

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

Kapitel 6

Das Internet Protokoll und seine Helfer

6.0 Inhalt

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

- Einführung
- Eigenschaften des Internet Protokolls
- Verkapselung
- IP-Paketkopf (Header)
- Fragmentierung und Reassemblierung
- IP Multicast
- IP Optionen
- Adressauflösung (ARP und ND)
- Das Internet Control Message Protocol (ICMP)

6.1 Einleitung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

- Das *Internet-Protokoll (IP)* ist die gemeinsame „Sprache“ aller Internet-Hosts
- Es definiert im Wesentlichen:
 - **Paketkopfaufbau** (Header)
 - **Adressierung** (bereits kennengelernt)
 - **Fragmentierung**
 - Verschiedene Dienste
- Neben IP selbst werden noch weitere Protokolle benötigt, um verschiedene Probleme zu lösen:
 - Adressauflösung (IP-Adresse → Hardware-Adresse einer Station)
→ *Address Resolution Protocol (ARP, IPv4), Neighbor Discovery (ND, IPv6)*
 - Kontrollbotschaften zur Fehlersuche, Netzwerkanalyse, etc.
→ *Internet Control Message Protocol (ICMP)*

6.1 Einleitung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

- **Mai 1974: Erstes Paper**
Vinton G. Cerf und Robert E. Kahn: *A Protocol for Packet Network Intercommunication*.
IEEE Transactions on Communications, Vol. 22, No. 5, May 1974 pp. 637–648
- **1981: Standardisierung von IPv4**
RFC 791: INTERNET PROTOCOL
<https://tools.ietf.org/html/rfc791>
- **1983: Einsatz von IP im ARPANet**
(Advanced Research Project Agency Network), dem Vorläufer des heutigen Internets
- **1998: Standardisierung von IPv6**
RFC 2460: Internet Protocol, Version 6 (IPv6)
- **Heute (2020):** Noch dominiert IPv4 das Internet, Verbreitung von IPv6 immer mehr im kommen (ca. 40%)



Vint Cerf (l) und Bob Kahn (r), die „Väter des Internet“. (Quelle: Wikimedia Commons)



6.2 Eigenschaften des Internet-Protokolls

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

- IP ist **paketvermittelnd**
- IP ist **verbindungslos**, Pakete werden unabhängig voneinander vermittelt (Datagram Routing)
- IP ist **ungesichert**, Pakete können
 - Verloren gehen
 - Einander überholen
 - Dupliziert werden
 - Verändert werden
- Die **Dienstgüte** (*Quality of Service, QoS*) von IP ist *Best Effort*
 - Jedes Paket wird „so gut wie möglich“ zugestellt
 - Keine Stau- oder Flusskontrolle an sich
 - Da IP über alle mögliche Hardware übertragen wird, die Verluste verursachen kann, müssen darüberliegende Schichten diese behandeln (z.B. TCP, Erklärung später)

Terminologie:

- *Datagramm* bezeichnet ein ungesichertes Paket in einem verbindungslosen Protokoll
→ In IP wird statt “Paket” oft “Datagramm” verwendet

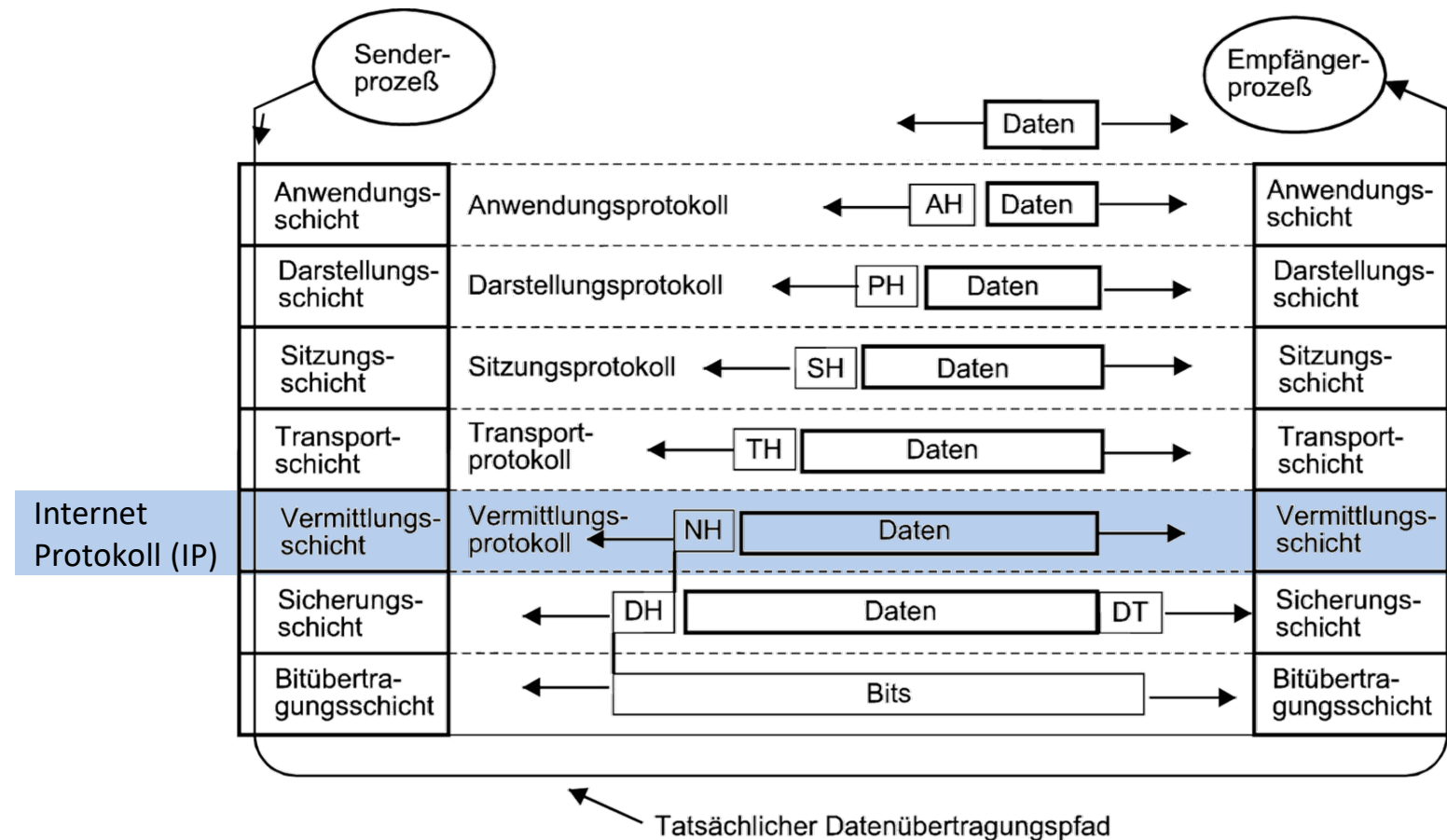
6.3 Verkapselung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ Encapsulation und Decapsulation im ISO-OSI-Modell

- Jede Schicht fügt den Daten, die sie von der darüberliegenden Schicht zur Übermittlung bekommt, eigene Protokollinformationen im Header hinzu.



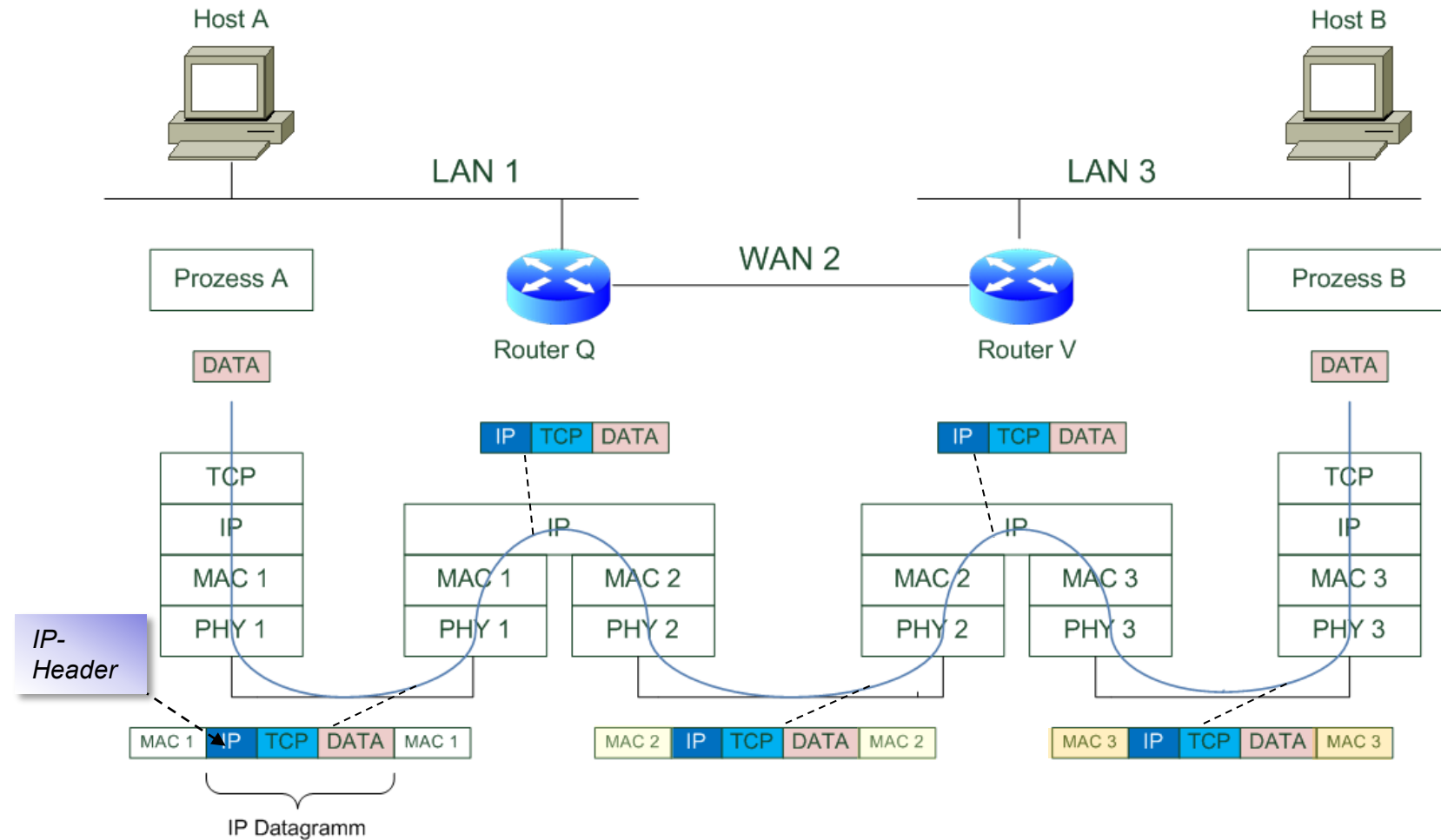
- IP fügt seinen Nutzdaten (= TH + Daten) den IP-Header (NH = Network Header) hinzu

