

Auszüge aus Folien der Schulung

# Heterogene Netze mit TCP/IP

von

**Gerhard M. Glaser**

(<http://home.t-online.de/home/Gerhard.Glaser/>)

präsentiert für

**IIR Technologie**

Lyoner Str. 26, 60528 Frankfurt/ Main

Tel.: 069/ 669817-0

# Überblick (1)

- Grundlagen (OSI-Modell, Standards, Bridges/Switches)
- TCP/IP-History (Statistiken, RFCs)
- **IP-Protokoll (Funktionsweise, Optionen)**
- **IP-Adressierung (Adreßklassen, Subnetting)**
- IP über serielle Leitungen (SLIP, PPP)

## Überblick (2)

- IPv6
- **ARP/ RARP**
- **Routing (Routingverfahren etc.)**
- Proxy ARP
- **ICMP**
- **Routing Protokolle (RIP, OSPF)**
- Routing vs. Bridging
- **TCP**
- **UDP**
- **TELNET**

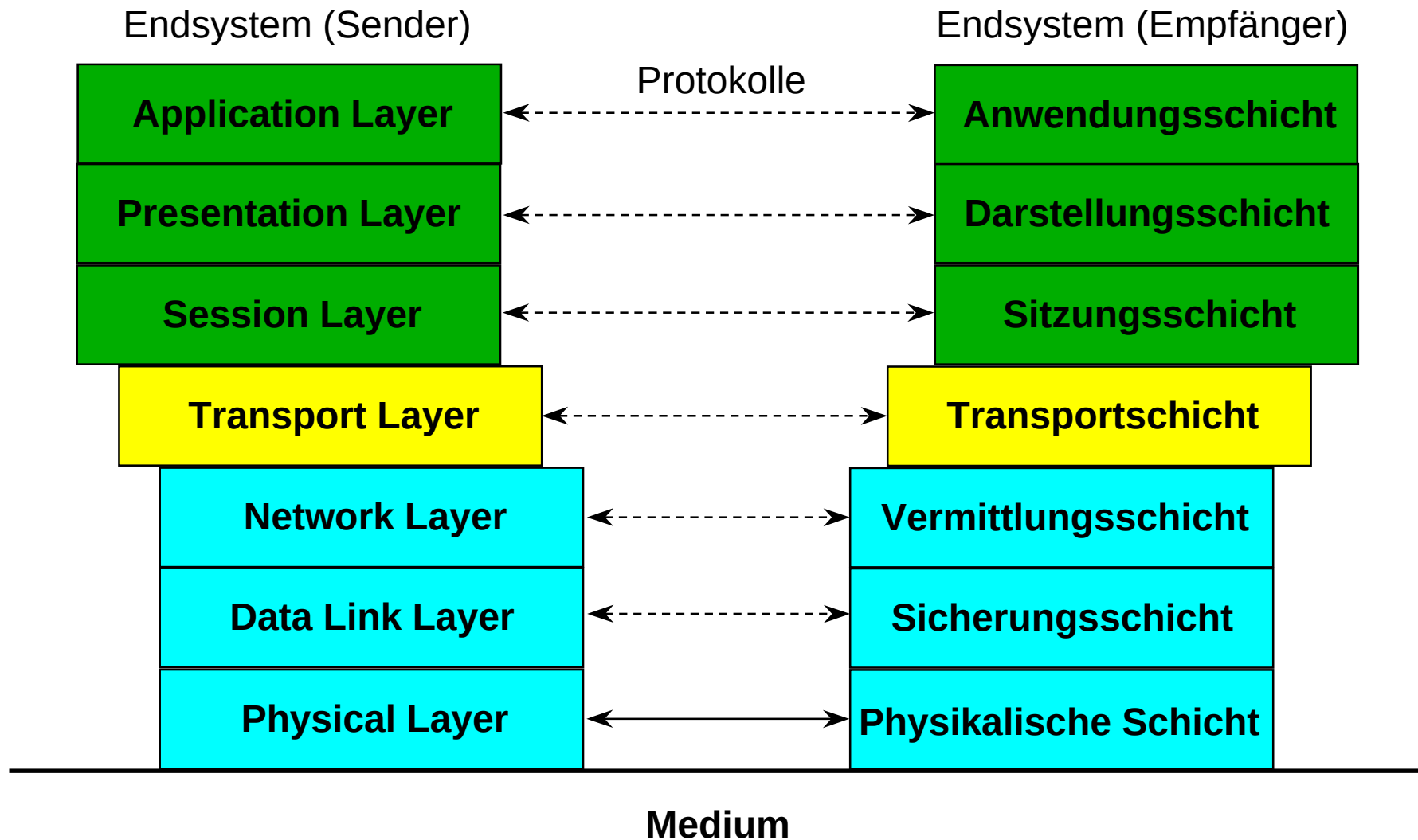
## Überblick (3)

- **FTP**
- **SMTP**
- **Name Services (IEN 116, DNS)**
- **BOOTP/ DHCP**
- **TFTP**
- **R-Utilities**
- **NFS**
- **Internetworking (WWW, Proxies/ Firewalls)**
- **SNMP**
- **Trouble-Shooting**

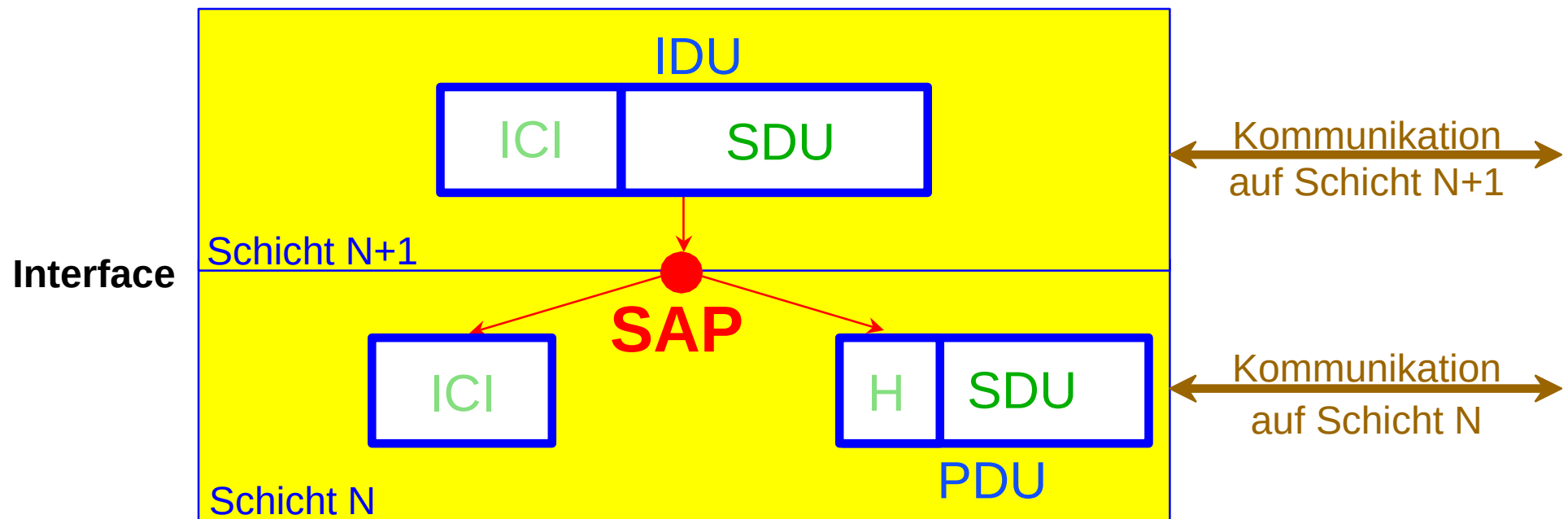
# Kapitel 1

# Grundlagen

## ISO/OSI-Modell - Schichten



## ISO/OSI-Modell - Schnittstelle



**SAP** Service Access Point  
**IDU** Interface Data Unit  
**PDU** Protocol Data Unit

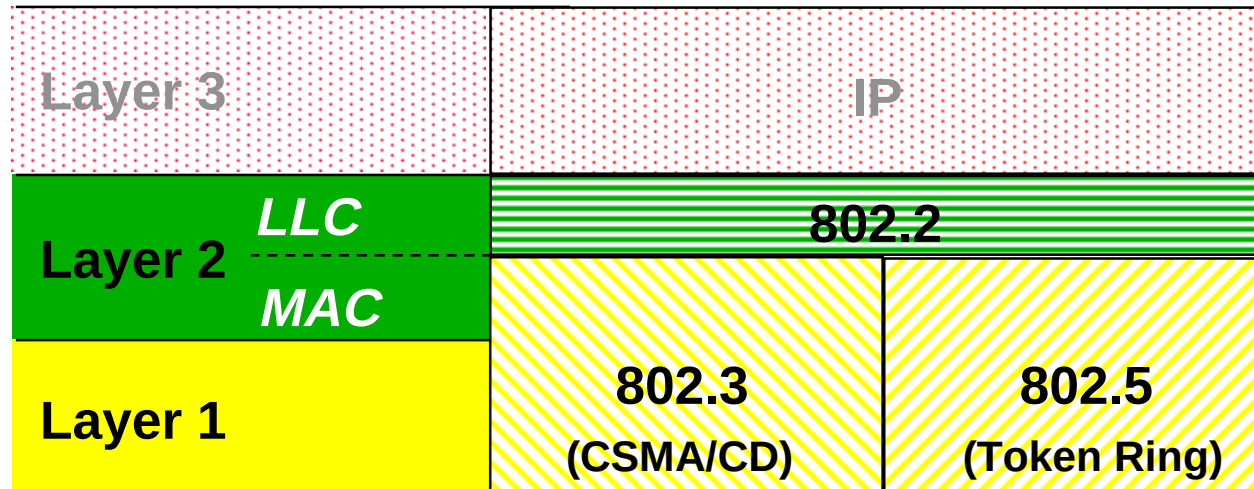
**ICI** Interface Control Information  
**SDU** Service Data Unit  
**H** Header

## Standards der Arbeitsgruppe 802

|        |                                                     |
|--------|-----------------------------------------------------|
| 802.1  | Umfeld, LAN-/MAN-Management                         |
| 802.1d | Transparent-/ SRT-Bridging                          |
| 802.2  | <b>Logical Link Control</b>                         |
| 802.3  | <b>CSMA/CD<sup>*)</sup> ("Ethernet")</b>            |
| 802.4  | Token Bus                                           |
| 802.5  | <b>Token Ring</b>                                   |
| 802.6  | Distributed Queue Dual Bus (DQDB)                   |
| 802.7  | Broadband LANs                                      |
| 802.8  | Multimode Fiber Optic Media                         |
| 802.9  | Integrated Services LAN (Wiederaufnahme am 19.9.96) |
| 802.10 | Std. for Interoperable LAN/MAN Security (SILS)      |
| 802.11 | Wireless LANs                                       |
| 802.12 | Demand Priority LAN > 10 MB ("VGanyLAN")            |
| 802.13 | n/a                                                 |
| 802.14 | CATV-based Braodband Connectivity Networks          |

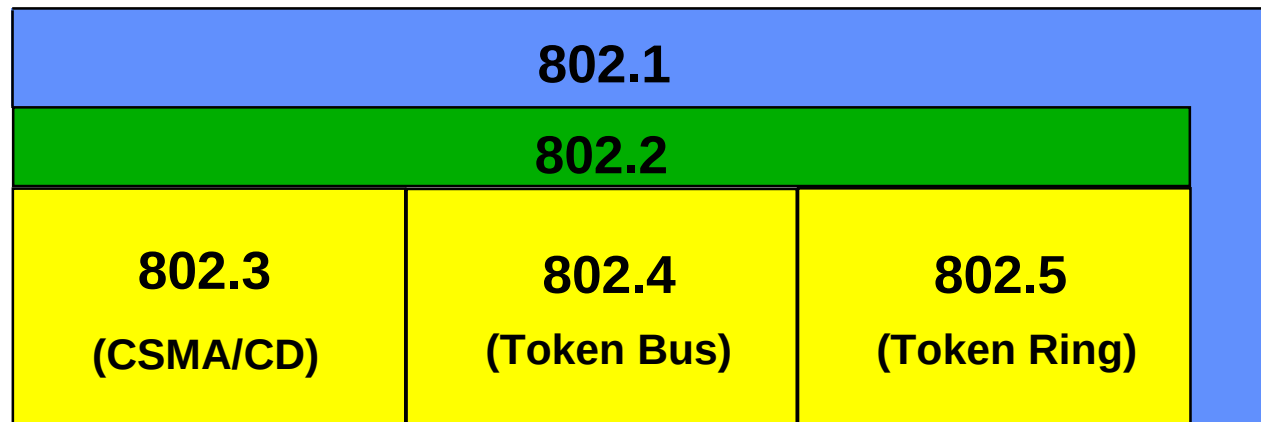
<sup>\*)</sup> Carrier Sense Multiple Access with Collision Detection

## IEEE-Standards, MAC und LLC



MAC    Medium Access Control  
LLC    Logical Link Control

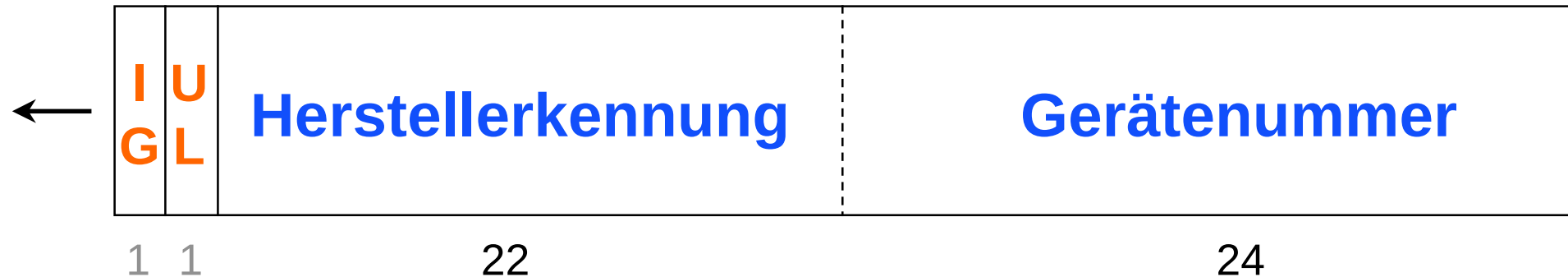
## IEEE-Standards 802.1, 802.2, 802.3, 802.4, 802.5



## Ausgewählte Standards der Arbeitsgruppe 802.3

|               |                                                            |
|---------------|------------------------------------------------------------|
| <b>802.3</b>  | <b>CSMA/CD (Ethernet): 10Base5</b>                         |
| <b>802.3a</b> | <b>10Base2 (Cheapernet)</b>                                |
| 802.3b        | 10Broad36                                                  |
| 802.3e        | 1Base5 Starlan                                             |
| <b>802.3i</b> | <b>10Base-T</b>                                            |
| 802.3j        | 10Base-F                                                   |
| <b>802.3u</b> | <b>100Base-T ("100 Mbit-Ethernet")</b>                     |
| 802.3x        | Full Duplex/ Flow Control                                  |
| <b>802.3z</b> | <b>1000 Mbit Ethernet</b> (Vorschlagsfrist bis Ende 11/96) |

## 802.3 Paket (Aufbau)



### Darstellung lt. IEEE 802.3 Standard:

Anordnung der Bits/ Bytes in Übertragungsreihenfolge  
(höchstwertiges Byte und niederwertigstes Bit werden zuerst übertragen)

- Das *I/G-Bit* entscheidet über Multicast-/Broadcast- bzw. „Unicast“-Adressen
- Das *U/L-Bit* kennzeichnet eine nichtregistrierte Adresse

## Wichtige Herstellerkennungen

|          |                                     |          |                                    |
|----------|-------------------------------------|----------|------------------------------------|
| 00-00-0C | Cisco                               | 00-60-B0 | Hewlett-Packard                    |
| 00-00-1D | Cabletron                           | 00-80-00 | Multitech Systems Inc              |
| 00-00-24 | Olicom                              | 00-80-16 | Wandel & Goltermann                |
| 00-00-63 | HP (LanProbe)                       | 00-80-5F | Compaq Computer Corporation        |
| 00-00-65 | Network General                     | 00-80-63 | Richard Hirschmann GmbH & Co       |
| 00-00-81 | Synoptics                           | 00-80-C7 | Xircom, Inc.                       |
| 00-00-A2 | Wellfleet                           | 00-80-C8 | D-Link                             |
| 00-00-AC | Conware                             | 00-A0-00 | Bay Networks Ethernet switch       |
| 00-00-B0 | RND                                 | 00-DD-00 | Ungermann-Bass IBM RT              |
| 00-00-C0 | SMC (früher: WD)                    | 00-DD-01 | Ungermann-Bass                     |
| 00-00-F4 | Allied Telesis, Inc.                | 00-DD-08 | Ungermann-Bass                     |
| 00-00-F8 | DEC                                 | 00-E0-14 | Cisco Ethernet switch              |
| 00-02-04 | Novell NE3200                       | 08-00-05 | Symbolics LISP machines            |
| 00-20-AF | 3COM Corporation                    | 08-00-06 | Siemens Nixdorf PC clone           |
| 00-60-09 | Cisco Catalyst 5000 Ethernet switch | 08-00-0F | SMC (Standard Microsystems Corp.)  |
| 00-60-2F | Cisco                               | 08-00-1B | Data General                       |
| 00-60-3E | Cisco 100Mbps interface             | 08-00-1E | Apollo                             |
| 00-60-5C | Cisco                               | 08-00-36 | Intergraph CAE stations            |
| 00-60-70 | Cisco routers (2524 and 4500)       | 08-00-38 | Bull                               |
| 00-60-83 | Cisco 3620/3640 routers             | 08-00-39 | Spider Systems                     |
| 00-60-8C | 3Com                                | 08-00-3E | Motorola VME bus processor modules |
| 00-60-97 | 3Com                                | 08-00-7C | Vitalink TransLAN III              |

