NTNU

KANDIDAT

10326

PRØVE

# TTM4100 1 Kommunikasjon - Tjenester og nett

| | |
|---|---|
| Emnekode | TTM4100 |
| Vurderingsform | Skriftlig eksamen |
| Starttid | 02.06.2025 07:00 |
| Sluttid | 02.06.2025 11:00 |
| Sensurfrist | 24.06.2025 21:59 |
| PDF opprettet | 02.06.2025 10:07 |

**Part 0**

| Oppgave | Tittel | Oppgavetype |
|---|---|---|
| ℹ | Cover page | Informasjon eller ressurser |

**Part I - Automatically Marked Questions**

| Oppgave | Tittel | Oppgavetype |
|---|---|---|
| ℹ | Part I - Automatically Marked Questions | Informasjon eller ressurser |
| 1 | Part I - Question 1 | Flervalg |
| 2 | Part I - Question 2 | Flervalg |
| 3 | Part I - Question 3 | Flervalg |
| 4 | Part I - Question 4 | Sant/usant |
| 5 | Part I – Question 5 | Sant/usant |
| 6 | Part I – Question 6 | Sant/usant |
| 7 | Part I – Question 7 | Sant/usant |
| 8 | Part I – Question 8 | Sant/usant |
| 9 | Part I – Question 9 | Sant/usant |
| 10 | Part I – Question 10 | Sant/usant |
| 11 | Part I – Question 11 | Sant/usant |
| 12 | Part I – Question 12 | Sant/usant |
| 13 | Part I – Question 13 | Sant/usant |
| 14 | Part I – Question 14 | Sant/usant |
| 15 | Part I – Question 15 | Flervalg |
| 16 | Part I – Question 16 | Paring |
| 17 | Part I - Question 17 | Plasser i tekst |
| 18 | Part I - Question 18 | Plasser i tekst |
| 19 | Part I - Question 19 | Plasser i tekst |
| 20 | Question 20 | Plasser i tekst |
| 21 | Part I – Question 21 | Flervalg |
| 22 | Part I - Question 22 | Flervalg |
| 23 | Part I - Question 23 | Flervalg |
| 24 | Part I - Question 24 | Flervalg |

**Part II - Manually Marked Questions**

| Oppgave | Tittel | Oppgavetype |
|---|---|---|

| i | Part II - Manually Marked Questions | Informasjon eller ressurser |
|---|---|---|
| 25 | Part II - Question 1 | Langsvar |
| 26 | Part II - Question 2 | Langsvar |
| 27 | Part II - Question 3 | Langsvar |
| 28 | Part II - Question 4 | Langsvar |
| 29 | Part II - Question 5 | Langsvar |
| 30 | Part II - Question 6 | Langsvar |
| 31 | Part II - Question 7 | Langsvar |

## 1 Part I - Question 1

Hvordan strømmes innhold (valgt blant millioner av videoer) til hundretusenvis av samtidige brukere?
**Velg ett alternativ:**

- Ved å lagre alt på én server
- Ved å lagre flere kopier av videoer på flere geografisk distribuerte steder

Maks poeng: 1

## 2 Part I - Question 2

Vi vet at DNS-tjenesten kjører over UDP, men kan den også kjøre over TCP?
**Velg ett alternativ:**

- Nei
- Ja

Maks poeng: 1

## 3 Part I - Question 3

Er denne påstanden korrekt: Overbelastningskontroll (congestion control) og flytkontroll (flow control) er det samme.
**Velg ett alternativ:**

- Nei
- Ja

Maks poeng: 1

## 4 Part I - Question 4

På internett sendes pakker uavhengig av hverandre, og kan bruke ulike ruter gjennom nettverket.
**Velg ett alternativ:**

- False
- True

Maks poeng: 1

## 5 Part I – Question 5

En protokoll er et sett med regler som bestemmer oppførselen mellom enheter på angrensende lag, altså mellom enheter på lag (N+1) og lag (N)

