IP Version 4

by

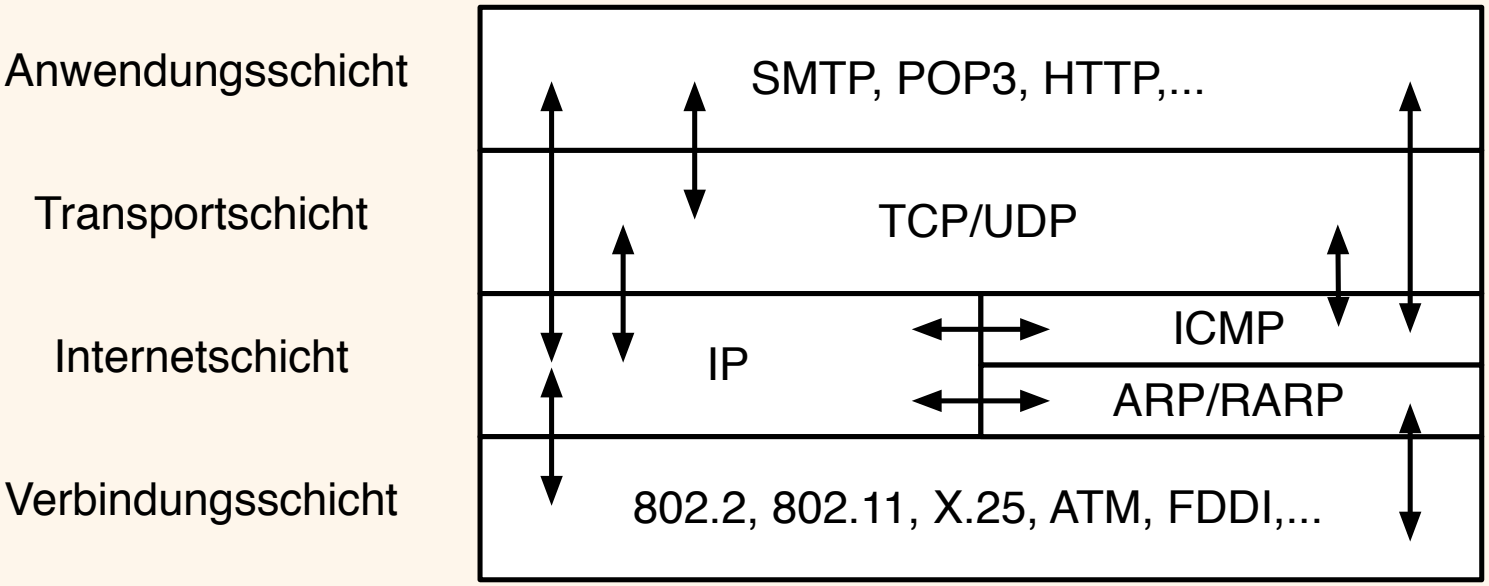
Dr. Günter Kolousek

ISO/OSI Stack – Wiederholung

Anwendungsschicht (application layer)
Darstellungsschicht (presentation layer)
Sitzungsschicht (session layer)
Transportschicht (transport layer)
Vermittlungsschicht (network layer)
Sicherungsschicht (datalink layer)
Bitübertragungsschicht (physical layer)

TCP/IP Stack

kein striktes Schichtenmodell!



Internet Protocol Version 4

- Teil des TCP/IP Stacks
- verbindungslos, Schicht 3 des ISO/OSI
- Hauptfunktionen
  - Adressierung
  - Weiterleitung
  - Abstraktion der unterliegenden physikalischen Schichten
- nicht zuverlässig
  - arbeitet nach dem best-effort Prinzip
  - Pakete können
    - verloren gehen
    - nicht in der richtigen Reihenfolge ankommen
    - mehrfach ankommen

$\rightarrow$ IP geht davon aus, dass sich höhere Schichten um diese Punkte kümmern!

