NTNU
Kunnskap for en bedre verden

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Eksamensoppgave i
TTM4100 Kommunikasjon – tjenester og nett

Faglig kontakt under eksamen: Norvald Stol

Tlf.: 97080077

SOLUTION

Eksamensdato: 11. aug 2018

Eksamenstid (fra-til): 0900-1300

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

Målform/språk: Engelsk / Bokmål

Antall sider (uten forside): 4

Antall sider vedlegg: 0

Informasjon om trykking av eksamensoppgave

Originalen er:

1-sidig ☐ **2-sidig** ☐

sort/hvit ☐ **farger** ☐

skal ha flervalgskjema ☐

Kontrollert av:

Dato Sign

Merk! Studenter finner sensur i Studentweb. Har du spørsmål om din sensur må du kontakte instituttet ditt. Eksamenskontoret vil ikke kunne svare på slike spørsmål.

1. Link layer / Linklag (4+4+4+5+4+4=25 points)

1.1 E: Give a brief overview of the link layer. (Keywords: main tasks/functions, protocol(s) used, where in network it is present).
B: Gi en kort oversikt over linklaget. (Stikkord: hovedoppgaver/funskjoner, protokoll(er) brukt, hvor i nettet det er til stede).

The link layers main task is to transport frames between network units, i.e. one link at a time. Different types of physical links needs different protocols. For this reason there are many possible link layer protocols in use, e.g. Ethernet protocol (with or without CSMA/CD), CSMA/CA (for WiFi), PPP, or more fixed link sharing protocols like TDM, FDM, CDMA, etc. The link layer is present in all active network elements.

1.2 E: Give short high-level explanations of the channel partitioning techniques denoted TDM (Time Division Multiplexing), FDM (Frequency Division Multiplexing) and CDMA (Code Division Multiple Access). (Keywords: only main principles of each technique are necessary, no details).
B: Gi korte høynivå forklaringer på virkemåte for teknikkene for kanaldeling kalt TDM (tidsdelt multipleksing), FDM (frekvensdelt multipleksing) og CDMA (Kodedelt multippel aksess). (Stikkord: kun hovedprinsipper for virkemåte er nødvendig, ingen detaljer).

TDM: Divides time into time frames and further divides each time frame into time slots. Each (periodically repeating) time slot is assigned to a given sender and used when a sender has something to send. In a given time frame a time slot may be empty if the sender did not have anything to send at that time.
FDM: A channel is divided into different frequencies (each with parts of the bandwidth available for the total channel) and each frequency is assigned to a given sender. Information can be sent at any time on the given frequency, but only by the sender it is allocated to.
CDMA: Each sender is allocated different codes (with special properties) to be used to encode the data bits to be sent. All senders can then send continuously over the same channel (full bandwidth). A receiver in principle receives all transmissions, but uses the code of a specific sender to filter out the data intended for it. All other transmissions look like noise for this receiver.

1.3 E: Complete the two-dimensional even parity matrix shown in Figure 1. Give answers left to right for xxxx and from top down for yyyy, and z as single value.
B: Fullfør den to-dimensjonale lik ("even") paritetsmatrisen vist i Figur 1. Gi svaret fra venstre til høyre for xxxx, fra topp til bunn for yyyy, og z som enkeltverdi.

1	0	0	1	y
0	1	0	0	y
0	1	0	1	y
0	1	0	1	y
x	x	x	x	z

Figure 1: Two-dimensional even parity matrix

xxxx = 1101
yyyy = 0100
z = 1

1.4 E: Find the Cyclic Redundancy Check (CRC) code for the data bit pattern 101010 using the generator 1011. When is the computed CRC value sent to the receiver?
B: Finn "Cyclic Redundancy Check" (CRC) koden for datastrengen 101010 når generatoren 1011 brukes. Når sendes den beregnede CRC verdien til mottaker?

Following the same set-up as the textbook (ref. Fig. 6.7, but with changed values):

```
        100111 (<- division result; not used for anything)
1011  101010000 (<- zeros added to compute CRC; one less than generator)
      1011
      0001100
         1011
         01110
          1011
          01010
           1011
           0001 = CRC
```

The CRC is sent after the data, instead of the added zeros for the division, i.e. 101010001. This will give remainder zero (000) at receiver as check of successful transmission.

1.5 E: What is the Address Resolution Protocol (ARP) used for and where are the ARP tables located?
B: Hva brukes "Address Resolution Protocol" (ARP) for og hvor er ARP tabellene plassert?

