# CSC/ECE 573 Section 001

# Spring 2017

# Homework 5

**Keywords:** Bootstrap, auto-configuration, VPN, NAT, DNS, IP Multicast

Name 1: Pooja Indrajit Gosavi Student ID1: pigosavi

Name 2: Guru Darshan Pollepalli Manohara Student ID2: gpollep

## Instructions

* You can do this homework in groups of two (at most).
* The total number of points is 70.
* You must answer all questions for full credit.
* Use only this paper for your answers, in the space provided.
* The due date is as posted on the web page. You must submit your answers through Wolfware by the due time.

# Question 1: (Bootstrap and autoconfiguration) [20 points]

1. [5 points] When a machine obtains its subnet mask with BOOTP instead of ICMP, it places less load on other machines. Explain.

ICMP Address Mask messages allow a computer to obtain a subnet mask. Though the computer can decide which items to obtain over the network, the disadvantage of this method is apparent when we consider the network traffic and delay. Also, if the computer is unaware of its IP address, it must request the IP address first using techniques like RARP (since the ICMP message is encapsulated in IP header). Each ICMP response returns a small value. Also, because the network enforces a minimum packet size, the space in each packet is wasted.

The designers invented the BOOTP protocol to provide a service through which the server could supply more than one configuration information. To obtain configuration information, protocol software broadcasts a BOOTP Request message. A BOOTP server that receives the request looks up several pieces of configuration information for the computer that issued the request, places the information in a single BOOTP Response

message, and returns the reply to the requesting computer. Thus, in a single step, a computer can obtain information such as the computer's IP address, the server's name and IP address, and the IP address of a default router.

BOOTP requests are broadcasted on port 68. As a result, the broadcast does not place additional load on the machines which do not wish to process such requests.

1. [5 points] When a BOOTP client receives a reply via hardware broadcast, how does it know whether the reply is intended for another BOOTP client on the same physical net?

In the BOOTP request, the client can include its MAC address and any previously bound IP address, if such information has been stored. The BOOTP server can then respond with an IP address for the client, based on either the MAC address mapping or the IP address that had been previously assigned. Also, the client can match the transaction id of the incoming BOOTP reply with its own transaction id.

Also, as per RFC 951, the BOOTP client discards the packets when –

* The incoming packets are not IP/UDPs addressed to the boot port.
* The incoming packets are not BOOTREPLYs.
* The incoming packets do not match the client’s IP (if known) or MAC address.
* The incoming packets do not match the client’s transaction id.

1. [5 points] Read the RFC to find out how DHCP specifies renewal and rebinding timers. Should a server ever set one without the other? Why or why not?

Renewal timer –

The renewal timer is set by default to 50% of the lease length. The client however, may initiate the lease renewal process prior to the expiration of the renewal timer.

Rebinding timer –

The rebinding timer is set to 87.5% of the lease length. After the rebinding timer expires, the client transitions from the renewing state to the rebinding state i.e., the client can broadcast a DHCPREQUEST to any of the DHCP servers.

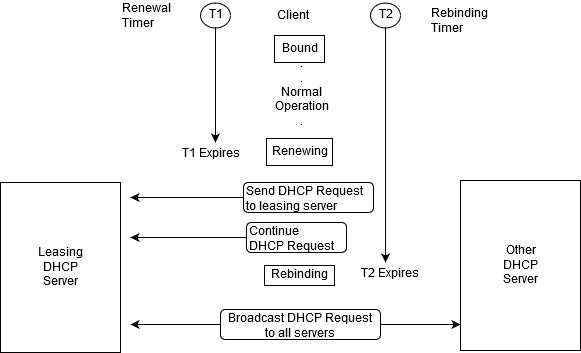


Figure 1. Renewal and Rebinding timers

Both the timers need to be set together since Renewal timer needs to have an expiration time before the Rebinding timer to manage the client’s lease renewal. If they are not set together, and the Rebinding timer goes off before the Renewal timer, the client might not have a chance to renew the lease on time.

1. [5 points] Explain how a network address is chosen when server receives a DHCPDISCOVER message.(see the RFC).

The DHCPDISCOVER message broadcasted by the client contains the following fields –

* Hardware address of the client
* Random transaction id
* Requested IP Address (optional)

On receiving the DHCPDISCOVER message, the server performs the following set of actions in its response –

* If the client has any current binding, the server determines if it can offer the lease and its terms.
* The server looks up the client’s hardware address in the database for any previous mappings, if available.
* If the client has requested a particular IP Address or lease length etc., the server checks if it is valid and if it can be allocated.
* If none of the above is applicable, a new IP address is chosen from a pool of IP addresses.
* Also, the server may decline the request at times.

When an IP address is requested, the sender’s subnet is also taken into consideration.

# Question 2: (VPNs and Private network Interconnection) [15 points]

1. [5 points] Is NAT completely transparent to a host? Try to find a sequence of packets that a host can transmit to determine whether it is located behind a NAT box.

Use STUN protocol to find if u are behind a NAT box

stunclient stun.2talk.com 3478

1. [5 points] Should a NAT box modify *all* ICMP error messages? Explain.

