NTNU
Det skapende universitet

Institutt for telematikk

Eksamensoppgave/oppgåve i

TTM4100 KOMMUNIKASJON – TJENESTER OG NETT

SOLUTION

Faglig/fagleg kontakt under eksamen: Norvald Stol

Tlf.: 970 800 77

Eksamensdato: 11. aug 2017

Eksamenstid (fra-til): 0900-1300

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

Tillatne hjelpemiddel: D (Ingen prenta eller handskrivne hjelpemiddel tillatne. Bestemt, enkel kalkulator tillaten)

Målform/språk: Engelsk / Bokmål / Nynorsk

Antall sider: 9 (inkludert denne forsiden)

Antall sider vedlegg: 0

Kontrollert av:

_____

Dato Sign

1. General tasks / Generelle oppgaver (3+3+3+3+4+4 = 20 points)

1.1 E: Explain briefly protocol layering as defined and applied for the Internet. (Keywords: terminology, services, encapsulation, number and name of layers).

B: Gi en kort forklaring på protokoll lag modellen slik den er definert og brukt for Internet. (Stikkord: terminologi, tjenester, innkapsling («encapsulation»), antall og navn brukt på lagene).

N: Gje ei kort forklaring på protokoll lag modellen slik han er definert og brukt for Internet. (Stikkord: terminologi, tenester, innkapsling («encapsulation»), mengd og namn brukt på lagene).

Done to provide structure to the design of network protocols. Each protocol is said to belong to a given layer and is based on using services from the layer(s) below it in the protocol stack. From top to bottom the layers are (data unit name in parenthesis): Application (message), Transport (segment), Network (datagram), Link (frame), and Physical ("transported bits"). Encapsulation: A new header is added to a data unit when it moves downwards in the protocol stack, or removed when it moves upwards. (See also 1.2 below).

1.2 E: Give an example of encapsulation as used in the Internet layered model above (in 1.1) when sending an application message from a user to a server through the Internet. Use sketches to show the encapsulation process and what is present at different points in a network.

B: Gi et eksempel på innkapsling ("encapsulation") slik det brukes i den lagdelte modellen for Internet ovenfor (i 1.1) når en applikasjonsmelding sendes fra en bruker til en tjener gjennom Internet. Bruk skisser til å vise hvordan innkapslingen gjøres og hva som er til stede på ulike steder i et nett.

N: Gje eit døme på innkapsling ("encapsulation") slik det vert brukt i den lagdelte modellen for Internet ovanfor (i 1.1) når ei applikasjonsmelding vert sendt frå ein bruker til ein tenar gjennom Internet. Bruk skisser til å visa korleis innkapslingen vert gjort og kva som er til stades på ulike stadar i eit nett.

*As an example: A link layer frame will consist of a **link layer header** and a **datagram** (from the network layer) as «payload». A datagram consists of a **network layer header** and a **segment** (from the transport layer) as payload, etc. See e.g. Figure 1.24 in Kurose and Ross (either 6th and 7th edition of the book). The figure also shows that inside the network (not end-systems) we have to go up to either the link layer (to switch a frame) or the network layer (to route a segment), but the Transport or Application layers are present only in end-systems.*

1.3 E: How is variation in delay (or "jitter") usually handled when streaming video over the public Internet?

B: Hvordan håndteres vanligvis variasjon i forsinkelse ("jitter") når video streames over det offentlige Internettet?

N: Korleis vert variasjon i forseinking ("jitter") vanlegvis handtert når video streames over det offentlege Internettet?

Client-side buffering is used to handle jitter.

1.4 E: Explain briefly the difference between "Access networks" and "The network core" (or "Core network" or "Transport network"). (Keywords: relative to users, protocol layers present, examples of typical technologies used).

B: Forklar kort forskjellene mellom aksessnett og transportnett ("Transport network", "core network", eller "The network core"), (Stikkord: relativt til brukerne, protokoll-lag til stede, eksempler på teknologier som typisk brukes).

N: Forklar kort skilnadene mellom aksessnett og transportnett ("Transport network", "core network", eller "The network core"), (Stikkord: relativt til brukarane, protokoll-lag til stades, døme på teknologiar som typisk vert brukte).

