

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgave i

TTM4100 KOMMUNIKASJON – TJENESTER OG NETT

Faglig kontakt under eksamen: Norvald Stol

Tlf.: 97080077

Eksamensdato: 22 mai 2017

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: 15







Antall sider vedlegg: 22

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: </p> <p>Hvis du har krysset av feil boks, skraver den fullstendig, slik: </p> <p>Kryss deretter av i korrekt boks. Korrigering på andre måter er ikke tillatt.</p> <p>For hver gruppe av 10 Riktig/Galt spørsmål: Poeng = $\text{Max}\{(\text{antall rette avkrysninger} - \text{straffepoeng}), 0\}$ * 1 feil gir ingen straffepoeng; * 2 feil gir 1,5 straffepoeng; * $i > 2$ feil gir i straffepoeng.</p> <p>Denne sammenhengen mellom feile avkrysninger og 'straffepoeng' tillater at du svarer feil en gang uten å bli straffet for det.</p> <p>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: </p> <p>If you check the wrong box, fill it completely, like this: </p> <p>Then check the correct box. Other correction methods are not permitted.</p> <p>For each group of 10 True/False questions: Points = $\text{Max}\{(\text{number of correct marks} - \text{discount points}), 0\}$ * 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.</p> <p>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 oppgåver 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: </p> <p>Viss du har kryssa av feil boks, skraver den fullstendig, slik: </p> <p>Kryss deretter av i korrekt boks. *Korrigering på andre måtar er ikkje tillate.</p> <p>For kvar gruppe av 10 Riktig/Gale spørsmål: Poeng = $\text{Max}\{(\text{mengd rette avkrysningar} - \text{straffepoeng}), 0\}$ * 1 feil gjev ingen straffepoeng; * 2 feil gjev 1,5 straffepoeng; * $i > 2$ feil gjev i straffepoeng.</p> <p>Denne samanhengen mellom feile avkrysningar og 'straffepoeng' tillèt at du svarar feil ein gong utan å straffast for det.</p> <p>Legg merke til at riktig-gale-oppgåver ikkje gjev feil viss du lèt vera å kryssa av nokon av dei to boksane for ei gjeve 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 Application layer and multimedia / Applikasjonslaget og multimedia (10 p)

1.1.1	<p>E: When using HTTP with persistent connections, a brand-new connection must be established and maintained for each requested object.</p> <p>B: Når HTTP med persistente forbindelser brukes, opprettes og vedlikeholdes en ny forbindelse for hvert objekt som etterspørres.</p> <p>N: Når HTTP med persistente samband brukast, må ein etablera og vedlikehalde eit nytt samband for kvart objekt som bes om.</p>
1.1.2	<p>E: The Domain Name System (DNS) is used to translate hostnames into numerical IP addresses.</p> <p>B: Domain Name Systemet (DNS) brukes til å oversette tjenernavn til numeriske IP adresser.</p> <p>N: Domain Name Systemet (DNS) brukast til å oversetja tenarnavn til numeriske IP adressar.</p>
1.1.3	<p>E: An HTTP server is stateless.</p> <p>B: En HTTP tjener er tilstandsløs.</p> <p>N: Ein HTTP tenar er tilstandslaus.</p>
1.1.4	<p>E: The minimum time needed to distribute a file among a group of N users ($N > 2$) via a network is lower using a peer-to-peer architecture than when using a client-server architecture.</p> <p>B: Minimumstiden som trengs for å distribuere en fil mellom en gruppe på N brukere ($N > 2$) via et nett er lavere hvis en benytter en «peer-to-peer» arkitektur enn hvis en benytter en «client-server» arkitektur.</p> <p>N: Minimumstida ein treng for å distribuera ei fil mellom ei gruppe på N brukarar ($N > 2$) er lågare om ein nyttar ein «peer-to-peer» arkitektur enn om ein nyttar ein «client-server» arkitektur.</p>
1.1.5	<p>E: Sockets can only be used by an application which uses the TCP protocol as its transport layer protocol.</p> <p>B: «Sockets» kan bare benyttes av applikasjoner som bruker TCP protokollen som transportlagsprotokoll.</p> <p>N: «Sockets» kan berre nyttast av applikasjonar som brukar TCP protokollen som transportlagsprotokoll.</p>
1.1.6	<p>E: When streaming stored video through the Internet, we cannot use UDP as the transport layer protocol.</p> <p>B: Når vi streamer lagret video gjennom Internet, kan vi ikke bruke UDP som transportlagsprotokoll.</p> <p>N: Når me streamar lagra video gjennom Internet, kan me ikkje bruka UDP som transportlagsprotokoll.</p>
1.1.7	<p>E: Forward Error Correction (FEC) adds redundant information to a packet stream that can be used to recreate some (potentially) lost information in the network, at the destination.</p> <p>B: «Forward Error Correction (FEC)» legger til redundant informasjon til en pakkestrøm som kan brukes til å gjenopprette (potensielt) mistet informasjon i nettet, ved destinasjonen.</p> <p>N: «Forward Error Correction (FEC)» legg til redundant informasjon til ein pakkestrøm som kan nyttast til å retta opp igjen (potensielt) mista informasjon i nettet,</p>