IP Adressen

- 32 Bits
  - 4 Bytes
    - meist Dezimaldarstellung durch Punkt getrennt
- Arten
  - Unicast, Multicast, Broadcast
- Adressierungsvarianten
  - Standardadressen, Subnetzadressen, CIDR
- Adresse besteht aus
  - Netzanteil, Hostanteil

Standardadressen

- Klasse A
  - hohe Anzahl an Hosts
- Klasse B
  - mittlere Anzahl an Hosts
- Klasse C
  - kleine Anzahl an Hosts
- Klasse D
  - Multicast-Anwendungen
- Klasse E
  - zukünftige Anwendungen

Klasse A

- Netzanteil erstes Byte
- erstes Bit immer 0
- 0.0.0.0 – 127.255.255.255
  - 0.0.0.0 und 127.0.0.0 reserviert
  - 126 Klasse A Netze
  - 16777214 (2^{24} - 2) Hosts je Netz
- effektiver Bereich: 1.0.0.1 – 126.255.255.254

Klasse B

- Netzanteil ersten beiden Bytes
- ersten beiden Bits immer 10
- 128.0.0.0 – 191.255.255.255
  - 16384 (2^{14}) Klasse B Netze
  - 65534 (2^{16} - 2) Hosts je Netz
- effektiver Bereich: 128.0.0.1 – 191.255.255.254

Klasse C

- Netzanteil ersten drei Bytes
- ersten drei Bits immer 110
- 192.0.0.0 – 223.255.255.255
  - 2097152 (2^{21}) Klasse C Netze
  - 254 (2^8 - 2) Hosts je Netz
- effektiver Bereich: 128.0.0.1 – 191.255.255.254

Klassen D & E

- Klasse D
  - ersten vier Bits immer 1110
  - restlichen 28 Bits geben die Multicast-Gruppen-Id an
  - 224.0.0.0 – 239.255.255.255
    - etliche reserviert
- Klasse E
  - ersten fünf Bits immer 11110
  - ”für zukünftige Anwendungen reserviert”

Gründe für diese Einteilung

- Einträge in Routern minimieren
  - durch Klassenbildung
- Schnelle Analyse der Adresse
  - Router müssen sich (maximal) nur die ersten Bits ansehen
- Zugriff auf Host- und Netzwerkanteil einfach
  - auf Grund der Bytegrenzen
- Einteilung so, dass
  - große Organisationen $\rightarrow$ Klasse A
  - sehr kleine Organisationen $\rightarrow$ Klasse C
  - Mitte der 80er Jahre fast nur Klasse B Netze verteilt!
    - $\rightarrow$ Adressknappheit!
    - daher neue organisatorische und technische Regeln

Spezielle Adressen

- Hostanteil lauter 0er $\rightarrow$ dieser Host
- Netzanteil lauter 0er $\rightarrow$ dieses Netz
- Hostanteil lauter 1er $\rightarrow$ alle Hosts
- Netzanteil lauter 1er $\rightarrow$ alle Netze

Spezielle Adressen – 2

Netzanteil	Hostanteil	Bedeutung
Netz Id	Host Id	Normale Adresse
Netz Id	alle 0	Dieser Host (z.B. Host kennt seine IP noch nicht), aber auch Netzadresse
alle 0	Host Id	Host kennt seine Netz Id nicht oder nicht relevant
alle 0	alle 0	eigener Host (z.B. bei DHCP oder bei multi-homed Host um beliebige Adresse)
Netz Id	alle 1	alle Hosts im angegebenen Netz (Broadcast)
alle 1	alle 1	”alle Hosts in allen Netzen”, aber: Broadcast im eigenen Netz
alle 1	Host Id	sinnlos und wird nicht verwendet!

