Digitale Kommunikation und Internetdienste 1

Wintersemester 2004/2005 – Teil 6

Belegnummer Vorlesung: 39 30 02

Übungen: 39 30 05

Jan E. Hennig

AG Rechnernetze und Verteilte Systeme (RVS)
Technische Fakultät
Universität Bielefeld

jhennig@rvs.uni-bielefeld.de

basierend auf den Arbeiten von Michael Blume, Heiko Holtkamp, Marcel Holtmann und I Made Wiryana

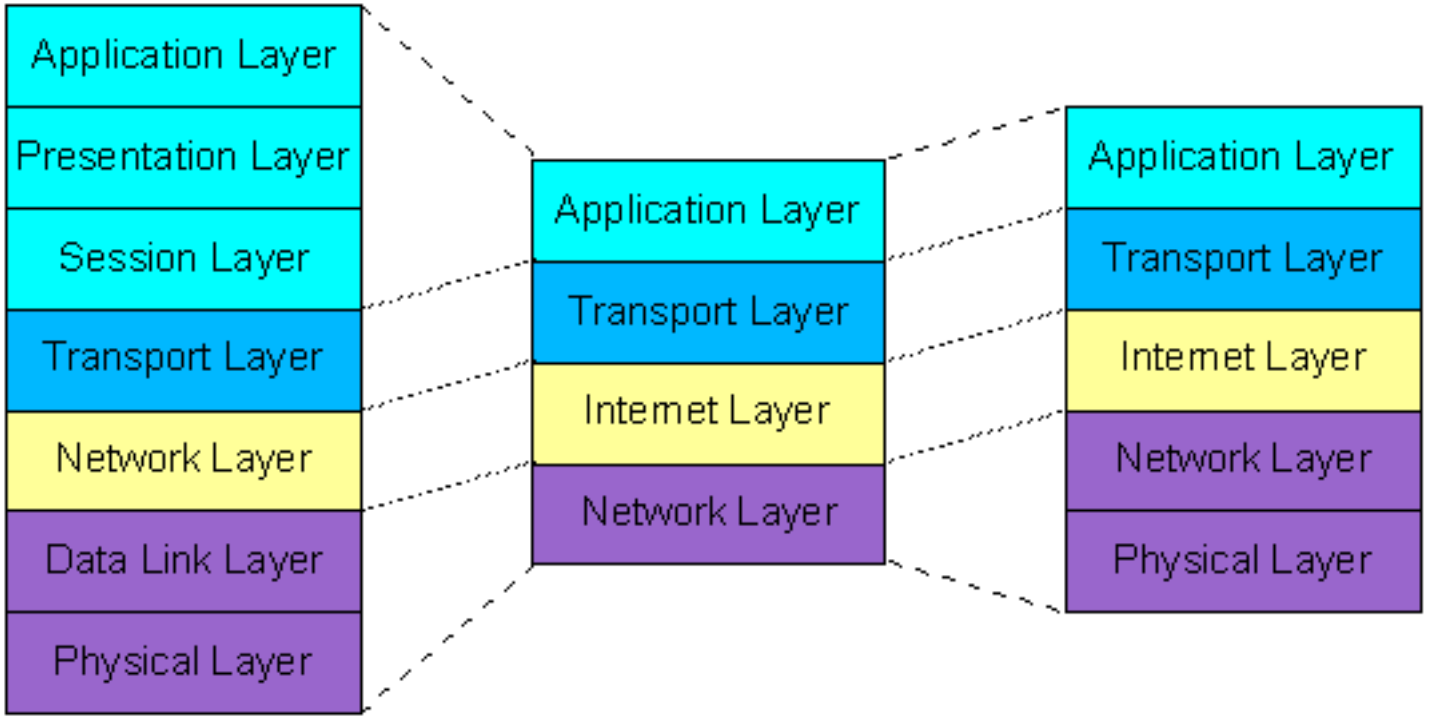
Übersicht

- Internet Layer
- Internet Protocol

Erinnerung

- verschiedene Protokolle und Techniken auf der Netzwerkebene
- z.B. Ethernet, Token Ring, Wireless
- unterschiedliche Paketformate
- unterschiedliche physische Adressen (IEEE 802.x bedingt kompatibel)
- → Protokolle sind zueinander im Allgemeinen inkompatibel

