

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgave i

TTM4100 KOMMUNIKASJON – TJENESTER OG NETT

Faglig kontakt under eksamen: Norvald Stol

Tlf.: 97080077

Eksamensdato: 6. juni 2019

Eksamenstid (fra-til): 1500-1900

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

Annen informasjon:

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

Målform/språk: Bokmål / Engelsk / Nynorsk

Antall sider: 19

Antall sider vedlegg: 0

Kontrollert av:

Dato

Sign

Important: Should there be any print errors (or wrong translations?) in the following text, the *English version (E:)* is the original and valid one.

Viktig: Om det skulle være noen trykkfeil (eller feil i oversetting?) nedenfor er det *den engelske versjonen (E:)* som er den originale og den som gjelder.

1. Multiple areas / Ulike områder (40 p)

E: Each of the ten subgroups below has zero, one or more correct answers. **The total number of correct answers (summed over 1.1 to 1.10 below) is 20.** Each correct answer gives 2 points. You are not penalized for a wrong answer, **up to a total of 20 answers.** Do not claim that **more** than 20 answers are correct in total for task 1. Doing so results in **a penalty of minus 3 points for each additional answer.**

B: Hver av de ti undergruppene nedenfor har ingen, ett eller flere riktige svar. **Totalt antall korrekte svar (summert over 1.1 til 1.10 nedenfor) er 20.** Hvert korrekt svar gir 2 poeng. Du blir ikke straffet for feil svar, **opp til totalt 20 svar.** Ikke påstå at **flere** enn 20 svar er korrekt totalt for oppgave 1. Å gjøre det resulterer i **en straff på minus 3 poeng for hvert ekstra svar.**

N: Kvar av dei ti undergruppene nedanfor har ingen, eit eller fleire riktige svar. **Totalt antal korrekte svar (summert over 1.1 til 1.10 nedanfor) er 20.** Kvart korrekt svar gjev 2 poeng. Du vert ikkje straffa for feil svar, **opp til totalt 20 svar.** Ikkje påstå at **fleire** enn 20 svar er korrekt totalt for oppgåve 1. Å gjera det resulterer i **ei straff på minus 3 poeng for kvart ekstra svar.**

1.1

E: Assume that S and T have an active Transmission Control Protocol (TCP) connection between them. Assume that the last successful byte S has received from T is numbered as 123, and the last successful byte T has successfully received from S is numbered as 267. Which (if any) of the alternatives below are possible exchanges between them following this situation?

B: Anta at S og T har en aktiv TCP forbindelse satt opp mellom seg. Anta videre at den siste vellykkede byten S har mottatt fra T er nummerert som 123, og den siste vellykkede byten T har mottatt fra S er nummerert som 267. Hvilke (om noen) av alternativene under beskriver mulige videre utvekslinger mellom dem etter dette?

N: Anta at S og T har eit aktivt TCP samband sett opp mellom seg. Anta vidare at den siste vellykka byten S har mottatt frå T er nummerert som 123, og den siste vellykka byten T har mottatt frå S er nummerert som 267. Kva for (om nokon) av alternativa under beskriver moglege vidare utvekslingar mellom dei etter dette?

E:

- a)** S sends 50 bytes of data to T and appends ACK=124; after receiving this T sends 76 bytes of data to S and appends ACK=344.
- b)** S sends 100 bytes of data to T and appends ACK=224; after receiving this T sends 96 bytes of data to S and appends ACK=364.
- c)** S sends no data to T but sends ACK=124; after receiving this T sends 76 bytes of data to S and appends ACK=268.
- d)** T sends 100 bytes of data to S and appends ACK=224; after receiving this S sends 100 bytes of data to T and appends ACK=368.
- e)** T sends 50 bytes of data to S and appends ACK=268; after receiving this S sends 90 bytes of data to T and appends ACK=174.
- f)** T sends no data to S but sends ACK=268; after receiving this S sends 100 bytes of data to T and appends ACK=224.

- g)** Both S and T send segments to each other in parallel: S sends 50 bytes of data to T and appends ACK=174 and T sends 16 bytes of data to S and appends ACK=284.
- h)** Both S and T send segments to each other in parallel: S sends 50 bytes of data to T and appends ACK=124 and T sends 36 bytes of data to S and appends ACK=268.

B:

- a)** S sender 50 bytes med data til T og ACK=124; etter å ha mottatt dette sender T 76 bytes med data til S og ACK=344.
- b)** S sender 100 bytes med data til T og ACK=224; etter å ha mottatt dette sender T 96 bytes med data til S og ACK=364.
- c)** S sender ikke data til T men sender ACK=124; etter å ha mottatt dette sender T 76 bytes med data til S og ACK=268.
- d)** T sender 100 bytes med data til S og ACK=224; etter å ha mottatt dette sender S 100 bytes med data til T og ACK=368.
- e)** T sender 50 bytes med data til S og ACK=268; etter å ha mottatt dette sender S 90 bytes med data til T og ACK=174.
- f)** T sender ikke data til S men sender ACK=268; etter å ha mottatt dette sender S 100 bytes med data til T og ACK=224.
- g)** Både S og T sender segmenter til hverandre parallelt: S sender 50 bytes med data til T og ACK=174 og T sender 16 bytes med data til S og ACK=284.
- h)** Både S og T sender segmenter til hverandre parallelt: S sender 50 bytes med data til T og ACK=124 og T sender 36 bytes med data til S og ACK=268.

N:

- a)** S sender 50 bytes med data til T og ACK=124; etter å ha mottatt dette sender T 76 bytes med data til S og ACK=344.
- b)** S sender 100 bytes med data til T og ACK=224; etter å ha mottatt dette sender T 96 bytes med data til S og ACK=364.
- c)** S sender ikkje data til T men sender ACK=124; etter å ha mottatt dette sender T 76 bytes med data til S og ACK=268.
- d)** T sender 100 bytes med data til S og ACK=224; etter å ha mottatt dette sender S 100 bytes med data til T og ACK=368.
- e)** T sender 50 bytes med data til S og ACK=268; etter å ha mottatt dette sender S 90 bytes med data til T og ACK=174.
- f)** T sender ikkje data til S men sender ACK=268; etter å ha mottatt dette sender S 100 bytes med data til T og ACK=224.
- g)** Både S og T sender segmenter til kvarandre parallelt: S sender 50 bytes med data til T og ACK=174 og T sender 16 bytes med data til S og ACK=284.
- h)** Både S og T sender segmenter til kvarandre parallelt: S sender 50 bytes med data til T og ACK=124 og T sender 36 bytes med data til S og ACK=268.

1.2

E: Which (if any) of the following terms/terminology are used to describe elements of the TCP congestion control scheme?

B: Hvilke (om noen) av følgende uttrykk/terminology blir brukt for å beskrive elementer av TCP «congestion control» mekanismen?

