Possible SOLUTION

Exam TTM4100 SUMMER (5. August) 2020

1.1 Service types

Explain what we mean by "connection oriented" and "connectionless" services in a communication networking context. Can a service be both at the same time?

Answer:

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 Switching principle

Explain circuit switching and packet switching and give at least three differences between them.

Answer:

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 (usually) 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 Protocol layers

Explain the protocol stack as it is defined and used for the Internet. (Keywords: purpose of the model, terminology, services, encapsulation).

Answer:
Defined 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. 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.

1.4 HTTP

Explain what HTTP is and explain (at a high level) the behavior of the protocol (Keywords: what is it used for; stateless or stateful (why?); persistent or not persistent and what it means; caching).

Answer:
The HyperText Transfer Protocol (HTTP) is the World Wide Web's application layer protocol. It is implemented in two programs: a client program (normally a "Web browser") and a server program ("Web server"). These two programs communicate with each other via HTTP. The protocol is stateless, meaning that the server program (Web server) does not maintain any information about specific clients. HTTP uses TCP as its underlying transport protocol. Both persistant and non-persistant connections are supported by HTTP. Persistant means that a client and server communicates via one TCP connection for a period of time, while non-persistant means that a new TCP connection is established for every new request/response interaction between client and server. Web caches are used in the network to reduce traffic and processing in the WWW. They are present in most end-user equipment, so you do not need to request the same page again, if nothing has changed since last time you requested it, but also inside the network (e.g. Content Distribution networks - CDN's), storing the most popular web-pages or content. In addition to reducing traffic and processing, this also reduces waiting times for content access.

2.1 Reliable data transfer

Explain the most important challenges of creating a reliable data transfer service based on an unreliable (datagram) service, e.g. IP. (Keywords: packet loss; delay; required functionality).

Answer:
The fundamental challenge of creating a reliable data transfer service is that a communication channel is not perfect with respect to loss of information, and the fact that information transport takes time. For economic reasons it is also of importance that resources are utilized

if there is a need for them, e.g. an efficient use of channel capacities and processing power in network elements.

Bit error detection (e.g. a checksum) is necessary to discover loss of information at the lowest level of communication. Some form of forward error correction (FEC) (e.g. two dimensional parity bits) could also be added to allow repair of simple bit level errors at the receiver. However, this gives a trade-off between the amount of extra "parity" information transmitted (usually not needed if the quality of the medium is high; thus wasted most of the time) and extra use of resources, both channel capacity and processing of more advanced "checksums".

Some form of positive and/or negative acknowledgements (ACK/NACK) is also useful, in case larger chunks of data ("packets") are lost (out of bounds for handling by the bit error detection mechanisms). A mechanism for retransmission is then also necessary; possibly also timeouts at the sender, if a packet is lost without resulting in an explicit NACK. Since communication may take time, especially if communicating over some distance, it is not practical to wait for ACKs for each chunk of data before continuing. Some form of window mechanism ("pipelining") is therefore used, to speed up the allowable data rates and utilization of the channels. (An example of what happens if "pipelining" is **not** used is illustrated in Problem 2.4 of this exam).

2.2 Set-up of TCP connection

Explain how a TCP connection is established.

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.

2.3 Sequence numbers and ACKs

Explain how sequence numbers and acknowledgments are used for flow control in the TCP protocol.

Answer:

TCP views data as an unstructured, but ordered, stream of bytes. Both sequence numbers and acknowledgements are therefore related to number of bytes sent or received, not number of segments.

The sender maintain a variable called the receive window, reflecting how much free space is available at the receiver side. The sequence number is the byte-stream number of the first byte in a segment. Successfully transmitted segments are acknowledged from the receiver to the sender (giving the number of bytes successfully received), 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, since losing segments is often an indication of network congestion).

2.4 Stop-and-wait flowcontrol

Given two hosts that are directly connected via a channel. The channel has a transmission rate of 250 Mbit/s. The maximum packet size in the network is 10,000 bytes. Assume that the propagation delay between the two hosts is 600 ms. What is the maximum data rate that can be achieved when using "stop-and-wait" flow control?

Write mathematical expressions as plain text. Use "*" for multiplication and "/" for division, in addition to enough parentheses (and possibly "+" and "-") for it to be correct.

