# DAT204 KRÆSJKURS

19. November 2019





```
2x UDP sockets (UDP) (2pts)
TCP & UDP sockets (tcp vs udp true or false) (3pts)
TCP & UDP Statements (what is true regarding tcp & udp) (3pts)
2x HTTP Protocol (2pts)
DHCP (utalleser og hvordan den fungerer) (3pts)
2x TCP congestion handling(how does top work?) (2pts)
TCP claims (claims about how congestion work) (2pts)
2x UDP Claims(how the UDP protocol works) (2pts)
TCP Quality Of Service (Which Service quality guarantees does TCP give) (2pts)
3x TCP Sequence (3pts/6pts/5pts)
3x TCP Congestion Window (5pts/2pts/5pts)
TCP Congestion window (5pts)
2x IP Address Assignment (2pts)
2x Packet Scheduling (2pts)
3x Binary to IP (2pts/5pts)
3x IP og subnetting (4pts/6.5pts/6pts)
3x Routing Tables (5pts)
TCP/IP switch layers (2pts)
TCP/IP router layers (2pts)
3x Link Layer (2pts/3pts)
Wireless Concepts (6pts)
2x Self-learning switches (6pts)
3x SSL statements (2pts)
3x SSL Quality Of Service (3pts/7pts/2pts)
Wireshark HTTP (16pts)
2x Link Utilisation (4pts)
2x Transmission and Propagation delay (10pts/8pts)
ARP (wireshark screenshot, true or false) (3pts)
Ethernet LAN (Svar på følgende spørsmål) (3pts)
Ethernet Switch (what is true regarding the statements) (3pts)
SSL/TLS master secret encryption (2pts)
HTTP GET request (how many bytes data are returned to the application layet in the wireshark screenshot)
Application Layer Protocol (Which protocols Belongs to application layer) (2pts)
Link-state Algorithm (10pts)
```



3x TCP Sequence (3pts/6pts/5pts)

3x TCP Congestion Window (5pts/2pts/5pts)

3x Binary to IP (2pts/5pts)

3x IP og subnetting (4pts/6.5pts/6pts)

3x Routing Tables (5pts)

3x Link Layer (2pts/3pts)

3x SSL statements (2pts)

3x SSL certificate (2pts/7pts)

3x SSL Quality Of Service (3pts/7pts/2pts)



2x Select Protocol (Application Layer/Link Layer) (2pts)

2x UDP sockets (UDP) (2pts)

2x HTTP Protocol (2pts)

2x E-mail transfer (http, smtp, imap) (3pts/2pts)

2x TCP congestion handling(how does tcp work?) (2pts)

2x UDP Claims(how the UDP protocol works) (2pts)

2x Routing Standards (2pts)

2x IP Address Assignment (2pts)

2x Packet Scheduling (2pts)

2x Self-learning switches (6pts)

2x Wireshark SSL (11pts)

2x Link Utilisation (4pts)

2x Transmission and Propagation delay (10pts/8pts)

2x SSL nonces (what is the purpose of nonces in SSL/TLS) (2pts)

2x Wireless Concepts (6pts)



TCP & UDP sockets (tcp vs udp true or false) (3pts)

TCP & UDP Statements (what is true regarding tcp & udp) (3pts)

E-mail (Protokoller, kryptering) (4pts)

DHCP (utalleser og hvordan den fungerer) (3pts)

TCP claims (claims about how congestion work) (2pts)

TCP Quality Of Service (Which Service quality guarantees does TCP give) (2pts)

TCP Congestion window (5pts)

Routing Algorithms (5pts)

AS Routing (4pts)

Routing Protocols (4.5pts)

TCP/IP switch layers (2pts)

TCP/IP router layers (2pts)

Wireless Concepts (6pts)

Email Encryption (2pts)

Wireshark HTTP (16pts)

Routers and SDN (3pts)

ARP (wireshark screenshot, true or false) (3pts)

Ethernet LAN (Svar på følgende spørsmål) (3pts)

Ethernet Switch (what is true regarding the statements) (3pts)

Wireless Concepts (6pts)

SSL/TLS master secret encryption (2pts)

HTTP GET request (how many bytes data are returned to the application layet in the wireshark screenshot) (2pts)

Application Layer Protocol (Which protocols Belongs to application layer) (2pts)

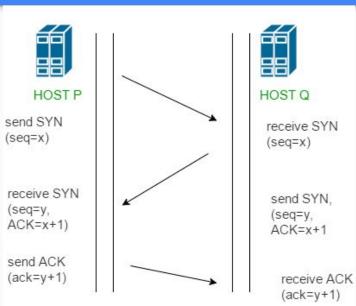
Wireshark IPv4 vs IPv6 (2pts)

Link-state Algorithm (10pts)

Spørsmål?



# 3x 3 Way Handshake (SYN, SYN-ACK, ACK)



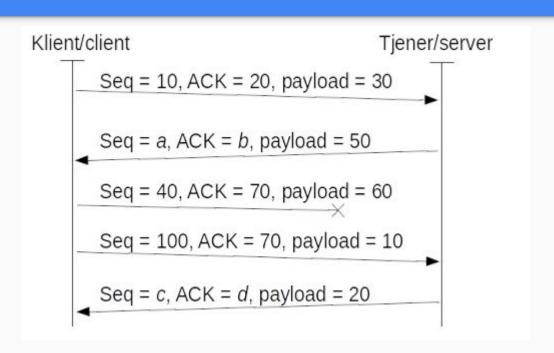
SYN: The active open is performed by the client sending a **SYN** to the server. The client sets the segment's sequence number to a random value A.

SYN-ACK: In response, the server replies with a **SYN-ACK**. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.

