

# i IKT204-G V24, Front page

**Subject code:** IKT204-G

**Subject name:** Data communication

**Date:** 07.05.2024

**Duration:** 3 hours

**Resources allowed:** Calculator (note that graphing calculators are **NOT** allowed and that programmable calculators must have **ALL** installed programs deleted).

## Technical information:

- The exam is both in English and Norwegian (with some headings and expressions in English). You select language in the menu at the upper right corner. Note that you can select to view assignments in English or Norwegian at any time during the exam.
- The exam contains assignments of the type multiple choice, multiple answer, pulldown menu, fixed text and calculation.
- Each correctly answered assignment gives from 2 to 12 points, in total 104 points. For each part of an assignment:
  - Correct answer gives 0.35 - 2 points for each question, depending on difficulty.
  - Wrong answer gives 0 points for all questions except multiple answer assignments.
  - Wrong answers in multiple answer assignments give a negative score, so if you click on all the options in the assignment the sum will be 0 points. A negative score for the assignment as a whole is not possible.
- There is an open text field on the last page which may be used for writing additional comments and assumptions to the assignments of the exam. This text field does not give any points in itself, but it may impact the judgement of other assignments. It is not necessary to use the text field since correct answer on all questions will give full score. If the question is not correct, then you may get additional points if you explain a partially correct solution or give a good assumption in the text field.

# 1 IKT204-G V24, Internet 5-layer model

What are the data packets on the different layers called? (6 points)

Application layer  Select alternative (Protocol stack, Segment, Datagram, **Message**, Protocol suite, Bits, Bytes, Request, Frame, Response)

Transport layer  Select alternative (Message, Bits, Frame, Protocol stack, Datagram, Request, Bytes, Response, **Segment**, Protocol suite)

Network layer  Select alternative (Message, **Datagram**, Response, Frame, Bytes, Segment, Protocol stack, Request, Bits, Protocol suite)

Link layer  Select alternative (Bits, Request, Message, Response, Protocol stack, Datagram, Protocol suite, **Frame**, Segment, Bytes)

Physical layer  Select alternative (**Bits**, Protocol suite, Datagram, Frame, Bytes, Request, Message, Response, Protocol stack, Segment)

All these layers are together called a:  Select alternative (**Protocol stack**, Segment, Datagram, Response, Protocol suite, Bits, Frame, Message, Bytes, Request)

---

Maximum marks: 6

## 2 IKT204-G V24, Wireshark HTTP

The PDF document shows two excerpts from a Wireshark capture. Both excerpts are from the same TCP connection and shows the start and end of a session. **Note that you need to scroll down to the bottom of the PDF document to see the end of the session.** Answer the following questions: (12 points)

Which link layer protocol is used here?  Select alternative (IEEE 802.11, UDP, TCP, DHCP, Ethernet, IP, ARP, HTTP, SSL)

Which protocol is encapsulated in the link layer frame?  Select alternative (TCP, Ethernet, IPv6, IEEE 802.11, UDP, DHCP, IPv4, SMTP, HTTP, ARP, SSL)

How large is the announced window size in number of bytes in packet 330?  Select alternative (65024, 554, 256, 1573, 113978, 254)

What type of window is this?  Select alternative (Sliding window in number of packets, Congestion window, Window size of the user interface, Receiver window)

Which application layer protocol is used here?  Select alternative (IPv4, Ethernet, ARP, IPv6, UDP, HTTP, TCP, DHCP)

Who sends packet 330?  Select alternative (The client, None, The server)

What is the client's port number in this TCP connection?  (60104)

What type of connection is the application layer protocol using?  Select alternative (Persistent connection, One-shot connection, Time-out connection, Non-persistent connection)  
The application layer protocol in use here uses cookies. But what is a cookie?

Select alternative (It is a cache of previously downloaded web page objects., It is a piece of data which is sent from a website and stored on the client's end-system in a special cookie file managed by the browser., It is an executable code snippet that is downloaded from a website and stored on the client's end system to improve the website's performance., It is a list of previously opened websites.)

Is cookie information exchanged in packet 330?  Select alternative (Yes, No)

How many bytes of application data are sent with packet 330?  (554)

How many routers may packet 330 pass through before it is discarded?  (127)

Who initiates termination of this TCP connection?  Select alternative (None, The client, The server)

Which sequence number did the very first byte get in application data exchanged between the client and the server?  (1)

How many bytes of application data have been transferred during this TCP session?

Client has sent:  (1572 - 1574) Server has sent:  (114406 - 114408)

---

Maximum marks: 12

### 3 IKT204-G V24, DNS

Below are some statements about Domain Name System (DNS) and how it works. (5 points)

**Select correct alternatives:**

- DNS queries use port 53 over UDP. ✓
- Top-level domain (TLD) DNS servers are located at the top of the hierarchy of DNS servers.
- The DNS service belongs to the application layer in the Internet five-layer protocol stack. ✓
- DNS queries use port 5353 over TCP.
- Root DNS servers are located at the top of the hierarchy of DNS servers. ✓
- The DNS service belongs to the network layer in the Internet five-layer protocol stack.
- Authoritative DNS servers are located at the top of the hierarchy of DNS servers.
- An iterative DNS query puts the burden for resolving the domain name on the server requested.
- A domain name may be added to DNS by an usual DNS query.
- A domain name may be added to DNS by an accredited registrar. ✓
- A recursive DNS query puts the burden for resolving the domain name on the server requested. ✓
- A domain name may be added to DNS by a Certificate Authority (CA).
- DNS queries are by default encrypted.

---

Maximum marks: 5

## 4 IKT204-G V24, DHCP

Below are some statements about Dynamic Host Configuration Protocol (DHCP) and how it works. (6 points)

**Select correct alternatives:**

- DHCP provides IP addresses to root DNS servers.
- DHCP allows a host to obtain an IP address automatically. ✓
- DHCP is a network layer protocol.
- DHCP provides LAN subnet mask. ✓
- DHCP provides IP address to nearest switch.
- DHCP provides ISP subnet mask.
- DHCP is a link layer protocol.
- DHCP provides IP address to LAN gateway (nearest router). ✓
- DHCP provides IP addresses to local DNS servers. ✓
- DHCP provides IP addresses to TLD DNS servers.
- DHCP allows a host to obtain a MAC address automatically.
- DHCP allows a host to obtain a socket port number automatically.
- DHCP is an application layer protocol. ✓
- DHCP is a client-server protocol. ✓

---

Maximum marks: 6

## 5 IKT204-G V24, UDP quality of service

Which service quality guarantees does User Datagram Protocol (UDP) give? (2 points)

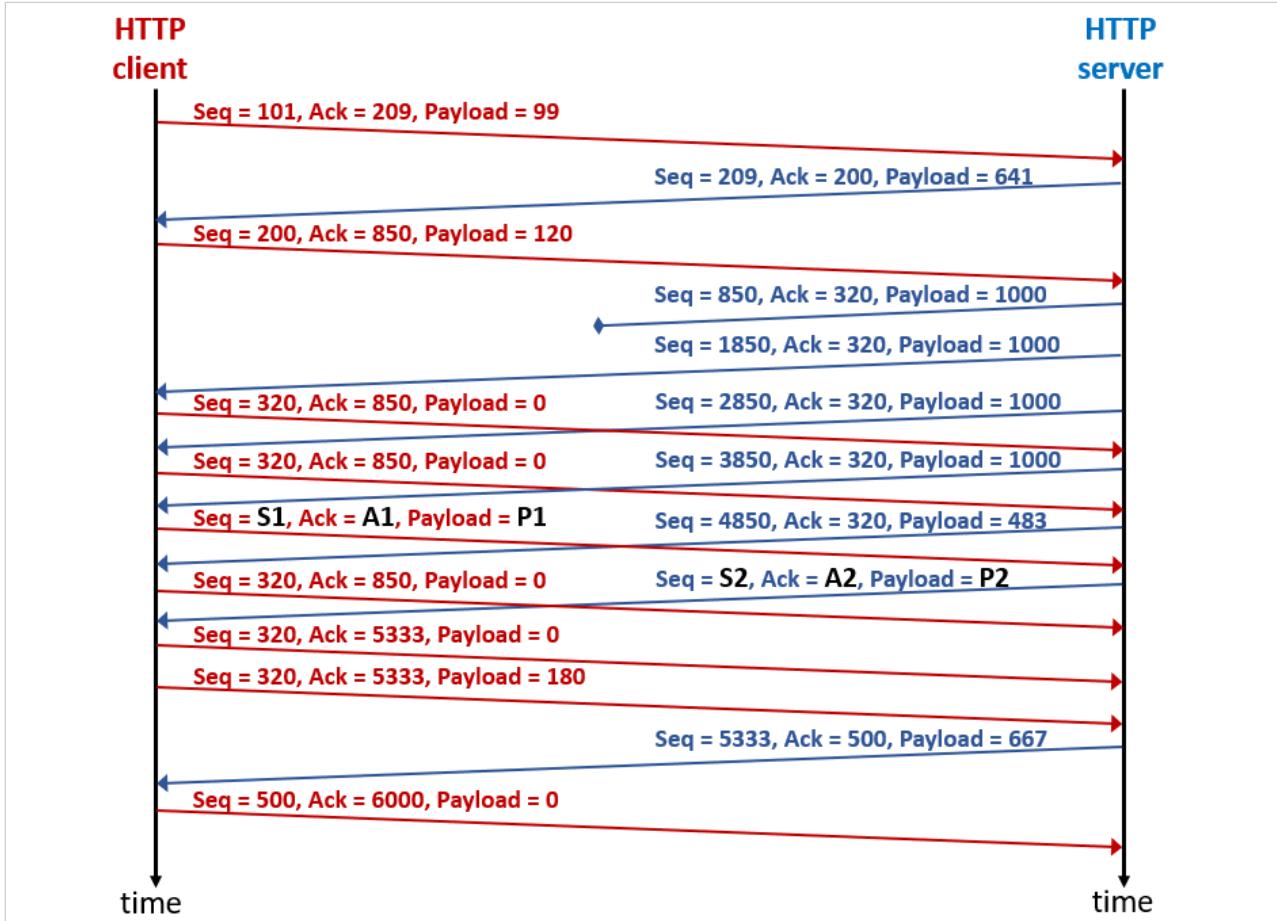
**Select one or more alternatives:**

- Server authentication
- Data integrity
- Bounded delay
- In-order data delivery
- Reliable data transfer
- Data confidentiality
- Guaranteed bandwidth
- None of these ✓

---

Maximum marks: 2

## 6 IKT204-G V24, TCP sequence



Above is an excerpt from a TCP (Reno version) transmission. What will the sequence number, acknowledgement number and payload length denoted **S1**, **A1**, **P1**, **S2**, **A2** and **P2** be in the segments shown in the figure? (9 points)

$$\begin{array}{llll} S1 = & \boxed{\phantom{000}} (320) & A1 = & \boxed{\phantom{000}} (850) & P1 = & \boxed{\phantom{000}} (0) \\ S2 = & \boxed{\phantom{000}} (850) & A2 = & \boxed{\phantom{000}} (320) & P2 = & \boxed{\phantom{000}} (1000) \end{array}$$

The fourth segment is lost somewhere in the network on its route to the client. How does TCP ensure that this segment is delivered as shown in the excerpt above?

Select alternative (Segment is re-transmitted after receiving triple duplicate ACK., It is up to the application layer to re-transmit the lost segment., Segment is re-transmitted on timeout., The link layer will ensure reliable data transfer in this case.)

TCP also have a re-transmission timer. What happens when this timer expires?

Select alternative (On timeout the connection is shut down., On timeout only the segment that caused the timeout is re-transmitted., On timeout all unacknowledged segments are re-

transmitted.)

The client has received segments out of sequence. What has the client done with these?

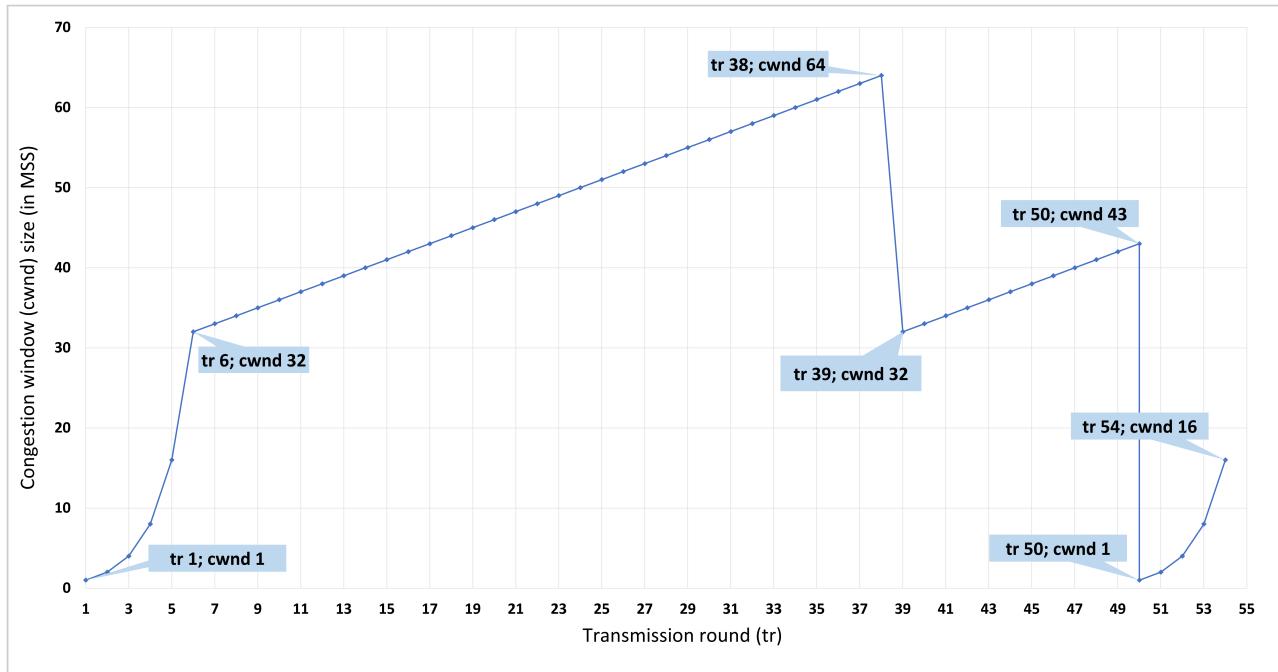
Select alternative

(The client has only taken care of the segment that succeeded the segment that was lost., The client has stored them and can acknowledge accumulated., Impossible to say based on the excerpt shown., The client has discarded them, so the server must resend the segments.)

---

Maximum marks: 9

## 7 IKT204-G V24, TCP congestion control



TCP Reno's congestion control algorithm has 3 states: Slow Start, Congestion Avoidance and Fast Recovery. The figure shows the size of TCP Reno's congestion window (cwnd) in number of segments as a function of the transmission round (tr). Answer the following questions: (7 points)

Identify an interval where TCP Slow Start is in action?  Select alternative ([38,39], [6,38], [1,6], [6,50])

Identify an interval where TCP Congestion Avoidance is in action?  Select alternative ([50,54], [6,38], [1,6], [38,39])

TCP is in the state Fast Recovery in the transmission round [38,39]. What caused TCP to end up

in this state?  Select alternative (Received a triple duplicate ACK., Received an Explicit Congestion Notification (ECN)., An ACK timeout occurred., Received a new ACK.)

When does TCP enter the state Slow Start?  Select alternative (When establishing a TCP connection and when there is a timeout on ACK., When establishing a TCP connection and when a new ACK is received., Upon receiving a triple duplicate ACK., Upon receipt of an Explicit Congestion Notification (ECN).)

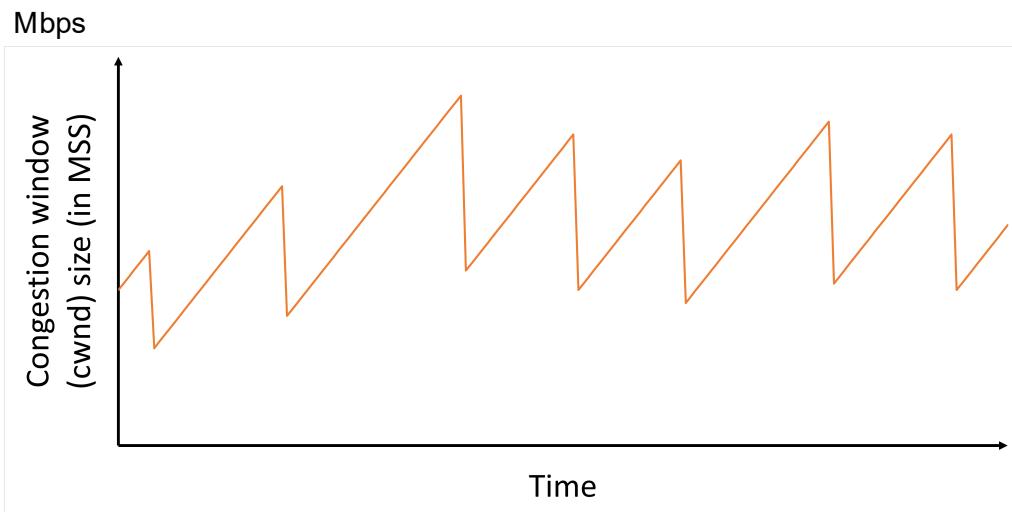
TCP Reno's congestion control mechanism is called AIMD - Additive Increase Multiplicative

Decrease. What is driving the additive increase of the congestion window?  Select alternative (Reception of segments containing payload., Receipt of Explicit Congestion Notification (ECN)., A recurring timer., Receiving new ACKs.) And what is the speed this window increases at

associated with? Select alternative (The amount of received data in bytes within a specified interval., How often the retransmission timer gives timeouts., The end-to-end delay on the TCP connection., Round trip time - RTT)

The result of AIMD congestion control is that we get such a "saw tooth-like" behavior on the congestion window over time with TCP Reno in normal operating mode as shown in the figure below. Assume that the **maximum** size of the congestion window is roughly constant and equal to **250** over the duration of a TCP connection. Assume further that the Maximum Segment Size (MSS) is **560 bytes** and that the round-trip time RTT is **20 milliseconds**.

What would be the average data transfer rate on such a TCP connection in **Mbps**?  (41 - 43)



---

Maximum marks: 7

## 8 IKT204-G V24, IPv4 and subnet

Suppose an ISP owns the block of addresses of the form 85.175.130.0/23. Suppose it wants to create four subnets from this block, with each block having the same number of IPv4 addresses. (7 points)

**What are the prefixes (of the format a.b.c.d/x) for the four subnets in increasing order?**

Subnet 1: 85.175.  (130) .  (0) /  (25)

Subnet 2: 85.175.  (130) .  (128) /  (25)

Subnet 3: 85.175.  (131) .  (0) /  (25)

Subnet 4: 85.175.  (131) .  (128) /  (25)

How many bits constitutes the host portion of the prefixes created for the four subnets?  (7) bits.

How many hosts may be assigned an IPv4 address within each of the four subnets?   
(126 - 128) hosts.

---

Maximum marks: 7

## 9 IKT204-G V24, Routing standards

Below are some statements about routing at the network layer. (4 points)

**Fill in the correct expression in each sentence:**

The  Select alternative (OpenFlow protocol, RIP - Routing Information Protocol, OSPF - Open Shortest Path First, **BGP - Border Gateway Protocol**) is the de facto standard protocol for advertising routing information between autonomous systems. An important attribute exchanged is

the  Select alternative (IP-LIST, GW-PATH, **AS-PATH**, NEXT-HOP) which is a list of autonomous systems that datagrams are offered to pass through to reach the advertised remote

prefix. For this reason, this protocol is called a  Select alternative ("shortest path", "prefix

vector", "fastest path", "path vector") protocol. A prefix in this context  Select alternative (an SDN control plane, an IPv4 or IPv6 address, a DNS server that manages the prefix, **a block of IP addresses specified in CIDR format**).

---

Maximum marks: 4

## 10 IKT204-G V24, Routing tables

In this assignment, the objective is to determine the correct forwarding link given the routing table below. (5 points)

A router has the following entries in its forwarding table (IPv4 prefixes given in dotted-decimal form and binary):

Link1:	46.168.4.0/22	00101110.10101000.00000100.00000000/22
Link2:	46.168.6.0/23	00101110.10101000.00000110.00000000/23
Link3:	46.168.7.0/24	00101110.10101000.00000111.00000000/24
Link4:	46.168.0.0/15	00101110.10101000.00000000.00000000/15
Link5:	All other addresses	

Assume the router receives IPv4 datagrams destined to the following addresses and decide which link they are forwarded to:

A:	46.168.3.80	00101110.10101000.00000011.01010000
B:	46.168.5.254	00101110.10101000.00000101.11111110
C:	46.168.7.152	00101110.10101000.00000111.10011000
D:	46.168.6.130	00101110.10101000.00000110.10000010
E:	46.169.5.15	00101110.10101001.00000101.00001111

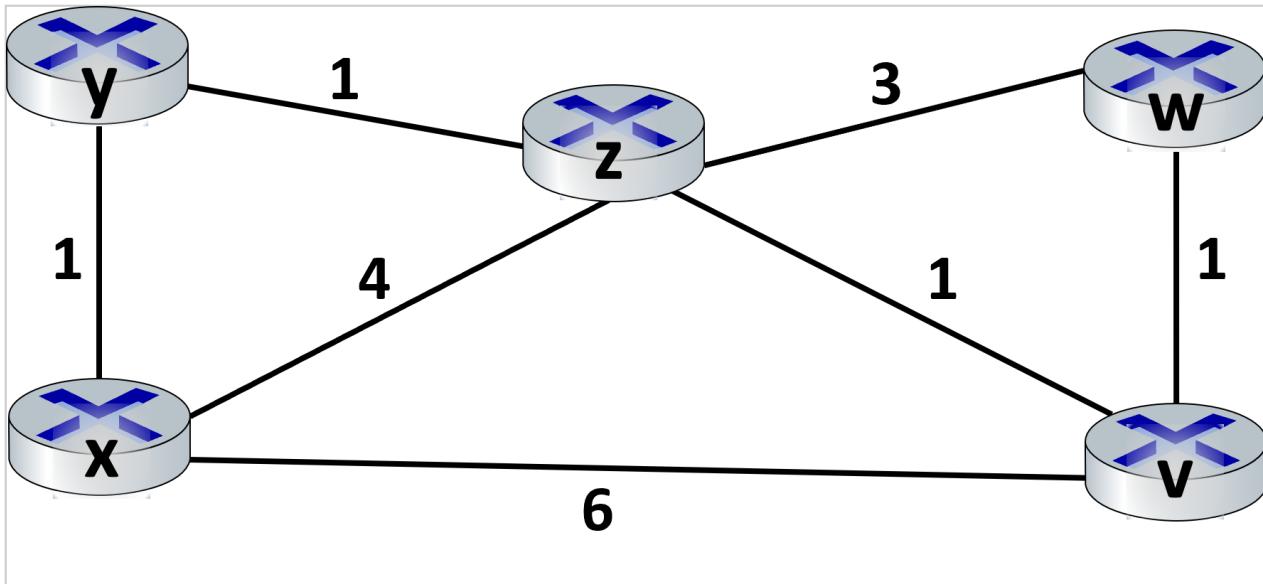
**On which link will they be forwarded?**

- A: link  (4)    B: link  (1)    C: link  (3)    D: link  (2)    E: link  (4)

---

Maximum marks: 5

## 11 IKT204-G V24, Link-state algorithm



First read the information under the table about the notation to be used. Then run Dijkstra's shortest-path algorithm in node **x** on the network of routers shown in the figure above and complete the table below. (5 points)

Step	$N'$	$D(z), p(z)$	$D(y), p(y)$	$D(v), p(v)$	$D(w), p(w)$
0	x	(4,x, 4x) 1x)	(1,x, 6x)	(6,x, 6x)	(inf, -)
1	(xy, x,y)	(2,y, 2y)		(6,x, 6x)	(inf, -)
2	(xyz, x,y,z)			(3,z, 3z)	(5,z, 5z)
3	(xyzv, x,y,z,v)				(4,v, 4v)
4	(xyzvw, x,y,z,v,w)				

Notation:

**N'** contains the visited nodes, listed in the **order** they are visited (e.g.: **uvxwy** or with comma **u,v,x,w,y**).

**D(n)** is the distance to node n.

**p(n)** is the previous node along this distance.

Use the following notation for **D(n),p(n)**: integer,node (e.g.: **4,z** or without comma **4z**).

If the node is **not** reachable, use **inf** or **single dash** for **D(n),p(n)**.

Maximum marks: 5



## 12 IKT204-G V24, Ethernet LAN and switches

Ethernet is the most widely used technology for wired Local Area Network (LAN). Answer the following questions and fill in the correct statement in the sentences at the bottom: (8 points)

Which IEEE standards specifies wired Ethernet? Select alternative (802.3, 802.13, 802.5, 802.11)

Which wired LAN topology is by far the most common today? Select alternative (Ring with token passing., Bus with all nodes in same collision domain., Star with point-to-point links and switch in the middle.)

Which cable type is most common in LANs today? Select alternative (Coaxial cable, Twisted-pair cable, Two-pair cable, Fiber optic cable)

A host in a LAN has been assigned IPv4 address: 10.10.99.17/22 in CIDR (Classless Inter-Domain Routing) format.

What is the network mask written in dotted-decimal notation?

Select alternative (22.22.22.22, 0.0.0.22, 255.255.252.0, 10.10.252.0, 255.255.1.0)

What is the correctly configured IPv4 address of the gateway router located in the same subnet as this host? Select alternative (10.10.99.0, 255.255.252.22, 10.10.96.1, 10.10.22.1, 10.10.1.1)

Ethernet switches are Select alternative (complex, fast and quite expensive, simple, fast and relatively inexpensive).

They forward frames based on the destination's Select alternative (host name, MAC address, IP address) and they have to Select alternative (get their switch tables configured by a network administrator, maintain their switch tables all by themselves, exchange information with other switches to update their switch tables).

