Lab 5 ICMP

ICMP (Internet Control Message Protocol) is a companion protocol to IP that helps IP to perform its functions by handling various error and test cases. It is covered in Chapter 5.7.4 of the textbook. Review the textbook section before doing this lab.

Objective

- Know the format of ICMP datagram.
- Understand how ICMP works, e.g., operations of ICMP Echo, Timestamp, TTL Exceeded and Host Unreachable messages.
- Know common network failures.

Requirements

You need to install following tools on your computer beforehand:

- **Wireshark:** This lab uses the Wireshark software tool to capture and examine a packet trace. Refer to previous labs for details.
- ***ping*:** The parameters on Windows and Linux are different. Refer to previous labs for details.
- ***traceroute / tracert*:** Refer to previous labs for details. Parameters and detailed operations are different on Windows and Linux. Check referenced materials provided on course website!

Some tasks need to write *socket programs* to generate ICMP message, e.g., ICMP Timestamp Message. I have provided you the source code and **executable binaries** on the course website. You can directly use **the executable binary on Windows**. Or, you can compile your source code by yourself. If so, you need to install MinGW on Windows. (The source code of the program can be easily ported to Linux OS.)

- **MinGW:** MinGW, a contraction of "Minimalist GNU for Windows", is a minimalist development environment for native Microsoft Windows applications. Refer to http://www.mingw.org/ to install the basic runtime environment of MinGW. (You MUST install packages of both "MinGW Base System" and MSYS).

Exercise

Before starting following tasks, choose a remote server that you can both *ping* and *traceroute*.

Tips:

- For *ping*, use "*ping* www.jnu.edu.cn" or "*ping* www.baidu.com". Use the parameter "-4" to instruct to use IPv4 if *ping* uses IPv6, e.g., "*ping* -4 www.jnu.edu.cn".

- For traceroute: On Windows, "*tracert* www.jnu.edu.cn" or "*tracert* -4 www.jnu.edu.cn" to indicate using of IPv4. On Linux/MacOS, use "*traceroute* -I www.jnu.edu.cn", where "-I" (lower case "i") tells *traceroute* to send ICMP probes.
- If you can not find an available remote server for both *ping* and *traceroute*, use the traces that we supply on the course website.

Task 1: Capture and Explore Trace of Echo (*ping*)

The *ping* command will use ICMP Echo request and reply.

1. Launch Wireshark and start a capture with a filter of "*icmp"*. (Remember to choose correct interface)
2. *ping* the remote server that you choose, e.g., "*ping* www.jnu.edu.cn"
3. Stop Wireshark and inspect the trace you captured.

Answer the following questions:

1. What are the *Type* and *Code* values for ICMP echo request and echo reply messages, respectively?
2. Identifier and Sequence Number:
   (a) What are the values of *Identifier* and *Sequence Number* for an echo request and its corresponding echo reply? Compare values of these two fields with successive echo request messages?
   (b) Explain how to match an ICMP echo request to an echo reply message?
3. Are the data in the echo reply the same as in the echo request or different?

Task 2 Capture and Explore Trace of TTL Exceeded (traceroute)

The *traceroute* command will use ICMP TTL Exceeded message. (Remember to add "-I" on Linux!)

1. Launch Wireshark and start a capture with a filter of "*icmp"*. (Remember to choose correct interface)
2. *traceroute* the remote server that you choose, e.g., "*tracert* www.jnu.edu.cn" on Windows.
3. Stop Wireshark and inspect the trace you captured.

Tips: Look at the traceroute portion of the trace, which will have a series of ICMP echo request packets followed by ICMP TTL Exceeded packets. The echo requests are sent from the source (your computer) to the destination whose path is being probed. The TTL Exceeded packets are coming from routers along the path back to your computer, triggered by the TTL field counting down to zero

Answer the following questions:

1. What is the *Type* and *Code* values for an ICMP TTL Exceeded packet?
2. 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.
3. The ICMP payload contains an IP header. What is the TTL value in this IP header?

Explain why it has this value.

4. By looking at the details of the packets, answer the following questions:
   (1) How does your computer (the source) learn the IP address of a router along the path from a TTL exceeded packet? Or where on this packet the IP address is found?
   Tips:
   - You may check an echo packet to see the source and destination IP addresses. The routers along the path will have a different IP address, and this address will be present on the TTL Exceeded packet.
   - If you are unsure, you can examine the *traceroute* text output to see the IP addresses of routers and look for these addresses on the TTL Exceeded packets.

   (2) How many times does each router along the path probed by *traceroute*?
   Tips: Look at the TTL Exceeded responses and see if you can discern a pattern.

   (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.
   Tips: The echo request packets sent by traceroute are probing successively more distant routers along the path. You can check these packets and see how they differ when they elicit responses from different routers.

Task 3 Capture and Explore Trace of ICMP Timestamp

To send ICMP Timestamp message, you need to write your own programs. I have provided you a *C program* on the course website. You can also use the *executable binary* file that I have compiled for you. Check the course website to download them.

1. Download and compile the "*icmp-timestamp.c*" in MinGW. Or you can also use the "*icmp.exe*" that I have already compiled for you on Windows OS.
2. Launch Wireshark and start a capture with a filter of "*icmp"*. (Remember to choose correct interface)
3. Run the "cmd.exe" or "MSYS" as Administrator on Windows.
   Tips:
   - You can run the compiled "*icmp.exe*" in either "cmd.exe" or "MSYS" of MinGW on Windows.
   - To run a program as Administrator on Windows, choose "*Run as Administrator*" in the right-click menu of either "cmd.exe" or "MSYS". See following figure.
   - The source code is implemented using *Winsocket*, which follows the style of *Berkeley socket*. Thus, it can be easily ported to compile and run on Linux with minor modification. In case of Linux, you may need to run it with "*sudo*".