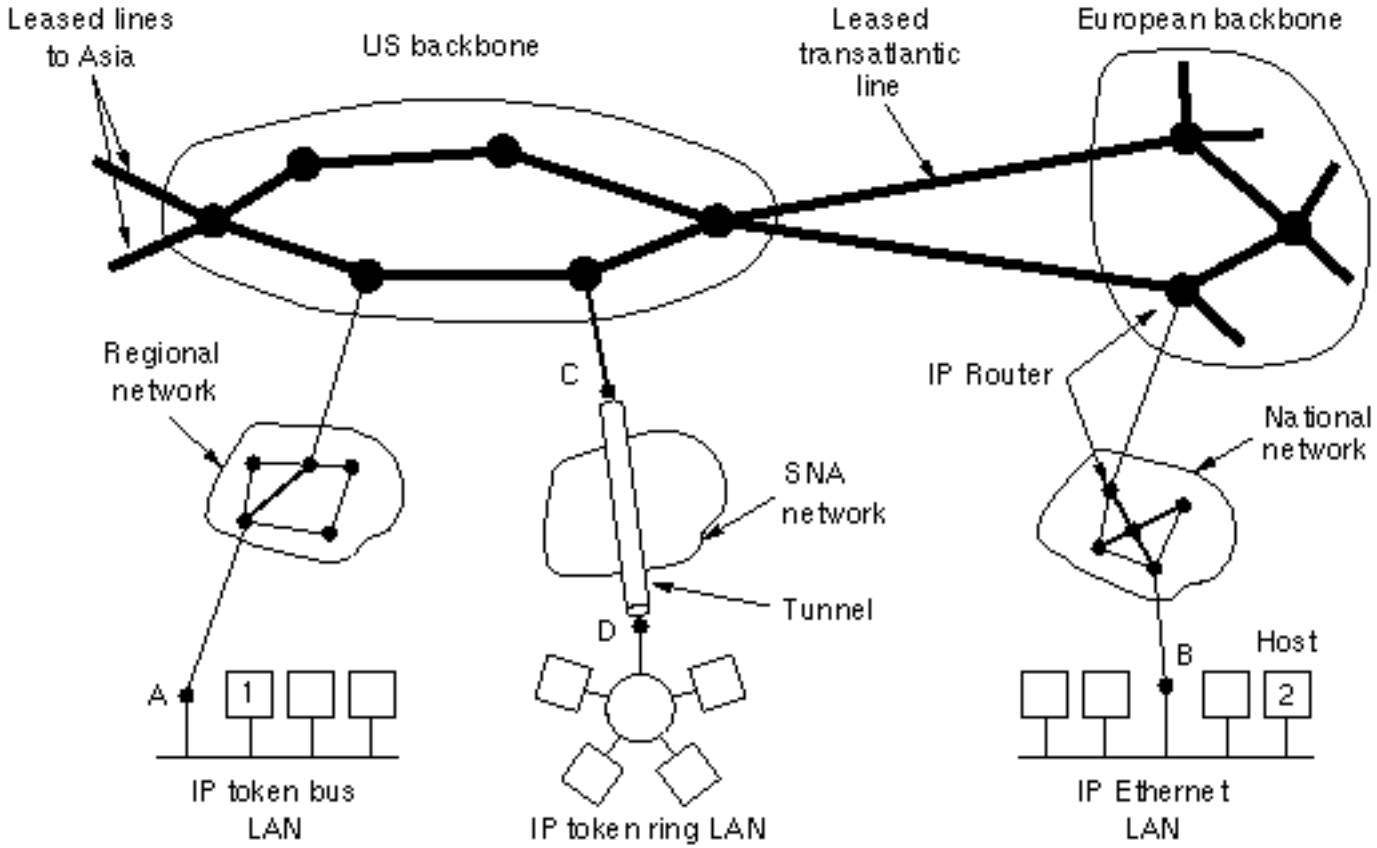
Internet Layer



Internet-Ebene: Vermittlung zwischen verschiedenen Protokollen der Netzwerk-Ebene

Internet, Internetworking

- das Internet ist eine Sammlung von Teilnetzen, die miteinander verbunden sind
- es gibt keine echte Struktur des Netzes
- mehrere größere *Backbones* bilden ein *Rückgrat* des Internets
- diese werden aus Leitungen mit sehr hoher Bandbreite und schnellen Routern gebildet
- daran wiederum größere regionale Netze angeschlossen
- daran dann LANs von Universitäten, Behörden, Unternehmen und Service-Providern


Leased lines to Asia
US backbone
Leased transatlantic line
European backbone
Regional network
C
IP Router
National network
SNA network
Tunnel
D
Host
B
A
1
2
IP token bus LAN
IP token ring LAN
IP Ethernet LAN

