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: 14. aug 2019

Eksamenstid (fra-til): 0900-1300

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

Målform/språk: Engelsk / Bokmål / Nynorsk

Antall sider (uten forside): 6

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. Mix / Diverse (3+3+3+3+3+5 = 20 points)

1.1 E: Make a simple drawing of the five layer Internet protocol stack and explain the term "encapsulation" in this context.

Answer: See e.g. Figure 1.24 in Kurose and Ross (either 6th or 7th edition):

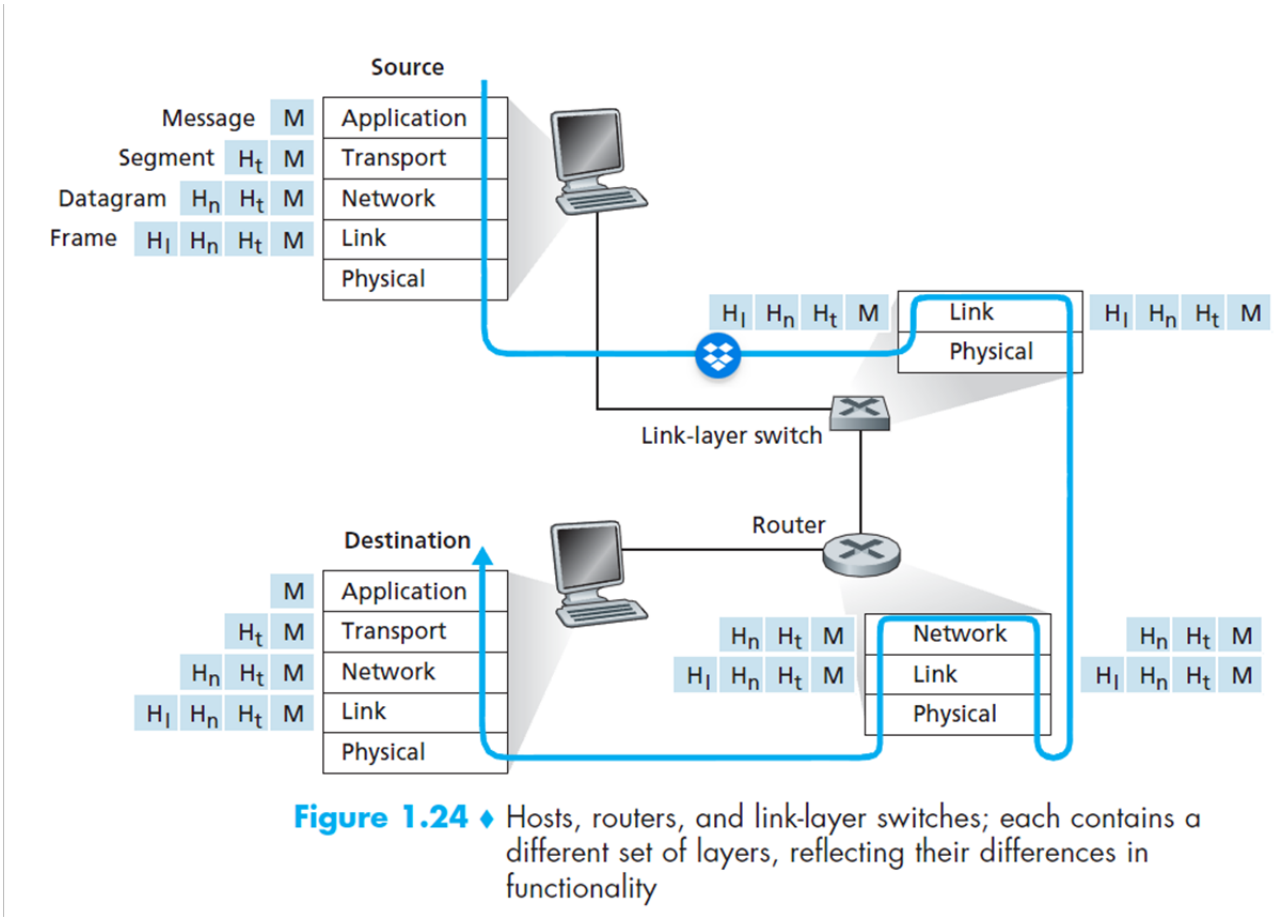


Figure 1.24 ♦ Hosts, routers, and link-layer switches; each contains a different set of layers, reflecting their differences in functionality

A 100% answer does not have to be this detailed: A figure showing the five layers, with an additional explanation of how encapsulation is done, is sufficient.

