

NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE

Computer Networks Lab (CL307)

Lab Session 04

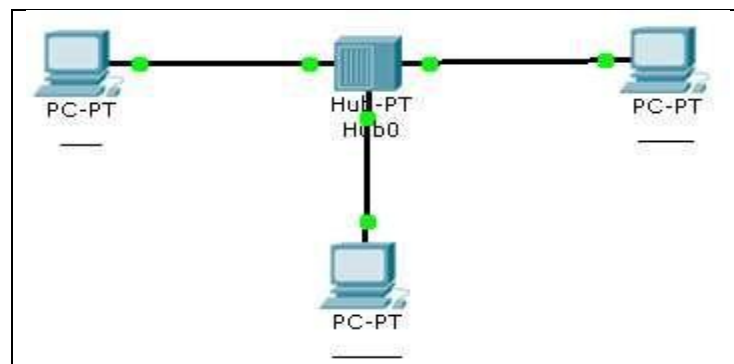
INTRODUCTION TO CISCO PACKET TRACER

Network Infrastructure

Aim: Study of following Network (Layer 1, Layer 2 and Layer 3) Devices in Detail.

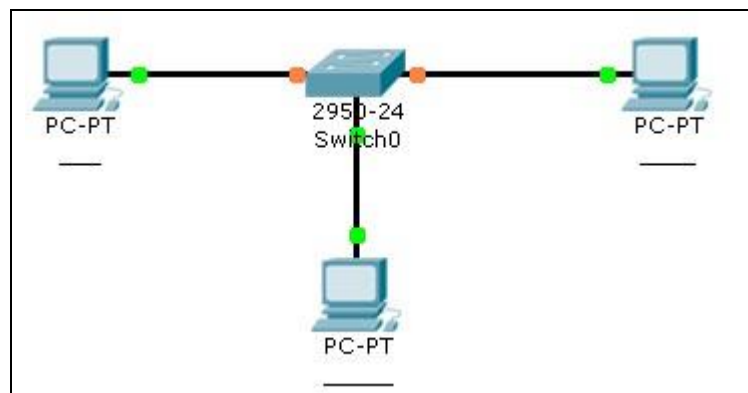
- Hub
- Switch
- Router

Task#1: Understand Network Topology and network hardware (L1) devices.