Das Internet Protocol

- „das *Internet Protokoll (Internet Protocol - IP)* ist der Leim, der dies alles zusammenhält”
- ist im RFC 791 spezifiziert
- Hauptaufgaben: Adressierung von Hosts und das Fragmentieren von Paketen
- Pakete werden nach bestem Bemühen („*best effort*”) von der Quelle zum Ziel befördert
- unabhängig davon, ob sich die Hosts im gleichen Netz befinden oder andere Netze dazwischen liegen
- jedoch keine Zustellungsgarantie und keine Flußkontrolle

IP-Funktionen

Aufgaben bzw. Funktionen:

- Die Definition von *Datengrammen (datagram)*: Basiseinheiten für die Übermittlung von Daten im Internet
- Definition des Adressierungsschemas
- Übermittlung der Daten von der Transportebene zur Netzwerkschicht
- Routing von Datengrammen durch das Netz
- Fragmentierung und Zusammensetzen von Datengrammen

IP-Eigenschaften

- verbindungsloses Protokoll
- d.h. keine Ende-zu-Ende-Verbindung der Kommunikationspartner wird etabliert
- unzuverlässiges Protokoll
- d.h. keine Mechanismen zur Fehlererkennung und -behebung
- aber: sind die Daten beim Zielhost angelangt, sind diese Daten auch korrekt

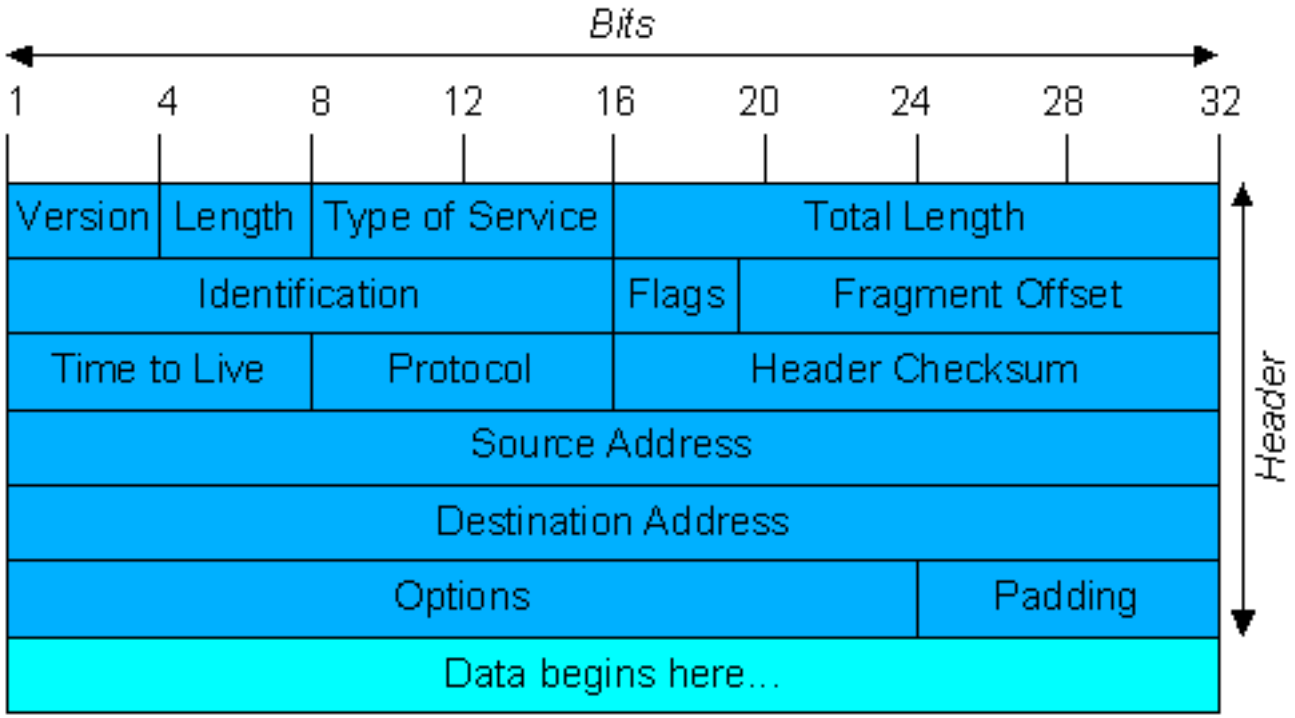
IP-Datengramm (1)