ARP translates between IP and MAC addresses within a subnet. The ARP tables are located in the memory of each host and router.

1.6 E: What type of addresses do you find in the switch table of a link-layer switch?
B: Hvilke(n) type addresser finner du i en svitsjetabell for en linklagssvitsj**?**

MAC addresses.

2. Network layer /Nettverkslag (3+3+3+4+4+3+5=25 points)

2.1 E: Give a brief overview of the network layer. (Keywords: main tasks/functions, protocol(s) used, where in network it is present).
B: Gi en kort oversikt over nettverkslaget. (Stikkord: hovedoppgaver/funksjoner, protokoll(er) brukt, hvor i nettet det er til stede).

The most important function of the network layer is to get datagrams routed to their intended destinations. The Internet Protocol (IP) is the main protocol used. The network layer is present in all network routers, and in all end-systems.

2.2 E: What is meant by the term "fragmentation" (in an Internet context) and why is it used for IPv4 datagrams?

B: Hva menes med fragmentering (i Internet protokoll sammenheng) og hvorfor brukes det for IPv4 datagrammer?

Fragmentation is to divide an IP datagram into two or more smaller IP datagrams, encapsulate each of these smaller IP datagrams in a separate link-layer frame; and send these frames over the outgoing link. This is necessary because different link layer protocols allow different maximum sizes of the frames they can carry, e.g. given by different physical constraints on different physical media.

2.3 E: Where are fragments reassembled when using IPv4?
B: Hvor blir fragmenter reassemblert ("reassembled") når IPv4 brukes?

The reassembly is done in the end systems, not in the routers.

2.4 E: How does one know when all fragments have been received so the reassembly can be done/finished?
B: Hvordan vet en at alle fragmenter er mottatt slik at reassembleringen kan gjøres/fullføres?

This is signaled via one of the three "Flag" bits. It contains a 1 for all fragments except the last one which is 0.

2.5 E: When using the IPv6 protocol, fragmentation is not allowed in routers, only in end-systems. What happens if an IPv6 router receives an IPv6 segment which is too large to be forwarded on an outgoing link?
B: Ved bruk av IPv6 protokollen tillates ikke bruk av fragmentering i rutere, kun i endesystemer. Hva skjer hvis en IPv6 ruter mottar et IPv6 segment som er for stort til å bli sendt videre på en utgående link?

If an IPv6 datagram received by a router is too large to be forwarded over the outgoing link, the router simply drops the datagram and sends a "Packet Too Big" ICMP error message back to the sender. The sender can then resend the data, using a smaller IP datagram size.

2.6 E: Assume the (CIDR) IPv4 address 223.1.8.0/xx. If we need around 1500 IP addresses available for hosts and router interfaces in our network, what is the maximum value we can use for xx?
B: Anta (CIDR) IPv4 adressen 223.1.8.0/xx. Hvis vi trenger omtrent 1500 IP addresser tilgjengelige for verter og ruterinterface i nettet vårt, hva er den maksimale verdien vi kan bruke for xx?

xx = 21 which gives (almost) 2048 addresses (xx = 22 would give (almost) 1024 addresses, which is too low). ("Almost" above because a couple of addresses are always reserved for special purposes).

2.7 E: Suppose a router in the network has the (CIDR) entries in its routing table as shown below. For each of the following destination IP addresses, indicate which interface the router sends the packet to.
B: Anta at en ruter i nettet har (CIDR) innslag i rutingstabellen som nedenfor. For hver av følgende destinasjons IP addresser, angi hvilket interface ruteren sender pakken til.

Address/mask	**Next hop**
135.46.128.0/22	Interface 0

135.46.188.0/22	Interface 1
135.46.144.0/23	Interface 2
Default	Interface 3

2.7.1: 135.46.189.128 ***(sent to interface 1)***
2.7.2: 135.46.50.20 ***(sent to interface 3)***
2.7.3: 135.46.146.30 ***(sent to interface 3)***
2.7.4: 135.46.145.7 ***(sent to interface 2)***
2.7.5: 135.46.130.35 ***(sent to interface 0)***

3. Application layer and multimedia / Applikasjonslag og multimedia (4+4+4+4+4=20 points)

3.1 E: Explain circuit switching and packet switching and list at least three differences between them.
B: Forklar linjesvitsjing og pakkesvitsjing og nevn minst tre forskjeller mellom dem.

Circuit switching is a switching technique for communication networks. Circuit switching creates a direct physical connection/path between two devices. The transmission capacity on the path is exclusively reserved for the connection.

