

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgave i

TTM4100 KOMMUNIKASJON – TJENESTER OG NETT

Faglig kontakt under eksamen: Norvald Stol

Tlf.: 97080077

Eksamensdato: 15. mai 2018

Eksamenstid (fra-til): 0900-1300

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

Annen informasjon:

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

Målform/språk: Bokmål / Engelsk / Nynorsk

Antall sider: 14







Antall sider vedlegg: 21

Kontrollert av:

Dato

Sign

Regler/Rules/Reglar:

B: BOKMÅL	E: ENGLISH	N: NYNORSK
<p>Maksimum poengsum er 100. Oppgavesettet består av 2 deler:</p> <ul style="list-style-type: none"> • Del I, oppgavetekst, - denne del. • Del II, svarsidene, inkluderer svaralternativer for “riktig-galt” oppgaver og “skriftlige svar”-felter. Del II inkluderer også 3 sider for kommentarer relatert til formelle problemer i Del I eller Del II. Sidene kan også brukes for ”skriftlige svar”. <p>Del II skal leveres inn som ditt svar. To kopier av Del II blir levert ut. Bare en kopi skal innleveres som ditt svar. Kandidatnummeret skal skrives på alle svarark. Skriv ikke utenfor boks-feltene. Bruk svart eller blå penn, ikke blyant. Skriftlig svar oppgave skal besvares innenfor den tildelte boksen i Del II.</p> <p>Riktig-Galt oppgaver besvares ved ett kryss for hvert utsagn, eller la være å sette kryss. Hvis både 'Riktig' og 'Galt' er krysset av for et utsagn, teller det som feil.</p> <p>Kryss av slik:  Hvis du har krysset av feil boks, skraver den fullstendig, slik:  Kryss deretter av i korrekt boks. Korrigering på andre måter er ikke tillatt.</p> <p>For hver gruppe av 10 Riktig/Galt spørsmål: Poeng = Max{(antall rette avkryssninger – straffepoeng), 0} * 1 feil gir ingen straffepoeng; * 2 feil gir 1,5 straffepoeng; * i > 2 feil gir i straffepoeng.</p> <p>Denne sammenhengen mellom feile avkryssninger og 'straffepoeng' tillater at du svarer feil en gang uten å bli straffet for det. Legg merke til at riktig-galt-oppgaver ikke gir feil hvis du lar være å krysse av noen av de to boksene for et gitt utsagn.</p>	<p>The maximum score is 100 points. The problem set consists of 2 parts:</p> <ul style="list-style-type: none"> • Part I, the problem specifications - this part. • Part II, the answer pages, includes answer boxes for true-false and “written text” problems. Part II also includes 3 pages for comments related to <i>formal issues</i> about Part I or Part II. These pages may also be used for “written text” answers. <p>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.</p> <p>Written text problems shall be answered within the assigned box of Part II.</p> <p>True-False problems are answered by checking one box per statement, or no check. If both ‘true’ and ‘false’ are checked for a statement, it counts as an incorrect mark.</p> <p>Check the boxes like this:  If you check the wrong box, fill it completely, like this:  Then check the correct box. Other correction methods are not permitted.</p> <p>For each group of 10 True/False questions: Points = Max{(number of correct marks – discount points), 0} * 1 incorrect gives no discount; * 2 incorrect gives 1,5 discount; * i > 2 incorrect gives i discounts.</p> <p>This mapping between incorrect marks and discount points allow you to answer wrong once without being punished. Note that the true-false problems do not give incorrect marks if you do not check any of the two boxes for a given statement.</p>	<p>Maksimum poengsum er 100. Oppgavesettet består av 2 delar:</p> <ul style="list-style-type: none"> • Del I, oppgavetekst, - denne delen. • Del II, svarsidene, inkluderer svaralternativ for “riktig-gale” oppgaver og “skriftlege svar”-felt. Del II inkluderer òg 3 sider for kommentarar relatert til formelle problem i Del I eller Del II. Sidene kan òg brukast for ”skriftlege svar”. <p>Del II skal leverast inn som svaret ditt. To kopiar av Del II vert levert ut. Berre ein kopi skal innleverast som svaret ditt. Kandidatnummeret skal skrivast på alle svarark. Skriv ikkje utanfor boks-felta. Bruk svart eller blå penn, ikkje blyant. Skriftleg svar oppgåve skal svarast på innanfor den tildelte boksen i Del II.</p> <p>Riktig-Gale oppgaver vert svara på ved eitt kryss for kvar utsegn, eller la vera å setja kryss. Viss både 'Riktig' og 'Gale' er kryssa av for ei utsegn, tel det som feil.</p> <p>Kryss av slik:  Viss du har kryssa av feil boks, skraver den fullstendig, slik:  Kryss deretter av i korrekt boks. *Korrigering på andre måtar er ikkje tillate.</p> <p>For kvar gruppe av 10 Riktig/Gale spørsmål: Poeng = Max{(mengd rette avkryssningar – straffepoeng), 0} * 1 feil gjev ingen straffepoeng; * 2 feil gjev 1,5 straffepoeng; * i > 2 feil gjev i straffepoeng.</p> <p>Denne samanhengen mellom feile avkryssningar og 'straffepoeng' tillèt at du svarar feil ein gong utan å straffast for det. Legg merke til at riktig-gale-oppgaver ikkje gjev feil viss du lèt vera å kryssa av nokon av dei to boksane for ei gjevte utsegn.</p>

1. True - False questions / Riktig – Galt spørsmål (50 points / 50 poeng)

(E: For each statement, check the 'True' or the 'False' box in the answer page, or do not check.

B: For hver påstand, kryss av 'Riktig' eller 'Galt' på svarsiden, eller la være å krysse.

N: For kvar utsegn, kryss av 'Riktig' eller 'Galt' på svarsida, eller la vera å kryssa.)