- Gemeinsamkeit: Netzwerke mit Paketvermittlung
- *Paket*: Datenblock zusammen mit den Informationen, die notwendig sind, um sie dem Empfänger zuzustellen
- Analogie Post-Paket: das Paket enthält die Daten, auf dem Paket ist die Adresse des Empfängers notiert
- *Datengramm (datagram)* ist das Paketformat, das vom Internet Protocol definiert wird
- besteht aus einem Header und den zu übertragenden Daten

IP-Datengramm (2)

- Header hat einen festen 20 Byte großen Teil
- gefolgt von einem optionalen Teil variabler Länge
- er umfaßt alle Informationen, die notwendig sind, um das Datengramm dem Empfänger zuzustellen
- kann bis zu 64KByte groß sein
- in Praxis üblich: bis 1500 Byte (wg. max. Ethernet-Rahmengröße)

IP-Datengramm (3)



IP-Header (1)

Version

- Versionsnummer des IP-Protokolls
- eröffnet Möglichkeit, über eine längere Zeit mit verschiedenen Versionen des IP Protokolls zu arbeiten
- einige Hosts können mit der alten und andere mit der neuen Version arbeiten
- derzeitige weit verbreitete Versionsnummer ist 4 (IPv4)
- Version 5 übersprungen (war rein experimentelles Protokoll)
- Version 6 (IPv6) wird zunehmend eingesetzt

IP-Header (2)

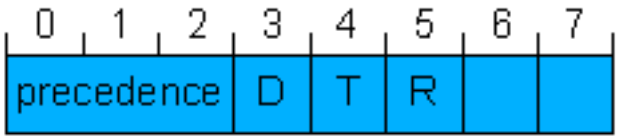
Länge (length) – Internet Header Length (IHL)

- Länge des Protokollkopfs (Header)
- denn diese ist nicht konstant
- wird in 32-Bit-Worten angegeben (also hier 1 Wort = 4 Byte)
- kleinster zulässiger Wert ist 5 (entspr. 20 Byte, keine Optionen gesetzt)
- Maximalwert ist 15 (entspr. 60 Byte)

IP-Header (3)

Type of Service

- Vorschläge, wie Datengramm zu behandeln ist
- *Precedence* gibt die Priorität von 0 (normal) bis 7 (Steuerungspaket) an
- dabei besonders achten auf: *Verzögerung (Delay - D)*, *Durchsatz (Throughput - T)*, *Zuverlässigkeit (Reliability - R)*
- wird in der Praxis oft ignoriert, hat dann den Wert 0



IP-Header (4)

Gesamtlänge (total length)

- enthält die gesamte Paketlänge (Header und Daten)
- Maximallänge eines Datengramms: 65535 Byte
- jeder Host muß in der Lage sein Pakete bis zu einer Länge von 576 Bytes zu verarbeiten (RFC 791)
- i.d.R. aber größere Pakete möglich

IP-Header (5)

Identification

- eindeutige Nummer
- vom Absender vergeben
- bezeichnet Datengramm
- alle Fragmente eines Datengramms enthalten gleiche Identifikationsnummer
- Zielhost kann so Fragmente wieder zuordnen

IP-Header (6)

Flags

- drei Bit, erstes Bit ungenutzt
- *Don't fragment (DF)* signalisiert, daß ein Datengramm nicht fragmentiert werden darf
- muß dann evtl. verworfen werden
- *More Fragments (MF)* signalisiert, daß weitere Fragmente folgen
- ist bei allen Fragmenten außer dem letzten gesetzt

IP-Header (7)

Fragmentabstand (fragment offset)

- bezeichnet, an welche Stelle ein Fragment gehört.
- relativ zum Beginn des gesamten Datengramms
- Zielhost kann hiermit Fragmente wieder zusammensetzen
- maximal 8192 Fragmente pro Datengramm
- elementare Fragmenteinheit: 8
- alle Fragmente, außer dem letzten, müssen ein Vielfaches von 8 Byte sein

IP-Header (8)

Time to Live (TTL)

- Zähler, mit dem die Lebensdauer von IP-Paketen begrenzt wird
- Einheit: Sekunden (RFC 791)
- maximale Lebensdauer von 255 Sekunden (8 Bit)
- außerdem: Zähler muß von jedem Netzknoten, der durchlaufen wird um mindestens 1 verringert werden
- bei längerer Zwischenspeicherung mehrfach
- Wert 0: Paket muß verworfen werden
- verhindert, daß ein Paket endlos in einem Netz umherwandert
- dann: ICMP-Nachricht über „Ableben” an Sender

