

NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE

Computer Network Lab (CL3001)Lab

Session 03

Objective:

- Introduction to Telnet & configuration of Telnet in Cisco Packet Tracer
- Introduction to SSH & configuration of SSH in Cisco Packet Tracer
- Introduction of WireShark tool.

SSH & Telnet

1. Introduction to Telnet:

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers. To telnet means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface.

2. Configuration of Telnet:

Below are the steps for Telnet Protocol. Follow the figure 1 till figure 8 for the configuration of Telnet Protocol.

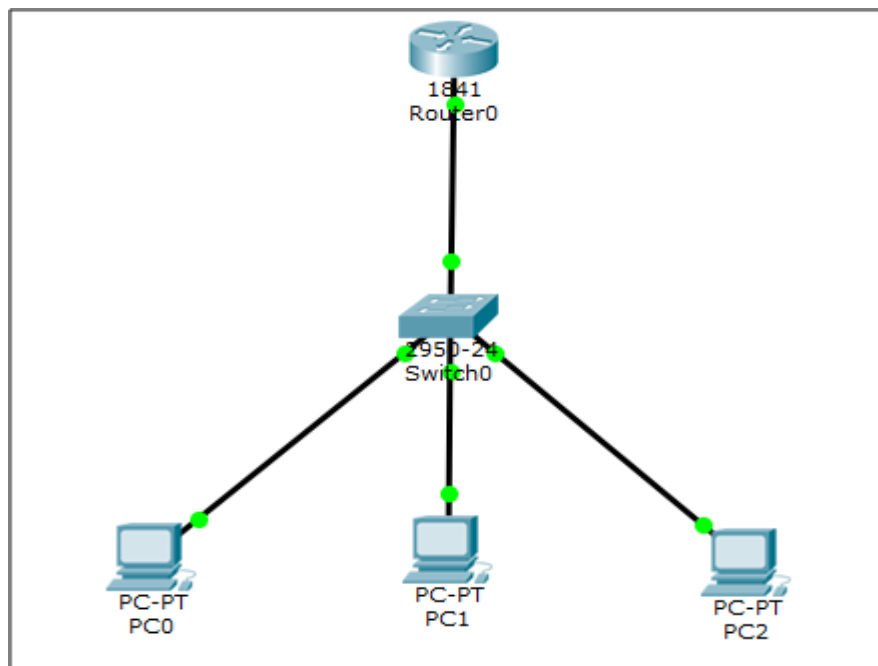
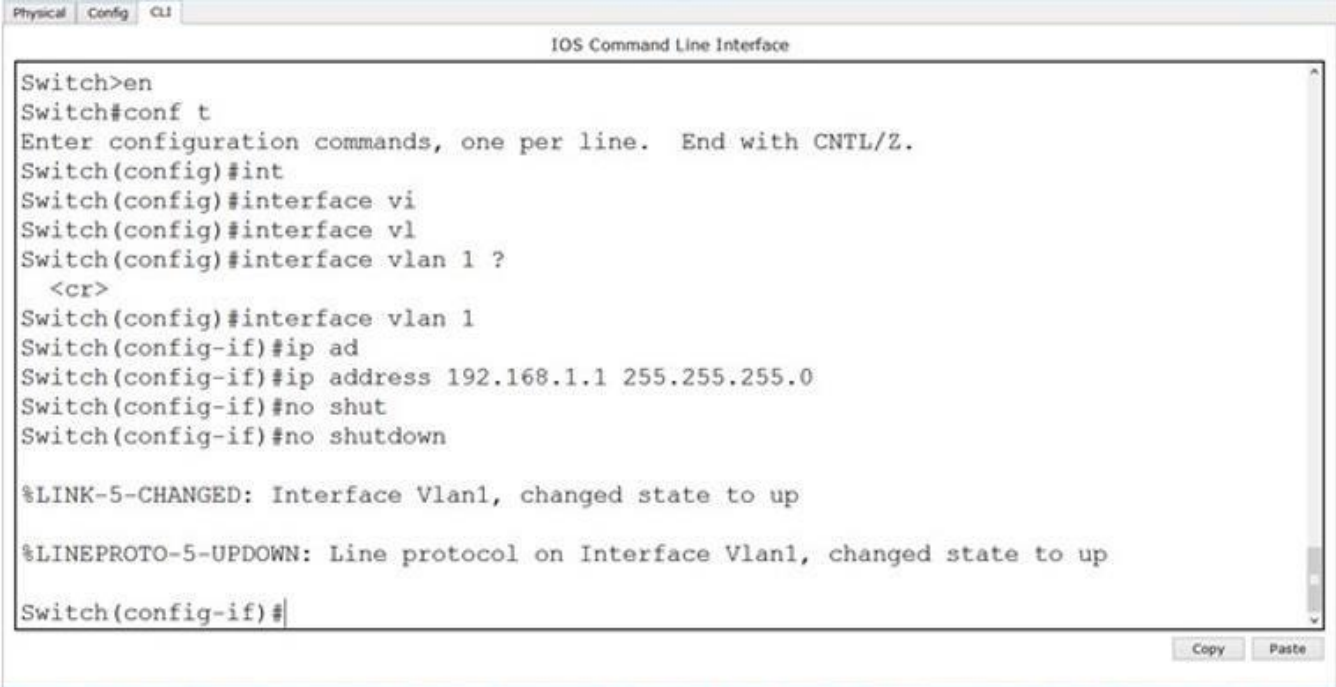


Fig-1:Network Topology

Take the topology as in the above diagram. Set IPs on the PCs. As, by default, all PCs are in vlan. We will create a virtual interface on switch with vlan 1 as follows.



```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface vi
Switch(config)#interface vl
Switch(config)#interface vlan 1 ?
  <cr>
Switch(config)#interface vlan 1
Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#no shutdown


%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#
```

Fig-2: Configuring VLAN Connection

Now, try to telnet the switch from our PC, it refuses because we have not applied authentication on the switch yet.

