



# NATIONAL UNIVERSITY OF COMPUTER & EMERGINGSCIENCE

## Computer Network Lab (CL3001)

### Lab Session 08

## SSH, Telnet, DHCP, and SUBNETTING

### Objective:

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

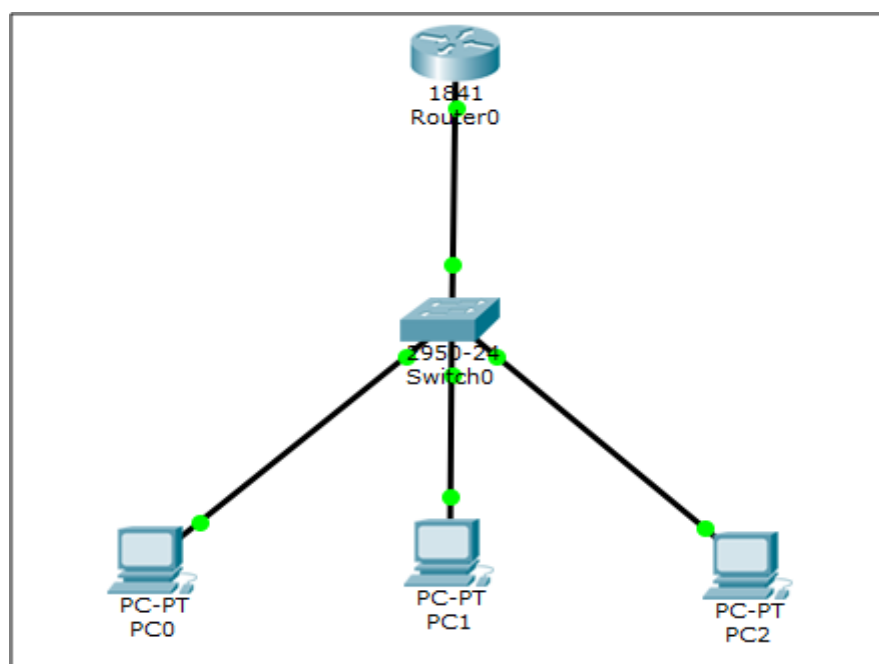
### SSH and Telnet

#### 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 connection with the Telnet protocol, either with commandline client or with a programmatic interface.

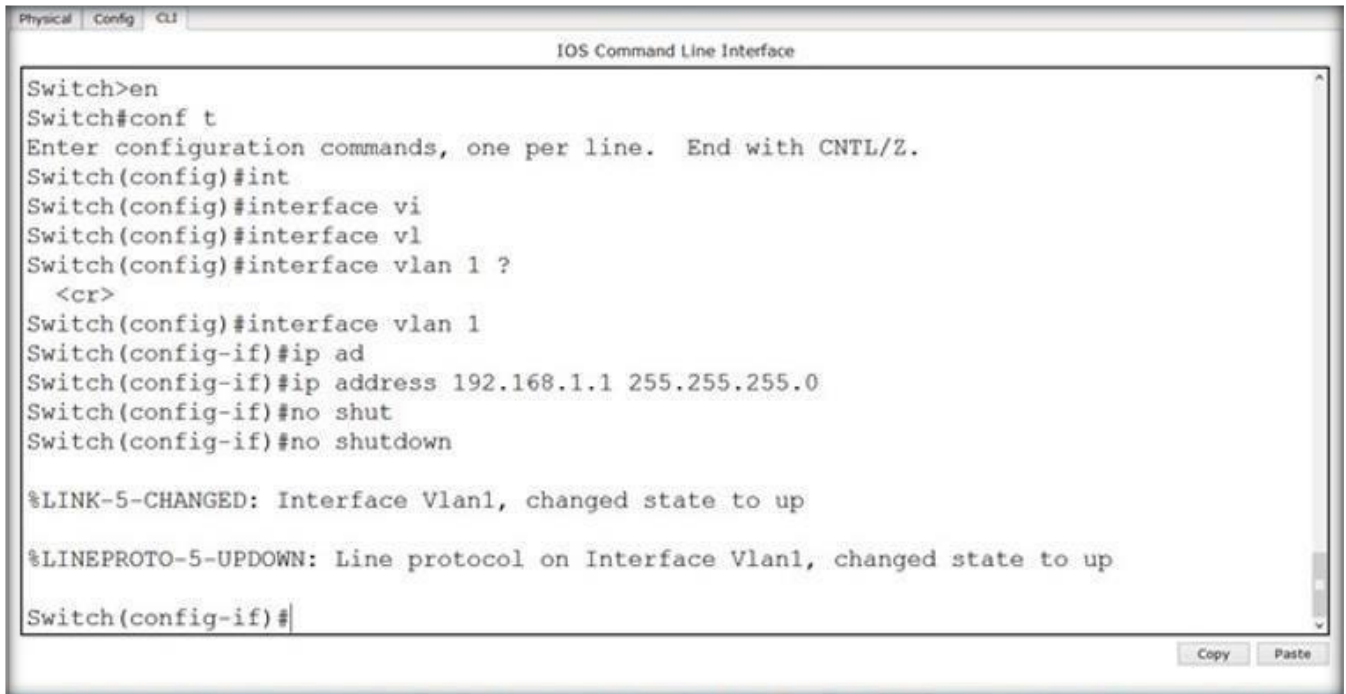
#### Configuration of Telnet:

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

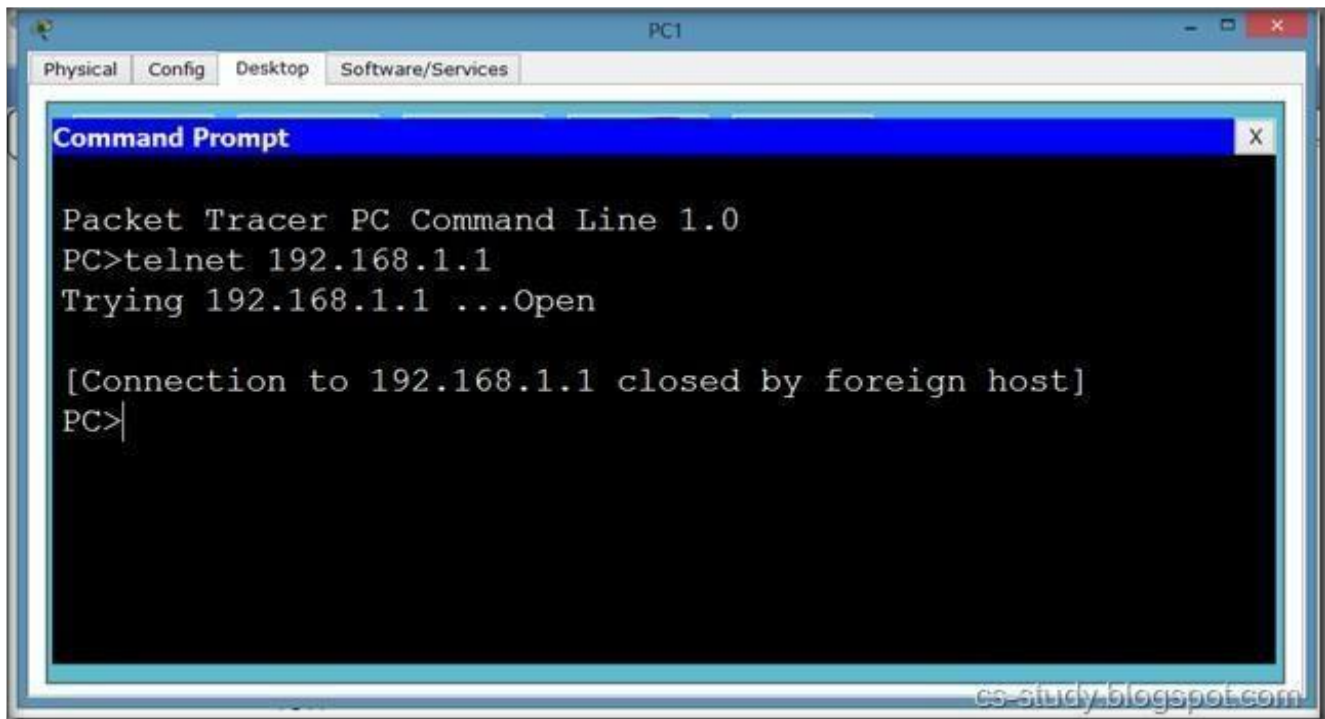
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%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.



```
PC1
Physical Config Desktop Software/Services

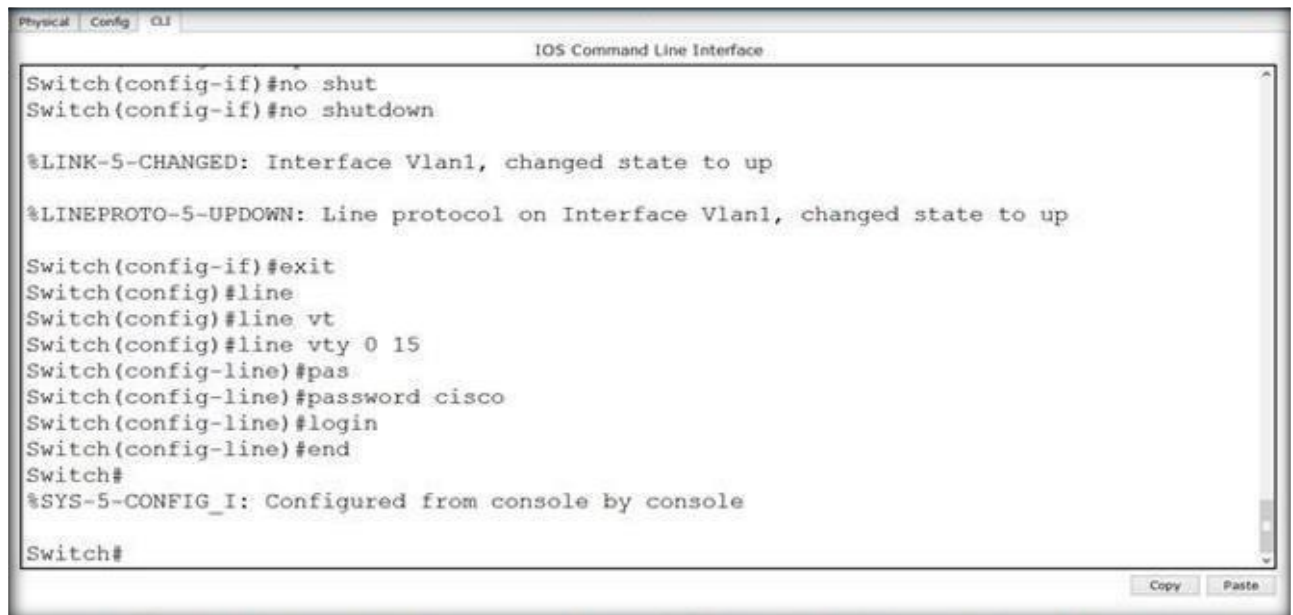
Command Prompt

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>
```

*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

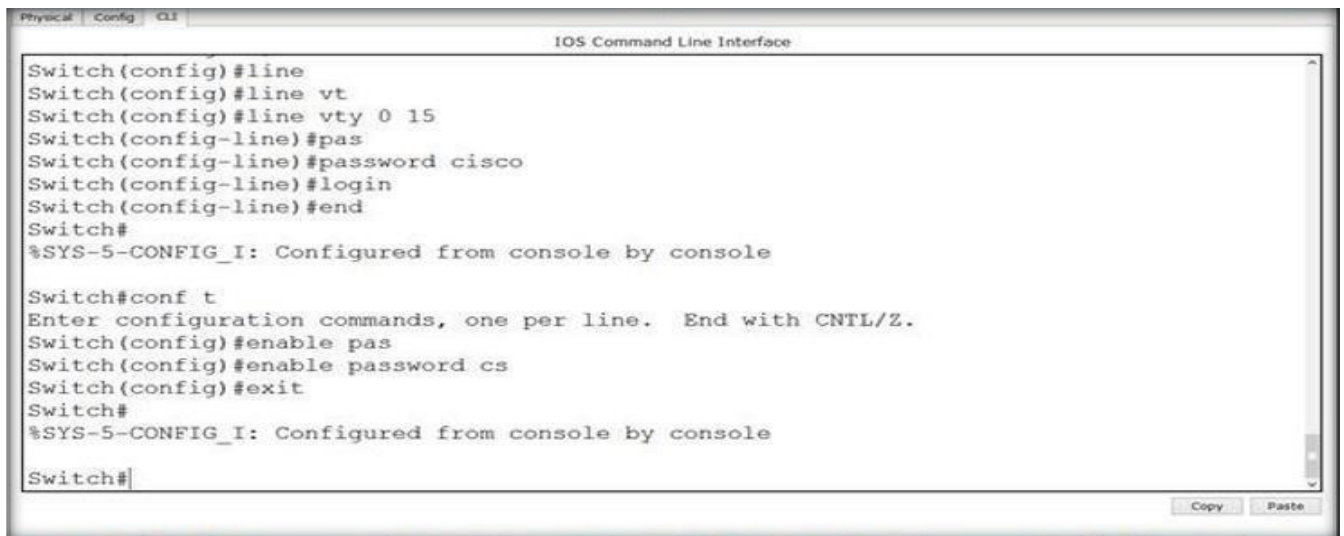
[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

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.