N: Kva for (om nokon) fylgjande uttrykk/terminology vert brukt for å beskrive elementer av TCP «congestion control» mekanismen?

- a) cyclic redundancy check
- b) interleaving
- c) forward error correction
- d) short inter-frame spacing
- e) slow start
- f) clear-to-send
- g) two-dimensional parity
- h) congestion avoidance

1.3

E: Which (if any) of the following statements are correct about the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP)?

B: Hvilke (om noen) av påstandene nedenfor er korrekte, om UDP eller TCP.

N: Kva for (om nokon) av påstandane nedanfor er korrekte, om UDP eller TCP

E:

- a) UDP provides a reliable transport service to an application using it.
- b) TCP provides an unreliable transport service to an application using it.
- c) UDP uses congestion control.
- d) UDP sets up an end-to-end connection before transfer of data can be started.
- e) UDP provides a connection-oriented transport service to an application using it.
- f) The TCP segment contains no checksum field.
- g) A TCP connection provides only a one-way (simplex) transport service.
- h) The UDP segment includes a checksum for error detection.

B:

- a) UDP gir en pålitelig overføringstjeneste for en applikasjon som bruker den.
- b) TCP gir en upålitelig overføringstjeneste for en applikasjon som bruker den.
- c) UDP bruker overbelastningskontroll.
- d) UDP setter opp en end-til-ende forbindelse før data kan overføres.
- e) UDP gir en forbindelsesorientert overføringstjeneste for en applikasjon som bruker den.
- f) TCP segmentet inneholder ikke sjekksum-felt.
- g) En TCP forbindelse gir kun en en-veis (simpleks) overføringstjeneste.
- h) UDP segmentet inneholder en sjekksum for feildeteksjon.

N:

- a) UDP gir ei påliteleg overføringsteneste for ein applikasjon som bruker han.
- b) TCP gir ei upåliteleg overføringsteneste for ein applikasjon som bruker han.
- c) UDP bruker overbelastningskontroll.
- d) UDP set opp eit end-til-ende samband før data kan overførast.
- e) UDP gir ei sambandsorientert overføringsteneste for ein applikasjon som bruker han.
- f) TCP segmentet inneheld ikkje sjekksum-felt.
- g) Eit TCP samband gir berre ein ein-veis (simpleks) overføringsteneste.
- h) UDP segmentet inneheld ein sjekksum for feildeteksjon.

1.4

E: Which (if any) of the remainders (R) from CRC calculations are correct for the given data (D) and generator (G) values?

B: Hvilke (om noen) av restene (R) fra CRC beregninger er korrekte, for de oppgitte data (D) og generator (G) verdiene?

N: Kva for (om nokon) restar (R) er riktige, for dei gjevne data (D) og generator (G) verdiane?

- a) D = 101110, G = 1001, R = 001
- b) D = 101110, G = 1001, R = 100
- c) D = 101110, G = 1001, R = 011
- d) D = 1010101010, G = 10011, R = 0100
- e) D = 1010101010, G = 10011, R = 1010
- f) D = 1010101010, G = 10011, R = 0000
- g) D = 11111, G = 1011, R = 110
- h) D = 11111, G = 1011, R = 100
- i) D = 11111, G = 1011, R = 001

1.5

No.	Source	Destination	Protocol	Length	Info
1	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xed2c39ac
2	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xed2c39ac
3	129.241.67.129	129.241.67.134	DHCP	342	DHCP Offer - Transaction ID 0xed2c39ac
4	129.241.67.129	129.241.67.220	DHCP	342	DHCP Offer - Transaction ID 0xed2c39ac
5	0.0.0.0	?	DHCP	342	DHCP Request - Transaction ID 0xed2c39ac
6	129.241.67.129	?	DHCP	342	DHCP ACK - Transaction ID 0xed2c39ac
7	Apple_44:c6:33	Broadcast	ARP	42	Who has 129.241.67.129? Tell 129.241.67.134
8	Cisco_0b:d9:c2	Apple_44:c6:33	ARP	60	129.241.67.129 is at 40:55:39:0b:d9:c2
9	129.241.67.134	129.241.0.200	DNS	74	Standard query 0x4d2e A www.google.com
10	129.241.0.200	129.241.67.134	DNS	90	Standard query response 0x4d2e A www.google.com
11	129.241.67.134	216.58.209.100	TCP	78	55485 > http(80) [SYN] Seq=0 Win=65535 Len=0 MS
12	216.58.209.100	129.241.67.134	TCP	74	http(80) > 55485 [SYN, ACK] Seq=0 Ack=1 Win=4254
13	129.241.67.134	216.58.209.100	TCP	66	55485 > http(80) [ACK] Seq=1 Ack=1 Win=131872 Len=0
14	129.241.67.134	216.58.209.100	HTTP	614	GET / HTTP/1.1
15	216.58.209.100	129.241.67.134	TCP	66	http(80) > 55485 [ACK] Seq=1 Ack=549 Win=43648 Len=0
16	216.58.209.100	129.241.67.134	HTTP	586	HTTP/1.1 302 Found (text/html)
17	129.241.67.134	216.58.209.100	TCP	66	55485 > http(80) [ACK] Seq=549 Ack=521 Win=1313
18	129.241.67.134	129.241.0.200	DNS	73	Standard query 0x0e58 A www.google.no
19	129.241.0.200	129.241.67.134	DNS	89	Standard query response 0x0e58 A www.google.no
20	129.241.67.134	216.58.209.99	TCP	78	55486 > http(80) [SYN] Seq=0 Win=65535 Len=0 MS
21	216.58.209.99	129.241.67.134	TCP	74	http(80) > 55486 [SYN, ACK] Seq=0 Ack=1 Win=4254
22	129.241.67.134	216.58.209.99	TCP	66	55486 > http(80) [ACK] Seq=1 Ack=1 Win=131872 Len=0
23	129.241.67.134	216.58.209.99	HTTP	647	GET /?gfe_rd=cr&ei=MBrwVNzBDaur8wep9IAQ HTTP/1
24	216.58.209.99	129.241.67.134	TCP	66	http(80) > 55486 [ACK] Seq=1 Ack=582 Win=43776 Len=0
25	216.58.209.99	129.241.67.134	HTTP	672	HTTP/1.1 302 Found (text/html)
26	129.241.67.134	216.58.209.99	TCP	66	55486 > http(80) [ACK] Seq=582 Ack=607 Win=1312

Figure 1: Wireshark trace

E: Figure 1 shows packets sent over a network of type ethernet. Which (if any) of the following statements about packets in the trace are correct?

- a) Line 5 destination address is 129.241.67.129.
- b) All packets include an IP protocol header.
- c) The TCP connections use options.
- d) The TCP connections are set-up to send packets in parallel.
- e) All application protocols use TCP end-to-end.
- f) First hop router cannot be 129.241.67.129.
- g) The TCP ACK segments have a TCP header of length 46 bytes.
- h) All packets are forwarded by a router.

