NTNU
Det skapende universitet

Institutt for telematikk

SOLUTION

Eksamensoppgave i

TTM4100 KOMMUNIKASJON – TJENESTER OG NETT

Faglig kontakt under eksamen: Alvaro Fernandez

Tlf.: 451 70 987

Eksamensdato: 10 aug 2016

Eksamenstid (fra-til): 1500-1900

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

Målform/språk: Engelsk / Bokmål /Nynorsk

Antall sider: 12

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. Miscellaneous (20 points)

1.1 E: Explain briefly connection-oriented service and connectionless service. Can a service be both connection-oriented and connectionless?

B: Forklar kort forbindelsesorienterte tjenester og forbindelsesløse tjenester. Kan en tjeneste være både forbindelses-orientert og forbindelsesløs?

N: Forklar kort forbindelsesorienterte tenester og forbindelseslause tenester. Kan ei teneste vera både forbindelsesorientert og forbindelseslaus?

In connection-oriented service, a connection is set up before information data transfer. All information data are transmitted along the same connection path to reach the destination. After the transmission, the connection is released.

In connectionless service, no connection is set up before the information data are transmitted. In addition, data are transferred as units, each with an address. Each unit is routed independently to the destination.

A service can NOT be both connection-oriented and connectionless.

1.2 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.

N: Forklar linjesvitsjing og pakkesvitsjing og nemn minst tre skilnader mellom dei.

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 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 employs statistical multiplexing and hence can make better 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 nothing being sent on the connection.

1.3 E: Consider sending a file of 800K bytes from Host A to Host B over a circuit-switched network. Suppose it takes 300 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 64 Kbps. At least how much time does it take to send the file from Host A to Host B?

B: En datafil på 800K bytes sendes fra Host A til Host B over et linjesvitsjet nett. Sett at det tar 300 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 64Kbps. Hvor lang tid vil det minst ta å sende datafilen fra Host A til Host B?

N: Ei datafil på 800K bytes vert sendt frå Host A til Host B over eit linjesvitsja nett. Sett at det tar 300 ms å oppretta eit ende-til-ende samband mellom Host A og Host B før Host A kan begynne å sende datafila. Anta vidare at ende-til-ende sambandet passerer igjennom fem lenkar, og at kvar lenke har ei transmisjonsrate på 64Kbps. Kor lang tid vil det minst ta å senda datafila fra Host A til Host B?

The transmission time or delay is simply 800K x 8bits /64Kbps = 100 s, no matter how many links the circuit crosses. Additionally, it has to be waited for 300 ms until the circuit is established. So, at least it takes 300 ms + 100 s = 100.3 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).

1.4 E: Consider a broadcast channel with 5 nodes and transmission rate of 10 Mbps. 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 1 ms. Suppose that within a polling round, a given node is allowed to transmit at most 10K bits. What is the maximum throughput of the broadcast channel?

B: Ta utgangspunkt i en kringkastingskanal (broadcast channel) med 5 noder og en transmisjonsrate på 10 Mbps. Kringkastingskanalen bruker ’polling’ (med en ekstra ’polling node’) for multippel aksess. Polling-forsinkelsen, som er tiden det tar fra en node fullfører sin transmisjon til den neste noden får lov til å starte sin transmisjon, er 1 ms. Anta at hver node har lov til å sende opptil 10K bit innenfor en ’polling-runde’. Hva er da den maksimale gjennomstrømningen (throughput) for kringkastingskanalen?

N: Ta utgangspunkt i ein kringkastingskanal (broadcast channel) med 5 nodar og ein transmisjonsrate på 10 Mbps. Kringkastingskanalen nyttar ’polling’ (med ein ekstra ’polling node’) for multippel aksess. Polling-forseinkinga, som er tida det tar frå ei node fullfører sin transmisjon til den neste noden får lov til å starte sin transmisjon, er 1 ms. Anta at kvar node har lov til å sende opptil 10K bit innafor ein ’polling-runde’. Kva er da den maksimale gjennomstrauminga (throughput) for kringkastingskanalen?

*In each round, each node can at most transmit 10Kb, so the total is 50Kb. Each round takes time of: 5 * (1 ms + 10Kb/10Mbps) = 10 ms. So, the maximum throughput is 50Kb/10ms = 5 Mbps.*

1.5 E: Consider two hosts that are connected by a channel. The channel has a transmission rate of 100 Mbps. The maximum packet size in the network is 5K bytes. Assume the propagation delay between the two hosts is 300 ms. What is the maximum data rate that can be achieved by the **stop-and-wait** flow control?

