Unterrichtsblöcke

Bl	Inhalt	Buch
01	Einleitung, Übersicht, Grundbegriffe	
02	OSI-Modell: L1 und L2	
03	OSI-Modell: L2 und L3	
04	OSI-Modell: L3 bis L7	
05	IP (Adressierung)	
06	IP (ARP, ICMP)	
07	Labor	
08	TCP	598-601
09	Internet	
10	Anwendungsprotokolle: DNS	
11	Anwendungsprotokolle: DHCP, Mail, rLogin	
12	Labor	
13	Anwendungsprotokolle: HTTP (+HTML)	
14	Labor	
15	WLAN und Netzsicherheit	

ND07: Transportschicht im Internet

Lernziele

- Sie können erklären, was die Hauptaufgaben und -Eigenschaften von TCP sind, wie ein TCP-Paket grob aufgebaut ist
- Sie können mit einem entsprechenden Tool TCP-Pakete auf dem Ethernet auffangen und deren Inhalt interpretieren.

Themen

- TCP
- UDP
- **Labor:** Lernübung zu TCP. Mit Ethereal/Wireshark TCP-Pakete auf dem Ethernet aufzeichen und interpretieren.

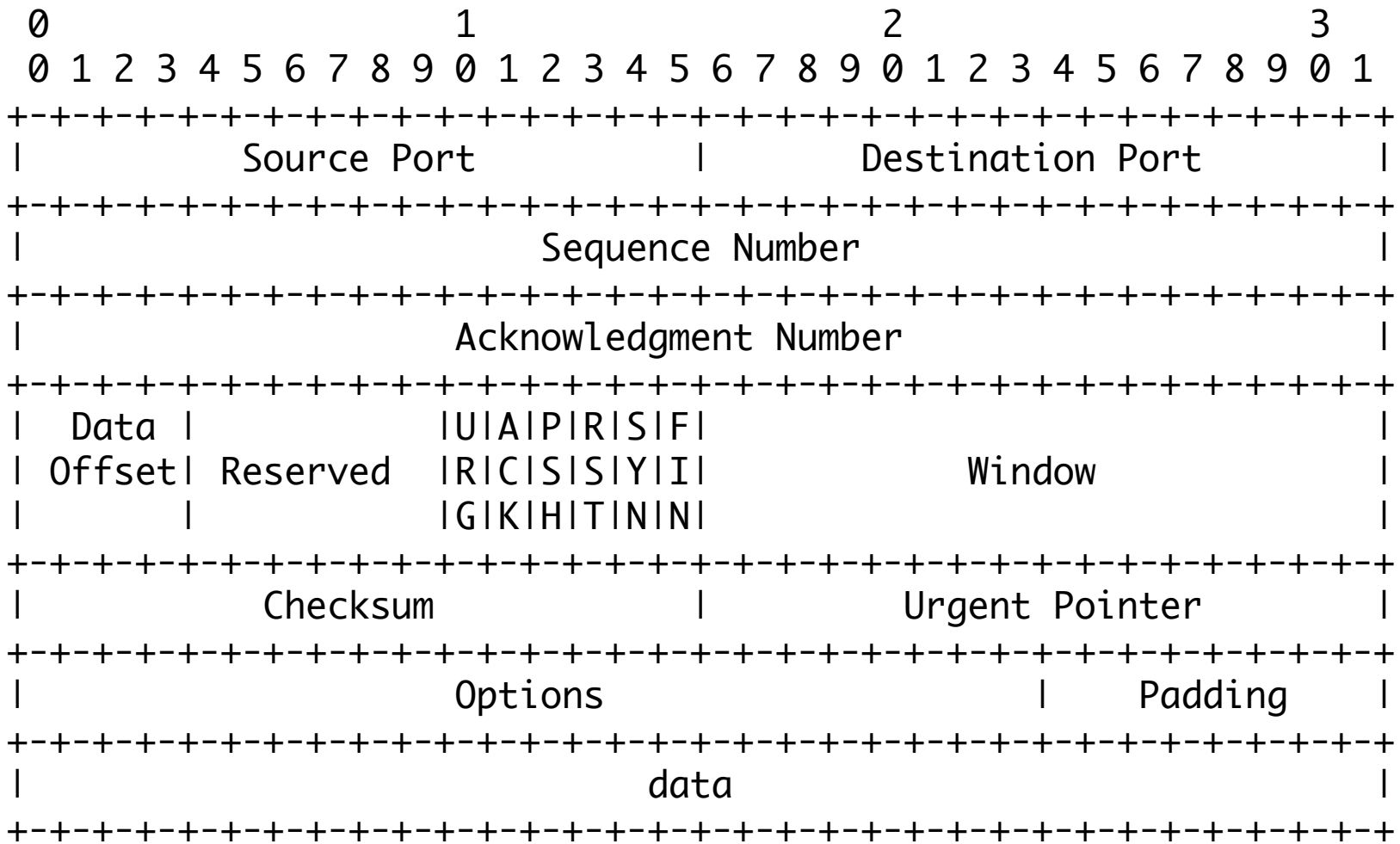
TCP (Transport Control Protocol)