1.1 General, application layer and multimedia / Generelle, applikasjonslaget og multim. (10 p)

1.1.1	<p>E: The Real-Time Protocol (RTP) typically uses the TCP protocol for transport.</p> <p>B: RTP protokollen bruker vanligvis TCP protokollen for transport.</p> <p>N: RTP protokollen brukar vanlegvis TCP protokollen for transport.</p>
1.1.2	<p>E: Domain Name System (DNS) caching is used to improve delay performance and reduce the number of DNS messages traversing the Internet.</p> <p>B: "DNS caching" brukes for å redusere forsinkelse og antall DNS meldinger som må sendes over Internet.</p> <p>N: "DNS caching" brukast for å minske forseinkinga og antallet DNS meldingar som må sendast over Internet.</p>
1.1.3	<p>E: Propagation delay is given by the physical properties of the medium used, while the transmission delay is given by the equipment (e.g. electronics or optics) used to push bits onto the medium.</p> <p>B: Propagasjonsforsinkelse bestemmes av de fysiske egenskapene til det mediet som benyttes, mens transmisjonsforsinkelse er gitt av det utstyret (f.eks. elektronikk eller optikk) som brukes for å sende bit ut på mediet.</p> <p>N: Propagasjonsforseinking vert bestemd av dei fysiske eigenskapane til det mediet som vert nytta, medan transmisjonsforseinking vert bestemd av det utstyret (f.eks. elektronikk eller optikk) som brukast for å senda bit ut på mediet.</p>
1.1.4	<p>E: In the five-layer Internet protocol stack, the Link layer is placed between the Transport layer and the Network layer.</p> <p>B: I fem-lags protokollstakken brukt for Internett er Linklaget plassert mellom Transportlaget og Nettverkslaget.</p> <p>N: I fem-lags protokollstakken nytta for Internett er Linklaget plassert mellom Transportlaget og Nettverkslaget.</p>
1.1.5	<p>E: The User Datagram Protocol (UDP) provides a more reliable transport service than the Transmission Control Protocol (TCP).</p> <p>B: UDP realiserer en mer pålitelig transporttjeneste enn TCP.</p> <p>N: UDP realiserer ei meir påliteleg transporttjeneste enn TCP.</p>
1.1.6	<p>E: The signal propagation speed of an optical fiber is almost the same as the speed of light in air.</p> <p>B: Propagasjonshastigheten for et signal i en optisk fiber er nesten det samme som lyshastigheten gjennom luft.</p> <p>N: Propagasjonshastigheten for eit signal i ein optisk fiber er nesten det same som lyshastigheten gjennom luft.</p>
1.1.7	<p>E: When using protocol encapsulation the payload field at a given protocol layer contains the full protocol unit from the layer above, including higher layer address information.</p> <p>B: Når protokoll-innpakning («protocol encapsulation») brukes vil nyttedatadelen («payload field») på et gitt protokoll-lag inneholde hele protokoll-enheten («protocol unit») fra laget over, inkludert høyere lags adresseinformasjon.</p> <p>N: Når protokoll-innpakning («protocol encapsulation») brukast vil nyttedatadelen («payload field») på eit gjeve protokoll-lag innehalda heile protokoll-eininga («protocol unit») frå laga over, inkludert adresseinformasjonen på høgare lag.</p>
1.1.8	<p>E: All web servers must listen for client requests on port 80.</p> <p>B: Alle webtjenere må lytte etter klientforespørsler på port 80.</p> <p>N: Alle webtjenere må lytta etter klientførespurnader på port 80.</p>

1.1.9	<p>E: When streaming stored video through the Internet, we can use UDP as the transport layer protocol.</p> <p>B: Når vi streamer lagret video gjennom Internet, kan vi bruke UDP som transportlagsprotokoll.</p> <p>N: Når me streamar lagra video gjennom Internet, kan me bruke UDP som transportlagsprotokoll.</p>
1.1.10	<p>E: The network load is reflected in the end-to-end delay of the application.</p> <p>B: Lasten i nettverket reflekteres i applikasjonens ende-til-ende forsinkelse.</p> <p>N: Lasten i nettverket reflekterast i applikasjonens ende-til-ende forseinking.</p>

1.2 Communication security and link layer / Kommunikasjonssikkerhet og linklag (10 p)

1.2.1	<p>E: With Carrier Sense Multiple Access/Collision Detection (CSMA/CD), when a collision is detected, the transmitting node stops its transmission and uses some procedure/rule to determine when it should attempt to transmit the next time.</p> <p>B: Med CSMA/CD, når en kollisjon blir oppdaget, så vil noden som sender avbryte sendingen og bruke en prosedyre/regel for å bestemme når den skal prøve å sende neste gang.</p> <p>N: Med CSMA/CD, når ein kollisjon blir oppdaga, så vil noden som sender avbryte sendinga og bruke ein prosedyre/regel for å bestemme når den skal prøve å sende neste gång.</p>
1.2.2	<p>E: SSL (Secure Socket Layer) is used at the network layer to secure IP communication.</p> <p>B: SSL ("Secure Socket Layer") brukes på nettverkslaget for å sikre IP kommunikasjon.</p> <p>N: SSL ("Secure Socket Layer") brukast på nettverkslaget for å sikre IP kommunikasjon.</p>
1.2.3	<p>E: A Cryptographic Hash Function is used to provide message confidentiality.</p> <p>B: En "Cryptographic Hash Function" brukes for å oppnå konfidensialitet for en melding.</p> <p>N: Ein "Cryptographic Hash Function" brukast for å oppnå konfidensialitet for ei melding.</p>
1.2.4	<p>E: The "Caesar cipher" is an example of a symmetric key algorithm for encrypting data.</p> <p>B: "Caesar Cipher" er et eksempel på en symmetrisk nøkkel algoritme for å kryptere data.</p> <p>N: "Caesar Cipher" er eit eksempel på ei symmetrisk nøkkel algoritme for å kryptera data.</p>
1.2.5	<p>E: With the two-dimensional parity check scheme, the receiver can detect a double bit error.</p> <p>B: Ved bruk av to-dimensjonal paritets-sjekk kan mottakeren oppdage en dobbel bitfeil.</p> <p>N: Ved bruk av to-dimensjonal paritets-sjekk kan mottakaren oppdage ein dobbel bitfeil.</p>
1.2.6	<p>E: FEC (Forward Error Correction) techniques will increase the number of required sender retransmissions.</p> <p>B: FEC («forward error correction») teknikker vil øke antall nødvendige retransmisjoner fra avsender.</p> <p>N: FEC («forward error correction») teknikkar vil auke antallet naudsynte retransmisjonar frå avsendar.</p>
1.2.7	<p>E: Operating systems always use MAC (Medium Access Control) based IPv6 addresses.</p> <p>B: Operativsystemer benytter alltid MAC-baserte (Medium Access Control) IPv6 adresser.</p> <p>N: Operativsystemer nyttar alltid MAC-baserte (Medium Access Control) IPv6 adressar.</p>
1.2.8	<p>E: Using a VPN client (Virtual Private Network) on a device connected to an unencrypted wireless local area network (WLAN), the various IP addresses you communicate with cannot be seen by others connected to the same WLAN subnet.</p>

