Information

- This exam is for course codes IK2215, IK2204, and 2G1701
- The duration of the exam is 4 hours (14.00-18.00).
- 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 no later than November 15, 2016. Requests for grading re-evaluations should be made according to the routines specified by KTH School of Information and Communication Technology.
- 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 indistinct hand-writing makes it hard to differ between the two.
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. A RIP router regularly sends its distance vector to all other routers in the network. (1p)
B. In UDP there is an optional checksum covering header and data. (1p)
C. A BGP router assigns an AS path to a prefix when adveritising it to its neighbors, (1p)
D. Multicast routing is supported in large parts of the Internet backbone. (1p)
E. The majority of the power consumption in high-end routers can be attributed to the control plane functions. (1p)
F. In diff-serv (differentiated services), traffic is divided into a small set of traffic classes, and resources are allocated on a per-class basis. (1p)
G. In IPv6 only the sending host can do IP fragmentation, routers cannot. (1p)
H. In IP multicast, a router needs to keep track of each individual receiver on a subnet. (1p)
I. RTP (Real-time Transport Protocol) is typically run on top of TCP and tries to smoothen out delay jitter introduced by flow control and congestion control. (1p)
J. BitTorrent uses an infrastructure node called tracker to keep track of the peers in a torrent. (1p)

Answer:

A. False
B. True
C. True
D. False
E. False
F. True
G. True
H. False (it only needs to know if there are any receivers on the subnet)
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 four protocols at the correct layer in the TCP/IP protocol stack: SMTP, QUIC, IGMP, and ICMPv6. (1p)
B. Assume you aggregate the prefixes 189.1.2.0/26, 189.1.2.64/26, and 189.1.2.128/25 to one single subnet. Specify (in CIDR notation) the resulting aggregated prefix. (1p)
C. At a given time, a TCP sender has a congestion window of 2048 bytes and a receiver-advertised window of 4096 bytes. What is the maximum number of bytes that the sender can transmit before waiting for an ACK? (1p)
D. Gnutella query flooding can be described as a simple an elegant design. However, the desing has also been critized—for what? (1p)
E. Multicast routing protocols use either source-based delivery trees or group-shared delivery trees. Which one of these is likely to lead to most memory consumption in the routers? (1p)
F. What is roughly the highest tolerable delay for an interacive audio application? (1p)
G. 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)? (1p)
H. Router A is running OSPF and sends out a link state advertisement (LSA). Which routers are the ultimate receivers of this ~~distance vector~~ LSA? (1p)
I. What was the main reason for starting the transition from IPv4 to IPv6? (1p)
J. BGP uses a path vector when it advertizes routes. What does that mean? (1p)

Answers

A. SMTP: Application layer, QUIC: Transport layer, IGMP, ICMPv6: Network layer.
B. 189.1.2.0/24.
C. 2048 bytes.
D. For not being scalable since it uses flooding.
E. Source-based tree protocols.
F. Up to 400 ms.
G. EEE uses low-power idle.
H. All routers in the same OSPF area.
I. The world was running out of IPv4 addresses.
J. BGP assigns a cost and a path to each route it advertizes.

3) Transport layer (2p) (Word limit: 100)

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:

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.

4) Multicast (2p) (Word limit: 80)

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:

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.

5) Distance vector routing (2p) (Word limit: 50)

Consider a router *D* in a network where distance vector routing is used. *D* has the following routing table:

Network	Next router	Distance
N_1	*B*	4
N_2	*A*	5
N_3	*B*	6
N_4	*A*	6
N_5	*C*	4
N_7	*C*	2

D receives a routing message from router A, with the following information:

Network	Distance
N_1	5
N_2	4
N_3	2
N_4	3
N_5	4
N_6	2

Show the routing table in *D*, after *D* has processed the routing message.