	ved destinasjonen.
1.1.8	<p>E: “Interleaving” can be used by a Voice-over-IP application to mitigate the effect of packet loss. This results in reducing the quality of the received voice signal for a longer time period instead of losing the whole voice signal for a shorter time period.</p> <p>B: «Interleaving» kan brukes av «Voice-over-IP» applikasjoner for å motvirke effekten av pakketap. Resultatet er at kvaliteten på det mottatte talesignalet reduseres for en lengre tidsperiode, i stedet for at hele talesignalet blir borte i en kortere tidsperiode.</p> <p>N: «Interleaving» kan brukast av «Voice-over-IP» applikasjonar for å motverke effekten av pakketap. Resultatet er at kvaliteten på det mottekne talesignalet reduserast for ei lengre tidsperiode, i staden for at heile talesignalet vert borte i ei kortare tidsperiode.</p>
1.1.9	<p>E: When streaming stored video, client side buffers can be used to absorb variations in the server-to-client delay.</p> <p>B: Når lagret video streames, kan buffer brukes hos klienten for å utjevne variasjoner i tjener-til-klient forsinkelsen.</p> <p>N: Når lagra video streamast, kan buffer brukast hos klienten for å jamna ut variasjonar i tenar-til-klient forseinkinga.</p>
1.1.10	<p>E: “Packet jitter” is a result of packet loss in a network.</p> <p>B: «Packet jitter» er et resultat av pakketap i et nett.</p> <p>N: «Packet jitter» er eit resultat av pakketap i eit nett.</p>

1.2 Communication security / Kommunikasjonssikkerhet (10 p)

1.2.1	<p>E: In symmetric key cryptography, both sender and receiver share a secret key.</p> <p>B: I symmetrisk-nøkkel kryptering (“symmetric key cryptography”) deler sender og mottaker en hemmelig nøkkel.</p> <p>N: I symmetrisk-nøkkel kryptering (“symmetric key cryptography”) deler sendar og mottakar ein løyenleg nøkkel.</p>
1.2.2	<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 løyenleg.</p>
1.2.3	<p>E: “Message integrity” is the concept of detecting if (or making sure that) the content of a message has (not) been changed.</p> <p>B: Meldingsintegritet («Message integrity») er konseptet for å detektere om (eller sikre mot at) innholdet i meldingen (ikke) har blitt endret.</p> <p>N: Meldingsintegritet («Message integrity») er konseptet for å detektera om (eller sikra mot at) innhaldet i meldinga (ikkje) har vorte endra.</p>
1.2.4	<p>E: A “cryptographic hash function” is a special type of checksum to detect unauthorized changes to the content of a message.</p> <p>B: En kryptografisk hash funksjon («cryptographic hash function») er en spesiell type sjekksm for å detektere uautoriserte endringer av innholdet i en melding.</p> <p>N: Ein kryptografisk hash funksjon («cryptographic hash function») er ein spesiell type sjekksm for å detektera uautoriserte endringar av innhaldet i ei melding.</p>
1.2.5	<p>E: A “digital signature” is used to protect against unauthorized access to the content of a message.</p> <p>B: En digital signatur («digital signature») brukes til å beskytte mot uautorisert aksess til innholdet i en melding.</p> <p>N: Ein digital signatur («digital signature») brukast til å verna mot uautorisert aksess til</p>

	innhaldet i ei melding.
1.2.6	<p>E: In a “known-plaintext” attack, an intruder has access to the encryption process and can get access to the encrypted version (i.e. the ciphertext) corresponding to any chosen plaintext.</p> <p>B: I et kjent klartekst («known-plaintext») angrep har ein inntrenger adgang til krypteringsfunksjonen og kan få adgang til den krypterte versjonen («ciphertext») korresponderende til enhver valgt klartekst («plaintext»).</p> <p>N: I ei kjend klartekst («known-plaintext») angrep har ein inntrenger tilgjenge til krypteringsfunksjonen og kan få tilgjenge til den krypterte versjonen («ciphertext») korresponderande til kvar og ein valt klartekst («plaintext»).</p>
1.2.7	<p>E: “Cipher-Block Chaining” (CBC) is used to make sure that identical blocks of plaintext results in different blocks of ciphertext.</p> <p>B: «Cipher-Block Chaining» (CBC) brukes til å sikre at identiske blokker med klartekst («plaintext») resulterer i ulike blokker med kryptert tekst («ciphertext»).</p> <p>N: «Cipher-Block Chaining» (CBC) brukast til å sikra at identiske blokker med klartekst («plaintext») resulterer i ulike blokker med kryptert tekst («ciphertext»).</p>
1.2.8	<p>E: “Secure Sockets Layer” (SSL) is an (application layer) enhancement or extension of TCP to make communication secure.</p> <p>B: “Secure Sockets Layer” (SSL) er et tillegg eller en utvidelse av TCP (på applikasjonslaget) for å realisere sikker kommunikasjon.</p> <p>N: “Secure Sockets Layer” (SSL) er eit tillegg eller ei utviding av TCP (på applikasjonslaget) for å realisera sikker kommunikasjon.</p>
1.2.9	<p>E: “IPsec” provides security at the link layer.</p> <p>B: «Ipsec» realiserer sikkerhet på linklaget.</p> <p>N: «Ipsec» realiserer sikkerhet på linklaget.</p>
1.2.10	<p>E: A firewall is used to protect an internal network or a single server or PC against attacks via the public Internet.</p> <p>B: En brannmur («Firewall») brukes til å beskytte et internt nett eller en enkelt tjener eller PC mot angrep via det offentlig internettet.</p> <p>N: Ein brannmur («Firewall») brukast til å verna eit internt nett eller ein enkelt tenar eller PC mot angrep via det offentlege internettet.</p>

