Løsningskladdebok august 2021

1.1

E: When an application in a host uses TCP to communicate with a server, what is the difference between a ServerSocket and a ConnectionSocket?

B: Når en applikasjon i en vert bruker TCP til å kommunisere med en tjener, hva er forskjellen mellom en «ServerSocket» og en «ConnectionSocket»?

N: Når ein applikasjon i ein vert bruker TCP til å kommunisera med ein tenar, kva er skilnaden mellom ein «ServerSocket» og ein «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.

1.2

a)
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.

b)
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:

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.

c)
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).

1.3

E: Consider sending a file of 1400K 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 1 Mbps. At least how much time does it take to send the file from Host A to Host B?
B: En datafil på 1400K 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 1 Mbps. Hvor lang tid vil det minst ta å sende datafilen fra Host A til Host B?

The transmission time or delay is simply 1400K x 8bits / 1 Mbps = 11.2 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 + 11.2 s = 11.5 seconds. (Note: if propagation time is taken into account, this value will be added to the total time. But since the lengths of the links are not given this value is unknown).

2.1

a)
E: Does a TCP segment contain IP addresses as part of its payload? Explain why or why not.
B: Inneholder et TCP-segment IP-adresser som en del av nyttelasten? Forklar hvorfor eller hvorfor ikke.
N: Inneheld eit TCP-segment IP-adresser som ein del av nyttelasta? Forklar kvifor eller kvifor ikkje.
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.

b)
E: Is there any difference in how checksums are implemented in TCP and UDP segments? If so, explain.
B: Er det noen forskjell på hvordan sjekksum er implementert i TCP og UDP segmenter? Hvis ja, forklar.
N: Er det nokon skilnad på korleis sjekksum er implementert i TCP og UDP segment? Viss ja, forklar.
Answer: No difference. The same type of checksum is implemented for both UDP and TCP segments.

c)
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.
B: UDP er en upålitelig protokoll i forhold til TCP, siden den er forbindelsesløs og uten støtte for strømnings- eller overbelastningskontroll. Men den har også noen fordeler for noen bruksområder sammenlignet med TCP. Gi et eksempel på minst et slikt bruksområde eller tilfelle.
N: UDP er ein upåliteleg protokoll i forhold til TCP, sidan han er forbindelseslaus og utan støtte for strømnings- eller overbelastingskontroll. Men han har òg nokre fordelar for nokre bruksområde samanlikna med TCP. Gi eit døme på minst eit slikt bruksområde eller tilfelle.

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.

2.2

a)

E: Give a brief overview of how a TCP connection is established.
B: Gi en kort oversikt over hvordan en TCP forbindelse blir etablert (eller «satt opp»).
N: Gi ei kort oversikt over korleis eit TCP samband blir etablert (eller «sett opp»).

Answer:
TCP uses a three-way handshake procedure for connection establishment. This is done as follows (assuming a host connecting to a server):

1. SYN: The host sends segment 1, which is a SYN (i.e. the SYN bit is set to 1), to the server. The host has set this segment's sequence number to a random value A.

2. SYN-ACK: When received, the server allocates TCP buffers and variables for the connection. In response, the server replies in segment 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 segment is another random number B.

3. ACK: When received, the host also allocates buffers and variables to the connection. Finally, the host sends an ACK back to the server in segment 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.

b)

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).
B: Hva vil du (generelt) oppnå ved å bruke flytkontroll? Hvilken type flytkontroll er implementert i TCP? (Korte svar er tilstrekkelige på begge spørsmålene, ingen detaljer om hvordan flytkontroll er implementert i TCP er nødvendig).
N: Kva vil du (generelt) oppnå ved å bruka flytkontroll? Kva for ein type flytkontroll er implementert i TCP? (Korte svar er tilstrekkelege på begge spørsmåla, ingen detaljar om korleis flytkontroll er implementert i TCP er nødvendig).
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.

