IKT204-G V24, Front page

Subject code: IKT204-G
Subject name: Data communication
Date: 07.05.2024
Duration: 3 hours

Resources allowed: Calculator (note that graphing calculators are **NOT** allowed and that programmable calculators must have **ALL** installed programs deleted).

Technical information:

- The exam is both in English and Norwegian (with some headings and expressions in English). You select language in the menu at the upper right corner. Note that you can select to view assignments in English or Norwegian at any time during the exam.
- The exam contains assignments of the type multiple choice, multiple answer, pulldown menu, fixed text and calculation.
- Each correctly answered assignment gives from 2 to 12 points, in total 104 points. For each part of an assignment:
  - Correct answer gives 0.35 - 2 points for each question, depending on difficulty.
  - Wrong answer gives 0 points for all questions except multiple answer assignments.
  - Wrong answers in multiple answer assignments give a negative score, so if you click on all the options in the assignment the sum will be 0 points. A negative score for the assignment as a whole is not possible.
- There is an open text field on the last page which may be used for writing additional comments and assumptions to the assignments of the exam. This text field does not give any points in itself, but it may impact the judgement of other assignments. It is not necessary to use the text field since correct answer on all questions will give full score. If the question is not correct, then you may get additional points if you explain a partially correct solution or give a good assumption in the text field.

1 IKT204-G V24, Internet 5-layer model

What are the data packets on the different layers called? (6 points)

Application layer Select alternative (Protocol stack, Segment, Datagram, Message, Protocol suite, Bits, Bytes, Request, Frame, Response)

Transport layer Select alternative (Message, Bits, Frame, Protocol stack, Datagram, Request, Bytes, Response, Segment, Protocol suite)

Network layer Select alternative (Message, Datagram, Response, Frame, Bytes, Segment, Protocol stack, Request, Bits, Protocol suite)

Link layer Select alternative (Bits, Request, Message, Response, Protocol stack, Datagram, Protocol suite, Frame, Segment, Bytes)

Physical layer Select alternative (Bits, Protocol suite, Datagram, Frame, Bytes, Request, Message, Response, Protocol stack, Segment)

All these layers are together called a: Select alternative (Protocol stack, Segment, Datagram, Response, Protocol suite, Bits, Frame, Message, Bytes, Request)

Maximum marks: 6

2 IKT204-G V24, Wireshark HTTP

The PDF document shows two excerpts from a Wireshark capture. Both excerpts are from the same TCP connection and shows the start and end of a session. **Note that you need to scroll down to the bottom of the PDF document to see the end of the session.** Answer the following questions: (12 points)

Which link layer protocol is used here? Select alternative (IEEE 802.11, UDP, TCP, DHCP, Ethernet, IP, ARP, HTTP, SSL)

Which protocol is encapsulated in the link layer frame? Select alternative (TCP, Ethernet, IPv6, IEEE 802.11, UDP, DHCP, IPv4, SMTP, HTTP, ARP, SSL)

How large is the announced window size in number of bytes in packet 330? Select alternative (65024, 554, 256, 1573, 113978, 254)

What type of window is this? Select alternative (Sliding window in number of packets, Congestion window, Window size of the user interface, Receiver window)

Which application layer protocol is used here? Select alternative (IPv4, Ethernet, ARP, IPv6, UDP, HTTP, TCP, DHCP)

Who sends packet 330? Select alternative (The client, None, The server)

What is the client's port number in this TCP connection? (60104)

What type of connection is the application layer protocol using? Select alternative (Persistent connection, One-shot connection, Time-out connection, Non-persistent connection)

The application layer protocol in use here uses cookies. But what is a cookie?

Select alternative (It is a cache of previously downloaded web page objects., It is a piece of data which is sent from a website and stored on the client's end-system in a special cookie file managed by the browser., It is an executable code snippet that is downloaded from a website and stored on the client's end system to improve the website's performance., It is a list of previously opened websites.)

Is cookie information exchanged in packet 330? Select alternative (Yes, No)

How many bytes of application data are sent with packet 330? (554)

How many routers may packet 330 pass through before it is discarded? (127)

Who initiates termination of this TCP connection? Select alternative (None, The client, The server)

Which sequence number did the very first byte get in application data exchanged between the client and the server? (1)

How many bytes of application data have been transferred during this TCP session?

Client has sent: (1572 - 1574) Server has sent: (114406 - 114408)

Maximum marks: 12

3 IKT204-G V24, DNS

Below are some statements about Domain Name System (DNS) and how it works. (5 points)

Select correct alternatives:

- [ ] DNS queries use port 53 over UDP. ✔
- [ ] Top-level domain (TLD) DNS servers are located at the top of the hierarchy of DNS servers.
- [ ] The DNS service belongs to the application layer in the Internet five-layer protocol st ✔ .
- [ ] DNS queries use port 5353 over TCP.
- [ ] Root DNS servers are located at the top of the hierarchy of DNS servers. ✔
- [ ] The DNS service belongs to the network layer in the Internet five-layer protocol stack.
- [ ] Authoritative DNS servers are located at the top of the hierarchy of DNS servers.
- [ ] An iterative DNS query buts the burden for resolving the domain name on the server requested.
- [ ] A domain name may be added to DNS by an usual DNS query.
- [ ] A domain name may be added to DNS by an accredited registrar. ✔
- [ ] A recursive DNS query buts the burden for resolving the domain name on the server ✔ requested.
- [ ] A domain name may be added to DNS by a Certificate Authority (CA).
- [ ] DNS queries are by default encrypted.