---

Maximum marks: 8



**13 IKT204-G V24, ARP**

```
> 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: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)
  Padding: 0000000000000000000000000000000000000000000000000000000000000000
  └ 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

  0000 ff ff ff ff ff ff 3c a8 2a dd a3 00 08 06 00 01
  0010 08 00 06 04 00 01 3c a8 2a dd a3 00 80 27 c8 71
  0020 00 00 00 00 00 00 80 27 c8 a5 00 00 00 00 00 00
  0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Review the Wireshark capture above and assess the claims below regarding the Address Resolution Protocol (ARP). (5 points)

**Select correct alternatives:**

- A host can only have one MAC address.
- A host can have multiple IP addresses and multiple MAC addresses. ✓
- A MAC address has a fixed length of 48 bits. ✓
- ARP is a protocol that reside somewhere between the network layer and the link layer in the Internet 5-layer model. ✓
- Hosts and routers use ARP to associate an IP address to a MAC address and maintain an ARP table in their memory. ✓
- A MAC address has a fixed length of 64 bits.
- ARP broadcast address is ff:ff:ff:ff:ff:ff. ✓
- ARP replies always use the broadcast address as destination address.
- Host with IP address 128.39.200.165 has MAC address 3c:a8:2a:dd:a3:00.
- ARP requests ends up in a ARP server which will assign a MAC address to the requesting host.
- The MAC address of a host (client) in a LAN is encapsulated in the link layer frames it sends and follows the frames all the way to a host (server) in another LAN.
- ARP broadcast address is 00:00:00:00:00:00.

---

Maximum marks: 5

**14 IKT204-G V24, Transfer delay**

A gamer in Honningsvåg is connected to a Massively Multiplayer Online (MMO) server in Oslo. The transfer link from Honningsvåg to Oslo is 1620 km long and the propagation speed in the link medium is 200 000 km/s. The player has a 50 Mbps internet connection, and all routers and switches have high capacity, low load and negligible transmission delay. The game exchanges state messages of 434 bytes over TCP between clients and the server. Assume that TCP header is 20 bytes, IP header is 20 bytes, and the link layer overhead (Ethernet framing) is 26 bytes, and that each game message is sent in separate TCP segments to increase interactivity. (4 points)

What is the length of the link layer frame in **bits**?  (4000) bits

How large is the transmission delay in **microseconds** in this scenario? The answer is given without decimals:  (78 - 82)  $\mu\text{s}$

How large is the propagation delay in **milliseconds** in this scenario? The answer is given with 1 decimal:  (7.9 - 8.3) ms

What is the minimum round-trip time (RTT) in **milliseconds** for the game? The answer is given with 2 decimals:  (15.95 - 16.77) ms

---

Maximum marks: 4

## 15 IKT204-G V24, Wireless concepts and Wi-Fi LAN

Below are some general statements about wireless transmission as well as some more specific statements about how wireless IEEE 802.11 (Wi-Fi) LANs function. (9 points)

**Fill in the correct term in each sentence:**

Attenuation of the wireless signal when travelling through matter is called Select alternative (phase shifting, **path loss**, multipath propagation, modulation, interference).

When two or more sources within a basic service set (BSS) transmit at the same time on the

same frequency then Select alternative (multipath propagation, path loss, modulation, phase shifting, **interference**) may occur.

Blurring of the received signal due to several reflections of the electromagnetic wave from

objects and ground is called Select alternative (**multipath propagation**, interference, modulation, path loss, phase shifting).

In Select alternative (**infrastructure mode**, de facto mode, data mode, ad-hoc mode) each wireless host is connected to the Internet via an access point (AP).

In Select alternative (de facto mode, data mode, infrastructure mode, **ad-hoc mode**) wireless hosts themselves provide routing, address assignment and DNS-like services.

Wireless 802.11 (Wi-Fi) LAN uses a Select alternative (**Carrier Sense Multiple Access (CSMA)**, Code Division Multiple Access (CDMA), Frequency Division Multiple Access (FDMA),

Time Division Multiple Access (TDMA)) protocol with a Select alternative (collision detection mechanism (CD), first come, first served mechanism (FCFS), best possible signal-to-noise ratio mechanism (SNR), **collision avoidance mechanism (CA)**).

Wireless stations discover and identify the 802.11 (Wi-Fi) access point (AP) using

Select alternative (**RTS**, **beacon**, CTS, SIFS, DIFS, broadcast) frames.

A  Select alternative (broadcast, DIFS, SIFS, RTS, **CTS**, beacon) frame gives the 802.11 (Wi-Fi) transmitter of the  Select alternative (SIFS, CTS, broadcast, **RTS**, beacon, DIFS) frame explicit permission to send.

A 802.11 (Wi-Fi) station that has gone to sleep mode will  Select alternative (only wake up when it has something to send, **wake up regularly to receive beacon frames**, wake up regularly to ask the access point (AP) if it has frames waiting).

Wireless 802.11 (Wi-Fi) LAN operates on the  Select alternative (1.8 GHz and 4 GHz, **2.4 GHz and 5 GHz**, 3.5 GHz and 7 GHz) ISM bands.

---

Maximum marks: 9

## 16 IKT204-G V24, SSL socket and cryptographic algorithms

```
import socket
import ssl

name = 'localhost'
port = 8443
sslCtx = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
sslCtx.load_cert_chain(certfile = 'ca.crt', keyfile = 'private.key')
ls = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ls.bind((name, port))
ls.listen(1)

while True:
    cs, addr = ls.accept()
    print(cs.getpeername())
    sslSock = sslCtx.wrap_socket(cs, server_side = True)
    print(sslSock.cipher())
    while True:
        data = sslSock.recv(1024)
        if not data: break
        sslSock.sendall(data)
    sslSock.shutdown(socket.SHUT_RDWR)
    sslSock.close()
```

Here is a Python script that has printed ('127.0.0.1', 17425) as well as the negotiated cipher suite ('ECDHE-RSA-AES256-GCM-SHA384', 'TLSv1.2', 256) when it has been run. Below are some statements about this script and the cipher algorithms that were used in this session. (10 points)

**Select correct alternatives:**

- AES in Galois/Counter Mode with 256-bit key was used to encrypt the exchanged application messages, as well as to authenticate and verify the integrity of the messages. ✓
- AES is a one-way function and was used to make a digest (hash) of the messages sent.
- The server has port number 17425.
- SHA is a one-way function and produces a hash of specified size 384 bits. ✓
- The script shows a client that returns received data on port 8443.
- The negotiation protocol used was Transport Layer Security version 1.2. ✓
- SHA was used to make a digest (hash) of the exchanged TLS handshake messages in order to verify that they have not been tampered with. ✓
- The key exchange parameters were signed with the server's public RSA key.
- The key exchange parameters were signed with the server's private RSA key. ✓
- A digital certificate was used in this session to authenticate the server. ✓
- The client had port number 17425. ✓
- The script shows a server that is listening on port 8443. ✓
- ECDHE including a session authentication key ensured data integrity.
- The secret keys for the session were exchanged with RSA.
- A cryptographic digest (hash) ensures data confidentiality.
- A digital certificate was used to sign all the messages exchanged during this session.
- The secret keys for the session were created with the method Diffie-Hellman key exchange over elliptic curves. ✓
- Symmetric-key encryption ensures data confidentiality. ✓
- SHA with 384-bit key was used to encrypt the exchanged application messages.

---

Maximum marks: 10

## 17 IKT204-G V24, Comments and assumptions

Here you can write assumptions, clarifications and comments to your answers. These comments do not give additional points themselves, but may influence the judgement of commented assignments. (max 500 words)

**Write assumptions and comments to the assignments here:**

Format ▼ | **B** *I* U  $\times_{\text{e}}$   $\times^{\text{a}}$  | **I<sub>x</sub>** | | |  $\frac{1}{z} =$   $\ddot{z} =$  |  $\Omega$  | |

$\Sigma$  |

---

Words: 0

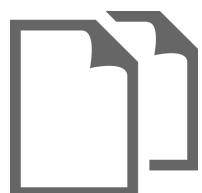
---

Maximum marks: 0



## Question 2

Attached



## Start of session:

No.	Time	Source	Destination	Protocol	Length	Info
61	1.684489	128.39.200.255	85.165.93.169	TCP	66	60104 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
65	1.698851	85.165.93.169	128.39.200.255	TCP	66	80 → 60104 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=128
66	1.698973	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
77	1.758497	128.39.200.255	85.165.93.169	HTTP	528	GET /assets/delta-vod-webapp.js.gz HTTP/1.1
83	1.772638	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [ACK] Seq=1 Ack=475 Win=30336 Len=0
87	1.776730	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=1 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
88	1.776732	85.165.93.169	128.39.200.255	TCP	316	80 → 60104 [PSH, ACK] Seq=1401 Ack=475 Win=30336 Len=262 [TCP segment of a reassembled PDU]
89	1.776817	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=1663 Win=65792 Len=0
93	1.779707	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=1663 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
94	1.779708	85.165.93.169	128.39.200.255	TCP	194	80 → 60104 [PSH, ACK] Seq=3063 Ack=475 Win=30336 Len=140 [TCP segment of a reassembled PDU]
95	1.779786	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=3203 Win=65792 Len=0
99	1.781707	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=3203 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
100	1.781707	85.165.93.169	128.39.200.255	TCP	114	80 → 60104 [PSH, ACK] Seq=4603 Ack=475 Win=30336 Len=60 [TCP segment of a reassembled PDU]
101	1.781775	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=4663 Win=65792 Len=0
105	1.784687	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=4663 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
106	1.784689	85.165.93.169	128.39.200.255	TCP	114	80 → 60104 [PSH, ACK] Seq=6063 Ack=475 Win=30336 Len=60 [TCP segment of a reassembled PDU]
107	1.784744	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=6123 Win=65792 Len=0
111	1.786679	85.165.93.169	128.39.200.255	TCP	662	80 → 60104 [PSH, ACK] Seq=6123 Ack=475 Win=30336 Len=608 [TCP segment of a reassembled PDU]

> Frame 66: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 > Ethernet II, Src: LcfCHefc\_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco\_ff:fd:90 (00:08:e3:ff:fd:90)  
 ✓ Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169

```

  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x54d9 (21721)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.39.200.255
    Destination: 85.165.93.169
  ✓ Transmission Control Protocol, Src Port: 60104, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 60104
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 1 (relative sequence number)
    [Next sequence number: 1 (relative sequence number)]
    Acknowledgment number: 1 (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x010 (ACK)
    Window size value: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
    Checksum: 0xfc8f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    > [SEQ/ACK analysis]
    > [Timestamps]
  
```

## End of session:

No.	Time	Source	Destination	Protocol	Length	Info
329	2.066686	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1019 Ack=113978 Win=65024 Len=0
330	2.082790	128.39.200.255	85.165.93.169	HTTP	608	GET /api/delta/fan/status HTTP/1.1
333	2.098738	85.165.93.169	128.39.200.255	HTTP	483	HTTP/1.1 200 OK (application/json)
336	2.138861	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1573 Ack=114407 Win=64512 Len=0
602	7.007701	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [FIN, ACK] Seq=114407 Ack=1573 Win=32512 Len=0
603	7.007777	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1573 Ack=114408 Win=64512 Len=0
609	7.273461	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [FIN, ACK] Seq=1573 Ack=114408 Win=64512 Len=0
611	7.287815	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [ACK] Seq=114408 Ack=1574 Win=32512 Len=0

```
> Frame 330: 608 bytes on wire (4864 bits), 608 bytes captured (4864 bits) on interface 0
> Ethernet II, Src: LcfHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)
```

Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 594
Identification: 0x5529 (21809)
> Flags: 0x4000, Don't fragment
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 128.39.200.255
Destination: 85.165.93.169
▼ Transmission Control Protocol, Src Port: 60104, Dst Port: 80, Seq: 1019, Ack: 113978, Len: 554
  Source Port: 60104
  Destination Port: 80
  [Stream index: 1]
  [TCP Segment Len: 554]
  Sequence number: 1019    (relative sequence number)
  [Next sequence number: 1573    (relative sequence number)]
  Acknowledgment number: 113978    (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window size value: 254
[Calculated window size: 65024]
[Window size scaling factor: 256]
Checksum: 0xeb9 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (554 bytes)
```

## ▼ Hypertext Transfer Protocol

```
> GET /api/delta/fan/status HTTP/1.1\r\n
Host: fanctrl.andersenitc.no\r\n
Connection: keep-alive\r\n
Accept: application/json, text/plain, */*\r\n
Date: Mon, 26 Nov 2018 07:55:58 GMT\r\n
Authorization: None\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36\r\n
Referer: http://fanctrl.andersenitc.no/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: nb,en-US;q=0.9,en;q=0.8\r\n
Cookie: _ga=GA1.2.870541523.1517819979; _biz_uid=cd6799c7fb3a4913b32c5dc59832da5d; _biz_nA=3; _biz_pendingA=%5B%5D\r\n
Cookie pair: _ga=GA1.2.870541523.1517819979
Cookie pair: _biz_uid=cd6799c7fb3a4913b32c5dc59832da5d
Cookie pair: _biz_nA=3
Cookie pair: _biz_pendingA=%5B%5D
\r\n
```



## DAT204 Exam h2019

Datakommunikasjon (Universitetet i Agder)



Skann for å åpne på Studocu

**DAT204-G H19, general information**

**Emnekode:** DAT204

**Emnenavn:** Datakommunikasjon

**Dato:** 17.12.2019

**Varighet:** 3 timer

**Tillatte hjelpeemidler:** Kalkulator

**Merknader:** Eksamenen er både på engelsk og norsk (med noen overskrifter og uttrykk på engelsk). Du velger språk i menyen øverst til høyre. Merk at du kan velge å vise oppgavene på engelsk eller norsk når som helst under eksamenen.

Hver korrekt besvart oppgave gir fra 2 til 12 poeng, totalt 100 poeng. For hver del av en oppgave:

- Korrekt svar gir 0,25 - 2 poeng for hvert spørsmål, avhengig av vanskelighetsgrad.
- Feil svar gir 0 poeng for alle spørsmål, unntatt flersvarsoppgavene.
- Feil svar i flersvarsoppgavene gir en negativ poengsum, slik at klikker du på alle valgmulighetene i oppgaven vil summen bli 0 poeng. En negativ poengsum er ikke mulig.

Eksamenen inneholder oppgaver av typen flervalg, flersvar, nedtrekksmeny, fast tekst og beregning. Det finnes et åpent tekstmfelt på den siste siden som kan brukes til å skrive ytterligere kommentarer og antagelser til oppgavene til eksamenen. Dette tekstmfeltet gir ingen poeng i seg selv, men det kan påvirke vurderingen av kommenterte oppgaver. Det er ikke nødvendig å bruke tekstmfeltet, siden riktig svar på alle spørsmålene vil gi full score. Hvis spørsmålet ikke er riktig, kan du få flere poeng hvis du forklarer en delvis korrekt løsning eller gir en god antagelse i tekstmfeltet.

---

Det forekommer av og til spørsmål om bruk av eksamensbesvarelser til undervisnings- og læringsformål. Universitetet trenger kandidatens tillatelse til at besvarelsen kan benyttes til dette. Besvarelsen vil være anonym.

**Tillater du at din eksamensbesvarelse blir brukt til slikt formål?**

- Ja  
 Nei

# 1 DAT204-G H19, Internet 5-layer model

Hva heter data pakkene på de forskjellige lagene? (3 poeng)

Applikasjonslaget  (Forespørsel, Datagram, Protokollstakk, Response, Segment, Bits, Protokoll suite, Melding, Bytes, Ramme)

Transportlaget  (Datagram, Protokollstakk, Protokoll suite, Melding, Forespørsel, Bits, Ramme, Bytes, Segment, Response)

Nettverkslaget  (Ramme, Forespørsel, Protokoll suite, Datagram, Protokollstakk, Bytes, Segment, Melding, Bits, Response)

Linklaget  (Protokoll suite, Protokollstakk, Forespørsel, Melding, Ramme, Bytes, Bits, Segment, Datagram, Response)

Fysisk lag  (Bits, Ramme, Datagram, Protokoll suite, Response, Segment, Protokollstakk, Bytes, Forespørsel, Melding)

Alle disse lagene kalles til sammen en:  (Bits, Ramme, Protokoll suite, Datagram, Response, Melding, Protokollstakk, Bytes, Forespørsel, Segment)

---

Maks poeng: 3

## 2 DAT204-G H19, Wireshark HTTP

PDF-dokumentet viser to utdrag fra en Wireshark-fangst. Begge utdragene er fra den samme TCP forbindelsen og viser starten og slutten av en økt. Svar på følgende spørsmål: (12 poeng)

Hvilken linklagsprotokoll brukes her?  (IEEE 802.15.4, DHCP, Ethernet, UDP, IP, HTTP, ARP, SSL, TCP)

Hvilken protokoll er innkapslet i linklagsrammen?  (UDP, DHCP, HTTP, SMTP, IEEE 802.9, IPv6, ARP, IPv4, TCP, SSL, Ethernet)

Hvor stor er den annonserede vindustørrelsen i antall byte i pakken 330?  (1573, 254, 256, 554, 113978, 65024)

Hva slags vindu er dette?  (Vindustørrelsen på brukergrensesnittet, Mottakervindu, Glidende vindu i antall pakker, Metningsvindu ("congestion window"))

Hvilken applikasjonslagsprotokoll brukes her?  (IPv6, HTTP, DHCP, Ethernet, ARP, IPv4, UDP, TCP)

Hvem sender pakke 330?  (Klienten, Serveren, Ingen)

Hva er klientens portnummer i denne TCP forbindelsen?

Hvilken type forbindelse bruker applikasjonslagsprotokollen?  (Vedvarende forbindelse, Tidsstyrt forbindelse, Engangs forbindelse, Ikke-vedvarende forbindelse)

Applikasjonslagsprotokollen i bruk her benytter informasjonskapsler ("cookies"). Men hva er en "cookie"?

(Det er en fil som lagrer server autentiseringsdata., Det er en liten tekstfil som er sendt fra et nettsted og lagret på klientens slutt-system., Det er en liste over tidligere åpnede nettsteder., Det er en cache for tidligere nedlastede nettsideobjekter.)

Er "cookie" informasjon utvekslet i pakke 330?  (Nei, Ja)

Hvor mange bytes med applikasjonsdata er sendt med pakke 330?

Hvor mange rutere kan pakken 330 passere før den blir forkastet?

Hjem initierer avslutning av denne TCP forbindelsen?  (Serveren, Klienten, Ingen)

Hvilket sekvensnummer fikk den aller første byten i applikasjonsdata utvekslet mellom klienten og serveren?

Hvor mange bytes med applikasjonsdata har blitt overført i løpet av denne TCP sesjonen?

Klienten har sendt:

Serveren har sendt:

---

Maks poeng: 12

### 3 DAT204-G H19, DNS

Nedenfor er noen utsagn om Domain Name System (DNS) og hvordan det fungerer. (5 poeng)

**Velg riktige alternativer:**

- Autoritative DNS-servere er plassert øverst i hierarkiet av DNS-servere.
- Et domenenavn kan legges til DNS med en vanlig DNS forespørsel.
- AA er en gyldig DNS oppføring.
- CNAME er en gyldig DNS oppføring.
- Top-level domain (TLD) DNS-servere er plassert øverst i hierarkiet av DNS-servere.
- En iterativt DNS forespørsel setter byrden for å løse domenenavnet på den forespurte serveren.
- Root DNS-servere er plassert øverst i hierarkiet av DNS-servere.
- DNS forespørsler bruker port 25 over TCP.
- DNS forespørsler er som standard kryptert.
- Et domenenavn kan legges til DNS av en akkreditert registrator.
- Et domenenavn kan legges til DNS av en Certificate Authority (CA).
- DNS forespørsler bruker port 53 over UDP.
- En rekursiv DNS forespørsel setter byrden for å løse domenenavnet på den forespurte serveren.

---

Maks poeng: 5

#### 4 DAT204-G H19, DHCP

Nedenfor er noen utsagn om Dynamic Host Configuration Protocol (DHCP) og hvordan den fungerer. (3 poeng)

**Velg riktige alternativer:**

- DHCP er en applikasjonslagsprotokoll.
- DHCP er en klient-server protokoll.
- DHCP er en linklagsprotokoll.
- DHCP gir IP-adresse til nærmeste svitsj.
- DHCP gir IP-adresse til LAN gateway (nærmeste ruter).
- DHCP tillater en vert å skaffe et socket portnummer automatisk.
- DHCP tillater en vert å skaffe en MAC-adresse automatisk.
- DHCP gir IP-adresser til lokale DNS servere.
- DHCP tillater en vert å skaffe en IP-adresse automatisk.
- DHCP gir LAN nettverksmaske.
- DHCP gir ISP nettverksmaske.
- DHCP er en nettverkslagprotokoll.
- DHCP gir IP-adresser til TLD DNS-servere.
- DHCP gir IP-adresser til root DNS servere.

---

Maks poeng: 3

## 5 DAT204-G H19, P2P

Ta i betrakting en server som distribuerer en fil på  $F = 15$  Gbits til  $N = 1000$  verter (kalt peers). Serveren har en opplastingsrate på  $u_s = 30$  Mbit/s, og hver peer har en nedlastingshastighet på  $d_{min} = d_i = 2$  Mbit/s og en opplastingshastighet på  $u_i = 700$  Kbit/s.

Filen kan distribueres med en klient-server arkitektur eller en peer-til-peer (P2P) arkitektur. Anta at minimum distribusjonstid er gitt av ligningene nedenfor for henholdsvis klient-server-arkitekturen og P2P-arkitekturen, og svar på følgende spørsmål. (4,5 poeng)

$$D_{cs} = \max \left\{ \frac{NF}{u_s}, \frac{F}{d_{min}} \right\}$$

$$D_{P2P} = \max \left\{ \frac{F}{u_s}, \frac{F}{d_{min}}, \frac{NF}{u_s + \sum_{i=1}^N u_i} \right\}$$

Hva er minimum distribusjonstid ved bruk av en klient-server arkitektur?  sekunder

Hva er minimum distribusjonstid ved bruk av en P2P arkitektur?  sekunder

Hvilken protokoll er en populær P2P-protokoll for fildistribusjon?

**Velg ett alternativ:**

- BitTorrent
- BitCoin
- BitBucket
- BitP2P
- BitXfer

---

Maks poeng: 4.5

## 6 DAT204-G H19, TCP and UDP statements

Hvilke av påstandene angående TCP og UDP er riktige? (5 poeng)

**Velg riktige alternativer:**

- For en TCP forbindelse kan antallet ubekrefte bytes ikke være større enn mottakerens annonserete vindusstørrelse.
- UDP segmenter med feil sjekk sum blir forkastet og sendt på nytt når rundturtiden (RTT) er utløpt.
- UDP headeren er liten, kun 8 bytes.
- Når UDP brukes, må eventuell feilkorreksjon gjøres i applikasjonen.
- UDP flytkontroll sikrer at mottakeren ikke oversvømmes.
- UDP tilbyr enkle transporttjenester uten noen form for pålitelig dataoverføring.
- TCP header parameter "Window size" er del av TCP metningskontroll algoritme.
- TCP har ingen flytkontroll mekanisme.
- UDP sikrer at meldingene blir levert til applikasjonen på mottakersiden i ordnet rekkefølge.
- TCP tilbyr en pålitelig dataoverføringstjeneste over et upålitelig internett.

---

Maks poeng: 5

**7 DAT204-G H19, TCP/UDP checksum**

TCP og UDP bruker 1-komplement (ener-komplement) for sine sjekksummer. Nedenfor er noen uttalelser om denne sjekksummen og hvordan det fungerer, samt en beregningsoppgave. (4,5 poeng)

**Velg ett alternativ:**

- Sjekksummen tas kun på TCP/UDP header.
- Sjekksummen tas over hele TCP/UDP segmentet, samt en pseudo header som inneholder noen felter fra IP headeren.
- Sjekksummen tas kun på nyttelasten i TCP/UDP segmentet.

**Velg ett alternativ:**

- Sjekksummen sikrer deteksjon av feil på kun ett bit.
- Sjekksummen sikrer deteksjon av alle mulige bit feil.
- Sjekksummen sikrer deteksjon av feil på inntil 16 bit.

Anta disse tre 16-bits ordene:

- 1010 0001 1000 0010
- 0100 0000 0000 0110
- 1010 1100 0001 0000

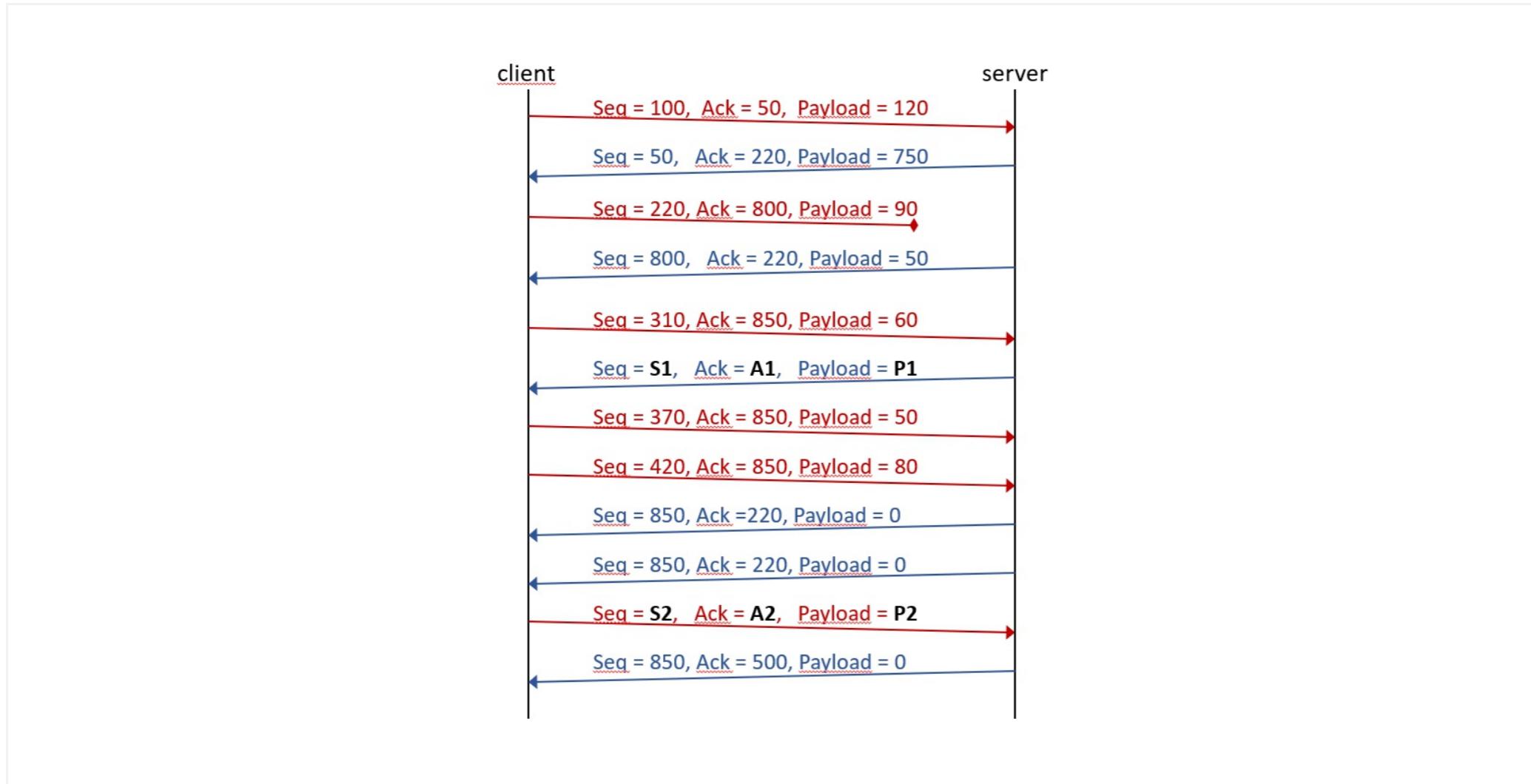
Hva er 1-komplement til summen av disse tre ordene? (Merk: eventuell mente fra det mest signifikante bit legges til resultatet fra en binær addisjon)

Sjekksum:

---

Maks poeng: 4.5

## 8 DAT204-G H19, TCP sequence



Ovenfor er et utdrag av en TCP (Reno versjon) overføring. Hva vil sekvensnummeret, bekreftelsesnummeret og nyttelastlengden benevnt **S1**, **A1**, **P1**, **S2**, **A2** og **P2** være i segmentene vist på figuren? (8 poeng)

S1=  A1=  P1=   
 S2=  A2=  P2=

Det tredje segmentet går tapt et sted i nettverket på sin vei til serveren. Hvordan sikrer TCP at dette segmentet blir levert som vist i utdraget over?