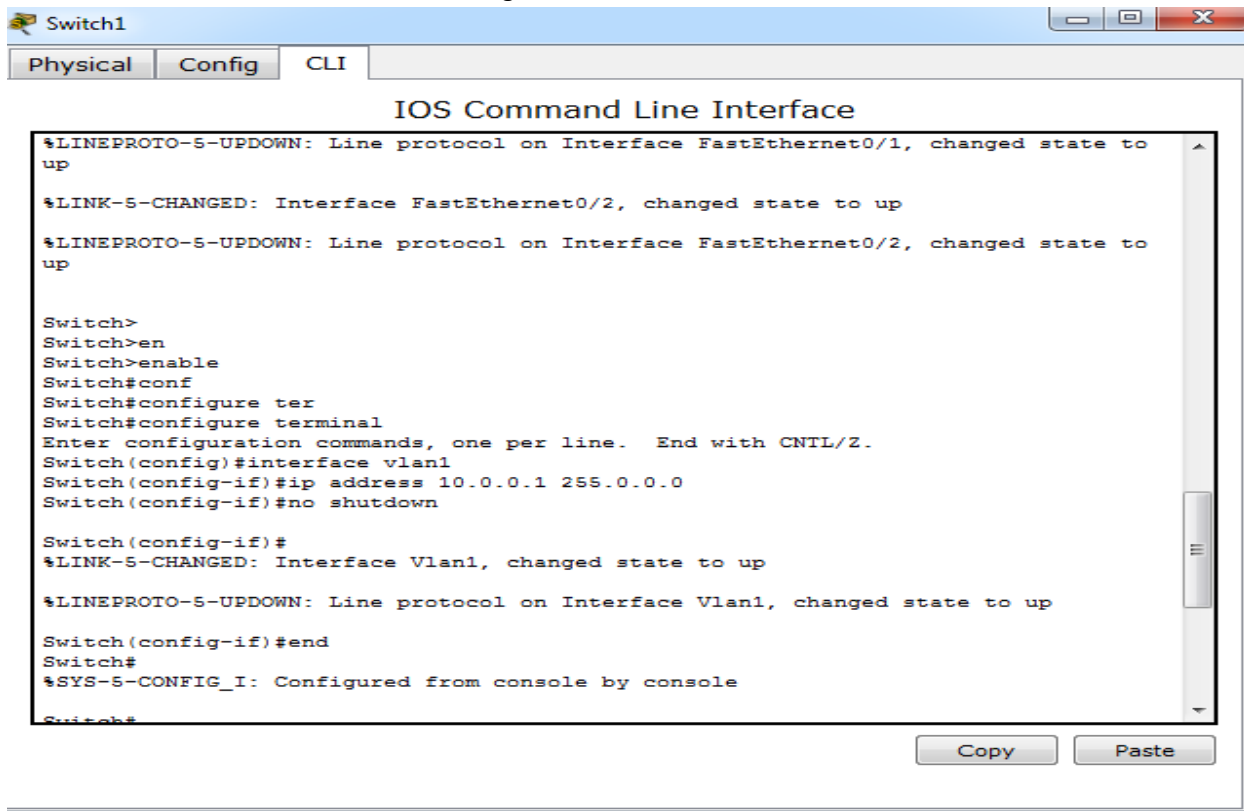
At which layer the HUB operates? _____

Task#2: Understand Network Topology and network hardware (L2) devices.

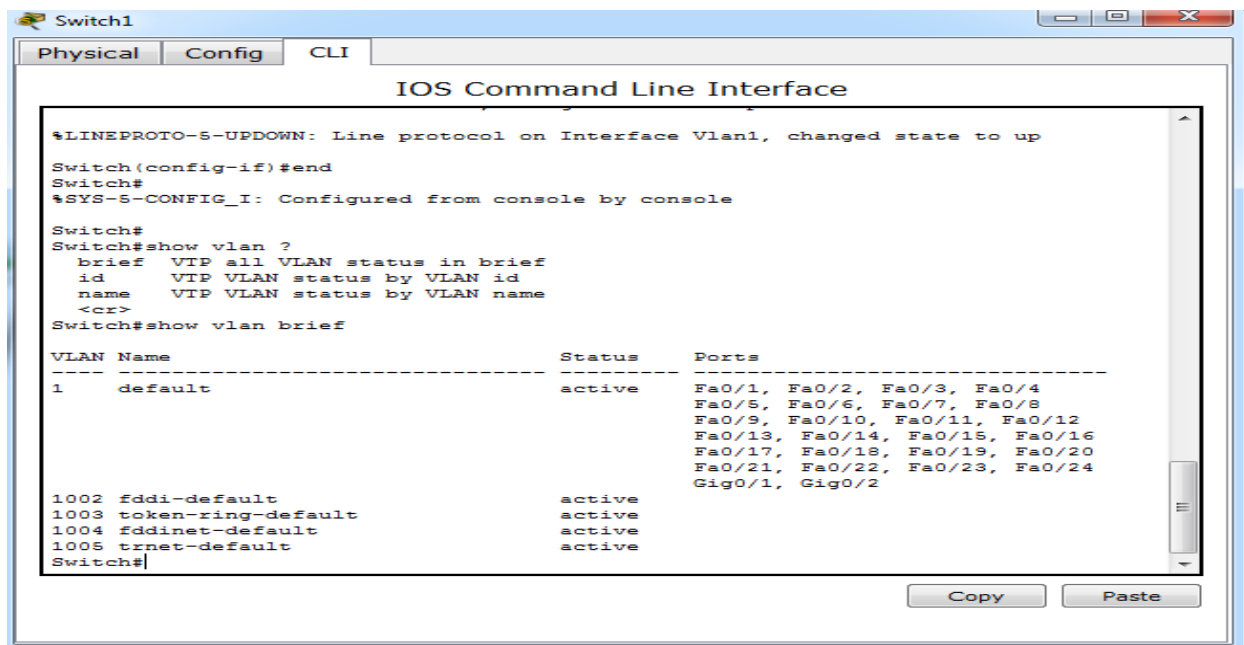


CONFIGURATION:

Click Switch → CLI → then run following commands.

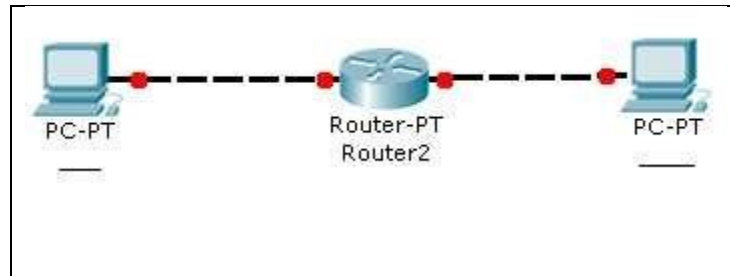


We have to assign IP address on Interface Vlan1 which is default interface in Switch as shown below.