Maximum marks: 5

4 IKT204-G V24, DHCP

Below are some statements about Dynamic Host Configuration Protocol (DHCP) and how it works. (6 points)

Select correct alternatives:

- [ ] DHCP provides IP addresses to root DNS servers.
- [ ] DHCP allows a host to obtain an IP address automatically. ✔
- [ ] DHCP is a network layer protocol.
- [ ] DHCP provides LAN subnet mask. ✔
- [ ] DHCP provides IP address to nearest switch.
- [ ] DHCP provides ISP subnet mask.
- [ ] DHCP is a link layer protocol.
- [ ] DHCP provides IP address to LAN gateway (nearest router). ✔
- [ ] DHCP provides IP addresses to local DNS servers. ✔
- [ ] DHCP provides IP addresses to TLD DNS servers.
- [ ] DHCP allows a host to obtain a MAC address automatically.
- [ ] DHCP allows a host to obtain a socket port number automatically.
- [ ] DHCP is an application layer protocol. ✔
- [ ] DHCP is a client-server protocol. ✔

Maximum marks: 6

5 IKT204-G V24, UDP quality of service

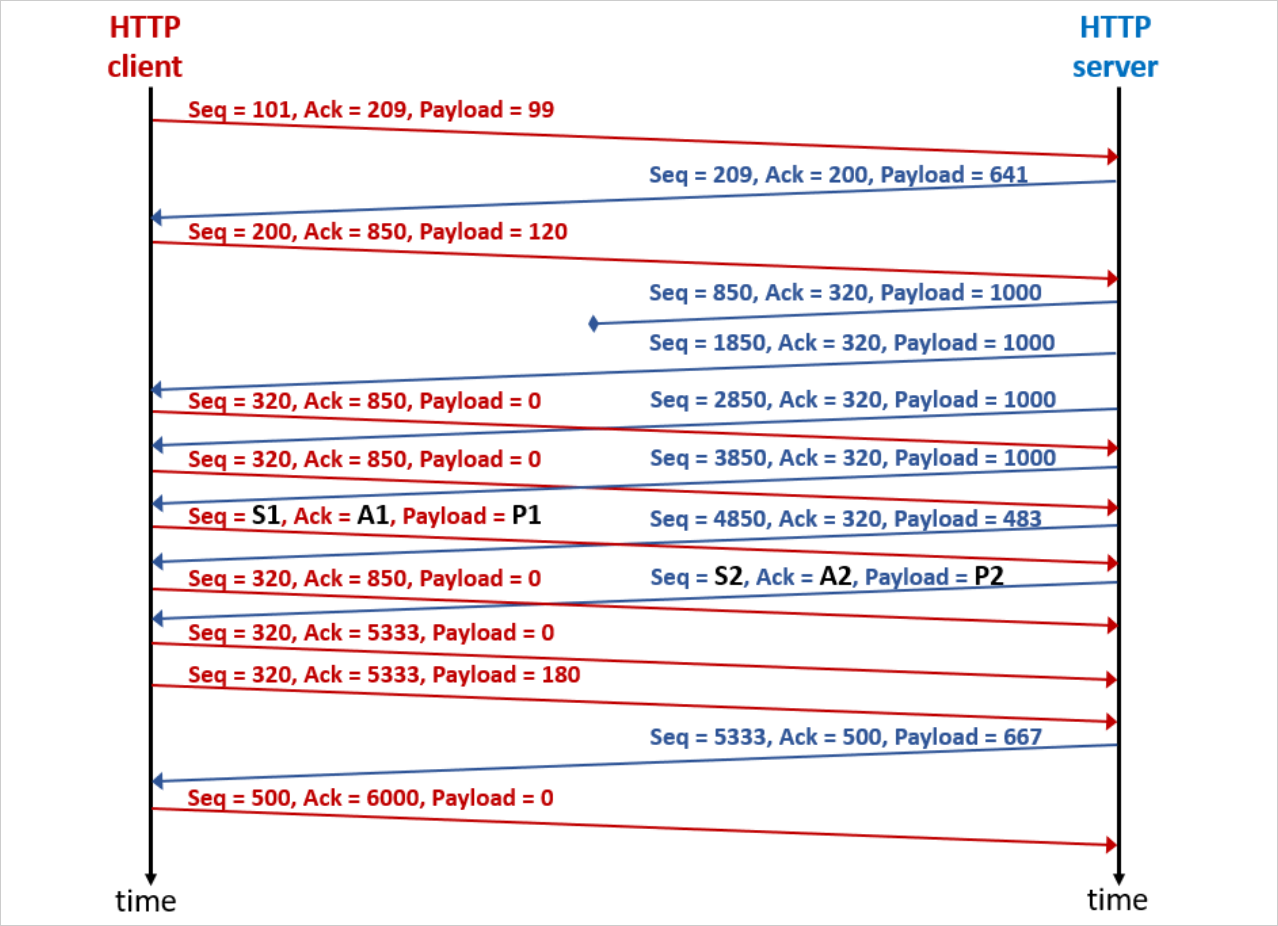
Which service quality guarantees does User Datagram Protocol (UDP) give? (2 points)