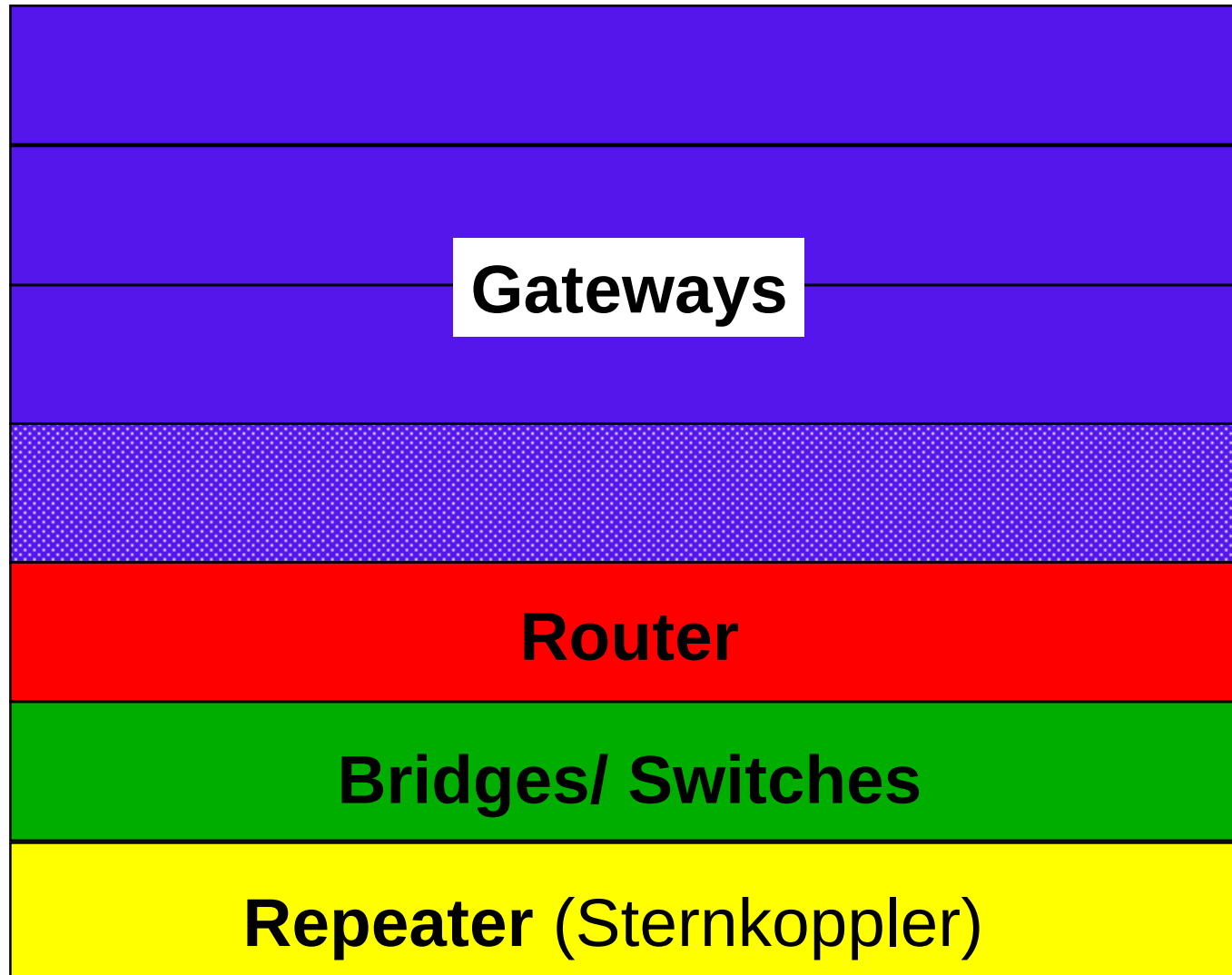
## Wichtige Typfelder im Ethernet-Header

|              |            |              |                                                                                |
|--------------|------------|--------------|--------------------------------------------------------------------------------|
| <b>00-00</b> | <b>...</b> | <b>05-DC</b> | <b>IEEE802.3 Length Field</b> ( <b>05-DD</b> ... <b>05-FF</b> nicht vergeben!) |
| <b>06-00</b> |            |              | <b>Xerox NS IDP</b>                                                            |
| <b>08-00</b> |            |              | <b>DOD Internet Protocol (IP)</b>                                              |
| <b>08-06</b> |            |              | <b>Address Resolution Protocol (ARP)</b>                                       |
| <b>0B-AD</b> |            |              | <b>Banyan Systems</b>                                                          |
| <b>0B-AF</b> |            |              | <b>Banyon VINES Echo</b>                                                       |
| <b>60-00</b> |            |              | <b>DEC unassigned, experimental</b>                                            |
| <b>60-01</b> | <b>...</b> | <b>60-08</b> | <b>DEC</b>                                                                     |
| <b>80-05</b> |            |              | <b>HP Probe protocol</b>                                                       |
| <b>80-35</b> |            |              | <b>Reverse Address Resolution Protocol (RARP)</b>                              |
| <b>80-38</b> | <b>...</b> | <b>80-42</b> | <b>DEC</b>                                                                     |
| <b>80-7D</b> | <b>...</b> | <b>80-80</b> | <b>Vitalink</b>                                                                |
| <b>80-9B</b> |            |              | <b>EtherTalk (AppleTalk over Ethernet)</b>                                     |
| <b>80-F3</b> |            |              | <b>AppleTalk Address Resolution Protocol (AARP)</b>                            |
| <b>80-FF</b> | <b>...</b> | <b>81-03</b> | <b>Wellfleet Communications</b>                                                |
| <b>81-37</b> | <b>...</b> | <b>81-38</b> | <b>Novell, Inc.</b>                                                            |
| <b>90-00</b> |            |              | <b>Loopback (Configuration Test Protocol)</b>                                  |
| <b>90-01</b> | <b>...</b> | <b>90-03</b> | <b>3Com (früher: Bridge Communications)</b>                                    |

## Wichtige DSAPs/ SSAPs im 802.3 Header

|           |                                                  |
|-----------|--------------------------------------------------|
| 00        | Null SAP                                         |
| 02        | Individual LLC Sublayer Mgmt Function            |
| 03        | Group LLC Sublayer Mgmt Function                 |
| <b>06</b> | <b>ARPANET Internet Protocol (IP)</b>            |
| 42        | IEEE 802.1 Bridge Spanning Tree Protocol         |
| 80        | Xerox Network Systems (XNS)                      |
| <b>98</b> | <b>ARPANET Address Resolution Protocol (ARP)</b> |
| AA        | Sub-Network Access Protocol (SNAP)               |
| BC        | Banyan VINES                                     |
| E0        | Novell Netware                                   |
| F0        | IBM NetBIOS                                      |
| F4/ F5    | IBM LAN Management                               |
| FE        | ISO Network Layer Protocol                       |
| FF        | Global SAP                                       |

## Transitsysteme im OSI-Modell



## Transitsysteme im OSI-Modell (Aufgaben)

- Repeater:** Regeneriert und verstärkt das elektrische Signal.  
Es findet **keine “Bitinterpretation”** statt
- Bridge/ Switch:** Nimmt physikalische Trennung von Netzen vor. Führt **Fehler- und Lasttrennung** durch. Mechanismen zum Filtern meist implementiert. Rudimentäre Mechanismen zur Wegefindung u.U. vorhanden (“Routing Bridge”)
- Router:** Entkoppelt die (Sub-) Netze auf logischer (Protokoll-) Basis aufgrund von **Layer 3-Adressen**.  
Steuert den Verkehr zwischen Netzen (**“Wegefindung”**).  
Arbeitet **protokollabhängig!**
- Gateway:** Nimmt eine **Umwandlung von Diensten** vor.  
Security-Mechanismen möglich (“Firewall”, “Proxy”).

## TCP/IP-History (Überblick)

|       |                                                                                                          |
|-------|----------------------------------------------------------------------------------------------------------|
| 1969  | erste Arbeiten an einem paketvermittelnden Rechnernetz                                                   |
| 1972  | das ARPANET wird der Öffentlichkeit vorgestellt                                                          |
| 1973  | “Ethernet is born”                                                                                       |
| 1975  | Die DCA (Defence Communications Agency) übernimmt die Federführung im ARPANET                            |
| 1976  | Grundsteinlegung zu TCP/IP durch die IFIP (International Federation Of Information Processing)           |
| 1979  | DEC, Intel und XEROX ( <b>DIX</b> -Group) entwickeln gemeinsam das Ethernet weiter                       |
| 1980  | Ethernet Version 1.0 wird veröffentlicht<br>Bercley UNIX (BSD 4.1) wird entwickelt und enthält TCP/IP    |
| 1983  | Das ARPANET wird endgültig von NCP auf TCP/IP umgestellt<br>Aufteilung des ARPANET in MILNET und ARPANET |
| 1985  | Einführung von TCP/IP in kommerzielle Anwendungen                                                        |
| 1991  | Mehr als 1000 Hersteller unterstützen TCP/IP                                                             |
| 1993  | Mehr als 10000 Hersteller unterstützen TCP/IP                                                            |
| 1996  | Das Internet umfaßt ca. 15 Mio. Anschlüsse                                                               |
| heute | monatlich werden um die 100.000 .COM-Domainnamen reserviert                                              |

## Kapitel 2

# Internet Protokoll (IP)

## Internet Protokoll (IP)

**RFC 791   MIL-Std. 1777**

- setzt auf dem Data Link Layer (Ethernet, TR etc.) auf
- (Ethernet-) Typefield: **08-00**
- 802.2 DSAP/SSAP: 06
- Datagramme
- Verbindungen zwischen Netzen
- Datentransport von einer Quell- zu einer Zieladresse

## IP - Wichtige RFCs

**RFC 791      IP-Protokoll (MIL Std. 1777)**

**RFC 815      IP over X.25 Networks**

**RFC 894      IP over Ethernet-Networks**

**RFC 948      IP over 802.3 Networks**

**RFC 1051     IP over Arcnet-Networks**

**RFC 1055     IP over Serial Lines ("SLIP")**

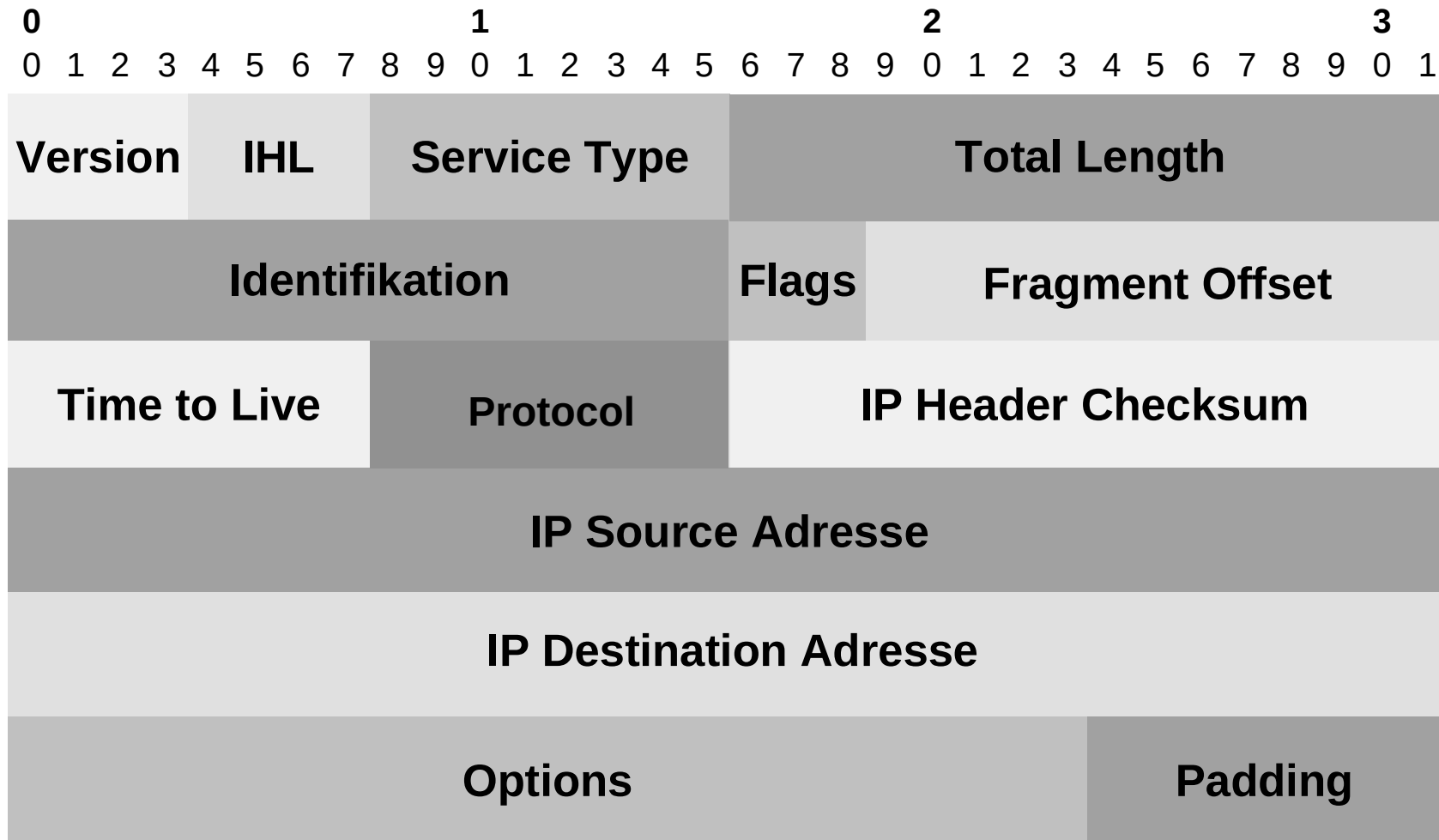
**RFC 1088     IP over Netbios Networks**

**RFC 1577     IP over ATM Networks ("Classical IP")**

## IP - Eigenschaften

- **Datagram-Service (ungesichert!)**
- **Definition/ Adressierung höherer Protokolle**
- **Adreßfunktion**
- **Routing** zwischen Netzen
- **Fragmentierung von Datenpaketen**
- **Wahl von Übertragungsparametern**

## IP v4 - Header



## IP - Type Of Service (TOS)

### Default-Werte bei verschiedenen Diensten

|                      |      |                                 |
|----------------------|------|---------------------------------|
| TELNET               | 1000 | minimize delay                  |
| FTP Control          | 1000 | minimize delay                  |
| FTP Data             | 0100 | maximize throughput             |
| SMTP (Command Phase) | 1000 | minimize delay                  |
| SMTP (Data Phase)    | 0100 | maximize throughput             |
| SNMP                 | 0010 | maximize reliability            |
| ICMP                 | 0000 | <i>aber: request = response</i> |

## **IP - Fragmentierung**

### **Warum Fragmentierung**

- **Hardware-/ Software-Beschränkungen**
- **Definition des Protokolles/ Beschränkung durch Norm**
- **Maßnahmen zur Fehlerreduktion**
- **zum Erhöhen der “Zugangsgerechtigkeit” auf Datenkanal (Begrenzung der Zugriffszeit)**

## **IP - Fragmentierung**

### **Paketlänge (in Bit) auf verschiedenen Netzen**

- |                   |              |
|-------------------|--------------|
| • Token Ring      | <b>32768</b> |
| • Ethernet        | <b>12144</b> |
| • X.25 (Maximum)  | <b>8192</b>  |
| • X.25 (Standard) | <b>1024</b>  |

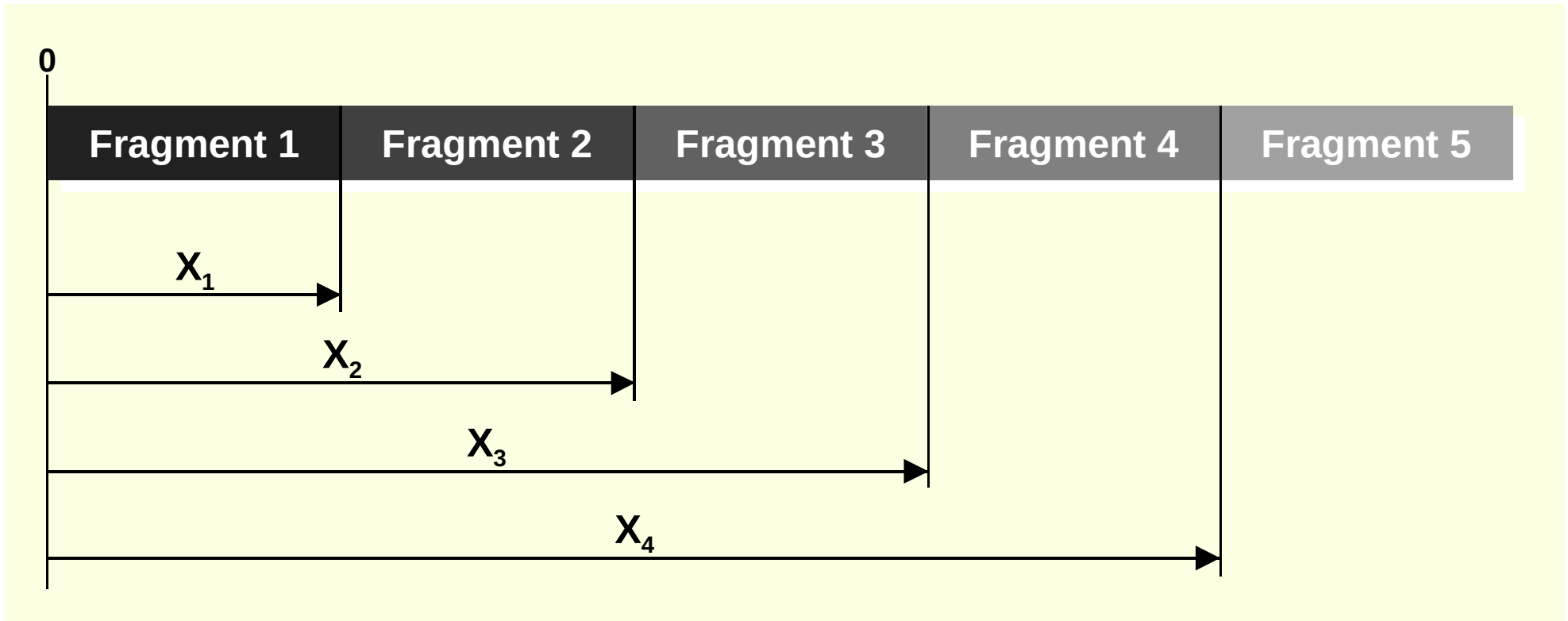
## **IP - Fragmentierung**

### **Fragment Offset**

- **Gibt die Länge relativ zum Beginn des Datenbereichs im ursprünglichen Datagram an**
- **Ermöglicht dem Empfänger mehrere Fragmente in der richtigen Reihenfolge zusammenzusetzen**
- **Bei vollständigen Datagrammen (keine Fragmentierung) und beim ersten Fragment hat der Fragment Offset immer den Wert 0**

## IP - Fragmentierung

### Fragment Offset (Grafik)



## IP - Fragmentierung Flags



|                      |   |   |                |
|----------------------|---|---|----------------|
| DF (Don't Fragment): | 0 | = | May Fragment   |
|                      | 1 | = | Don't Fragment |
| MF (More Fragment):  | 0 | = | Last Fragment  |
|                      | 1 | = | More Fragment  |

## IP - Paket-Lebenszeit (1)

- **Problem**

- beim Routen durch vermaschte Netze, können Datagramme/ Fragmente ziellos und unendlich lange kreisen

