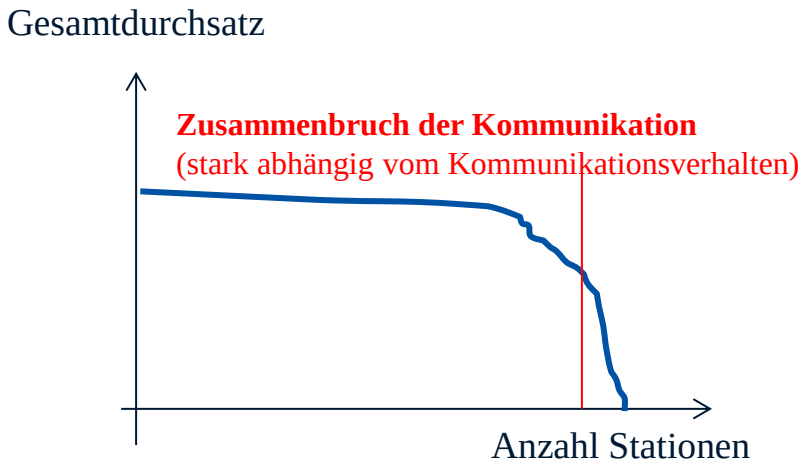
Problem bei konkurrierender Nutzung durch mehrere Rechner :

CSMA/CD – Verfahren:

- jede Netzwerkkarte im ETHERNET hat weltweite eine eindeutige ID – die MACID bestehend aus 3 Byte Herstellercode und 3 Byte laufende Nr.)
- Versand von Daten erfolgt parallel an alle Stationen ("Packet Broadcasting") in Datenpaketen mit MAC-Adresse
- bis auf Spezialfälle filtert jede Station nur die sie betreffenden Daten heraus
- jede Station kann bei freier Leitung mit einer Sendung beginnen
- sollten zwei Stationen genau gleichzeitig beginnen, ist eine derartige Kollision durch eine Verfälschung bzw. ungültige elektrische Pegel erkennbar

Bei einer erkannten Kollision gilt :

1. Alle Stationen beenden ihre Datensendung
2. Jede Station ermittelt per Zufallsgenerator eine zufällige Wartezeit und beginnt danach erneut mit der Sendung
3. Sollte es doch wieder zu einer Kollision kommen -> erneut zu 1.



Effekt dieser Regel: rascher Einbruch der Übertragungskapazität bei Überlast

Schicht 1 – Bitübertragung : Tokenring

- Nachteiliges Lastverhalten von ETHERNET wird durch Konzept einer generellen Kollisionsvermeidung ausgeschaltet

TOKENRING-Netze

- vorrangig durch IBM entwickelt und eingesetzt (Standard **IEEE 802.5)**
- ein Token (=Marke oder spezielles Datenpaket) kreist ständig im Netz
- eine Station kann nur bei Besitz des Tokens senden !
- Keine Kollision möglich, aber dafür Problem mit verlorenen Token ...

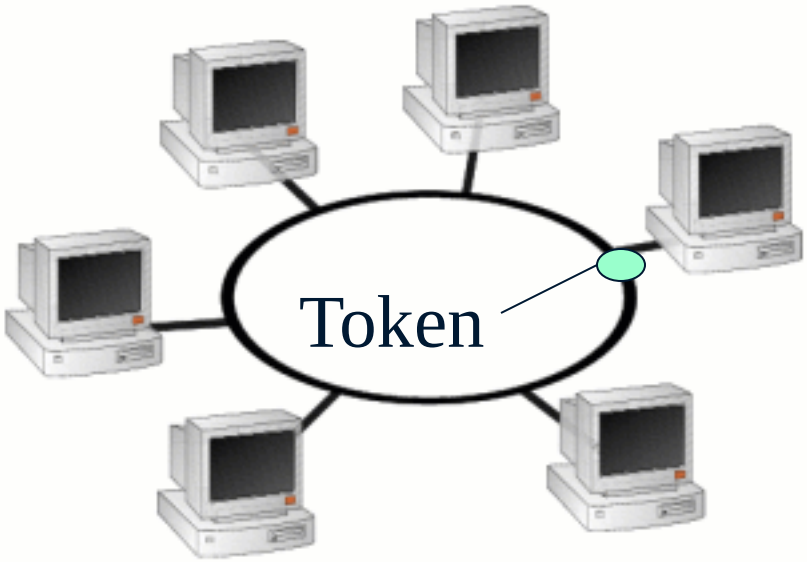


Abb. Quelle(n): [SelfLinux]

- auch neue Tokenring-Technologien durch Einsatz von Lichtleitern (FDDI "Fiber Distributed Data Interconnect") mit 100Mbit/s
- teilweise doppelter Ring zu Überbrückung einer einzelnen Fehlerstelle
- **Leider wird Tokenring von IBM nicht weiter gepflegt und ist damit VERALTET !**
- schlechtes Lastverhalten von Standard-Ethernet wird behoben durch echtzeitfähiges Ethernet – wie z.B. EtherCAT (z.B. in Industrie 4.0)

Schicht 1 – Bitübertragung : ATM - Asynchronus Transfer Mode

ATM-Netze

- ATM entspricht eher der zentralen Vermittlungstechnik bei der Telekommunikation
- durch ATM-Switches (=Matrix von Vermittlungsschaltern) werden dauerhafte Verbindungen hergestellt

Vorteile:

- durch einheitliche, relativ kleine Paketgröße geringer Verwaltungsaufwand und damit insgesamt sehr schnell
- Übertragungsgeschwindigkeit kann GARANTIERT werden (Quality of Service) !!!
- Besonders interessant für künftige Video und andere Multimediaanwendungen

Nachteile:

- sehr aufwändig, meist mit Glasfaser für Backbones

Schicht 1 – Bitübertragung : per Modem

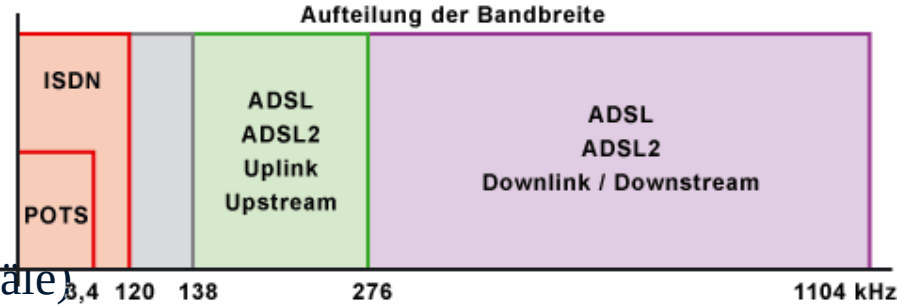
Modem

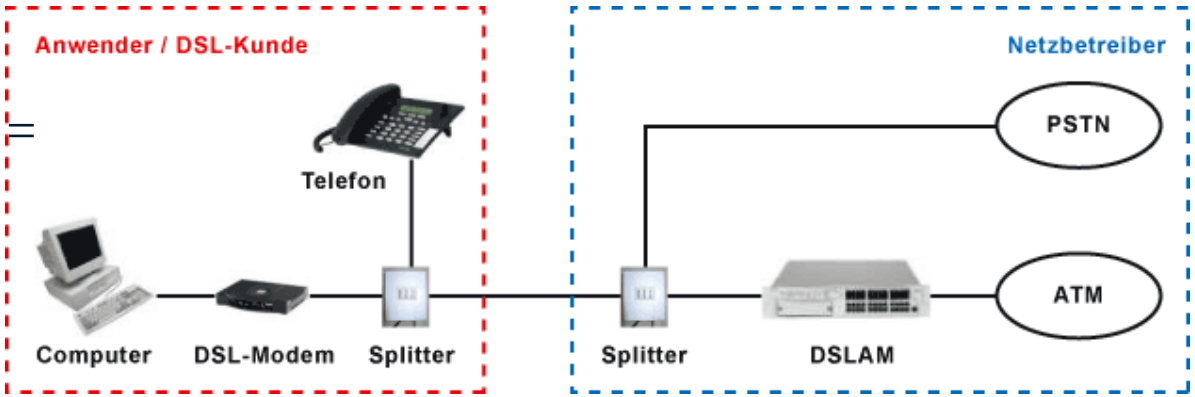
- = **Mo**dulator / **Dem**odulator
- erste Verfahren arbeiteten noch mit echten Akustikwandlern
- Analogmodem
  - wandelt Bits in Tonfrequenzen und wieder zurück
  - Geschwindigkeit in Baud: 2400 bis maximal 56000 maximal auf Standardtelefonleitung (Bit/s etwas geringer, da noch Startbits und Prüfsummen)
- ISDN-Modem
  - sendet Daten direkt – 64 Kbit/s = etwa 7-8 Kbyte / s
- spezielle Protokolle zur Fehlererkennung (Prüfsummen, selbstkorrigierende Codes)
- Umwandlung der Datenpakete aus dem Netz in entsprechende Modemprotokolle

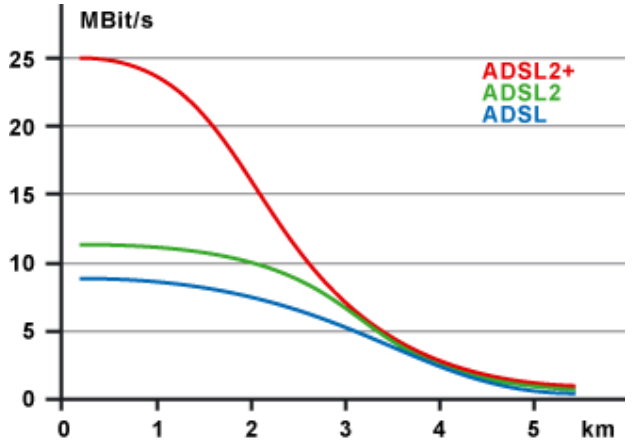
Schicht 1 – Bitübertragung : per DSL

Aktuelle Technologie: DSL - Digital Subscriber Line

- Parallele Übertragung von Telefon-und Netzdaten über normale Telefon-Kupferkabel per Frequenzmultiplex (bis 120 kHz Telefon, darüber z.B. ab 138 kHz 256 Frequenzkanäle a ca. 4,3 kHz)
- Kodierung mit Digit. Multitonverfahren
- Verteilung der Kanäle unterschiedlich:
  - ASDL – asymmetrisch (mehr Downloadkanäle) Geschwind.: Down ca. 12 Mbit/s / Up 1 Mbit/s
  - ASDL2+ mit bis zu 25 Mbits/s Download / Up 1 Mbits/s
- die genaue Bandbreite hängt von der Kabelqualität ab (Länge, Dämpfung, Störungen),da die Anzahl der Bits pro Kanal und die Anzahl verwendeter Kanäle dyn. angepasst werden







Bildquelle und weitere Details: http://www.elektronik-kompendium.de/sites/kom/0305235.htm

Unterstützung von OSI-Schicht 1 und 2

Repeater

- reine Verstärkung der Signal auf dem Netzwerk (nur Funktion auf OSI-Ebene 1)
- Zur Vergrößerung der Netzwerklänge über die physikalische-technischen Grenzen hinaus (z.B. bei 10Base2 mehrere Segmente zu 185 m)
- Keine Vorteile für Lastverhalten, da alle Daten im gesamten System verteilt werden

Bridges

- verteilen die Datenpakete in Abhängigkeit von der MAC-Adresse des Empfängers
- Pakete für gleiches Segment werden von der Bridge NICHT in das andere Segment weitergegeben, dadurch Entlastung von segmentfremden Daten (Funktion OSI-Level 1 und 2)