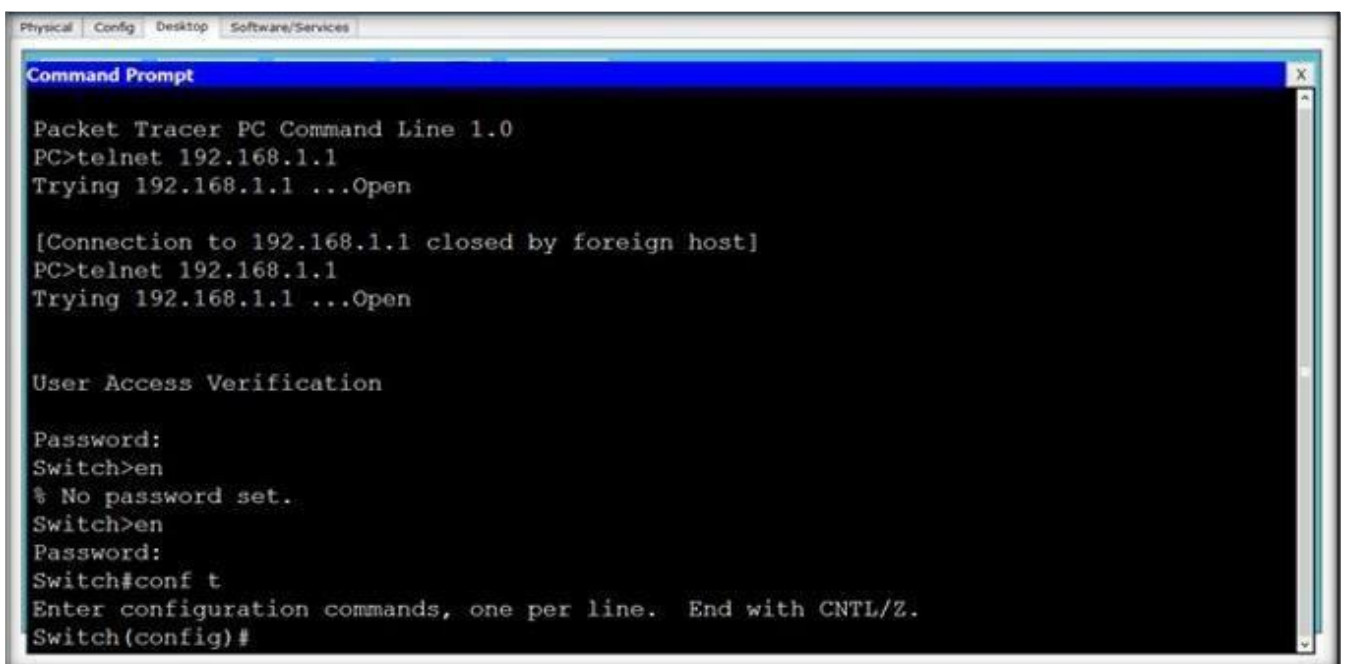
```
Switch(config)#line
Switch(config)#line vt
Switch(config)#line vty 0 15
Switch(config-line)#pas
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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*

## Introduction to SSH:

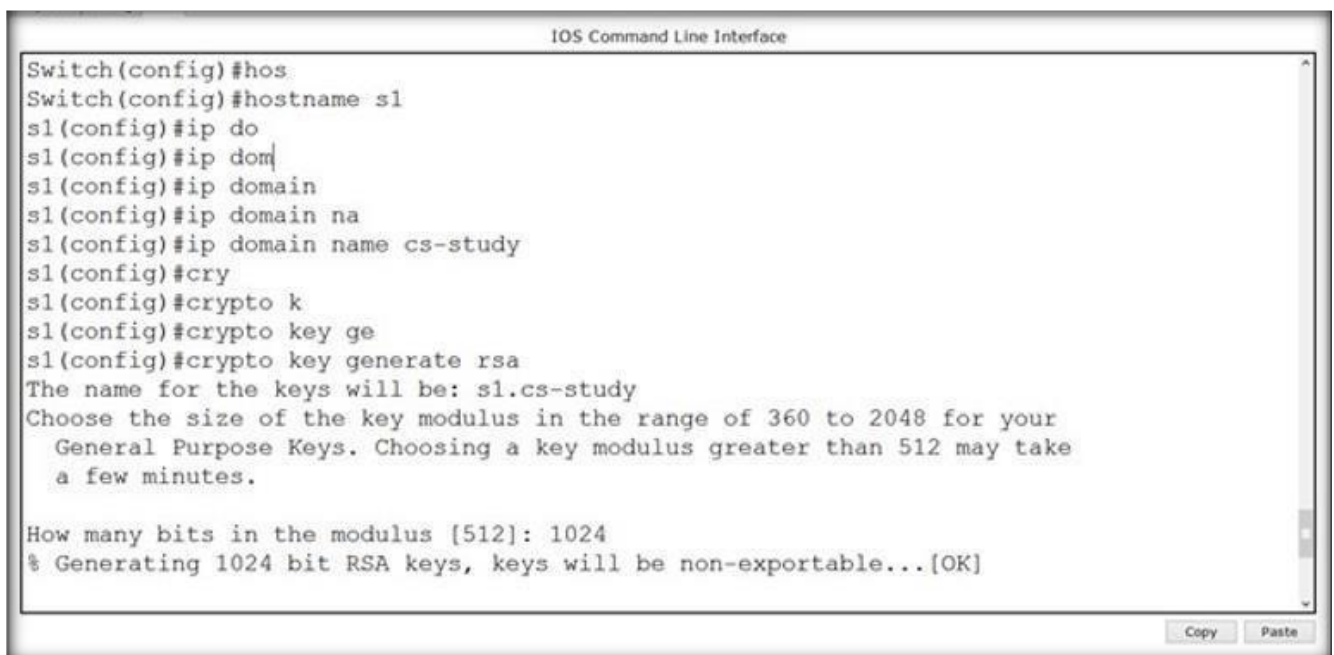
Secure Shell or Secure Socket Shell is a network protocol. It is an application layer protocol that is in the 7th layer of the Open Systems Interconnection (OSI) network model. It also refers to the suite of utilities that implements the SSH protocol.

Secure Shell also supports both password and key-based authentication. Password-based authentication lets 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.

## Configuration of SSH:

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

A screenshot of a Cisco IOS Command Line Interface window. The window title is "IOS Command Line Interface". The terminal shows the following commands and output:

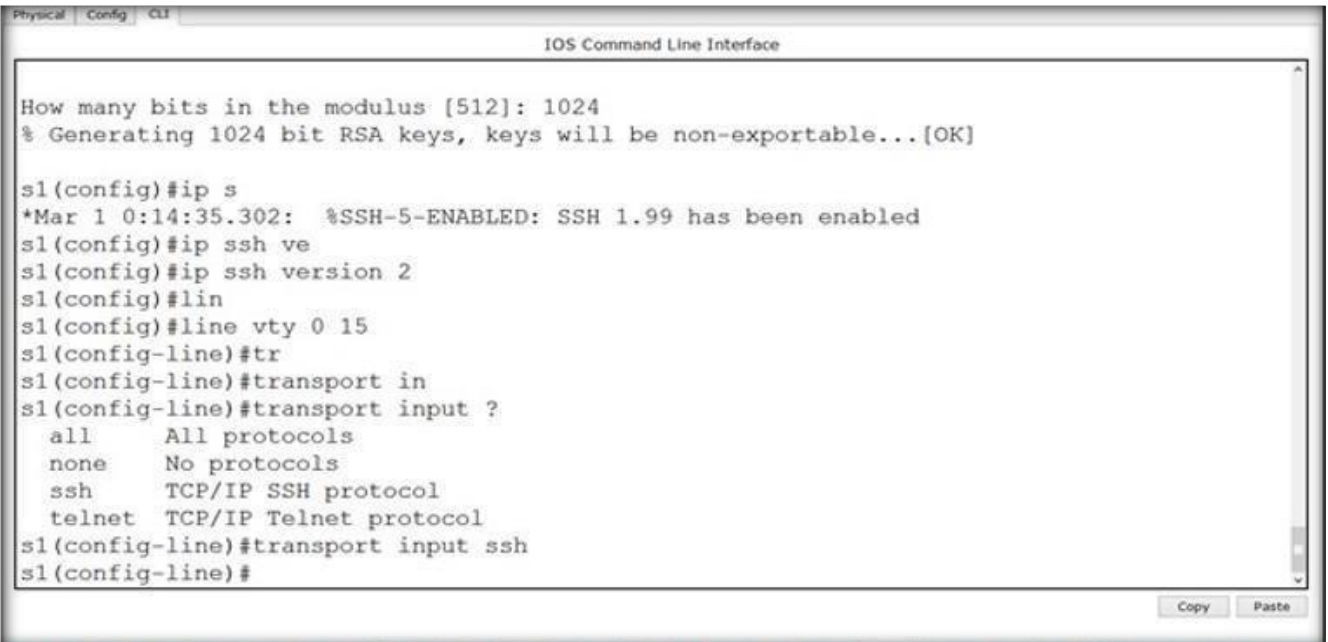
```
Switch(config)#hos
Switch(config)#hostname s1
s1(config)#ip do
s1(config)#ip dom
s1(config)#ip domain
s1(config)#ip domain na
s1(config)#ip domain name cs-study