IP-Header (9)

Protokoll (protocol)

- Protokollnummer des Transportprotokolls
- an dieses muß die Nachricht weitergegeben werden
- Nummerierung ist im gesamten Internet einheitlich
- früher: Protokollnummern im RFC 1700 definiert
- heute: Internet Assigned Numbers Authority (IANA)
  `http://www.iana.org`

IP-Header (10)

Header Checksum

- Prüfsumme der Felder im IP-Header
- umfaßt nicht Nutzdaten (werden von Transportprotokoll geprüft)
- muß an jedem Zwischenknoten neu berechnet werden (da TTL verändert)
- *1er-Komplement der Summe aller 16-Bit-Halbwörter der zu überprüfenden Daten*

IP-Header (11)

- Quelladresse (32 Bit)
- Zieladresse (32 Bit)
- Optionen (variabel)
  - Options-Code (1 Byte) identifiziert die Option
  - evtl. weiterer Sub-Code
  - evtl. weitere Datenbytes
- Padding (auffüllen auf ein Vielfaches von 4 Byte)

IP-Header-Optionen (1)

- End of Option List
- No Option (zum Auffüllen zwischen Optionen)
- Security: Bezeichnet wie „geheim” ein Paket ist, in der Praxis meist ignoriert
- Record Route: Jeder Zwischenknoten hängt seine IP-Adresse an die Option an
- Time Stamp: wie Record Route, zusätzlich Uhrzeit des Knotendurchlaufs

IP-Header-Optionen (2)

Loose Source-Routing, Strict Source-Routing

- Liste von IP-Adressen, die das Paket durchlaufen soll
- schreibt also explizit vor, welche *Route* genommen werden soll
- impliziert Record Route
- strict: die vorgegebene Route muß exakt eingehalten werden
- loose: die vorgegebenen Knoten müssen besucht werden, dazwischen dürfen aber auch andere Knoten liegen

Adressen

- vier verschiedene Adressen bei TCP/IP:
- 1. eine Netzwerkadresse bzw. MAC-Adresse (z.B. eine Ethernet-Adresse)
- 2. eine Internet-Adresse (IP-Adresse)
- 3. eine Transportprotokoll-Adresse (Identifikation des Transportprotokolls)
- 4. eine Portnummer (logische Anschlußkennung)
- IP-Adresse und Protokolladresse auf Internet-Ebene im IP-Header vertreten

Protokollnummer

- bezeichnet Protokoll oberhalb von IP
- Nummerierung einheitlich
- ausreichende Information für IP an welches höhere Protokoll es Daten beim Zielhost weiterreichen soll
- unter Unix z.B. in Datei `/etc/protocols` gespeichert
- z.B. Empfang eines Pakets mit Protokollnummer 6 → weiterreichen an TCP (Transmission Control Protocol)
- z.B. Empfang eines Pakets mit Protokollnummer 17 → weiterreichen an UDP (User Datagram Protocol)

Ausschnitt aus /etc/protocols


```
ip          0     IP              # internet protocol, pseudo protocol number
icmp        1     ICMP            # internet control message protocol
igmp        2     IGMP            # Internet Group Management
ggp         3     GGP             # gateway-gateway protocol
ipencap     4     IP-ENCAP        # IP encapsulated in IP (officially ‘‘IP’’)
st          5     ST              # ST datagram mode
tcp         6     TCP             # transmission control protocol
egp         8     EGP             # exterior gateway protocol
pup         12    PUP             # PARC universal packet protocol
udp         17    UDP             # user datagram protocol
hmp         20    HMP             # host monitoring protocol
xns-idp     22    XNS-IDP         # Xerox NS IDP
rdp         27    RDP             # "reliable datagram" protocol
iso-tp4     29    ISO-TP4         # ISO Transport Protocol class 4
xtp         36    XTP             # Xpress Tranfer Protocol
ddp         37    DDP             # Datagram Delivery Protocol
idpr-cmtp   38    IDPR-CMTP       # IDPR Control Message Transport
ipv6        41    IPv6            # IPv6
ipv6-route  43    IPv6-Route      # Routing Header for IPv6
ipv6-frag   44    IPv6-Frag       # Fragment Header for IPv6
idrp        45    IDRP            # Inter-Domain Routing Protocol
gre         47    GRE             # General Routing Encapsulation
esp         50    ESP             # Encap Security Payload for IPv6
ah          51    AH              # Authentication Header for IPv6
ipv6-icmp   58    IPv6-ICMP       # ICMP for IPv6
ipv6-nonxt  59    IPv6-NoNxt      # No Next Header for IPv6
ipv6-opts   60    IPv6-Opts       # Destination Options for IPv6
rspf        73    RSPF            # Radio Shortest Path First.
ospf        89    OSPFIGP         # Open Shortest Path First IGP
ipip        94    IPIP            # IP-within-IP Encapsulation Protocol
pim         103   PIM             # Protocol Independent Multicast
```