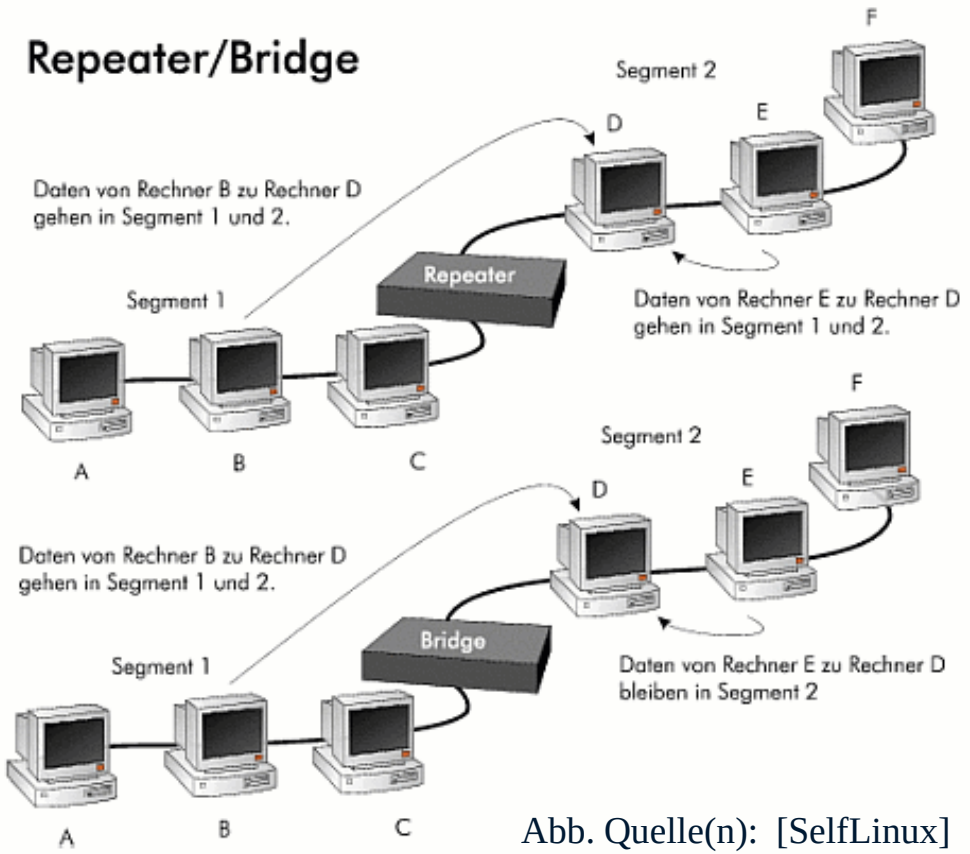


Abb. Quelle(n): [SelfLinux]

Hardware-Unterstützung von OSI-Schicht 1 bis 3

Hubs

- sternförmige Kopplung der Rechner (nur OSI-Ebene 1)
- Daten werden an ALLE Segmente gesendet

Switches

- Sternförmige MAC-adressenabhängige Schaltung von direkten Verbindungen zwischen Sender und Empfänger
- sehr effizient, da keine unnötigen Aussendungen

Gateway

- Kopplung verschiedener Rechnernetze mit unterschiedlichen Protokollen
- Wandlung der Protokolle erfordert beträchtlichen Aufwand

Uplink in andere Netze durch Bridge oder Gateway

Backbone

Unterstützung von OSI-Schicht 1 bis 3

Router

- sorgen für Verteilung der Datenpakete über unterschiedliche Netzsegmente
- verfügen über Routingtabellen mit Angaben zur Erreichbarkeit entfernter Rechner
- Können die Routinginformationen teilweise auch dynamisch an die Netzlast oder das Datenaufkommen eines Senders anpassen
- der Weg der Pakete ist nicht fixiert, sondern wird von Routern nach sehr komplexen (und geheimen) Regeln dynamisch gesteuert:

  mögliche Routing-Regeln:

  - aktuelle Auslastung (bei Überlastung über Alaska)
  - Adressenbezogen (Bevorzugung bzw. Ablehnung bestimmter Ziele)
  - Mengenregeln (kleine Mengen JA / Große Menge NEIN)

Firewall-Rechner

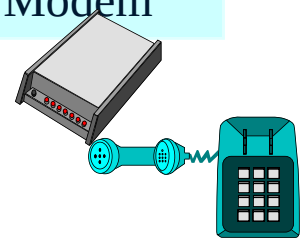
- Können als spezielle Form eines Routers/Gateways aufgefasst werden
- Filtern bzw. sperren bestimmte Datenpakete in Abhängigkeit von Adressen und Inhalt der Daten (Details siehe Sicherheit)

Vergleich der Internetstruktur mit der OSI-Referenzstruktur

OSI-Ebene	OSI-allgemein
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Logical
1	Physical

Am Beispiel der Internet-Ebenen

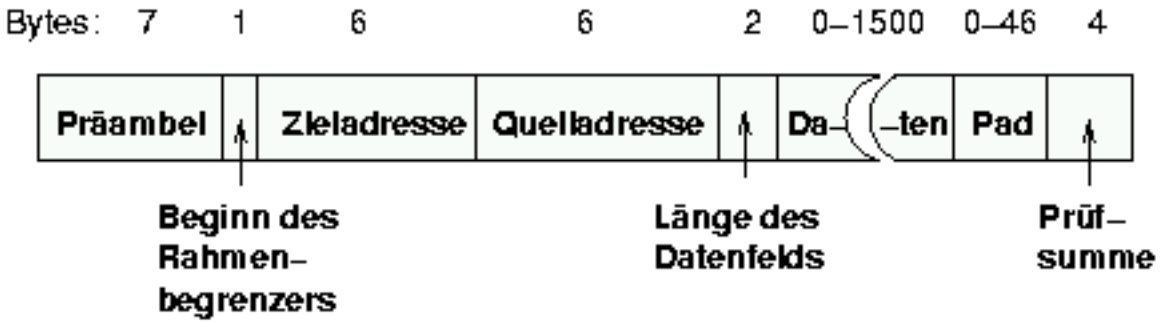
Programme Netscape Navigator Internet Explorer mailer Eudora, ...	Schnelle Spezial-anwendungen und Netzwerke NFS (File System von UNIX)
Protokoll **TCP**	Protokoll **UDP**
Protokoll **IP**	**ICMP**
Ethernet framing protocol	SLIP PPP
Netzwerkkarte (Ethernet)	Modem



Obwohl das Internet gut der OSI-Struktur entspricht, erfolgte seine Entwicklung zur damaligen Zeit ohne den OSI-Standard. Internetprotokolle sind definiert in den RFC's (Request for Comment) und sind verfügbar unter http://www.rfc-editor.org.

