Information

- This exam is for course codes IK2215, IK2204, and 2G1701
- The duration of the exam is 4 hours (9.00-13.00).
- Answers should be well structured and readable.
- 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 8, 2010. Graded exams can be found as PDF files in Daisy. Complaints about the grading should be done in writing, and sent to IK2215@ict.kth.se, no later than November 22, 2010.
- The exam consists of 2 parts; Part A and Part B. Part A is a set of questions with short answers. **Respect the word limits!** Answers longer than the word limit will be truncated, meaning that we will disregard from the part of your answer that exceeds the word limit during the exam marking. 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 42-50 points in total	5
23-30 points on Part A and 37-41 points in total	4
23-30 points on Part A and 23-36 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) (Note the word limits)

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. OSPF and IS-IS are both based on link state routing. (1p)
B. UDP provides an optional flow control. (1p)
C. DVMRP is a distance vector protocol for multicast routing. (1p)
D. An ICMP error is not sent in response to an IP packet carrying another ICMP error message. (1p)
E. DCCP provides an unreliable congestion-controlled transport service. (1p)
F. Diff-serv typically provides IP QoS guarantees for individual application traffic flows. (1p)
G. IPv6 has a stronger checksum compared to IPv4. (1p)
H. An L1 VPN can be used to provide an Ethernet LAN service. (1p)
I. RTP includes a mechanism to ensure timely delivery of data to the receiving host.(1p)
J. Napster is a peer-to-peer application using a central directory. (1p)

Answer:

A. True
B. False
C. True
D. True
E. True
F. False
G. False
H. False
I. False
J. True

2) Various questions with short answers (10p)

Answer the following questions with short answers.

Note:

- You will get 1p for each entirely correct answer
- Word limit per question: 30 words

A. Place the following protocols/mechanisms in the correct TCP/IP protocol layer: VLAN, SCTP, IGMP, and SMTP. (1p)
B. What is the result of aggregating the two following subnets: 199.1.1.0/25 and 199.1.1.128/25? (1p)
C. Briefly characterize the kind of service that TCP offers to applications? (1p)
D. How is DNS redirection typically helpful in a CDN? (1p)

E. Name one multicast routing protocol using source based tree and one using group shared tree. (1p)
F. Mention briefly what RTSP is used for. (1p)
G. What is the overall purpose of the tracker in BitTorrent? (1p)
H. What is the main problem with scaling a link state routing protocol to a global level? (1p)
I. Mention three types strategies, devised by the IETF, for the transitioning from IPv4 to IPv6. (1p)
J. What is sliding windows used for in TCP? (1p)

Answer:

A. VLAN: Link, SCTP: Transport, IGMP: Network, SMTP: Application
B. 199.1.1.0/24
C. Connection-oriented, reliable, stream service.
D. To guide browsers to the correct server.
E. Source based trees: MOSPF, DVMRP. Group shared trees: CBT, PIM-SM.
F. RTSP is a protocol for exchanging playback control information (pausing, fast forwarding, rewinding, etc).
G. To keep track of the peers in a torrent.
H. A link state protocol is based on full topology knowledge, so the database would be enormous.
I. Tunneling, dual-stack, header translation.
J. Flow control.

3) IPv6 (2p) (Word limit: 50+50)

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.

4) SCTP (2p) (Word limit: 75)

Explain what multi-homing means in the context of SCTP. Why is this a problem in TCP?

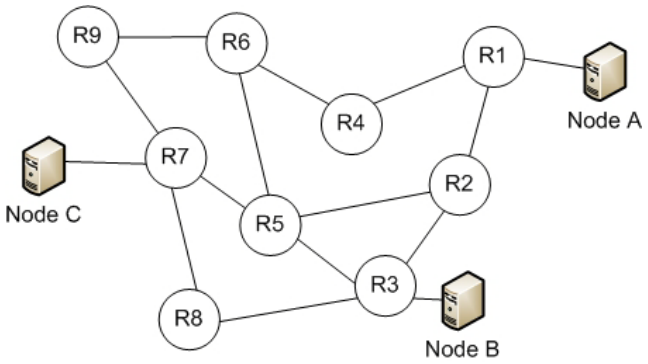
Answer:

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.

