Forelesning 1

Introduksjon til (eller repetisjon av) TCP/IP

Praktisk informasjon

- Forelesninger
  - Torsdag 12:15-14:00 (15:00)
  - A128
- Øvinger
  - Frivillige, men...

Forelesningsform

- Vær aktiv deltaker på forelesningene!
- Still spørsmål!
  De dummeste spørsmålene er de som ikke blir stilt
- Går det for fort? Si fra!
- Går det for langsomt? Vel....
- Foilene forsøkes lagt ut senest dagen før...

Lærebok

- **Willam Stallings**: Cryptography and Network Security *Principles and Practice* (Second Edition)
- ISBN 0-13-869017-0

Lærebok forts.

- Hjemmeside:
  http://www.williamstallings.com/security2e.html
- Errata-side
  ftp://shell.shore.net/members/w/s/ws/Errata/Errata-Security2e-0701
  - Gå gjennom med en gang!

Eksamen

- Skriftlig, 4 timer
- Bokstavkarakter (A-F)

TCP/IP

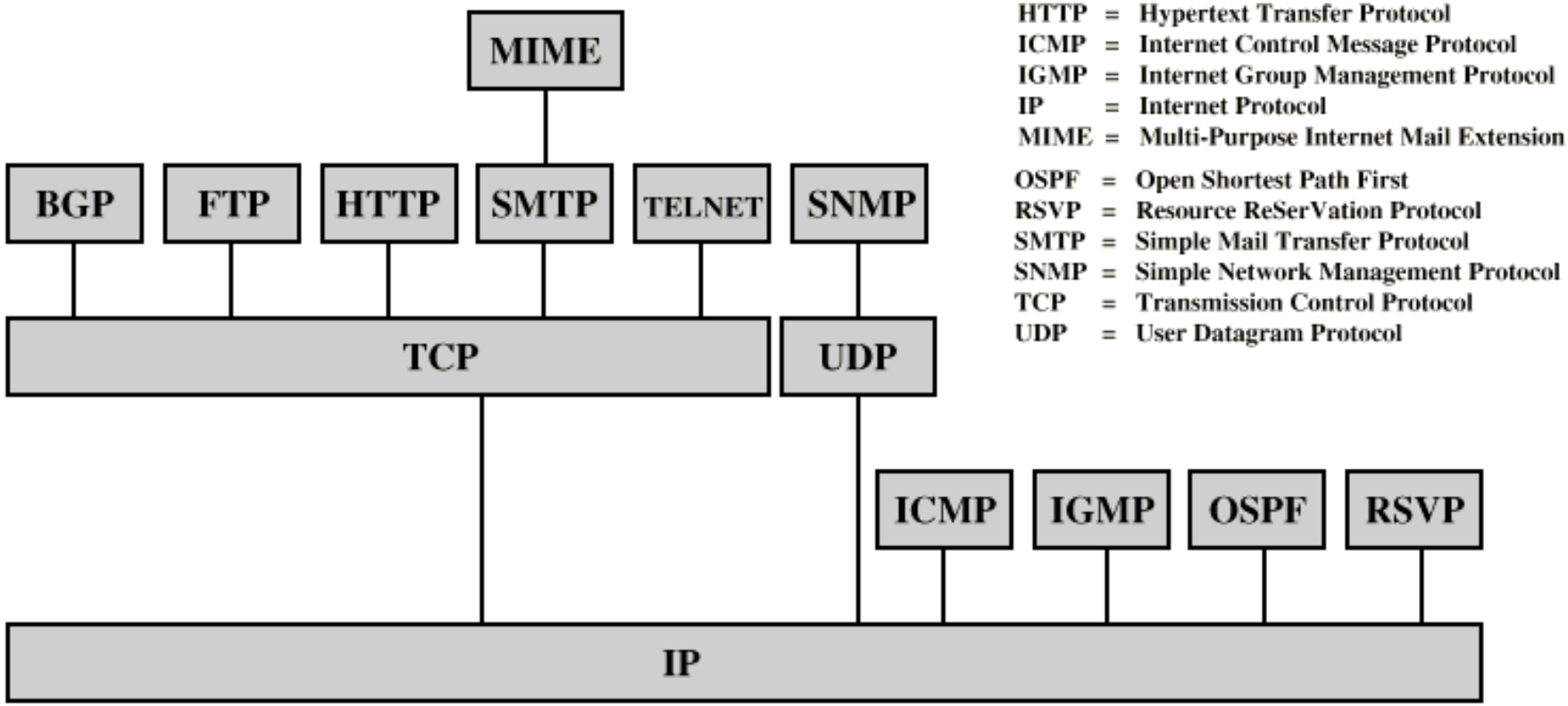
Noen ord om standarder

- To typer standarder
  - Standarder bestemt av komiteer
  - Standarder folk bruker
- Disse er ikke nødvendigvis sammenfallende!
- TCP/IP er noe folk bruker

Address Resolution Protocol

- ARP mapper mellom Ethernet adresser og IP adresser
- For å finne Ethernet adresse gitt IP:
  - ARP Broadcast med IP
  - Host med IP svarer med sin Ethernet adresse
- For å finne IP gitt Ethernet adresse
  - RARP - Reverse ARP