	<p>B: Ved bruk av en VPN-klient (Virtuelt Privat Nett) på en enhet knyttet til et ukryptert trådløst lokalnett (WLAN), kan de ulike IP-adressene du kommuniserer med ikke sees av andre tilknyttet det samme WLAN-subnett.</p> <p>N: Ved bruk av ein VPN-klient (Virtuelt Privat Nett) på ein enhet knytta til eit ukryptert trådløst lokalnett (WLAN), kan dei ulike IP-adressane du kommuniserer med ikkje sjåast av andre tilknytta det same WLAN-subnett.</p>
1.2.9	<p>E: Using a VPN client (Virtual Private Network) on a device connected to an unencrypted wireless local area network (WLAN), hinders others connected to the same WLAN subnet to see which local IP address you are assigned.</p> <p>B: Ved bruk av en VPN-klient (Virtuelt Privat Nett) på en enhet knyttet til et ukryptert trådløst lokalnett (WLAN), hindrer andre tilknyttet det samme WLAN-subnett å se hvilken lokal IP-adresse du er tildelt.</p> <p>N: Ved bruk av ein VPN-klient (Virtuelt Privat Nett) på ein enhet knytta til eit ukryptert trådløst lokalnett (WLAN), hindrar andre tilknytta det same WLAN-subnett å sjå kva lokal IP-adresse du er gjeven.</p>
1.2.10	<p>E: In public key cryptography, all keys are public but the algorithm used is secret.</p> <p>B: I offentlig nøkkel kryptering («public key cryptography») er alle nøkler offentlige, men algoritmen som brukes er hemmelig.</p> <p>N: I offentlig nøkkel kryptering («public key cryptography») er alle nøklar offentlege, men algoritmen som vert brukt er løynleg.</p>

1.3 Wireless and mobile communication / Trådløs og mobil kommunikasjon (10 p)

1.3.1	<p>E: An AP (“Access Point”) sends beacon frames periodically to inform potential wireless devices about its existence.</p> <p>B: Et AP (“Access point”) sender periodiske “beacon frames” for å informere potensielle trådløse enheter om at det eksisterer.</p> <p>N: Eit AP (“Access point”) sender periodiske “beacon frames” for å informere potensielle trådløse einingar om at det eksisterer.</p>
1.3.2	<p>E: An “infrastructure wireless LAN” has no AP (“Access Point”).</p> <p>B: Et “infrastructure wireless LAN” har ikke noe AP (aksesspunkt).</p> <p>N: Eit “infrastructure wireless LAN” har ikkje noko AP (aksesspunkt).</p>
1.3.3	<p>E: Radio transmission in the 3G (UMTS) mobile system is based on variants of the CDMA (“Code Division Multiple Access”) principle.</p> <p>B: Radiotransmisjon i et 3G (UMTS) mobilsystem er basert på varianter av CDMA (“Code Division Multiple Access”) prinsippet.</p> <p>N: Radiotransmisjon i eit 3G (UMTS) mobilsystem er basert på varianter av CDMA (“Code Division Multiple Access”) prinsippet.</p>
1.3.4	<p>E: Different variants of the WiFi (802.11xx) LAN standard use the 2.4 GHz frequency range or the 5 GHz frequency range, or both, for communication.</p> <p>B: Ulike varianter av WiFi (802.11xx) LAN standarden bruker 2.4 GHz frekvensområdet eller 5 GHz frekvensområdet, eller begge, for kommunikasjon.</p> <p>N: Ulike variantar av WiFi (802.11xx) LAN standarden nyttar 2.4 GHz frekvensområdet eller 5 GHz frekvensområdet, eller baa, for kommunikasjon.</p>
1.3.5	<p>E: In a WiFi (802.11) LAN the Request-to-Send (RTS) and Clear-to-Send (CTS) frames are used to reserve access to the communication channel.</p> <p>B: I et WiFi (802.11) lokalnett blir “Request-to-Send (RTS)” og “Clear-to-Send” (CTS)” rammer brukt for å reservere aksess på kommunikasjonskanalen.</p> <p>N: I eit WiFi (802.11) lokalnett vert “Request-to-Send (RTS)” og “Clear-to-Send” (CTS)” rammer brukte for å reservera aksess på kommunikasjonskanalen.</p>
1.3.6	<p>E: Communication over a radio channel is more susceptible to noise than communication over a fiber or copper channel.</p> <p>B: Kommunikasjon over en radiokanal er mer utsatt for støy enn kommunikasjon over</p>

	<p>en optisk - eller koppar kanal.</p> <p>N: Kommunikasjon over ein radiokanal er meir utsett for støy enn kommunikasjon over ein optisk - eller koppar kanal.</p>
1.3.7	<p>E: The 4G (LTE) mobile architecture has an all-Internet Protocol (all-IP) core network.</p> <p>B: Mobilarkitekturen 4G (LTE) har et IP-over-alt («all-IP») kjernenett.</p> <p>N: Mobilarkitekturen 4G (LTE) har eit IP-over-alt («all-IP») kjernenett.</p>
1.3.8	<p>E: Frames sent over a WiFi (802.11) LAN are never acknowledged.</p> <p>B: Rammer sende over WiFi (802.11) lokalnett blir aldri kvitterte («acknowledged»).</p> <p>N: Rammer sende over WiFi (802.11) lokalnett vert aldri kvitterte («acknowledged»).</p>
1.3.9	<p>E: The 2G (GSM) mobile architecture is a pure circuit-switched network, made mainly for voice conversations.</p> <p>B: Mobilarkitekturen 2G (GSM) er et rent linjesvitsjet nett, laget primært for talekommunikasjon.</p> <p>N: Mobilarkitekturen 2G (GSM) er eit reint linjesvitsja nett, laga primært for talekommunikasjon.</p>
1.3.10	<p>E: An 802.11 wireless LAN uses CSMA/CD as medium access protocol.</p> <p>B: Et 802.11 trådløst LAN bruker CSMA/CD som medium aksess protokoll.</p> <p>N: Eit 802.11 trådløst LAN brukar CSMA/CD som medium aksess protokoll.</p>