6.3 Verkapselung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ Der Weg eines IP-Datagramms durch mehrere Subnetze



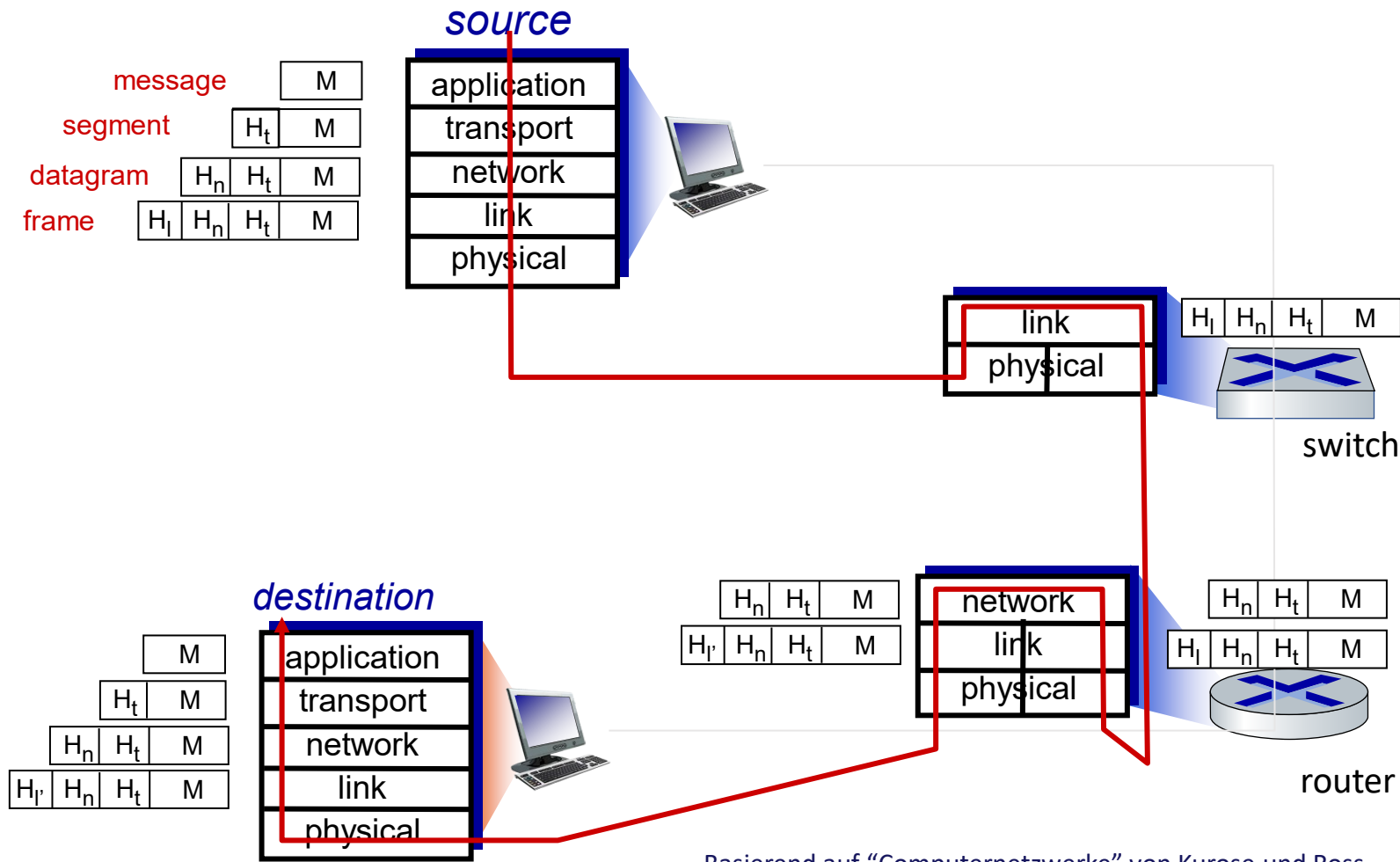
- Ständiges En- und Decapsulation („Ein- und Auspacken“)
- Layer 3 Daten bleiben unverändert, Layer 2 Header/Trailer ändert sich ständig

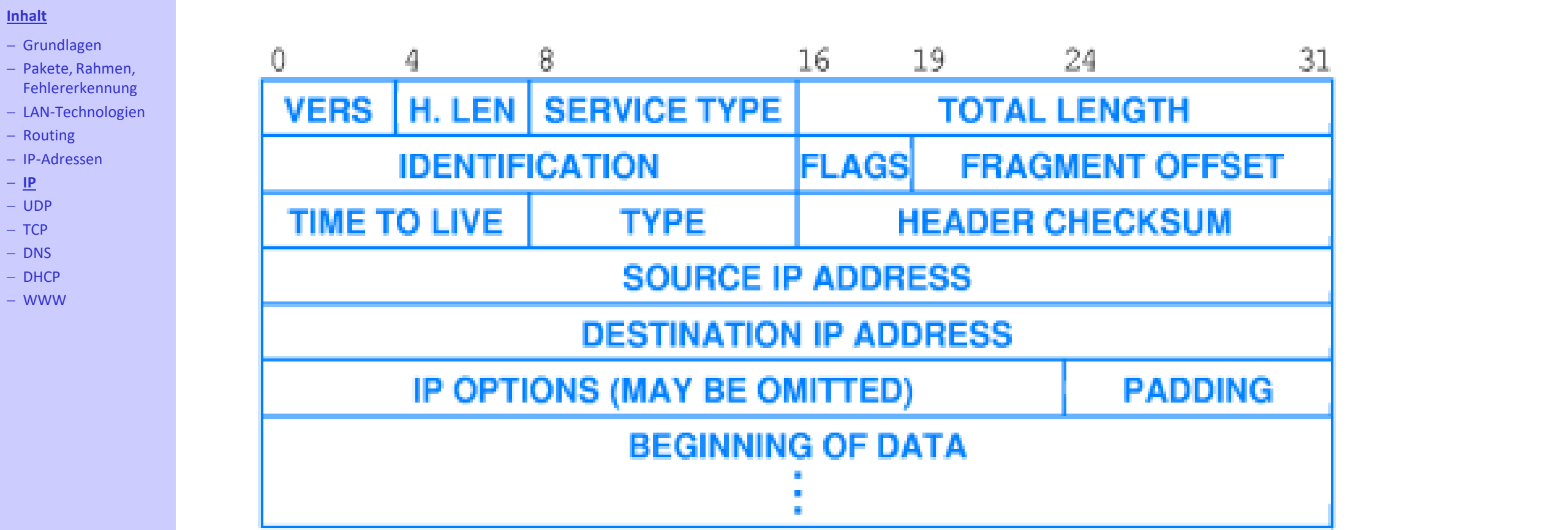
6.3 Verkapselung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ Unterschied Switch (Layer 2) und Router (Layer 3)





Picture taken from Comer

Figure 20.4 Fields in the IP datagram header. Both the source and destination addresses are Internet addresses.