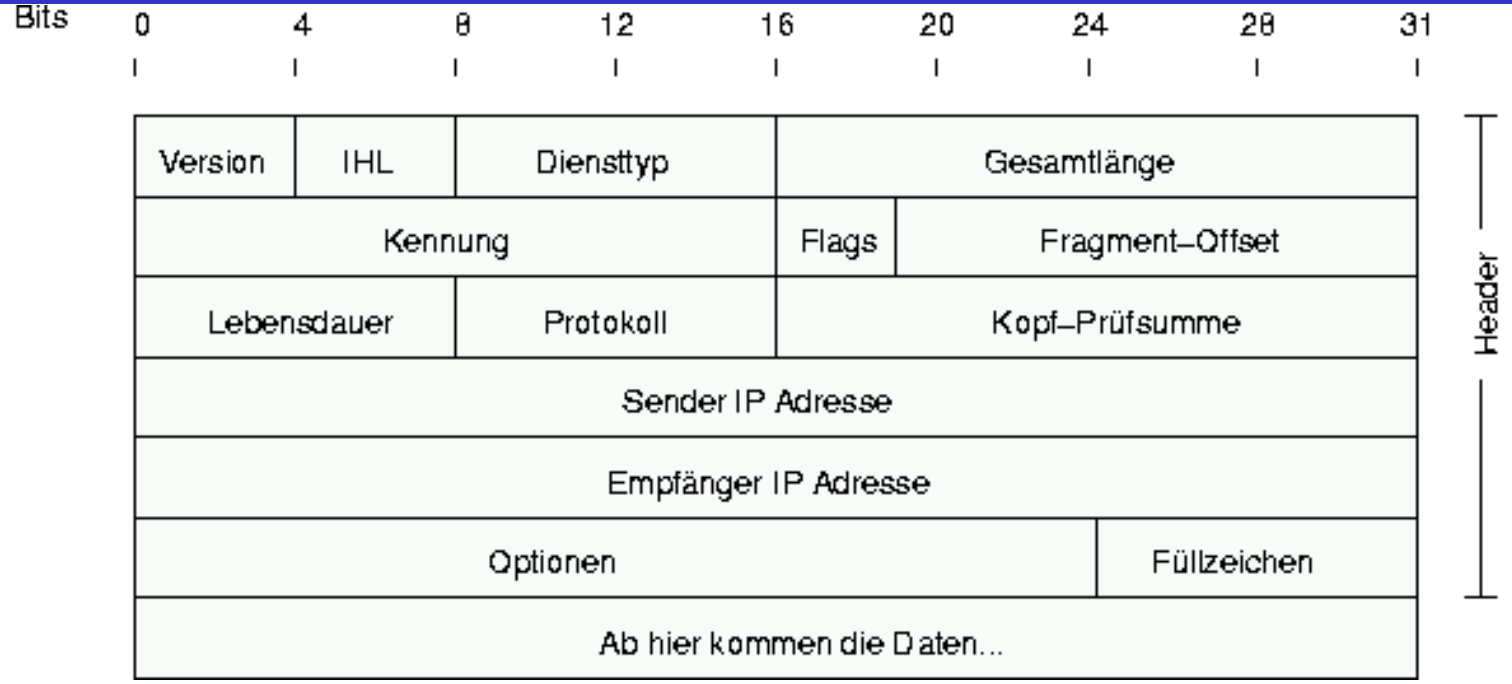
Datenformate : Der Ethernetframe

- Daten werden in Frames nach Norm IEEE Norm 802.2 verpackt :



- Präambel von 7 Bytes mit Bitfolge 10101010 zur Synchronisation der Sender/Empfänger und Kollisionserkennung (10 MHz Schwingung von 5,6 µs)
- Rahmenstartbyte mit Bitfolge 10101011 als Anfangsmarkierung
- Zieladresse und Quelladresse enthalten die physikalischen Netzwerkadressen (MAC-Adressen) von Empfängers und Sender
- Länge von 46 bis 1500 (bei Notwendigkeit Auffüllung mit PAD-Kennung) .
- Datenfeld mit entsprechender variabler Länge
- Prüfsumme zur Kontrolle des Datenfelds, bei Abweichung kann Empfänger erneute Zusendung des Pakets beantragen

Datenformate : Das Internet Protokoll (IP)



Analog zum Ethernet-Frame verpackt auch IP wieder seine Daten :

- Version - 4 Bit (aktuell = 4), zukünftig bei IP 6 =6
- Internet Header Length (IHL) - 4 Bit – Länge des Header in 32-Bit Worten an (meist 5)
- TOS (Type of Service - Diensttyp) - 8 Bit (interne Verwendung)
- Gesamtlänge - 16 Bit des Datagramms (incl. Kopf) in Byte (max. 65535 Byte)
- Kennung - 16 Bit für Reihenfolgebestimmung bei späteren Zusammenbau

Datenformate : Das Internet Protokoll (IP) - II

Weitere Felder des IP-Datagramms :

- Flags - 3 Bit zur Steuerung der Fragmentierung
- Fragment-Offset - 13 Bit zur Steuerung der Fragmentierung (Zerlegung) größerer Pakete in unterschiedlichen Routingstrecken
- **Lebensdauer** - 8 Bit : zur Vermeidung endloser Schleifen in den Routing muß jeder Router diese Zahl um 1 verringern, Bei Erreichen der Null ist das Paket zu vernichten
  (übliche Startwerte sind 32 oder 4 innerhalb lokaler Netze)
- **Protokoll** - 8 Bit zur Definition der Weiterleitung an richtige Transportschichtprotokoll beim Empfänger:
  17 - UDP 6 - TCP 1 - ICMP
- Kopf-Prüfsumme - 16 Bit - Prüfsumme nur über den Header
- **Sender IP-Adresse** - 32 Bit (siehe IP-Adressierung)
- **Empfänger IP-Adresse** - 32 Bit
- Optionen - <= 32 Bit für Optionen zum Debugging (Fehlersuche) oder Routenprüfung
- Füllzeichen zur Auffüllung des Bereiches zwischen den jeweils gesetzten Optionen und dem Ende des 32 Bit Wortes auf.