1.4 Transport layer / Transportlaget (10 p)

1.4.1	<p>E: TCP has implemented both end-to-end flow control and congestion control.</p> <p>B: TCP har implementert både ende-til-ende flytkontroll og overbelastningskontroll.</p> <p>N: TCP har implementert både ende-til-ende flytkontroll og overlastkontroll.</p>
1.4.2	<p>E: UDP has no congestion control implemented.</p> <p>B: UDP har ikke implementert noen overbelastningskontroll.</p> <p>N: UDP har ikkje implementert nokon overlastkontroll.</p>
1.4.3	<p>E: UDP has implemented end-to-end flow control.</p> <p>B: UDP har implementert end-til-ende flytkontroll.</p> <p>N: UDP har implementert ende-til-ende flytkontroll.</p>
1.4.4	<p>E: When TCP is used, the TCP port number of the destination must be the same as the TCP port number of the source.</p> <p>B: Når TCP blir brukt, må destinasjonens TCP-portnummer være det samme som kildens TCP-portnummer.</p> <p>N: Når TCP vert brukt, må destinasjonens TCP-portnummer være det same som kjelda sitt TCP-portnummer.</p>
1.4.5	<p>E: TCP flow control is implemented through a window variable at the sender side, indicating the available buffer space at the receiver side.</p> <p>B: TCP flytkontroll implementeres ved å bruke en vindusvariabel på sendersiden, som indikerer tilgjengelig bufferplass på mottakersiden.</p> <p>N: TCP flytkontroll vert implementert ved å bruka ein vindaugsvariabel på sendarsida, som indikerer tilgjengeleg bufferplass på mottakarsida.</p>
1.4.6	<p>E: The protocol header of the TCP segment contains source and destination ports and IP addresses of both sender and receiver.</p> <p>B: Protokollhodet til et TCP segment inneholder kilde- og destinasjonsporter, samt IP adresser for både sender og mottaker.</p> <p>N: Protokollhovudet til eit TCP segment inneheld kjelde- og destinasjonsportar, og dessutan IP adresser for både sendar og mottakar.</p>
1.4.7	<p>E: Transport layer protocols are always present both in end-systems and in network routers.</p> <p>B: Transportlagsprotokoller er alltid til stede både i endesystemer og i nettverksrutere.</p> <p>N: Transportlagsprotokoller er alltid til stades både i endesystem og i nettverksruterar.</p>

1.4.8	<p>E: It is primarily the application requirements that decides the complexity of the transport protocol</p> <p>B: Det er primært kravene fra applikasjonen som bestemmer kompleksiteten til transportprotokollen.</p> <p>N: Det er primært krava frå applikasjonen som avgjer kompleksiteten til transportprotokollen.</p>
1.4.9	<p>E: In TCP a “three-way handshake” is used to establish a connection before starting to transfer data.</p> <p>B: I TCP brukes en «three-way handshake» for å etablere en forbindelse før en starter å overføre data.</p> <p>N: I TCP vert brukt ein «three-way handshake» for å etablere eit samband før ein startar å overføra data.</p>
1.4.10	<p>E: Sequence numbers start counting from zero after a new TCP connection is established.</p> <p>B: Sekvensnummer starter å telle fra null når en ny TCP forbindelse er etablert.</p> <p>N: Sekvensnummer startar å telja frå null når eit nytt TCP samband er etablert.</p>

1.5 Network layer / Nettlag (10 p)

1.5.1	<p>E: The Internet Protocol (IP) guarantees that the packets will arrive in the right sequence.</p> <p>B: IP garanterer at pakker vil ankomme i riktig rekkefølge.</p> <p>N: IP garanterer at pakker vil komme fram i riktig rekkefølge.</p>
1.5.2	<p>E: A Class C IP subnet, which has a CIDR address of the form a.b.c.d/24, has enough addresses for about 500 hosts.</p> <p>B: Et Klasse C IP subnett, som har en CIDR adresse på formen a.b.c.d/24, har adresser nok for omtrent 500 verter.</p> <p>N: Eit Klasse C IP subnett, som har ein CIDR adresse på formen a.b.c.d/24, har adresser nok for omtrent 500 verter.</p>
1.5.3	<p>E: The IPv4 address space is much larger than the IPv6 address space.</p> <p>B: Adresserommet til IPv4 er mye større enn adresserommet til IPv6.</p> <p>N: Adresserommet til IPv4 er mykje større enn adresserommet til IPv6.</p>
1.5.4	<p>E: With the Dynamic Host Configuration Protocol (DHCP), a host may be assigned an IP address that is different each time the host is connected to the network.</p> <p>B: Med DHCP kan en vert bli tildelt en IP adresse som er forskjellig hver gang verten blir tilkoblet nettet.</p> <p>N: Med DHCP kan ein vert bli tildelt ein IP adresse som er ulik kvar gong verten blir tilkobla nettet.</p>
1.5.5	<p>E: The main purpose of NAT (Network Address Translation) is to allow for the re-use of the IPv4 subnet addresses.</p> <p>B: Hovedhensikten med “NAT (network address translation)” er å tillate gjenbruk av IPv4 subnett adresser.</p> <p>N: Hovudføremålet med “NAT (network address translation)” er å tillata gjenbruk av IPv4 subnett adresser.</p>
1.5.6	<p>E: Datagram fragmentation is a result of link layers having different abilities in which packet sizes they can carry.</p> <p>B: Datagram fragmentering skjer fordi ulike linklag har ulike egenskaper med hensyn til hvilke pakkestørrelser de kan transportere.</p> <p>N: Datagram fragmentering skjer fordi ulike linklag har ulike eigenskapar med omsyn til kva for pakkestørleikar dei kan transportera.</p>
1.5.7	<p>E: The Internet is a virtual circuit network at the network (IP protocol) layer.</p>

	<p>B: Internet er et virtuelt forbindelsesnett («virtual circuit network») på nettverks- (IP protokoll) laget.</p> <p>N: Internet er eit virtuelt sambandsnett («virtual circuit network») på nettverks- (IP protokoll) laget.</p>
1.5.8	<p>E: When forwarding packets, a router updates the IP address with the address of the next router.</p> <p>B: Ved videresending av pakker, oppdaterer ruterer IP-adressen med IP-adressen til neste ruter.</p> <p>N: Ved vidaresending av pakkar, oppdaterar ruterer IP-adressa med IP-adressa til neste ruter.</p>
1.5.9	<p>E: Within the same subnet, it is the network part of the IP-address which identifies the receiver.</p> <p>B: Innen samme subnett er det nettverksdelen av IP-adressen som identifiserer mottaker.</p> <p>N: Innan same subnett er det nettverksdelen av IP-adressen som identifiserer mottakaren.</p>
1.5.10	<p>E: It is possible to actively provoke error messages from ICMP (Internet Control Message Protocol).</p> <p>B: Det er mulig å aktivt framprovosere feilmelding fra ICMP (Internet Control Message Protocol).</p> <p>N: Det er mogleg å aktivt framprovosera feilmelding frå ICMP (Internet Control Message Protocol).</p>