B: Figur 1 viser pakker som sendes over et nettverk av type ethernet. Hvilke (om noen) av påstandene om pakkene i figuren er korrekte?

- a) Linje 5 destinasjonsadresse er 129.241.67.129.
- b) Alle pakkene inkluderer et IP protokollhode.
- c) TCP-forbindelsene benytter opsjoner.
- d) TCP-forbindelsene er satt opp til å sende pakker i parallell.
- e) Alle applikasjonsprotokollene bruker TCP ende-til-ende.
- f) First hopp ruter kan ikke være 129.241.67.129.
- g) TCP ACK-segmentene har et TCP hode på 46 byte.
- h) Alle pakkene blir videresendt av en ruter.

N: Figur 1 viser pakkar som vert sende over eit nettverk av type ethernet. Kva for (om nokon) av påstandane om pakkane i figuren er korrekte?

- a) Linje 5 destinasjonsadresse er 129.241.67.129.
- b) Alle pakkar inkluderer eit IP protokollhovud.
- c) TCP-forbindelsene nyttar opsjonar.
- d) TCP-forbindelsene er sett opp til å senda pakkar i parallell.
- e) Alle applikasjonsprotokollane bruker TCP ende-til-ende.
- f) First hopp ruter kan ikkje vera 129.241.67.129.
- g) TCP ACK-segmentene har eit TCP hovud på 46 byte.
- h) Alle pakkar blir vidaresende av ein ruter.

1.6

Figure 1 displays eight 5x5 binary matrices, labeled a) through h), arranged in two rows of four. Each matrix consists of a 4x4 grid of elements (rows 1-4, columns 1-4) and a single element in the fifth column (row 5, column 5). The elements are either 0 or 1. The matrices are defined as follows:

- a)**

1	0	0	1	1
0	1	1	0	1
0	0	1	0	0
1	1	1	0	0
1	1	0	0	1
- b)**

1	0	0	0	0
0	1	1	0	1
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
- c)**

1	0	0	1	1
0	1	1	1	1
0	0	1	0	0
1	1	1	0	0
1	1	0	1	0
- d)**

1	0	0	0	1
0	1	1	0	1
0	0	1	0	0
1	1	1	0	0
1	1	0	0	1
- e)**

1	0	0	1	1
0	1	0	0	0
0	0	1	0	1
1	1	1	0	0
1	0	0	0	1
- f)**

1	0	0	1	1
0	1	1	0	1
0	0	0	0	0
1	1	1	0	0
1	1	0	0	0
- g)**

1	1	0	1	1
0	1	1	0	1
0	1	1	0	0
1	1	1	0	0
1	1	0	0	0
- h)**

1	0	0	1	0
0	1	0	0	1
0	0	1	0	1
1	1	1	0	0
0	0	0	1	1

Figure 2: Potential implementations of the two-dimensional even parity scheme.

E: Which (if any) of the alternatives in Figure 2 show correct implementation of a two-dimensional even parity scheme?

B: Hvilke (om noen) av alternativene i Figur 2 viser korrekt implementering av en two-dimensjonal lik («even») paritets ordning?

N: Kva for (om nokon) av alternativa i Figur 2 viser korrekt implementering av ein two-dimensjonal lik («even») paritets ordning?

1.7

E: Which (if any) of the following statements are correct related to the Internet Protocol (IP), versions 4 and 6?

B: Hvilke (om noen) av følgende påstander er korrekte, relatert til IP, versjon 4 og 6?

N: Kva for (om nokon) av følgjande påstandar er korrekte, relatert til IP, versjon 4 og 6?

E:

- a) IPv4 uses 48 bit addresses.
- b) IPv6 uses 132 bit addresses.
- c) IPv4 does not allow routers inside the network to do any fragmentation of packets.
- d) IPv6 does allow routers inside the network to assemble fragments back into packets.
- e) IPv6 has no header checksum.
- f) IPv4 has no header checksum.
- g) IPv6 provides a reliable, connection-oriented transport service.
- h) IPv4 provides a reliable, connection-oriented transport service.

B:

- a) IPv4 bruker adresser med 48 bit.
- b) IPv6 bruker adresser med 132 bit.
- c) IPv4 tillater ikke rutere i nettet å fragmentere pakker.
- d) IPv6 tillater rutere i nettet å sette sammen fragmenter til pakker.
- e) IPv6 har ingen sjekksum i protokollhodet.
- f) IPv4 har ingen sjekksum i protokollhodet.
- g) IPv6 gir en pålitelig, forbindelsesorientert overføringstjeneste.
- h) IPv4 gir en pålitelig, forbindelsesorientert overføringstjeneste.

N:

- a) IPv4 bruker adresser med 48 bits.
- b) IPv6 bruker adresser med 132 bits.
- c) IPv4 tillèt ikkje ruterar i nettet å fragmentera pakkar.
- d) IPv6 tillèt ruterar i nettet å setja saman fragment til pakkar.
- e) IPv6 har ingen sjekksum i protokollhovudet.
- f) IPv4 har ingen sjekksum i protokollhovudet.
- g) IPv6 gir ei påliteleg, forbindelsesorientert overføringsteneste.
- h) IPv4 gir ei påliteleg, forbindelsesorientert overføringsteneste.

1.8

E: Which (if any) of the following definitions related to Quality of Service (QoS) are correct?

B: Hvilke (om noen) av de følgende definisjonene relatert til tjenestekvalitet (QoS) er korrekte?

N: Kva for (om nokon) av dei følgjande definisjonane relatert til tenestekvalitet (QoS) er korrekte?

E:

- a) Propagation delay is the physical delay of sending bits end-to-end over a transmission link.
- b) Transmission delay is the physical delay of sending bits end-to-end over a transmission link.
- c) Propagation delay is the time needed to put all bits of a packet out on a transmission link, e.g. from a buffer.
- d) Queuing delay in a router is influenced by the propagation delay.
- e) End-to-end delay is the total time of sending an information unit from a source to a destination in a network.
- f) End-to-end delay is the total time of sending an information unit from a source to a destination in a network and back again.
- g) Processing delay is the physical delay of sending bits end-to-end over a transmission link.
- h) Transmission delay is the time needed for analyzing an information unit (e.g. to find outgoing address) in a router.
- i) End-to-end throughput is given by the maximum capacity link used.