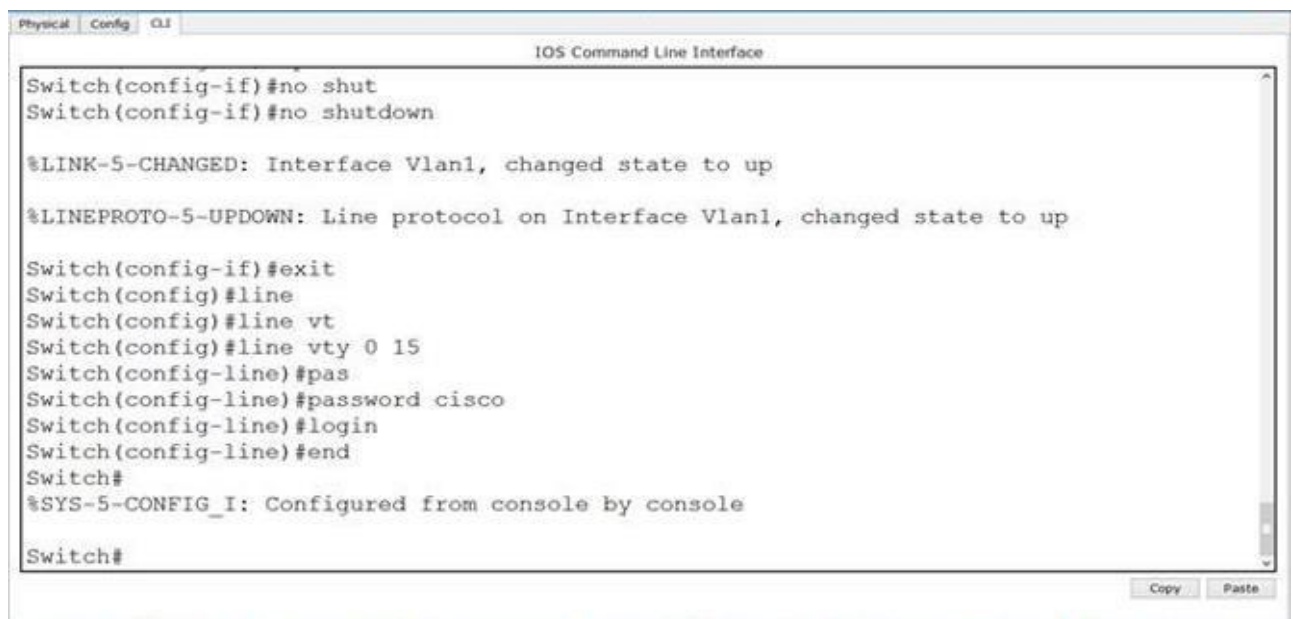


```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>
```

Fig-3: Initial Checking of Vlan

Secure Shell Server (SSH) and FTP services. Each Telnet, SSH, or FTP session requires one vty-line. You can add security to your system by configuring the software to validate login requests.



```
Switch(config-if)#no shut
Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#line
Switch(config)#line vt
Switch(config)#line vty 0 15
Switch(config-line)#pas
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Fig-4: Creating Vty-line connection for Telnet

Now, we can easily telnet. But it does not let us go in the switch enabled mode because we have not set the password on the switch yet.



```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

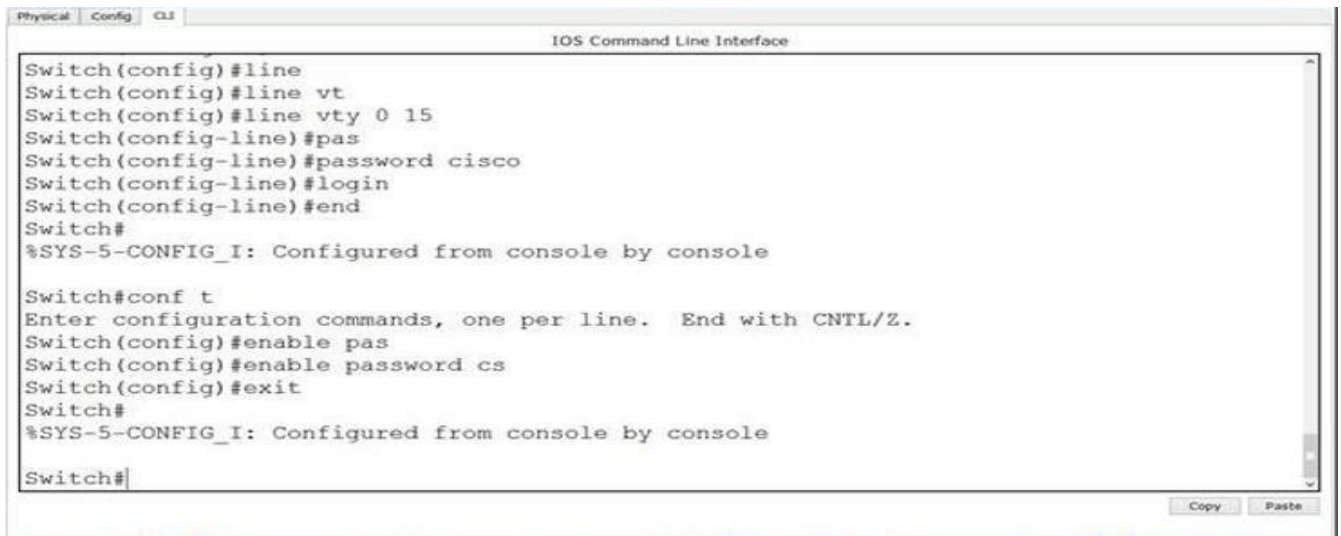
[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>en
% No password set.
Switch>
```

Fig-5: Checking Vty-line connection for Telnet

Let's apply password on the switch enabled mode.



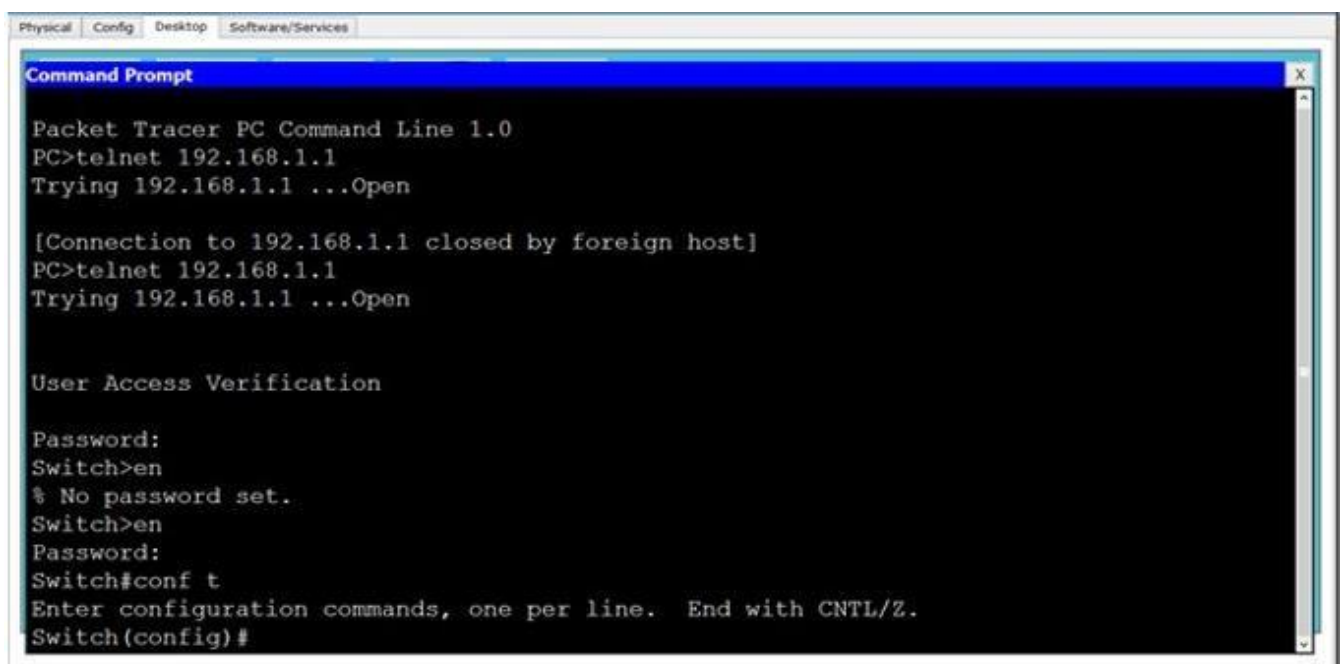
```
Switch(config)#line
Switch(config)#line vt
Switch(config)#line vty 0 15
Switch(config-line)#pas
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable pas
Switch(config)#enable password cs
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Fig-6: Adding password in enable mode