The NAT box should modify all the ICMP Error messages (other than the redirect message).

In order for the NAT to be transparent to end-host, the IP address of the IP header embedded within the payload of ICMP – Error message must be modified, the checksum field of the embedded IP header must also be modified along with the ICMP header checksum.

For example, consider the example of ICMP destination unreachable error message. The NAT must change the ICMP error message, translate the network address in datagram, recompute the checksums and forward the message to the localhost.

The redirect message does not contain the source IP address in its data and doesn’t need to be modified.

(Reference – RFC 3022)

1. [5 points] Explain how privacy can be breached while using VPNs. Specifically, state how the techniques used by VPNS for privacy can be compromised.

Reference: <http://searchenterprisewan.techtarget.com/news/2240104696/VPN-security-breaches-How-to-avoid-them>

1. MITM (Man in the Middle Attack) – This usually happens when people have access to either a wireless or a wired LAN. Thus, somebody can snoop on this connection, gather information (credentials for the session) in order to launch an attack on the session.
2. Physically accessing the VPN enabled device – If somebody loses their VPN enabled device. Consider the VPN client has pre-populated credentials and thus can connect very easily.
3. VPN security information, if obtained, can be another way to breach the VPN. This can be obtained via insider knowledge – social engineering or malicious emails or phone calls.
4. An SSL certificate or some shortcoming in the authentication system of the VPN could be exploited or spoofed or recreated maliciously in order to breach the VPN.

**Question 3: [25 points] [Multicast]**

3

2

2

1

1

1

2

4

Consider the topology shown in the Figure where all routers A, B, C, D, E, F are multicast-enabled routers.

1. [5 points] The *Steiner tree* is defined as the tree that has the minimum “cost” (that is, the tree having the smallest sum of the tree link costs). Find the Steiner tree that connects all of the routers. Suppose the link cost from B to D changes from 1 to 10. Find the resulting Steiner tree.
2. [5 points] Suppose that node C is chosen as the center in a center-based multicast routing algorithm. Assuming that each attached router in the multicast group uses its least cost path to node C to send join messages to C, draw the resulting center-based multicast routing tree. Is the resulting tree a minimum-cost Steiner tree? Justify your answer.
3. [5 points] The *least unicast-cost path tree* is defined as the union of the least cost unicast paths between a source and a set of destinations. Suppose that node E is chosen as the source. Compute the least unicast-cost path multicast routing tree from E to routers A, B, and F.
4. [5 points] Suppose that node E is the multicast source. Indicate paths over which packets will be forwarded using RPF.
5. [5 points] Suppose that each of the multicast routers receive one unit of traffic per unit of time from an attached host. This traffic must be forwarded to the other multicast routers. Suppose that node C is chosen as the center node in a center-based multicast routing protocol. Given the resulting tree, compute the rate of traffic on each link in the topology. (Compute the total amount of traffic on each link, regardless of the direction of the traffic flow). Suppose next that RPF is used to build four source-specific routing trees rooted at each of the routers A, B, E, and F. re-compute the rate of traffic on each of the links in this second scenario. In this example, does a center-based tree or a source-specific tree tend to *cencentrate* traffic?

**Question 4: (Mobile IP) [10 points]**

One of the advantages of IP tunneling is to allow the incremental deployment of new protocols in the Internet.

1. [3 points] What is IP tunneling?

IP Tunneling (Generic Routing Encapsulation) –

IP tunneling (IP encapsulation) is a technique that encapsulates IP datagrams within IP datagrams. It is a technique that allows datagrams to be encapsulated into IP packets and then redirected to an intermediate host. At this intermediate destination, the datagrams are de-capsulated and then routed to the next leg. In doing so, the trip to the intermediate host appears to the inner datagrams as one hop. The general outline of IP Tunneling or Generic Routing Encapsulation can be found in RFC 1701.

1. [3 points] How is IP tunneling used in Mobile IP?

The mobile node on a foreign network completes its registration with the home agent. After this, the Mobile IP datagram forwarding process is activated. The home agent then will intercept the datagrams for the mobile node as they pass through its home network and then forwarded to the mobile node. This is achieved by encapsulating the datagrams and sending them to the node’s address.

This encapsulation thus creates a “tunnel” between the device that encapsulates and the receiver that de-capsulates. The same concept is used in IPSec or VPN or the other tunneling protocols. The “tunnel” represents a medium over which the datagrams are forwarded across arbitrary networks with the details of the encapsulated datagram hidden.

1. [4 points] If a mobile host uses a foreign agent to receive and forward its messages, in most cases the mobile host need not even worry about IP tunneling. However, this is not true in the case of multicast messages forwarded from the home agent to the foreign agent, to the mobile host. Explain.

If a mobile host is a part of a multicast group, the address carrying the mobile host’s messages will be the address of this multicast group.

In a multicast group, if the home agent does not know about the mobile host’s membership, it will not listen to the messages for the multicast group. Hence, these messages will not be forwarded to the mobile host in its foreign network.

Thus, it is important for the mobile host to convey about its membership in a multicast group to a home agent.