6.4.1 IPv4 Header

Inhalt

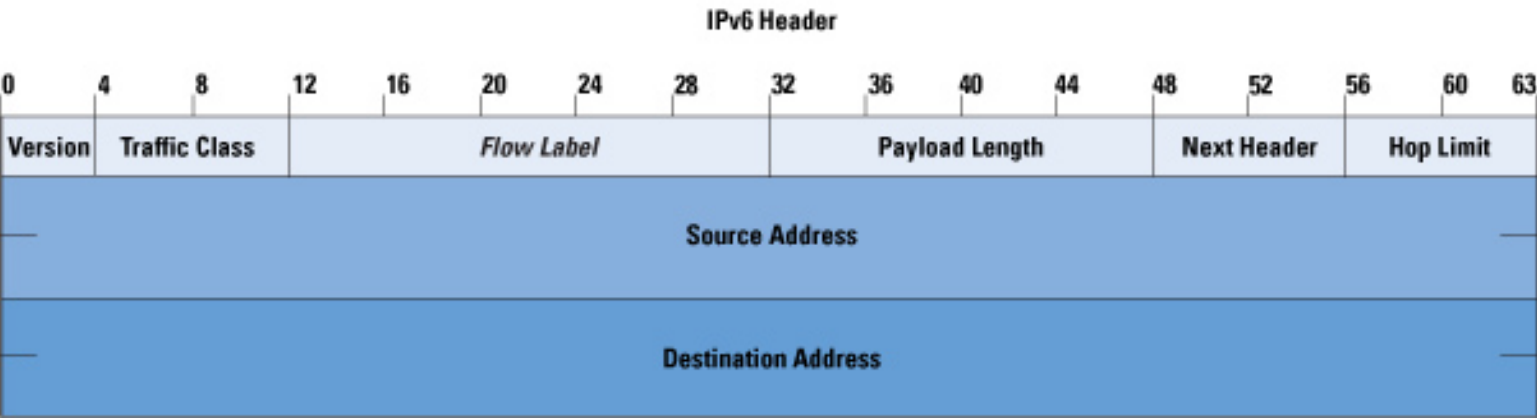
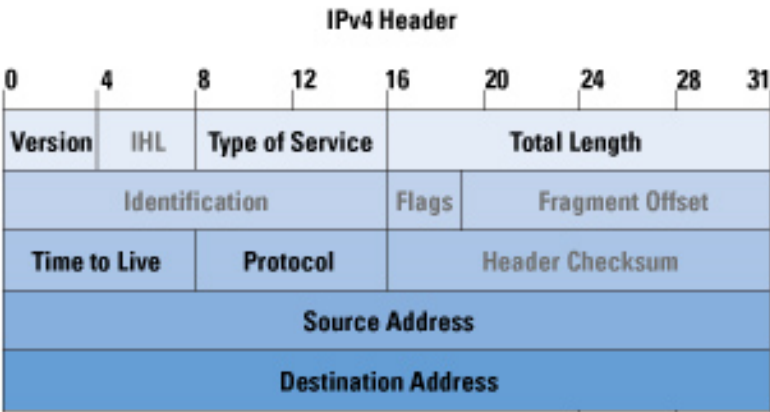
- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

- Figure 20.4 zeigt die Felder eines IPv4 Datagram Headers
- VERS → a 4-bit protocol version (currently 4)
- H.LEN → a 4-bit datagram header length
- SERVICE TYPE → field specifies
 - whether the sender prefers the datagram to travel over a route
 - with “minimal delay” or a route with “maximal throughput”
 - a router that knows multiple routes can use the value to choose a route
- TOTAL LENGTH → specifies number of octets: header + the data.
- TIME TO LIVE (TTL) → used to prevent a datagram from traveling forever around a path that contains a loop
 - TTL can be set to a value 0 - 255
 - Each router that handles the datagram decrements TTL by 1
 - If the counter reaches zero, the datagram is discarded and an error message is sent back to the source
- PADDING → to make header multiple of 32 bits, when needed

6.4.2 IPv4/IPv6 Header

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW



6.4.2 IPv6 Header

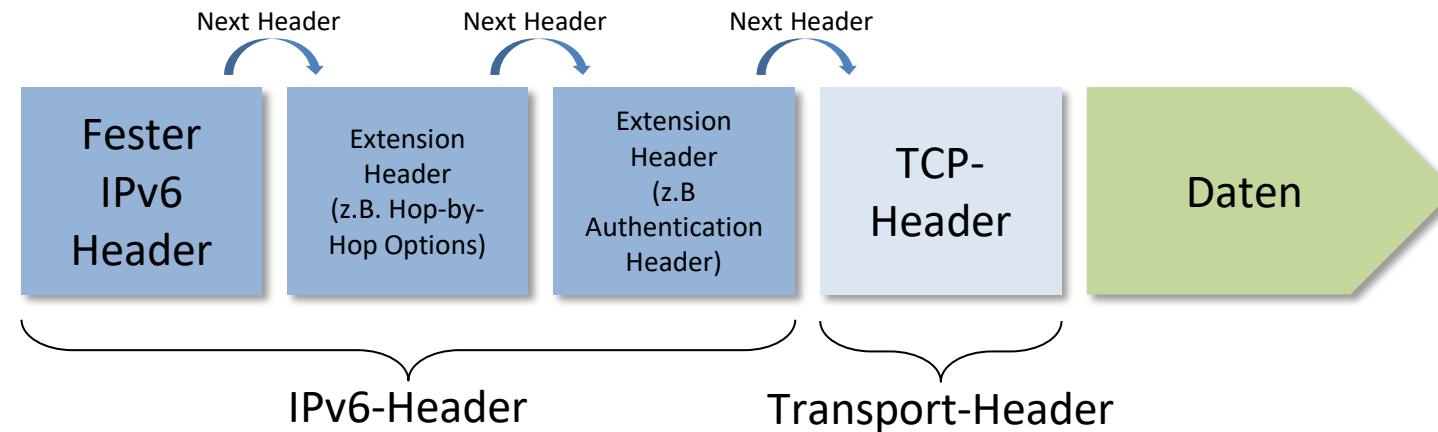
Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

Feld	Länge	Inhalt
Version	4 Bit	IP-Versionsnummer (6)
Traffic Class	8 Bit	Quality of Service (QoS). Eine Art Prioritätsvergabe.
Flow Label	20 Bit	Pakete, die dasselbe Flow Label tragen, werden gleich behandelt (QoS).
Payload Length	16 Bit	Länge der Nutzdaten in Byte
Next Header	8 Bit	Typ des folgenden Headers, z. B. 6=TCP, 17=UDP.
Hop Limit	8 Bit	Wie TTL bei IPv4
Source Address	128 Bit	Adresse des Senders
Destination Address	128 Bit	Adresse des Empfängers

6.4.3 IPv6 Next Header

- Nicht immer benötigte Informationen sind bei IPv6 in optionalen *Extension Headers* enthalten, die **nur bei Bedarf** angehängt werden
- Dadurch wird der Header nicht unnötig aufgebläht, und ist an die jeweiligen Anforderungen anpassbar



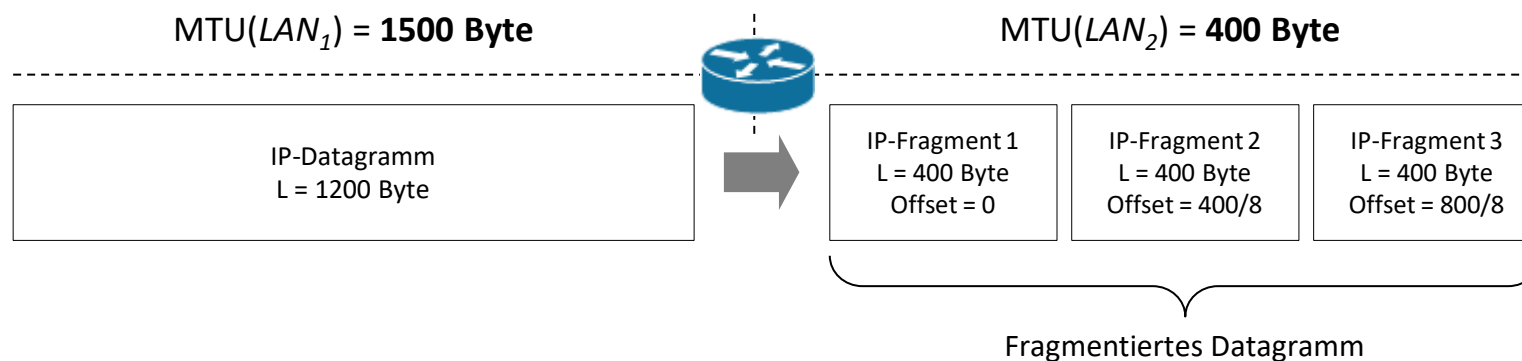
- Jeder Header enthält ein Feld „Next Header“, der den Typ des darauffolgenden Headers angibt (bis zum Transportschicht-Header)

6.5 IPv4: Fragmentierung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

- Unterschiedliche Netzwerktechnologien haben unterschiedlich lange maximale Paketlängen
- *Maximum Transmission Unit (MTU)*: Definiert die maximale Nutzdatenlänge eines Pakets innerhalb eines physikalischen Netzwerkes, d.h. auf Layer 2
 - Ethernet: MTU = 1500 Byte
 - IP-Datagramme passieren auf ihrem Weg mehrere Netzwerke mit verschiedenen MTUs.
 - IP-Datagramme, die in ein Netz gelangen dessen MTU kleiner ist als die Länge des Datagrammes müssen von IP **fragmentiert** (= zerlegt) werden.
- *Fragmentierung*: Aufteilen eines Datagrammes in mehrere *Fragmente*, jedes kleiner als die MTU des Netzes.



