ICMP messages are encapsulated directly in UDP messages.

* False (ICMP runs directly on top of IP)

In the Integrated Services (int-serv) model, application data for a reserved flow is carried in RSVP (Resource Reservation Protocol) messages.

* False (RSVP is used to set up the reserved flow)

Multicast Source Discovery Protocol (MSDP) is a protocol for   
sharing information between routers to transport IP Multicast   
packets, and it is based on RIP for forwarding of packets.

* False (MSDP is not based on RIP)与RIP无关，是PIM协议

Real-Time Streaming Protocol (RTSP) is used to carry real-time   
data such as audio and video.

* False (RTSP is for control information only) 该协议定义了一对多应用程序如何有效地通过 IP 网络传送多媒体数据

If a bridge becomes overloaded and is not able to handle all packets,   
why is it important that the bridge is still able to process spanning   
tree configuration messages?   
Answer:   
If a bridge is not able to handle spanning tree configuration messages   
it will not be able to maintain the spanning tree properly. This could

lead to forwarding loops in the in the LAN which, resulting in   
multiplication of traffic, which could bring the whole down.

Why are temporary loops in a bridged network more problematic than   
temporary loops in a routed network?   
Answer:   
There are two main reasons for this:   
• There is no hop count field in the data link header, so packets will   
loop indefinitely until the topology stabilizes.   
• Packets in a bridged network can proliferate since a bridge may   
forward a packet onto several LANs. Routers forward a packet in one direction to a specific next hop, i.e., there is no packet proliferation.

Briefly explain the difference between routing and forwarding.   
Answer:   
Routing is the process of finding out the best path to a destination. Forwarding is the actual moving of packets from an incoming interface to an outgoing interface.

Within a domain, both an interior and an exterior routing protocol may be used. What is the purpose of redistributing routes between these protocols?   
Answer:   
Interior routes may need to be advertised to the Internet (typically   
the interior routes will be aggregated). Exterior routes (normally a subset) may need to be injected into the interior network, e.g., for domains carrying transit traffic.

How is packet forwarding in MPLS different from IPv4 packet forwarding?   
Answer:   
In MPLS, the forwarding is based on a small fixed-size label. In IPv4,   
forwarding is based on the destination IP address and longest prefix   
match.

PIM stands for Protocol Independent Multicast and is a multicast   
routing protocol. Explain what it means that PIM is “protocol independent”.   
Answer:   
The “protocol independent” part refers to the fact that PIM does not   
include its own topology discovery mechanism, but instead uses routing information supplied by other traditional unicast routing protocols (such as OSPF or BGP)

Kazaa (and several other peer-to-peer applications) uses a distributed hash table (DHT). What is the DHT used for and why should the hash   
table be distributed?   
Answer: hash table的作用  
The DHT is used for mapping file identifiers (names) to locations (IP addresses). By making the hash table distributed, the method scales very well with an increasing number of users and single point of failures are avoid.

Briefly describe how real-time applications normally deal with network induced delay jitter. For full score you should be able to explain the mechanism and the suitable protocol support.   
Answer:   
Normally, a playback buffer is used on the receiver side so that data can be somewhat delayed and played out at the correct pace.

Suitable protocol support is to make it possible for the sender to communicate “time stamp” and “sequence number” for the data units (as in RTP).

Ethernet is a point-to-point link technology.

* False (Ethernet is a broadcast link technology)

STP (Spanning Tree Protocol) results in optimized routing.

* False (Traffic concentrates towards the root)

RSVP is described as a receiver-oriented protocol. What does that   
mean? (1p)

* The receiver is responsible for requesting resource reservations.

What transport protocol does ICMP use?

* None, ICMP is encapsulated directly in IP

OSPF (Open Shortest Path First) consists of three different   
protocols. Which ones?

* The Hello protocol, the Exchange protocol, and the Flooding   
  protocol

What does “torrent” mean in the context of BitTorrent?

* The collection of all peers participating in the distribution of a particular file.

Describe the difference between static and dynamic routing.

Answer:

Static routing is configured by the network administrator and is not capable of adjusting to changes in the network without network administrator intervention.

Dynamic routing adjusts to changing network circumstances by analyzing incoming routing update messages without administrator intervention.

Integrated services (int-serv) and differentiated services (diff-serv) are two different IETF approaches for quality-of-service in IP networks. How do these two approaches differ when it comes to allocation of resources?   
You only need to mention the overall principle.   
Answer:   
Integrated services: resources are allocated on a per-application basis.   
Differentiated services: resources are allocated on a per-class basis

Explain how the RPF mechanism works in IP multicast. What happens when the RPF check passes and when the RPF check fails?

