NTNU

Department of Information Security and Communication Technology

Examination paper for TTM4100 - Communication - Services and Networks.

Academic contact during examination: Tu Dac Ho

Phone: 9300 6185

Academic contact present at the exam location: YES (0900 - 1300)

Examination date: 08.05.2024

Examination time (from-to): 0900 - 1300

Permitted examination support material: D (No printed or hand-written support material is allowed. A specific basic calculator is allowed).

Other information:

- **The exam consists of two parts:**
  - **Part I: Assignment text**
  - **Part II: Own answer sheets.**

Language: English

Number of pages for Part I (front page/regulation excluded): 10

Number of pages enclosed for Part II: 11

Informasjon om trykking av eksamensoppgave
Originalen er:
1-sidig ☐ **2-sidig** √
sort/hvit ☐ **farger** ☐
skal ha flervalgskjema ☐

Checked by:

_____

Date Signature

Multiple Choice Questions

Regler/Rules/Reglar:

B: BOKMÅL	E: ENGLISH	N: NYNORSK
Maksimal poengsum er 100 poeng. Oppgavesettet består av 2 deler: ● Del I, problemspesifikasjonene - denne delen. ● Del II, svarsidene, inneholder svarbokser for flervalgsspørsmål og "skriftlig tekst"-oppgaver. Del II inkluderer også 3 sider for kommentarer relatert til formelle spørsmål om del I eller del II. Disse sidene kan også brukes til "skriftlig tekst"-svar. Del II skal leveres som ditt svar. To eksemplarer av del II deles ut. Kun ett eksemplar skal leveres. Kandidatnummeret skal stå på alle svarsidene. Ikke skriv utenfor feltene i boksen. Bruk en blå eller svart penn, ikke en blyant. **Skriftlige tekstoppgaver** skal besvares innenfor den tildelte boksen i del II. **Flervalgsspørsmål** skal besvares ved å angi dine valg i den tildelte boksen i del II. For hvert flervalgsspørsmål kan det være ett eller flere riktige valg. For flervalgsspørsmål: Poeng = Maks {(antall riktige valg – minuspoeng), 0}*x - 1 feil gir ingen minuspoeng; - i > 1 feil gir (i-1)*0,5 minuspoeng. Denne avbildningen mellom feilvalg og minuspoeng lar deg svare feil én gang uten å bli straffet. Et manglende riktig valg for et flervalgsspørsmål regnes ikke med i feil valg. Verdien av x bestemmes som (totalt poeng for flervalgsspørsmål)/ (totalt antall riktige valg).	The maximum score is 100 points. The problem set consists of 2 parts: ● Part I, the problem specifications - this part. ● Part II, the answer pages, includes answer boxes for multiple-choice questions and “written text” problems. Part II also includes 3 pages for comments related to *formal issues* about Part I or Part II. These pages may also be used for “written text” answers. Part II shall be delivered as your answer. Two copies of Part II are handed out. Only one copy shall be delivered. The candidate number should be written on all answer pages. Do not write outside the box fields. Use a blue or black pen, not a pencil. **Written text** problems shall be answered within the assigned box of Part II. **Multiple-choice** questions shall be answered by providing your choices within the assigned box of Part II. For each multiple-choice question, there may be one or more correct choices. For multiple-choice questions as whole: Points = Max {(number of correct choices – discount points), 0}*x - 1 incorrect gives no discount; - i > 1 incorrect gives (i-1)*0,5 discount points. This mapping between incorrect choices and discount points allows you to answer wrong once without being punished. A missing correct choice for a multiple-choice question is not counted in incorrect choices. *The value of x is decided as (total points, i.e. 65, for multiple choice questions)/ (total number of correct choices, i.e. 45.)*	Maksimal poengsum er 100 poeng. Oppgåvesettet består av 2 delar: ● Del I, problemspesifikasjonane - denne delen. ● Del II, svarsidene, inneheld svarboksar for fleirvalspørsmål og "skriftleg tekst"-oppgåver. Del II inkluderer også 3 sider for kommentarar relatert til formelle spørsmål om del I eller del II. Desse sidene kan også brukast til "skriftleg tekst"-svar. Del II skal leverast som svaret ditt. To eksemplar av del II blir delt ut. Berre eitt eksemplar skal leverast. Kandidatnummeret skal stå på alle svarsidene. Ikkje skriv utanfor felta i boksen. Bruk ein blå eller svart penn, ikkje ein blyant. **Skriftlege tekstoppgåver** skal svarast på innanfor den tildelte boksen i del II. **Fleirvalspørsmål** skal svarast på ved å angi dine val i den tildelte boksen i del II. For kvart fleirvalspørsmål kan det vera eitt eller fleire rette val. For fleirvalspørsmål: Poeng = Maks {(talet på rette val – minuspoeng), 0}*x - 1 feil gir ingen minuspoeng; - i > 1 feil gir (i-1)*0,5 minuspoeng. Denne avbildinga mellom feilval og minuspoeng lèt deg svara feil éin gong utan å bli straffa. Eit manglande rett val for eit fleirvalspørsmål blir ikkje rekna med i feil val.Verdien av x blir bestemd som (totalt poeng for fleirvalspørsmål)/ (det samla talet rette val).

Q1. (There are 45 correct choices out of 128) [65 points]

Q1.1 General (Chapter 1)

Q1.1.1 Circuit switching and packet switching have many differences. Which of the following is/are correct?

a) *While a circuit-switched network can guarantee a certain amount of end-to-end bandwidth for the duration of a call, typically packet-switched networks cannot.*
b) *Most packet-switched networks today (including the Internet) can make end-to-end guarantees for bandwidth.*
c) *Typically, the delay variation among packets/messages in a circuit-switched network is smaller than that in a packet-switched network.*
d) *The costs for dedicated resources in packet-switched network are usually higher than the costs for resources in circuit-switched network.*
e) *In circuit-switched networks, the bandwidth is shared among the users and allocated only when data needs to be transmitted. It has a better bandwidth efficiency than in packet-switched networks.*

Q1.1.2 Suppose there is exactly one packet switch between a sending host and a receiving host. The transmission rates between the sending host and the switch and between the switch and the receiving host are *R1* and *R2*, respectively. If the switch uses store-and-forward packet switching, what is the total end-to-end delay to send a packet of length *L* when queuing, propagation delay, and processing delay are ignored?

a) *L/(R1+R2)*
b) *L/R1+L/R2*
c) *2L/Max {R1, R2}*
d) *2L/Min {R1, R2}*
e) *None of the above*

Q1.1.3 Consider a client and a server connected through one router. Assume the router can start transmitting an incoming packet after receiving its first 80 bytes instead of waiting for the whole packet. Suppose that the link rates are 1000 byte/s and that the client transmits one packet with a size of 3000 bytes to the server. What is correct for the end-to-end delay?

a) *3,808s*
b) *3,800s*
c) *3,008s*
d) *3,080s*
e) *None of the above*

Q1.1.4 Protocol Layering is commonly used in computer networks because:

a) *It prevents network functionalities to be divided into separate layers, each with a specific purpose.*
b) *Encapsulation is the most efficient way to transmit data.*
c) *It provides a simple design for implementation and maintenance but more complication in network developments.*
d) *It keeps networks structured and enables them to communicate faster.*
e) *Protocol layering can accommodate future enhancements and changes.*

Q.1.1.5 Consider sending *P* packets through a packet-switched network from source to destination. There are *N* store-and-forward routers between the source and the destination. Each packet has a length of *L* bits.

Assume that all of the links in the network (e.g., the links between the source and the router, between the routers, and between the router and the destination) have the same transmission rate of *R* bps. What is the minimum end-to-end delay of sending P such packets back-to-back over the network? Ignore queuing, processing, and propagation delays.

*a) P*N*L/R*
*b) (N+P-1)*L/R*
c) P(N+1)*L/R*
*d) (N+P+2)*L/R*
e) None of the above.

Q1.2 Application Layer and Transport Layer (Chapters 2 & 3)

Q1.2.1 Which of the following protocols is/are **not** an Application-Layer protocol?

a) Telnet (User Data Protocol)
b) TDM (Time Division Multiplexing)
c) SMTP (Simple Mail Transfer Protocol)
d) HTTP (Hypertext Transfer Protocol)
e) IMAP (Internet Message Access Protocol)

Q1.2.2 Web caching is normally set in between the clients (PCs in a university network) and an original server (e.g., a commercial website server). Which of the following statements is/are correct about Web caching?

a) It does not reduce the average delay for all objects.
b) Averagely, it reduces the delay only for the objects that are cached.
c) Potentially, it can reduce the average delay for all the objects, even objects that are not cached.
d) It increases the average traffic on the links (implies the links between a client and the original server)
e) It has a storage on its own disk, and it prevents from keeping copies of recently requested objects in this storage.

Q1.2.3 Suppose a process in Host D has a UDP socket with a predefined port. Suppose Host A, Host B, and Host C each wants to send a UDP segment to Host C. What is minimal number of sockets required for sending those segments from Host A, B, and C to Host D?

a) One socket
b) Two sockets
c) Three sockets
d) More than three sockets
e) None of the above

Q1.2.4 Which of the following statement(s) is/are true?

a) SMTP uses UDP as its underlying transport protocol.
b) Both UDP and TCP do not provide reliable data transfer service.
c) UDP is a connection-oriented protocol.
d) Internet Telephony application (e.g. SIP) can use UDP or TCP.
e) FDM (Frequency Division Multiplexing) requires more sophisticated analog hardware to shift

signal into appropriate frequency bands than what TDM (Time Division Multiplexing) does.

Q1.2.5 Consider distributing a file of F=10 Gbits to N=100 peers using ***Client-Server*** architecture. The server has an upload rate of u_s=1Gbps. Each peer has a download rate of d_i=200Mbps. What is the minimum time to distribute this file to all the peers:

a) 50s
b) 5000s
c) 500s
d) 1000s
e) None of the above

Q1.3 Network Layer (Chapters 4&5)

Q1.3.1 Assign network addresses from 214.97.250/23 to a subnet that should have enough addresses to support 250 interfaces. The assignment takes the form a.b.c/x. Which of the following is/are possible correct subnet(s)?

a) 214.97.245/24
b) 214.97.251/24
c) 214.97.253/24
d) 214.97.254/24
e) 214.97.254/25

Q1.3.2 About DHCP (Dynamic Host Configuration Protocol), which of the following statement(s) is/are **false**?

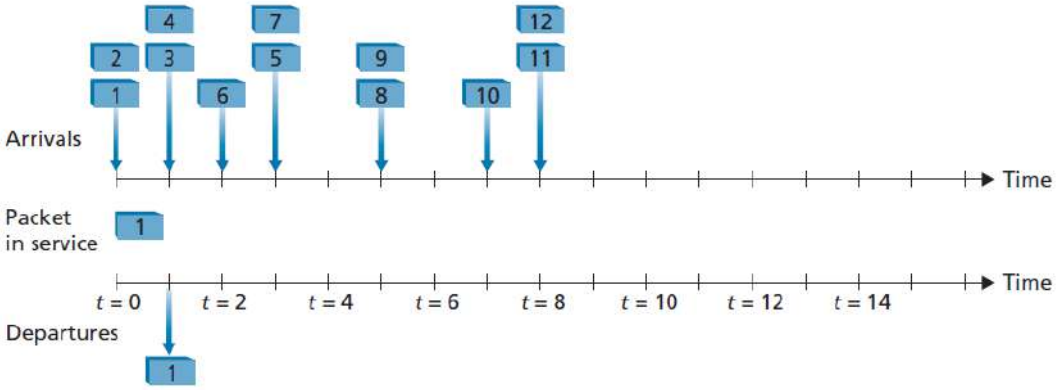
a) When an internet host arrives, it implements 4-step process with a DHCP server for acquiring a new IP address.
b) DHCP uses TCP (Transmission Control Protocol) as its transport protocol.
c) DHCP provides dynamic IP address assignment to network clients.
d) DHCP is primarily used for routing data packets between networks.
e) DHCP servers can offer additional configuration parameters such as DNS server addresses and subnet masks.

Q1.3.3 What is/are **false** about the Internet Control Message Protocol (ICMP)?

a) ICMP is not primarily used in the network layer.
b) ICMP is a supporting protocol in the Internet protocol suite.
c) ICMP provides functions like error reporting and network diagnosis.
d) ICMP messages are used not only for signaling error conditions.
e) ICMP is a transport protocol used for data exchange between devices on the network.

Q1.3.4 In FIFO (First Input First Output) service below, the upper timeline shows arrival times of packets, and the lower timeline shows the start of timeslots where a packet is transmitted. Queuing delay for a packet is the period between its arrival time and the beginning of the slot in which the packet is transmitted. One example, packet 1 will be transmitted at the time of t=1, hence its delay is also 1. What is the average delay

for the next three packets (packets 2, 3, and 4)?



