

Netzwerke

Technische Grundlagen der Informatik

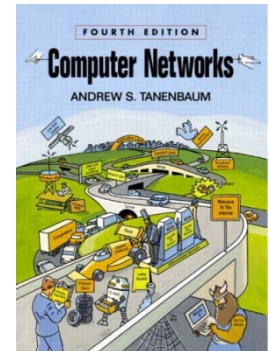
Übersicht

Netzwerke

- Das OSI 7-Schicht Modell
- MAC
- Netzwerkelemente
- IP (v4) und Networking
 - Subnetting
 - Klassensysteme
- TCP / UDP
- IP (v6)

Andrew S. Tanenbaum,
Computer Networks, 4th ed., Prentice Hall, 2002.

<http://www.rfc-editor.org>,
Request for Comments (RFC)

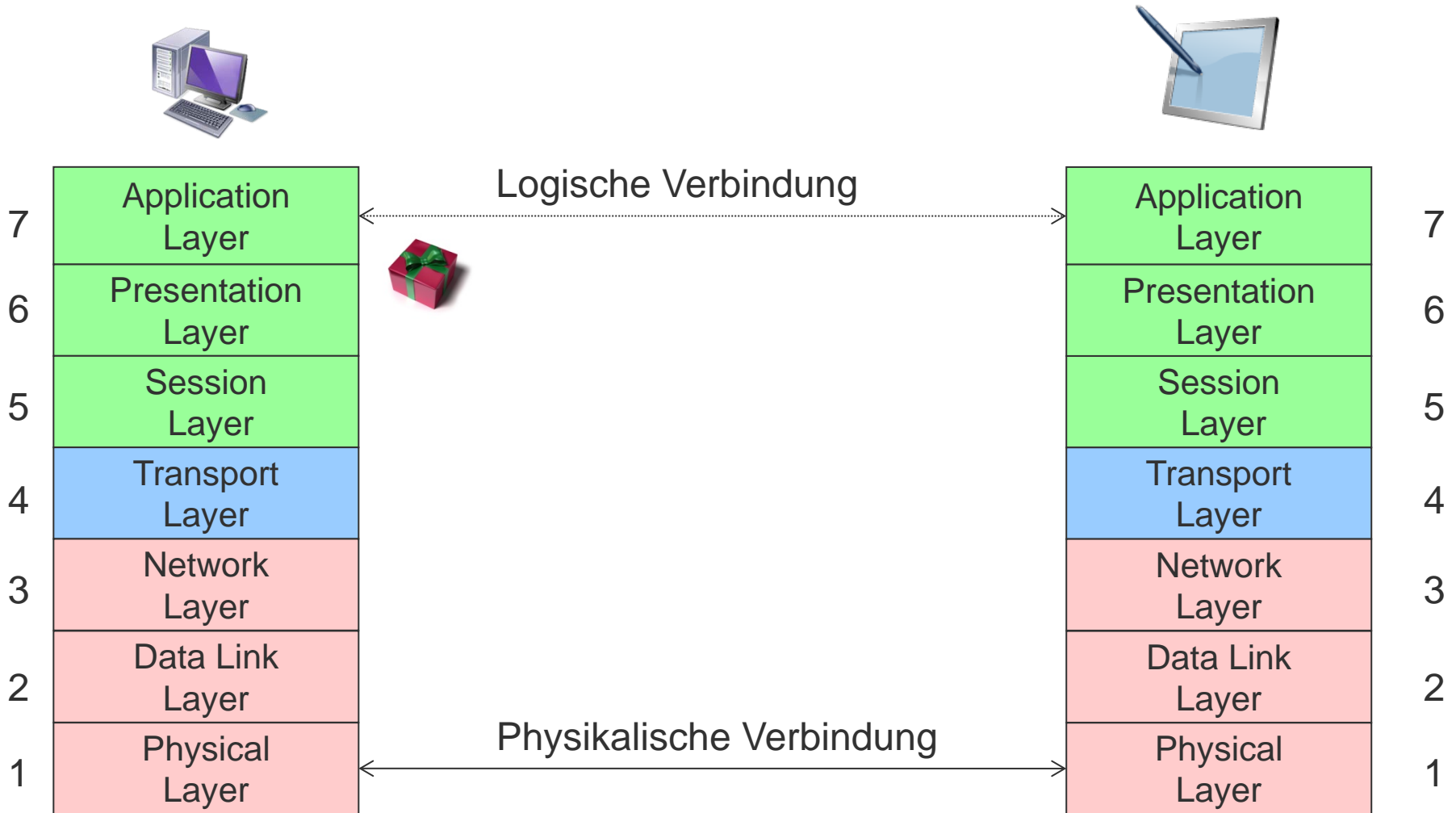


2-3 Stunden um Folgendes zu verstehen:

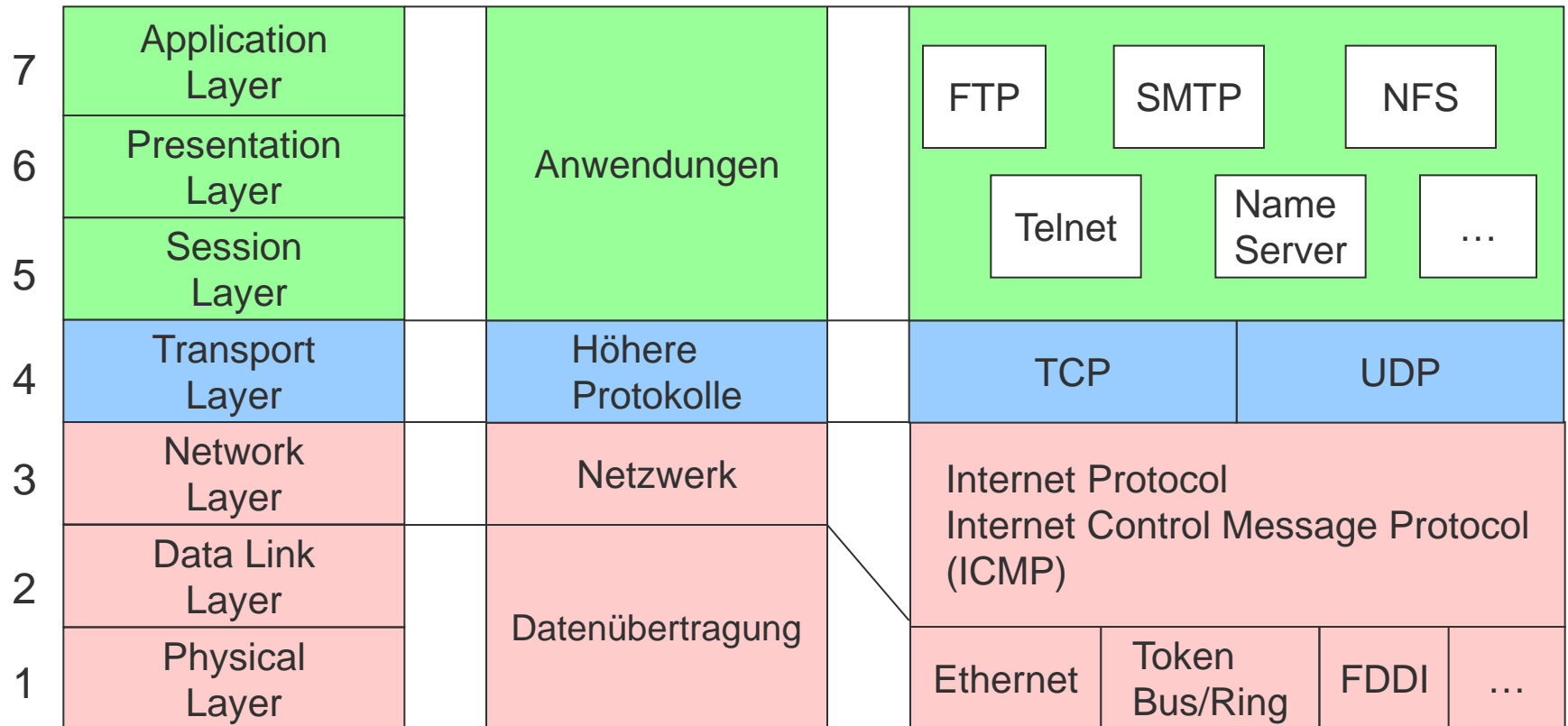
```
user@meinRechner:~$ ifconfig
```

```
eth0  Link encap:Ethernet  HWaddr 00:1e:c9:2d:20:45  
      inet addr:128.130.60.13  Bcast:128.130.60.127  Mask:255.255.255.128  
      inet6 addr: fe80::21e:c9ff:fe2d:2045/64  Scope:Link  
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
      RX packets:4206193 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:6694449 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:766746719 (766.7 MB)  TX bytes:8334752712 (8.3 GB)  
      Interrupt:17
```