2. Multiple areas / Ulike områder (20 p)

E: Each of the five subgroups below has one or more correct answers. **The total number of correct answers (summed over 2.1 to 2.5 below) is 10.** Each correct answer gives 2 points. You are not penalized for a wrong answer, **up to a total of 10 answers.** Do not claim that **more** than 10 answers are correct in total for task 2. Doing so results in a **penalty of minus 3 points for each additional answer.**

B: Hver av de fem undergruppene nedenfor har ett eller flere riktige svar. **Totalt antall korrekte svar (summert over 2.1 til 2.5 nedenfor) er 10.** Hver korrekt svar gir 2 poeng. Du blir ikke straffet for feil svar, **opp til totalt 10 svar.** Ikke påstå at **flere** enn 10 svar er korrekt totalt for oppgave 2. Å gjøre det resulterer i **en straff på minus 3 poeng for hvert ekstra svar.**

N: Kvar av dei fem undergruppene nedanfor har eit eller fleire riktige svar. **Totalt antal korrekte svar (summert over 2.1 til 2.5 nedanfor) er 10.** Kvar korrekt svar gjev 2 poeng. Du vert ikkje straffa for feil svar, **opp til totalt 10 svar.** Ikkje påstå at **fleire** enn 10 svar er korrekt totalt for oppgave 2. Å gjera det resulterer i **ei straff på minus 3 poeng for kvart ekstra svar.**

2.1

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

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

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

- a) D = 101110, G = 1001, R = 100
- b) D = 101110, G = 1001, R = 001
- c) D = 101110, G = 1001, R = 011

- d) D = 1010101010, G = 10011, R = 0100
- e) D = 1010101010, G = 10011, R = 0000
- f) D = 1010101010, G = 10011, R = 1010
- g) D = 11111, G = 1011, R = 001
- h) D = 11111, G = 1011, R = 100

2.2

E: Which of the network prefix(es) below (following Classless Interdomain Routing - CIDR rules) gives more than 1000 IP addresses for local use?

B: Hvilke(n) av nettverks-prefiksene nedenfor (en eller flere)(basert på «Classless Interdomain Routing – CIDR reglene) gir mer enn 1000 IP adresser for lokal bruk?

N: Kva for nettverks-prefiks nedanfor (ein eller fleire)(basert på «Classless Interdomain Routing – CIDR reglane) gir meir enn 1000 IP adressar for lokal bruk?

- a) 200.112.5.0/24
- b) 100.5.7.16/28
- c) 300.1.2.0/23
- d) 130.10.5.0/24
- e) 123.45.4.0/22
- f) 70.80.9.128/25
- g) 105.6.128.0/17
- h) 233.56.4.16/28

2.3

E: Which of the following terms/terminology are used to describe elements of the 802.11 Wireless LAN random access scheme (including both mandatory and optional mechanisms)?

B: Hvilke av følgende uttrykk/terminology blir brukt for å beskrive elementer av 802.11 Trådløs LAN random aksess mekanismen (inkludert både obligatoriske og opsjonelle mekanismer)?

N: Kva for fylgjande uttrykk/terminology vert brukt for å beskrive elementer av 802.11 Trådløs LAN random aksess mekanismen (inkludert både obligatoriske og opsjonelle mekanismar)?

- a) Short Inter-Frame Spacing (SIFS)
- b) Acknowledgement (ACK)
- c) Cyclic Redundancy Check (CRC)
- d) Internet Control Message Protocol (ICMP)
- e) Clear-to-Send/Request-to-Send (CTS/RTS)
- f) Forward Error Correction (FEC)
- g) Two-dimensional parity
- h) Interleaving

2.4

E: Which of the following (IP address, port number) pairs are involved in setting up (a) new TCP connection(s) in the Wireshark trace given in Figure 1? (Note: There could also be other pairs involved in setting up connections in the trace, not included below).

B: Hvilke av følgende (Ip adresse, portnummer) par er involvert i å sette opp (en) TCP forbindelse(r) i Wireshark tracet gitt i Figur 1? (Merk: Det kan også være andre par involvert i oppsett av forbindelser i tracet, men som ikke er inkludert nedenfor).

N: Kva for (Ip adresse, portnummer) par er involvert i å settje opp (ein) TCP forbindelse(r) i Wireshark tracet gjeve i Figur 1? (Merk: Det kan også være andre par involvert i å settje opp forbindelsar i tracet, men som ikkje er inkludert nedanfor).

- a) 160.68.205.231, 51765
- b) 239.255.255.250, 1900
- c) 129.241.0.200, 61709
- d) 129.241.200.195, 51765
- e) 129.241.200.195, 51764
- f) 129.241.200.80, 55428
- g) 160.68.205.231, 443
- h) 129.241.200.195, 443