Reservierte Adressen

- 127.0.0.0 … lokaler IP Verkehr (loopback Netz)
  - meist nur eine Adresse 127.0.0.1 ist dem Loopback Interface zugeordnet
  - Loopback Interface: Jedes gesendete Paket kommt zurück
- private Adressen

Klasse	von	bis	Bemerkung
A	10.0.0.0	10.255.255.255	1 Klasse A
B	172.16.0.0	172.31.255.255	16 Klasse B
C	192.168.0.0	192.168.255.255	256 Klasse C

Reservierte Adressen – 2

- 169.254.0.0/16 (link local) zur automatischen Zuweisung einer privaten Adresse (wenn DHCP konfiguriert, aber keine Adresse erhalten)
  1. zufällig aus 169.254.1.0 – 169.254.254.255 (andere reserviert!)
  2. Versenden von 3 ARP-probes (Zieladresse: gewählte IP, Absenderadresse 0.0.0.0)
  3. kein Antwortpaket erhalten $\rightarrow$ OK, anderenfalls weiter!
- weitere reservierte Adressbereiche sind vorhanden
  - keinerlei Notwendigkeit diese zu kennen, da diese nicht vergeben werden

Bildung von Teilnetzen

- organisatorische Gründe
  - z.B. abteilungsweise Gliederung der Teilnetze.
- geographische Gründe
  - große Distanz zw. Hosts, dann naheliegend oder gefordert
- neuer Typ von physikalischem Netz installiert
- Hinzufügen weiterer Hosts $\rightarrow$ Teilung des Netzes notwendig

Nachteile Standardadressen

- Routertabellen wachsen explosionsartig
- Adresse in einem Netz wird neu benötigt, dann neuer Adressbereich muss angefordert werden, obwohl u.U. noch Adressen in den schon vergebenen Netzen zur Verfügung wären
- Änderung der internen Netzstruktur $\rightarrow$ Auswirkung auf Adressen

$\rightarrow$ Subnetting wurde eingeführt

Subnetting

- Prinzip
  - Subnetting lokal vornehmen
  - von außen unsichtbar (wie ein Netz)
- Durchführung
  - aus (Netzanteil & Hostanteil) wird (Netzanteil & Subnetzanteil & Hostanteil)
  - d.h. ursprünglicher Hostanteil wird geteilt

Vorteile von Subnetting

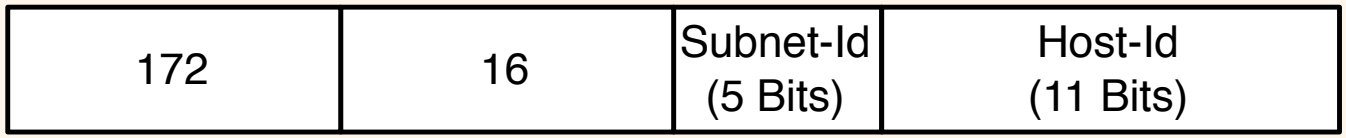
- Routertabellen vergrößern sich nicht
- Es müssen seltener neue Adressen angefordert werden
- Flexibilität, da bei Änderung der Netzstruktur $\rightarrow$ keine Änderung der Adressen
- Netze können besser auf die physikalischen Gegebenheiten abgestimmt
- Interne Netzstruktur von außen nicht sichtbar
  - auch aus sicherheitstechnischen Überlegungen positiv!

Subnetzmaske

- 32 Bit
- 1er Bit $\rightarrow$ Netzanteil, 0er $\rightarrow$ Hostanteil
- für klassenbasierte Adressen
  - Klasse A … 255.0.0.0
  - Klasse B … 255.255.0.0
  - Klasse C … 255.255.255.0

Static subnetting

- Alle Teilnetze gleiche Größe
- Klasse B Netz 172.16.0.0 mittels 5 Bit Subnetzmaske in 32 Subnetze
  - Subnetzbildung



  - Subnetzmaske: 11111111.11111111.11111000.0000000 = 255.255.248.0
  - Subnetze
    - 172.16.0.0/255.255.248.0 $\equiv$ 172.16.0.0/21
    - 172.16.8.0/21
    - …