IP-Adressen (1)

- 32 Bit lang, jeder Host im Internet hat mindestens eine
- Knoten, die an mehrere Netze angeschlossen sind, haben in jedem Netz eine eigene IP-Adresse
- IP-Adresse ist eindeutig: kein Knoten im Internet hat die gleiche IP-Adresse wie ein anderer
- früher: vom Network Information Center (NIC) vergeben
  `http://www.internic.net`
- heute: Internet Assigned Numbers Authority (IANA) `http://www.iana.org` bzw. ihre Vertreter in den verschiedenen Gebieten – z.B. Asia Pacific Network Information Center (APNIC), American Registry for Internet Numbers (ARIN), Réseaux IP Européens (RIPE)

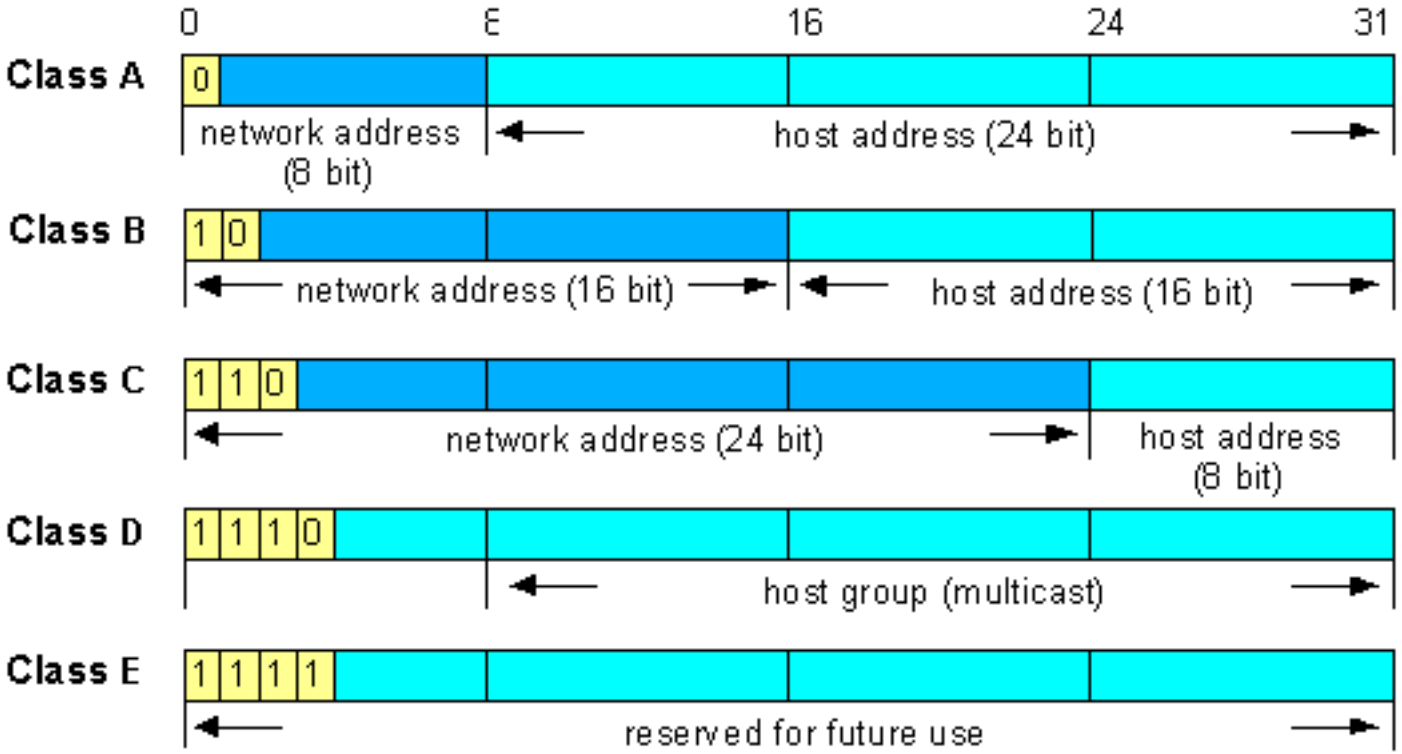
IP-Adressen (2)