Internettprotokoller

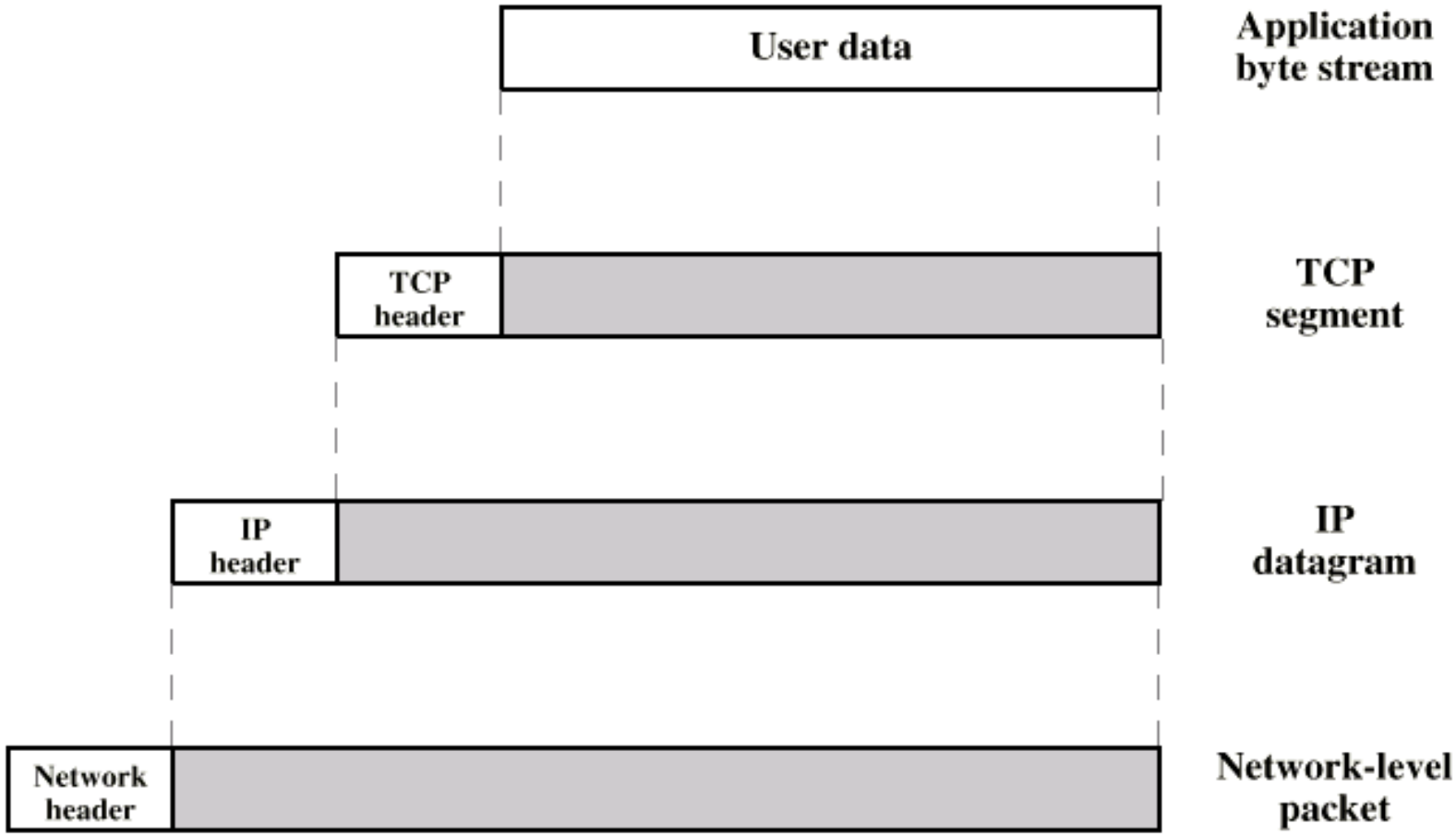


BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension

OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

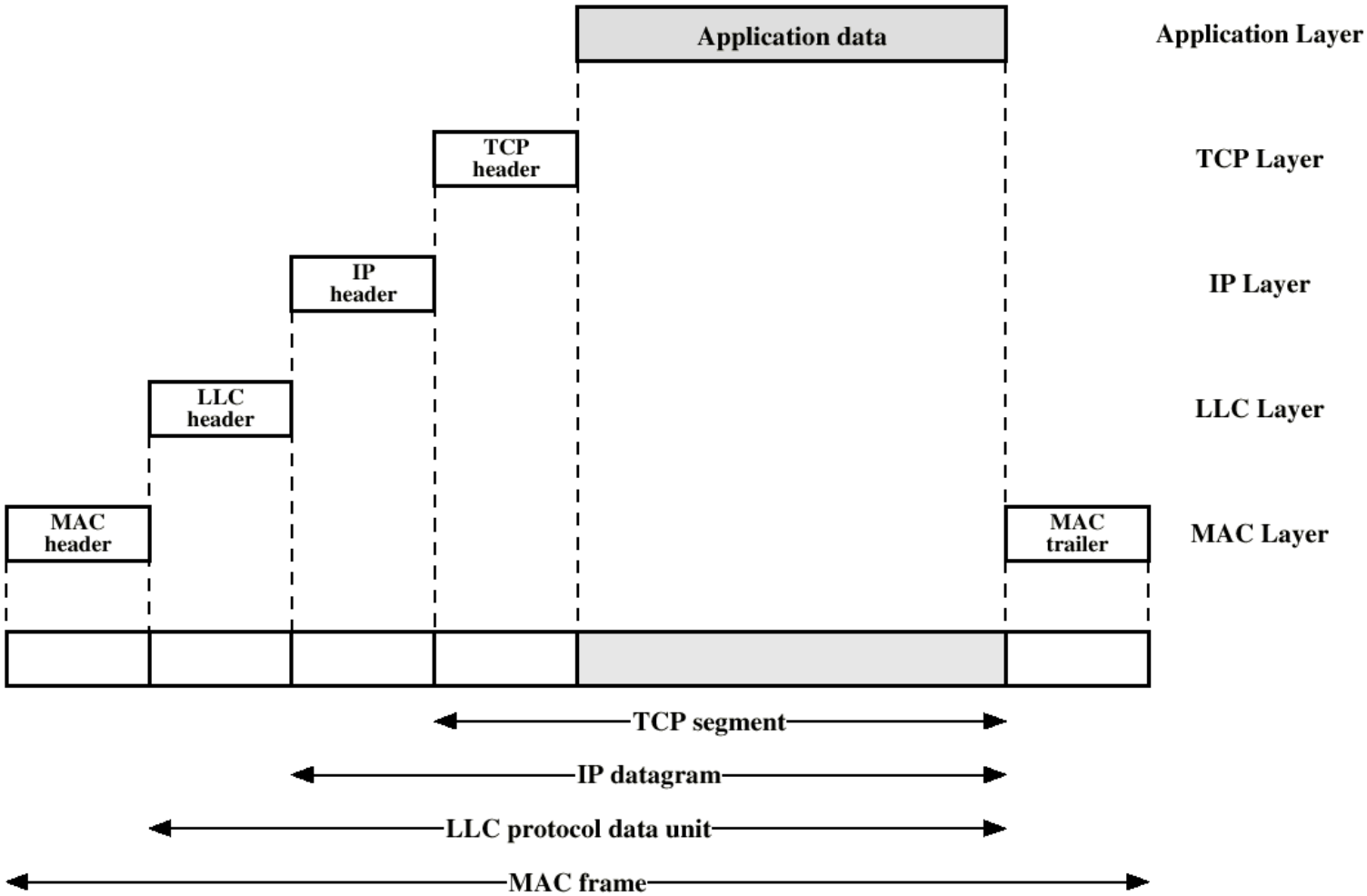
Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

PDUer i TCP/IP



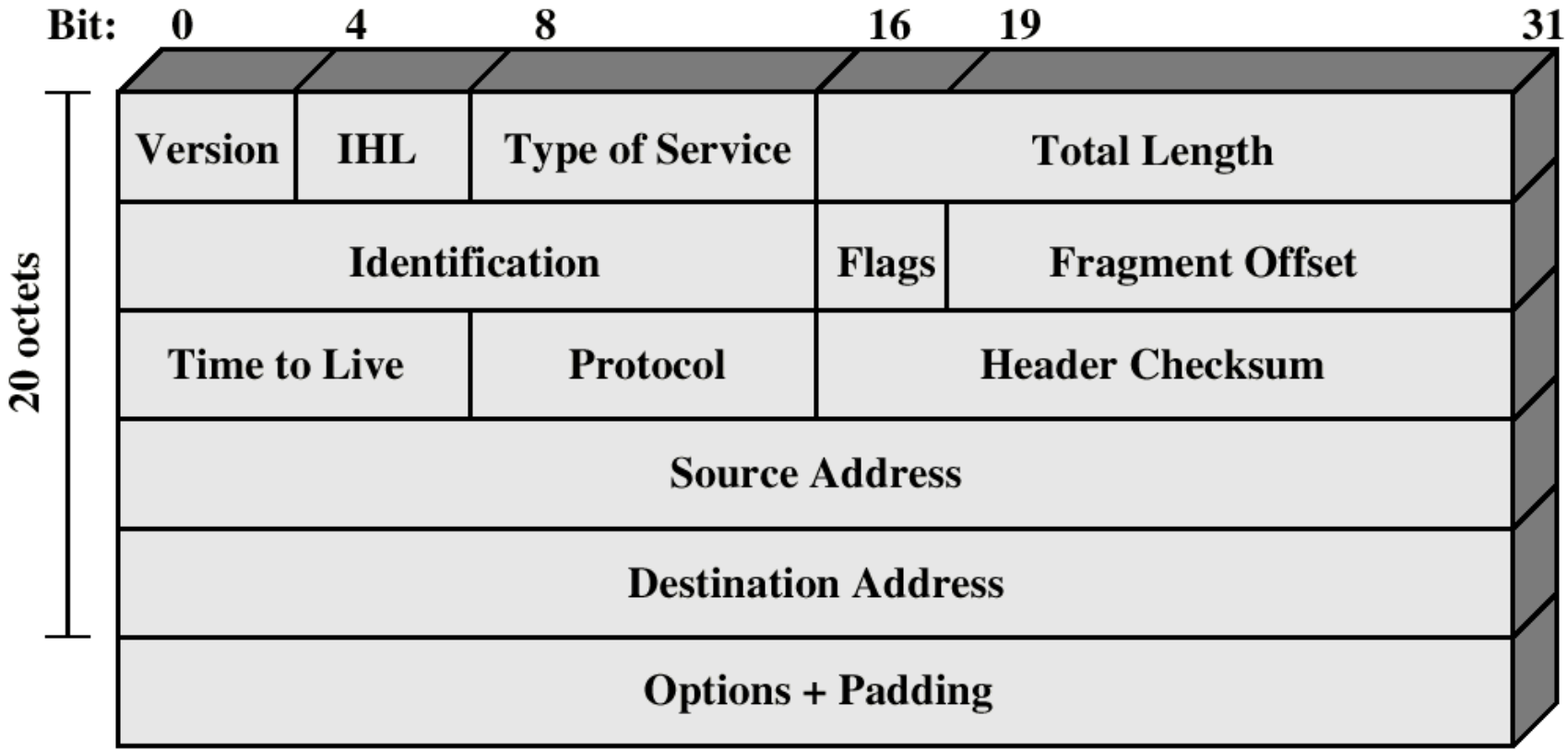
Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