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

1.3.1	<p>E: In a wireless ad hoc network, the mobile units do not communicate via a common access point.</p> <p>B: I et trådløst ad hoc nett kommuniserer ikke de mobile enhetene via et felles aksesspunkt.</p> <p>N: I eit trådløst ad hoc nett kommuniserer ikkje dei mobile einingane via eit felles aksesspunkt.</p>
1.3.2	<p>E: Wireless links are more reliable than wired links (e.g. copper cables, fiber links), thus resulting in fewer bit errors during transmissions.</p> <p>B: Trådløse linker er mer pålitelige enn faste linker (f.eks. kobberkabler, fiberlinker) og gir derfor færre bitfeil under transmisjon.</p> <p>N: Trådlause linkar er meir pålitelege enn faste linkar (t.d. koparkablar, fiberlinkar) og gjev difor færre bitfeil under transmisjon.</p>
1.3.3	<p>E: The “hidden terminal” problem of wireless communication denotes the challenge of synchronizing transmissions to the same frequencies.</p> <p>B: «Hidden terminal» problemet i trådløs kommunikasjon er utfordringen med å</p>

	<p>synkroniserer transmisjoner til de samme frekvensene.</p> <p>N: «Hidden terminal» problemet i trådløs kommunikasjon er utfordringa med å synkroniserer transmisjonar til dei same frekvensane.</p>
1.3.4	<p>E: An 802.11 wireless LAN use 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>
1.3.5	<p>E: An 802.11 wireless LAN using an Access Point (AP) is an example of an ad hoc network.</p> <p>B: Et 802.11 trådløst LAN som benytter et aksesspunkt («Access Point (AP)») er et eksempel på et ad hoc nett.</p> <p>N: Eit 802.11 trådløst LAN som nyttar eit aksesspunkt («Access Point (AP)») er eit døme på eit ad hoc nett.</p>
1.3.6	<p>E: The optional “Request-To-Send” (RTS) / “Clear-To-Send” (CTS) mechanism defined by the 802.11 standard may help solve the hidden terminal problem.</p> <p>B: Den opsjonelle “Request-To-Send” (RTS) / “Clear-To-Send” (CTS) mekanismen definert av 802.11 standarden kan hjelpe til med å løse «hidden terminal» problemet.</p> <p>N: Den opsjonelle “Request-To-Send” (RTS) / “Clear-To-Send” (CTS) mekanismen definert av 802.11 standarden kan hjelpa til med å løysa «hidden terminal» problemet.</p>
1.3.7	<p>E: The 4G (LTE) mobile architecture has an 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: The 4G (LTE) mobile architecture has a Radio Access Network (RAN) based on CDMA for transmissions over the air.</p> <p>B: Mobilarkitekturen 4G (LTE) har et radioaksessnett («Radio Access Network» (RAN)) basert på bruk av CDMA for trådløs transmisjon.</p> <p>N: Mobilarkitekturen 4G (LTE) har eit radioaksessnett («Radio Access Network» (RAN)) basert på bruk av CDMA for trådløs transmisjon.</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: The “Wired Equivalent Privacy” (WEP) protocol, designed to provide authentication and data encryption between a wireless 802.11 station and the AP, has a lot of weaknesses and should not be used.</p> <p>B: Protokollen “Wired Equivalent Privacy” (WEP), laget for å gi autentisering og konfidensialitet mellom en 802.11 trådløs enhet og AP, har mange svakheter og bør ikke brukes.</p> <p>N: Protokollen “Wired Equivalent Privacy” (WEP), laga for å gje autentisering og konfidensialitet mellom ein 802.11 trådløs eining og AP, har mange veikskapar og bør ikkje brukast.</p>

1.4 Transport layer / Transportlaget (10 p)

1.4.1	<p>E: The “Transmission Control Protocol” (TCP) is the most used transport protocol in the Internet.</p> <p>B: “Transmission Control Protocol” (TCP) er den mest brukte transportprotokollen i Internet.</p> <p>N: “Transmission Control Protocol” (TCP) er den meste brukte transportprotokollen i Internet.</p>
1.4.2	<p>E: The “User Datagram protocol” (UDP) is a connection oriented protocol, well suited for reliable data transfer.</p> <p>B: “User Datagram protocol” (UDP) er en forbindelsesorientert protokoll, velegnet for pålitelig dataoverføring.</p> <p>N: “User Datagram protocol” (UDP) er ein forbindelsesorientert protokoll, velegna for påliteleg dataoverføring.</p>
1.4.3	<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 overføre data.</p>
1.4.4	<p>E: The “Go-Back-N” (GBN) protocol cannot use cumulative acknowledgements.</p> <p>B: “Go-Back-N” (GBN) protokollen kan ikke bruke kumulative kvitteringer («acknowledgements»).</p> <p>N: “Go-Back-N” (GBN) protokollen kan ikkje bruka kumulative kvitteringar («acknowledgements»).</p>
1.4.5	<p>E: Sequence numbers in TCP flow control is based on the number of packets transmitted.</p> <p>B: Sekvensnummer i TCP flytkontroll er basert på antall pakker sent.</p> <p>N: Sekvensnummer i TCP flytkontroll er basert på antalet pakkar som er sende.</p>
1.4.6	<p>E: TCP flow control uses cumulative acknowledgements.</p> <p>B: TCP flytkontroll bruker kumulative kvitteringer («acknowledgements»).</p> <p>N: TCP flytkontroll brukar kumulative kvitteringer («acknowledgements»).</p>
1.4.7	<p>E: “Slow start”, “congestion avoidance”, and “fast recovery” are all components of the TCP congestion control mechanism.</p> <p>B: “Slow start”, “congestion avoidance”, og “fast recovery” er alle ulike deler av TCP metningskontroll («congestion control») mekanismen.</p> <p>N: “Slow start”, “congestion avoidance”, og “fast recovery” er alle ulike delar av TCP metningskontroll («congestion control») mekanismen.</p>
1.4.8	<p>E: Sequence numbers in data transmission are used for addressing purposes.</p> <p>B: Sekvensnummer i dataoverføring brukes i forbindelse med adressering.</p> <p>N: Sekvensnummer i dataoverføring vert brukt i samband med adressering.</p>
1.4.9	<p>E: The transport layer is below the network layer in the protocol stack.</p> <p>B: Transportlaget er under nettverkslaget i protokollstakken.</p> <p>N: Transportlaget er under nettverkslaget i protokollstakken.</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 and link layers / Nett- og linklag (10 p)