Answer:

Network	Next router	Distance
N_1	*B*	4
N_2	*A*	5
N_3	*A*	3
N_4	*A*	4
N_5	*C*	4
N_6	*A*	3

N_7	C	2

6) Multimedia networking (2p) (Word limit: 70)

a) What is the purpose with the protocol RTSP (Real-Time Streaming Protocol). (1p)
b) What is the purpose with a playback buffer? (1p)

Answer:

a) It is a protocol for controlling multimedia streams. It is used to exchange playback control information, such as pause, fast-forward, rewind, etc.
b) The purpose with the playback buffer is to absorb delay variations (jitter) in the network on the receiver side.

7) Internet application services (2p) (Word limit: 100)

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:

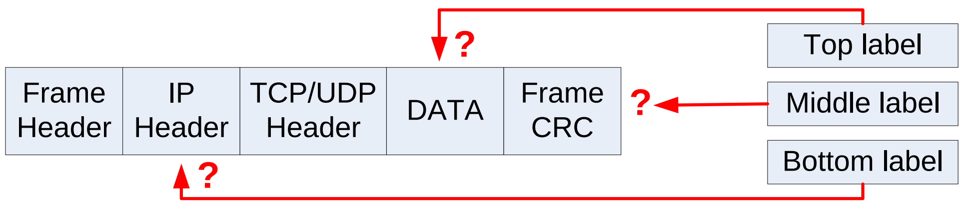
a) The root hints file contains host information (i.e. records for the root DNS servers on the Internet) that is needed to resolve names outside of the authoritative zones of the DNS server.
b) To locate content, Gnutella uses query flooding to fine content from near by peers.
Query flooding is not scalable. With limited flooding scope, it may not find the content within the near by peers.

Exam Part B (20p)

8) MPLS label (5p)

Answer the following questions on MPLS label.

A. Name and briefly describe the four fields of the MPLS label (2p)
B. Give the Ethernet frame below. Where does MPLS impose label stacks to the frame assumed that there are three labels in the label stack? (1P)



C. 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)

Answer:

A. **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.

B. The label is imposed between frame header and IP header. The top label appears first and the bottom appears last.

Frame Header	Top Label	Middle Label	Bottom Label	IP Header	TCP/UDP Header	DATA	Frame CRC

C. 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.

9) Transport layer (5p)

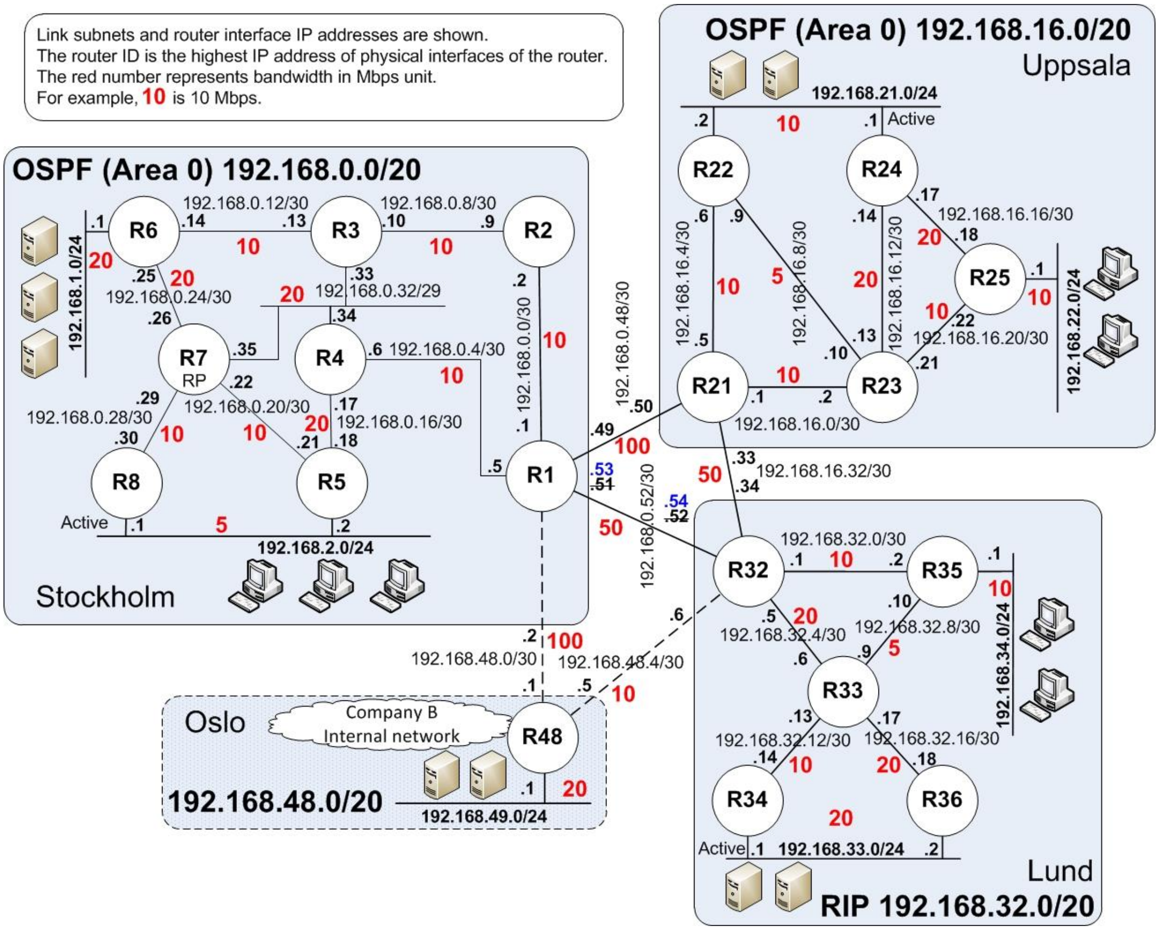
Two important functions of a transport protocol are flow and congestion control.