Das OSI Modell – Idee



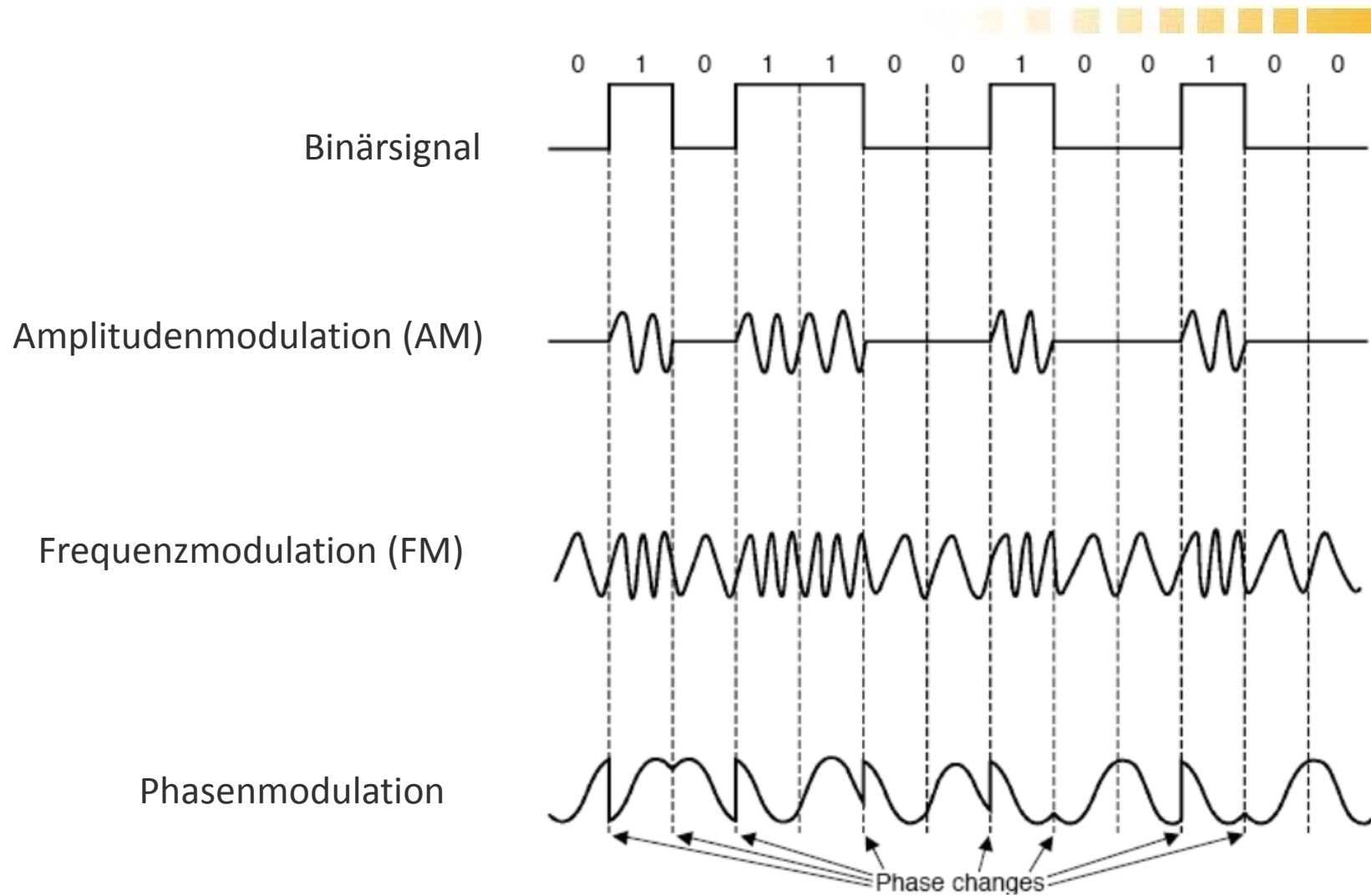
Das OSI Modell



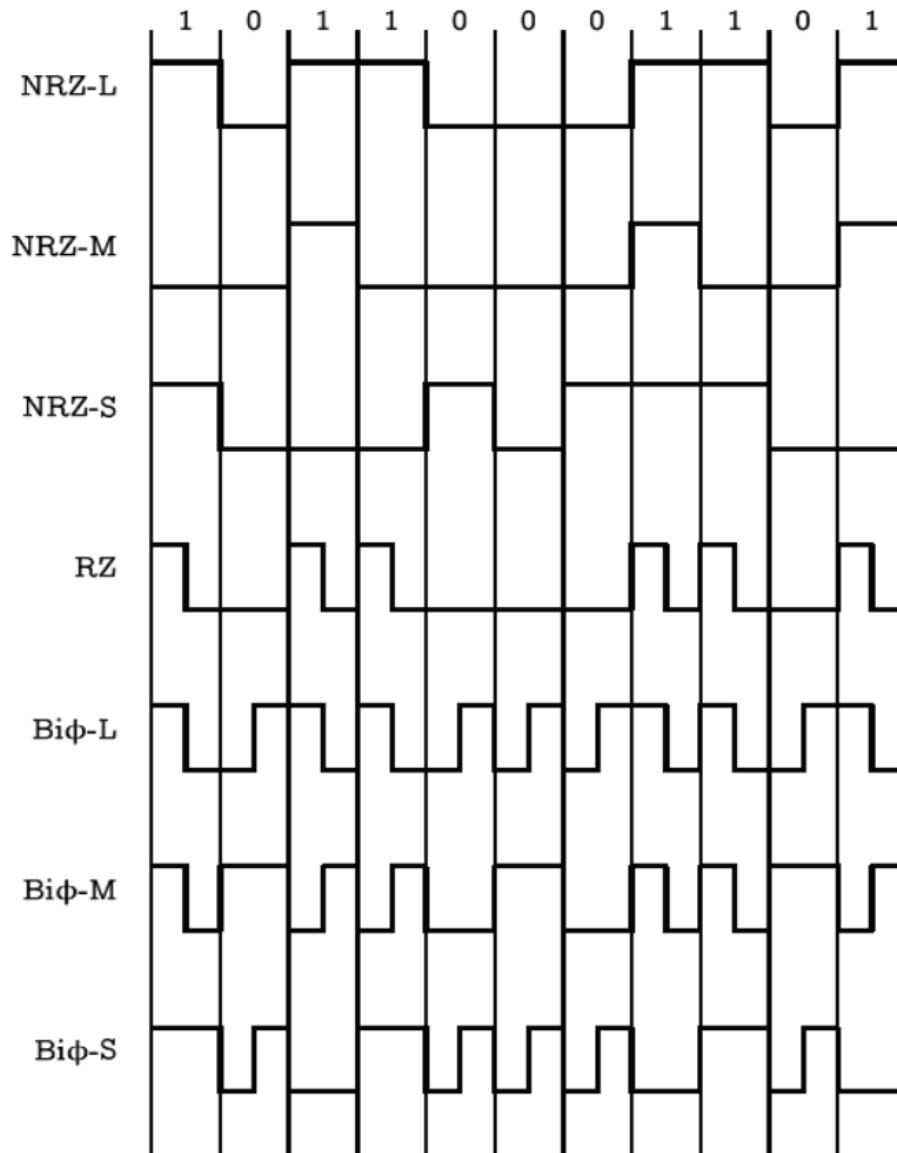
Layer 1: Physical Layer (Bitübertragungsschicht)

- Tatsächliche Übertragung einzelner Bits
- Übertragungsstrecke variiert
 - Twisted Pair (bis 10 Gbit/s)
 - Koaxialkabel (bis 10 Mbit/s)
 - Lichtleiter (bis 40 Gbit/s)
 - Luft (bis 1,3 Gbit/s)
- Übertragungstechnik:
 - Modulationsarten
 - Kodierungstechniken
 - Bittaktgenerierung
 - Wortsynchronisierung

Modulationsarten



Kodierung



NRZ-LEVEL (oder NRZ-CHANGE)

„1“ durch einen bestimmten,
„0“ durch einen entgegengesetzten Pegel dargestellt

NRZ-MARK

„1“ durch eine Pegeländerung,
„0“ durch keine Pegeländerung dargestellt

NRZ-SPACE

„1“ durch keine Pegeländerung,
„0“ durch eine Pegeländerung dargestellt

RZ

„1“ durch 1/2 Bit breiten Impuls,
„0“ durch keine Pegeländerung dargestellt

BI-PHASE-LEVEL (SPLIT-PHASE)

„1“ durch 1-0-Sprung,
„0“ durch 0-1-Sprung dargestellt

BI-PHASE-MARK

Pegeländerung alle Bitanfang
„0“ keine zweite Pegeländerung,
„1“ zweite Pegeländerung 1/2 Bit später

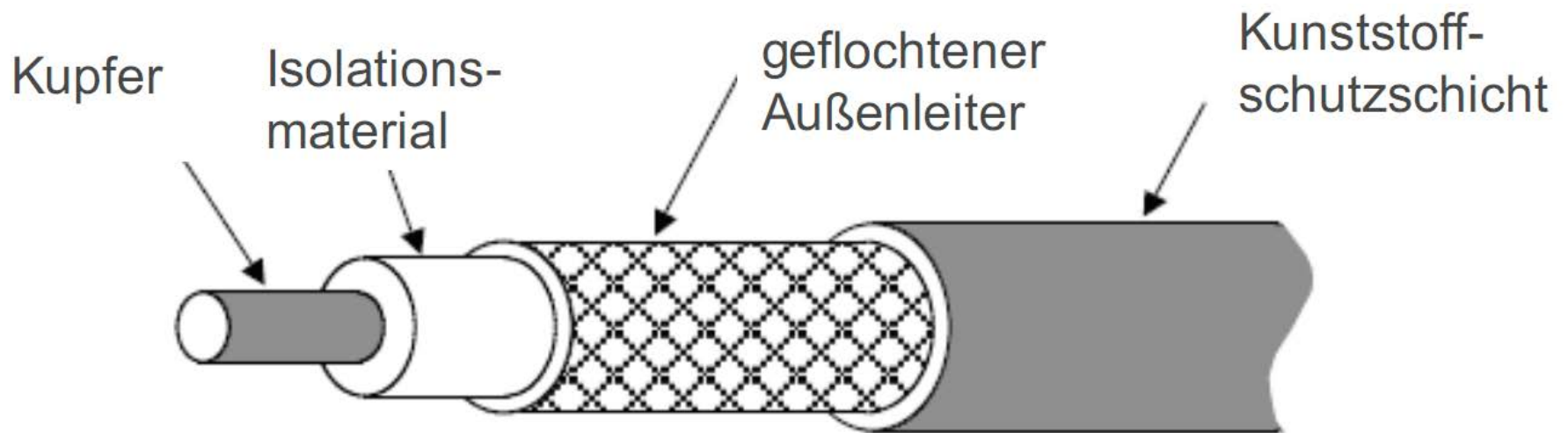
BI-PHASE-SPACE

Pegeländerung alle Bitanfang
„1“ keine zweite Pegeländerung,
„0“ zweite Pegeländerung 1/2 Bit später

- Koaxialkabel
 - Cheapernet (10Base2)
 - Thicknet (10Base5)

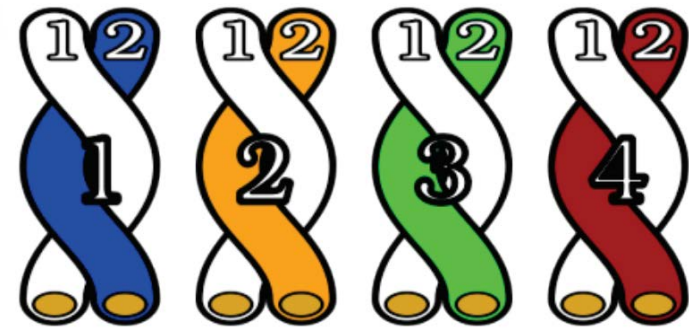


BNC (Bayonet Neill Concelman)

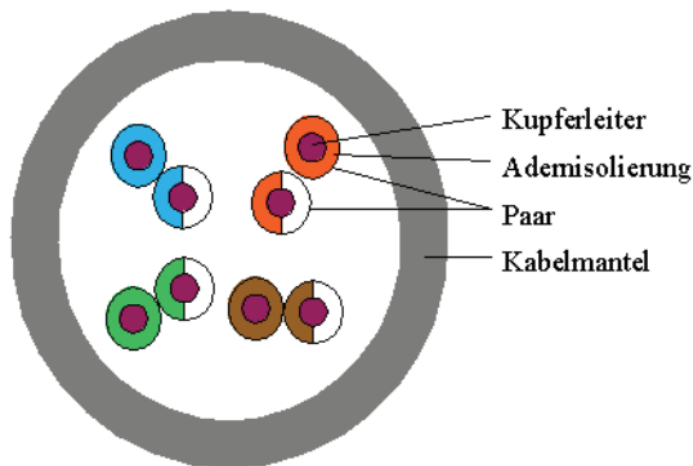


Übertragungsmedien

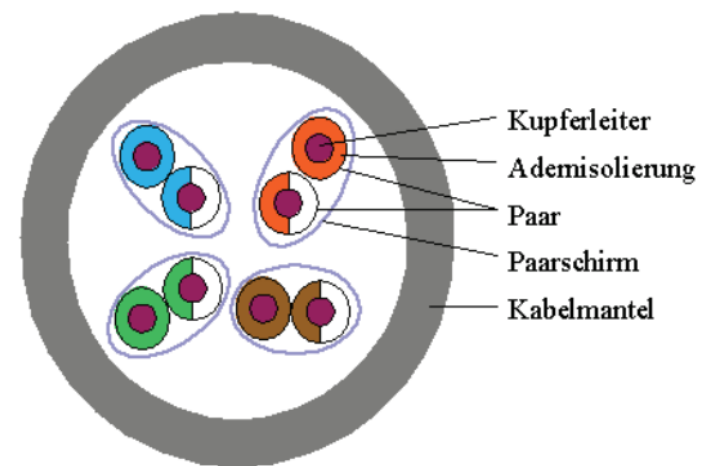
- Verdrilltes Adernpaar (Twisted Pair)
 - 2 x 1 mm dicke Kupferdrähte, schneckenförmig gewunden
 - Verdrillte Form wirkt elektromagnetischen Störungen entgegen
 - Unshielded/Shielded Twisted Pair
 - CAT5 (1000Base-T)



UTP



STP



Layer 2: Data Link Layer (Sicherungsschicht)

- Um Daten auszutauschen, müssen mehrere Stationen auf demselben Übertragungsmedium operieren
 - Koaxialkabel / Twisted Pair Kabel (Ethernet)
 - Glasfaser (FDDI)
 - Stromleitung
 - Luft (WLAN)
- Je nach Medium kann es zu Fehlern kommen
 - Gleichzeitiges Senden von zwei Stationen
 - Reichweite überschritten
 - Korrupte Daten
- Layer 2 kümmert sich um diese Probleme
 - MAC = Medium Access Control

MAC auf Kabelmedien

- IEEE 802.3
 - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection (CSMA/CD)
- Halbduplex Variante
 - Entweder Senden oder Empfangen
 - Bei gleichzeitigem Senden: Kollision
 - Jam-Signal senden, Übertragung wiederholen
- Vollduplex Variante
 - Kein CSMA/CD mehr notwendig
- Eingesetzt bis 1 Gigabit (1000Base-T)
- Ab 10GBase-T nur noch Vollduplex, kein CSMA/CD mehr



Beispiel:

```
user@meinRechner:~$ ifconfig
```

```
eth0  Link encap:Ethernet  HWaddr 00:1e:c9:2d:20:45  
      inet addr:128.130.60.13  Bcast:128.130.60.127  Mask:255.255.255.128  
      inet6 addr: fe80::21e:c9ff:fe2d:2045/64  Scope:Link  
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
      RX packets:4206193 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:6694449 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:766746719 (766.7 MB)  TX bytes:8334752712 (8.3 GB)  
      Interrupt:17
```

MAC auf geteilten Medien

- CSMA/CA
 - Carrier Sense Multiple Access with Collision Avoidance
 - Auch heute noch im Einsatz (WiFi)
- Wird verwendet, wenn das Medium während des Sendens nicht überwacht werden kann (z.B. WLAN)
- „First listen then talk“
- ACK vom Receiver statt Jam-Signal
- Nur für Halbduplex

Medium Access Control

- Netzwerkgeräte brauchen eine Adresse um auf Schicht 2 des OSI Modells operieren zu können
 - Unabhängig von der verwendeten Übertragungsmethode
- MAC-Adressen sind 6 x 8 Bit Tupel in HEX dargestellt
 - z.B. 02-00-54-55-4E-01
- Eindeutige Zuordnung für Netzwerkelemente
 - Verschiedene Prefixe pro Hersteller (z.B. 70-1A-04-XX-XX-XX für Liteon)
- Sicherheitsaspekte:
 - MAC Spoofing (Schicht 2 Attacke)
 - Abhören
 - DOS