Now, we can go inside Switch configuration mode from our pc.



```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>en
% No password set.
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

Fig-7: Checking by it using command

3. Introduction to SSH:

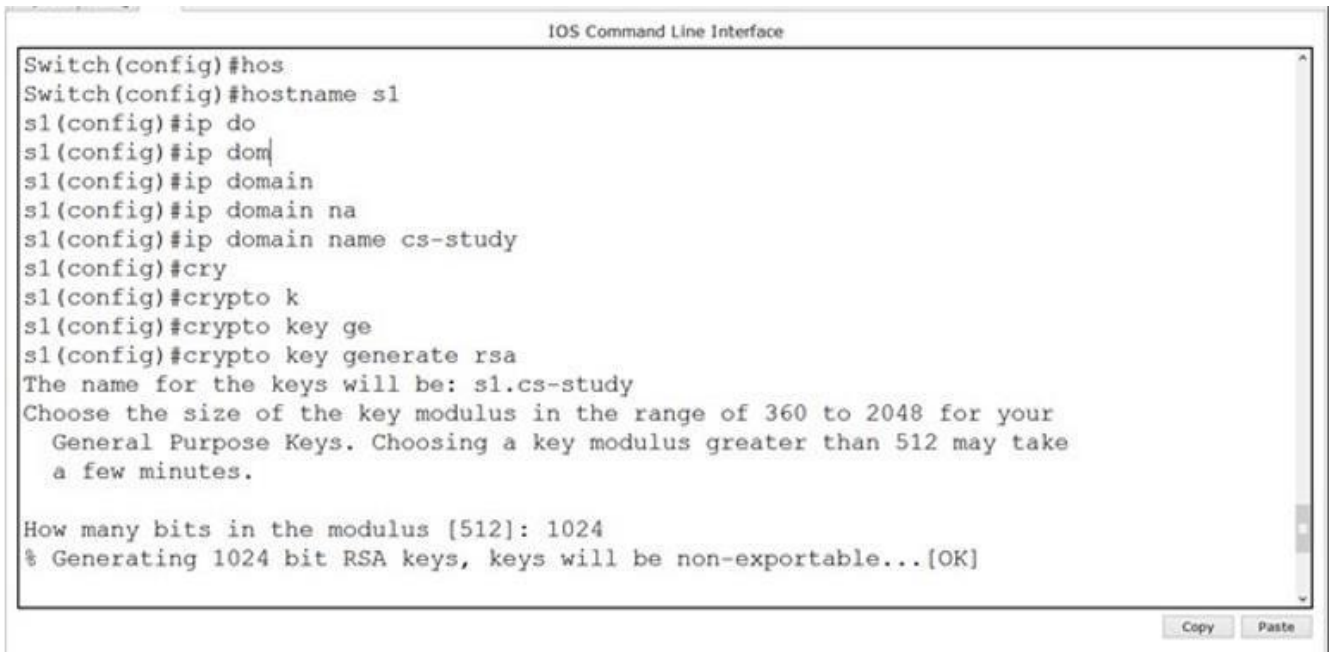
Secure Shell or Secure Socket Shell is a network protocol. It is an application layer protocol that is in the 7th later of the Open Systems Interconnection (OSI) network model. It also refers to the suite of utilities that implements the SSH protocol.

Secure Shell also supports both password and key-based authentication. Password-based authentication let users provide username and password to authenticate to the remote server. A key-based authentication allows users to authenticate through a key-pair. The key pairs are two cryptographically secure keys for authenticating a client to a Secure Shell server.

Furthermore, the Secure Shell protocol also encrypts data communication between two computers. It is extensively used to communicate with a remote computer over the Internet.

4. Configuration of SSH:

Taking the same topology as mentioned in figure 1. Below are the steps for SSH Protocol. Follow the figure 9 till figure 14 for the configuration of SSH Protocol.

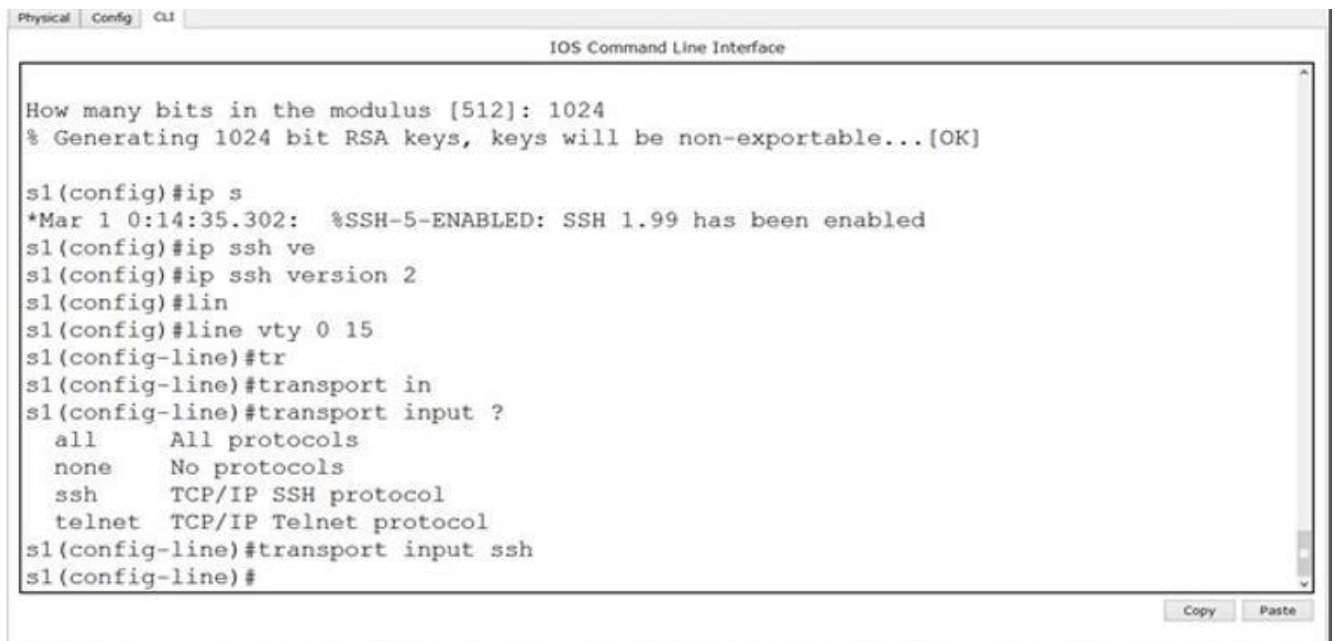