- Bereitstellen eines zuverlässigen End-to-End Bytestromes (Virtueller Kanal)
  - Reihenfolge (Auf IP-Ebene beliebig) wird durch Sequenznummern festgelegt
  - Retransmit bei Timeout
  - Verwerfen von doppelten Paketen
- Die Endpunkte einer TCP-Verbindung werden Ports genannt
- Repräsentiert durch eine 16-Bit Zahl
- Programmiertechnisch werden die Endpunkte als Socket bezeichnet
- Die Flusssteuerung geschieht mittels sliding windows

→ TCP ist im RFC 793 beschrieben

TCP Paket-Header

Quelle: RFC 793



TCP Headerfelder 1/2

Source Port: Portnummer der Quelle

Destination Port: Portnummer des Ziels

Sequence Nbr: Sequenznummer des ersten Bytes in diesem Segment (Bei SYN=1: ISN (Initial Sequence Number)

Ackn. Nbr: Quittung, enthält die Sequenznummer des nächsten erwarteten Bytes

Data Offset: Anzahl der 32-Bit Worte des Headers (Offset an dem die Daten beginnen)

URG: Wenn "1": Urgent-Pointer ist gültig

ACK: Wenn "1": Acknowledgment Feld ist gültig

PSH: Push-Funktion, wenn "1": Empfänger soll die Daten direkt weiterleiten, ohne darauf zu warten, bis der Puffer gefüllt ist

TCP Headerfelder 2/2

RST: Wenn "1": Zurücksetzen der Verbindung (Abweisen von unerwünschten Verbindungen, technische Probleme)

SYN: Synchronisierung (Verbindungsaufbau)

FIN: Verbindungsabbau

Window: Grösse des Schiebefensters, gibt an, wieviele Bytes gesendet werden können

Checksum: Prüfsumme

Urgent Pointer: Position der "Urgent"-Daten im Datenstrom (selten benutzt)

Options: Weitere Optionen, z.B. Maximalgrösse des Datensegmentes

Padding: Fullbits umd auf eine 4-Wort-Grenze zu kommen

(Data: Nutzdaten, gehören nicht mehr zum Header)