1.2 E: Given the data 101110 and the generator 1001, find the CRC code (bits) to be added to the data before transmission over a communication link.

Answer:

Following the same set-up as the textbook (ref. Fig. 6.7):

```
          101011 (<- division result; not used for anything)
1001  101110000 (<- zeros added to compute CRC; one less than generator)
      1001
      00101
        000
        1010
        1001
          110
          000
            1100
            1001
```

1010
1001
0011 = CRC

The CRC is sent after the data, instead of the added zeros for the division, i.e. 101110011. This will give remainder zero (000) at receiver as check of successful transmission.

1.3 E: Assume that two-dimensional even parity is used to check for errors in transmission (parity bits are given in row *V* and column *e* in Figure 1). If the data and parity bits received are as shown in Figure 1, are you able to identify which bit(s) are in error? If so, give the position of this/these bit(s) by indicating either a combination of row and column (e.g. (*II*, *d*) or *(III*, *b*)), or the rows and columns where bits in error are detected (e.g. *II* or *c*). Can this/these bit(s) in error be corrected? Explain why or why not.

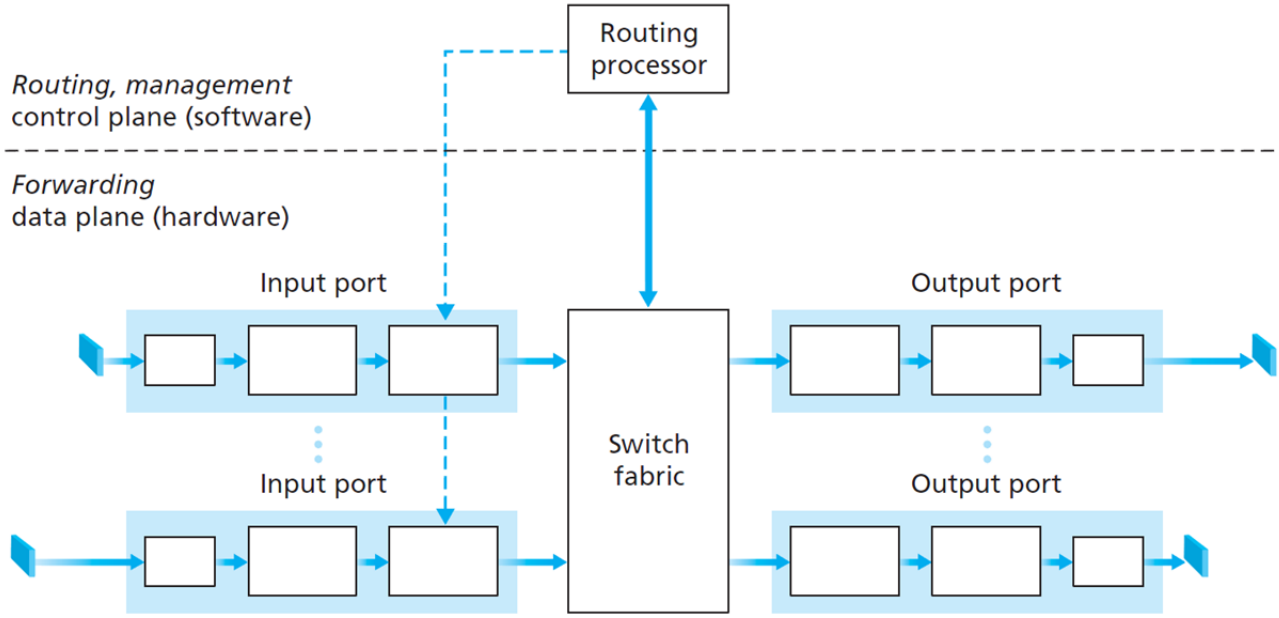
	a	*b*	*c*	*d*	*e*
I	1	0	0	1	0
II	0	1	0	0	0
III	0	1	0	1	0
IV	0	1	0	1	0
V	1	1	0	1	1

Figure 1: Data and parity bits as received / Data og paritetsbit som mottatt

Answer: Row *II* and Column *e* does not contain even numbers of 1 bits. We therefore assume that the parity bit in position (*II*, *e*) is in error. This bit can then be corrected to bit value 1. If more than one row or column did not match our criteria we would have to assume multiple errors, which cannot (in general) be corrected. (Note: We cannot be 100% sure that there are no additional errors that just happen to match our even parity criteria. But assuming a high quality transmission media, e.g. an optical fiber, with very low bit rate probability, our assumption has a high degree of success. If the media used has high bit error rate, e.g. some form of radio transmission, better error detection and correction techniques should be used).

