Eksamensoppgave i

TTM4100 KOMMUNIKASJON – TJENESTER OG NETT

Faglig kontakt under eksamen: Norvald Stol

Tlf.: 97080077

ENGELSK FASIT

Eksamensdato: 6. juni 2019

Eksamenstid (fra-til): 1500-1900

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:---- / Engelsk / -----

Antall sider: --

Antall sider vedlegg: 0

Kontrollert av:

_____

Dato   Sign

1. Multiple areas / Ulike områder (40 p)

E: Each of the ten subgroups below has zero, one or more correct answers. **The total number of correct answers (summed over 1.1 to 1.10 below) is 20**. Each correct answer gives 2 points. You are not penalized for a wrong answer, **up to a total of 20 answers**. Do not claim that **more** than 20 answers are correct in total for task 1. Doing so results in **a penalty of minus 3 points for each additional answer**.

1.1
E: Assume that S and T have an active Transmission Control Protocol (TCP) connection between them. Assume that the last successful byte S has received from T is numbered as 123, and the last successful byte T has successfully received from S is numbered as 267. Which (if any) of the alternatives below are possible exchanges between them following this situation?

E:
a) S sends 50 bytes of data to T and appends ACK=124; after receiving this T sends 76 bytes of data to S and appends ACK=344.
b) S sends 100 bytes of data to T and appends ACK=224; after receiving this T sends 96 bytes of data to S and appends ACK=364.
c) S sends no data to T but sends ACK=124; after receiving this T sends 76 bytes of data to S and appends ACK=268.
d) T sends 100 bytes of data to S and appends ACK=224; after receiving this S sends 100 bytes of data to T and appends ACK=368.
e) T sends 50 bytes of data to S and appends ACK=268; after receiving this S sends 90 bytes of data to T and appends ACK=174.
f) T sends no data to S but sends ACK=268; after receiving this S sends 100 bytes of data to T and appends ACK=224.
g) Both S and T send segments to each other in parallel: S sends 50 bytes of data to T and appends ACK=174 and T sends 16 bytes of data to S and appends ACK=284.
h) Both S and T send segments to each other in parallel: S sends 50 bytes of data to T and appends ACK=124 and T sends 36 bytes of data to S and appends ACK=268.

1.2
E: Which (if any) of the following terms/terminology are used to describe elements of the TCP congestion control scheme?

a) cyclic redundancy check
b) interleaving
c) forward error correction
d) short inter-frame spacing
e) slow start
f) clear-to-send
g) two-dimensional parity
h) congestion avoidance

1.3
E: Which (if any) of the following statements are correct about the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP)?

E:
a) UDP provides a reliable transport service to an application using it.
b) TCP provides an unreliable transport service to an application using it.
c) UDP uses congestion control.
d) UDP sets up an end-to-end connection before transfer of data can be started.
e) UDP provides a connection-oriented transport service to an application using it.
f) The TCP segment contains no checksum field.
g) A TCP connection provides only a one-way (simplex) transport service.
h) The UDP segment includes a checksum for error detection.

1.4

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

a) D = 101110, G = 1001, R = 001
b) D = 101110, G = 1001, R = 100
c) D = 101110, G = 1001, R = 011
d) D = 1010101010, G = 10011, R = 0100
e) D = 1010101010, G = 10011, R = 1010
f) D = 1010101010, G = 10011, R = 0000
g) D = 11111, G = 1011, R = 110
h) D = 11111, G = 1011, R = 100
i) D = 11111, G = 1011, R = 001