1.5.1	<p>E: “Routing” is used locally for one router to denote the process of getting a packet from an input link to the (correct) output link; “Forwarding” denotes the whole process of determining a path for a packet from source to destination node, thus involving all network routers.</p> <p>B: Ruting (“routing”) brukes lokalt i en ruter for å angi prosessen med å få en pakke fra en inngangslink til (korrekt) utgangslink; «Forwarding» angir hele prosessen med å bestemme en sti gjennom nettet for en pakke fra kilde til destinasjonsnode, ved å involvere alle ruterne i nettet.</p> <p>N: Ruting (“routing”) brukast lokalt i ein ruter for å angje prosessen med å få ein pakke frå ein inngangslink til (korrekt) utgangslink; «Forwarding» angjev heile prosessen med å avgjera ein stig gjennom nettet for ein pakke frå kjelde til destinasjonsnode, ved å involvera alle ruterane i nettet.</p>
1.5.2	<p>E: The Internet Protocol (IP) version 4 uses 48 bit addresses.</p> <p>B: Internet protokoll (IP) versjon 4 bruker 48 bits addresser.</p> <p>N: Internet protokoll (IP) versjon 4 nyttar 48 bits addressar.</p>
1.5.3	<p>E: The Internet protocol (IP) version 6 uses 128 bit addresses.</p> <p>B: Internet protokoll (IP) versjon 6 bruker 128 bits addresser.</p> <p>N: Internet protokoll (IP) versjon 6 nyttar 128 bits addressar.</p>
1.5.4	<p>E: Parity bits can be used to detect (and sometimes correct) bit errors in frames sent over a link between two neighboring nodes.</p> <p>B: Paritetsbit kan brukes til å detektere (og noen ganger korrigere) bitfeil i rammer sendt over en link mellom to nabonoder.</p> <p>N: Paritetsbit kan brukast til å detektere (og nokon gonger korrigera) bitfeil i ramer sendt over ein link mellom to nabonoder.</p>
1.5.5	<p>E: “Cyclic Redundancy Check” (CRC) codes (or polynomial codes) are based on modulo-2 arithmetic without carries in addition or borrows in subtraction.</p> <p>B: “Cyclic Redundancy Check” (CRC) koder (eller polynomiske koder) er basert på modulo-2 aritmetikk uten overføring («carries») i addisjon eller låning («borrows») i substraksjon.</p> <p>N: “Cyclic Redundancy Check” (CRC) kodar (eller polynomiske kodar) er basert på modulo-2 aritmetikk utan overføring («carries») i addisjon eller låning («borrows») i substraksjon.</p>
1.5.6	<p>E: Shared broadcast medium Ethernets use “Carrier Sense Multiple Access with Collision Detection” (CSMA/CD) as the multiple access protocol.</p> <p>B: Delt-medium Ethernet bruker “Carrier Sense Multiple Access with Collision Detection” (CSMA/CD) som multippel aksess protokoll.</p> <p>N: Delt-medium Ethernet brukar “Carrier Sense Multiple Access with Collision Detection” (CSMA/CD) som multippel aksess protokoll.</p>
1.5.7	<p>E: Switched Ethernets uses “collision-less” (layer 2) store-and-forward frame switches.</p> <p>B: Svitsjet Ethernet bruker kollisjonsfrie (“collision-less”)(lag 2) «store-and-forward» rammesvitsjer.</p> <p>N: Svitsjet Ethernet nyttar kollisjonsfrie (“collision-less”)(lag 2) «store-and-forward» rammesvitsjar.</p>
1.5.8	<p>E: Both routers and link-layer switches forward packets or frames based on IP addressing.</p> <p>B: Både rutere og linklags svitsjer sender ut (“forward”) pakker eller rammer basert på IP adressering.</p> <p>N: Både ruter og linklags svitsjer sender ut (“forward”) pakkar eller ramer basert på IP adressering.</p>

