School of Computer Science and Cybersecurity

CUC

Lab Report #

|  |  |
| --- | --- |
| Lab Name | xxxxx |
| Course Name | Computer Networks |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | 赵婧宇 | Student ID | 201711123028 |

|  |  |
| --- | --- |
| Partners |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | 2019.06.03 | Lab Location | #48 |

|  |
| --- |
| Notes： |

**Section I Introduction**

Prepares the reader to understand the whole experiment.

|  |  |
| --- | --- |
| **Must Have:**  1. Clearly stated purpose of the experiment  2. Important background and/or theory | **May include:**  1. Description of specialized equipment  2. Justification of experiment's importance |

In this lab, we’ll explore several aspects of the ICMP protocol:

• ICMP messages generating by the Ping program;

• ICMP messages generated by the Traceroute program;

• the format and contents of an ICMP message.

**Section II Methods & Materials**

Can be lists or even "refer to lab manual" where appropriate.

**Section III Procedure & Results**

Describes ACTUAL process, especially changes from planned method.

|  |
| --- |
| * **number** and **title** tables and graphs correctly and clearly * draw attention to key points in tables or graphs with a sentence * provide sample calculation only * state key result in sentence form |

1. ICMP and Ping：

**• Let’s begin this adventure by opening the Windows Command Prompt application (which can be found in your Accessories folder).**

**• Start up the Wireshark packet sniffer, and begin Wireshark packet capture.**

**• The ping command is in c:\windows\system32, so type either “ping –n 10 hostname” or “c:\windows\system32\ping –n 10 hostname” in the MS-DOS command line (without quotation marks), where hostname is a host on another continent. If you’re outside of Asia, you may want to enter www.ust.hk for the Web server at Hong Kong University of Science and Technology. The argument “-n 10” indicates that 10 ping messages should be sent. Then run the Ping program by typing return.**