1.5

No.	Source	Destination	Protocol	Length	Info			
1	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xed2c39ac			
2	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xed2c39ac			
3	129.241.67.129	129.241.67.134	DHCP	342	DHCP Offer - Transaction ID 0xed2c39ac			
4	129.241.67.129	129.241.67.220	DHCP	342	DHCP Offer - Transaction ID 0xed2c39ac			
5	0.0.0.0		DHCP	342	DHCP Request - Transaction ID 0xed2c39ac			
6	129.241.67.129		DHCP	342	DHCP ACK - Transaction ID 0xed2c39ac			
7	Apple_44:c6:33	Broadcast	ARP	42	Who has 129.241.67.129? Tell 129.241.67.134			
8	Cisco_0b:d9:c2	Apple_44:c6:33	ARP	60	129.241.67.129 is at 40:55:39:0b:d9:c2			
9	129.241.67.134	129.241.0.200	DNS	74	Standard query 0x4d2e A www.google.com			
10	129.241.0.200	129.241.67.134	DNS	90	Standard query response 0x4d2e A www.google.co			
11	129.241.67.134	216.58.209.100	TCP	78	55485 > http(80) [SYN] Seq=0 Win=65535 Len=0 MS			
12	216.58.209.100	129.241.67.134	TCP	74	http(80) > 55485 [SYN, ACK] Seq=0 Ack=1 Win=4254			
13	129.241.67.134	216.58.209.100	TCP	66	55485 > http(80) [ACK] Seq=1 Ack=1 Win=131872 Le			
14	129.241.67.134	216.58.209.100	HTTP	614	GET / HTTP/1.1			
15	216.58.209.100	129.241.67.134	TCP	66	http(80) > 55485 [ACK] Seq=1 Ack=549 Win=43648 L			
16	216.58.209.100	129.241.67.134	HTTP	586	HTTP/1.1 302 Found (text/html)			
17	129.241.67.134	216.58.209.100	TCP	66	55485 > http(80) [ACK] Seq=549 Ack=521 Win=1313			
18	129.241.67.134	129.241.0.200	DNS	73	Standard query 0x0e58 A www.google.no			
19	129.241.0.200	129.241.67.134	DNS	89	Standard query response 0x0e58 A www.google.no			
20	129.241.67.134	216.58.209.99	TCP	78	55486 > http(80) [SYN] Seq=0 Win=65535 Len=0 MS			
21	216.58.209.99	129.241.67.134	TCP	74	http(80) > 55486 [SYN, ACK] Seq=0 Ack=1 Win=4254			
22	129.241.67.134	216.58.209.99	TCP	66	55486 > http(80) [ACK] Seq=1 Ack=1 Win=131872 Le			
23	129.241.67.134	216.58.209.99	HTTP	647	GET /?gfe_rd=cr&ei=MBrwVNzBDaur8wep9IAQ HTTP/1			
24	216.58.209.99	129.241.67.134	TCP	66	http(80) > 55486 [ACK] Seq=1 Ack=582 Win=43776 L			
25	216.58.209.99	129.241.67.134	HTTP	672	HTTP/1.1 302 Found (text/html)			
26	129.241.67.134	216.58.209.99	TCP	66	55486 > http(80) [ACK] Seq=582 Ack=607 Win=1312			

Figure 1: Wireshark trace

E: Figure 1 shows packets sent over a network of type ethernet. Which (if any) of the following statements about packets in the trace are correct?

a) Line 5 destination address is 129.241.67.129.
b) All packets include an IP protocol header.
c) The TCP connections use options.
d) The TCP connections are set-up to send packets in parallel.
e) All application protocols use TCP end-to-end.
f) First hop router cannot be 129.241.67.129.
g) The TCP ACK segments have a TCP header of length 46 bytes.
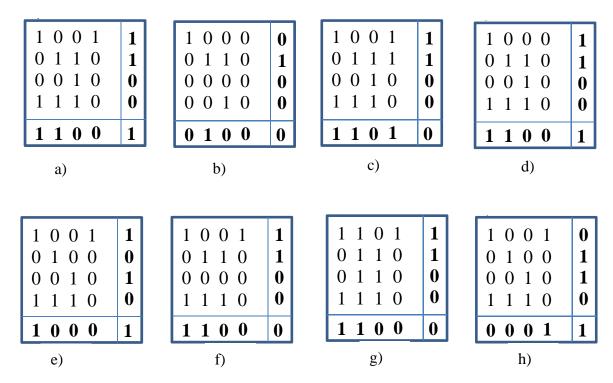h) All packets are forwarded by a router.