Select one or more alternatives:

- [ ] Server authentication
- [ ] Data integrity
- [ ] Bounded delay
- [ ] In-order data delivery
- [ ] Reliable data transfer
- [ ] Data confidentiality
- [ ] Guaranteed bandwidth
- [ ] None of these ✔

Maximum marks: 2

6 IKT204-G V24, TCP sequence



Above is an excerpt from a TCP (Reno version) transmission. What will the sequence number, acknowledgement number and payload length denoted **S1**, **A1**, **P1**, **S2**, **A2** and **P2** be in the segments shown in the figure? (9 points)

S1= (320) A1= (850) P1= (0)

S2= (850) A2= (320) P2= (1000)

The fourth segment is lost somewhere in the network on its route to the client. How does TCP ensure that this segment is delivered as shown in the excerpt above?

Select alternative (Segment is re-transmitted after receiving triple duplicate ACK., It is up to the application layer to re-transmit the lost segment., Segment is re-transmitted on timeout., The link layer will ensure reliable data transfer in this case.)

TCP also have a re-transmission timer. What happens when this timer expires?

Select alternative (On timeout the connection is shut down., On timeout only the segment that caused the timeout is re-transmitted., On timeout all unacknowledged segments are re-

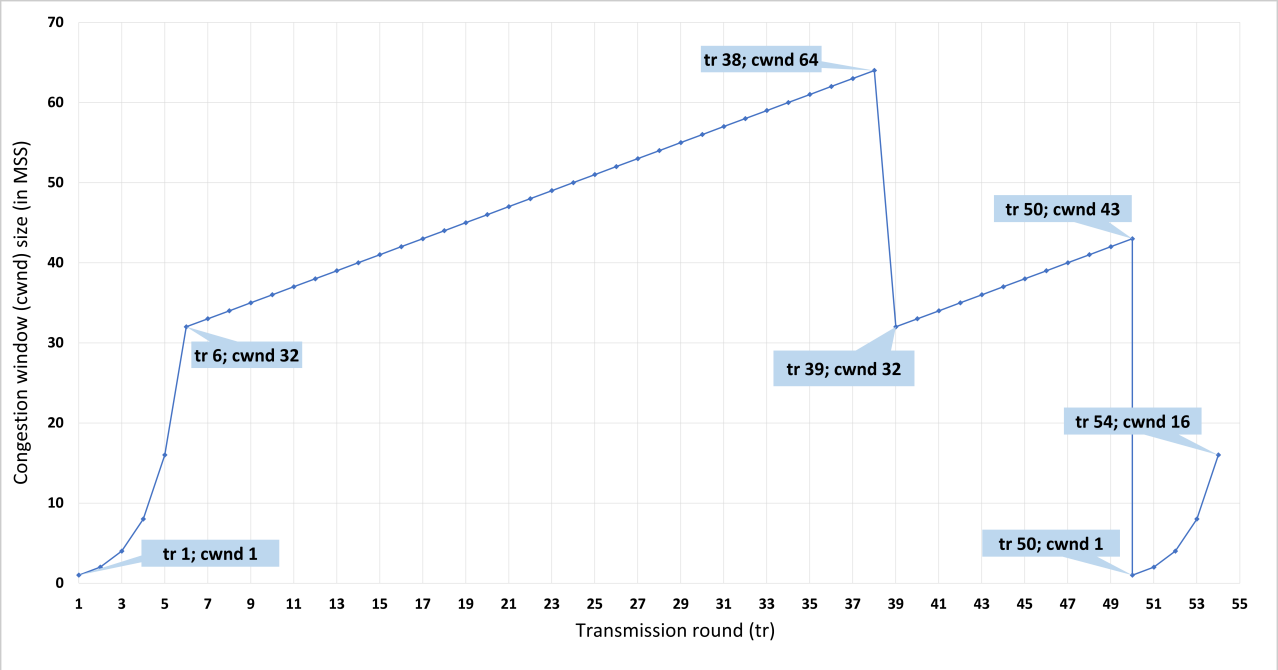
transmitted.)

The client has received segments out of sequence. What has the client done with these?

Select alternative (The client has only taken care of the segment that succeeded the segment that was lost., The client has stored them and can acknowledge accumulated., Impossible to say based on the excerpt shown., The client has discarded them, so the server must resend the segments.)

Maximum marks: 9

7 IKT204-G V24, TCP congestion control



TCP Reno's congestion control algorithm has 3 states: Slow Start, Congestion Avoidance and Fast Recovery. The figure shows the size of TCP Reno's congestion window (cwnd) in number of segments as a function of the transmission round (tr). Answer the following questions: (7 points)

Identify an interval where TCP Slow Start is in action? Select alternative ([38,39], [6,38], [1,6], [6,50])

Identify an interval where TCP Congestion Avoidance is in action? Select alternative ([50,54], [6,38], [1,6], [38,39])
TCP is in the state Fast Recovery in the transmission round [38,39]. What caused TCP to end up

in this state? Select alternative (Received a triple duplicate ACK., Received an Explicit Congestion Notification (ECN)., An ACK timeout occurred., Received a new ACK.)