5) IP multicast (2p) (Word limit: 75)

What is the key advantage of using multicast routing with a source tree over multicast routing with a shared tree?

Given the topology below, identify the path that multicast packets in a source tree topology will take if the sender is node A and the receivers are node B and node C. Assume that the cost for all the links is 1 and that R6 is the Rendezvous Point (RP).



Example answer:

Node A -> R88 -> R99 -> Node B

Answer:

In multicast routing with a source tree, the traffic follows an optimal (shortest) path to the receivers while the traffic might follow non-optimal path in a shared tree scenario.

Node A **->** R1 **->** R2 **->** R3 **->** Node B

Node A **->** R1 **->** R2 **->** R5 **->** R7 **->** Node C

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

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.

7) VPNs (2p) (Word limit: 50)

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.

Exam Part B (20p)

8) IP (5p)

Assume a new link layer, called dream-net, with MTU 1400 bytes and a UDP datagram with 4096 bytes of user data is to be sent over a dream-net link. There are no IP options involved. How many IP fragments are transmitted and what is the offset and IP payload length of each fragment? (5p)

Answer:

There are 4104 bytes of data for IP to send (4096 bytes UDP data and 8 bytes UDP header). Each dream-net frame can contain 1400 bytes of data, out of which an IP header consumes 20 bytes. Thus, we can fit 1380 bytes IP payload (UDP datagram) into an IP fragment. 1380 cannot be evenly divided by 8, and fragment offset is given in 8-bytes units. Therefore, we can only fit 1376 bytes of the UDP datagram into each fragment (1376 = 172x8).

Fragment 1: 1376 bytes IP payload, offset = 0 (fragment offset field = 0)
Fragment 2: 1376 bytes IP payload, offset = 1376 (fragment offset field = 172)
Fragment 3: 1352 bytes IP payload, offset = 2752 (fragment offset field = 344)

9) Transport layer (4p)

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

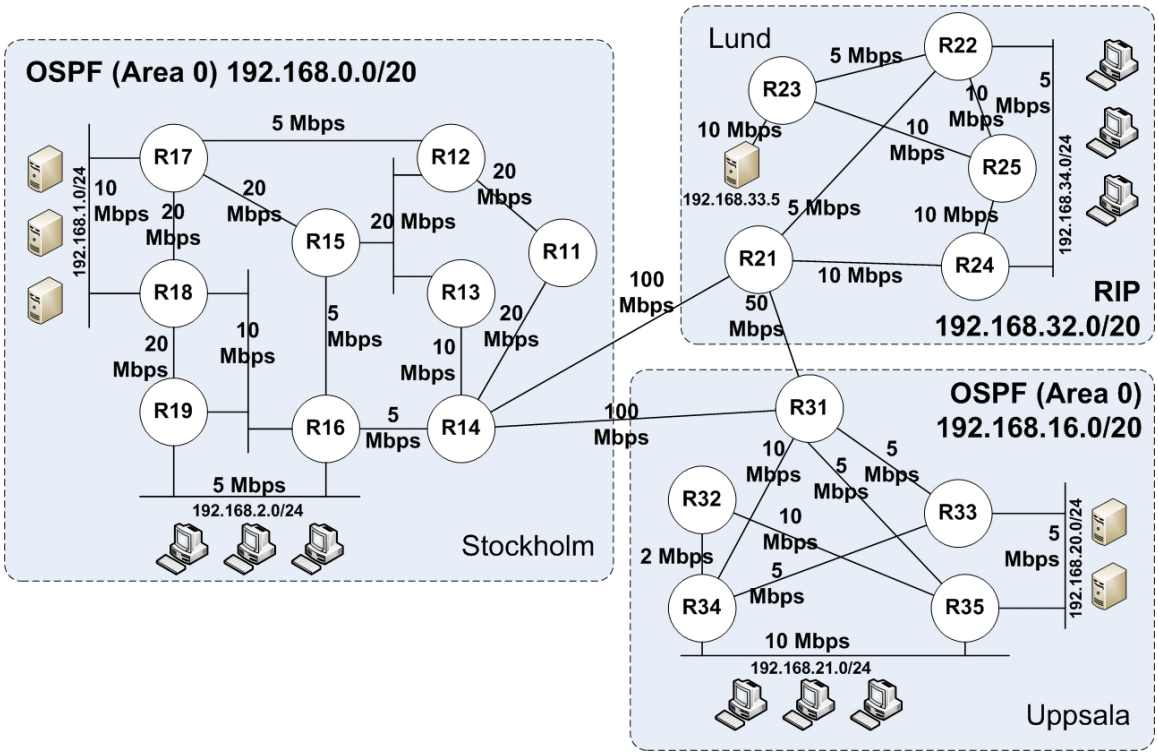
- How congestion occurs and how TCP would act without congestion control
- The different phases of congestion control
- How the size of the sender's window changes during the two different phases.