Static subnetting – Problematik

Beispiel

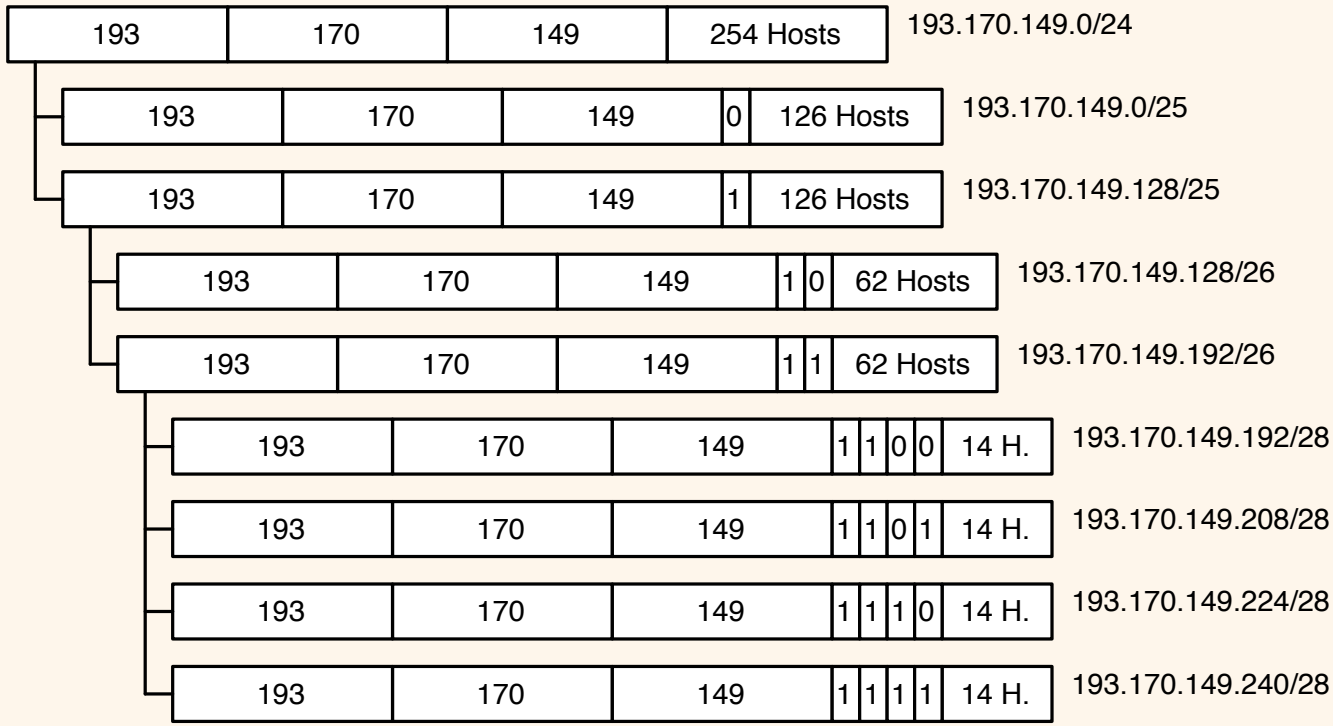
- Organisation bekommt 193.170.149.0 (Klasse C) zugeteilt
- Bedarf an folgenden Netzen
  - 4 Netze zu je 10 Hosts
  - 1 Netz zu 50 Hosts
  - 1 Netz zu 100 Hosts

  d.h. 190 Hosts < 254 IP Adressen (Klasse C)
- aber es werden 6 Netze benötigt, d.h. Subnet-ID muss die Länge 3 haben
- $\rightarrow$ es stehen 5 Bits für den Hostanteil zur Verfügung
- $\rightarrow$ d.h. max. 30 Hosts je Subnetz
- $\rightarrow$ d.h. nicht möglich

$\rightarrow$ VLSM wird benötigt!

VLSM

- Variable Length Subnet Masking
- Unterteilung der Subnetze
- jedes Subnetz eigene Subnetzmaske
- Lösung zu vorhergehender Aufgabenstellung



Weiterleiten (forward)

1. Wenn Zielsystem $\rightarrow$ stopp (d.h. Router ist Ziel)
2. Für jeden Eintrag (Subnetznummer, Subnetzmaske, nächster Hop) der Weiterleitungstabelle:
   - 2.1 D1 = Zieladresse & Subnetzmaske
   - 2.2 Wenn D1 == Subnetznummer dann:
     Wenn nächster Hop ein Interface:
     - dann Paket an Interface ausliefern
     - anderenfalls Paket an Interface ausliefern, das zu diesem Router gehört
3. Wenn kein Router gefunden dann: an Default-Router!

prinzipieller Ablauf!!

