COMP 3331/9331: Computer Networks and Applications

Lab Exercise 4: IP, Network Layer and Ethernet (Solutions)

AIM

To gain a better understanding of the IP, ICMP and Ethernet protocols.

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 week. If you have any questions or are experiencing difficulty with executing the lab please consult your lab instructor.

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 -R www.fbe.unsw.edu.au
```

The *–c 4* option limist 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.

Question 1. What is the path taken by the ping packet?

Answer:
(NOTE: This answer is a sample; you might get different answers depending on what host you are running this command on and where you are located.)
Path:

```
wagner.orchestra.cse.unsw.EDU.AU (129.94.242.19)
gaszr1.uwn.unsw.EDU.AU (129.94.6.121)
129.94.6.114
129.94.108.130
emuweb.fbe.unsw.EDU.AU (129.94.108.143)
vlan379.redcr1.gw.unsw.EDU.AU (129.94.6.113)
129.94.6.122
vlan385.gaszr1.gw.unsw.EDU.AU (129.94.242.1)
wagner.orchestra.cse.unsw.EDU.AU (129.94.242.19)
```

This query was made from host *wagner*. The path shows that there are 3 routers in the path from *wagner* to the web server at FBE, starting with *gaszr1.uwn.unsw.EDU.AU* (129.94.6.121). The return path from *emuweb.fbe..* also spans 3 routers back to wagner.

Question 2. Why do you think that the IP addresses along the forward and reverse route for the different routers are different?

Answer: Note that a router has at least two interfaces, hence although a packet may traverse the same routers in the forward and return paths, the actual interfaces that forward the packet will have different IP addresses.

Step 3: Now run the *traceroute* program with the same web server as the destination.

```
traceroute www.fbe.unsw.edu.au
```

Question 3. What is the path indicated by *traceroute*? Is the path given by *ping* the same as *traceroute*?

Answer:
(NOTE: This answer is a sample; you might get different answers depending on what host you are running this command on and where you are located.)
The path indicated by traceroute is:

```
1   vlan385.gaszr1.gw.unsw.EDU.AU (129.94.242.1)   4.606 ms  3.097 ms  3.978 ms
2  129.94.6.122 (129.94.6.122)  0.232 ms  0.261 ms  0.239 ms
```

```
3   vlan379.redcr1.gw.unsw.EDU.AU (129.94.6.113)   1.114 ms
0.384 ms  0.422 ms
4  emuweb.fbe.unsw.EDU.AU (129.94.108.143)  0.357 ms  0.450
ms  0.361 ms
```

The traceroute path is the same as the return interfaces traced by ping. This is because the mechanism for traceroute is such that the return interface is recorded (the interface that receives a packet with a ttl value of 1 sends a "time exceeded" message to the source). In contrast, ping records both the forward and return path interfaces.

Question 4. Why are there three time values indicated for each router along the path? What does this time value indicate?

Answer: There are 3 time values for each router along the path because traceroute by default sends three probe packets with the same TTL value. The time measures the RTT between the source and this particular router.

Question 5. 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?

Answer: Yes this is possible. As seen in the above response, the time indicated for the first router is greater than the second one. The reason for this is that the probe packets sent out for the successive routers experience different queuing delays. The difference in the value of the queuing delays is far greater than the actual difference between the propagation delays for these successive routers.

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 https://www.telstra.net/cgi-bin/trace.

Question 6. Go to this site (http://network-tools.com/) and trace the path from there to your host. What is the path? Explain the meaning of * and any other special characters in the path listing you get?

Answer:
(NOTE: This answer is a sample; you might get different answers depending on what host you are running the traceroute on and where you are located.)

```
TraceRoute from Network-Tools.com to 202.171.168.114 [202-171-168-
114.static.cpe.bigair.net.au]
Hop  (ms)  (ms)  (ms)          IP Address     Host name
1     *     *     *           -
2     *     *     *           -
3     *     *     *           -
4     *     *     *           -
5     *     *     *           -
6     32    32    32     4.69.144.80    ae-2-70.edge1.losangeles6.level3.net
7     216   216   220    4.26.0.166     aapt-limite.edge1.losangeles6.level3.net
8     *     *     223    202.10.14.201       lag41.sclarinte01.aapt.net.au
9     *     *     219    202.10.14.196       lag30.sglebinte01.aapt.net.au
```

```
10     *     *     *           -
11     216   216   216     202.171.175.196     -
12     210   209   210     202.171.175.101     -
13     218   218   217     202.171.168.114     202-171-168-114.static.cpe.bigair.net.au
Trace complete
```

This particular router shows some * signs; there are a number of possible explanations for an asterisk in place of the time value in front of a router: the router might not be sending any 'time exceeded' messages at all, it may be sending the message but with a small ttl value such that the message never gets to the source.

You might also see this symbol in the output: *!A*
!A means access to the network on which www.telstra.net resides is prohibited. As a result all probe packets with a ttl value larger than the value this string appears in front of do not give us any new information.

If other special characters appear in your output, check out the man pages for the explanation.

Step 5: Now do a reverse trace from your host to network-tools.com (or any other traceroute site that you have used from the above list), by typing, for example:
`traceroute network-tools.com`

Question 7. Is the path the same as in Question 6? Explain any abnormalities that you notice in the output?

Answer:
(NOTE: This answer is a sample and generated from a windows machine; you might get different answers depending on what host you are running the traceroute on and where you are located. Look up any special characters that appear in your output and make sure you understand why they occur.)