***Konsequenz: Ressourcen werden vergeudet***

## IP - Lebenszeit (2)

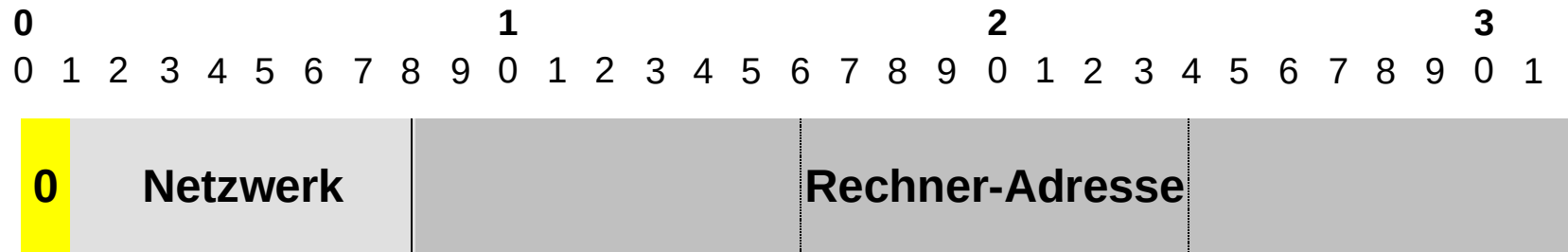
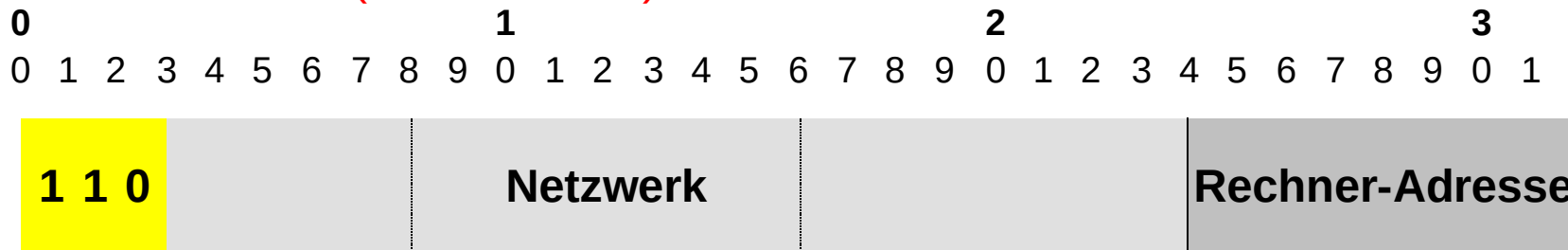
- **Lösung:**
  - ➔ **TTL-Feld (Time To Live)**
    - ➔ Reduzierung des Wertes in jedem Router
    - ➔ Bei Erreichen des Wertes "0", wird Paket vernichtet (nicht weitergereicht)

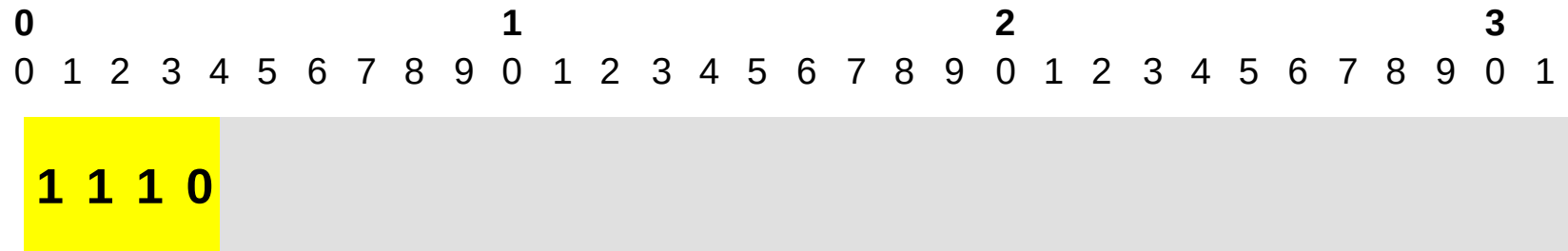
## Ausgewählte IP-Protokollnummern

|           |                                                 |
|-----------|-------------------------------------------------|
| <b>01</b> | <b>ICMP</b>                                     |
| 04, 94    | IP in IP (capsulation)                          |
| <b>06</b> | <b>TCP</b>                                      |
| 08        | EGP                                             |
| 09        | IGP (any private interior gateway)              |
| <b>17</b> | <b>UDP</b>                                      |
| 29        | ISO-TP4 (ISO-Transport-Protocol Class 4)        |
| 83        | Vines                                           |
| 88        | IGRP (Interior Gateway Routing Protocol; CISCO) |

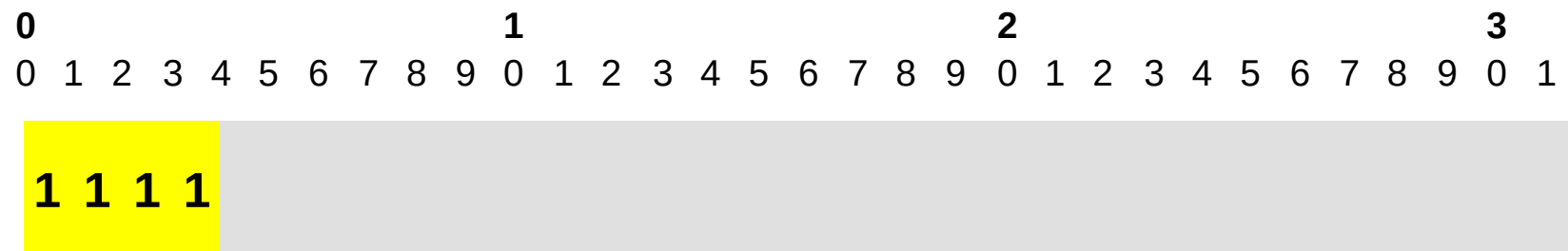
## Kapitel 3

# IP - Addressing/ -Subnetting

**Klasse-A-Adressen (Wert 0-127)****Klasse-B-Adressen (Wert 128-191)****Klasse-C-Adressen (Wert 192-223)**

**Klasse-D-Adressen** (Wert 224-239)

*Multicast-Adressen*

**Klasse-E-Adressen** (Wert 240-255)

*undefiniertes Format*

## Ausgewählte IP-Multicast-Adressen

|                  |                                   |
|------------------|-----------------------------------|
| 224.0.0.0        | Base Address (reserved)           |
| 224.0.0.1        | All <i>Systems</i> on this subnet |
| 224.0.0.2        | All <i>Routers</i> on this subnet |
| <b>224.0.0.5</b> | <b>OSPF - All Routers</b>         |
| 224.0.0.9        | RIP-2                             |
| 224.0.0.10       | IGRP-Routers                      |
| 224.0.1.8        | SUN NIS ('Yellow Pages')          |
| 224.0.1.24       | microsoft-ds                      |
| 224.0.2.2        | SUN RPC (NFS)                     |

## Adressen/ Werte mit besonderer Bedeutung

**127.x.x.x**

**Local Host (meist: 127.0.0.1)**

**255** (im Host-Teil)  
**255.255.255.255**

**All-One-Broadcast**  
**All Hosts on this net**

**0** (im Host-Teil)  
**0** (im Netz-Teil)

**All-Zero-Broadcast (veraltet)**  
**This Net**

## IP - Subnetting mit erweiterter Subnetz-Maske

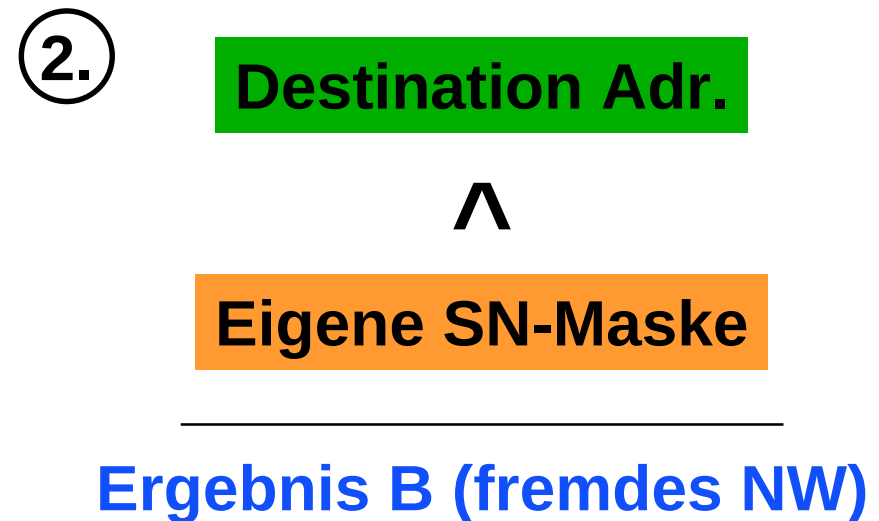
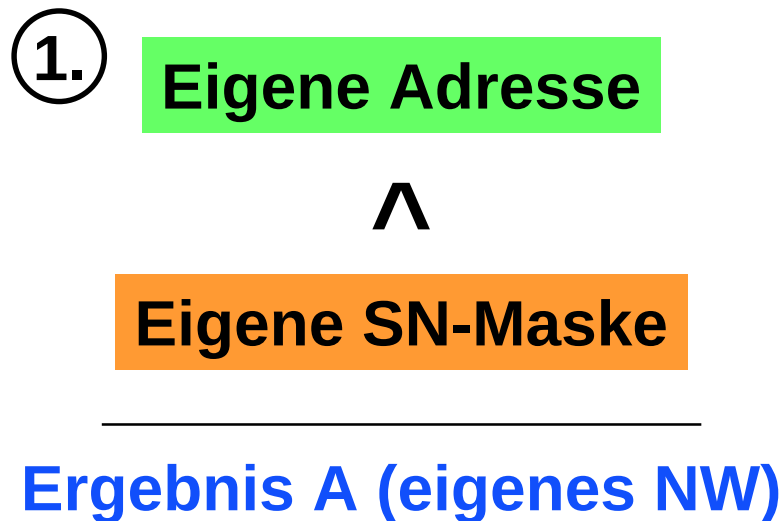
|           |                        | 1. Octett        | 2. Octett         |
|-----------|------------------------|------------------|-------------------|
| <b>IP</b> | <b>126.xxx.xxx.xxx</b> | <b>0111 1110</b> | <b>.xxxx xxxx</b> |
| <b>SN</b> | <b>255.128.000.000</b> | <b>1111 1111</b> | <b>.1000 0000</b> |

IP = IP-Adresse

SN = Subnetz-Maske

## IP - Subnetting

### Interne Vorgehensweise des Rechners



|      |            |               |                                                               |
|------|------------|---------------|---------------------------------------------------------------|
| Wenn | $A = B$    | $\Rightarrow$ | Destination in <span style="color: blue;">selbem</span> Netz  |
| Wenn | $A \neq B$ | $\Rightarrow$ | Destination in <span style="color: blue;">anderem</span> Netz |

## Point To Point Protocol (PPP)

RFC 1661/ 1662 - Juli 1994

- **Verbindungsaufbau auf Layer 2 (HDLC-basierend bzw. asynchron)**
- **Fehlerkorrektur**
- **Adreßinformationen**
  - ↳ multipointfähig (derzeit nicht genutzt)
- **Protokoll-Feld**
  - ↳ multiprotokollfähig (auf einer Leitung)
- **feste maximale Paketlänge (1500 Byte)**
- **echte Datenkomprimierung (optional)**
- **Testen der Leitungsqualität (optional)**

## Point To Point Protocol (PPP)

### Paketaufbau (synchron)

| Flag      | Address   | Control   | Protocol | <i>DATA</i><br><i>(Information)</i> | FCS    | Flag      |
|-----------|-----------|-----------|----------|-------------------------------------|--------|-----------|
| 0111 1110 | 1111 1111 | 0000 0011 | 16 bit   | ≤ 1500 Byte                         | 16 bit | 0111 1110 |

# IPng (IP Version 6)

## IPng (IP Version 6) - Neue Eigenschaften

- **Adreßbereich umfaßt 128 Bit (16 Byte) -**  
665.570.793.348.866.943.898.599 Adressen pro Quadratmeter (bzw. 666 Billionen/ mm<sup>2</sup>)  
[vgl.: 32 Bit/ 4 Byte bei IP v.4]
- **Reduzierung des Header-Overheads durch Weglassen von nicht benötigten Feldern/ Funktionen (z.B. Fragmentierung)**
- **Realtime-Fähigkeiten (“Flow Label”)**
- **Security-Features (Authentifizierung, Datenintegrität)**
- **Nutzdatenanzeige (“Payloadlength”)**
- **“Jumbo-Payload”- Feld (> 65535 Byte)**

## IPng - Adreßschema und Adreßarten

- Format Prefix - Registry ID - Provider ID - Subscriber ID
- Subnet ID - Interface ID (48 Bit)
- „Anycast Adresse“ (“doppelte” Adresse)
- Multicast Adressen (**keine** Broadcast Adressen)
- Adreßbereich für andere Protokolle (z.B. IPX) werden unterstützt/ sind reserviert

# Adreßaufteilung

## Aktueller Vorschlag



**FP**    **Format Prefix (001)**

**TLA**   **Top Level Aggregator (Public Transport Topology)**

**NLA**   **Next Level Aggregator (Provider)**

**SLA**   **Site Level Aggregator (Subnet)**

**Interface (Device)**

## IPng (IP Version 6) - RFCs

- RFC 1881 Address Allocation Management
  - RFC 1883 Specification (neue in Vorbereitung)
  - RFC 1884 Addressing (neue in Vorbereitung)
  - RFC 1887 Address Allocation
  - RFC 1897 Testing Address Allocation
- 
- RFC 1825 Security Architecture
  - RFC 1826 IP Authentication Header
  - RFC 1827 IP Encapsulation Security Payload (ESP)
  - RFC 1828 IP Authentication Using Keyed MD5
  - RFC 1829 The ESP DES-CBC Transform

# Kapitel 4

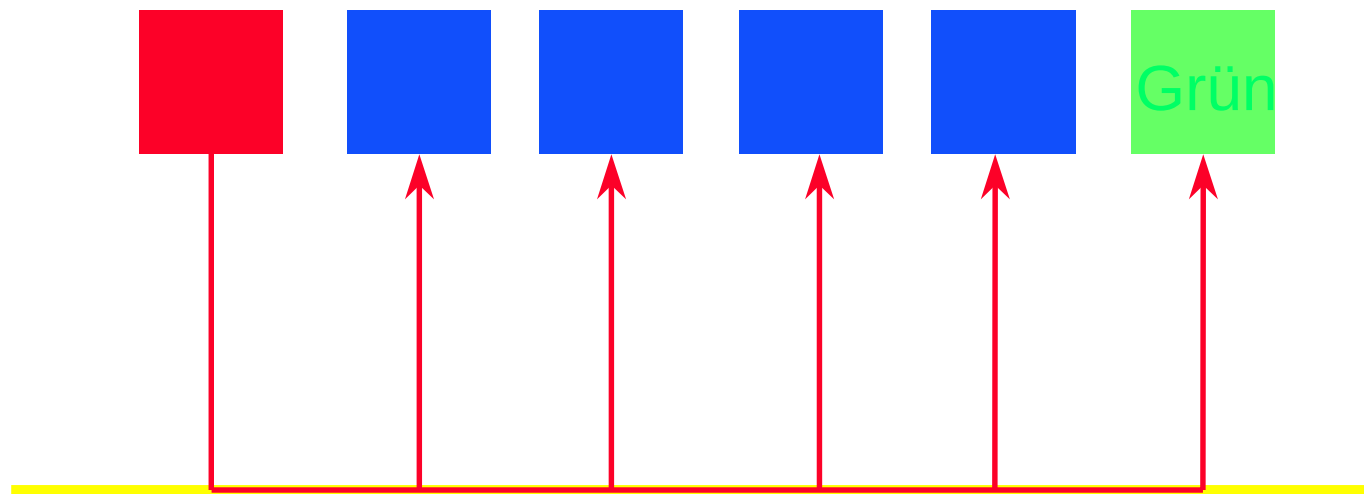
# Address Resolution Protocol (ARP)

## Adress Resolution Protocol (ARP)

RFC 826

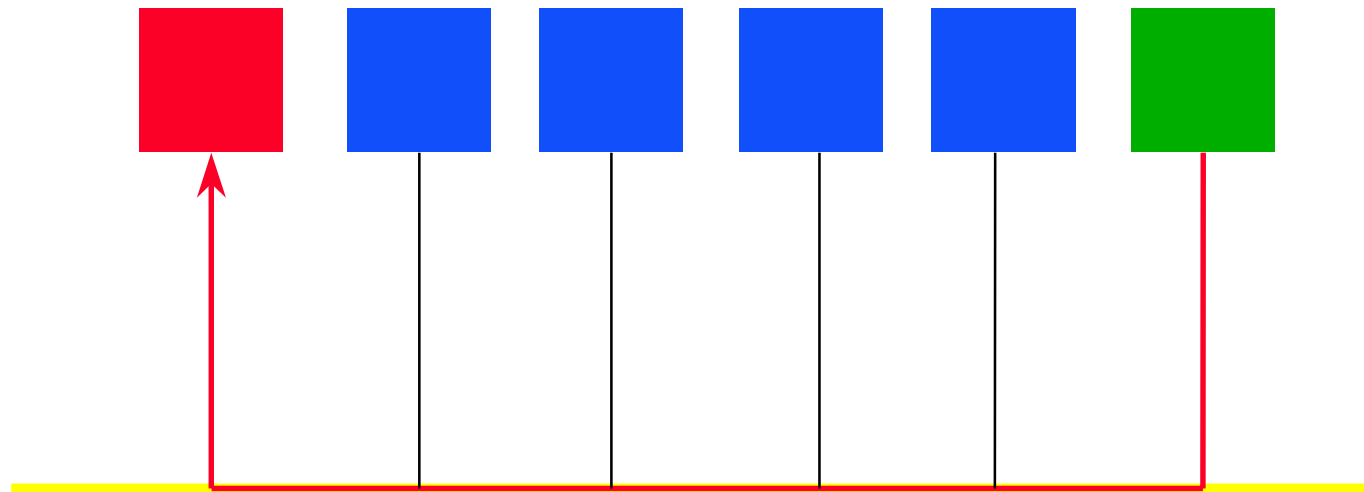
- setzt auf dem Data Link Layer (Ethernet, TR etc.) auf
- (Ethernet-) Typefield: **08-06**
- keine Definition (bei IEEE) in 802.2 (DSAP/SSAP)
- Datagramme
- Zuordnung von Ebene 3 (IP-) Adressen zu Ebene 2 (physikalische) Adressen