Datenformate : ICMP - Internet Control Message Protocol

- Internet Control Message Protocol (ICMP) dient zur Übermittlung technischer Meldungen und ist ein integraler Bestandteil von IP (kein Datenfluß, sondern Kontrollfluß

Aufgaben:

- Flußkontrolle
  - Steuerung der Übertragungsgeschwindigkeit : Meldungen zum Stoppen und Wiederaufnehmen der Übertragung bei Verarbeitungsproblemen beim Empfänger
- Erkennen von unerreichbaren Zielrechnern
  - Falls ein bestimmter Rechner nicht erreichbar ist, so schickt er an den Absender des Paketes eine "Destination unreachable" – Meldung (siehe Browser-Meldungen)
- Routenoptimierung
  - wenn ein Gateway erkennt, daß er einen Umweg darstellt, so schickt er an den Absender eine Meldung, in der die schnellere Route steht.
- Überprüfen von erreichbaren Hosts
  - Mit Hilfe des ICMP Echo Message kann ein Rechner überprüfen ob ein Empfänger ansprechbar ist. Das ping-Kommando nutzt diese Echo-Meldung durch Senden eines ICMP echo request an den Zielrechner und erhält bei Verfügbarkeit dessen ein "ICMP echo reply" zurück

Adressierung der Rechner im Internet

- Die IP-Adresse definiert weltweit eindeutig den Rechner.
- IPv4-Adr. sind zur Zeit 4 Byte lang (bei IPv6 sind es 128 bit = 16 Byte)
- Schreibweise als einzelne Bytes in Dezimalschreibweise : 141.56.132.162
- die 32 Bit der Adresse werden immer in eine Netzadresse und einen Bereich für Rechneradressen unterteilt
- Die Netzadressbits werden in der Subnetmask auf 1 gesetzt.
- 3 verschiedene Klassen :
  - Klasse A (CLASS A-Netz) 1 Byte Netzkennung / 3 Byte Hostadresse
    - Nur 126 Netze von 1.0.0.0 bis 126.0.0.0 mit jeweils maximal 16777214 Rechnern
  - Klasse B (CLASS B-Netz) 2 Byte Netzkennung / 2 Byte Hostadresse
    - 16382 Netze von 128.0.0.0 bis 191.255.0.0 mit jeweils maximal 65000 Rechnern
  - Klasse C (CLASS C-Netz) 3 Byte Netzkennung / 1 Byte Hostadresse
    - 2097150 Netze von 192.0.0.0 bis 223.255.255.0 mit jeweils maximal 254 Rechnern
- Der Adressbereich von 224.0.0.0 bis 255.255.255.255 ist für zukünftige Anwendungen reserviert.

Vergabe von IP - Adressen (DHCP-Dynamic Host Configuration Protocol)

Feste Zuordnung zu einem Rechner (am sinnvollsten für Server !)

- Setzt ausreichend großen, verfügbaren Adressbereich voraus, welcher auch im Internet definiert sein muss (Vergabe durch Landesorganisation - DENIC)

Dynamische Zuweisung einer IP-Adresse

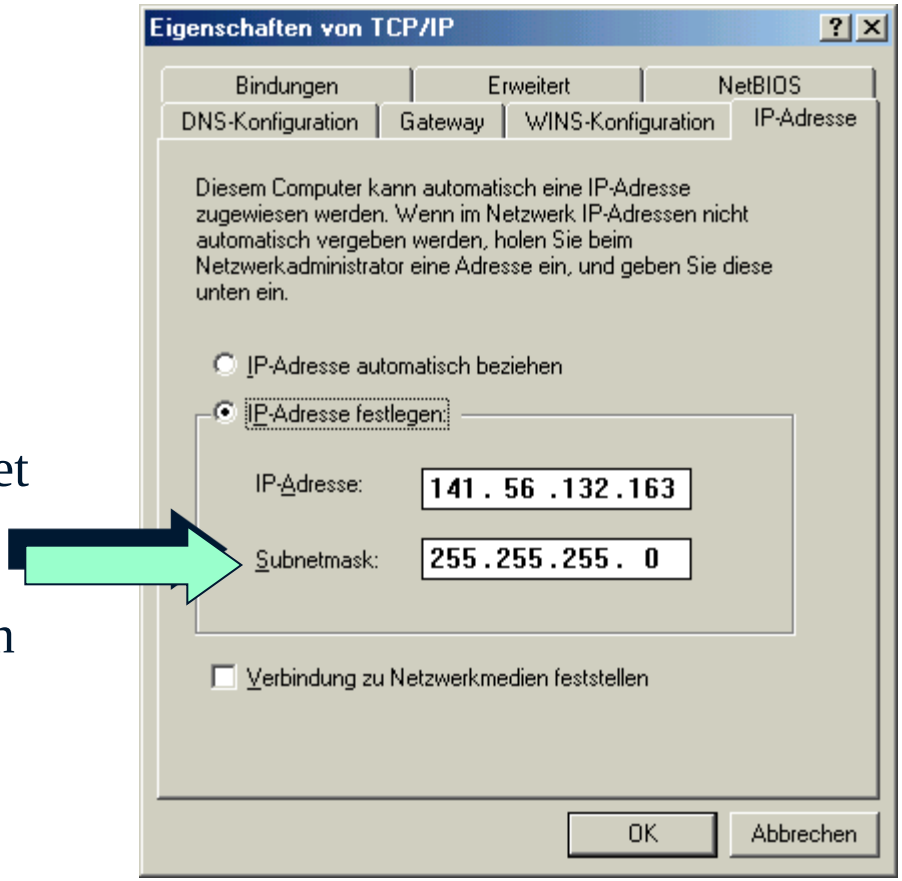
- sinnvoll für nur zeitweise angebundene Client-Rechner (der Provider braucht nur einen Adressbereich für die Online-Kunden bereit halten)
- sehr schlecht für Server, da ständig wechselnde IP-Adresse
- Vergabe durch DHCP-Server über DHCP-Protokoll (RFC-2131)
  - Zuteilung von Netzwerkinformationen in lokalen TCP/IP-Netzen. z.B. IP-Nummer, Domainname, Routing, DNS-Server u.s.w.
  - beim Booten kennt der Rechner nur die MAC-Adresse seiner Netzwerkkarte.
  - Mit der MAC-Adresse startet der Rechner eine Rundfrage (Broadcast) ins Netz, mit der Bitte, ihm doch eine Netzwerkkonfiguration mitzuteilen.
  - Der DHCP-Server wartet auf solche Rundfragen und teilt Ihm die entsprechenden Daten mit. Außerdem merkt sich der Server die MAC-Adresse des Klienten und die zugeteilte IP-Adresse in einer Datei.
  - Nach einer gewissen Zeit muß eine Erneuerung der Adressvergabe erfolgen !