**Velg ett alternativ:**

- False
- True

Maks poeng: 1

## 6 Part I – Question 6

«Best effort» betyr at avsenderen bruker gjensending (retransmission) om nødvendig.
**Velg ett alternativ:**

- False
- True

Maks poeng: 1

## 7 Part I – Question 7

Linklaget og nettverkslaget kjøres alltid sammen
**Velg ett alternativ:**

- True
- False

Maks poeng: 1

## 8 Part I – Question 8

En maskin finner første hopp-ruteren og DNS-serverens adresse ved hjelp av DHCP.
**Velg ett alternativ:**

- False
- True

Maks poeng: 1

## 9 Part I – Question 9

Det er nettverksdelen av IP-destinasjonsadressen som identifiserer mottakeren innenfor et subnettverk.
**Velg ett alternativ:**

- True
- False

Maks poeng: 1

## 10 Part I – Question 10

Rutere bruker ARP til å finne det neste hoppet når de videresender (forward) pakker.
**Velg ett alternativ:**

- True
- False

Maks poeng: 1

## 11 Part I – Question 11

Aksessrutere (access routers) bruker hele IP-adressen når de videresender datagrammer mot destinasjonen.
**Velg ett alternativ:**

- False
- True

Maks poeng: 1

## 12 Part I – Question 12

Kjernerutere (core routers) bruker kun nettverksdelen av IP-adressen når de videresender datagrammer.
**Velg ett alternativ:**

- False
- True

Maks poeng: 1

## 13 Part I – Question 13

IP-adresser i nettverkslaget er alltid globalt unike.
**Velg ett alternativ:**

- True
- False

Maks poeng: 1

## 14 Part I – Question 14

Internettprotokollen (IP) garanterer at pakkene kommer frem i riktig rekkefølge.
**Velg ett alternativ:**

- (●) False
- ( ) True

Maks poeng: 1

## 15 Part I – Question 15

Anta at du har blitt tildelt nettverksblokken 208.27.1.0/22 og blitt bedt om å lage minst 12 subnett fra den.
Hvor mange brukbare verter (hosts) kan hver av disse subnettene ha?

**Velg ett alternativ:**

- ( ) 62
- (●) 64
- ( ) 32
- ( ) 60

Maks poeng: 1

## 16 Part I – Question 16

**Gitt en tabell med følgende struktur:**

- Den **øverste raden** inneholder tre klasser av flertilgangsprotokoll-klasse (multiple access protocol classes): **Kanalfordeling (Channel Partitioning)**, **Tilfeldig tilgang (Random Access)** og **Tur-taking (Taking Turns)**.
- Den **første kolonnen** viser seks multiple access-protokoller (f.eks. **Bluetooth**, **Ethernet CSMA/CD**, osv.).

**Oppgave:**
For hver av de oppførte multiple access-protokollene, kategoriser den i riktig flertilgangsprotokoll-klasse (multiple access protocols class) det tilbehører.

**Finn de som passer sammen:**

| | Taking Turns | Channel Partitioning | Random Access |
|---|---|---|---|
| CDMA (Code Division Multiple Access) | ( ) | (●) | ( ) |
| Bluetooth | (●) | ( ) | ( ) |
| FDDI (Fiber Distributed Data Interface) | (●) | ( ) | ( ) |
| Ethernet CSMA/CD | ( ) | ( ) | (●) |
| Slotted ALOHA | ( ) | ( ) | (●) |
| FDMA (Frequency Division Multiple Access) | ( ) | (●) | ( ) |