## ARP - Request



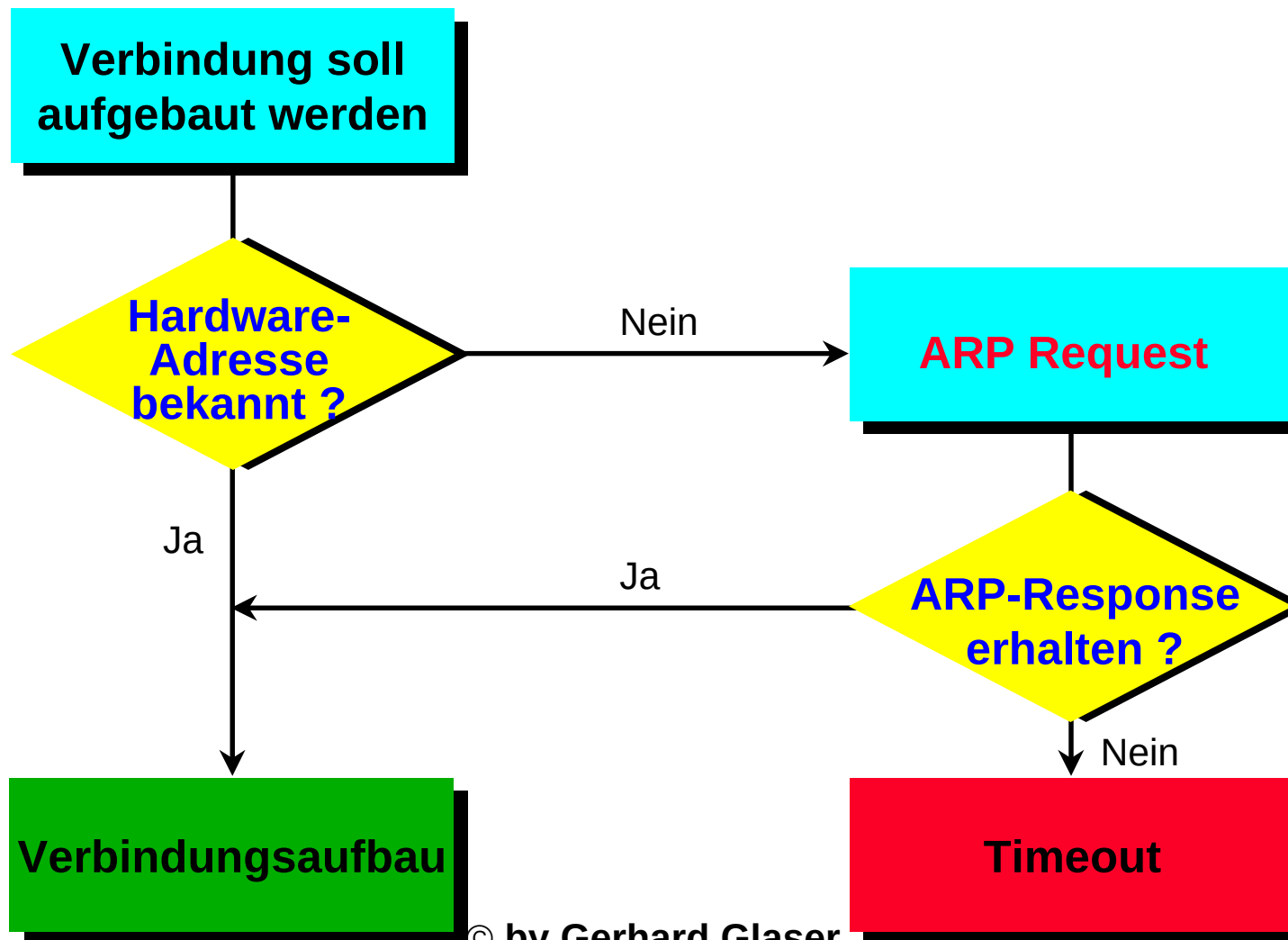
Broadcast: "Wer kennt die Ebene 2 Adresse von GRÜN?"

## ARP - Response (1)

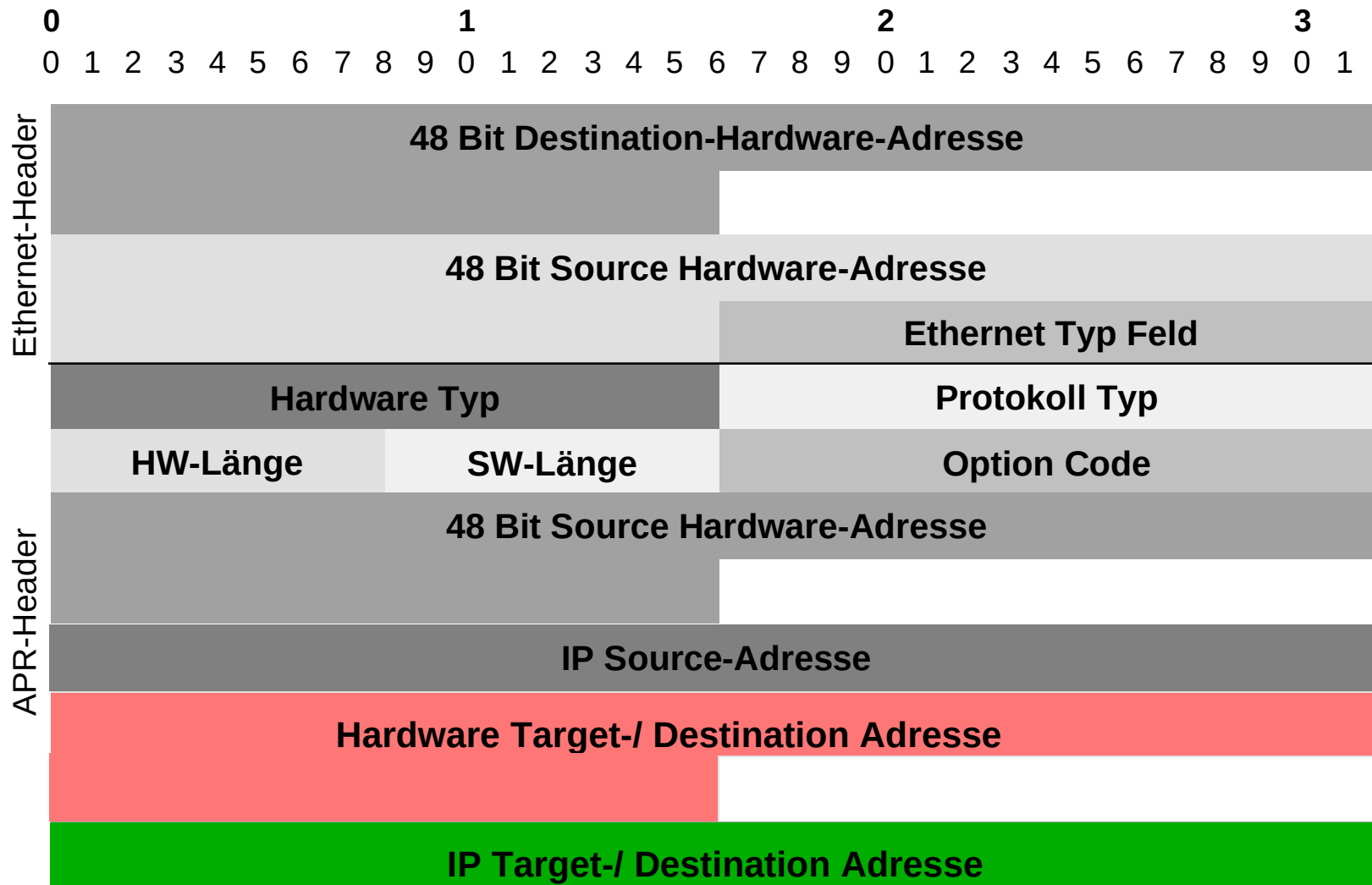


Gerichtete Antwort (Unicast):  
“Hier ist die gesuchte (**meine**) Ebene 2 Adresse”

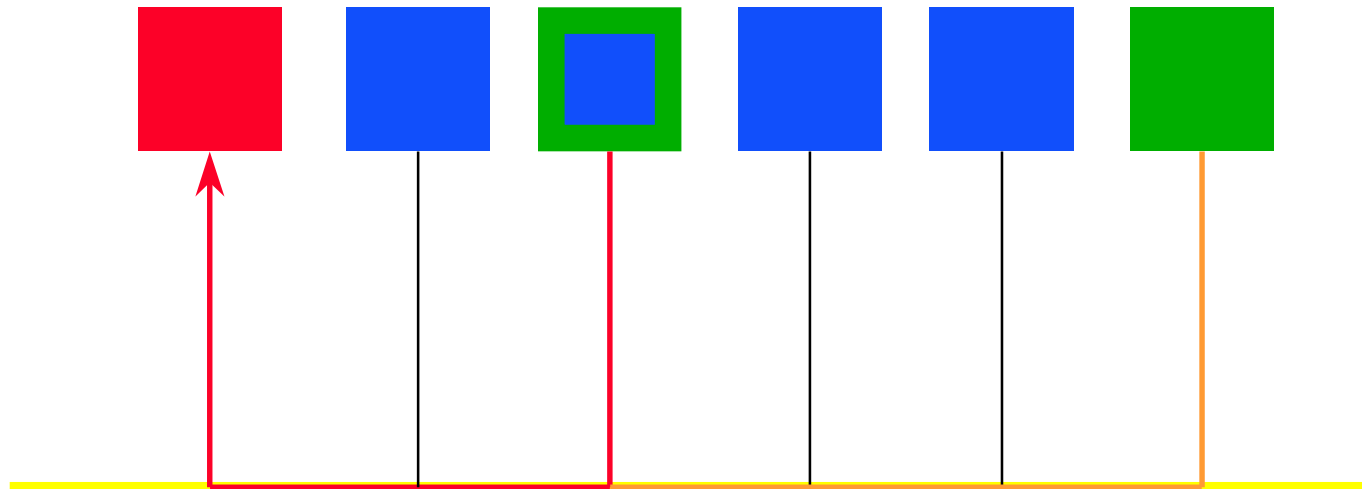
## ARP - Ablaufdiagramm



## ARP - Datenformat



## ARP - Response (2)

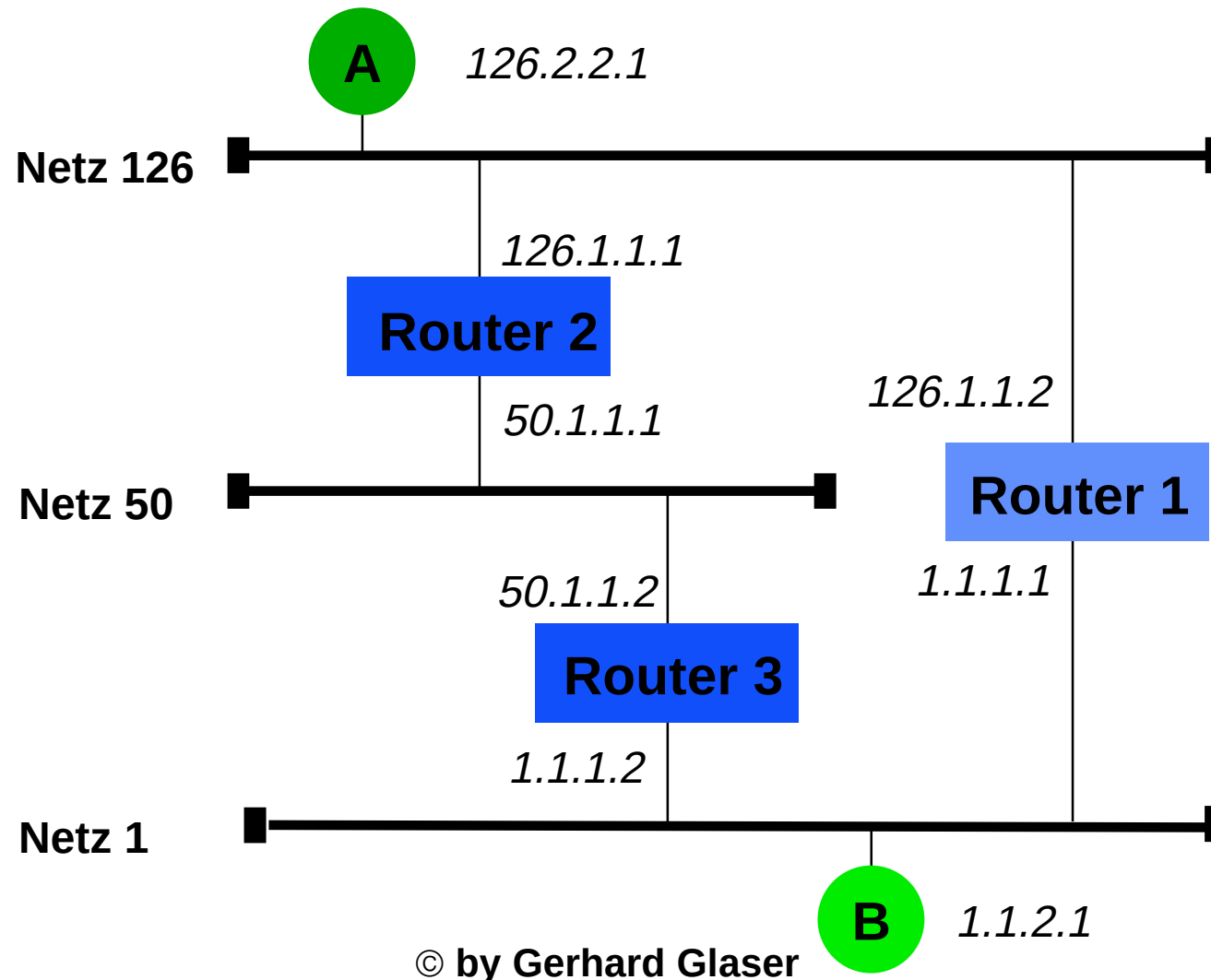


- Unicast: "Hier ist die gesuchte Ebene 2 Adresse"
- Unicast: "Hier ist die gesuchte (**meine**) Ebene 2 Adresse"

# Kapitel 5

# IP - Routing

## Routing in vermaschtem Netz



## Routing - Verfahren

- statisches Routing
- dynamisches Routing
- default Routing

nicht zu verwechseln mit den IP-Optionen:

- Source-Route
  - ➡ Loose Source-Route
  - ➡ Strict Source-Route
- Record Route

# Proxy ARP

## Proxy ARP

- **Kein Protokoll, sondern Programm (Daemon) auf Router**
- **Leitet ARP-Anfragen an Routing-Table weiter**
- **Erspart (temporär) Routingeinträge auf Hosts**
- **Belastet den Router durch notwendige zusätzliche ARP-Bearbeitung**

**Kapitel 6**  
**Internet Control Message**  
**Protocol**  
**(ICMP)**

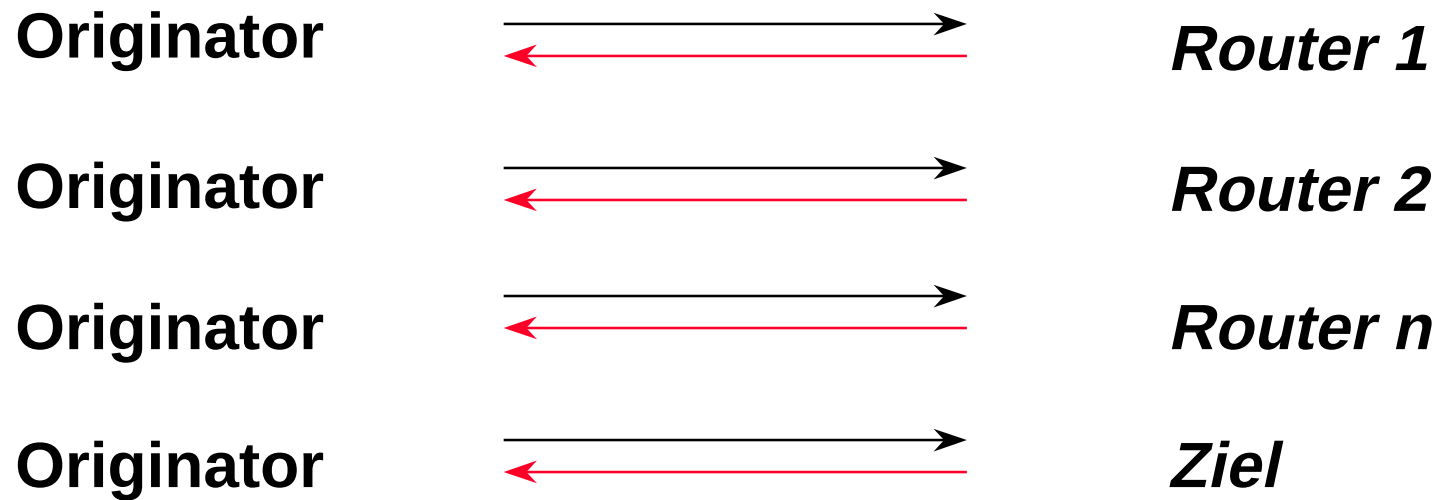
# Internet Control Message Protocol (ICMP)

RFC 792

- setzt direkt auf dem Internet Protokoll (IP) auf
- IP-Protokoll-Nr.: 01
- es dient dem Informationsaustausch der Endgeräte über den aktuellen Status der Ebene 3 (IP)
- es gibt Error-Meldungen und Info-Meldungen.
  - **Error-Pakete** beinhalten, neben der Fehlermeldung, auch immer den **Header** und **die ersten 64 Byte** des den Fehler verursachenden Paketes.
  - **Info-Meldungen** basieren auf einem Request-/ Response-Verfahren

## IP / ICMP “Trace-Route”

Bisherige/ einfache Methode (z.B. Microsoft)



 IP-Paket mit TTL = 1, 2, ..., n

 ICMP Error (n-Mal)

## IP / ICMP “Trace-Route”

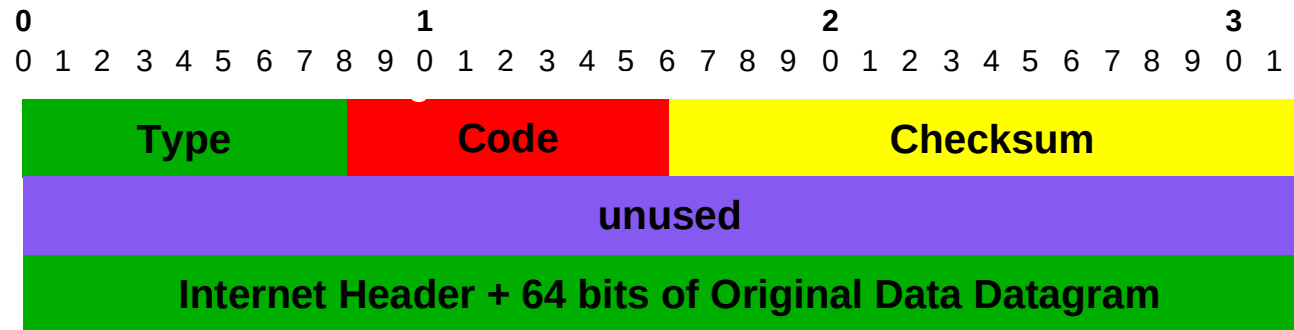
### Neue Methode mittels Trace-Route-Option