1.4 E: Give at least two different ways that data packets can disappear on their way through a packet switched network.
Answer: (Two of these are sufficient).
1: A packet may be removed in a network element if non-correctable bit errors are detected (to save network resources data packets in error are usually not forwarded).
2: If the load situation in (parts of) the network is very high, buffers may overflow so arriving packets are lost.
3: Different types of failures in the network, e.g. link cuts or failing network elements (switches, routers, repeaters, amplifiers …) can also lead to loss of packets under transport.
4: If using a wireless/radio network or another shared media system (e.g. classical Ethernet): packets may collide and be lost.

1.5 E: Make a sketch of a generic router architecture, including all necessary main parts in both the data plane and the control plane.
Answer: A figure like (from the textbook):



1.6 E: Given a broadcast channel with *N* nodes and transmission rate of *R* bit/s. The broadcast channel uses polling (with an additional polling node) for multiple access. Suppose the polling delay, which is the amount of time from when a node completes transmission until the subsequent node is permitted to transmit, is *d*. Within a polling round, a given node is allowed to transmit at most *Q* bits. What is the maximum throughput of the broadcast channel?
Answer: The maximum number of bits transmitted in a polling round is N * Q [bits]. The length of a (maximum) polling round is N * (d [sec] + Q [bits] / R [bits/sec]). Maximum throughput is then given as maximum number of bits during a (maximum length) round, i.e. N * Q [bits] / (N * (d [sec] + Q [bits] / R [bits/sec])) =
Q [bits] / (d [sec] + Q [bits] / R [bits/sec]) = R [bits/sec] / (1 + d [sec] * R [bits/sec] / Q [bits]). (Or simpler: R/(1 + dR/Q).

2. TCP and UDP / TCP og UDP (3+3+3+3+4+4 = 20 points)

2.1 E: Does a TCP segment contain IP addresses as part of its payload? Explain why or why not.
Answer: No. The payload of a TCP segment is from the Application layer. IP addresses are added in the Network layer, where the TCP segment is the payload.

2.2 E: Is there any difference in how checksums are implemented in TCP and UDP segments? If so, explain.
Answer: No difference. The same type of checksum is implemented for both UDP and TCP segments.

2.3 E: UDP is an unreliable protocol compared to TCP, i.e. being connectionless and with no support for flow- or congestion control. However it also has some advantages for some uses compared to TCP. Give an example of at least one such use or case.
Answer: For real-time applications where you can both accept some (small) errors in transmission (e.g. loss tolerant conversational voice or video) and do not have time to do a retransmission (strict real-time demands), UDP may be a good choice. Some (small) errors may also be corrected or concealed by using forward error correction (FEC) instead of

retransmissions. Advantages of UDP are e.g. no connection set-up delay and less overhead than TCP. Another example is therefore also cases where you just need to send a single (non-critical) message and do not want to set up a connection first, e.g. DNS.

2.4 E: Give a brief overview of how a TCP connection is established.
Answer: TCP uses a three-way handshake procedure for connection establishment. This works as follows (assuming a host connecting to a server):
1. SYN: The host sends Packet 1, which is a SYN (i.e. the SYN bit is set to 1), to the server, which performs the active open. The client sets the segment's sequence number to a random value A.
2. SYN-ACK: In response, the server replies in Packet 2 with a SYN-ACK (i.e. the SYN bit is set to 1). The acknowledgment number is set to one more than the received sequence number (A + 1), and the sequence number that the server chooses for the packet is another random number B.
3. ACK: Finally, the host sends an ACK back to the server in Packet 3 (SYN bit is set to 0). The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgment number is set to one more than the received sequence number i.e. B+1.

2.5 E: What do you (in general) want to achieve by using flow control? What type of flow control is implemented in TCP? (Short answers are sufficient on both questions; no detail of how flow control is implemented in TCP is necessary).
Answer: Flow control is that the receiver controls the data flow sending rate from the sender. The reason of having flow control is that, due to limited processing capacity, limited storage space and/or other reasons, the receiver may not be able to handle the incoming data as they arrive and will lose them, if the sender sends the data too fast. The version of flow control implemented in TCP is based on counting bytes sent to a destination and keeping track of acknowledgements from destination for successfully received bytes. A window of sent, not acknowledged bytes is maintained. Acknowledgements are cumulative.