- keine Einzelzuordnung (wäre zu hoher Verwaltungsaufwand)
- sondern nach Netzklassen vergeben
- Beantragt man IP-Adressen für ein Netz,
- so erhält man nicht für jeden Rechner eine Adresse zugeteilt,
- sondern einen Bereich von Adressen, der selbst zu verwalten ist

Aufbau

- Aufteilung der 32 Bits in Netzwerk- und Hostteil
- *Netzwerkadresse* definiert das Netzwerk, in dem sich ein Host befindet
- alle Hosts eines Netzes haben die gleiche Netzwerkadresse
- *Hostadresse* identifiziert einen bestimmten Rechner innerhalb eines Netzes

IP-Adreßklassen



Aufbau einer IP-Adresse

- „Eine IP-Adresse identifiziert keinen bestimmten Computer [Host],
- sondern eine Verbindung zwischen einem Computer [Host] und einem Netz.”[1]
- Schreibweise: nicht alle Bits einzeln (01111111111111111111111111111111)
- sondern à 4 Bytes: 127.255.255.255
- kleineste Adresse: 0.0.0.0, größte: 255.255.255.255

[1] Comer D.E.: Computernetzwerke und Internets. Prentice Hall, München, 1998

Adreßklassen (1)

Einteilung nach Adreßklassen:

Adreß-klasse	Erstes Byte	Bytes für Netzadresse	Bytes für Hostadresse	Adreß-format	Anzahl Hosts
Klasse A	1-126	1	3	N.H.H.H	2^{24} (ca. 16 Mio.)
Klasse B	128-191	2	2	N.N.H.H	2^{16} (ca. 65000)
Klasse C	192-223	3	1	N.N.N.H	254

(N steht für einen Teil der Netzadresse, H für einen Teil der Hostadresse)

Adreßklassen (2)

Klasse A:

- das erste Byte hat einen Wert kleiner als 128
- d.h. das erste Bit der Adresse ist 0
- das erste Byte ist die Netzwerkadresse
- die letzten drei Bytes identifizieren einen Host im Netz
- es gibt also 126 Klasse A Netze
- die bis zu 16 Millionen Host in einem Netz

Adreßklassen (3)

Klasse B:

- erstes Byte: Wert von 128 bis 191
- d.h. das erste Bit ist gleich 1, Bit 2 gleich 0
- die ersten beiden Bytes identifizieren das Netzwerk
- die letzen beiden Bytes identifizieren einen Host
- es gibt also 16382 Klasse B Netze
- mit bis zu 65534 Hosts in einem Netz

Adreßklassen (4)

Klasse C:

- erstes Byte: Werte von 192 bis 223
- d.h. die ersten beiden Bits sind gleich 1, Bit 3 gleich 0
- die ersten drei Bytes identifizieren das Netzwerk
- das letzte Byte identifiziert einen Host
- es gibt 2^{24} Millionen Klasse C Netze
- mit je bis zu 254 Hosts

Adreßklassen (5)

Klasse D:

- *Multicast-Adressen*: Datengramm richtet sich an mehrere Hosts gleichzeitig
- erstes Byte im Wertebereich von 224 bis 239
- d.h. die ersten drei Bit sind gesetzt und Bit 4 ist gleich 0
- Übermittlung erfolgt wie üblich nach bestem Bemühen (ohne Garantie)
- es wird spezielles Protokoll namens *Internet Group Management Protocol (IGMP)* verwendet

Adreßklassen (6)

Klasse E:

- IP-Adressen von 240 bis 254 im ersten Byte
- „reservierter” Bereich
- für künftige Nutzung
- Bezeichnung „Klasse E” nicht einheitlich

Private Adreßbereiche (1)

- im Internet müssen die Netzkennungen eindeutig sein
- daher zentrale Vergabe
- jedoch für Netze ohne Kontakt zum Internet unnötig
- daher: Adreßbereiche festgelegt, die nur für private Netze bestimmt sind
- sind in RFC 1918[2] festgelegt (*Address Allocation for Private Internets*)

[2] RFC 1597, auf das sich oft auch neuere Literatur bezieht, ist durch RFC 1918 ersetzt

Private Adreßbereiche (2)