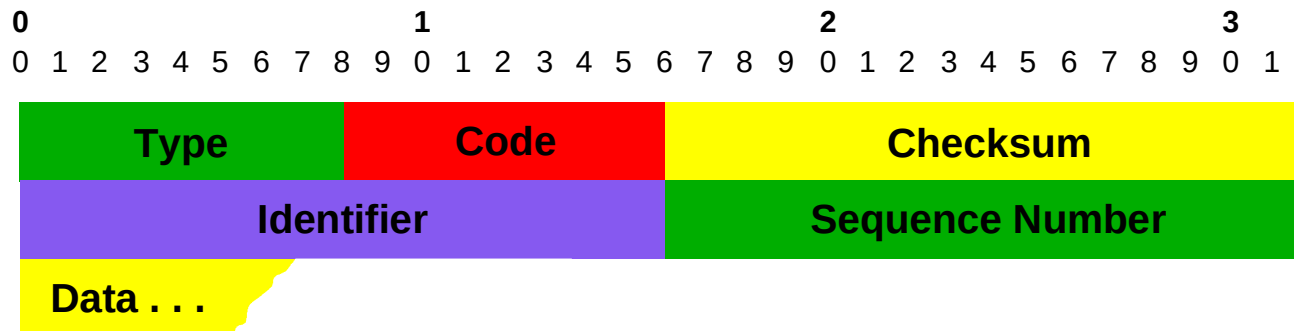
- IP-Paket “Trace Route” (OHC wird incrementiert)
- ← ICMP-Message “Trace Route” (1, 2, ..., n) (RHC wird incrementiert)

OHC = Outbound Hop Count

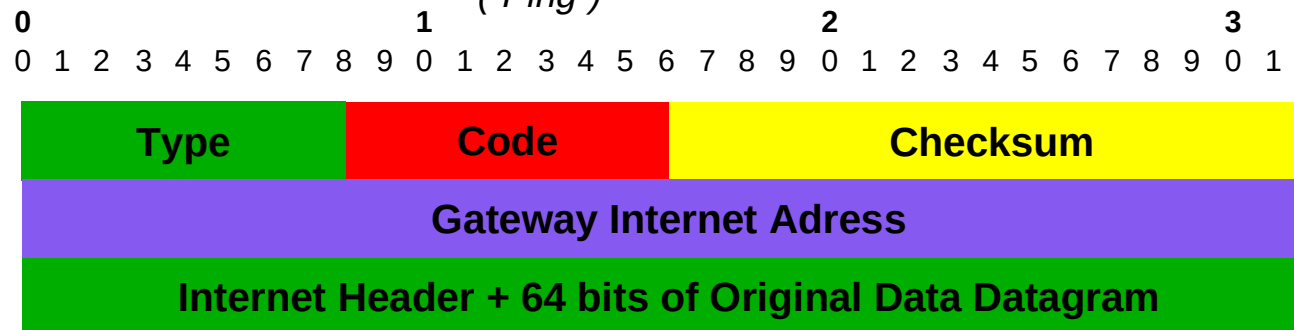
RHC = Return Hop Count



*Destination Unreachable Message*



*Echo or Echo Reply Message*  
(“Ping”)



*Redirect Message*

## ICMP - Messages

### Type Numbers (Auswahl)

|    |                         |
|----|-------------------------|
| 00 | Echo Reply              |
| 02 | Destination Unreachable |
| 04 | Source Quench           |
| 05 | Redirect                |
| 08 | Echo Request            |
| 11 | Time Exceed             |
| 12 | Parameter Problem       |
| 30 | Traceroute              |

**37 - 255**    **“reserved”**

## Kapitel 7

# Routing Protokolle

# Routing Information Protocol (RIP)

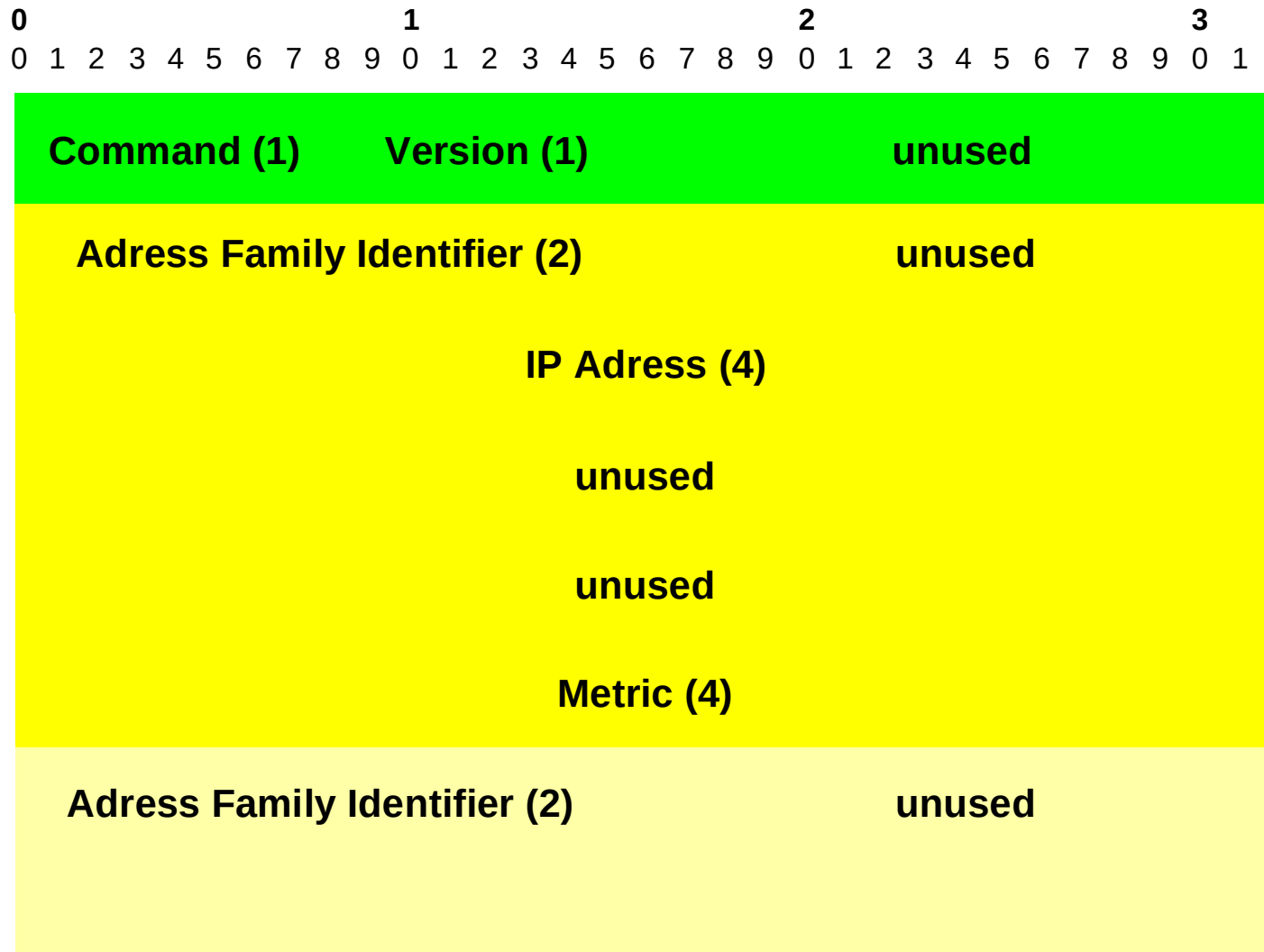
**RFC 1058**

- kein MIL-Standard
- setzt auf dem Datagram-Transport-Dienst des UDP auf
- **UDP-Port 520**
- stammt ursprünglich aus der XNS-Protokoll-Familie
- ist Bestandteil des BSD 4.3-UNIX (routed-Daemon)
- gehört zu der Familie der Distance-Vektor-Protokolle (Bellman-Ford-Algorithmus)

## RIP - Routing Tabelle/ - Routing Updates

- Regelmäßige Routing-Updates (alle 30 sec)
- Überprüfen, ob
  - neue “Distance” < alte “Distance”
  - ⇒ **JA:** Wert übernehmen - Update des Eintrags beendet
  - ⇒ **NEIN:** Wert beibehalten und
- Überprüfen, ob Routingupdate von dem Router kam, der den letzten Eintrag erstellt hat
  - ⇒ **JA:** Wert *auf jeden Fall* übernehmen (auch wenn größer) Update des Eintrags beendet
  - ⇒ **NEIN:** Update des Eintrags beendet

# RIP - Paketaufbau



## RIP - Paketaufbau

### Bedeutung der Felder

- Command Feld: 1 = Request  
2 = Response
  - Address Family Identifier: 2 = IP
  - IP-Adress: Ziel-Netz bzw. -Rechner
  - Metric (=Hops): Entfernung bis Ziel  
(Länge: 4 Bit = max. 15 Hops)
- Länge des Paketes: max. 512 Byte  
(~ 25 Info-Felder)

# Open Shortest Path First (Version 2)

## OSPF 2

RFC 1583

- Erweiterung von OSPF (RFC 1131)
- setzt auf IP auf (**IP-Protokoll-Nr.: 89**)
- Interior Gateway Protocol
- Link State Protocol
- Virtuelle Topologie (Autonomous System = AS)  
⇒ alle Router haben identische Datenbank
- Dynamisches Routing Protokoll

Kapitel 8

# Transmission Control Protocol (TCP)

# Transmission Control Protocol (TCP)

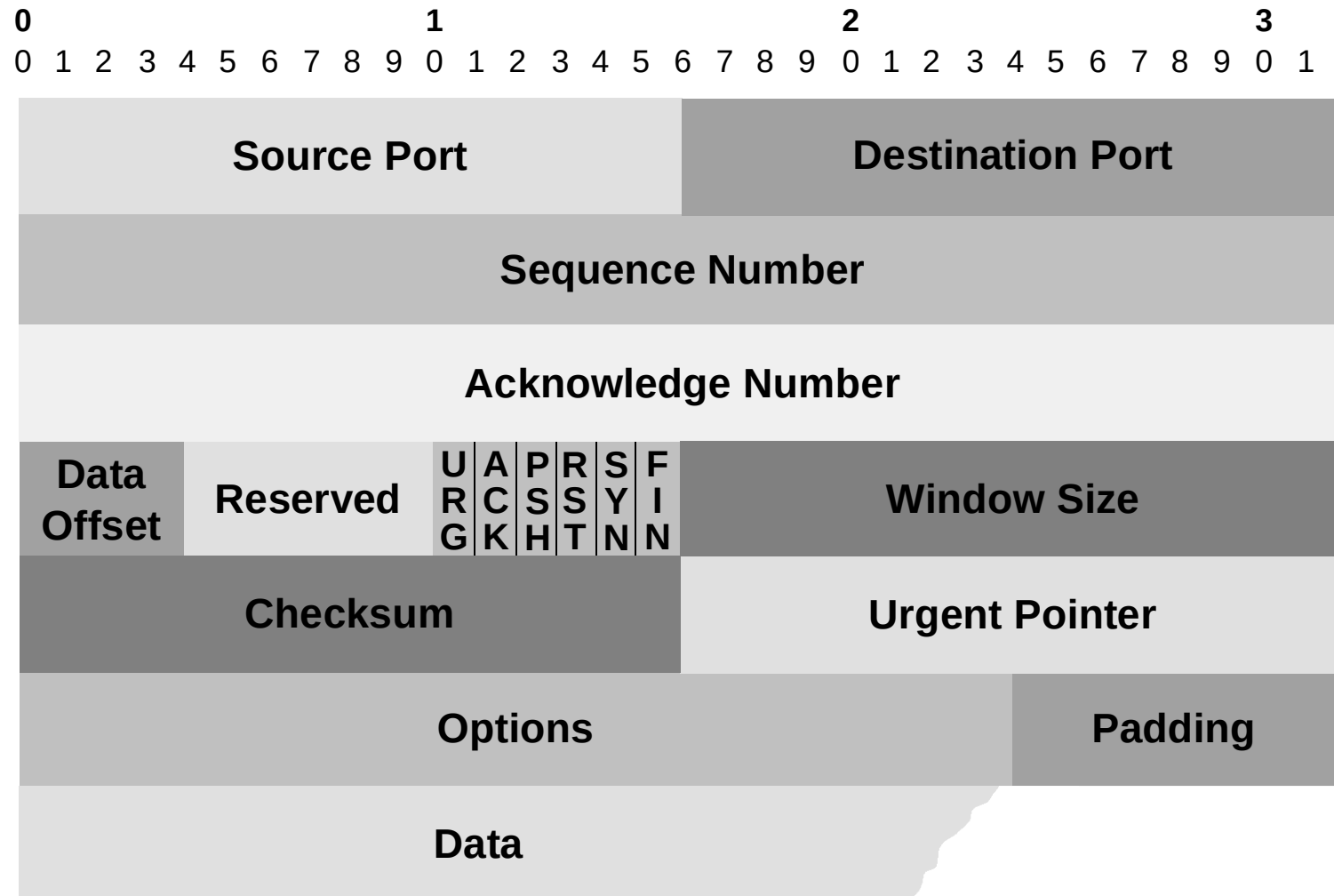
RFC 793 MIL-Std. 1778

- setzt direkt auf dem Internet Protokoll (IP) auf
- IP-Protokoll-Nr.: 06
- garantiert eine **fehlergesicherte, zuverlässige Transport-  
verbindung** zwischen zwei Rechnersystemen  
(End zu End Kontrolle)

## TCP - Eigenschaften

- Multiplexing
- End To End
- Verbindungsmanagement (Three-Way-Handshake)
- Flußkontrolle (Sliding-Window-Mechanismus)
- Zeitüberwachung
- Fehlerbehandlung

## TCP - Header



## TCP - Well-Known-Ports (Auswahl I)

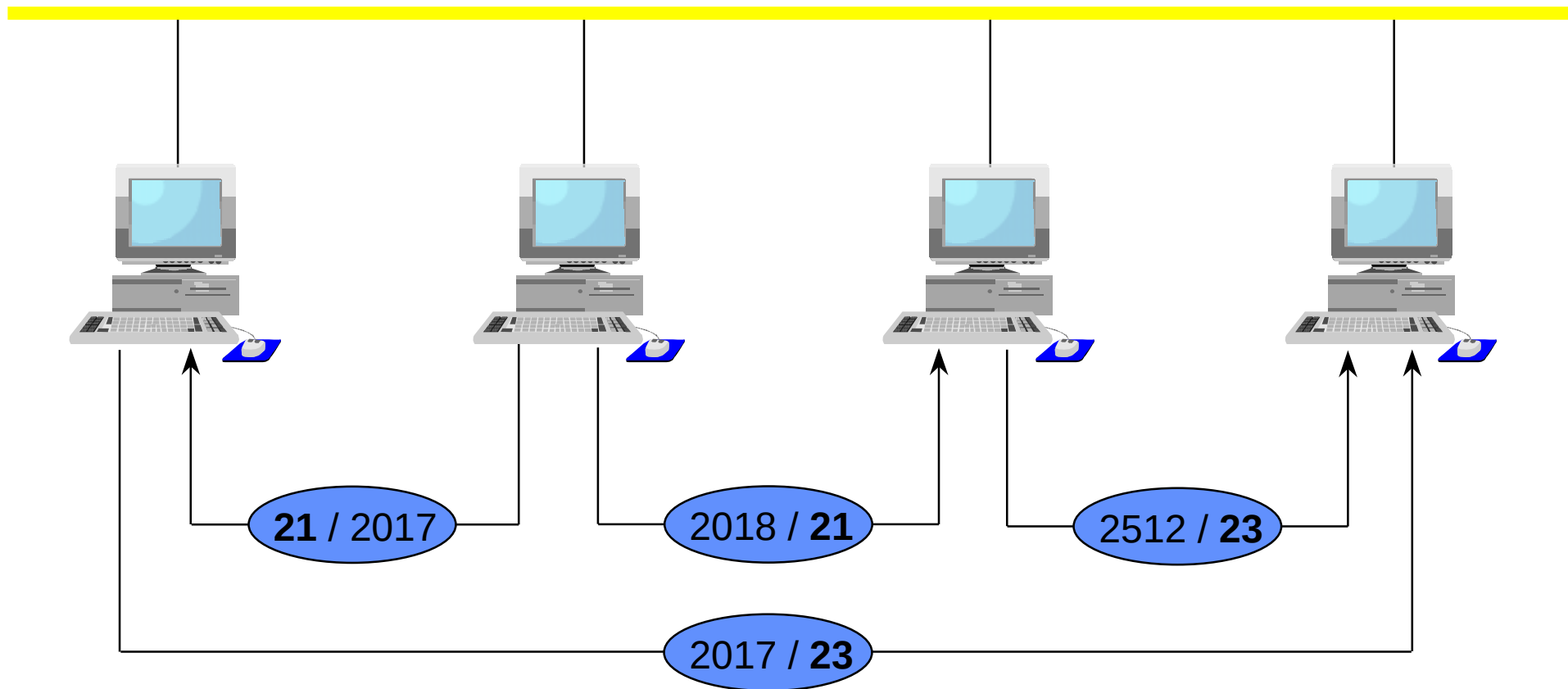
|               |              |                                      |
|---------------|--------------|--------------------------------------|
| 20            | FTP-Data     |                                      |
| 21            | FTP          | (Steuerleitung)                      |
| 23            | TELNET       |                                      |
| 25            | SMTP         | (Simple Mail Transfer Protocol)      |
| 43            | nicname      | (Who Is)                             |
| 53            | domain       | (DNS)                                |
| 66            | sql*net      | (Oracle SQL*NET)                     |
| 67/68         | BOOTP        | (Server/Client)                      |
| 70            | gopher       |                                      |
| 80            | WWW-HTTP     |                                      |
| 111           | sunrpc       | ("NFS" - SUN Remote Procedure Calls) |
| 137/ 138/ 139 | netbios      | (name-/ datagram-/ session service)  |
| 161/ 162      | SNMP         | (SNMP/ SNMP-Trap)                    |
| 445           | microsoft-ds |                                      |
| 512/ 514      | exec/ cmd    | (rexec/ rsh)                         |

## TCP - Well-Known-Ports (Auswahl II)

### Besonderheiten

|                 |               |                                                |
|-----------------|---------------|------------------------------------------------|
| 513/ <b>tcp</b> | login         | (rlogin; <i>nur</i> <b>TCP</b> -Port!)         |
| 513/ <b>udp</b> | who           | (rwho/ ruptime; <i>nur</i> <b>UDP</b> -Port!)) |
| 1352            | Lotus Notes   |                                                |
| 1416            | Novell LU 6.2 |                                                |
| 1525            | orasrv        | (Oracle)                                       |
| 1527            | tlisrv        | ( " )                                          |
| 1529            | coauthor      | ( " )                                          |
| 1986-1999       | cisco         | (u.a. licensmanager, snmp-rcp-port)            |
| 1989            | mshnet        | (MHSnet system)                                |
| 2784            | www-dev       | (world wide web - development)                 |

## TCP - Multiplexmechanismus (2)



## TCP - Verbindungsaufbau (Three-Way-Handshake)

**A****B**

Verbindungsaufbauwunsch (SYN = 1)

*Sequenz-Nr. = I*



Bestätigung + Verbindungsaufbauwunsch (ACK = 1, SYN = 1)