When does TCP enter the state Slow Start? Select alternative (When establishing a TCP connection and when there is a timeout on ACK., When establishing a TCP connection and when a new ACK is received., Upon receiving a triple duplicate ACK., Upon receipt of an Explicit Congestion Notification (ECN).)
TCP Reno's congestion control mechanism is called AIMD - Additive Increase Multiplicative

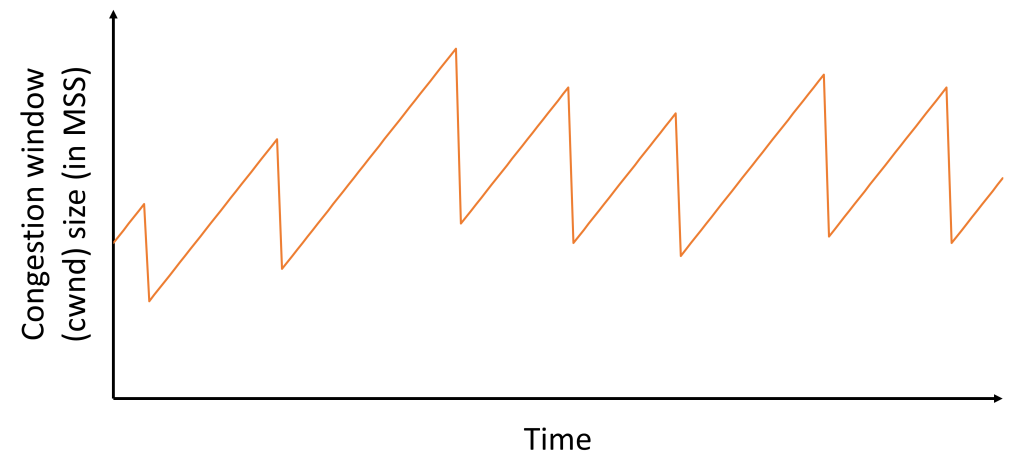
Decrease. What is driving the additive increase of the congestion window? Select alternative (Reception of segments containing payload., Receipt of Explicit Congestion Notification (ECN)., A recurring timer., Receiving new ACKs.) And what is the speed this window increases at

associated with? Select alternative (The amount of received data in bytes within a specified interval., How often the retransmission timer gives timeouts., The end-to-end delay on the TCP connection., Round trip time - RTT)

The result of AIMD congestion control is that we get such a "saw tooth-like" behavior on the congestion window over time with TCP Reno in normal operating mode as shown in the figure below. Assume that the **maximum** size of the congestion window is roughly constant and equal to **250** over the duration of a TCP connection. Assume further that the Maximum Segment Size (MSS) is **560 bytes** and that the round-trip time RTT is **20 milliseconds**.

What would be the average data transfer rate on such a TCP connection in **Mbps**? (41 - 43)

Mbps



Maximum marks: 7

8 IKT204-G V24, IPv4 and subnet

Suppose an ISP owns the block of addresses of the form 85.175.130.0/23. Suppose it wants to create four subnets from this block, with each block having the same number of IPv4 addresses. (7 points)

What are the prefixes (of the format a.b.c.d/x) for the four subnets in increasing order?

Subnet 1: 85.175. [ ] (130) . [ ] (0) / [ ] (25)

Subnet 2: 85.175. [ ] (130) . [ ] (128) / [ ] (25)

Subnet 3: 85.175. [ ] (131) . [ ] (0) / [ ] (25)

Subnet 4: 85.175. [ ] (131) . [ ] (128) / [ ] (25)

How many bits constitutes the host portion of the prefixes created for the four subnets? [ ] (7) bits.

How many hosts may be assigned an IPv4 address within each of the four subnets? [ ] (126 - 128) hosts.

Maximum marks: 7

9 IKT204-G V24, Routing standards

Below are some statements about routing at the network layer. (4 points)

Fill in the correct expression in each sentence:

The Select alternative (OpenFlow protocol, RIP - Routing Information Protocol, OSPF - Open Shortest Path First, BGP - Border Gateway Protocol) is the de facto standard protocol for advertising routing information between autonomous systems. An important attribute exchanged is

the Select alternative (IP-LIST, GW-PATH, AS-PATH, NEXT-HOP) which is a list of autonomous systems that datagrams are offered to pass through to reach the advertised remote

prefix. For this reason, this protocol is called a Select alternative ("shortest path", "prefix

vector", "fastest path", "path vector") protocol. A prefix in this context Select alternative (an SDN control plane, an IPv4 or IPv6 address, a DNS server that manages the prefix, a block of IP addresses specified in CIDR format).