6.5 IPv4: Fragmentierung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

- Fragmentierung wird durch Sender und Router vorgenommen
 - Sender bzw. Router ermittelt aus MTU, Datagramm- und Headerlänge die Anzahl und Größe der benötigten Nutzdatenfragmente
 - Datagramm-Nutzdaten werden in diese Fragmente zerlegt, und jedes mit einem eigenen IP-Header versehen.
- Header-Informationen zur Fragmentierung:
 - **Flags-Feld**
 - Bit 0: Reserviert
 - Bit 1: ,1' → Segment darf nicht fragmentiert werden
 - Bit 2: ,1' → es folgen weitere Fragmente;
,0' → letztes Fragment
 - **Offset**
 - Gibt die Position des Fragments im Original-Datagramm in der Einheit 8 Byte an. Dies wird beim Zusammenfügen (Reassemblierung) benötigt.
 - **Identification**
 - Zur Unterscheidung unterschiedlicher IP-Datagramme

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

0	4	8	16	19	24	31
VERS	H. LEN	SERVICE TYPE	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TIME TO LIVE		TYPE	HEADER CHECKSUM			
SOURCE IP ADDRESS						
DESTINATION IP ADDRESS						
IP OPTIONS (MAY BE OMITTED)					PADDING	
BEGINNING OF DATA						
⋮						

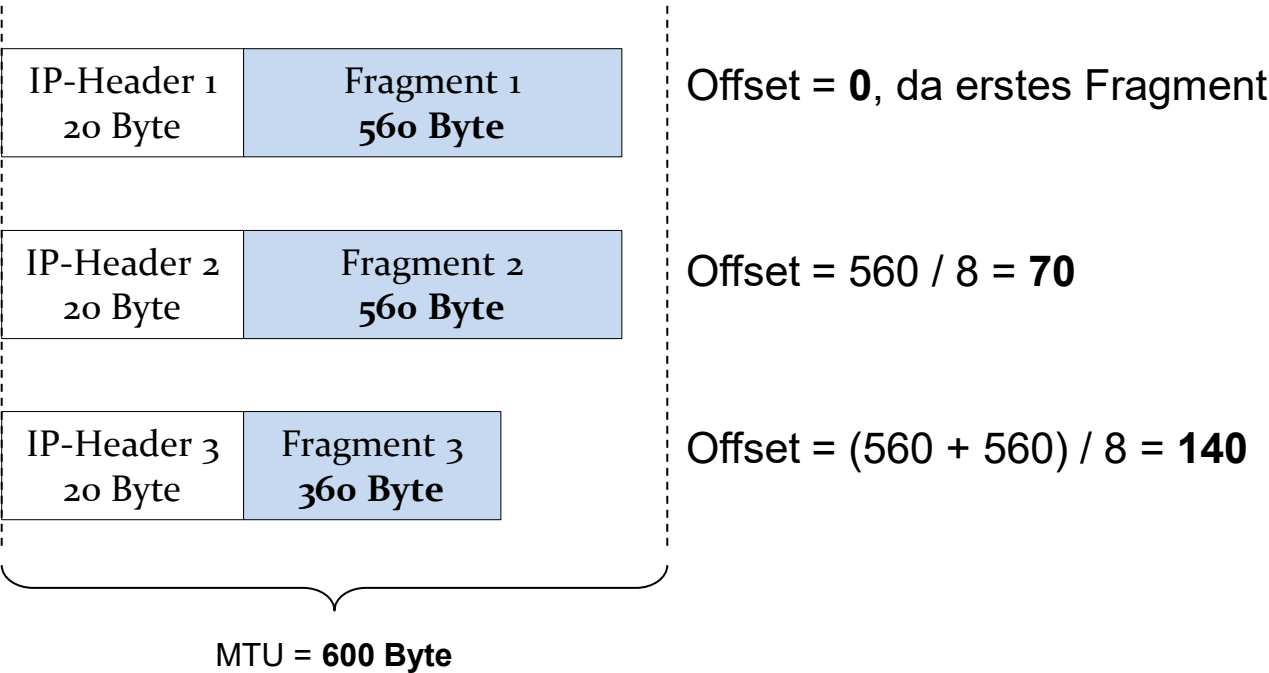
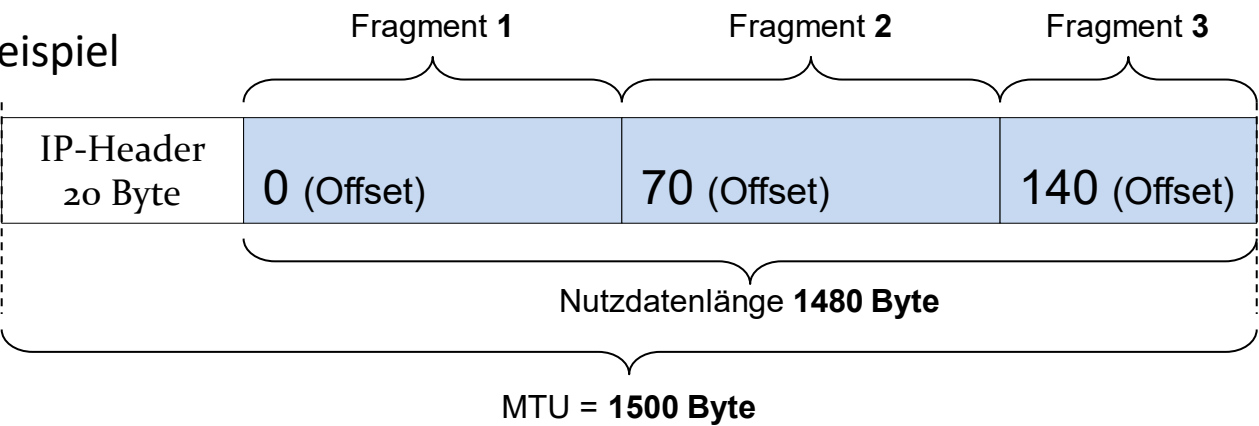
Figure 20.4 Fields in the IP datagram header. Both the source and destination addresses are Internet addresses.

6.5 IPv4: Fragmentierung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

Beispiel



Fragmentierung in Vielfachen von 8 Byte

6.5 IPv4: Fragmentierung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

- **Reassemblierung ::** Das Zusammensetzen aller erhaltenen IP-Fragmente zum ursprünglichen Datagramm
- Dies wird **NICHT** in den Routern vorgenommen, sondern erfolgt erst am **Zielhost!**
 - Routen können sich ändern, d.h. ein Router hat ggf. nicht alle Fragmente eines Datagramms erhalten
 - Router müssten Fragmente und Informationen zwischenspeichern
- Empfänger wartet eine **maximale Zeit** auf das Eintreffen fehlender Fragmente:
 - Kommen alle Fragmente eines Datagrammes innerhalb dieser Zeit an, wird das Datagramm zusammengesetzt, und an die nächst-höhere Schicht übergeben
 - Fehlen nach Ablauf der Zeit Fragmente, wird das gesamte Datagramm verworfen
→ „*All or nothing*“

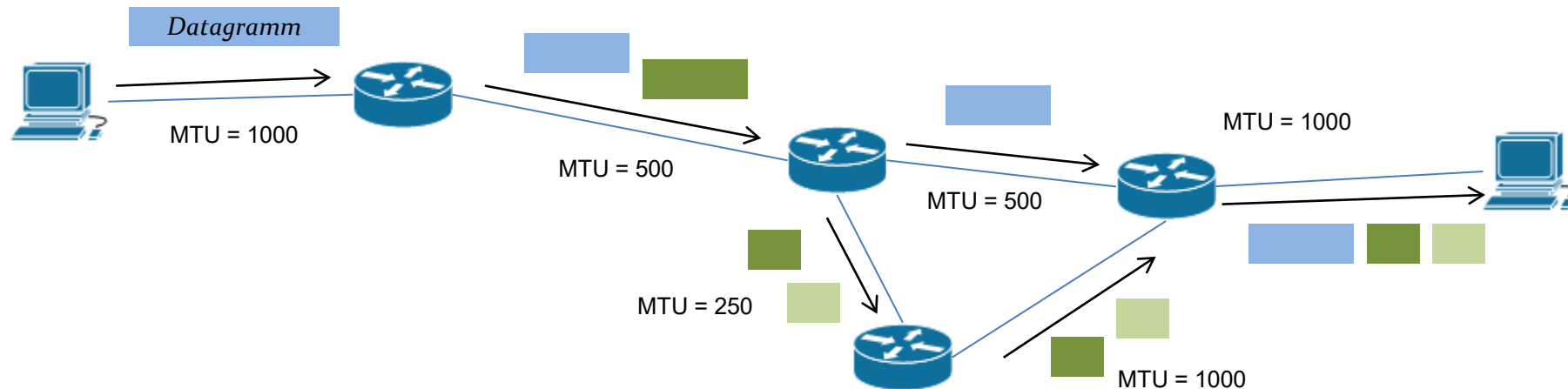
6.5 IPv4: Fragmentierung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

Fragmentierung von Fragmenten

- Wenn ein Fragment eines bereits fragmentierten Datagrammes auf ein Netzwerk mit noch kleinerer MTU trifft:
 - Fragment wird abermals fragmentiert, mit entsprechenden Offsets
 - Gleiche Behandlung wie ursprüngliche Fragmente beim Empfänger, nur dass diese eben kleiner sind.