A. Explain the difference between flow and congestion control? (1p)
B. Suppose that the round-trip time between two hosts running TCP is 100 ms, and that at a particular point in time, the sender's congestion window is 32 000 bytes and the advertised receiver window is 20 000 bytes. What is the maximum throughput that can be achieved by the sender? (1p)
C. Assume that a TCP sender starts with an initial congestion window of 1 segment and that the slow-start threshold is at that time 16 segments. How many segments need to be transmitted by the sender until TCP enters congestion avoidance? (1p)
D. When TCP exits Fast Recovery, the congestion window is deflated to the size it had at the time Fast Recovery was entered. Why? (2p)

Answer:

A. Flow control is a way for the receiver to throttle the sender so that the receiver doesn't get overwhelmed with data. The purpose with congestion control is to make the sender adapt to the network conditions (so that routers don't get overloaded).
B. Since the sender window = min(congestion window, receive window) = 20 000 bytes, the maximum possible throughput is 20 000 bytes / 100 ms = 1.6 Mbps.
C. TCP enters congestion avoidance after four transmission rounds during which 1 + 2 + 4 + 8 = 15 segments have been transmitted.
D. 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.

10) Large-scale network scenario (10p)



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 set.

Each office has designed its own internal network and runs its own routing protocol internally. The Stockholm office uses OSPF as its sole routing protocol within its network. All routers (R1-R8) 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 R21-R25). All routers are running in the backbone area (OSPF area 0). The Lund office uses RIPv2 on all its routers (R32-36). These routing protocols are not running on the links between the offices (no OSPF or RIP on the R1-R21 link, the R21-R32 link, or the R1-R32 link). However, different routing schemes are used for communication between branch offices.

Static route commands are configured as follows:

On R21: ip route 192.168.32.0 255.255.240.0 192.168.16.34
On R32: ip route 0.0.0.0 0.0.0.0 192.168.16.33

Company A runs two iBGP peerings as follows:
between Stockholm's R1 and Uppsala's R21 (over R1-R21 link)
between Stockholm's R1 and Lund's R32 (over R1-R32 link)

All routers run iBGP peering with private AS 65001 and have "no auto-summary" and "no synchronization" commands configured. They also have the following route advertisements:

R1 is configured to advertises its aggregated route 192.168.0.0/20 with "summary-only" to all BGP peers (longer-prefix routes are suppressed and NOT advertised). R21 redistribute OSPF routes into BGP. R32 advertises default route (0.0.0.0/0) route to all BGP peers.