ACK: Finally, the client sends an **ACK** back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

At this point, both the client and server have received an acknowledgment of the connection.

# 3x TCP Sequence



# 3x TCP Sequence



Next Seq = last\_Ack
Next Ack = last\_seq + last\_payload

a = 20, b = 40

c = 70, d = 40

# 3x TCP Sequence



Next Seq = last\_Ack

Next Ack = last\_seq + last\_payload

seq = 150, ack = 70

# 3x Binary To IP

Q: IP-adressen 01101001.00010000.01010000.10101011 kan skrives på punktum desimalform som

01101001.00010000.01010000.<mark>10101011</mark>

01101001 - 1.oktet 64 + 32 + 8 +1 = 105 
 0
 1
 1
 0
 1
 0
 0
 1

 128
 64
 32
 16
 8
 4
 2
 1

00010000 - 2.oktet 16 = 16

 $\frac{01010000}{64 + 16 = 80}$  - 3.oktet

<mark>10101011</mark> - 4.oktet 128 + 32 + 8 + 2 + 1 = 171

# 3x IP og Subnett

Anta at en ISP eier adresseblokken på formatet **105.16.80.0/23**. Anta at den vil skape **åtte** subnett fra denne blokken, hvor hver blokk har samme antall IP-adresser. (6,5 poeng)

/23 - Subnett 11111111.111111111.111110.00000000

2° == 512 Ledige IP addresser 512 / 8 == 64 addresser pr.nett

105.16.80.0/26105.16.81.0/26105.16.80.64/26105.16.81.64/26105.16.80.128/26105.16.81.128/26105.16.80.192/26105.16.81.192/26

### **Subnet Mask Hierarchy**

Subnet Mask	CIDR	Binary Notation	Available Addresses Per Subnet
255.255.255.255	/32	11111111.111111111.11111111.11111111	1
255.255.255.254	/31	11111111.111111111.11111111.11111110	2
255.255.255.252	/30	11111111.111111111.11111111.11111100	4
255.255.255.248	/29	11111111.111111111.11111111.11111000	8
255.255.255.240	/28	11111111.111111111.11111111.11110000	16
255.255.255.224	/27	11111111.111111111.11111111.11100000	32
255.255.255.192	/26	11111111.111111111.11111111.11000000	64
255.255.255.128	/25	1111111.11111111.11111111.10000000	128
255.255.255.0	/24	1111111.111111111.11111111.00000000	256
255.255.254.0	/23	11111111.111111111.11111110.00000000	512

# 3x IP og Subnett

Q: Hvor mange bits utgjør vertsdelen av prefiksene som er opprettet for de åtte subnettene?

```
A: 11111111.111111111.1111111111.11000000 \....../
```

Q: Hvor mange verter kan tildeles en IP-adresse innenfor hvert av de åtte subnettene?

A: 64 - 62 Addresser.

# 3x Routing tables

Q: I denne oppgaven er målet å bestemme den riktige videresending linken gitt ruting tabellen nedenfor.

En ruter har følgende oppføringer i sin videresendingstabell:

Link1: 00001010.10101000.00000100.00000000/22

Link2: 00001010.10101000.00000110.00000000/23 Link3: 00001010.10101000.00000111.00000000/24

Link4: 00001010.10101000.00000000.00000000/16

Link5: Alle andre adresser

Anat at ruteren mottar datagramer med følgende destinasjonsadresser og bestem hvilken link de skal videresendes til:

A: 00001010.10101000.00000111.11111110

B: 00001010.10101000.00000011.00000000

C: 00001010.10101000.00000111.00000001

D: 00001010.10101000.00000110.10000000

E: 00001010.10111000.00000101.00000000

# 3x Routing tables - fiks

Q: I denne oppgaven er målet å bestemme den riktige videresending linken gitt ruting tabellen nedenfor.

Link1: 10.168.4.0 A: 10.168.7.254

Link2: 10.168.6.0 B: 10.168.3.0

Link3: 10.168.7.0 C: 10.168.7.1

Link4: 10.168.0.0 D: 10.168.6.128

Link5: Alle andre addresser E: 10.184.5.0

# OSI Model

	OSI Layer	TCP/IP	Datagrams are called	
Software	Layer 7 Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP		
	Layer 6	ASCII Characters, MPEG, SSL, TSL,	Upper Layer Data	
	Presentation	Compression (Encryption & Decryption)		
	Layer 5	NetBIOS, SAP, Handshaking connection		
	Session	Netbios, SAI, Haliushaking confilection		
	Layer 4	TCP, UDP	Segment	
	Transport	icr, obr		
	Layer 3	IDVA IDVE ICNAD IDSOC MOIS ADD	Packet	
	Network	IPv4, IPv6, ICMP, <u>IPSec</u> , MPLS, ARP		
Hardware -	Layer 2	Ethernet, 802.1x, PPP, ATM, Fiber	Frama	
	Data Link	Channel, MPLS, FDDI, MAC Addresses	Frame	
	Layer 1	Cables, Connectors, Hubs (DLS, RS232,	Bits	
	Physical	10BaseT, 100BaseTX, ISDN, T1)	DILS	

# 3x Link Layer

The link layer is the place in the protocol stack where software meets hardware.

The link layer performs error detection.

In computer networking, the link layer is the lowest layer in the Internet Protocol Suite, the networking architecture of the Internet. It is described in RFC 1122 and RFC 1123.

The link layer is the group of methods and communications protocols that only operate on the link that a host is physically connected to.

Link layer performs the framing of datagrams

#### 3x SSL Statements

#### **Secure Sockets Layer**

SSL allows agreeing on cryptographic algorithms during the handshake phase.

#### 3x SSL Certificate

Authenticate the server.