```
Tracing route to network-tools.com [190.93.242.109] over a maximum of 30 hops:

  1     6 ms     4 ms     4 ms  192.168.0.1
  2     *        4 ms     3 ms  newcollegevillage.bacb.com.au [172.16.0.1]
  3    14 ms     7 ms     8 ms  202-171-168-125.static.cpe.bigair.net.au [202.171.168.125]
  4     *        *        *     Request timed out.
  5    17 ms    14 ms    22 ms  202.171.175.203
  6    11 ms     7 ms     7 ms  13335.syd.equinix.com [202.167.228.154]
  7     6 ms     5 ms     5 ms  cf-190-93-242-109.cloudflare.com [190.93.242.109]

Trace complete.
```

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 lab. Before you begin go to the "Lab Traces" link on the course webpage and download the trace for the IP lab.

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 week. If you have any questions or are experiencing difficulty with executing the lab please consult your lab instructor.

Step 1: Open an xterm and run Wireshark.

Step 2: Load the trace file *ip-ethereal-trace-1* by using the *File* pull down menu, choosing *Open* and selecting the appropriate trace file. 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?

Answer: The IP address of the source host is 192.168.1.102

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

Answer: The contents of the upper layer protocol field are 0x01. This is represented in hexadecimal and the decimal equivalent for this is 1. Note the corresponding values for TCP and UDP are 6 and 17 respectively.

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.

Answer: The IP header is 20 bytes long. The Header length field in the IP headers indicates this. The total size of the IP datagram is 84 bytes as indicated by the Total Length field in the IP header. Since the header constitutes 20 bytes, the payload of the IP datagram (which contains the ICMP packet: ping request) is 64 bytes.

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

Answer: No this IP datagram has not been fragmented. First of all the fragment flag (More fragments flag) is zero indicating that this is surely not the first or middle fragment (Note that only the last fragment of a fragmented datagram can have the flag set to 0). Further the fragment-offset field is also zero. (Note that the last fragment of a fragmented datagram cannot have a zero value from the fragment-offset field).

Step 4: Next, sort the traced packets according to IP source address by clicking on the *Source* column header; a small upward pointing arrow should appear next to the word *Source*. If the arrow points down, click on the *Source* column header again (because you want to sort the packets from one source address in order of arrival). 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)?

Answer: If you observe the series of IP datagrams carefully you will notice that the TTL (Time To Live) field is increasing for each subsequent segment send by the host. This is due to the fact that these datagarms are being generated by the Traceroute program.

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

Answer: The following header fields in the IP daragarm remain unchanged across the subsequent messages: Version, Header Length, Type of Service (indicated by Differentiated Service Field in Wireshark), Flags (for fragmentation), Fragmentation Offset, Upper Layer Protocol (which is ICMP), Source IP address and Destination IP address. Of these fields, the Version, Upper Layer Protocol, Source IP address and Destination IP address fields *must* remain the same. Other fields may change. The identifier field must change in each of the datagrams since this uniquely identifies each IP datagram. The TTL field must change since Traceroute changes the TTL field in each subsequent packet sent to a particular router. Finally the header checksum must change since the above two header fields are surely different in each subsequent datagram.

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

Answer: The identification field is incremented by one in the sequence of IP datagrams.

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?

Answer The identifier field within the ICMP message is the same: 0x0300. Note that this traceroute program was run on a Windows machine in which the OS inserts the process id of this program into the identifier field of the ICMP packet. This value will be the same for all ICMP messages generated by the host.

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. Do not look for reply messages from the host that is in the destination of the Echo request – we are looking for messages from routers along the path to the destination, not the destination itself.

Question 9. Now examine the payload of the first response message. What is the value in the Identifier field in the ICMP message (which is contained in the payload) 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 contained in the payload for the Identifier field).
Hint: The first hop router will usually be the one that responds earliest and it will have the maximum TTL value among all TTL exceeded replies sent to the host.

Answer: Note that the first hop router has the IP address 10.216.228.1. The Identifier field contains the value: 0x0300 (which is copied from the ICMP request message). The TTL value is 255.

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?

Answer: The values of the TTL field in the IP datagram and the Identifier field in the ICMP message remain unchanged in all the ICMP TTL-exceeded replies received from the first hop router. The value contained in the Identifier field is simply copied from the ICMP echo request messages that are received from the host. Now since this value is always 0x0300 in all the echo request packets (as explained earlier), the corresponding value in the Identifier field for the TTL-exceeded replies will also be the same. The TTL field is also the same in all the replies since the TTL value in the IP datagram generated by the nearest (first hop) router is always 255 and this router is just one hop away from the host. Notice that the TTL value is not decremented as a result of this.

END OF LAB