Lab Exercise 4: IP & Network Layer

AIM

To gain a better understanding of the IP and ICMP protocol.

EXPERIMENT 1: Understanding IP by using ping and traceroute

Tools

For this experiment, we will use the ***traceroute*** and ***ping*** programs. These utilities are usually used by the network administrators to identify problems in the network. ***Traceroute*** is a program used to print the route that packets take from the source host to the destination host. This program utilises the IP protocol "time to live" filed and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host. Traceroute operates by first sending one or more datagrams with the time-to-live (TTL) field in the IP header set to 1; it then sends a series of one or more datagrams towards the same destination with a TTL value of 2; it then sends a series of datagrams towards the same destination with a TTL value of 3; and so on. Recall that a router must decrement the TTL in each received datagram by 1 (actually, RFC 791 says that the router must decrement the TTL by at least one). If the TTL reaches 0, the router returns an ICMP message (type 11 – TTL-exceeded) to the sending host. As a result of this behaviour, a datagram with a TTL of 1 (sent by the host executing traceroute) will cause the router one hop away from the sender to send an ICMP TTL-exceeded message back to the sender; the datagram sent with a TTL of 2 will cause the router two hops away to send an ICMP message back to the sender; the datagram sent with a TTL of 3 will cause the router three hops away to send an ICMP message back to the sender; and so on. In this manner, the host executing traceroute can learn the identities of the routers between itself and destination X by looking at the source IP addresses in the datagrams containing the ICMP TTL-exceeded messages.

The ***ping*** program sends ICMP ECHO_REQUEST datagrams to elicit an ICMP ECHO_RESPONSE from a host or gateway.

Exercise

Follow the steps described below. You will notice certain questions as you attempt the exercise. Write down the answers for your own reference. The solutions will be put up on the webpage at the end of the lab. If you have any questions or are experiencing difficulty with executing the lab please consult your lab teacher.

Step 1: Open an xterm.

Step 2: Use the ping command to trace the route/path between your host and the following web server: www.fbe.unsw.edu.au. Type the following command:

```
ping –c 4 www.fbe.unsw.edu.au
```

The –c 4 option limits the number of ping packets that your host sends to 4. The –R option stands for record route. This includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Some hosts ignore or discard this option.

Step 3: Now run the traceroute program with the same web server as the destination. traceroute www.fbe.unsw.edu.au

Question 1. What is the path indicated by traceroute? Is the path given by ping the same as traceroute?

Question 2. Why are there three time values indicated for each router along the path? What does this time value indicate?

Question 3. Do you observe a situation in the traceroute output where the time for an earlier router is less than that for the next router? If so, what is reason for this?

Step 4: A number of sites on the Internet provide traceroute services. A user specifies the host whose route they want to trace and the site returns the path from the specified host to the site (not to the user's host). One such site is http://www.kloth.net/services/traceroute.php.

Question 4. Go to this site (http://www.kloth.net/services/traceroute.php) and trace the path from there to www.cse.du.ac.bd and also your host. What is the path? Explain the meaning of * and any other special characters in the path listing you get?

Step 5: Now do a reverse trace from your host to www.kloth.net (or any other traceroute site that you have used) by typing:

```
traceroute www.kloth.net
```

Question 5. Is the path the same as in Question 6? Explain any abnormalities that you notice in the output?

EXPERIMENT 2: Using Wireshark to study Traceroute

Tools

For this experiment, we will use the Wireshark packet analyser that we used extensively in the previous labs. Before you begin go to the "Trace Files" link and download the trace for the IP lab.

Step 1: Open an xterm and run Wireshark.

Step 2: Load the trace file ip-ethereal-trace-1 . This file captures the packets exchanged between a host in mit.edu and gaia.cs.umass.edu while running the traceroute program. Filter out all other protocol packets by typing "icmp" in the filter field. In this trace, you should be able to see the series of ICMP Echo Request packets sent by the host (in mit.edu) and the ICMP TTL-exceeded messages returned to this host by the intermediate routers to gaia.cs.umass.edu.

Step 3: Select the first ICMP Echo Request message sent by the host, and expand the Internet Protocol part of the packet in the packet details window.

Question 1. What is the IP address of the source host?

Question 2. Within the IP packet header, what is the value in the upper layer protocol field?

Question 3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Question 4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented?

Step 4: Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Navigate in the window till you reach the Echo requests sent by the host computer (search for the IP address that you wrote as the answer to Question 1 of this experiment). Select the first ICMP Echo Request message sent by the host computer, and expand the Internet

Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP below this first ICMP packet. Use the down arrow to move through the ICMP messages sent by the host.

NOTE: Only consider the first 39 echo requests sent from the host. Neglect the other echo requests.

Question 5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by the host (in mit.edu)?

Question 6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Question 7. Describe the pattern you see in the values in the Identification field of the IP datagram.

Question 8. Now examine the ICMP messages and observe the pattern of the Identifier field within the ICMP messages (Note that this is different from the IP Identification field in the IP header). What do you observe?

Step 5: Now (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to this host by the nearest (first hop) router.

Question 9. What is the value in the Identifier field in the ICMP message and the TTL field in the IP header for the first response? (NOTE: Do not look at the identification field in the IP datagram header, look at the contents of the ICMP message for the Identifier field).

Question 10. Do these values remain unchanged for all of the ICMP TTL-exceeded replies to the host from the nearest (first hop) router? Why?