(Linklaget vil sikre pålitelig

dataoverføring i dette tilfellet., Segmentet sendes på nytt etter å ha mottatt trippel duplikat ACK., Det er opp til applikasjonslaget å sende det tapte segmentet på nytt., Segmentet sendes på nytt ved tidsavbrudd.)

TCP har også en re-transmisjonstimer. Hva skjer når denne timeren utløper?



(Ved tidsavbrudd tas

forbindelsen ned., Ved tidsavbrudd sendes kun det segmentet som forårsaket tidsavbruddet på nytt., Ved tidsavbrudd sendes alle ubekrefteede segmenter på nytt.)

Maks poeng: 8

**9 DAT204-G H19, TCP congestion handling**

Nedenfor er noen påstander om hvordan TCP (Reno) protokollen fungerer. Velg riktig påstand. (2 poeng)

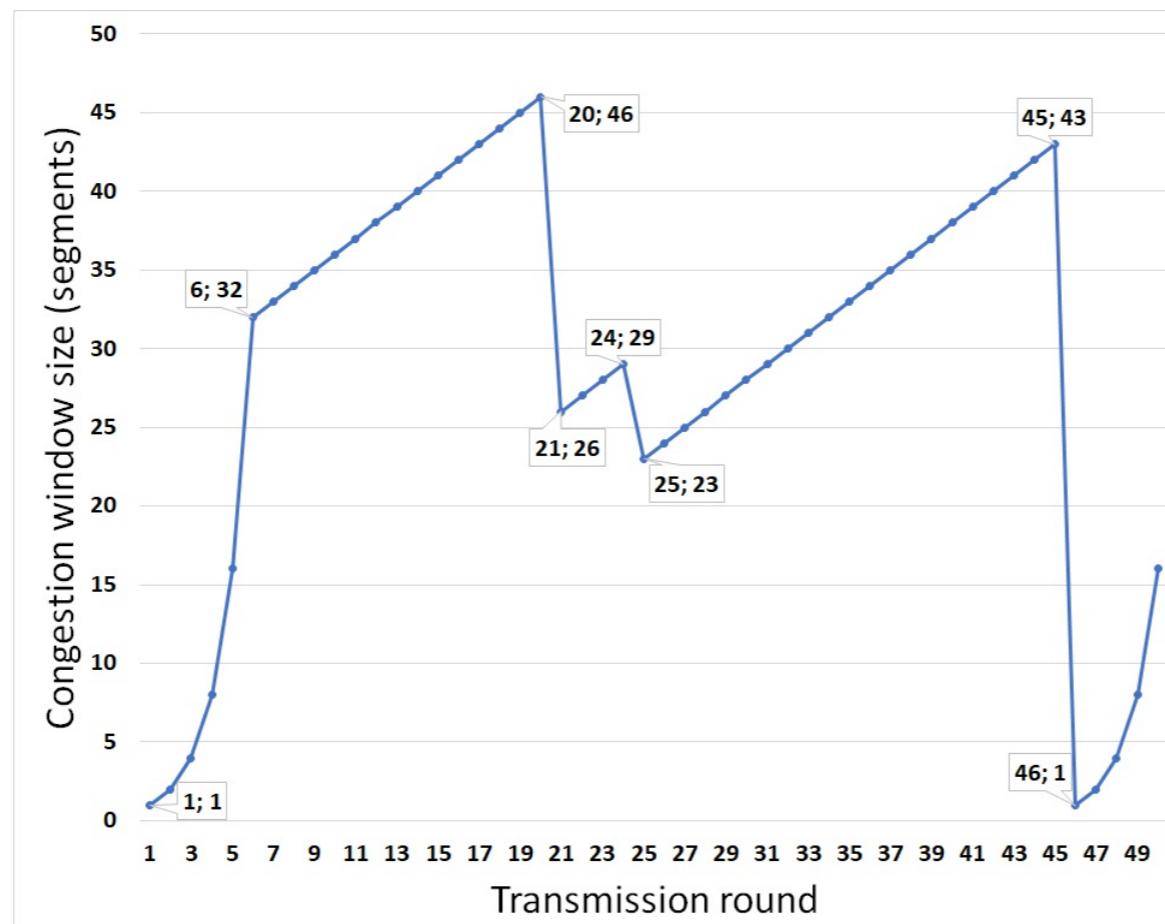
**Velg ett alternativ:**

- "Fast recovery" er betegnelsen på fasen i en TCP overføring der metningsvinduet (congestion window) øker eksponensielt raskt.
- "Congestion avoidance" er relatert til "Receive window" i TCP headeren.
- "Congestion avoidance" er betegnelsen på fasen i en TCP overføring der metningsvinduet (congestion window) øker lineært.
- TCP tidsavbrudd trigger "fast recovery".

---

Maks poeng: 2

## 10 DAT204-G H19, TCP congestion window



Figuren viser størrelsen på TCP Reno sitt metnings vindu (congestion window) i antall segmenter som en funksjon av overføringsrunden. Svar på følgende spørsmål: (7 poeng)

Identifiser et intervall der TCP "slow start" er i aksjon?  ([25,45], [6,20], [21,24], [1,6], [24,25], [20,21])

Identifiser et intervall der TCP "congestion avoidance" er i aksjon?  ([20,21], [1,6], [21,24], [24,25], [6,20], [46,49])

Identifiser et intervall der TCP "fast recovery" er i aksjon?  ([46,49], [1,6], [6,20], [21,24], [24,25], [25,45])

Hvordan er segmenttap identifisert etter den 20. overføringsrunden?

(Trippel duplikat ACK, RM celle med Congestion Indication (CI), Explicit Congestion Notification (ECN), Tidsavbrudd på ACK)

Hvordan er segmenttap identifisert etter den 45. overføringsrunden?

(RM celle med Congestion Indication (CI), Tidsavbrudd på ACK, Explicit Congestion Notification (ECN), Trippel duplikat ACK)

Hva er slow-start terskelen ved den 47. overføringsrunden?

Anta at Maximum Segment Size (MSS) er 1460 bytes og rundturtiden RTT=120 millisekunder, hva er gjennomsnittlig båndbredde i Mbit/s benyttet av TCP forbindelsen i overføringsintervallet [25,45]?  Mbit/s

Maks poeng: 7

**11 DAT204-G H19, IP and subnet**

Anta at en ISP eier IPv4 adresseblokken på formatet 105.16.80.0/23. Anta at den vil skape totalt fem sub-nett (SN) fra denne blokken, ved **først** å dele adresseblokken i fire sub-nett og deretter dele det **siste** sub-nettet i to slik at de tre første blokkene har samme antall IP-adresser og de to siste blokkene har samme antall IP-adresser. (4,25 poeng)

**Hva er prefiksene (på formatet a.b.c.d/x) for de fem sub-nettene i stigende rekkefølge?**

SN1: 105.16.  .  /

SN2: 105.16.  .  /

SN3: 105.16.  .  /

SN4: 105.16.  .  /

SN5: 105.16.  .  /

Hvor mange **bits** utgjør vertsdelen av prefiksene som er opprettet for SN1, SN2 og SN3?  bits

Hvor mange **verter** kan tildeles en IP-adresse innenfor SN4 og SN5?  verter

---

Maks poeng: 4.25

**12 DAT204-G H19, NAT**

Network Address Translation (NAT) er en mye brukt funksjon i lokalnett (LAN). Nedenfor er noen påstander om NAT. (4,5 poeng)

**Velg riktige alternativer:**

- NAT kan ha mer enn 60 000 samtidige TCP/UDP-forbindelser på en enkelt unik offentlig IP-adresse.
- NAT-funksjonen utføres vanligvis i en LAN svitsj konfigurert med en NAT-oversettingstabell.
- For pakker fra Internettet til et LAN, vil NAT-funksjonen bytte ut destinasjonens TCP/UDP-portnummer med et nummer kjent av mottaker og lagret i noden som utfører NAT-funksjonen.
- Adresseblokk IPv4 10.0.0.0/8 er reservert for tildeling av private IP-adresser til verter i et LAN.
- En sikkerhetsfordel med NAT er at vertsmaskiner i et LAN ikke kan adresseres direkte fra utsiden, dvs. fra Internett.
- For pakker fra Internett til et LAN, vil NAT-funksjonen erstatte avsenderens (kildens) TCP/UDP-portnummer med et nummer kjent av mottakeren.
- Adresseblokk IPv4 88.0.0.0/8 er reservert for tildeling av private IP-adresser til verter i et LAN.
- NAT-funksjonen utføres vanligvis i en LAN ruter på grensen mellom LAN-et og ISP-en/Internettet.
- NAT sparer ikke IPv4-adresser, siden hver private IP-adresse må byttes ut med sin egen unike offentlige IP-adresse.
- NAT-funksjonen utføres vanligvis av alle vertene i et LAN.
- NAT-funksjonen utføres vanligvis av ISP-en som LAN-et er tilkoblet.
- For pakker fra et LAN til Internettet, vil NAT-funksjonen bytte ut avsenders private IPv4-adresse med en unik offentlig IP adresse.

---

Maks poeng: 4.5

### 13 DAT204-G H19, Routing tables

I denne oppgaven er målet å bestemme den riktige videresendingslinken gitt ruting tabellen nedenfor. (5 poeng)

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

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

- A: 00001010.10111000.00000101.00000000
- B: 00001010.10101000.00000111.11111110
- C: 00001010.10101000.00000011.00000000
- D: 00001010.10101000.00000111.00000001
- E: 00001010.10101000.00000110.10000000

**På hvilken link vil de bli videresendt?**

- A: link
- B: link
- C: link
- D: link
- E: link

---

Maks poeng: 5

## 14 DAT204-G H19, Routing protocols

Nedenfor noen spørsmål om ruting protokoller. (3 poeng)

Hvilken protokoll er ansett som limet som holder Internettet sammen?

**Velg ett alternativ:**

- BGP
- ICMP
- RIP
- SNMP
- OSPF

Hvilken protokoll er vanlig brukt for å utveksle informasjon innad i autonome systemer som benytter en «link-state» (LS) algoritme for å beregne videresendingstabeller?

**Velg ett alternativ:**

- ICMP
- BGP
- RIP
- SNMP
- OSPF

Hvilken protokoll er vanlig brukt for å utveksle informasjon innad i autonome systemer som benytter en «distance-vector» (DV) algoritme for å beregne videresendingstabeller?

**Velg ett alternativ:**

- OSPF
- RIP
- BGP
- SNMP
- ICMP

---

Maks poeng: 3

## 15 DAT204-G H19, ARP

```

> 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: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)
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
  ▼ 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

0000 ff ff ff ff ff 3c a8 2a dd a3 00 08 06 00 01 .....< *.
0010 08 00 06 04 00 01 3c a8 2a dd a3 00 80 27 c8 71 .....< *....'q
0020 00 00 00 00 00 00 80 27 c8 a5 00 00 00 00 00 00 .....'.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....'.

```

Se gjennom Wireshark-fangsten ovenfor og vurder påstandene nedenfor angående Address Resolution Protocol (ARP). (4 poeng)

**Velg riktige alternativer:**

- ARP svar bruker alltid kringkastingsadressen som destinasjons adresse.
- En MAC-adresse har fast lengde på 48 bits.
- ARP forespørslar ender opp hos en ARP-server som tilordner en MAC-adresse til den spørrende verten.
- ARP er en protokoll som ligger et sted mellom nettverkslaget og linklaget i Internett 5-lags modellen.
- ARP kringkastingsadresse er 00:00:00:00:00:00.
- MAC-adressen til en vert (klient) i et LAN er innkapslet i link-lags rammene den sender og følger med rammene hele veien til en vert (server) i et annet LAN.
- En vert kan ha flere IP-adresser og flere MAC-adresser.
- En vert kan bare ha en MAC-adresse.
- 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.

Maks poeng: 4

**16 DAT204-G H19, Ethernet LAN**

Ethernet er den mest brukte teknologien for kablede Local Area Network (LAN). Svar på følgende spørsmål: (3,75 poeng)

Hvilke IEEE standarder spesifiserer kablet Ethernet?  (802.11, 802.3, 802.5, 802.13)

Hvilken kablet LAN topologi er den aller mest vanligste i dag?

(Stjerne med punkt-til-punkt linker og svitsj i midten..)

Ring med token passering., Buss med alle noder i samme kollisjons-domene.)

Hvilken kabel type er mest vanlig i LAN i dag?  (Fiberoptisk kabel, To-parkabel,

Koaksialkabel, Tvunnet parkabel)

En vert i et LAN har fått tildelt IPv4 adresse: 192.168.129.89/23 på CIDR format.

Hva er nettverksmasken skrevet på punktum-desimal format?  (0.0.0.23, 23.23.23.23,  
192.168.254.0, 255.255.254.0, 255.255.1.0)

Hva er korrekt konfigurerert adresse til gateway ruteren som befinner seg i samme subnett som denne verden?

(192.168.130.100, 192.168.1.1, 255.255.254.23, 192.168.23.1, 192.168.128.1)

---

Maks poeng: 3.75

**17 DAT204-G H19, Transfer delay**

Data sendes over en fiberlink på 6 000 km fra Oslo og til New York. Linken har en hastighet på 1 Gbit/s. Forplantningshastigheten på fiberen er 250 000 km/s. En ramme på 1500 bytes sendes på denne linken. Ruterne og svitsjene har høy kapasitet og er ikke overbelastet. (3 poeng)

Hvor stor er tidsforsinkelsen i millisekunder fra rammen sendes på linken fra Oslo og til den har blitt mottatt i New York? Avrund svaret til nærmeste millisekund.  ms

Hvor stor blir den minimale rundturforsinkelsen (RTT) i millisekunder for datagrammer på denne linken?

Avrund svaret til nærmeste millisekund.  ms

Hvilken type forsinkelse gir det største bidraget til den totale tidsforsinkelsen i dette scenariet?

(Transmisjonsforsinkelse, Forplantningsforsinkelse, Prosesseringsforsinkelse,  
Køforsinkelse)

Det gjennomføres en IP telefonisamtale over linken der avspillingsbufferet for å jevne ut jitter gir en tilleggsforsinkelse på 100 millisekunder. Er ende-til-ende tidsforsinkelsen på denne linken akseptabel for en IP telefonisamtale ut fra tjenestekvalitetskravene til slike samtaler?

**Velg et alternativ:**

- Nei
- Ja

---

Maks poeng: 3

## 18 DAT204-G H19, Wireless LAN ("Wi-Fi")

Hvilke av påstandene angående trådløst LAN er riktige? (6 poeng)

**Velg riktige alternativer:**

- En trådløs stasjon signaliserer at den går i dvale ved å sette et Power Management bit i rammens header.
- Trådløst LAN benytter en CSMA protokoll med en unngå kollisjonsmekanisme (CA).
- En trådløs stasjon informerer om at den går i dvale ved å sende en CTS ramme.
- Trådløst LAN er standardisert i en serie av IEEE 802.15 spesifikasjoner.
- En trådløs stasjon som har gått i dvale modus vil kun våkne opp når den har noe å sende.
- Trådløst LAN benytter en TDMA protokoll.
- Trådløst LAN opererer på 2,4 GHz og 5 GHz ISM båndene.
- En CTS ramme gir senderen av RTS rammen eksplisitt tillatelse til å sende.
- En RTS ramme instruerer alle andre stasjoner innenfor BSS om ikke å sende innenfor et reservert tidsrom.
- Trådløst LAN benytter en CSMA protokoll med deteksjon av kollisjoner (CD).
- En trådløs stasjon som har gått i dvale modus vil våkne opp regelmessig for å motta beacon rammer.
- Trådløst LAN opererer på 3,5 GHz og 6 GHz ISM båndene.
- En trådløs stasjon som har gått i dvale modus vil våkne opp regelmessig for å spørre aksesspunktet om den har rammer liggende å vente.
- Trådløst LAN er standardisert i en serie av IEEE 802.11 spesifikasjoner.

---

Maks poeng: 6

## 19 DAT204-G H19, SSL quality of service

Nedenfor er noen spørsmål om SSL sockets og tjenestekvaliteter: (3,5 poeng)

Hvilken socket type forbedrer Secure Socket Layer (SSL) med sikkerhetstjenester?

**Velg ett alternativ:**

- TCP
- IPv4
- HTTP
- IPv6
- UDP

Hva heter den oppdaterte, sikrere og i dag mest brukte versjonen av SSL protokollen?

**Velg ett alternativ:**

- Transport Layer Security (TLS)
- Link Layer Security (LLS)
- Application Layer Security (ALS)
- Network Layer Security (NLS)

Hvilke servicegarantier gir SSL sockets?

**Velg riktige alternativer:**

- Applikasjonsprogram troverdighet
- Server autentisering
- Pålitelig data overføring
- Data integritet
- Avgrenset forsinkelse
- Data konfidensialitet
- Garantert båndbredde
- I rekkefølge data levering

---

Maks poeng: 3.5

## 20 DAT204-G H19, SSL socket and cryptographic algorithms

```

import socket
import ssl

name = 'localhost'
port = 8443
sslCtx = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
sslCtx.load_cert_chain(certfile = 'ca.crt', keyfile = 'private.key')
ls = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ls.bind((name, port))
ls.listen(1)

while True:
    cs, addr = ls.accept()
    print(cs.getpeername())
    sslSock = sslCtx.wrap_socket(cs, server_side=True)
    print(sslSock.cipher())
    while True:
        data = sslSock.recv(1024)
        if not data: break
        sslSock.sendall(data)
    sslSock.shutdown(socket.SHUT_RDWR)
    sslSock.close()

```

Her vises et Python skript som har skrevet ut ('127.0.0.1', 62529) samt den fremforhandlede chiffer suite ('ECDHE-RSA-AES256-SHA384', 'TLSv1.2', 256) når det har blitt kjørt. Nedenfor er noen påstander om dette skriptet og om hvilke chiffer algoritmer som har vært i bruk i denne sesjonen. (9 poeng)

#### Velg riktige alternativer:

- Serveren har port nummer 62529.
- AES er benyttet for å lage et avtrykk av meldingene som er sendt.
- Symmetrisk-nøkkel kryptering sikrer data konfidensialitet.
- Et digitalt sertifikat er benyttet i denne sesjonen for å signere alle meldingene som er utvekslet i denne sesjonen.
- Et kryptografisk avtrykk (hash) sikrer data konfidensialitet.
- Parametrene for nøkkelutveksling er signert med serverens offentlige RSA nøkkel.
- ECDHE inkludert en autentiseringsnøkkel for sesjonen sikrer data integritet.
- Parametrene for nøkkelutveksling er signert med serverens private RSA nøkkel.
- De hemmelige nøklene for sesjonen er generert med metoden Diffie-Hellman nøkkelutveksling over elliptiske kurver.
- Skriptet viser en SSL server som returnerer mottatt data på port 8443.
- SHA er benyttet for å lage et avtrykk av meldingene som er sendt.
- AES med 256 bits nøkkel er benyttet for kryptering av applikasjonsmeldingene som er utvekslet.
- SHA med 384 bits nøkkel er brukt for kryptering av applikasjonsmeldingene som er utvekslet.
- De hemmelige nøklene for sesjonen er utvekslet med RSA.
- SHA inkludert en autentiseringsnøkkel for sesjonen sikrer data integritet.
- Skriptet viser en SSL klient som returnerer mottatt data på port 8443.
- Klienten har port nummer 62529.
- Et digitalt sertifikat er benyttet i denne sesjonen for å autentisere serveren.

**21 DAT204-G H19, comments and assumptions**

Her kan du skrive antagelser, avklaringer og kommentarer til svarene dine. Disse kommentarene gir ikke flere poeng i seg selv, men kan påvirke vurderingen av kommenterte oppgaver. (maks 500 ord)

**Skriv antagelser og kommentarer til oppgavene her:**

Format Font size | **B** *I* U  $\mathbf{x}_1$   $\mathbf{x}^2$  |  $\mathbf{I}_{\mathbf{x}}$  | | | | |  $\Sigma$  |

Words: 0

---

Maks poeng: 0



## Question 2

Attached



## Start of session:

No.	Time	Source	Destination	Protocol	Length	Info
61	1.684489	128.39.200.255	85.165.93.169	TCP	66	60104 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
65	1.698851	85.165.93.169	128.39.200.255	TCP	66	80 → 60104 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=128
66	1.698973	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
77	1.758497	128.39.200.255	85.165.93.169	HTTP	528	GET /assets/delta-vod-webapp.js.gz HTTP/1.1
83	1.772638	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [ACK] Seq=1 Ack=475 Win=30336 Len=0
87	1.776730	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=1 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
88	1.776732	85.165.93.169	128.39.200.255	TCP	316	80 → 60104 [PSH, ACK] Seq=1401 Ack=475 Win=30336 Len=262 [TCP segment of a reassembled PDU]
89	1.776817	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=1663 Win=65792 Len=0
93	1.779707	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=1663 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
94	1.779708	85.165.93.169	128.39.200.255	TCP	194	80 → 60104 [PSH, ACK] Seq=3063 Ack=475 Win=30336 Len=140 [TCP segment of a reassembled PDU]
95	1.779786	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=3203 Win=65792 Len=0
99	1.781707	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=3203 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
100	1.781707	85.165.93.169	128.39.200.255	TCP	114	80 → 60104 [PSH, ACK] Seq=4603 Ack=475 Win=30336 Len=60 [TCP segment of a reassembled PDU]
101	1.781775	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=4663 Win=65792 Len=0
105	1.784687	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=4663 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
106	1.784689	85.165.93.169	128.39.200.255	TCP	114	80 → 60104 [PSH, ACK] Seq=6063 Ack=475 Win=30336 Len=60 [TCP segment of a reassembled PDU]
107	1.784744	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=6123 Win=65792 Len=0
111	1.786679	85.165.93.169	128.39.200.255	TCP	662	80 → 60104 [PSH, ACK] Seq=6123 Ack=475 Win=30336 Len=608 [TCP segment of a reassembled PDU]

> Frame 66: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0  
 > Ethernet II, Src: LcfCHefc\_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco\_ff:fd:90 (00:08:e3:ff:fd:90)  
 ✓ Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169

```

  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x54d9 (21721)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.39.200.255
    Destination: 85.165.93.169
  ✓ Transmission Control Protocol, Src Port: 60104, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 60104
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 1 (relative sequence number)
    [Next sequence number: 1 (relative sequence number)]
    Acknowledgment number: 1 (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x010 (ACK)
    Window size value: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
    Checksum: 0xfc8f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    > [SEQ/ACK analysis]
    > [Timestamps]
  
```

## End of session:

No.	Time	Source	Destination	Protocol	Length	Info
329	2.066686	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1019 Ack=113978 Win=65024 Len=0
330	2.082790	128.39.200.255	85.165.93.169	HTTP	608	GET /api/delta/fan/status HTTP/1.1
333	2.098738	85.165.93.169	128.39.200.255	HTTP	483	HTTP/1.1 200 OK (application/json)
336	2.138861	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1573 Ack=114407 Win=64512 Len=0
602	7.007701	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [FIN, ACK] Seq=114407 Ack=1573 Win=32512 Len=0
603	7.007777	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1573 Ack=114408 Win=64512 Len=0
609	7.273461	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [FIN, ACK] Seq=1573 Ack=114408 Win=64512 Len=0
611	7.287815	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [ACK] Seq=114408 Ack=1574 Win=32512 Len=0
> Frame 330: 608 bytes on wire (4864 bits), 608 bytes captured (4864 bits) on interface 0						
> Ethernet II, Src: LcfHeFe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)						
▼ Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169						
0100 .... = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 594						
Identification: 0x5529 (21801)						
> Flags: 0x4000, Don't fragment						
Time to live: 128						
Protocol: TCP (6)						
Header checksum: 0x0000 [validation disabled]						
[Header checksum status: Unverified]						
Source: 128.39.200.255						
Destination: 85.165.93.169						
▼ Transmission Control Protocol, Src Port: 60104, Dst Port: 80, Seq: 1019, Ack: 113978, Len: 554						
Source Port: 60104						
Destination Port: 80						
[Stream index: 1]						
[TCP Segment Len: 554]						
Sequence number: 1019 (relative sequence number)						
[Next sequence number: 1573 (relative sequence number)]						
Acknowledgment number: 113978 (relative ack number)						
0101 .... = Header Length: 20 bytes (5)						
> Flags: 0x018 (PSH, ACK)						
Window size value: 254						
[Calculated window size: 65024]						
[Window size scaling factor: 256]						
Checksum: 0xeb9 [unverified]						
[Checksum Status: Unverified]						
Urgent pointer: 0						
> [SEQ/ACK analysis]						
> [Timestamps]						
TCP payload (554 bytes)						
▼ Hypertext Transfer Protocol						
> GET /api/delta/fan/status HTTP/1.1\r\n						
Host: fanctrl.andersenitc.no\r\n						
Connection: keep-alive\r\n						
Accept: application/json, text/plain, */*\r\n						
DateX: Mon, 26 Nov 2018 07:55:58 GMT\r\n						
Authorization: None\r\n						
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36\r\n						
Referer: http://fanctrl.andersenitc.no\r\n						
Accept-Encoding: gzip, deflate\r\n						
Accept-Language: nb,en-US;q=0.9,en;q=0.8\r\n						
Cookie: _ga=GA1.2.870541523.1517819979; _biz_uid=cd6799c7fb3a4913b32c5dc59832da5d; _biz_nA=3; _biz_pendingA=%5B%5D\r\n						
Cookie pair: _ga=GA1.2.870541523.1517819979						
Cookie pair: _biz_uid=cd6799c7fb3a4913b32c5dc59832da5d						
Cookie pair: _biz_nA=3						
Cookie pair: _biz_pendingA=%5B%5D						
\r\n						



## DAT204 Exam h2018

Datakommunikasjon (Universitetet i Agder)



Skann for å åpne på Studocu

**DAT204-G, general information**

**Emnekode:** DAT204

**Emnenavn:** Datakommunikasjon

**Dato:** 19.12.2018

**Varighet:** 3 timer

**Tillatte hjelpeemidler:** Kalkulator

**Merknader:** Eksamens er både på engelsk og norsk (med noen overskrifter og uttrykk på engelsk).

Hver korrekt besvart oppgave gir fra 2 til 16 poeng, totalt 100 poeng. For hver del av en oppgave:

- Korrekt svar gir 0,25 - 2 poeng for hvert spørsmål, avhengig av vanskelighetsgrad.
- Feil svar gir 0 poeng for alle spørsmål, unntatt flersvarsoppgavene.
- Feil svar i flersvarsoppgavene gir en negativ poengsum, slik at klikker du på alle valgmulighetene i oppgaven vil summen bli 0 poeng. En negativ poengsum er ikke mulig.