TCP/IP og Lavere Lag



Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

IP Header



Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

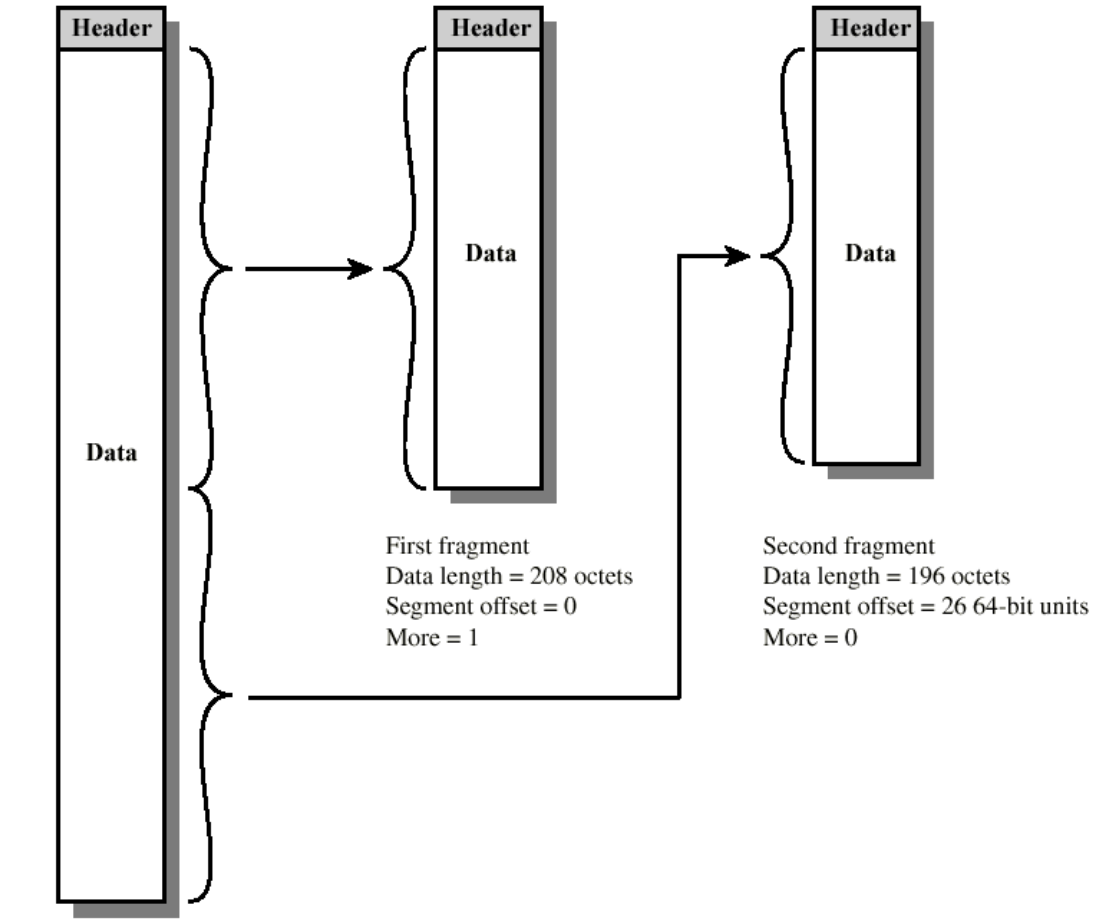
IP Header Felter

- VERS [4 bit]
  - IP versjon (IPv4)
- IHL [4 bit]
  - IP Header Length i 32-bit words
  - Vanligvis = 5 (ingen IP Options)
- TOTAL LENGTH [16 bit]
  - Lengde av hele IP datagrammet i oktetter
- TYPE OF SERVICE [8 bit]
  - Prioritet + QoS, vanligvis ikke i bruk

IP Header Felter

- IDENTIFICATION [16 bit]
  - Identifiserer datagrammet
- FLAGS [3 bit]
  - do not fragment
  - more fragments
- FRAGMENT OFFSET [13 bit]
  - Indikerer hvor et fragment hører til i det opprinnelige datagrammet

IP Fragmentering

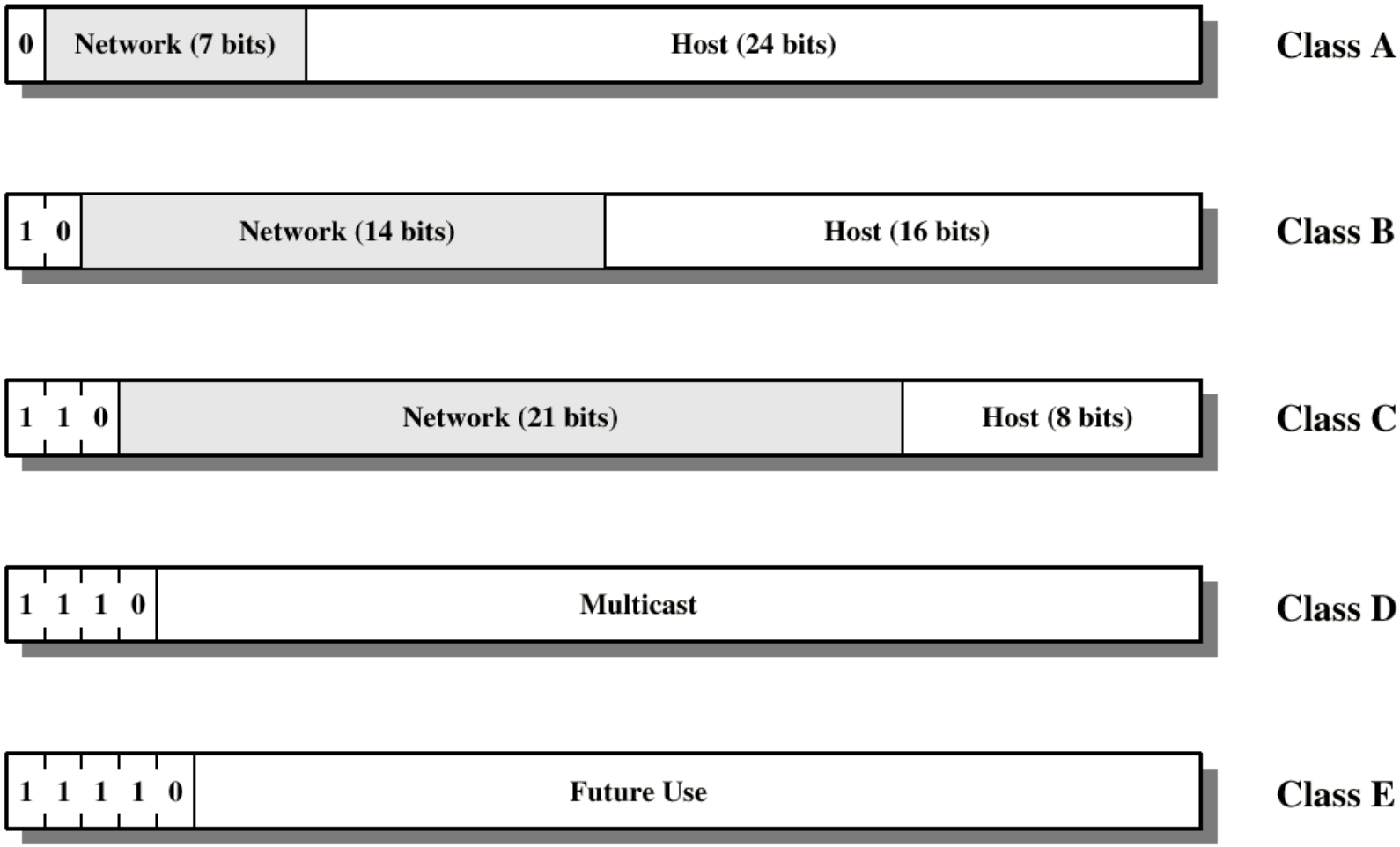


Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

IP Header Felter

- TIME TO LIVE [8 bit]
  - Indikerer hvor lenge datagrammet er gyldig
- PROTOCOL [8 bit]
  - Indikerer hvilken protokol på neste lag som skal ha datagrammet
- HEADER CHECKSUM [16 bit]
  - For å detekterer feil i headeren
- SOURCE ADDRESS [32 bit]
- DESTINATION ADDRESS [32 bit]