What is the average of this delay for the next 3 packets (packets 2, 3,4)?

a) 8/3s

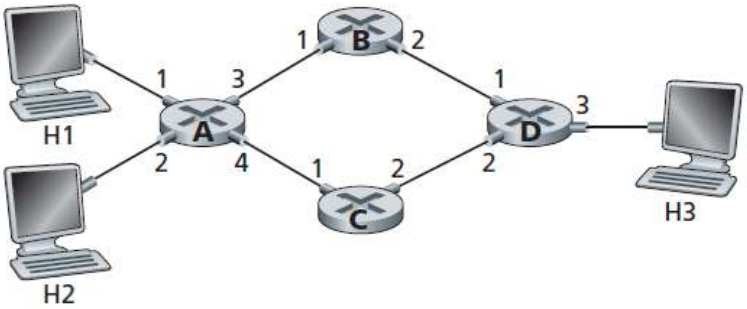
b) 7/3s

c) 2s

d) 5/3s

e) Nove of the above

Q1.3.5 Consider the network below. Which of the following statements is/are true?



a) It is possible to configure forwarding table in router A, such that all traffic destined to host H3 is forwarded through interface 3.

b) It is not possible to configure forwarding table in router A, such that all traffic destined to host H3 is forwarded through interface 3.

c) It is possible to configure a forwarding table in router A, such that all traffic from H1 destined to host H3 is forwarded through interface 3, while all traffic from H2 destined to host H3 is forwarded through interface 4.

d) It is not possible to configure a forwarding table in router A, such that all traffic from H1 destined to host H3 is forwarded through interface 3, while all traffic from H2 destined to host H3 is forwarded through interface 4

e) None of the above

Q1.4 Link Layer, Wireless and Mobile Networks (Chapters 6&7)

Q1.4.1 What is/are **false** when comparing between switches and routers?

a) Both routers and switches are the connecting devices in networking.

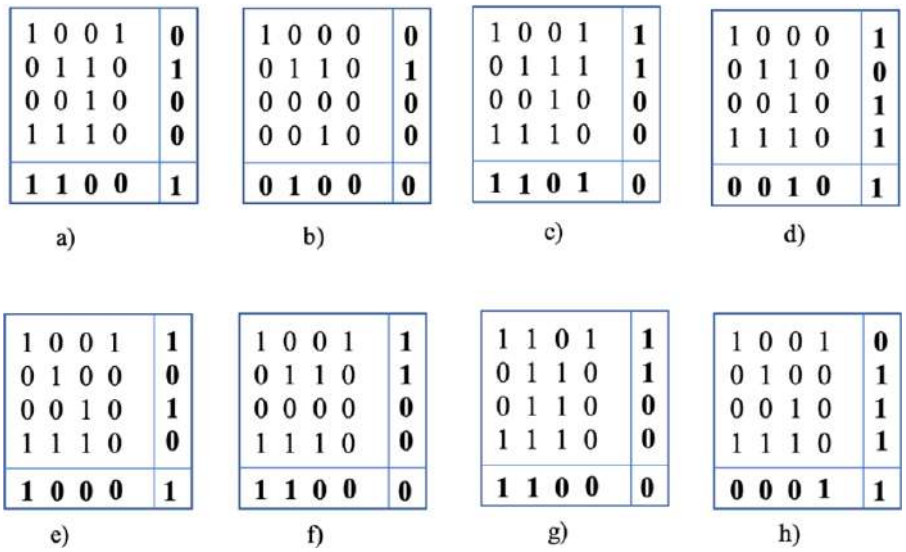
b) *Routers operate at the Data link layer and switches operate at the Network layer.*

c) *Switches operate at the Data link layer and routers operate at the Network layer.*

d) *Switches connect various networks together while a router connects devices within a network.*

e) *In operation, routers rely on IP addresses while switches rely on MAC addresses.*

Q1.4.2 Which of the following alternatives show(s) correct implementation(s) of a two- dimensional **even** parity scheme?



Q1.4.3 About wireless physical-layer characteristics, which of the following statement(s) is/are correct regarding the relations between SNR (Signal-to-noise ratio), BER (Bit Error Rate), and Modulation schemes?

a) *For a given a modulation scheme, the lower the SNR, the higher the BER.*

b) *For a given modulation scheme, the lower the SNR, the lower the BER.*

c) *For a given SNR, a modulation technique with a higher bit transmission rate has a lower BER.*

d) *For a given SNR, a modulation technique with a higher bit transmission rate has a higher BER.*

e) *None of the above is correct.*

Q1.4.4 What is/are correct about CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protocol and RTS (Request to Send)/CTS (Clear to Send) message exchange?

a) *Hidden node issue still physically happens with systems use CSMA/CA*

b) *In CSMA/CA, when a node wants to transmit, it sends a RTS to the AP (Access Point). The AP responds with a CTS, granting permission for the node to transmit*

c) *During the RTS/CTS exchange, hidden nodes can not overhear these frames.*

d) *The RTS/CTS mechanism completely solves the exposed node problem.*

e) *The RTS/CTS mechanism is used in CSMA/CA to improve channel access.*

Q.1.4.5 This question considers two access protocols: ALOHA (pure ALOHA) and slotted ALOHA. What of the following statements is/are true?

a) *Pure ALOHA has lower efficiency compared to slotted ALOHA.*
b) *Maximum efficiency achievable in slotted ALOHA is two times higher than that in pure ALOHA.*
c) *Slotted ALOHA reduces the number of collisions compared to pure ALOHA.*
d) *In Slotted ALOHA, any station can transmit data at any time without synchronization.*
e) *In pure ALOHA, stations must wait for the beginning of the next time slot to transmit data.*

Q1.5 Security and Multimedia Networking (Chapter 8, and Edition 7 - Chapter 9)

Q1.5.1 Which of the following are desirable properties of secure communication:

a) *Network reliability.*
b) *Confidentiality*
c) *Message integrity.*
d) *Operational security*
e) *High bandwidth to transmit the message quickly.*

Q1.5.2 Suppose *N* people want to communicate with each other using symmetric key encryption. All communication between any two people is visible to all other people in this group and no other person in this group should be able to decode their communication. How many keys are required in the system as a whole?

a) *N*N*
b) *2*N-1*
c) *N*(N-1)*
d) *N*(N-1)/2*
e) *None of the above*

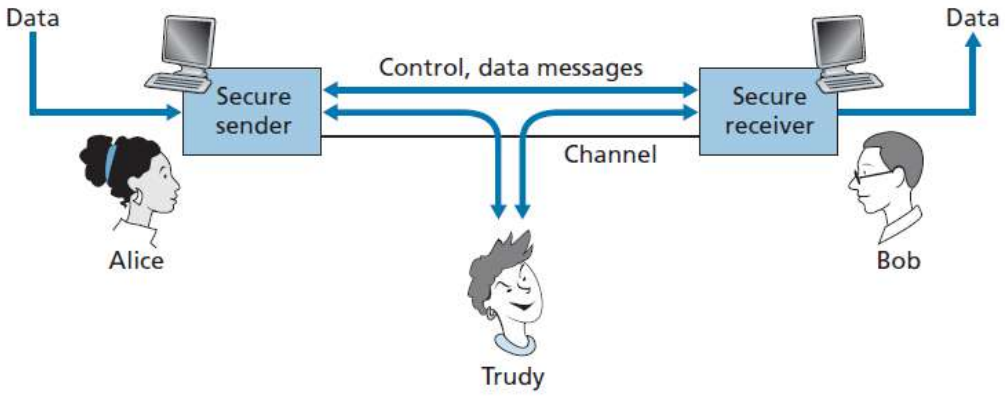
Q1.5.3 For message integrity, which of the following statement(s) is/are correct?

a) *Message integrity is the property that the identity of the sender can be confirmed to be who or what they claim to be.*
b) *Message integrity is the property that the receiver can detect whether the message sent was altered in transit.*
c) *Both checksumming and hashing techniques may be used.*
d) *Generally, a hash provides a better message integrity check than a checksum.*
e) *To ensure message integrity, the transport layer protocol used to communication the message has to be TCP.*

Q1.5.4 In video streaming applications, HTTP streaming (over TCP) is more popular than UDP streaming. The major reasons include:

a) *UDP is connectionless.*
b) *UDP lacks retransmission, ordering, and error-checking mechanism result in higher error rate.*
c) *UDP streaming lacks handshakes and acknowledgement results in lower latency.*
d) *Many firewalls are often configured to block most UDP traffic but to allow most HTTP traffic.*
e) *None of the above*

Q1.5.5 Considering information transmission between Alice and Bob through a network with the existence of an intruder (Trudy). Choose which of these statements is/are correct regarding what kinds of information the intruder can access and what kinds of action can be taken:



a) *Sniffing and recording control messages on the channel*
b) *Recording data messages on the channel*
c) *Modifying or insertion of messages*
d) *Deletion of message or message content*
e) *None of the above*

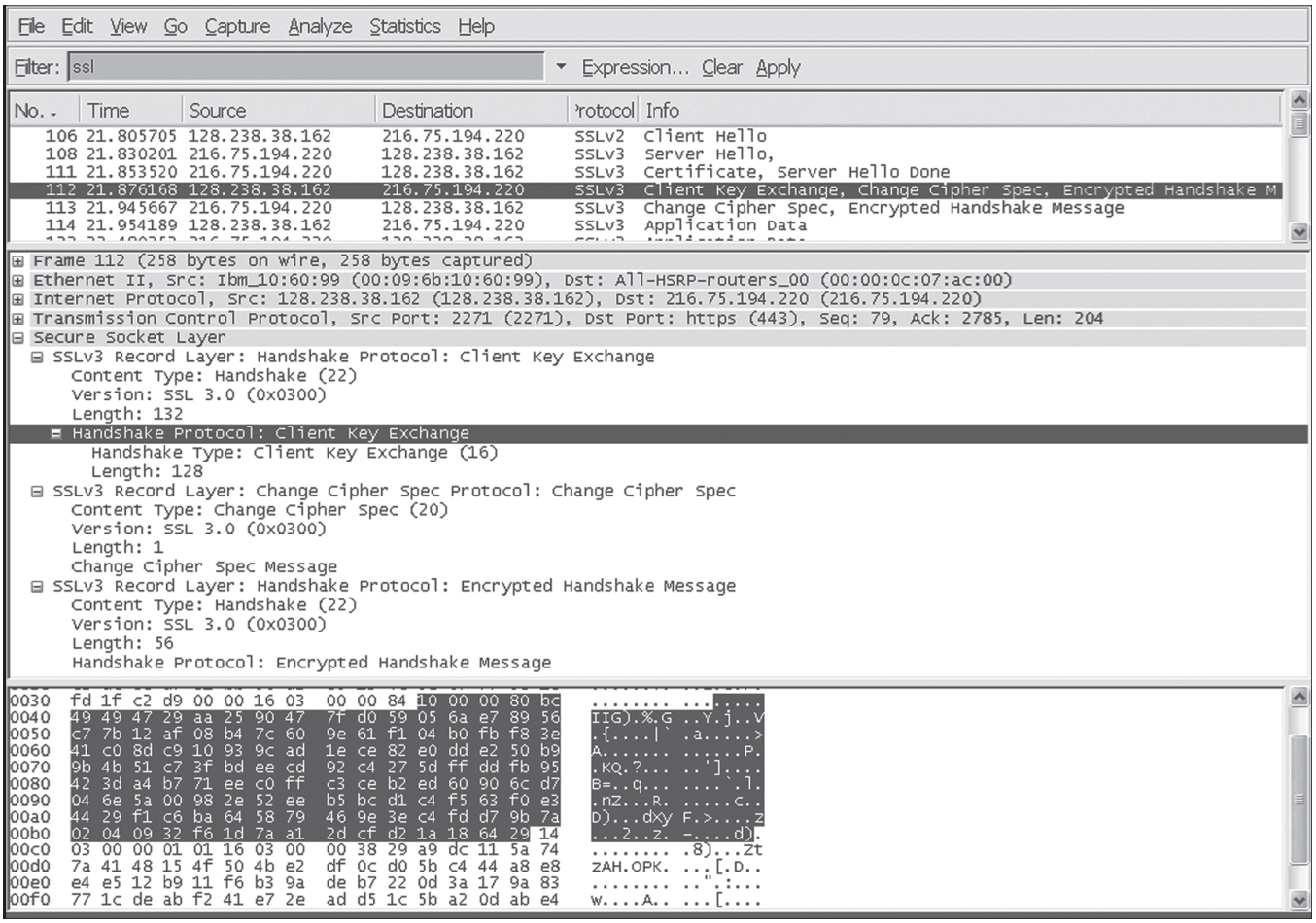
Ordinary Questions (Q2-Q6) [35 points]

Q2: Flow control [6 points]

There are two hosts, Host A and B are directly connected with a 10 Gbps link. There is one TCP connection between the two hosts, and Host A is sending to Host B an enormous file over this connection. Host A can send its application data into its TCP socket at a rate as high as 1 Gbps, but Host B can read out of its TCP receive buffer at a maximum rate of 600 Mbps.