n|w

TCP Verbindungsaufbau

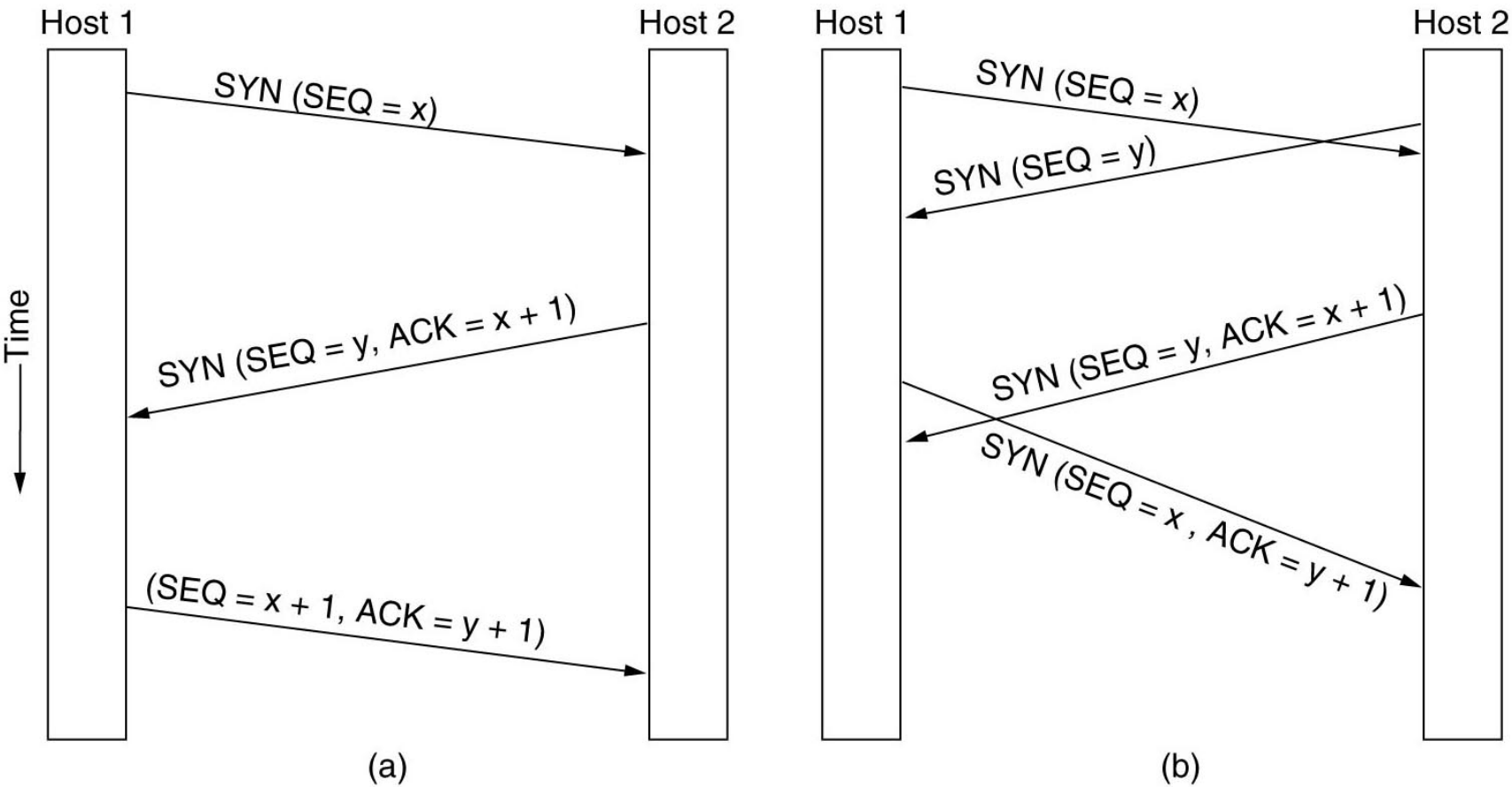


Fig: 6-31[1], Verbindungsaufbau

[1] A. Tanenbaum, "Computer Networks", http://authors.phptr.com/tanenbaumcn4/

TCP Verbindungsaufbau (wireshark)

```
Internet Protocol, Src Addr: 10.1.94.40 (10.1.94.40), Dst Addr: 209.85.135.103 (209.85.135.103)
    [...]
Transmission Control Protocol, Src Port: 42713 (42713), Dst Port: www (80),
                               Seq: 3790047064, Ack: 0, Len: 0
    [...]
    Flags: 0x0002 (SYN)
    [...]
```

```
Internet Protocol, Src Addr: 209.85.135.103 (209.85.135.103), Dst Addr: 10.1.94.40 (10.1.94.40)
    [...]
Transmission Control Protocol, Src Port: www (80), Dst Port: 42713 (42713),
                               Seq: 1340889640, Ack: 3790047065, Len: 0
    [...]
    Flags: 0x0012 (SYN, ACK)
    [...]
```

```
Internet Protocol, Src Addr: 10.1.94.40 (10.1.94.40), Dst Addr: 209.85.135.103 (209.85.135.103)
    [...]
Transmission Control Protocol, Src Port: 42713 (42713), Dst Port: www (80),
                               Seq: 3790047065, Ack: 1340889641, Len: 0
    [...]
    Flags: 0x0010 (ACK)
    [...]
```