```
Switch(config)#hos
Switch(config)#hostname s1
s1(config)#ip do
s1(config)#ip dom
s1(config)#ip domain
s1(config)#ip domain na
s1(config)#ip domain name cs-study
s1(config)#cry
s1(config)#crypto k
s1(config)#crypto key ge
s1(config)#crypto key generate rsa
The name for the keys will be: s1.cs-study
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Fig-8: Creating Domain & RSA key

Commands continued.



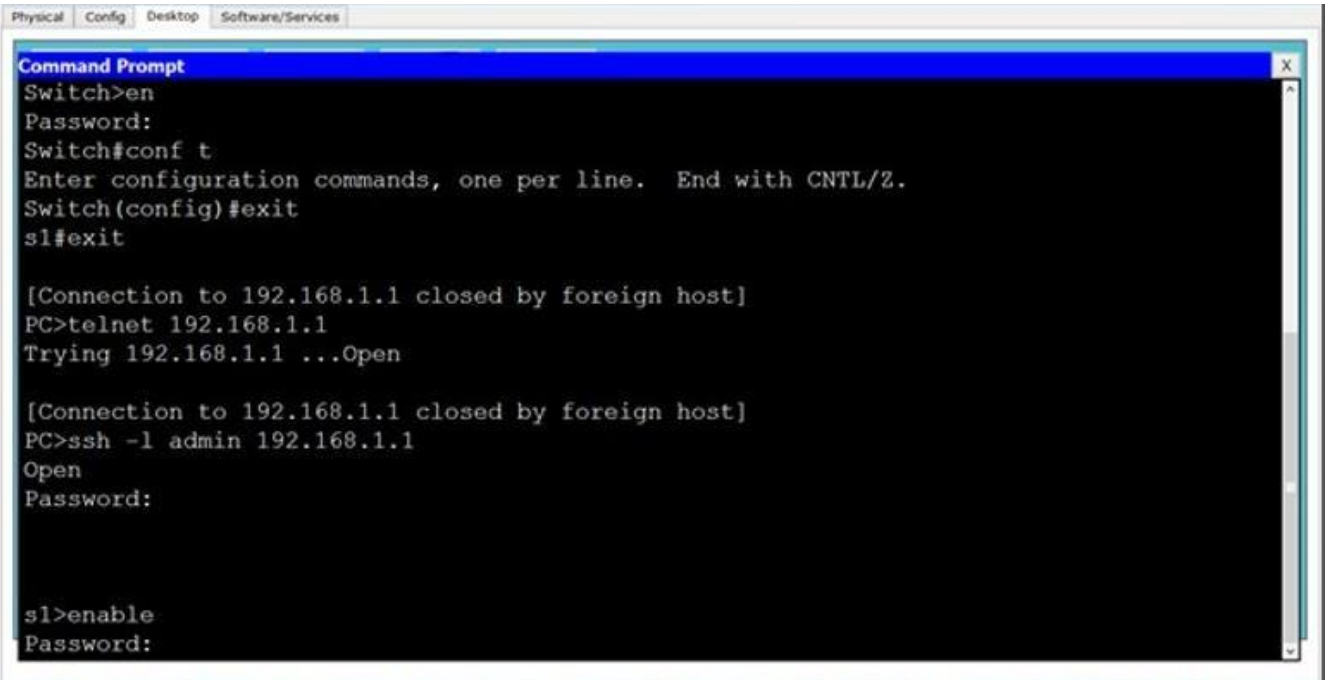
```
Physical Config CLI
IOS Command Line Interface

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

s1(config)#ip s
*Mar 1 0:14:35.302: %SSH-5-ENABLED: SSH 1.99 has been enabled
s1(config)#ip ssh ve
s1(config)#ip ssh version 2
s1(config)#lin
s1(config)#line vty 0 15
s1(config-line)#tr
s1(config-line)#transport in
s1(config-line)#transport input ?
all      All protocols
none     No protocols
ssh      TCP/IP SSH protocol
telnet   TCP/IP Telnet protocol
s1(config-line)#transport input ssh
s1(config-line)#
```