2.3

E: Give at least two different ways that data packets can disappear on their way through a packet switched network.
B: Oppgi minst to forskjellige måter datapakker kan forsvinne på vei gjennom et pakkesvitsjet nett.
N: Oppgi minst to ulike måtar datapakkar kan forsvinna på veg gjennom eit pakkesvitsjet nett.

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.

3.1

B: Gjør rede for fremgangsmåten for å finne CRC koden for en gitt datastreng D med en gitt generator G hos en sender av data. (Stikkord: hvilke matematiske operasjoner inngår; hva sendes til mottaker).
E: Explain the procedure for finding the CRC code of a given data string D with a given generator G at a transmitter of data. (Keywords: which mathematical operations are included; what is sent to the recipient).
N: Gjer greie for fremgangsmåten for å finna CRC koden for ein gitt datastreng D med ein gitt generator G hos ein sendar av data. (Stikkord: kva for nokre matematiske operasjonar inngår; kva blir sendt til mottakar).

Answer:
A number of zeroes, equal to the length of G minus 1, is added to the data string D, i.e. as placeholders for the CRC code, e.g. 101010000 (for data D=101010 and G with length 4).

The CRC is then found as the remainder of a modulo-2 division of D (plus added zeroes) by the generator G.

The division result is not used for anything.

The CRC is sent after the data, instead of the added zeros for the division, e.g. 101010001 (for G=1011). This should give remainder zero in division at receiver if successful transmission.

3.2

B: Gjør rede for hvordan en linklagssvitsj virker. På hvilke måter er den ulik en ruter?
E: Explain how a link layer switch works. In what ways is it different from a router?
N: Gjer greie for korleis ein linklagssvitsj verkar. På kva måtar er den ulik ein ruter?

Answer:
The main function of a link layer switch is to forward (or switch) incoming frames from one interface to one or more outgoing interfaces, or potentially filter (drop) frames if it belongs in the direction of the interface it arrived on. The switching is based on link layer (MAC) addresses. A switch table is used to decide which interface(s) a frame is forwarded to. If the link layer address is not in the table the frame is sent in all directions except where it arrived from. If the address exists in the table but is associated with the interface it arrived on, it is dropped. Otherwise it is sent to the interface given by the table. Link layer switches are self-learning, in the sense that the table is updated with “from” (link layer) addresses when receiving frames on the different interfaces. All mappings in the table are deleted after a certain time interval to make sure that information learned and stored is dynamic and up to date. In addition to the above a link layer switch differs from a router in that it operates only within a subnet and are transparent to hosts and servers, i.e. they do not have their own addresses (neither MAC or IP) like routers have (IP addresses in the network layer). Link layer switches also have the advantage of being self-configuring (“plug-and-play”).

3.3

B: Hva er ARP og hvorfor er den nødvendig?
E: What is ARP and why is it necessary?
N: Kva er ARP og kvifor er den nødvendig?

ARP er «Address Resolution Protocol». Den brukes for å oversette mellom IP- og linklags-adresser (i praksis ofte Ethernett-adresser) lokalt i et subnett. ARP tabellene er plassert i minne til hver vert og ruter.

4.1

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.

4.2

a)

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.

b)

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.

4.3

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, e.g. RTS and CTS).

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.

5.1

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

5.2

E: Explain briefly how one of the methods above (in 5.1) 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 5.1) 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 5.1) 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.

5.3

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.
B: Tre kategorier av brannmurer er gitt i pensum: “Traditional packet filters”, “Stateful packet filters”, og “Application gateways”. Gi korte forklaringer av funksjonaliteten til hver av disse, med spesiell fokus på forskjellene mellom dem.
N: Tre kategoriar av brannmurar er gitte i pensum: “Traditional packet filters”, “Stateful packet filters”, og “Application gateways”. Gi korte forklaringar av funksjonaliteten til kvar av desse, med spesiell fokus på skilnadene mellom dei.

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.