B:

- a) Forplantningsforsinkelse ("Propagation delay") er den fysiske forsinkelsen ved å sende bits ende-til-ende over en transmisjonslink.
- b) Transmisjonsforsinkelse ("Transmission delay") er den fysiske forsinkelsen ved å sende bits ende-til-ende over en transmisjonslink.
- c) Forplantningsforsinkelse ("Propagation delay") er tiden som er nødvendig å bruke for å få lagt alle bitene i en pakke ut på transmisjonslinken, f.eks. fra et buffer.
- d) Køforsinkelse ("Queuing delay") i en ruter påvirkes av forplantningsforsinkelsen ("Propagation delay").
- e) Ende-til-ende forsinkelsen ("End-to-end delay") er den totale tiden det tar å sende en informasjonsenhet fra en kilde til en destinasjon i et nett.
- f) Ende-til-ende forsinkelsen ("End-to-end delay") er den totale tiden det tar å sende en informasjonsenhet fra en kilde til en destinasjon i et nett og tilbake igjen.
- g) Prosesseringsforsinkelse ("Processing delay") er den fysiske forsinkelsen ved å sende bits ende-til-ende over en transmisjonslink.
- h) Transmisjonsforsinkelse ("Transmission delay") er tiden som trengs for å analysere en informasjonsenhet (f.eks. for å finne utgående adresse) i en ruter.
- i) Ende-til-ende gjennomstrømning ("End-to-end throughput") er gitt av linken med maksimum kapasitet.

N:

- a) Forplantningsforseinking ("Propagation delay") er den fysiske forseinkinga ved å senda bitar ende-til-ende over ein transmisjonslink.
- b) Transmisjonsforseinking ("Transmission delay") er den fysiske forseinkinga ved å senda bitar ende-til-ende over ein transmisjonslink.
- c) Forplantningsforseinking ("Propagation delay") er tida som er nødvendig å bruka for å få lagt alle bitane i ei pakke ut på transmisjonslinken, t.d. frå eit buffer.
- d) Køforseinking ("Queuing delay") i ein ruter blir påverka av forplantningsforseinkinga ("Propagation delay").
- e) Ende-til-ende forseinkinga ("End-to-end delay") er den totale tida det tar å senda ei informasjonseining frå ei kjelde til ein destinasjon i eit nett.
- f) Ende-til-ende forseinkinga ("End-to-end delay") er den totale tida det tar å senda ei informasjonseining frå ei kjelde til ein destinasjon i eit nett og tilbake igjen.
- g) Prosesseringsforsinkelse ("Processing delay") er den fysiske forseinkinga ved å senda bitar ende-til-ende over ein transmisjonslink.

- h)** Transmisjonsforseinking (“Transmission delay”) er tida som trengst for å analysa ei informasjonseining (t.d. for å finna utgående adresse) i ein ruter.
- i)** Ende-til-ende gjennomstrauming (“End-to-end throughput”) er gitt av linken med maksimum kapasitet.

1.9

E: Which (if any) of the following statements are true, related to the area of information security?

B: Hvilke (om noen) av følgende påstander er sanne, relatert til informasjonssikkerhet?

N: Kva for (om nokon) av følgjande påstandar er sanne, relatert til informasjonssikkerheit?

E:

- a)** Public key encryption is an example of symmetric key cryptography.
- b)** Use of a cryptographic hash function and a shared authentication key together is sufficient to achieve message integrity.
- c)** SSL is used for securing TCP connections.
- d)** SSL is used for securing IP connections.
- e)** A message authentication code (MAC) is used to achieve message integrity.
- f)** Public key encryption is based on using only public keys.
- g)** Digital signatures can be realized by using a combination of public key encryption and public key certification.
- h)** The IEEE 802.11 WEP protocol (from 1999) for securing wireless LANs is still regarded as giving a high level of security.

B:

- a)** Offentlig nøkkel kryptering er et eksempel på symmetrisk nøkkel kryptering.
- b)** Bruk av en kryptografisk «hash»-funksjon og en felles autentiseringsnøkkel er tilstrekkelig til å oppnå meldingsintegritet.
- c)** SSL brukes til å sikre TCP forbindelser.
- d)** SSL brukes til å sikre IP forbindelser.
- e)** En meldingsautentiseringskode (MAC) brukes til å oppnå meldingsintegritet.
- f)** Offentlig nøkkelkryptering er basert på bruk av bare offentlige nøkler.
- g)** Digitale signaturer kan realiseres ved å bruke en kombinasjon av offentlig nøkkel kryptering og offentlig nøkkel sertifisering.
- h)** IEEE 802.11 WEP-protokollen (fra 1999) for å sikre trådløse LAN anses fortsatt å gi et høyt sikkerhetsnivå.

N:

- a)** Offentleg nøkkel kryptering er eit døme på symmetrisk nøkkel kryptering.
- b)** Bruk av ein kryptografisk «hash»-funksjon og ein felles autentiseringsnøkkel er tilstrekkeleg til å oppnå meldingsintegritet.
- c)** SSL blir brukt til å sikra TCP samband.
- d)** SSL blir brukt til å sikra IP samband.
- e)** Ein meldingsautentiseringskode (MAC) blir brukt til å oppnå meldingsintegritet.
- f)** Offentleg nøkkelkryptering er basert på bruk av berre offentlege nøklar.
- g)** Digitale signaturar kan realiserast ved å bruka ein kombinasjon av offentleg nøkkel kryptering og offentleg nøkkel sertifisering.
- h)** IEEE 802.11 WEP-protokollen (frå 1999) for å sikra trådlause LAN blir framleis sedde på å gi eit høgt tryggningsnivå.

1.10

E: Circuit switching and packet switching have many differences. Which (if any) of the following statements are true?

B: Linjesvitsjing og pakkesvitsjing har mange ulikheter. Hvilke (om noen) av følgende påstander er sanne?

N: Linjesvitsjing og pakkesvitsjing har mange forskjellar. Kva for (om nokon) av følgjande påstandar er sanne?

E:

- a) In a circuit switched network, there is little or no delay variation among packets/messages, while in a packet-switched network, delay variation can be large.
- b) A circuit-switched network cannot guarantee a certain amount of end-to-end bandwidth for a connection, but a packet-switched network can.
- c) Both packet switching and circuit switching use the end system network address in the same way.
- d) A circuit switched network does need to use buffers inside a network to handle queues at outgoing network links, while a packet switched network do not.
- e) Both circuit switching and packet switching can provide connection-oriented services.
- f) Loss of information due to contention at outgoing links is possible in a circuit switched network but not in a packet switched network.
- g) Both circuit switching and packet switching can provide connectionless transport services.
- h) A circuit switched network can be built on top of a packet switched network.

B:

- a) I et linjesvitsjet nett er det liten eller ingen variasjon i forsinkelse mellom pakker/meldinger, men i et pakkesvitsjet nett kan det være store variasjoner i forsinkelse.
- b) Et linjesvitsjet nett kan ikke garantere en gitt mengde ende-til-ende båndbredde for en forbindelse, men det kan et pakkesvitsjet nett.
- c) Både pakkesvitsjing og linjesvitsjing bruker nettverksadressen til endesystemet på samme måte.
- d) Et linjesvitsjet nett må bruke buffere i nettet for å håndtere kø ved utgående linker, mens et pakkesvitsjet nett ikke trenger å gjøre dette.
- e) Både linjesvitsjing og pakkesvitsjing kan tilby forbindelses-orienterte tjenester.
- f) Tap av informasjon på grunn av kødannelse ved utgående linker er mulig i et linjesvitsjet nett, men ikke i et pakkesvitsjet nett.
- g) Både linjesvitsjing og pakkesvitsjing kan brukes for å realisere forbindelsesløse overføringstjenester.
- h) Et linjesvitsjet nett kan bygges på toppen av et pakkesvitsjet nett.