IP Adresser



Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

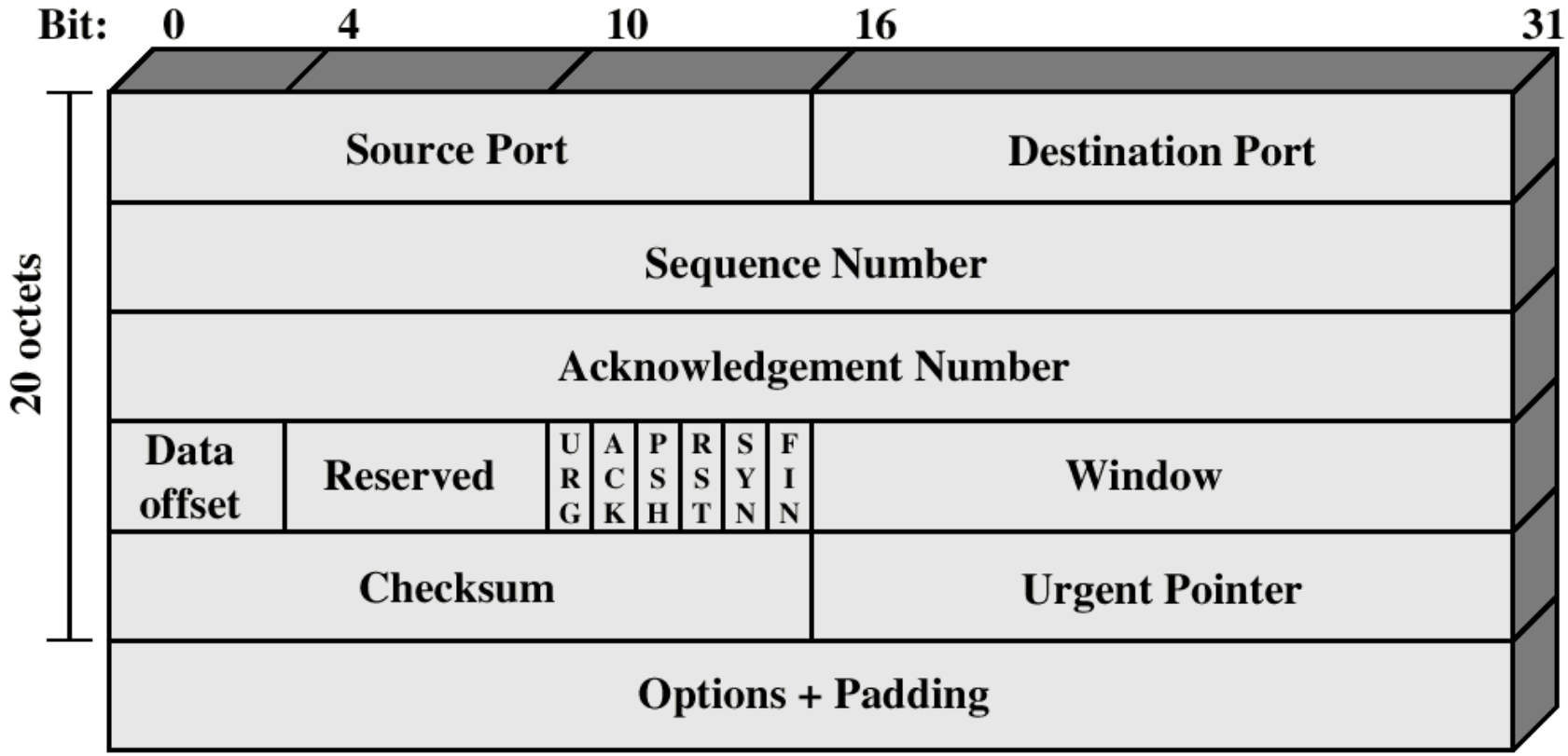
Mer IP-adresser

- A-adresse: 99.10.13.12
  Netmask: 255.0.0.0
- B-adresse: 184.23.45.112
  Netmask: 255.255.0.0
- C-adresse 193.156.99.113
  Netmask: 255.255.255.0

IP Options

- Datagram or Network Control
  - Security and handling restrictions
  - Loose source routing
  - Record route
  - Stream identifier
  - Strict source routing
- Debugging and Measurement
  - Internet timestamp

TCP Header



Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

TCP Header Felter

- SOURCE PORT [16 bit]
  - Indikerer hvilken port pakken kommer fra
- DESTINATION PORT [16 bit]
  - Indikerer hvilken port pakken skal til
- SEQUENCE NUMBER [32 bit]
  - Identifiserer pakkens posisjon i datastrømmen fra avsender
- ACKNOWLEDGEMENT NUMBER [32 bit]
  - Identifiserer hvilken pakke mottaker forventer neste gang

TCP Porter

- Indikerer endepunker
  - Avsender
    - Hvilket program som sender data
  - Mottaker
    - Hvilket program som skal motta data
- Portnumre < 1024
  - Reservert for standard tjenester
  - Kun root kan sette opp disse portene
- Portnumre >=1024
  - Allmenn bruk

TCP Standard Tjenester

- Noen porter som mapper til tjenester
  - Port 7 Echo
  - Port 21 FTP Control
  - Port 23 Telnet
  - Port 25 SMTP
  - Port 53 Domain Name Service
  - Port 79 Finger
  - Port 80 World Wide Web (HTTP)
  - Port 139 NETBIOS Session Service
  - Port 546 Dynamic Host Control Protocol Client
  - Port 547 Dynamic Host Control Protocol Server

TCP Header Felter

- DATA OFFSET [4 bit]
  - Lengde av header i 32-bit words
- RESERVED [6 bit]
  - Reservert for fremtidig bruk
- CODE BITS [6 bit] (dvs. flagg)
- WINDOW [16 bit]
  - Indikerer hvor mye data mottaker kan håndtere
- CHECKSUM [16 bit]
  - Feilsjekk
- Urgent Pointer
  - Posisjon hvor urgent data slutter

TCP Code Bits (flags)

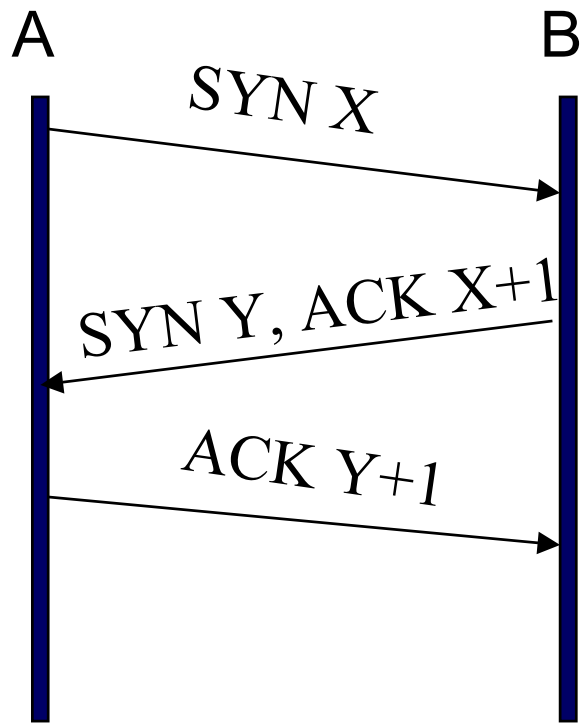
- URG
  - Urgent Pointer feltet er gyldig
- ACK
  - Acknowlegement feltet er gyldig
- PSH
  - Beskjed til mottaker om å gi all mottatt data til applikasjon-en NÅ
- RST
  - Reset koblingen
- SYN
  - Synchronize sequence numbers
- FIN
  - Finished, kobling kan tas ned

TCP Options

- TCP Options feltet brukes blant annet til å forhandle frem Maximum Segment Size (MSS)