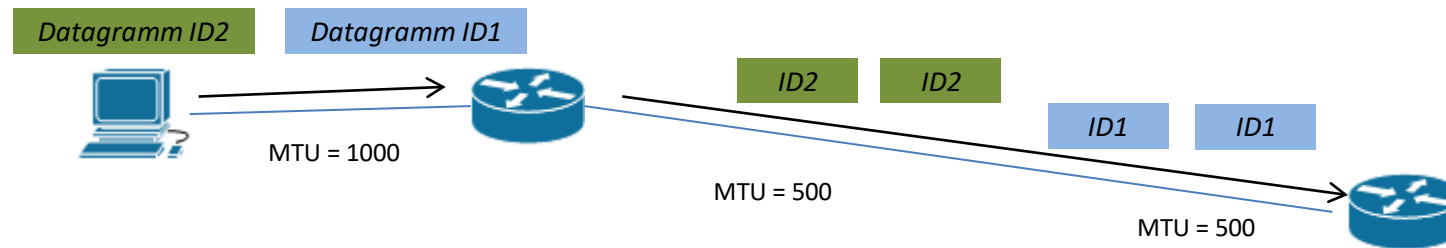


6.5 IPv4: Fragmentierung

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

- **ID**entification dient zur Unterscheidung unterschiedlicher Datagramme
- Beispiel: Sender sendet zwei IP-Datagramme



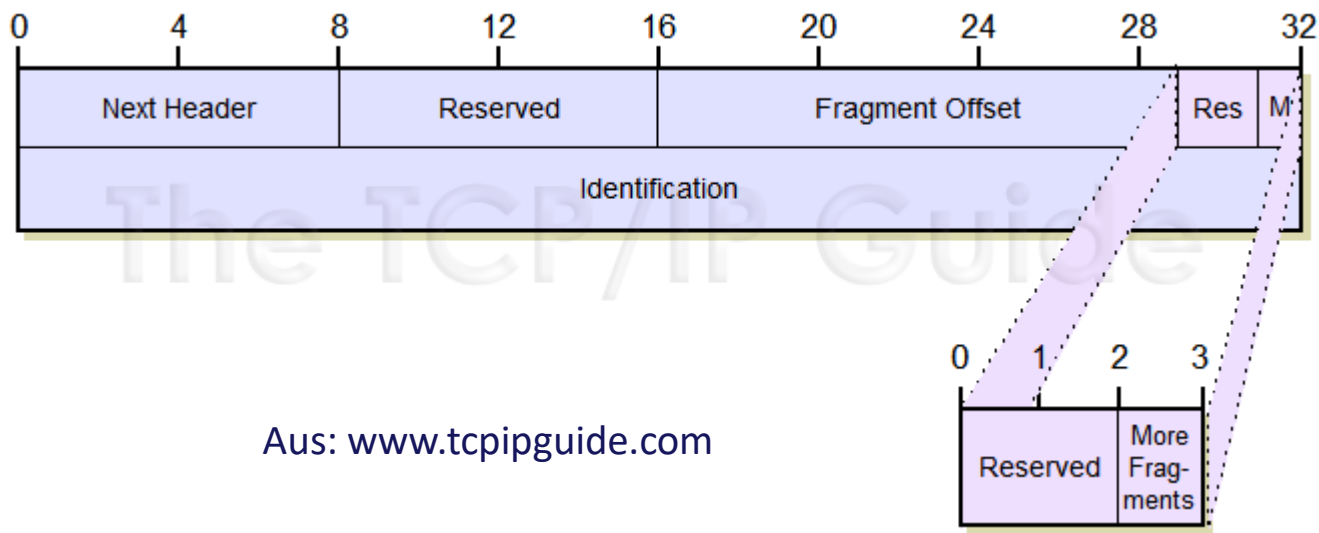
- Empfänger kann anhand der **ID** die Fragmente den ursprünglichen Datagrammen zuordnen

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

Fragmentierung in IPv6

- Next Header: Fragment



Aus: www.tcpipguide.com

- Nur Sender fragmentiert, Router nicht!
- Router verwerfen zu große Pakete, liefern ICMP Fehlernachricht an Sender

6.7 IP-Multicast

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

- **Multicast** :: Adressierung einer Gruppe von Teilnehmern (*Multicast-Group*)
- IP sieht speziellen Adressbereich für Multicast vor:
 - IPv4: 224.0.0.0 bis 239.255.255.255
 - IPv6: ff00::/8
- Verwaltung der Gruppen-Zugehörigkeiten:
Internet Group Management Protocol (IGMP)

6.8 IP-Optionen

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ IP kennt verschiedene Optionen

➤ IPv4

- Strict Routing: Option gibt den kompletten Pfad an, welchen das Paket durchlaufen muss
- Free Routing: Option gibt eine Liste von Routern an, die vom Paket nicht verfehlt werden dürfen
- Record Route: Lässt die komplette Route aufzeichnen (Heute reicht die Größe des Option-Feldes meist nicht mehr dafür aus)
- Time Stamp: Zeitstempel
- Security: Bezeichnet, wie „böartig“ das Paket ist (RFC3514)

➤ IPv6

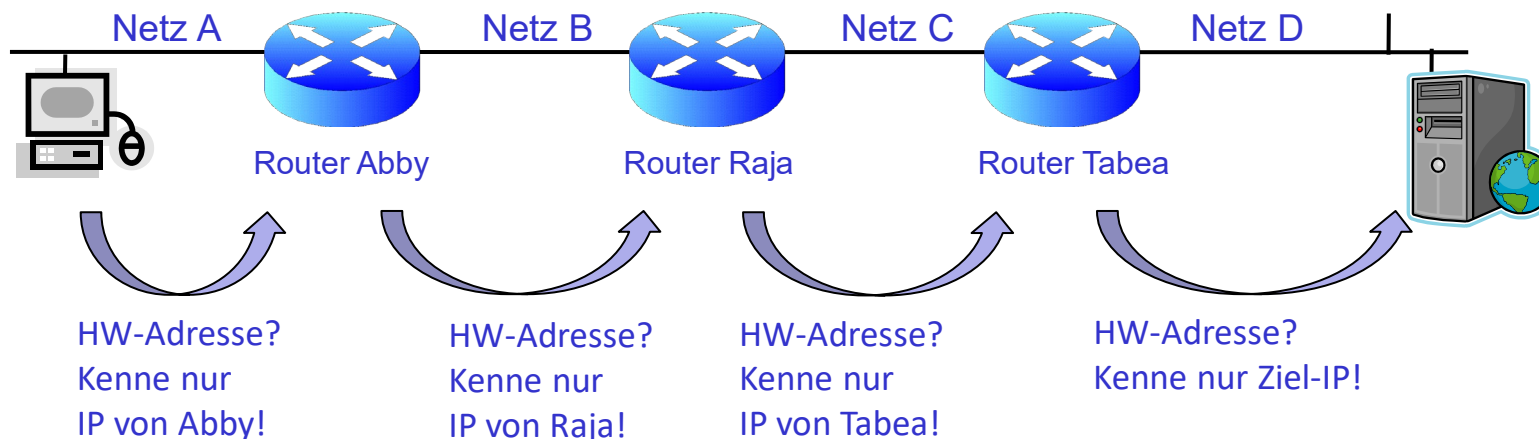
- Hop by Hop Options: Müssen von allen durchlaufenden Router beachtet werden
- Routing: Weg kann beeinflusst werden
- Fragment
- Authentication Header: Security
- Encapsulating Security Payload: Security
- Destination Options: Optionen die vom Zielgerät beachtet werden müssen
- Mobility: Mobile IPv6

6. 9 Adressauflösung

Inhalt

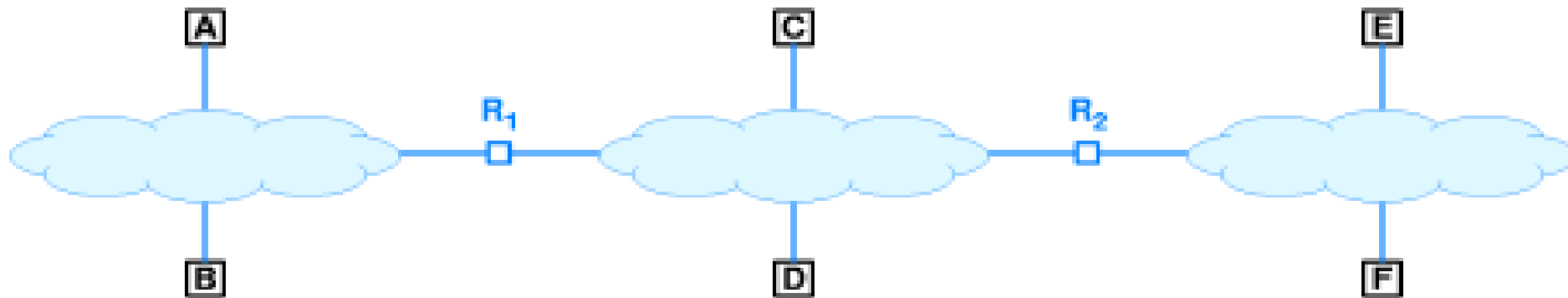
- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