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

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

10) Scenario (11p)



The above figure illustrates Company A's network topology. Company A has three branch offices in different cities, each with different networks. The first office is located in Stockholm using the 192.168.0.0/20 subnet. The second office is located in Uppsala using the 192.168.16.0/20 subnet. The last office is located in Lund using the 192.168.32.0/20 subnet. All routers are interconnected with different link bandwidths as shown in the figure. All routers are Cisco routers with default parameters.

Each office has designed its own internal network and runs its own routing protocol internally. There is no routing protocol running between the different offices (no routing protocol is used between the R14-R21 link, the R21-R31 link, and the R31-R14 link).

For its internal network, the Stockholm office uses OSPF as its sole routing protocol within its network. All routers (R11-R19) are running in the backbone area (OSPF area 0). Similar to the Stockholm office, the Uppsala office uses OSPF as its sole routing protocol within its network (on routers R31-R35). All routers are running in the backbone area (OSPF area 0). On the other hand, the Lund office uses RIPv2 on all its routers (R21-R25).

To communicate between branch offices, the following static routes are configured:

On R14,
All traffic destined to 192.168.16.0/20 is forwarded to R21

All traffic destined to 192.168.32.0/20 is forwarded to R31
On R21,
All traffic destined to 192.168.0.0/20 is forwarded to R14
Set default route for all traffic to forward to R31
On R31,
All traffic destined to 192.168.32.0/20 is forwarded to R21
Set default route for all traffic to forward to R14

In addition to configure static routes, the Stockholm office has been configured to originate default route from R14 to all other routers within the branch office. The Uppsala office has configured R31 to redistribute all static routes into OSPF. The Lund office has configured R21 to redistribute all static routes into RIP.

The Stockholm office has one server network (192.168.1.0/24) and one user network (192.168.2.0/24). HSRP (Hot Standby Router Protocol) is used to provide fault tolerance for each network. For the server network, R17 is active router and R18 is passive router. For the user network, R19 is active router and R16 is passive router.

The Uppsala office has one server network (192.168.20.0/24) and one user network (192.168.21.0/24). HSRP is used to provide fault tolerance for each network. For the server network, R35 is active router and R33 is passive router. For the user network, R35 is active router and R34 is passive router.

The Lund office has one server network (192.168.33.0/24) and one user network (192.168.34.0/24). HSRP is used to provide fault tolerance for the user network. R22 is active router and R24 is passive router. (Note that only one server is shown in the figure.)

Assume that default cost models are used for OSPF and RIP as well as for static routes (a static route has a fixed cost of 1). When a route is redistributed from one protocol to the other, the original cost of the route will be inherited to the new protocol and accumulated with the new cost before the route is forwarded to other routers. In addition, if a router learns a route with equal cost from multiple routers, it will prefer to use the route from the router with lowest number. For example, if R51 learns a route 10.0.0.0/24 from R55 and R60, it will prefer to use the route learned from R55.