Eksamens inneholder oppgaver av typen flervalg, flersvar, nedtrekks meny, fast tekst og beregning. Det finnes et åpent tekstfelt på den siste siden som kan brukes til å skrive ytterligere kommentarer og antagelser til oppgavene til eksamen. Dette tekstfeltet gir ingen poeng i seg selv, men det kan påvirke vurderingen av kommenterte oppgaver. Det er ikke nødvendig å bruke tekstfeltet, siden riktig svar på alle spørsmålene vil gi full score. Hvis spørsmålet ikke er riktig, kan du få flere poeng hvis du forklarer en delvis korrekt løsning eller gir en god antagelse i tekstfeltet.

---

Det forekommer av og til spørsmål om bruk av eksamensbesvarelser til undervisnings- og læringsformål. Universitetet trenger kandidatens tillatelse til at besvarelsen kan benyttes til dette. Besvarelsen vil være anonym.

**Tillater du at din eksamensbesvarelse blir brukt til slikt formål?**

- Ja  
 Nei

## 1 Wireshark HTTP

PDF-dokumentet viser to utdrag fra en Wireshark-fangst. Begge utdragene er fra den samme TCP forbindelsen og viser starten og slutten av en økt. Svar på følgende spørsmål: (16 poeng)

Hvilken linklagsprotokoll brukes her?  (DHCP, SSL, UDP, IEEE 802.11, ARP, Ethernet, HTTP, IP, TCP)

Hvilken protokoll er innkapslet i linklagsrammen?  (SMTP, ARP, IPv4, HTTP, UDP, TCP, SSL, Ethernet, IPv6, DHCP, IEEE 802.11)

Hvor stor er den annonserede vindustørrelsen i antall byte i pakken 129?  (67179, 257, 5155, 256, 438, 65792)

Hva slags vindu er dette?  (Metningsvindu ("congestion window"))

Vindustørrelsen på brukergrensesnittet, Mottakervindu, Glidende vindu i antall pakker)

Hvilken fase av en TCP forbindelse tilhører pakker 126 - 131?  (Forbindelse, Frakobling, Dataoverføring, Treveis håndtrykk, Lytt til nye forbindelser (LISTEN))

Hvilken applikasjonslagsprotokoll brukes her?  (DHCP, ARP, IPv4, HTTP, Ethernet, UDP, IPv6, TCP)

Hjem sender pakke 129?  (Serveren, Ingen, Klienten)

Hva er det velkjente portnummeret til servere som kjører applikasjonslagsprotokollen som benyttes her?

Hvilken type forbindelse bruker applikasjonslagsprotokollen?  (Tidsstyrt forbindelse, Vedvarende forbindelse, Ikke-vedvarende forbindelse, Engangs forbindelse)

Applikasjonslagsprotokollen i bruk her benytter informasjonskapsler ("cookies"). Men hva er en "cookie"?

(Det er en liste over tidligere åpnede nettsteder., Det er en liten tekstfil som er sendt fra et nettsted og lagret på klientens slutt-system., Det er en cache for tidligere nedlastede nettsideobjekter., Det er en fil som lagrer server autentiseringsdata.)

Er "cookie" informasjon utvekslet i pakke 129?  (Nei, Ja)

Hvor mange bytes med applikasjonsdata er sendt med pakke 129?

Hvor mange rutere kan pakken 129 passere før den blir forkastet?

Hjem initierer avslutning av denne TCP forbindelsen?  (Ingen, Klienten, Serveren)

Hvor mange bytes med applikasjonsdata har blitt overført i løpet av denne TCP sesjonen?

Klienten har sendt:

Serveren har sendt:

---

Maks poeng: 16

## 2 E-mail

Svar på spørsmålene nedenfor angående elektronisk post: (4 poeng)

```

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?

**Velg ett alternativ:**

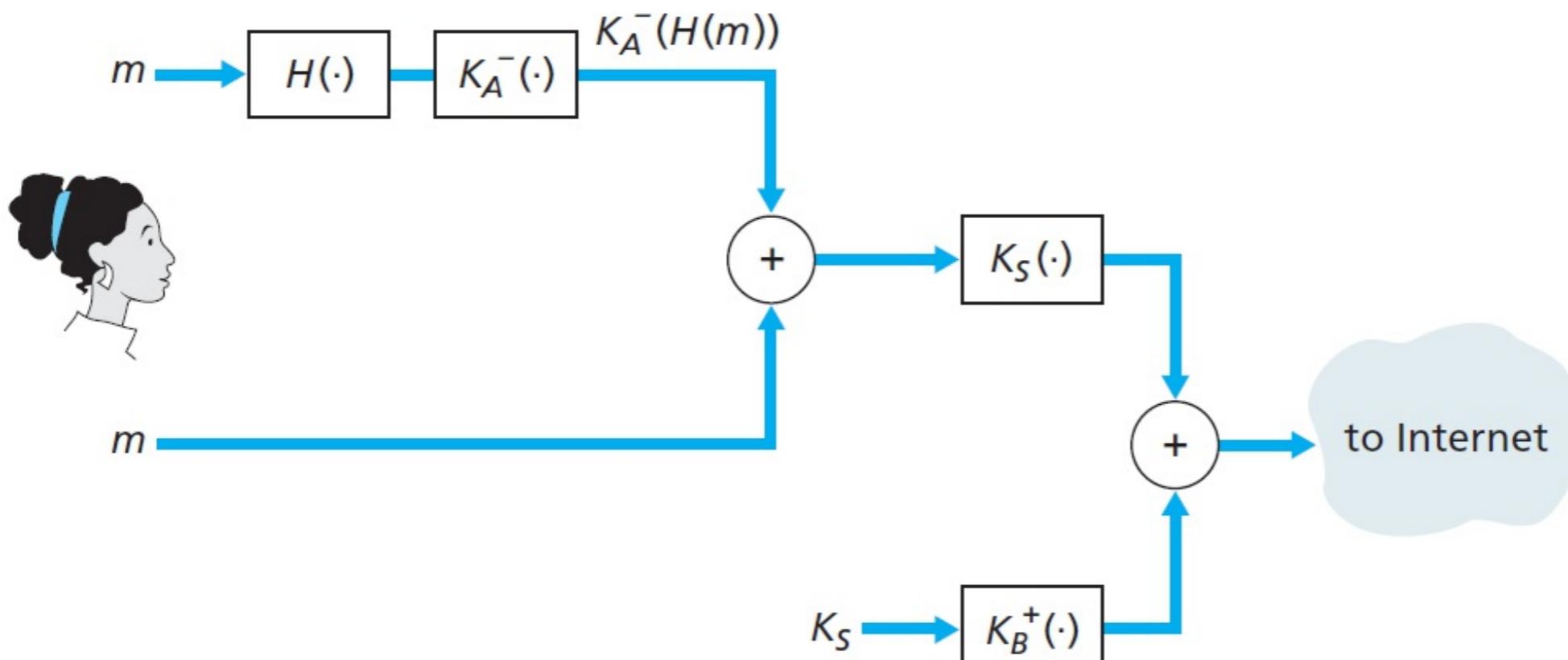
- SMTP
- HTML
- POP3
- IMAP
- HTTP

Hvilke av de følgende protokollene er definert som e-post tilgangsprotokoller?

**Velg ett eller flere alternativer:**

- HTTP
- POP3
- SNMP
- IMAP
- SMTP

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



**Velg ett alternativ:**

- MIME (Multipurpose Internet Mail Extension)
- DSA (Digital Signature Algorithm)
- RSA (Rivest, Shamir, Adelman)
- PGP (Pretty Good Privacy)
- TLS (Transport Layer Security)

---

Maks poeng: 4

### 3 DHCP

Nedenfor er noen uttalelser om DHCP og hvordan den fungerer. (3 poeng)

**Velg riktige alternativer:**

- DHCP gir IP-adresser til TLD DNS-servere.
- DHCP gir LAN nettverksmaske.
- DHCP gir IP-adresser til root DNS servere.
- DHCP gir IP-adresse til nærmeste svitsj.
- DHCP gir IP-adresser til lokale DNS servere.
- DHCP gir ISP nettverksmaske.
- DHCP er en applikasjonslagsprotokoll.
- DHCP gir IP-adresse til gateway (nærmeste ruter).
- DHCP er en nettverkslagprotokoll.
- DHCP tillater en vert å skaffe en IP-adresse automatisk.
- DHCP tillater en vert å skaffe en MAC-adresse automatisk.
- DHCP er en klient-server protokoll

---

Maks poeng: 3

#### 4 TCP/UDP sockets

Hvilken påstand om TCP versus UDP sockets er riktig? (3 poeng)

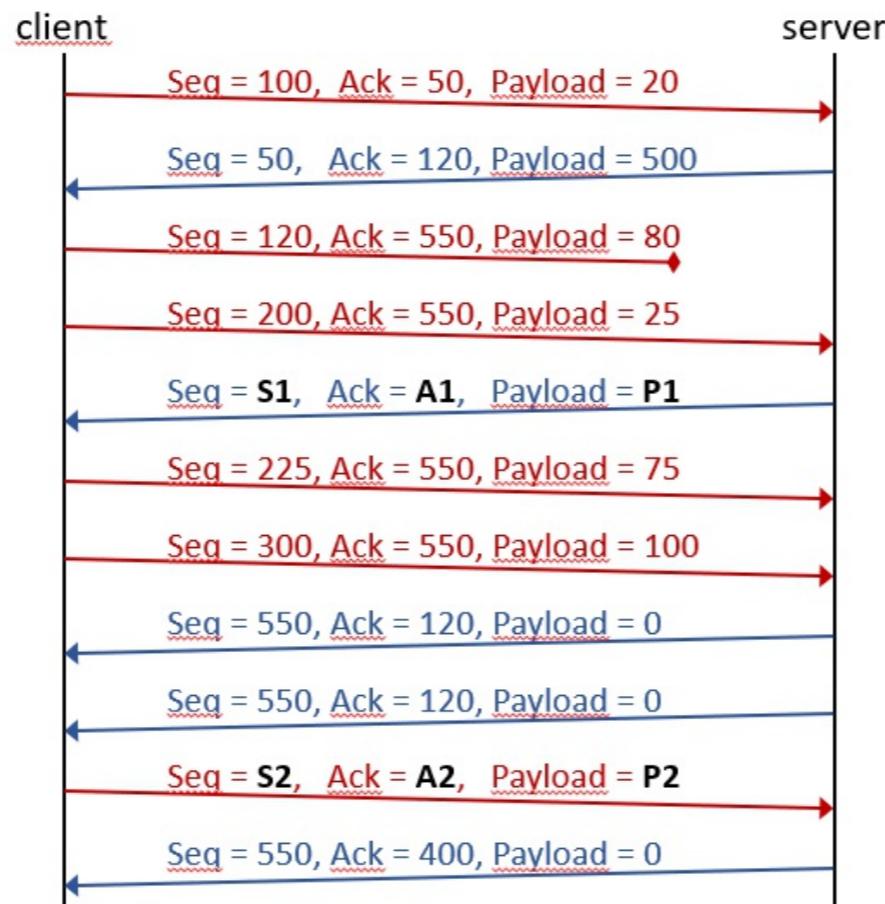
**Velg ett alternativ:**

- En UDP socket er identifisert ved hjelp av sender og mottakers IP-adresser samt sender og mottakers port nummer.
- TCP trafikk fra forskjellige klienter til den samme applikasjonen bruker en felles socket fra forbindelsen blir satt opp til den tas ned og skiller mellom sender og mottaker IP-adresse samt sender og mottaker port nummer.
- TCP bruker to sockets for å opprette en forbindelse, en som mottar oppkoblings forespørsler og en for datautveksling.
- En UDP socket er identifisert ved hjelp av senderens port og IP-adresse.

---

Maks poeng: 3

## 5 TCP sequence



Ovenfor er et utdrag av en TCP (Reno versjon) overføring. Hva vil sekvensnummeret, bekreftelsesnummeret og nyttelastlengden benevnt **S1**, **A1**, **P1**, **S2**, **A2** og **P2** være i segmentene vist på figuren? (6 poeng)

S1=  A1=  P1=   
 S2=  A2=  P2=

Den tredje meldingen går tapt et sted i nettverket på sin vei til serveren. Hvordan sikrer TCP at denne meldingen blir levert som vist i utdraget over?

(Det er opp til applikasjonslaget å sende den tapte meldingen på nytt., Meldingen sendes på nytt ved tidsavbrudd., Meldingen sendes på nytt etter å ha mottatt trippel duplikat ACK., Linklaget vil sikre pålitelig dataoverføring i dette tilfellet.)

TCP har også en re-transmisjonstimer. Hva skjer når denne timeren utløper?

(Ved tidsavbrudd tas forbindelsen ned., Ved tidsavbrudd sendes kun det segmentet som forårsaket tidsavbruddet på nytt., Ved tidsavbrudd sendes alle ubekrefteede segmenter på nytt.)

Maks poeng: 6

## 6 TCP and UDP statements

Hvilke av påstandene angående TCP og UDP er riktige? (4 poeng)

**Velg ett eller flere alternativer:**

- UDP flytkontroll sikrer at mottakeren ikke oversvømmes.
- UDP tilbyr kun en upålitelig dataoverføringstjeneste over et upålitelig internett.
- For en TCP forbindelse kan antallet ubekrefte bytes ikke være større enn mottakerens annonerte vindusstørrelse.
- TCP header parameter "Window size" er del av TCP metningskontroll algoritme.
- UDP segmenter med feil sjekk sum blir forkastet og sendt på nytt når rundturtiden (RTT) er utløpt.
- TCP har ingen flytkontroll mekanisme.
- TCP tilbyr en pålitelig dataoverføringstjeneste over et upålitelig internett.
- Når UDP brukes, må eventuell feilkorreksjon gjøres i applikasjonen.

---

Maks poeng: 4

## 7 TCP congestion handling

Nedenfor er noen påstander om hvordan TCP protokollen fungerer. Velg riktig påstand. (2 poeng)

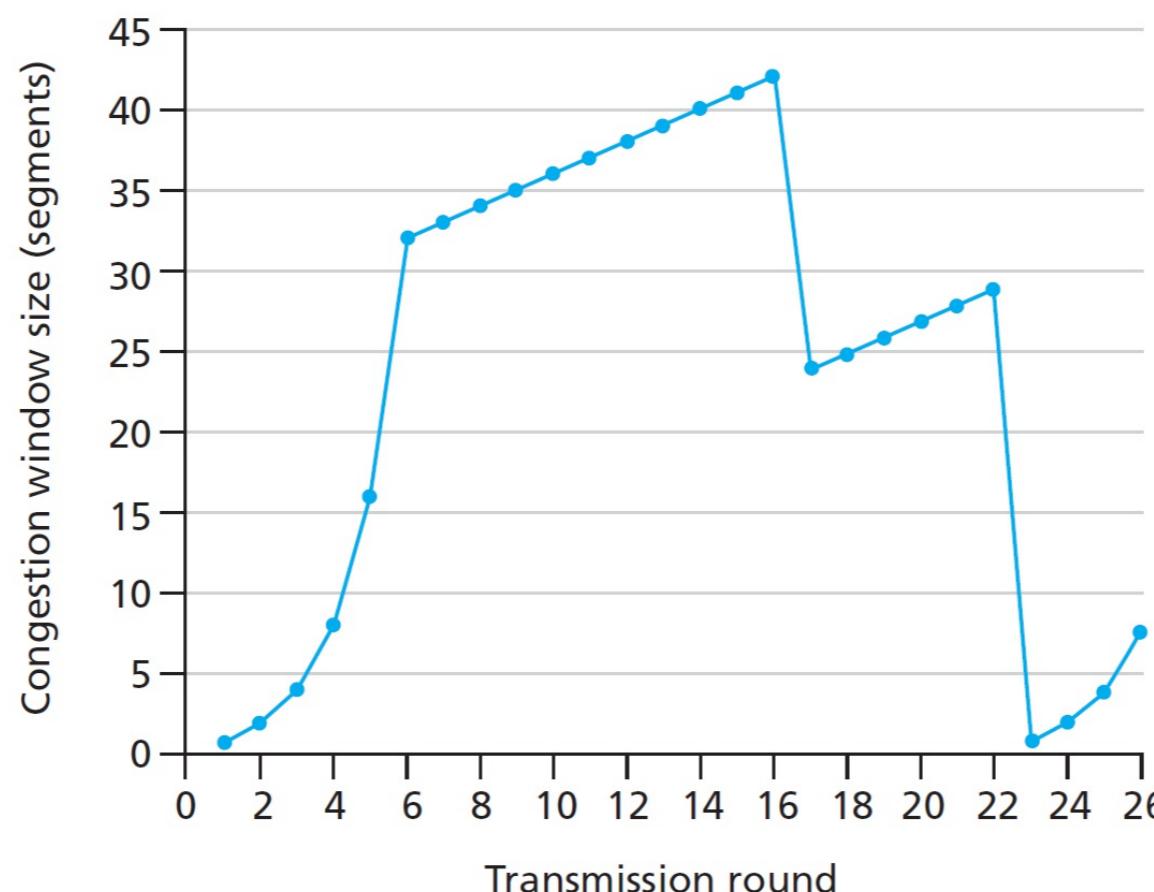
**Velg ett alternativ:**

- "Congestion avoidance" er betegnelsen på fasen i en TCP overføring der metningsvinduet (congestion window) øker lineært.
- "Fast recovery" er betegnelsen på fasen i en TCP overføring der metningsvinduet (congestion window) øker eksponensielt raskt.
- "Congestion avoidance" er relatert til "Receive window" i TCP headeren.
- TCP tidsavbrudd trigger "fast recovery".

---

Maks poeng: 2

## 8 TCP congestion window



Figuren viser størrelsen på TCP Reno sitt metnings vindu (congestion window) i antall segmenter som en funksjon av overføringsrunden. Svar på følgende spørsmål: (5 poeng)

Identifiser et intervall der TCP slow start fungerer.  ([17,22], [1,6], [16,17], [22,23], [6,16])

Hvordan er segmenttap identifisert etter den 16. overføringsrunden?

(Trippel duplikat ACK, Explicit Congestion Notification (ECN), RM celle med Congestion Indication (CI), Tidsavbrudd på ACK)

Hvordan er segmenttap identifisert etter den 22. overføringsrunden?

(Trippel duplikat ACK, RM celle med Congestion Indication (CI), Explicit Congestion Notification (ECN), Tidsavbrudd på ACK)

Hva er slow-start terskelen ved den 24. overføringsrunden?

Anta at Maximum Segment Size (MSS) er 1460 bytes og rundturtiden RTT=200 millisekunder, hva er

gjennomsnittlig båndbredde i Mbit/s benyttet av TCP forbindelsen i overføringsintervallet [6,16]?

Maks poeng: 5

## 9 Binary to IP

IP-adressen 01101001.00010000.01010000.10101011 kan skrives på punktum desimalform som: (2 poeng)

.  .  .

Maks poeng: 2

**10 IP and subnet**

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)

**Hva er prefiksene (på formatet a.b.c.d/x) for de åtte subnettene i stigende rekkefølge?**

Subnett 1: 105.16.  .  /

Subnett 2: 105.16.  .  /

Subnett 3: 105.16.  .  /

Subnett 4: 105.16.  .  /

Subnett 5: 105.16.  .  /

Subnett 6: 105.16.  .  /

Subnett 7: 105.16.  .  /

Subnett 8: 105.16.  .  /

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

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

---

Maks poeng: 6.5

**11 Routers and SDN**

I de senere årene, har Software-Defined Networking (SDN) fått økende interesse. Nedenfor er noen uttalelser angående tradisjonelle rutere og SDN. (3 poeng)

**Velg riktige alternativer:**

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

---

Maks poeng: 3

## 12 Routing tables

I denne oppgaven er målet å bestemme den riktige videresendingslinken gitt ruting tabellen nedenfor. (5 poeng)

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

**På hvilken link vil de bli videresendt?**

- A: link
- B: link
- C: link
- D: link
- E: link

---

Maks poeng: 5

## 13 Routing protocols

Nedenfor er noen spørsmål om klasser av ruting protokoller og hvordan de opererer. Fyll inn riktig uttrykk i setningene under og svar på spørsmålene: (4,5 poeng)

Dijkstra's korteste vei algoritme er mye brukt med  (distance-vector (DV), traffic-control (TC), link-utilization (LU), link-state (LS)) ruting protokoller. Hvilke utsagn passer til en ruter som kjører denne klassen av ruting protokoller?

**Velg ett eller flere alternativer:**

- Ruteren kjenner bare fysisk tilkoblede naboer.
- Ruteren kan kjøre OSPF.
- Ruteren kan kjøre RIP.
- Ruteren er avhengig av at direkte tilknyttede naboer annonserer sine vektortabeller for å kunne oppdatere sin egen rutingtabell.
- Ruteren kjenner kun avstand til fysisk tilkoblede naboer.
- Ruteren har fullstendig informasjon om alle link kostnader innenfor sitt autonome system.
- Ruteren har fullstendig informasjon om alle link kostnader i hele Internettet.
- Ruteren har fullstendig topologi over alle andre rutere i hele Internettet.
- Ruteren har fullstendig topologi over alle andre rutere innenfor sitt autonome system.

Bellman-Ford ligningen er mye brukt med  (distance-vector (DV), link-state (LS), link-utilization (LU), traffic-control (TC)) ruting protokoller. Hvilke utsagn passer til en ruter som kjører denne klassen av ruting protokoller?

**Velg ett eller flere alternativer:**

- Ruteren har fullstendig topologi over alle andre rutere i hele Internettet
- Ruteren har fullstendig topologi over alle andre rutere innenfor sitt autonome system.
- Ruteren kjenner bare fysisk tilkoblede naboer.
- Ruteren kan kjøre RIP.
- Ruteren kan kjøre OSPF.
- Ruteren er avhengig av at direkte tilknyttede naboer annonserer sine vektortabeller for å kunne oppdatere sin egen rutingtabell.
- Ruteren kjenner kun avstand til fysisk tilkoblede naboer.
- Ruteren har fullstendig informasjon om alle link kostnader innenfor sitt autonome system.
- Ruteren har fullstendig informasjon om alle link kostnader i hele Internettet.

---

Maks poeng: 4.5

## 14 Link layer

Nedenfor er noen generelle uttalelser om hvordan linkaget fungerer. Velg riktig alternativer. (3 poeng)

**Velg ett eller flere alternativer:**

- Linkaget utfører innramming av datagramer.
- Linkaget er det stedet i protokollstakken hvor software møter hardware.
- Linkaget kan ikke tilby noen form for pålitelig dataoverføring.
- Linkaget er kun implementert i hardware.
- Linkaget utfører feildeteksjon.
- Linkaget er implementert kun i software.

---

Maks poeng: 3

## 15 ARP

```

> 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: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)
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
  ▼ 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