Access networks are the closest to users. Transport networks exist to connect different (and different types of) access networks together, i.e. allowing communication over larger distances and between different types of technologies. Transport networks will implement the three lowest layers, i.e. Physical, Link and Network layers. If end-systems are regarded as part of the Access networks they will have to implement the full protocol stack; but not everywhere – also communication inside an access network may use switches (and sometimes even routers). Examples of technologies: Digital Subscriber Line (DSL), Cable, Fiber to the Home (FTTH) or Wireless (Satellite, WiFi, etc.) for access from home; Ethernet or WiFi for access from Enterprises. For the network core: large packet switches (routers or link layer switches) connected with optical fibers, or Circuit switches (e.g. large Optical Cross connects (OXC)) and fiber links.

1.5 E: Consider sending a file of 100K 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 passes through 3 links, and on each link the circuit has a transmission rate of 64 Kbps. At least how much time does it take to send the file from Host A to Host B?

B: En datafil på 100K Bytes skal sendes fra Vert A til Vert B over et linjesvitsjet nett. Anta at det tar 100 ms for å etablere en ende-til-ende forbindelse mellom Vert A og Vert B før Vert A kan starte å sende. Anta videre at denne forbindelsen er etablert gjennom tre linker (dvs. to svitsjepunkter) som hver har en transmisjonsrate på 64 Kbps. Hvor lang tid vil det minimum ta å overføre denne filen fra Vert A til Vert B?

N: Ei datafil på 100K Bytes skal sendast frå Vert A til Vert B over eit linjesvitsjet nett. Anta at det tek 100 ms for å etablera eit ende-til-ende samband mellom Vert A og Vert B før Vert A kan starta å senda. Anta vidare at dette sambandet er etablert gjennom tre linkar (dvs. to svitsjepunkter) som kvar har ei transmisjonsrate på 64 Kbps. Kor lang tid vil det minimum ta å overføra denne fila frå Vert A til Vert B?

The transmission time or delay is simply 100K x 8bits /64Kbps = 12.5 s, no matter how many links the circuit crosses. Additionally, it has to be waited for 100 ms until the circuit is

established. So, at least it takes 100 ms + 12.5 s = 12.6 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).

1.6 E: Consider sending a file of 100K 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 2 store-and-forward routers (i.e. traversing 3 links), and each link has a transmission rate of 64 Kbps. At least how much time does it take to send the file from Host A to Host B?

B: En datafil på 100K Bytes skal sendes fra Vert A til Vert B over et forbindelsesløst pakkesvitsjet nett. Anta at hele filen sendes som en stor pakke, dvs. uten fragmentering. Anta videre at ende-til-ende stien pakken følger går gjennom to «store-and-forward» rutere (dvs. over tre linker), og hver link har en transmisjonsrate på 64 Kbps. Hvor lang tid vil det minimum ta å overføre denne filen fra Vert A til Vert B?

N: Ei datafil på 100K Bytes skal sendast frå Vert A til Vert B over eit sambandslaust pakkesvitsjet nett. Anta at heile fila vert sendt som ein stor pakke, dvs. utan fragmentering. Anta vidare at ende-til-ende stigen pakken følgjer går gjennom to «store-and-forward» ruterar (dvs. over tre linkar), og kvar link har ei transmisjonsrate på 64 Kbps. Kor lang tid vil det minimum ta å overføra denne fila frå Vert A til Vert B?

Each store-and-forward router must receive the full packet before it can be sent out on the next link, thus the delay is now: 3 x 100K x 8 bits / 64 Kbps = 3 x 12.5 s = 37.5 seconds. There is no set-up delay to be added.

2. Transport layer / Transportlag (3+3+3+3+2+3+3 = 20 points)

2.1 E: What is the difference between “flow control” and “congestion control” in a network?

B: Hva er forskjellen på flytkontroll («flow control») og overlastkontroll («congestion control») i et nett?

N: Kva er skilnaden på flytkontroll («flow control») og overlastkontroll («congestion control») i eit nett?

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.
Congestion control is needed to prevent the network itself from being overloaded, i.e. buffers overflowing due to links not being able to handle the amount of offered traffic.

2.2 E: Give a brief overview of flow control as implemented in the TCP protocol. (Keywords: variables, resources and actions at sender and receiver sides).