Fig-9: Creating SSH connection

Protocol working on it. By default, username is admin.



```
Physical Config Desktop Software/Services
Command Prompt
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#exit
sl#exit

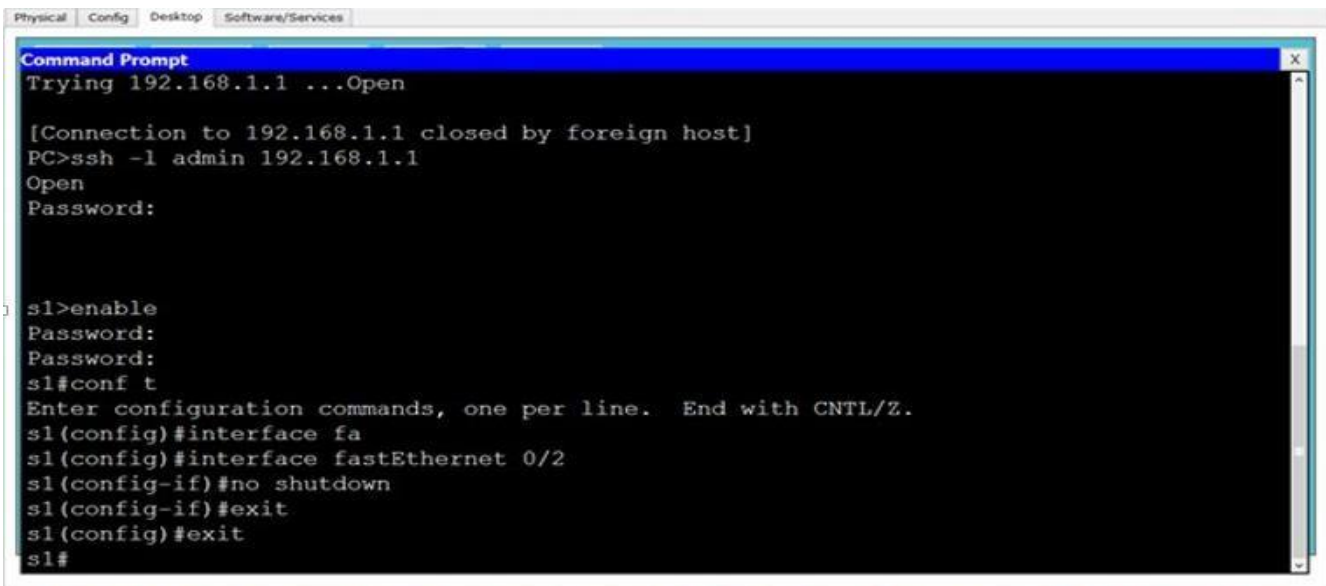
[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l admin 192.168.1.1
Open
Password:

sl>enable
Password:
```

Fig-10: Checking SSH connection of Admin user

And we can apply any sort of configuration on our switch from our pc



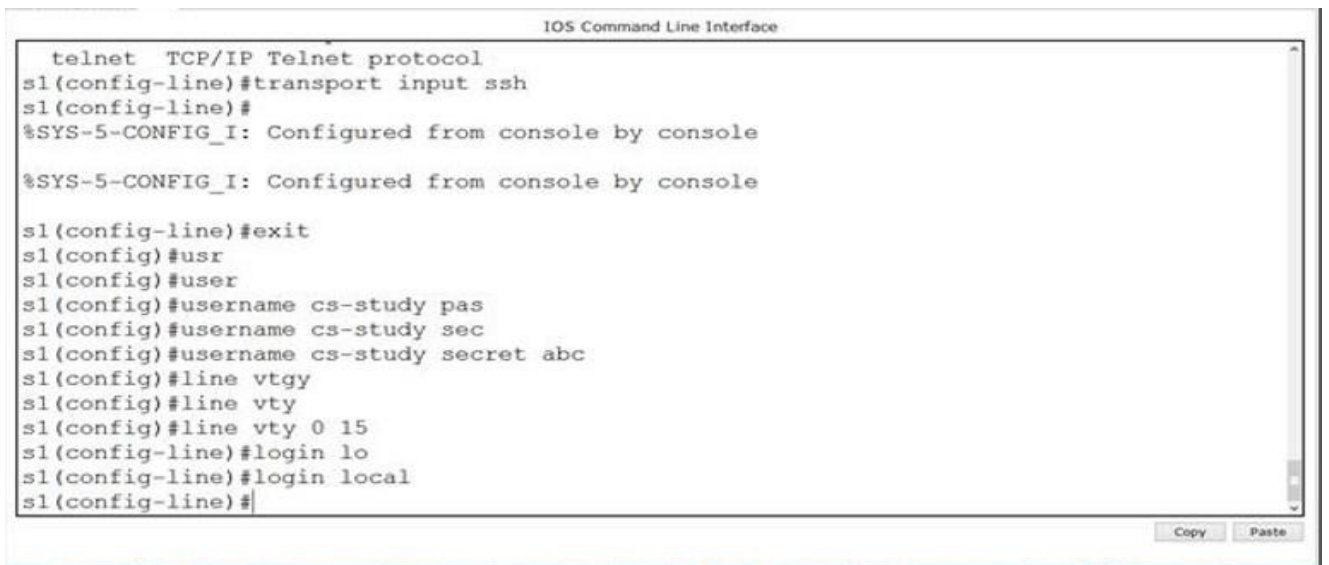
```
Physical Config Desktop Software/Services
Command Prompt
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l admin 192.168.1.1
Open
Password:

sl>enable
Password:
Password:
sl#conf t
Enter configuration commands, one per line. End with CNTL/Z.
sl(config)#interface fa
sl(config)#interface fastEthernet 0/2
sl(config-if)#no shutdown
sl(config-if)#exit
sl(config)#exit
sl#
```

Fig-11: Moving to enable mode using specific computer

Now, if we want to change the username from admin to something else, we will do it as follows.