- IP Adressen sind „virtuell“; durch SW verwaltet
- Ein IP-Paket wandert auf dem Weg zum Ziel durch viele verschiedene phys. NW
 - Hop by Hop Prinzip
- Ein Paket, das über ein phys. NW zum nächsten Hop gesendet wird,
 - braucht die HW-Adresse des nächsten Hops
 - nächster Hop ist Teil des lokalen NW
- SW muss die IP-Adresse des nächsten Hops in dessen HW-Adresse umwandeln
- Bei IPv4 übernimmt das das ARP: Address Resolution Protokol



6.9.1 ARP

- Ein Host/Router verwendet ARP, sobald er ein Paket an eine Netzwerkkarte des lokalen NW sendet
- Ein Computer löst (resolves) nie die HW-Adresse einer Netzwerkkarte auf, die sich in einem fremden NW befindet



Picture taken from Comer

Figure 19.1 A simple internet with routers R_1 and R_2 connecting three physical networks; each network has two host computers attached. A computer can only resolve the address of a computer attached to the same physical network.

Inhalt

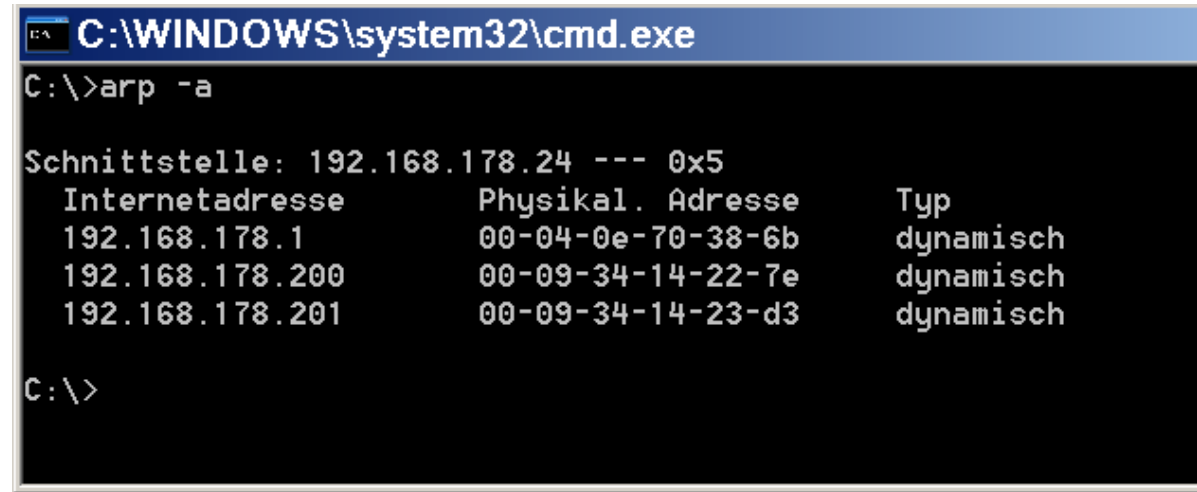
- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

6.9.1 ARP

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ Jeder Rechner verwaltet eine ARP-Tabelle



```
C:\WINDOWS\system32\cmd.exe
C:\>arp -a

Schnittstelle: 192.168.178.24 --- 0x5
Internetadresse      Physikal. Adresse    Typ
192.168.178.1        00-04-0e-70-38-6b    dynamisch
192.168.178.200      00-09-34-14-22-7e    dynamisch
192.168.178.201      00-09-34-14-23-d3    dynamisch

C:\>
```

ARP-Tabelle eines Hosts im NW 192.168.178.0/24. Jeder Eintrag beinhaltet eine IP-Adresse und die zugehörige HW-Adresse

- Einträge können per Hand gesetzt werden „statisch“
- Dynamisch erzeugt werden: Nachrichtenaustausch mittels ARP
 - siehe Figure 19.5

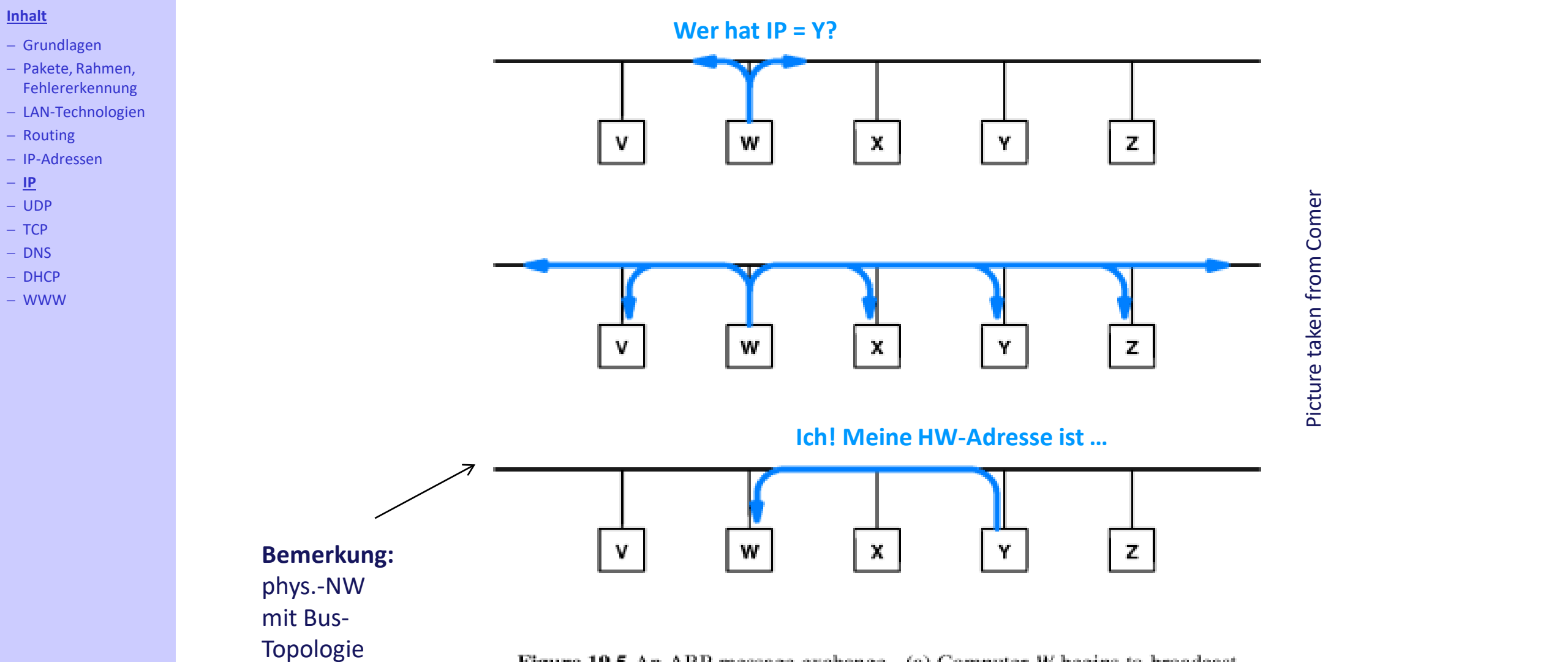


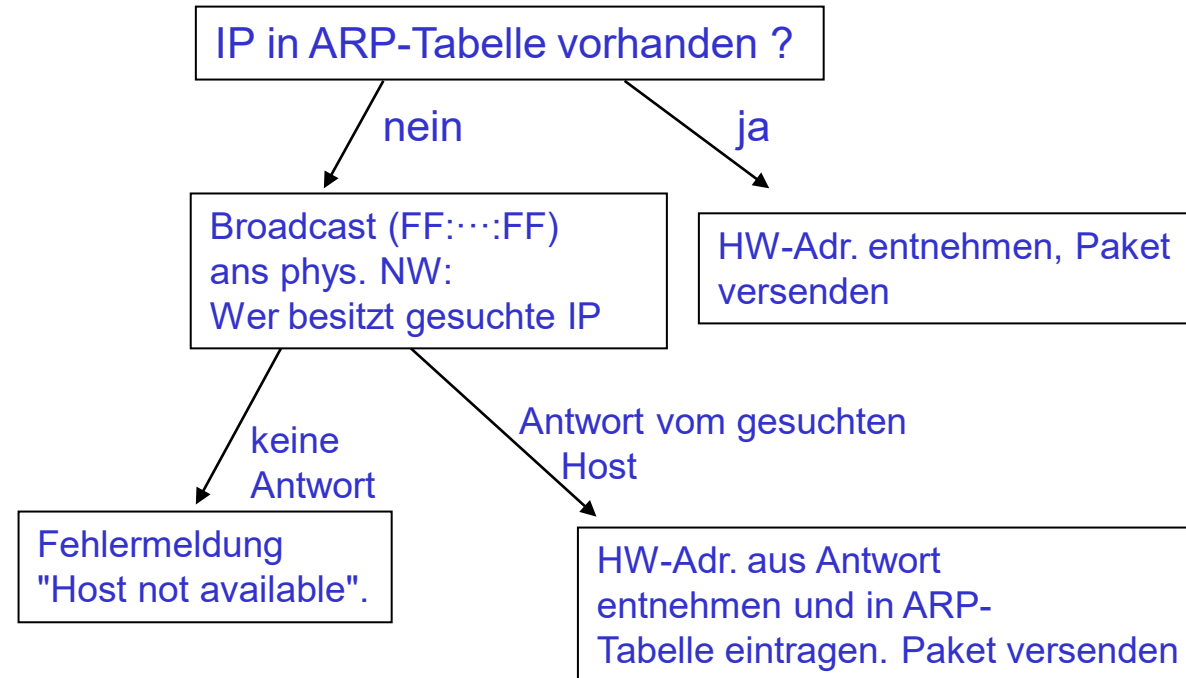
Figure 19.5 An ARP message exchange. (a) Computer *W* begins to broadcast an ARP request that contains computer *Y*'s IP address. (b) All computers receive the request, and (c) computer *Y* sends a response directly to *W*.