N:

- a) I eit linjesvitsjet nett er det liten eller ingen variasjon i forseinking mellom pakkar/meldingar, men i eit pakkesvitsjet nett kan det vera store variasjonar i forseinking.
- b) Eit linjesvitsjet nett kan ikkje garantera ei gitt mengde ende-til-ende bandbreidde for eit samband, men det kan eit pakkesvitsjet nett.
- c) Både pakkesvitsjing og linjesvitsjing bruker nettverksadressa til endesystemet på same måte.
- d) Eit linjesvitsjet nett må bruka bufferar i nettet for å handtera kø ved utgående linkar, medan eit pakkesvitsjet nett ikkje treng å gjera dette.
- e) Både linjesvitsjing og pakkesvitsjing kan tilby forbindelses-orienterte tenester.
- f) Tap av informasjon på grunn av kødannelse ved utgående linkar er mogleg i eit linjesvitsjet nett, men ikkje i eit pakkesvitsjet nett.
- g) Både linjesvitsjing og pakkesvitsjing kan brukast for å realisera forbindelseslause overføringstenester.
- h) Eit linjesvitsjet nett kan byggast på toppen av eit pakkesvitsjet nett.

2. Forsinkelse og gjennomstrømning / Delays and throughput (20 p)(5+5+5+5)

E: Each subtask below has exactly **one** correct answer. If you choose more than one answer you get zero points on this subtask.

B: Hver deloppgave nedenfor har kun **ett** riktig svar. Hvis du velger flere enn ett svar får du null poeng på deloppgaven.

N: Kvar deloppgave nedanfor har berre **eitt** riktig svar. Velger du meir enn eit svar får du null poeng på denne deloppgåva.

NB! 1200K bytes = 1 200 000 bytes; 1200M bytes = 1 200 000 000 bytes below/nedenfor.
(i.e. /dvs. 1 kilobyte \neq 1024 bytes)

2.1

E: Consider sending a file of 1200K bytes from Host A to Host B over a circuit-switched network. Suppose it takes 100 ms to establish an end-to-end circuit between Host A and Host B before Host A can begin to transmit the file. Also suppose the end-to-end circuit pass through four cross-connect switches and traverse five optical fiber links with lengths 450 km, 450 km, 800 km, 1200 km, and 500 km respectively. On each link the circuit has a transmission rate of 640 Kbit/s. How much time does it minimum take to send the file from Host A to Host B? (Assume a speed of light in fiber of 200 000 000 m/s).

B: En datafil på 1200K bytes sendes fra Host A til Host B over et linjesvitsjet nett. Anta at det tar 100 ms å opprette en ende-til-ende forbindelse mellom Host A og Host B før Host A kan begynne å sende datafilen. Anta videre at ende-til-ende forbindelsen passerer gjennom fire cross-connect svitsjer og fem optiske fiber lenker med lengder på henholdsvis 450 km, 450 km, 800 km, 1200 km, og 500 km. Hver lenke har en transmisjonsrate på 640 Kbit/s. Hvor lang tid vil det minst ta å sende datafilen fra Host A til Host B? (Anta en lyshastighet i fiber lik 200 000 000 m/s).

N: Ei datafil på 1200K bytes vert sendt frå Host A til Host B over eit linjesvitsja nett. Sett at det tar 100 ms å oppretta eit ende-til-ende samband mellom Host A og Host B før Host A kan begynne å sende datafila. Anta vidare at ende-til-ende sambandet passerer gjennom fire cross-connect svitsjar og fem optiske fiber lenker som har lengdene 450 km, 450 km, 800 km, 1200 km, og 500 km. Kvar lenke har ei transmisjonsrate på 640 Kbit/s. Kor lang tid vil det minst ta å senda datafila fra Host A til Host B? (Anta ei lyshastighet i fiber lik 200 000 000 m/s).

- a) 1.992 s
- b) 75.017 s
- c) 60.117 s
- d) 7.617 s
- e) 1.975017 s
- f) 75.117 s
- g) 15.117 s
- h) 15.100017 s

2.2

E: Consider sending a file of 1200K bytes from Host A to Host B over a connectionless packet switched network. Assume that the whole file is sent as one large packet, i.e. without any fragmentation. Suppose the end-to-end path passes through four store-and-forward routers, traversing five optical fiber links with lengths 450 km, 450 km, 800 km, 1200 km, and 500 km respectively, and each link has a transmission rate of 640 Kbit/s. What is the minimum time needed to send the file from Host A to Host B? (Assume a speed of light in fiber of 200 000 000 m/s).

B: En datafil på 1200K bytes skal sendes fra Host A til Host B over et forbindelsesløst

pakkesvitsjet nett. Anta at hele filen sendes som en stor pakke, dvs. uten fragmentering. Anta vidare at ende-til-ende stien pakken følger går gjennom fire «store-and-forward» rutere, og over fem lenker med lengder på henholdvis 450 km, 450 km, 800 km, 1200 km, og 500 km. Hver lenke har en transmisjonsrate på 640 Kbit/s. Hvor lang tid vil det minimum ta å overføre denne filen fra Host A til Host B? (Anta en lyshastighet i fiber lik 200 000 000 m/s).

N: Ei datafil på 1200K bytes skal sendast frå Host A til Host B over eit sambandslaust pakkesvitsjet nett. Anta at heile fila vert sendt som ein stor pakke, dvs. utan fragmentering. Anta vidare at ende-til-ende stigen pakken følgjer går gjennom fire «store-and-forward» ruterar, og over fem lenker med lengder på 450 km, 450 km, 800 km, 1200 km, og 500 km. Kvar lenke har ei transmisjonsrate på 640 Kbit/s. Kor lang tid vil det minimum ta å overføra denne fila frå Host A til Host B? (Anta ei lyshastighet i fiber lik 200 000 000 m/s).

- a) 1.992 s
- b) 75.017 s
- c) 60.117 s
- d) 7.617 s
- e) 1.975017 s
- f) 75.117 s
- g) 15.117 s
- h) 15.100017 s

2.3

E: Consider a broadcast channel with 10 nodes and transmission rate of 100 Mbit/s. The broadcast channel uses polling (with an additional polling node) for multiple access. The polling delay, which is the amount of time from when a node completes transmission until the subsequent node is permitted to transmit, is 1ms. Suppose that within a polling round, a given node is allowed to transmit at most 100K bits. What is the maximum throughput of the broadcast channel?