In addition, the Stockholm office has configured R1 to always originate default route in OSPF. The Uppsala office has configured to redistribute static routes into OSPF on R21. The Lund office has configured to redistribute BGP into RIP on R32.

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-tolerant default gateway for the user network. R8 is active router and R5 is passive router. The virtual IP address is 192.168.2.3, which is used as the default gateway by all hosts.

The Uppsala office has one server network (192.168.21.0/24) and one user network (192.168.22.0/24). HSRP is used to provide fault-tolerant default gateway for the server network. R24 is active router and R22 is passive router. The virtual IP address is 192.168.21.3, which is used as the default gateway by all servers.

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-tolerant default gateway for the server network. R34 is active router and R36 is passive router. The virtual IP address is 192.168.33.3, which is used as the default gateway by all servers.

Assume that default cost models are used for OSPF, RIP, as well as for static routes (a static route has a fixed cost of 1, OSPF cost formula is *cost = <100,000,000 bps>/<bandwidth in bps>*). 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. For BGP originated routes, the cost will be set to 10. In addition, if a router learns the same route from different routing protocols, it will prefer the route from the routing protocol in the following order: static, eBGP, OSPF, RIP, and iBGP. If a router learns a route with equal cost from the same routing protocol through multiple routers, it will prefer to use the route from the router with the lowest router ID. For example, if R51 (router ID 1.1.1.1) learns an OSPF route 10.0.0.0/24 from R55 (router ID 2.2.2.2) and R60 (router ID 3.3.3.3), it will prefer to use the OSPF route learned from R55 since its router ID 2.2.2.2 is lower than R60 (router ID 3.3.3.3). The router ID is the highest IP address on physical interfaces. The virtual IP address is not considered when deciding the router ID.

Assume that the topology has converged. Answer the following questions:

A. What path does a packet traverse when a host in Stockholm with IP address 192.168.2.11 sends an ICMP echo request to a server in Uppsala with IP address 192.168.21.5? (1p)
B. What path does a packet traverse when a host in Uppsala with IP address 192.168.22.11 sends an ICMP echo request to a server in Lund with IP address 192.168.33.5? (1p)
C. What path does a packet traverse when a host Lund with IP address 192.168.34.11 sends an ICMP echo request to a server in Stockholm with IP address 192.168.1.5? (1p)

IMPORTANT: You must specify the next-hop IP address of every hop the packet traverses. If the ICMP echo request cannot reach the destination then identify what happens to the request.
Example answer
10.0.0.11 -> 10.0.0.1 -> 10.0.1.1 -> 10.0.2.2 -> 10.0.3.3
1.1.1.1 -> 1.1.1.2 -> 2.2.2.2 -> 3.3.3.3 -> 3.3.3.3 drops the packet
4.4.4.4 -> 4.4.4.5 <-> 5.5.5.5 (Loop between 4.4.4.5 and 5.5.5.5!)

Assume that the physical link between Uppsala and Lund (on R21-R32 link) was taken down and the border routers lose all routing information on this link. All routes on this link (including static routes) are removed from the routing tables. Assume that the topology has converged. Answer the following questions:

D. What path does a packet traverse when a server in Uppsala with IP address 192.168.21.5 sends an ICMP echo request to a host in Lund with IP address 192.168.34.5? (1p)
E. What path does a packet traverse when a server in Lund with IP address 192.168.33.5 sends an ICMP echo request to a host in Uppsala with IP address 192.168.22.5? (1p)

IMPORTANT: if the ICMP echo request cannot reach the destination then identify what happens to the request. See example answer above.

Assume that the R21-R32 link is back to normal and the original topology in the figure has converged. 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. PIM sparse mode is used for this purpose and R7 is selected as a rendezvous point (RP).

To avoid confusion caused by having two routers on the network (HSRP routers), assume that the links between the passive routers and the server and client networks in each office are removed from the topology (R5-192.168.2.0/24 link, R22-192.168.21.0/24 link, and R36-192.168.33.0/24 link).