1.5.9	<p>E: The IP version 4 address 223.1.1.0/24 denotes a subnet with a maximum of $2^8 - 2 = 254$ addresses available for local hosts.</p> <p>B: IP versjon 4 adressen 223.1.1.0/24 angir et subnet med maksimum $2^8 - 2 = 254$ adresser tilgjengelige for lokale verter.</p> <p>N: IP versjon 4 adressa 223.1.1.0/24 angjev eit subnet med maksimum $2^8 - 2 = 254$ adressar tilgjengelege for lokale vertar.</p>
1.5.10	<p>E: The “Internet Control Message Protocol” (ICMP) is used to communicate network layer information between hosts and routers.</p> <p>B: “Internet Control Message Protocol” (ICMP) brukes til å kommunisere nettlagsinformasjon mellom verter og rutere.</p> <p>N: “Internet Control Message Protocol” (ICMP) brukast til å kommunisera nettlagsinformasjon mellom vertar og ruterar.</p>

2. Multiple areas / Ulike områder (16 p)

E: Each of the four subgroups below has 1 to 5 correct answers. **The total number of correct answers (summed over 2.1 to 2.4 below) is 8.** Each correct answer gives 2 points. You are not penalized for a wrong answer, **up to a total of 8 answers.** Do not claim that **more** than 8 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 fire undergruppene nedenfor har 1 til 5 riktige svar. **Totalt antall korrekte svar (summert over 2.1 til 2.4 nedenfor) er 8.** Hver korrekt svar gir 2 poeng. Du blir ikke straffet for feil svar, **opp til totalt 8 svar.** Ikke påstå at **flere** enn 8 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 fire undergruppene nedanfor har 1 til 5 riktige svar. **Totalt antal korrekte svar (summert over 2.1 til 2.4 nedanfor) er 8.** Kvart korrekt svar gjev 2 poeng. Du vert ikkje straffa for feil svar, **opp til totalt 8 svar.** Ikkje påstå at **fleire** enn 8 svar er korrekt totalt for oppgave 2. Å gjera det resulterer i **ei straff på minus 3 poeng for kvart ekstra svar.**

2.1 (“Security”)

E: Bob wants to make sure that Alice can trust that a message is from him, and that the content of the message is not changed in any way. Which of the following security mechanism(s) or method(s) are directly involved in achieving this? (Note that more of these could be used at the same time, but for different purposes).

B: Bob vil være sikker på at Alice kan stole på at en melding faktisk er fra ham, og at innholdet i meldingen ikke er endret på noen måte. Hvilke(n) av følgende sikkerhetsmekanisme(r) eller metode(r) er direkte involvert i å oppnå dette? (Merk at flere av disse kan brukes samtidig, men for andre formål).

N: Bob vil vera sikker på at Alice kan stola på at ei melding faktisk er frå han, og at innhaldet i meldinga ikkje er endra på nokon måte. Kva for (ein eller fleire) av følgjande tryggleiksmekanisme(r) eller metode(r) er direkte involvert i å oppnå dette? (Merk at fleire av desse kan verta brukte samstundes, men for andre føremål).

- a) Symmetric key cryptography
- b) Firewall
- c) Cryptographic hash function
- d) Digital signature
- e) Packet filters
- f) Message authentication code

- g) Cipher-block chaining
- h) Stateful packet filters

2.2 (“TCP flow control”)

E: Alice and Bob are communicating using an established TCP connection. The most recent packet sent from Alice to Bob has Sequence number = 344 and contains 90 bytes of data. We do not know if this packet was correctly received by Bob, but we do know that Bob received and acknowledged the *previous* packet from Alice. Which of the following could be possible Acknowledgement number(s) in the next packet Bob sends to Alice?

B: Alice og Bob kommuniserer ved hjelp av en etablert TCP forbindelse. Den siste pakken sendt fra Alice til Bob har sekvensnummer = 344 og inneholder 90 bytes data. Vi vet ikke om denne pakken ble riktig mottatt av Bob, men vi vet at Bob mottok og kvitterte den forrige pakken fra Alice. Hvilke(n) av følgende kan være mulig kvitteringsverdier («Acknowledgement number(s)») i neste pakke Bob sender til Alice?

N: Alice og Bob kommuniserer ved hjelp av eit etablert TCP samband. Den siste pakken sendt frå Alice til Bob har sekvensnummer = 344 og inneheld 90 bytes med data. Vi veit ikkje om denne pakken vart riktig motteke av Bob, men vi veit at Bob mottok og kvitterte den førre pakken frå Alice. Kva for (ein eller fleire) av følgjande kan vera mogleg kvitteringsverdier («Acknowledgement number(s)») i neste pakke Bob sender til Alice?

- a) 253
- b) 254
- c) 255
- d) 344
- e) 345
- f) 433
- g) 434
- h) 435

2.3 (“IP addressing”)

E: Bob and Alice works at two different companies. Bob works at a small sales company where only ca. 200 IP addresses are needed, while Alice belongs to a large company where ca. 30 000 IP addresses are needed. Which of the following “subnet” combination(s) (following “Classless Inter Domain Routing” (CIDR) principles) would provide enough IP addresses for both these two companies?

(Legend/sequence: “Bob’s small sales company” - “Alice’s large company”).

B: Bob og Alice jobber i to ulike bedrifter. Bob jobber på en liten salgsbedrift hvor kun ca. 200 IP adresser er nødvendige, mens Alice er ansatt i en stor bedrift der ca. 30 000 IP adresser er nødvendige. Hvilke(n) av de følgende "subnet" -kombinasjonene (i henhold til “Classless Inter Domain Routing” (CIDR) prinsippene) gir nok IP adresser for begge disse to bedriftene?

(Syntaks/rekkefølge: "Bobs lille salgsbedrift" - "Alices store bedrift").