s1(config)#cry
s1(config)#crypto k
s1(config)#crypto key ge
s1(config)#crypto key generate rsa
The name for the keys will be: s1.cs-study
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]
```

At the bottom right of the window, there are "Copy" and "Paste" buttons.

*Fig-8: Creating Domain & RSA key*

Commands continued.

A screenshot of the IOS Command Line Interface (CLI) window. The window has a title bar with tabs for 'Physical', 'Config', and 'CLI'. The main area displays a series of commands and their outputs. The commands entered are: 's1(config)#ip s', '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 ?', 's1(config-line)#transport input ssh', and 's1(config-line)#'. The outputs include: 'How many bits in the modulus [512]: 1024', '% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]', '\*Mar 1 0:14:35.302: %SSH-5-ENABLED: SSH 1.99 has been enabled', and a list of transport input options: 'all All protocols', 'none No protocols', 'ssh TCP/IP SSH protocol', and 'telnet TCP/IP Telnet protocol'. At the bottom right, there are 'Copy' and 'Paste' buttons.

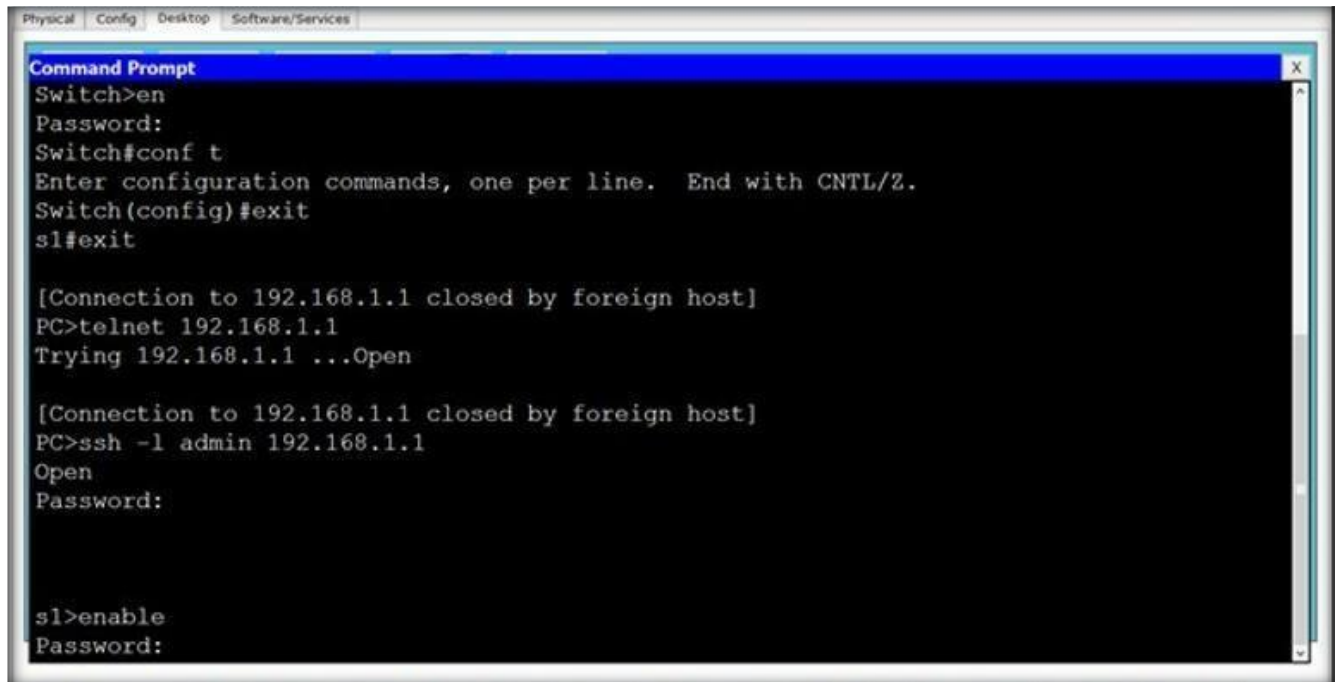
```
Physical Config CLI
IOS Command Line Interface