Source	Source Port	Destination	Dest. Port	Protocol	Length	Info
129.241.0.200		53 129.241.200.195	61709	DNS	144	Standard query response 0x342b A www.google-analytics.com CNAME www-google-an-
129.241.200.195	57852	129.241.0.200	53	DNS	84	Standard query 0xb7d7 AAAA www.google-analytics.com
129.241.200.195	54253	129.241.0.200	53	DNS	70	Standard query 0x63ec A www.nrk.no
129.241.0.200		53 129.241.200.195	57852	DNS	156	Standard query response 0xb7d7 AAAA www.google-analytics.com CNAME www-google-
129.241.0.200		53 129.241.200.195	54253	DNS	100	Standard query response 0x63ec A www.nrk.no CNAME nrk.no A 160.68.205.231
129.241.200.195	61994	129.241.0.200	53	DNS	70	Standard query 0xdf66 AAAA www.nrk.no
129.241.0.200		53 129.241.200.195	61994	DNS	135	Standard query response 0xdf66 AAAA www.nrk.no CNAME nrk.no SOA ns1.nrk.no
129.241.0.200		53 129.241.200.195	58344	DNS	122	Standard query response 0xd1b8 AAAA ssl-nrk.tns-cs.net SOA ns.tns-cs.net
Micro-St_74:3f:7e		Broadcast		ARP	60	Who has 129.241.200.90? Tell 129.241.200.194
129.241.200.80	55428	239.255.255.250	1900	SSDP	159	M-SEARCH * HTTP/1.1
129.241.200.195	57062	129.241.0.200	53	DNS	84	Standard query 0x4fff A translate.googleapis.com
129.241.200.195	57792	129.241.0.200	53	DNS	89	Standard query 0x673c A clientservices.googleapis.com
129.241.0.200		53 129.241.200.195	57792	DNS	105	Standard query response 0x673c A clientservices.googleapis.com A 172.217.20.35
129.241.0.200		53 129.241.200.195	57062	DNS	100	Standard query response 0x4fff A translate.googleapis.com A 172.217.20.42
129.241.200.195	59186	129.241.0.200	53	DNS	84	Standard query 0x0365 AAAA translate.googleapis.com
129.241.0.200		53 129.241.200.195	59186	DNS	112	Standard query response 0x0365 AAAA translate.googleapis.com AAAA 2a00:1450:4...
2001:700:300:2211:6094:d4...	51763	2a00:1450:400f:80c::200a	443	TCP	86	51763 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
129.241.200.195	61911	129.241.0.200	53	DNS	89	Standard query 0x84f8 AAAA clientservices.googleapis.com
129.241.0.200		53 129.241.200.195	61911	DNS	117	Standard query response 0x84f8 AAAA clientservices.googleapis.com AAAA 2a00:1...
2001:700:300:2211:6094:d4...	51764	2a00:1450:400f:806::2003	443	TCP	86	51764 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
Cisco_0c:12:c2		Broadcast		ARP	60	Who has 129.241.200.99? Tell 129.241.200.1
2a00:1450:400f:80c::200a	443	2001:700:300:2211:6094:d417:10f2:5c51	51763	TCP	86	443 → 51763 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1 WS=256
2001:700:300:2211:6094:d4...	51763	2a00:1450:400f:80c::200a	443	TCP	74	51763 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
2001:700:300:2211:6094:d4...	51763	2a00:1450:400f:80c::200a	443	TLSv1.2	591	Client Hello
129.241.200.195	51765	160.68.205.231	443	TCP	66	51765 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2a00:1450:400f:806::2003	443	2001:700:300:2211:6094:d417:10f2:5c51	51764	TCP	86	443 → 51764 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1 WS=256
2001:700:300:2211:6094:d4...	51764	2a00:1450:400f:806::2003	443	TCP	74	51764 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
2001:700:300:2211:6094:d4...	51764	2a00:1450:400f:806::2003	443	TLSv1.2	591	Client Hello
2a00:1450:400f:80c::200a	443	2001:700:300:2211:6094:d417:10f2:5c51	51763	TCP	74	443 → 51763 [ACK] Seq=1 Ack=518 Win=28416 Len=0
160.68.205.231	443	129.241.200.195	51765	TCP	62	443 → 51765 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
129.241.200.195	51765	160.68.205.231	443	TCP	54	51765 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
129.241.200.195	51765	160.68.205.231	443	TLSv1.2	571	Client Hello
160.68.205.231	443	129.241.200.195	51765	TCP	60	443 → 51765 [ACK] Seq=1 Ack=518 Win=4897 Len=0
2a00:1450:400f:806::2003	443	2001:700:300:2211:6094:d417:10f2:5c51	51764	TCP	74	443 → 51764 [ACK] Seq=1 Ack=518 Win=28416 Len=0
2a00:1450:400f:80c::200a	443	2001:700:300:2211:6094:d417:10f2:5c51	51763	TLSv1.2	1294	Server Hello

Figure 1: Part of a Wireshark trace

2.5

E: With reference to Figure 2, which of the statements below are true?

B: Med referanse til Figur 2, hvilke av påstandene nedanfor er sanne?

N: Med referanse til Figur 2, kva for påstandar nedanfor er sanne?

E:

a) The destination of packet No. 5 is a broadcast address.

b) The broadcast address is 255.255.255.255.

c) The first-time association is done with SSID=eduroam because this is the first Probe Response.

d) An “Association Request” always depends on a previous “Probe Request” + “Probe Response” frame exchange.

B:

a) Mottakeradressen til pakke No. 5 er en kringkastingsadresse.

b) Kringkastingsadressen er 255.255.255.255.

c) Første gangs tilknytning gjøres mot SSID-eduroam siden dette er den første “Probe Response”.

d) En «Association Request» er alltid avhengig av en tidligere “Probe Request” + “Probe Response” rammeutveksling.

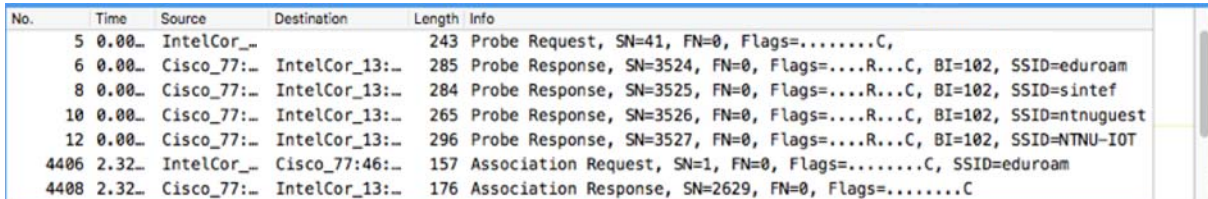
N:

a) Mottakeradressa til pakke No. 5 er ei kringkastingsadresse.

b) Kringkastingsadressa er 255.255.255.255.

c) Første gangs tilknytning gjerast mot SSID-eduroam sidan dette er den første “Probe Response” .

d) Ein «Association Request» er alltid avhengig av ein tidlegare “Probe Request” + “Probe Response” rammeutveksling.