TCP Verbindungsabbau

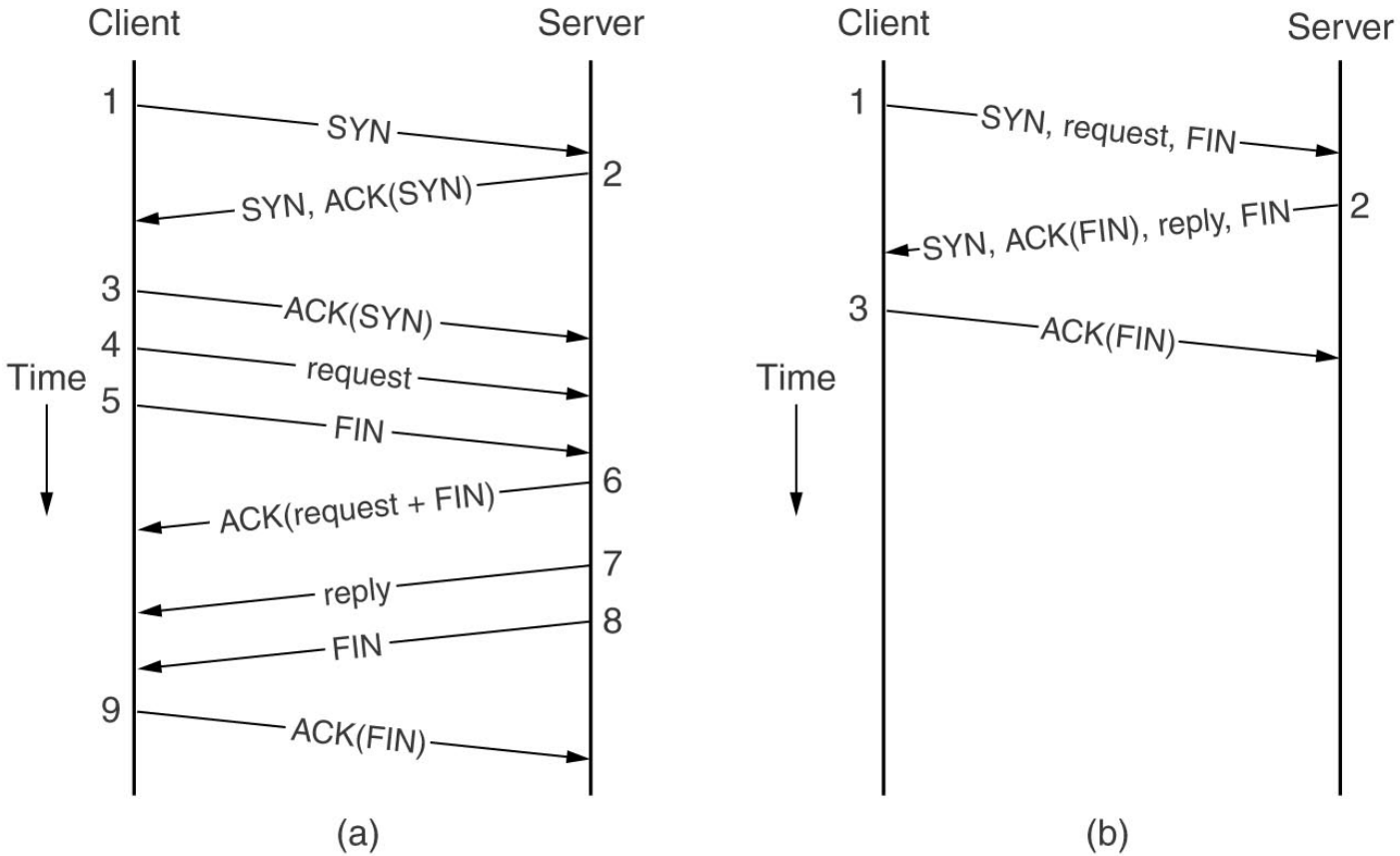


Fig: 6-40[1], Verbindungsabbau

[1] A. Tanenbaum, "Computer Networks", http://authors.phptr.com/tanenbaumcn4/

TCP: State-Event Diagramm

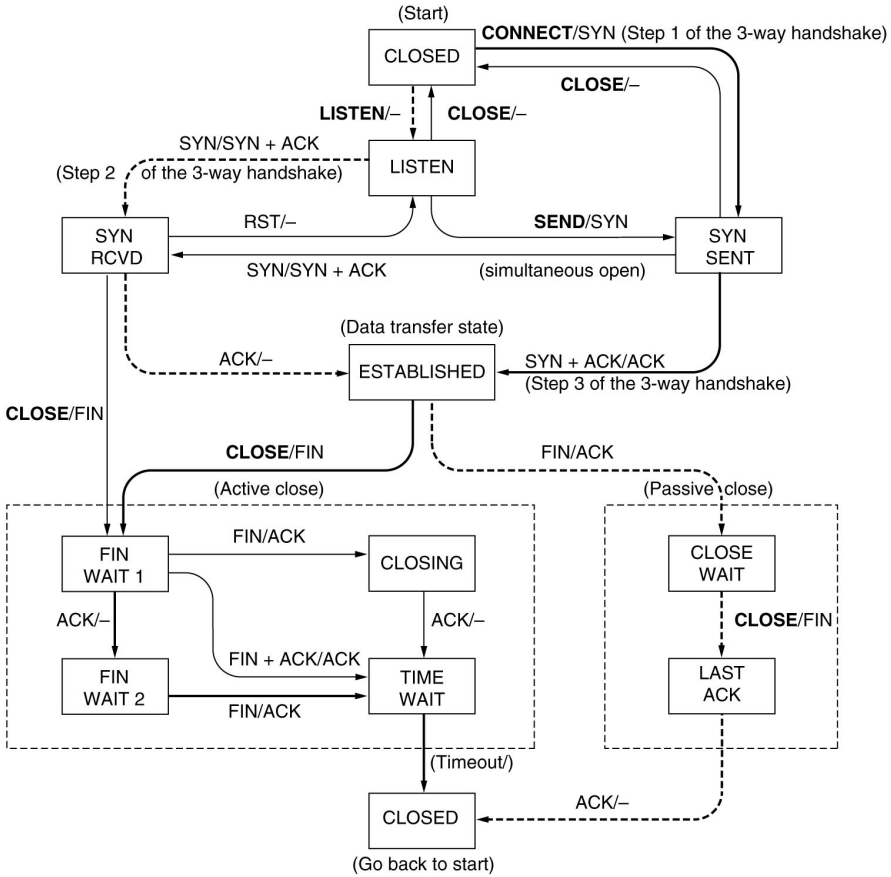


Fig: 6-33[1], Verbindungsabbau

[1] A. Tanenbaum, "Computer Networks", http://authors.phptr.com/tanenbaumcn4/

UDP: User Datagram Protocol