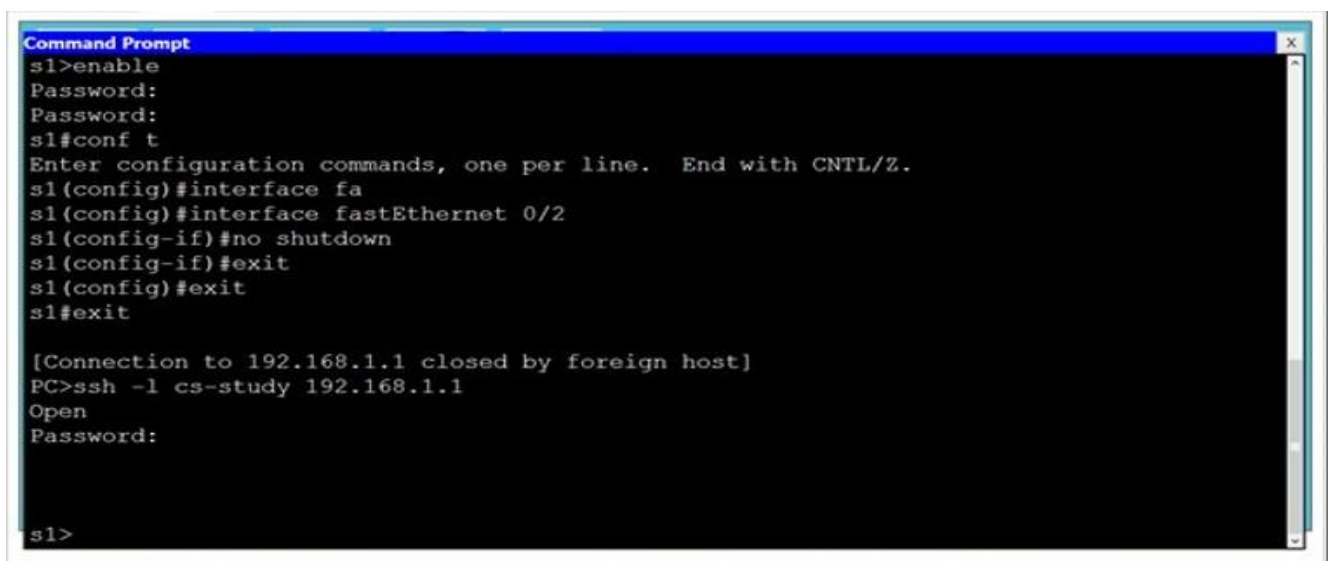
```
telnet TCP/IP Telnet protocol
s1(config-line)#transport input ssh
s1(config-line)#
%SYS-5-CONFIG_I: Configured from console by console

%SYS-5-CONFIG_I: Configured from console by console

s1(config-line)#exit
s1(config)#usr
s1(config)#user
s1(config)#username cs-study pas
s1(config)#username cs-study sec
s1(config)#username cs-study secret abc
s1(config)#line vty
s1(config)#line vty
s1(config)#line vty 0 15
s1(config-line)#login lo
s1(config-line)#login local
s1(config-line)#
```

Fig-12: Creating Vty connection on specific domain

and from our pc as follows.



```
Command Prompt
s1>enable
Password:
Password:
s1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
s1(config)#interface fa
s1(config)#interface fastEthernet 0/2
s1(config-if)#no shutdown
s1(config-if)#exit
s1(config)#exit
s1#exit

[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l cs-study 192.168.1.1
Open
Password:

s1>
```

Fig-13: Checking the connection

5. Lab Exercise 1:

Question # 1

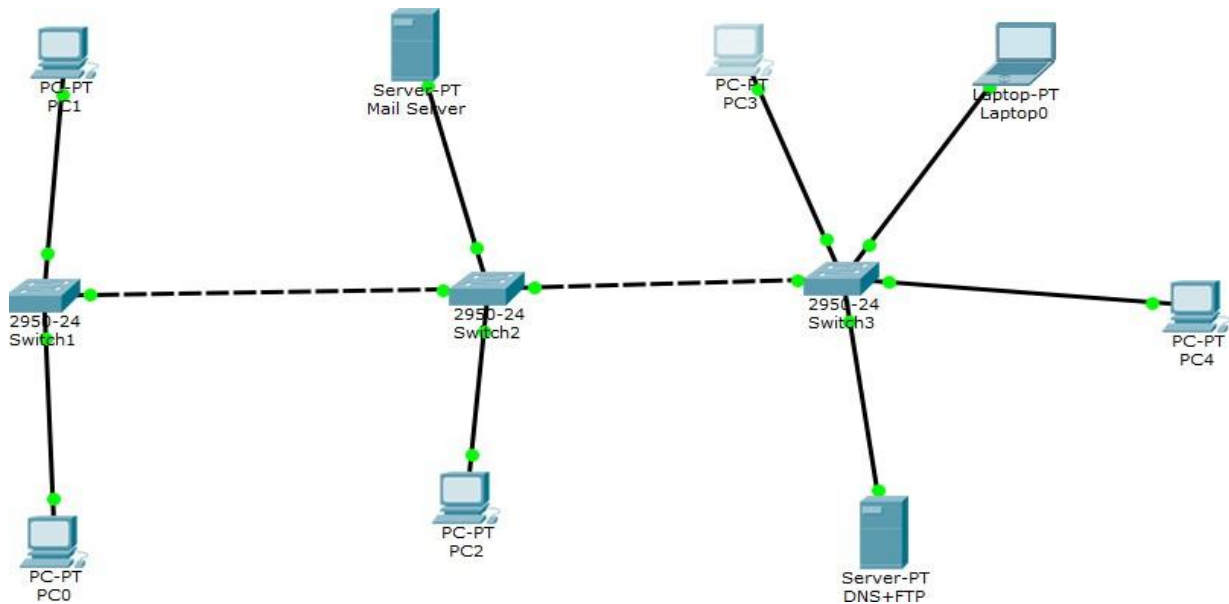


Fig-14a: Network Topology

1. Implement the topology given in figure A on cisco packet tracer.
2. Assign IP to the computers. The Network should like this XX.XX.0.0
i.e. your roll number like 3879(38.79.0.0)
3. Ping the server from any computer.
4. Verify the telnet connection from all switches nearest to the computer.
5. Do change the IP of Switch2 from PC2 using its command prompt.