Answer:

When a multicast packet enters a router's interface it will lookup the list of networks that are reachable via that input interface i.e., it checks the reverse path of the packet. If the router finds a matching routing entry for the source IP of the multicast packet, the RPF check passes and the packet is   
forwarded to all other interfaces that are participating in multicast for this multicast group. If the RPF check fails the packet will be dropped. As a result the forwarding of the packet is decided based upon the reverse path of the packet rather than the forward path.

A. What is the advantage of using query flooding for locating   
content comparing to using a centralized directory. (1p)   
B. What is the drawback of query flooding? (1p)   
C. Explain the technique called “rarest first” used for requesting chunks in BitTorrent? (1p)   
D. How does a BitTorrent client know which peers have the file it wants? (1p)   
Answer:   
A. Query flooding is fully distributed, thus no single point of failure.   
B. It is not scalable since flooding introduces a significant amount of traffic into the network.   
C. The technique is used to determine the chunks that are the rarest   
(i.e. chunks that have the fewest repeated copies among the   
neighbors) among the neighbors and then request those rarest   
chunk first.   
D. A torrent client will contact the tracker for list of peers who have the file.

Diff-serv is a more coarse-grained model of IP QoS compared to Int-serv.

In IPv6, only hosts are allowed to fragment IP datagram.

An L1 VPN provides a transparent connection service.

RTSP (Real-Time Streaming Protocol) defines a standardized way to   
encapsulate audio/video data in packets.(正确答案是RTP)

* False (it is a protocol for exchanging control information).

What is the purpose of a CDN (Content Distribution Network)   
distribution node?

To replicate and push content to selected CDN servers.

In BitTorrent, how does a peer determine which requests to serve first?

The peer will give priority to neighbors currently supplying data at the highest rate.

How does the TCP congestion window increase in size during “slow start” and “congestion avoidance” respectively?

The congestion window increases exponentially during slow start   
and linearly during congestion avoidance.

In the past ten years, two new transport protocols have been   
standardized within IETF: SCTP and DCCP. What are the main characteristics of these two protocols that distinguish them from TCP and UDP, respectively?

Answer:   
SCTP inherits many of its features from TCP, but introduces multi-  
streaming to avoid head-of-line blocking in between different   
transactions, and multi-homing to realize highly available transport   
connections. Similar to UDP, DCCP is unreliable and message based. However, unlike   
UDP, DCCP is congestion aware and provides for a connection to   
dynamically select a suitable congestion control mechanism.

Many peer-to-peer network applications make use of so-called Distributed Hash Tables (DHTs) for their operation. What is the principal idea behind a DHT, and in what way does a DHT differ from an ordinary hash table?

Answer:   
The principal idea behind a DHT is the same as for a hash table: to be able to insert, and delete large amounts of information associated with keys. However, the concept of “bucket” is now replaced by a physical node, which could be located anywhere globally (distributed). Keys are hashed, and the hashed keys are mapped to the nodes according to the DHT algorithm; the nodes hold the key and value pairs.

Ethernet VPWS (Virtual Private Wire Service) and VPLS (Virtual Private LAN Service) are two different types of Ethernet VPNs. What is the difference between their services?   
Answer:   
Ethernet VPWS: provides a virtual link service where the VPN appears as a point-to-point circuit.

VPLS: provides a virtual switch service where the VPN appears as a (distributed) Ethernet switch, or learning bridge.

A. You are writing an application to send interactive unicast real-  
time audio over the Internet, such as an IP telephony service.   
Should you use TCP or UDP as your transport protocol? Briefly   
motivate you answer. (2p)

B. You are writing an application to send video files over IP   
multicast. Is it possible to use TCP as your transport protocol?   
Briefly motivate your answer. (1p)

C. What is the difference between offered window and usable window in TCP? (2p)   
Answer:   
A. The preferred choice is UDP. TCP provides retransmissions and a reliable service. This may give extra delay that is undesirable for such an application.

B. No. TCP is not defined for IP multicast transmissions.

C. The offered window is advertised by the receiver and defines how   
much data the receiver is ready to accept. The usable window is   
maintained by the sender and defines the amount of data the   
sender can transmit immediately.

OSPF and IS-IS are both based on link state routing.

UDP doesn’t provide an optional flow control.(可选checksum校验)

DCCP provides an unreliable congestion-controlled transport service.

Diff-serv typically provides IP QoS guarantees for individual   
application traffic flows.

* False. Diff-serv面向class, int-serv 面向individual

IPv6 has a stronger checksum compared to IPv4

* False. IPV6没有checksum

RTP includes a mechanism to ensure timely delivery of data to the   
receiving host.

* False. 没有mechanism to ensure timely delivery.

