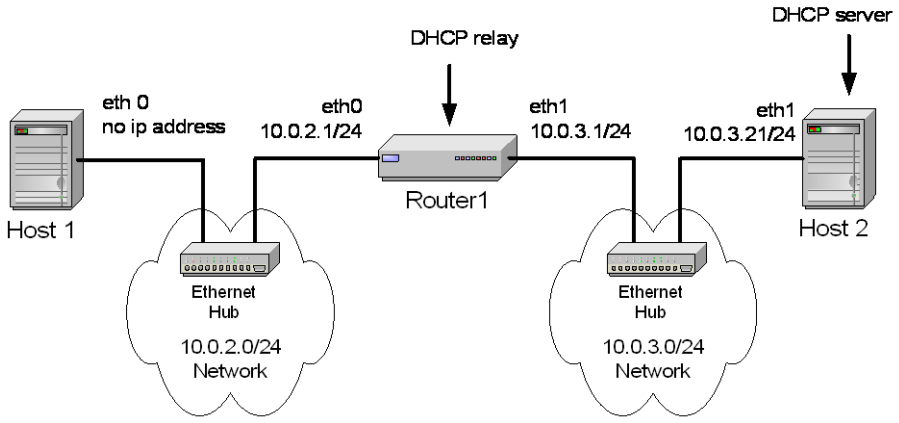
ECE 461 – Internetworking

Problem Set 8

Problem 1. In the figure below, Host1 is a DHCP client, Host 2 is a DHCP server. Router 1 is an IP router (i.e., IP forwarding is enabled), that is also configured as DHCP relay server.



a. *(4 Points)* Explain why Router1 needs to be configured as a DHCP relay server.

b. *(3 Points)* Describe how the relay server processes and directs a DHCP Discovery message from Host 1 and the DHCP Offer message to Host 1. Does the DHCP relay server modify the IP headers of the DHCP packets?

c. *(3 Points)* List the IP source and destination addresses in the DHCP Discovery and the DHCP Apply. If the addresses are changed at Router1, show the original and the modified addresses.

The following steps describe how a DHCP relay agent works:

1. The DHCP client broadcasts a DHCPDISCOVER packet.
2. The DHCP relay agent on the client's subnet forwards the DHCPDISCOVER message to the DHCP server by using unicast.
3. The DHCP server uses unicast to send a DHCPOFFER message to the DHCP relay agent.

4. The DHCP relay agent unicasts or broadcasts the DHCPOFFER packet to the DHCP client's subnet.
5. The DHCP client broadcasts a DHCPREQUEST packet.
6. The DHCP relay agent on the client's subnet forwards the DHCPREQUEST message to the DHCP server by using unicast.
7. The DHCP server uses unicast to send a DHCPACK message to the DHCP relay agent.
8. The DHCP relay agent unicasts or broadcasts the DHCPACK to the DHCP client's subnet.

Note: Communication between DHCP client and DHCP relay agent is identical to the "usual" communication between DCHP client and DHCP server. Note that the protocol allows broadcast and unicast for the transmission

a) Host 1 and DHCP server are on different subnets. DHCP server does not forward DHCP Discovery message since it has destination address 255.255.255.255.

b) DHCP relay agent replaces destination IP address in the DHCP Discovery message, by inserting the IP address of the DHCP server, and forwards the message to the 10.0.3.0/24 subnet.

   When the DHCP relay agent receives the DHCP Offer from the DHCP server, it replaces the IP destination address to either 255.255.255.255 (if the reply is made as broadcast) or the IP address of Host 1 (if the reply is made as unicast).

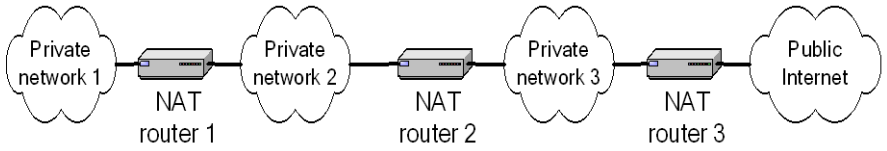
c) We assume that DHCP Discovery is sent as broadcast and DHCP Offer is sent as unicast) (Note that DHCP can force that replies are sent as broadcast).

Host 1:	DHCP Discovery	Dest. IP address: 255.255.255.255
Router 1 → DHCP server:	DHCP Discovery	Dest. IP address: 10.0.3.21
DHCP server → Router 1:	DHCP Discovery	Dest. IP address: 255.255.255.255
Router 1 → Host 1:	DHCP Discovery	Dest. IP address: offered IP address or 255.255.255.255

Problem 2. Consider a home network with a router that performs IP masquerading ("NAT router").

a. Normally, the NAT router assigns experimental IP addresses to the hosts in the home network. Explain the consequences (good and bad) if the NAT router assigns IP addresses which are not experimental.

b. Suppose a home network is set up with multiple cascaded NAT routers, as shown in the figure. Can such a configuration work? Explain.



c. NAT routers that perform IP masquerading support the use of "ping" from the internal to the external network. Why is this an issue, and how is it resolved?

Solutions:

a. The only consequence is that the systems in the private network cannot reach hosts in the public Internet with the assigned addresses.
Say, the NAT router assigns addresses 128.100.0.0/16 to the home network. Then, the systems in the home network cannot send packets to Internet hosts in the range 128.100.0.0/16 (since these packets are not routed to the public Internet).

b. Such a configuration works as long as the NAT routers assign addresses from a different address range.
For example, a problem exists when NAT router 3 assigns 10.0.1.0/24 addresses to Private Network 3, and NAT router 1 also assigns 10.0.1.0/24 to systems in Private Network 1. The (obvious) problem is that there are two IP networks with the same address block.

c. The problem is that ping issues ICMP Echo Request/Reply messages, which do not have TCP or UDP headers (and therefore, do not have port numbers).
Now, when two nodes in the private network (say 10.0.1.1 and 10.0.1.2) send a ping to the same external system with IP address 128.100.100.128, and the ICMP Echo reply returns to the NAT router, how does the NAT router decide which internal host (10.0.1.1 or 10.0.1.2) should receive the reply.

The solution is that NAT routers must be aware of ICMP traffic, and must maintain information on ICMP Echo Request packet, so that they can be matched with returning ICMP Echo Reply messages.
Since ICMP Echo Reply messages contain the ICMP Echo Request Message which triggered the reply, the NAT router can perform a matching of ICMP messages as long as it caches the ICMP Echo Request message.