Maks poeng: 6

## 17 Part I - Question 17

**Dette spørsmålet handler om Cyclic Redundancy Check (CRC). Anta en datastreng på 101110.**
Gitt følgende begreper:

Hjelp

**Oppgave:**
Match hver av de følgende beskrivelsene med ett av begrepene som er oppgitt ovenfor.

Cyclic Redundancy Check (CRC) value: 001

CRC length: 3

CRC generator 1001

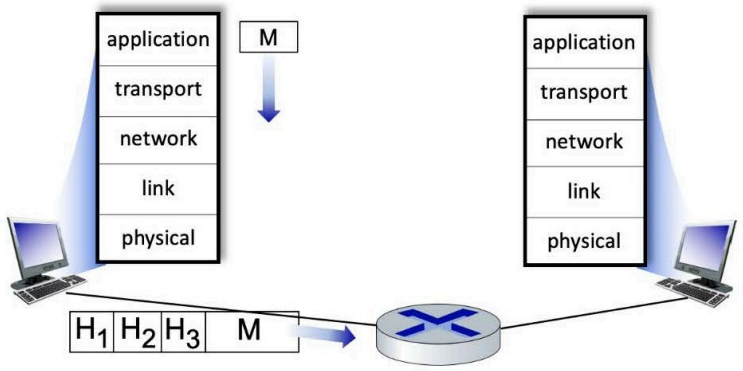
Total bits sent: 9

CRC generator polynom: x^3 + 1

Maks poeng: 5

## 18 Part I - Question 18

Se på figuren nedenfor, som viser en link-lag-ramme på vei fra en vert til en ruter.




Du får oppgitt fem lag som er plassert i disse boksene:

Hjelp

Application Layer Physical Layer

Hver header skal matches med riktig lag. Match én boks til hver av følgende headere:

Header $H_1$: Link Layer

Header $H_2$: Network Layer

Header $H_3$ Transport Layer

Maks poeng: 3

## 19 Part I - Question 19

Du får utdelt disse boksene som viser tilgangstype (Wired/Wireless) og omtrentlige hastigheter en abonnent kan forvente å oppleve i ulike aksessnettverk.

Hjelp

| | |
|---|---|
| Wired. Up to 10's of Mbps downstream / user | Wireless. 10's to 100's Mbps / device |
| Wired. 100 Mbps to 1 Gbps / link | Wired. 1 to 10 Gbps / link |
| Wireless. Up to 10's Mbps / device | Wireless, up to 10's Kbps / device. |
| Wired. Up to 10's to 100's Mbps downstream / user | |

Match en passende hastighet som abonnenter kan forvent å oppleve til hvert av følgende aksessnettverk:

Ethernet: Wired. 1 to 10 Gbps / link

4G cellular LTE: Wireless. 10's to 100's Mbps / device

Optical fiber: Wired. 1 to 10 Gbps / link

Cable access network: Wired. Up to 10's to 100's Mbps downstream / user

Maks poeng: 4

## 20 Question 20

Gitt en liste over TCP socket-relaterte handlinger som følger:

Hjelp

| | |
|---|---|
| Send using the socket created using socket (AF_INET, SOCK_DGRAM) | |
| Use the call socket (AF_INET, SOCK_DGRAM) | |
| Send using a socket not explicitly created via a call to socket () | |
| As the result of an accept(), a new socket is created, which binds the client and server together via this new socket without the need to explicitly specify the destination IP ad | |
| The client must explicitly include the server's IP address, port number, when sending | |

Match hver av disse tre generelle klient-side-handlingene med en spesifikk TCP socket-relatert handling som implementerer den.

1. Opprett en socket (Create a socket):
   Use the call socket (AF_INET, SOCK_STREAM)

2. Når man sender til en server, er dette hvordan en spesifikk server identifiseres
   (When sending to a server, this is how a specific server is identified):
   The client uses connect () to explicitly bind its socket to specific server, and so the server IP address and port number ne

3. Send til serveren, ved å bruke denne socketen (Send to server, using this socket):
   Send using the socket created using socket (AF_INET, SOCK_STREAM)

Maks poeng: 3

## 21 Part I – Question 21

Hvor implementeres transportlagets funksjonalitet primært?

**Velg ett alternativ:**

- Transportlagsfunksjoner implementeres primært i rutere og svitsjer i nettverket.
- Transportlagsfunksjoner implementeres primært i hver ende av en fysisk link som kobler én vert/ruter/svitsj til en annen vert/ruter/svitsj.
- Transportlagsfunksjoner implementeres primært i vertene i «enden» (the edge) av nettverket.

Maks poeng: 1

## 22 Part I - Question 22

Hvilket av følgende er en egenskap ved Advanced Encryption Standard (AES)?