Beispiel:

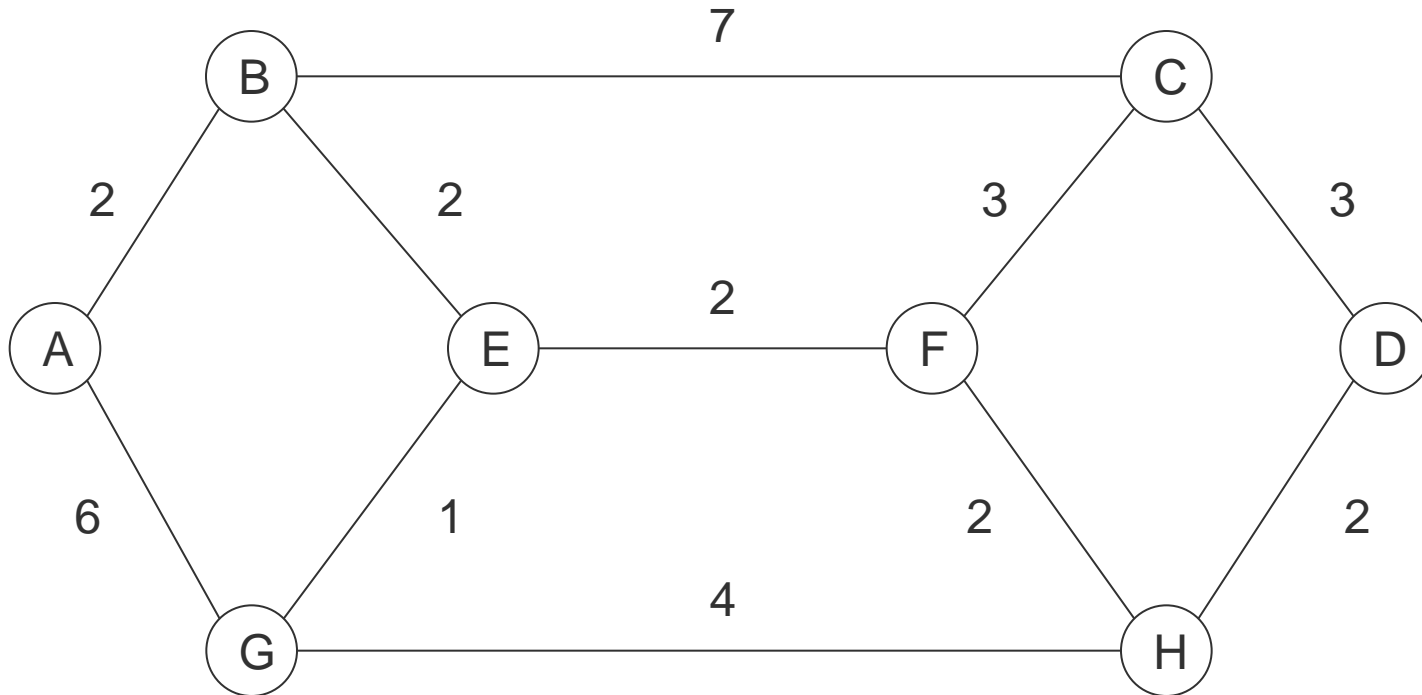
```
user@meinRechner:~$ ifconfig
```

```
eth0  Link encap:Ethernet  HWaddr 00:1e:c9:2d:20:45  
      inet addr:128.130.60.13  Bcast:128.130.60.127  Mask:255.255.255.128  
      inet6 addr: fe80::21e:c9ff:fe2d:2045/64  Scope:Link  
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
      RX packets:4206193 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:6694449 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:766746719 (766.7 MB)  TX bytes:8334752712 (8.3 GB)  
      Interrupt:17
```


Schicht 3: Network Layer (Vermittlungsschicht)

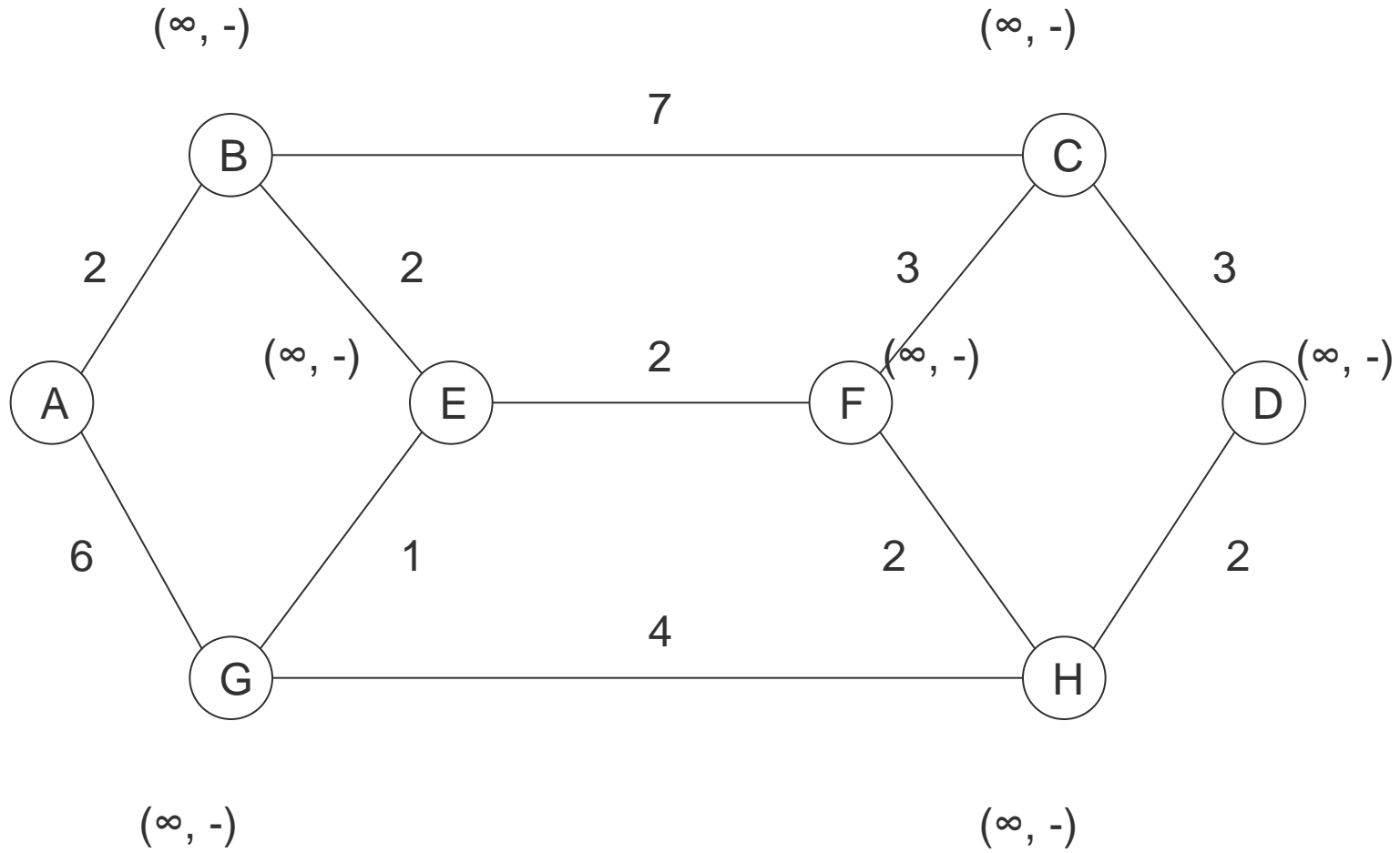
- Pakete vom Ursprung zum Ziel zu bringen (End-to-End Connection)
- Wegwahl (Routing) innerhalb von Netzwerken sowie über Netzwerkgrenzen hinweg
 - Virtuelle Verbindungen
 - Kann entweder von einem dedizierten Gerät (Router) oder Softwareservices erledigt werden
- Nicht adaptive/adaptive Routing-Algorithmen
 - Shortest Path/Flooding vs. Distance Vector/Link-State Routing
- Traffic Shaping und Reservierung von Bandbreite