Use public key to encrypt master secret

I typiske klient/server sesjoner, SSL bruker et digitalt sertifikat for å autentisere serveren

I typiske klient/server sesjoner, SSL bruker et digitalt sertifikat for å kryptere master secret med serverens offentlige nøkkel

SSL sockets vil typisk utveksle applikasjons meldinger kryptert med en **symmetrisk-nøkkel blokk chiffer AES** er et eksempel på en slik algoritme

For å sikre at en melding ikke blir endret, vil SSL vanligvis bruke en **kryptografisk hash algoritme** til å lage et avtrykk av meldingen.

**SHA** er et eksempel på en slik algoritme

Ved å inkludere en autentiseringsnøkkel til avtrykket, blir en Message Authentication Code (MAC) laget og utvekslet sammen med den krypterte meldingen

# SSL Quality Of Service

Hvilken socket type forbedrer secure socket layer (SSL) med sikkerhetstjenester TCP

Hva heter den oppdaterte, sikrere og i dag mest brukte versionen av SSL protokollen ? TLS (Transport Layer security)

Hvilke Service garantier gir SSL sockets?

I rekkefølge data leveringer

Server Autentisering

Data konfidensialitet

Pålitelig data overføring

Data integritet

Spørsmål?



#### Select Protocol

Which of the following protocols run as a service on the application layer? **DNS** 

Which of the following protocols identify the MAC addresses on the LAN corresponding to the IP addresses of hosts on the LAN to allow link layer frames being sent from sender to receiver on the LAN segment?

**ARP** 

### **UDP** sockets

UDP traffic towards the same application in a server uses a common socket even if the traffic comes from different clients.

# HTTP Sockets

Several Web pages can be sent over the same persistent connection.

Two distinct Web pages can be sent over the same persistent connection.

#### E-mail transfer

Alice sends an e-mail to Bob using a Web-based e-mail account

**HTTP** 

Bob reads email using his e-mail client which uses a mail access protocol for presenting the emails that are stored on his e-mail server.

**SMTP** 

This mail access protocol keeps e-mails and email folders on the server also after they have been downloaded.

**IMAP** 

Mallory reads their email, as soon it has downloaded email folders on the server it is deleted from the server.

POP3

# TCP congestion handling

Congestion avoidance denotes the phases in a TCP transmission where the congestion window increases linearly.

Transmission Control Protocol (TCP) uses a network congestion-avoidance algorithm that includes various aspects of an additive increase/multiplicative decrease (AIMD) scheme, along with other schemes including slow start and congestion window, to achieve congestion avoidance.

The TCP congestion-avoidance algorithm is the primary basis for congestion control in the Internet

#### **UDP Claims**

When UDP is used, then any fault correction is up to the application.

# Routing Standards

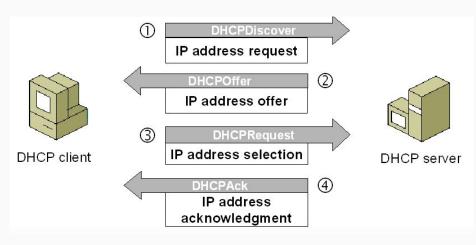
What is the de-facto standard for inter-AS routing? BPG - Border Gateway Protocol

Border Gateway Protocol (**BGP**) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (**AS**) on the Internet.

The protocol is classified as a path vector protocol. The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

# IP Address Assignment

How does a host usually get an IP address when it connects to a network? **DHCP** 



# Packet Scheduling

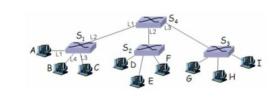
Which packet scheduling discipline ensures that a data flow gets a defined fraction (of arbitrary size) of the total bandwidth?

Weighted Fair Queueing

Which packet scheduling discipline ensures that each data flow gets an equal share of the total bandwidth, but does not support assigning different bandwidth shares?

Round Robin (RR)

# Self-learning switches - fiks



The figure above shows a network with four self-learning Ethernet switches and nine hosts. The switches have just been started, and the switch table is empty. (6 points)

Assume the following frames are being sent:

D to H

H to B

C to H

Then A to B.

#### How will the switch table in S<sub>4</sub> be after this sequence?

Switch table for S<sub>4</sub>

Address	Interface	
D	(L4, L3, L1, L2)	
н	(L3, L1, L4, L2)	
С	(L4, L3, L1, L2)	
(A, I, D, E, H, C, B)	(L4, L2, L1, L3)	

Which hosts receive the last frame?

(Only B, A, B and C, A and B, All except sender)

#### Wireshark SSL2

Which link layer protocol is used here? Which protocol is encapsulated in the link layer frame?

How many bytes payload are sent in segment 1815?

How many bytes data are sent in the current SSL record?

Packet 1821 shows "Win=151168". What type of window is this? Reciving

Which phase of a TCP connection do packets 3412 - 3446 belong to? Disconnect

Who sends packet 1815? Server

How many bytes payload have been sent and received in total from the start of the session and until inclusive packet 3433?