*ACK-Nr. = I + 1*

*Sequenz-Nr. = J*



Bestätigung

*ACK-Nr. = J + 1*

*Sequenz-Nr. = I + 1*

(ACK = 1)

*Datenübertragung*



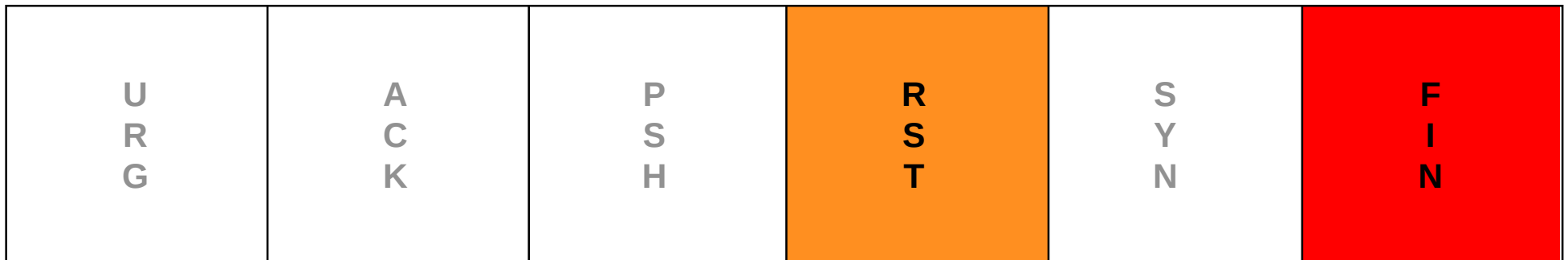
## TCP - Flags (SYN, ACK)



**SYN** zeigt an, daß eine Verbindung aufgebaut (synchronisiert) werden soll

**ACK** bestätigt den Empfang von Daten (acknowledgement)

## TCP - Flags (RST, FIN)



**RST** zeigt an, daß der Sender die Verbindung abbauen will (reset)

**FIN** bestätigt, daß die Verbindung endgültig abgebaut ist (final) und keine weiteren Daten folgen

## TCP - Flags (PSH, URG)



**PSH** teilt dem Empfänger mit, daß die Daten sofort an die höhere Schicht weitergereicht werden müssen (push)

**URG** zeigt an, daß der “**Urgent-Pointer**” berücksichtigt werden muß. Dieser kennzeichnet das Ende von Vorrangsdaten

## TCP - Verbindungsmanagement

- **Daten können beim Transport**
  - ➔ verloren gehen
  - ➔ verfälscht werden (defekte Pakete)
  - ➔ durcheinander gebracht werden (falsche Reihenfolge)
  - ➔ verzögert werden
  - ➔ dupliziert werden

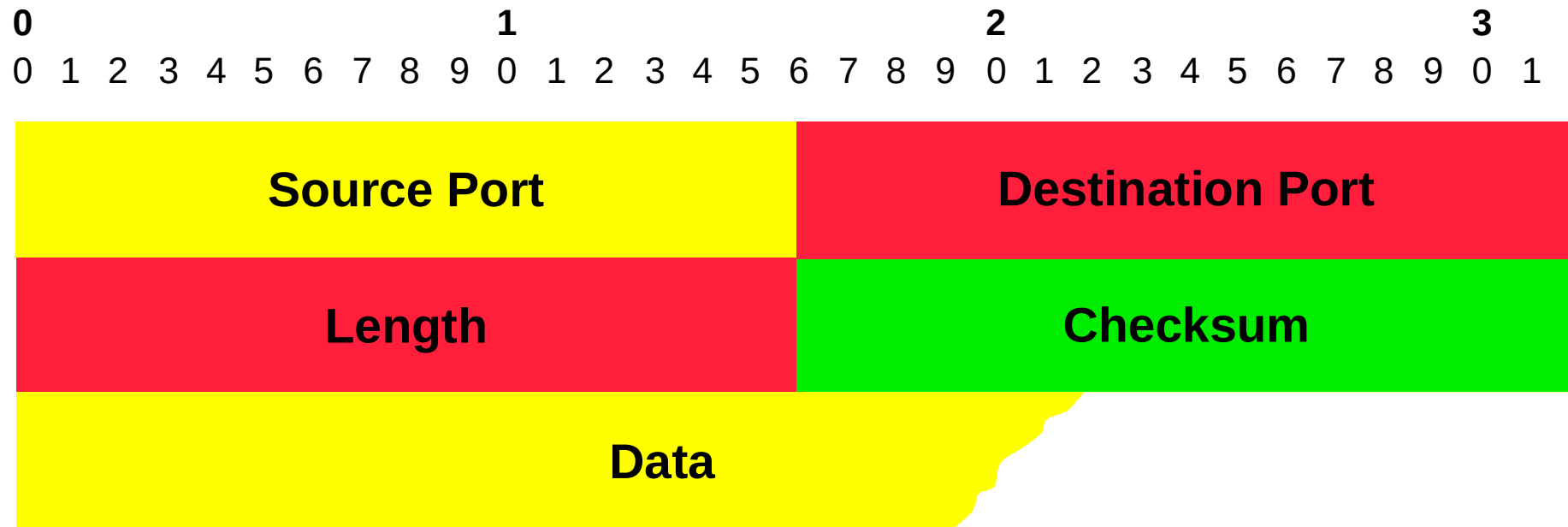
## Wichtige TCP - Timer

- **Retransmission Timer**
  - nach Ablauf werden Daten neu geschickt
- **Give Up Timer**
  - max. Zeit, die der Sender bis zur Bestätigung seiner Pakete wartet
- **Reconnection Timer**
  - min. Zeit zwischen Abbau und Aufbau einer Verbindung
- **Retransmit-Syn Timer**
  - min. Zeit zwischen erfolglosem Verbindungsaufbau und erneutem Connection Request
- **Window Timer**
  - max. Zeit zur Umstellung der Window-Size

# Kapitel 9

# User Datagram Protocol (UDP)

## UDP - Header



  = obligatorisch

# User Datagram Protocol (UDP)

RFC 768

- Kein MIL-Standard
- setzt direkt auf dem Internet Protokoll (IP) auf
- IP-Protokoll-Nr.: 17
- **Datagram Service** zwischen Rechnern  
(keine virtuelle Verbindung)

## UDP - Eigenschaften

- **Transport Protokoll ohne “End to End”- Kontrolle**
  - **Kein Verbindungsmanagement**  
(keine aktiven Verbindungen!)
  - **Keine Flußkontrolle**
  - **Kein Multiplexmechanismus**
  - **Keine Zeitüberwachung**
  - **Keine Fehlerbehandlung**

## Dienste auf UDP

| Dienst          | UDP-Portnummer |
|-----------------|----------------|
| IEN 116         | 42             |
| DNS             | 58             |
| RIP             | 520            |
| BootP           | 67, 68         |
| TFTP            | 69             |
| sunrpc (NFS)    | 111            |
| SNMP/ SNMP-TRAP | 161/ 162       |

## Vergleich der Layer-4-Protokolle TCP und UDP

| Eigenschaft                         | TCP          | UDP         |
|-------------------------------------|--------------|-------------|
| Ende zu Ende Kontrolle              | ja           | nein        |
| Zeitüberwachung der Verbindung      | ja           | nein        |
| Flow-Controle (über das Netz)       | ja           | nein        |
| Reihenfolgerichtige Übertragung     | ja           | nein        |
| Erkennung von Duplikaten            | ja           | nein        |
| Fehlererkennung                     | ja           | einstellbar |
| Fehlerbehebbug                      | ja           | nein        |
| Addressierung der höheren Schichten | ja           | ja          |
| Three-Way-Handshake                 | ja           | nein        |
| Größe des Headers                   | 20 - 60 Byte | 8 Byte      |
| Geschwindigkeit                     | langsam      | schnell     |
| Belastung der Systemressourcen      | normal       | gering      |

# Kapitel 10

# Telekommunikations Network

# (TELNET)

## TELNET

RFC 854 MIL-Standard 1782

- Setzt auf dem gesicherten Transport Service von TCP auf
- TCP/UDP Port 23
- Remote Login-Dienst

## **TELNET - Problematik**

- **Vielzahl von Terminal-Typen**
- **Verbindung zu Rechnern verschiedener Hersteller**
- **Unterschiedliche Übertragungseigenschaften**

## TELNET - Arbeitsweise

### Lösung des Problems

- **Beim TELNET wirken drei Funktionsgruppen zusammen:**
  - Network Virtual Terminal (NVT)
  - TELNET-Kommandos
  - Optionen
- **TELNET verwendet keinen eigenen *Protokoll-Header*, sondern verpackt die Steuerzeichen in dem Datenstrom**
  - Das Interpret As Command (**IAC**) (Hex FF) wird unmittelbar vor die Kommandodaten gestellt

## TELNET - Network Virtual Terminal

- Fiktive Ein-/Ausgabe-Einheit mit bekannten Eigenschaften
- “Drucker” zur Anzeige von Ausgabedaten
- Tastatur zur Dateneingabe
- (per default) 7 Bit ASCII in 8 Bit Wort
- Unbegrenzte Zeilen- und Seitenlänge
- Steuerfunktionen
- “Drucker” für Steuerzeichen

## TELNET - Optionen

- |                          |            |            |
|--------------------------|------------|------------|
| • Extended ASCII         | (dez. 17)  | (RFC 698)  |
| • Binary Transmit        | (dez. 0)   | (RFC 856)  |
| • (local) Echo           | (dez. 1)   | (RFC 857)  |
| • Suppress GA            | (dez. 3)   | (RFC 858)  |
| • Terminal Speed         | (dez. 32)  | (RFC 1079) |
| • Terminal Type, X.3 PAD | (dez. 24)  | (RFC 1091) |
| • Extended Options List  | (dez. 255) | (RFC 861)  |

# Kapitel 11

# File Transfer Protocol

# (FTP)

## **File Transfer Protocol (FTP)**

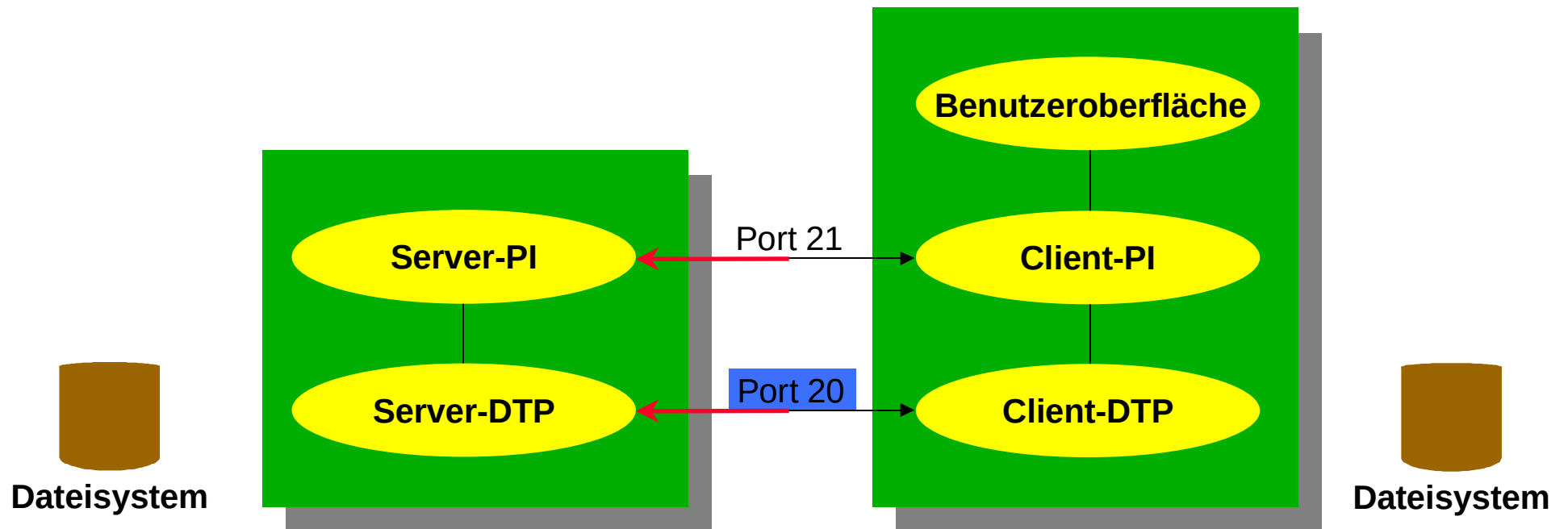
RFC 959 MIL-Standard 1780

- **Setzt auf dem gesicherten Transport Service von TCP auf**
- **TCP/UDP Port 20 und 21**
- **File-Transfer-Dienst**

## FTP-Session

- **Aufbau einer Steuerleitung/-verbindung (Port 21)**
- **Austausch von Befehlen und Parametern**
  - **Aufbau einer Datenleitung/ -verbindung (Port 20)**
  - **Datenübertragung**
  - **Abbau der Datenverbindung**
- **Abbau der Steuerleitung**

## Das FTP - Modell



PI = Protocol Interpreter  
DTP = Data Transfer Process

## Wichtige FTP - Befehle

- **dir, ls** Inhaltsverzeichnis anzeigen
- **cd** Inhaltsverzeichnis wechseln
- **pwd** Name des aktuellen Inhaltsverz. anzeigen
- **bin bzw. ascii**  
Übertragungsmodus binär/ ascii
- **hash** Übertragung grafisch darstellen (mit #####)
- **get bzw. put (mget bzw. mput)**  
eine Datei (ein komplettes Verzeichnis) holen  
bzw. senden

**Kapitel 12**

**Simple Mail Transfer Protocol  
(SMTP)**

# Simple Mail Transfer Protocol (SMTP)

RFC 821 MIL-Standard 1781

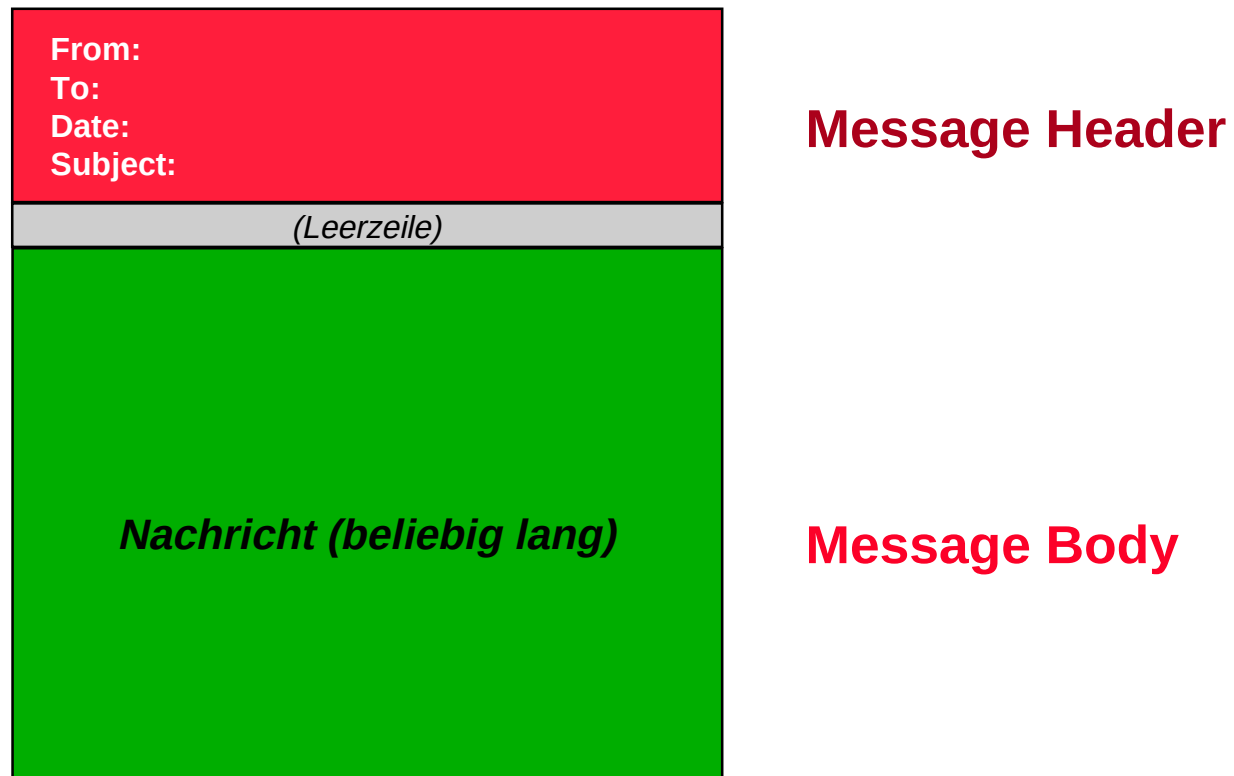
- Setzt auf dem gesicherten Transport Service von TCP auf
- TCP/UDP Port 25
- E-Mail-Dienst

## SMTP - Message-Format (Beschreibung)

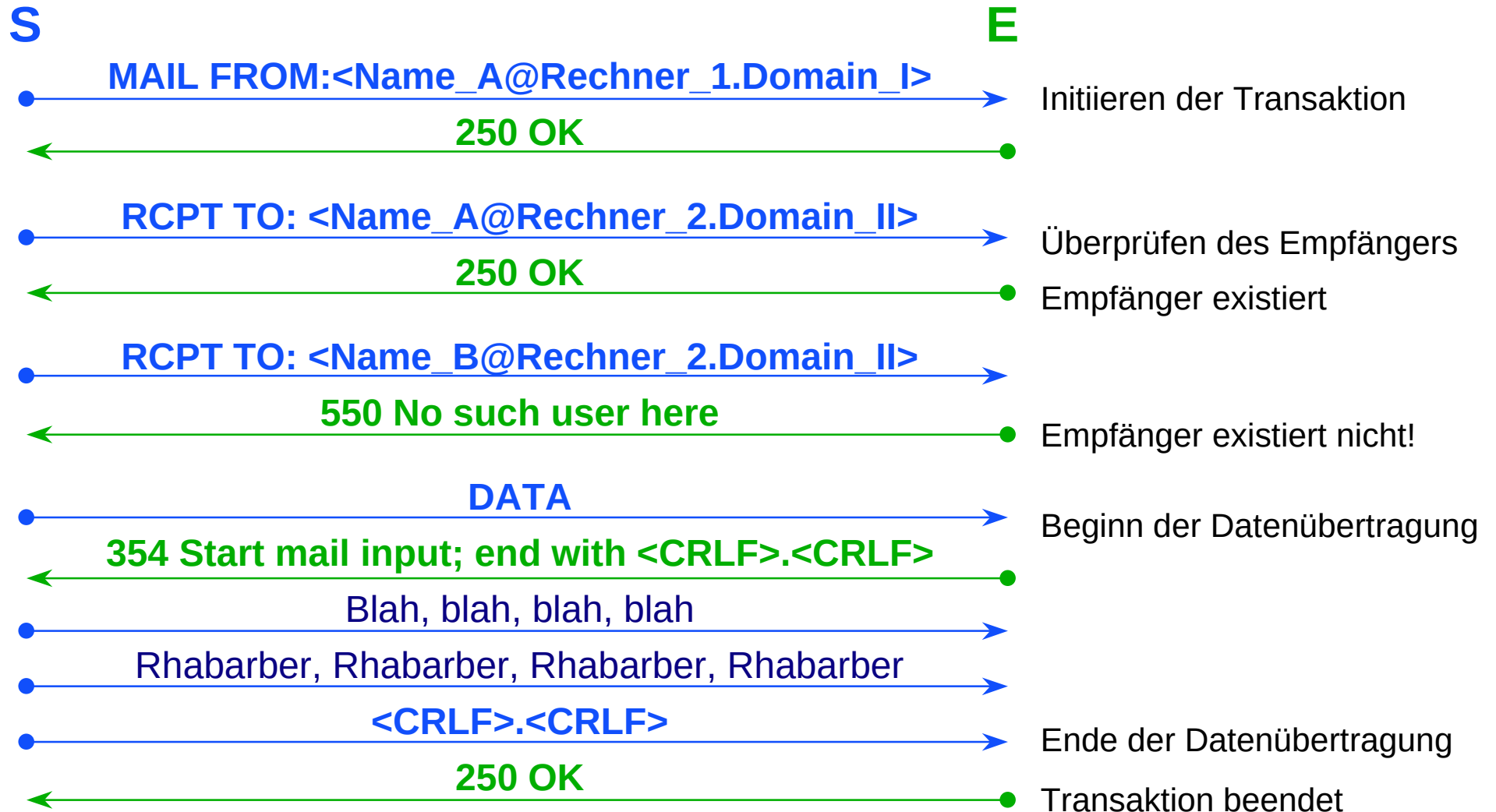
- definiert in RFC 822 (“822-Message-Format”)
- verwendet nur 7-Bit-ASCII-Zeichensatz<sup>\*)</sup>
- Message setzt sich zusammen aus Header und Body

<sup>\*)</sup> Zur Übertragung von 8 Bit-Zeichen werden deshalb 8 Bit-Verschlüssler wie „MIME“ oder „UUENCODE“ benötigt!