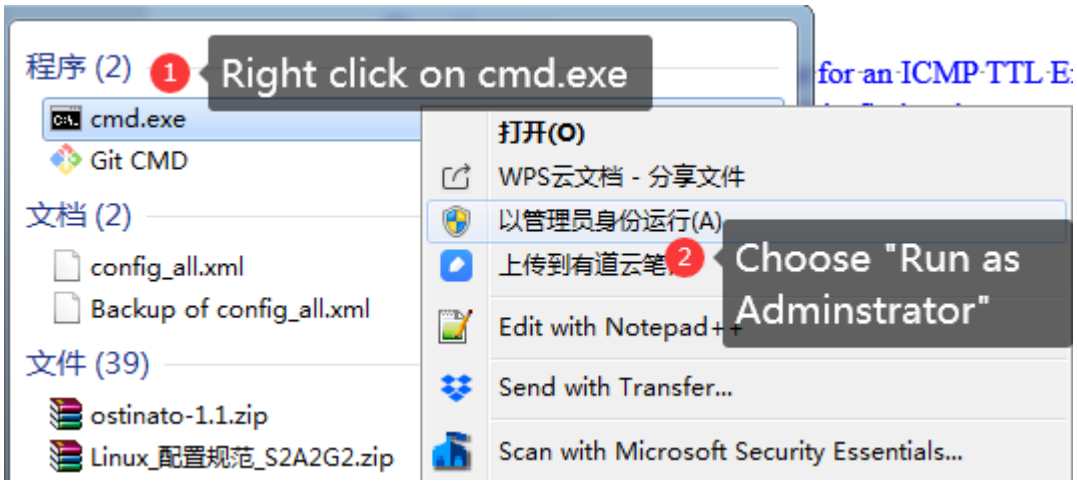

Figure 1: Run CMD as Administrator on Windows

4. Run the following command of the compiled program: "*icmp.exe* 192.168.1.168". You NEED to replace the IP address with either your *default gateway* or *another remote server*.

   Tips:

   - Some servers may DO NOT respond ICMP Timestamp requests. And some networks may block ICMP timestamp messages. If so, try another remote server, e.g., your default gateway or another server in the same local LAN.
   - If you still cannot receive any ICMP Timestamp replies, please USE the ICMP Timestamp Wireshark trace that we supply on the course website.

5. Stop Wireshark and inspect each fields of packets in the trace you captured. Fill the following table:

Table 1 Experimental results of ICMP Timestamp

Timestamp Request Message		**Timestamp Reply Message**	
Field	**Value**	**Filed**	**Value**
Type		**Type**	
Identification		**Identification**	
Sequence		**Sequence**	
Originate Time		**Originate Time**	
Receive Time		**Receive Time**	
Transmit Time		**Transmit Time**	

Answer the following questions:

1. What's the usage of ICMP Timestamp messages?
2. What is the advantage of using timestamp rather than the system time of each host?
3. Explain at least one drawback of ICMP Timestamp.

   Tips: The timestamp here is the number of milliseconds since midnight of UTC. How about the date?

Task 4 Capture and Explore Trace of ICMP Host Unreachable

When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a *destination-unreachable message* back to the source host that initiated the datagram. Destination-unreachable messages can be created by either a router or the destination host.

Detailed reasons for destination unreachable include: Network Unreachable, Host Unreachable, Port Unreachable, Protocol Unreachable, Fragmentation Needed and "Don't Fragment" bit set and Source Route failed.

In this task, we only investigate *Host Unreachable ICMP message*. (**Tips:** It is usually sent by the last router in the path to an existing network).

1. Launch Wireshark and start a capture with a filter of "*icmp*". (Remember to choose correct interface)
2. Use *ping* command to probe an IP address that does NOT exist.
   Tips:
   - Since Host Unreachable is sent by a router, you'd better *ping* an IP address that does NOT belong to local network (i.e., different network ID).
   - You may receive many "Request timed out" of *ping* before receiving a "Host Unreachable". Thus, try more times! And try other non-exist IP addresses until you receive a "Host Unreachable" message in the Wireshark.
   - If you still cannot capture a "Host Unreachable" message, use the Wireshark trace supplied for you on course website.
3. Stop Wireshark and inspect the trace you captured.

Answer the following questions:

1. What's the *Type* and *Code* value of the Host Unreachable message? Research by yourself to explain the meaning of other code values under the same *Type*?
2. Who can generate the destination unreachable message?

Task 5: Explore on Your Own (Not required in the lab report)

We encourage you to explore ICMP on your own once you have completed both IPv4 and ICMP labs, since IP and ICMP are strongly related. Some ideas:

- We studied ICMP traffic produced by *ping* and *traceroute*. There are a variety of other ICMP messages that indicate other network conditions, such as path MTU discovery and port unreachable messages. See if you can capture other ICMP messages, and examine these messages.
- Explore other ICMP based tools that examine the network, such as *pathchar* which estimates the speed of the links along the network path.
- You can also write your own program to generate more other types of ICMP messages.

Questions:

1. Different ICMP messages can have different formats. For instance, Echo has *Sequence* and *Identifier* fields while TTL Exceeded does not. Explain 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.

2. Why TTL should be configured in IP packets?
3. Why ICMP error-reporting message cannot be generated if error happens during transmitting ICMP datagrams?
4. What kinds of ICMP messages could be sent by a router? What kinds of ICMP messages could be sent by a destination host?
5. In ICMP messages, does the checksum cover payload?