N: Bob og Alice jobbar i to ulike føretak. Bob jobbar på eit lite salsføretak der berre ca. 200 IP adressar er naudsynte, medan Alice er tilsett i eit stort føretak der ca. 30 000 IP adressar er naudsynte. Kva for (ein eller fleire) av dei følgjande "subnet" -kombinasjonane (i samsvar med “Classless Inter Domain Routing” (CIDR) prinsippa) gjev nok IP adressar for begge desse to føretaka?

(Syntaks/rekkjefølgje: "Bobs vesle salsføretak" - "Alices store føretak").

- a) 223.211.222.128/25 - 223.111.0.0/16
- b) 223.121.222.192/26 - 223.111.0.0/16
- c) 223.111.222.0/24 - 223.111.128.0/17

- d) 223.112.240.0/20 - 223.111.240.0/20
- e) 223.11.22.128/25 - 223.110.0.0/15
- f) 223.231.22.248/29 - 223.111.0.0/16
- g) 223.17.240.0/20 - 223.111.192.0/18
- h) 223.151.222.0/24 - 223.111.240.0/20

2.4 ("CRC/Parity")

E: Bob wants to use a two-dimensional even parity scheme to make his transmission to Alice more reliable. Which of the statements below are true for such a scheme?

- a) One data bit error can be detected but not corrected
- b) One data bit error can be detected and corrected
- c) Two data bit errors can be detected but not corrected
- d) Two data bit errors can be detected and corrected
- e) Three data bit errors can be detected but not corrected
- f) Three data bit errors can be detected and corrected
- g) One parity bit error can be detected but not corrected
- h) Two parity bit errors can be detected and corrected

B: Bob vil bruke todimensjonal lik («even») paritet prinsippet for å gjøre overføringen til Alice mer pålitelig. Hvilke(n) av uttalelsene nedenfor er sann(e) for en slik ordning?

- a) En databitfeil kan detekteres, men ikke korrigeres
- b) En databitfeil kan detekteres og korrigeres
- c) To databitfeil kan detekteres, men ikke korrigeres
- d) To databitfeil kan detekteres og korrigeres
- e) Tre databitfeil kan detekteres, men ikke korrigeres
- f) Tre databitfeil kan detekteres og korrigeres
- g) En paritetsbitfeil kan detekteres, men ikke korrigeres
- h) To paritetsbitfeil kan detekteres og korrigeres

N: Bob vil bruke todimensjonal lik («even») paritet prinsippet for å gjera overføringa til Alice meir påliteleg. Kva for (ein eller fleire) av utsegnene nedanfor er sann(e) for ei slik ordning?

- a) Ein databitfeil kan detekteres, men ikkje korrigeres
- b) Ein databitfeil kan detekteres og korrigeres
- c) To databitfeil kan detekteres, men ikkje korrigeres
- d) To databitfeil kan detekteres og korrigeres
- e) Tre databitfeil kan detekteres, men ikkje korrigeres
- f) Tre databitfeil kan detekteres og korrigeres
- g) Ein paritetsbitfeil kan detekteres, men ikkje korrigeres
- h) To paritetsbitfeil kan detekteres og korrigeres

3. Delays in a ring network / Forsinkelse i ringnett (14 p)(2+2+2+3+3+2)

E: We focus on the network shown in Figure 1. This is a ring topology network with four store-and-forward packet switches. Packets flow in only one direction around the ring, as indicated by the arrows. Propagation delays are ignored. Furthermore we assume that processing delays in switches are very low relative to transmission delays and can therefore also be ignored. There is no background traffic in the ring network, thus there are no additional delays from buffer or link contention. Infinite buffer space is assumed in the switches.

B: Vi fokuserer på nettet som vises i Figur 1. Dette er et ringtopologi-nett med fire «store-and-forward» pakkesvitsjer. Pakker flyter kun i én retning rundt ringen, som vist med pilene. Signalforsinkelser («propagation delays») ignoreres. Videre antar vi at prosesseringsforsinkelser i svitsjene er svært lave i forhold til overføringsforsinkelser («transmission delays»), og derfor også kan ignoreres. Det er ingen bakgrunnstrafikk i ringnettet, og derfor heller ingen ekstra forsinkelser i buffere eller på linkene av den grunn. Uendelig bufferplass antas i svitsjene.

N: Vi fokuserer på nettet som vert vist i Figur 1. Dette er eit ringtopologi-nett med fire «store-and-forward» pakkesvitsjar. Pakkar flyt berre i éi retning rundt ringen, som vist med pilene. Signalforseinkingar («propagation delays») ignorerast. Vidare antek vi at prosesseringsfirseinkingar i svitsjane er svært låge i høve til overføringsfirseinkingar («transmission delays»), og difor òg kan ignorerast. Det er ingen bakgrunnstrafikk i ringnettet, og difor heller ingen ekstra forseinkingar i buffere eller på linkane av den grunn. Uendeleg bufferplass vert antek i svitsjane.