Shortest Path Routing

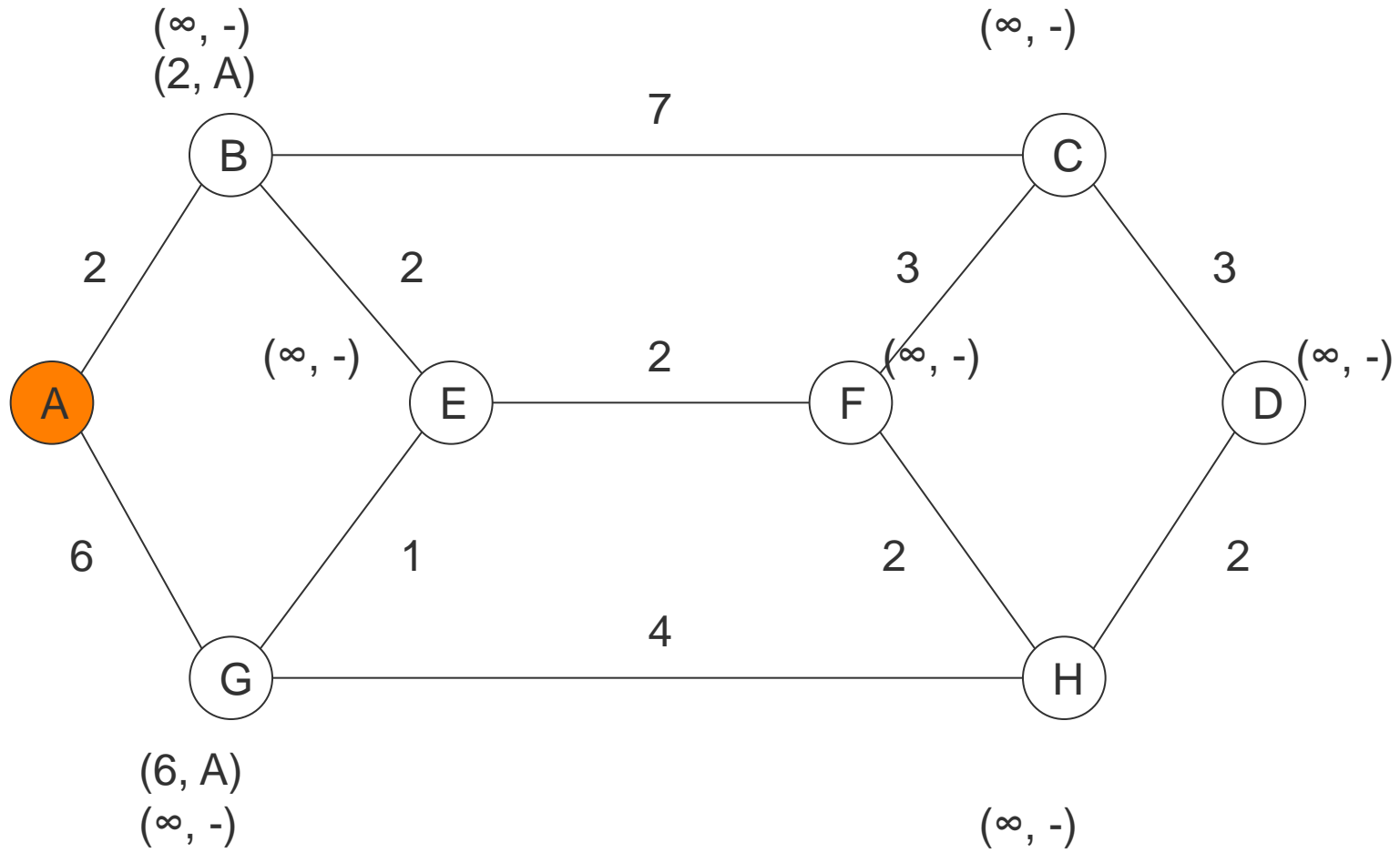


E. W. Dijkstra: *A note on two problems in connexion with graphs.*
In: *Numerische Mathematik 1* (1959), S. 269-271

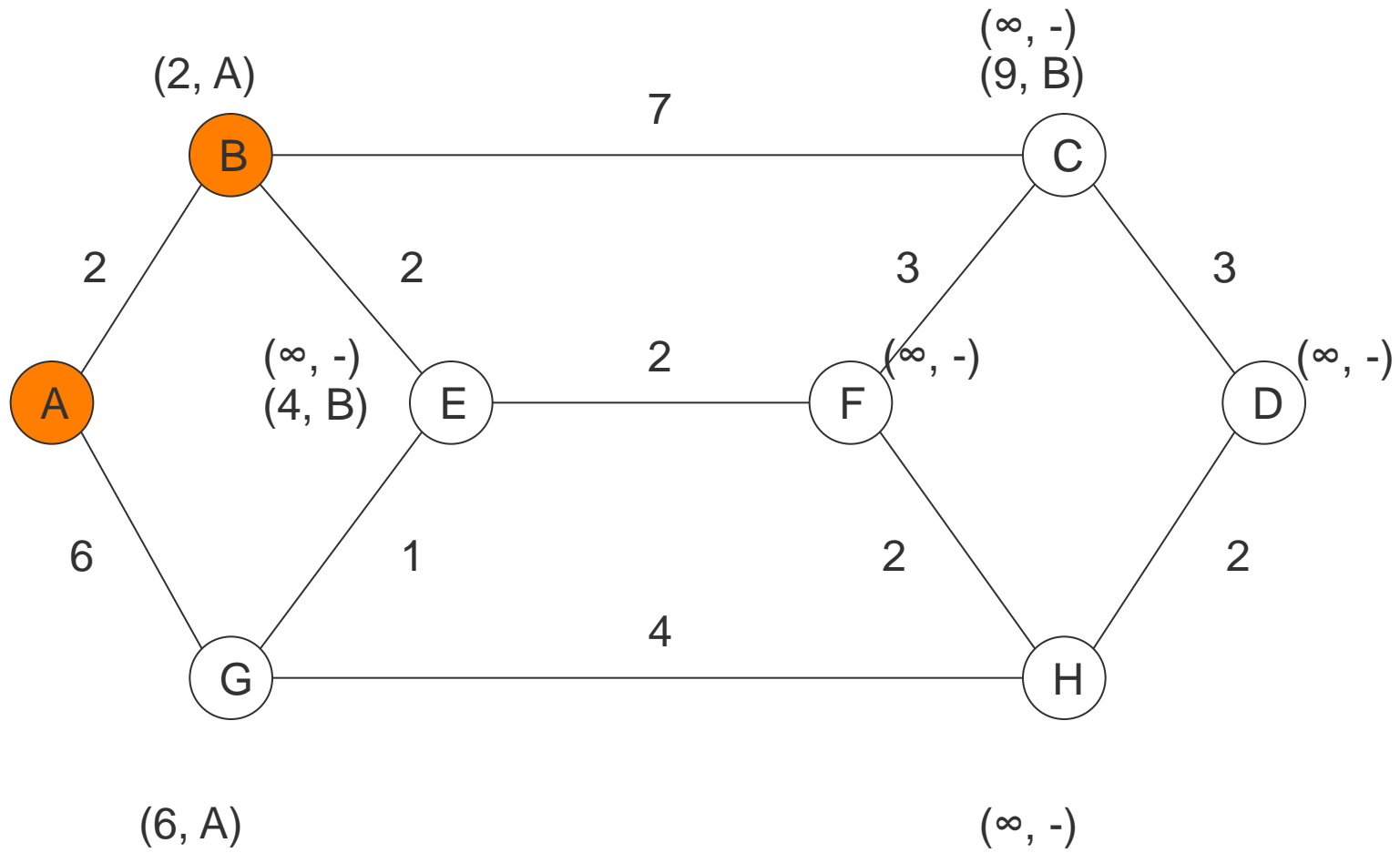
Shortest Path Routing



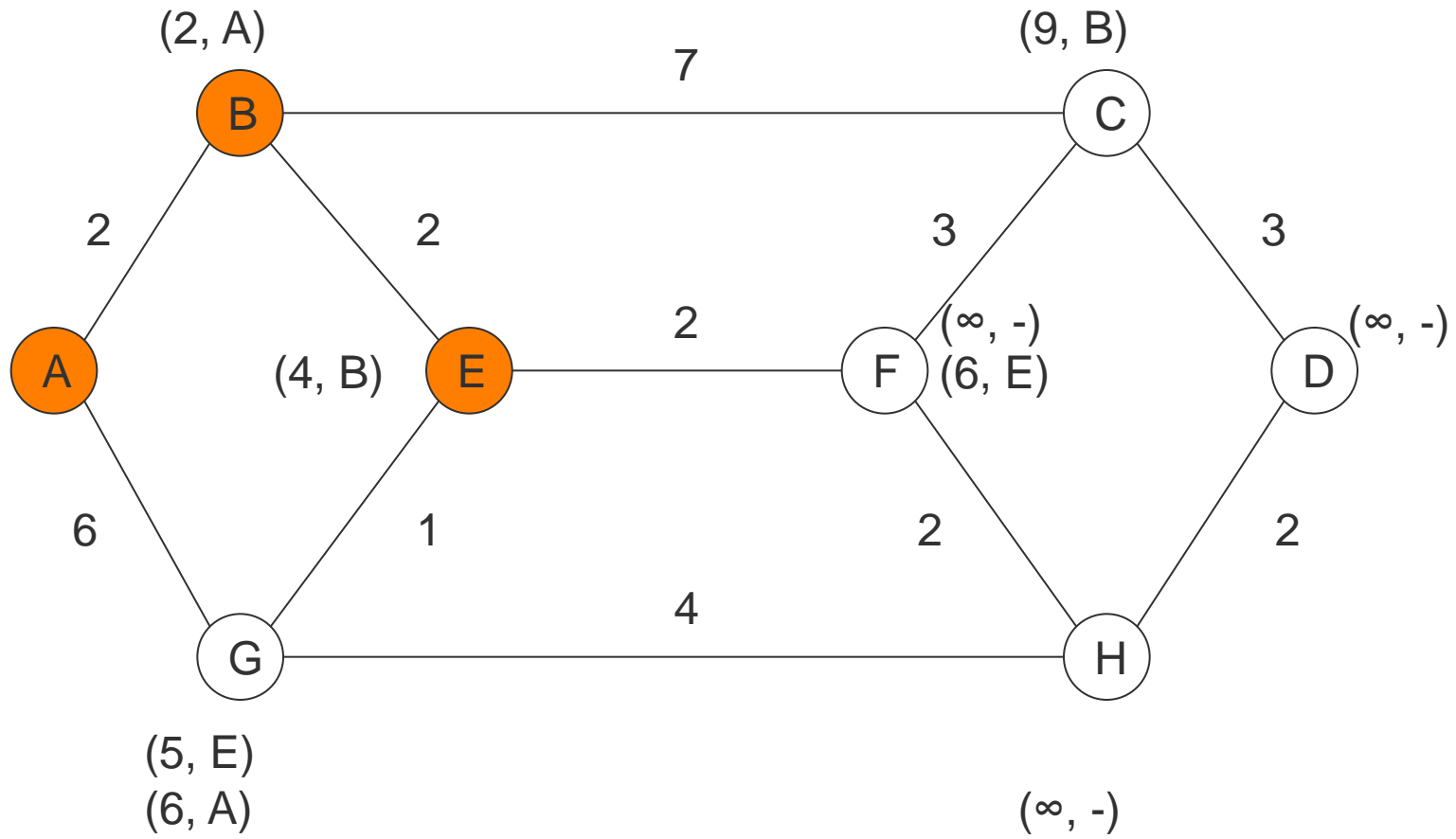
Shortest Path Routing



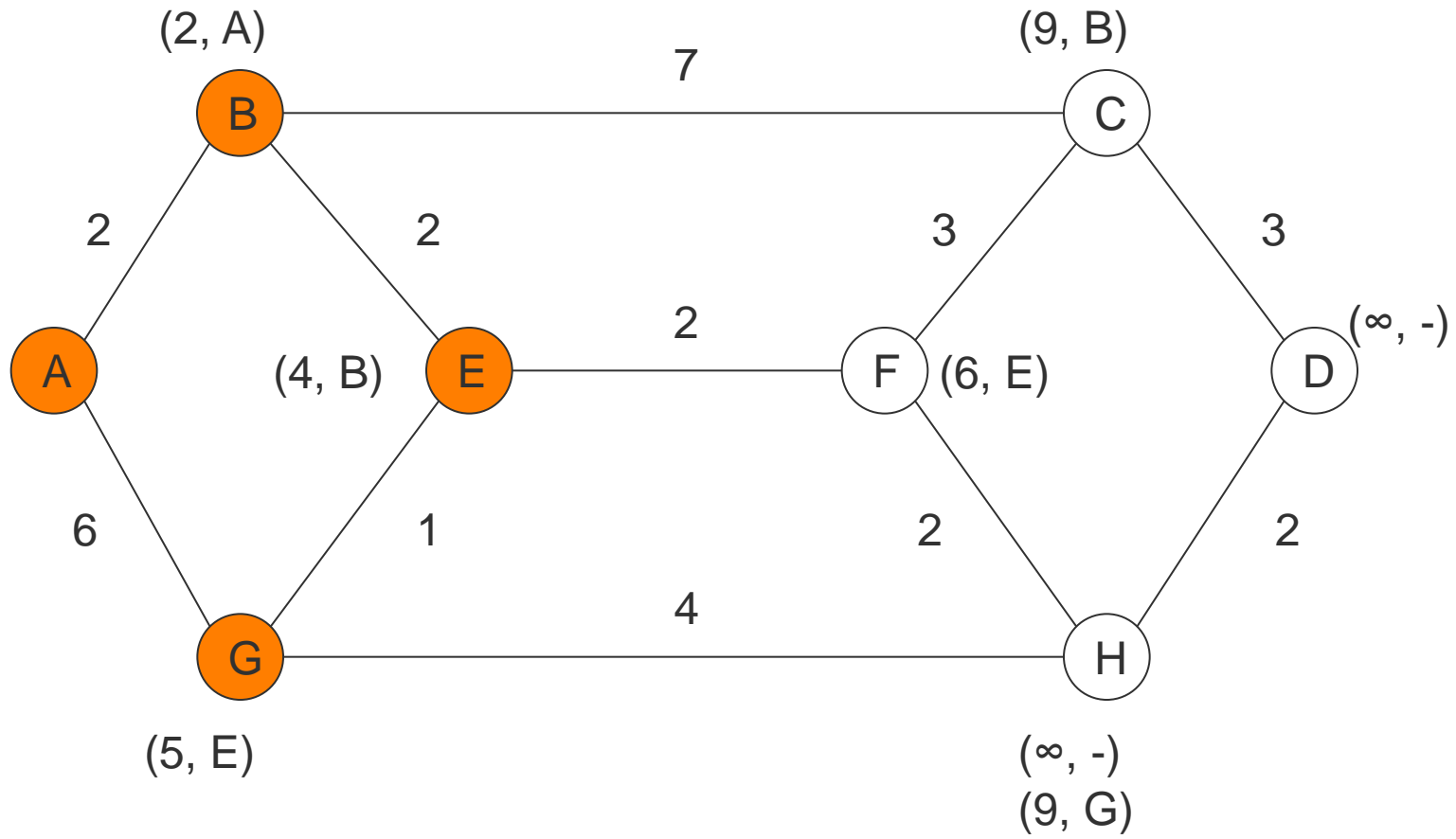
Shortest Path Routing



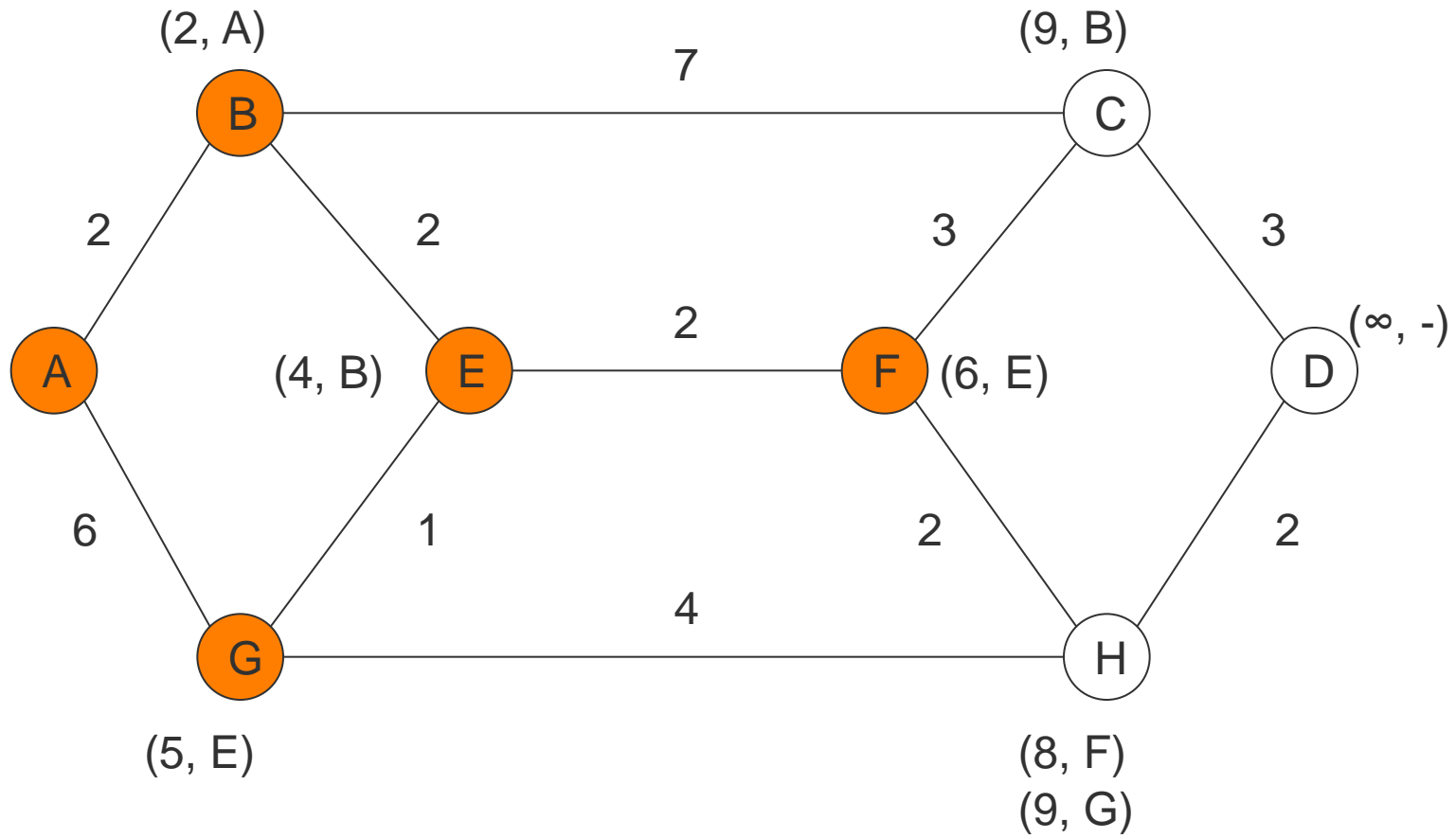
Shortest Path Routing



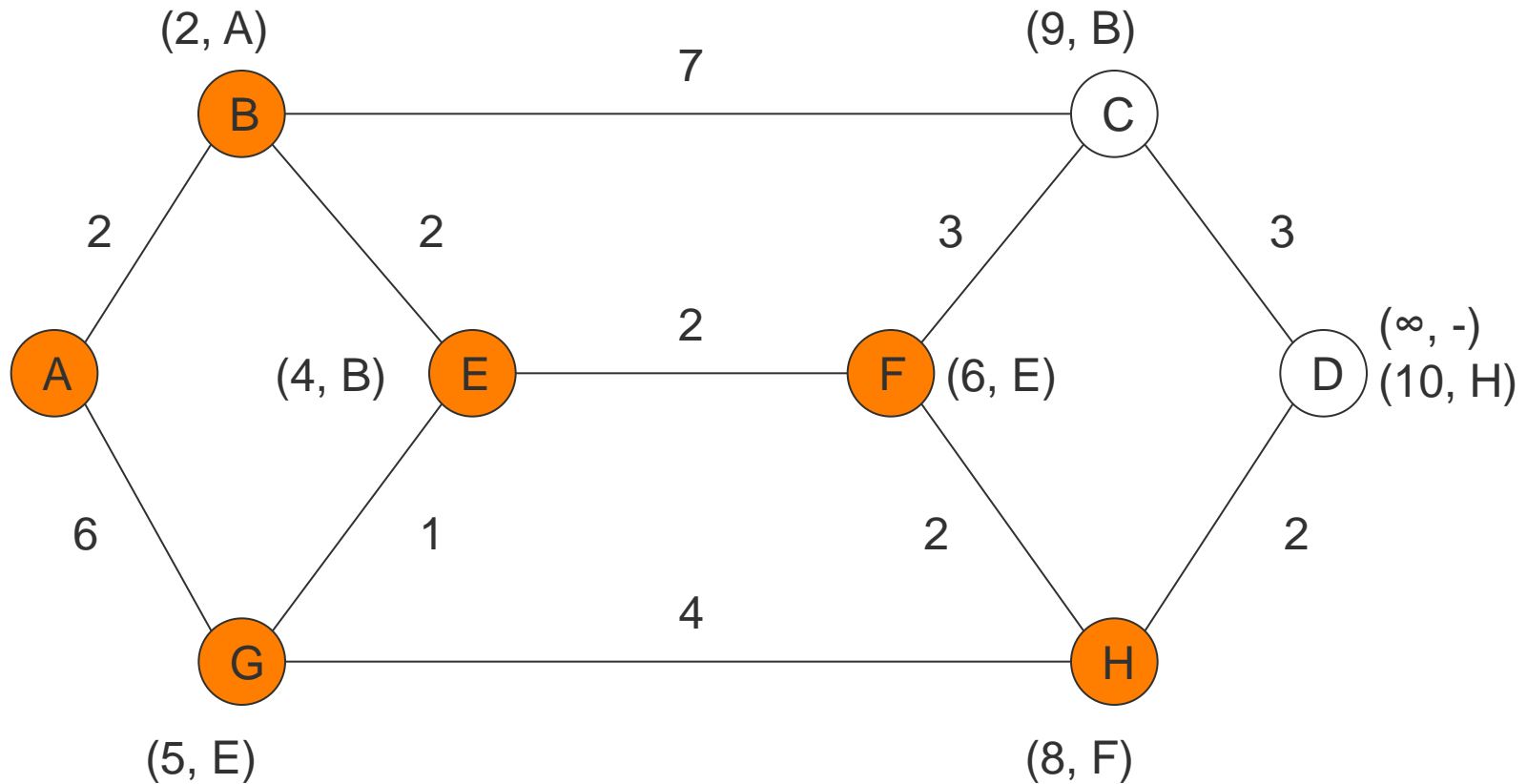
Shortest Path Routing



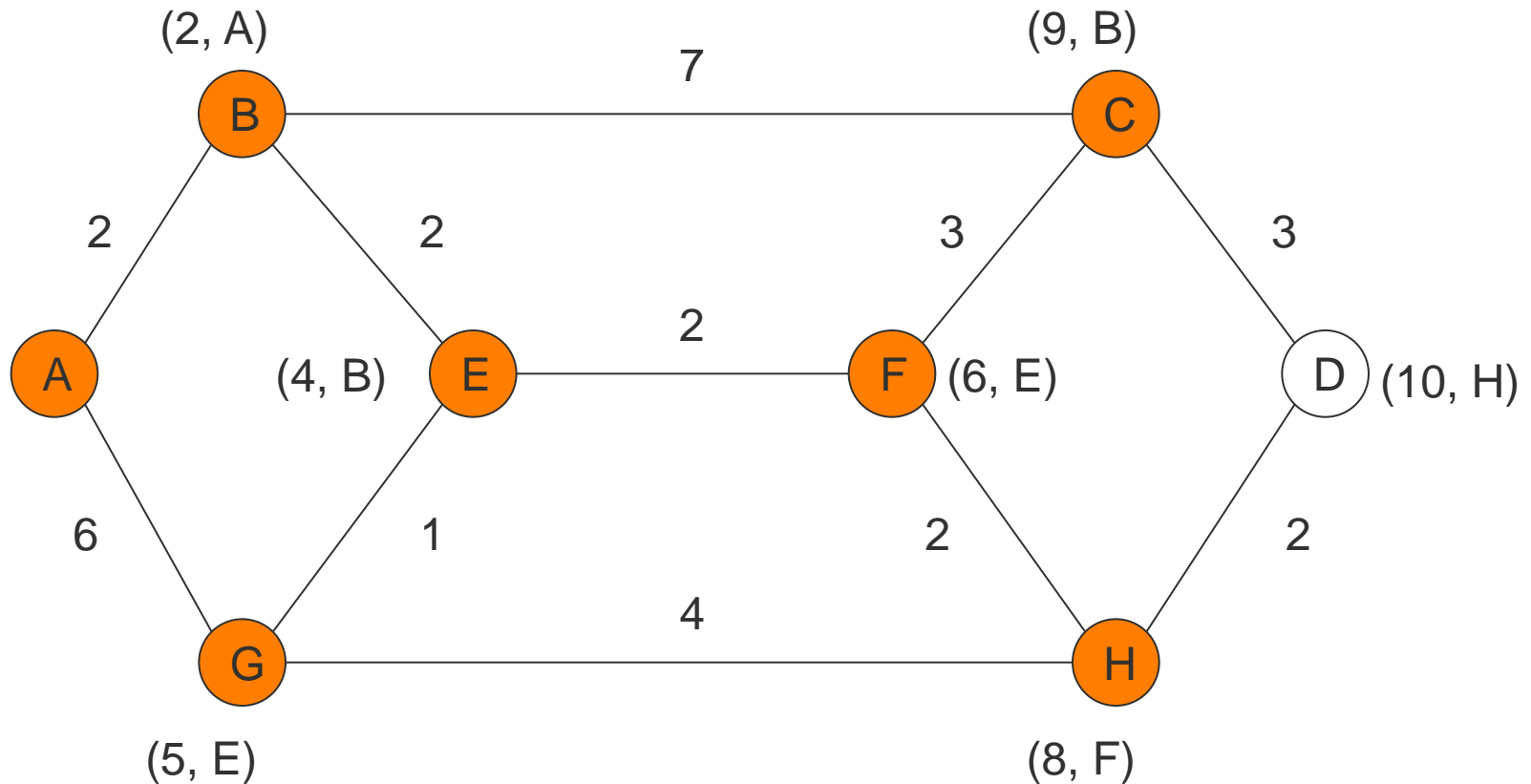
Shortest Path Routing



Shortest Path Routing



Shortest Path Routing



→ Gefundener Pfad: A – B – E – F – H – D mit Distanz 10

Layer 4: Transport Layer (Transportschicht)

- Logische Kanäle (Multiplexen und Demultiplexen)
 - z.B. Einrichten eines Sockets
- Zerlegung von Nachrichten in kleinere Einzelpakete
- Einhaltung der richtigen Reihenfolge