Sent: 1408

**Recived: 79230** 

```
Which application layer protocol(s) are used
here? Select any that apply:
```

```
Destination
                                                                         Protocol
                                                                                   Length Info
                                                19.6.0.79
                                                                         TLSv1.2
                                                                                        932 Application Data
                                                                         TCP
                                                                                         66 35542 - 443 [ACK] Seg=1409 Ack=79200 Win=151168 Len=0
    1821 18.216124988 10.0.0.70
                                                87.238.38.3
                                                                         TLSv1.2
    3410 22.997511054 87.238.38.3
                                                10.0.0.70
                                                                                         97 Encrypted Alert
                                                                                         66 35542 - 443 [FIN, ACK] Seq=1409 Ack=79231 Win=163584 |
    3412 22.997745815 10.0.0.70
                                                87.238.38.3
                                                10.0.0.70
                                                                         TCP
                                                                                         66 443 - 35542 [FIN, ACK] Seq=79231 Ack=1409 Win=31744 Le
                                                                         TCP
    3434 23.001025506 10.0.0.70
                                                87.238.38.3
                                                                                         66 35542 - 443 [ACK] Seq=1410 Ack=79232 Win=163584 Len=0
                                                                                         66 443 - 35542 [ACK] Seq=79232 Ack=1410 Win=31744 Len=0 T
    3446 23.101532258 87.238.38.3
                                                10.0.0.78
                                                                         TCP
Frame 1815: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface 9
Ethernet II, Src: ZyxelCom_45:b1:62 (60:31:97:45:b1:62), Dst: IntelCor_55:ad:9c (8c:70:5a:55:ad:9c)
Internet Protocol Version 4, Src: 87.238.38.3, Dst: 10.0.0.70

    Transmission Control Protocol, Src Port: 443 (443), Dst Port: 35542 (35542), Seq: 78334, Ack: 1409, Len: 866

     Source Port: 443
     Destination Port: 35542
      [Stream index: 41]
      TCP Segment Len: 866]
     Sequence number: 78334
                                (relative sequence number)
      [Next sequence number: 79200
                                      (relative sequence number)]
     Acknowledgment number: 1409
                                     (relative ack number)
     Header Length: 32 bytes
   Flags: 0x018 (PSH, ACK)
     Window size value: 248
      [Calculated window size: 31744]
      [Window size scaling factor: 128]

    Checksum: 0x6e16 [validation disabled]

     Urgent pointer: 0

    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

     [SEQ/ACK analysis]
      TCP segment data (866 bytes)
▶ [6 Reassembled TCP Segments (7873 bytes): #1810(1215), #1811(1448), #1812(1448), #1813(1448), #1814(1448), #1815(866)]
▼ Secure Sockets Layer
   ▼ TLSv1.2 Record Layer: Application Data Protocol: http
        Content Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 7868
        Encrypted Application Data: 7d329b9129b775fbc68d07ddcf40049060e27e8dd972681e...
      8c 70 5a 55 ad 9c 60 31 97 45 b1 62 08 00 45 00
                                                          .pZU.. 1 .E.b..E.
```

#### Link Utilisation

Consider an intercontinental fibre link between two hosts, where the round-trip propagation delay between these two end systems, RTT, is 200 ms. Suppose that the size of a packet is 625 bytes, including both header fields and data, and that the transmission rate is 100 Mbit/s. (4 points)

What is transmission delay in microseconds?

# Transmission and Propagation delay

#### SSL nonces

Beskytte mot "replay" angrep

- The primary reason why SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can access it.
- This is important because the information you send on the Internet is passed from computer to computer to get to the destination server.
- Any computer in between you and the server can see your credit card numbers, usernames and passwords, and other sensitive information if it is not encrypted with an SSL certificate.
- When an SSL certificate is used, the information becomes unreadable to everyone except for the server you are sending the information to. This protects it from hackers and identity thieves.

# Spørsmål?



#### TCP & UDP sockets

#### **TCP**

TCP bruker to sockets for å opprette en forbindelse, en som mottar oppkobling forespørsler og en for datautveksling.

TCP provides a connection oriented service, since it is based on connections between clients and servers.

TCP provides reliability. When a TCP client send data to the server, it requires an acknowledgement in return. If an acknowledgement is not received, TCP automatically retransmit the data and waits for a longer period of time.

We have mentioned that UDP datagrams are characterized by a length. TCP is instead a byte-stream protocol, without any boundaries at all

#### **UDP**

UDP is a simple transport-layer protocol. The application writes a message to a UDP socket, which is then encapsulated in a UDP datagram, which is further encapsulated in an IP datagram, which is sent to the destination.

There is **no guarantee that** a UDP will reach the destination, that the order of the datagrams will be preserved across the network or that datagrams arrive only once.

The problem of UDP is its lack of reliability: if a datagram reaches its final destination but the checksum detects an error, or if the datagram is dropped in the network, it is not automatically retransmitted.

#### TCP & UDP Statements

For en TCP forbindelse kan antallet ubekreftede bytes ikke være større enn mottakerens annonserte vindusstørrelse.

UDP tilbyr kun en upålitelig dataoverføringstjeneste over et upålitelig internett

TCP tilbyr en pålitelig dataoverføringstjeneste over et upålitelig internett.

Når UDP brukes, må eventuell feilkorreksjon gjøres i applikasjonen.

Hvilken protokoll er vist i eksemplet ovenfor og ansett som hjertet av Internett elektronisk post?

S: 220
C: HEL
S: 250
C: MAI
S: 250
C: RCP
S: 250
C: DAT
S: 354
C: Do
C: How

S: 220 hamburger.edu C: HELO crepes.fr S: 250 Hello crepes.fr, pleased to meet you C: MAIL FROM: <alice@crepes.fr> S: 250 alice@crepes.fr ... Sender ok C: RCPT TO: <bob@hamburger.edu> S: 250 bob@hamburger.edu ... Recipient ok C: DATA S: 354 Enter mail, end with "." on a line by itself C: Do you like ketchup? C: How about pickles? C: . S: 250 Message accepted for delivery C: QUIT S: 221 hamburger.edu closing connection

Hvilken protokoll er vist i eksemplet ovenfor og ansett som hjertet av Internett elektronisk post?