No.	Time	Source	Destination	Length	Info
5	0.00...	IntelCor_...		243	Probe Request, SN=41, FN=0, Flags=.....C,
6	0.00...	Cisco_77:...	IntelCor_13:...	285	Probe Response, SN=3524, FN=0, Flags=...R...C, BI=102, SSID=eduroam
8	0.00...	Cisco_77:...	IntelCor_13:...	284	Probe Response, SN=3525, FN=0, Flags=...R...C, BI=102, SSID=sintef
10	0.00...	Cisco_77:...	IntelCor_13:...	265	Probe Response, SN=3526, FN=0, Flags=...R...C, BI=102, SSID=ntnuguest
12	0.00...	Cisco_77:...	IntelCor_13:...	296	Probe Response, SN=3527, FN=0, Flags=...R...C, BI=102, SSID=NTNU-IOT
4406	2.32...	IntelCor_...	Cisco_77:46:...	157	Association Request, SN=1, FN=0, Flags=.....C, SSID=eduroam
4408	2.32...	Cisco_77:...	IntelCor_13:...	176	Association Response, SN=2629, FN=0, Flags=.....C

Figur 2: Part of Wireshark trace

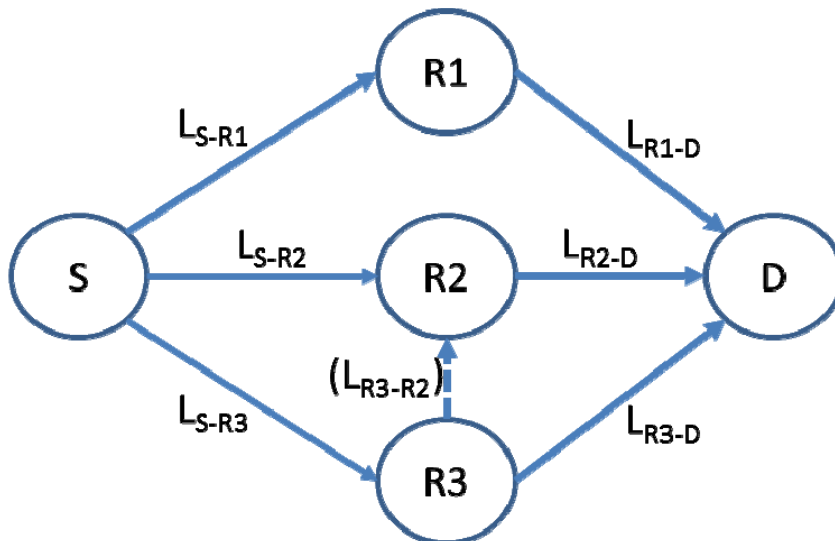
3. Network performance (20 p)(4+4+4+4+4)

E: We focus on the core network shown in Figure 3. All switches (S, D, Ri) are store-and-forward packet switches. Packets flow in only one direction from source (S) to destination (D). Propagation speed on all links is 200 000 000 meters per second. The length of each link and the link capacity is given in the table on the right of Figure 3. Processing delays in all switches are assumed fixed and equal to 0.1 millisecond per packet processed. Processing delay in the source S can be ignored since it is done before packets are sent towards the destination. There is no background traffic in the network, thus there are no additional delays from buffer or link contention. Infinite buffer space is assumed in all switches. All packets sent from S to D have length 1500 Bytes. A primitive form of load sharing is used: packet 1 is sent to D via R1, packet 2 is sent to D via R2, packet 3 is sent to D via R3, packet 4 is sent to D via R1, etc. However, due to limited processing capabilities the source S cannot send out packets in parallel.

B: Vi fokuserer på kjernenettet vist i Figur 3. Alle svitsjer (S, D, Ri) er «store-and-forward» pakkesvitsjer. Pakker går kun i en retning gjennom nettet, fra kilde («Source» – S) til destinasjon (D). Signalthastigheten («propagation speed») på alle lenkene er 200 000 000 meter per sekund. Lengden på hver lenke og lenkekapasiteten er gitt i tabellen til høyre i Figur 3. Prosesseringsforsinkelsen i alle svitsjene antas konstant og lik 0.1 ms per pakke som prosesseres. Prosesseringsforsinkelse i kilden (S) kan ignoreres siden det antas at disse gjøres før pakker sendes mot destinasjonen. Det er ikke noe bakgrunnstrafikk i nettet, slik at det ikke er noen tilleggsforsinkelser fra bufning eller venting på lenker ut. Uendelig bufferplass antas i alle svitsjene. Alle pakker sent fra S til D har lengde 1500 Bytes. En primitiv form for lastdeling brukes: pakke 1 sendes til D via R1, pakke 2 sendes til D via R2, pakke 3 sendes til D via R3, pakke 4 sendes til D via R1, osv. Men likevel, på grunn av begrensede prosesseringsmuligheter, kan ikke kilden (S) sende ut pakker i parallell.

N: Vi fokuserer på kjernenettet vist i Figur 3. Alle svitsjar (S, D, Ri) er «store-and-forward» pakkesvitsjar. Pakker går kun i ei retning gjennom nettet, frå kjelde («Source» – S) til destinasjon (D). Signalthastigheten («propagation speed») på alle lenkane er 200 000 000 meter per sekund. Lengden på kvar lenke og lenkekapasiteten er gjeven i tabellen til høyre i Figur 3. Prosesseringsforseinkinga i alle svitsjane antas konstant og lik 0.1 ms per pakke som prosesserast. Prosesseringsforseinking i kjelda (S) kan ignorerast sidan det antas at desse vert gjort før pakkar vert sende mot destinasjonen. Det er ikkje nokon bakgrunnstrafikk i nettet, slik at det ikkje er nokre

tilleggsforseinkingar frå bufring eller venting på lenker ut. Uendelig bufferplass antas i alle svitsjane. Alle pakker sende frå S til D har lengd 1500 Bytes. Ein primitiv form for lastdeling brukast: pakke 1 svert send til D via R1, pakke 2 vert send til D via R2, pakke 3 vert send til D via R3, pakke 4 vert send til D via R1, osv. Men likevel, på grunn av begrensa prosesseringsmuligheitar, kan ikkje kjelda (S) sende ut pakkar i parallell.



Link	Length [km]	Link cap. [Mbit/s]
L_{S-R1}	350	100
L_{S-R2}	220	100
L_{S-R3}	450	100
L_{R1-D}	310	300
L_{R2-D}	400	200
L_{R3-D}	350	300
L_{R3-R2}	270	50

Figure 3: Core network

3.1

E: What is the total end-to-end delay for a packet using the path S to D via R1?

B: Hva er total ende-til-ende forsinkelse for en pakke som går fra S til D via R1?

N: Kva er total ende-til-ende forseinking for ein pakke som går frå S til D via R1?

- a) 2.16 ms
- b) 3.30 ms
- c) 4.55 ms
- d) 3.46 ms
- e) 6.30 ms
- f) 3.66 ms
- g) 6.46 ms

3.2

E: Assume that only 4 packets are sent from S to D in sequence, via R1, R2, R3, and (again) R1, respectively. In what sequence will they arrive at the destination D?

B: Anta at kun 4 pakker sendes fra S til D i rekkefølge via R1, R2, R3, og (igjen) R1. I hvilken rekkefølge vil disse ankomme til destinasjonen D?