B: Gi en kort oversikt over flytkontroll ("flow control") slik det er implementert i TCP protokollen. (Stikkord: variabler, ressurser og aksjoner på sender og mottakersidene).

N: Gje eit kort oversyn over flytkontroll ("flow control") slik det er implementert i TCP protokollen. (Stikkord: variablar, ressursar og aksjonar på sendar og mottakarsidene).

The sender maintain a variable called the receive window, reflecting how much free space is available at the receiver side. Successfully transmitted segments are acknowledged from the receiver to the sender (or rather the number of bytes they contain), so the sender can adjust the receive window. The sender has to stop transmitting if the receive window become too small to accept any further segments from the sender, until more acknowledgements are received. (In addition to this timeouts are used at the sender side to decide when to retransmit segments that are not acknowledged within an acceptable timeframe. This is however more related to congestion control below, since losing segments is often an indication of network congestion).

2.3 E: How is flow control for the UDP protocol different from the one above (for TCP)?

B: På hvilken måte er flytkontroll ("flow control") for UDP protokollen forskjellig fra den over (for TCP)?

N: På kva for ein måte er flytkontroll ("flow control") for UDP protokollen ulikt frå den over (for TCP)?

UDP has no defined flow control.

2.4 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).

B: Gi en kort høy-nivå oversikt over overlastkontroll ("congestion control") slik det er implementert i TCP protokollen. (Stikkord: tre hoveddeler, hovedhensikt og funksjonalitet for hver del; detaljer om implementering er ikke nødvendig å ta med).

N: Gje eit kort høg-nivå oversyn over overlastkontroll ("congestion control") slik det er implementert i TCP protokollen. (Stikkord: tre hovuddelar, hovudføremål og funksjonalitet for kvar del; detaljar om implementering er ikkje naudsynt å ta med).

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.

2.5 E: How is congestion control for the UDP protocol different from the one above (for TCP)?

B: På hvilken måte er overlastkontroll ("congestion control") for UDP protokollen forskjellig fra den over (for TCP)?

N: På kva for ein måte er overlastkontroll ("congestion control") for UDP protokollen ulikt frå den over (for TCP)?

UDP has no defined congestion control.

2.6 E: Host A and Host B are communicating over a TCP connection, and Host B has already received from A all data up through byte 350. Suppose Host A then sends two data segments to Host B back-to-back. The first and the second segments contain 28 and 78 bytes of data, respectively. In the first segment, the sequence number is 351, the source port number is 502, and the destination port number is 80. Host B sends an acknowledgement whenever it receives a segment from Host A. In the second segment sent from Host A to Host B, what are the sequence number, source port number, and destination port number?

B: Vert A og Vert B kommuniserer over en TCP forbindelse, og Vert B har allerede mottatt fra A alle data opp til og med byte 350. Anta at Vert A deretter sender to segmenter med data til Vert B uten opphold mellom dem («back-to-back»). Første og andre segment inneholder henholdsvis 28 og 78 bytes med data. I det første segmentet er sekvensnummeret 351, kildeportnummeret er 502, og destinasjonsportnummeret er 80. Vert B sender alltid en kvittering når den mottar et segment fra Vert A. Hva er sekvensnummeret, kildeportnummeret og destinasjonsportnummeret i det andre segmentet som sendes fra Vert A til Vert B?

N: Vert A og Vert B kommuniserer over eit TCP samband, og Vert B har allereie motteke frå A alle data opp til og med byte 350. Anta at Vert A deretter sender to segment med data til Vert B utan opphald mellom dei («back-to-back»). Første og andre segment inneheld høvesvis 28 og 78 bytes med data. I det første segmentet er sekvensnummeret 351, kjeldeportnummeret er 502, og destinasjonsportnummeret er 80. Vert B sender alltid ei kvittering når han mottek eit segment frå Vert A. Kva er sekvensnummeret, kjeldeportnummeret og destinasjonsportnummeret i det andre segmentet som vert sendt frå Vert A til Vert B?

In the second segment from Host A to B:
Sequence number: 351 + 28 = 379
Source port number: 502
Destination port number: 80

2.7 E: For the situation described in 2.6 above: If the second segment sent arrives before the first segment sent, in the acknowledgement of the first arriving segment, what is the acknowledgement number?