Maximum marks: 4

10 IKT204-G V24, Routing tables

In this assignment, the objective is to determine the correct forwarding link given the routing table below. (5 points)

A router has the following entries in its forwarding table (IPv4 prefixes given in dotted-decimal form and binary):

Link1:	46.168.4.0/22	00101110.10101000.00000100.00000000/22
Link2:	46.168.6.0/23	00101110.10101000.00000110.00000000/23
Link3:	46.168.7.0/24	00101110.10101000.00000111.00000000/24
Link4:	46.168.0.0/15	00101110.10101000.00000000.00000000/15
Link5:	All other addresses	

Assume the router receives IPv4 datagrams destined to the following addresses and decide which link they are forwarded to:

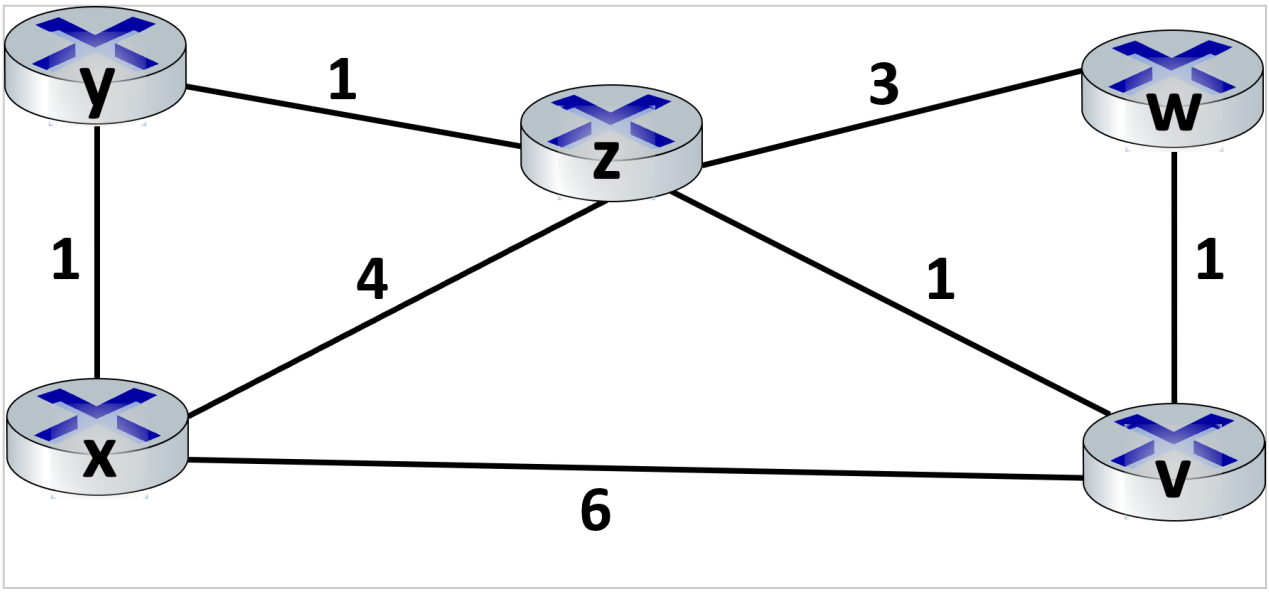
A:	46.168.3.80	00101110.10101000.00000011.01010000
B:	46.168.5.254	00101110.10101000.00000101.11111110
C:	46.168.7.152	00101110.10101000.00000111.10011000
D:	46.168.6.130	00101110.10101000.00000110.10000010
E:	46.169.5.15	00101110.10101001.00000101.00001111

On which link will they be forwarded?

A: link (4) B: link (1) C: link (3) D: link (2) E: link (4)

Maximum marks: 5

11 IKT204-G V24, Link-state algorithm



First read the information under the table about the notation to be used. Then run Dijkstra's shortest-path algorithm in node **x** on the network of routers shown in the figure above and complete the table below. (5 points)

Step	N'	D(z),p(z)	D(y),p(y)	D(v),p(v)	D(w),p(w)
0	x	(4,x, 4x)	(1,x, 1x)	(6,x, 6x)	(inf, -)
1	(xy, x,y)	(2,y, 2y)		(6,x, 6x)	(inf, -)
2	(xyz, x,y,z)			(3,z, 3z)	(5,z, 5z)
3	(xyzv, x,y,z,v)				(4,v, 4v)
4	(xyzvw, x,y,z,v,w)				

Notation:
N' contains the visited nodes, listed in the **order** they are visited (e.g.: **uvxwy** or with comma **u,v,x,w,y**).
D(n) is the distance to node n.
p(n) is the previous node along this distance.

Use the following notation for **D(n),p(n)**: integer,node (e.g.: **4,z** or without comma **4z**).
If the node is **not** reachable, use **inf** or **single dash** for **D(n),p(n)**.

Maximum marks: 5

12 IKT204-G V24, Ethernet LAN and switches

Ethernet is the most widely used technology for wired Local Area Network (LAN). Answer the following questions and fill in the correct statement in the sentences at the bottom: (8 points)

Which IEEE standards specifies wired Ethernet? Select alternative (802.3, 802.13, 802.5, 802.11)

Which wired LAN topology is by far the most common today? Select alternative (Ring with token passing., Bus with all nodes in same collision domain., Star with point-to-point links and switch in the middle.)

Which cable type is most common in LANs today? Select alternative (Coaxial cable, Twisted-pair cable, Two-pair cable, Fiber optic cable)

A host in a LAN has been assigned IPv4 address: 10.10.99.17/22 in CIDR (Classless Inter-Domain Routing) format.
What is the network mask written in dotted-decimal notation?