#### **SMTP**

Simple Mail Transfer Protocol

HELO – Identifies the client to the server, fully qualified domain name, only sent once per session

MAIL – Initiate a message transfer, fully qualified domain of originator

RCPT – Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee and for multiple addressees use one RCPT for each addressee

DATA – send data line by line

S: 220 hamburger.edu

C: HELO crepes.fr

S: 250 Hello crepes.fr, pleased to meet you

C: MAIL FROM: <alice@crepes.fr>

S: 250 alice@crepes.fr ... Sender ok

C: RCPT TO: <bob@hamburger.edu>

S: 250 bob@hamburger.edu ... Recipient ok

C: DATA

S: 354 Enter mail, end with "." on a line by itself

C: Do you like ketchup?

C: How about pickles?

C: .

S: 250 Message accepted for delivery

C: QUIT

S: 221 hamburger.edu closing connection

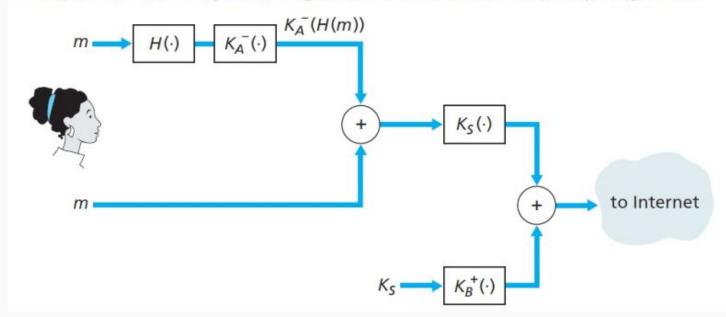
**POP3**(Post Office Protocol)

Laster ned email-mappene fra serveren, for å så slette de fra serveren

IMAP(Internet Message Access Protocol)

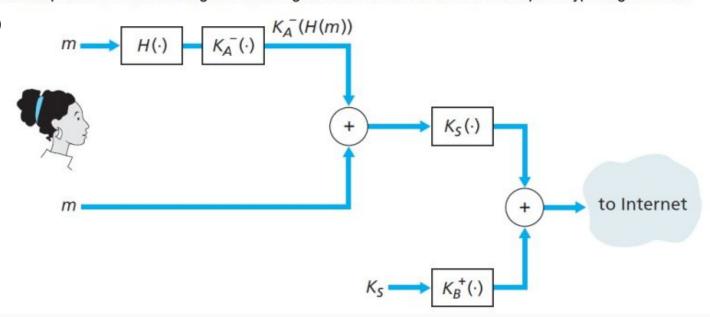
Beholder email-mappene fra serveren etter at de har blitt lastet ned

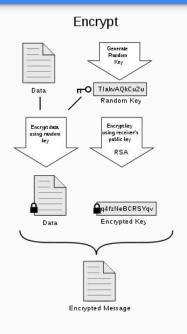
Hvilken protokoll er illustrert i figuren under og betraktet som de-facto standard e-post krypteringsmetode?

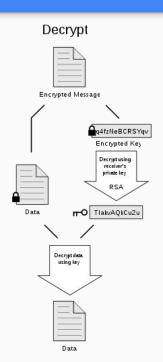


Hvilken protokoll er illustrert i figuren under og betraktet som de-facto standard e-post krypteringsmetode?

PGP (Pretty Good Privacy)







### **DHCP**

DHCP tillater en vert å skaffe en IP-adresse automatisk.

DHCP er en applikasjonslags protokoll.

DHCP er en applikasjonslags protokoll.

DHCP gir IP-adresser til lokale DNS servere.

DHCP er en klient-server protokol

DHCP gir LAN nettverks maske.

### **TCP Claims**

For a TCP connection, the number of unacknowledged bytes can not be larger than the receiver buffer.

## Quality of Service

#### **SSL Quality of Service**

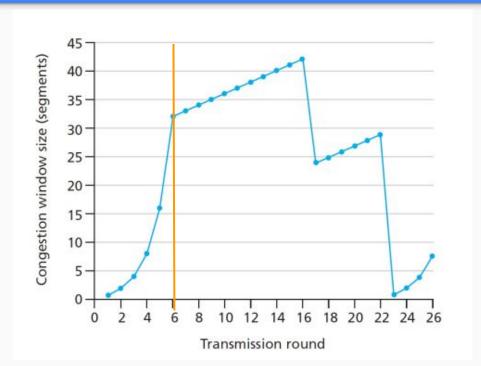
- Data transfer are done in order
- Data integrity
- Server authentication
- Data confidentiality
- Pålitelig data overføring

#### **TCP Quality of Service**

- In-order data delivery
- Reliable data transfer

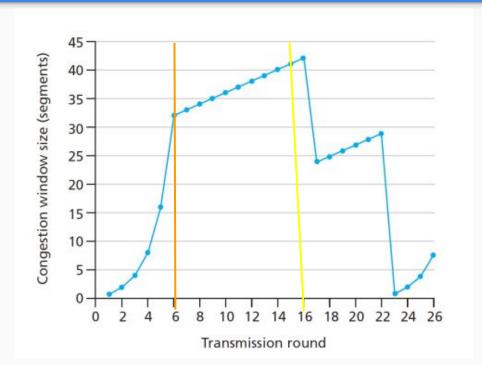
## TCP Congestion window

Identifiser et intervall der TCP slow start fungerer.



## TCP Congestion window

Identifiser et intervall der TCP slow start fungerer. Hvordan er segmenttap identifisert etter den 16. overføringsrunden(**Trippel duplikat ACK**)



## Routing Algorithms

OSPF(Open Shortest Path First) - Uses Dijkstra's algorithm to find the shortest path

**OSPF**(Open Shortest Path First) - exchanges information about neighbour routers with all routers in the network.

**BGP** (Border Gateway Protocol) - is dominated by routing policies instead of focusing on finding the path with lowest cost in the network.