B: Ta utgangspunkt i en kringkastingskanal (broadcast channel) med 10 noder og en transmisjonsrate på 100 Mbit/s. Kringkastingskanalen bruker 'polling' (med en ekstra 'polling node') for multippel aksess. Polling-forsinkelsen, som er tiden det tar fra en node fullfører sin transmisjon til den neste noden får lov til å starte sin transmisjon, er 1ms. Anta at hver node har lov til å sende opptil 100K bit innenfor en 'polling-runde'. Hva er da den maksimale gjennomstrømningen (throughput) for kringkastingskanalen?

N: Ta utgangspunkt i ein kringkastingskanal (broadcast channel) med 10 nodar og ein transmisjonsrate på 100 Mbit/s. Kringkastingskanalen nyttar 'polling' (med ein ekstra 'polling node') for multippel aksess. Polling-forseinkinga, som er tida det tar frå ei node fullfører sin transmisjon til den neste noden får lov til å starte sin transmisjon, er 1ms. Anta at kvar node har lov til å sende opptil 100K bit innafor ein 'polling-runde'. Kva er da den maksimale gjennomstrauminga (throughput) for kringkastingskanalen?

- a) 75 Mbit/s
- b) 25 Mbit/s
- c) 12.5 Mbit/s
- d) 10 Mbit/s
- e) 5 Mbit/s
- f) 2.5 Mbit/s
- g) 1.25 Mbit/s
- h) 50 Mbit/s

2.4

E: Consider two hosts that are connected by a channel. The channel has a transmission rate of 100 Mbit/s. The maximum packet size in the network is 10K bytes. Assume the stations are far apart so the propagation delay between the two hosts is 30 ms. Assume that acknowledgements can be issued immediately when the last bit of a packet has been received (i.e. processing delay is ignored) and that the ACK packets are so small that their transmission times can be ignored. What is the maximum data rate that can be achieved by the **stop-and-wait** flow control protocol in this situation?

B: Gitt to verter (hosts) som er sammenkoblet av en kanal. Kanalen har en transmisjonsrate på 100 Mbit/s. Den maksimale pakkestørrelsen i nettet er 10K bytes. Anta at vertene er langt fra hverandre så propagasjonsforsinkelsen mellom de to vertene (hosts) er på 30 ms. Anta at kvitteringer (ACK) sendes umiddelbart når siste bit i pakken er mottatt (dvs. prosesseringsforsinkelse ignoreres) og at kvitteringene (ACK) er så små at transmisjonsforsinkelser for disse kan ignoreres. Hva er den maksimale datarate som kan oppnås når ”**stop-and-wait**” flytkontroll protokollen brukes?

N: Gitt to vertar (hosts) som er sammenkoble av ein kanal. Kanalen har ei transmisjonsrate på 100 Mbit/s. Den maksimale pakkestørrelsen i nettet er 10K bytes. Anta at dei to vertane er langt frå kvarandre så propagasjonsforseinkinga mellom dei to vertane (hosts) er på 30 ms. Anta at kvitteringar (ACK) sendes med ein gong når siste bit i pakken er motteken (dvs. prosesseringsforseinkinga ignorerast) og at kvitteringane (ACK) er så små at transmisjonsforseinkingane for desse kan ignorerast. Kva er den maksimale datarate som kan nåast når ein nyttar ”**stop-and-wait**” flytkontroll protokollen?

- a) 96.385542 Mbit/s
- b) 93.023256 Mbit/s
- c) 0.166389 Mbit/s
- d) 1.315789 Mbit/s
- e) 2.597403 Mbit/s
- f) 0.332226 Mbit/s
- g) 23.185112 Mbit/s
- h) 65.887734 Mbit/s

3. Mix / Miks (20 p)(4+4+4+4+4)

E: Each subtask below has exactly **one** correct answer. If you choose more than one answer you get zero points on this subtask.

B: Hver deloppgave nedenfor har kun **ett** riktig svar. Hvis du velger flere enn ett svar får du null poeng på deloppgaven.

N: Kvar deloppgåve nedanfor har berre **eitt** riktig svar. Velger du meir enn eit svar får du null poeng på denne deloppgåva.

3.1

E: Identify the ciphertext you end up with when using the Caesar cipher with distance 5 to encrypt the text: “What do you say to the God of death? Not today”.

B: Identifiser den krypterte teksten du ender opp med når du bruker Caesar cipher med avstand 5 for å kryptere teksten: “What do you say to the God of death? Not today”.

N: Identifiser den krypterte teksten du endar opp med når du bruker Caesar cipher med avstand 5 for å kryptera teksten: “What do you say to the God of death? Not today”.

- a) Hwlz mr ked lke bw pla Okl vw hkweu? Rke bdoex.
- b) Alex kr csy wec ok ndr Mkw me bsrth? Zdr mwsrj.
- c) Bmfy it dtz xfd yt ymj Lti tk ijfym? Sty ytifd.
- d) Mrfz ke xun wlk cr iks Pts bw khnts? Hty nwzau.
- e) Hwlz mr dtz wec xs pla Okl vw klsrd? Rke bslrd.
- f) Mrfz kr ned wec ok ymc Wks le mestd? Mus stien.
- g) Alex hs csy wec xs xli Ksh sj hiexl? Rxs xshec.
- h) Bmfy kr ned zrg lw mrt Lti wg merdt? Hwe vstkd.

3.2

E: Assume that you want to send a confidential and digitally signed contract via a public network. Which combination of information security services and mechanisms are needed to do this securely?

B: Anta at du vil sende en konfidensiell og digitalt signert kontrakt via et offentlig nettverk. Hvilken kombinasjon av informasjonssikkerhetstjenester og -mekanismer er nødvendig for å gjøre dette sikkert?

N: Anta at du vil senda ein konfidensiell og digitalt signert kontrakt via eit offentleg nettverk. Kva for ein kombinasjon av informasjonstryggingstenester og -mekanismar er nødvendig for å gjera dette sikkert?

w = Digital Signature

x = Message Authentication Code (MAC)

y = Certification Authority (CA)

z = Encryption

E:

- a) w, x, y and z (i.e. all four)
- b) only x
- c) w, x and z but not y
- d) only y
- e) w, y and z but not x
- f) x and z, not w or y
- g) only z
- h) none (i.e. none of the four)

B:

- a) w, x, y og z (dvs. alle fire)
- b) kun x
- c) w, x og z men ikke y
- d) kun y
- e) w, y og z men ikke x
- f) x og z, ikke w eller y
- g) kun z
- h) ingen (dvs. ingen av de fire)

N:

- a) w, x, y og z (dvs. alle fire)
- b) berre x
- c) w, x og z men ikkje y
- d) berre y
- e) w, y og z men ikkje x

- f) x og z, ikkje w eller y
- g) berre z
- h) ingen (dvs. ingen av dei fire)

3.3

E: Assume that a company needs to partition its allocated IP address range (200.23.96.0/21) into four different parts, to cater to different needs. The main administration (ADM) needs at least 1000 addresses, the sales department (SAL) needs at least 500 addresses, the manufacturing department (MAN) needs at least 200 addresses, and the research and developing department (R&D) needs at least 100 addresses. Which of the following alternatives represent the numbering plan best suited for this situation? (Hint: We want to allocate the minimum needed number of IP addresses to each subnet - to keep a pool of spare addresses for potential later use - and all subnets must be uniquely defined within the allocated address range).