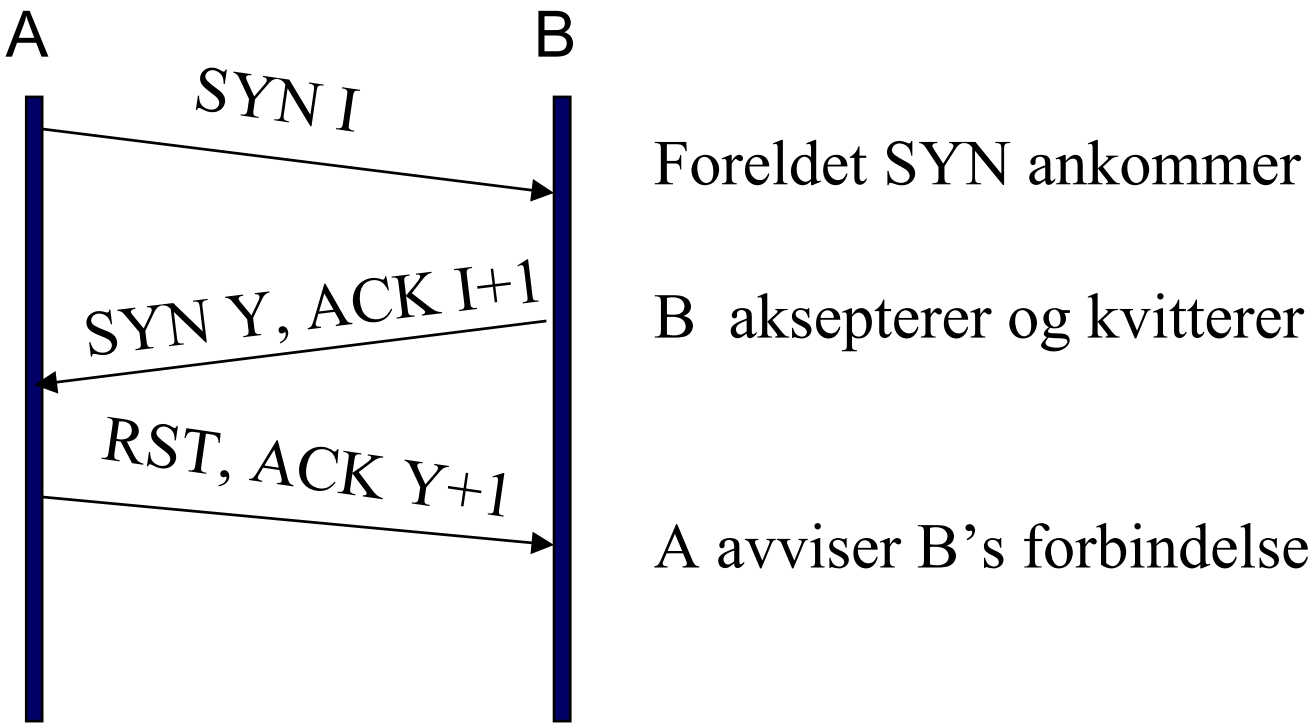
TCP Handshakes

- For å sette opp en ny kobling, brukes SYN pakker



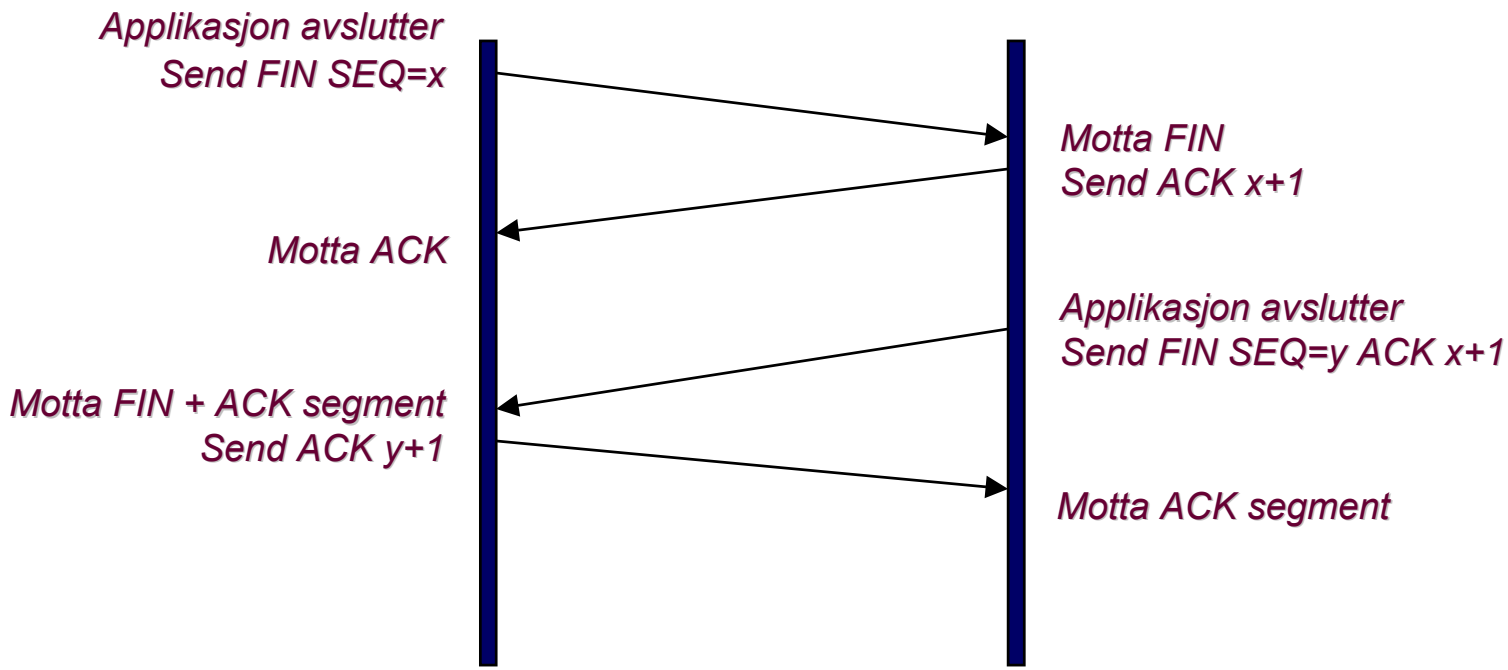
TCP Handshakes

- Dersom en ugyldig SYN mottas svarer man med en RST

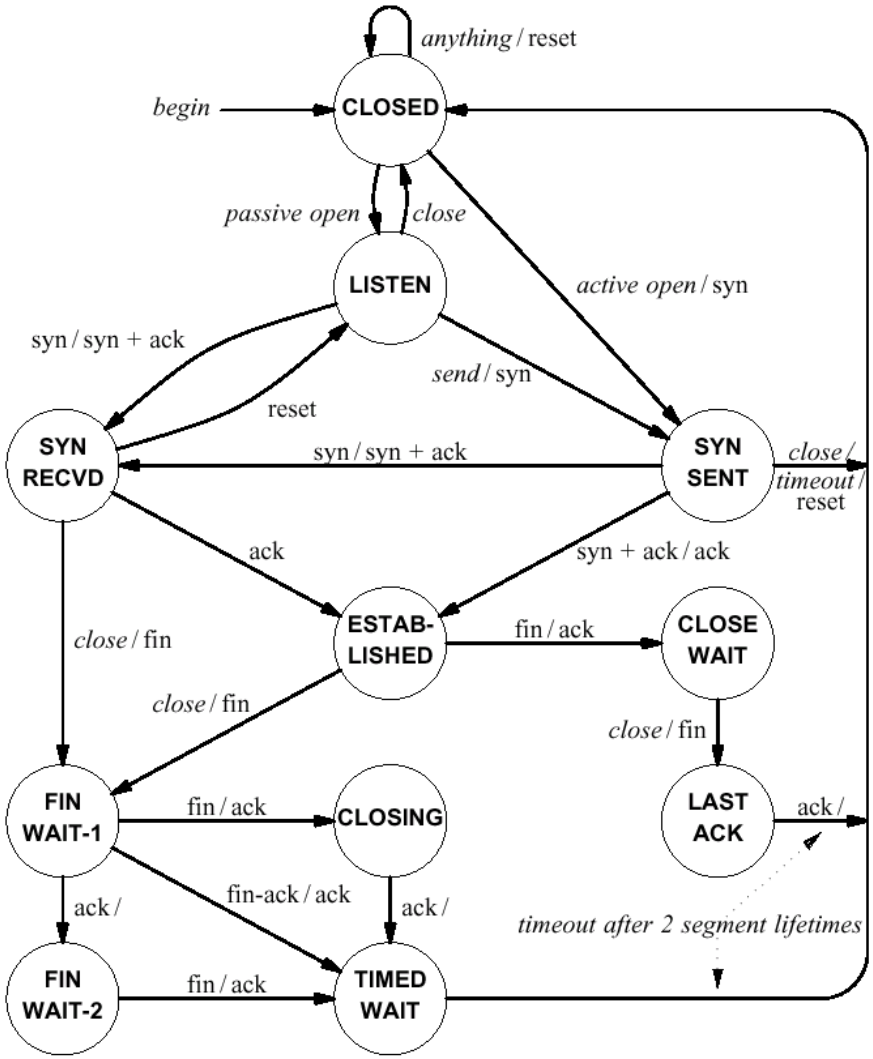


TCP Handshakes

- Når en Kobling er ferdig brukes FIN flagget



TCP tilstandsdiagram

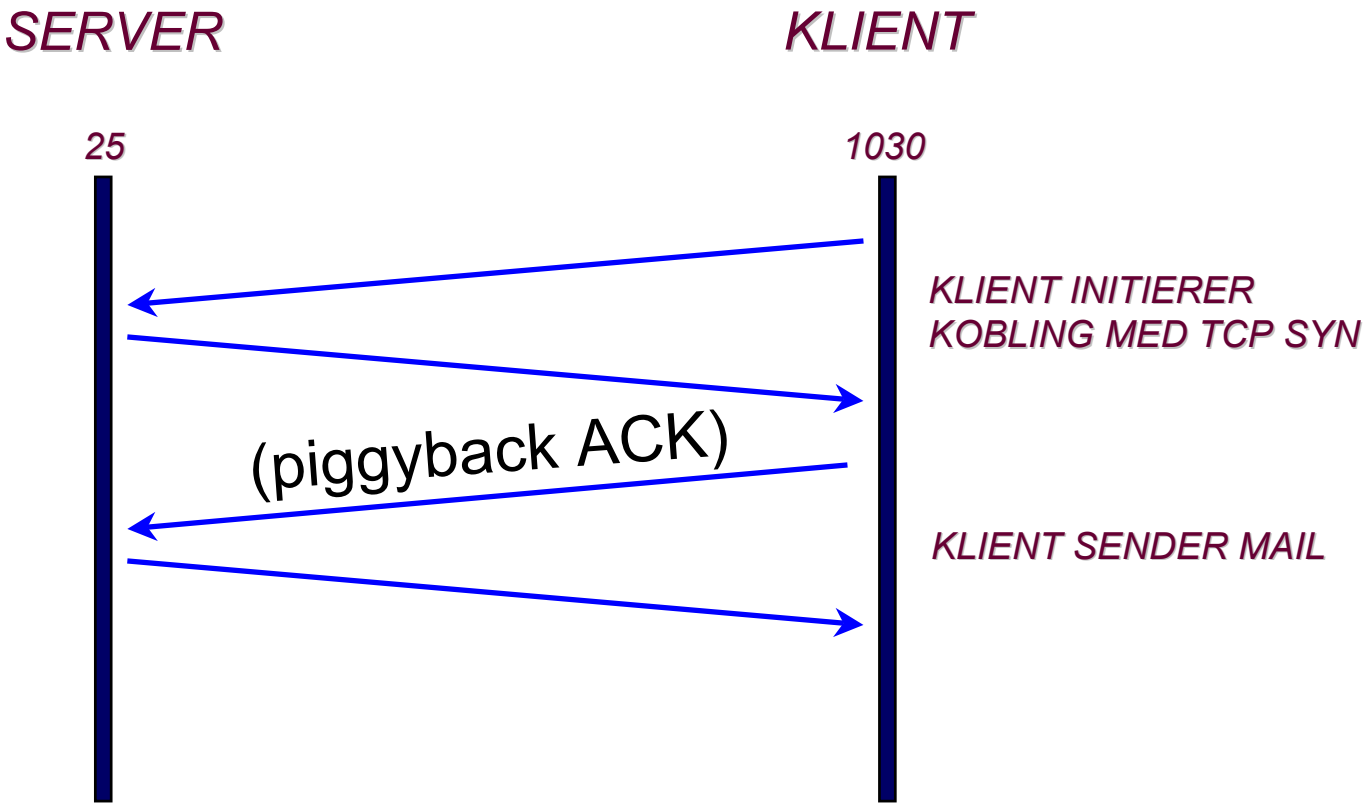


Fra Douglas E. Comer "Internetworking with TCP/IP", Prentice-Hall 1995

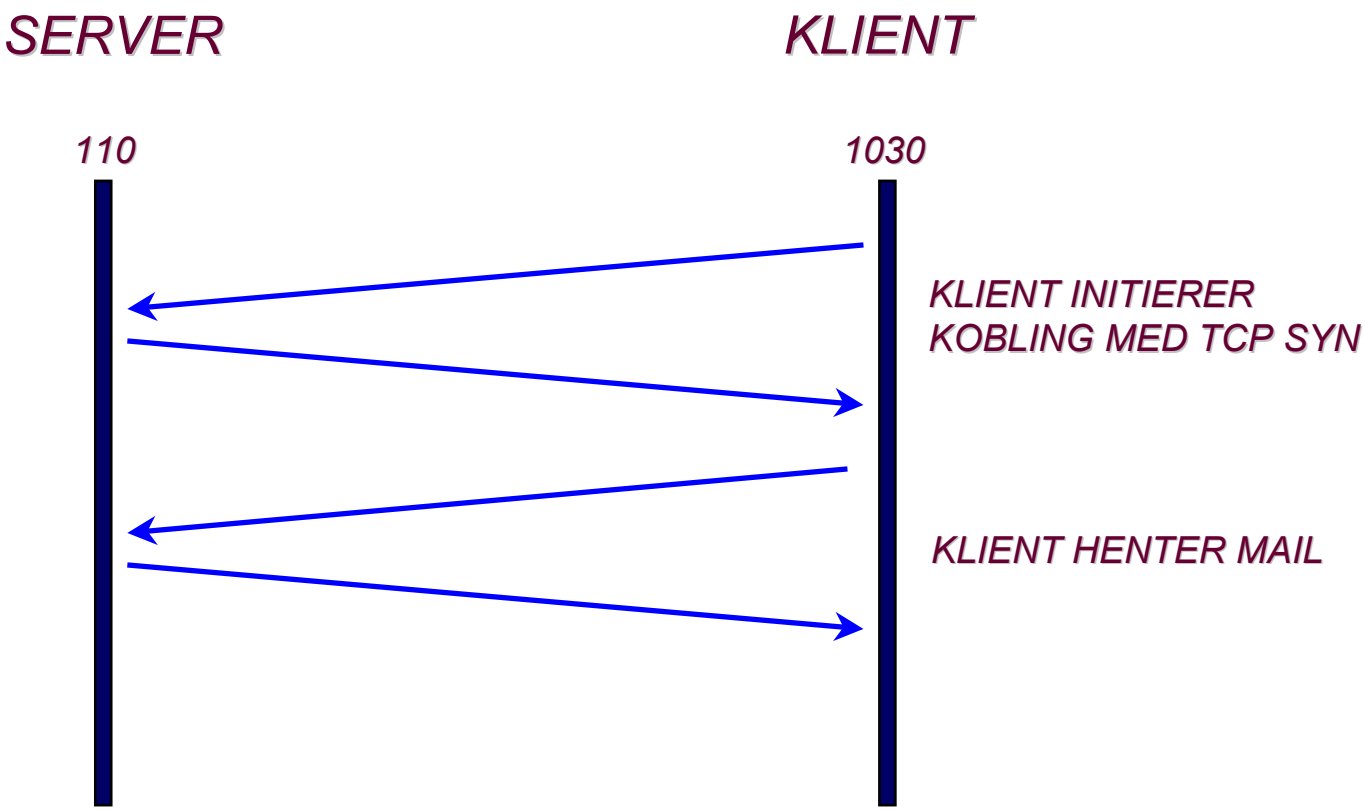
Applikasjonsprotokoller