Describe the effect of TCP flow control in this TCP connection.

Q3. Consider the Wireshark output below for a portion of an SSL (Secured Socket Layer) session. Answer these questions [5 points]



Q3.1 Was Wireshark packet 112 sent by the client or server?

Q3.2 What is the server's IP address and port number?

Q3.3 Assuming no loss and no retransmissions, what will be the sequence number of the next TCP segment sent by the client? Explain how you got this number.

Q3.4 How many SSL records does Wireshark packet 112 contain?

Q3.5 Does packet 112 contain a Master Secret or an Encrypted Master Secret or neither?

Q.4 IP addressing [8 points]

An IP address consists of a subnet part and a host part. To determine which the subnet an IP address belongs to, you must know the subnet mask. Answer these questions:

Q.4.1. How to find out the subnet based on the IP address and the subnet mask?

Q.4.2 Given an IP address of 192.168.1.108 and the subnet mask /30 (255.255.255.252), what is the subnet address? Justify your answer.

Q.4.3 Given an IP address of 192.168.2.108 and the subnet mask /29 (255.255.255.248), what is the subnet address? Justify your answer.

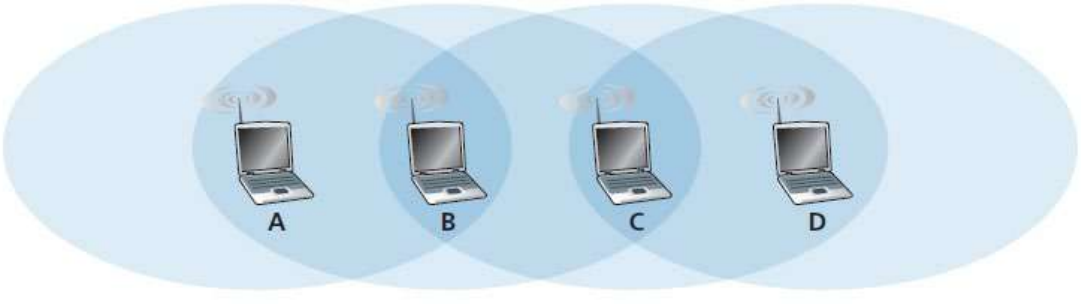
Q.4.4 Given an IP address of 192.168.3.108 and the subnet mask /28 (255.255.255.240), what is the subnet address? Justify your answer.

Q.5 Multiple Access Mechanism [12 points]

In the Figure below, there are four wireless nodes, A, B, C, and D. The radio coverages of these nodes are shown as the shaded ovals; all nodes share the same frequency. When A transmits, it can only be heard/received by B; when B transmits, both A and C can hear/ receive from B; when C transmits, both B and D can hear/receive from C; when D transmits, only C can hear/receive from D. Suppose now that each node has an infinite supply of messages that it wants to send to each of the other nodes. If a message's destination is not an immediate neighbor, then the message must be relayed via intermediate node(s).

Time is slotted and it take exactly one time slot for one message transmission. During a slot, a node can do one of the following: (*i*) send a message, (*ii*) receive a message, (*iii*) remain silent. As always, if a node hears two or more simultaneous transmissions, a collision occurs and none of the transmitted messages are received successfully. Assume that when one message is sent, it will be received correctly by other nodes within the transmission radius of the sender if no collision occurred at those nodes.

Assume a message has a length of L (bits) and a time slot of T (second). Provide answers to these questions:



Q.5.1 Suppose now that A sends messages to B, and D sends messages to C.
What is the combined maximum rate at which data messages can flow from A to B and from D to C?
Justify your answer.

Q.5.2 Suppose now that A sends messages to B, and C sends messages to D.
What is the combined maximum rate at which data messages can flow from A to B and from C to D?
Justify your answer.

Q.5.3. In this scenario, suppose that for every data message sent from source to destination, the destination will send an ACK message back to the source (e.g., as in TCP). Also suppose that each ACK message takes up one time slot.

Q.5.3.1 Repeat the question Q.5.1 for this scenario.

Q.5.3.2 Repeat the question Q.5.2. for this scenario.

Q.6 Answer following questions relate to DNS (Domain name service) [4 points]

Q.6.1 Describe the format of a Resource Record (RR) in DNS.

Q.6.2 What kind of information can be communicated to a client when it sends a DNS query?

NTNU

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgave i

TTM4100 KOMMUNIKASJON – TJENESTER OG NETT

Faglig kontakt under eksamen: Tu Dac Ho

Tlf.: 9300 6185

Faglig kontakt møter i eksamenslokalet: JA (0900 - 1300)

Eksamensdato: 08.05.2024

Eksamenstid (fra-til): 0900-1300

Hjelpemiddelkode/Tillatte hjelpemidler: D (Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkelkalkulator tillatt.)

Annen informasjon:

- **Eksamen består av to deler**
  - **Del I: Oppgavetekst**
  - **Del II: Egne svarark**

Målform/språk: Norsk

Antall sider (Del I uten forside/regler side): 10

Antall sider vedlegg (Del II): 11

Informasjon om trykking av eksamensoppgave
Originalen (Del I) er:
1-sidig ☐ **2-sidig** √
sort/hvit ☐ **farger** ☐
skal ha flervalgskjema ☐

Kontrollert av:

Dato Sign

Merk! Studenter finner sensur i Studentweb. Har du spørsmål om din sensur må du kontakte instituttet ditt. Eksamenskontoret vil ikke kunne svare på slike spørsmål.

Regler/Rules/Reglar:

B: BOKMÅL	E: ENGLISH	N: NYNORSK
Maksimal poengsum er 100 poeng. Oppgavesettet består av 2 deler: ● Del I, problemspesifikasjonene - denne delen. ● Del II, svarsidene, inneholder svarbokser for flervalgsspørsmål og "skriftlig tekst"-oppgaver. Del II inkluderer også 3 sider for kommentarer relatert til formelle spørsmål om del I eller del II. Disse sidene kan også brukes til "skriftlig tekst"-svar. Del II skal leveres som ditt svar. To eksemplarer av del II deles ut. Kun ett eksemplar skal leveres. Kandidatnummeret skal stå på alle svarsidene. Ikke skriv utenfor feltene i boksen. Bruk en blå eller svart penn, ikke en blyant. **Skriftlige tekstoppgaver** skal besvares innenfor den tildelte boksen i del II. **Flervalgsspørsmål** skal besvares ved å angi dine valg i den tildelte boksen i del II. For hvert flervalgsspørsmål kan det være ett eller flere riktige valg. For flervalgsspørsmål: Poeng = Maks{(antall riktige valg – minuspoeng), 0}*x - 1 feil gir ingen minuspoeng; - i > 1 feil gir (i-1)*0,5 minuspoeng. Denne avbildningen mellom feilvalg og minuspoeng lar deg svare feil én gang uten å bli straffet. Et manglende riktig valg for et flervalgsspørsmål regnes ikke med i feil valg. Verdien av x bestemmes som (totalt poeng for flervalgsspørsmål)/ (totalt antall riktige valg).	The maximum score is 100 points. The problem set consists of 2 parts: ● Part I, the problem specifications - this part. ● Part II, the answer pages, includes answer boxes for multiple-choice questions and "written text" problems. Part II also includes 3 pages for comments related to *formal issues* about Part I or Part II. These pages may also be used for "written text" answers. Part II shall be delivered as your answer. Two copies of Part II are handed out. Only one copy shall be delivered. The candidate number should be written on all answer pages. Do not write outside the box fields. Use a blue or black pen, not a pencil. **Written text** problems shall be answered within the assigned box of Part II. **Multiple-choice** questions shall be answered by providing your choices within the assigned box of Part II. For each multiple-choice question, there may be one or more correct choices. For multiple-choice questions as whole: Points = Max{(number of correct choices – discount points), 0}*x - 1 incorrect gives no discount; - i > 1 incorrect gives (i-1)*0,5 discount points. This mapping between incorrect choices and discount points allows you to answer wrong once without being punished. A missing correct choice for a multiple-choice question is not counted in incorrect choices. *The value of x is decided as (total points, i.e. 65, for multiple choice questions)/ (total number of correct choices, i.e. 45.)*	Maksimal poengsum er 100 poeng. Oppgåvesettet består av 2 delar: ● Del I, problemspesifikasjonane - denne delen. ● Del II, svarsidene, inneheld svarboksar for fleirvalspørsmål og "skriftleg tekst"-oppgåver. Del II inkluderer også 3 sider for kommentarar relatert til formelle spørsmål om del I eller del II. Desse sidene kan også brukast til "skriftleg tekst"-svar. Del II skal leverast som svaret ditt. To eksemplar av del II blir delt ut. Berre eitt eksemplar skal leverast. Kandidatnummeret skal stå på alle svarsidene. Ikkje skriv utanfor felta i boksen. Bruk ein blå eller svart penn, ikkje ein blyant. **Skriftlege tekstoppgåver** skal svarast på innanfor den tildelte boksen i del II. **Fleirvalspørsmål** skal svarast på ved å angi dine val i den tildelte boksen i del II. For kvart fleirvalspørsmål kan det vera eitt eller fleire rette val. For fleirvalspørsmål: Poeng = Maks{(talet på rette val – minuspoeng), 0}*x - 1 feil gir ingen minuspoeng; - i > 1 feil gir (i-1)*0,5 minuspoeng. Denne avbildinga mellom feilval og minuspoeng lèt deg svara feil éin gong utan å bli straffa. Eit manglande rett val for eit fleirvalspørsmål blir ikkje rekna med i feil val.Verdien av x blir bestemd som (totalt poeng for fleirvalspørsmål)/ (det samla talet rette val).

Flervalgspørsmål

Q1. (There are 45 correct choices out of 128) [65 poeng]

Q1.1 Generelt (Kapittel 1)

Q1.1.1 Linjesvitsjing (Circuit switching) og pakkesvitsjing (packet switching) har mange forskjeller. Hvilke(t) av disse utsagnene stemmer?

a) Et linjesvitsjet nettverk kan som regel garantere for en viss båndbredde i løpet av en ende-til-ende tilkobling, noe et pakkesvitsjet nettverk ikke kan.

b) De fleste pakkesvitsjede nettverk i dag (inkludert Internett) kan gi garantier for båndbredde fra ende til ende.

c) Variasjonen i forsinkelse blant pakker/meldinger i et linjesvitsjet nettverk er vanligvis mindre enn i et pakkesvitsjet nettverk.

d) Kostnadene for dedikerte ressurser i et pakkesvitsjet nettverk er vanligvis høyere enn kostnadene for ressurser i et linjesvitsjet nettverk.

e) I linjesvitsjede nettverk deles båndbredden blant brukerne og tildeles bare når data må overføres. Det har bedre båndbreddeeffektivitet enn i pakkesvitsjede nettverk.

