EL-GY 5373 Internet Architecture and Protocols

Homework 5 - Solutions

Question 1

There are multiple hosts on a LAN that would like to join the same multicast group and thus, will respond to the same host membership query sent by the router. Briefly describe how the IGMP Report messages will be transmitted by these hosts and why the protocol is designed this way.

Solution

In order to avoid flooding of reports in response to the query sent by the router, a host delays an IGMP report for a random amount of time before actually sending it. During this wait, if it overhears a report indicating the same group address, it cancels the transmission of its own report. Thus, the total number of reports transmitted is suppressed and the probability of potential collision reduced.

Question 2

Compare the multicast routing protocols DVMRP, CBT and PIM. List their advantage(s), and disadvantage(s).

Solution

DVMRP

This is a Distance Vector Multicast Routing protocol.

- Suffers from count to infinity problem.

+ It uses a multicast tree for each source.

- Very expensive when the network is large and/or there are many active multicast sessions.

CBT

+ It uses a shared tree approach for all sources in the group.

- It has the traffic concentration problem (all source traffic through a single link) resulting in congestion and larger delay than multiple-tree schemes.

PIM

This is a multi-modal protocol.

+ It can adapt to different operation scenarios.

Question 3

In a VoIP session, explain the functions of the RTP, RTCP and SIP protocols. In which phase(s) of the VoIP session is each protocol used?

Solution

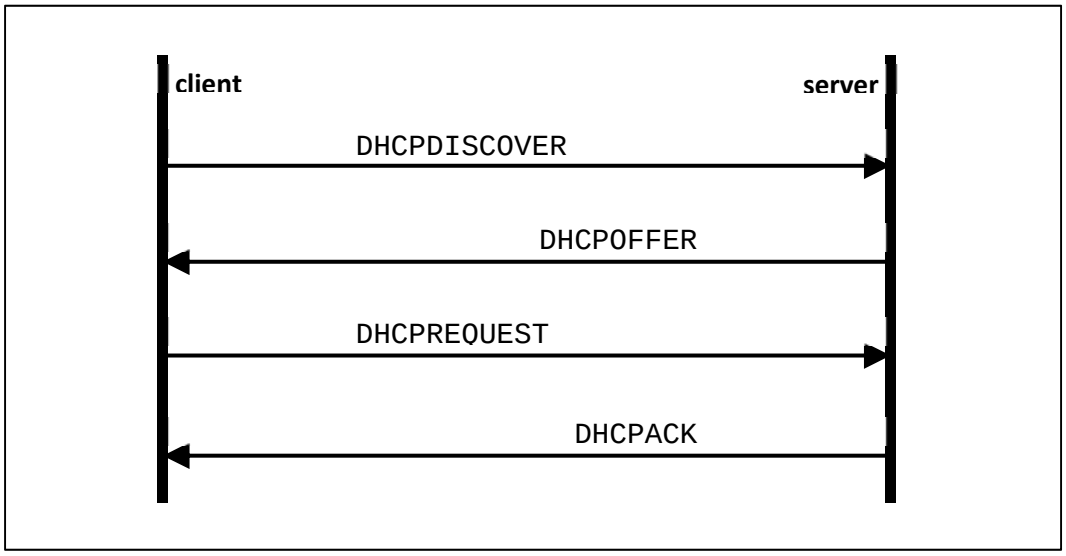
SIP is used for signaling in the call establishment and tear down phases.

RTP is used to carry packetized voice traffic.

RTCP is used in conjunction with RTP to provide real time channel monitoring and QoS feedback.

Question 4

What IP Layer and MAC Layer addresses are used in DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACK messages? Why?
The order of the messages and their directions are shown below for convenience.



Solution

The **DHCPDISCOVER** message is transmitted as broadcasts. Broadcast is the client's only option now as the client doesn't even have an IP Address.

How the **DHCPOFFER** message is transmitted is determined by various factors. Chief among these is the state of the *broadcast bit*, which is included in the Flags field of the DHCPDISCOVER message. This bit indicates whether the server should transmit its responses as broadcasts or unicasts. In most cases, the server transmits the DHCPOFFER message as a broadcast because the client still doesn't have an IP address that the server can use as the unicast destination.

However, if the broadcast bit is not enabled, the server can generate a unicast message using the IP Address it is offering (found in the *Your IP Address* field) as the destination at IP Layer and the client's physical Address (found in the *Client Hardware Address* field of the DHCPDISCOVER message) as the destination at Link Layer. It is also possible for a client to request a specific IP Address in its DHCPDISCOVER message by including an address in the *Client IP Address* field. The server can then send the DHCPOFFER message as unicast directly to the client using that address.

The DHCPREQUEST message is always transmitted by the client as broadcast, both because it isn't yet configured to use the offered IP Address and also in order to inform the other DHCP servers that it is rejecting their offers.