B: Anta at et selskap må dele opp sitt tildelte IP adresseområde (200.23.96.0/21) i fire forskjellige deler for å imøtekomme ulike behov. Hovedadministrasjonen (ADM) trenger minst 1000 adresser, salgsavdelingen (SAL) trenger minst 500 adresser, produksjonsavdelingen (MAN) trenger minst 200 adresser, og forsknings- og utviklingsavdelingen (FoU) trenger minst 100 adresser. Hvilken av følgende alternativer representerer nummerplanen som passer best for denne situasjonen? (Hint: Vi ønsker å tildele det minste nødvendige antall IP-adresser til hvert delnett - for å beholde reserve-adresser for potensiell senere bruk - og alle delnett må være unikt definert innenfor det tildelte adresseområdet).

N: Anta at eit selskap må dela opp sitt tildelte IP adresseområde (200.23.96.0/21) i fire ulike delar for å imøtekomme ulike behov. Hovudadministrasjonen (ADM) treng minst 1000 adresser, salsavdelinga (SAL) treng minst 500 adresser, produksjonsavdelinga (MAN) treng minst 200 adresser, og forskings- og utviklingsavdelinga (FoU) treng minst 100 adresser. Kva for ein av følgjande alternativ representerer nummerplanen som passar best for denne situasjonen? (Hitt: Vi ønsker å tildela den minste nødvendige mengda IP-adresser til kvart delnett - for å behalda reserve-adresser for potensiell seinare bruk - og alle delnett må vera unikt definert innanfor det tildelte adresseområdet).

- a) ADM: 200.23.96.0/22; SAL: 200.23.104.0/23; MAN: 200.23.108.0/24; R&D: 200.23.110.0/25
- b) ADM: 200.23.96.0/22; SAL: 200.23.104.0/23; MAN: 200.23.108.0/24; R&D: 200.23.110.0/24
- c) ADM: 200.23.97.0/22; SAL: 200.23.104.0/23; MAN: 200.23.108.0/24; R&D: 200.23.110.0/25
- d) ADM: 200.23.97.0/22; SAL: 200.23.104.0/23; MAN: 200.23.108.0/24; R&D: 200.23.110.0/24
- e) ADM: 200.23.97.0/22; SAL: 200.23.100.0/23; MAN: 200.23.102.0/24; R&D: 200.23.103.0/25
- f) ADM: 200.23.97.0/22; SAL: 200.23.100.0/23; MAN: 200.23.102.0/24; R&D: 200.23.103.0/24
- g) ADM: 200.23.96.0/22; SAL: 200.23.100.0/23; MAN: 200.23.102.0/24; R&D: 200.23.103.0/25
- h) ADM: 200.23.96.0/22; SAL: 200.23.100.0/23; MAN: 200.23.102.0/24; R&D: 200.23.103.0/24

3.4

E: Which of the following services are provided by the Domain Name System (DNS)?

B: Hvilke (om noen) av de følgende tjenestene tilbys av DNS?

N: Kva for (om nokon) av dei følgjande tenestene blir tilbodne av DNS?

E:

w = assist in server load distribution

x = translate hostnames to IP addresses

y = allocate an address to a host machine

z = translate alias hostnames into canonical hostnames

a) w, x, y and z (i.e. all four)

b) only x

- c) only y
- d) x and z, not w or y
- e) only z
- f) w, x and z but not y
- g) y and z, not w or x
- h) none (i.e. none of the four services listed)

B:

w = hjelpe til med lastfordeling over tjenere
 x = oversette vertsnavn til IP-adresser
 y = tilordne en adresse til en vertsmaskin
 z = oversette alias vertsnavn til kanoniske vertsnavn

- a) w, x, y og z (dvs. alle fire)
- b) bare x
- c) bare y
- d) x og z, ikke w eller y
- e) bare z
- f) w, x og z men ikke y
- g) y og z, ikke w eller x
- h) ingen (det vil si ingen av de fire tjenestene som er oppført)

N:

w = hjelpa til med lastfordeling over tenarar
 x = oversette vertsnamn til IP-adresser
 y = tilordna ei adresse til ein vertsmaskin
 z = oversette alias vertsnamn til kanoniske vertsnamn

- a) w, x, y og z (dvs. alle fire)
- b) berre x
- c) berre y
- d) x og z, ikkje w eller y
- e) berre z
- f) w, x og z men ikkje y
- g) y og z, ikkje w eller x
- h) ingen (det vil seia ingen av dei fire tenestene som er oppførte)

3.5

E: Which of the following elements is part of the Medium Access Control (MAC) for wireless LANs following the 802.11 standard (including optional parts)?

B: Hvilke av følgende elementer er en del av medium aksess kontrollen (MAC) for trådløse LAN som følger 802.11-standarden (inkludert opsjonelle tillegg)?

N: Kva for av følgjande element er ein del av medium aksess kontrollen (MAC) for trådlause LAN som følgjer 802.11-standarden (inkludert opsjonelle tillegg)?

v = Request to Send / Clear to Send (RTS/CTS)
 w = Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
 x = Acknowledgement (ACK)
 y = Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
 z = Distributed Inter-frame Space (DIFS)

E:

- a) v, x, y and z, but not w.
- b) v, w and z, but not x or y.
- c) v, w, x and z but not y.
- d) v, x and y, but not w or z.
- e) x, y and z, but not v or w.
- f) only w.
- g) v, x and y, but not w or z.
- h) only y.

B:

- a) v, x, y og z, men ikke w.
- b) v, w og z, men ikke x eller y.
- c) v, w, x og z men ikke y.
- d) v, x og y, men ikke w eller z.
- e) x, y og z, men ikke v eller w.
- f) kun w.
- g) v, x og y, men ikke w eller z.
- h) kun y.

N:

- a) v, x, y og z, men ikkje w.
- b) v, w og z, men ikkje x eller y.
- c) v, w, x og z men ikkje y.
- d) v, x og y, men ikkje w eller z.
- e) x, y og z, men ikkje v eller w.
- f) berre w.
- g) v, x og y, men ikkje w eller z.
- h) berre y.

4. Kortsvar oppgaver / Short answer tasks (20 p)(4+4+4+4+4)

Note:

E: Maximum three short sentences are allowed, to answer each question.