Q1.1.2 Anta at det er nøyaktig én pakkesvitsj mellom en sendende vert og en mottakende vert. Overføringshastighetene mellom den sendende verten og svitsjen, og mellom svitsjen og den mottakende verten, er henholdsvis R1 og R2. Hvis svitsjen bruker lagre-og-send-pakkesvitsjing (store-and-forward packet switching), hva er den totale ende-til-ende forsinkelsen for å sende en pakke av lengde L når køforsinkelse, propagasjonsforsinkelse og prosesseringsforsinkelse ignoreres?

a) L/(R1+R2)

b) L/R1+L/R2

c) 2L/Max {R1, R2}

d) 2L/Min {R1, R2}

e) Ingen av de nevnte

Q1.1.3 Anta at en klient og en server kobles sammen gjennom en router. Anta at routeren kan begynne å sende en innkommende pakke etter å ha mottatt de første 80 byte, i stedet for å vente på hele pakken. Anta at koblingshastighetene er 1000 byte/s, og at klienten sender én pakke med en størrelse på 3000 byte til serveren. Hva blir ende-til-ende forsinkelsen?

a) 3,808s

b) 3,800s

c) 3,008s

d) 3,080s

e) Ingen av de nevnte

Q1.1.4 Protokoll-lagdeling (Protocol layering) brukes vanligvis i datanettverk fordi:

a) Den hindrer at nettverksfunksjonaliteter deles opp i separate lag, hver med et spesifikt formål.

b) Innkapsling er den mest effektive måten å overføre data på.

c) Det gir et enkelt design for implementering og vedlikehold, men mer komplikasjon i nettverksutvikling.

d) Det holder nettverk strukturert og gjør at de kan kommunisere raskere.

e) *Protokoll-lagdeling kan tilpasse seg fremtidige forbedringer og endringer.*

Q.1.1.5 Anta at P pakker skal sendes gjennom et pakkesvitsjet nettverk fra kilde til destinasjon. Det er N lagre-og-send (store-and-forward) routere mellom kilde og destinasjon. Hver pakke har en lengde på L bits. Anta at alle koblingene i nettverket (for eksempel kobling mellom kilde og router, mellom routere og mellom router og destinasjon) har samme overføringshastighet på R bps. Hva er den minste ende-til-ende forsinkelsen du vil ha ved å sende P slike pakker etter hverandre gjennom nettverket? Ignorer køforsinkelse, prosesseringsforsinkelse og propagasjonsforsinkelse.

a) *P*N*L/R*
b) *(N+P-1)*L/R*
c) *P*(N+1)*L/R*
d) *(N+P+2)*L/R*
e) *Ingen av de nevnte.*

Q1.2 Applikasjonslag og transportlag (Application Layer and Transport Layer – Kapittel 2 & 3)

Q1.2.1 Hvilke(n) av disse protokollene tilhører ikke applikasjonslaget (Application Layer)?

a) *Telnet (User Data Protocol)*
b) *TDM (Time Division Multiplexing)*
c) *SMTP (Simple Mail Transfer Protocol)*
d) *HTTP (Hypertext Transfer Protocol)*
e) *IMAP (Internet Message Access Protocol)*

Q1.2.2 Nettleserbuffering (Web caching) er vanligvis satt opp mellom klientene (PC-er i et universitetsnettverk) og en opprinnelig server (for eksempel en kommersiell nettsideserver). Hvilke av følgende påstander er korrekte om nettleserbuffering?

a) *Det reduserer ikke gjennomsnittlig forsinkelse for alle objekter.*
b) *Gjennomsnittlig, reduserer det forsinkelsen for bare objektene som er lagret i bufferen (cachen).*
c) *Det kan potensielt redusere gjennomsnittlig forsinkelse for alle objekter, selv objekter som ikke er lagret i bufferen.*
d) *Det øker gjennomsnittlig trafikk på koblingene (koblingen mellom en klient og den opprinnelige serveren).*
e) *Den har en lagring på sin egen disk, og den forhindrer lagring av kopier av nylig forespurte objekter i denne lagringen.*

Q1.2.3 Anta at en prosess hos vert D har en UDP-socket med en forhåndsdefinert port. Anta at vert A, vert B og vert C hver ønsker å sende et UDP-segment til vert D. Hva er det minimale antallet porter som er nødvendig for å sende disse segmentene fra vert A, B og C til vert D?

a) *En socket*
b) *To socketer*
c) *Tre socketer*
d) *Fler enn tre socketer*
e) *Ingen av de nevnte*

Q1.2.4 Hvilke(n) av disse påstandene er sanne?

a) *SMTP bruker UDP som sin underliggende transportprotokoll.*

b) *Hverken UDP eller TCP gir pålitelig dataoverføring.*
c) *UDP er en tilkoblingsorientert (connection oriented) protokoll.*
d) *Internett-telefoniapplikasjoner (Internet telephony) (for eksempel SIP) kan bruke både UDP eller TCP.*
e) *FDM (frekvensdivisjonsmultipleksering) krever mer sofistikert analog maskinvare for å skifte signal til passende frekvensbånd enn det TDM (tidsdivisjonsmultipleksering) gjør.*

Q1.2.5 Du skal distribuere en fil på F=10 Gbit til N=100 peers ved hjelp av **klient-serverarkitektur** (**client-server arcitecture**). Serveren har en opplastningshastighet på u_s =1 Gbps. Hver peer har en nedlastingshastighet på d_i =200 Mbps. Hva er den minimale tiden for å distribuere denne filen til alle peers?

a) *50s*
b) *5000s*
c) *500s*
d) *1000s*
e) *Ingen av de nevnte*

Q1.3 Nettverkslaget (Network layer – Kapittel 4 & 5)

Q1.3.1 Tildel nettverksadresser fra 214.97.250/23 til et subnett som skal ha nok adresser til 250 grensesnitt (interfaces). Tildelingen tar formen a.b.c/x. Hvilke(t) av følgende er mulige riktige subnett?

a) *214.97.245/24*
b) *214.97.251/24*
c) *214.97.253/24*
d) *214.97.254/24*
e) *214.97.254/25*

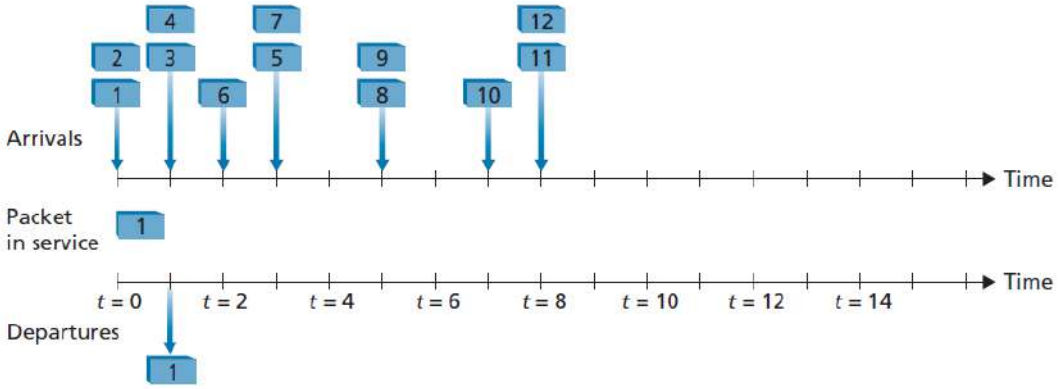
Q1.3.2 Hvilke(t) av følgende utsagn om DHCP (Dynamic Host Configuration Protocol) er **usanne?**

a) *En ny internettvert gjennomfører en 4-trinns prosess med en DHCP-server for å skaffe seg en ny IP-adresse.*
b) *DHCP bruker TCP (Transmission Control Protocol) som sin transportprotokoll.*
c) *DHCP gir dynamisk tildeling av IP-adresser til nettverksklienter.*
d) *DHCP brukes primært for å route datapakker mellom nettverk.*
e) *DHCP-servere kan tilby konfigurasjonsparametere som DNS-serveradresser og subnettmasker.*

Q1.3.3 Hva stemmer **ikke** om Internet Control Message Protocol (ICMP)?

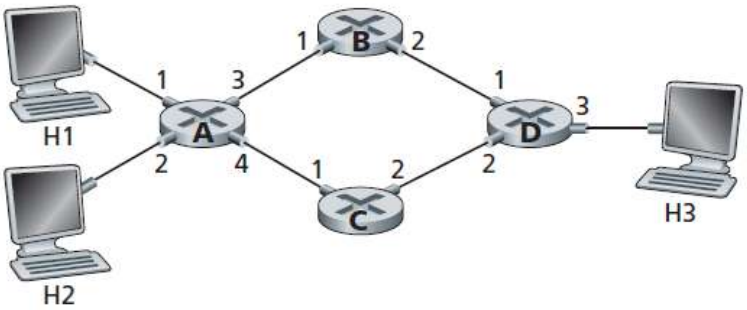
a) *ICMP brukes ikke primært i nettverkslaget.*
b) *ICMP er en støtteprotokoll i Internett-protokollpakken.*
c) *ICMP gir funksjoner som feilrapportering og nettverksdiagnose.*
d) *ICMP-meldinger brukes ikke bare for å signalisere feiltilstander.*
e) *ICMP er en transportprotokoll som brukes for datautveksling mellom enheter på nettverket*

Q1.3.4 I FIFO (First Input First Output) tjenesten nedenfor viser den øverste tidslinjen ankomsttider for pakker, og den nederste tidslinjen viser når pakken blir sendt videre. Køforsinkelsen for en pakke er perioden mellom dens ankomsttid og når den blir sendt. For eksempel vil pakke 1 ankomme ved t = 0 og bli sendt ved tiden t=1, noe som gir en forsinkelse på 1. Hva er gjennomsnittlig forsinkelse for de neste tre pakkene (pakke 2, 3 og 4)?



a) *8/3s*
b) *7/3s*
c) *2s*
d) *5/3s*
e) *Ingen av de nevnte.*

Q1.3.5 Hva er **sant** om dette nettverket?



a) *Det er mulig å konfigurere videresendingstabellen (forwarding table) i router A slik at all trafikk som skal til H3 videresendes via grensesnitt 3.*
b) *Det er ikke mulig å konfigurere videresendingstabellen (forwarding table) i router A slik at all trafikk som skal til H3 videresendes via grensesnitt 3.*
c) *Det er mulig å konfigurere en videresendingstabell i router A slik at all trafikk fra H1 som skal til H3 videresendes via grensesnitt 3, mens all trafikk fra H2 som skal til H3, videresendes via grensesnitt 4.*
d) *Det er ikke mulig å konfigurere en videresendingstabell i router A slik at all trafikk fra H1 som skal til H3 videresendes via grensesnitt 3, mens all trafikk fra H2 som skal til H3, videresendes via grensesnitt 4.*
e) *Ingen av de nevnte*

Q1.4 Linklaget, trådløse og mobile nettverk (Link Layer, Wireless and Mobile Networks – Kapittel 6 & 7)

Q1.4.1 Hvilke(t) av disse utsagnene om switcher og routere **stemmer ikke**?

a) Både routere og switcher er tilkoblingsenheter (connecting devices) i nettverk.

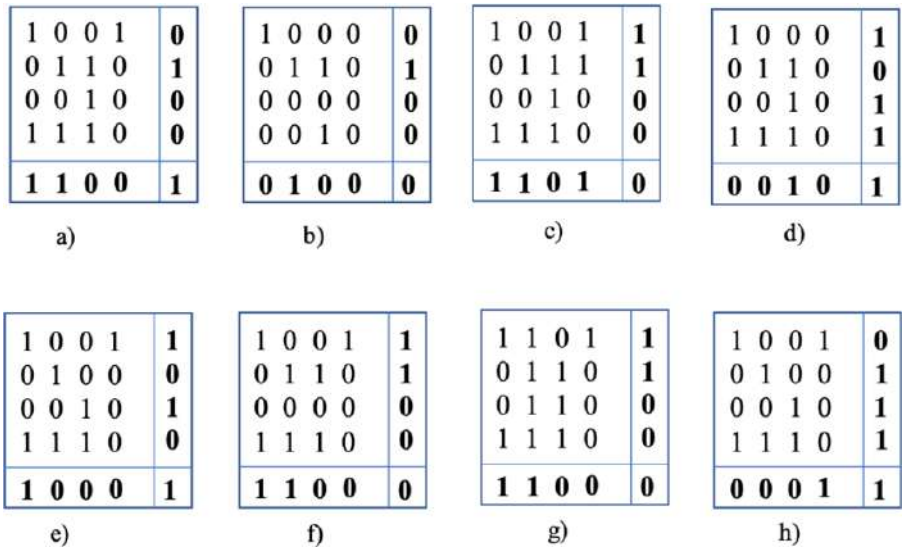
b) Routere opererer på datalinklaget (Data link layer), mens switcher opererer på nettverkslaget (network layer).

c) Routere opererer på nettverkslaget (network layer), mens switcher opererer på datalinklaget (Data link layer).

d) Switcher kobler sammen ulike nettverk, mens en router kobler sammen enheter innenfor et nettverk.

e) I drift baserer rutere seg på IP-adresser mens switcher baserer seg på MAC-adresser.

Q1.4.2 Hvilke(n) av disse alternativene viser en korrekt implementasjon av et «two- dimensional **even** parity scheme»?



Q1.4.3 Hva er riktig av følgende utsagn om forholdet mellom SNR (Signal-to-noise ratio), BER (Bit Error Rate), og modulasjon (Modulation schemes)?

a) For en gitt modulasjon, jo lavere SNR, desto høyere BER.

b) For en gitt modulasjon, jo lavere SNR, desto lavere BER.

c) For en gitt SNR har en modulasjonsteknikk med høyere bitoverføringshastighet en lavere BER.

d) For en gitt SNR har en modulasjonsteknikk med høyere bitoverføringshastighet en høyere BER.

e) Ingen av de nevnte.