B: Gitt to verter (hosts) som er sammenkoblet av en kanal. Kanalen har en transmisjonsrate på 100 Mbps. Den maksimale pakkestørrelsen i nettet er 5K bytes. Anta at propagasjonsforsinkelsen mellom de to vertene (hosts) er på 300ms. Hva er den maksimale datarate som kan oppnås når ”**stop-and-wait**” flytkontroll brukes?

N: Gitt to vertar (hosts) som er sammenkobla av ein kanal. Kanalen har ei transmisjonsrate på 100 Mbps. Den maksimale pakkestørrelsen i nettet er 5K bytes. Anta at propagasjonsforseinkinga mellom dei to vertane (hosts) er på 300ms. Kva er den maksimale datarate som kan nåast når ein nyttar ”**stop-and-wait**” flytkontroll?

Using the formula below (taken from and explained in the curriculum), the maximum datarate can be calculated as follows, where U denotes the maximum channel utilization; X packet size; C the channel capacity; and τ the one way propagation delay.

$U = (X/C)/[(X/C)+2\tau]$

Maximum ***datarate*** *is then given as (U*C) = 5KB/[(5KB/100Mbps)+2*300 ms] = 40Kb/600.4ms ≈ 66.6 Kbps*

2. Fragmentation (15 points)

2.1 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?

N: Kva meinast med fragmentering (i Internet protokoll sammanhang) og kvifor brukast det for IPv4 datagram?

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.

2.2 E: The IPv4 header is shown in Figure 1. In addition to the field “13-bit Fragmentation offset”, which other two fields are specially defined to be used in connection with fragmentation?

B: IPv4 headeren er vist i Figur 1. I tillegg til feltet “13-bit Fragmentation offset”, hvilke andre to felt er spesielt definert for bruk i forbindelse med fragmentering?

N: IPv4 headeren er vist i Figur 1. I tillegg til feltet “13-bit Fragmentation offset”, kva for andre to felt er spesielt definerte for bruk i samband med fragmentering?

The two other fields defined for use with fragmentation are the “16-bit Identifier” and the “Flags” (3 bit).

2.3 E: Where are fragments reassembled when using IPv4?

B: Hvor blir fragmenter reassemblert (“reassembled”) når IPv4 brukes?

N: Kor blir fragment reassemblerte (“reassembled”) når ein nyttar IPv4?

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?

N: Korleis veit ein om alle fragmenta er tatt imot slik at reassembleringa kan gjerast/fullførast?

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

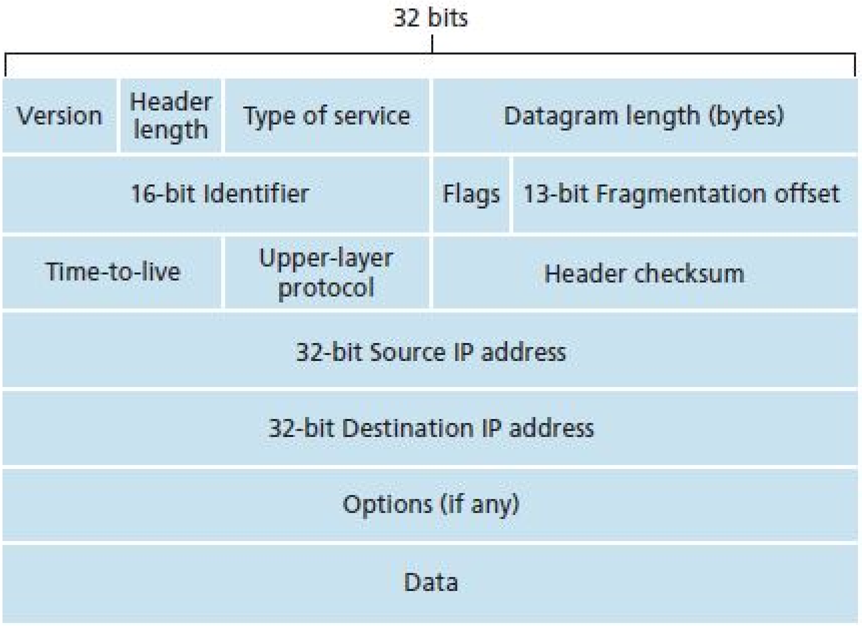
2.5 E: When using the IPv6 protocol, fragmentation is not allowed in routers, only in end-systems. What happens if an IPv6 router receives an IPv6 segment which is too large to be forwarded on an outgoing link?