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

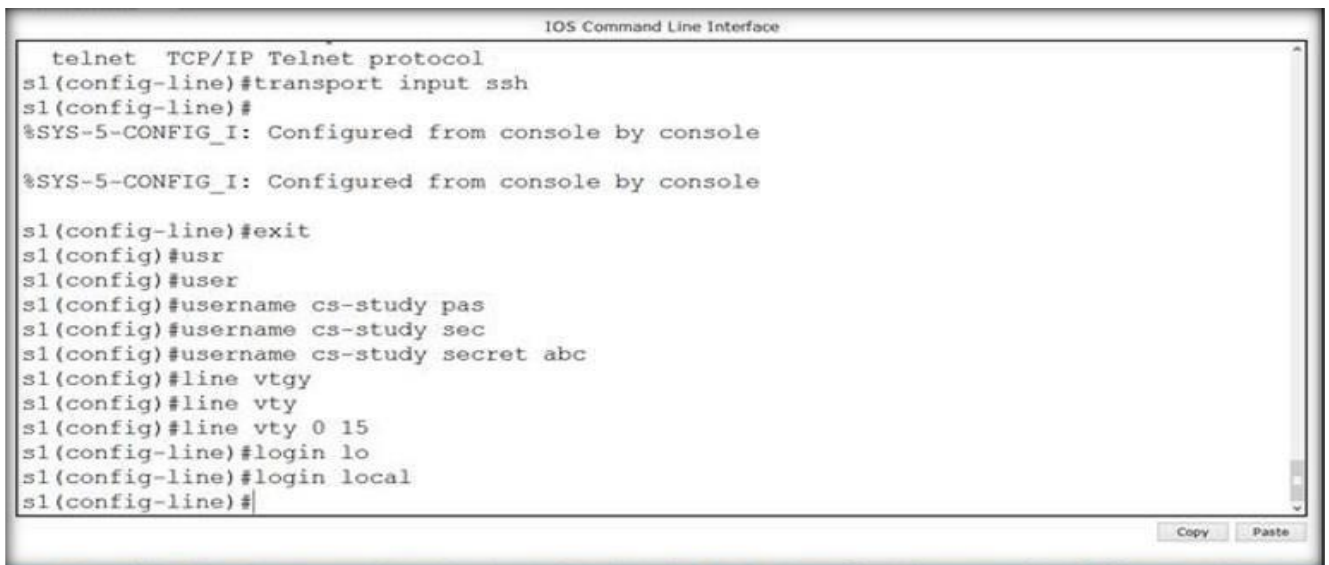
[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l admin 192.168.1.1
Open
Password:

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.



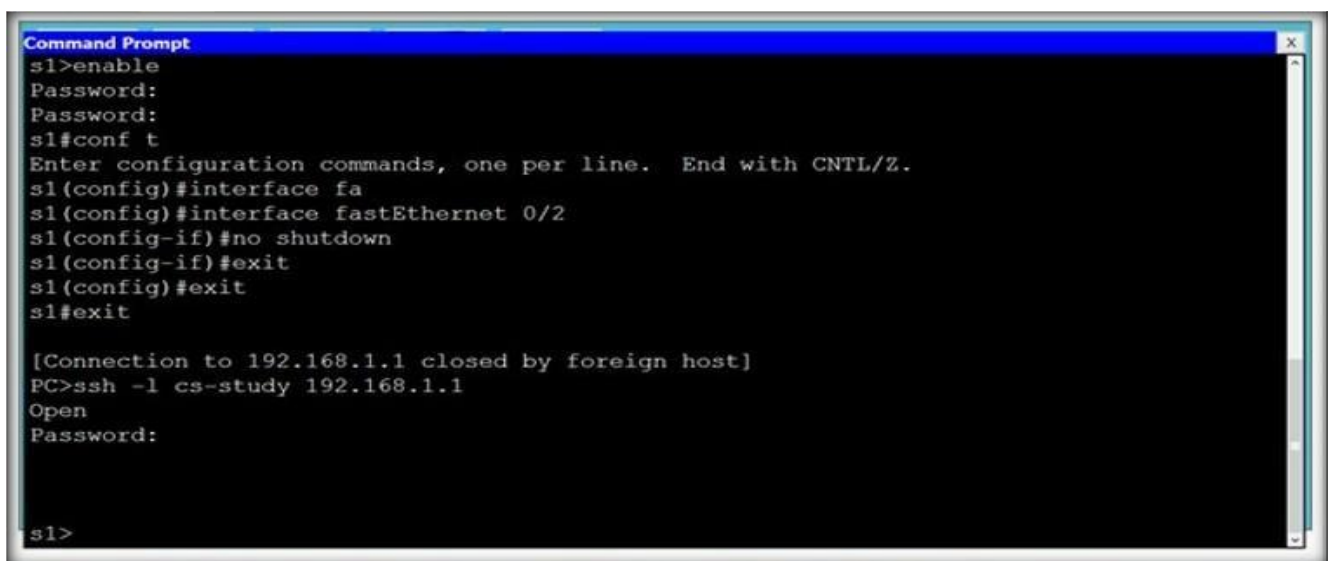


```
IOS Command Line Interface
telnet TCP/IP Telnet protocol
s1(config-line)#transport input ssh
s1(config-line)#
%SYS-5-CONFIG_I: Configured from console by console
%SYS-5-CONFIG_I: Configured from console by console

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:

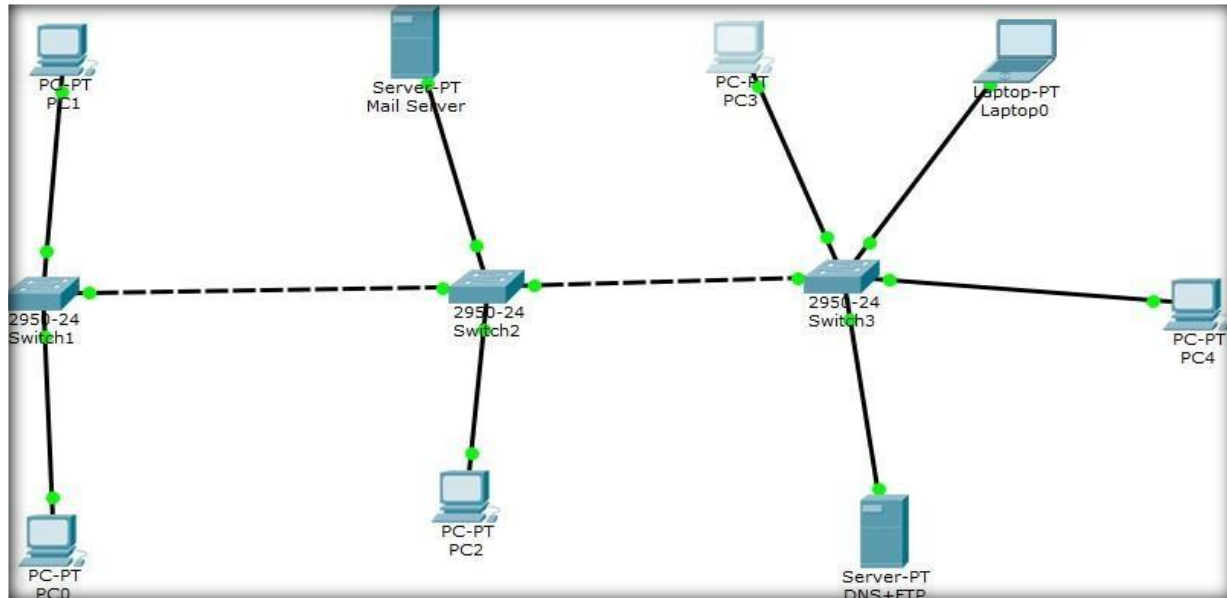
s1>
```