Q1.4.4 Hva er **riktig** om CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protokollen og RTS (Request to Send)/CTS (Clear to Send) meldingsutveksling?

a) Problemer med skjulte noder (hidden node issue) oppstår fremdeles med systemer som bruker CSMA/CA.

b) *I CSMA/CA, når en node ønsker å sende, så sender den en RTS til AP (Tilgangspunktet). AP-en svarer med en CTS, og gir tillatelse til at noden kan starte overføring.*

c) *Under en RTS/CTS-utveksling kan ikke skjulte noder lytte til rammene (frames) som sendes.*

d) *RTS/CTS-mekanismen løser eksponerte-noder-problemet (exposed node problem).*

e) *RTS/CTS-mekanismen brukes i CSMA/CA for å forbedre kanaltilgang (channel access).*

Q.1.4.5 Hvilke påstander om de to protokollene ALOHA (pure ALOHA) og slotted ALOHA er **sanne**?

a) *Pure ALOHA er mindre effektiv enn slotted ALOHA.*

b) *Maksimal oppnåelig effektivitet i slotted ALOHA er dobbelt så høy som hos pure ALOHA.*

c) *Slotted ALOHA har færre kollisjoner enn pure ALOHA.*

d) *I Slotted ALOHA kan hvilken som helst stasjon sende data når som helst uten synkronisering.*

e) *I pure ALOHA må stasjoner vente på neste tidsrom (time slot) før de overfører data.*

Q1.5 Sikkerhet og multimedia-nettverk (Security and Multimedia Networking – Kapittel 8, og kapittel 9 fra Edition 7)

Q1.5.1 Hvilke(n) av disse er ønskelige egenskaper hos sikre nettverk?

a) *Nettverkspålitelighet (Network reliability.)*

b) *Konfidensialitet (Confidentiality)*

c) *Meldingsintegritet (Message integrity.)*

d) *Driftssikkerhet (Operational security)*

e) *Høy båndbredde for rask dataoverføring*

Q1.5.2 Anta at N personer vil kommunisere med hverandre ved hjelp av symmetrisk nøkkelkryptering (symmetric key encryption). All kommunikasjon mellom to personer er synlig for alle andre i denne gruppen, og ingen annen person i denne gruppen skal kunne dekode deres kommunikasjon. Hvor mange nøkler er nødvendig i hele dette systemet?

a) *N*N*

b) *2*N-1*

c) *N*(N-1)*

d) *N*(N-1)/2*

e) *Ingen av de nevnte.*

Q1.5.3 Hvilke utsagn er **sanne** om meldingsintegritet (message integrity)?

a) *Meldingsintegritet betyr at det er mulig å verifisere at avsender er den som den hevder å være.*

b) *Meldingsintegritet betyr at det er mulig for mottaker å detektere om meldingen har blitt endret underveis.*

c) *Både sjekksummer og hasheteknikker kan brukes for å sjekke meldingsintegritet.*

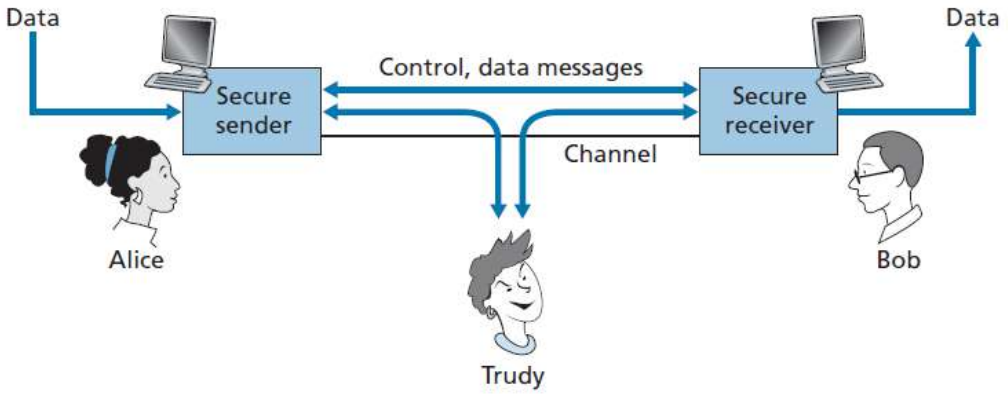
d) *Generelt gir en hash bedre meldingsintegritet enn en sjekksum.*

e) *For at en melding skal ha meldingsintegritet må transportlaget ha brukt TCP som overføringsprotokoll.*

Q1.5.4 I videostrømmetjenester er HTTP streaming (over TCP) mer populært enn UDP strømming. Hovedgrunnene til dette er:

a) *UDP er ikke tilkoblingsorientert (UDP er connectionless)*
b) *UDP mangler retransmisjon, rekkefølgekontroll og feilsjekkingsmekanismer (retransmission, ordering and error-checking mechanisms), som fører til høyere feilrate.*
c) *UDP mangler håndtrykk og bekreftelser (handshakes and acknowledements), noe som resulterer i lavere forsinkelse.*
d) *Mange brannmurer er konfigurert til å blokkere mesteparten av UDP-trafikk, mens de tillater HTTP trafikk.*
e) *Ingen av de nevnte.*

Q1.5.5 Alice og Bob sender informasjon over et nettverk som blir avlyttet av en inntrenger (Trudy). Hvilke(t) av disse utsagnene stemmer om hva slags informasjon inntrengeren har tilgang til og hva slags handlinger inntrengeren kan utføre?



a) *Avlytting og opptak av kontrollmeldinger på kanalen*
b) *Opptak av datameldinger på kanalen*
c) *Modifisering og innsetting av meldinger.*
d) *Sletting av meldinger eller meldingsinnhold.*
e) *Ingen av de nevnte.*

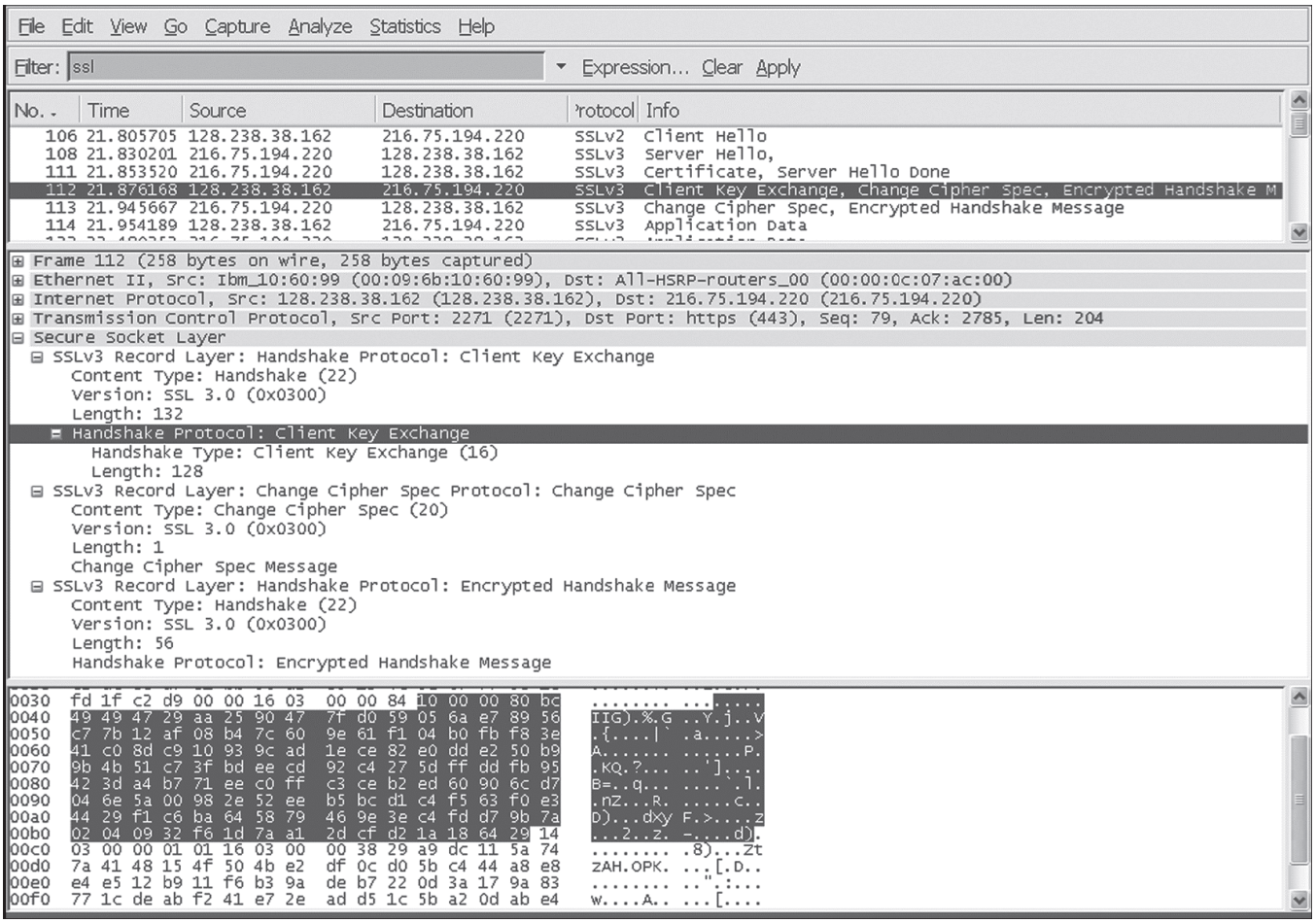
Langsvarspørsmål (Q2-Q6) [35 poeng]

Q2: Flytkontroll (Flow control) [6 poeng]

To verter, Vert A og Vert B er direkte sammenkoblet over en 10 Gbps kobling. Det er en TCP-kobling mellom de to vertene, og Vert A skal sende en enorm fil til Vert B over denne koblingen. Vert A kan sende data ut på sin TCP socket med en hastighet på 1 Gbps, men Vert B klarer bare å lese data fra sin TCP-mottaksbuffer med en hastighet på 600 Mbps.

Beskriv effektene av TCP flytkontroll i denne TCP-koblingen.

Q3. Wireshark-outputen nedenfor er en del av en SSL (Secured Socket Layer) sesjon. Svar på spørsmålene [5 poeng]



Q3.1 Ble Wireshark-pakke 112 sendt av klienten eller serveren?

Q3.2 Hva er serverens IP-adresse og portnummer?

Q3.3 Forutsatt at det ikke forekommer tap eller retransmisjon, hva vil sekvensnummeret til det neste TCP-segmentet som sendes fra klienten være? Forklar hvordan du fikk dette nummeret.

Q3.4 Hvor mange SSL-oppføringer (SSL records) inneholder Wireshark-pakke 112?

Q3.5 Inneholder pakke 112 en «Master secret», en kryptert «Master secret» eller ingen av delene?

Q.4 IP adressering (IP addressing) [8 poeng]

En IP-adresse består av en subnett-del og en host-del. For å avgjøre hvilket subnet en IP-adresse tilhører, må du kjenne til subnet-masken. Svar på følgende spørsmål:

Q.4.1. Hvordan finner du subnettet fra IP-adressen og subnet-masken?

Q.4.2 Gitt følgende IP-adresse 192.168.1.108 og subnet-masken /30 (255.255.255.252), hva er subnet-adressen? Begrunn svaret ditt.

Q.4.3 Gitt følgende IP-adresse 192.168.2.108 og subnet-masken /29 (255.255.255.248), hva er subnet-adressen? Begrunn svaret ditt.

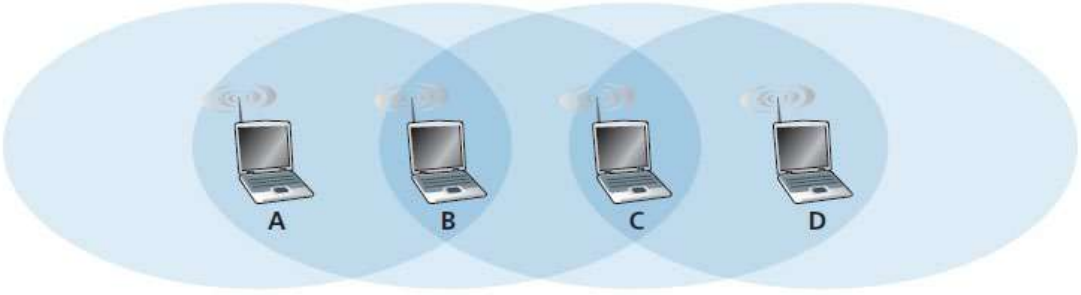
Q.4.4 Gitt følgende IP-adresse 192.168.3.108 og subnet-masken /28 (255.255.255.240), hva er subnet-adressen? Begrunn svaret ditt.

Q.5 Multiple Access Mekanisme [12 poeng]

Figuren nedenfor inneholder fire trådløse noder: A, B, C og D. Dekningsområdene til disse nodene er vist som skyggelagte ovaler; alle noder deler samme frekvens. Når A sender, kan den bare høres/mottas av B; når B sender, kan både A og C høre/motta fra B; når C sender, kan både B og D høre/motta fra C; når D sender, kan bare C høre/motta fra D. Anta at hver node har et uendelig antall meldinger som den ønsker å sende til hver av de andre nodene. Hvis en meldings destinasjon ikke er en umiddelbar nabo, må meldingen videreformidles via mellomliggende node(r).