**BGP**(Border Gateway Protocol) - announces a subnet to all autonomous systems on the Internet.

**RIP** (Routing Information Protocol) - exchanges information about changed routing tables with neighbour routers.

# **AS Routing**

## Routing Protocols

Dijkstra's korteste vei algoritme er mye brukt med Link-State(LS) ruting protokoller.

- Ruteren har fullstendig informasjon om alle link kostnader innenfor sitt autonome system.
- Ruteren har fullstendig topologi over alle andre rutere innenfor sitt autonome system
- Ruteren har fullstendig topologi over alle andre rutere i hele Internettet

Bellman-Ford ligningen er mye brukt med **Distance-Vector(DV)** rutin protokoller.

- Ruteren kan kjøre RIP
- Ruteren kjenner kun avstand til fysisk tilkoblede naboer.
- Ruteren er avhengig av at direkte tilknyttede naboer annonserer sine vektortabeller for å kunne oppdatere sin egen rutingtabell
- Ruteren kjenner bare fysisk tilkoblede naboer.

## TCP/IP Switch Layers

Which layers in the TCP/IP model are involved when an Ethernet switch forwards packets?

- Link layer
- Physical Layer

## TCP/IP Router Layers

Which layers in the data plane are involved when a router forwards packets from an input port and to an output port in the router?

- Network layer
- Link Layer
- Physical layer

## Wireless Concepts

In **infrastructure mode** each wireless host is connected to the internet via an access point.

In ad-hoc mode wireless hosts themselves provide routing, address assignment and DNS

Wireless stations discover and identify the access point using beacon frames.

Attenuation of the wireless signal when travelling through matter is called **path loss** 

When two or more sources within a basic service set transmit at the same time on the same frequency then **interference** may occur.

Blurring of the received signal due to several reflections of the electromagnetic wave from objects and ground is called **multipath propagation** 

## Wireshark HTTP

Hvilken linklagsprotokoll brukes her?

#### **ARP**

- Verter og rutere bruker ARP til å knytte en IP-adresse til en MAC-adresse og vedlikeholde en ARP-tabell i sitt minne.
- Vert med IP-adresse 128.39.200.113 har MAC-adresse 3c:a8:2a:dd:a3:00.
- ARP er en protokoll som ligger et sted mellom nettverkslaget og linklaget i Internett protokollstakk

```
> Frame 647: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: HewlettP dd:a3:00 (3c:a8:2a:dd:a3:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

→ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
       Address: Broadcast (ff:ff:ff:ff:ff)
       .... .1. .... ... = LG bit: Locally administered address (this is NOT the factory default)
       .... ...1 .... = IG bit: Group address (multicast/broadcast)
  Source: HewlettP_dd:a3:00 (3c:a8:2a:dd:a3:00)
       Address: HewlettP_dd:a3:00 (3c:a8:2a:dd:a3:00)
       .... .0. .... - LG bit: Globally unique address (factory default)
       .... ...0 .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)

✓ Address Resolution Protocol (request)

    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HewlettP dd:a3:00 (3c:a8:2a:dd:a3:00)
    Sender IP address: 128.39.200.113
    Target MAC address: 00:00:00 00:00:00 (00:00:00:00:00:00)
    Target IP address: 128.39.200.165
```

98 88 88 88 88 88 88 88 88 88 88 88

#### Routers and SDN

I de senere årene, har Software-Defined Networking (SDN) fått økende interesse. Nedenfor er noen sanne uttalelser

angående tradisjonelle rutere og SDN

- Med tradisjonelle rutere håndteres både videresending og ruting funksjonen (kontroll, kommunikasjon, beregning av videresendingstabeller) per-ruter
- Tradisjonelle rutere utfører destinasjonsbasert videresending ved å matche destinasjonens IP-adresse mot deres respektive videresendingstabell
- SDN pakkesvitsjer kan utføre videresending ved å matche flere felter i linklagets, nettverkslagets og transportlagets headere mot deres respektive flyt tabell

### **Ethernet LAN**

Ethernet er den mest brukte teknologien for kablede Local Area Network (LAN)

- Hvilke IEEE standarder spesifiserer kablet Ethernet?
  - 0 802.3

#### **Ethernet LAN**

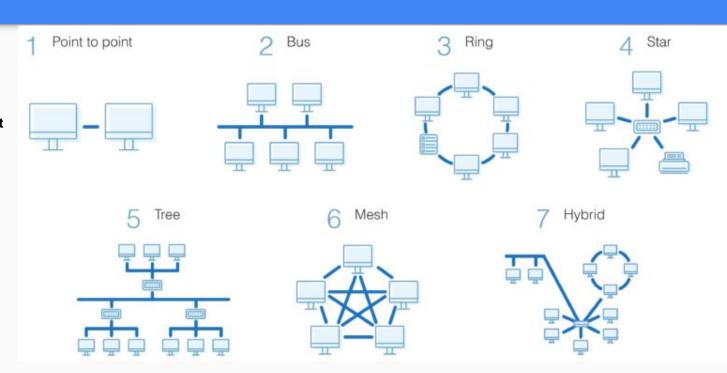
Ethernet er den mest brukte teknologien for kablede Local Area Network (LAN)

<u>Hvilken kablet LAN topologi er den</u> <u>aller mest vanligste i dag?</u>

Stjerne med punkt-til-punkt linker og svitsj i midten

<u>Hvilken kabel type er mest vanlig i</u> <u>LAN i dag?</u>

Tvunnet parkabel



### **Ethernet Switch**

Svitsjer videresender rammer basert på destinasjonens MAC-adresse.

Svitsjer er enkle, raske og relativt billige

Svitsjer må vedlikeholde sine svitsjetabeller på egenhånd

# Wireless Concepts

## HTTP GET request

The Wireshark log shows response to a HTTP-GET request.