Question # 2

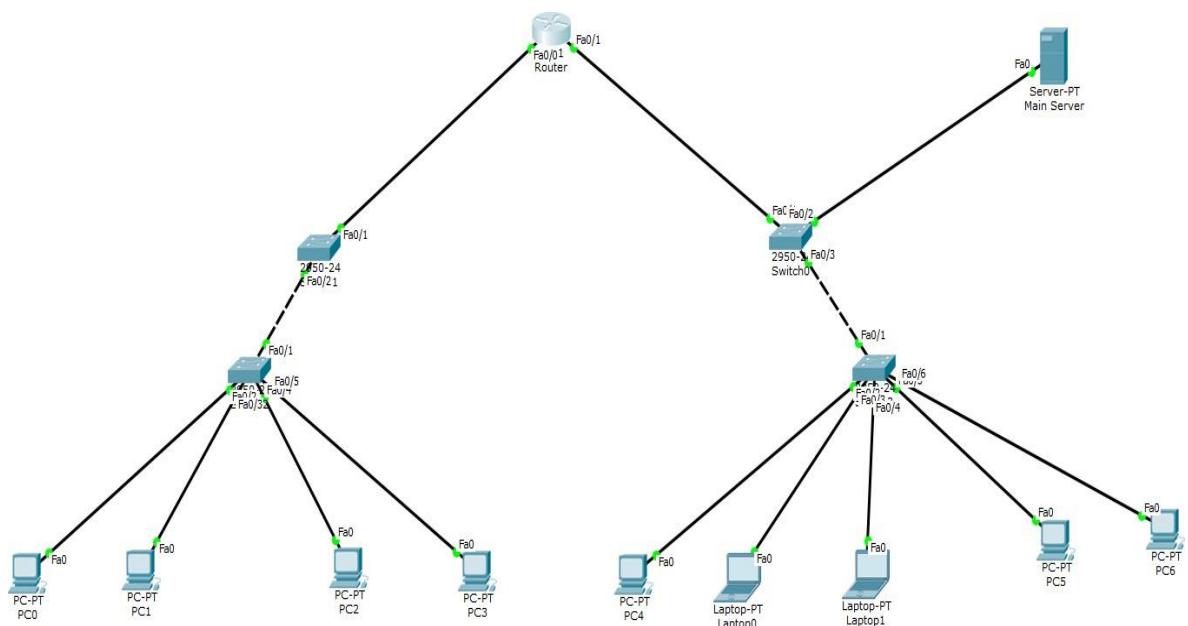


Fig-14b: Network Topology

1. Implement the figure B topology on cisco packet tracer.
2. The IP should assign to the computer using static method. The Network on one side of FastEthernet should like this XX.XX.0.0 i.e. your roll number like 3879(38.79.0.0) and on another side it should be 3880(38.80.0.0).
3. Run command of show run on Switch0 and Switch0 and take screenshot of it.
Verify SSH and do assign IP to another interface of Router. It should be done through laptop0. Take screenshot of it.

INTRODUCTION TO WIRESHARK

6. Introduction:

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today

7. Some intended purposes:

Here are some reasons people use Wireshark:

Network administrators use it to troubleshoot network problems
Network security engineers use it to examine security problems
QA engineers use it to verify network applications

Developers use it to debug protocol implementations
People use it to learn network protocol internals
Wireshark can also be helpful in many other situations

In this lab, we'll explore several aspects of the ICMP protocol
ICMP messages generating by the Ping program;
The format and contents of an ICMP message.

8. ICMP & 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:

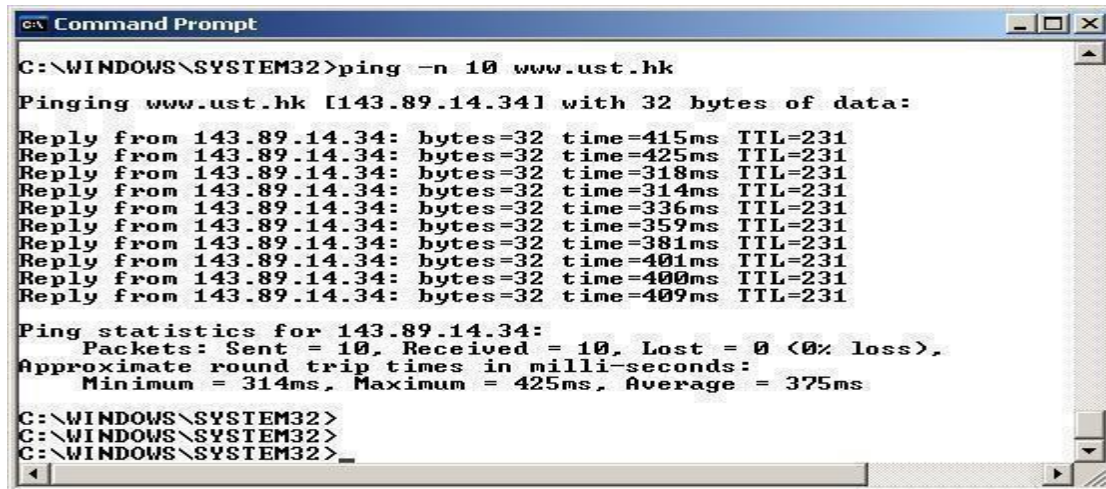
- Let's begin this adventure by opening the Windows Command Prompt application (which can be found in your Accessories folder).
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.

- 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-15: Ping response on CMD

Figure 1 Command Prompt window after entering Ping command. Figure 16 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.