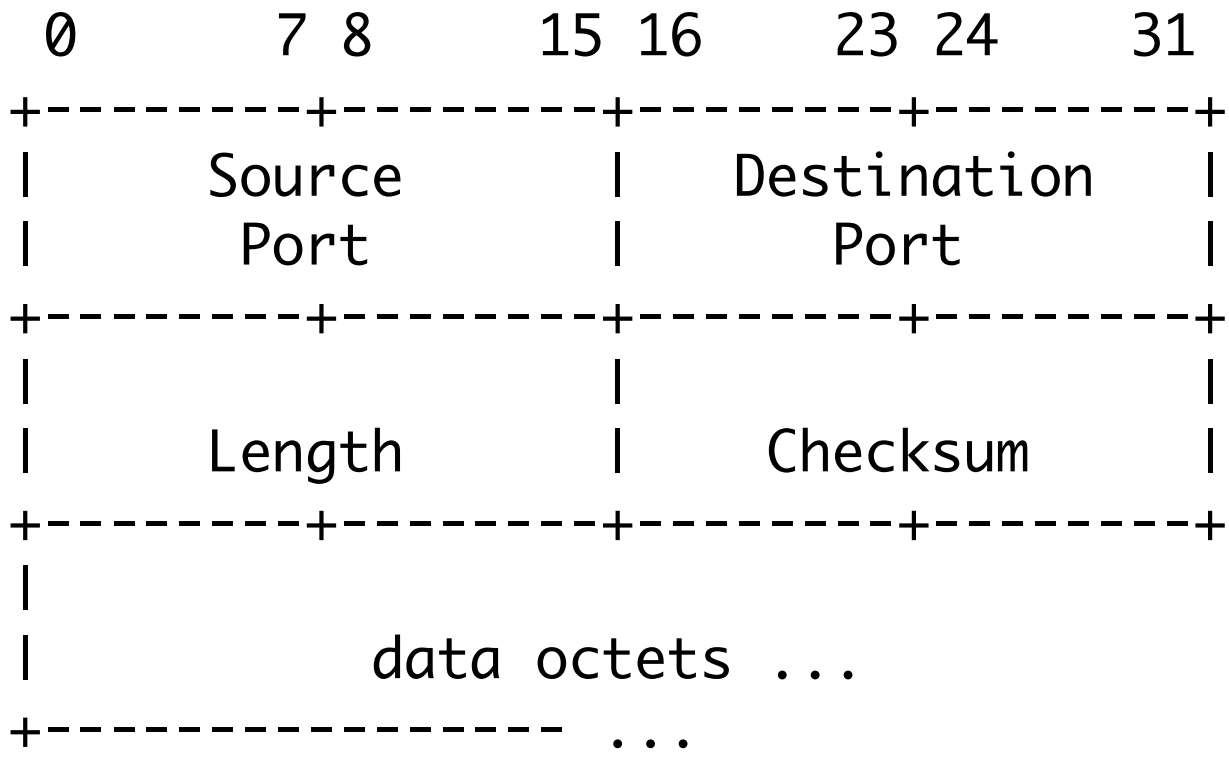
- Verbindungsloses, unzuverlässiges Transportprotokoll
  - Pakete können verlorengehen, in der falschen Reihenfolge oder doppelt eintreffen
- Einfacher als TCP, erfordert keinen Verbindungsauf und -abbau
- Unterstützt keine Flusskontrolle
- Geringere Netzwerk- und Ressourcenbelastung
- Das DNS (Domain Name System) benutzt z.B. UDP