*Fig-13: Checking the connection*



## Lab Exercise SSH & Telnet

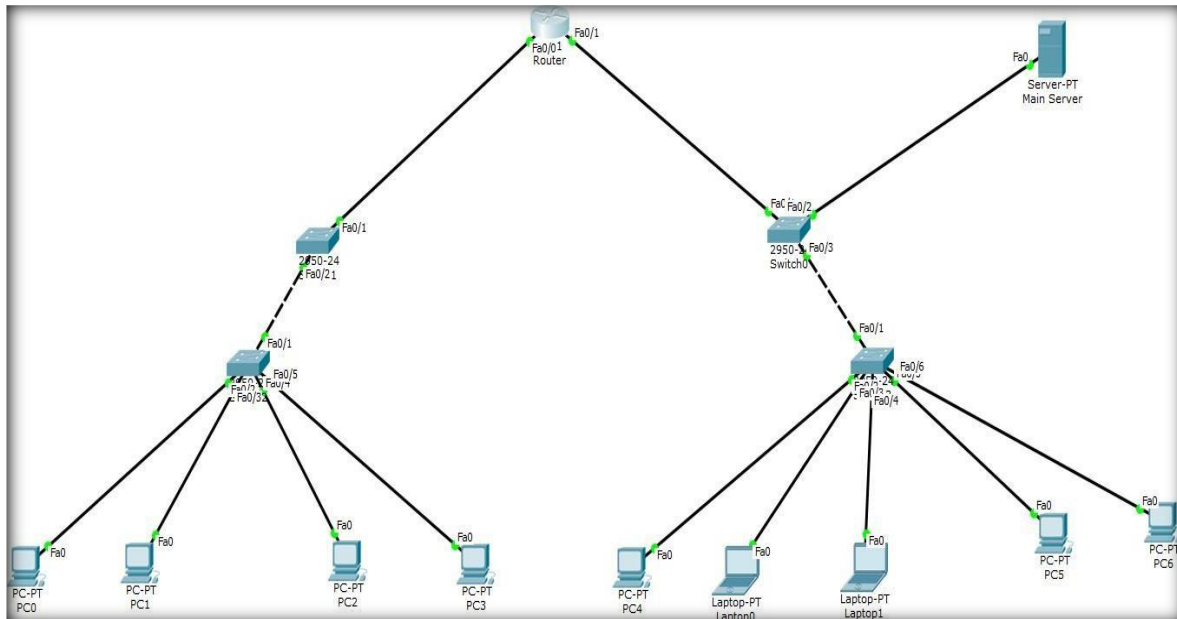
### Question # 1



*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 3479(34.79.0.0)**
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 Fast Ethernet should like this XX.XX.0.0 i.e. your roll number like 4879(48.79.0.0) and on another side it shouldbe 4880(48.80.0.0).
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.Takescreenshot of it.

## Objective:

- Introduction to DHCP & configuration of DHCP on server & router in Cisco Packet Tracer
- Analyzing DHCP packet in Wireshark tool.

### 1. Introduction to DHCP:

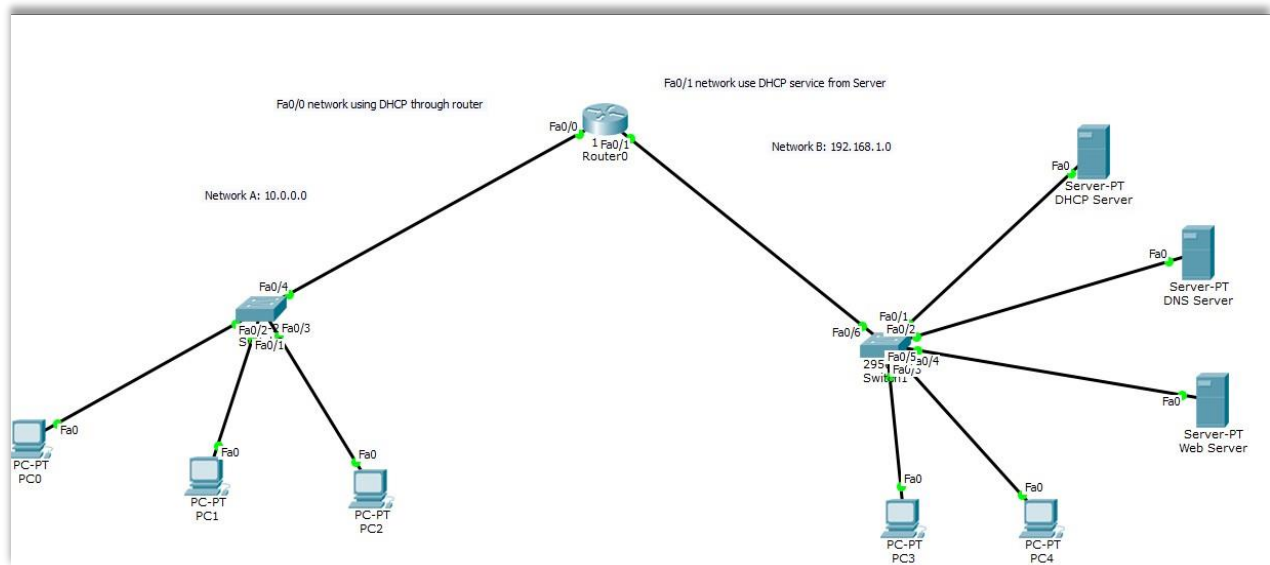
The **Dynamic Host Configuration Protocol** is used by computers for requesting Internet Protocol parameters, such as an IP address from a network server. The protocol operates based on the client-server model. **DHCP** is very common in all modern networks ranging in size from home networks to large campus networks and regional Internet service provider networks. Most residential network routers receive a globally unique IP address within the provider network. Within a local network, **DHCP** assigns a local IP address to devices connected to the local network.

