Answer sheet for Lab – ICMP

# The diagrams are based on the trace route provided by the book author and found in the Resources in Miscellaneous Folder.

# Step 2: Echo (ping) Packets

Answers to the questions:

1. Echo Request: Type = 8, Code = 0 ; Echo Reply: Type = 0, Code = 0
2. The Identifier and Sequence number for both the echo reply and echo request are the same which is: Identifier (BE): 20731 (0x50fb), Identifier (LE): 64336 (0xfb50), Sequence number (BE): 0 (0x0000) Sequence number (LE): 0 (0x0000).
3. The Identifier numbers in successive echoes remain the same. The Sequence number s change(BE:1,2,3,4,5,etc)(LE:256,512,768,1024,etc)
4. The data in the echo request and the date in the echo reply are the same (44 bytes)

**Step 3: TTL Exceeded (traceroute) Packets**

IP header fields

Type

=11

1 byte

1 byte

IP header

20 bytes

ICMP payload

28 bytes

Start of message

Code

=0

2 bytes

Checksum

ICMP header

8 bytes

IP header

ICMP header

Figure : Format of an ICMP TTL Exceeded Message

There are several features to note:

* The length of 20 bytes is for a typical IPv4 header with no IP option fields.
* The Type and Code values are for an ICMP TTL Exceeded in transit message.
* The ICMP header is given as 8 bytes, yet the fields only add up to 4 bytes. There are an extra four bytes after the checksum that are historically unused. They are not shown in the figure because they are not shown in most versions of Wireshark.
* The size of the ICMP payload depends on the router implementation. The value of 28 bytes is what we saw in practice. The start of an IP packet is shown in these bytes, including an IP header and ICMP header for the echo request packet that triggered the ICMP TTL Exceeded message.

Answers to the questions:

1. Type: 11, Code: 0
2. All ICMP messages start with the same Type/Code (and Checksum) fields, so the receiver can process these fields. Their value tells the receiver the kind of ICMP message, and hence what fields follow.
3. The Type/Code and Checksum fields take up 4 bytes. However, the ICMP header is actually 8 bytes long. These fields are followed by 4 bytes that are unused (except for recent ICMP extensions) and hence do not show up in Wireshark as named fields. You can still see that they are there by selecting the ICMP block and the payload, and observing that they differ by 8 bytes.
4. The inner IP packet has TTL=1 in our case, but depending on the router implementation it is possible that you will see TTL=0. It must be one of these values for the case of an ICMP TTL Exceeded message because the message is triggered when the TTL is decremented during processing and reaches 0, i.e., the TTL held a value of 1 when the packet arrived at the router.

# Step 4: Internet Paths

Answers to the questions:

1. The IP source address of the TTL Exceeded packet is the IP address of the router, because the router created the TTL Exceeded packet putting its own IP address in the source field.
2. Traceroute probes each piece path more than once just in case of packets are lost.
3. The echo request packet should have an IP source of your computer, an IP destination of the far end of the path, and a TTL value set to N. The last part is the key where the routers will decrement the TTL and it will reach zero N hops away from the source towards the destination. The ICMP TTL Exceeded message will be sent back to the source.



Your computer

IP addr = 192.168.1.122

Destination www.cs.vu.nl

IP addr = 130.37.20.20

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Hops

from

source

??

??

comcast.net

surf.net

as6453.net

vu.nl

Figure : Path from computer to www.cs.vu.nl found by traceroute

There are several features to note:

* The start of the path is not named because it starts within a home; the address 192.168.xx.xx is in private address space that is NATed to reach the public Internet. This will likely be the case if you run the traceroute from a home.
* as6453.net is Tata Communications, comcast.net is Comcast, surf.net is SURFnet, and vu.nl is Vrijie Universitiet Amsterdam. You can often find names like this with a Web search and an educated guess, or by using a WhoIS lookup service such as whois.net to consult domain registration records.