Select alternative (22.22.22.22, 0.0.0.22, 255.255.252.0, 10.10.252.0, 255.255.1.0)

What is the correctly configured IPv4 address of the gateway router located in the same subnet

as this host? Select alternative (10.10.99.0, 255.255.252.22, 10.10.96.1, 10.10.22.1, 10.10.1.1)

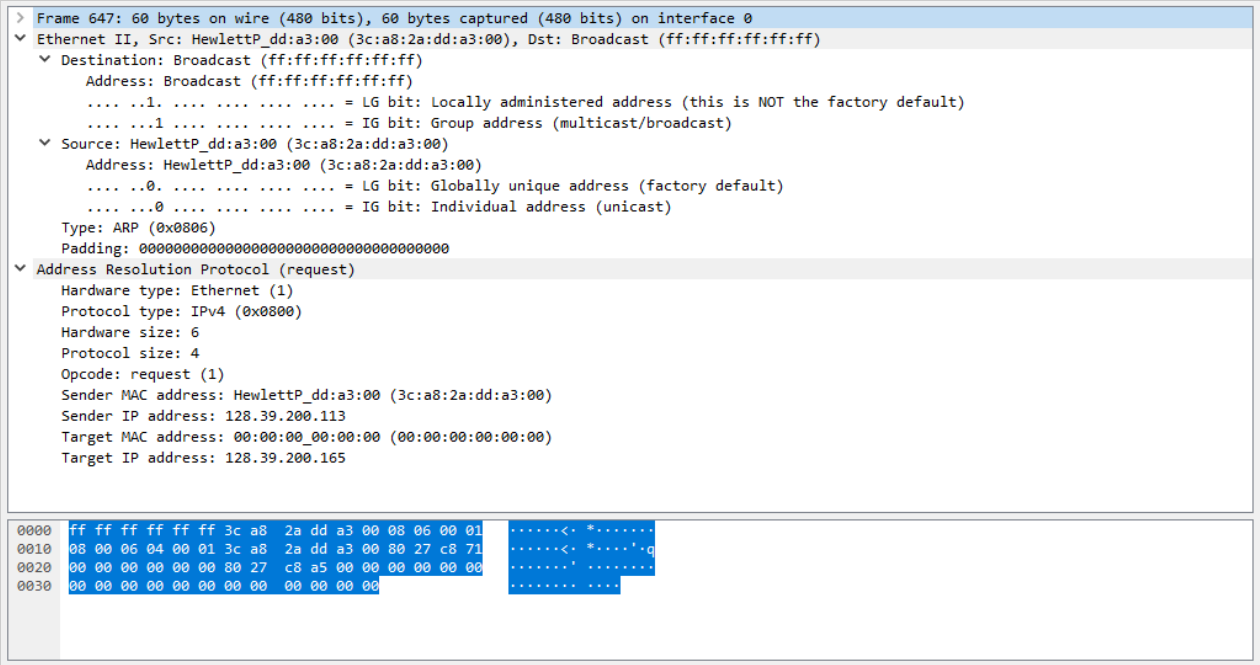
Ethernet switches are Select alternative (complex, fast and quite expensive, simple, fast and

relatively inexpensive). They forward frames based on the destination's Select alternative

(host name, MAC address, IP address) and they have to Select alternative (get their switch tables configured by a network administrator, maintain their switch tables all by themselves, exchange information with other switches to update their switch tables).

Maximum marks: 8

13 IKT204-G V24, ARP



Review the Wireshark capture above and assess the claims below regarding the Address Resolution Protocol (ARP). (5 points)

Select correct alternatives:

- [ ] A host can only have one MAC address.
- [ ] A host can have multiple IP addresses and multiple MAC addresses. ✔
- [ ] A MAC address has a fixed length of 48 bits. ✔
- [ ] ARP is a protocol that reside somewhere between the network layer and the link layer in the Internet 5-layer model. ✔
- [ ] Hosts and routers use ARP to associate an IP address to a MAC address and maintain an ARP table in their memory. ✔
- [ ] A MAC address has a fixed length of 64 bits.
- [ ] ARP broadcast address is ff:ff:ff:ff:ff:ff. ✔
- [ ] ARP replies always use the broadcast address as destination address.
- [ ] Host with IP address 128.39.200.165 has MAC address 3c:a8:2a:dd:a3:00.
- [ ] ARP requests ends up in a ARP server which will assign a MAC address to the requesting host.
- [ ] The MAC address of a host (client) in a LAN is encapsulated in the link layer frames it sends and follows the frames all the way to a host (server) in another LAN.
- [ ] ARP broadcast address is 00:00:00:00:00:00.

Maximum marks: 5

14 IKT204-G V24, Transfer delay

A gamer in Honningsvåg is connected to a Massively Multiplayer Online (MMO) server in Oslo. The transfer link from Honningsvåg to Oslo is 1620 km long and the propagation speed in the link medium is 200 000 km/s. The player has a 50 Mbps internet connection, and all routers and switches have high capacity, low load and negligible transmission delay. The game exchanges state messages of 434 bytes over TCP between clients and the server. Assume that TCP header is 20 bytes, IP header is 20 bytes, and the link layer overhead (Ethernet framing) is 26 bytes, and that each game message is sent in separate TCP segments to increase interactivity. (4 points)

What is the length of the link layer frame in ***bits***? [ ] (4000) bits

How large is the transmission delay in ***microseconds*** in this scenario? The answer is given without decimals: [ ] (78 - 82) µs

How large is the propagation delay in ***milliseconds*** in this scenario? The answer is given with 1 decimal: [ ] (7.9 - 8.3) ms