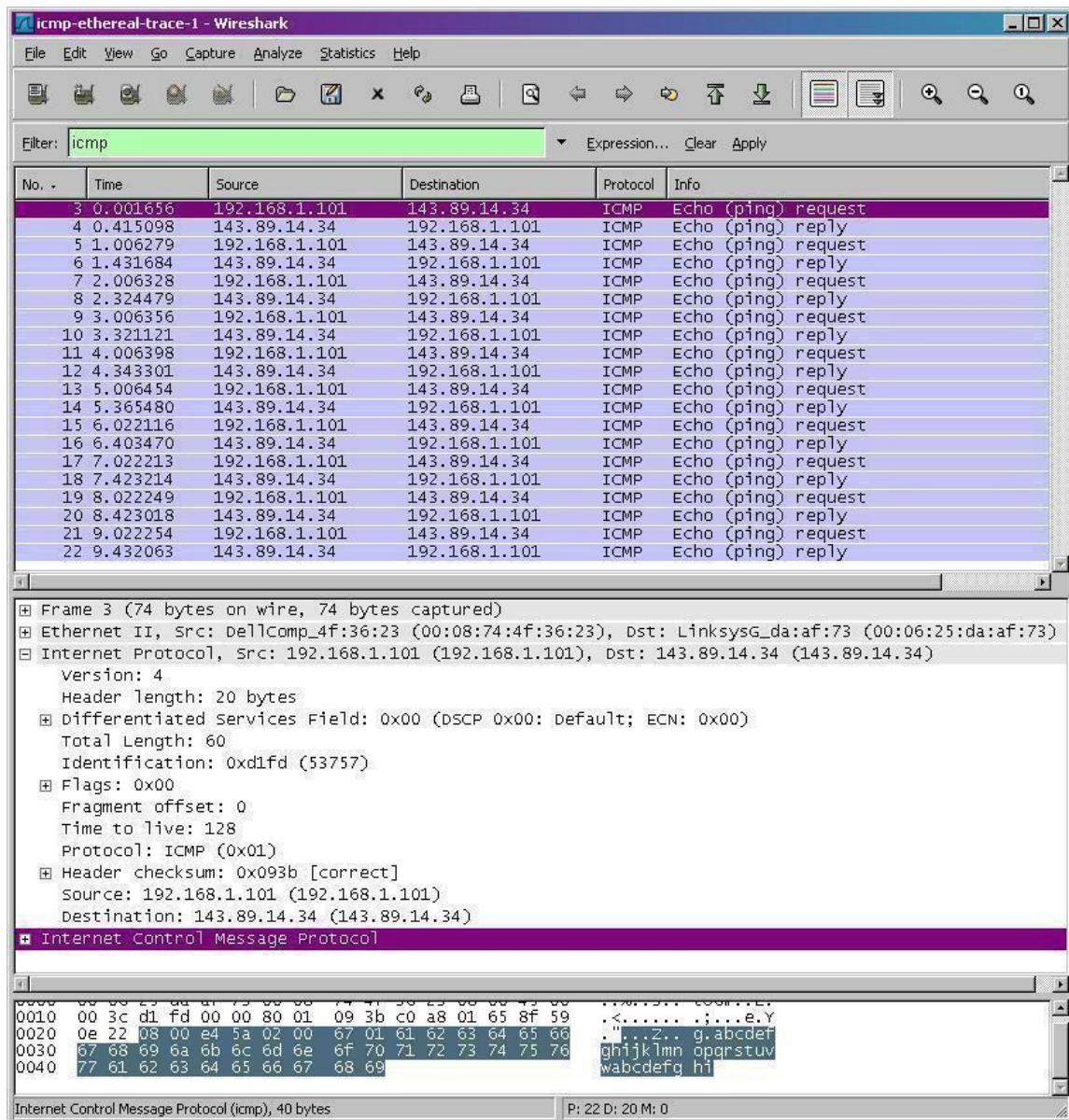


Fig-16: Wireshark output for Ping program with Internet Protocol expanded

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.

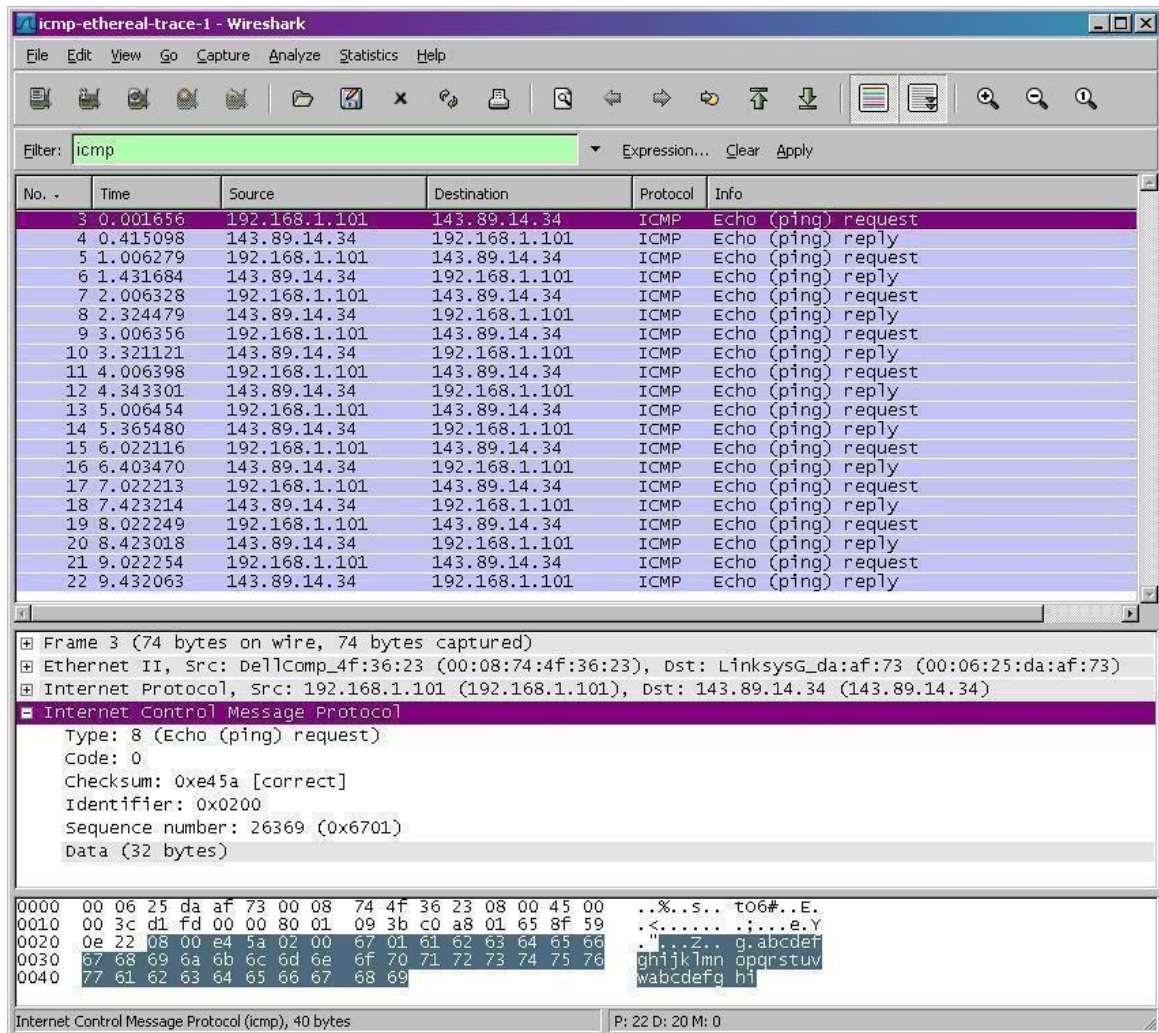


Fig-17: Wireshark capture of ping packet with ICMP packet expanded.

9. Lab Task 2:

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?
5. Open your browser and go to www.google.com capture packets on wireshark, attach screenshots in submission.

Run command of show ip route on router using PC0. It should be done in secure method. Take screenshot of it.