B: Det er lov å bruke maksimum tre korte setninger til å svare på hvert spørsmål.

N: Det er lov å bruka maksimum tre korte setningar til å svara på kvart spørsmål.

4.1

E: When an application in a host uses TCP to communicate with a server, what is the difference between a `ServerSocket` and a `ConnectionSocket`?

B: Når en applikasjon i en vert bruker TCP til å kommunisere med en tjener, hva er forskjellen mellom en «`ServerSocket`» og en «`ConnectionSocket`»?

N: Når ein applikasjon i ein vert bruker TCP til å kommunisera med ein tenar, kva er skilnaden mellom ein «`ServerSocket`» og ein «`ConnectionSocket`»?

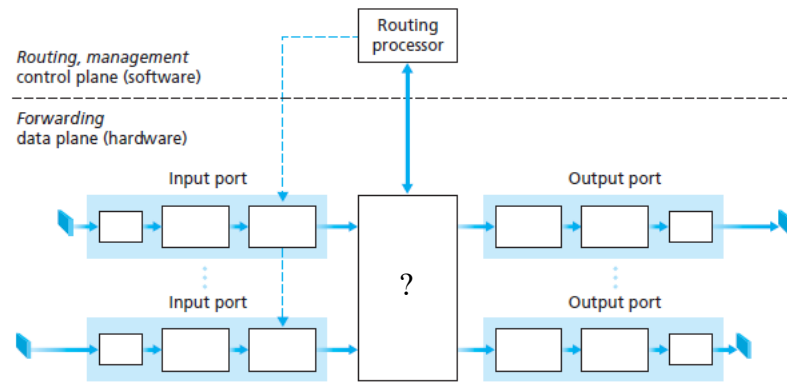


Figure 3: Generic router architecture

4.2

E: A generic router architecture is shown in Figure 3. What is the main function of the box marked with a “?”.

B: En generisk ruter-arkitektur er vist i Figur 3. Hva er hovedfunksjonen til boksen merket med «?» i figuren?

N: Ein generisk ruter-arkitektur er vist i Figur 3. Kva er hovudfunksjonen til boksen merka med «?» i figuren?

4.3

E: Does a TCP segment contain any address information? Give a short explanation of your answer.

B: Inneholder et TCP-segment noen adresseinformasjon? Gi en kort forklaring på svaret ditt.

N: Inneheld eit TCP-segment nokon adresseinformasjon? Gi ei kort forklaring på svaret ditt.

4.4

E: Compare the loss anticipation schemes Forward Error Correction (FEC) and Interleaving, used for Voice over IP, with regard to overhead and latency.

B: Sammenlign metodene «Forward Error Correction (FEC)» og «Interleaving», når brukt for å motvirke tap av informasjon i Voice over IP, med hensyn til overhead og tidsbruk/forsinkelse.

N: Samanlikn metodane «Forward Error Correction (FEC)» og «Interleaving», når brukt for å motverka tap av informasjon i Voice over IP, med omsyn til overhead og tidsbruk/forseinking.

No.	Time	Source	Source Port	Destination	Dest. Port	Protocol	Length	Info
87	16:38:22,023789	2a00:1450:400f:80b::200d	443	2001:4645:f082:0:783c:6926:5982:3601	54476	TLSv1.3	1294	Continuation Data
88	16:38:22,023836	2001:4645:f082:0:783c:6926:5982:3601	54476	2a00:1450:400f:80b::200d	443	TCP	74	54476 → 443 [ACK] Seq=518 Ack=2441 Win=
89	16:38:22,025029	2a00:1450:400f:80b::200d	443	2001:4645:f082:0:783c:6926:5982:3601	54476	TLSv1.3	688	Continuation Data
90	16:38:22,029610	2a00:1450:4010:c07::bc	5228	2001:4645:f082:0:783c:6926:5982:3601	54474	TCP	74	5228 → 54474 [ACK] Seq=1 Ack=518 Win=
91	16:38:22,029842	2a00:1450:4010:c07::bc	5228	2001:4645:f082:0:783c:6926:5982:3601	54474	TLSv1.3	1294	Server Hello, Change Cipher Spec
92	16:38:22,029843	2a00:1450:4010:c07::bc	5228	2001:4645:f082:0:783c:6926:5982:3601	54474	TLSv1.3	1294	Continuation Data
93	16:38:22,029911	2001:4645:f082:0:783c:6926:5982:3601	54474	2a00:1450:4010:c07::bc	5228	TCP	74	54474 → 5228 [ACK] Seq=518 Ack=2441 W
94	16:38:22,031599	2a00:1450:4010:c07::bc	5228	2001:4645:f082:0:783c:6926:5982:3601	54474	TLSv1.3	1294	Continuation Data
95	16:38:22,031822	2a00:1450:4010:c07::bc	5228	2001:4645:f082:0:783c:6926:5982:3601	54474	TLSv1.3	137	Continuation Data
96	16:38:22,031856	2001:4645:f082:0:783c:6926:5982:3601	54474	2a00:1450:4010:c07::bc	5228	TCP	74	54474 → 5228 [ACK] Seq=518 Ack=3724 W
97	16:38:22,036308	10.0.0.81	137	10.0.0.255	137	NBNS	92	Name query NB WPAD<00>
98	16:38:22,113495	2001:4645:f082:0:783c:6926:5982:3601	54475	2a00:1450:400f:80a::2004	443	TLSv1.3	138	Change Cipher Spec, Application Data
99	16:38:22,114565	2001:4645:f082:0:783c:6926:5982:3601	54473	2a00:1450:400f:80b::200a	443	TLSv1.3	138	Change Cipher Spec, Application Data
100	16:38:22,115990	2001:4645:f082:0:783c:6926:5982:3601	54476	2a00:1450:400f:80b::200d	443	TLSv1.3	138	Change Cipher Spec, Application Data
101	16:38:22,117326	2001:4645:f082:0:783c:6926:5982:3601	54474	2a00:1450:4010:c07::bc	5228	TLSv1.3	138	Change Cipher Spec, Application Data
102	16:38:22,118429	2001:4645:f082:0:783c:6926:5982:3601	54474	2a00:1450:4010:c07::bc	5228	TLSv1.3	251	Application Data
103	16:38:22,118434	2001:4645:f082:0:783c:6926:5982:3601	54475	2a00:1450:400f:80a::2004	443	TLSv1.3	160	Application Data

Figure 4: Wireshark trace

4.5

E: What type of source and destination addresses are shown in line no. 100 in the Wireshark trace given in Figure 4?

B: Hvilken type kilde- og destinasjonsadresser vises i linje nr. 100 i Wireshark utskriften gitt i Figur 4?

N: Kva for ein type kjelde- og destinasjonsadresser blir vist i linje nr. 100 i Wireshark utskriften gitt i figur 4?