Aufbau von Subnetzen

- abweichend von den 3 Klassen A,B und C kann auch mit sogenannten Classless-Adressen gearbeitet werden
- diese verwenden eine von den Bytegrenzen abweichende Aufteilung der Netz- und Hostadressbereiche

Beispiel: Aufteilung eines Klasse C-Netzes in 2 Subnetze

- das erste Bit des 4. Bytes wird als Netzadresse verwendet
- statt 255.255.255.0 wird in der Subnetmask 255.255.255.128 verwendet
- als Adressbereich für die beiden Subnetze stehen damit die Hostadressen 1-127 (Subnetz 1) und 129-254 (Subnetz 2 zur Verfügung)
- andere Aufteilungen sind analog



Spezielle IP - Adressen

- Zum Aufbau lokaler Netze ohne direkten Internetschluß (bzw. über Proxies) stehen spezielle Adressbereiche zur Verfügung :
  - in Klasse A das Netz 10.0.0.0
  - in Klasse B der Bereich 172.16.0.0 bis 172.31.0.0
  - in Klasse C der Bereich 192.168.0.0 bis 192.168.255.0
- Adresse aus diesen Bereichen werden NICHT WEITER GEROUTET !

Weitere Spezialadressen:

- Alle Hostadressbits = 1 -> sendet an alle Rechner im Netz (Broadcast)
- Alle Hostadressbits=0 -> meint das Netz selbst
- Adresse 0.0.0.0 ist die sogenannte default route (voreingestellte Route) und wird immer verwendet, wenn die Route zum anderen Rechner unbekannt ist
- Adresse 127.0.0.0 adressiert immer das lokale Netz
- Adresse 127.0.0.1 adressiert den Rechner selbst (LOOPBACK – günstig für Tests) – die Daten laufen bis auf die Transportschicht, kommen von der Netzkarte jedoch direkt wieder zurück – funktioniert auch OHNE angeschlossenes Netz !

Vergabe von ALIAS-Namen für IP-Adressen (DNS)

- für IP-Adressen können ALIAS-Namen vergeben werden:
  - Host 141.56.132.162 :

    162 = ishk1 =Rechnername 141.56.132.* = htw-dresden = Domain

    -> ergibt URL (Uniform Resource Locator)

    ishk1.htw-dresden.de
- die ALIAS-Namen müssen von einem speziellen Name-Space-Rechner (auch als DNS - Domain Name System bezeichnet) wieder in die IP-Adresse übersetzt werden, bevor es zum einem Datentransfer kommen kann
- die Namensauflösung ist verteilt realisiert, damit wird von hinten nach vorn aufgelöst (vor langer Zeit gab es mal eine zentrale Datei (wäre heute ca. 25 Mbyte groß und entsprechend langsam)
- im Beispiel :
  1. -> Deutschland
  2. -> HTW Dresden
  3. -> www.htw-dresden.de

Internet-Transportschicht: TCP/IP und UDP

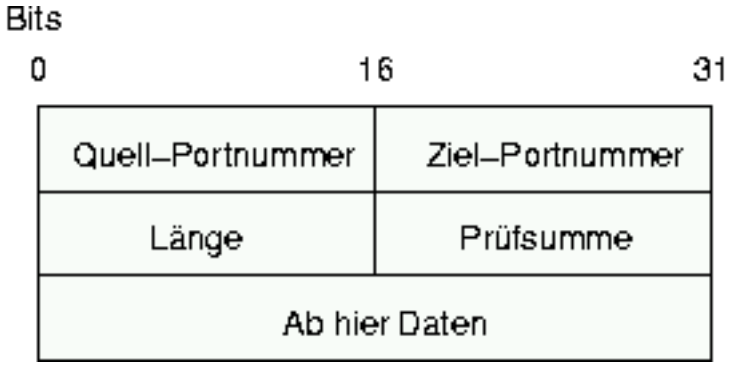
- die Protokolle TCP/IP und UDP setzen beide auf IP auf

Wesentliche Erweiterungen:

- beide Protokolle erlauben die Unterscheidung von **mehreren Empfängern** bzw. Anwendungsprogrammen auf einem Rechner durch sogenannte **Portnummern**
- Portnummern können als Unteradresse zu einer IP-Adresse gesehen werden
- mit den 16 bit – Portadressen können theoretisch $2^{64} = 65535$ Ports definiert werden, praktisch werden aber meist nur 1024 oder 4096 Ports unterstützt
- auf TCP/IP und UDP aufsetzende Protokolle haben teilweise vorgegebene oder Standard-Portnummern, z.B.
  - HTTP - Port 80
  - FTP - Port 20 / 21
- Achtung: da Ports erst durch die Transportschicht erzeugt werden, kennt IP keine Ports, auch sind UDP und TCP/IP-Ports jeweils getrennte Portbereiche !

Das UDP-Protokoll

- Name von User Datagram Protocol (UDP)
- UDP setzt auf IP auf und dient zum Datagrammaustausch
- als Datagramm wird eine kurze (meist <500 Byte) Nachricht verstanden
- Übermittlung von Daten mit einem Minimum an Protokollinformationen
- keine Empfangskontrolle

