DAT204 Exam h2019

Datakommunikasjon (Universitetet i Agder)

DAT204-G H19, general information

Emnekode: DAT204
Emnenavn: Datakommunikasjon
Dato: 17.12.2019
Varighet: 3 timer

Tillatte hjelpemidler: Kalkulator

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

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

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

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

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

Tillater du at din eksamensbesvarelse blir brukt til slikt formål?

- Ja
- Nei

1

DAT204-G H19, Internet 5-layer model

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

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

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

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

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

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

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

Maks poeng: 3

2

DAT204-G H19, Wireshark HTTP

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

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

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

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

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

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

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

Hva er klientens portnummer i denne TCP forbindelsen?

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

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

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

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

Hvor mange bytes med applikasjonsdata er sendt med pakke 330?

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

Hvem initierer avsluttning av denne TCP forbindelsen? (Serveren, Klienten, Ingen)

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

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

Klienten har sendt: Serveren har sendt:

Maks poeng: 12

3

DAT204-G H19, DNS

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

Velg riktige alternativer:

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

Maks poeng: 5

4

DAT204-G H19, DHCP

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

Velg riktige alternativer:

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

Maks poeng: 3

5

DAT204-G H19, P2P

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

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

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

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

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

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

Hvilken protokoll er en populær P2P-protokoll for fildistribusjon?
Velg ett alternativ:

- BitTorrent
- BitCoin
- BitBucket
- BitP2P
- BitXfer

Maks poeng: 4.5

6

DAT204-G H19, TCP and UDP statements

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

Velg riktige alternativer:

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

Maks poeng: 5

7

DAT204-G H19, TCP/UDP checksum

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

Velg ett alternativ:

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

Velg ett alternativ:

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

Anta disse tre 16-bits ordene:

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

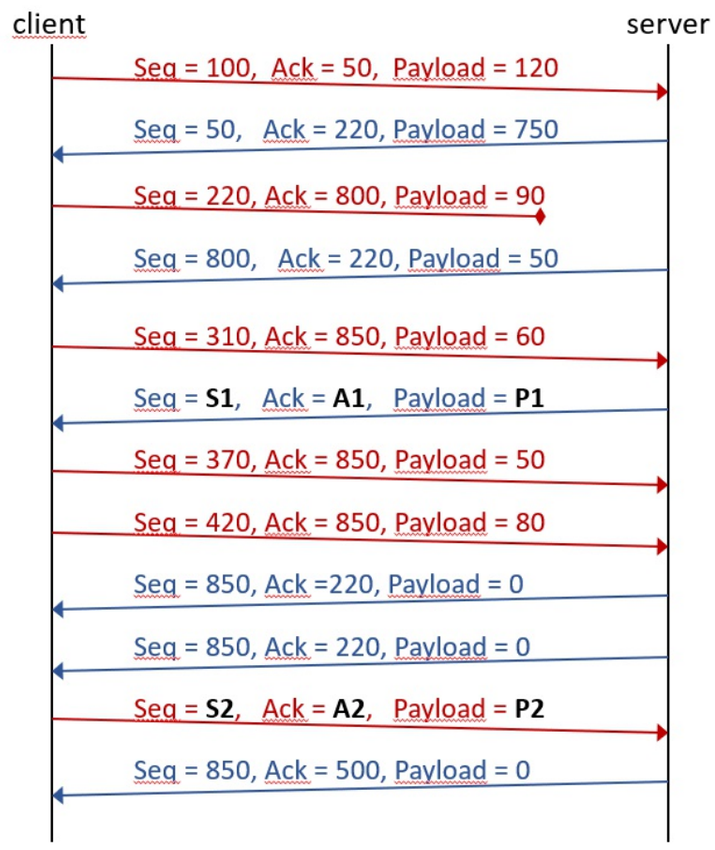
Hva er 1-komplement til summen av disse tre ordene? (Merk: eventuell mente fra det mest signifikante bit legges til resultatet fra en binær addisjon)

Sjekksum:

