Lab Exercise – ICMP Ying Di

Step 2: Echo (ping) Packets

1. What are the Type/Code values for an ICMP echo request and echo reply packet, respectively?

A: echo request: 8; echo reply: 0

2. How do the Identifier and Sequence Number compare for an echo request and the corresponding echo reply?

A: The Identifier and Sequence Number compare for an echo request and the corresponding echo reply should be same

3. How do the Identifier and Sequence Number compare for successive echo request packets?

A: For the same echo request packets, the Identifier should remain the same and the Sequence Number should increase. For successive echo request packets, the Identifier should be different too.

4. Is the data in the echo reply the same as in the echo request or different?

A: Yes the data are the same.

Step 3: TTL Exceeded (traceroute) Packets

|----20 bytes---|----1 byte---|----1 byte----|-----2 bytes----|

IP Headers	Type=11	Code=0	Checksum	IP Header	ICMP Header

|---------ICMP Header: 8 bytes-------------|------ICMP payload 28 bytes------|

1. What is the Type/Code value for an ICMP TTL Exceeded packet?

A: The Type/Code value for an ICMP TTL Exceeded packet is 11/0

2. Say how the receiver can safely find and process all the ICMP fields if it does not know ahead of time what kind of ICMP message to expect. The potential issue, as you have probably noticed, is that different ICMP messages can have different formats. For instance, Echo has Sequence and Identifier fields while TTL Exceeded does not.

A: Since the ICMP messages would contain the same Type/Code, so the receiver can recognize the correct ICMP fields and process them.

3. How long is the ICMP header of a TTL Exceeded packet? Select different parts of the header in Wireshark to see how they correspond to the bytes in the packet.

A: The ICMP header of a TTL Exceeded packet is 8 bytes long.

4. The ICMP payload contains an IP header. What is the TTL value in this header? Explain why it has this value. Guess what it will be before you look!

A: The TTL value in this header is 1, because the TTL is decremented during processing.

Step 4: Internet Paths

1. How does your computer (the source) learn the IP address of a router along the path from a TTL exceeded packet? Say where on this packet the IP address is found.

A: The IP source address of the TTL Exceeded packet is the IP address of the router. Where is found: The IP source address of the TTL Exceeded packet.

2. How many times is each router along the path probed by traceroute? Look at the TTL Exceeded responses and see if you can discern a pattern.

A: three times; pattern: triples of echo / TTL exceeded from a given router

3. How does your computer (the source) craft an echo request packet to find (by eliciting a TTL Exceeded response) the router N hops along the path towards the destination? Describe the key attributes of the echo request packet.

A: An echo request will contain 3 parts: 1. IP source of your computer; 2. an IP destination of the far end of the path; 3. TTL value = N, which is the key
The TTL value will be decremented by the router, and it will reach zero N hops away from the source towards the destination.