- Wiederholungsanforderungen
 - Handshake Implementierung
- Fehlerkontrolle von Endsystem zu Endsystem
 - Checksummen

Layer 5: Session Layer (Sitzungsschicht)

- Aufbau/Abbau von Sitzungen
- Überwachung eines Betriebs während einer Sitzung
 - Dialogsteuerung
 - „Token Management“
- Synchronisation
 - Atomic Actions
 - Check Points

Layer 6: Presentation Layer (Darstellungsschicht)

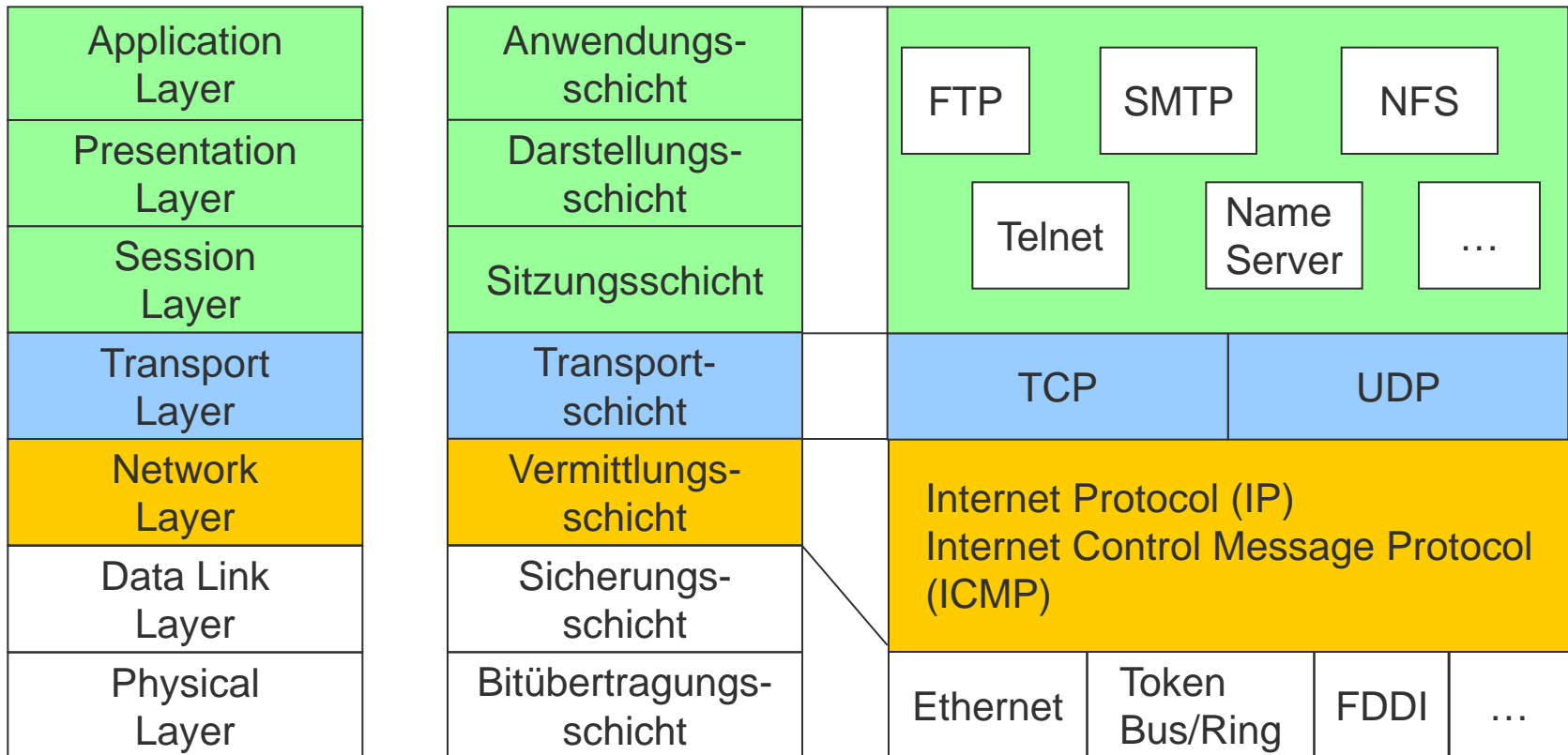
- Festlegung der Syntax und Semantik der zu übertragenden Daten
 - „Codierung“ der Daten
 - Implementierung von Protokollen (SMTP, HTTP, usw.)
- Schutz der Daten vor Zugriff unberechtigter Benutzer
 - Authentifizierung
 - Verfahren zur Verschlüsselung

Layer 7: Application Layer (Anwendungsschicht)

- Anbieten von Diensten für die eigentlichen Applikationen
 - Email-Service
 - Übertragung von Dateien
 - Remote Job Entry
 - Verzeichnisabfragen
 - virtuelle Netzterminals
 - ...