At which layer the SWITCH operates? _____

Task#3: Understand Network Topology and network hardware (L3) devices.



CONFIGURATION:

```
Router0
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

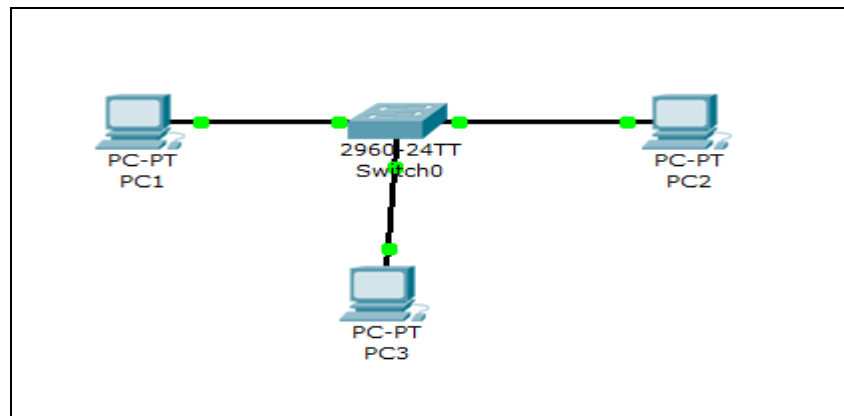
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#ip address 11.0.0.1 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```

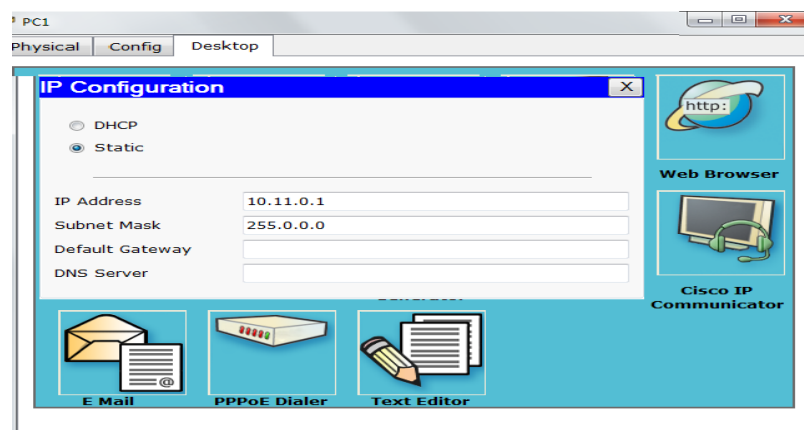
At which layer the ROUTER operates? _____

Task#4: Start the packet tracer and configure the following network and show the packet header format of ICMP protocol.

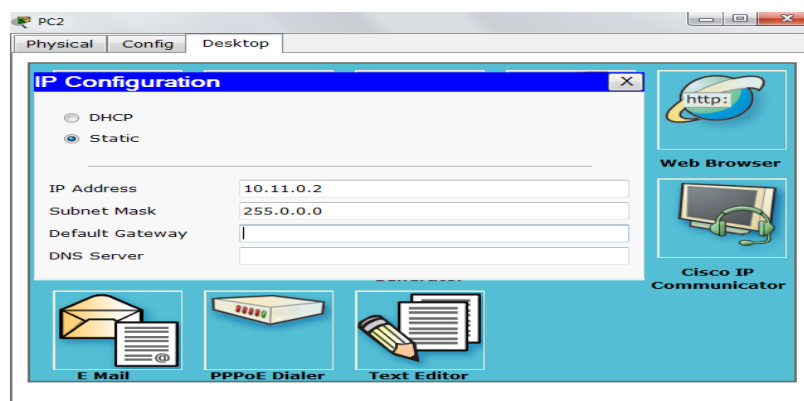


Step#1: configure PC1.

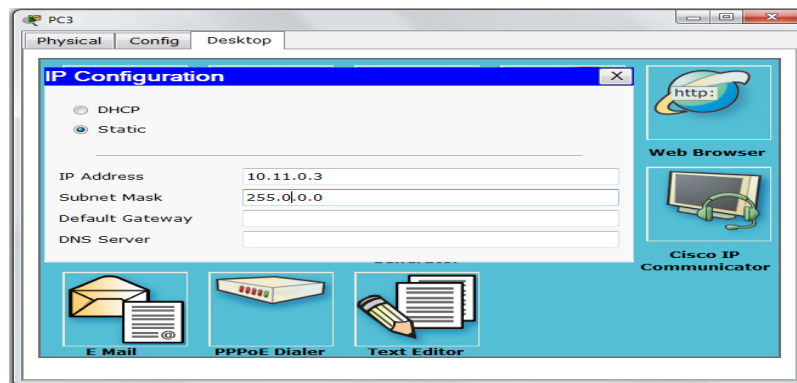
a) Click on the PC1 and go to Desktop →IP Configuration