Mention briefly what RTSP is used for？

RTSP is a protocol for exchanging playback control information   
(pausing, fast forwarding, rewinding, etc

IP fragmentation is handled differently in IPv6 compared to IPv4. How   
is it different and what is the motivation for this change? Why is reassembly always done at the receiver?

Answer:   
IPv6 does not allow for fragmentation by the intermediate routers. This operation is done only by the source. Fragmentation is a time-consuming process, so removing this from the routers releases the burden on the network. Reassembly has to be done at the receiving host since different fragments may take different paths through the network. A router can thus not be assumed to receive all fragments of a packet.

Explain what multi-homing means in the context of SCTP. Why is this a problem in TCP?   
Answer:   
Multi-homing in SCTP means that SCTP allows the end points of a single association to have multiple IP addresses. In SCTP, each of the two endpoints can associate with multiple points of attachment during an SCTP association setup. A TCP connection can only bind a single point of attachment at each end point so it cannot support this type of multi-homing.

Explain the meaning of a tit-for-tat strategy in the context of peer-to-peer networking. How is this strategy beneficial for swarms in a P2P network?

Answer:

In a P2P context, tit-for-tat strategy is a strategy to optimize

download speed between peers. A peer assigns upload slots to random

peers and keeps uploading to the peers from which it gets faster

download speeds. This strategy introduces an incentive for peers to

upload data to other peers at high speed, increasing the total upload capacity of the swarm.

Explain how congestion control works in TCP. You should cover:

• How congestion occurs and how TCP would act without congestion

control

• The different phases of congestion control

• How the size of the sender’s window changes during the two

different phases.

Answer

Congestion can occur in the network when it is overloaded. For example,

buffers in routers are of limited size, and when the router is running out of buffer space, packets will be dropped. For TCP, lost packets will result in lost ACKs. Lost ACKs will result in retransmissions, and this will add to the congestion in the network. To deal with congestion, the sender maintains 2 windows per TCP

connection: Receiver-advertised window and congestion window (CWND).

The actual window size used is the smaller of the two. Congestion control involves the following phases: Slow Start (exponential increase), congestion avoidance (additive increase), and congestion detection (multiplicative decrease). Initially, CWND is set

to 1 MSS (maximum segment size). During Slow Start, CWND increases

exponentially (increases 1 MSS for each ACKed segment). The Slow Start phase continues until CWND has reached a threshold value. Thereafter, the Congestion Avoidance phase takes over. During Congestion Avoidance phase, CWND increases linearly. The linear growth will continue until either the receiver-advertised window is reached or congestion occurs. When congestion is detected, the window size is decreased multiplicatively, either to one MSS or to half the previous value

IK2215 Advanced Internetworking (depending on whether Fast Retransmit and Fast Recovery is used or not).

If an IP packet is fragmented, the destination system is the only   
place where reassembly occurs.

RTSP (Real-Time Streaming Protocol) provides time stamps and   
sequence numbers for proper playback of received data.

* False 应该为RTP协议

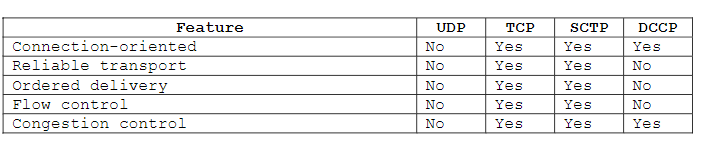
BitTorrent uses a central tracker to handle peer discovery. (1p)

What is the purpose with using “rarest chunk first” in BitTorrent?

To achieve good replication of data.

An OSPF router has just built an LSA (Link State Advertisement).   
Where does it send the LSA?

To all other OSPF routers in its area.



IP multicast address to Ethernet multicast address mapping is not   
unique. What implication does this have on the IP and how is it solved?   
Answer:   
It means that IP may receive multicast packets for which there is no receiving process. Such packets are filtered out in software by the IP layer (based on IP multicast address).

Briefly describe what each of the following IP QoS terms mean (you should not use more than 20 words per term):   
• Classification   
• Policing   
• Shaping   
• Scheduling   
Answer:   
Classification   
– Identifying the packets belonging to a certain traffic flow   
Policing   
– Ensure that the flow conforms to a traffic specification   
Shaping   
– Smoothing out packet bursts (traffic is often bursty)   
Scheduling   
– Manage packets in queues so that they receive desired service

BGP uses UDP as the transport service to reduce complexity

* False. BGP使用TCP

In IP QoS, the term “policing” means to ensure that a traffic   
flow conforms to the traffic specification

In IPv6, only the sender of an IP datagram is allowed to do   
fragmentation.

A multicast router is said to listen promiscuously to all   
multicast addresses.

BitTorrent does not support uploading while downloading

* False

What is the main task of a CDN distribution node?

To replicate content and push it to selected CDN servers.

What do we call the mechanism(机制) that BitTorrent uses to favor “good” peers?