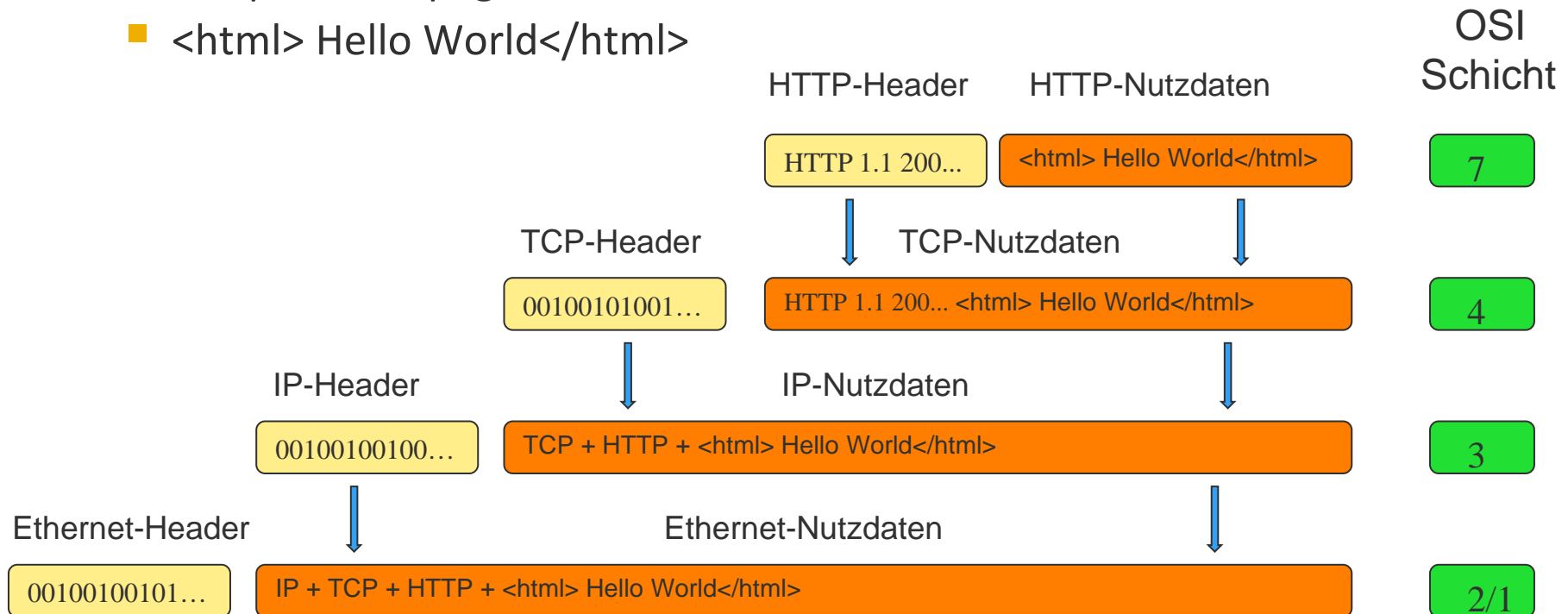
- Repeater (**Schicht 1**)
 - Keine Paket-Inspektion
 - Wird verwendet um entfernte Netze zu verbinden (Signalverstärkung)
- Bridge
 - Inspiziert eingehende Pakete (**Schicht 2**)
 - Stellt die Pakete nur zu, wenn die Empfänger-MAC sich auch wirklich auf der Gegenseite befindet
- Hub
 - Multi-Port Repeater
- Switch
 - Multi-Port Bridge
- Router
 - Arbeitet auf **Schicht 3**
 - Kann Routing-Tabellen verarbeiten um Pakete entsprechend zuzustellen (versteht das IP Protokoll)

Internetprotokoll Familie



Kapselung

- Nutzdaten werden durch Protokolle übertragen
- Jede Schicht verpackt ihre Daten in das darunterliegende Protokoll
- Beispiel: Webpage mit dem Inhalt
- `<html> Hello World</html>`

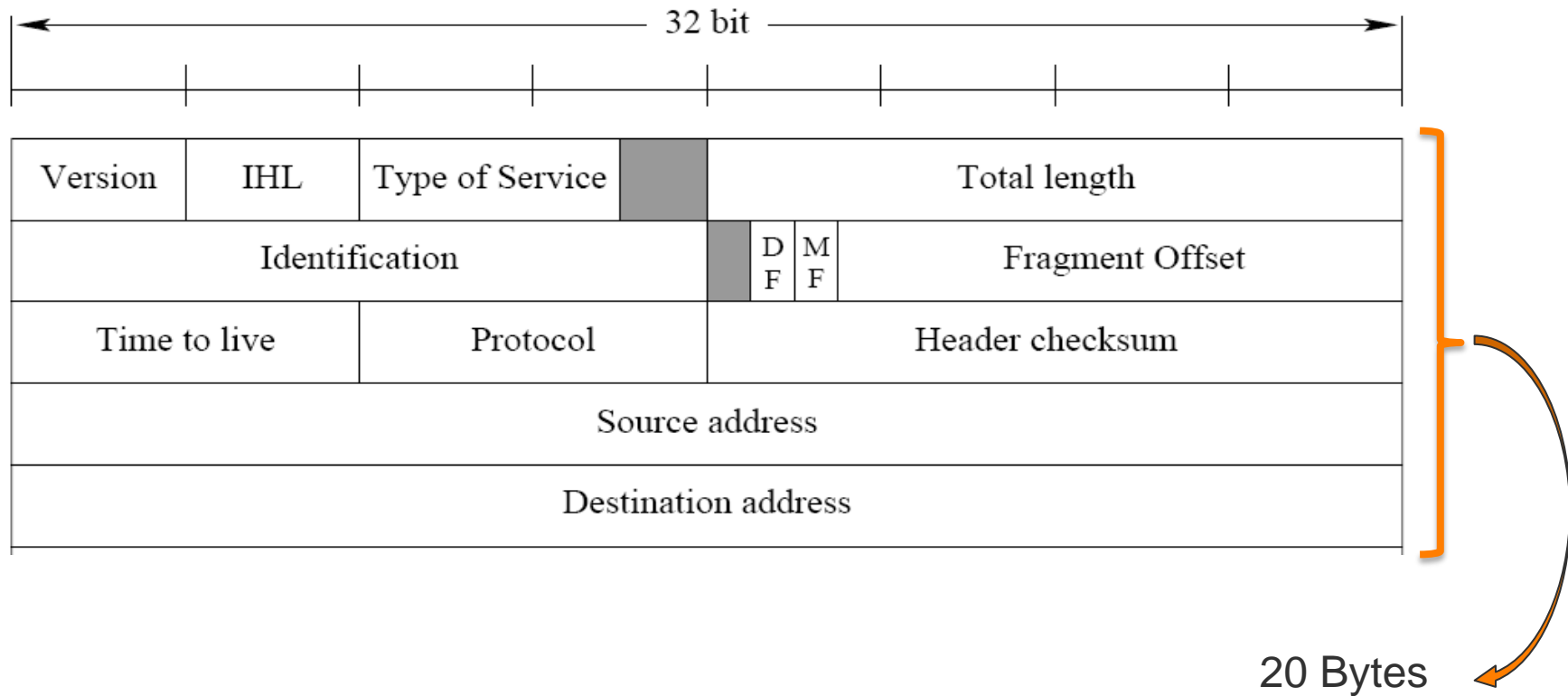


Beispiel:

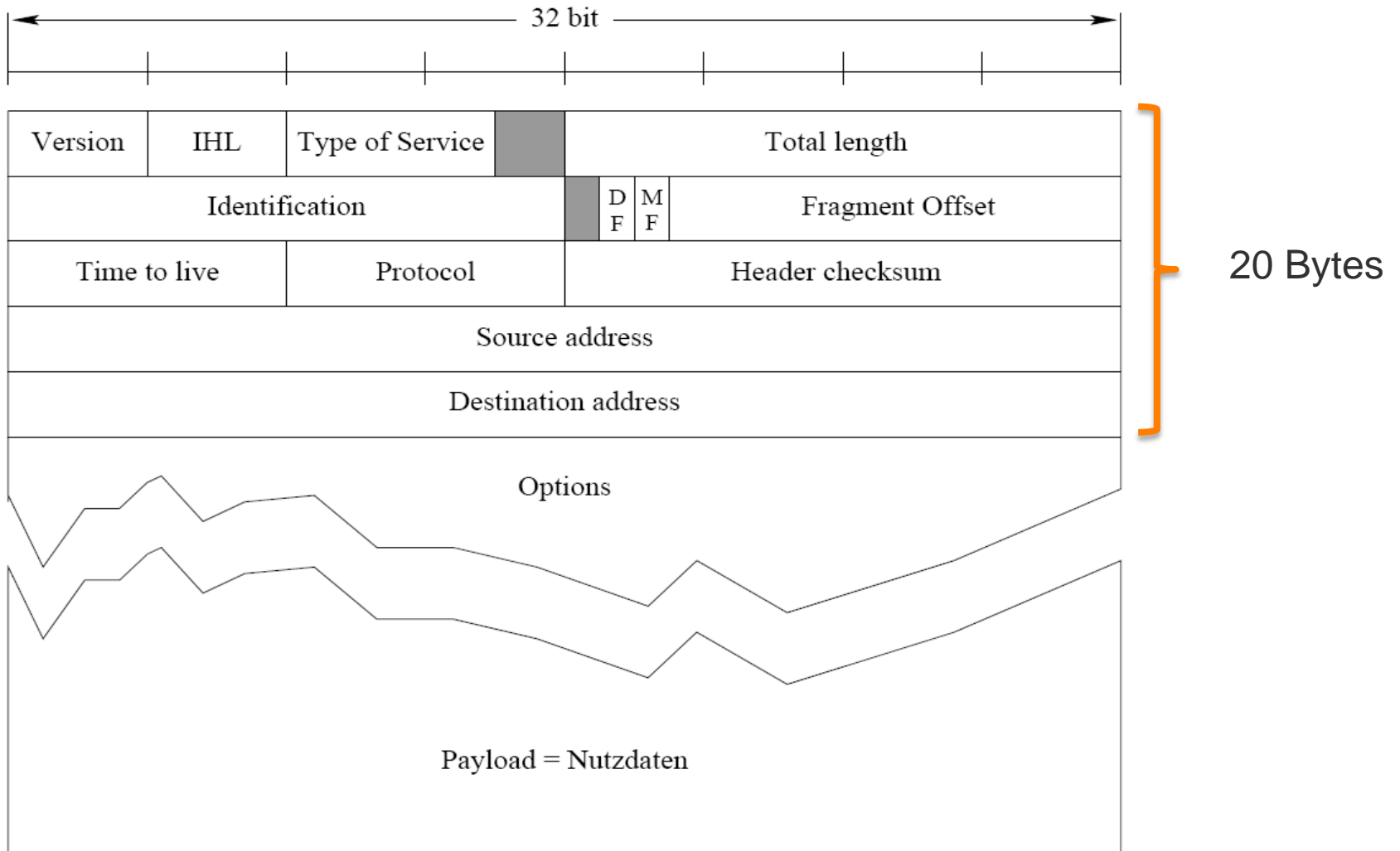
```
user@meinRechner:~$ ifconfig
```

```
eth0  Link encap:Ethernet  HWaddr 00:1e:c9:2d:20:45  
      inet addr:128.130.60.13  Bcast:128.130.60.127  Mask:255.255.255.128  
      inet6 addr: fe80::21e:c9ff:fe2d:2045/64  Scope:Link  
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
      RX packets:4206193 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:6694449 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:766746719 (766.7 MB)  TX bytes:8334752712 (8.3 GB)  
      Interrupt:17
```