b) Click on the PC2 and go to Desktop →IP Configuration

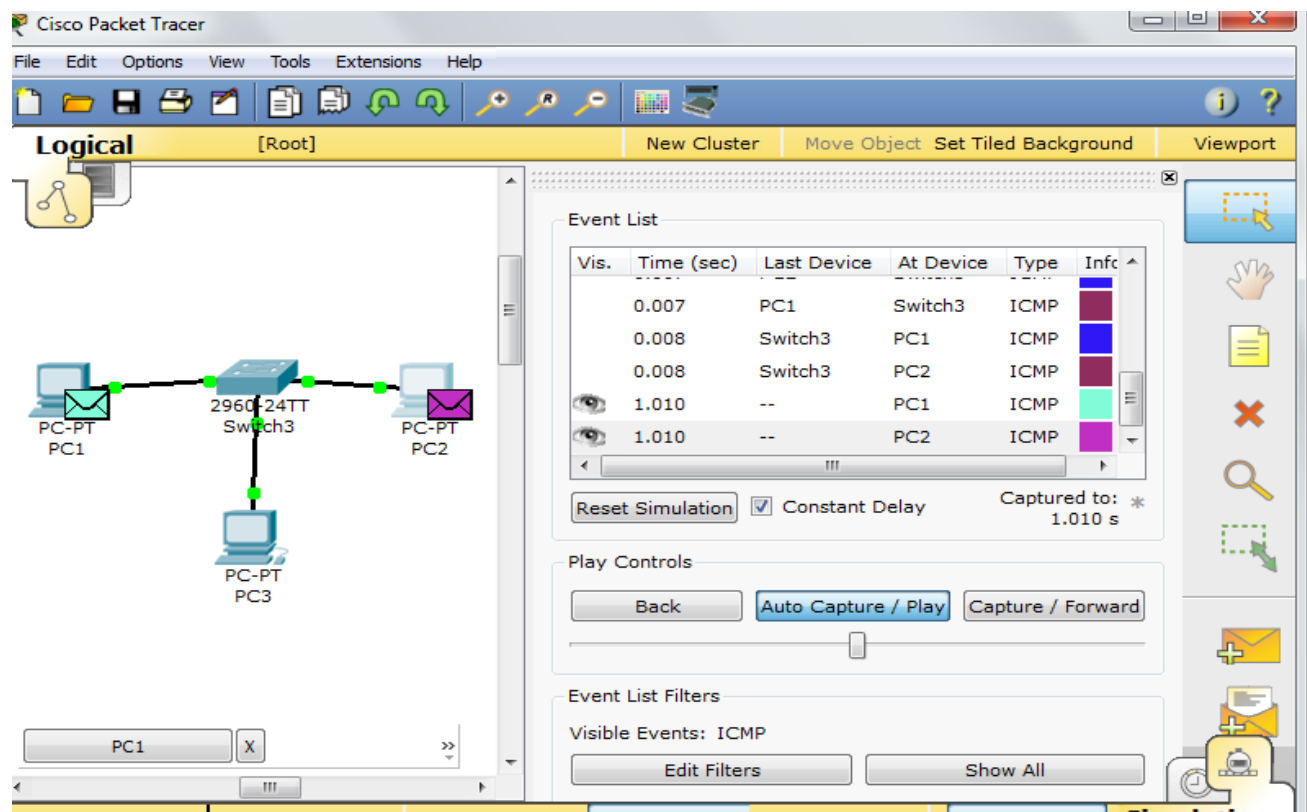


c) Click on the PC3 and go to Desktop → IP Configuration



Step#2:

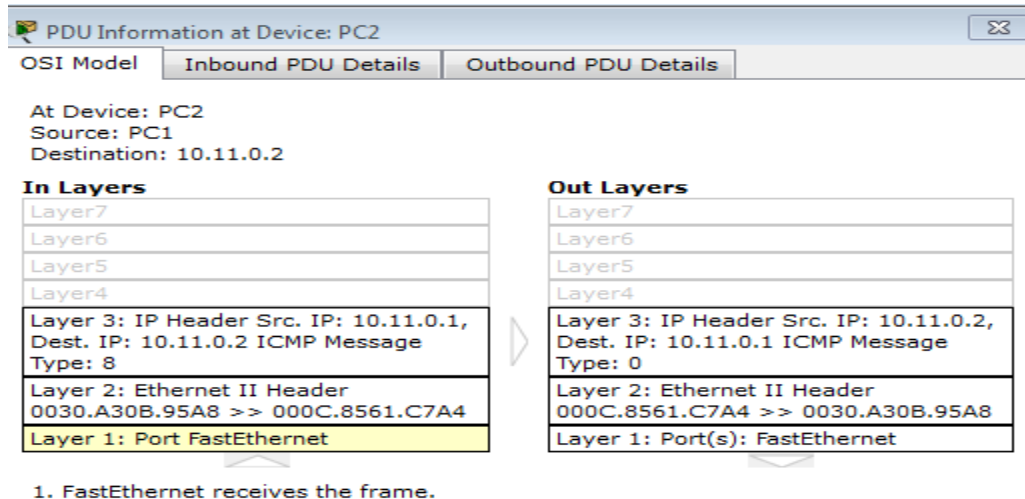
- a) Now click on simulation icon in the right bottom of packet Tracer.
- b) Now click on edit filter and to capture ICMP protocol packets, Click on ICMP check box.
- c) Now click on auto capture /play icon for packet capturing.
- d) Click on the PC1 and go to Desktop →Command Prompt then Ping PC1 from PC2.



Step#3: Now click on the ICMP packet show its header.

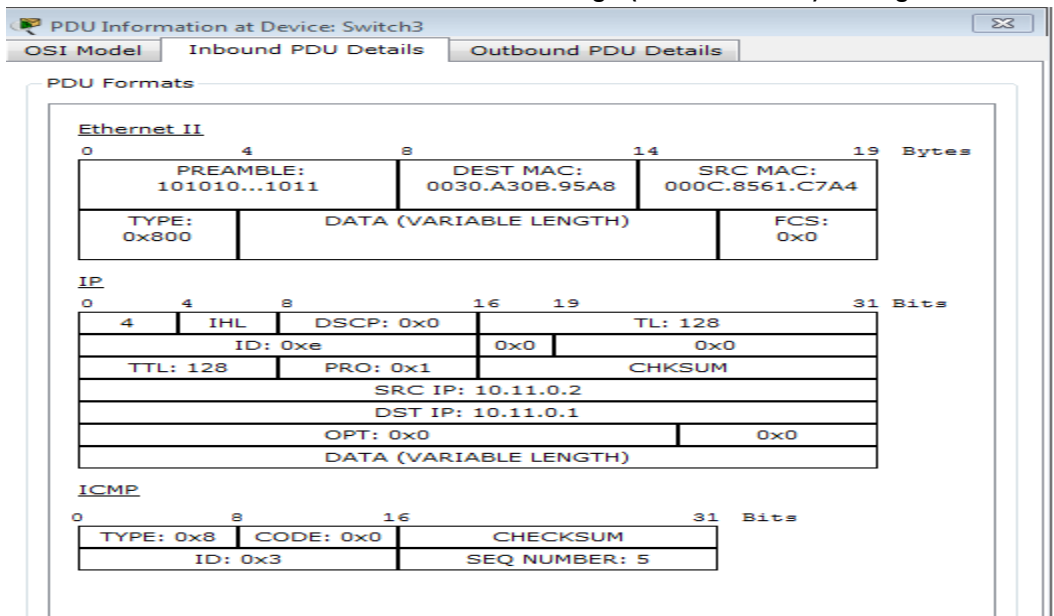
a) Shows OSI layers involved in transmission.