**Velg ett alternativ:**

- Den er sårbar for kvanteangrep
- Den bruker en variabel nøkkellengde på 128, 192 eller 256 biter
- Det er en offentlig nøkkelalgoritme
- Den brukes primært for digitale signaturer
- Den ble utviklet av RSA Laboratories

Maks poeng: 1

## 23 Part I - Question 23

Hvilken transporttjeneste tilbys en applikasjon når den bruker en UDP-socket?

**Velg ett alternativ:**

- Flytkontroll (flow control). Tjenesten sikrer at senderen ikke sender så fort at bufrene hos mottakeren overfylles.
- Best effort-tjeneste. Det gjøres en best mulig innsats for å levere dataene til destinasjonen, men det gis ingen garanti for at noe bestemt datasegment faktisk når frem.
- Tapsfri dataoverføring. Tjenesten vil pålitelig overføre all data til mottakeren. Den sørger for å gjenopprette pakker som går tapt som følge av overfylte bufre.
- Gjennomstrømmingsgaranti (throughput guarantee). Socketen kan konfigureres til å gi en minimumsgjennomstrømning mellom avsender og mottaker.
- Sanntidslevering. Tjenesten garanterer at data leveres til mottakeren innenfor en gitt tidsramme.

Maks poeng: 1

## 24 Part I - Question 24

Hva er hovedformålet med en brannmur i nettverkssikkerhet?

**Velg ett alternativ:**

- Å kryptere data
- Å tilby VPN-tjenester
- Å blokkere uautorisert tilgang
- Å overvåke nettverksytelse
- Å håndtere nettverkstrafikk

Maks poeng: 1

## 25 Part II - Question 1

(5 poeng)
Hva er den viktigste forskjellen mellom videresending (forwarding) og ruting (routing)?

**Skriv ditt svar her**

Den viktigste forskjellen mellom videresending og ruting, er at videresending er en lokal handling som utføres av en enkel ruter/svitsj, mens ruting er en global handling utført av en mengde ruter som samhandler gjennom en rutingalgoritme.

Ord: 36

Maks poeng: 5

## 26 Part II - Question 2

(5 poeng)
Forklar forskjellen mellom transmisjonsforsinkelse (transmission delay) og propagasjonsforsinkelse (propagation delay) i datakommunikasjon.

**Skriv ditt svar her**

Transmisjonsforsinkelse er den mengden tid det tar å 'legge' bitsene/pakken ut på linken og er avhengig av hastigheten (bandwidth) til linken, mens propagasjonsforsinkelse er den tiden det tar for en bit å propagere (reise) gjennom linken, for eksempel fra en ende til en annen i en kabel, og er avhengig av propagasjonshastigheten til mediumet som den propagerer i (f.eks optisk fiber eller luften) og lengden på mediumet

Ord: 67

Maks poeng: 5

## 27 Part II - Question 3

(15 poeng)
En forsker har nettopp begynt på NTNU og fått sin NTNU-brukerkonto, som han også kan bruke til e-post. Han kobler deretter laptopen sin til Ethernet-porten på kontoret for å få nettverkstilkobling. Så sender han en e-post til sin samarbeidspartner ved Eindhoven University of Technology med sin NTNU-adresse via Outlook-desktop-applikasjonen. Gjør rede for hvilke protokoller som brukes i hvert trinn fra det øyeblikket han koblet inn laptopen, sendte e-posten fra Outlook-applikasjonen til samarbeidspartnerens nettbaserte e-posttjeneste, og samarbeidspartneren leste e-posten.