Tit-for-tat exchange.

What does it mean that RSVP maintains “soft state” in hosts and   
routers?

That any state will automatically expire（过期） unless it is refreshed periodically.

One of the underpinning principles behind TCP congestion control is the so-called “self-clocking” principle. Briefly explain the meaning of this principle.   
Answer:   
The answer should include the key observation that in equilibrium, the acknowledgements return to the sender at about the rate that packets can be sent over the slowest link in the path.

BitTorrent makes use of a technique called “speculative upload”. What are the two main purposes for using speculative upload? Also, mention a disadvantage/risk with speculative upload.   
Answer:   
The two main purposes with speculative upload are:

1) To find better peers

2) To give new peers a chance to join.

A disadvantage with speculative upload is that it can be exploited by   
free-riders.

What are the main drawbacks with the integrated service model for   
IP quality of service?

Answer:

The end-to-end connection set-up and the resource reservations on a per flow basis make int-serv very unpractical (impossible) to scale. There could literally be millions of flows to keep track of, each requiring its own buffer. The required state per flow in each router along the path is very costly for router.

In RIP, each node calculates the shortest past based on first   
hand information about the network topology.

* False RIP 使用distance-vector

IPv6 uses a fixed size header format and extension headers are   
used instead of IP options in IPv4.

The mapping between IP multicast addresses and Ethernet multicast   
addresses is not unique—in fact several IP multicast addresses   
can be mapped to the same Ethernet multicast address.(IP组播地址和以太网组播地址映射不唯一)

The purpose RTP (Real-time Transport Protocol) is to guarantee a   
low delay between sending and receiving host

* False

BitTorrent uses a central directory to locate files。

* False， 没有中央目录

What mechanism do CDNs typically use to allow users to find the   
most suitable server?

DNS redirection.

An IP multicast packet arrives to a router and the router does reverse path forwarding. What address does the router then use for lookup in the forwarding table?

The source address of the multicast packet.

What is the overall purpose of RSTP (Real-Time Streaming   
Protocol)?

To exchange playback control information (play, stop, rewind   
etc).

What is flooding used for in OSPF?  
To distribute LSAs (Link State Advertisements) to all routers in   
the network (area).  
What is a “token bucket” in the context of IP QoS?

A way to represent the bandwidth characteristics of a variable   
data rate.

In deciding what chunks to request when using BitTorrent for file distribution, a method called rarest chunks first is used. Explain two advantages with the rarest chunk first technique.   
Answer:   
The two main advantages are: 1) To get good replication of data in the swarm 2) Increase the chance to get chunks that others want—good for “tit-for-tat”

In IPv6, IP fragmentation is done differently than in IPv4. Explain the changes that have been made in this regard. Your answer should cover where fragmentation can be performed, where reassembly is performed, and what support that might be needed to do fragmentation differently in IPv6 compared to IPv4.   
Answer: IPv4 IPv6的fragmentation  
In IPv4, fragmentation can be done both by the sender and by the routers along the path between sender and receiver (hop-by-hop.

In IPv6, IP fragmentation can only be done by the sending host and path MTU discovery can be used by the sender to   
determine the smallest MTU between sender and receiver.

In both IPv4 and IPv6, reassembly is done by the receiver

Briefly explain the process (including the messages involved) of how an IPv6 host obtains its IPv6 address using stateless address   
autoconfiguration.   
Answer: Stateless address autoconfiguration in IPv6  
First the host creates an IPv6 with the link local prefix and its own   
MAC address.

Then:

1. A Multicast listener report. The host starts to listen on the multicast address associated with the link local address it intends to use.

2. A Neighbor Solicitation request sent to that multicast address. (If another host has already been configured with the same link local address that host would also listen to this multicast address and send a Neighbor solicitation reply back to the same multicast address.)

3. A Router Solicitation request. It looks for a router on the link   
to advertise a link prefix (in order to form a global IPv6   
address).

4. The router replies to the router solicitation. (Thereby the   
client can form a global IPv6 address)

5. The host sends another DAD message to the associated multicast address. But this time it sends ICMPv6 with the global address as target address.

UDP will discard a datagram with checksum errors on the receiver   
side without sending feedback to the sender

MSDP can be used to interconnect multiple IPv4 PIM-SM domains

因为都是group-shared tree

In IPv6 the IP address identifies the host instead of a network   
interface card as in IPv4

* False，使用的还是interface IP

Is the EEE (Energy-Efficient Ethernet) standard based on rate   
switching (switch to lower tranimssion rate when possible) or   
low-power idle (sleep between packets when possible)?

G. EEE uses low-power idle.

BGP is neither based on link state nor on distance vector.   
Instead BGP uses path vector. How is this different from distance   
vector?