The popped up window (below) will enable you to trace the content of the message through the OSI layer and what changes will occur at each layer (use next and previous buttons to trace each layer content).



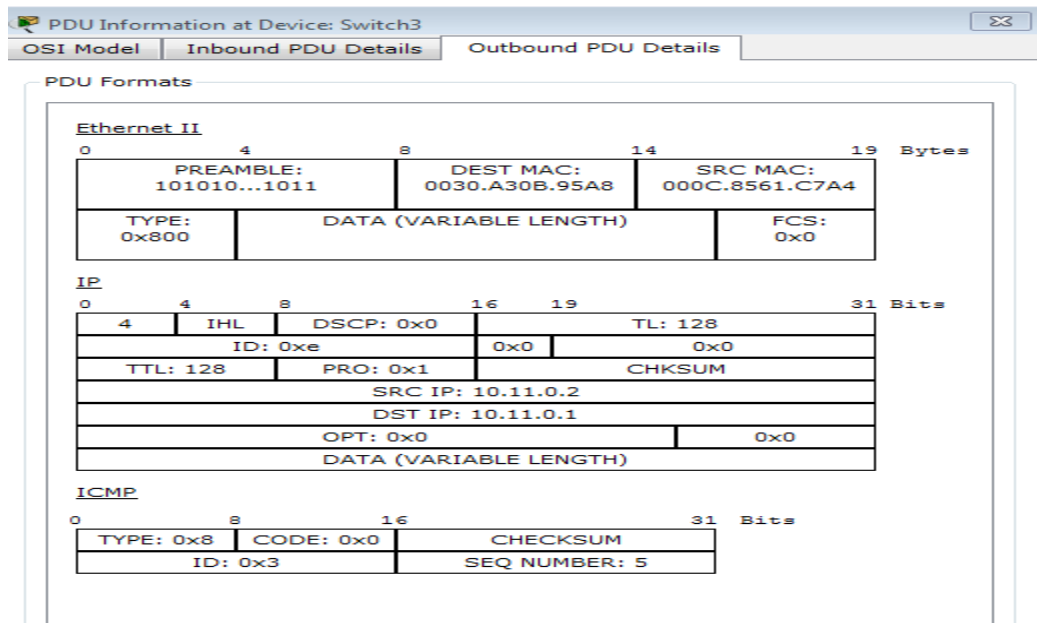
b) Shows Inbound PDU Details.

The inbound tab shows the content of the message (header format) during the receiving process.



c) Shows Outbound PDU Details.

The outbound tab shows the content of the message (header format) during the Sending process



Exercise:

Show the packet header format of ARP in Cisco Packet tracer.

INTRODUCTION TO WIRESHARK

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

- ICMP messages generated by the Ping program;
- The format and contents of an ICMP message.

1. ICMP and Ping