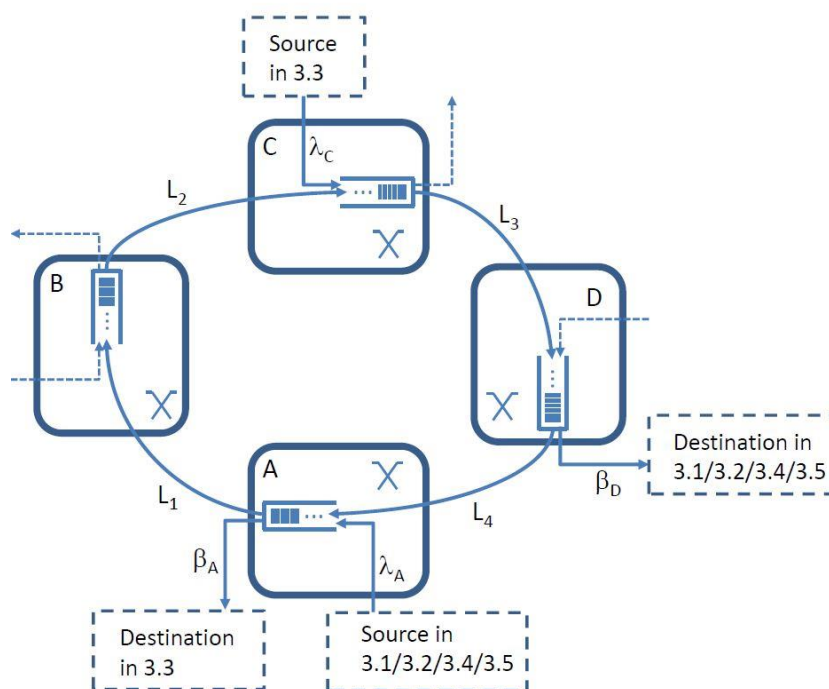


Figure 1: Ring network

3.1

E: One packet of size 1500 Bytes is sent from a source (e.g. a PC) connected to Switch A, to a destination (e.g. another PC) connected to switch D. All link capacities are the same, i.e. $L_1 = L_2 = L_3 = L_4 = \lambda_A = \lambda_C = \beta_A = \beta_D = 100$ Mbit/second. What is the end-to-end delay for this packet?

B: En pakke med størrelsen 1500 Bytes sendes fra en kilde (f.eks. en PC) som er koblet til svitsj A, til en destinasjon (f.eks. en annen PC) som er koblet til svitsj D. Alle linkkapasiteter er like, dvs. $L_1 = L_2$

$= L_3 = L_4 = \lambda_A = \lambda_C = \beta_A = \beta_D = 100$ Mbit/sekund. Hva er ende-til-ende forsinkelsen for denne pakken?

N: Ein pakke med storleik 1500 Bytes sendast frå ei kjelde (t.d. ein PC) som er kopla til svitsj A, til ein destinasjon (t.d. ein annan PC) som er kopla til svitsj D. Alle linkkapasitetar er like, dvs. $L_1 = L_2 = L_3 = L_4 = \lambda_A = \lambda_C = \beta_A = \beta_D = 100$ Mbit/sekund. Kva er ende-til-ende forseinkinga for denne pakken?

- a) 0.12 ms
- b) 0.36 s
- c) 0.60 ms
- d) 0.50 ms
- e) 6.00 ms
- f) 0.60 s
- g) 3.50 s

3.2

E: Same situation as above, except that $L_3 = L_4 = 10$ Mbit/second. (The other link capacities stay the same as above). What is the end-to-end delay for the packet now?

B: Samme situasjon som ovenfor, bortsett frå at $L_3 = L_4 = 10$ Mbit/sekund. (De andre linkkapasitetene er som ovenfor). Hva er ende-til-ende forsinkelsen for pakken nå?

N: Same situasjon som ovanfor, bortsett frå at $L_3 = L_4 = 10$ Mbit/sekund. (Dei andre linkkapasitetane er som ovanfor). Kva er ende-til-ende forseinkinga for pakken no?

- a) 1.20 ms
- b) 0.48 ms
- c) 0.12 ms
- d) 1.50 s
- e) 1.68 ms
- f) 6.00 s
- g) 2.73 s

3.3

E: Assume the same situation as in 3.2, i.e. $L_1 = L_2 = \lambda_A = \lambda_C = \beta_A = \beta_D = 100$ Mbit/second and $L_3 = L_4 = 10$ Mbit/second, but now the packet is sent from a source connected to switch C, to a destination connected to switch A. What is the end-to-end delay for the packet now?

B: Anta samme situasjon som i 3.2, dvs. $L_1 = L_2 = \lambda_A = \lambda_C = \beta_A = \beta_D = 100$ Mbit/sekund og $L_3 = L_4 = 10$ Mbit/sekund, men nå sendes pakken fra en kilde som er koblet til svitsj C, til en destinasjon som er koblet til svitsj A. Hva er ende-til-ende forsinkelsen for pakken nå?

N: Anta same situasjon som i 3.2, dvs. $L_1 = L_2 = \lambda_A = \lambda_C = \beta_A = \beta_D = 100$ Mbit/sekund og $L_3 = L_4 = 10$ Mbit/sekund, men no vert pakken sendt frå ei kjelde som er kopla til svitsj C, til ein destinasjon som er kopla til svitsj A. Kva er ende-til-ende forseinkinga for pakken no?

- a) 2.64 ms
- b) 1.32 ms
- c) 0.64 ms
- d) 1.50 s
- e) 6.00 s
- f) 1.68 ms
- g) 0.60 ms

3.4

E: Now again assume the same situation as in 3.1, i.e. all link capacities are the same and equal to 100 Mbit/second. We now want to send three different packets back-to-back from a source connected to switch A to a destination connected to switch D. The first packet has length 1500 Bytes, the second packet has length 6000 Bytes and the third and final packet has length 1500 Bytes. No packet fragmentation is used. What is the delay from we send out the first bit of the first packet until the last bit of the final packet is received at the destination?

