Information

- The duration of the exam is 4 hours (9.00-13.00).
- Answers should be well structured and readable, remember that quality is better than quantity.
- Write your name and personal-id/date-of-birth on each page.
- No help material is allowed.
- Answers will be posted on the course web within 2 weeks after the exam.
- Results will be published in Daisy no later than November 14, 2007. Graded exams can be collected from STEX on floor 6 (elevator A) in Forum by November 14, 2007. Complaints about the grading should be handed in (in writing) via the white post box on floor 6 next to STEX addressed to “Markus Hidell, KTH/ICT/ECS/TSLAB, Forum Floor 8” no later than November 28, 2007.
- The exam consists of 2 parts; Part A and Part B. Part A is a set of questions with short answers (typically less than four lines), and Part B is a smaller set of questions that require more elaborative answers. To pass the exam you need to attain a certain number of points (preliminary 75%) on Part A. Higher grades (A-C or 4-5) will be based on the total score (Part A + Part B). **Part B will not be graded for those who do not pass Part A.**
- Preliminary grading is as follows:

Points	**Grade (A-F)**
23-30 points on Part A and 45-50 points in total	A
23-30 points on Part A and 40-44 points in total	B
23-30 points on Part A and 35-39 points in total	C
23-30 points on Part A and 23-34 points in total	D
21-22 points on Part A and passed complementary assignment	E
21-22 points on Part A (complementary assignment offered)	Fx
0-20 points on Part A	F (Fail)

Points	**Grade (U-5)**
23-30 points on Part A and 43-50 points in total	5
23-30 points on Part A and 36-42 points in total	4
23-30 points on Part A and 23-35 points in total	3
21-22 points on Part A (complementary assignment offered)	U
0-20 points on Part A	U (Fail)

Good Luck!

Exam Part A (30p)

1) Various true/false statements (10p)

Mark the following statements as true or false. Don't write "t" or "f", since it may be hard to differ between the two if the hand-writing is indistinct.

Note:

- you will get 1p for each correct answer
- you will get -1p for each wrong answer
- you will get 0p for each "no answer"
- you will **not** get less than 0p in total on this question

A. In the initial state of the spanning tree protocol, the bridge with the highest ID assumes it is the root. (1p)
B. The service offered by IP is connectionless and best-effort. (1p)
C. ICMP messages are encapsulated directly in UDP messages. (1p)
D. Asynchronous Transfer Mode (ATM) is a connection-oriented network. (1p)
E. In the Integrated Services (int-serv) model, application data for a reserved flow is carried in RSVP (Resource ReSerVation Protocol) messages. (1p)
F. Routing Information Protocol (RIP) uses a distance-vector algorithm to find the best path. (1p)
G. 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. (1p)
H. Voice over IP (VOIP) is an example of an application that is suitable for using peer-to-peer networks. (1p)
I. Real-Time Streaming Protocol (RTSP) is used to carry real-time data such as audio and video. (1p)
J. The Domain Name System consists of a hierarchical set of DNS servers that serve as a directory to lookup hostnames and IP addresses. (1p)

Answer:

A. True (everyone assumes it is root initially)
B. True
C. False (ICMP runs directly on top of IP)
D. True
E. False (RSVP is used to set up the reserved flow)
F. True
G. False (MSDP is not based on RIP)
H. True
I. False (RTSP is for control information only)
J. True

2) STP—Spanning Tree Protocol (2p)

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 LAN down.

3) Layer 2 versus Layer 3 protocol design (2p)

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.

4) Network layer (2p)

In virtual circuit networks, each packet contains a (small) connection identifier (CI) instead of a (large) network unique destination address.
Does an end-station in a virtual circuit network still need a network unique address? (Briefly motivate your answer.)

Answer:

A global unique address is needed in the connection establishment phase.

5) Network layer (2p)

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.

6) Dynamic Routing (2p)

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.

7) MPLS—Multi-Protocol Label Switching (2p)

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.

8) VPN—Virtual Private Networks (2p)

What is the goal of a provider provisioned VPN?

Answer:

To build a network that, as much as possible, acts like an extension of the private corporate network on a service provider's shared network infrastructure.

9) Multicast routing (2p)

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).

10) Peer-to-peer networking (2p)

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:

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 avoided.

11) Multimedia networking (2p)

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).