Let's begin our ICMP adventure by capturing the packets generated by the Ping program. You may recall that the Ping program is a simple tool that allows anyone (for example, a network administrator) to verify if a host is live or not. The Ping program in the source host sends a packet to the target IP address; if the target is live, the Ping program in the target host responds by sending a packet back to the source host. As you might have guessed (given that this lab is about ICMP), both of these Ping packets are ICMP packets.

Do the following:

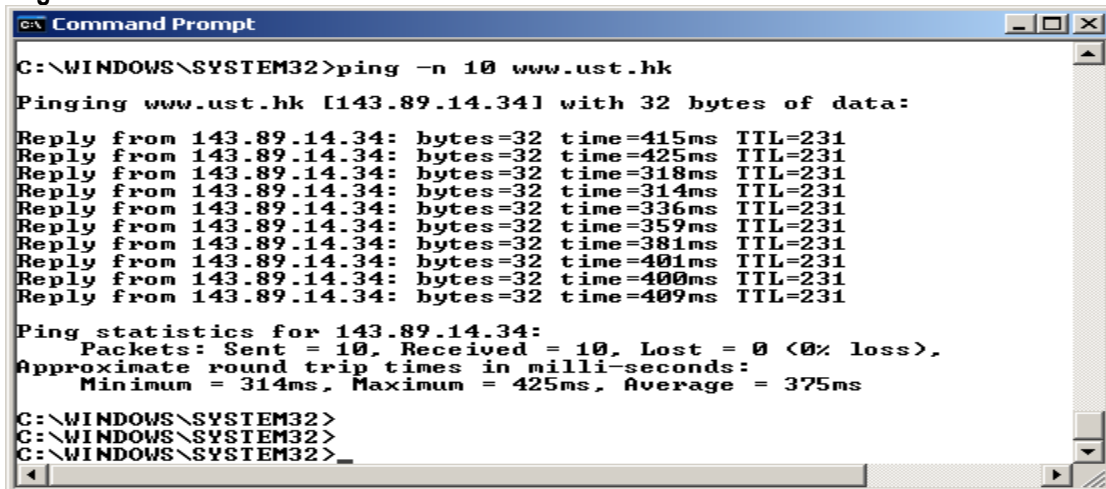
• Let's begin this adventure by opening the Windows Command Prompt application (which can be found in your Accessories folder).

• 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.

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.