Packet switching is a switching technique for communication networks. In packet switching, each packet has a header providing an address to identify the destination. In the network, packets are (usually) switched in the store-and-forward manner, i.e., at each node, packets are received and stored, before being forwarded to the next hop.

Three out of the four following for full score:

i) A circuit-switched network can guarantee a certain amount of end-to-end bandwidth for the duration of a call. Most packet-switched networks today (including the Internet) cannot make any end-to-end guarantees for bandwidth.

ii) In a circuit switched network, there is no delay variation (or jitter) among packets/messages, while in a packet-switched network, delay variation can be big. Essentially, circuit-switching is better in providing quality of service than packet-switching.

iii) Circuit switching typically provides connection-oriented services, while both connection-oriented and connectionless services may be provided in a packet-switched network.

iv) Packet switching employ statistical multiplexing and hence can make better use of the resource of a link, i.e. link capacity, while in circuit switching, a connection (i.e. circuit) does not share the circuit with others even though there is nothing being sent on the connection.

3.2 E: What is the main task of the "Domain Name System (DNS)" in the Internet and which two fundamental components does it consist of?
B: Hva er hovedoppgaven til "Domain Name System (DNS)" i internett og hvilke to fundamentale komponenter er det satt sammen av?

The main task of DNS is to be a directory service that translates hostnames to IP addresses.

The two main parts:
i) a distributed database implemented in a hierarchy of DNS servers, and
ii) an application-layer protocol that allows hosts to query the distributed database.

3.3 E: Why must jitter (delay-variation) be removed (at the receiver) when audio is sent over the public Internet?
B: Hvorfor må jitter (forsinkelsesvariasjon) fjernes (hos mottaker) når lyd sendes over offentlig Internet?

To give smooth / time-corrected playback.

3.4 E: Give a short explanation of how "Forward Error Correction" (FEC) is done.
B: Gi en kort forklaring på hvordan «Forward Error Correction» (FEC) gjøres.

Extra information is added to the data (e.g. parity bits) at source. This is used to recreate lost or corrupted information at the destination (or alternatively it may be done locally for each link).

3.5 E: Consider sending a file of 1600K bytes from Host A to Host B over a circuit-switched network. Suppose it takes 400 ms to establish an end-to-end circuit between Host A and Host B before Host A can begin to transmit the file. Also suppose the end-to-end circuit passes through five links, and on each link the circuit has a transmission rate of 256 Kbps. At least how much time does it take to send the file from Host A to Host B?
B: En datafil på 1600K bytes sendes fra Host A til Host B over et linjesvitsjet nett. Sett at det tar 400 ms å opprette en ende-til-ende forbindelse mellom Host A og Host B før Host A kan begynne å sende datafilen. Anta videre at ende-til-ende forbindelsen passerer gjennom fem lenker, og at hver lenke har en transmisjonsrate på 256 Kbps. Hvor lang tid vil det minst ta å sende datafilen fra Host A til Host B?

The transmission time or delay is simply 1600K x 8bits /256Kbps = 50 s, no matter how many links the circuit crosses. Additionally, it has to be waited for 400 ms until the circuit is established. So, at least it takes 400 ms + 50 s = 50.4 seconds. (Note: if propagation time is taken into account, this value will be added to the total time. But since the length of links are not given this value is unknown).

4. Information security / Informasjonssikkerhet (4+3+4+4=15 points)

4.1 E: Explain briefly the main difference between "Symmetric Key Cryptography" and "Public Key Encryption". (Keywords: secret or known algorithm, secret or known key(s), examples of what may be used for).
B: Forklar kort hovedforskjellene på symmetrisk nøkkel kryptering ("Symmetric Key Cryptography") og offentlig nøkkel kryptering ("Public Key Encryption"). (Stikkord: hemmelig eller kjent algoritme, hemmelig(e) eller kjent(e) nøkkel/nøkler, eksempler på hva brukes til).

In modern cryptography the algorithms are always assumed to be known, so the security rests

with breaking the key(s). (Historically this is not true for symmetric key crypto; and for some military uses it may still not be true…). Symmetric key cryptography uses the same key to encrypt and decrypt, thus it is shared by both parts in a communication. For public key encryption there are two keys, one private and secret and one public and known to all. Both systems may e.g. be used to achieve confidentiality of information. Public key cryptography may also be used to achieve message integrity and to establish digital signatures.