**Skriv ditt svar her**

Når forskeren kobler laptopen til i ethernetporten, så vil laptopen automatisk prøve å finne en DHCP server (antar at den ikke kjenner til en fra før), den vil gjøre dette med å broadcaste en DHCP discover melding på ethernet porten, som er en UDP pakke. Den vil bruke MAC/link protokollen Ethernet for å sende denne pakken, Ethernet tar i bruk CSMA/CD (collision detection) som MAC protokoll for å unngå/detektere kollisjoner. Siden destinasjonen er IP broadcast så benyttes ikke ARP, istedet brukes bare MAC broadcast adressen som destinasjon for framen. Hver svitsj i subnettet vil da forwarde denne pakken til alle tilgjengelige linker. Til slutt når den frem til en DHCP server, som svarer med en liste med tilgjengelige IP-adresser, laptopen velger en av disse og spør om DHCP om den kan få en av de, og DHCP serveren svarer til slutt med en ok (alle disse pakkene broadcastes). Laptopen har nå fått en IP adresse, og mest sannsynelig også ruterens IP, subnett masken og en eller flere IP for DNS. Mest sannsynlig vil outlook først sende ut noen DNS queries når appen starter (microsoft skal tracke deg), men den sender ihvertfall en DNS query for mail serveren til NTNU (hvis den ikke er spesifisert med en IP i outlook), og får tilbake en MX-record (IP-en til mail serveren til NTNU), DNS bruker UDP. Link laget vil da bruke ARP når pakkene sendes til DNS serveren for å finne ut hvilke MAC adresse som den skal sendes til, hvis DNS serveren ligger på samme subnet så vil den svare, ellers vil ruteren svare. Outlook vil bruke IMAP for å sende denne mailen til NTNUs mail server, og da vil TCP bli brukt. NTNU vil videresende denne mailen til destinasjons mailadressens mailserver med SMTP, som også bruker TCP. Siden mottakeren bruker en nettbasert e-posttjeneste så vil han mest sannsynlig bruke HTTPS for å lese den, altså HTTP med TLS for kryptering. HTTP bruker TCP. Nevnte det ikke fordi det er åpenbart, men TCP og UDP bruker selvfølgelig protokollene lenger nede i protokollstakcen som nevnt i starten, altså IP, ARP, Ethernet og CSMA/CD.

Liste over protokoller:

- DHCP
- UDP
- CSMA/CD
- Ethernet
- IP
- ARP
- TCP
- IMAP
- SMTP
- DNS
- HTTPS (HTTP + TLS)

Ord: 378

---

Maks poeng: 15

## 28 Part II - Question 4

(5 poeng)
Anta at en webserver har fem pågående tilkoblinger som bruker TCP-mottaksport 80, og at det ikke finnes noen andre TCP-tilkoblinger (hverken åpne, under opprettelse eller lukkede) på serveren.

**Oppgave:**
1. (2 poeng) Hvor mange TCP-socketer er i bruk på denne serveren?

2. (3 poeng) Forklar hvordan du kom frem til dette resultatet.

**Skriv ditt svar her**

1. Det er 6 TCP-socketer i bruk på denne serveren, en som en velkomst-socket som tar imot nye tilkoblinger, og en hver for hver av de fem tilkoblingene til serveren

2. Hvis en server tar imot TCP tilkoblinger på en port så vil den ha en TCP velkomst-socket. Når den aksepterer en tilkobling på denne socketen, så vil en ny socket bli opprettet for å snakke med den nye klienten. Siden det er fem tilkoblinger og en mottaksport, så vil det være 5 + 1 = 6 TCP-socketer i bruk på serveren.

Ord: 92

---

Maks poeng: 5

## 29 Part II - Question 5

(15 poeng)
**Disse delspørsmålene handler om Caesar-chifferet.**

1. (3 poeng) Beskriv hvordan Cæsarchiffer (Caesar cipher) fungerer.

2. (6 poeng) Krypter meldingen **'PROTECT YOUR INFORMATION'** ved å bruke Caesar-chiffer med en forskyvning på k = 7, og ta kun hensyn til bokstavene i det engelske alfabetet.

3. (6 poeng) Dekrypter meldingen **'JHLZHY JPWOLY JHU WYVALJA FVBY KHAH'** ved å bruke Caesar-chiffer med en forskyvning på k = 7, og ta kun hensyn til bokstavene i det engelske alfabetet.