Internet Protocol (IP, RFC 793)



Internet Protocol (IP)



- 32-Bit numerisches 4-Tupel (z.B. 128.130.2.3)
 - 2^{32} mögliche IP-Adressen (4 GiBi)
- Spezielle Adressen
 - Limited (Local) Broadcast: 255.255.255.255
 - Callback (Localhost): 127.0.0.1 – 127.255.255.254
- “Private” oder lokale IP-Adressen
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0.0 – 172.31.255.255
 - 192.168.0.0 – 192.168.255.255

IP-Header revisited (Ping Request)

ID	Source Address	Destination Address	Length	Summary
14	128.130.60.106	128.130.60.8	74	ICMP: Echo Request

ETHERNET: 00:07:E9:A6:EB:7A --> 00:30:48:12:27:C9 ETYPE = 0x0800, Protocol = Internet Protocol

- ETHERNET: Destination Address = 00:30:48:12:27:C9
- ETHERNET: Source Address = 00:07:E9:A6:EB:7A
- ETHERNET: Protocol = Internet Protocol

IP: 128.130.60.106 --> 128.130.60.8 ID = 0x33EC, Protocol = ICMP, Length = 60(0x003C)

- IP: Header Length = 20(0x14)
- IP: Version = 0x04
- IP: Type of Service = Normal Service
- IP: Length = 60(0x003C)
- IP: Identification = 13292(0x33EC)
- IP: Flags = 0(0x00)
- IP: Fragment = 0(0x00)
- IP: Time to Live = 128(0x80)
- IP: Protocol = ICMP
- IP: Checksum = 0x8D5E
- IP: Source Address = 128.130.60.106
- IP: Destination Address = 128.130.60.8

ICMP: Echo Request

Welche Protokoll-Nummer hat ICMP?

Wo steht die Header Length?

0x00:	00 30 48 12 27 C9 00 07 E9 A6 EB 7A 08 00 45 00	.OH.'É..é!ëz..E.
0x10:	00 3C 33 EC 00 00 80 01 8D 5E 80 82 3C 6A 80 82	.<3i..I.I^I <jII
0x20:	3C 08 08 00 3A 5C 02 00 11 00 61 62 63 64 65 66	<...:\....abcdef
0x30:	67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76	ghijklmnopqrstuv
0x40:	77 61 62 63 64 65 66 67 68 69	wabcdefghi

Subnetting

- Warum?
 - Um Netzbereiche zu gruppieren / zu unterteilen
 - Um Routing zu ermöglichen
- Wie?
 - Definiert im Internet Standard Subnetting (RFC 950)
 - NIC (Network Information Center) verwaltet die Zuteilung
- Nicht zu verwechseln mit NAT (Network Address Translation)
 - Dient dazu, Subnetze mit NICHT öffentlichen IP-Adressen zu versorgen
 - Ermöglicht mehreren Clients den Zugriff über nur eine öffentliche IP-Adresse

Subnetting – Aufbau

- NIC vergibt eine Netzwerknummer + Größe und verwaltet diese
 - Bei Änderungen muss NIC kontaktiert werden
- Subnetze werden durch Nummer und Subnetzmaske identifiziert
 - z.B. 192.168.1.0 Subnetzmaske 255.255.255.0
 - Oder: 192.168.1.0/24 (CIDR-Notation)
- IP-Adressen (von einem Host) ebenfalls
 - z.B. 192.168.1.16 Subnetzmaske 255.255.255.0

Subnetting – Komponenten im Detail

Beispiel: 192.168.1.16 Subnetzmaske 255.255.255.0

	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
&	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
=	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0

Erste IP: **Netzwerkname:** 192.168.1.0 (IP AND Subnetzmaske)

Subnetting – Komponenten im Detail

Beispiel: 192.168.1.16 Subnetzmaske 255.255.255.0

	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
&	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
=	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0

Erste IP: Netzwerkname: 192.168.1.0 (IP AND Subnetzmaske)

Letzter Teil heißt **Hostnummer**: 16 (IP AND NOT Subnetzmaske)

Subnetting – Komponenten im Detail

Beispiel: 192.168.1.16 Subnetzmaske 255.255.255.0

OR
=

1	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
1	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

Erste IP: Netzwerkname: 192.168.1.0

(IP AND Subnetzmaske)

Letzter Teil heißt Hostnummer: 16

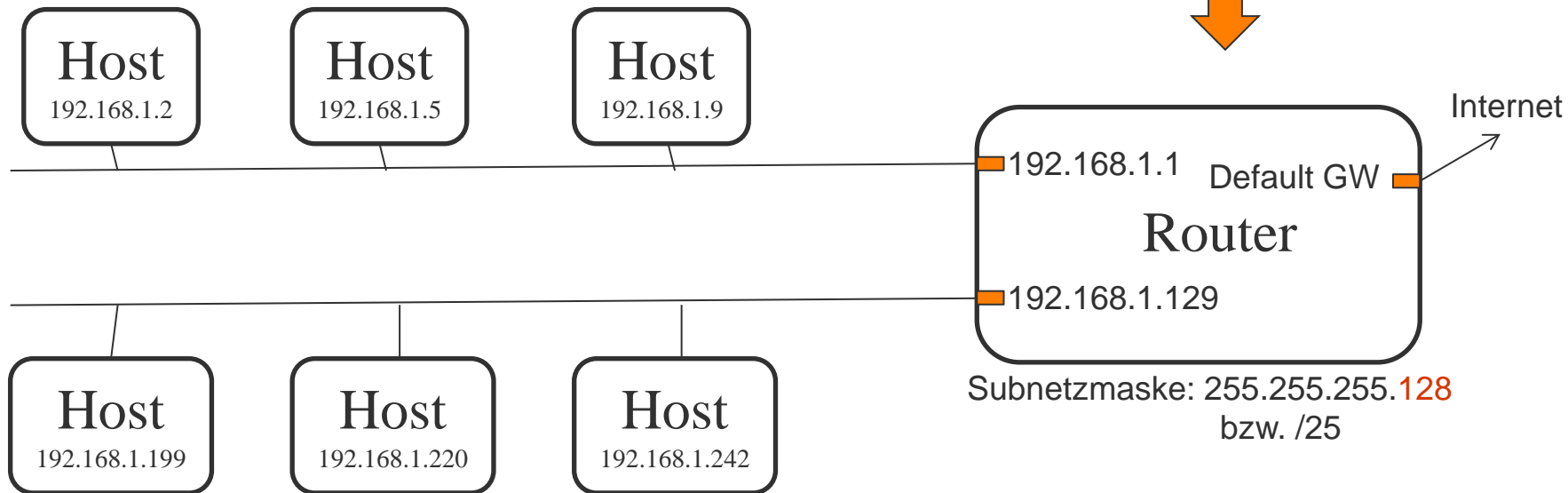
(IP AND NOT Subnetzmaske)

Letzte IP ist **Broadcast**: 192.168.1.255

(IP OR NOT Subnetzmaske)

Aufteilung von Subnetzen

- Nicht alle verfügbaren Adressen müssen demselben Subnetz zugeteilt werden
 - Aufteilung erfolgt nach denselben Regeln
 - Ein Router ist notwendig um die Subnetze zu verbinden
- Bsp: 192.168.1.0/24 in zwei gleich große Netze aufteilen
 - Netz 1: 192.168.1.0 bis 192.168.1.127
 - Netz 2: 192.168.1.128 bis 192.168.1.255



Zustellung eines IP-Pakets

- Schritte bei der Zustellung eines beliebigen IP-Pakets:

1) Ethernet Frame erstellen (Layer 2 Container)

- MAC der Quelle – eigene MAC-Adresse
- MAC des Ziels – wird durch ein eigenes Protokoll (ARP) ausgetauscht

2) IP-Frame erstellen (Layer 3 Container)

- IP-Adresse der Quelle – eigene Adresse
- IP-Adresse des Ziels

3) Paket abschicken. Aber wohin?

- a. Wenn Ziel-IP im eigenen Subnetz: Direkte Zustellung
- b. Wenn Ziel-IP in anderem Subnetz: Zustellung an das Gateway

Subnetztest: $(\text{Quell-IP AND Subnetzmaske}) == (\text{Ziel-IP AND Subnetzmaske})$

Beispiel:

```
user@meinRechner:~$ ifconfig
```

```
eth0  Link encap:Ethernet  HWaddr 00:1e:c9:2d:20:45
      inet addr:128.130.60.13  Bcast:128.130.60.127  Mask:255.255.255.128
      inet6 addr: fe80::21e:c9ff:fe2d:2045/64  Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:4206193 errors:0 dropped:0 overruns:0 frame:0
      TX packets:6694449 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:766746719 (766.7 MB)  TX bytes:8334752712 (8.3 GB)
      Interrupt:17
```

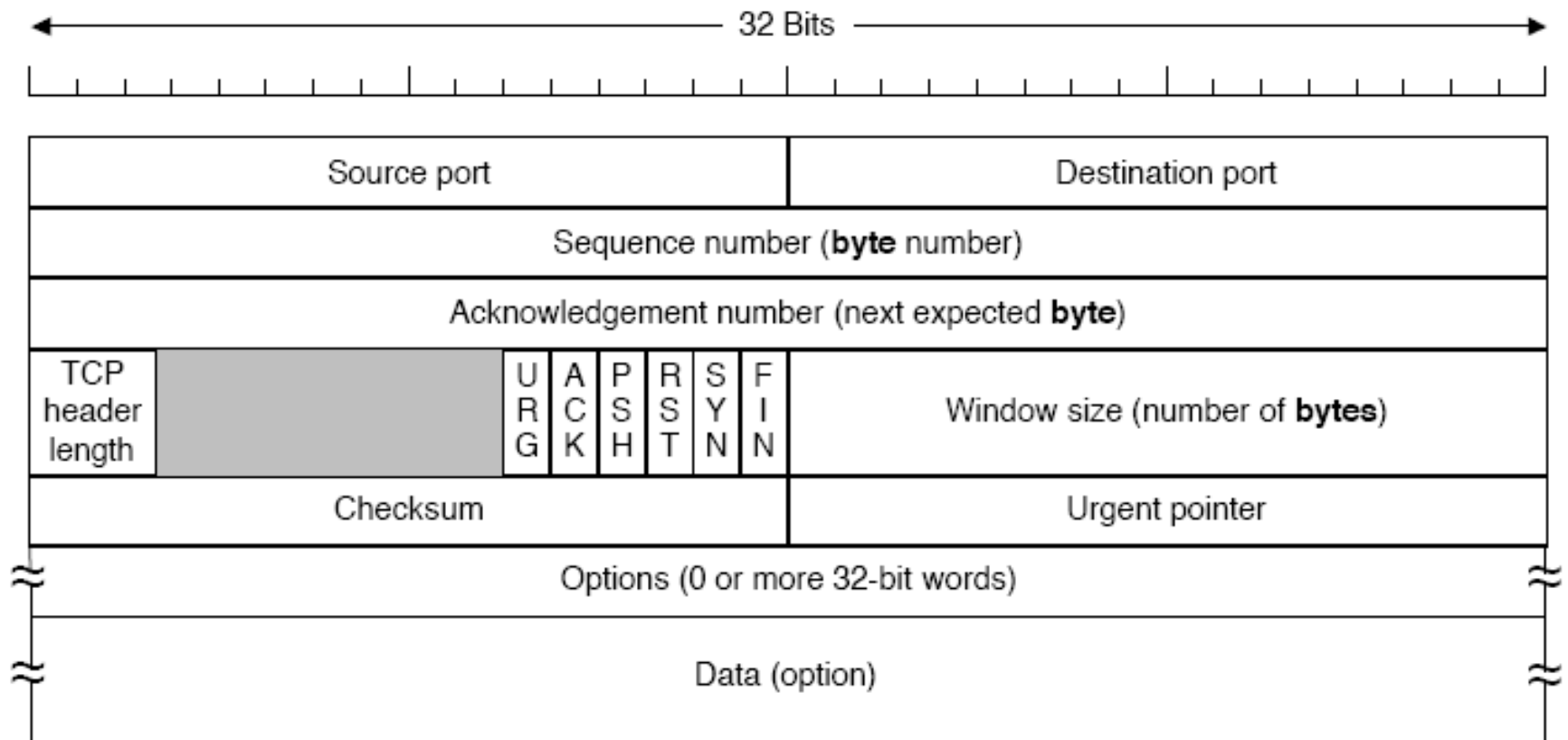
- Was passiert, wenn die Subnetzmaske 255.255.255.254 ist?
- Darf die Broadcast-Adresse frei vergeben werden?
- Darf der Netzwerkname vergeben werden?
- Gibt es „schräge“ Subnetzmasken?
 - Z.B. 255.255.255.12
- Kann man ein Netzwerk in ungleiche Teile aufteilen
 - Z.B. dritteln?