- private IP-Nummern dürfen im Internet nicht weitergeleitet werden
- somit ist es möglich, diese Adressen in beliebig vielen, nicht-öffentlichen Netzen einzusetzen
- Selbstverwaltung:
- jeder kann aus diesen Bereichen den Adreßbereich für sein eigenes privates Netz auswählen
- dies bedarf nicht die Koordination mit der IANA

Private Adreßbereiche (3)

- Klasse A: 10.0.0.0
  - für ein privates Klasse A-Netz ist der Adressbereich von 10.0.0.0 bis 10.255.255.254 reserviert
- Klasse B: 172.16.0.0 bis 172.31.0.0
  - für die private Nutzung sind 16 Klasse B-Netze reserviert
  - jedes dieser Netze kann aus bis zu 65534 Hosts bestehen
  - z.B. ein Netz mit den Adressen von 172.17.0.1 bis 172.17.255.254
- Klasse C: 192.168.0.0 bis 192.168.255.0
  - 256 Klasse C-Netzte stehen zur privaten Nutzung zur Verfügung
  - jedes dieser Netze kann jeweils 254 Hosts enthalten
  - z.B. ein Netz mit den Adressen 192.168.0.1 bis 192.168.0.254

Weitere Adressen (1)

- Adressen mit der Netznummer 0 beziehen sich auf das aktuelle Netz
- Hosts können sich auf ihr eigenes Netz beziehen, ohne die Netzadresse zu kennen (allerdings muß Netzklasse bekannt sein)
- 127 steht für das *Loopback Device* eines Hosts
- Pakete, die an eine Adresse der Form 127.x.y.z gesendet werden, werden lokal verarbeitet
- sie werden nicht auf einer Leitung ausgegeben

Weitere Adressen (2)

- Hostadressen 0 und 255 sind reserviert
- IP-Adresse, bei der alle Hostbits auf Null gesetzt sind, identifiziert das Netz selbst
- z.B. 80.0.0.0 bezieht sich so z.B. auf das Klasse A Netz 80
- z.B. 128.66.0.0 bezieht sich auf das Klasse B Netz 128.66
- IP-Adresse, bei der alle Host-Bytes den Wert 255 haben, ist eine *Broadcast-Adresse*
- damit werden alle Hosts in einem Netzwerk adressiert

CIDR (1)

- Problem: IPv4-Adressen sind inzwischen knapp
- durch die Vergabe von Internet-Adressen in Klassen wird eine große Anzahl von Adressen verschwendet
- besonders knapp: Klasse B
- viele Firmen haben mehr als 254 Hosts (Klasse C nicht ausreichend)
- wenig Bedarf an Klasse A – nimmt aber Großteil des Adreßraums ein
- früher sogar sehr großzügiger Umgang mit Adressen (z.B. mehrere Klasse A-Netze in USA zugeteilt)

CIDR (2)

- Klasse B aber dennoch oft viel zu groß → Verschwendung
- andere Firmen haben Angst ein Klasse C-Netz später nicht erweitern zu können
- Milderung wäre durch Klasse mit 10 Bit (1022 Hosts) möglich gewesen
- weiteres Problem: je mehr Netze desto mehr Einträge in Routing-Tabellen nötig
- Konzept: *Classless InterDomain Routing (CIDR)* (RFC 1519)

CIDR (3)

- verbleibende Netze der Klasse C werden in Blöcken variabler Größe zugewiesen
- z.B. 2000 Adressen benötigt: einfach 8 aufeinanderfolgende Netze der Klasse C vergeben
- zusätzlich: verbliebene Klasse C-Adressen werden restriktiver und strukturierter vergeben
- dazu ist Welt in Zonen eingeteilt worden

CIDR-Zonen

- 194.0.0.0 - 195.255.255.255: Europa
- 198.0.0.0 - 199.255.255.255: Nordamerika
- 200.0.0.0 - 201.255.255.255: Mittel- und Südamerika
- 202.0.0.0 - 203.255.255.255: Asien und pazifischer Raum
- 204.0.0.0 - 223.255.255.255: Reserviert für zukünftige Nutzung

CIDR-Vorteile

- jede Zone enthält ca. 32 Millionen Adressen
- wenige Einträge in Routing-Tabellen nötig:
- lokale Einträge für die jeweilige Zone
- sonst Einträge zum Weiterleiten in andere Zone

Aussicht

Themenübersicht für die kommende Vorlesung:

- IPv4 (Fortsetzung)
- ICMP
- IGMP
- IPv6

Ende Teil 6. Danke für die Aufmerksamkeit.