2.6 E: Give a brief high-level overview of congestion control as implemented in the TCP protocol. (Keywords: three major components, main objectives and functionalities of each component, details of implementation not necessary).
Answer: The three main components of TCP congestion control is “slow start”, “congestion avoidance”, and “fast recovery” (the two first are mandatory for any TCP implementation). Figure 3.51 in the textbook (7th edition; Figure 3.52 in the 6th edition) illustrates the TCP congestion control states. Some implementation variations exist for different versions of TCP. Together these mechanisms adds up to an “additive-increase, multiplicative-decrease” (AIMD) form of congestion control, with a typical saw tooth behavior.

3. Multimedia (4+4+4+4+4 = 20 points)

3.1 E: To provide optimal streaming media delivery to customers, service providers (e.g. Netflix) needs to maximize its control over the three basic components in the delivery chain: video player, video server, and network in-between. Describe which network parameters affect the users' experience of streaming quality, and briefly what service providers (e.g. Netflix) does to ensure the best possible user experience.
Answer: Video streaming is particularly sensitive to packet delay and loss, misordered arrival of packets, and unpredictable (jittery) round-trip times inherent to TCP/IP. Minimizing the network distance reduces the potential exposure to these anomalies:

Caching through Content Distribution Networks (CDNs).

3.2 E: Why and with what parameter does Netflix check your geolocation?
Answer: Licenses for content is paid for by geographical region. IP address is used to approximate location.

3.3 E: Explain how an "unblock Netflix" service works; illustrate with a protocol stack drawing.
Answer: To get a valid IP address in the area with the wanted content, a VPN service can be used. Illustration showing that communication must go via a third party (the VPN service) towards the destination. The VPN service will access the content with a valid IP address and then forward it to you.

3.4 E: Some schemes exist to recover from packet loss when realizing real-time conversational voice over the internet (Voice-over-IP). Two variants of FEC are amongst these. Give brief explanations of both methods based on this principle.
Answer: The two methods described in the curriculum for this use case are:
1: Send an additional packet of data after each n packets, constructed by XOR-ing the n original packets. If one of the n+1 packets are lost, it may then be fully reconstructed at the receiver.
2: Send a lower resolution (low bitrate) audio stream as the redundant information. This may e.g. be done by appending the (n-1) lower quality packet at the end of the full quality n packet in a stream. If a packet is lost the lower quality part of the next packet can then be used instead. This does not recreate the lost information, but normally conceals it well.

3.5 E: When using the public Internet for interactive voice communication, what are the main challenges to achieve good quality?
Answer: In this case it is limited how long you can buffer information to cancel out variation in delay through the network. Too large a value becomes noticeable as a delay in response from the other end of the interactive communication. On the other hand, some loss of information is usually acceptable and may not even be noticeable for speech. If enough processing power is available on both sides, forward error correction (FEC) could also be used to handle information loss. (But since this is real-time, processing demands may be prohibitive for legacy equipment). There is also a trade-off between the extra bandwidth needed for FEC and increased loss or delay that may be introduced in the network because of it.

4. Information security / Informasjonssikkerhet (4+4+4+4+4 = 20 points)

4.1 E: What is a digital certificate and how is the validity of digital certificates validated?
Answer: Digital certificate verifies the validity of public keys. The Certification Authority (CA) signs the digital certificate with its own secret key to confirm the validity.

4.2 E: How can a client check that a received public key is correct?
Answer: The digital certificate (containing the public key) must be signed by a Certification Authority (CA) you trust and know the public key for.

4.3 E: Describe how a message M is encrypted and sent from A and to B, which then decrypts the message. Asymmetric encryption is used with A's key pair.
Answer: A encrypts M with private key A and sends the encrypted M to B. B receives and decrypts the encrypted M with public key A.

4.4 E: If a company with offices in multiple geographical locations around the world wants to create a Virtual Private Network (VPN) over the existing public Internet, what is the security protocol involved?
Answer: Ipsec.

4.5 E: Three categories of firewalls are given in the curriculum: “Traditional packet filters”, “Stateful packet filters”, and “Application gateways”. Give short explanations of the functionality of each of these, with special attention to the differences between them.
Answer:
Traditional packet filters: A filter put at all router input(s) to an organizations internal network based on a security (filtering) policy. Normally this is based on a combination of addresses and port numbers, and may be different for incoming and outgoing packets. Other information could also be used, e.g. TCP ACK bit set or not in a TCP segment. Decisions are based on information in each packet in isolation. An access control list is implemented based on the rules.
Stateful packet filters: Unlike traditional packet filters this also tracks *connections* to make the filtering more efficient and secure. It uses a connection table in addition to an extended version of the access control list.
Application gateways: An application specific server through which all incoming and outgoing application data must pass. These base decisions on application data in addition to the filters above. Such a server may e.g. prompt a user trying to connect to provide a username and password before access is given. Application gateways are specific for each application, so many of them may be needed in an organization. They may be run on the same host(s) though.