A distance vector give the cost (distance) to each network.   
Instead of just the cost, BGP adds an AS path to every network it   
advertises.

In a large subnet there could be many simultaneous receivers of the same multicast group. When a router sends an IGMP query, this could then generate a large amount of IGMP reports. How is this avoided in an IGMP implementation?   
Answer: IGMP重复报文避免

IGMP reports are sent to the group address. The hosts can then snoop for other host’s IGMP reports. So, before sending its IGMP report a host will set a random timer and suppress its IGMP report if it detects that another host on the same subnet sends the report for this group

Int-serv (Integrated Services) and diff-serv (Differentiated Services) can be used to provide quality of service (QoS) for multimedia applications in IP networks. What are the main problems with int-serv and how are they addressed in diff-serv?   
Answer:   
The main problem with int-serv are that it requires end-to-end   
connection setup and resource reservation. Thus, for int-serv to work, all the routers along the traffic path must support it. Routers need to keep per-flow state information, which is not scalable.

In diff-serv, traffic flows are aggregated into a small number of classes. All packets belonging to the same traffic class get the same treatment in the diff-serv network. diff-serv requires no advance setup, no reservation, and no time-consuming end-to-end negotiation for each flow.

Assume two skype users, where each user is connected to his/her own private network behind a NAT (Network Address Translation) box. The NAT arrangement prevents hosts from outside the private network to initiate connections to hosts inside the private network. Still, skype will work without requiring the users to configure the NAT boxes for incoming calls. Describe the technique that skype uses to achieve this.   
Answer: Skype and super peers  
Skype uses super peers and relay nodes to solve the problem. When a skype user signs in on skype from his/her private network the user is assigned a non-NATed super peer. Sessions can then be initiated to the super peers, who inform each other and the calling parties. If the call is accepted, a public non-NATed relay node is selected: Bob—relay node—Alice.

Multipath TCP (MPTCP) is a set of extensions to standard TCP that are   
currently underway to become standardized by the Internet Engineering Task Force (IETF).

A. Give two design goals of MPTCP. (2p) B. Explain the resource pooling principle and how MPTCP adheres to   
this principle. (2p) C. Why does MPTCP employ coupled congestion control? (1p)   
Answer: MPTCP  
A. At least two of the following goals: improve throughput, i.e., should perform at least as good as a single-path flow over the best of the available network paths; improve resilience, i.e., should permit packets to be sent and re-sent on any available network path; do not harm, i.e., should not impede performance on other regular TCP flows; balance congestion, i.e., move traffic from the most to the least congested network paths; application compatible, i.e., provide the same API and service model to applications as standard TCP.

B. The resource pooling principle states that the network's   
resources should behave as though they make up a single pooled   
resource. MPTCP adheres to this principle by making it possible   
for a single TCP connection to consist of several network paths

C. Otherwise, an MPTCP multi-subflow connection would compete   
unfairly with competing standard TCP flows when the MPTCP   
subflows and the TCP flow go over the same link.   
   
RTP (Real-time Transport Protocol) provides a mechanism to   
guarantee delay-bounds between two hosts.

* False RTP没有这个东西

In Gnutella, an infrastructure node called tracker was introduced   
to keep track of the peers in an overlay network.

* False

Mention one (technical) drawback with a centralized directory   
architecture for peer-to-peer networking.  
It is a single point of failure and a performance bottleneck.

Setting the playback point in a playback buffer is basically a   
tradeoff between two parameters. Which ones?

It is a tradeoff between packet loss and latency.

What does BGP use to detect and prevent loops?

AS Path.

Briefly describe the overall difference between TCP flow control and TCP congestion control.   
Answer:   
TCP flow control (sliding windows) is a way for the receiver to throttle the sender so that the receiver doesn’t get overwhelmed with data.

The purpose with TCP congestion control is to make the sender   
adapt to the network conditions (so that routers don’t get overloaded.

Assume that you use anycast RP (Rendez-vous point) with two RPs with PIM sparse mode within your network. What problem could arise in this situation? How can you solve this problem?

Answer: MSDP  
A multicast source may register with one RP and receivers may join to a different RP. In this situation, a method is needed for the RPs to exchange information about active sources. You can run MSDP between the RPs to share information about active sources

a) A programmer is about to implement an application for streaming of stored multimedia content. She selects TCP as the transport protocol. Explain why that might be a good choice. (1p)

b) Her application includes both a web client and a media player. What is the purpose with each of these parts? (1p)   
Answer:   
a) Firewalls often block UDP traffic. TCP will ensure that the   
complete file is downloaded without errors and it can then be   
cached locally at the receiver.

b) The web client is used to request information and the media player is for display and control of the audio/video.