**• When the Ping program terminates, stop the packet capture in Wireshark.**



**Figure 1 Command Prompt window after entering Ping command.**

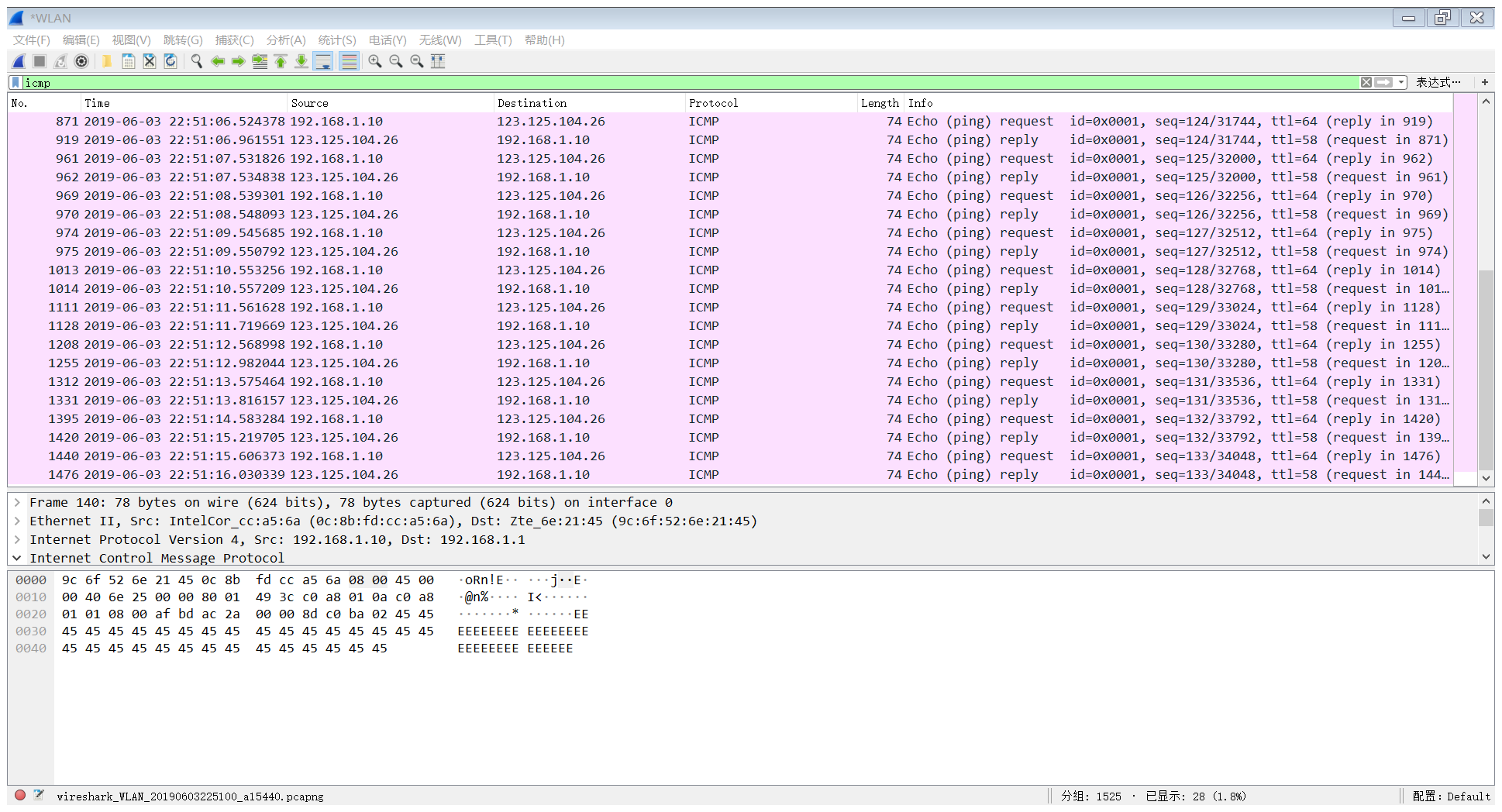


Figure 2 provides a screenshot of the Wireshark output, after “icmp” has been entered into the filter display window. Note that the packet listing shows 20 packets: the 10 Ping queries sent by the source and the 10 Ping responses received by the source. Also note that the source’s IP address is a private address (behind a NAT) of the form 192.168/12; the destination’s IP address is that of the Web server at HKUST. Now let’s zoom in on At the end of the experiment, your Command Prompt Window should look something like Figure 1. In this example, the source ping program is in Massachusetts and the destination Ping program is in Hong Kong. From this window we see that the source ping program sent 10 query packets and received 10 responses. Note also that for each response, the source calculates the round-trip time (RTT), which for the 10 packets is on average 375 msec. Figure 1 Command Prompt window after entering Ping command. the first packet (sent by the client); in the figure below, the packet contents area provides information about this packet. We see that the IP datagram within this packet has protocol number 01, which is the protocol number for ICMP. This means that the payload of the IP datagram is an ICMP packet.

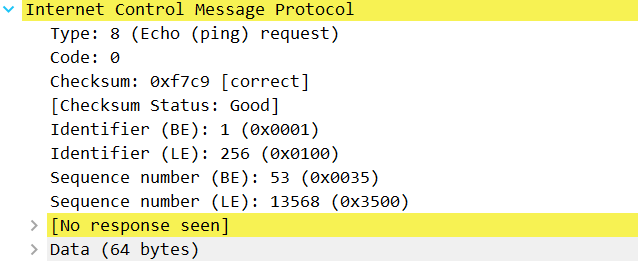


Figure 3 Wireshark capture of ping packet with ICMP packet expanded.

**Section IV Discussion**

Answer the questions in the section [what to hand in] of the lab guide, includes two aspects:

|  |
| --- |
| 1. Analysis = explanation of what can be clearly understood from lab results 2. Interpretation = logical deductions from analysis, explanations of ambiguities. 3. ICMP and Ping 4. What is the IP address of your host? What is the IP address of the destination host?   我主机的地址：192.168.1.10  目标主机的地址：192.168.1.1   1. Why is it that an ICMP packet does not have source and destination port numbers?   ICMP用于主机和路由器彼此交互网络层信息。ICMP报文有一个类型字段和一个编码字段，用来表示特定的消息被接收。因为它能解释所有消息，所以ICMP到应用层不需要端口号。   1. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?   ICMP类型：8  ICMP编码：0  ICMP报文其他字段：  Checksum, Sequence number and Identifier fields  均为两字节。   1. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?   ICMP类型：0  ICMP编码：0  ICMP报文其他字段：  Checksum, Sequence number and Identifier fields  均为两字节。  Sequence number(LE):33280   1. ICMP and Traceroute   5. What is the IP address of your host? What is the IP address of the target destination host?  6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be  01 for the probe packets? If not, what would it be?  答：不是01，因为它的上层协议UDP,所以它的protocol number 不是ICMP（1）  7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping  query packets in the first half of this lab? If yes, how so?  答：没有不同  8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo  packet. What is included in those fields?  Echo包：  Error 包  Error包比Echo包多了Internet Protocol Version4,Src: 10.196.4.109,Dst: 128.93.162.84  9. Examine the last three ICMP packets received by the source host. How are these packets  different from the ICMP error packets? Why are they different?  10. Within the tracert measurements, is there a link whose delay is significantly longer than  others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly  longer than others? On the basis of the router names, can you guess the location of the two  routers on the end of this link?  在第7步到第8步延时比较大，这个链接是位于中国和法国的路由器上。 |

**Section V Conclusion**

States what is known as a result of the experiment.

|  |  |
| --- | --- |
| **Must do:**  1. State what's known  2. Justify that statement | **May do:**  1. State significance of findings  2. Suggest further research |

In the first part, PING www.ust.hk will request a timeout, change to www.youku.com will also timeout, and finally, PING will change to [www.weibo.com](http://www.weibo.com) and it succeed.