- http://www.geocaching.com/seek/cache_details.aspx?guid=02950517-4351-403e-a814-97d26e0e0357



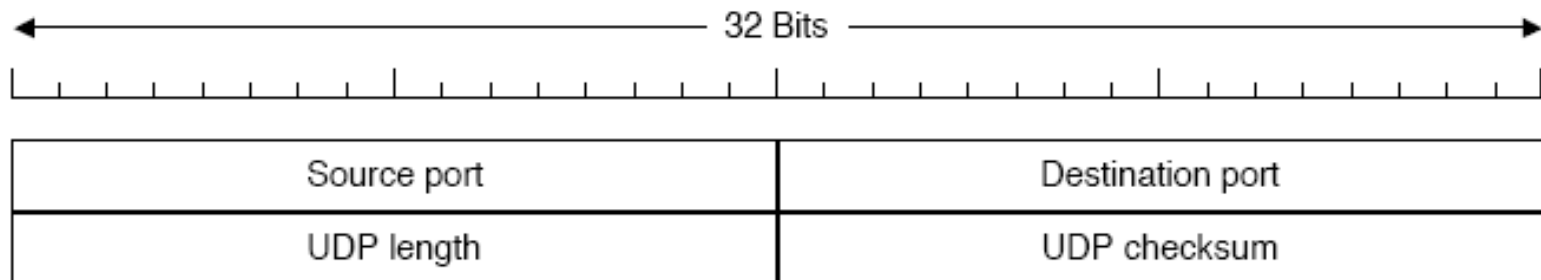
Transmission Control Protocol (TCP, RFC 793)

- Verbindungsorientiertes Protokoll
- Sockets: IP-Adresse und 16 Bit Nummer (Port)



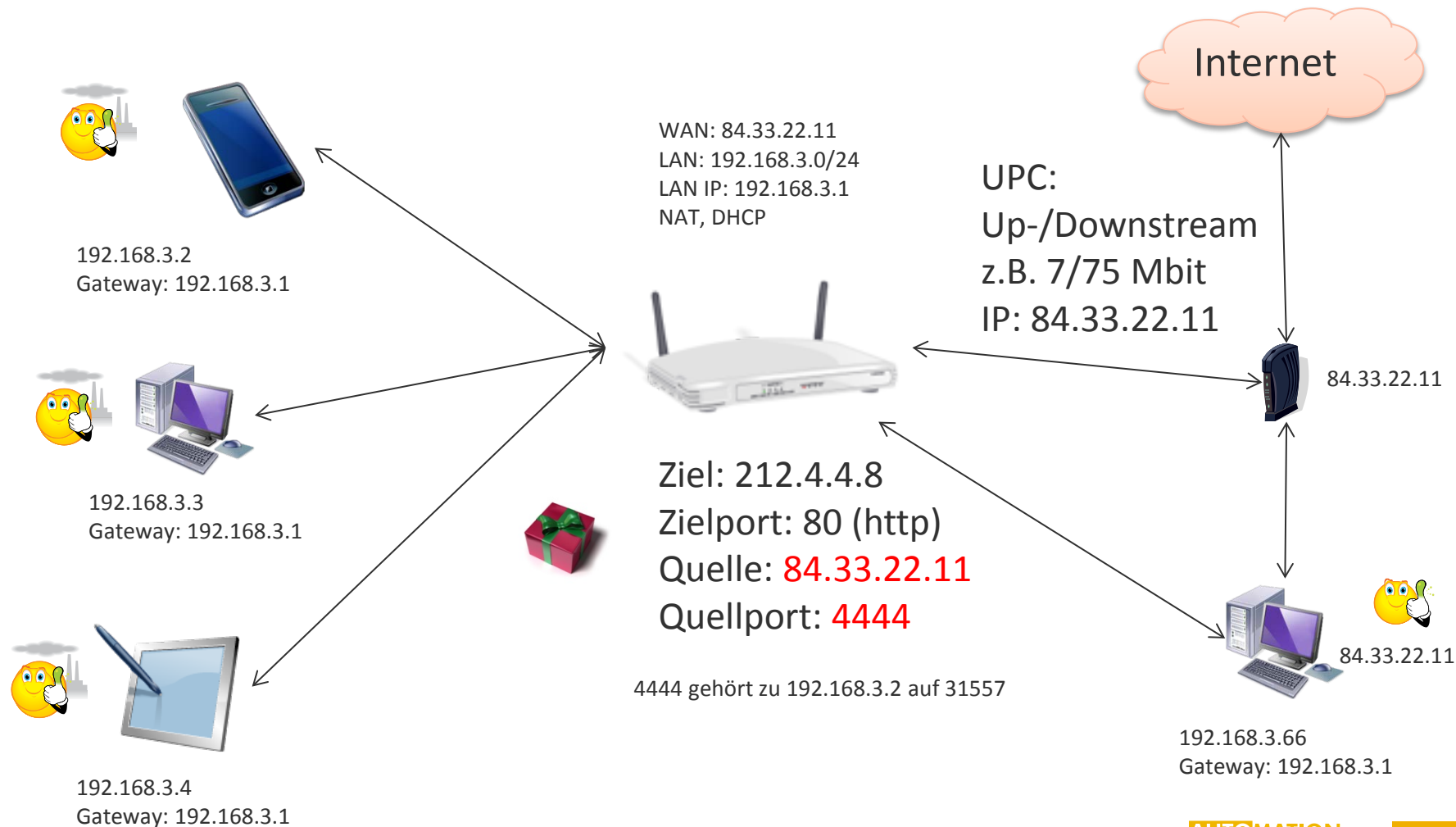
User Datagram Protocol (UDP, RFC 768)

- Verbindungsloses Protokoll
- Sockets: IP-Adresse und 16 Bit Nummer (Port)



NAT (Network Address Translation)

- Ziel: Eine externe IP für viele LAN-Teilnehmer.

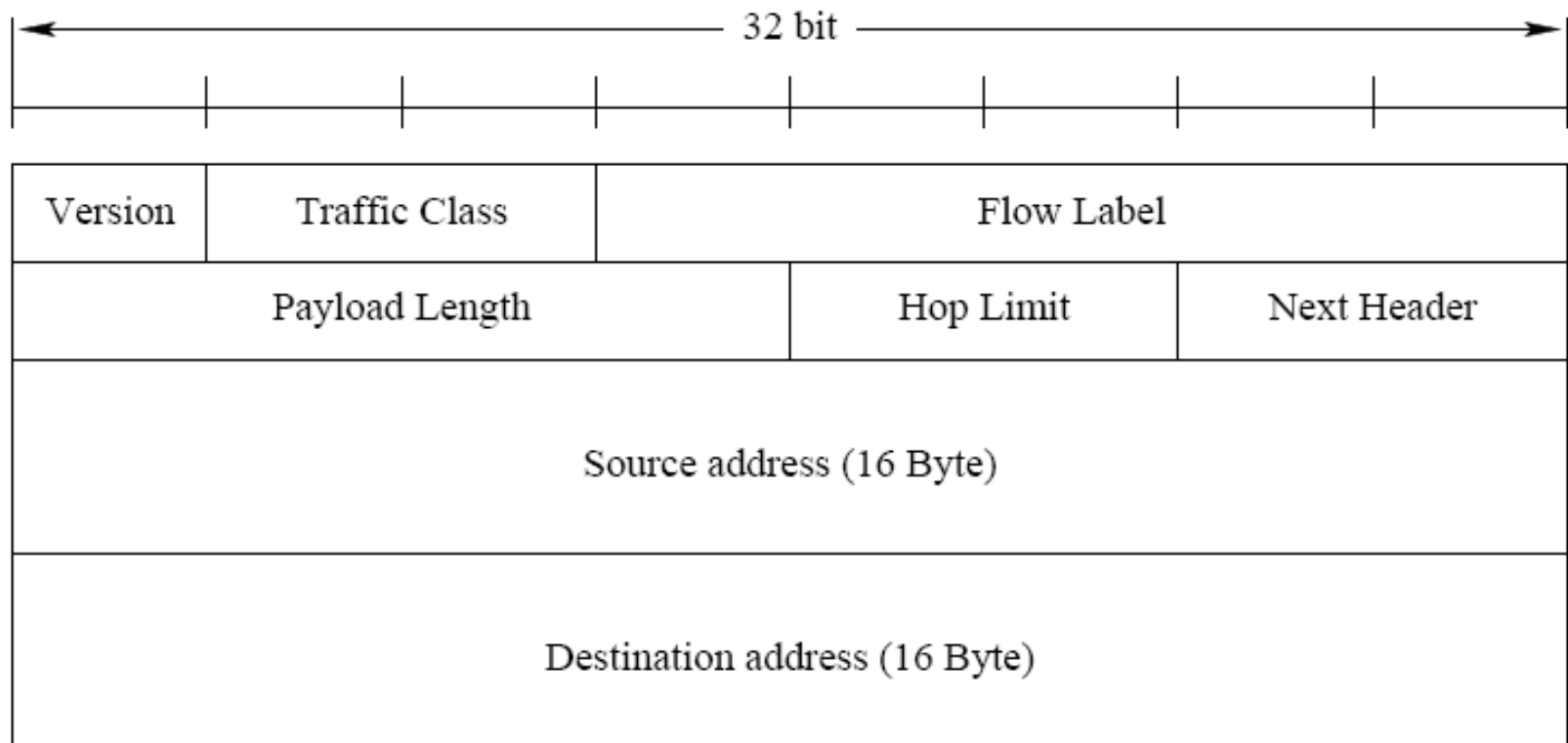


IPv4 vs IPv6

- IP-Adressbereich umfasst ca. 4 Milliarden Adressen
 - 1. Februar 2011: Die letzten beiden frei verfügbaren Netze wurden an APNIC vergeben (Asien, Pazifikraum)
 - 39.0.0.0/8 und 106.0.0.0/8
 - Adressen stark fragmentiert
 - Führt zu langen Routing-Tabellen
 - Benötigt starke Router
 - Prüfsummenfeld im IP-Header muss von JEDEM Router neu berechnet werden
 - Reger Handel mit IPv4 Adressen

- Abhilfe: IPv6

IP Version 6



- 16 Byte Adressen als 8x 2-Byte Hex Tupel (128 Bit)
 - Z.B. A687:0815:FEED:0000:0000:00AB:7F00:0001
 - Führende Nullen dürfen ausgelassen werden
 - A687:815:FEED:0:0:AB:7F00:1
 - Mehrere 0-Blöcke durch Doppelpunkt dargestellt (nur einmal!)
 - A687:815:FEED::AB:7F00:1
 - Letzten 4 Byte in Dezimalnotation zulässig
 - A687:815:FEED::AB:127.0.0.1
 - In URLs in eckigen Klammern
 - [http://\[A687:815:FEED::AB:127.0.0.1\]:80/](http://[A687:815:FEED::AB:127.0.0.1]:80/)
- Subnetze wie in IPv4 (allerdings nur in CIDR-Notation)
 - A687:815:FEED::AB:0:0 / 96
(A687:815:FEED::AB:0:0 bis A687:815:FEED::AB:FFFF:FFFF)

IP Version 6 – Unterschiede zu IPv4

- Broadcast-Adresse (Multicast)
 - Nicht mehr die letzte Adresse im Subnetz sondern:
 - ff02::1
- Localhost
 - ::1 (127.0.0.1)
- Lokale Adressen
 - Ähnlich wie z.B. 169.254.0.0/16
 - fe80:: /64
 - Wird aus der Interface – MAC Adresse errechnet
 - → Mehrere Adressen pro Interface sind in IPv6 üblich

Beispiel:

user@meinRechner:~\$ ifconfig

```
eth0  Link encap:Ethernet  HWaddr 00:1e:c9:2d:20:45
      inet addr:128.130.60.13  Bcast:128.130.60.127  Mask:255.255.255.128
      inet6 addr: fe80::21e:c9ff:fe2d:2045/64  Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:4206193 errors:0 dropped:0 overruns:0 frame:0
      TX packets:6694449 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:766746719 (766.7 MB)  TX bytes:8334752712 (8.3 GB)
      Interrupt:17
```


- Autokonfiguration und DNS
 - Ursprünglich von DHCP erledigt
- Hardware Infrastruktur fehlt
 - Firewalls
 - DOS Schutzmaßnahmen
 - Paketfilter
- Privacy
 - Besucher von Seiten sind auch Jahre später noch eruierbar
 - Direktes Mapping von IPs auf Menschen möglich
- Sicherheit

IPv6 – generelle Überlegungen

- Grundgedanke: Adressen für alles und jeden
 - Internet of Things
- Subnetting?
- IP sharing?
- Legacy...