B: For same situasjon som beskrevet i 2.6 over: Hvis det andre segmentet sendt ankommer til Vert B før det første segmentet sendt, hva er kvitteringsnummeret i kvitteringen for det segmentet som mottas først?

N: For same situasjon som skildra i 2.6 over: Viss det andre segmentet sendt kjem fram til Vert B før det første segmentet, kva er kvitteringsnummeret i kvitteringen for det segmentet som vert først motteke?

If the second segment arrives before the first segment, in the acknowledgement of the first arriving segment, the acknowledgement number is 351, indicating that it is still waiting for bytes 351 and onward.

3. Network layer / Nettverkslag (5+5+5+5 = 20 points)

3.1 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).

N: Gje eit kort oversyn over nettverksslaget. (Stikkord: hovudoppgåver/funksjonar, protokoll(ar) brukt, kor i nettet det er til stades).

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.

3.2 E: What is head-of-line (HOL) blocking?

B: Hva er "head-of-line" (HOL) sperr?

N: Kva er "head-of-line" (HOL) sperr?

HOL denotes that an information unit in a FIFO queue (buffer) may be hindered in reaching its free output port, if another information unit in front of it have to wait for another (not free) output port. This is typically a problem when implementing (shared) input queueing in switches or routers, instead of having dedicated output queues for each output port.

3.3 E: Assume the (CIDR) IPv4 address 223.1.2.0/xx. If we need around 400 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 223.1.2.0/xx. Hvis vi trenger omtrent 400 IP addresser tilgjengelige for verter og ruterinterface i nettet vårt, hva er den maksimale verdien vi kan bruke for xx?

N: Anta (CIDR) IPv4 adressa 223.1 .2.0/xx. Viss vi treng omtrent 400 IP addresser tilgjengelege for vertar og ruterinterface i nettet vårt, kva er den maksimale verdien vi kan bruka for xx?

xx = 23 som gir 512 adresser (xx=24 ville gi kun 256 adresser, som er for lite)

3.4 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.

N: Anta at ein ruter i nettet har (CIDR) innslag i rutingstabellen som vist nedanfor. For kvar

av følgjande destinasjons IP addresser, angje kva for eit 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

3.4.1: 135.46.192.128
3.4.2: 135.46.131.20
3.4.3: 135.46.190.30
3.4.4: 135.46.191.7
3.4.5: 135.46.75.35

3.4.1 : til Interface 3
3.4.2: til Interface 0
3.4.3: til Interface 1
3.4.4: til Interface 1
3.4.5: til Interface 3

4. Link layer and security / Linklag og sikkerhet (3+3+4+3+3+4 = 20 points)

4.1 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/funksjoner, protokoll(er) brukt, hvor i nettet det er til stede).

N: Gje eit kort oversyn over linklaget. (Stikkord: hovudoppgåver/funksjonar, protokoll(ar) brukte, kor i nettet det er til stades).

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.

4.2 E: Complete the two-dimensional even parity matrix shown in Figure 1. Give answer left to right for xxxx and from top down for yyyy, and z as a 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 en enkeltverdi.

N: Fullfør den to-dimensjonale lik («even») paritetsmatrisen vist i Figur 1. Gje svaret frå venstre til høgre for xxxx, frå topp til botn for yyyy, og z som ein enkeltverdi.

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

Figure 1 Two-dimensional even parity

xxxx = 0011
yyyy = 1111
z = 0

4.3 E: Find the Cyclic Redundancy Check (CRC) code for the data bit pattern 101110 using the generator 1001.

B: Finn "Cyclic Redundancy Check" (CRC) koden for datastrengen 101110 når generatoren 1001 brukes.

N: Finn "Cyclic Redundancy Check" (CRC) koden for datastrengen 101110 når generatoren 1001 vert brukt.

This example is taken from the textbook (fig. 6.7 in 7th edition; fig. 5.7 in the 6th edition). The CRC is equal to the remainder of the division, i.e. 011 in this case. This is added to the data when sent.

4.4 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).

N: Forklar kort hovudskilnadene på symmetrisk nøkkel kryptering ("Symmetric Key Cryptography") og offentleg nøkkel kryptering ("Public Key Encryption"). (Stikkord: løynleg eller kjend algoritme, løynleg(e) eller kjend(e) nøkkel/nøklar, døme på kva brukast 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.