N: Anta at kun 4 pakkar vert sende frå S til D i rekkefylgje via R1, R2, R3, og (igjen) R1. I kva rekkefylgje vil desse komme fram til destinasjonen D?

- a) 1 – 2 – 3 – 4
- b) 1 – 3 – 2 – 4
- c) 1 – 4 – 2 – 3

- d) 3 – 1 – 4 – 2
- e) 2 – 3 – 1 – 4
- f) 2 – 1 – 4 – 3
- g) 2 – 1 – 3 – 4

3.3

E: What is the actual achieved end-to-end throughput for the period we transport the four packets in 3.2?

B: Hva blir den faktisk oppnådde ende-til-ende gjennomstrømningen (“throughput”) for det tidsrommet vi overfører de fire pakkene i 3.2?

N: Kva vert den faktisk oppnådde ende-til-ende gjennomstrøyminga (“throughput”) for det tidsrommet vi overfører dei fire pakkane i 3.2?

- a) 124 Mbit/s
- b) 6.766 Mbit/s
- c) 100 Mbits
- d) 10.435 Mbit/s
- e) 1.555 Mbit/s
- f) 130 Mbit/s
- g) 8.562 Mbit/s

3.4

E: Assume that the link L_{R3-D} fails, so link L_{R3-R2} must be used to reroute traffic via R2 instead. What is the end-to-end delay for a packet using this path from S to D via R3 (and R2)?

B: Anta at lenken L_{R3-D} blir ødelagt, slik at lenken L_{R3-R2} må brukast for å rerute trafikk via R2 i stedet. Hva blir ende-til-ende forsinkelsen for en pakke som nå sendes til D via R3 (og R2).

N: Anta at lenka L_{R3-D} vert øydelagd, slik at lenka L_{R3-R2} må brukast for å rerute trafikk via R2 i staden. Kva vert ende-til-ende forseinkinga for ein pakke som nå sendast til D via R3 (og R2).

- a) 6.32 ms
- b) 10.54 ms
- c) 5.67 ms
- d) 8.65 ms
- e) 0.45 ms
- f) 9.66 ms
- g) 8.02 ms

3.5

E: Assume the same transport of 4 packets as described in 3.2 but with the failure situation in 3.4. In what sequence will the packets now arrive at the destination D?

B: Anta samme transport av 4 pakker som gitt i 3.2, men nå med feilsituasjonen gitt i 3.4. I hvilken rekkefølge vil pakkene nå ankomme destinasjonen D?

N: Anta same transport av 4 pakkane som gjeve i 3.2, men nå med feilsituasjonen gjeven i 3.4. I kva rekkefylgje vil pakkane nå komme fram til destinasjonen D?

- a) 1 – 2 – 3 – 4
- b) 1 – 3 – 2 – 4
- c) 1 – 4 – 2 – 3
- d) 3 – 1 – 4 – 2
- e) 2 – 3 – 1 – 4

- f) 2 – 1 – 4 – 3
- g) 2 – 1 – 3 – 4

4. Kortsvar oppgaver / Short answer tasks (10 p)(5+5)

4.1

E: Why is a CRC (Cyclic Redundancy Check) not sufficient to assure integrity of data transmitted between two parties? (Answer the question in your own words, using one to **maximum three short** sentences).

B: Hvorfor er ikke en CRC (Cyclic Redundancy Check) tilstrekkelig for å sikre integritet av data som sendes mellom to parter? (Svar på spørsmålet med dine egne ord, ved å bruke en til **maksimum tre korte** setninger).

N: Kvifor er ikkje ein CRC (Cyclic Redundancy Check) tilstrekkeleg for å sikre integritet av data som sendast mellom to parter? (Svar på spørsmålet med dine egne ord, ved å bruka ein til **maksimum tre korte** setningar).

4.2

E: The 802.11 uses three addresses in infrastructure mode. Draw a simple figure and mark the three network interfaces that each has an address field in the 802.11 frame.

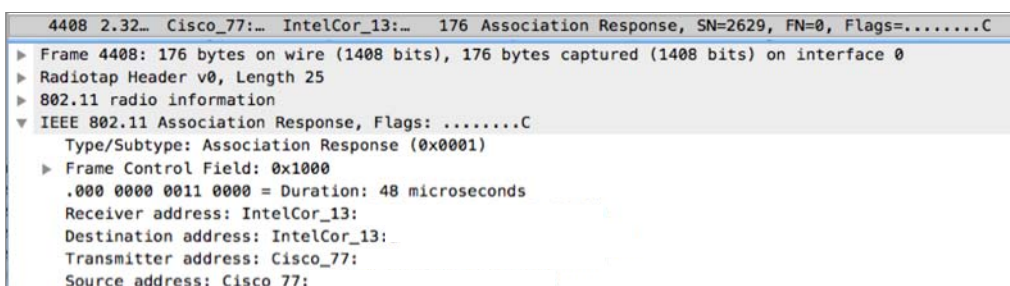
Why are only two different addresses used in an “Association Response” as presented by Wireshark in Figure 4? (Answer the question in your own words, using **a few short** sentences).

B: 802.11 gjør bruk av tre adresser i infrastrukturmodus. Tegn en enkel figur og marker de tre nettverksgrensesnittene som hver har et adressefelt i 802.11 rammen.

Hvorfor benyttes bare to ulike adresser i en «Association Response» slik som presentert av Wireshark i Figur 4. (Svar på spørsmålet med dine egne ord, ved å bruke **noen få korte** setninger).

N: 802.11 gjer bruk av tre adressar i infrastrukturmodus. Teikn ein enkel figur og marker dei tre nettverksgrensesnitta som kvar har eit adressefelt i 802.11 rama.

Kvifor nyttast berre to ulike adressar i ein «Association Response» slik som presentert av Wireshark i Figur 4. (Svar på spørsmålet med dine egne ord, ved å bruka **nokre få korte** setningar).



```
4408 2.32... Cisco_77:... IntelCor_13:... 176 Association Response, SN=2629, FN=0, Flags=.....C
▶ Frame 4408: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) on interface 0
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Association Response, Flags: .....C
  Type/Subtype: Association Response (0x0001)
  ▶ Frame Control Field: 0x1000
    .000 0000 0011 0000 = Duration: 48 microseconds
  Receiver address: IntelCor_13:
  Destination address: IntelCor_13:
  Transmitter address: Cisco_77:
  Source address: Cisco_77:
```

Figure 4: Part of a Wireshark trace