4.2 E: How are the following terms defined in an information security context?
B: Hvordan defineres følgende begrep i en informassjonssikerhets sammenheng?
4.2.1: Confidentiality / Konfidensialitet.
4.2.2: Integrity / Integritet.
4.2.3: Authentication / Autentisering (eller autentitet).

Confidentiality: Protect against unauthorized disclosure of information.
Integrity: Avoid intentional or unintentional modification of information.
Authentication: Genuineness of data or users.

4.3 E: The Caesar cipher is used to encrypt "Have a nice day" to "Ibwf b ojdf ebz". What key is used?
B: Cæsar cipher brukes til å kryptere "Have a nice day» til «Ibwf b ojdf ebz». Hvilken nøkkel ble brukt?

The key is +1 (modulo the length of the alphabet), i.e. a -> b, b -> c, …, z -> a (for english alphabet).

4.4 E: What is the purpose of the Secure Socket Layer» (SSL)?
B: Hva er hensikten med «Secure Socket Layer» (SSL)?

SSL is made to add security to the transport layer / TCP connections.

5. Wireless and cellular / Trådløs og mobil (4+4+4+3=15 points)

5.1 E: What is/are the main difference(s) between CSMA/CD and CSMA/CA with regard to functionality? What does "CA" in CSMA/CA mean and how is it achieved?
B: Hva er hovedforskjellen(e) mellom CSMA/CD og CSMA/CA med hensyn til virkemåte? Hva betyr "CA" i CSMA/CA og hvordan oppnås det?

In CSMA/CD a station begins transmitting as soon as the channel is sensed idle, while in CSMA/CA this is controlled via counting down a random back-off delay, to decrease the probability of collision with other stations. Also, some minimum space is in place after a successful transmission to allow priority access for ACK control frames (and other short control frames, see RTS and CTS below).

CA = Collision Avoidance. It is not really achieved in full, since frames sent from two or more stations may still collide, but the modified procedure described above at least makes it much less likely than in e.g. Ethernet.

5.2 E: What random access method is used in the 802.11 MAC protocol? Give a brief and high-level explanation of how it works. (Keywords: how stations access medium, how collisions are detected or handled).
B: Hvilken "random access" metode brukes i 802.11 MAC protokollen? Gi en kort høynivå beskrivelse av hvordan den virker. (Stikkord: hvordan stasjoner aksesserer mediet, hvordan kollisjoner detekteres eller håndteres).

"Carrier Sense Multiple Access with Collison Avoidance" (CSMA/CA) is used. When not transmitting, a station is listening for activity on the medium. Following certain rules made to (try to) avoid collisions and to let certain short frames have priority (e.g. acknowledgements) a station may attempt to transmit. This is controlled via counting down a random back-off delay, to decrease the probability of collision with other stations. Also, some minimum space is in place after a successful transmission to allow priority access for ACK control frames (and other short control frames). Collision Avoidance is not really achieved in full, since frames sent from two or more stations may still collide. Collisions cannot be observed by a sending station so explicit acknowledgements are necessary. Lack of such means that collision is assumed and the frame is resent.

5.3 E: 802.11 W-LAN defines an optional scheme based on the use of "Request-To-Send (RTS)" and "Clear-To-Send (CTS)" control frames. Explain briefly how it works and when it (potentially) is used.
B: 802.11 W-LAN definerer en tilleggsopsjon basert på bruk av "Request-To-Send (RTS)" og "Clear-To-Send (CTS)" kontrollrammer. Forklar kort hvordan det virker og når det (eventuelt) blir brukt.

Two wireless stations which both may communicate with the Access Point (AP) may still be hidden from each other, i.e. one station may think the channel is free when it is actually used by the other station. This will lead to potential collisions in the area around the AP. The RTS and CTS frames are used to reserve the channel ahead of time. The confirmation of this reservation (a short CTS frame) will be detected by all stations since it is broadcast by the AP. Although the RTS/CTS exchange can help reduce collisions, it also introduces delay and consumes channel resources. For this reason, the RTS/CTS exchange is only used (if at all) to reserve the channel for the transmission of a long DATA frame. In practice, each wireless station can set an RTS threshold such that the RTS/CTS sequence is used only when the frame is longer than the threshold.

5.4 E: What are the main differences between 3G and 4G mobile cellular systems?
B: Hva er hovedforskjellene på 3G og 4G mobile cellulære systemer?

The two most important changes from 3G to 4G is an all IP core network, and an enhanced radio access network based on use of orthogonal frequency division multiplexing (OFDM).