Maks poeng: 4.5

8

DAT204-G H19, TCP sequence



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

S1= A1= P1=

S2= A2= P2=

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

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

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

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

Maks poeng: 8

9

DAT204-G H19, TCP congestion handling

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

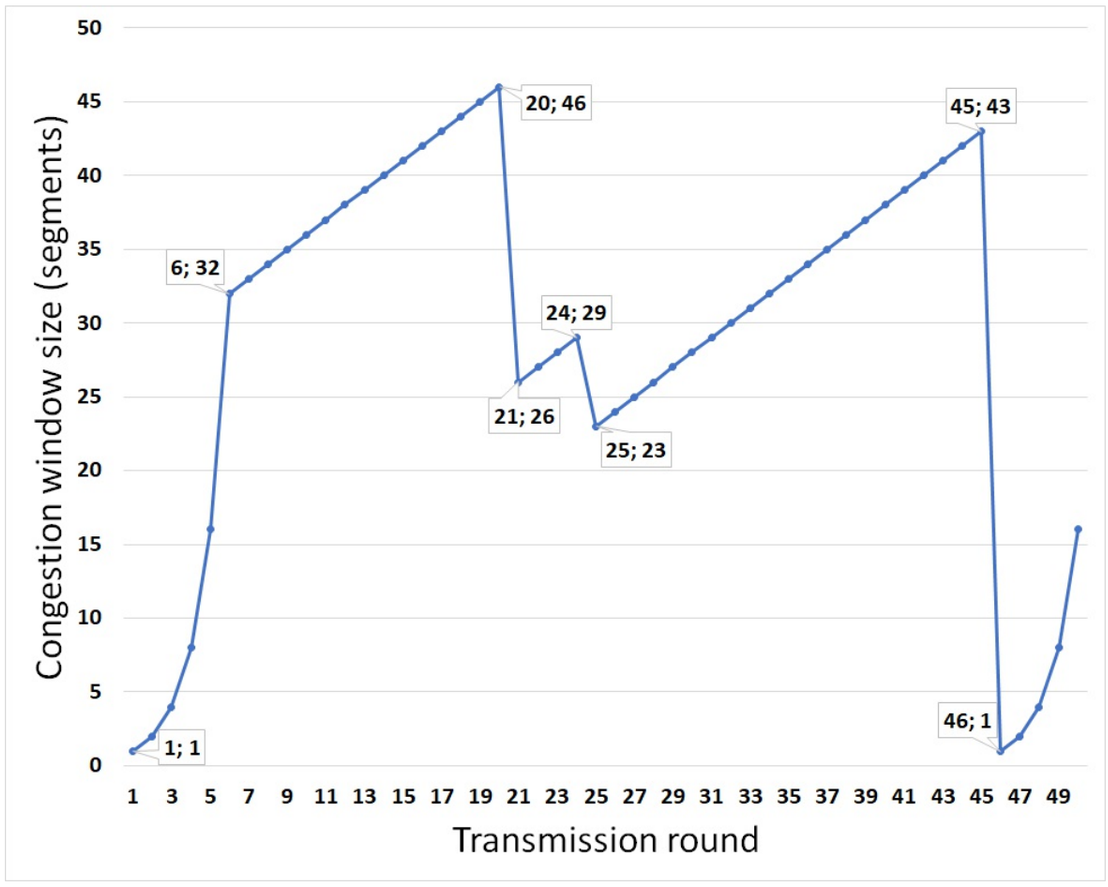
Velg ett alternativ:

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

Maks poeng: 2

10

DAT204-G H19, TCP congestion window



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

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

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

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

Hvordan er segmenttap identifisert etter den 20. overføringsrunden?

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

Hvordan er segmenttap identifisert etter den 45. overføringsrunden?

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

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

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

Maks poeng: 7

11

DAT204-G H19, IP and subnet

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

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

SN1: 105.16. [ ] . [ ] / [ ]

SN2: 105.16. [ ] . [ ] / [ ]

SN3: 105.16. [ ] . [ ] / [ ]

SN4: 105.16. [ ] . [ ] / [ ]

SN5: 105.16. [ ] . [ ] / [ ]

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

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

---

Maks poeng: 4.25

12

DAT204-G H19, NAT

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

Velg riktige alternativer:

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

Maks poeng: 4.5

13 DAT204-G H19, Routing tables

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

En ruter har følgende oppføringer i sin videresendingstabell:

Link1: 00001010.10101000.00000100.00000000/22
Link2: 00001010.10101000.00000110.00000000/23
Link3: 00001010.10101000.00000111.00000000/24
Link4: 00001010.10101000.00000000.00000000/16
Link5: Alle andre adresser

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

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

På hvilken link vil de bli videresendt?

A: link ☐ B: link ☐ C: link ☐ D: link ☐ E: link ☐

Maks poeng: 5

14

DAT204-G H19, Routing protocols

Nedenfor noen spørsmål om ruting protokoller. (3 poeng)

Hvilken protokoll er ansett som limet som holder Internettet sammen?
Velg ett alternativ:

- BGP
- ICMP
- RIP
- SNMP
- OSPF

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

- ICMP
- BGP
- RIP
- SNMP
- OSPF

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

- OSPF
- RIP
- BGP
- SNMP
- ICMP

Maks poeng: 3

15

DAT204-G H19, ARP

```
> Frame 647: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: HewlettP_dd:a3:00 (3c:a8:2a:dd:a3:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: HewlettP_dd:a3:00 (3c:a8:2a:dd:a3:00)
      Address: HewlettP_dd:a3:00 (3c:a8:2a:dd:a3:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000000000
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HewlettP_dd:a3:00 (3c:a8:2a:dd:a3:00)
    Sender IP address: 128.39.200.113
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 128.39.200.165
```

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

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

Velg riktige alternativer:

- ARP svar bruker alltid kringkastingsadressen som destinasjons adresse.
- En MAC-adresse har fast lengde på 48 bits.
- ARP forespørsler ender opp hos en ARP-server som tilordner en MAC-adresse til den spørrende verten.
- ARP er en protokoll som ligger et sted mellom nettverkslaget og linklaget i Internett 5-lags modellen.
- ARP kringkastingsadresse er 00:00:00:00:00:00.
- MAC-adressen til en vert (klient) i et LAN er innkapslet i link-lags rammene den sender og følger med rammene hele veien til en vert (server) i et annet LAN.
- En vert kan ha flere IP-adresser og flere MAC-adresser.
- En vert kan bare ha en MAC-adresse.
- Verter og rutere bruker ARP til å knytte en IP-adresse til en MAC-adresse og vedlikeholde en ARP-tabell i sitt minne.
- Vert med IP-adresse 128.39.200.113 har MAC-adresse 3c:a8:2a:dd:a3:00.