1 0 0 1	1
0 1 1 0	1
0 0 1 0	0
1 1 1 0	0
1 1 0 0	**1**

a)

1 0 0 0	0
0 1 1 0	1
0 0 0 0	0
0 0 1 0	0
0 1 0 0	**0**

b)

1 0 0 1	1
0 1 1 1	1
0 0 1 0	0
1 1 1 0	0
1 1 0 1	**0**

c)

1 0 0 0	1
0 1 1 0	1
0 0 1 0	0
1 1 1 0	0
1 1 0 0	**1**

d)

1 0 0 1	1
0 1 0 0	0
0 0 1 0	1
1 1 1 0	0
1 0 0 0	**1**

e)

1 0 0 1	1
0 1 1 0	1
0 0 0 0	0
1 1 1 0	0
1 1 0 0	**0**

f)

1 1 0 1	1
0 1 1 0	1
0 1 1 0	0
1 1 1 0	0
1 1 0 0	**0**

g)

1 0 0 1	0
0 1 0 0	1
0 0 1 0	1
1 1 1 0	0
0 0 0 1	**1**

h)

Figure 2: Potential implementations of the two-dimensional even parity scheme.

1.6
E: Which (if any) of the alternatives in Figure 2 show correct implementation of a two-dimensional **even** parity scheme?

1.7
E: Which (if any) of the following statements are correct related to the Internet Protocol (IP), versions 4 and 6?

E:

a) IPv4 uses 48 bit addresses.
b) IPv6 uses 132 bit addresses.
c) IPv4 does not allow routers inside the network to do any fragmentation of packets.
d) IPv6 does allow routers inside the network to assemble fragments back into packets.
e) IPv6 has no header checksum.
f) IPv4 has no header checksum.
g) IPv6 provides a reliable, connection-oriented transport service.
h) IPv4 provides a reliable, connection-oriented transport service.

1.8
E: Which (if any) of the following definitions related to Quality of Service (QoS) are correct?

E:
a) Propagation delay is the physical delay of sending bits end-to-end over a transmission link.
b) Transmission delay is the physical delay of sending bits end-to-end over a transmission link.
c) Propagation delay is the time needed to put all bits of a packet out on a transmission link, e.g. from a buffer.
d) Queuing delay in a router is influenced by the propagation delay.
e) End-to-end delay is the total time of sending an information unit from a source to a destination in a network.
f) End-to-end delay is the total time of sending an information unit from a source to a destination in a network and back again.
g) Processing delay is the physical delay of sending bits end-to-end over a transmission link.
h) Transmission delay is the time needed for analyzing an information unit (e.g. to find outgoing address) in a router.
i) End-to-end throughput is given by the maximum capacity link used.

1.9
E: Which (if any) of the following statements are true, related to the area of information security?

E:
a) Public key encryption is an example of symmetric key cryptography.
b) Use of a cryptographic hash function and a shared authentication key together is sufficient to achieve message integrity.
c) SSL is used for securing TCP connections.
d) SSL is used for securing IP connections.
e) A message authentication code (MAC) is used to achieve message integrity.
f) Public key encryption is based on using only public keys.
g) Digital signatures can be realized by using a combination of public key encryption and public key certification.
h) The IEEE 802.11 WEP protocol (from 1999) for securing wireless LANs is still regarded as giving a high level of security.

1.10
E: Circuit switching and packet switching have many differences. Which (if any) of the following statements are true?

E:

a) In a circuit switched network, there is little or no delay variation among packets/messages, while in a packet-switched network, delay variation can be large.
b) A circuit-switched network cannot guarantee a certain amount of end-to-end bandwidth for a connection, but a packet-switched network can.
c) Both packet switching and circuit switching use the end system network address in the same way.
d) A circuit switched network does need to use buffers inside a network to handle queues at outgoing network links, while a packet switched network do not.
e) Both circuit switching and packet switching can provide connection-oriented services.
f) Loss of information due to contention at outgoing links is possible in a circuit switched network but not in a packet switched network.
g) Both circuit switching and packet switching can provide connectionless transport services.
h) A circuit switched network can be built on top of a packet switched network.

