Internetworking/Internetteknik, Examination 2G1305
Date: January 11th 2005 at 9:00 – 13:00

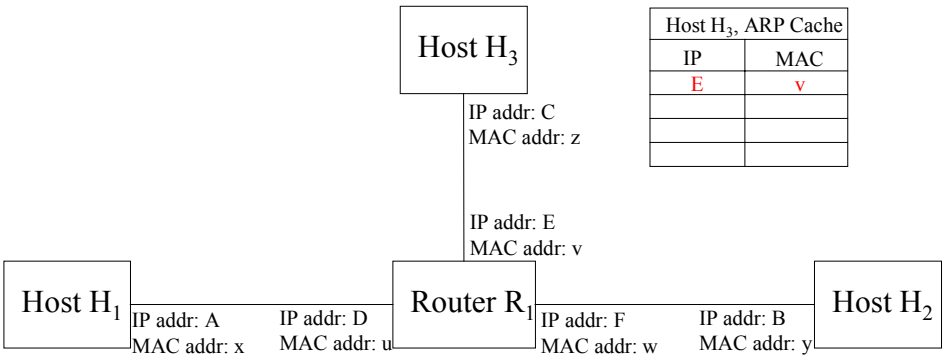
SOLUTIONS

1. General (5p)

a) Place each of the following protocols/functions in the correct TCP/IP layer and note the corresponding OSI layer: Ethernet encapsulation, UDP, IPSec, DHCP, IGMP, and FTP. (3p)
TCP/IP link layer (OSI layer 2): Ethernet encapsulation
TCP/IP network layer (OSI layer 3): IPsec, IGMP
TCP/IP transport layer (OSI layer 4): UDP
TCP/IP application layer (OSI layers 5,6,7): DHCP, FTP

b) Following the OSI reference model (and the terminology used in the course), where would you place each of the following communication devices: Repeater, Bridge, Router, Application Gateway? (2p)
Repeater: L1, Bridge: L2, Router: L3, Application Gateway: L4-L7

2. ARP (5p)



Host H_3, ARP Cache

IP	MAC
E	v

Host H_1, ARP Cache

IP	MAC
D	u

Router R_1, ARP Cache

IP	MAC
A	x
C	z

Host H_2, ARP Cache

IP	MAC

The figure above illustrates three hosts H_1, H_2 and H_3 running IPv4 over a routed network, connected by router R_1. The IP and MAC addresses of the hosts and the router's interfaces are given in the figure. The ARP cache of each host and the router are shown. Assume the ARP caches are initially empty, and that no packets have been sent yet. Now, host H_1 wants to send an IPv4 unicast datagram to host H_3.
Fill in the state of the four ARP caches as they will appear after the IPv4 unicast datagram has been delivered to host H_3, that is, after dynamic ARP resolution has been made. (5p)

3. IP Addressing (5p)

Assume a network N with address/prefix 25.32.40.32/27. Two nodes are attached to the network: Router R with address 25.32.40.33 and host H with address 25.32.40.40.

a) What is the direct broadcast address of N? (1p)
25.32.40.63
b) What is the limited broadcast address of N? (1p)
255.255.255.255
c) What is N's network address? (1p)
25.32.40.32
d) If H uses DHCP to get an IP address from R, which source address does it use initially? (1p)
0.0.0.0
e) What is the subnet mask of N? (1p)
255.255.255.224

4. IPv4 and ICMP (5p)

a) Which fields of the IP header change when a packet passes through a router? Assume that there are no IP options and that no fragmentation occurs. (2p)
TTL (Time To Live) field: it is decremented by one.
Header Checksum field: it has to be recalculated when the TTL is decremented
b) ICMP messages are grouped into *query* and *error* messages. Error messages are sent when errors in IP datagrams are detected, except for some special cases. Name at least two such special cases. (2p)
A datagram carrying another ICMP Error
A datagram destined to IP broadcast or multicast
A datagram sent as link-layer broadcast (e.g., Ethernet)
An IP fragment other than the first
A datagram whose source address does not define a single host
c) Why is there need for a header length field in the IP header? (1p)
The IP header may be of variable size since there may be options included in the header.

5. UDP (5p)

Which of the following statements about UDP are true and false respectively:

a) UDP provides a connection-oriented service. (1p)
False
b) UDP provides an unreliable service. (1p)
True
c) UDP gives feedback to the sender to adjust the data rate. (1p)
False
d) A receiving UDP never delivers duplicate messages to the receiving application. (1p)
False
e) SNMP (Simple Network Management Protocol) uses UDP. (1p)
True

6. TCP (5p)

a) What is the name of the mechanism used for flow control in TCP? (1p)
Sliding windows.
b) What is the difference between *offered window* and *usable window* in TCP? (2p)
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.
c) Someone complained about a throughput of 120,000 bits/sec on a 256,000bits/sec link with a 128-ms RTT (Round Trip Time) between the United States and Japan (47% utilization), and a throughput of 33,000 bits/sec when the link was routed over a satellite (13% utilization). Assume a 500 ms RTT for the satellite link.
What does the window size appear to be for both cases? (1p)
Terrestial link: capacity = throughput x RTT = 120000 bits/s x 128 ms = 1920 bytes
Satellite link: capcity = throughput x RTT = 33000 bits/s x 500 ms = 2062 bytes
It appears that the receiving TCP advertises a 2K window size.
d) How large should the window in the previous example be for optimal throughput over the satellite link? (1p)
For optimal throughput on the satellite link:
capacity = bandwidth x RTT = 256000 bits/s x 500 ms = 16000 bytes.