6.9.1 ARP

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ Algorithmus eines Hosts während der Address Resolution



➤ Dynamische ARP-Einträge werden regelmäßig gelöscht

- um die Tabelle aktuell zu halten

6.9.1 ARP

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

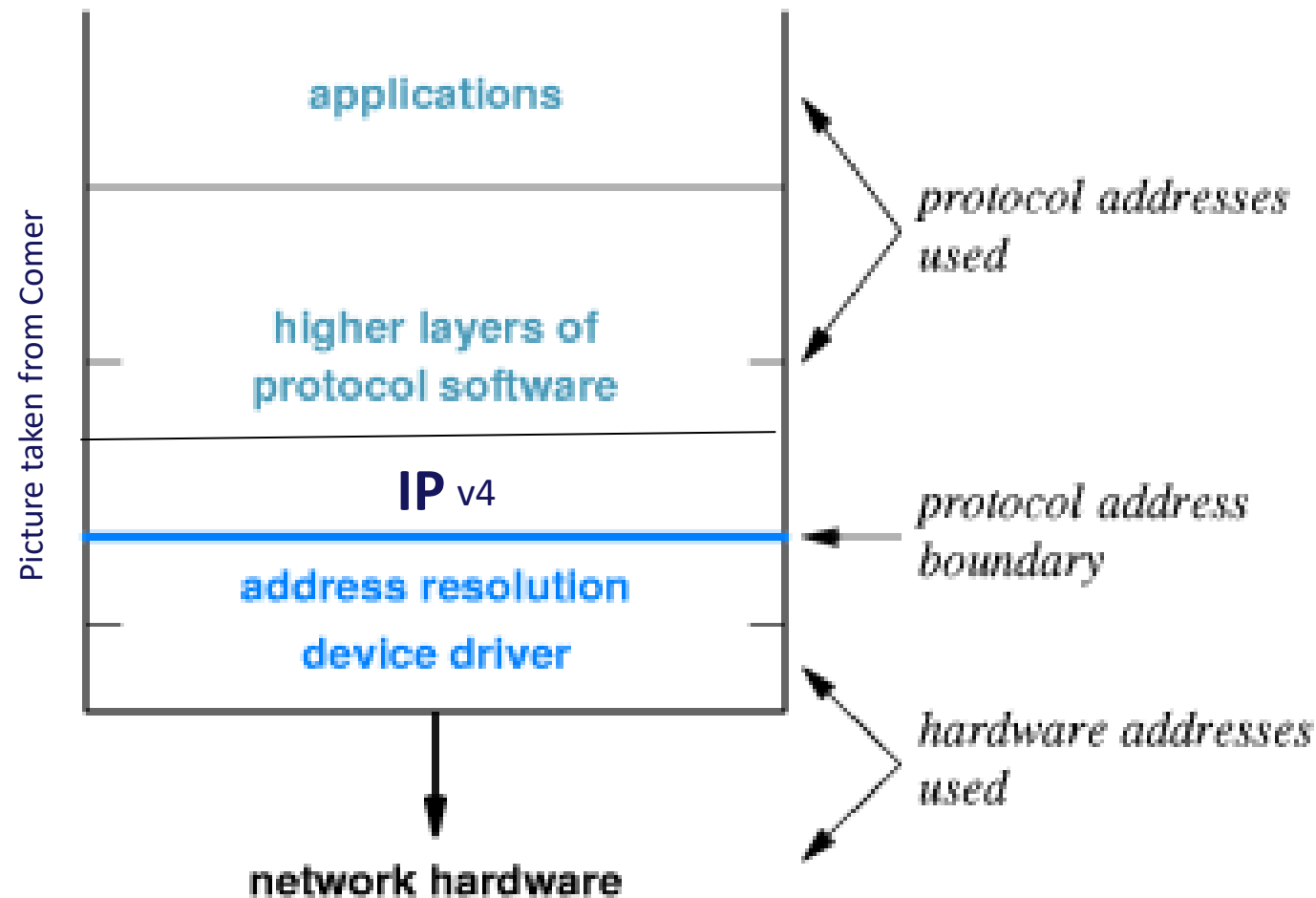


Figure 19.9 Layered protocol software in a computer and the conceptual boundary between the network interface layer and higher layers.

6.9.2 Neighbor Discovery (ND)

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

- Ersetzt ARP bei IPv6
- Funktioniert ähnlich ARP
- Verwendet ICMPv6 Nachrichten
- Einsatz für
 - Auflösung IPv6 Adressen in physikalischen Adresse
 - Finden benachbarter Router
 - Netzwerkinformationen vom Router zu Hosts
 - Erkennung doppelter Adressen
- Verwendung für Autokonfiguration des Hosts

6.10 Internet Control Message Protocol (ICMP)

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ Internet Control Message Protocol (ICMP)

➔ Austausch von Fehlermeldungen und Zustandsinformationen im Internet

- Ziel nicht erreichbar
- Echo-Anfrage und Antwort (Ping)
- Port nicht erreichbar
- TTL überschritten
- ...

➤ Standardisiert in

- **RFC 792:** Internet Control Message Protocol

<https://tools.ietf.org/html/rfc792>

- **RFC 4443:** Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

<https://tools.ietf.org/html/rfc4443>

6.10 Internet Control Message Protocol (ICMP)

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ Beispiele für ICMP-Meldungen

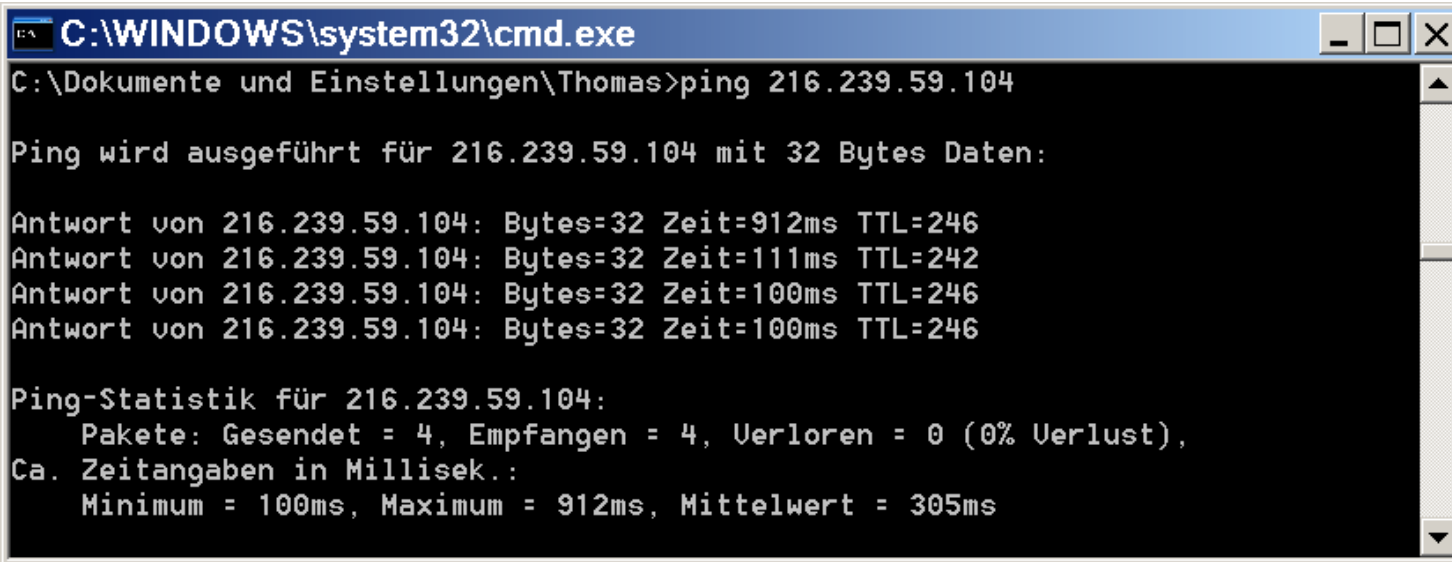
- ***ECHO-Request, ECHO Reply***: Aufforderung an einen Host, eine Antwort zu schicken
→ Erreichbarkeit einer Station Prüfen (Anwendung: **ping, traceroute**)
- ***Destination unreachable***: Ein Paket konnte nicht an den Zielhost zugestellt werden (z.B. wegen einer ausgefallenen Verbindung oder eines ausgefallenen Routers)
- ***TTL exceeded***: Ein Paket wurde aufgrund des Ablaufs seiner TTL verworfen.
(Zweckentfremdung: Routenverfolgung mit traceroute)
- ***Parameter problem***: Ein Paket wurde aufgrund eines ungültigen IP-Headers verworfen
- ***Packet Too Big***: z.B. IPv6 Router erhält zu großes Paket, darf aber nicht fragmentieren
- Einige mehr...

