# 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.

(RARP) only allowed a computer to obtain its IP address. When subnet masks were introduced, ICMP Address Mask messages were added to allow a computer to obtain a subnet mask. The chief advantage of such an approach lies in flexibility—a computer can decide which items to obtain from a local file on disk and which to obtain over the network. The chief disadvantage becomes apparent when one considers the network traffic and delay. A given computer must issue a series of small request messages. More important, each response returns a small value (for instance, a 4-octet IP address). Because networks enforce a minimum packet size, most of the space in each packet is wasted.

BOOTP

As the complexity of configuration grew, TCP/IP protocol designers observed that many of the configuration steps could be combined into a single step if a server was able to supply more than one item of configuration information. To provide such a service, the designers invented the

BOOTstrap Protocol

(BOOTP). 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.

Like other protocols used to obtain configuration information, BOOTP broadcasts each request.

* BOOTP server sends direct reply. Sometimes limited broadcast.
* ICMP = always broadcast. Floods the network with the

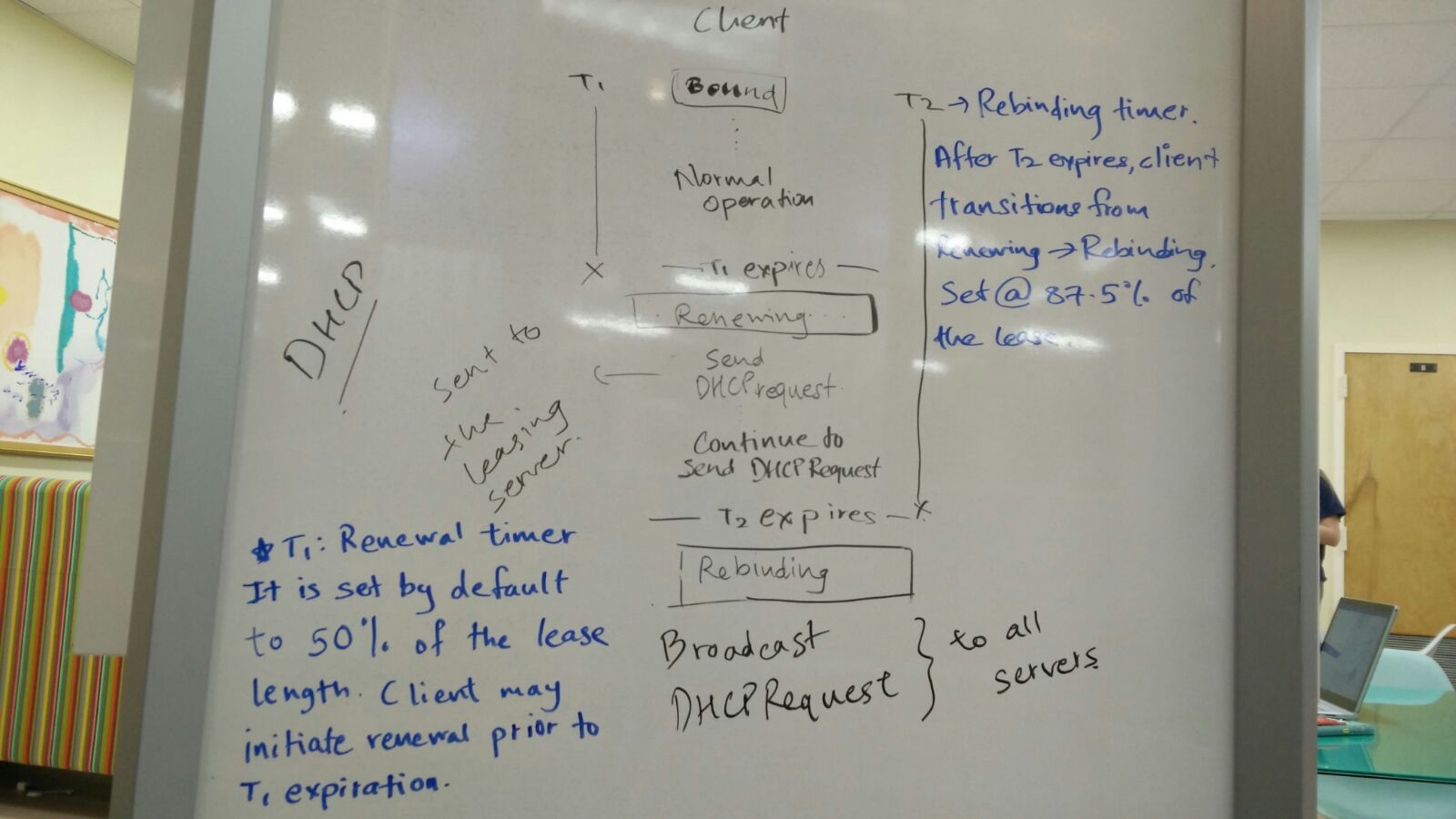
http://www.networksorcery.com/enp/protocol/icmp/msg17.htm

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?