Assuming that the SPT-threshold is set to inifinity (the threshold is never exceeded). Answer the following questions:

F. Which path is used for streaming from the streaming server to a host with IP 192.168.22.10 in Uppsala office? (1p)

G. Which path is used for streaming from the streaming server to a host with IP 192.168.34.10 in Lund office? (1p)

Assume the topology is the same as for question F and G above. (All passive rotuers are removed from the server/client networks). The router ID of all routers are also the same (based on IP address derived from company A's three /20 subnets).

Company A has bought company B in Oslo and decided to connect company B office to Company A's network with two physical links; one from Oslo to Stockholm (R48-R1 link) and another from Oslo to Lund (R48-R32 link). To keep the internal routing policy of Company B intact, the network administrator decided to use BGP as the routing protocol on these links. Company B is assigned a private AS 65002 and runs two eBGP peering sessions with AS 65001; one with R1 in Stockholm and another with R32 in Lund. R48 is configured with "no auto-summary", "no synchronization", and using 192.168.49.1 as its router-id. It is also configured to advertise only an aggregate address 192.168.48.0/20 to all BGP peerings with "summary-only" (longer-prefix routes are suppressed and NOT advertised). R48 also redistribute all BGP routes into its internal network. In addition, R48 has a BGP policy to set LOCAL_PREF to 300 on all routes learned via R48-R32 link.

Assuming that the existing iBGP configurations on R1, R21, and R32 as described earlier are still in place.
Then, R1 and R32 each adds the following configurations:

- eBGP peering with R48
- "next-hop-self" command for all iBGP peering

Assume that the topology has converged. Answer the following questions:

H. What path does a packet traverse when a host in Lund with IP address 192.168.34.5 sends an ICMP echo request to a server in Oslo with IP address 192.168.49.5? (1p)
I. What path does a packet traverse when a server in Oslo with IP address 192.168.49.5 sends an ICMP echo request to a server in Uppsala with IP address 192.168.21.5? (1p)
J. What path does a packet traverse when a server in Oslo with IP address 192.168.49.5 sends an ICMP echo request to a server in Lund with IP address 192.168.33.5? (1p]

IMPORTANT: if the ICMP echo request cannot reach the destination then identify what happens to the request. See example answer above.

Answer:

A. 192.168.2.11 -> 192.168.2.3 -> 192.168.0.29 -> 192.168.0.34 -> 192.168.0.5 -> 192.168.0.50 -> 192.168.16.6 -> 192.168.21.5
B. 192.168.22.11 -> 192.168.22.1 -> 192.168.16.21 -> 192.168.16.1 -> 192.168.16.34 -> 192.168.32.6 -> 192.168.32.14 -> 192.168.33.5
C. 192.168.34.11 -> 192.168.34.1 -> 192.168.32.1 -> 192.168.0.51(53) -> 192.168.0.6 -> 192.168.0.35 -> 192.168.0.25 -> 192.168.1.5
D. 192.168.21.5 -> 192.168.21.3 -> 192.168.21.3 drops the packet
E. 192.168.33.5 -> 192.168.33.3 -> 192.168.33.3 drops the packet

F. 192.168.1.9 -> 192.168.1.1 -> 192.168.0.26 -> 192.168.0.34 -> 192.168.0.5 -> 192.168.0.50 -> 192.168.16.2 -> 192.168.16.22 -> 192.168.22.10
G. 192.168.1.9 -> 192.168.1.1 -> 192.168.0.26 -> 192.168.0.34 -> 192.168.0.5 -> 192.168.0.52(54) -> 192.168.32.2 -> 192.168.34.10
H. 192.168.34.5 -> 192.168.34.1 -> 192.168.32.1 -> 192.168.48.5 -> 192.168.49.5
I. 192.168.49.5 -> 192.168.49.1 -> 192.168.48.2 -> 192.168.0.50 -> 192.168.16.2 -> 192.168.16.14 -> 192.168.21.5
J. 192.168.49.5 -> 192.168.49.1 -> 192.168.48.6 -> 192.168.32.6 -> 192.168.32.14 -> 192.168.33.5

You may remove this page from the exam and use it as your own note page