6.10 ICMP

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

Ping:



```
C:\WINDOWS\system32\cmd.exe
C:\Dokumente und Einstellungen\Thomas>ping 216.239.59.104

Ping wird ausgeführt für 216.239.59.104 mit 32 Bytes Daten:

Antwort von 216.239.59.104: Bytes=32 Zeit=912ms TTL=246
Antwort von 216.239.59.104: Bytes=32 Zeit=111ms TTL=242
Antwort von 216.239.59.104: Bytes=32 Zeit=100ms TTL=246
Antwort von 216.239.59.104: Bytes=32 Zeit=100ms TTL=246

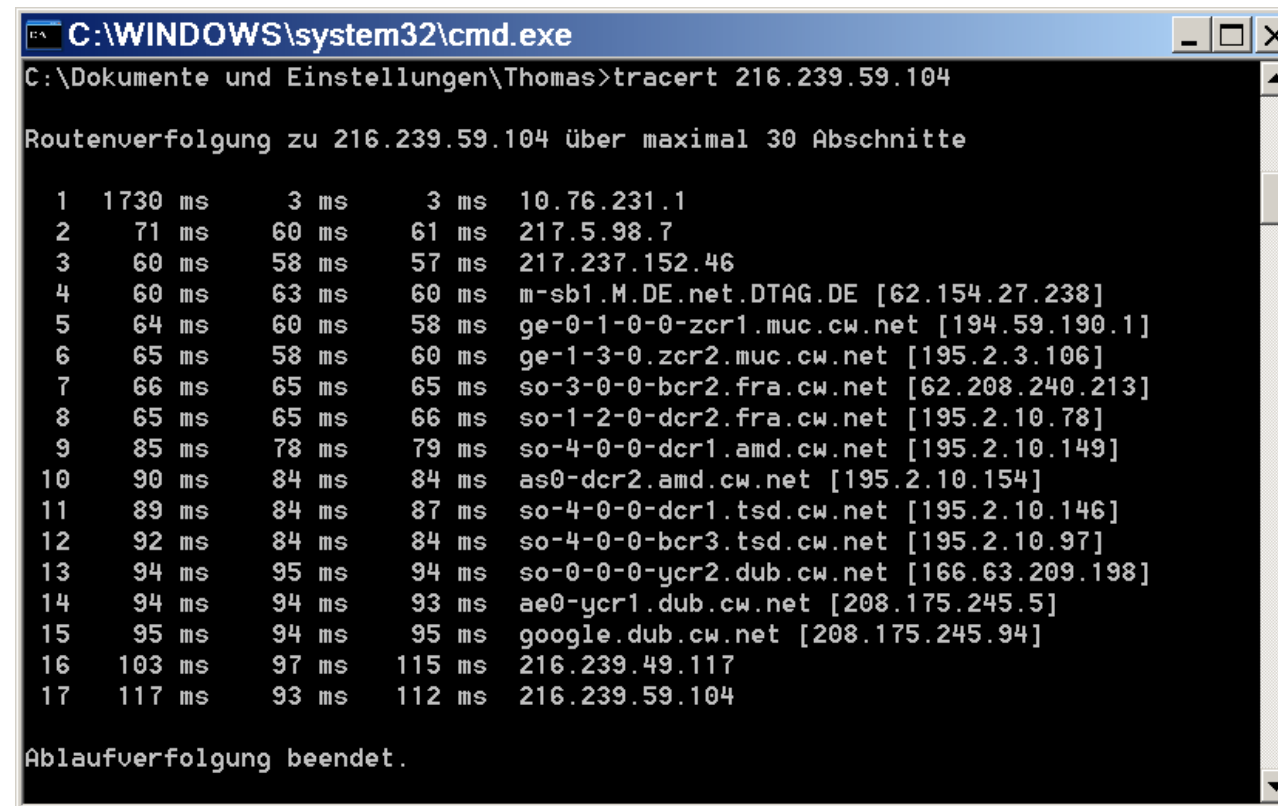
Ping-Statistik für 216.239.59.104:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 100ms, Maximum = 912ms, Mittelwert = 305ms
```

6.10 ICMP

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- **IP**
- UDP
- TCP
- DNS
- DHCP
- WWW

Tracert (Traceroute)



The screenshot shows a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The user has entered the command "tracert 216.239.59.104". The output shows the route from the source to the destination, including hop numbers, round-trip times, and IP addresses. The route ends at the destination IP 216.239.59.104.

```
C:\WINDOWS\system32\cmd.exe
C:\Dokumente und Einstellungen\Thomas>tracert 216.239.59.104

Routenverfolgung zu 216.239.59.104 über maximal 30 Abschnitte

 1  1730 ms    3 ms    3 ms    10.76.231.1
 2    71 ms   60 ms   61 ms   217.5.98.7
 3    60 ms   58 ms   57 ms   217.237.152.46
 4    60 ms   63 ms   60 ms   m-sb1.M.DE.net.DTAG.DE [62.154.27.238]
 5    64 ms   60 ms   58 ms   ge-0-1-0-0-zcr1.muc.cw.net [194.59.190.1]
 6    65 ms   58 ms   60 ms   ge-1-3-0-zcr2.muc.cw.net [195.2.3.106]
 7    66 ms   65 ms   65 ms   so-3-0-0-bcr2.fra.cw.net [62.208.240.213]
 8    65 ms   65 ms   66 ms   so-1-2-0-dcr2.fra.cw.net [195.2.10.78]
 9    85 ms   78 ms   79 ms   so-4-0-0-dcr1.amd.cw.net [195.2.10.149]
10    90 ms   84 ms   84 ms   as0-dcr2.amd.cw.net [195.2.10.154]
11    89 ms   84 ms   87 ms   so-4-0-0-dcr1.tsd.cw.net [195.2.10.146]
12    92 ms   84 ms   84 ms   so-4-0-0-bcr3.tsd.cw.net [195.2.10.97]
13    94 ms   95 ms   94 ms   so-0-0-0-ycr2.dub.cw.net [166.63.209.198]
14    94 ms   94 ms   93 ms   ae0-ycr1.dub.cw.net [208.175.245.5]
15    95 ms   94 ms   95 ms   google.dub.cw.net [208.175.245.94]
16   103 ms   97 ms   115 ms   216.239.49.117
17   117 ms   93 ms   112 ms   216.239.59.104

Ablaufverfolgung beendet.
```

Zusammenfassung und Ausblick

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

➤ Vermittlungsschicht im Internet sorgt für

- Adressierung von Rechnern weltweit
- Zustellung und Vermittlung von Datenpaketen (Routing)
- Auflösung von Adressen (ARP, ND)
- Kontrollnachrichten (ICMP)

➤ IP ist

- Verbindungslos
- Unzuverlässig (Datagramme können verloren gehen und sind unbestätigt)
- Hostgebunden → Noch offen: Wie können sich mehrere Anwendungen ein IP-Interface teilen (oder: wie erfolgt das *Multiplexing* zwischen verschiedenen Anwendungen auf dem selben Host?)

➔ Die Transportschicht

- Echte *Ende-zu-Ende* Protokolle zwischen zwei Hosts (Es sind nur zwei Transportschichtinstanzen bei der Kommunikation beteiligt, nicht eine auf jedem Hop)
- Verschiedene Dienstklassen (hinsichtlich Verbindung, Zuverlässigkeit, ...)
- Anwendungsadressierung anhand *Portnummern*

Zusammenfassung und Ausblick

Inhalt

- Grundlagen
- Pakete, Rahmen, Fehlererkennung
- LAN-Technologien
- Routing
- IP-Adressen
- IP
- UDP
- TCP
- DNS
- DHCP
- WWW

- Entscheidungspunkte beim Multiplexing auf den Weg von unten nach oben bzw. oben nach unten

TCP/IP-Schichten

Anwendungsschicht
(Application Layer)

↑ Port Number/ ↓ API

Transportschicht
(Transport Layer)

↑ Next Header/ ↓ IP Adresse

Vermittlungsschicht
(Network Layer)

↑ Ethertyp/ ↓ Routing Tabelle

Netzzugangsschicht
(Network Interface Layer)

Protokoll Graph: TCP/IP