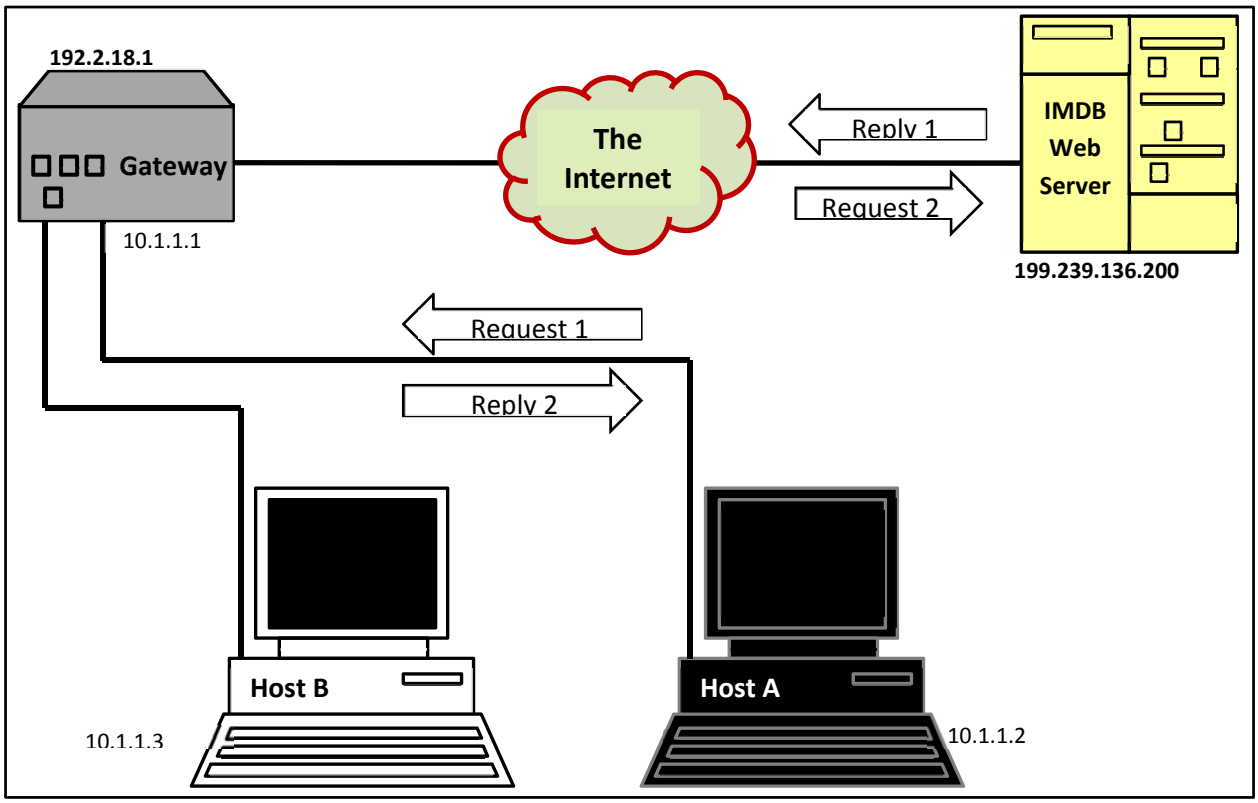
Question 5

As shown in the figure on the next page, Host A and Host B are inside a private address realm. Host A now attempts to access the website ***www.imdb.com***. The related binding in the NAT/PAT table is:

10.1.1.2:2000 - 192.2.18.1:3000

Now assume that Host A initiates the web access by sending out packet Request 1, whose source is 10.1.1.2:2000. Please verify the source and destinations of packets Request 1, Request 2, Reply 1 and Reply 2 in <IP Address>:<Port Number> format. Please note that Request 1 and Request 2 are referring to the same request packet observed at different stages. The same is true for Reply 1 and Reply 2.

The IP Addresses in **Bold** in the figure are public addresses.



Solution

From the IMDB Web Server point of view, it appears as if it is communicating with the Gateway. From the Hosts' point of view, it appears as if they are communicating with the IMDB Web Server directly.

	Source IP Address	/Port	Destination IP Address	/Port
Request 1	10.1.1.2	/2000	199.239.136.200	/80
Request 2	192.2.18.1	/3000	199.239.136.200	/80
Reply 1	199.239.136.200	/80	192.2.18.1	/3000
Reply 2	199.239.136.200	/80	10.1.1.2	/2000

Question 6

Will NAT/PAT have any negative impact on IPSec? Explain the reason in detail.

Solution

NAT + AH

The IPSec Authentication Header (AH) is one example where NAT causes trouble. AH runs on the entire IP Packet including the header fields such as Source IP Address and Destination IP Address using a Message Digest Algorithm to produce a keyed hash. This hash is used by the recipient to authenticate the packet. If anything in the original IP Packet is modified, this authentication will fail and the recipient will discard the packet. AH is designed with an intention to prevent unauthorized modification, source spoofing and man-in-the-middle attacks. But NAT by definition modifies IP Headers. Therefore NAT + AH can't work together.

NAT/PAT + ESP

The IPSec Encapsulating Security Payload (ESP) also employs a Message Digest algorithm for packet authentication. But unlike AH, the hash created by ESP doesn't include the outer header fields. This solves the problem discussed above, but leaves others. IPSec supports two modes. The Transport Mode provides end-to-end security between hosts, while the Tunnel Mode protects encapsulated IP packets between security gateways – for example, between two firewalls or between a roaming host and a remote access server.

When TCP is involved – as they are in transport mode ESP – there is a problem. Because NAT/PAT modifies the TCP packet, NAT/PAT must also recalculate the checksum used to verify integrity. If NAT/PAT updates the TCP checksum, ESP authentication will fail and if it doesn't then TCP verification will fail.