2. Forsinkelse og gjennomstrømning / Delays and throughput (20 p)(5+5+5+5)

2.1
E: Consider sending a file of 1200K bytes from Host A to Host B over a circuit-switched network. Suppose it takes 100 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 pass through four cross-connect switches and traverse five optical fiber links with lengths 450 km, 450 km, 800 km, 1200 km, and 500 km respectively. On each link the circuit has a transmission rate of 640 Kbit/s. How much time does it minimum take to send the file from Host A to Host B? (Assume a speed of light in fiber of 200 000 000 m/s).

a) 1.992 s
b) 75.017 s
c) 60.117 s
d) 7.617 s
e) 1.975017 s
f) 75.117 s
g) 15.117 s
h) 15.100017 s

2.2
E: Consider sending a file of 1200K bytes from Host A to Host B over a connectionless packet switched network. Assume that the whole file is sent as one large packet, i.e. without any fragmentation. Suppose the end-to-end path passes through four store-and-forward routers, traversing five optical fiber links with lengths 450 km, 450 km, 800 km, 1200 km, and 500 km respectively, and each link has a transmission rate of 640 Kbit/s. What is the minimum time needed to send the file from Host A to Host B? (Assume a speed of light in fiber of 200 000 000 m/s).

a) 1.992 s
b) 75.017 s
c) 60.117 s
d) 7.617 s
e) 1.975017 s
f) 75.117 s
g) 15.117 s
h) 15.100017 s

2.3

E: Consider a broadcast channel with 10 nodes and transmission rate of 100 Mbit/s. The broadcast channel uses polling (with an additional polling node) for multiple access. The polling delay, which is the amount of time from when a node completes transmission until the subsequent node is permitted to transmit, is 1ms. Suppose that within a polling round, a given node is allowed to transmit at most 100K bits. What is the maximum throughput of the broadcast channel?

a) 75 Mbit/s
b) 25 Mbit/s
c) 12.5 Mbit/s
d) 10 Mbit/s
e) 5 Mbit/s
f) 2.5 Mbit/s
g) 1.25 Mbit/s
h) 50 Mbit/s

2.4

E: Consider two hosts that are connected by a channel. The channel has a transmission rate of 100 Mbit/s. The maximum packet size in the network is 10K bytes. Assume the stations are far apart so the propagation delay between the two hosts is 30 ms. Assume that acknowledgements can be issued immediately when the last bit of a packet has been received (i.e. processing delay is ignored) and that the ACK packets are so small that their transmission times can be ignored. What is the maximum data rate that can be achieved by the **stop-and-wait** flow control protocol in this situation?

a) 96.385542 Mbit/s
b) 93.023256 Mbit/s
c) 0.166389 Mbit/s
d) 1.315789 Mbit/s
e) 2.597403 Mbit/s
f) 0.332226 Mbit/s
g) 23.185112 Mbit/s
h) 65.887734 Mbit/s

3. Mix / Miks (20 p)(4+4+4+4+4)

3.1

E: Identify the ciphertext you end up with when using the Caesar cipher with distance 5 to encrypt the text: "What do you say to the God of death? Not today".

a) Hwlz mr ked lke bw pla Okl vw hkweu? Rke bdoex.
b) Alex kr csy wec ok ndr Mkw me bsrdh? Zdr mwsrj.
c) Bmfy it dtz xfd yt ymj Lti tk ijfym? Sty ytifd.
d) Mrfz ke xun wlk cr iks Pts bw khnts? Hty nwzau.
e) Hwlz mr dtz wec xs pla Okl vw klsrd? Rke bslrd.
f) Mrfz kr ned wec ok ymc Wks le mestd? Mus stien.
g) Alex hs csy wec xs xli Ksh sj hiexl? Rsx xshec.
h) Bmfy kr ned zrg lw mrt Lti wg merdt? Hwe vstkd.

3.2

E: Assume that you want to send a confidential and digitally signed contract via a public network. Which combination of information security services and mechanisms are needed to do this securely?

w = Digital Signature
x = Message Authentication Code (MAC)
y = Certification Authority (CA)
z = Encryption

E:
a) w, x, y and z (i.e. all four)
b) only x
c) w, x and z but not y
d) only y
e) w, y and z but not x
f) x and z, not w or y
g) only z
h) none (i.e. none of the four)

3.3

E: Assume that a company needs to partition its allocated IP address range (200.23.96.0/21) into four different parts, to cater to different needs. The main administration (ADM) needs at least 1000 addresses, the sales department (SAL) needs at least 500 addresses, the manufacturing department (MAN) needs at least 200 addresses, and the research and developing department (R&D) needs at least 100 addresses. Which of the following alternatives represent the numbering plan best suited for this situation? (Hint: We want to allocate the minimum needed number of IP addresses to each subnet - to keep a pool of spare addresses for potential later use - and all subnets must be uniquely defined within the allocated address range).