Tiden er delt opp i intervaller, og det tar nøyaktig ett tidsintervall for én meldingsoverføring. I løpet av et tidsintervall kan en node gjøre en av følgende: (i) sende en melding, (ii) motta en melding, (iii) være stille. Som alltid, hvis en node hører to eller flere samtidige overføringer, oppstår en kollisjon, og ingen av meldingene blir overført. Anta at når en melding sendes, vil den bli mottatt korrekt av andre noder innenfor senderens overføringsradius hvis ingen kollisjon skjedde ved disse nodene.

En melding har lengde L (bits) og tidsintervall T (sekunder). Svar på spørsmålene:



Q.5.1 Hvis A sender meldinger til B, og D sender meldinger til C.
Hva er den samlede maksimale hastigheten på dataflyten fra A til B og D til C?
Begrunn svaret ditt.

Q.5.2 Hvis A sender meldinger til B, og C sender meldinger til D.
Hva er den samlede maksimale hastigheten på dataflyten fra A til B og fra C til D?
Begrunn svaret ditt.

Q.5.3. I dette scenarioet skal du anta at for hver datamelding som sendes fra avsender til mottaker vil mottaker sende en ACK-melding tilbake til kilden (slik som i TCP). Videre vil hver ACK-melding bruke 1 tidsintervall.

Q.5.3.1 Gjenta spørsmål Q.5.1 for dette scenarioet.

Q.5.3.2 Gjenta spørsmål Q.5.2 for dette scenarioet.

Q.6 Følgende spørsmål handler om DNS (Domain name service) [4 poeng]

Q.6.1 Beskriv formatet til en Resource Record (RR) i DNS.

Q.6.2 Hva slags informasjon kan sendes til en klient når klienten sender ut en DNS spørring (DNS query)?

(End of Questions)

NTNU

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgave i

TTM4100 KOMMUNIKASJON – TJENESTER OG NETT

Fagleg kontakt under eksamen: Tu Dac Ho

Tlf.: 9300 6185

Fagleg kontakt kjem til eksamenslokalet: JA (0900 - 1300)

Eksamensdato: 08.05.2024

Eksamenstid (frå-til): 0900-1300

Hjelpemiddelkode/Tillatne hjelpemiddel: D (Ingen trykte eller handskrivne hjelpemiddel tillatne. Bestemt, enkel kalkulator tillaten).

Annan informasjon:
- **Eksamen består av to delar**
- **Del I: Oppgåvetekst**
- **Del II: Eigne svarark**

Målform/språk: Nynorsk

Talet på sider (Del I utan framside/reglar side):10

Talet på sider vedlegg (Del II): 11

Informasjon om trykking av eksamensoppgave
Originalen (Del I) er:
1-sidig ☐ **2-sidig** √
sort/hvit ☐ **farger** ☐
skal ha flervalgskjema ☐

Kontrollert av:

Dato Sign

Merk! Studenter finner sensur i Studentweb. Har du spørsmål om din sensur må du kontakte instituttet ditt. Eksamenskontoret vil ikke kunne svare på slike spørsmål.

Regler/Rules/Reglar:

B: BOKMÅL	E: ENGLISH	N: NYNORSK
Maksimal poengsum er 100 poeng. Oppgavesettet består av 2 deler: ● Del I, problemspesifikasjonene - denne delen. ● Del II, svarsidene, inneholder svarbokser for flervalgsspørsmål og "skriftlig tekst"-oppgaver. Del II inkluderer også 3 sider for kommentarer relatert til formelle spørsmål om del I eller del II. Disse sidene kan også brukes til "skriftlig tekst"-svar. Del II skal leveres som ditt svar. To eksemplarer av del II deles ut. Kun ett eksemplar skal leveres. Kandidatnummeret skal stå på alle svarsidene. Ikke skriv utenfor feltene i boksen. Bruk en blå eller svart penn, ikke en blyant. **Skriftlige tekstoppgaver** skal besvares innenfor den tildelte boksen i del II. **Flervalgsspørsmål** skal besvares ved å angi dine valg i den tildelte boksen i del II. For hvert flervalgsspørsmål kan det være ett eller flere riktige valg. For flervalgsspørsmål: Poeng = Maks{(antall riktige valg – minuspoeng), 0}*x - 1 feil gir ingen minuspoeng; - i > 1 feil gir (i-1)*0,5 minuspoeng. Denne avbildningen mellom feilvalg og minuspoeng lar deg svare feil én gang uten å bli straffet. Et manglende riktig valg for et flervalgsspørsmål regnes ikke med i feil valg. Verdien av x bestemmes som (totalt poeng for flervalgsspørsmål)/ (totalt antall riktige valg).	The maximum score is 100 points. The problem set consists of 2 parts: ● Part I, the problem specifications - this part. ● Part II, the answer pages, includes answer boxes for multiple-choice questions and "written text" problems. Part II also includes 3 pages for comments related to *formal issues* about Part I or Part II. These pages may also be used for "written text" answers. Part II shall be delivered as your answer. Two copies of Part II are handed out. Only one copy shall be delivered. The candidate number should be written on all answer pages. Do not write outside the box fields. Use a blue or black pen, not a pencil. **Written text** problems shall be answered within the assigned box of Part II. **Multiple-choice** questions shall be answered by providing your choices within the assigned box of Part II. For each multiple-choice question, there may be one or more correct choices. For multiple-choice questions as whole: Points = Max{(number of correct choices – discount points), 0}*x - 1 incorrect gives no discount; - i > 1 incorrect gives (i-1)*0,5 discount points. This mapping between incorrect choices and discount points allows you to answer wrong once without being punished. A missing correct choice for a multiple-choice question is not counted in incorrect choices. *The value of x is decided as (total points, i.e. 65, for multiple choice questions)/ (total number of correct choices, i.e. 45.)*	Maksimal poengsum er 100 poeng. Oppgåvesettet består av 2 delar: ● Del I, problemspesifikasjonane - denne delen. ● Del II, svarsidene, inneheld svarboksar for fleirvalspørsmål og "skriftleg tekst"-oppgåver. Del II inkluderer også 3 sider for kommentarar relatert til formelle spørsmål om del I eller del II. Desse sidene kan også brukast til "skriftleg tekst"-svar. Del II skal leverast som svaret ditt. To eksemplar av del II blir delt ut. Berre eitt eksemplar skal leverast. Kandidatnummeret skal stå på alle svarsidene. Ikkje skriv utanfor felta i boksen. Bruk ein blå eller svart penn, ikkje ein blyant. **Skriftlege tekstoppgåver** skal svarast på innanfor den tildelte boksen i del II. **Fleirvalspørsmål** skal svarast på ved å angi dine val i den tildelte boksen i del II. For kvart fleirvalspørsmål kan det vera eitt eller fleire rette val. For fleirvalspørsmål: Poeng = Maks{(talet på rette val – minuspoeng), 0}*x - 1 feil gir ingen minuspoeng; - i > 1 feil gir (i-1)*0,5 minuspoeng. Denne avbildinga mellom feilval og minuspoeng lèt deg svara feil éin gong utan å bli straffa. Eit manglande rett val for eit fleirvalspørsmål blir ikkje rekna med i feil val.Verdien av x blir bestemd som (totalt poeng for fleirvalspørsmål)/ (det samla talet rette val).

Fleirvalspørsmål

Q1. (There are 45 correct choices out of 128) [65 poeng]

Q1.1 Generelt (Kapittel 1)

Q1.1.1 Linjesvitsjing (Circuit switching) og pakkesvitsjing (packet switching) har mange forskjellar. Kva/kva for eit av desse utsegnene stemmer?

a) *Eit linjesvitsja nettverk kan som regel garantera for ei viss bandbreidd i løpet av ein ende-til-ende tilkopling, noko eit pakkesvitsja nettverk ikkje kan.*
b) *Dei fleste pakkesvitsja nettverk i dag (inkludert Internett) kan gi garantiar for bandbreidd frå ende til ende.*
c) *Variasjonen i forseinking blant pakkar/meldingar i eit linjesvitsja nettverk er vanlegvis mindre enn i eit pakkesvitsja nettverk.*
d) *Kostnadene for dedikerte ressursar i eit pakkesvitsja nettverk er vanlegvis høgare enn kostnadene for ressursar i eit linjesvitsja nettverk.*
e) *I linjesvitsja nettverk blir delt bandbreidda blant brukarane og blir berre tildelte når data må overførast. Det har betre bandbreiddeeffektivitet enn i pakkesvitsja nettverk.*

Q1.1.2 Gå ut frå at det er nøyaktig éin pakkesvitsj mellom ein sendande vert og ein mottakande vert. Overføringshastigheitene mellom den sendande verten og svitsjen, og mellom svitsjen og den mottakande verten, er høvesvis R1 og R2. Viss svitsjen bruker lagre-og-send-pakkesvitsjing (store-and-forward packet switching), kva er den totale ende-til-ende forseinkinga for å senda ein pakke av lengd L når køforseinking, propagasjonsforsinkelse og prosesseringsforseinking blir ignorert?

a) *L/(R1+R2)*
b) *L/R1+L/R2*
c) *2L/Max {R1, R2}*
d) *2L/Min {R1, R2}*
e) *Ingen av dei nemnde*

Q1.1.3 Gå ut frå at ein klient og ein server blir saman kopla gjennom ein router. Gå ut frå at routeren kan byrja å senda ein innkommande pakke etter å ha fått dei første 80 byte, i staden for å venta på heile pakken. Gå ut frå at koplingshastigheitene er 1000 byte/s, og at klienten sender éin pakke med ein storleik på 3000 byte til serveren. Kva blir ende-til-ende forseinkinga?

a) *3,808s*
b) *3,800s*
c) *3,008s*
d) *3,080s*
e) *Ingen av dei nemnde*

Q1.1.4 Protokoll-lagdeling (Protocol layering) blir vanlegvis brukt i datanettverk fordi:

a) *Den hindrar at nettverksfunksjonalitetar blir delte opp i separate lag, kvar med eit spesifikt formål.*
b) *Innkapsling er den mest effektive måten å overføra data på.*
c) *Det gir eit enkelt design for implementering og vedlikehald, men meir komplikasjon i nettverksutvikling.*
d) *Det held nettverk strukturert og gjer at dei kan kommunisera raskare.*

e) *Protokoll-lagdeling kan tilpassa seg framtidige forbetringar og endringar.*

Q.1.1.5 Gå ut frå at P pakkar skal sendast gjennom eit pakkesvitsja nettverk frå kjelde til destinasjon. Det er N lagre-og-send (store-and-forward) routere mellom kjelde og destinasjon. Kvar pakke har ei lengd på L bits. Gå ut frå at alle koplingane i nettverket (til dømes kopling mellom kjelde og router, mellom routere og mellom router og destinasjon) har same overføringsfart på R bps. Kva er den minste ende-til-ende forseinkinga du vil ha ved å senda P slike pakkar etter kvarandre gjennom nettverket? Ignorer køforseinking, prosesseringsforseinking og propagasjonsforsinkelse.

a) *P*N*L/R*
b) *(N+P-1)*L/R*
c) *P*(N+1)*L/R*
d) *(N+P+2)*L/R*
e) *Ingen av dei nemnde*

Q1.2 Applikasjonslag og transportlag (Application Layer and Transport Layer – Kapittel 2 & 3)

Q1.2.1 Kva for ein/nokre av desse protokollane tilhøyrar ikkje applikasjonslaget (Application Layer)?

a) *Telnet (User Data Protocol)*
b) *TDM (Time Division Multiplexing)*
c) *SMTP (Simple Mail Transfer Protocol)*
d) *HTTP (Hypertext Transfer Protocol)*
e) *IMAP (Internet Message Access Protocol)*

Q1.2.2 Nettleserbuffring (Web caching) er vanlegvis sett opp mellom klientane (PC-ar i eit universitetsnettverk) og ein opphavleg server (til dømes ein kommersiell nettsideserver). Kva for nokre av følgjande påstandar er korrekte om nettlesarbuffring?

a) *Det reduserer ikkje gjennomsnittleg forseinking for alle objekt.*
b) *Gjennomsnittleg, reduserer det forseinkinga for berre objekta som er lagra i bufferen (cachen).*
c) *Det kan potensielt redusera gjennomsnittleg forseinking for alle objekt, sjølv objekt som ikkje er lagra i bufferen.*
d) *Det aukar gjennomsnittleg trafikk på koplingane (koplinga mellom ein klient og den opphavlege serveren).*
e) *Den har ei lagring på sin eigen disk, og han forhindrar lagring av kopiar av nyleg spurde objekt i denne lagringa.*