How many bytes data are returned to the application layer from the current TCP segment?

```
Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
E Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: 4272 (4272), Seq: 4381, Ack: 502, Len: 436

  [4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]

Hypertext Transfer Protocol
Line-based text data: text/html
      00 08 74 4f 36 23 00 06
                               25 da af 73 08 00 45 00
                                                          ..to6#.. %..s..E.
      01 dc 21 71 40 00 37 06
                               e9 18 80 77 f5 0c c0 a8
                                                          ..!q@.7. ...w....
                                                         .f.P..... P.
     01 66 00 50 10 b0 85 b2
                               bb 80 fb 98 e0 df 50 18
     19 20 25 ab 00 00 3e 3c
                               68 33 3e 41 6d 65 6e 64
                                                          . %...>< h3>Amend
     6d 65 6e 74 20 49 58 3c
                               2f 68 33 3e 3c 2f 73 74
                                                          ment IX< /h3></st
     72 6f 6e 67 3e 3c 2f 61
                               3e 0a 0a 3c 70 3e 3c 2f
                                                          rong></a >..</
     70 3e 3c 70 3e 54 68 65
                               20 65 6e 75 6d 65 72 61
                                                          p>The enumera
     74 69 6f 6e 20 69 6e 20
                               74 68 65 20 43 6f 6e 73
                                                          tion in the Cons
     74 69 74 75 74 69 6f 6e
                               2c 20 6f 66 20 63 65 72
                                                          titution, of cer
     74 61 69 6e 20 72 69 67
                               68 74 73 2c 20 73 68 61
                                                          tain rig hts. sha
     6c 6c 0a 6e 6f 74 20 62
75 65 64 20 74 6f 20 64
                                                          11. not b e constr
                               65 20 63 6f 6e 73 74 72
                               65 6e 79 20 6f 72 20 64
                                                          ued to d eny or d
     69 73 70 61 72 61 67 65
                               20 6f 74 68 65 72 73 20
                                                          isparage others
     72 65 74 61 69 6e 65 64
                               20 62 79 20 74 68 65 20
                                                          retained
                                                                   by the
     70 65 6f 70 6c 65 2e 0a
                               0a 3c 2f 70 3e 3c 70 3e
                                                          people...
     3c 61 20 6e 61 6d 65 3d
                               22 31 30 22 3e 3c 73 74
                                                          <a name= "10"><st
     72 6f 6e 67 3e 3c 68 33
6e 74 20 58 3c 2f 68 33
                               3e 41 6d 65
3e 3c 2f 73
                                                          rong><h3 >Amendme
                                                          nt X</h3 ></stron
     67 3e 3c 2f 61 3e 0a 0a
                               3c 70 3e 3c 2f 70 3e 0a
                                                          g></a>.. .
                               6f 77 65 72 73 20 6e 6f
     3c 70 3e 54 68 65 20 70
                                                          The p owers no
     74 20 64 65 6c 65 67 61
                                                          t delega ted to t
0150 68 65 20 55 6e 69 74 65
                               64 20 53 74 61 74 65 73
                                                          he Unite d States
     20 62 79 20 74 68 65 20
                               43 6f 6e 73 74 69 74 75
                                                          by the Constitu
     74 69 6f 6e 2c 20 6e 6f
                               72 20 70 72
                                                          tion, no r prohib
     69 74 65 64 20 0a 20 20
                               62 79 20 69 74 20 74 6f
                                                                  by it to
     20 74 68 65 20 73 74 61
                               74 65 73
                                                          the sta tes, are
     20 72 65 73 65 72 76 65
                               64 20 74 6f 20 74 68 65
                                                          reserve d to the
     20 73 74 61 74 65 73 20
                              72 65 73 70 65 63 74 69
                                                           states respecti
     76 65 6c 79 2c 20 6f 72
                              20 74 6f 20 74 68 65 20
                                                          vely, or to the
     70 65 6f 70 6c 65 2e 3c 2f 70 3e 0a 3c 2f 62 6f
                                                          people. . </bo
     64 79 3e 3c 2f 68 74 6d
                                                          dy></htm 1>
```

## HTTP GET request

The Wireshark log shows response to a HTTP-GET request.