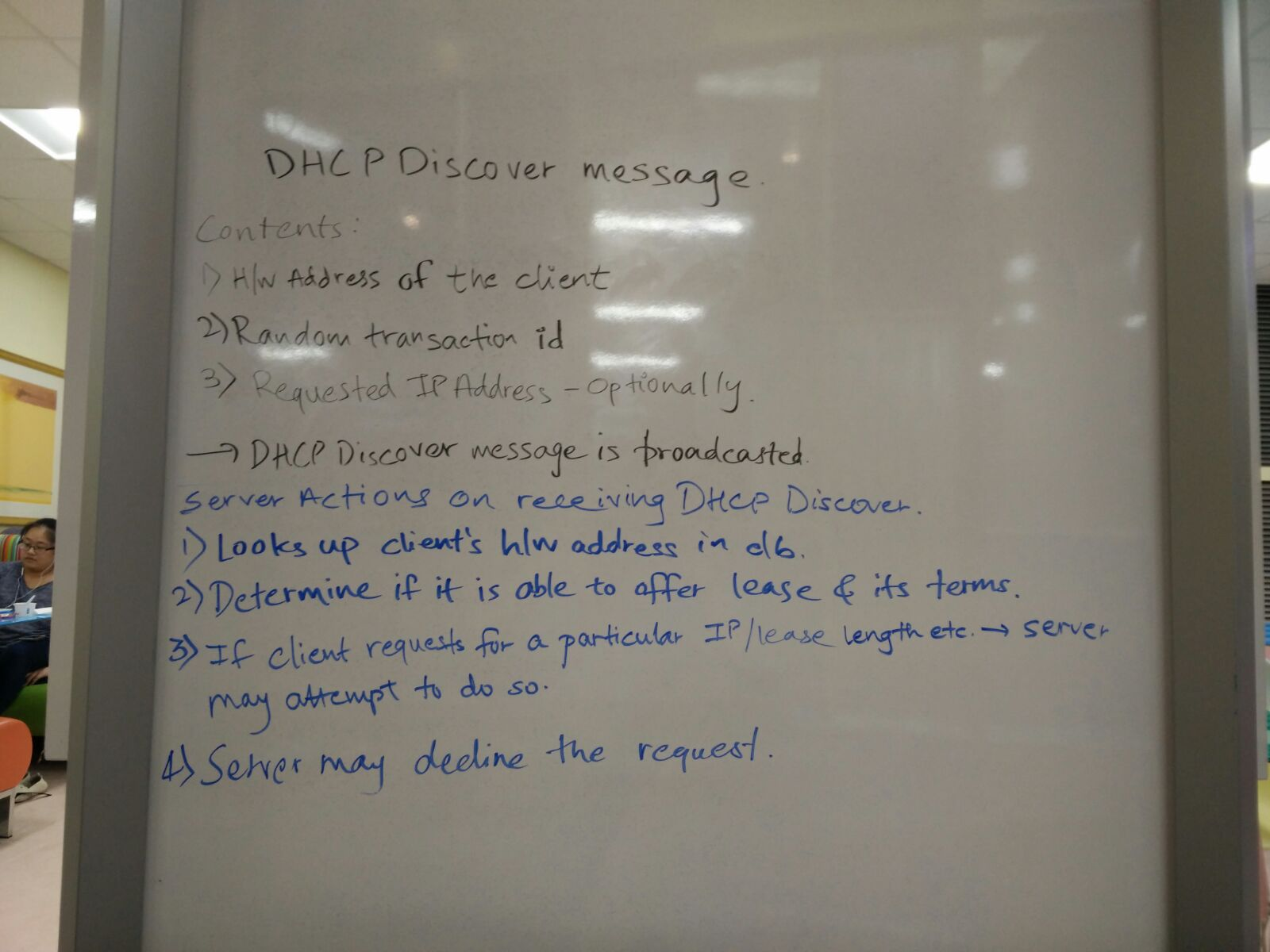
In the BOOTP request, the client can include its MAC address (typically held in non-volatile memory on the network card) and any previously bound IP address, if such information has been stored. The BOOTP server can then respond with a particular IP address for the client, based on either the MAC address mapping or the IP address that had been previously assigned.

https://technet.microsoft.com/en-us/library/dd296701(v=ws.10).aspx

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?



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



Response to DHCP Discover:

* The IP address to be assigned to the client, in the *YIAddr* field. If the server previously had a lease for this client it will attempt to reuse the IP address it used last time. Failing that, it will try to use the client's requested address if present; otherwise, it will select any available address.
* The length of the lease being offered.
* Any client-specific configuration parameters either requested by the client or programmed into the server to be returned to the client.
* Any general configuration parameters to be returned to all clients or clients in this client's class.
* The server's identifier in the DHCP *Server Identifier* option.
* The same transaction ID (*XID*) used in the *DHCPDISCOVER* message.

# 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.

Yes. The NAT box should modify all the ICMP error messages. 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.

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

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

4

3

2

1

2

2

1

1

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?
2. [3 points] How is IP tunneling used in Mobile IP?
3. [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.