- Brukere kommer ikke i direkte kontakt med protokollstakken før applikasjons-laget
  - SMTP
  - POP3
  - ...

Epost - SMTP


SERVER
KLIENT
25
1030
KLIENT INITIERER
KOBLING MED TCP SYN
(piggyback ACK)
KLIENT SENDER MAIL

Epost - POP


SERVER
KLIENT
110
1030
KLIENT INITIERER
KOBLING MED TCP SYN
KLIENT HENTER MAIL

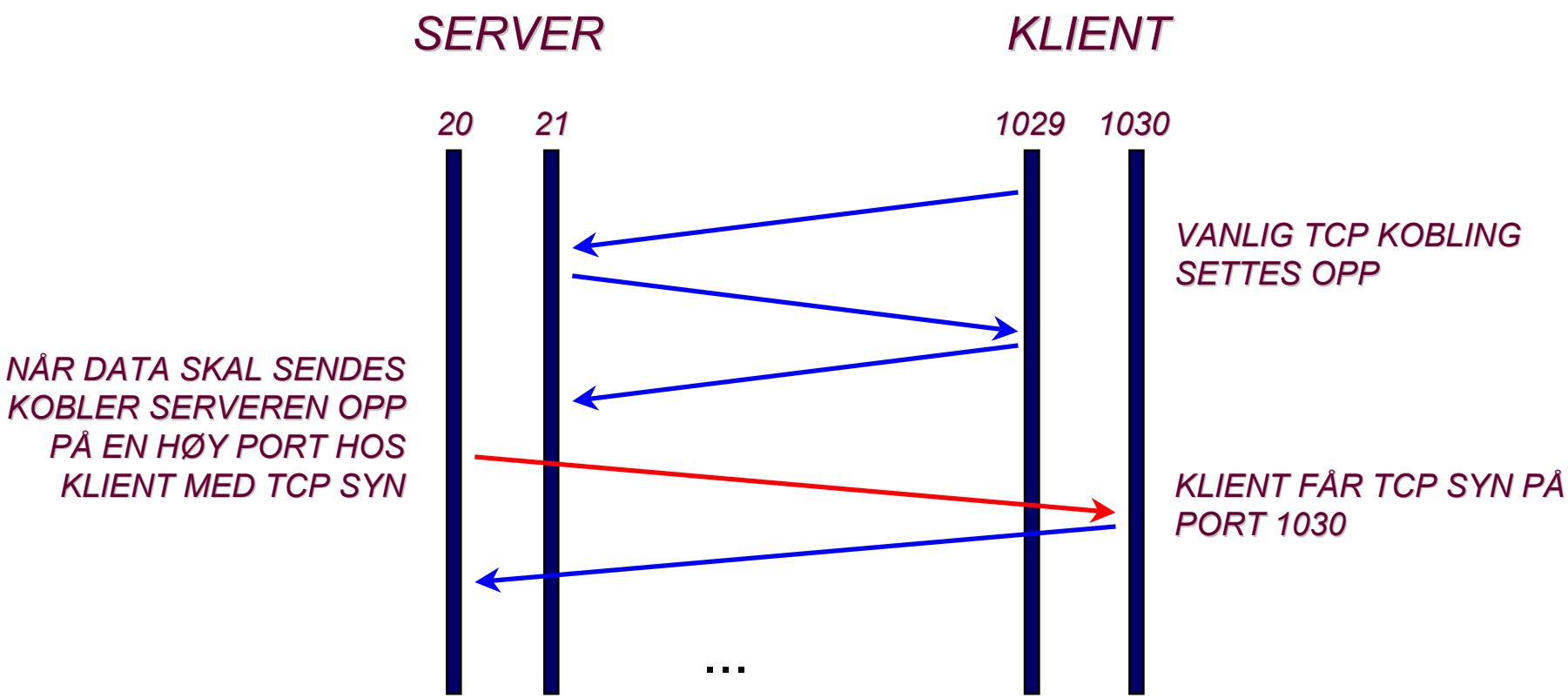
Andre Protokoller

- De fleste tjenestene bruker tilsvarende kommunikasjon som SMTP og POP
- For eksempel
  - DNS - port 53 (når TCP brukes)
  - Telnet - port 23
  - HTTP - port 80