A host in Lund with IP address 192.168.34.5 is trying to ping a host in Stockholm with IP address 192.168.2.3. Answer the following questions:

A. What path does an ICMP echo request take? (1p)
B. What path does an ICMP echo reply take? (1p)

Example answer
10.0.0.1 -> RTX -> RTY -> RTZ -> 10.0.0.2

A host in Uppsala with IP address 192.168.21.3 is trying to ping a server in Stockholm with IP address 192.168.1.2. Answer the following questions:

C. What path does an ICMP echo request take? (1p)
D. What path does an ICMP echo reply take? (1p)

Example answer
10.0.0.1 -> RTX -> RTY -> RTZ -> 10.0.0.2

Assume that R15, R25, and R35 have lost electricity and stop running. After the topology has converged, a host in Stockholm with IP address 192.168.2.3 is trying to ping a server in Uppsala with IP address 192.168.20.4. Answer the following questions:

E. What path does an ICMP echo request take? (1p)
F. What path does an ICMP echo reply take? (1p)

Example answer
10.0.0.1 -> RTX -> RTY -> RTZ -> 10.0.0.2

Assume the same scenario as shown in the figure above. A network administrator would like to run a multicast routing protocol in order to distribute recorded multimedia, stored on a streaming server (IP 192.168.1.9/24) in the Stockholm office, to all users in all branch offices.
Answer the following questions:

G. Assume that you are using PIM sparse mode to distribute your multicast stream, and that R16 is selected as a rendezvous point. Assume further that the SPT-threshold is set very high and never exceeded. Now, identify the paths that will be used for streaming from the streaming server to the different hosts in each office. To avoid confusion caused by having two routers on the network (HSRP routers), all traffic must come to the receiver via the receiver's active router. The sender can send via any of the routers as long as it is the best RPF path from the receiver. The hosts in each office are as follows:
   a. 192.168.21.10 in Uppsala office (1p)
   b. 192.168.34.10 in Lund office (1p)

Assume that in each office, there is one centralized DNS/DHCP server, which is responsible for DNS and DHCP service within each office's network. (These servers are 192.168.1.2 in Stockholm, 192.168.20.2 in Uppsala and 192.168.33.5 in Lund).

H. All DHCP servers are configured to be authoritative for all branches and they are acting as redundant DHCP servers for one another. However, when the DHCP server in the Lund office is taken offline, all hosts in Lund lose IP addresses and do not receive any new addresses from the other two DHCP servers. Explain what could be the reason for why the hosts do not get IP addresses from the redundant DHCP servers? (1p)
I. Company A is experiencing network congestion on R14 due to a high data transfer from the FTP server (ftp.company-a.com) in the Stockholm office to different hosts in the other branch offices. You are not allowed to make any changes on the routers and you want to keep your change as transparent as possible to the users. What would be the best solution to solve this problem? Explain briefly how it is done. (2p)

Answer:

A. 192.168.34.5 -> R22 -> R21 -> R14 -> R16 -> 192.168.2.3

B. 192.168.2.3 -> R19 -> R16 -> R14 -> R31 -> R21 -> R22 -> 192.168.34.5
C. 192.168.21.3 -> R35 -> R31 -> R14 -> R11 -> R12 -> R15 -> R17 -> 192.168.1.2
D. 192.168.1.2 -> R17 -> R15 -> R12 -> R11 -> R14 -> R21 -> R31 -> R34 -> 192.168.21.3
E. 192.168.2.3 -> R19 -> R16 -> R14 -> R21 -> R31 -> R33 -> 192.168.20.4
F. 192.168.20.4 -> R33 -> R31 -> R14 -> R16 -> 192.168.2.3
G. The paths used for sending the stream are as follow:
    a. 192.168.1.9 -> R18 -> R16 -> R14 -> R31 -> R35 -> 192.168.21.10
    b. 192.168.1.9 -> R18 -> R16 -> R14 -> R21 -> R22 -> 192.168.34.10
H. Since the DHCP server in each branch is not located in the same network as the hosts, there must be a DHCP relay agent that forwards the DHCP messages between the host and the server. However, it is likely that the relay agent in Lund is only configured to forward DHCP messages only to/from 192.168.33.5 but not to/from the other redundant DHCP servers.
I. The best solution is to create FTP replica on each branch and make a CDN by using DNS redirection. Each DNS should point ftp.company-a.com to its local FTP replica.