What is the minimum round-trip time (RTT) in ***milliseconds*** for the game? The answer is given with 2 decimals: [ ] (15.95 - 16.77) ms

---

Maximum marks: 4

15 IKT204-G V24, Wireless concepts and Wi-Fi LAN

Below are some general statements about wireless transmission as well as some more specific statements about how wireless IEEE 802.11 (Wi-Fi) LANs function. (9 points)

Fill in the correct term in each sentence:

Attenuation of the wireless signal when travelling through matter is called Select alternative (phase shifting, path loss, multipath propagation, modulation, interference).
When two or more sources within a basic service set (BSS) transmit at the same time on the same frequency then Select alternative (multipath propagation, path loss, modulation, phase shifting, interference) may occur.
Blurring of the received signal due to several reflections of the electromagnetic wave from objects and ground is called Select alternative (multipath propagation, interference, modulation, path loss, phase shifting).

In Select alternative (infrastructure mode, de facto mode, data mode, ad-hoc mode) each wireless host is connected to the Internet via an access point (AP).

In Select alternative (de facto mode, data mode, infrastructure mode, ad-hoc mode) wireless hosts themselves provide routing, address assignment and DNS-like services.

Wireless 802.11 (Wi-Fi) LAN uses a Select alternative (Carrier Sense Multiple Access (CSMA), Code Division Multiple Access (CDMA), Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA)) protocol with a Select alternative (collision detection mechanism (CD), first come, first served mechanism (FCFS), best possible signal-to-noise ratio mechanism (SNR), collision avoidance mechanism (CA)).
Wireless stations discover and identify the 802.11 (Wi-Fi) access point (AP) using Select alternative (RTS, beacon, CTS, SIFS, DIFS, broadcast) frames.

A Select alternative (broadcast, DIFS, SIFS, RTS, CTS, beacon) frame gives the 802.11 (Wi-Fi) transmitter of the Select alternative (SIFS, CTS, broadcast, RTS, beacon, DIFS) frame explicit permission to send.

A 802.11 (Wi-Fi) station that has gone to sleep mode will Select alternative (only wake up when it has something to send, wake up regularly to receive beacon frames, wake up regularly to ask the access point (AP) if it has frames waiting).

Wireless 802.11 (Wi-Fi) LAN operates on the Select alternative (1.8 GHz and 4 GHz, 2.4 GHz and 5 GHz, 3.5 GHz and 7 GHz) ISM bands.

Maximum marks: 9

16 IKT204-G V24, SSL socket and cryptographic algorithms

```
import socket
import ssl

name = 'localhost'
port = 8443
sslCtx = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
sslCtx.load_cert_chain(certfile = 'ca.crt', keyfile = 'private.key')
ls = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ls.bind((name, port))
ls.listen(1)

while True:
    cs, addr = ls.accept()
    print(cs.getpeername())
    sslSock = sslCtx.wrap_socket(cs, server_side = True)
    print(sslSock.cipher())
    while True:
        data = sslSock.recv(1024)
        if not data: break
        sslSock.sendall(data)
    sslSock.shutdown(socket.SHUT_RDWR)
    sslSock.close()
```

Here is a Python script that has printed ('127.0.0.1', 17425) as well as the negotiated cipher suite ('ECDHE-RSA-AES256-GCM-SHA384', 'TLSv1.2', 256) when it has been run. Below are some statements about this script and the cipher algorithms that were used in this session. (10 points)

Select correct alternatives:

- [ ] AES in Galois/Counter Mode with 256-bit key was used to encrypt the exchanged application messages, as well as to authenticate and verify the integrity of the messages. ✔
- [ ] AES is a one-way function and was used to make a digest (hash) of the messages sent.
- [ ] The server has port number 17425.
- [ ] SHA is a one-way function and produces a hash of specified size 384 bits. ✔
- [ ] The script shows a client that returns received data on port 8443.
- [ ] The negotiation protocol used was Transport Layer Security version 1.2. ✔
- [ ] SHA was used to make a digest (hash) of the exchanged TLS handshake messages in order to verify that they have not been tampered with. ✔
- [ ] The key exchange parameters were signed with the server's public RSA key.
- [ ] The key exchange parameters were signed with the server's private RSA key. ✔
- [ ] A digital certificate was used in this session to authenticate the server. ✔
- [ ] The client had port number 17425. ✔
- [ ] The script shows a server that is listening on port 8443. ✔
- [ ] ECDHE including a session authentication key ensured data integrity.
- [ ] The secret keys for the session were exchanged with RSA.
- [ ] A cryptographic digest (hash) ensures data confidentiality.
- [ ] A digital certificate was used to sign all the messages exchanged during this session.
- [ ] The secret keys for the session were created with the method Diffie-Hellman key exchange over elliptic curves. ✔
- [ ] Symmetric-key encryption ensures data confidentiality. ✔
- [ ] SHA with 384-bit key was used to encrypt the exchanged application messages.