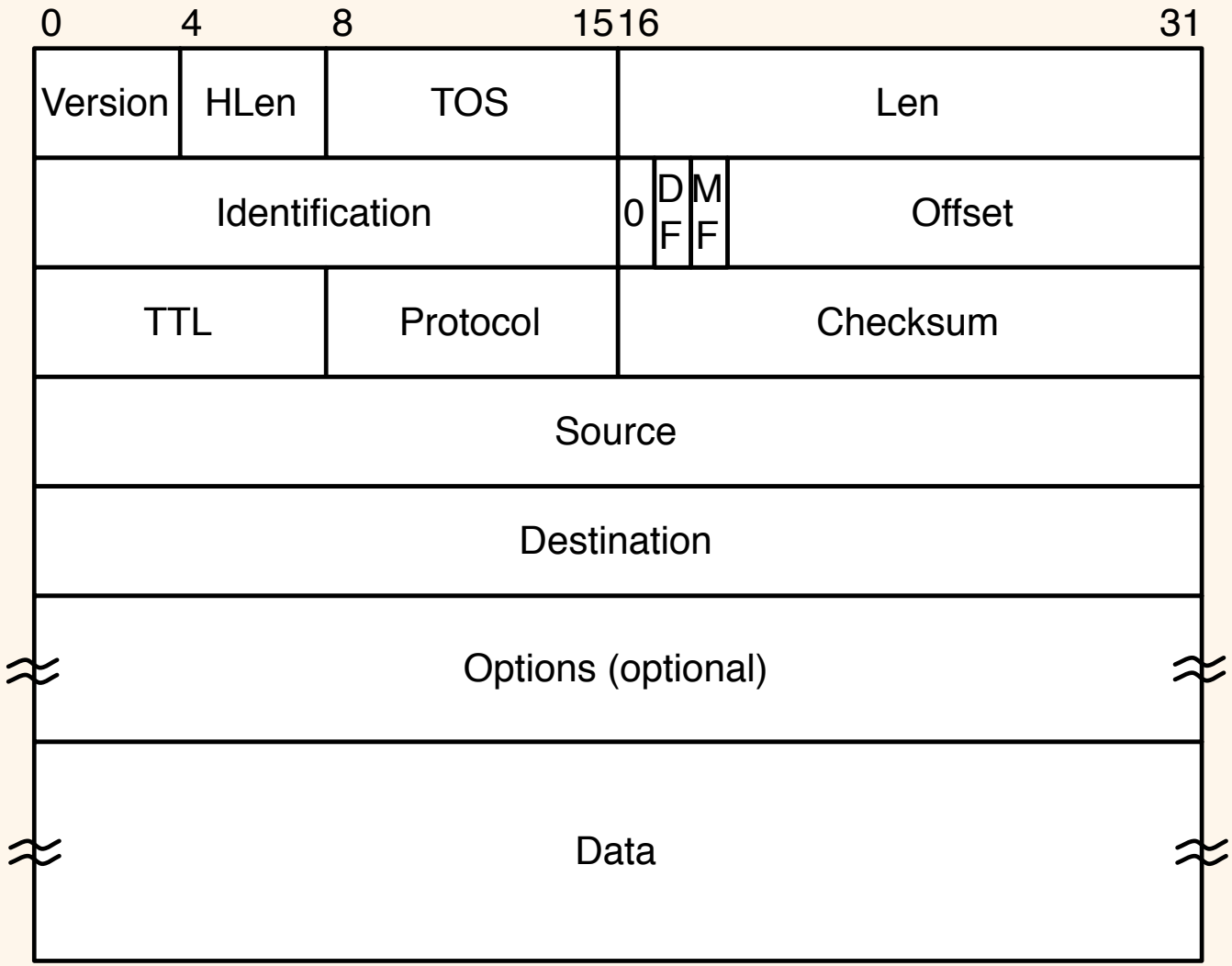
CIDR

- Classless Inter-Domain Routing
- Problematik
  - Annahme Organisation benötigt 256 Adressen $\rightarrow$ Klasse B zugewiesen
    - $\rightarrow$ Effizienz: $256/65534 \cdot 100\% = 0.39\%$
  - Erschöpfung der Adressen wird nicht vorgebeugt
- Besser: Zuweisung zweier Klasse C Netze
  - aber: 2 Routereinträge & 2 Klassen
- CIDR - Ansatz
  - Auflösung feste IP Adresse zu Netzklasse
    - keine Klassen mehr!
  - Zuweisung aufeinanderfolgender Klasse C Netze
  - Aggregation zu einem Routereintrag
    - $\rightarrow$ supernetting

CIDR – 2

- Annahme: Bedarf an 16 Klasse C Netzen
- Zuweisung von 192.4.16.0/24 bis 192.4.31.0/24
  - oberen 20 Bits gleich: 11000000 00000100 0001
  - $\rightarrow$ Netz 192.4.16.0/20!
- nur ein Routereintrag!
- lässt sich auch über mehrere Organisationen kaskadieren
- BGP, RIP v2, OSPF sind alle CIDR-tauglich
- keine IPv4 Bereiche zum Vergeben mehr vorhanden!

IP Datagram


0
4
8
15
16
31
Version
HLen
TOS
Len
Identification
0
DF
MF
Offset
TTL
Protocol
Checksum
Source
Destination
Options (optional)
Data

IP Datagram – 2

- Version: 4 oder 6
- HLen: in 32-Bitworten (inkl. Optionen)
- TOS: für QoS
- Len: Gesamtläng in Bytes
- Identification: $\rightarrow$ Fragmentierung
- Flags $\rightarrow$ Fragmentierung
  - DF … do not fragment
  - MF … more fragments
- Offset: $\rightarrow$ Fragmentierung
- TTL: Time To Live
  - übliche Anfangswerte: 64 oder 128

IP Datagram – 3

- Protocol: gibt (Transport)protokoll an
  - 1 … ICMP
  - 6 … TCP
  - 17 … UDP
- Checksum: über den gesamten Header