0000 ff ff ff ff ff 3c a8 2a dd a3 00 08 06 00 01 .....< *.
0010 08 00 06 04 00 01 3c a8 2a dd a3 00 80 27 c8 71 .....< *....'q
0020 00 00 00 00 00 00 80 27 c8 a5 00 00 00 00 00 00 .....'.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....'.

```

Se gjennom Wireshark-fangsten ovenfor og vurder påstandene nedenfor angående Address Resolution Protocol (ARP). (3 poeng)

**Velg ett eller flere alternativer:**

- ARP er en protokoll som ligger et sted mellom nettverkslaget og linklaget i Internett protokollstakken.
- Verter og rutere bruker ARP til å knytte en IP-adresse til en MAC-adresse og vedlikeholde en ARP-tabell i sitt minne.
- ARP svar bruker alltid kringkastingsadressen som destinasjons adresse.
- Vert med IP-adresse 128.39.200.113 har MAC-adresse 3c:a8:2a:dd:a3:00.
- ARP forespørslar ender opp hos en DHCP server som tilordner en MAC-adresse til den spørrende verten.
- ARP kringkastingsadresse er 00:00:00:00:00:00.

Maks poeng: 3

## 16 Ethernet LAN

Ethernet er den mest brukte teknologien for kablede Local Area Network (LAN). Svar på følgende spørsmål: (3 poeng)

Hvilke IEEE standarder spesifiserer kablet Ethernet?  (802.5, 802.11, 802.13, 802.3)

Hvilken kablet LAN topologi er den aller mest vanligste i dag?

(Buss med alle noder i samme kollisjons-domene.,

Stjerne med punkt-til-punkt linker og svitsj i midten., Ring med token passering.)

Hvilken kabel type er mest vanlig i LAN i dag?  (To-parkabel, Fiberoptisk kabel, T-vunnet

parkabel, Koaksialkabel).

---

Maks poeng: 3

## 17 Ethernet switch

Hvilke av de følgende utsagn om Ethernet svitsjer er riktige? (3 poeng)

**Velg ett eller flere alternativer:**

- Svitsjer videresender rammer basert på destinasjonens MAC-adresse.
- Svitsjer er enkle, raske og relativt billige.
- Svitsjer videresender rammer basert på destinasjonens IP-adresse.
- Svitsjer må få sine svitsjetabeller konfigurert av nettverksadministrator.
- Svitsjer må vedlikeholde sine svitsjetabeller på egenhånd.
- Svitsjer er komplekse, raske og ganske kostbare.

---

Maks poeng: 3

**18 Wireless concepts**

Nedenfor er noen generelle utsagn om trådløs overføring, samt noen mer konkrete utsagn om hvordan IEEE 802.11 trådløse LAN fungerer. (6 poeng)

**Fyll inn det korrekte uttrykket i hver setning:**

I  (ad-hoc modus, rate tilpasning, signal svekking (path loss), interferens, flerveisinterferens (multipath propagation), infrastrukturmodus, beacon rammer) er hver trådløs vert tilkoblet Internettet via et tilgangspunkt (aksesspunkt).

I  (flerveisinterferens (multipath propagation), interferens, signal svekking (path loss), beacon rammer, infrastrukturmodus, rate tilpasning, ad-hoc modus) må de trådløse vertene selv sørge for ruting, tildeling av adresser og DNS.

Trådløse stasjoner oppdager og identifiserer tilgangspunktet (aksesspunktet) ved hjelp av

 (signal svekking (path loss), flerveisinterferens (multipath propagation), ad-hoc modus, beacon rammer, rate tilpasning, interferens, infrastrukturmodus).

Demping av det trådløse signalet når det forplanter seg gjennom materie kalles

 (signal svekking (path loss), infrastrukturmodus, interferens, ad-hoc modus, rate tilpasning, beacon rammer, flerveisinterferens (multipath propagation)).

Når to eller flere kilder innenfor et "basic service set" (BSS) sender samtidig på den samme frekvensen så kan

 (infrastrukturmodus, signal svekking (path loss), ad-hoc modus, flerveisinterferens (multipath propagation), beacon rammer, rate tilpasning, interferens) oppstå.

Utflyting i mottatt signal på grunn av flere refleksjoner av den elektromagnetiske bølgen fra objekter og bakken kalles

 (interferens, signal svekking (path loss), rate tilpasning, beacon rammer, flerveisinterferens (multipath propagation), infrastrukturmodus, ad-hoc modus).

---

Maks poeng: 6

**19 SSL nonces**

Hva er hensikten med med nonces i SSL/TLS? (2 poeng)

**Velg ett alternativ:**

- Beskytte mot Denial-of-Service angrep
- Beskytte mot "replay" angrep
- Beskytte mot "man-in-the-middle" angrep
- Data autentisering
- Beskytte mot "known plaintext" angrep
- Beskytte mot "chosen plaintext" angrep

---

Maks poeng: 2

## 20 SSL certificate and cryptographic algorithms

Nedenfor er noen uttalelser angående digitale sertifikater og kryptografiske algoritmer som brukes av SSL sockets i typiske klient/server sesjoner. (7 poeng)

**Fyll inn det riktige uttrykket i hver setning:**

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

- (tillate lovlig sending av meldinger, autentisere serveren, autorisere klienten for kommunikasjon med serveren, skape signaturer for meldingene) og til å
- (kryptere master secret med CA offentlig nøkkel, kryptere master secret med serverens offentlige nøkkel, utveksle et signert avtrykk (hash value) av master secret, kryptere master secret med serverens private nøkkel).

SSL sockets vil typisk utveksle applikasjonsmeldinger kryptert med en

(symmetrisk-nøkkel blokk chiffer, offentlig-nøkkel chiffer, asymmetrisk-nøkkel blokk chiffer, kryptografisk avtrykk (hash) algoritme).  (MD5, RSA, AES, SHA) er et eksempel på en slik algoritme.

For å sikre at en melding ikke blir endret, vil SSL vanligvis bruke en  (symmetrisk-nøkkel blokk chiffer, asymmetrisk-nøkkel blokk chiffer, offentlig-nøkkel chiffer, kryptografisk hash algoritme) til å lage et avtrykk av meldingen.  (RSA, SHA, 3DES, AES) er et eksempel på en slik algoritme.

Ved å inkludere en autentiseringsnøkkel til avtrykket, blir en  (digital signature, Message Authentication Code (MAC), godkjenningskode, Certified Message Code (CMC)) laget og utvekslet sammen med den krypterte meldingen.

---

Maks poeng: 7

## 21 SSL statements

Nedenfor er noen påstander om SSL protokollen. Hva er riktig utsagn om SSL? (2 poeng)

**Velg ett alternativ:**

- SSL bruker alltid AES etter håndtrykksfasen.
- SSL forbindelser kobles ned ved å avslutte transportlagets tilkobling.
- SSL implementerer sekvensnummer i klartekst i SSL records.
- SSL forhandler chiffer suite i løpet av håndtrykksfasen.

---

Maks poeng: 2

## 22 SSL quality of service

Nedenfor er noen spørsmål om SSL sockets og tjenestekvaliteter: (7 poeng)

Hvilken socket type forbedrer Secure Socket Layer (SSL) med sikkerhetstjenester?

**Velg ett alternativ:**

- HTTP
- IPv6
- IPv4
- TCP
- UDP

Hva heter den oppdaterte, sikrere og i dag mest brukte versjonen av SSL protokollen?

**Velg ett alternativ:**

- Network Layer Security (NLS)
- Application Layer Security (ALS)
- Link Layer Security (LLS)
- Transport Layer Security (TLS)

Hvilke servicegarantier gir SSL sockets?

**Velg ett eller flere alternativer:**

- I rekkefølge data levering
- Avgrenset forsinkelse
- Server autentisering
- Garantert båndbredde
- Applikasjonsprogram troverdighet
- Data konfidensialitet
- Pålitelig data overføring
- Data integritet

---

Maks poeng: 7

## 23 Comments and assumptions

Her kan du skrive antagelser, avklaringer og kommentarer til svarene dine. Disse kommentarene gir ikke flere poeng i seg selv, men kan påvirke vurderingen av kommenterte oppgaver. (maks 500 ord)

**Skriv antagelser og kommentarer til oppgavene her:**

Format ▼ | **B** *I* U  $\times_2$   $\times^2$  |  $\frac{I}{x}$  |  $\frac{\Box}{\Box}$   $\frac{\Box}{\Box}$  |  $\leftarrow$   $\rightarrow$   $\circlearrowleft$  |  $\frac{1}{2} =$   $\frac{1}{2} \approx$  |  $\Omega$   $\frac{\Box}{\Box}$  |  $\frac{\Box}{\Box}$  |  $\Sigma$  |  $\frac{\Box}{\Box}$

---

Words: 0

---

Maks poeng: 0



## Question 1

Attached



## Start of session:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	128.39.200.255	85.165.93.169	TCP	66	60466 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.013867	85.165.93.169	128.39.200.255	TCP	66	80 → 60466 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=128
3	0.013990	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
4	0.014379	128.39.200.255	85.165.93.169	HTTP	454	GET / HTTP/1.1
5	0.027949	85.165.93.169	128.39.200.255	TCP	60	80 → 60466 [ACK] Seq=1 Ack=401 Win=30336 Len=0
6	0.029970	85.165.93.169	128.39.200.255	TCP	329	80 → 60466 [PSH, ACK] Seq=1 Ack=401 Win=30336 Len=275 [TCP segment of a reassembled PDU]
7	0.030895	85.165.93.169	128.39.200.255	TCP	659	80 → 60466 [PSH, ACK] Seq=276 Ack=401 Win=30336 Len=605 [TCP segment of a reassembled PDU]
8	0.030896	85.165.93.169	128.39.200.255	HTTP	467	HTTP/1.1 200 OK (text/html)
9	0.030957	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=401 Ack=1294 Win=64256 Len=0
10	0.074978	128.39.200.255	85.165.93.169	HTTP	428	GET /assets/delta-vod-webapp.css.gz HTTP/1.1
11	0.091886	85.165.93.169	128.39.200.255	TCP	1454	80 → 60466 [ACK] Seq=1294 Ack=775 Win=31360 Len=1400 [TCP segment of a reassembled PDU]