→ UDP ist im RFC 768 beschrieben

UDP Paket-Header

Quelle: RFC 768

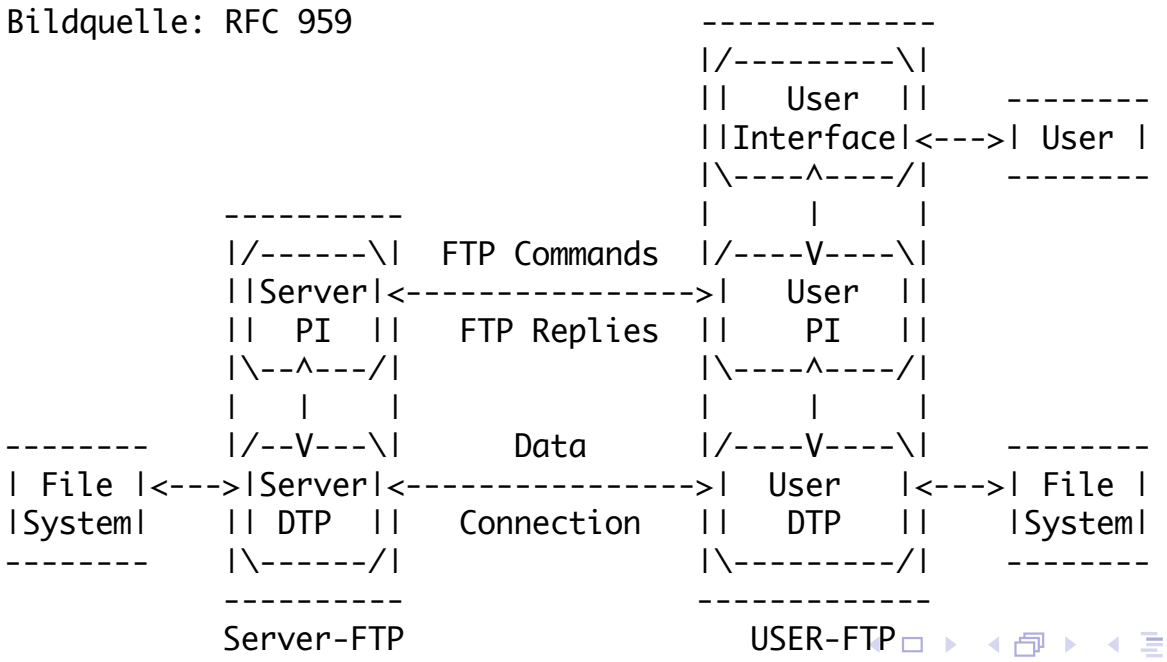
Der UDP-Header ist sehr einfach und 8 Byte lang. Das Prüfsummenfeld muss nicht benutzt werden, dann kann es auf "0" gesetzt werden.