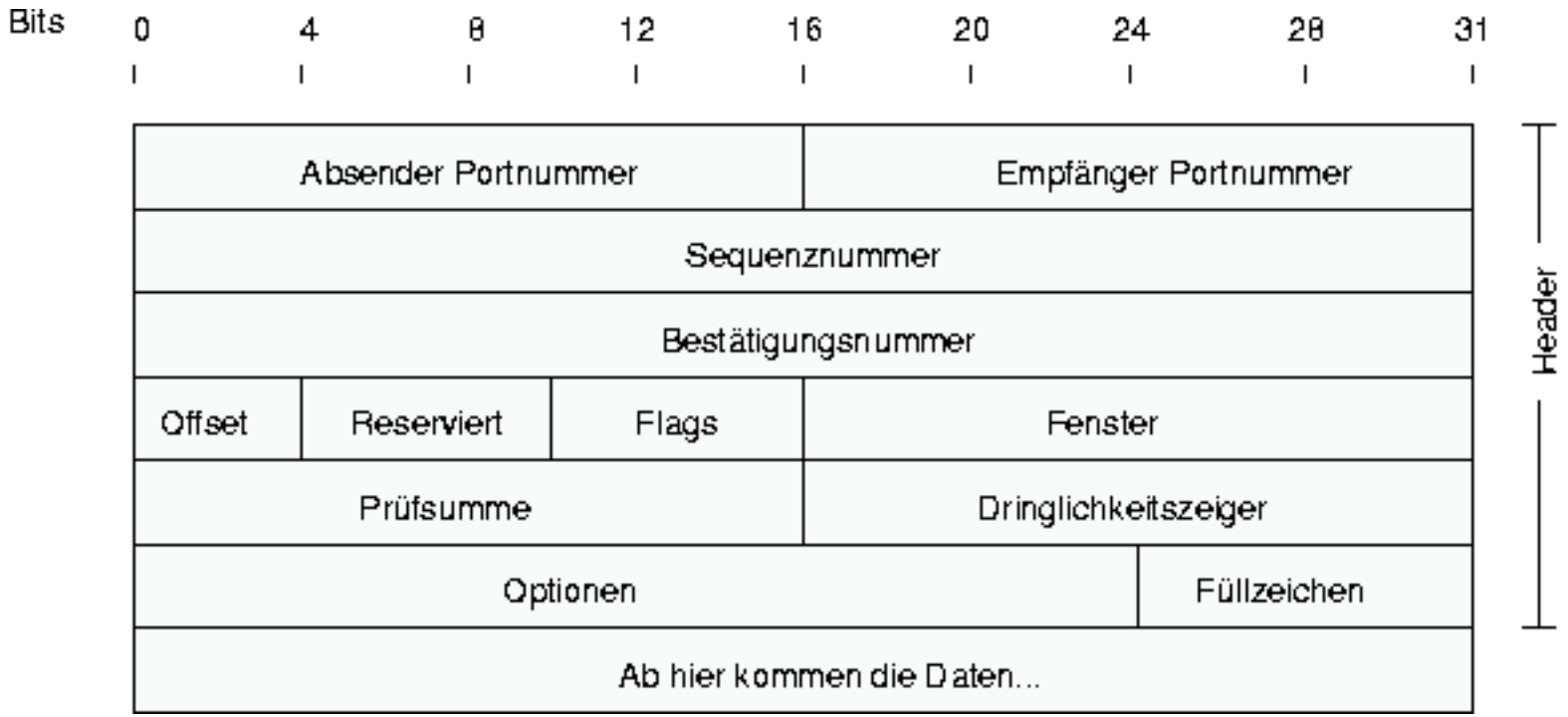


- Einsatz sinnvoll bei Anwendungen mit ständigem, aber stetigen Datenaustausch kleiner Datenmengen, bei denen der Verlust einzelner Pakete unkritisch ist oder der Kontrollaufwand zu groß wäre - Typisches Beispiele:
  - Voice over IP – Sprachdaten über IP mit relativ kleinem Datenaufkommen und Möglichkeiten den Zwischeninterpolation bei ausfallenden Teilstücken (System Paltalk mit sehr guter Sprachqualität !)
  - reine Frage-Antwort Mechanismen (Statusabfragen von Maschine oder Kameras) mit erneuter Fragestellung/Abfrage bei ausbleibender Antwort

Das TCP/IP-Protokoll

- Name von Transmission Control Protocol (TCP)
- TCP setzt auf IP auf und dient zum **verbindungsorientierten Datenaustausch**
- Es wird über IP (an sich verbindungslos, da Paketorientiert) eine virtuelle Verbindung aufgebaut (3-Way-Handshake)
  - Client fragt bei Server an
  - Server signalisiert Einverständnis mit Verbindung
  - Client bestätigt Verbindungsaufbau, danach können Daten gesendet werden ...
  - Abbau der Verbindung in analoger Weise (Achtung: Probleme mit Systemressourcen durch Angriffen mit sehr vielen Verbindungsanfragen)
- TCP überwacht selbst die Zerlegung und Wiederherstellung der Reihenfolge des Datenstromes
  - Paketbestätigungen werden automatisch verschickt (spezielles TCP Paket)
  - Kommt keine Bestätigung, so ist entweder das Datenpaket oder dessen Bestätigung verlorengegangen. Verlorengegangene Pakete werden von der TCP Schicht automatisch wiederholt.
  - Der Empfänger merkt sich die gefolgten Pakete, bis er die fehlenden erhalten hat. Dann kann er den Datenstrom wieder korrekt zusammensetzen.
- **TCP garantiert damit einen korrekten Datenstrom !**

Das TCP/IP-Protokoll-Format



- Portnummern zur eindeutigen Unterscheidung verschiedener, aufsetzender Dienste
- Sequenznummer: Nr. des Paketes im Datenstrom (aufsteigend)
- Bestätigungsnummer : dient zur Bestätigung des Empfangs eines Segments
- Dringlichkeitszeiger : wird bei besonders dringend zu verarbeitenden Paketen gesetzt. Wenn gesetzt enthält dieses Feld als Wert die Endadresse des Datenfeldes, das als dringlich gilt.

Die wichtigsten Portnummern

20	FTP-Data	TCP	Datenkanal einer FTP-Verbindung.
21	FTP	TCP	Kontrollkanal einer FTP-Verbindung.
22	SSH	TCP oder UDP	SecureShell (Verschlüsselter Login)
23	TELNET	TCP	Terminal Emulation over Network
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP oder meist UDP	Nameserver
80	WWW/http	meist TCP oder UDP	Hypertext Transfer Protokoll
110	POP3	TCP oder UDP	Post Office Protocol zum Holen von Mails
119	NNTP	TCP	Net News Transfer Protocol
139	NetBIOS-SSN	TCP oder meist UDP	Windows Netzwerk Sitzungsdienste
143	IMAP2	TCP oder UDP	Interim Mail Access Protocol (verschlüsselt)
161	SNMP	UDP	Simple Network Management Protocol

Sicherheitsproblem:

- durch die testweise Abfrage ALLER Ports eines Rechners kann aufgrund der obigen Tabelle bei positiven Antworten auf angreifbare Applikationen geschlossen werden
- Das einige Server auch das Betriebssystem und dessen Version mit melden, sind sehr spezifische Angriffe möglich (z.B. greife nur HTTP-Server unter Windows an).
- Alternative: Sperrung aller nicht benötigten Ports durch Firewalls (-> VL Sicherheit)