```

> Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: LcfcHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)
> Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x5a8b (23179)
> Flags: 0x4000, Don't fragment
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 128.39.200.255
  Destination: 85.165.93.169
> Transmission Control Protocol, Src Port: 60466, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 60466
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
  Window size value: 257
  [Calculated window size: 65792]
  [Window size scaling factor: 256]
  Checksum: 0xfc8f [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]

```

## End of session:

No.	Time	Source	Destination	Protocol	Length	Info
125	5.639047	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=4279 Ack=66750 Win=64512 Len=0
126	6.609348	128.39.200.255	85.165.93.169	HTTP	492	GET /api/delta/fan/status HTTP/1.1
127	6.625013	85.165.93.169	128.39.200.255	HTTP	483	HTTP/1.1 200 OK (application/json)
128	6.671326	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=4717 Ack=67179 Win=65792 Len=0
129	7.644949	128.39.200.255	85.165.93.169	HTTP	492	GET /api/delta/fan/status HTTP/1.1
130	7.660899	85.165.93.169	128.39.200.255	HTTP	483	HTTP/1.1 200 OK (application/json)
131	7.701551	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=5155 Ack=67608 Win=65280 Len=0
132	12.583914	85.165.93.169	128.39.200.255	TCP	60	80 → 60466 [FIN, ACK] Seq=67608 Ack=5155 Win=42112 Len=0
133	12.583989	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [ACK] Seq=5155 Ack=67609 Win=65280 Len=0
134	12.757137	128.39.200.255	85.165.93.169	TCP	54	60466 → 80 [FIN, ACK] Seq=5155 Ack=67609 Win=65280 Len=0
135	12.770847	85.165.93.169	128.39.200.255	TCP	60	80 → 60466 [ACK] Seq=67609 Ack=5156 Win=42112 Len=0

<	Frame 129: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0	>
> Ethernet II, Src: LcfcHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)		
▼ Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169		
0100 .... = Version: 4		
.... 0101 - Header Length: 20 bytes (5)		
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
Total Length: 478		
Identification: 0x5af5 (23285)		
> Flags: 0x4000, Don't fragment		
Time to live: 128		
Protocol: TCP (6)		
Header checksum: 0x0000 [validation disabled]		
[Header checksum status: Unverified]		
Source: 128.39.200.255		
Destination: 85.165.93.169		
▼ Transmission Control Protocol, Src Port: 60466, Dst Port: 80, Seq: 4717, Ack: 67179, Len: 438		
Source Port: 60466		
Destination Port: 80		
[Stream index: 0]		
[TCP Segment Len: 438]		
Sequence number: 4717 (relative sequence number)		
[Next sequence number: 5155 (relative sequence number)]		
Acknowledgment number: 67179 (relative ack number)		
0101 .... = Header Length: 20 bytes (5)		
> Flags: 0x018 (PSH, ACK)		
Window size value: 257		
[Calculated window size: 65792]		
[Window size scaling factor: 256]		
Checksum: 0xfe45 [unverified]		
[Checksum Status: Unverified]		
Urgent pointer: 0		
> [SEQ/ACK analysis]		
> [Timestamps]		
TCP payload (438 bytes)		
▼ Hypertext Transfer Protocol		
> GET /api/delta/fan/status HTTP/1.1\r\n		
Host: fanctrl.andersenitc.no\r\n		
Connection: keep-alive\r\n		
Accept: application/json, text/plain, */*\r\n		
DateX: Mon, 26 Nov 2018 08:22:35 GMT\r\n		
Authorization: None\r\n		
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36\r\n		
Referer: http://fanctrl.andersenitc.no/\r\n		
Accept-Encoding: gzip, deflate\r\n		
Accept-Language: nb,en-US;q=0.9,en;q=0.8\r\n\r\n		

## DAT204-G utsatt skoleeksamen 26.2.18

DAT204-G, general information

Subject code: DAT204

Subject name: Datakommunikasjon

Date: 26.02.2018

Duration: 3 hours

Permitted aids: Calculator

Comments. The exam is in English and each correctly answered assignment gives from 2 to 10 points, in total

100 points. For each part of an assignment

- Correct answer gives 0.5 – 2 points for each question, depending on difficulty
- Wrong answer gives 0 points for all questions except multiple-answer assignments
- Wrong answer for multiple-answer assignments gives a negative score so that clicking all options in an assignment sums up to 0 points. A negative score is not possible.

The exam contains a mix of multiple choice, multiple answer, pull-down menu, fixed-text and calculation

assignments. There is an open text field on the last page which may be used for writing additional comments and

assumptions to the assignments of the exam. This text field does not give any points in itself, but it may impact

the judgement of other assignments. It is not necessary to use the text field, since correct answer on all

questions will give full score. If the question is not correct, then you may get additional points if you explain  
a partially correct solution or good assumption in the text field.

There are also requests for using exam answers for educational and teaching purposes.  
The University  
needs the candidate's permission to use this. The answer will be anonymous.

Do you permit that your exam answer is used for such purposes?

Select one alternative

- Yes
  - No
- 

#### 1 Mail Access Protocols (Maks poeng: 2)

Which one(s) of the following protocols are defined as mail access protocols (I.e. IMAP4)?

Select one or more alternatives

- HTTP
- POP3
- Microsoft Outlook
- SMTP
- IMAP

#### 2 UDP sockets (Maks poeng: 2)

Below are some statements related to how UDP sockets work. Assume that this application communicates over

one well-known UDP port at the client side with another well-known UDP port at the server side (e.g. client at

port 67/UDP, server at port 68/UDP). Which statement is then true?

Select one alternative

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

different clients.

UDP traffic towards the same application in a server uses different sockets when the traffic comes from

different clients.

UDP traffic towards different applications in a server uses a common socket if the traffic comes from the

same client.

A UDP session socket is identified by the sender and receiver port and IP address.

### 3 HTTP protocol (Maks poeng: 2)

Below are some statements related to the behaviour of different types of HTTP connections. One of the following

statements is true, select the correct alternative.

Select one alternative

A user requests a Web page using HTTP GET that consists of a HTML page and three images. The web

client will then send one request message and receive four response messages from the server.

- The Date-header in the HTTP response message indicates when the object in the response was last modified.
- With non-persistent connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages.
- Several Web pages can be sent over the same persistent connection.

#### 4 Packet scheduling (Maks poeng: 2)

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?

Select one alternative

- Round Robin (RR)
- Weighted Fair Queueing
- Priority scheduling
- First In First Out (FIFO)

#### 5 HTTP GET request (Maks poeng: 2)

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?

Select one alternative

- 432
- 436
- 490
- 502

## 6 Application Layer Protocol (Maks poeng: 2)

Below is a list of protocols. Which one belongs to the application layer?

Select one alternative

- UDP
- ARP
- ICMP
- SMTP
- IPv6

## 7 UDP claims (Maks poeng: 2)

Below are some claims about how the UDP protocol works. Select the correct alternative.

Select one alternative

- UDP uses go-back-N so that many segments can be sent back to back before receiving an acknowledgement.
- UDP segments that are received with the wrong checksum are discarded and retransmitted on timeout by

the transport layer.

- When UDP is used, then any fault correction is up to the application.
- UDP segments with wrong sequence number are discarded.

#### 8 TCP congestion handling (Maks poeng: 2)

Below are some claims about how the TCP protocol works. Select the correct claim.

Select one alternative

- Congestion avoidance is related to the Receive window in the TCP header.
- Fast recovery denotes the phases in a TCP transmission where the congestion window increases exponentially fast.
- TCP timer expiry triggers fast recovery.
- Congestion avoidance denotes the phases in a TCP transmission where the congestion window increases linearly.

#### 9 TCP sequence (Maks poeng: 5)

Klient/client                    Tjener/server

Seq = 10, ACK = 20, payload = 30

Seq = a, ACK = b, payload = 50

Seq = 40, ACK = 70, payload = 60

Seq = 100, ACK = 70, payload = 10

Seq = c, ACK = d, payload = 20

Above is an excerpt from a TCP transmission. What will the sequence number and acknowledgement number

denoted a, b, c and d be in the segments shown in the figure?

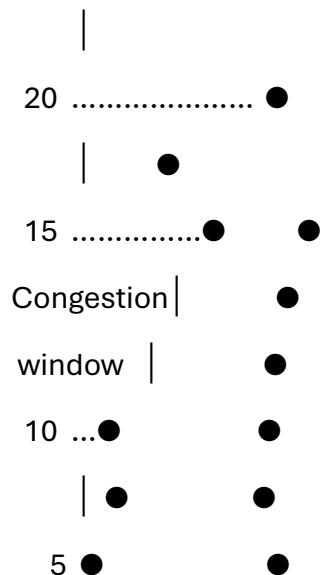
#### 10 TCP congestion window (Maks poeng: 5)

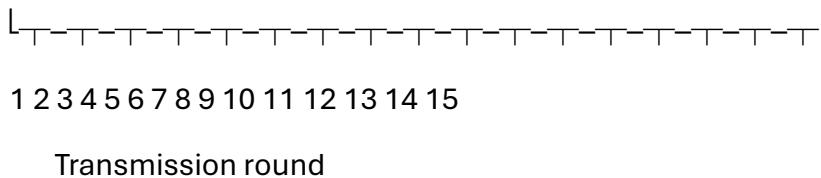
The third message is lost due to severe congestion in the network (both in forward and backward direction) which

lasts longer than EstimatedRTT + RxDevRTT. How does TCP ensure that this message is delivered?

- (Message is retransmitted on timeout.)
- (Message is retransmitted after receiving triple duplicate ACK.)
- (Link layer will ensure reliable data transfer in this case.)
- (Message is dropped, it is up to the application layer to retransmit it.)

#### TCP Congestion Window





The figure shows the size of TCP Reno's congestion window in number of segments as a function of

transmission round. Answer the following questions (5 points).

- Identify an interval where slow-start is operating

([1,5], [12,13], [9,10], [5,9])

- How is segment loss identified in transmission round 10?

(Timeout on ACK, Explicit Congestion Notification (ECN), RM cell w/ Congestion indication (CI),

Triple duplicate ACK)

- How is segment loss identified in transmission round 13?

(RM cell w/ CI, Triple duplicate ACK, Timeout on ACK, ECN)

- After segment loss is detected in transmission round 13, what is the slow-start threshold set to?

- Assuming the Maximum Segment Size (MSS) is 1460 bytes and the round-trip time RTT = 200 ms, what is

the average bandwidth in Mbit/s the TCP connection uses in transmission rounds [5,9]?

11 Select protocol (Maks poeng: 2)

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?

Select one alternative

- IEEE 802.11
- ARP
- DNS
- IP
- ICMP

12 IP Address Assignment (Maks poeng: 2)

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

Select one alternative

- DNS
- ARP
- BGP
- DHCP
- NAT

13 Routing standards (Maks poeng: 2)

What is the de-facto standard for inter-AS routing?

Select one alternative

- The Distance-Vector Algorithm (DV)
- BGP – Border Gateway Protocol
- The Link-State Algorithm (LS)
- OSPF – Open Shortest Path First
- RIP – Routing Information Protocol

14 TCP/IP router layers (Maks poeng: 2)

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?

Select one or more alternatives

- Application layer
- Transport layer
- Network layer
- Link layer
- Physical layer

15 Wireshark IPv4 vs IPv6 (Maks poeng: 2)

The Wireshark log in the figure illustrates:

Select one alternative

- IPv4 tunneling in IPv6
- Transition from IPv4 to IPv6
- IPv6 tunneling in IPv4
- A construction scenario that is not permitted
- IPv6 traffic

16 Binary to IP (Maks poeng: 2)

The IP address 00111000.11010010.10010101.10010000 can be written on dotted-decimal form as \_\_?

17 IP og subnetting (Maks poeng: 6)

Suppose an ISP owns the block of addresses of the form 104.16.58.0/23. Suppose it wants to create four subnets

from this block, with each block having the same number of IP addresses.

What are the prefixes (of the form a.b.c.d/x) for the four subnets in increasing order?

Subnet 1: 104.16.\_\_\_

Subnet 2: 104.16.\_\_\_

Subnet 3: 104.16.\_\_\_

Subnet 4: 104.16.\_\_\_

18 Routing tables (Maks poeng: 5)

In this assignment, the objective is to determine the correct forwarding link given the routing table below.

A router has the following routes in its forwarding table

00001010.10101000.00000100.00000000/22 → link 1

00001010.10101000.00000110.00000000/23 → link 2

00001010.10101000.00000111.00000000/24 → link 3

00001010.10101000.00000000.00000000/16 → link 4

All other addresses link 5

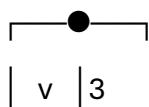
Assume the router receives datagrams destined to the following addresses and decide which link they are

forwarded to. On which link will they be forwarded?

- A. 00001010.10101000.00000111.00000001 → link \_\_\_\_\_
  - B. 00001010.10101000.00000110.10000000 → link \_\_\_\_\_
  - C. 00001010.10101000.00000101.00000000 → link \_\_\_\_\_
  - D. 00001010.10101000.00000100.00000001 → link \_\_\_\_\_
  - E. 00001010.10101000.00000111.11111110 → link \_\_\_\_\_

## 19 Link-state algorithm (Maks poeng: 10)

5





u 3 w 1 z

| |3

4 ●—● 4

x 1 y

Run Dijkstra's link-state algorithm on the network of routers shown in the figure.

Step	N	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	{u}					
1						
2						
3						
4						

### Notation

N contains the visited nodes, listed in the order they are visited

D(x) is the distance to node x

p(x) is the previous node along this distance

Use the following 3-character notation for D(x),p(x): integer,letter, e.g. 4,x

If the graph is not reachable, use inf for D(x),p(x)

Below are some general statements about how the link layer works. Select the correct alternative(s).

- The link layer is the place in the protocol stack where software meets hardware.
- The link layer is implemented only in software.
- The link layer is implemented only in hardware.
- The link layer performs error detection.
- The link layer cannot offer any form of reliable delivery.

## 21 Link utilisation (Maks poeng: 4)

Consider an intercontinental fibre link between two hosts, where the round-trip delay between these two end

systems, RTT, is 200 ms. Suppose that the size of a packet is 6 000 bytes (including both header fields and data), and that the transmission rate is 100 Mbit/s.

- What is the transmission delay in microseconds?
- How big would the window size have to be (in number of packets) for the channel utilisation to be greater than 98 %? Round up your answer.

## 22 Transmission and Propagation delay (Maks poeng: 8)

A gamer in Kviteseid is connected to a Massive Multiplayer Online (MMO) server in Oslo.  
The link distance from

Kviteseid to Oslo is 200 km, and the propagation speed in the medium is 200 000 km/s. The gamer has a

10 Mbit/s Internet connection, and all intermediate routers have low load and negligible transmission delay.

The game exchanges 184-byte game-state messages over TCP between clients and the server. Assume that the

TCP overhead is 20 bytes, the IP overhead is 20 bytes and the link layer overhead (Ethernet) is 26 bytes, and

that each game message is sent in separate TCP packets to increase interactivity.

- What is the length of the link layer frame in bits?
- How large is the transmission delay in ms in this scenario?
- How large is the propagation delay in ms in this scenario?
- What is the minimum round-trip-time (RTT) in ms for the game?

## 23 Self-learning switches (Maks poeng: 6)

[Figure with four switches S1–S4 and hosts A–I]

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.

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 S4 be after this sequence?

Switch table for S4

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

Which hosts receive the last frame?

- Only B
- A and B
- A and C and B
- All except sender

24 SSL Quality of Service (Maks poeng: 2)

Which service guarantees does SSL give?

Select correct answer(s)

- Data confidentiality

- Guaranteed bandwidth
- Server authentication
- Bounded delay
- Data integrity

#### 25 SSL certificate (Maks poeng: 2)

What is the digital certificate used for in the TLS/SSL protocol?

Select one or more alternatives

- Authenticate the server
- Create a signature for SSL messages
- Authorise the client to communicate with the server
- Use public key to encrypt master secret
- Licence for legal sending of SSL messages

#### 26 SSL statements (Maks poeng: 2)

Below are some clauses about the SSL protocol. What is the correct statement about SSL?

Select one alternative

- SSL connections are closed by terminating the TCP connection.
- SSL always uses AES after the handshake phase.
- SSL implements sequence numbers in clear-text in the SSL record.
- SSL allows agreeing on cryptographic algorithms during the handshake phase.

27 SSL nonces (Maks poeng: 2)

What is the purpose of nonces in SSL/TLS?

Select one alternative

- Data authentication
- Protect against chosen plaintext attacks
- Protect against known plaintext attacks
- Protect against replay attacks
- Protect against Denial of Service attacks
- Protect against man-in-the-middle attacks

28 SSL/TLS master secret encryption (Maks poeng: 2)

For SSL/TLS, how can the client securely send the master secret (MS) to the server?

Select one alternative

- Encrypt the MS with the common session key
- Use the signed hash value of MS as key
- Encrypt the MS with the public key of the server
- Encrypt the MS with the private key of the server

29 Wireshark SSL (Maks poeng: 11)

[Wireshark capture excerpt]

The figure above shows a TCP sequence from Wireshark. Answer the following questions:

- Which link layer protocol is used here? (DHCP, Ethernet, ARP, IP, HTTP, IEEE 802.11)
- Which protocol is encapsulated in the link layer frame? (IP, DHCP, ARP, SMTP, Ethernet, SSL, UDP, HTTP, TCP, IEEE 802.11)
- Packet 1821 shows “Win=151168”. What type of window is this?  
(Sliding window in number of packets, Window size of the user interface, Congestion window, Receiver window)
- Which phase of a TCP connection do packets 3412-3446 belong to?  
(Data transfer, Three-way handshake, Disconnection, Connection, Listen for new connections (LISTEN))
- Who sends packet 1815? (Client, None, Server, Do not know)
- How many bytes payload are sent in segment 1815? \_\_\_\_\_
- How many bytes data are sent in the current SSL record? \_\_\_\_\_
- How many bytes payload have been sent (from client to server) and received in total from the start of the session until inclusive packet 3433?  
Sent: \_\_\_\_\_  
Received: \_\_\_\_\_
- Which application layer protocol(s) are used here? Select any that apply  
 TCP    TLS    Frame    HTTP    IPv4    Ethernet

Please fill in comments and assumptions for the multiple choice part here. These comments do not give any points on their own, but may impact the evaluation of these questions.

Write your comments here.

---



## DAT204 Exam h2017

Datakommunikasjon (Universitetet i Agder)



Skann for å åpne på Studocu

## DAT204-G, general information

**Subject code:** DAT204

**Subject name:** Datakommunikasjon

**Date:** 6. 12. 2017

**Duration:** 3 timer

**Permitted aids:** Calculator

**Comments:** The exam is in English and each question gives from 1 to 2 points per correct answer, in total 100 points. Wrong answer gives 0 points for all assignments except multiple answer assignments, which give a negative score for wrong answers and a lowest threshold of 0 points per assignment. A negative score is not possible for multiple answer assignments. Some assignments contain several questions. The exam contains a mix of multiple choice, multiple answer and calculation assignments. There is an open text field on the last page which may be used for writing additional comments and assumptions to the assignments of the exam. This text field does not give any points in itself, but it may impact the judgement of other assignments. It is not necessary to use the text field, since correct answer on all questions will give full score. If the question is not correct, then you may however get additional points if you explain a partially correct solution or good assumption in the text field.

---

There are sometimes requests for using exam answers for educational and teaching purposes. The University needs the candidate's permission to use this. The answer will be anonymous.

**Do you permit that your exam answer is used for such purposes?**

**Velg et alternativ**

Ja

Nei

## 1 Select protocol

Which of the following protocols run as a service on the application layer?  
(2 points)

**Select one alternative**

- DNS
- ARP
- IP
- IEEE 802.11
- ICMP

Maks poeng: 2

**2 UDP sockets**

Below are some statement related to how UDP sockets work. Which statement is true? (2 points)

**Select an alternative**

- UDP traffic towards different applications in a server uses a common socket if the traffic comes from the same client.
- A UDP session socket is identified by the sender and receiver port and IP address.
- UDP traffic towards the same application in a server uses different sockets when the traffic comes from different clients.
- UDP traffic towards the same application in a server uses a common socket even if the traffic comes from different clients.

Maks poeng: 2

**3 HTTP protocol**

Below are some statements related to the behaviour of different types of HTTP connections. One of the following statements is true, select the correct alternative. (2 points)

**Select one alternative.**

- With nonpersistent TCP connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages.
- The Date: header in the HTTP response message indicates when the object in the response was last modified.
- A user requests a Web page that consists of a HTML page and three images. The web client will then send one request message and receive four response messages.
- Two distinct Web pages can be sent over the same persistent connection.

Maks poeng: 2

**4 E-mail transfer**

Suppose Alice sends an e-mail to Bob using a Web-based e-mail account (for example Gmail). Bob reads email using his e-mail client (e.g. Outlook or Thunderbird), which uses a mail access protocol for presenting the e-mails that are stored on his e-mail server. This mail access protocol keeps e-mails and email folders on the server also after they have been downloaded. (3 points)

**List the three application layer protocols that are used to move the e-mail from Alice to Bob in the correct time sequence.**

Alice ->  (POP3, MIME, HTTP, IMAP, HTML, SMTP) ->   
(HTTP, SMTP, IMAP, MIME, POP3, HTML) ->  (SMTP, MIME, IMAP, HTTP, POP3, HTML) -> Bob

Maks poeng: 3

**5 TCP congestion handling**

Below are some claims about how the TCP protocol works. Select the correct claim. (2 points)

**Select one alternative.**

- Congestion avoidance is related to the Receive window in the TCP header.
- TCP timer expiry triggers fast recovery.
- Fast recovery denotes the phases in a TCP transmission where the congestion window increases exponentially fast.
- Congestion avoidance denotes the phases in a TCP transmission where the congestion window increases linearly.

Maks poeng: 2

**6 TCP claims**

Below are some claims about how the congestion and flow control in TCP works. Select the correct alternative. (2 points)

**Select one alternative**

- The number of unacknowledged bytes can be larger than the receiver buffer (if the variable "Congestion Window" is larger than "Receive Window").
- TCP flow control ensures that the network is not being overloaded.
- The parameter "Receive Window" is a part of the TCP congestion control algorithm.
- For a TCP connection, the number of unacknowledged bytes can not be larger than the receiver buffer.

Maks poeng: 2

**7 UDP claims**

Below are some claims about how the UDP protocol works. Select the correct alternative. (2 points)

**Select one alternative**

- UDP segments that are received with the wrong checksum are discarded and retransmitted when the round-trip-time is expired.
- UDP uses selective repeat so that many segments can be sent back to back before receiving an acknowledgement.
- UDP segments with wrong sequence number are discarded.
- When UDP is used, then any fault correction is up to the application.

Maks poeng: 2

**8 TCP quality of service**

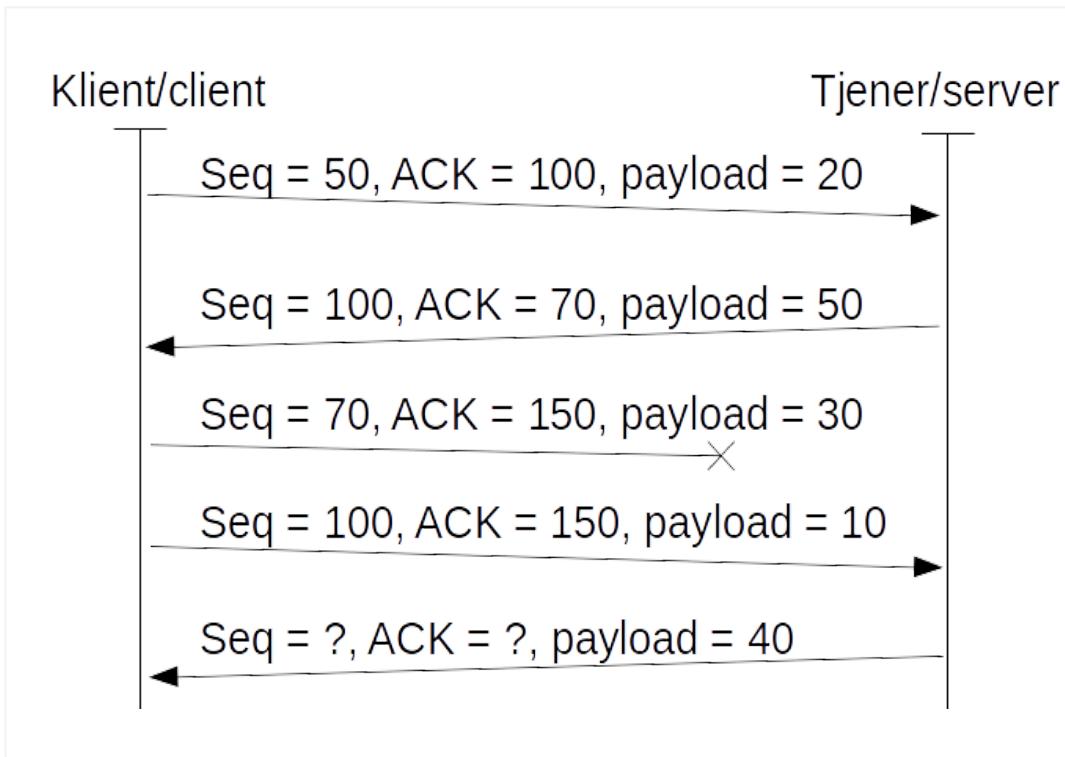
Which service quality guarantees does TCP give? (2 points)

**Select any that are correct.**

- Guaranteed bandwidth
- Bounded delay
- Server authentication
- In-order data delivery
- Data confidentiality
- Data integrity
- None of these
- Reliable data transfer

Maks poeng: 2

**9 TCP sequence**



Above is an excerpt from a TCP transmission. What will the next sequence number and acknowledgement number be in the last TCP segment? (3 points)

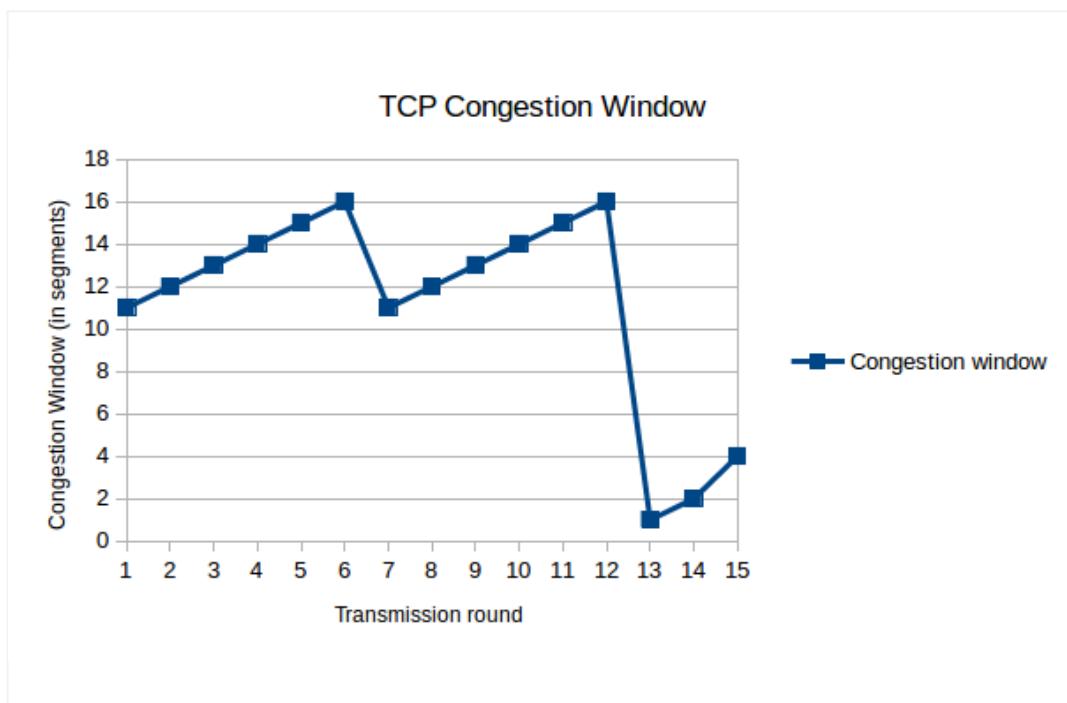
Seq=  ACK=

The third message is lost during transmission. How does TCP Reno ensure that this message is delivered?

(Message is retransmitted on timeout., Message is retransmitted after receiving triple duplicate ACK., Message is dropped, it is up to the application layer to retransmit it., The link layer will ensure reliable data transfer in this case.)

Maks poeng: 3

## 10 TCP Congestion Window



The figure shows the size of TCP Reno's congestion window in number of segments as a function of transmission round. Answer the following questions. (5 points)

Identify an interval where congestion avoidance is operating.

▼

([13,15], [12,13], [7,12], [6,7])

How is segment loss identified in transmission round 7?

▼ (Timeout on ACK, RM cell with

Congestion Indication (CI), Triple duplicate ACK, Explicit Congestion Notification (ECN))

How is segment loss identified in transmission round 13?

▼ (RM cell with Congestion

Indication (CI), Triple duplicate ACK, Timeout on ACK, Ecplicit Congestion Notification (ECN))

After segment loss is detected in transmission round 13, what is the slow-start threshold set to?

Assuming the Maximum Segment Size (MSS) is 1460 bytes and the round-trip-time RTT=135 ms, what is the average bandwidth in Mbits/s the TCP connection uses in transmission rounds [1,12]?

Maks poeng: 5

## 11 Routing standards

What is the de-facto standard for inter-AS routing? (2 points)

Select one

- The Link-State Algorithm (LS)
- The Distance-Vector Algorithm (DV)
- BGP - Border Gateway Protocol
- OSPF - Open Shortest Path First
- RIP - Routing Information Protocol

Maks poeng: 2

## 12 IP Address Assignment

How are IP addresses usually assigned to PCs that are connected to a network? (2 points)

Select one alternative

- ARP
- BGP
- DNS
- DHCP
- NAT

Maks poeng: 2

## 13 Packet scheduling

Which packet scheduling discipline ensures that a data flow gets a defined fraction (of arbitrary size) of the total bandwidth? (2 points)

**Select one alternative**

- Weighted Fair Queueing
- First In First Out (FIFO)
- Round Robin (RR)
- Priority scheduling

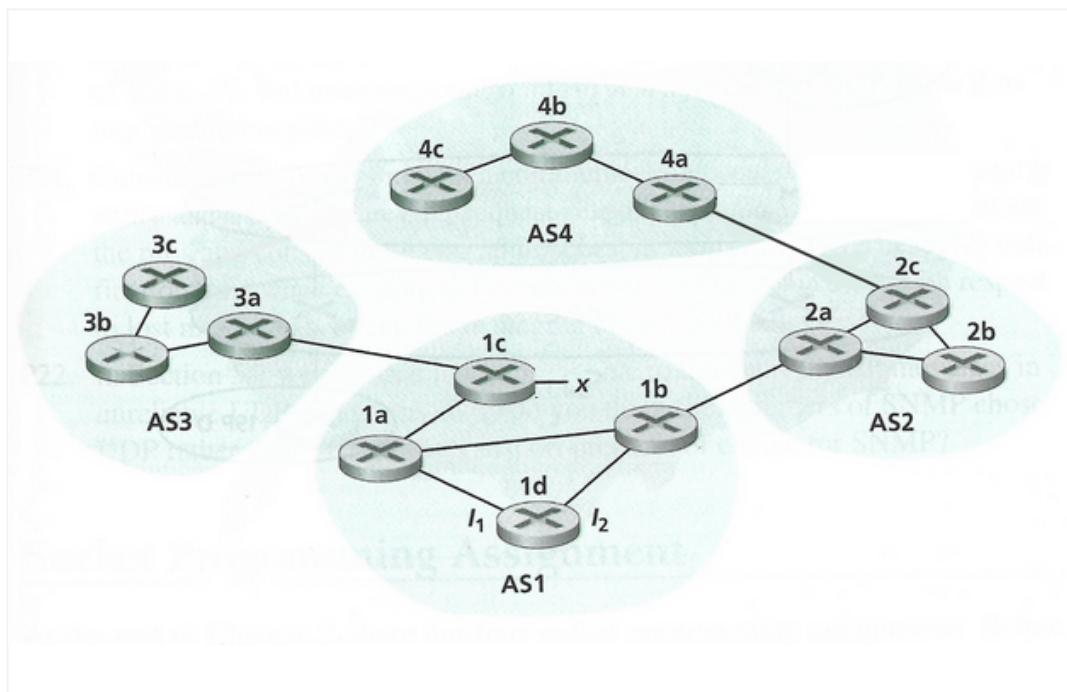
Maks poeng: 2

**14 Routing algorithms****Enter the routing algorithms that fit the expression (5 points).**

- ▼ (RIP, OSPF, IGMP, BGP)uses Dijkstra's algorithm to find the shortest path.
- ▼ (RIP, IGMP, OSPF, BGP)is dominated by routing policies instead of focusing on finding the path with lowest cost in the network.
- ▼ (BGP, OSPF, IGMP, RIP)exchanges information about changed routing tables with neighbour routers.
- ▼ (RIP, IGMP, OSPF, BGP)announces a subnet to all autonomous systems on the Internet.
- ▼ (BGP, IGMP, OSPF, RIP)exchanges information about neighbour routers with all routers in the network.

Maks poeng: 5

**15 AS Routing**



Consider the network shown above. Suppose AS1 and AS2 are running RIP as their intra-AS routing protocol. Suppose AS3 and AS4 are running OSPF as their intra-AS routing protocol. Suppose eBGP and iBGP are used as inter-AS routing protocol. (4 points)

**Select the correct protocol:**

a) Router 3a learns about prefix x from which routing protocol?

(RIP, OSPF, eBGP, iBGP)

b) Router 4b learns about prefix x from which routing protocol?

(RIP, OSPF, eBGP, iBGP)

c) Router 2b learns about prefix x from which routing protocol?

(RIP, OSPF, eBGP, iBGP)

d) Router 2a learns about prefix x from which routing protocol?

(RIP, OSPF, eBGP, iBGP)

Maks poeng: 4

## 16 Binary to IP

The IP address **10011000.01011010.01011110.00001001** can be written on dotted decimal form as: (2 points)

 .  .  . 

Maks poeng: 2

## 17 IP og subnetting

Suppose an ISP owns the block of addresses of the form 192.258.56.0/22. Suppose it wants to create four subnets from this block, with each block having the same number of IP addresses. (4 points)

**What are the prefixes (of the form a.b.c.d/x) for the four subnets?**

Subnet 1: 192.168.	<input type="text"/>	.0/	<input type="text"/>
Subnet 2: 192.168.	<input type="text"/>	.0/	<input type="text"/>
Subnet 3: 192.168.	<input type="text"/>	.0/	<input type="text"/>
Subnet 4: 192.168.	<input type="text"/>	.0/	<input type="text"/>

Maks poeng: 4

## 18 Routing tables

In this assignment, the objective is to determine the correct forwarding link given the routing table below (5 points).

A router has the following routes in its forwarding table:

00001010.10101000.00000100.00000000/22	link 1
00001010.10101000.00000010.00000000/23	link 2
00001010.10101000.00000100.00000000/24	link 3
00001010.10101000.00000000.00000000/16	link 4
All other addresses	link 5

Assume the router receives datagrams destined to the following addresses and decide which link they are forwarded to.

- A: 00001010.10101000.00000100.10000000
- B: 00001010.10101000.00001001.00000000
- C: 00001010.10101010.00000101.00000000
- D: 00001010.10101000.00000011.00000000
- E: 00001010.10101000.00000111.00000000

**On which link will they be forwarded? (5 points)**

A: link <input type="text"/>	B: link <input type="text"/>	C: link <input type="text"/>	D: link <input type="text"/>	E: link <input type="text"/>
------------------------------	------------------------------	------------------------------	------------------------------	------------------------------

Maks poeng: 5

## 19 TCP/IP switch layers

Which layers in the TCP/IP model are involved when an Ethernet switch forwards packets? (2 points)

**Select one or more alternatives**

- Application layer
- Transport layer
- Network layer
- Link layer
- Physical layer

Maks poeng: 2

## 20 Link layer

Below are some general statements about how the link layer works. Select the correct alternatives(s). (2 points)

**Select one or more alternatives**

- The link layer is the place in the protocol stack where software meets hardware.
- The link layer is implemented only in hardware.
- The link layer cannot offer any form of reliable delivery.
- The link layer performs error detection.
- The link layer is implemented only in software.

Maks poeng: 2

## 21 Wireless concepts

Below are some general statements about wireless transmission as well as some more specific statements about how IEEE 802.11 wireless LANs function. (6 points)

**Fill in the correct term in each sentence.**

In [ ] ▾ (rate adaptation, interference, path loss, ad-hoc

mode, multipath propagation, infrastructure mode, beacon frames) each wireless host is connected to the Internet via an access point.

In [ ] ▾ (interference, ad-hoc mode, path loss, infrastructure mode, rate adaptation, multipath propagation, beacon frames) wireless hosts themselves provide routing, address assignment and DNS.

Wireless stations discover and identify the access point using

[ ] ▾ (multipath propagation, infrastructure mode, path loss, ad-hoc mode, rate adaptation, interference, beacon frames).

Attenuation of the wireless signal when travelling through matter is called

[ ] ▾ (interference, rate adaptation, beacon frames, ad-hoc mode, multipath propagation, path loss, infrastructure mode).

When two or more sources within a basic service set transmit at the same time on the same frequency then [ ] ▾ (ad-hoc mode,

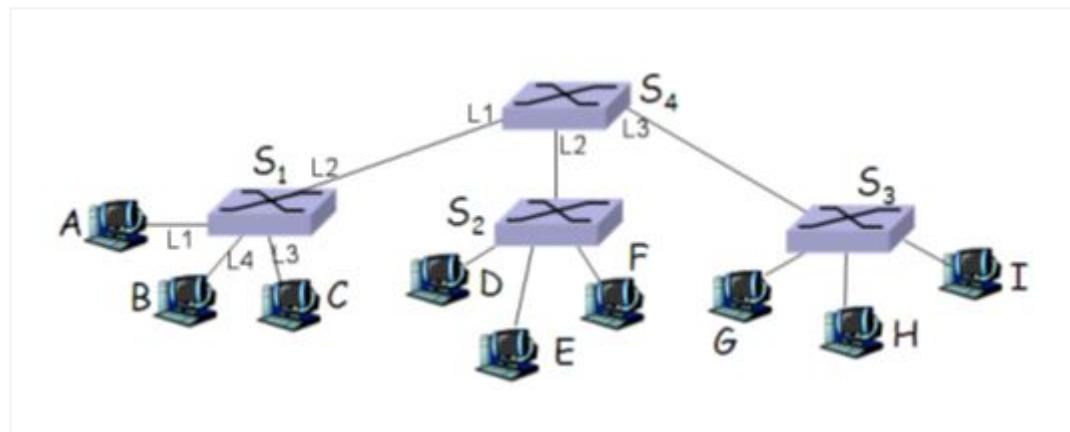
infrastructure mode, rate adaptation, multipath propagation, beacon frames, path loss, interference) may occur.

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

[ ] ▾ (infrastructure mode, ad-hoc mode, rate adaptation, path loss, interference, beacon frames, multipath propagation).

Maks poeng: 6

## 22 Self-learning switches



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:**

**A to B**

**E to I****I to A****Then D 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
A	▼ (L1, L4, L2, L3)
E	▼ (L3, L4, L1, L2)
I	▼ (L1, L4, L2, L3)
▼ (E, A, I, C, H, B, D)	▼ (L4, L1, L2, L3)

**Which hosts receive the last frame?**

▼ (All except D, D and

E, Only E, D, E and F)

Maks poeng: 6

## 23 E-mail encryption

What is the de-facto e-mail encryption scheme described in the textbook?  
(2 points)

**Select one alternative**

- DSA (Digital Signature Algorithm)
- TLS (Transport Layer Security)
- RSA (Rivest-Shamir-Adleman)
- PGP (Pretty Good Privacy)
- MIME (Multipurpose Internet Mail Extensions)

Maks poeng: 2

## 24 SSL statements

Below are some clauses about the SSL protocol. What is the correct statement about SSL? (2 points)

**Select one alternative**

- SSL connections are closed by terminating the TCP connection.
- SSL allows agreeing on cryptographic algorithms during the handshake phase.
- SSL implements sequence numbers in cleartext in the SSL record.
- SSL always uses AES after the handshake phase.

Maks poeng: 2

**25 SSL certificate**

What is the digital certificate used for in the TLS/SSL protocol? (2 points)

**Select one or more alternatives**

- Licence for legal sending of SSL messages.
- Authorise the client to communicate with the server.
- Authenticate the server.
- Create a signature for SSL messages.
- Use public key to encrypt master secret.

Maks poeng: 2

**26 SSL Quality of Service**

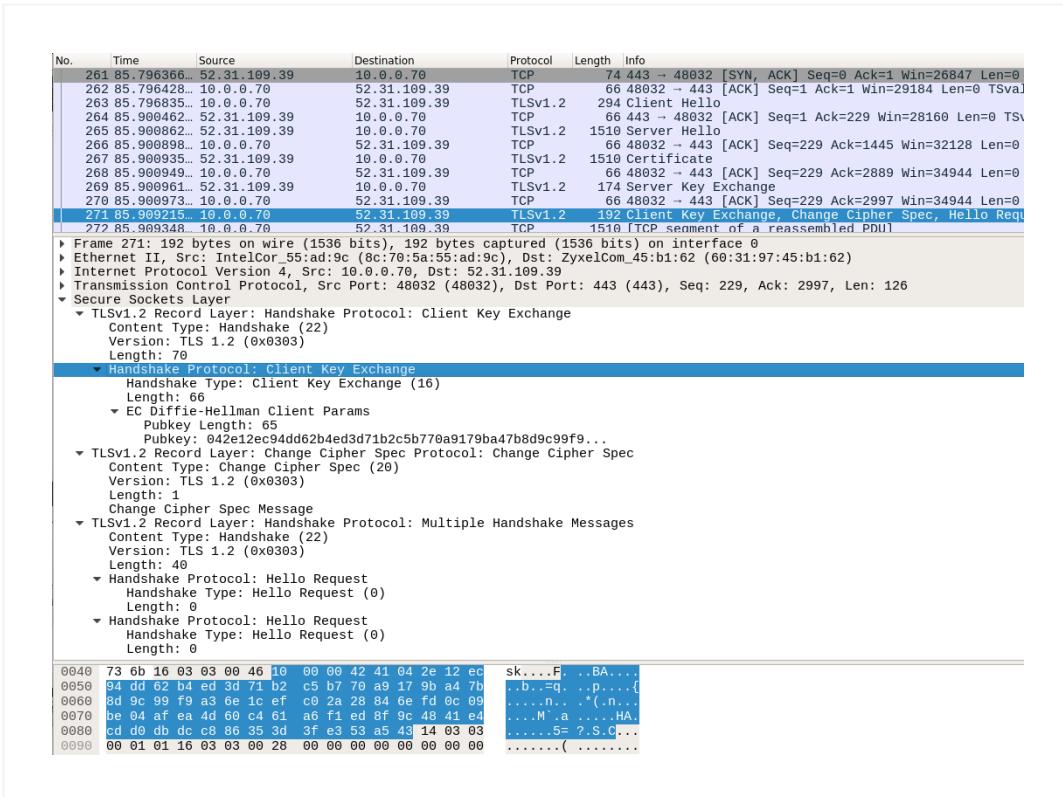
Which service quality guarantees does SSL give? (3 points)

**Select correct answer(s)**

- Bounded delay
- Data integrity
- Data confidentiality
- Guaranteed bandwidth
- Server authentication

Maks poeng: 3

## 27 Wireshark SSL



Which link layer protocol is used here? ▼ (ARP, DHCP, Ethernet, IEEE 802.11, HTTP, IP)

Which protocol is encapsulated in the link layer frame? ▼ (ARP, DHCP, Ethernet, IEEE 802.11, HTTP, IP, SNMP, SMTP, TCP, UDP)

Packet 270 shows "Win=34944". What type of window is this?

▼ (Congestion window, Receiver

window, Sliding window in number of packets, Window size of the user interface)

Which phase of a TCP connection does packet 261 belong to?

▼ (Connection, Data transfer,

Disconnection, Three-way handshake, Listen for new connections (LISTEN))

Who sends packet 261? ▼ (None, Client, Server, Do not know)

How many bytes payload are sent in packet 271?

How many bytes payload have been sent (from client to server) and received in total from the start of the session and until inclusive packet 271?

Sent:  Received:

Which application layer protocol is used here?  ▾ (ARP, DHCP,

**DNS, Ethernet, FTP, HTTP, SNMP, SMTP, TLS/SSL)**

Packets 263 and 265 contain nonces. What is the purpose of these nonces?  ▾ (Data authentication,

Protect against chosen plaintext attacks, Protect against replay attacks, Protect against man-in-the-middle attacks, Protect against denial-of-service attacks, Protect against known plaintext attacks)

For SSL, how can the client securely send the Master Secret (MS) to the server?  ▾ (Encrypt MS with

the private key of the server., Encrypt MS with the public key of the server., Encrypt MS with the common session key., Use the signed hash value of MS as key.)

Maks poeng: 11

## 28 Link utilisation

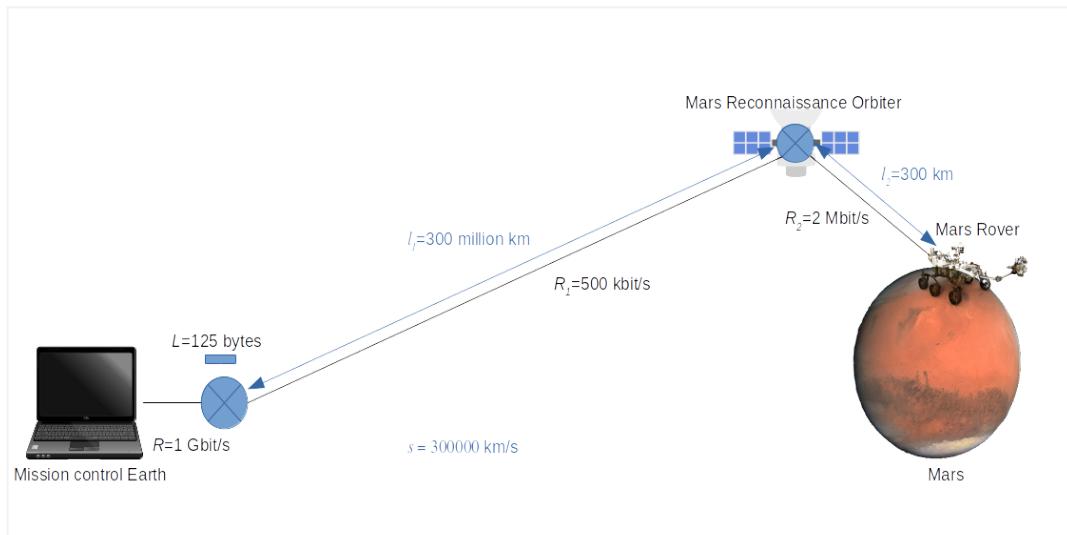
Consider a long fibre link between two hosts, where the round-trip propagation delay between these two end systems, RTT, is 30 ms. Suppose that the size of a packet is 1250 bytes, including both header fields and data, and that the transmission rate is 1 Gbit/s. (4 points)

What is the transmission delay in  $\mu s$ ?

How big would the window size have to be (in number of packets) for the channel utilisation to be greater than 97 percent? Round up your answer

Maks poeng: 4

## 29 Transmission and Propagation delay



The Mars Rover is connected to Earth via the Mars Reconnaissance Orbiter satellite as shown in the figure. The bandwidth from Earth to the satellite is 500 kbit/s and the bandwidth from the satellite to the Rover is 2 Mbit/s. The satellite is 300 km from the surface of Mars and 300 million km from Earth, and works like a router (store and forward). The speed of light is 300 000 km/s. Routers and switches before the satellite link are not overloaded and use a 1 Gbit/s network. (10 points)

How large is the propagation delay between the Earth and the satellite in seconds?

A 125 bytes control frame is sent from Earth to the Mars Rover. How large is the total transmission delay in milliseconds through all routers?

What is the minimal round-trip-time (RTT) in seconds for the control frames?

Assuming that a continuous sequence of control frames is sent to the Rover, what is the maximum end-to-end bandwidth in Mbit/s that is attainable from Mission control and to the Rover?

Assuming the Mars Rover has a speed of 5 km/h, is it then possible to successfully perform controlled navigation of the Rover on Mars from Earth interactively in a terrain full of craters and boulders?

**Select one**

- Yes
- No

Maks poeng: 10

## 30 Comments

Here you can write assumptions, clarifications and comments to your answers. These comments do not give additional points themselves, but may influence the judgement of commented assignments. (max 500 words)

**Write assumptions and comments to the assignments here.**

Format ▾ | | | |

| ✎ | Σ | ✖

Words: 0/500

Maks poeng: 0



## DAT204 Exam v2017

Datakommunikasjon (Universitetet i Agder)



Skann for å åpne på Studocu

## 1 DAT204 spring 2017

**Emnekode:** DAT204

**Emnenavn:** Datakommunikasjon

**Dato:** 06.03.2017

**Varighet:** 4 timer

**Tillatte hjelpeemidler:** Godkjent kalkulator

<http://www.uio.no/studier/admin/eksamen/hjelpemiddel/mn-math-kalkulatorer.html>

**Merknader:** The exam is in both Norwegian and English. You select language in the menu at the upper right corner. Hvert delspørsmål gir fra 1 til 3 poeng, totalt 100 poeng. Enkelte oppgaver inneholder flere delspørsmål. Oppgaven benytter hovedsaklig flervalgsspørsmål (multiple choice) og har noen utregningsoppgaver. Det er et åpent tekstfelt på siste side som kan brukes til å skrive utfyllende kommentarer og antagelser til oppgavene i eksamenen. Dette tekstfeltet gir ikke poeng i seg selv, men kan påvirke vurderingen av andre oppgaver. Det er ikke nødvendig å benytte tekstfeltet, rett svar på alle spørsmål vil gi full score.

Lykke til!

---

Det forekommer av og til spørsmål om bruk av eksamensbesvarelser til undervisnings- og læringsformål. Universitetet trenger kandidatens tillatelse til at besvarelsen kan benyttes til dette. Besvarelsen vil være anonym.

**Tillater du at din eksamensbesvarelse blir brukt til slikt formål?**

Ja

Nei

Maks poeng: 0

## 2 DAT204\_V17\_1

**Hva heter meldingene på de forskjellige lagene? (6 poeng)**

Applikasjonslaget

Transportlaget

Nettverkslaget  ▾

Linkkaget  ▾

Fysisk lag  ▾

Alle disse lagene kalles til sammen en:  ▾

Maks poeng: 6

### 3 DAT204\_V17\_2

Nedenfor finnes en liste over protokoller. Hvilken tilhører applikasjonslaget?  
(2 poeng)

**Velg et alternativ**

- IPv6
- SMTP
- UDP
- ICMP
- ARP

Maks poeng: 2

### 4 DAT204\_V17\_3

Et av utsagnene nedenfor er riktig, de andre er feil eller meningsløse. Kryss av for det som er riktig. (2 poeng)

**Velg et alternativ**

- Når UDP benyttes overlates eventuell feilretting til applikasjonen.
- UDP segmenter som mottas med feil sjekksum blir kastet og sendt på nytt når rundturforsinkelsen er utløpt.
- UDP segmenter med feil sekvensnummer blir kastet.
- Hvis vi var garantert at alle linkene i et IP nett var uten bitfeil, ville feilsjekk og retransmisjoner være unødvendige.

Maks poeng: 2

## 5 DAT204\_V17\_4

RTP protokollen brukes for å transportere sanntidstrafikk. Hvordan kan ruterne finne ut hvor RTP-pakkene skal sendes? ( 2 poeng)

**Velg et alternativ**

- SIP gir denne informasjonen.
- De bruker portnummeret i UDP-headeren.
- IP-header gir denne informasjonen.
- RTP-pakkene går direkte mellom brukerne.

Maks poeng: 2

## 6 DAT204\_V17\_5

En av påstandene nedenfor er riktig. De andre er feil eller meningsløse.  
Kryss av for den riktige.

(2 poeng)

**Velg et alternativ**

- Hvis CRC feltet i en ethernetramme viser at rammen inneholder en feil, vil rammen bli kastet og ICMP gir tilbakemelding til avsender slik at rammen kan bli retransmittert.
- ARP protokollen returnerer MAC adressen som svarer til IP adressen til en vertsmaskin på lokalnettet. Forbindelsen mellom dem lagres så i ARP tabellen.
- En ethernettsvitsj kan ikke håndtere både IP v4 og IP v6 trafikk uten å kreve egen programvare for hver protokollstakk.
- MAC adresser tildeles v.h.a. DHCP server.

Maks poeng: 2

## 7 DAT204\_V17\_6

Nedenfor kommer noen påstander om TCP. Kryss av for den påstanden som er riktig.

(2 poeng)

**Velg et alternativ**

- TCP gir en pålitelig virtuell ende til ende forbindelse over et upålitelig IP nett.
- En TCP forbindelse må alltid reetableres hvis en ruter i det underliggende IP nettet går ned slik at datagrammene må begynne å gå en annen vei.
- TCP headeren har en minimumslengde på 32 byte.
- TCP SYN inneholder feltet "Duration" som forteller mottakeren hvor lenge forbindelsen som er i ferd med å etableres skal vare.

Maks poeng: 2

## 8 DAT204\_V17\_7

Hvilken av påstandene under er riktig? (2 poeng)

**Velg et alternativ**

- UDP trafikk mot forskjellige applikasjoner i en server benytter en felles socket hvis trafikken kommer fra samme klient.
- En UDP sesjonssocket identifiseres ved hjelp av sender og mottaker port og IP adresse.
- UDP trafikk mot den samme applikasjonen i en server benytter hver sin socket når trafikken kommer fra forskjellige klienter.
- UDP trafikk mot den samme applikasjonen i en server benytter en felles socket selv om trafikken kommer fra forskjellige klienter.

Maks poeng: 2

## 9 DAT204\_V17\_8

Hvilken påstand er riktig? (2 poeng)

## **Velg et alternativ**

- Parameteren "Receive Window" er en del av TCP metnings kontroll algoritmen.
  - TCP flytkontroll algoritmen sikrer at ikke nettet overbelastes.
  - Antall ukvitterte byte kan være større enn mottakerbufferet. (Hvis variabelen "Congestion Window" er større enn "Receive Window").
  - På en TCP forbindelse kan ikke antall ukvitterte byte være større enn mottakerbufferet.

Maks poeng: 2

10 DAT204\_V17\_9

Figurer over viser en Ethernet ramme med en ARP pakke. En av påstandene under er riktig, de andre er feil. Kryss av for den riktige. (2 poeng)

## **Velg et alternativ**

- "Padding" er satt inn fordi Ethernetramma i utgangspunktet inneholdt for lite nyttelast.
  - Den som besvarte denne ARP forespørselen har MAC adresse 00:d0:59:a9:3d:68
  - Enheten som sendte den originale forespørselen har IP adresse 192.168.1.1
  - ARP pakka har lengde 48 byte.

Maks poeng: 2

## 11 DAT204\_V17\_10

Nedenfor fremsettes noen påstander om TCP. Kryss av for den riktige. (2 poeng)

### Velg et alternativ

- "Congestion avoidance" er knyttet til "Receive Window" i TCP headeren.
- TCP timer utløp trigger "Fast recovery".
- "Fast recovery" er betegnelsen på fasene i en TCP overføring der "Congestion Window" øker eksponentielt (raskt).
- "Slow start" er betegnelsen på fasene i en TCP overføring der "Congestion Window" øker eksponentielt (raskt).

Maks poeng: 2

## 12 DAT204\_V17\_11