A video source is generating video frames of size 10,000 bytes at a constant rate of 25 frames per second. The frames are transmitted over a network with 1 Gb/s Ethernet links, and arrive at the receiver with a maximum jitter (delay variation) of 200 milliseconds.

A. What is the minimum size of the playback buffer in order to ensure smooth playback of the video stream at the receiver? (2p) B. The video frames are encapsulated in RTP and then transmitted over UDP. What is the reason for using RTP on top of UDP? What does it provide, that UDP does not? (1P)

C. Consider the statement “A TCP connection has large variations in   
delay because of its error control, flow control and congestion   
control mechanisms. Therefore, it cannot be used for multimedia   
communication.” Do you agree with the conclusion? Explain you   
answer. (2p)   
Answer: TCP实际上也可以用于多媒体  
A. The buffer needs to be large enough to compensate for the worst-  
case delay, which is 200 milliseconds, corresponding to 5 frames   
or 50,000 bytes.

B. RTP has support for timestamps (which can be used to synchronize   
playout) and sequence numbers (to detect packet loss or   
reordering).

C. No. In practice, it is not correct to say that TCP has unpredictable delay. Variations in delay might be larger for TCP than UDP, so it requires a larger playout buffer, but there are many applications that can tolerate longer variations, streaming video for instance.

A RIP router regularly sends its distance vector to all other   
routers in the network

* False RIP仅仅和neighbor交换

Gnutella query flooding can be described as a simple an elegant design. However, the desing has also been critized—for what?

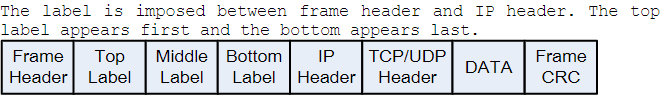
For not being scalable since it uses flooding.

Quick UDP Internet Connections (QUIC) is an experimental protocol proposed by Google and designed to provide security and reliability along with reduced connection and transport latency. a) What is the rationale behind the QUIC protocol? (1p) b) One of the major features of QUIC is that it reduces transfer   
delays. What is it mainly that gives QUIC shorter transfer delays   
compared TCP? (1p)   
Answer: QUIC  
a) Build an efficient and reliable transport protocol for Web/http-  
traffic that is deployable in today’s Internet. b) When QUIC is used, the connection setup time is at most one round-trip time; in the case the two parties involved in the connection has already talked to each other, the startup latency takes zero RTT.

Which protocol does a multicast router use to keep track of which host joins and which host leaves a group? Explain how this works in case of 1) joining a group and 2) leaving a group (you should describe which messages are sent from which entity to which entity).   
Answer: IGMP  
Internet Group Membership Protocol (IGMP) is used for this purpose. To join a group, a host sends a membership\_report message to the multicast router. To leave a group, a host may send an IGMPv2 leave\_group message, but this is optional. Thus, the router need to periodically send a membership\_query message to determine whether the host is still active in the group. The active hosts will reply with a membership\_report message.

a) DNS service: what does the root hints file in a DNS server   
normally contain? Why do we need it? (1p) b) Peer-to-peer: What architecture is used to locate content in Gnutella? What is the drawback in this method (1p)   
Answer:   
a) The root hints file contains host information (i.e. records for the root DNS servers on the Internet) that is needed to resolve   
names outside of the authoritative zones of the DNS server. b) To locate content, Gnutella uses query flooding to fine content   
from near by peers. Query flooding is not scalable. With limited flooding scope, it may not find the content within the near by peers.

Name and briefly describe the four fields of the MPLS label

Label field (20 bits) contains the actual value of the label.   
Traffic class field (3 bits) used to carry traffic class   
information. This is deined in RFC5462 to replace EXP field that   
was defined in RFC3032 as reserved for experimental use.   
Bottom of the stack (S) field (1 bit) that is set to one for the   
last entry in the label stack, and zero for all other label stack   
entries.   
Time to Live (TTL) field (8 bit) is used to encode a time-to-live   
value.  


If you look at the MPLS label table of the penultimate router, you may see implicit null (label 3) or explicit NULL (lable 0) labels. Explain what the difference is between using these different labels. You should mention one benefit in using each label and how it impacts the egress router. (2p)

**With implicit null**, the penultimate router will actually perform   
a pop operation and send the packet without an MPLS label to the   
egress router. This implies that the egress router only needs to   
perform an IP lookup to forward the packet without having to   
perform MPLS label lookup. Reducing the lookup task will enhance   
the performance of the egress router.

**With explicit null**, the penultimate router will forward the packet with MPLS label 0 to the egress router. This means that the egress router have to perform two lookups; one for the MPLS label lookup to figure out that the label should be removed, and the other for IP lookup of the actual packet. The main benefit of sending the MPLS label is that the egress router can derive the QoS information from the traffic class field.