When a computer or other networked device connects to a network, its **DHCP** client software in the operating system sends a broadcast query requesting necessary information. Any **DHCP** server on the network may service the request. The **DHCP** server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, time servers. On receiving a request, the server may respond with specific information for each client, as previously configured by an administrator, or with a specific address and any other information valid for the entire network, and the time period for which the allocation (*lease*) is valid. A host typically queries for this information immediately after booting, and periodically thereafter before the expiration of the information. When an assignment is refreshed by the client computer, it initially requests the same parameter values, but may be assigned a new address from the server, based on the assignment policies set by administrators.

We can use **DHCP** service from router as well as from Server.

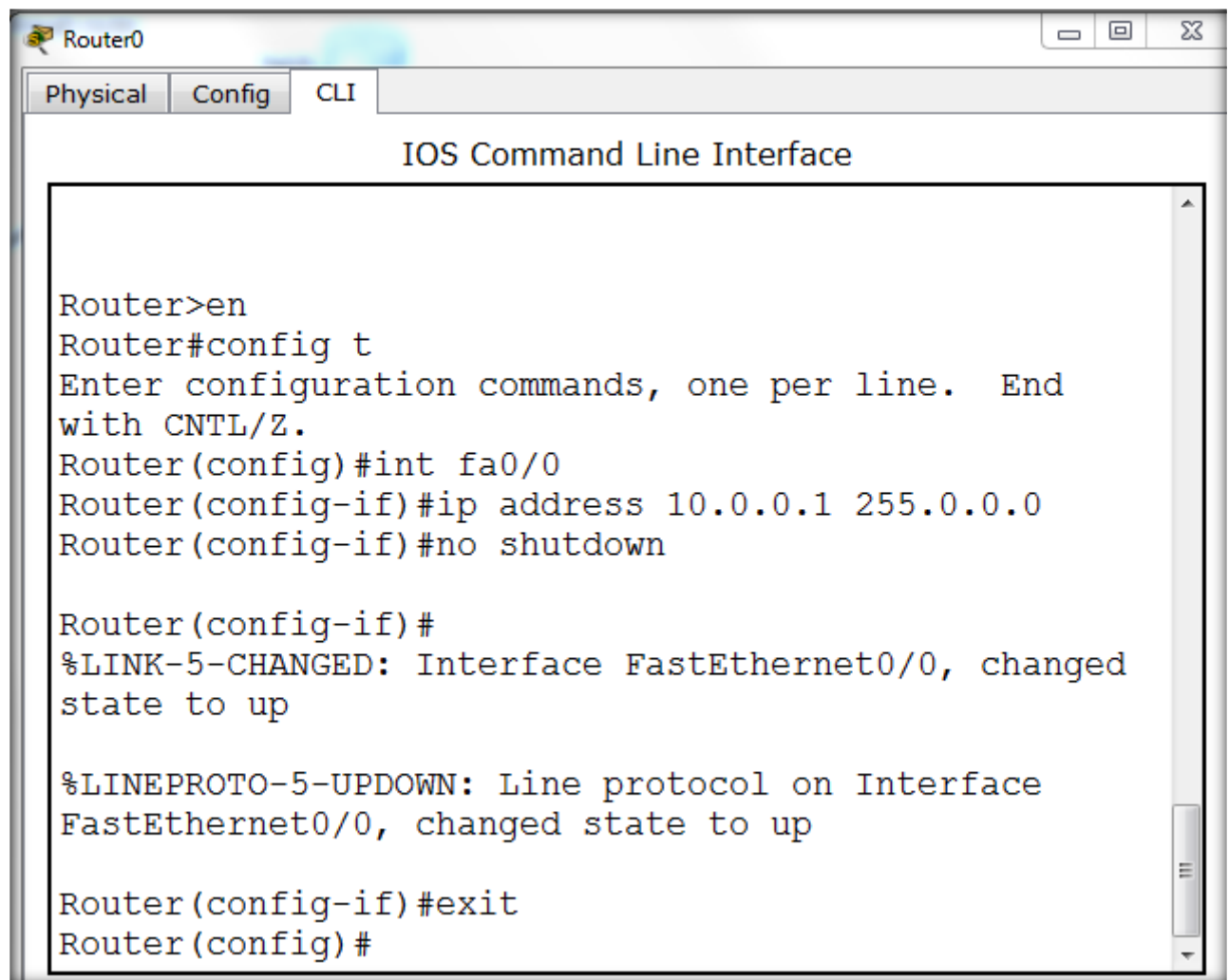
### 2. Configuration of DHCP:

Below are the steps to configure DHCP protocol in Cisco Packet Tracer. DHCP is implemented on router or server these two devices are responsible to assign IP address to host using DHCP protocol. In the given network topology, we have two networks as shown in figure 1. DHCP for network on interface Fa0/0 is implemented on router & for network on Fa0/1 we have DHCP server. First construct given network in packet tracer.