Maks poeng: 4

16

DAT204-G H19, Ethernet LAN

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

Hvilke IEEE standarder spesifiserer kablet Ethernet? (802.11, 802.3, 802.5, 802.13)
Hvilken kablet LAN topologi er den aller mest vanligste i dag?
(Stjerne med punkt-til-punkt linker og svitsj i midten., Ring med token passering., Buss med alle noder i samme kollisjons-domene.)
Hvilken kabel type er mest vanlig i LAN i dag? (Fiberoptisk kabel, To-parkabel, Koaksialkabel, Tvunnet parkabel)

En vert i et LAN har fått tildelt IPv4 adresse: 192.168.129.89/23 på CIDR format.
Hva er nettverksmasken skrevet på punktum-desimal format? (0.0.0.23, 23.23.23.23, 192.168.254.0, 255.255.254.0, 255.255.1.0)
Hva er korrekt konfigurert adresse til gateway ruteren som befinner seg i samme subnett som denne verten? (192.168.130.100, 192.168.1.1, 255.255.254.23, 192.168.23.1, 192.168.128.1)

Maks poeng: 3.75

17

DAT204-G H19, Transfer delay

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

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

Hvor stor blir den minimale rundturforsinkelsen (RTT) i millisekunder for datagrammer på denne linken? Avrund svaret til nærmeste millisekund. ms

Hvilken type forsinkelse gir det største bidraget til den totale tidsforsinkelsen i dette scenariet? (Transmisjonsforsinkelse, Forplantningsforsinkelse, Prosesseringsforsinkelse, Køforsinkelse)

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

Velg et alternativ:

- Nei
- Ja

Maks poeng: 3

18

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

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

Velg riktige alternativer:

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

Maks poeng: 6

19

DAT204-G H19, SSL quality of service

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

Hvilken socket type forbedrer Secure Socket Layer (SSL) med sikkerhetstjenester?
Velg ett alternativ:

- TCP
- IPv4
- HTTP
- IPv6
- UDP

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

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

Hvilke servicegarantier gir SSL sockets?
Velg riktige alternativer:

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

Maks poeng: 3.5

20

DAT204-G H19, SSL socket and cryptographic algorithms

```
import socket
import ssl

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

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

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

Velg riktige alternativer:

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

Maks poeng: 9

21 # DAT204-G H19, comments and assumptions

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

Skriv antagelser og kommentarer til oppgavene her:

Format

Words: 0

Maks poeng: 0

Question 2

Attached

Start of session:

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

```
> Frame 66: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: LcfcHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)
v Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x54d9 (21721)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.39.200.255
    Destination: 85.165.93.169
v Transmission Control Protocol, Src Port: 60104, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 60104
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
    Checksum: 0xfc8f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

End of session:

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

```
> Frame 330: 608 bytes on wire (4864 bits), 608 bytes captured (4864 bits) on interface 0
> Ethernet II, Src: LcfcHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)
v Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 594
    Identification: 0x5529 (21801)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.39.200.255
    Destination: 85.165.93.169
v Transmission Control Protocol, Src Port: 60104, Dst Port: 80, Seq: 1019, Ack: 113978, Len: 554
    Source Port: 60104
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 554]
    Sequence number: 1019    (relative sequence number)
    [Next sequence number: 1573    (relative sequence number)]
    Acknowledgment number: 113978    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 254
    [Calculated window size: 65024]
    [Window size scaling factor: 256]
    Checksum: 0xfeb9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (554 bytes)
v Hypertext Transfer Protocol
  > GET /api/delta/fan/status HTTP/1.1\r\n
    Host: fanctrl.andersenitc.no\r\n
    Connection: keep-alive\r\n
    Accept: application/json, text/plain, */*\r\n
    DateX: Mon, 26 Nov 2018 07:55:58 GMT\r\n
    Authorization: None\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36\r\n
    Referer: http://fanctrl.andersenitc.no/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: nb,en-US;q=0.9,en;q=0.8\r\n
  v Cookie: _ga=GA1.2.870541523.1517819979; _biz_uid=cd6799c7fb3a4913b32c5dc59832da5d; _biz_nA=3; _biz_pendingA=%5B%5D\r\n
      Cookie pair: _ga=GA1.2.870541523.1517819979
      Cookie pair: _biz_uid=cd6799c7fb3a4913b32c5dc59832da5d
      Cookie pair: _biz_nA=3
      Cookie pair: _biz_pendingA=%5B%5D
    \r\n
```