7. Dynamic Routing (5p)

OSPF and RIP are dynamic routing protocols for routing within an autonomous system.

a) How does OSPF handle network topology: How does OSPF partition the network, and what are the limitations of this partitioning (with respect to how partitions are connected)? (2p)
OSPF partitions network topologies by areas. The backbone area (area 0) may have sub-areas (but sub-areas may not be further partitioned). All traffic must pass through the backbone area. Routers connecting areas are called Area Border Routers.

b) OSPF and RIP use fundamentally different algorithms, but OSPF is said to *converge* faster than RIP. What does this mean, and why is this so? In your answer, you should compare the two protocols with respect to convergence. (3p)
OSPF is based on link-state routing, whereas RIP uses distance-vector. Link-state routing distributes original link information by flooding to every other node. Thus, every node has complete link information fast. The system can reach a correct routing state in a short time. In contrast, distance-vector uses periodic updates between neighbours to distribute information. In addition, distance-vector re-computes routes – nodes do not have access to original data. Therefore, RIP takes longer time to reach a correct state. Thus, the system may be inconsistent causing routing loops during a relatively long time.

8. Autoconfiguration – DHCP and DNS (5p)

a) What is the purpose of a DHCP relay agent? (1p)
A DHCP relay agent (a proxy) can serve several subnets by forwarding local requests to a remote server and then relaying the replies from the server back to the appropriate subnet.

b) DHCP uses well-known ports both at the client side and the server side. Why is a well-known port used at the client side? (1p)
The reply may be broadcast from the server back to the client, and broadcasting to a random port is considered bad form. The reply would then reach all nodes on the subnet that happens to listen to this port.

c) Assume that two clients use DHCP simultaneously on the same subnet, and that the DHCP replies are broadcast from the server back to the clients. How can a client then distinguish between the replies (1p)?
Through the use of the Transaction ID field in the DHCP header.

d) DNS stores its data in general mapping entries called Resource Records (RRs). The following are four examples of such entries: PTR, MX, NS, SOA. What is the purpose of each entry: what mapping does each entry define (for each entry, state "from" and "to" data-type)? (2p)
PTR: IP address → name
MX: domain name → mail server name
NS: domain name → name-server name
SOA: name → zone information

9. IPv4 Multicast (5p)

a) Briefly describe the IPv4 multicast service model. Mention the two different parts of the model, what kind of protocols that are used in each part, and the purpose of these kinds of protocols. (3p)
There are two parts: the host-to-router part and the multicast routing part. The host-to-router part uses IGMP, which enables routers to keep track of multicast group members on each interface. The multicast routing part uses protocols like DVMRP, PIM, etc to establish delivery paths for multicast packets.

b) What does "reverse path forwarding" mean in IP multicast? (2p)
It means that a multicast packet should be forwarded only if it arrives on the interface that would be used as the outgoing interface for a packet sent to the unicast source address.

10. Applications (5p)

a) Briefly describe the SNMP (Simple Network Management Protocol) architecture. Your description should cover the following: manager, agent, query, response, client, server, and traps. (3p)
The SNMP managers run the client side of the protocol. The SNMP agents run the server side of the protocol. Managers query agents about their status, and agents send responses back to the managers. Agents may also send traps spontaneously to managers, e.g., to inform about an unusual situation.

b) RTP (Real-Time Protocol) is used on top of UDP. What are the two main contributions of RTP? (2p)
A sequence number to detect out-of-order delivery and a time-stamp to control playback at the receiver. (Mixing of several sources could also be considered an important contribution).

11. IPv6 (5p)

a) There is no option field in the IPv6 header. However, there is another mechanism used to give more functionality to IP. Briefly describe this IPv6 mechanism. (2p)
IPv6 uses extension headers instead of options to give additional functionality. Extension headers are placed between the IPv6 base header and the transport level header (TCP/UDP). Several extension headers can be linked in a list. Several of the extension headers are options in IPv4.

b) There are three different transition strategies that have been devised by the IETF to make the transition period from IPv4 to IPv6 smooth. Give the name and meaning of each of these three strategies. (3p)
Dual stack – hosts run IPv4 and IPv6 simultaneously
Tunneling – different types of encapsulation of IPv6 packets in IPv4 packets
Header translation – when a header is converted from IPv6 to IPv4 (or vice versa)

12. Internet security (5p)

a) IPsec uses two different modes. Which are these modes? When are the two modes used? How do they differ? (2p)
The two modes are transport and tunnel mode. Transport mode has a SA (Security Association) between two end-hosts, while tunnel mode has a SA between two routers. Tunnel mode encapsulates the original datagram within an IPsec encapsulated header, while transport mode inserts the IPsec headers between the original header and its payload.

b) Three aspects of IP security are integrity, authentication, and privacy. Briefly describe each aspect. (2p)
Integrity – proof that a message is received exactly as it was sent
Authentication – Ther receiver is sure of the sender's identity
Privacy – The transmitted message is only readable by the receiver (and the sender)

c) Which of the aspects in b) can be dealt with through IPSEC AH? (1p)
IPSEC AH provides authentication and integrity. It cannot provide privacy.