## SMTP - Message-Format (Grafik)



## SMTP - Übertragung



# Kapitel 13

# Name-Services

## **Name-Services**

- dienen der Zuordnung Rechnername → IP-Adresse
- werden im einfachsten Fall durch eine lokale Datei (/etc/hosts, hosts.txt etc.) realisiert
- können, je nach Ausprägung, recht komplex aufgebaut sein und vielartige Informationen weiterreichen (DNS)

# Domain Name System/ Service (DNS)

## DNS

empfehlenswert!

**RFC 1033 Administrators Operations Guide**

**RFC 1034 Concepts and Facilities**

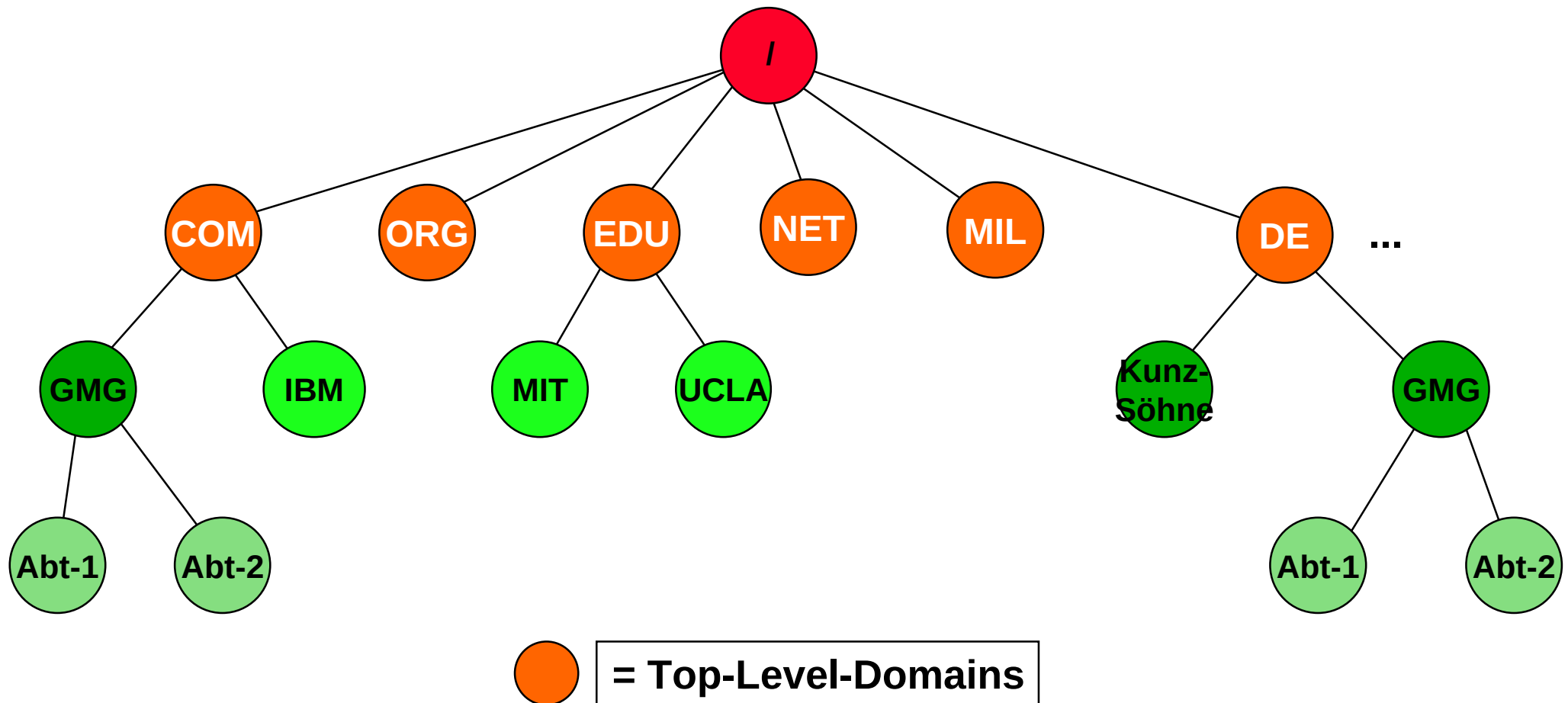
**RFC 1035 Implementation and Specification**

- **kein MIL-Standard**
- **setzt auf dem Datagramm-Transport-Service von UDP auf**
- **UDP/TCP Port 58**
- **Zuordnen von Hostnamen zu IP-Adressen**

## DNS - Funktionsweise

- basiert auf der Idee einer verteilten Datenhaltung
- basiert auf einem hierarchischen Modell
- kennt verschiedene DNS-Servertypen
- verfügt, neben der Namen-IP-Zuordnung, über zusätzliche - teilweise optionale - Möglichkeiten

## DNS - Funktionsweise (hierarchisches Modell)



## DNS - Servertypen

- **Primary Name Server (Master)**
  - Enthält Datenbank mit autorisierten Daten
  - Ort der Datenpflege
- **Secondary Name Server (Slave)**
  - Enthält Datenbank mit autorisierten Daten
  - Holt sich regelmäßig Updates von Master
- **Caching Server**
  - Merkt ("cacht") sich nur Daten (nicht autorisiert)
  - verwirft "gecachte" Daten nach vorgegebener Zeit (TTL-Feld mit 32 Bit Länge)

## **DNS - Einschränkungen**

- **Namen (Labels): max. 63 Byte**
- **Rechnernamen: max. 255 Byte**
- **TTL: positive Werte einer vorzeichen-behafteten 32 bit Integer Zahl**
- **UDP Nachricht: max. 512 Byte**

## Kapitel 14

# UDP Bootstrap Protocol (BootP)

---

# Dynamic Host Configuration Protocol (DHCP)

# BOOTP

**RFC 951 und RFC 1497, 1532 (Vendor Specific Extensions)**

- kein MIL-Standard
- setzt auf dem Datagramm-Transport-Service von UDP auf
- UDP/TCP Port 67 (Client → Server)  
68 (Server → Client)
- Umwandlung von Ebene 2-Adressen in IP-Adressen
- Übertragen von Informationen, die zum Booten notwendig sind (Vendor Specific Extensions)

## **BOOTP - Funktionsweise**

- **BOOTP-Request erfolgt gerichtet oder per IP-Broadcast**
- **wird ein BOOTP-Request nicht beantwortet, erfolgt eine erneute Anfrage**
- **um das Netzwerk nicht mit (unnötigen) Paketen zu überschütten (“flooding”), wird eine dem Ethernetverhalten ähnliche Backoff-Strategie empfohlen.**
- **durch das “seconds”-Feld, kann eine Antwortpriorität erreicht werden**
- **das Booten über Router (“Gateways”) hinweg ist optional und benötigt einen BOOTP-Relay-Agent**

## **BOOTP - Vendor Specific Area (Auswahl)**

- **Time-of-Day**      **aktuelle Zeit**
- **Subnet-Mask**      **IP-Subnetz-Maske**
- **Router**      **IP-Adresse von Routern**
- **Time-Server**      **IP-Adresse eines Time-Servers**
- **IEN116-Server**      **IP-Adresse eine IEN 116 Name-Servers**
- **Domain Server**      **IP-Adresse eines Domain-Name-Servers**
- **LPR-Server**      **IP-Adresse eines BSD-Print-Servers**
- **Hostname**      **Name des Client (local station)**
- **Boot Size**      **Größe des Boot-Files (in 512 Byte Blocks)**
- **Extensions Path**      **Definiert TFTP-File, das als VSA interpretiert wird**
- **End (255h)**      **Ende der Vendor Specific Area**

# DHCP

## RFC 2131

- nutzt BOOTP
- Paketaufbau identisch zu BOOTP
  - ◆ Ausnahme:
    - “Vendor Specific Extensions” → “Options” (RFC 2132)
      - Minimumlänge des VSA-Feldes: 312 Byte
      - definiertes “Magic Cookie” (99.130.83.99)
- automatisches Zuweisen von IP-Adressen auf Zeit bzw. unendlich (32 Bit-Wort = 1 sec - 136 Jahre)
- manuelle Vergabe von IP-Adressen möglich
- DHCP-Server muß BOOTP-Clients bedienen können

## Automatische Adreßvergabe durch DHCP

- Client sucht DHCP-Server; ggf. Vorschläge” für Netzwerk-Adresse und Gültigkeitsdauer (DHCP**DISCOVER**)
- DHCP-Server antworten mit IP-Adresse (DHCP**OFFER**)
- Client sucht sich eine Antwort aus und antwortet allen Servern (DHCP**REQUEST**) - “Server Identifier Option” muß gesetzt sein
- Der ausgesuchte Server reserviert die vorgeschlagene Adresse und schickt Konfigurations-Parameter - ggf. vorher Test der Adresse durch ICMP-Echo Request (DHCP**ACK**)

Alle anderen Server wissen, daß ihr “Angebot” abgelehnt wurde und die vorgeschlagene IP-Adresse wieder frei verfügbar ist

# Kapitel 15

# Trivial File Transfer Protocol (TFTP)

## **Trivial File Transfer Protocol (TFTP) RFC 783**

- **kein MIL-Standard**
- **setzt auf dem Datagramm-Transport-Service von UDP auf**
- **UDP/TCP Port 69**
- **einfacher File-Transfer-Dienst ohne Login-Prozedur (“Poor Man’s File Transfer”)**
- **wird (meist) für Netz-Boot-Vorgänge eingesetzt**

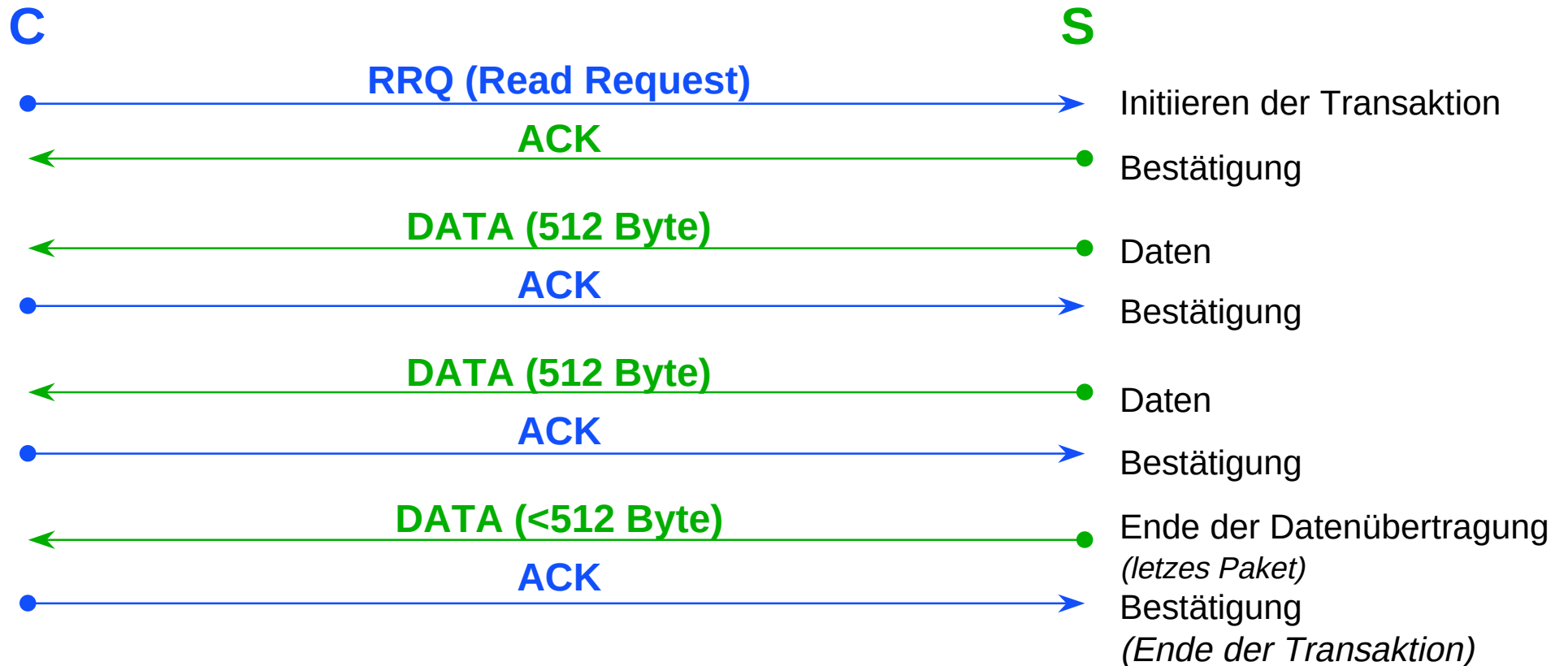
## TFTP - Funktionsweise

- **TFTP verfügt über fünf Funktionen:**
  - **Read Request (RRQ):**
    - fordert File von Remote-Rechner an
  - **Write Request (WRQ):**
    - sendet File zu Remote-Rechner
  - **Data (DATA):**
    - kennzeichnet den eigentlichen Datenstrom
  - **Acknowledgement (ACK):**
    - bestätigt empfangene Pakete
  - **Error (ERROR):**
    - zeigt Übertragungsfehler an

## TFTP - Übertragungsmechanismus

- Verbindungsaufbau mit RRQ bzw. WRQ
- Pakete werden in festem Format (512 Byte) übertragen
- Pakete < 512 Byte zeigen Ende der Übertragung an
- jedes gesendete Paket wird einzeln bestätigt
- ERROR verursacht Übertragungsabbruch - kein Retransmit!

## TFTP - Übertragungsmechanismus



**Kapitel 16**

**Die “R”-Utilities**

**rlogin, rcp, rsh/rexec**

## Die “R” Utilities (rlogin, rcp, rsh/ rexec)

- setzen auf dem gesicherten Transport Service von TCP auf
- TCP/UDP Port 512 (rsh), 513 (rlogin), 514 (rexec)
- erlauben ein *login* und ein *copy* (rcp), so wie das Ausführen fremder Dateien (*shell-scripts*) auf einem fremden Rechner, **ohne aktive Identifizierung** und Authentifizierung

**Kapitel 17**  
**Network File System**  
**(NFS)**

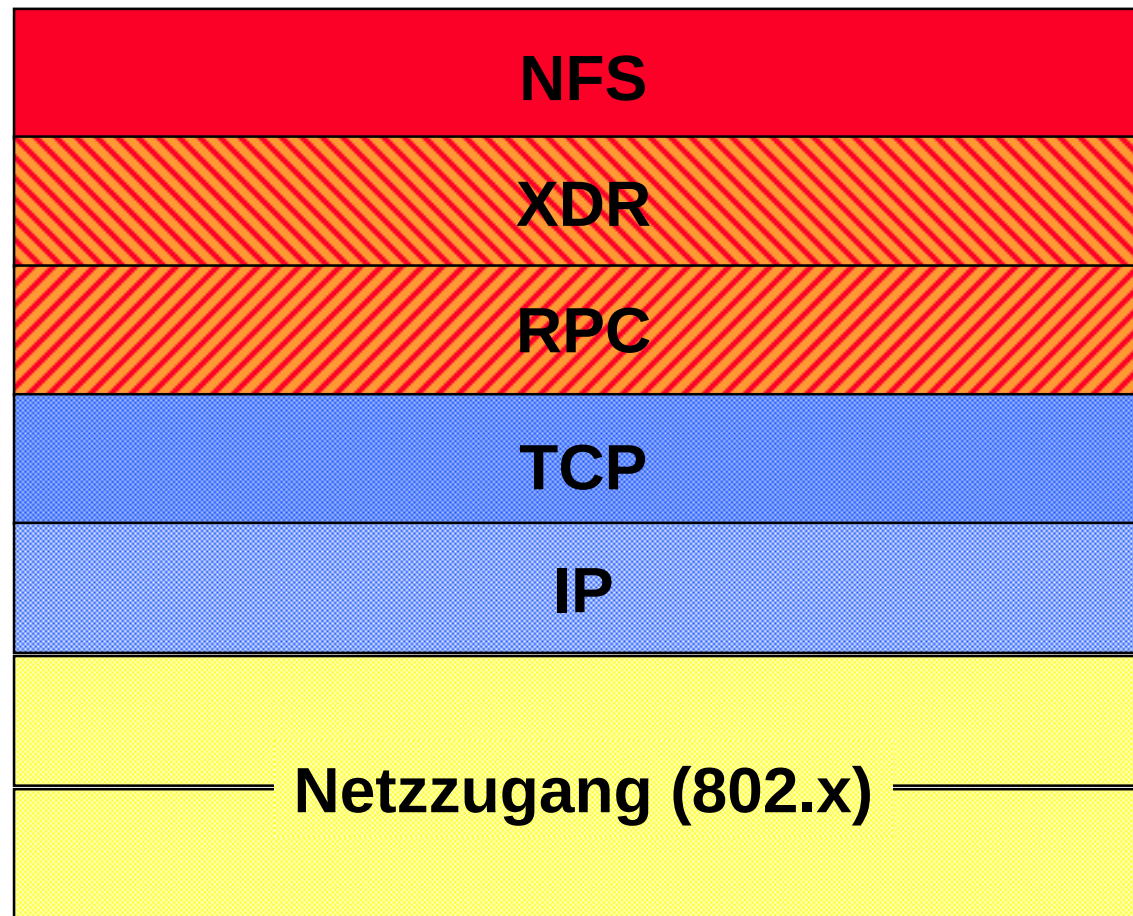
## Network File System (NFS)