FTP (File Transfer Protocol)

- FTP ist ein Anwendungsprotokoll zur Dateiübertragung in TCP/IP Netzen und ist im RFC 959 beschrieben
- Dateien können sowohl vom Client auf den Server, wie auch vom Server auf den Client übertragen werden.
- Das FTP-Protokoll wird zwischen einem FTP-Server Prozess und einem FTP-Client Prozess eingesetzt, wobei der FTP-Client häufig ein User-Interface hat

Bildquelle: RFC 959



FTP Session Example

```
$ ftp mirror.switch.ch
Trying 130.59.10.34...
Connected to moon.switch.ch.
220-SWITCHmirror (formerly known as Swiss SunSITE) welcomes you!
220
Name (mirror.switch.ch:markus): anonymous
331 Please specify the password.
Password:
230- Welcome to SWITCHmirror                    ftp://mirror.switch.ch/
230- ----------------------                   http://mirror.switch.ch/
[....]
230-
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> quit
221 Goodbye.
```

Abschluss

Behandelte Themen:

- Transportschicht: TCP und UDP
- FTP als Beispiel für ein Anwendungsprotokoll

Mögliche Prüfungsfragen

- Was unterscheidet die Adressierung auf Layer TCP von der Adressierung auf Layer IP?
- Welcher Unterschied besteht zwischen TCP und UDP, welches sind die Einsatzgebiete?

Labor/Selbststudium

- Lesen sie das RFC 793 und beantworten Sie dazu die Fragen auf der Folgeseite
- Laborübung

Fragen zum RFC 793

Suchen Sie die Antworten zu den folgenden Fragen im RFC 793. Es ist nicht die Intention, dass Sie das komplette RFC lesen, vielmehr sollen sie das RFC überfliegen und dabei die Struktur und die Art der beschriebenen Information erfassen. Vergleichen und diskutieren Sie die gefundenen Antworten mit einer Kollegin/einem Kollegen.

1. Welche Informationen werden im Kontext von TCP unter einer "connection" zusammengefasst?
2. TCP bietet eine zuverlässige (reliable) Kommunikationsschicht, dies wird durch die Verwendung von ..... und Bestätigungen (acknowledgments) erreicht. Garantiert TCP, dass die Daten beim *Enduser* fehlerfrei ankommen? Wieso bzw. Wieso nicht?
3. Das TCP-Headerfield bietet Platz für zusätzliche Optionen, welche Optionen sind im RFC definiert?
4. Das RFC schlägt die Wahl der ISN aufgrund einer internen Uhr vor. Wie lange dauert es bei der vorgeschlagenen Zeiteinheit, bis die selbe ISN wieder verwendet wird?
5. Wieso ist das aushandeln der ISN beim "three way handshaking" überhaupt notwendig?
6. Was tut ein Empfänger, der im "Listen" State ist und ein "RST" kriegt?
7. Das RFC schlägt ein Set von "User Commands' vor, welche sind dies?
8. Wenn der Status einer Verbindung "LISTEN" ist und ein "ACK" empfangen wird, was wird die Reaktion sein?
9. Welche Timeouts werden im RFC beschrieben?
10. Was wird mit TCB bezeichnet? Kennen Sie eine ähnliche Struktur aus dem Gebiet der Betriebssysteme?

Laborübung zu TCP

Vorbemerkung: Die im folgenden vorgeschlagene Übung ist als Leitfaden für eigene Experimente gedacht. Geben Sie sich nicht damit zufrieden, die angegebenen Kommandos einfach nur einzugeben; Beobachten Sie die Systemreaktion und reflektieren sie die Ergebnisse.

- Starten Sie Ihr System mit Knoppix, werden Sie Superuser und verifizieren Sie die Netzwerkkonnektivität mit `ping`
- Zeichnen Sie nun eine ganze FTP-Session mit ethereal/wireshark auf, stellen Sie dabei die Filterung vernünftig ein.
- Analysieren Sie nun die Pakete, beachten Sie insbesondere die folgenden Punkte:
  - 3-Way Handshake und initiale Sequenznummern
  - Ihr eingegebenes Passwort
  - Die seq und ack Felder (Sie können die Nummerierung der von "relativ" auf "absolut" umstellen: Menue "Edit"→"Preferences"→"Protocols" →"TCP" (Deselect Checkbox))
  - Den Verbindungsabbau
  - Die Pakete auf den verschiedenen Protokollschichten (FTP/TCP/IP/Ethernet), insbesondere auf die Adressierung.

n|w