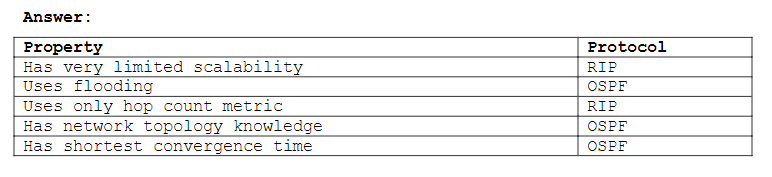
When TCP exits Fast Recovery, the congestion window is deflated   
to the size it had at the time Fast Recovery was entered. Why?  
Because Fast Recovery is typically exited by an acknowledgement   
that acknowledges all outstanding segments which is roughly the   
amount of segments contained in a window of the size TCP had when   
it entered Fast Recovery. By restoring the size of the congestion   
window, TCP avoids a burst of packets. Instead, packets continues   
to be ack-paced.  
BGP can use AS prepending to affect the routing of outgoing   
traffic

* False, 影响的是incoming traffic

MSDP can be used to interconnect multiple IPv4 PIM-SM domains.

6LowPAN is an adaptation layer designed for making it possible to run IPv6 on low-power constrained devices

Explain what “constrained devices” means in the context of Internet-of-Things.   
Answer: Internet-of-Things.  
Internet-of-Things is about connecting “non-computers” to the Internet. In contrast to regular computers, IoT devices are constrained in the sense that they are small units with very limited memory and CPU resources. IoT devices often have tiny operating systems with limited functionality and they need low-power communication technology.



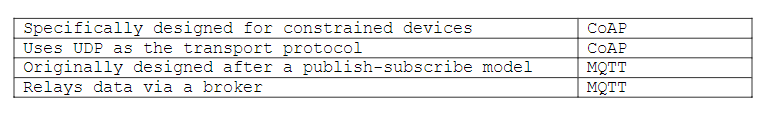
Make a detailed comparison between CoAP and MQTT and point out   
similarities and differences between these two protocols. You should consider things like overall purpose, message formats, transport protocol used, communication models, etc.   
Answer:   
MQTT and CoAP are both application layer protocols designed for IoT devices. They are both supposed to be suitable for implementations in tiny operating systems for IoT devices. CoAP implementations in particular can have a very small memory footprint. MQTT uses TCP as transport protocol (a variant of called **MQTT**-SN using UDP also exists) and is based on a publish-subscribe model. With publish-subscribe, the sensors can publish data to a broker whenever they wake up and have some data to share. The users will interact with the broker, which can be hosted on a server-like machine capable of serving large amounts of user requests.

**CoAP** uses UDP as transport protocol and is originally designed more like a client-server model using URI:s (such as coap://example.se:5683/~sensors./temp1.xml) to access the sensor data. As of last year a publish-subscribe communication model for CoAP has been suggested and is on its way to be standardized in IETF. CoAP has a small message size to fit in a minimum IPv6 MTU size.

IP multicast only works for link technologies with multicast-  
capable networking hardware, such as Ethernet

* False.

In a hierarchical peer-to-peer overlay network, flooding is   
normally limited to an overlay of super peers.



Inter-domain routing protocols are responsible for computing routes across Internet networks. A. Explain why RIP would not be a good inter-domain routing protocol. Mention two reasons. B. Are RIP and BGP guaranteed to converge to a stable routing state   
when operated in a static topology (i.e., no failures in the   
network)? Briefly motivate your answer.   
Answer:   
A. Reason 1: RIP does not support expressive enough ranking of   
routes, e.g., per-neighbor ranking. Reasons 2: RIP does not allow to filter or export routes in a selective manner.

B. RIP is a shortest-path distance-vector routing protocol. We   
proved in class that such protocols are guaranteed to converge to   
a stable routing in the absence of failures. In contrast, BGP is   
a policy-based path-vector protocol where operators are allowed   
to override the shortest-path best path selection with local-  
preferences over routes. When local-preferences among different   
networks are conflicting, the routing may never converge to a   
stable state.

Explain how the throughput of a TCP Reno connection is affected by the RTT between the sender and the receiver and the drop rate. How can a sender improve its own throughput when competing against a TCP connection with a smaller RTT?

For a single flow, the higher the RTT the lower the throughput.   
The higher the packet drop, the lower the throughput. A user   
could open multiple TCP connections to increase the throughput.

What problem of HTTP/2 does QUIC solve and how?

In HTTP/2 all streams are multiplexed within a single TCP   
connection. If there is a packet drop on one stream, all the   
other streams are also affected because TCP delivers packets in   
order. In QUIC, streams are multiplexed using UDP, which does not   
enforce packet ordering.