How many bytes data are returned to the application layer from the current TCP segment?

```
Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: 4272 (4272), Seq: 4381, Ack: 502, Len: 436

  [4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]

Hypertext Transfer Protocol
Line-based text data: text/html
                                                         ..to6#.. %..s..E.
     00 08 74 4f 36 23 00 06
     01 dc 21 71 40 00 37 06
                               e9 18 80 77 f5 0c c0 a8
                                                         ..! q@.7. ...w....
     01 66 00 50 10 b0 85 b2
                              bb 80 fb 98 e0 df 50 18
                                                         .f.P..... P.
     19 20 25 ab 00 00 3e 3c
                              68 33 3e 41 6d 65 6e 64
                                                         . %...>< h3>Amend
     6d 65 6e 74 20 49 58 3c
                              2f 68 33 3e 3c 2f 73 74
                                                         ment IX< /h3></st
     72 6f 6e 67 3e 3c 2f 61
                                                         rong></a >..</
                               3e 0a 0a 3c 70 3e 3c 2f
     70 3e 3c 70 3e 54 68 65
                               20 65 6e 75 6d 65 72 61
                                                         p>The enumera
     74 69 6f 6e 20 69 6e 20
                               74 68 65 20 43 6f 6e 73
                                                         tion in the Cons
     74 69 74 75 74 69 6f 6e
                              2c 20 6f 66 20 63 65 72
                                                         titution, of cer
     74 61 69 6e 20 72 69 67
                               68 74 73 2c 20 73 68 61
                                                         tain rig hts. sha
     6c 6c 0a 6e 6f 74 20 62
75 65 64 20 74 6f 20 64
                                                         11. not b e constr
                               65 20 63 6f 6e 73 74 72
                               65 6e 79 20 6f 72 20 64
                                                         ued to d eny or d
     69 73 70 61 72 61 67 65
                              20 6f 74 68 65 72 73 20
                                                          isparage others
     72 65 74 61 69 6e 65 64
                               20 62 79 20 74 68 65 20
                                                         retained by the
     70 65 6f 70 6c 65 2e 0a
                               0a 3c 2f 70 3e 3c 70 3e
                                                         people...
     3c 61 20 6e 61 6d 65 3d
                               22 31 30 22 3e 3c 73 74
                                                          <a name= "10"><st
     72 6f 6e 67 3e 3c 68 33
6e 74 20 58 3c 2f 68 33
                              3e 41 6d 65
3e 3c 2f 73
                                                         rong><h3 >Amendme
                                                         nt X</h3 ></stron
     67 3e 3c 2f 61 3e 0a 0a
                              3c 70 3e 3c 2f 70 3e 0a
                                                         g></a>.. .
                               6f 77 65 72 73 20 6e 6f
     3c 70 3e 54 68 65 20 70
                                                          The p owers no
     74 20 64 65 6c 65 67 61
                                                         t delega ted to t
     68 65 20 55 6e 69 74 65
                               64 20 53 74 61 74 65 73
                                                         he Unite d States
     20 62 79 20 74 68 65 20
                               43 6f 6e 73 74 69 74 75
                                                          by the Constitu
     74 69 6f 6e 2c 20 6e 6f
                              72 20 70 72
                                                         tion, no r prohib
     69 74 65 64 20 0a 20 20
                                                                  by it to
     20 74 68 65 20 73 74 61
                              74 65 73
                                                          the sta tes, are
     20 72 65 73 65 72 76 65
                              64 20 74 6f 20 74 68 65
                                                          reserve d to the
     20 73 74 61 74 65 73 20
                              72 65 73 70 65 63 74 69
                                                          states respecti
     76 65 6c 79 2c 20 6f 72
                              20 74 6f 20 74 68 65 20
                                                         vely, or to the
     70 65 6f 70 6c 65 2e 3c 2f 70 3e 0a 3c 2f 62 6f
                                                         people. . </bo
     64 79 3e 3c 2f 68 74 6d
                                                         dy></htm 1>
```

# **Application Layer Protocol**

#### Wireshark IPv4 vs IPv6

Which network scenario does the Wireshark log in the figure illustrate?

```
Frame 4749: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
*Ethernet II, Src: ZyxelCom 38:89:63 (cc:5d:4e:38:89:63), Dst: 60:31:97:45:b1:62 (60:31:97:45:b1:62)
 *Destination: 68:31:97:45:b1:62 (68:31:97:45:b1:62)
 ▶ Source: ZyxelCom 38:89:63 (cc:5d:4e:38:89:63)
  Type: IPv6 (8x86dd)
Internet Protocol Version 6, Src: 2001:464d:e5d4:0:ce5d:4eff:fe38:8963 (2001:464d:e5d4:0:ce5d:4eff:fe38:8963), Dst: 2a02:c0:ac::e51:1 (2a02:c0:ac::e51:1)
 ▶8118 .... = Version: 6
 +.... 0000 0000 .... .... .... = Traffic class: 0x00000000
  .... .... 8888 8888 8888 8888 8888 = Flowlabel: 8x888888888
  Payload length: 32
  Next header: TCP (6)
  Hop limit: 64
  Source: 2001:464d:e5d4:0:ce5d:4eff:fe38:8963 (2001:464d:e5d4:0:ce5d:4eff:fe38:8963)
  [Source SA MAC: ZyxelCom 38:89:63 (cc:5d:4e:38:89:63)]
  Destination: 2a02:c0:ac::e51:1 (2a02:c0:ac::e51:1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
* Transmission Control Protocol, Src Port: 44645 (44645), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0
```

#### Wireshark IPv4 vs IPv6

Which network scenario does the Wireshark log in the figure illustrate?

IPv6 traffic

```
Frame 4749: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
*Ethernet II, Src: ZyxelCom 38:89:63 (cc:5d:4e:38:89:63), Dst: 60:31:97:45:b1:62 (60:31:97:45:b1:62)
 *Destination: 68:31:97:45:b1:62 (68:31:97:45:b1:62)
 ▶ Source: ZyxelCom 38:89:63 (cc:5d:4e:38:89:63)
  Type: IPv6 (8x86dd)
→ Internet Protocol Version 6, Src: 2001:464d:e5d4:0:ce5d:4eff:fe38:8963 (2001:464d:e5d4:0:ce5d:4eff:fe38:8963), Dst: 2a02:c0:ac::e51:1 (2a02:c0:ac::e51:1)
 ▶8118 .... = Version: 6
 >.... 0000 0000 .... = Traffic class: 0x000000000
  .... .... 8888 8888 8888 8888 8888 = Flowlabel: 8x888888888
  Payload length: 32
  Next header: TCP (6)
  Hop limit: 64
  Source: 2001:464d:e5d4:0:ce5d:4eff:fe38:8963 (2001:464d:e5d4:0:ce5d:4eff:fe38:8963)
  [Source SA MAC: ZyxelCom 38:89:63 (cc:5d:4e:38:89:63)]
  Destination: 2a02:c0:ac::e51:1 (2a02:c0:ac::e51:1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
* Transmission Control Protocol, Src Port: 44645 (44645), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0
```

# Link-state Algorithm