**Skriv ditt svar her**

1. Cæsarchiffer fungerer med at du forskyver hver bokstav en forhåndsbestemt mengde i forhold til alfabetet, så med en forskyvning på 2 så ville alle 'a' i ordet bli til 'c', den vil loope rundt hvis du kommet etter 'z', så 'y' med forskyvning på 2 vil bli 'a', for å komme tilbake til originalordet forskyver du bare med -forskyvning

2. 'PROTECT YOUR INFORMATION' kryptert med Caesar-chiffer med en forskyvning på k = 7: **'WYVALJA FVBY PUMVYTHAPVU'**

3. 'JHLZHY JPWOLY JHU WYVALJA FVBY KHAH' dekryptert med Caesar-chiffer med en forskyvning på k = 7: **'CAESAR CIPHER CAN PROTECT YOUR DATA'**

Ord: 100

---

Maks poeng: 15

## 30 Part II - Question 6

(5 poeng)
Hva er den viktigste forskjellen mellom symmetriske nøkkelsystemer og offentlige nøkkelsystemer i kryptografi?

**Skriv ditt svar her**

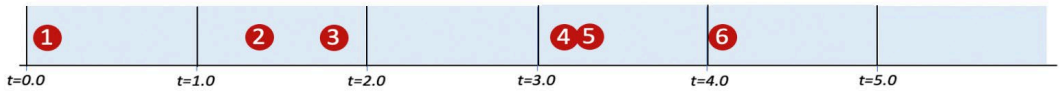
Den viktigste forskjellen er at i symmetriske nøkkelsystemer så har du bare en nøkkel som både krypterer og dekrypterer, som gjør at alle som kan kryptere også kan dekryptere og omvendt (ikke alltid ønskelig). Mens i offetlige nøkkelsystemer så har du en nøkkel som krypterer og en nøkkel som dekrypterer. Disse nøklene er sammenkoblet, og du vil som oftest gjøre en av de offentlig og den andre privat.

Ord: 68

Maks poeng: 5

## 31 Part II - Question 7

(10 poeng)
Se på figuren nedenfor, som viser tidspunktene for når 6 pakker ankommer ulike trådløse flertilgangsnoder (multiple access wireless nodes) for overføring (transmission). Tidspunktene for ankomst er = 0.1, 1.4, 1.8, 3.2, 3.3, 4.1. Hver overføring krever nøyaktig én tidsenhet.




Anta at det tar 0.2 tidsenhet for et signal å propagere fra én node til hver av de andre nodene.

Gitt overføringsforsøkene vist i tidslinjen ovenfor, **identifiser hvilke pakker som blir vellykket overført under CSMA-protokollen (uten kollisjonsdeteksjon). Begrunn svaret ditt basert på protokollens virkemåte."**

Du kan anta at hvis en pakke opplever en kollisjon eller merker at kanalen er opptatt, vil ikke noden forsøke ny overføring av den pakken før en gang etter t = 5 (utenfor den gitte tidsskalaen).

**Skriv ditt svar her**

Antar at det brukes CSMA-persistant siden det ikke er spesifisert en spesifikk CSMA protokoll. Den vil da lytte på mediumet og sende dataen sin med en gang det ikke er en annen overgang i mediumet. Den første noden vil da sende pakke 1 når t=0.1, de andre vil se denne når t=0.3 og den vil vare til t=1.3. Så pakke 1 vil bli vellykket. Pakke 2 vil bli sendt t=1.4 siden mediumet er ledig, node 3 vil se denne overføringen t=1.7 og vil da vente med sin, overføringen 2 er ferdig t=2.7. Så pakke 2 vil bli vellykket. Node 3 vil begynne å sende når t=2.7 og vil bli ferdig t=4, alle andre node vil se overføringen når de vil sende pakke og vente. Så pakke 3 vil bli vellykket. Node 4 og 5 vil begge sende overføring når t=4 siden de ventet på overføring 3, node 6 vil sende sin når t=4.1 siden node 4 og 5 sin overføring har ikke nådd den enda. Alle disse tre vil kollidere. Så det vil bare være pakke 1, 2 og 3 som vil bli overført vellykket.

Ord: 185

Maks poeng: 10