Maximum marks: 10

17 IKT204-G V24, Comments and assumptions

Here you can write assumptions, clarifications and comments to your answers. These comments do not give additional points themselves, but may influence the judgement of commented assignments. (max 500 words)

Write assumptions and comments to the assignments here:

Format

Words: 0

Maximum marks: 0

Question 2
Attached

Start of session:

No.	Time	Source	Destination	Protocol	Length	Info
61	1.684489	128.39.200.255	85.165.93.169	TCP	66	60104 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
65	1.698851	85.165.93.169	128.39.200.255	TCP	66	80 → 60104 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=128
66	1.698973	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
77	1.758497	128.39.200.255	85.165.93.169	HTTP	528	GET /assets/delta-vod-webapp.js.gz HTTP/1.1
83	1.772638	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [ACK] Seq=1 Ack=475 Win=30336 Len=0
87	1.776730	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=1 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
88	1.776732	85.165.93.169	128.39.200.255	TCP	316	80 → 60104 [PSH, ACK] Seq=1401 Ack=475 Win=30336 Len=262 [TCP segment of a reassembled PDU]
89	1.776817	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=1663 Win=65792 Len=0
93	1.779707	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=1663 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
94	1.779708	85.165.93.169	128.39.200.255	TCP	194	80 → 60104 [PSH, ACK] Seq=3063 Ack=475 Win=30336 Len=140 [TCP segment of a reassembled PDU]
95	1.779786	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=3203 Win=65792 Len=0
99	1.781707	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=3203 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
100	1.781707	85.165.93.169	128.39.200.255	TCP	114	80 → 60104 [PSH, ACK] Seq=4603 Ack=475 Win=30336 Len=60 [TCP segment of a reassembled PDU]
101	1.781775	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=4663 Win=65792 Len=0
105	1.784687	85.165.93.169	128.39.200.255	TCP	1454	80 → 60104 [ACK] Seq=4663 Ack=475 Win=30336 Len=1400 [TCP segment of a reassembled PDU]
106	1.784689	85.165.93.169	128.39.200.255	TCP	114	80 → 60104 [PSH, ACK] Seq=6063 Ack=475 Win=30336 Len=60 [TCP segment of a reassembled PDU]
107	1.784744	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=475 Ack=6123 Win=65792 Len=0
111	1.786679	85.165.93.169	128.39.200.255	TCP	662	80 → 60104 [PSH, ACK] Seq=6123 Ack=475 Win=30336 Len=608 [TCP segment of a reassembled PDU]

```
> Frame 66: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: LcfcHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)
v Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x54d9 (21721)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.39.200.255
    Destination: 85.165.93.169
v Transmission Control Protocol, Src Port: 60104, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 60104
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
    Checksum: 0xfc8f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

End of session:

No.	Time	Source	Destination	Protocol	Length	Info
329	2.066686	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1019 Ack=113978 Win=65024 Len=0
330	2.082790	128.39.200.255	85.165.93.169	HTTP	608	GET /api/delta/fan/status HTTP/1.1
333	2.098738	85.165.93.169	128.39.200.255	HTTP	483	HTTP/1.1 200 OK (application/json)
336	2.138861	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1573 Ack=114407 Win=64512 Len=0
602	7.007701	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [FIN, ACK] Seq=114407 Ack=1573 Win=32512 Len=0
603	7.007777	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [ACK] Seq=1573 Ack=114408 Win=64512 Len=0
609	7.273461	128.39.200.255	85.165.93.169	TCP	54	60104 → 80 [FIN, ACK] Seq=1573 Ack=114408 Win=64512 Len=0
611	7.287815	85.165.93.169	128.39.200.255	TCP	60	80 → 60104 [ACK] Seq=114408 Ack=1574 Win=32512 Len=0

```
> Frame 330: 608 bytes on wire (4864 bits), 608 bytes captured (4864 bits) on interface 0
> Ethernet II, Src: LcfcHefe_8c:69:eb (50:7b:9d:8c:69:eb), Dst: Cisco_ff:fd:90 (00:08:e3:ff:fd:90)
v Internet Protocol Version 4, Src: 128.39.200.255, Dst: 85.165.93.169
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 594
    Identification: 0x5529 (21801)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.39.200.255
    Destination: 85.165.93.169
v Transmission Control Protocol, Src Port: 60104, Dst Port: 80, Seq: 1019, Ack: 113978, Len: 554
    Source Port: 60104
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 554]
    Sequence number: 1019    (relative sequence number)
    [Next sequence number: 1573    (relative sequence number)]
    Acknowledgment number: 113978    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 254
    [Calculated window size: 65024]
    [Window size scaling factor: 256]
    Checksum: 0xfeb9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (554 bytes)
v Hypertext Transfer Protocol
  > GET /api/delta/fan/status HTTP/1.1\r\n
    Host: fanctrl.andersenitc.no\r\n
    Connection: keep-alive\r\n
    Accept: application/json, text/plain, */*\r\n
    DateX: Mon, 26 Nov 2018 07:55:58 GMT\r\n
    Authorization: None\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36\r\n
    Referer: http://fanctrl.andersenitc.no/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: nb,en-US;q=0.9,en;q=0.8\r\n
  v Cookie: _ga=GA1.2.870541523.1517819979; _biz_uid=cd6799c7fb3a4913b32c5dc59832da5d; _biz_nA=3; _biz_pendingA=%5B%5D\r\n
      Cookie pair: _ga=GA1.2.870541523.1517819979
      Cookie pair: _biz_uid=cd6799c7fb3a4913b32c5dc59832da5d
      Cookie pair: _biz_nA=3
      Cookie pair: _biz_pendingA=%5B%5D
    \r\n
```