Q1.2.3 Gå ut frå at ein prosess hos vert D har ein UDP-socket med ein førehandsdefinert port. Gå ut frå at vert A, vert B og vert C kvar ønskjer å senda eit UDP-segment til vert D. Kva er det minimale talet på porter som er nødvendig for å senda desse segmenta frå vert A, B og C til vert D?

a) *Ein socket*
b) *To socketer*
c) *Tre socketer*
d) *Fleire enn tre socketer*
e) *Ingen av dei nemnde*

Q1.2.4 Kva for ein/nokre av desse påstandane er sanne?

a) *SMTP brukar UDP som den underliggjande transportprotokollen sin.*

b) *Verken UDP eller TCP gir påliteleg dataoverføring.*
c) *UDP er ein tilkoplingsorientert (connection oriented) protokoll.*
d) *Internett-telefoniapplikasjonar (Internet telephony) (til dømes SIP) kan bruka både UDP eller TCP.*
e) *FDM (frekvensdivisjonsmultipleksering) krev meir sofistikert analog maskinvare for å skifta signal til passande frekvensband enn det TDM (tidsdivisjonsmultipleksering) gjer.*

Q1.2.5 Du skal distribuera ei fil på F=10 Gbit til N=100 peers ved hjelp av **klient-serverarkitektur (client-server arcitecture)**. Serveren har ein opplastningshastighet på u_s =1 Gbps. Kvar peer har ein nedlastingsfart på d_i =200 Mbps. Kva er den minimale tida for å distribuera denne fila til alle peers?

a) *50s*
b) *5000s*
c) *500s*
d) *1000s*
e) *Ingen av dei nemnte*

Q1.3 Nettverkslaget (Network layer – Kapittel 4 & 5)

Q1.3.1 Tildel nettverksadresser frå 214.97.250/23 til eit subnett som skal ha nok adresser til 250 grensesnitt (interfaces). Tildelinga tek forma a.b.c/x. Kva for eit/nokre av følgjande er moglege rette subnett?

a) *214.97.245/24*
b) *214.97.251/24*
c) *214.97.253/24*
d) *214.97.254/24*
e) *214.97.254/25*

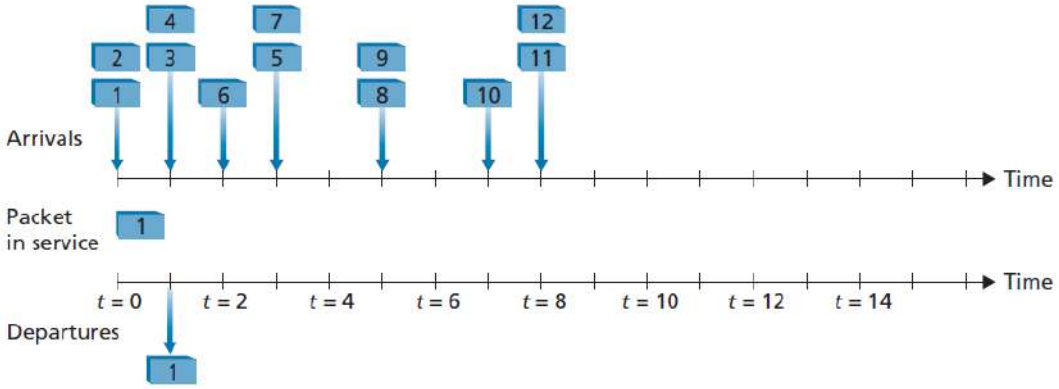
Q1.3.2 Kva for eit/nokre av følgjande utsegn om DHCP (Dynamic Host Configuration Protocol) er **usanne?**

a) *Ein ny internettvert gjennomfører eit 4-trinns prosess med ein DHCP-server for å skaffa seg ei ny IP-adresse.*
b) *DHCP bruker TCP (Transmission Control Protocol) som transportprotokollen sin.*
c) *DHCP gir dynamisk tildeling av IP-adresser til nettverksklientar.*
d) *DHCP brukas primært for å route datapakker mellom nettverk.*
e) *DHCP-serverar kan tilby konfigurasjonsparametrar som DNS-serveradresser og subnettmasker.*

Q1.3.3 Kva stemmer **ikkje** om Internet Control Message Protocol (ICMP)?

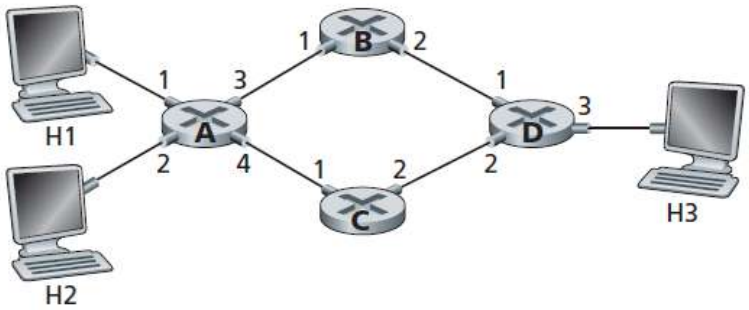
a) *ICMP brukas ikkje primært til nettverkslaget.*
b) *ICMP er ein støtteprotokoll i Internet protocol suite.*
c) *ICMP tilbyr funksjonar som feilrapportering og nettverksdiagnose.*
d) *ICMP-meldingar blir ikkje berre brukte for å signalisera feiltilstandar..*
e) *ICMP er ein transportprotokoll som blir brukt til datautveksling mellom einingar i nettverket.*

Q1.3.4 I FIFO (First Input First Output) tenesta nedanfor viser den øvste tidslinja innkomsttider for pakkar, og den nedste tidslinja viser når pakken blir send vidare. Køforseinkinga for ein pakke er perioden mellom dens framkomsttid og når ho blir send. Til dømes vil pakka 1 komma ved t = 0 og bli sende ved tida t=1, noko som gir ei forseinking på 1. Kva er gjennomsnittleg forseinking for dei neste tre pakkane (pakke 2, 3 og 4)?



a) 8/3s
b) 7/3s
c) 2s
d) 5/3s
e) Ingen av dei nemnte.

Q1.3.5 Kva er **sant** om dette nettverket?



a) Det er mogleg å konfigurera vidaresendingstabellen (forwarding table) i router A slik at all trafikk som skal til H3 vidaresendast via grensesnitt 3.
b) Det er ikkje mogleg å konfigurera vidaresendingstabellen (forwarding table) i router A slik at all trafikk som skal til H3 vidaresendast via grensesnitt 3.
c) Det er mogleg å konfigurera ein vidaresendingstabell i router A slik at all trafikk frå H1 som skal til H3 vidaresendast via grensesnitt 3, medan all trafikk frå H2 som skal til H3, blir vidaresend via grensesnitt 4.
d) Det er ikkje mogleg å konfigurera ein vidaresendingstabell i router A slik at all trafikk frå H1 som skal til H3 vidaresendast via grensesnitt 3, medan all trafikk frå H2 som skal til H3, blir vidaresend via grensesnitt 4.
e) Ingen av de nemnte

Q1.4 Linklaget, trådlause og mobile nettverk (Link Layer, Wireless and Mobile Networks – Kapittel 6 & 7)

Q1.4.1 Kva for eit/nokre av desse utsegnene om switcher og routere **stemmer ikkje**?

a) Både routere og switcher er tilkoplingseiningar (connecting devices) i nettverk..

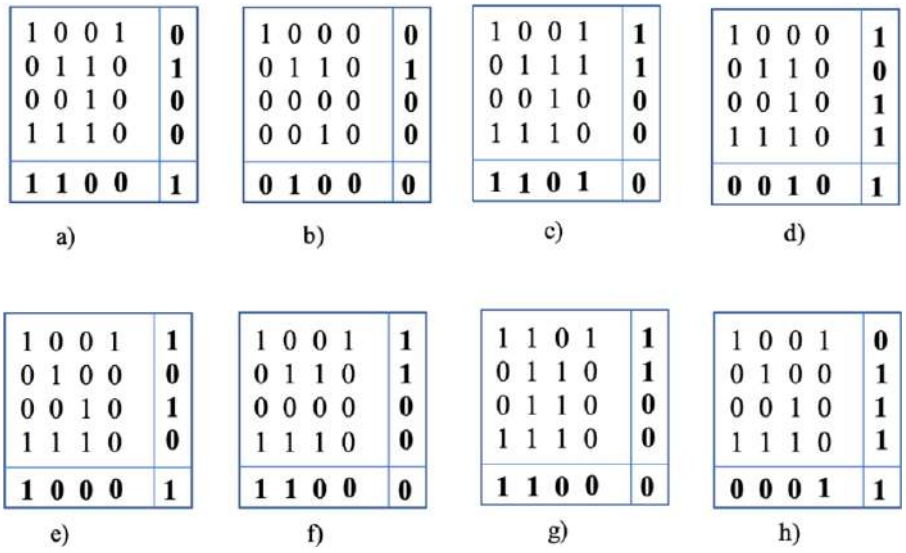
b) Routere opererer på datalinklaget (Data link layer), medan switcher opererer på nettverkslaget (network layer).

c) Routere opererer på nettverkslaget (network layer), medan switcher opererer på datalinklaget (Data link layer).

d) Switcher koplar saman ulike nettverk, medan ein router koplar saman einingar innanfor eit nettverk.

e) I drift baserer routerar seg på IP-adresser medan switcher baserer seg på MAC-adresser.

Q1.4.2 Kva for eit/nokre av desse alternativa viser ein korrekt implementasjon av «two-dimensional **even** parity scheme»?



Q1.4.3 Kva er rett av følgjande utsegn om forholdet mellom SNR (Signal-to-noise ratio), BER (Bit Error Rate), og modulasjon (Modulation schemes)?

a) For ein gitt modulasjon, jo lågare SNR, desto høgare BER.

b) For ein gitt modulasjon, jo lågare SNR, desto lågare BER.

c) For ein gitt SNR har ein modulasjonsteknikk med høgare bitoverføringshastighet ein lågare BER.

d) For ein gitt SNR har ein modulasjonsteknikk med høgare bitoverføringshastighet ein høgare BER.

e) Ingen av dei nemnde.

Q1.4.4 Kva er rett om CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protokollen og RTS (Request to Send)/CTS (Clear to Send) meldingsutveksling?

a) Problem med skjulte node (hidden node issue) oppstår framleis med system som

bruker CSMA/CA.

b) *I CSMA/CA, når eit node ønskjer å senda, så sender den ein RTS til AP (Tilgangspunktet). AP-en svarar med ein CTS, og gir løyve til at nodet kan starta overføring.*

c) *Under ein RTS/CTS-utveksling kan ikkje skjulte node lytta til rammene (frames) som blir sende.*

d) *RTS/CTS-mekanismen løyser eksponerte-noder-problemet (exposed node problem).*

e) *RTS/CTS-mekanismen blir brukt i CSMA/CA for å forbetra kanaltilgang (channel access).*

Q.1.4.5 Kva påstandar om dei to protokollane ALOHA (pure ALOHA) og slotted ALOHA er sanne?

a) *Pure ALOHA er mindre effektiv enn slotted ALOHA.*

b) *Maksimal oppnåeleg effektivitet i slotted ALOHA er dobbelt så høg som hos pure ALOHA.*

c) *Slotted ALOHA har færre kollisjonar enn pure ALOHA.*

d) *Slotted ALOHA kan kva stasjon som helst senda data når som helst utan synkronisering.*

e) *I pure ALOHA må stasjonar venta på neste tidsrom (time slot) før dei overfører data.*

Q1.5 Sikkerheit og multimedia-nettverk (Security and Multimedia Networking – Kapittel 8, og kapittel 9 frå Edition 7)

Q1.5.1 Kva for ein/nokre av desse er ønskjelege eigenskapar hos sikre nettverk?

a) *Nettverkspålitelighet (Network reliability.)*

b) *Konfidensialitet (Confidentiality)*

c) *Meldingsintegritet (Message integrity.)*

d) *Driftstryggleik (Operational security)*

e) *Høy bandbreidd for rask dataoverføring*

Q1.5.2 Gå ut frå at N personar vil kommunisera med kvarandre ved hjelp av symmetrisk nøkkelkryptering (symmetric key encryption). All kommunikasjon mellom to personar er synleg for alle andre i denne gruppa, og ingen annan person i denne gruppa skal kunna dekoda kommunikasjonen deira. Kor mange nøklar er nødvendig i heile dette systemet?

a) *N*N*

b) *2*N-1*

c) *N*(N-1)*

d) *N*(N-1)/2*

e) *Ingen av de nemnte.*

Q1.5.3 Kva for eit/nokre utsegn er **sanne** om meldingsintegritet (message integrity)?

a) *Meldingsintegritet betyr at det er mogleg å verifisera at avsendar er den som han hevdar å vera.*

b) *Meldingsintegritet betyr at det er mogleg for mottakar å detektere om meldinga har vorte endra undervegs.*

c) *Både sjekksummar og hasheteknikker kan brukast for å sjekka meldingsintegritet.*

d) *Generelt gir ein hash betre meldingsintegritet enn ein sjekksum.*

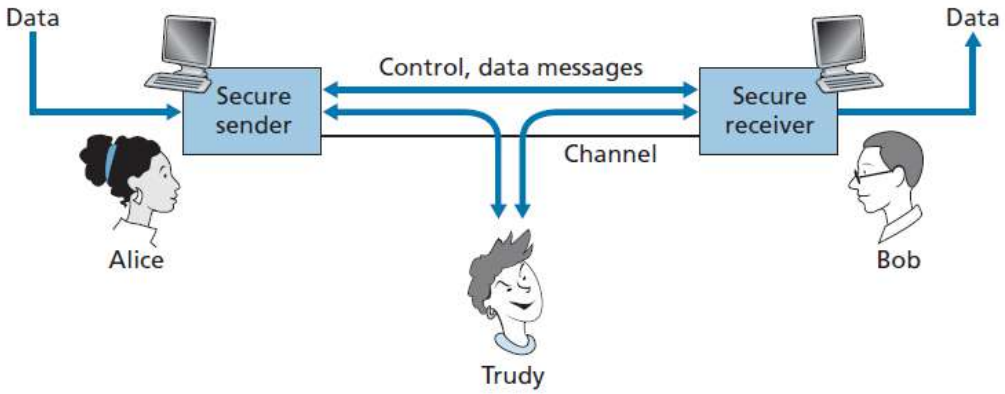
e) *For at ei melding skal ha meldingsintegritet må transportlaget ha brukt TCP som*

overføringsprotokoll.