Hot Standby Router Protocol (HSRP) utilizes a virtual address to   
provide a fault-tolerant default gateway.

What is the overall idea with peer-to-peer networking when it   
comes to scalability?  
The more users that are connected, the more resources provided.

Arrange the following BGP attributes in their respective order as   
they are evaluated by the decision process: ORIGIN, AS\_PATH,   
MULTI\_EXIT\_DISC (MED), LOCAL\_PREF

LOCAL\_PREF, AS\_PATH, ORIGIN, MULTI\_EXIT\_DISC (MED)

What happens if a reserved flow in RSVP does not get refreshed in   
time?  
The resources of the reserved flow will then be released.

Describe the role of the DNS in a CDN. Does the DNS have to be modified to support a CDN? What information, if any, must a CDN provide to the DNS?   
Answer:   
The role of the DNS is to forward DNS queries to the authorativie DNS   
server managed by the CDN, which in turn redirects the request to an appropriate CDN server. The DNS does not have to be modified to support a CDN. A CDN should provide DNS with the host name and IP address of its authoritative name server.

A. Does the RTT influence the throughput of a TCP Reno connection? Explain intuitively why.

B. Explain how TCP BBR computes a model of the network path.   
Describe why there are four operations and why the operations   
cannot be performed simulataneously.   
Answer:   
A. Yes, the higher the RTT, the lower the throughput. TCP Reno increases the congestion window by 1 per RTT.

B. See slides 138 to 143 of the Transport lecture. The STARTUP and   
DRAIN operations cannot be performed simultaneously since the   
DRAIN operation is needed to remove the possible queue created by   
the STARTUP operation. The PROBE\_BW operation and the PROBE\_RTT   
operation cannot be performed at the same time since the minimum   
RTT must be estimated when the network is not congested, which is   
not the case if the protocol increases the transmission speed.

What is the main difference in terms of how resources are allocated in the int-serv model (Integrated Services) compared to diff-serv model (Differentiated Services)?   
Answer:   
In **int-serv,** resources are allocated on a fine-granular scale—resources can be reserved on a per-application level. Also, a resource reservation protocol is used (RSVP).

In **diff-serv**, a more coarse-grained approach is used where a small set of traffic classes are defined and resources are allocated on a per-class basis. No resource reservation protocol is used.

Explain what is the fundamental problem tackled by distributed hash tables. Explain why do we need hash functions in the design of a DHT.   
Answer:   
DHTs are distributed systems that provide a directory lookup service while requiring limited memory and low communication overhead. Hash functions are used to deterministically and uniformly spread a set of object identifiers into a smaller bounded space. This operation is key for spreading the resources of the directory system across all the peers in the system in a uniform manner.

The publish-subscribe model has several advantages in IoT scenarios. Illustrate and describe the publish-subscribe model in an IoT scenario where small sensor devices produce data that users are interested in. Your answer should include IoT devices and users who are interested in the data produced by the IoT devices. You should also compare the publish-subscribe model to the traditional client-server model and explain why the publish-subscribe model might be advantageous compared to running a server on the IoT devices.   
Answer:   
A sensor device is typically constrained and might not be capable to serve users who are requesting data from it. Furthermore, the sensor network can be a lossy and low-power network meaning that the sensor devices might be intermittently connected. Accordingly, the sensors are not very suitable to act as server in a traditional client-server model. With publish-subscribe, the sensors can publish data to a broker whenever they wake up and have some data to share. The users will interact with the broker, which can be hosted on a server-like machine capable of serving large amounts of user requests.

Explain the main differences between the control and the data   
planes. What are their responsibilities? What is the order of   
magnitude at which they operate? Where are they typically deployed: hardware of software? Motivate your answers

Slide 26 of the Routing lecture. The forwarding plane is faster than the control plane because it needs to forward the actual traffic used by the users' applications. The control plane performs at a slower rate as it does not need to compute the forwarding path for each single new packet entering traversing a network. The control plane is implemented in software since it does not need performance. The data plane has been traditionally implemented in hardware since we need speed. Recently, many implementations of the data-plane have been realized in software as it supports more flexible forwarding operations

Describe how link-state routing protocols work. Compare link-  
state routing protocols to distance-vector ones in terms of   
memory occupancy.  
See slides 29 to 35 of the Routing lecture. Link-state protocols needs to store the entire topology and a mapping between IP prefixes and routers connected to these IP prefixes. Distance-vector protocols need to store the best route learnt by each neighbor.

Why do OSPF require messages to be flooded in a reliable manner?   
Why is OSPF not implemented on top of TCP or UDP?

OSPF floods messages so that each node can reconstruct the   
network topology. It requires reliability otherwise the topology   
may not be consistent at all nodes. TCP does not support flooding   
while UDP does not support reliability