```
C:\WINDOWS\SYSTEM32>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.14.34] with 32 bytes of data:

Reply from 143.89.14.34: bytes=32 time=415ms TTL=231
Reply from 143.89.14.34: bytes=32 time=425ms TTL=231
Reply from 143.89.14.34: bytes=32 time=318ms TTL=231
Reply from 143.89.14.34: bytes=32 time=314ms TTL=231
Reply from 143.89.14.34: bytes=32 time=336ms TTL=231
Reply from 143.89.14.34: bytes=32 time=359ms TTL=231
Reply from 143.89.14.34: bytes=32 time=381ms TTL=231
Reply from 143.89.14.34: bytes=32 time=401ms TTL=231
Reply from 143.89.14.34: bytes=32 time=400ms TTL=231
Reply from 143.89.14.34: bytes=32 time=409ms TTL=231

Ping statistics for 143.89.14.34:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 314ms, Maximum = 425ms, Average = 375ms

C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
```

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 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.

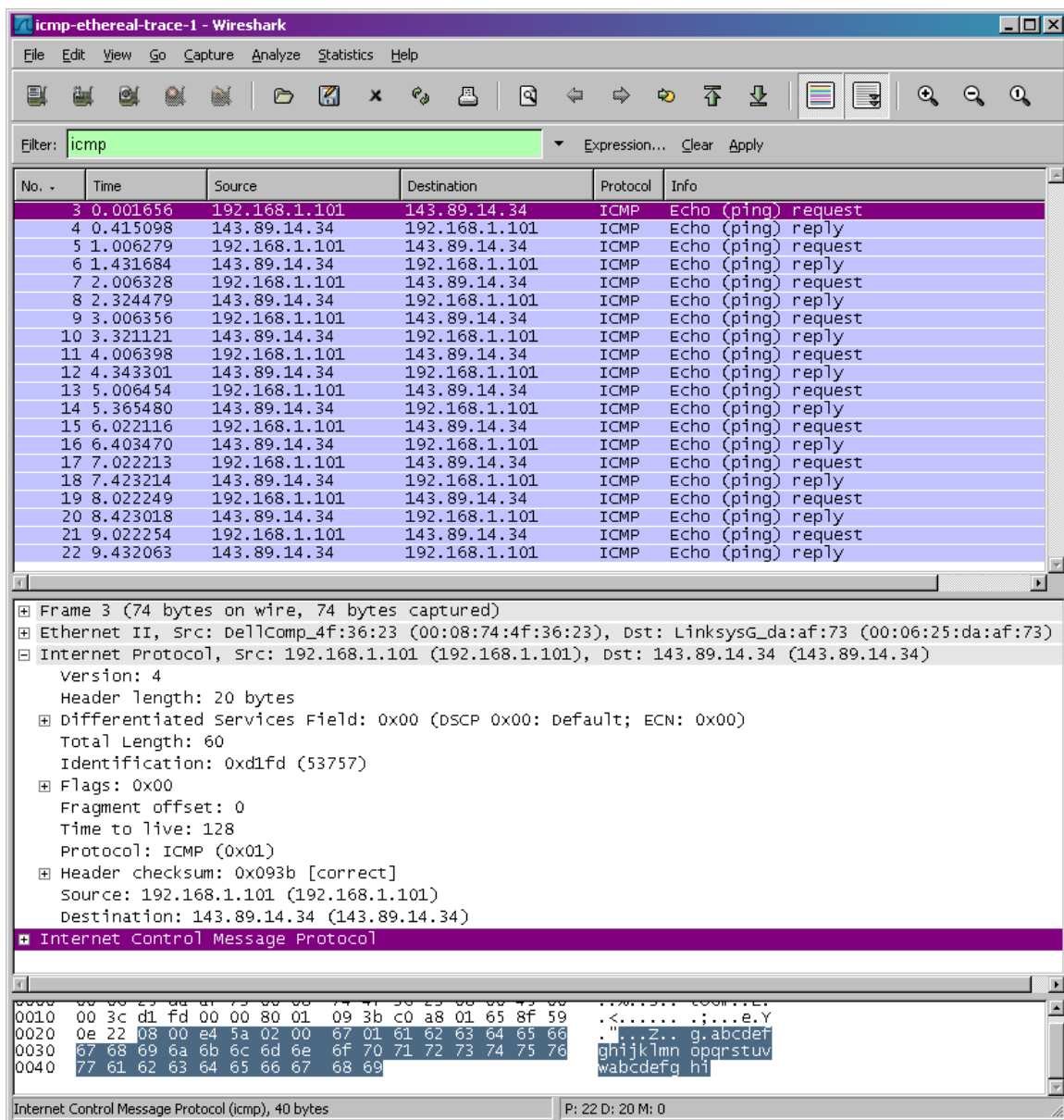


Figure 2 Wireshark output for Ping program with Internet Protocol expanded.

Figure 3 focuses on the same ICMP but has expanded the ICMP protocol information in the packet contents window. Observe that this ICMP packet is of Type 8 and Code 0 - a so-called ICMP “echo request” packet. (See Figure 5.19 of text.) Also note that this ICMP packet contains a checksum, an identifier, and a sequence number.

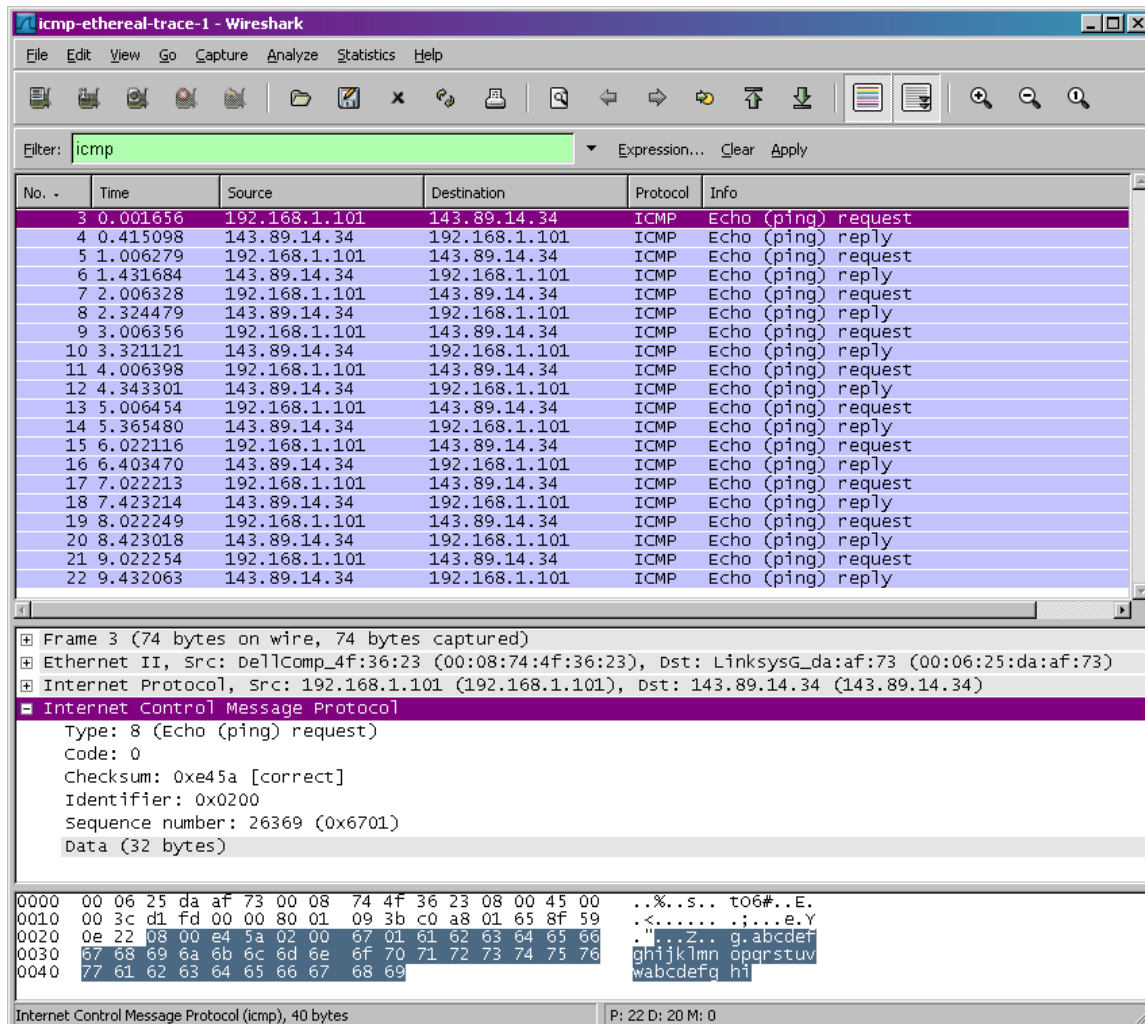


Figure 3 Wireshark capture of ping packet with ICMP packet expanded.

You should answer the following questions:

1. What is the IP address of your host? What is the IP address of the destination host?
2. Why is it that an ICMP packet does not have source and destination port numbers?
3. 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?
4. 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?