NB! Explain what you are doing and why the result is as shown; putting numbers into a formula taken from the book is not a good enough answer.

Answer:
Time to put one packet out on the channel is (10,000 * 8) [bits] / 250,000,000 [bits/s] = 0.32 ms. Propagation time is 600 ms for the packet to reach the receiver. Assuming (since we ask for the maximum data rate) that we can ignore the time it takes to put a very small acknowledgement packet (ACK) out on the channel, the propagation time for the ACK still needs another 600 ms to reach the sender. The total time before we can allow the sender to continue with the next packet is then (0.32 + 600 + 600) = 1,200.32 ms. In other words we are able to send 80,000 bits in 1,200.32 ms which gives a maximum data rate of 80,000 / 1,200.32 = 66.64 bit/ms = 66.64 kbit/s. (Thus a really bad utilization of a 250 Mbit/s channel).

3.1 Networking layer in general

Provide an overview of the network layer. (Keywords: main tasks/functions; protocol(s) used; where in the network it is present).

Answer:
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 Fragmentation

Explain the use of fragmentation when transmitting with the IP protocol. (Keywords: why is it used; reassembly (where and how); differences between IPv4 and IPv6?).

Answer:
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.

For IPv4 fragmentation can be done by routers, but the reassembly is done in the end systems, not in the routers. Segments are marked by using one of the "Flag" bits in the IPv4 header. It contains a 1 for all fragments except the last one which is 0.

When using the IPv6 protocol, fragmentation is not allowed in routers, only in end-systems. 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.

3.3 IPv4 CIDR
Assume (CIDR) IPv4 address 223.1.2.0/xx. If we need about 500 IP addresses available for hosts and router interfaces in our network, what is the maximum value we can use for xx? Explain why.

Answer:
xx = 23 which gives 510 adresses (xx=24 would give 254 adresses only, i.e. too few). The number of addresses is given as $2^{(32 - xx)}$ - 2. (The two addresses subtracted are reserved for special purposes).

3.4 IPv6
Explain the most important changes/improvements in the transition from IPv4 to IPv6. Also include arguments used for why the changes are necessary or desired. (Keywords: address space; fragmentation; checksums; protocol header structure).

Answer:
The main reason that started the development of a new version of the IP protocol was the realization that the IPv4 address space would become too small at some point. But as indicated below, some other improvements are also implemented.

- Address space: Increase from 32 bit addresses to 128 bits addresses.
- Processing in routers: since routers (at least for now) are electronic, it is important to optimize processing of packets for both scalability and energy use. Some contributions to this:
  - A more streamlined fixed length 40 byte IP packet header is easier to process.
  - Not allow routers to do fragmentation, but leave this processing to the end systems.
  - Removal of header checksum. It is assumed that this is sufficiently taken care of by the transport and link layers.
- Flow labelling: It is not completely clear what this is to be used for but it could be important in future communication, e.g. to give different QoS to different types of

traffic in the network. Flow labels allow you to keep track of connections also in the network layer, i.e. in routers, not only end-to-end on the transport layer, as with TCP.

4.1 Link layer in general

Give an overview of the link layer. (Keywords: main tasks/functions; protocols used; where in the network it is present).

Answer:

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 CRC

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).

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.

4.3 Link layer switching

Explain how a link layer switch works. In what ways is it different from a router?

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”).

4.4 QoS

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

Answer:
It is limited how long you can buffer information to cancel out variation in delay through the network, since 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 realtime, 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.

5.1 Caesar cipher

Use Caesar cipher with key k = 5 to encrypt the text "Koronaviruset er skummelt".
(Use the Norwegian alphabet a to å).

Answer:
The key k=5 is the same as adding +5 (modulo the length of the alphabet), i.e. a -> f,
b -> g, …, å -> e (for the Norwegian alphabet).

For the given text string this should then become: “Ptwtsfænwzxjy jw xpzrrjqy”.

5.2 Digital certificate

What is a digital certificate and how is it 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.

5.3 RTS /CTS

802.11 W-LAN defines an additional option based on the use of "Request-To-Send (RTS)" and "Clear-To-Send (CTS)" control frames. Explain how it works and when it (potentially) is used.

Answer:
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.

5.4 HOL blocking

What is the "Head-Of-Line (HOL)" blocking?

Answer:
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.