```

Frame 2964: 742 bytes on wire (5936 bits), 742 bytes captured (5936 bits)
Ethernet II, Src: Oracle_94:63:3e (00:03:ba:94:63:3e), Dst: 00:00:00_60:dd:19 (00:00:00:60:dd:19)
Internet Protocol Version 4, Src: 200.57.7.195 (200.57.7.195), Dst: 200.57.7.204 (200.57.7.204)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip-tls (5061)
Session Initiation Protocol
Request-Line: INVITE sip:francisco@bestel.com:55060 SIP/2.0
Message Header
Message Body
Session Description Protocol
Session Description Protocol version (v): 0
Owner/Creator, Session Id (o): clarent 121082 121083 IN IP4 200.57.7.196
Session Name (s): Clarent C5CM
Connection Information (c): IN IP4 200.57.7.196
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 40360 RTP/AVP 8 18 4
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): rtpmap:18 G729/8000
Media Attribute (a): rtpmap:4 G723/8000
Media Attribute (a): SendRecv

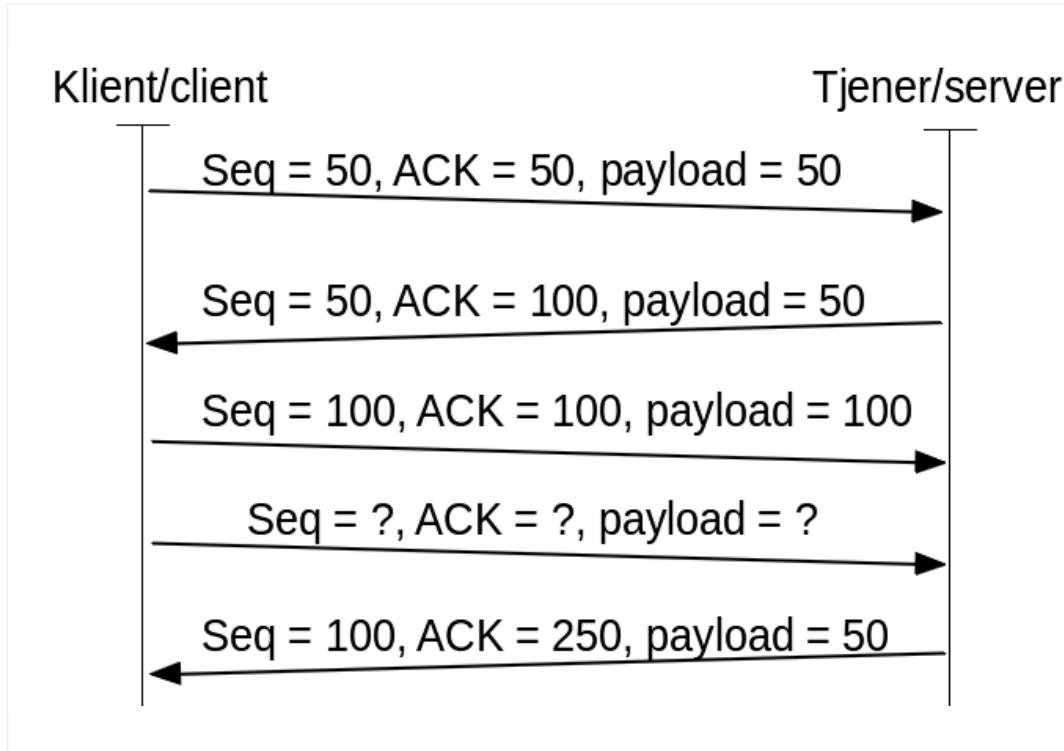
```

Denne SIP INVITE meldingen angir at RTP-pakkene skal ( 2 poeng)

**Velg et alternativ**

- Mottas på portnummer 40360
- Mottas på IP adresse 200.57.7.195
- Sendes fra IP adresse 200.57.7.204
- Mottas på portnummer 5061

Maks poeng: 2

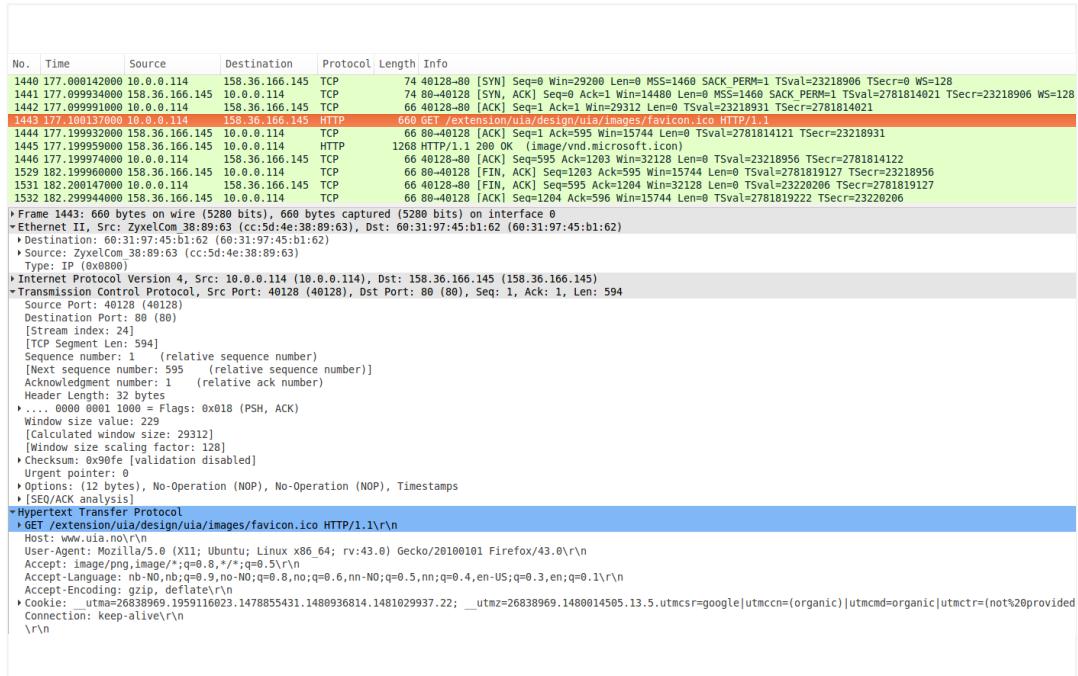
**13 DAT204\_V17\_12**

Ovenfor er det vist et utsnitt av en TCP overføring. Hva vil sekvensnummer, ACK og payload være i det nest siste segmentet i den viste overføringen? (3 poeng)

Seq =  ACK =  payload =

Maks poeng: 3

**14 DAT204\_V17\_13**



## Figuren over viser en TCP sekvens fra Wireshark. Besvar følgende spørsmål. (18 poeng)

Hvilken linklagsprotokoll brukes her?

Hvilken type protokoll er pakket inn i linklagsramma?

Hvor stor er vindusstørrelsen i bytes for det gitte segmentet?

Hva slags vindu er dette?

Hvilken fase av en TCP forbindelse tilhører valgt segment?

Hvor mange bytes nyttelast overføres i det viste segmentet?

Hvem sender det valgte TCP segmentet?

Hvor mange bytes nyttelast fra applikasjonslaget har blitt sendt og mottatt til sammen i denne TCP sesjonen?

Sendt:

Mottatt:

Hvilken applikasjonslagsprotokoll er det som benyttes her?

Hva slags type forbindelse bruker applikasjonslagsprotokollen?

Hvilken type data kan mottas i følge applikasjonslagsprotokollen?

Maks poeng: 18

**15 DAT204\_V17\_14****Sett inn rutingalgoritmen som passer med uttrykket. (5 poeng)**

- ▼ benytter Dijkstras algoritme for å finne korteste sti.
- ▼ er dominert av rutingpolicyer istedenfor å fokusere på å finne stien med lavest kostnad i nettet.
- ▼ utveksler informasjon om endrede rutingtabeller med naboruterne.
- ▼ annonserer et subnett til alle autonome systemer på Internett.
- ▼ utveksler informasjon om naboruterne med alle ruterne i nettet.

Maks poeng: 5

**16 DAT206\_V17\_15****Hvilket eller hvilke lag i TCP/IP modellen prosesseres normalt i rutere? (2 poeng)**

- Transportlaget og Nettverkslaget
- Fysisk lag, Linklaget og Rutinglaget
- Fysisk lag og Linklaget
- Alle lag opp til Applikasjonslaget
- Fysisk lag, Linklaget og Nettverkslaget

Maks poeng: 2

**17 DAT204\_V17\_16**

En av påstandene under er riktig, de andre er feil eller meningsløse. Kryss av for den riktige.

(2 poeng)

**Velg et alternativ**

- Internett bruker selvlærende svitsjer for å gi mulighet for ruteaggregering.
- Feltet "Identifier" i IP v4 headeren brukes sammen med den lokale IP adressen i en NAT server for å gi en unik identitet i det globale internettet.
- CIDR (Classless Inter Domain Routing) er på formen a.b.c.d/x der x er antall bits i nettverksdelen av adressen.
- "Type of service" feltet i IP v4 headeren forteller mottakeren hva slags nytte last datagrammet inneholder.

Maks poeng: 2

**18 DAT204\_V17\_17**

En av påstandene nedenfor er riktig, resten er feil eller meningsløse. Sett kryss ved den riktige påstanden. (2 poeng)

**Velg et alternativ**

- Feltet "Next header" i IP v6 datagrammene har samme funksjon som feltet "payload" i IEEE802.11 rammene.
- Feltet "Next header" i IP v6 datagrammer beskriver blant annet protokollen til laget over i datagrammet.
- Feltet "Datagram length" i IP v4 headeren har samme funksjon som feltet "Duration" i IEEE802.11 rammene. (De skal begge fortelle hvor lenge mediet blir opptatt).
- Feltet "Next header" i IP v6 datagrammene fungerer som en erstatning for "type of service" feltet i IP v4 datagrammene.

Maks poeng: 2

**19 DAT204\_V17\_18**