Exam Part B (20p)

12) IP fragmentation and reassembly (5p)

A. Why should IP fragmentation be avoided? (1p)
B. Explain the mechanism used in IP for handling fragmentation. (2p)
C. What is the standard term for the mechanism that figures out the biggest packet that can be transferred from sender to receiver without being fragmented? (1p)
D. How do you force routers along the way not to fragment an IP datagram? (1p)

Answer:

A. Fragmentation is not good for the network efficiency.
B. Three header fields are used: Identification field, Fragment offset field, and a flags field. Flags used are “Don't Fragment” and “More Fragment”. All fragments belonging to a specific datagram have the same ID (in the Identification field) so that the destination can determine what fragments that belong to what datagram. Fragmentation offset gives the relative position of this fragment with respect to the whole datagram. If “More Fragment” flag is set, it means the datagram is not the last fragment. If it is not set, it means that this is the last fragment.
C. MTU (Maximum Transmission Unit) discovery.
D. There is a “Don’t fragment” flag in the flags field. If this flag is set, routers along the way are not allowed to fragment the packet.

13) Dynamic routing (5p)

A. When electing a designated router (DR) on a LAN, IS-IS (Intermediate System-Intermediate System) implements a "deterministic behavior", while OSPF (Open Shortest Path First) is said to have a "sticky" behavior. What is meant with “deterministic” and “sticky” behavior in this case? (1p)
B. Briefly explain how a router can distribute Link State Packets (LSPs) to other routers? (2p)
C. Give one reason why link state routing protocols generally can adapt faster to network topology changes than distance vector protocols? (2p)

Answer:

A. The algorithm to elect a designated router (DR) is based on comparing a “priority value” of each attached router. In the deterministic case, the router with the “best” priority always becomes the DR (if a router with a better priority appears, it will take over the role as DR). In the sticky behavior, the election is done only once (unless the current DR crashes). Once a router becomes DR it will continue to act as DR even if a router with better priority appears.
B. When distributing routing information, the normal routing schemes can’t be used, since the distribution of routing messages can’t depend on the forwarding tables that should be created based on the LSP information. Instead they can use a scheme based on "enhanced" flooding, which works independently of the forwarding tables.

C. When a router receives an LSP with information about topology change, it can immediately forward that LSP to other neighbors. In distance vector routing, a router that receives a distance vector from a neighbor router will have to recompute a new distance vector before it can inform its other neighbors. Furthermore, link state protocols do not suffer from the counting-to-infinity problem, which can occur in distance vector routing.

14) Quality of service in IP networks (5p)

Suppose that the following flows, specified with token bucket traffic specifications, have been accepted by an int-serv (Integrated Services) capable router:

Flow #	R (rate in packets/second)	B (bucket depth in no of packets)
1	2	9
2	5	6
3	8	5

All flows are in the same direction and the router forwards 20 packets per second. Note that the example is unrealistic in its use of packets, instead of bytes.

A. What is the maximum delay a packet may face? Show your calculations. (2p)
B. What is the maximum number of packets from the third flow (r = 8, B = 5) that the router would send over 4.0 seconds, assuming the router sends packets at its maximum rate uniformly? Show your calculations. (1p)
C. What are the main drawbacks with the integrated service model for IP quality of service? (2p)

Answer:

A. Max delay is given by max queue length, which is the sum of all buckets. B_{tot} = 9+6+5 = 20. Max delay = B_{tot}/link capacity = 20/20 = 1 second.
B. Max no of packets over 4 seconds for the third flow = rT + B = 8x4 + 5 = 37 pkts.
C. 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 routers.

15) Unicast versus multicast (5p)

Make the following assumptions:

- The topology consists of a single switch with a bunch of ports, all in the same broadcast domain.
- The switch does not filter packets sent to layer 2 multicast addresses; it forwards all such packets to all ports.
- Source S has a high volume of data to send to n recipients.

Compare the strategy of having S send *n* unicast packets, one to each of the *n* recipients, versus sending a single multicast packet for each

data packet in S's data stream. How does multicast affect maximum aggregate bandwidth, considering all conversations going on in this LAN and not just what S's data stream can achieve?

Answer:

With unicast, S can only send at $1/n$ of the rate since each packet has to traverse the link from S n times. However, with unicast, nodes that are not one of the destinations will not be bothered with the traffic. If neither A nor B are recipients, they can carry on a full-bandwidth conversation despite S sending n unicasts. If S were sending multicast though, and the switch does not filter multicast (as stated in the problem), then S’s traffic will compete for bandwidth on A and B’s links.

Assuming the switch has infinite capacity and the only limitation is the bandwidth on the links, n unicasts would slow down S, but be equivalent in bandwidth use on each of the links to each recipient. But unicast would actually make better use of bandwidth for nodes that are not recipients, since the unicast packet would not appear on the link, whereas the multicast one would.