Q1.5.4 I videostrøymetenester er HTTP strøyming (over TCP) meir populært enn UDP strøyming. Hovudgrunnane til dette er:

a) *UDP er ikkje tilkoplingsorientert (UDP er connectionless)*
b) *UDP manglar retransmisjon, rekkjefølgjekontroll og feilsjekkingsmekanismar (retransmission, ordering and error-checking mechanisms), som fører til høgare feilrate.*
c) *UDP manglar handtrykk og stadfestingar (anda til handshake acknowledements), noko som resulterer i lågare forseinking.*
d) *Mange brannmurar er konfigurerte til å blokkera mesteparten av UDP-trafikk, medan dei tillèt HTTP trafikk.*
e) *Ingen av de nemnte.*

Q1.5.5 Alice og Bob sender informasjon over eit nettverk som blir avlytta av ein inntrengjar (Trudy). Kva for eit/nokre av desse utsegnene stemmer om kva slags informasjon inntrengjaren har tilgang til og kva slags handlingar inntrengjaren kan utføra?



a) *Avlytting og opptak av kontrollmeldingar på kanalen*
b) *Opptak av datameldingar på kanalen*
c) *Modifisering og innsetjing av meldingar.*
d) *Sletting av meldingar eller meldingsinnhald.*
e) *Ingen av de nemnte.*

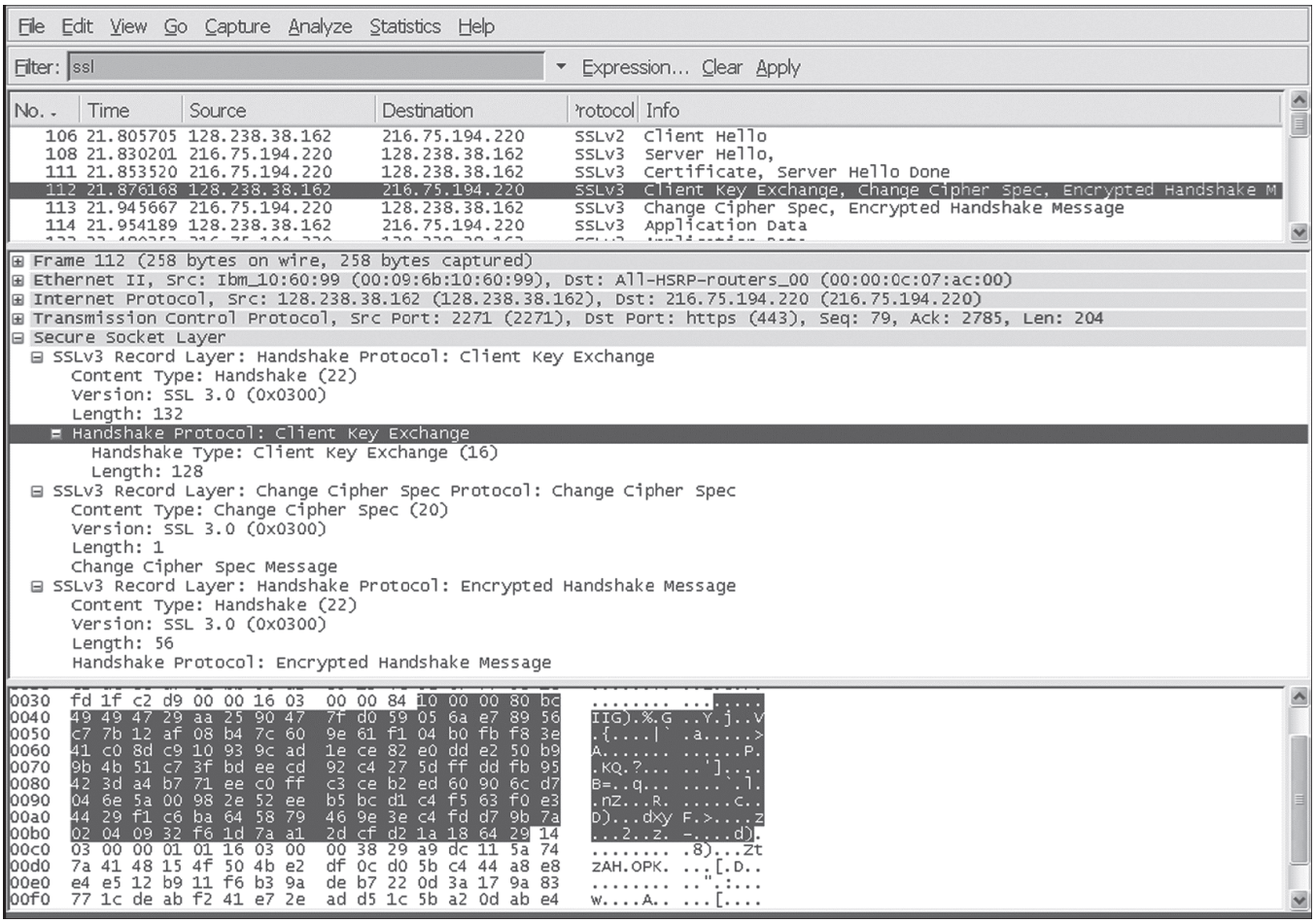
Langsvarspørsmål (Q2-Q6) [35 poeng]

Q2: Flytkontroll (Flow control) [6 poeng]

To vertar, Vert A og Vert B er direkte samankoppelet over ein 10 Gbps kopling. Det er ei TCP-kopling mellom dei to vertane, og Vert A skal senda ein enorm fil til Vert B over denne koplinga. Vert A kan senda data ut på sin TCP socket med ein fart på 1 Gbps, men Vert B klarer berre å lesa data frå TCP-mottaksbufferen sin med ein fart på 600 Mbps.

Beskriv effektane av TCP flytkontroll i denne TCP-koplinga.

Q3. Wireshark-outputen nedanfor er ein del av ein SSL (Secured Socket Layer) sesjon. Svar på spørsmåla [5 poeng]



Q3.1 Vart Wireshark-pakke 112 sende av klienten eller serveren?

Q3.2 Kva er IP-adressa og portnummeret til serveren?

Q3.3 Føresett at det ikkje finst tap eller retransmisjon, kva vil sekvensnummeret til det neste TCP-segmentet som blir sendt frå klienten vera? Forklar korleis du fekk dette nummeret.

Q3.4 Kor mange SSL-oppføringar (SSL records) inneheld Wireshark-pakke 112?

Q3.5 Inneheld pakke 112 ein «Master secret», ein kryptert «Master secret» eller ingen av delane?

Q.4 IP adressering (IP addressing) [8 poeng]

Ei IP-adresse består av ein subnett-del og ein host-del. For å avgjera noko som subnet ei IP-adresse tilhøyrer, må du kjenna til subnet-masken. Svar på følgjande spørsmål:

Q.4.1. Korleis finn du subnettet frå IP-adressa og subnet-masken?

Q.4.2 Gitt følgjande IP-adresse 192.168.1.108 og subnet-masken /30 (255.255.255.252), kva er subnet-adressa? Grunngi svaret ditt.

Q.4.3 Gitt følgjande IP-adresse 192.168.2.108 og subnet-masken /29 (255.255.255.248), kva er subnet-adressa? Grunngi svaret ditt.

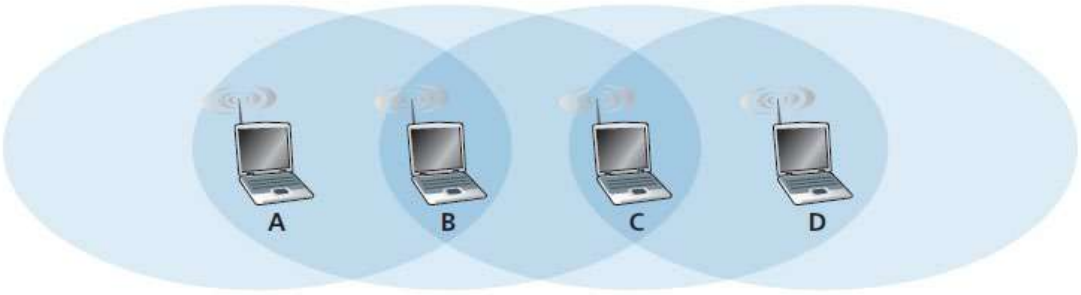
Q.4.4 Gitt følgjande IP-adresse 192.168.3.108 og subnet-masken /28 (255.255.255.240), kva er subnet-adressa? Grunngi svaret ditt.

Q.5 Multiple Access Mekanisme [12 poeng]

Figuren nedanfor inneheld fire trådlause node: A, B, C og D. Dekningsområdene til desse noda er viste som skuggelagte ovalar; alle node deler same frekvens. Når A sender, kan han berre høyrast av B; når B sender, kan både A og C høyra/få frå B; når C sender, kan både B og D høyra/få frå C; når D sender, kan berre C høyra/få frå D. Anta at kvart node har eit uendeleg tal meldingar som han ønskjer å senda til kvar av dei andre noda. Viss ei meldings destinasjon ikkje er ein uvilkårleg nabo, må meldinga vidareformidlast via mellomliggjande node(r).

Tida er delt opp i intervall, og det tek nøyaktig eitt tidsintervall for éi meldingsoverføring. I løpet av eit tidsintervall kan eit node gjera ein av følgjande: (i) senda ei melding, (ii) få ei melding, (iii) vera stille. Som alltid, viss eit node høyrer to eller fleire samtidige overføringar, oppstår ein kollisjon, og ingen av meldingane blir overførte. Gå ut frå at når ei melding blir send, vil ho bli motteken korrekt av andre node innanfor overføringsradiusen til sendaren viss ingen kollisjon skjedde ved desse noda.

Ei melding har lengd L (bits) og tidsintervall T (sekund). Svar på spørsmåla:



Q.5.1 Viss A sender meldingar til B, og D sender meldingar til C.
Kva er den samla maksimale farten på dataflyten frå A til B og D til C?
Grunngi svaret ditt.

Q.5.2 Viss A sender meldingar til B, og C sender meldingar til D.
Kva er den samla maksimale farten på dataflyten frå A til B og frå C til D?
Grunngi svaret ditt.

Q.5.3. I dette scenarioet skal du rekna med at for kvar datamelding som blir send frå avsendar til mottakar vil mottakar senda ei ACK-melding tilbake til kjelda (slik som i TCP). Vidare vil kvar ACK-melding bruka 1 tidsintervall.

Q.5.3.1 Gjenta spørsmål Q.5.1 for dette scenarioet.

Q.5.3.2 Gjenta spørsmål Q.5.2 for dette scenarioet.

Q.6 Følgande spørsmål handlar om DNS (Domain name service) [4 poeng]

Q.6.1 Beskriv formatet til ein Resource Record (RR) i DNS.

Q.6.2 Kva slags informasjon kan sendast til ein klient når klienten sender ut ein DNS spørjing (DNS query)?

(End of Questions)