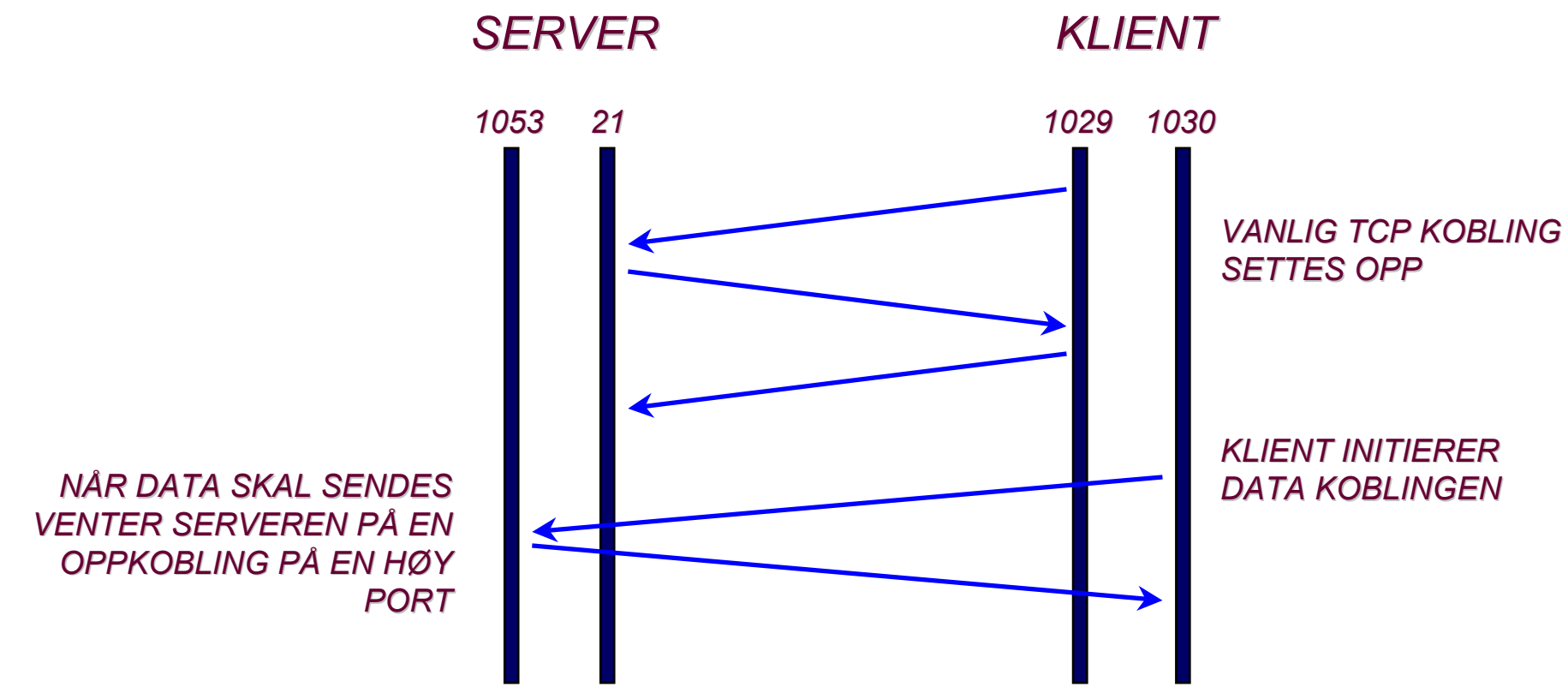
File Transfer Protocol - FTP

- FTP er spesiell fordi den kan oppføre seg på to forskjellige måter
- Active FTP
  - ”Den gode, gamle måten”
  - Ikke som man skulle forvente!
- Passive FTP
  - Stadig mer vanlig

Aktiv FTP


SERVER
KLIENT
20
21
1029
1030
VANLIG TCP KOBLING SETTES OPP
NÅR DATA SKAL SENDES KOBLER SERVEREN OPP PÅ EN HØY PORT HOS KLIENT MED TCP SYN
KLIENT FÅR TCP SYN PÅ PORT 1030
...

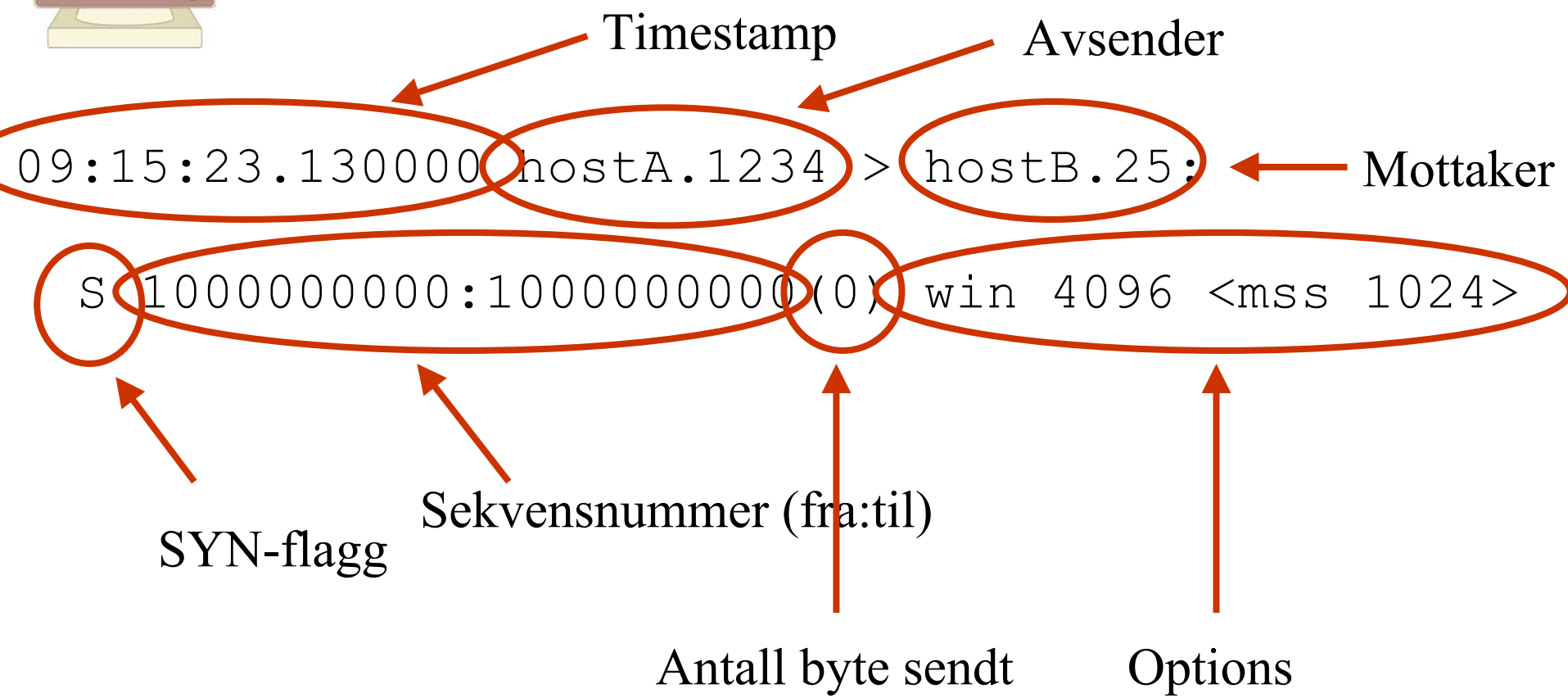
Passiv FTP


SERVER
KLIENT
1053
21
1029
1030
VANLIG TCP KOBLING SETTES OPP
KLIENT INITIERER DATA KOBLINGEN
NÅR DATA SKAL SENDES VENTER SERVEREN PÅ EN OPPKOBLING PÅ EN HØY PORT

tcpdump

- Standardprogram for overvåking av tcp-trafikk på lokalnett
- Linux, FreeBSD, etc.
- Konfigurerbar – se bare det du er interessert i
- ”man tcpdump”

tcpdump eksempel



Eksempel forts.