B: Gå tilbake til den samme situasjonen som i 3.1, dvs. alle linkkapasiteter er den samme og lik 100 Mbit/sekund. Vi ønsker nå å sende tre forskjellige pakker «back-to-back» fra en kilde som er koblet til svitsj A til en destinasjon som er koblet til svitsj D. Den første pakken har lengde 1500 Bytes, den andre pakken har lengde 6000 Bytes og den tredje og siste pakken har lengde 1500 Bytes. Ingen pakkefragmentering brukes. Hva er forsinkelsen fra vi sender ut første bit av den første pakken til siste bit i den siste pakken er mottatt ved destinasjonen?

N: Gå tilbake til den same situasjonen som i 3.1, dvs. alle linkkapasitetar er den same og lik 100 Mbit/sekund. Vi ynskjer no å senda tre ulike pakkar «back-to-back» frå ei kjelde som er kopla til svitsj A til ein destinasjon som er kopla til svitsj D. Den første pakken har lengde 1500 Bytes, den andre pakken har lengde 6000 Bytes og den tredje og siste pakken har lengde 1500 Bytes. Ingen pakkefragmentering vert brukt. Kva er forseinkinga frå vi sender ut første bit av den første pakken til siste bit i den siste pakken er motteken ved destinasjonen?

- a) 0.68 ms
- b) 0.16 ms
- c) 1.05 s
- d) 2.64 ms
- e) 2.50 s
- f) 0.72 ms
- g) 1.68 ms

3.5

E: Assume the same situation as in 3.4 except that now $L_3 = 10$ Mbit/second. What is the delay from we send out the first bit of the first packet until the last bit of the final packet is received at the destination?

B: Anta samme situasjon som i 3.4 bortsett fra at $L_3 = 10$ Mbit/sekund. Hva er forsinkelsen fra vi sender ut første bit av den første pakken til siste bit i den siste pakken er mottatt ved destinasjonen?

N: Anta same situasjon som i 3.4 bortsett frå at $L_3 = 10$ Mbit/sekund. Kva er forseinkinga frå vi sender ut første bit av den første pakken til siste bit i den siste pakken er motteken ved destinasjonen?

- a) 0.26 ms
- b) 1.68 ms
- c) 9.50 ms
- d) 1.50 ms
- e) 7.68 ms
- f) 1.80 s
- g) 1.50 s

3.6

E: What is the average throughput for the connection between source and destination in 3.5 above during this data transmission?

B: Hva er gjennomsnittlig «throughput» for forbindelsen mellom kilde og destinasjon i 3.5 over under denne dataoverføringen?

N: Kva er gjennomsnittleg “throughput” for sambandet mellom kilde og destinasjon i 3.5 over under denne dataoverføringa?

- a) 10.0 Mbit/s
- b) 100.0 Mbit/s
- c) 5.885 Mbit/s
- d) 5.0 kbit/s
- e) 55.234 Mbit/s
- f) 1.50 Mbit/s
- g) 9.375 Mbit/s

4. Multimedia (20 p)(4+4+4+4+4)

E: Answer these questions in your own words, using one to **maximum three short** sentences.

B: Svar på disse spørsmålene med dine egne ord, ved å bruke en til **maksimum tre korte** setninger.

N: Svar på desse spørsmåla med dine egne ord, ved å bruka ein til **maksimum tre korte** setningar.

4.1

E: What is the most important mechanism, related to “Quality of Service” (QoS) or “Quality of Experience” (QoE), needed at the destination when stored video is received over the public Internet.

B: Hva er den viktigste mekanismen, relatert til «Quality of Service» (QoS) eller «Quality of Experience» (QoE), som trengs ved destinasjonen når lagret video mottas over offentlig Internet.

N: Kva er den viktigaste mekanismen, relatert til «Quality of Service» (QoS) eller «Quality of Experience» (QoE), som trengst ved destinasjonen når lagra video vert mottaken over offentleg Internet.

4.2

E: For what type of service can streaming of end-to-end video using UDP have an advantage over streaming using TCP, over the public Internet?

B: For hvilken type tjeneste kan streaming av ende-til-ende video ved å bruke UDP ha en fordel over streaming ved å bruke TCP, over offentlig Internet?

N: For kva for ein type teneste kan streaming av ende-til-ende video ved å bruka UDP ha ein fordel over streaming ved å bruka TCP, over offentleg Internet?

4.3

E: Why must jitter be removed at the destination when audio is sent over the public Internet?

B: Hvorfor må jitter fjernes ved destinasjonen når lyd sendes over offentlig Internet?

N: Kvifor må jitter fjernast ved destinasjonen når lyd vert sendt over offentleg Internet?

4.4

E: Give a very short explanation of how “Forward Error Correction” (FEC) is done.

B: Gi en veldig kort forklaring på hvordan «Forward Error Correction» (FEC) virker.

N: Gje ei veldig kort forklaring på korleis «Forward Error Correction» (FEC) verkar.

4.5

E: What is the most obvious disadvantage of using “interleaving” of data in transport of audio over the public Internet?

B: Hva er den mest åpenbare ulempen ved å bruke "interleaving" av data i transport av lyd over offentlig Internet?

N: Kva er den mest openberre ulempa ved å bruka "interleaving" av data i transport av lyd over offentleg Internet?