```

> 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: 60:31:97:45:b1:62 (60:31:97:45:b1:62)
> Source: ZyxelCom 38:89:63 (cc:5d:4e:38:89:63)
> Type: IPv6 (0x86dd)
> 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)
> 0110 ... = Version: 6
> ... 0000 0000 ... .... .... .... = Traffic class: 0x00000000
> ... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
> 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

```

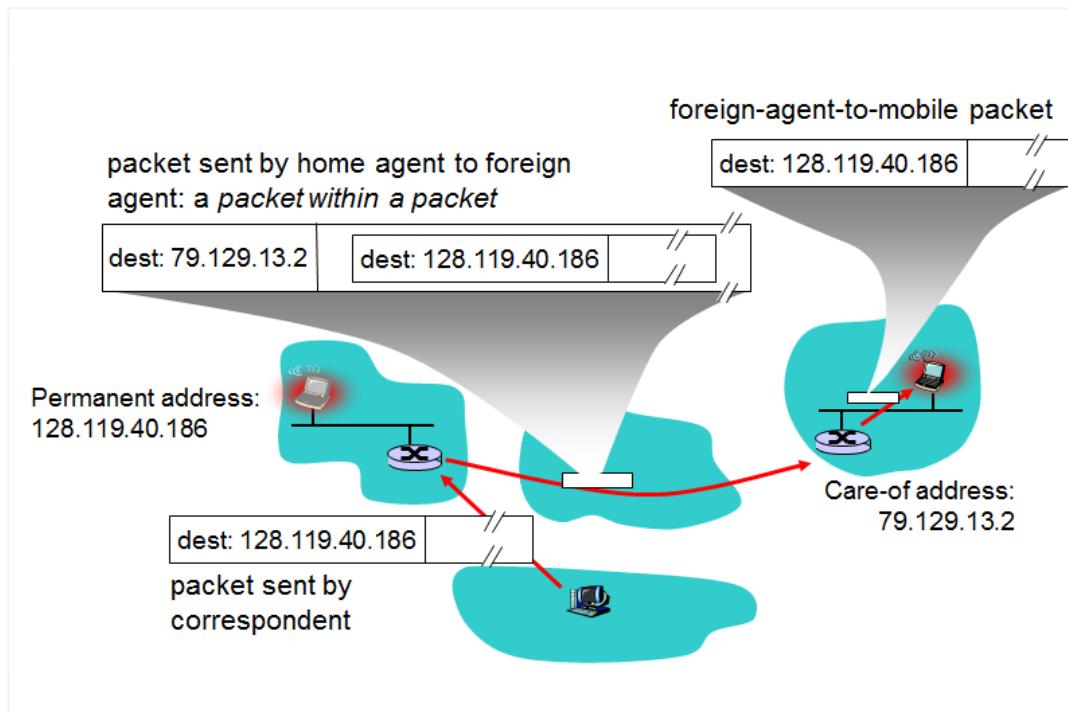
Se Wireshark log. Hva er dette et eksempel på ? ( 2 poeng)

### Vælg et alternativ

- Ingen tunnelling.
- IPv6 tunnelering i IPv4.
- IPv4 tunnelering i IPv6.
- Eksempel som viser overgang fra IPv4 til IPv6.
- En konstruert oppstilling som ikke er tillatt.

Maks poeng: 2

## 20 DAT204\_V17\_19



Figuren illustrerer funksjoner i Mobile IPv4. (Figuren er hentet fra boka "Computer Networking - A Top\_Down\_Approach"). Hva skjer i enheten med adresse 79.129.13.2 ? ( 2 poeng)

### Velg et alternativ

- Datagrammet sendes tilbake til Mobile Nodes permanente adresse.
- Datagrammet har feil adresse og vil bli kastet.
- Den "ytre" headeren fjernes. Datagram videresendes til Mobile Node.
- Dette fungerer ikke siden vi mangler en Home Agent.
- Mottatt datagram sendes uendret til Mobile Node.

Maks poeng: 2

## 21 DAT204\_V17\_20

IP adressen **10011110.00100100.10100110.10010001** kan skrives på desimalform som:

(2 poeng)

--	--	--	--

Maks poeng: 2

## 22 DAT204\_V17\_21

I en ruter finnes følgende ruter i rutingtabellen:

00001010.00000001.00000010.00000000/23	link 1
00001010.00000001.00000010.00000000/24	link 2
00001010.00000001.00000010.10000000/25	link 3
00001010.00000001.00000000.00000000/16	link 4
Alle andre adresser	link 5

Anta at ruteren mottar to datagram med følgende mottakeradresser:

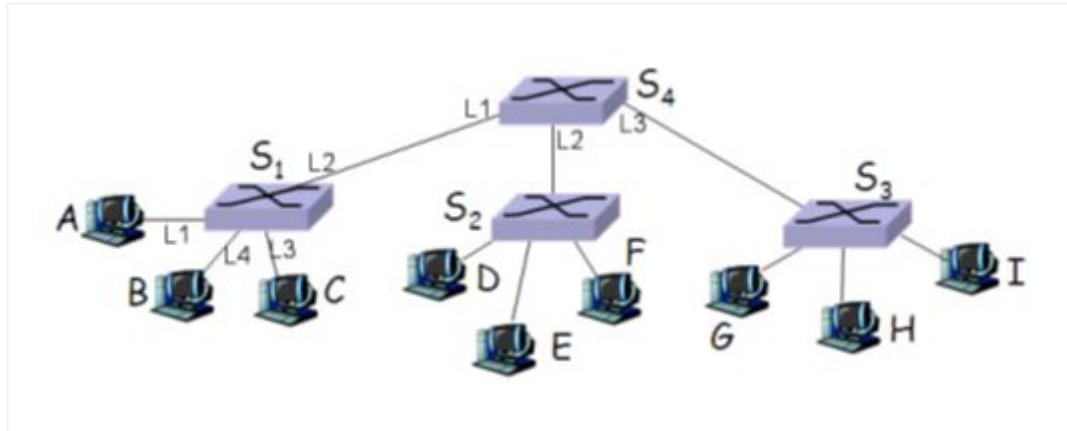
A: 00001010.00000001.00000010.10000010

B: 00001010.00000001.00000011.11111101

På hvilke linker skal disse sendes videre? (3 poeng)

A: link  B: link

## 23 DAT204\_V17\_22



Figuren over viser et nettverk med fire selvlærende ethernetsvitsjer og 9 vertsmaskiner (hosts). Svitsjene er nettopp skrudd på og svitsjetabellene er tomme. (6 poeng totalt)

**Anta at vi sender følgende rammer:**

A til B

E til I

H til A

Deretter C til B.

**Hvordan vil svitsjetabellen i S<sub>1</sub> se ut etter denne sekvensen?**

Svitsjetabell (switch table) for S<sub>1</sub>

Adresse	Grensesnitt/interface
A	▼
E	▼
H	▼
▼	▼

**Hvilke vertsmaskiner (hosts) mottar denne rammen?**

Maks poeng: 6

## 24 DAT204\_V17\_23

**Plasser riktig protokoll på rett sted. (5 poeng)**

Denne protokollen brukes i telefoni og deler hver ramme inn i N tidsluker (time slots), der forskjellige tidsluker tilordnes til forskjellige forbindelser:

Denne protokollen deler frekvensbåndet inn i forskjellige kanaler der hvert frekvensbånd kan tilordnes en forbindelse:

Denne protokollen multipliserer hvert bit med en mye raskere "chipping code" for å redusere problemet med interferens i trådløse systemer:

Denne protokollen brukes i trådløse nett (IEEE 802.11) for å unngå problemet med skjulte terminaler:

Denne protokollen brukes i Ethernett der enheten lytter før den sender:

Maks poeng: 5

## 25 DAT2016\_V17\_24

**Hvilke teknikker må til for at ruterne i et IP basert nettverk skal kunne tilby garantert tjenestekvalitet? (6 poeng)**

Hvordan kan første ruter merke pakkene slik at den kan skille mellom forskjellige trafikklasser?

Hvordan kan en ruter garantere at en trafikkklasse får minst en gitt andel av den totale båndbredden?

Hvordan kan ruterne begrense størrelsen på datautbrudd (burst size) for en gitt forbindelse for å redusere latenstiden og tidsforsinkelsen i nettet?

Hvordan kan inngangsruten sørge for at ressursene i nettet ikke blir overbooket?

Hvordan kan man overordnet håndheve at ikke en vertsmaskin tilegner seg flere ressurser enn det den har krav på i henhold til tjenestenivåavtale?

Hvordan kan man sikre at man velger en bestemt rute gjennom nettet?

Maks poeng: 6

**26 DAT204\_V17\_25**

**Setningene under beskriver trådløse nettverk. Fyll inn rett uttrykk. (6 poeng)**

Et aksesspunkt sammen med vertsmaskinene som kommuniserer via dette aksesspunktet former til sammen:

Problemet med skjulte terminaler kan håndteres ved å bruke:

Et aksesspunkt annonserer at et Wifi nettverk finnes via:

Fysiske hindringer eller signal fading kan føre til:

Et aksesspunkt identifiseres via dets:

Hvis en 802.11 node merker at kanalen er opptatt, så vil den benytte:

Maks poeng: 6

**27 DAT204\_V17\_26**

Anta at et analogt audiosignal samples 10000 ganger i sekundet og at hver sample er kvantifisert i 256 nivåer (2 poeng).

**Hvor mange bits er hver sample?**

**Hva blir den resulterende bitraten av PCM audiosignalet i bits/s?**

Maks poeng: 2

**DAT204\_V17\_27**

**28**

Data sendes over en fiberlink på 1000 km fra Oslo og til London. Linken har en hastighet på 1 Gbit/s. Utbredelseshastigheten på fiberen er 250 000 km/s. En ramme på 1500 bytes denne linken. Ruterne og svitsjene har høy kapasitet og er ikke overbelastet. (8 poeng)

**Hvilken type forsinkelse gir det største bidraget til den totale tidsforsinkelsen i dette scenariet?**



**Hvor stor er tidsforsinkelsen i sekunder fra rammen sendes på linken fra Oslo og til den har blitt mottatt i London? Avrund svaret til tre desimaler.**

**Hvor stor blir den minimale rundturforsinkelsen i sekunder for datagrammer på denne linken? Avrund svaret til tre desimaler**

**Det gjennomføres en IP telefonisamtale over linken der avspillingsbufferet for å jevne ut jitter gir en tilleggsforsinkelse på 140 ms. Er ende til ende tidsforsinkelsen på denne linken akseptabel for en IP telefonisamtale ut fra tjenestekvalitetskravene til slike samtaler?**

- Ja
- Nei

Maks poeng: 8

**29 DAT204\_V17\_Comments**

Her kan du beskrive antagelser, begrunnelser og kommentarer til besvarelsen din. Disse kommentarene gir ikke tilleggsspoeng i seg selv, men vil kunne påvirke vurderingen av kommenterte oppgaver. (maks 500 ord)

**Beskriv antagelser og kommentarer til oppgavene her.**

Format | | | | |

| | |

Words: 0/500

Maks poeng: 0



## DAT204 Exam h2016

Datakommunikasjon (Universitetet i Agder)



Skann for å åpne på Studocu

## 1 DAT204 autumn 2016

**Emnekode:** DAT204

**Emnenavn:** Datakommunikasjon

**Dato:** 25.11.2016

**Varighet:** 4 timer

**Tillatte hjelpeemidler:** Godkjent kalkulator

<http://www.uio.no/studier/admin/eksamen/hjelpemiddel/mn-math-kalkulatorer.html>

**Merknader:** Hvert delspørsmål gir fra 1 til 3 poeng, totalt 100 poeng. Enkelte oppgaver inneholder flere delspørsmål. Oppgaven benytter hovedsaklig flervalgsspørsmål (multiple choice) og har noen utregningsoppgaver. Det er et åpent tekstfelt på siste side som kan brukes til å skrive utfyllende kommentarer og antagelser til oppgavene i eksamenen. Dette tekstfeltet gir ikke poeng i seg selv, men kan påvirke vurderingen av andre oppgaver. Det er ikke nødvendig å benytte tekstfeltet, rett svar på alle spørsmål vil gi full score. Eksamenen er på bokmål og engelsk.

Lykke til!

---

Det forekommer av og til spørsmål om bruk av eksamensbesvarelser til undervisnings- og læringsformål. Universitetet trenger kandidatens tillatelse til at besvarelsen kan benyttes til dette. Besvarelsen vil være anonym.

**Tillater du at din eksamensbesvarelse blir brukt til slikt formål?**

Ja

Nei

Maks poeng: 0

## 2 DAT204\_H16\_1

**Hva heter meldingene på de forskjellige lagene? (6 poeng)**

Applikasjonslaget

Transportlaget

Nettverkslaget

Linkkaget

Fysisk lag

Alle disse lagene kalles til sammen en:

Maks poeng: 6

### 3 DAT204\_H16\_2

Hvilken protokoll kjører som en tjeneste på applikasjonslaget? (2 poeng)

- ARP
- ICMP
- IPv6
- DHCP

Maks poeng: 2

### 4 DAT206\_H16\_3

Hvilket eller hvilke lag i TCP/IP modellen prosesseres normalt i rutere? (2 poeng)

- Transportlaget og Nettverkslaget
- Fysisk lag, Linklaget og Rutinglaget
- Fysisk lag, Linklaget og Nettverkslaget
- Alle lag opp til Applikasjonslaget
- Fysisk lag og Linklaget

Maks poeng: 2

## 5 DAT204\_H16\_4

**Kun et av utsagnene nedenfor er riktig, resten er feil eller meningsløse. Kryss av for det riktige utsagnet. (3 poeng)**

- Adresser på linklaget tildeles ved hjelp av en DHCP server.
- ARP protokollen finner MAC adressen til en enhet når vertsmaskinen bare kjenner IP adressen. Koblingen mellom dem blir så lagret i ARP tabellen.
- Hvis CRC feltet i et IP datagram viser at den inneholder en bitfeil vil rammen bli kastet.
- En ethernetsvitsj ser på nyttelasten i ethernetrammene og kan derfor ikke svitsje rammer med både IPv4 og IPv6 samtidig.

Maks poeng: 3

## 6 DAT204\_H16\_5

Nummerering og tidsangivelser i RTP pakker samt buffer hos mottaker gjør det mulig å (2 poeng)

**Velg ett alternativ**

- Enkelt få til retransmisjon av tapte pakker
- Enkelt introdusere SIP-protokollen
- Sikre en vei gjennom nettet med fast forsinkelse
- Redusere virkningen av jitter

Maks poeng: 2

## 7 DAT204\_H16\_6

**Plasser rett begrep inn i rett setning relatert til nettverksadministrasjon. (6 poeng)**

- 1.3.6.1.2.1.7.1 er et eksempel på en □ ▼ .
- ▼ inneholder informasjon om administrerte objekter (managed objects).
  - ▼ er en IETF standard for nettverksadministrasjon, som definerer kommandoer mellom en administrerende enhet og agenter som kjører i administrerte nettverksheter.
  - ▼ beskriver en maskinuavhengig måte å utveksle data mellom maskiner på.
  - ▼ er en måte agenter i administrerte enheter kan bruke for å rapportere unntakshendelser til den sentrale informasjonsdatabasen.
  - ▼ er et datadefinisjonsspråk for administrerte objekter.

Maks poeng: 6

## 8 DAT204\_H16\_7

**Ett av utsagnene nedenfor er riktig, de andre er feil eller meningsløse.  
Kryss av for det som er riktig (3 poeng)**

- Hvis alle linkene i et IP nett var garantert feilfrie ville feilsjekk og retransmisjoner vært unødvendig.
- UDP segmenter med feil sekvensnummer blir kastet.
- UDP benytter "go-back-n" slik at mange segmenter kan sendes rett etter hverandre før man får bekreftelse.
- UDP tilbyr ikke pålitelig dataoverføring.

Maks poeng: 3

## 9 DAT204\_H16\_8

**Kryss av for den riktige påstanden om TCP. (3 poeng)**

- Time to live (TTL) verdien i TCP bestemmer levetiden til segmentet i sekunder.
- TCP forbindelser kobles ned ved hjelp av RST segmenter.
- Tredobbel duplikat ACK reduserer mottakervinduet.
- TCP har en algoritme som beregner rundturforsinkelsen og dermed sikrer at timerverdien normalt er større enn rundturforsinkelsen.

Maks poeng: 3

**10 DAT204\_H16\_9**

Kun et av utsagnene nedenfor er riktig, resten er feil eller meningsløse. Kryss av for det riktige utsagnet. (3 poeng)

**Velg et alternativ**

- På en TCP forbindelse måles rundturforsinkelsen så lenge det sendes fragmenter, men kun en måling pågår av gangen.
- Terskelverdien for slow start settes til halve verdien av metningsvinduet ved timeout.
- Timerfunksjonen i UDP og TCP har i prinsippet samme oppgave, men er forskjellig konstruert.
- TCP er mest lik en "Selective Repeat" protokoll.
- Et vanlig IP nett prioriterer UDP trafikk framfor TCP for å gi god ytelse til streamingapplikasjoner.

Maks poeng: 3

**11 DAT204\_H16\_10**

**Hvilken av påstandene under er riktig? (3 poeng)**

- En UDP socket identifiseres med avsenderens port og IP adresse.
- TCP trafikk fra forskjellige klienter mot samme applikasjon benytter en felles socket fra oppkobling til nedkobling som skiller på avsender og mottaker IP adresse samt avsender og mottaker portnummer.
- TCP benytter to sockets for å opprette en forbindelse, en som mottar oppkoblings forespørsler og en som data utveksles over.
- En UDP socket identifiseres med avsender og mottaker IP adresser samt avsender og mottaker portnummer.

Maks poeng: 3

**12 DAT204\_H16\_11****En av påstandene under om TCP er FEIL. Kryss av for feil påstand. (2 poeng)**

- TCP sekvensnummeret i neste segment økes ikke når forbindelsen settes opp dersom lengden på nyttelast (payload) i forrige segment er 0.
- Sekvensnummeret til neste TCP segment er normalt lik forrige sekvensnummer pluss lengden av nyttelast (payload) i forrige segment.
- TCP benytter kumulativ bekreftelse av tidligere segmenter.
- TCP gir en pålitelig ende til ende forbindelse over et upålitelig IP nett.

Maks poeng: 2

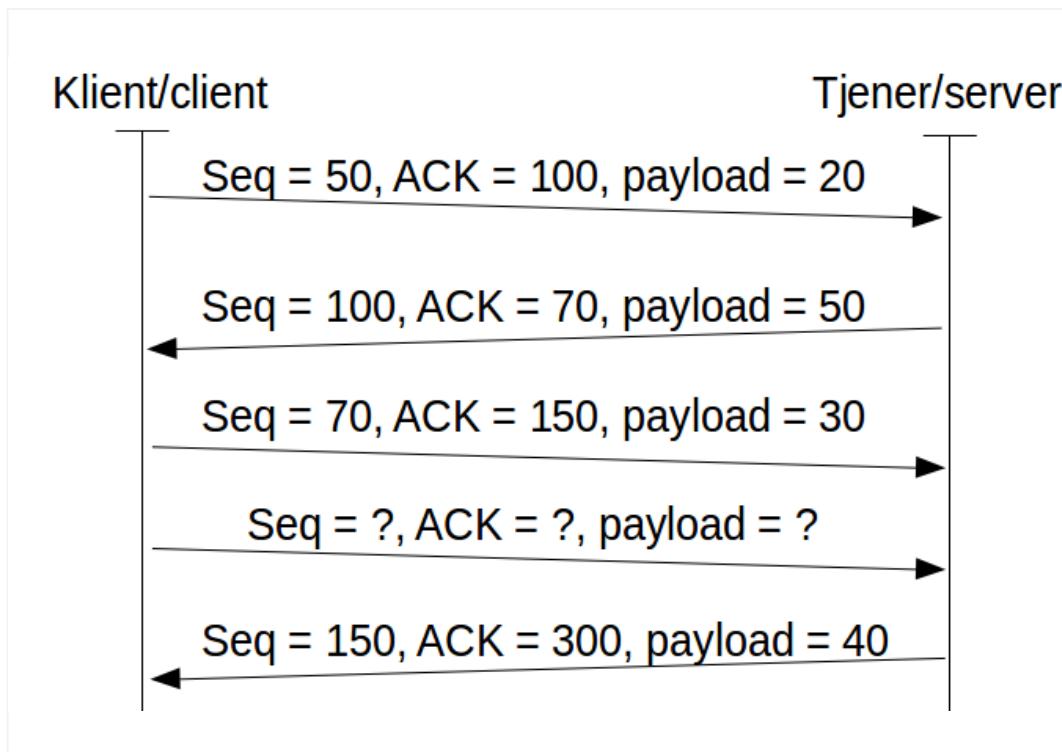
**13 DAT204\_H16\_12**

### Hvilken av følgende påstårer om TCP er riktig? (3 poeng)

- Trippel duplikat ACK medfører at metningsvinduet resettes til verdien det hadde før pakketap oppsto.
- TCP timerutløp trigger "Fast recovery".
- "Fast recovery" er betegnelsen på fasen i en TCP overføring der metningsvinduet (congestion window) øker eksponensielt raskt.
- "Congestion avoidance" er betegnelsen på fasen i en TCP overføring der metningsvinduet (congestion window) øker lineært.

Maks poeng: 3

### 14 DAT204\_H16\_13



Ovenfor er det vist et utsnitt av en TCP overføring. Hva vil sekvensnummer, ACK og payload være i det nest siste segmentet i den viste overføringen? (3 poeng)

Seq =  ACK =  payload =

Maks poeng: 3

### DAT204\_H16\_14

**15**

No.	Time	Source	Destination	Protocol	Length	Info
1615	305.46988906	10.0.2.1	10.0.2.15	TCP	66	25-57172 [FIN, ACK] Seq=120 Ack=73 Win=29056 Len=0 TStamp=281649268 TSecr=153729663
1616	305.47098406	10.0.2.15	10.0.2.1	TCP	66	57172-25 [ACK] Seq=73 Ack=120 Win=29312 Len=0 TStamp=153729663 TSecr=281649268
1617	305.47148206	10.0.2.15	10.0.2.1	TCP	66	57172-25 [FIN, ACK] Seq=73 Ack=121 Win=29312 Len=0 TStamp=153729663 TSecr=281649268
1618	305.47151406	10.0.2.1	10.0.2.15	TCP	66	57172-25 [ACK] Seq=121 Ack=74 Win=0 TStamp=281649269 TSecr=153729663
Frame 1615: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0						
Ethernet II, Src: AsustekC e3:3d:15 (bc:ae:c5:e3:3d:15), Dst: IntelCor_55:ad:9c (8c:70:5a:55:ad:9c)						
Source: AsustekC e3:3d:15 (bc:ae:c5:e3:3d:15)						
Type: IP (0x0800)						
Internet Protocol Version 4, Src: 10.0.2.1 (10.0.2.1), Dst: 10.0.2.15 (10.0.2.15)						
Version: 4						
Header Length: 20 bytes						
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))						
Total Length: 52						
Identification: 0xf54f (62799)						
Flags: 0x02 (Don't Fragment)						
Fragment offset: 0						
Time to live: 64						
Protocol: TCP (6)						
Header checksum: 0x2d65 [validation disabled]						
Source: 10.0.2.1 (10.0.2.1)						
Destination: 10.0.2.15 (10.0.2.15)						
[Source GeoIP: Unknown]						
[Destination GeoIP: Unknown]						
Transmission Control Protocol, Src Port: 25 (25), Dst Port: 57172 (57172), Seq: 120, Ack: 73, Len: 0						
Source Port: 25 (25)						
Destination Port: 57172 (57172)						
[Stream index: 43]						
[TCP Segment Len: 0]						
Sequence number: 120 (relative sequence number)						
Acknowledgment number: 73 (relative ack number)						
Header Length: 32 bytes						
... 0000 0001 0000 Flags: 0x011 (FIN, ACK)						
Window scale value: 227						
[Calculated window size: 29056]						
[Window size scaling factor: 128]						
Checksum: 0x963 [validation disabled]						
Urgent pointer: 0						
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps						
No-Operation (NOP)						
No-Operation (NOP)						
Timestamps: TStamp 281649268, TSecr 153729663						

**Figuren over viser et utdrag av en TCP sekvens fra Wireshark. Besvar følgende spørsmål. (15 poeng)**

Hvilken type protokoll er pakket inn i linklagsramma?

Hvor stor er vindusstørrelsen i bytes for det gitte segmentet?

Hva slags vindu er dette?

Hvilken fase av en TCP forbindelse er det som vises her?

Hvor mange bytes overføres i det viste segmentet?

Hvem starter sekvensen som er vist i dette eksemplet?

Hvor mange bytes data har blitt sendt og mottatt i det gitte TCP segmentet?

Sendt:  Mottatt:

Hvor mange rutere kan denne pakken maksimalt gå gjennom før den vil bli kastet og en ICMP feilmelding vil bli sendt tilbake?

Hvilken applikasjonslagsprotokoll er det som benyttes her?

Maks poeng: 15

**16 DAT204\_H16\_15**

I en ruter finnes følgende ruter i rutingtabellen:

00001010.00000001.00000010.00000000/23	link 1
00001010.00000001.00000010.00000000/24	link 2
00001010.00000001.00000010.00000000/25	link 3
00001010.00000001.00000010.00000000/16	link 4
Alle andre adresser	link 5

Anta at ruten mottar to datagram med følgende mottakeradresser:

A: 00001010.00000001.00000001.10000000

B: 00001010.00000001.00000011.10000000

**På hvilke linker skal disse sendes videre? (3 poeng)**

A: link

B: link

Maks poeng: 3

**17 DAT204\_H16\_16**

IP adressen 00001010.00000001.00000010.10000000 kan skrives på desimalform som:

(2 poeng)





Maks poeng: 2

**18 DAT204\_H16\_17**

**Sett inn rutingalgoritmen som passer med uttrykket. (5 poeng)**

▼ benytter Dijkstras algoritme for å finne korteste sti.

▼ er dominert av rutingpolicyer istedenfor å fokusere på å finne stien med lavest kostnad i nettet.

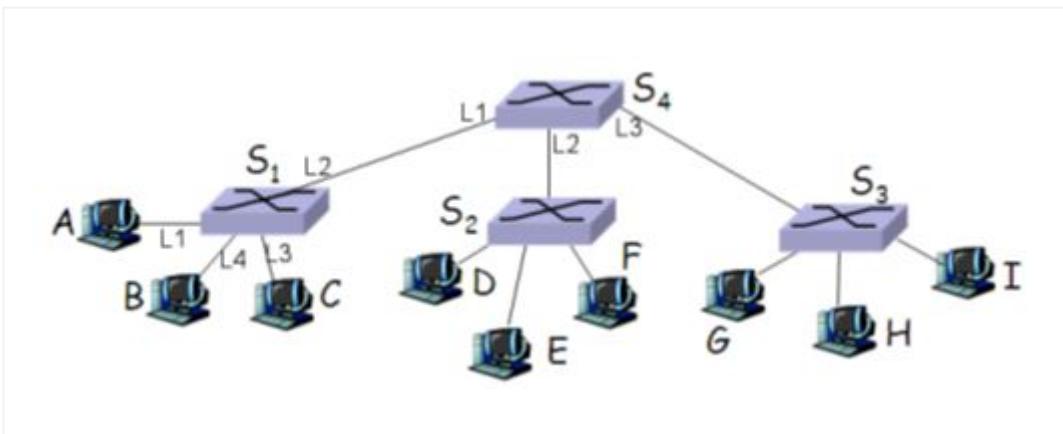
▼ utveksler informasjon om endrede rutingtabeller med naboruterne.

▼ annonserer et subnett til alle autonome systemer på Internett.

▼ utveksler informasjon om naboruterne med alle ruterne i nettet.

Maks poeng: 5

## 19 DAT204\_H16\_18



Figuren over viser et nettverk med fire selvlærende ethernetsvitsjer og 9 vertsmaskiner (hosts). Svitsjene er nettopp skrudd på og svitsjetabellene er tomme. (5 poeng totalt)

**Anta at vi sender følgende rammer:**

A til B

E til I

H til A

**Deretter A til E. Hvilke vertsmaskiner (hosts) mottar denne rammen?**

**Hvordan vil svitsjetabellen i S<sub>1</sub> se ut etter denne sekvensen?**

Svitsjetabell (switch table) for S<sub>1</sub>

Adresse	Grensesnitt/interface
A	▼
E	▼
▼	▼

Maks poeng: 5

## 20 DAT204\_H16\_19

**Plasser riktig multippel aksess kontroll protokoll på rett sted. (5 poeng)**

Denne protokollen deler hver ramme inn i N tidsluker (time slots), der forskjellige tidsluker tilordnes til forskjellige forbindelser:

Denne protokollen deler frekvensbåndet inn i forskjellige kanaler der hvert frekvensbånd kan tilordnes en forbindelse:

Denne protokollen multipliserer hvert bit med en mye raskere "chipping code" for å redusere problemet med interferens i trådløse systemer:

Denne protokollen brukes i trådløse nett (IEEE 802.11) for å unngå problemet med skjulte terminaler:

Denne protokollen brukes i Ethernett der enheten lytter før den sender:

Maks poeng: 5

## 21 DAT2016\_H16\_20

**Hvilke teknikker må til for at ruterne i et IP basert nettverk skal kunne tilby garantert tjenestekvalitet? (6 poeng)**

Hvordan kan første ruter merke pakkene slik at den kan skille mellom forskjellige trafikklasser?

Hvordan kan ruterne garantere at en trafikkasse får en garantert minimumsbåndbredde?

Hvordan kan ruterne begrense størrelsen på datautbrudd (burst size) for en gitt forbindelse for å redusere latenstiden og tidsforsinkelsen i nettet?

Hvordan kan man sørge for at ressursene i nettet ikke blir overbooket?

Hvordan kan man håndheve at ikke en vertsmaskin tilegner flere ressurser enn det den har krav på?

Hvordan kan man sikre at man velger en bestemt rute gjennom nettet?

Maks poeng: 6

**22 DAT204\_H16\_21**

**Setningene under beskriver trådløse nettverk. Fyll inn rett uttrykk. (6 poeng)**

Et aksesspunkt sammen med vertsmaskinene som kommuniserer via dette aksesspunktet former til sammen:

Problemet med skjulte terminaler kan løses ved å bruke:

Et aksesspunkt annonserer at et Wifi nettverk finnes via:

Fysiske hindringer eller signal fading kan føre til:

Et aksesspunkt identifiseres via dets:

Hvis en 802.11 node merker at kanalen er opptatt, så vil den benytte:

Maks poeng: 6

**23 DAT204\_H16\_22**

Anta at et analogt audiosignal samples 20000 ganger i sekundet og at hver sample er kvantifisert i 1024 nivåer (2 poeng).

**Hvor mange bits er hver sample?**

**Hva blir den resulterende bitraten av PCM audiosignalet i bits/s?**

Maks poeng: 2

**24 DAT204\_H16\_23**

Bjørnøya meteorologiske stasjon har bredbånd med 20 Mbit/s hastighet for nedlasting og 4 Mbit/s for opplasting som går via en satellittlink. Satellitten er 39 000 km fra Norge og lyshastigheten er 300 000 km/s. Et datagram sendes over denne satellittlinken og behandles av flere rutere og svitsjer på sin vei til mottakeren. Ruterne og svitsjene før og etter satellittlinken er i et fibernett med høy kapasitet og er ikke overbelastet. (10 poeng)

**Hvilken type forsinkelse vil sannsynligvis gi det største bidraget til den totale tidsforsinkelsen?**



Anta at datagrammet i oppgaven over pakkes inn i en ramme på 1500 bytes. Hvor stor er tidsforsinkelsen i sekunder fra rammen sendes på satellittlinken fra Bjørnøya og til den har blitt mottatt på fastlandet? Avrund svaret til to desimaler.

Hvor stor er tidsforsinkelsen på responsmeldingen fra fastlandet i sekunder, dersom datagrammet er like stort som i forrige delspørsmål? Avrund svaret til to desimaler.

Hvor stor blir den minimale rundturforsinkelsen i sekunder for datagrammer på denne linken? Avrund svaret til to desimaler

Det gjennomføres en IP telefonisamtale over satellittlinken der avspillingsbufferet for å jevne ut jitter gir en tilleggsforsinkelse på 140 ms. Er ende til ende tidsforsinkelsen på denne linken akseptabel for en IP telefonisamtale ut fra tjenestekvalitetskravene til slike samtaler?

- Ja
- Nei

Maks poeng: 10

## 25 DAT204\_H16\_Comments

Her kan du beskrive antagelser og kommentarer til besvarelsen din. Disse kommentarene gir ikke poeng i seg selv, men vil kunne påvirke vurderingen av kommenterte oppgaver. (maks 500 ord)

**Beskriv antagelser og kommentarer til oppgavene her.**

Format | | | | |

| | |

Words: 0/500

Maks poeng: 0