Portnummer

```
09:15:23.132400 hostB.25 > hostA.1234:
   S 4567000000:4567000000(0) ack 1000000001
   win 4096 <mss 1024>
```

ACK flagg

ACK nummer (SYN + 1)

```
09:15:23.134800 hostA.1234 > hostB.25:
   . ack 4567000001 win 4096
```

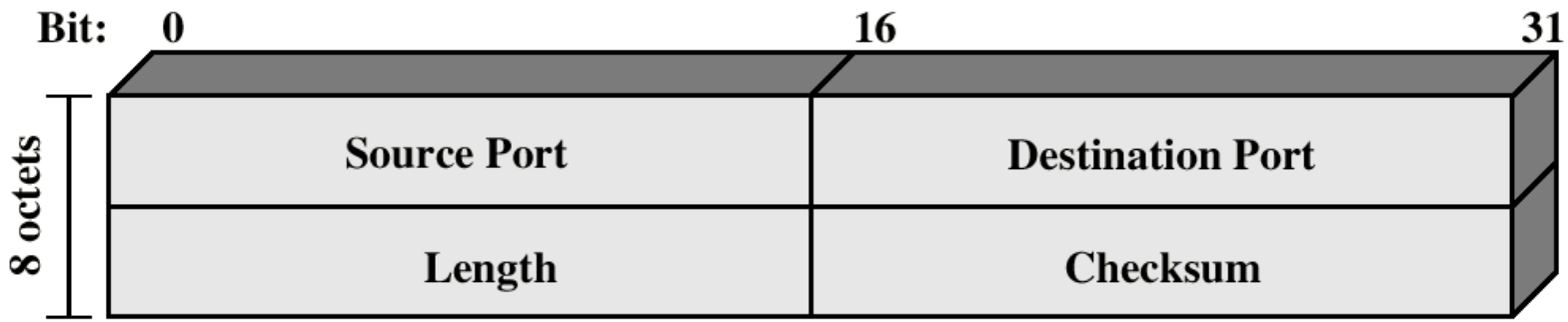
”Placeholder” for sekvensnummer

Flytkontroll: Sliding Window

- Poenget med sekvensnumre er at hver enkelt pakke ikke må kvitteres for før neste kan sendes
- Vindusstørrelse avgjør hvor mange pakker som kan sendes før første ACK mottas
- Kan ACK'e flere pakker i en jafs – ACK 938757 betyr "alle pakker til og med 938756"

UDP Header

- User Datagram Protocol



Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

ICMP

0	8	16	31
Type	Code	Checksum	
Unused			
IP Header + 64 bits of original datagram			

(a) Destination Unreachable; Time Exceeded; Source Quench

0	8	16	31
Type	Code	Checksum	
Pointer	Unused		
IP Header + 64 bits of original datagram			

(b) Parameter Problem

0	8	16	31
Type	Code	Checksum	
Gateway Internet Address			
IP Header + 64 bits of original datagram			

(c) Redirect

Ping

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Optional data			

(d) Echo, Echo Reply

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Originate Timestamp			

(e) Timestamp

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

(f) Timestamp Reply

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	

(g) Address Mask Request

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Address Mask			

(h) Address Mask Reply

Fra Stallings "Data and Computer Communications", Prentice-Hall 1999

Noen angrep

- Portscanning
- SYN-angrep
- TCP Hijacking

TCP Port Scanning

- For å finne ut hva slags tjenester en host tilbyr
- Kobler seg opp med TCP SYN på alle kjente porter
- Responsen indikerer om porten er åpen eller stengt
- Medfører mye trafikk, og er ikke vanskelig å detektere

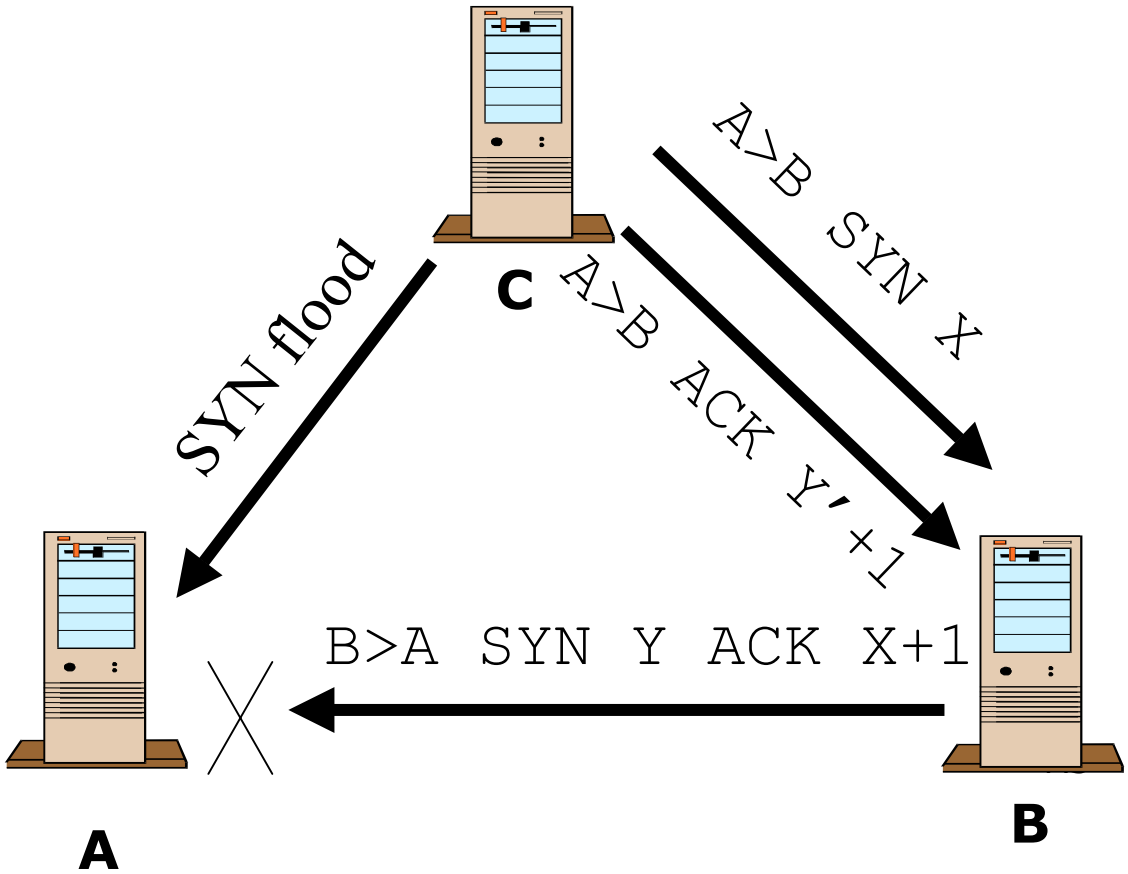
TCP Port Scanning, forts.

- Vanilla TCP scanning
  - Full connect
- TCP SYN Scanning
  - Sender SYN, Mottar SYN ACK, Sender RST
- TCP Stealth Scanning
  - FIN Scan
    - Sender FIN, åpne porter skal ignorere FIN, stengte porter skal returnere RST
  - Xmas Scan
    - FIN scan med FIN, URG og PSH Flagg
  - Null Scan
    - Pakke uten flagg

SYN-angrep

- Klassisk angrep beskrevet av Bellovin
- Baserer seg på utnyttelse av tillitsforhold mellom datamaskiner
- Krever gjetting av sekvensnummer på målmaskin
- Angriper kan få sendt pakker til målmaskin, men kan ikke lese svar.

SYN-angrep forts.



Ferdig, B tror han har forbindelse til A

SYN-angrep forts.

- Fremgangsmåte
  - Angriper C setter tiltrodd maskin A ut av spill ved SYN flood
  - Angriper C lager pakke med avsender A, sender til B
  - B svarer til A, men A kan ikke ta i mot
  - C må gjette sekvensnummer til B, men kan i så fall få utført kommandoer på B

TCP Hijacking

- ”Ta over” en forbindelse
- Forskjellige fremgangsmåter
  - ARP Cache Poisoning
    - Forutsetter angriper på samme nettsegment
  - Benytte SYN-angrep
    - Setter først den ene parten ut av spill
    - Må gjette sekvensnummer til begge parter
    - Må ”kjøre i blinde”

Dagens Website

- http://fag.sib.hibo.no/kurs/11174
  - Foiler
  - Øvingsoppgaver
  - Annen kursinformasjon