- Source: IP Adresse des Senders
- Destination: IP Adresse des Empfängers
- Options
  - variable Information
  - z.B. für Routing, Security, Zeitstempel
  - ggf. mit 0en bis zur nächsten 32-Bit Wortgrenze

Fragmentierung

- Anpassung der Paketgröße an unterliegende Schicht
  - MTU: Maximum Transmission Unit
    - max. Größe in Bytes der PDU einer
    - minimale MTU für IPv4 576 Bytes
- Beispiel:
  - FDDI Paket: 4352 Byte an Daten
  - Ethernet-Frame: 1500 Byte an Daten
    - $\rightarrow$ Fragmentierung beim Übergang
- Prinzip
  - Segmentierung und Reassemblierung
    - Reassemblierung nur beim Empfänger
  - 1 Fragment verloren $\rightarrow$ alle Fragmente verworfen
  - Offset eines Fragmentes in 8 Bytes
  - DF $\rightarrow$ ICMP *Fragmentation needed but DF was set*

Fragmentierung – Beispiel

- 1400 Byte
- nicht fragmentiert
  - Identification = x; MF = 0; Offset = 0; Data (1400)
- fragmentierte Pakete mit MTU = 532
  1. Identification = x; MF = 1; Offset = 0; Data (512)
  2. Identification = x; MF = 1; Offset = 64; Data (512)
  3. Identification = x; MF = 0; Offset = 128; Data (376)

ICMP

- Internet Message Control Protocol
- Hilfprotokoll für IP
  - Status, Steuer, Fehlermeldungen
- Wichtigste Beispiele
  - Echo Request & Echo Reply. Query-Nachricht
  - Ziel nicht erreichbar. Fehlernachricht
    - Netzwerk nicht erreichbar
    - Host nicht erreichbar
    - Port nicht erreichbar
    - …
  - Quelle unterdrücken (source quench). Fehlernachricht

ARP

- Address Resolution Protocol
- jeder Host merkt sich Zuordnungen IP zu MAC in Cache
- Broadcast…