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?

N: Når ein nyttar IPv6 protokollen tillet ein ikkje bruk av fragmentering i ruterar, kun i endesystem. Kva skjer om ein IPv6 rutar mottek eit IPv6 segment some er for stort til å bli sendt vidare på ein utgåande 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.

Fig. 1: IPv4 protocol header



3. Flow control / TCP (20 points)

3.1 E: What is flow control? Which Layer(s) need flow control? Why?

B: Hva er flytkontroll? Hvilke lag trenger flytkontroll? Forklar hvorfor.

N: Kva er flytkontroll? Kva for lag treng flytkontroll? Forklar kvifor.

Flow control is the receiver controls the data flow sending rate from the sender.

Flow control is commonly used in ***Transport Layer*** *and* ***Data Link Layer****. It may also be used in* ***Application Layer.***

The reason of having flow control in these layers 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. This scenario can happen in Transport Layer, Data Link Layer and Application Layer.

3.2 E: Give a brief description of the TCP three-way handshake procedure for connection establishment. (Keywords: type of segments exchanged; content of segments exchanged).

B: Gi en kort beskrivelse av TCP “three-way handshake” prosedyren for å etablere en forbindelse. (Stikkord: type segmenter som utveksles; innhold i segmentene som utveksles).

N: Grei kort ut om TCP “three-way handshake” prosedyren for å etablera eit samband. (Stikkord: type av segment som utvekslast; innhald i segment som utvekslast).

Three-way handshake 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 acknowledgement number is set to one more than the received sequence number i.e. B+1.

E: For tasks 3.3 to 3.5 below: Host A and Host B are communicating over a TCP connection, and Host B has already received from A all bytes up through byte 300. Suppose Host A then sends two segments to Host B back-to-back. The first and the second segments contain 32 and 62 bytes of data. In the first segment, the sequence number is 301, 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.

B: For oppgavene 3.3 til 3.5 nedenfor: Host A og Host B kommuniserer over en TCP-forbindelse, og Host B har allerede mottatt fra A alle byte opp til byte 300. Anta at Host A deretter sender to segmenter til Host B 'back-to-back'. Det første og det andre segmentet inneholder henholdsvis 32 og 62 byte med data. I det første segmentet er sekvensnummeret 301, source-portnummeret er 502 og destinasjons-portnummeret er 80. Host B sender acknowledgement hver gang den mottar et segment fra Host A.

N: For oppgåvene 3.3 til 3.5 nedanfor: Host A og Host B kommuniserer over eit TCP-samband, og Host B har allereie motteke frå A alle byte opp til byte 300. Anta at Host A deretter sender to segment til Host B 'back-to-back'. Det første og det andre segmentet inneheld høvesvis 32 og 62 byte med data. I det første segmentet er sekvensnummeret 301, source-portnummeret er 502 og destinasjons-portnummeret er 80. Host B sender acknowledgement kvar gong den mottar eit segment frå Host A.

3.3 E: In the second segment sent from Host A to Host B, what are the sequence number, source port number, and destination port number?

B: Hva er sekvensnummeret, source-portnummer og destinasjons-portnummer for det andre segmentet som sendes fra Host A til Host B?

N: Kva er sekvensnummeret, source-portnummer og destinasjons-portnummer for det andre segmentet som sendast frå Host A til Host B?

In the second segment from Host A to B:
Sequence number: 301 + 32 = 333
Source port number: 502
Destination port number: 80

3.4 E: If the first segment arrives before the second segment, in the acknowledgement of the first arriving segment, what are the acknowledgement number, the source port number, and the destination port number?

B: Hvis det første segmentet ankommer før det andre segmentet, hva er da acknowledgement-nummeret, source-portnummeret og destinasjons-portnummeret for dette segmentets tilhørende

”acknowledgement”?

N: I fall det første segmentet kjem fram før det andre segmentet, kva er da acknowledgement-nummeret, source-portnummeret og destinasjons-portnummeret for dette segmentets tilhøyrande ”acknowledgement”?

The acknowledgement number is 333
Source port number: 80
Destination port number: 502

3.5 E: If the second segment arrives before the first segment, in the acknowledgement of the first arriving segment, what is the acknowledgement number?