Die Zukunft von IP – IPv6

- Im Verlauf der Entwicklung stellten sich einige Schwachstellen beim aktuellen Internetstandard IPv4 heraus.
- Mit einer neuen Version IPv6 (auch IPng – IP next generation) bezeichnet, sollen die Probleme behoben werden.
- die 6 bei IPv6 hat keine technische Bedeutung ! (es gab eine Zwischenversion IPv5, welche keine Bedeutung erlangte)
- **Seit 2011/2012 sind ALLE IPv4-Adressen vergeben !**

Wesentliche Ziel von IPv6 sind daher

- **neuer und damit größerer Adressraum**
- **einfacherer, schneller auswertbarer Aufbau der Pakete zur Verbesserung der Performance**
- **bessere Routen im Internet durch Zusammenfassen von Adressen in sinnvolle Gruppen**

Der vergrößerte Adressraum bei IPv6

- mit IPv4 sind theoretisch etwa 4 Mrd. Rechner verwaltbar
- am Anfang (vor 1990) jedoch relativ großzügige Vergabe von Class A und B-Netzen, Folge: schlechte Ausnutzung der Class B Bereiche mit nur einigen 1000 statt 65.000 Rechnern - **IPv4 Adressraum ist erschöpft !**
  (dabei sind infolge der Geschhte 74% der IPv4-Adressen in den USA …)

IPv6 : Erweiterung der Adressen auf 16 Byte = 128 bit

- entspricht 340.282.366.920.938.463.463.374.607.431.768.211.456. Rechnern
- oder pro Quadratmillimeter der Erde jeweils 667 Billionen Adressen
- selbst bei großzügiger Vergabe wie bisher noch einige Tausend Adressen/ m²
- Neue Schreibweise der Adressen:
- Statt Dezimal nun **Hexadezimal** mit jeweils 2 Byte als Gruppe
  - 213:0:217:118 bisherige IPv4-Adresse
  - 4711:0:0:0:8:A:EEC:6008 neue IPv6-Adresse
  - 4711::::8:A:EEC:6008 ein Bereich Nullen kann entfallen

Schnellere Verarbeitung der IP6-Pakete

- Die sehr variable Struktur der IP-Header erschwert eine schnelle (und hardwarebasierte) Auswertung beim Routing

IPv6 definiert daher :

- einen verkürzten, einheitlichen, fest definierten Basisheader von 40 Byte
- mit einer Reihe von optionalen Zusatzheadern

Weiterhin bessere Unterstützung von

- Engpasserkennung und Flusskontrolle
- Verschlüsselung, Authentisierung , Prüfung der Datenintegrität
- Erkennung von Datentypen (Video / Voice ...) mit dem Ziel besserer Übertragungscharakteristiken

Verbessertes Routing bei IPv6

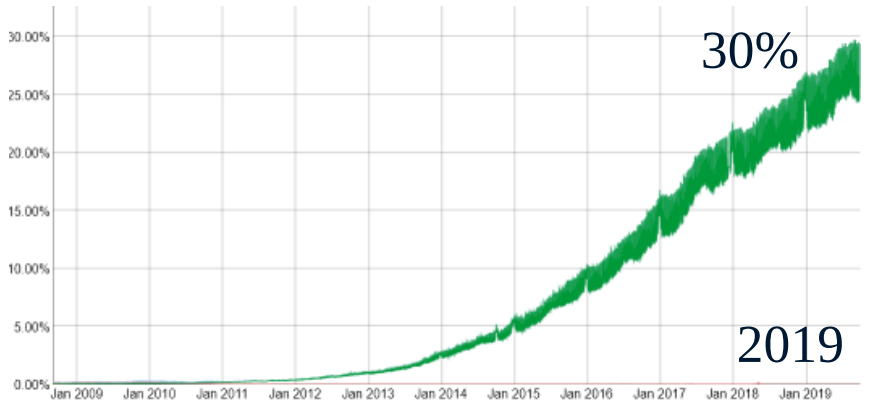
- einen sehr grossen Aufwand bereitet gegenwärtig das effiziente Routing

IPv6 stellt zusätzliche Mechanismen bereit :

- zum einfacheren Erkennen von regionalen Einheiten (Ländern) und geografischen Regionen
- zum Erkennen benachbarter Rechner
- zur Verteilung auf Rechnerfarmen mit gleichartigen Servern
- zur Multicast-Verteilung an Gruppen von Rechnern (ähnlich Broadcasting) z.B. für Videoverteilung
- zur Zuteilung mehrerer IP-Adressen zu einem Gerät
- zu besseren Unterstützung mobiler Geräte (mit einer Art Nachsendeadresse) -> „Mobile IPv6“ (RFC 6275)

Aktueller Status der IPv6-Einführung

- obwohl der Standard IPv6 technisch seit 1999 im Regelbetrieb ist, dauert die Einführung immer noch an …
- verschiedene Netzprovider messen nur ca. 10 bis 40% IPv6-Traffic (-> 30% bei https://www.google.de/ipv6/statistics.html)



<u>Hauptursachen für die langsame Einführung:</u>

- IPv6 kann über IP4 getunnelt werden
- viele Dualstack-Implementierungen machen den Umstieg nicht zwingend, bis auf die Adressmenge wurden viele IPv6-Technolgien auch nach IP4 „herunterportiert“
- es gibt auch keine Anwendung, welche zwingend IPv6 erfordert
- weiteres Kontra: feste IPv6-Adressen erleichtern Tracking der Nutzer …

=> Empfehlung: IPv6-Entwicklung beobachten und bei vorhandenen Ressourcen IPv6-Einführung vorbereiten (und durchführen)

Zusammenfassung Netzwerktechnik

- bezogen auf das Fach „Entwicklung webbasierter Anwendungen“ gehen wir von **funktionierenden Netzwerken** aus !
- Nützlich ist aber eine schnelle Erkennung/Unterscheidung von Netzwerkproblemen und Softwareproblemen, da auf der Clientseite ggf. gleiche Fehlermeldungen kommen (im Browser „Seite nicht erreichbar“)
- Für Sie als WiInf: Bei echten Netzwerkproblemen ist i.d.R. der Netzwerk-Admin der Organisation zur kontaktieren !

Test der Fehlersuche im Praktikum (siehe Übung 1 ab Woche 2):

- sind die IP-Adressen der Server und Dienste per Ping erreichbar ? (HTTP / SMTP / DNS / …)
- Können Firewalls die Kommunikation stören (auch ICMP für Ping wird heute oft geblockt ..) ?
- Laufen die Server als Software (-> Check Admin-Panels / Logs … ??)