4.5 E: Explain briefly how one of the methods above (in 4.4) in principle can be used directly to establish a "digital signature" (but not necessarily in an efficient manner for large messages). What is needed (as a minimum) in addition for this to work at all in principle?

B: Forklar kort hvordan en av metodene over (i 4.4) prinsipielt kan brukes direkte for å lage en digital signatur (men ikke nødvendigvis en effektiv løsning for store meldinger). Hva trengs (som minimum) i tillegg for at dette overhode skal virke som prinsipp?

N: Forklar kort korleis ein av metodane over (i 4.4) prinsipielt kan brukast direkte for å laga ein digital signatur (men ikkje naudsynlegvis ei effektiv løysing for store meldingar). Kva trengst (som minimum) i tillegg for at dette overhovudet skal verka som prinsipp?

The simplest possible way to do this is to use a private key (of a public key crypto system) to encrypt a message or statement. By using the public key corresponding to this private key anyone may then confirm validity. However, you have to know for certain that the public key actually belong to the person you are validating, thus a trusted third party, issuing a certificate, is also necessary.

4.6 E: What is the purpose of the Secure Socket Layer» (SSL)?

B: Hva er hensikten med «Secure Socket Layer» (SSL)?

N: Kva er føremålet med «Secure Socket Layer» (SSL)?

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

5. Wireless and Multimedia / Trådløs og multimedia (4+4+4+4+4 = 20 points)

5.1 E: Make sketches and explain briefly the difference between an "infrastructure" and an "ad hoc" wireless LAN as defined by the 802.11 specifications.

B: Lag skisser og forklar kort forskjellen på et infrastruktur ("infrastructure") og et «ad hoc» trådløst lokalnett (LAN) som definert av 802.11 spesifikasjonene.

N: Lag skisser og forklar kort skilnaden på ein infrastruktur ("infrastructure") og eit «ad hoc» trådlaust lokalnett (LAN) som definert av 802.11 spesifikasjonane.

While in infrastructure mode hosts are associated with (/connected to) a base station, the wireless hosts in ad hoc mode have no infrastructure with which to connect, but may communicate (mostly directly) with each other. In the absence of an infrastructure, the hosts themselves must provide for services such as routing, address assignment, DNS-like name translation, and more. Figure 7.7 and 7.8 in the textbook (7th edition; Fig. 6.7 and 6.8 in 6th edition) shows these two principles.

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).

N: Kva for ein "random access" metode vert brukt i 802.11 MAC protokollen? Gje ein kort høynivå skildring av korleis han verkar. (Stikkord: korleis stasjonar aksesserer mediet, korleis kollisjonar detekteres eller handterast).

"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: What are the main differences between 3G and 4G mobile cellular systems?

B: Hva er hovedforskjellene på 3G og 4G mobile cellulære systemer?

N: Kva er hovudskilnadene på 3G og 4G mobile cellulære system?

*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).*

5.4 E: When streaming stored video over the public Internet, what is the main challenge for getting good quality at the receiving end (assuming enough capacity is available end-to-end to handle the mean transmission rate needed)?

B: Når en streamer lagret video over det offentlige Internettet, hva er hovedutfordringen for å oppnå god kvalitet hos mottaker (hvis vi antar at nok kapasitet er tilgjengelig ende-til-ende for å håndtere den nødvendige midlere transmisjonsraten)?

N: Når ein streamer lagra video over det offentlege Internettet, kva er hovudutfordringa for å oppnå god kvalitet hos mottakar (viss vi antek at nok kapasitet er tilgjengeleg ende-til-ende for å handtera den naudsynte midlare transmisjonsraten)?

The main challenge is to handle variation in delay (jitter). Since streaming is one-way, long distance/delay or even some packet loss is acceptable since the fixed delay (by buffering) at the receiver can be increased without noticeable quality loss for the user, assuming enough buffer space is available.

5.5 E: When using the public Internet for interactive voice communication, what are the main challenges to achieve good quality?

B: Når en bruker det offentlige Internettet for interaktiv talekommunikasjon, hva er hovedutfordringene for å oppnå god kvalitet?

N: Når ein brukar det offentlege Internettet for interaktiv talekommunikasjon, kva er hovudutfordringane for å oppnå god kvalitet?

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.