B: Hva er ”acknowledgement”-nummeret tilhørende det først ankomne segmentet hvis det andre segmentet ankommer før det første?

N: Kva er ”acknowledgement”-nummeret tilhøyrande det først ankomne segmentet hvis det andre segmentet kjem fram før det første?

If the second segment arrives before the first segment, in the acknowledgement of the first arriving segment, the acknowledgement number is 301, indicating that it is still waiting for bytes 301 and onward.

4. Domain Name System (DNS) (15 points)

4.1 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?

N: Kva er hovedoppgåva til “Domain Name System (DNS)” i internett og kva for to fundamentale komponentar er det sett saman av?

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

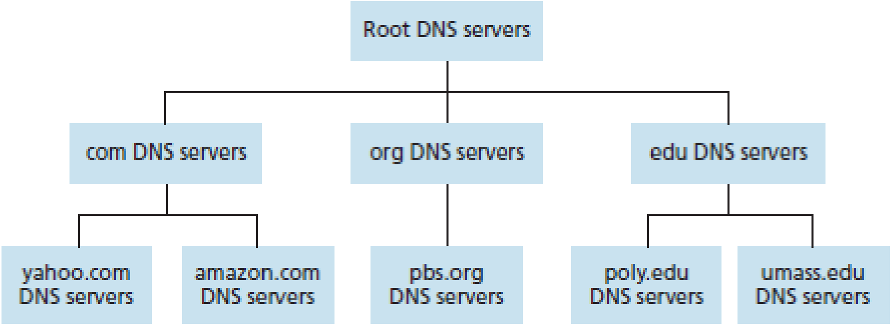
The two main parts:
(1) a distributed database implemented in a hierarchy of DNS servers, and
(2) an application-layer protocol that allows hosts to query the distributed database.

4.2 E: Give a brief overview of the server hierarchy of the DNS.

B: Gi en kort oversikt over tjener-hierarkiet til DNS.

N: Gje ei kort oversikt over tenar-hierarkiet i DNS.

Three classes of DNS servers—root DNS servers, top-level domain (TLD) DNS servers, and authoritative DNS servers—organized in a hierarchy as shown in the figure below (examples at 2. and 3. Level):



1) Root DNS servers: In the Internet there are 13 root DNS servers. Each of the 13 root DNS servers is actually a network of replicated servers, for both security and reliability purposes.
2) Top-level domain (TLD) servers: These servers are responsible for top-level domains such as com, org, net, edu, and gov, and all of the country top-level domains such as uk, fr, and no.
3) Authoritative DNS servers. Every organization with publicly accessible hosts (such as Web servers and mail servers) on the Internet must provide publicly accessible DNS records that map the names of those hosts to IP addresses. An organization's authoritative DNS server houses these DNS records. An organization can choose to implement its own authoritative DNS server to hold these records; alternatively, the organization can pay to have these records stored in an authoritative DNS server of some service provider. Most universities and large companies implement and maintain their own primary and secondary (backup) authoritative DNS server.

4.3 E: Assume you are setting up a new web-server with your own unique domain name. Describe briefly the process of getting the information about your new server into the DNS.

B: Anta at du setter opp en ny web-tjener med ditt eget unike domene navn. Forklar kort den nødvendige prosessen for å få informasjonen om din nye tjener lagt inn i DNS.

N: Anta at du set opp ein ny web-tenar med ditt eige unike domene namn. Forklår kort den naudsynte prosessen for å få informasjonen om din nye tenar lagt inn i DNS.

Very often this process is taken care of by a registrar, so it is hidden from a normal user. A registrar checks that your domain name is unique (i.e. not in use already by someone else). If ok, you need to supply the names and IP addresses of your primary and secondary authoritative DNS servers. For each of these two the registrar then makes sure that the necessary information is entered into the relevant Top-Level Domain servers. (One Type NS and one Type A record for each – but not necessary to know for full score).
In addition you will also have to make sure that the resource record for your Web server and the resource record for your Mail server are entered into your authoritative DNS servers. (Type A and Type MX, respectively – but not necessary to know for full score).

5. Wireless LAN (15 points)

5.1 E: Explain the difference between "infrastructure mode" and "ad hoc mode" in 802.11 W-LAN.

B: Forklar forskjellen på "infrastructure mode" og "ad hoc mode" i 802.11 W-LAN.