a) ADM: 200.23.96.0/22; SAL: 200.23.104.0/23; MAN: 200.23.108.0/24; R&D: 200.23.110.0/25
b) ADM: 200.23.96.0/22; SAL: 200.23.104.0/23; MAN: 200.23.108.0/24; R&D: 200.23.110.0/24
c) ADM: 200.23.97.0/22; SAL: 200.23.104.0/23; MAN: 200.23.108.0/24; R&D: 200.23.110.0/25
d) ADM: 200.23.97.0/22; SAL: 200.23.104.0/23; MAN: 200.23.108.0/24; R&D: 200.23.110.0/24
e) ADM: 200.23.97.0/22; SAL: 200.23.100.0/23; MAN: 200.23.102.0/24; R&D: 200.23.103.0/25
f) ADM: 200.23.97.0/22; SAL: 200.23.100.0/23; MAN: 200.23.102.0/24; R&D: 200.23.103.0/24
g) ADM: 200.23.96.0/22; SAL: 200.23.100.0/23; MAN: 200.23.102.0/24; R&D: 200.23.103.0/25
h) ADM: 200.23.96.0/22; SAL: 200.23.100.0/23; MAN: 200.23.102.0/24; R&D: 200.23.103.0/24

3.4

E: Which of the following services are provided by the Domain Name System (DNS)?

E:
w = assist in server load distribution
x = translate hostnames to IP addresses
y = allocate an address to a host machine
z = translate alias hostnames into canonical hostnames

a) w, x, y and z (i.e. all four)
b) only x
c) only y

d) x and z, not w or y
e) only z
f) w, x and z but not y
g) y and z, not w or x
h) none (i.e. none of the four services listed)

3.5
E: Which of the following elements is part of the Medium Access Control (MAC) for wireless LANs following the 802.11 standard (including optional parts)?

v = Request to Send / Clear to Send (RTS/CTS)
w = Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
x = Acknowledgement (ACK)
y = Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
z = Distributed Inter-frame Space (DIFS)

E:
a) v, x, y and z, but not w.
b) v, w and z, but not x or y.
c) v, w, x and z but not y.
d) v, x and y, but not w or z.
e) x, y and z, but not v or w.
f) only w.
g) v, x and y, but not w or z.
h) only y.

4. Kortsvar oppgaver / Short answer tasks (20 p)(4+4+4+4+4)

4.1
E: When an application in a host uses TCP to communicate with a server, what is the difference between a ServerSocket and a ConnectionSocket?
Answer: ServerSocket is the (open for all) port you send a request to establish a TCP connection to; ConnectionSocket is then established by the server for a specific TCP connection to be used during a connection.
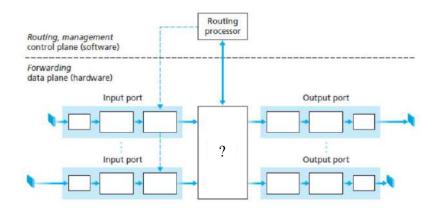

Figure 3: Generic router architecture

4.2

E: A generic router architecture is shown in Figure 3. What is the main function of the box marked with a "?".

Answer: Switching function.

4.3

E: Does a TCP segment contain any address information? Give a short explanation of your answer.

Answer: Yes, it contains the source and destination port numbers.

4.4

E: Compare the loss anticipation schemes Forward Error Correction (FEC) and Interleaving, used for Voice over IP, with regard to overhead and latency.

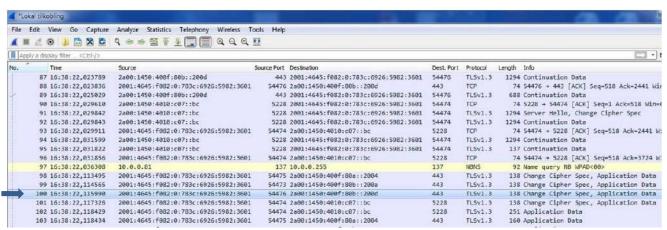Answer: FEC adds overhead; Interleaving adds delay.

Figure 4: Wireshark trace

4.5

E: What type of source and destination addresses are shown in line no. 100 in the Wireshark trace given in Figure 4?

Answer: IP version 6 addresses.