5. Wireshark (4+4+4+4+4 = 20 points)

No.	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000	192.168.10.135	80.232.110.250		78	49279 > https(443) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=924892603
2	0.006918	80.232.110.250	192.168.10.135		74	https(443) > 49279 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK
3	0.006952	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=924892608 TSecr=171
4	0.007724	192.168.10.135	80.232.110.250		292	Client Hello
5	0.018918	80.232.110.250	192.168.10.135		1514	https(443) > 49279 [ACK] Seq=1 Ack=227 Win=66560 Len=1448 TSval=171904247 TSec
6	0.018919	80.232.110.250	192.168.10.135		1514	https(443) > 49279 [ACK] Seq=1449 Ack=227 Win=66560 Len=1448 TSval=171904247 T
7	0.018921	80.232.110.250	192.168.10.135		1514	https(443) > 49279 [ACK] Seq=2897 Ack=227 Win=66560 Len=1448 TSval=171904247 T
8	0.018922	80.232.110.250	192.168.10.135		1288	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
9	0.018960	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=227 Ack=2897 Win=128864 Len=0 TSval=924892619 TSe
10	0.018962	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=227 Ack=5567 Win=126176 Len=0 TSval=924892619 TSe
11	0.019000	192.168.10.135	80.232.110.250		66	[TCP Window Update] 49279 > https(443) [ACK] Seq=227 Ack=5567 Win=131072 Len=0
12	0.547766	192.168.10.135	80.232.110.250		141	Client Key Exchange
13	0.547770	192.168.10.135	80.232.110.250		72	Change Cipher Spec
14	0.547771	192.168.10.135	80.232.110.250		167	Encrypted Handshake Message
15	0.557383	80.232.110.250	192.168.10.135		66	https(443) > 49279 [ACK] Seq=5567 Ack=409 Win=66304 Len=0 TSval=171904301 TSec
16	0.559636	80.232.110.250	192.168.10.135		173	Change Cipher Spec, Encrypted Handshake Message
17	0.559687	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=409 Ack=5674 Win=130944 Len=0 TSval=924893125 TSe
18	0.659774	192.168.10.135	80.232.110.250		615	Application Data
19	0.674109	80.232.110.250	192.168.10.135		967	Application Data
20	0.674138	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=958 Ack=6575 Win=130144 Len=0 TSval=924893230 TSe
21	13.888212	192.168.10.135	80.232.110.250		66	49279 > https(443) [FIN, ACK] Seq=958 Ack=6575 Win=131072 Len=0 TSval=924906288
22	13.894695	80.232.110.250	192.168.10.135		66	https(443) > 49279 [FIN, ACK] Seq=6575 Ack=959 Win=65792 Len=0 TSval=171905635
23	13.894745	192.168.10.135	80.232.110.250		66	49279 > https(443) [ACK] Seq=959 Ack=6576 Win=131072 Len=0 TSval=924906293 TSe

? (5.1)

Figure 2: Data from Wireshark

5.1 E: Enter the correct protocol in the protocol column for each package.
Answer: Most are TCP, except for TLS/SSL in packets 4, 8, 12-14, 16, and 18-19.

5.2 E: What does the packet sequence represent?
Answer: A TCP connection is set up, followed by establishment of a TSL/SSL session with encrypted data transmission. After this the connection is terminated.

5.3 E: Package No 4 / Client hello includes a random field, Random, with a random number (nonce = number used once). What two functions does this protocol field have?

```
▼ Random: 58924d8397635cfb164d7363a8e8b3c3983eca45e6f2af99...
    GMT Unix Time: Feb  1, 2017 22:05:07.000000000 CET
    Random Bytes: 97635cfb164d7363a8e8b3c3983eca45e6f2af9997762815...
```

Answer: Provide input for computing the Master Secret (MS) used in key generation. Nonce also protects against "connection replay" attacks.

5.4 E: How is the algorithm to be used to encrypt user data decided?
Answer: The client states which algorithms it supports in the "Client Hello" message. The Server chooses which one to use and returns the choice in the "Server Hello" message.

5.5 E: Which packages contain user data that is encrypted?
Answer: Packets 18 and 19.