N: Forklår skilnaden på "infrastructure mode" og "ad hoc mode" i 802.11 W-LAN.

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.

5.2 E: What is (are) the main reason(s) why CSMA/CD cannot be used in 802.11 W-LAN?

B: Hva er hovedgrunnen(e) til at CSMA/CD ikke kan brukes i 802.11 W-LAN?

N: Kva er hovudårsaka(-ene) til at CSMA/CD ikkje kan brukast i 802.11 W-LAN?

1) The ability to detect collisions requires the ability to send (the station's own signal) and receive (to determine whether another station is also transmitting) at the same time. Because the strength of the received signal is typically very small compared to the strength of the transmitted signal at the 802.11 adapter, it is costly to build hardware that can detect a collision.
2) Even if the adapter could transmit and listen at the same time (and presumably abort transmission when it senses a busy channel), the adapter would still not be able to detect all collisions, due to the hidden terminal problem and fading.

5.3 E: Since "Collision Detection" (in CSMA/CD) is not used, how do you know if data frames have been succesfully transmitted to a receiver in 802.11 W-LAN?

B: Siden "Collision Detection" (i CSMA/CD) ikke brukes, hvordan vet en om datarammer har blitt vellykket overført til en mottaker i 802.11 W-LAN?

N: Sidan "Collision Detection" (i CSMA/CD) ikkje nyttast, korleis veit ein om dataramer har blitt overførde vellykka til ein mottakar i 802.11 W-LAN?

Explicit ACK frames are sent back to the sender for all successfully received data frames. If an ACK is not received it is assumed that the frame was lost.

5.4 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?

N: Kva er hovudskilnaden(-ane) mellom CSMA/CD og CSMA/CA med omsyn til verkemåte? Kva betyr "CA" i CSMA/CA og korleis oppnår ein 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.

5.5 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.

N: 802.11 W-LAN definerer ein tilleggsopsjon basert på bruk av “Request-To-Send (RTS)” og “Clear-To-Send (CTS)” kontrollramer. Forklar kort korleis det verker 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.

6. Multi-Protocol Label Switching (MPLS) (15 points)

6.1 E: What was the original main motivation for developing Multi-Protocol Label Switching (MPLS)?

B: Hva var den opprinnelige hovedmotivasjonen for å utvikle Multi-Protocol Label Switching (MPLS)?

N: Kva var den opprinnelige hovudmotivasjonen for å utvikle Multi-Protocol Label Switching (MPLS)?

To improve the forwarding speed of IP routers by adopting a key concept from the world of virtual-circuit networks: a fixed-length label. The goal was not to abandon the destination-based IP datagram-forwarding infrastructure for one based on fixed-length labels and virtual circuits, but to augment it by selectively labeling datagrams and allowing routers to forward datagrams based on fixed-length labels (rather than destination IP addresses) when possible.

6.2 E: Does IP addressing or IP routing change in any way when MPLS is used together with IP in a (label switched) router?

B: Medfører det noen endringer i IP adressering eller IP ruting når MPLS brukes sammen med IP i en (label switched) ruter?

N: Fører det med seg nokre endringar i IP adressering eller IP ruting når MPLS brukast saman med IP i ein (label switched) rutar?

Importantly, these techniques work hand-in-hand with IP, using IP addressing and routing. So the answer is basically no, at least not as seen by an end user.
(An MPLS enhanced frame can only be sent between routers that are both MPLS capable. However: all routers are able to handle IP datagrams with IP addressing, as before; the IP header with full address information is not changed in any way).

6.3 E: In addition to the original main motivation (in 6.1 above), other advantages has appeared that is at least equally important. Mention at least one of these advantages or uses of MPLS.

B: I tillegg til den opprinnelige motivasjonen (i 6.1 over) har det vist seg at MPLS har andre fordeler som er minst like viktige. Nevn minst en av disse fordelene eller bruksmåtene.

N: I tillegg til den opprinnelige motivasjonen (i 6.1 over) har det vist seg at MPLS har andre fordelar som er minst like viktige. Nemn minst ein av desse fordelane eller bruksmåtane.

One (or more) of the following should be mentioned:
1) Traffic engineering: use of labels is more flexible for load sharing over multiple paths towards a destination address than IP routing.
2) Reliability: Alternative paths via labels give options for fast restoration in case of failures in a network.
3) Virtual Private networks (VPN): Parallel logical networks on top of a common physical network can be established, with full resource and address isolation.