RFC 1094 (Version 2)

RFC 1813 (Version 3)

- kein MIL-Standard
- setzt auf **XDR** (“**E**xternal **D**ata **R**epresentation” - RFC 1014) und den SUN-**RPC**s (RFC 1057) auf
- UDP/TCP Port 111 (RPC)
- Erlaubt den Zugriff auf ein “Netzwerklaufwerk” mit 80% der lokalen Performance
- es handelt sich um eine “stateless” Verbindung
- **neu:** **Web-NFS** (RFC 2054, 2055)

## NFS im OSI-Modell



# Kapitel 18

# WWW, HTML und HTTP

## WWW, HTML und HTTP (Begriffserklärungen)

- **WWW**    World Wide Web (Anwendung, Dienst)
- **HTML**    Hypertext Markup Language (Programmiersprache)
- **HTTP**    Hypertext Transfer Protocol (Dienst, Protokoll)
- **URI**      Unified Ressource Identifier (Verweis auf Dokument)
- **URL**      Unified Ressource Locator  
(Verweis auf Dokument incl. **Protokollangabe**)

Bsp.: <http://home.t-online.de/home/Gerhard.Glaser>

# Hypertext Transfer Protocol (HTTP)

RFC 1945 HTTP 1.0 (Mai 1996)

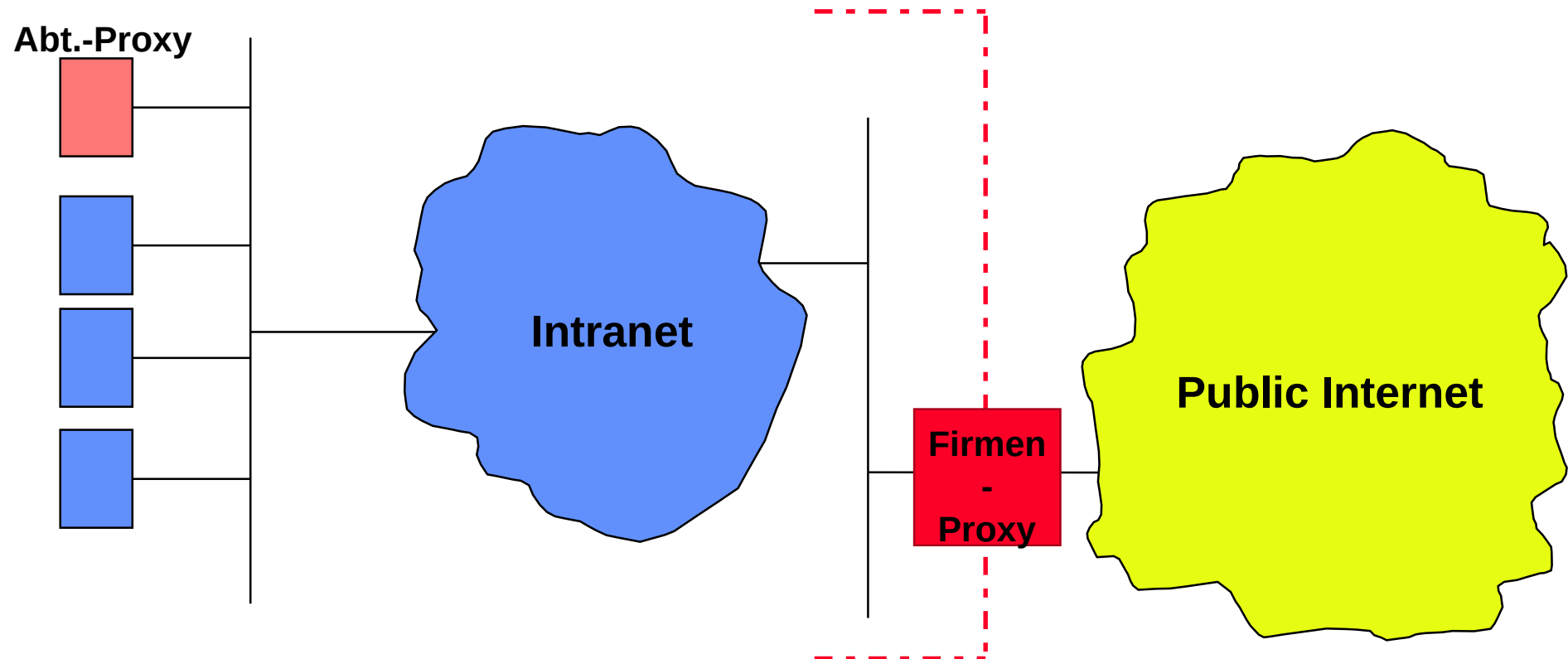
RFC 2068 HTTP 1.1 (Januar 1997)

- setzt auf dem gesicherten Transport Service von TCP auf
- TCP-Port 80 (veränderbar)
- basiert auf einem Request-/ Response-Verfahren zur Abfrage von Dokumenten
  - ① Verbindungsaufbau
  - ② Anforderung (Request)  
URI, protocol version, request modifier, client information
  - ③ Antwort (Response)  
message protocol version, success-/ error-code, server information, "data"
  - ④ Verbindungsabbau

## Proxy-Server

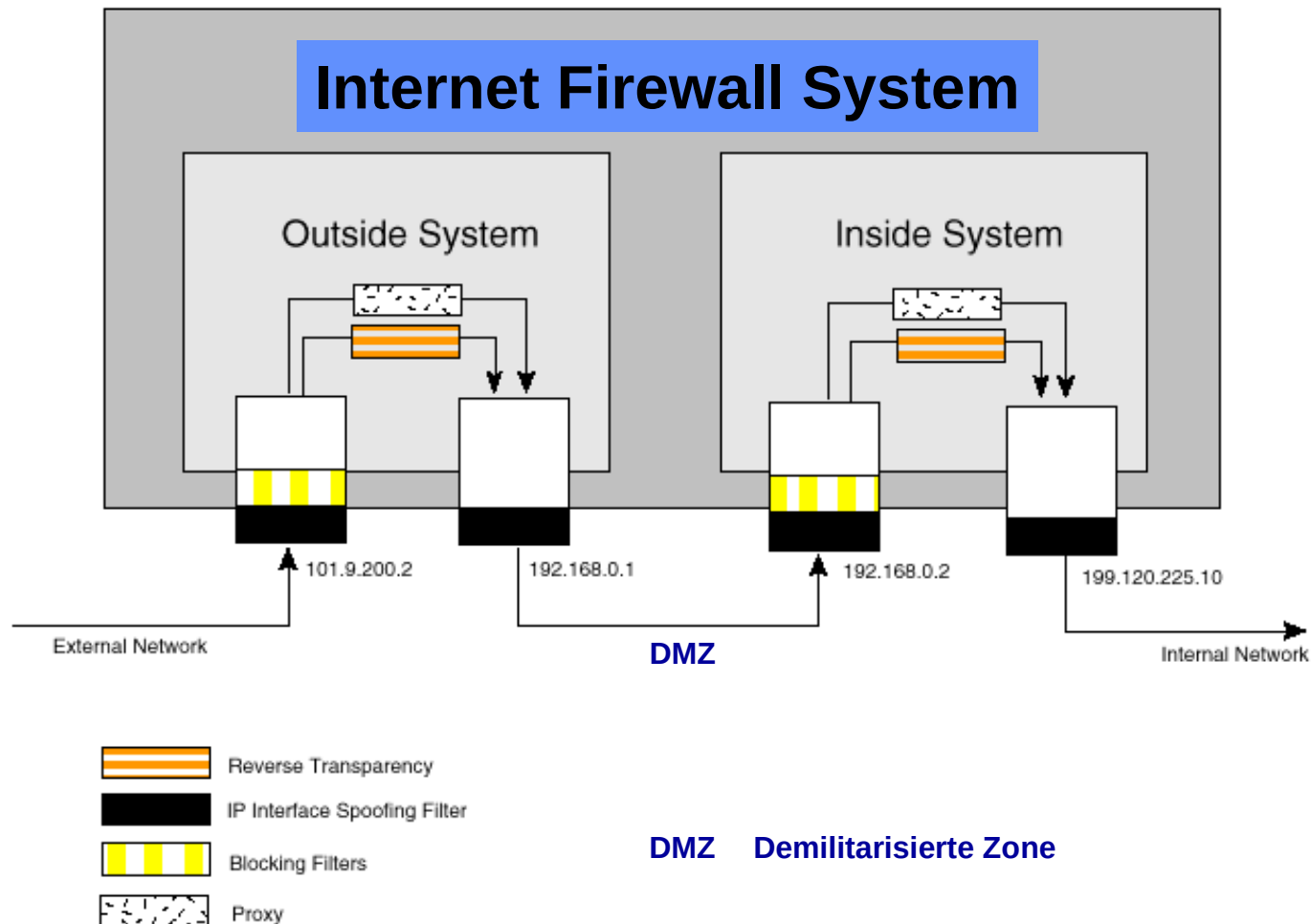
- Ein zwischengeschaltetes Programm (Rechner), das sowohl als Client als auch als Server arbeitet
- Anfragen werden bearbeitet ggf. übersetzt und dann weitergereicht
- Proxies dienen dazu, Zugriffe zu steuern (“Firewall”) und Anfragen für nicht unterstützte Protokolle weiterzureichen
- Die physikalische Ausprägung (Rechner) verfügt i.a. noch über eine Caching-Funktionalität
- Können kaskadiert werden

## Proxy-Server



# Firewall

In Bound Packet Flow



**Kapitel 19**

**Simple Network Management  
Protocol  
(SNMP)**

# Simple Network Management Protocol (SNMP)

RFC 1155 - 1157 (SNMP)

RFC 1441 - 1452 bzw. 1902 - 1908 (SNMP v2)

- kein MIL-Standard
- setzt auf dem Datagram-Transport-Service von UDP auf
- UDP/TCP Port 161 und 162 (für Traps)
- dient zur Vereinheitlichung der erfaßten Daten (Variablen) und zur Übertragung derselben
- erlaubt herstellerspezifische “Ergänzungen”

## SNMP v2 - gültige RFCs

- RFC 1441 Introduction to SNMP v2
- RFC 1442/ 1902 SMI (Structure of Management Information) for SNMP v2
- RFC 1443/ 1903 Textual Conventions for SNMP v2
- RFC 1444/ 1904 Conformance Statements for SNMP v2
- RFC 1445 Administrative Model for SNMP v2
- RFC 1446 Security Protocols for SNMP v2
- RFC 1447 Party MIB for SNMP v2
- RFC 1448/ 1905 Protocol Operations for SNMP v2
- RFC 1449/ 1906 Transport Mappings for SNMP v2
- RFC 1450/ 1907 MIB for SNMP v2
- RFC 1451 Manager to Manager MIB
- RFC 1452/ 1908 Coexistence between SNMP v1 and SNMP v2

## SNMP - weitere wichtige RFCs (1)

- RFC 1213 MIB II
- RFC 2011 - 2013 MIB II (Update zu 1213)
- RFC 1515 MAU MIB
- RFC 1573 IF-Group
- RFC 1650 Ether-like MIB (Ethernet/ 802.3)
- RFC 1694 SMDS MIB
- RFC 1695 ATM
- RFC 1696 Modem MIB
- RFC 2127 ISDN MIB (März 97)
- RFC 2108 Repeater MIB
- RFC 1493 Bridge-MIB
- RFC 1749 Station Source Routing MIB
- RFC 1850 OSPF MIB

## SNMP - weitere wichtige RFCs (2)

- RFC 1513      Token Ring RMON
- RFC 1748      Token Ring MIB
- RFC 1749      Station Source-Routing MIB
- RFC 1666      SNA NAU MIB
- RFC 1747      SNA SDLC MIB
- RFC 1559      DECnet MIB (27.12.93)
- RFC 1742      Apple Talk MIB
- RFC 1514      Host Ressources MIB
- RFC 1565      Network Service Monitoring MIB
- RFC 1566      Mail Monitoring MIB
- RFC 1611      DNS-Server MIB
- RFC 1628      UPS MIB
- RFC 1757      RMON MIB

# Kapitel 20

# Trouble-Shooting

## Trouble-Shooting - Befehle (1)

- **arp** **Zeigt/ modifiziert den ARP-Cache**
  - **-a** Darstellen aller Einträge
  - **-d** Löschen von Einträgen
  - **-s** Setzen von Einträgen
  - **-s PUB** Antwortet auf Anfragen

## Trouble-Shooting - Befehle (2)

- **netstat** **Zeigt eine (Karten-) Statistik**
  - **-a** alle Verbindungen
  - **-e** Ebene 2 (Ethernet-) Statistik
  - **-p [Protokoll]** über TCP oder UDP
  - **-r** **Routingtable**
  - **-s** Statistik (ausführlich)
  - **interval [sec]** automatischer Update (in sec)

## Trouble-Shooting - Befehle (3)

- **route**                      Zeigt/ modifiziert die Routingtabelle und routingspezifische Einträge

**Syntax: route [*command* [dest.] [MASK netmask] [GW]]**

- *command*                  PRINT
- ADD
- DELETE
- CHANGE
- *dest.*                      Zieladresse für die der Eintrag gelten soll
- *MASK*                      Subnetzmaske
- *GW*                        Gateway (Router) für dest.

## Trouble-Shooting - Befehle (4)

- **ping**      **Testet die Erreichbarkeit eines IP-Rechners**

- -t unbegrenzt
- -n *<count>* Anzahl von Pings
- -l *<size>* Paketgröße (Vorsicht!)
- -f don't fragment
- -i *<TTL>* TTL-Wert setzen/ vorgeben
- -v *<TOS>* TOS-Wert setzen
- -j *<host-list>* Loose Source Routing
- -k *<host-list>* Strict Source Routing
- -w *<timeout>* Wartezeit in ms
- -R trace route

## Trouble-Shooting - Befehle (5)

- **tracert**    **trace route**

**Syntax:** **tracert** [-d] [-h *max\_hops*] [-j *host-list*] [-w *ms*] **Name**

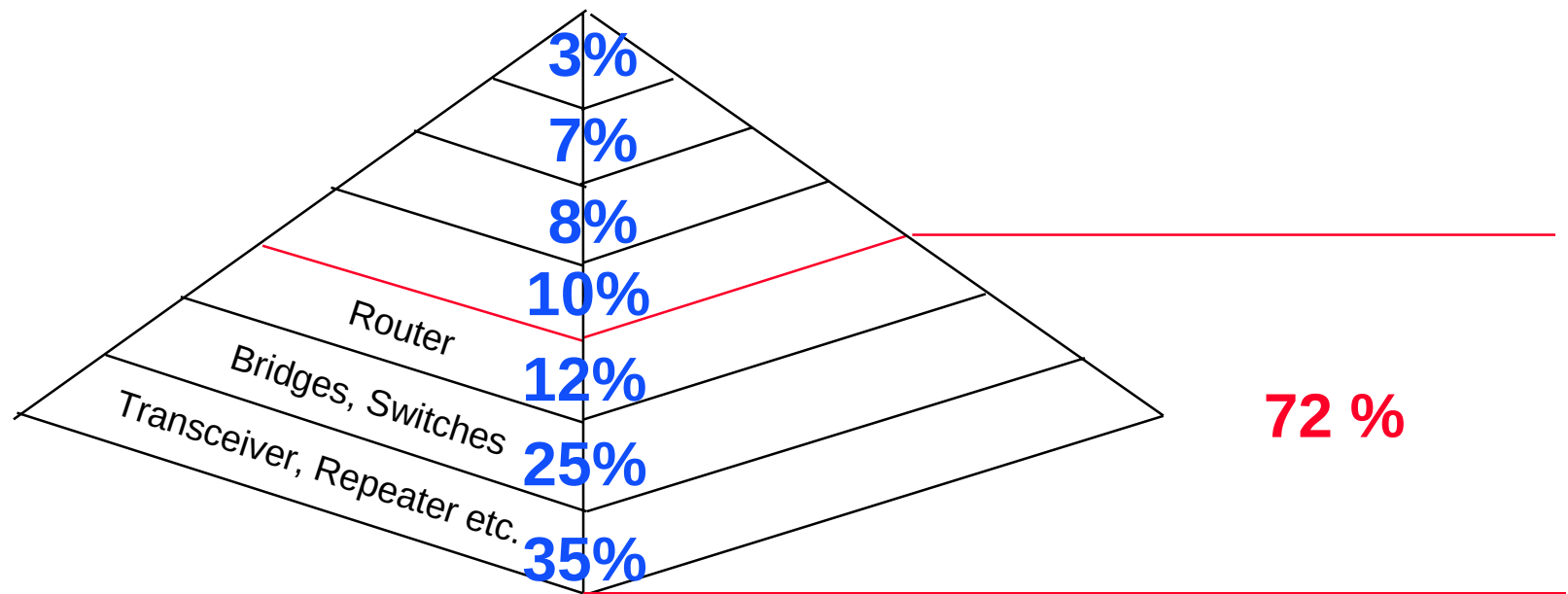
- -d    keine Hostnamen (nur IP-Adressen) anzeigen
- -h    TTL-Feld
- -j    Loose Source Routing
- -w    Time Out (in ms)

## Probe vs. Analyzer

- fest installiert
- auf eine Topologie festgelegt - nur "Punktmessungen"
- Daten müssen über das Netz übertragen werden
- bei Ausfall des Netzes keine Überwachung möglich bzw. nur "outbound"
- benötigt Managementstation (muß konfiguriert werden)
- nutzt (proprietäre!) MIBs
- kann permanent verschiedene wichtige Segmente "remote" überwachen

- unabhängig von Standort
- ist für verschiedene Netztopologien (gleichzeitig) einsetzbar - Messen von Topologieübergängen möglich
- Daten werden lokal bearbeitet und gespeichert
- funktioniert unabhängig von Netz
- ist unabhängig von Managementstation (sofort einsetzbar)
- großer Funktionsumfang
- i.a. physische Anwesenheit notwendig (u.U. sinnvoll beim Troubleshooting)

## Fehlerursachen



- Layer 1: fehlerhafte Kabel; elektrische Störungen; Kollisionen etc.
- Layer 2: 802.x-Inkompatibilitäten; falsch konfigurierte Hardware-Adressen; Broadcaststorms
- Layer 3: falsch konfigurierte IP-Adressen, Subnetzmasken und Broadcast-Adressen; falsche Routing-Tabellen/ Einträge; Protokollinkompatibilitäten
- Layer 4 - 7: unkorrekt implementierte Protokolle