**Fig-1: Network Topology**

**Assign IP to router interface Fa0/0 and turn it on.**



The screenshot shows a window titled "Router0" with three tabs: "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal text is as follows:

```
Router>en
Router#config t
Enter configuration commands, one per line.  End
with CNTL/Z.
Router(config)#int fa0/0
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

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

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

*Fig-2: Assigning IP on Fa0/0 interface*

Now implement DHCP on router to assign IP address to Fa0/0 network

```
Router(config)#ip dhcp pool MY_Net
Router(dhcp-config)#network 10.0.0.0 255.0.0.0
Router(dhcp-config)#default-router 10.0.0.1
Router(dhcp-config)#dns-server 192.168.1.3
Router(dhcp-config)#
```

Copy Paste

Fig-3: Implementing DHCP on router

Now assigning IP to PC0, PC1 & PC2

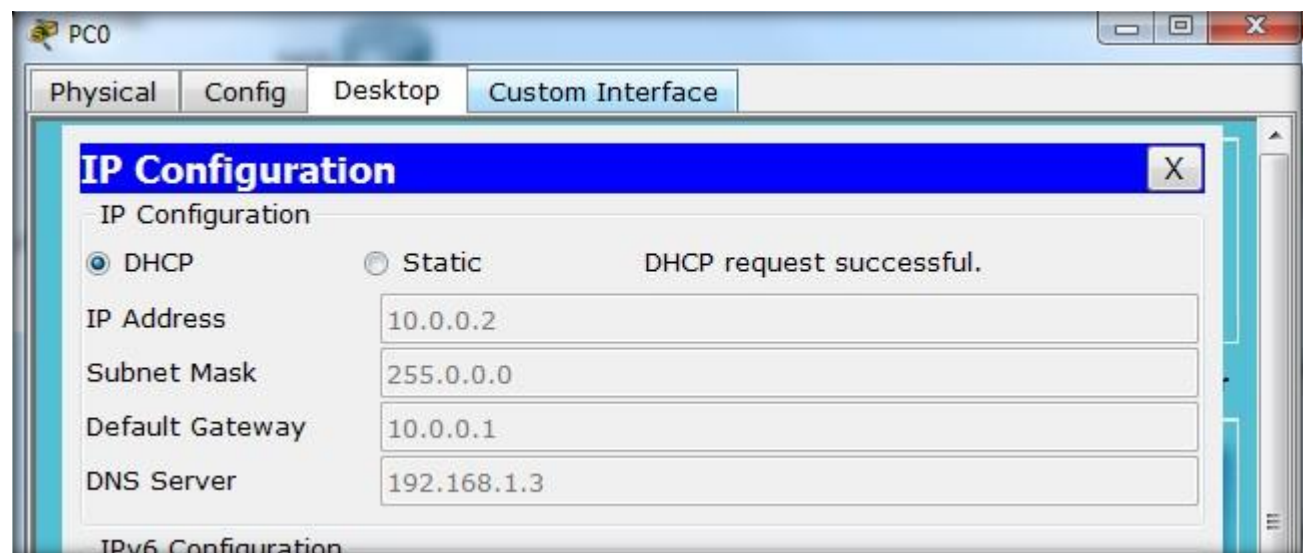


Fig-4: PC0 getting IP through DHCP

You can check the status of assigned IP addresses as shown below.

```
Router#show ip dhcp bin
Router#show ip dhcp binding
IP address      Client-ID/      Lease expiration    Type
                Hardware address
10.0.0.2        000A.F3BA.52C6   --                  Automatic
10.0.0.3        0005.5E56.26DB   --                  Automatic
10.0.0.4        000A.41B3.7946   --                  Automatic
Router#
```

Fig-5: Checking DHCP binding status in router

Note: To exclude an IP address range from DHCP pool use this following command

*Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10*

Now configure router interface Fa0/1. Assign IP address and turn the interface on

```
Router(config)#int fa0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up

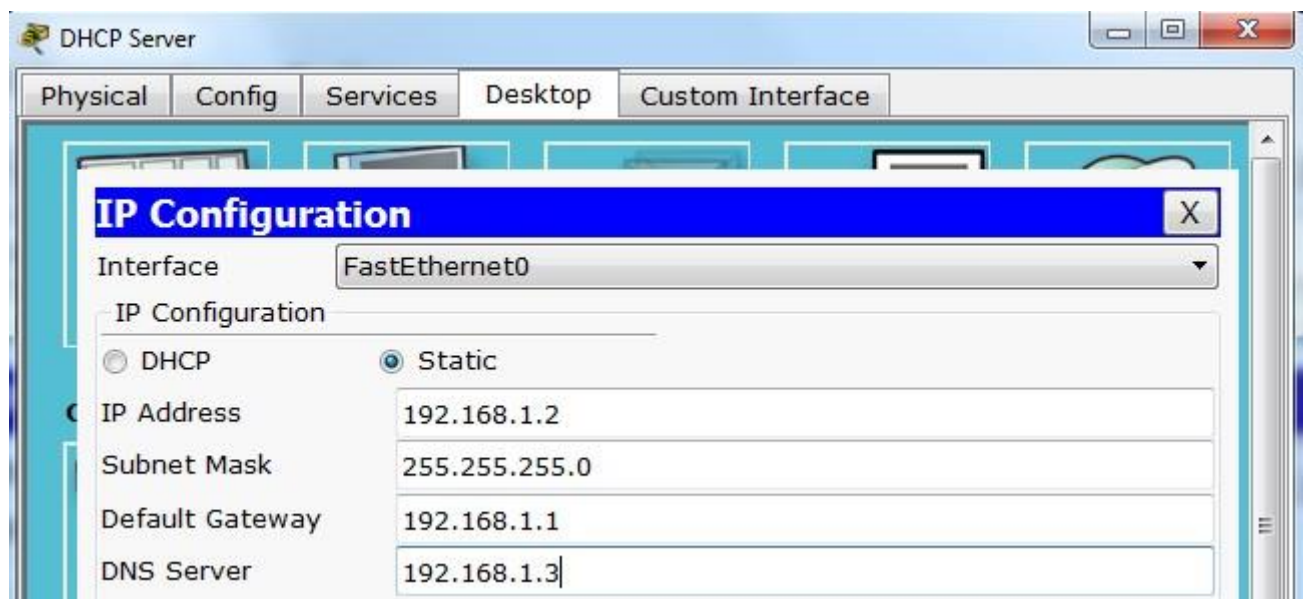
Router(config-if)#
```

Copy

Paste

*Fig-6: Configuring router Fa0/1 interface*

**Click on DHCP server and assign IP address.**



*Fig-7: Assigning IP address to DHCP server*

Now assigning DHCP pool on Server. Go to server → services → DHCP

Physical

Config

Services

Desktop

Custom Interface

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

DHCP

Interface

FastEthernet0

Service

On

Off

Pool Name

serverPool

Default Gateway

192.168.1.1

DNS Server

192.168.1.3

Start IP Address :

192

168

1

3

Subnet Mask:

255

255

255

0

Maximum number of Users :

253

TFTP Server:

0.0.0.0

Add

Save

Remove

Pool Nam	efault Gatew	DNS Serve	art IP Addre	ubnet Mas	Max User	TFTP
server...	192.168.1.1	192.168.1.3	192.168.1.3	255.255....	253	0.0.0.0

Fig-8: Configuring DHCP server



Now assigning IP to DNS server & PCs

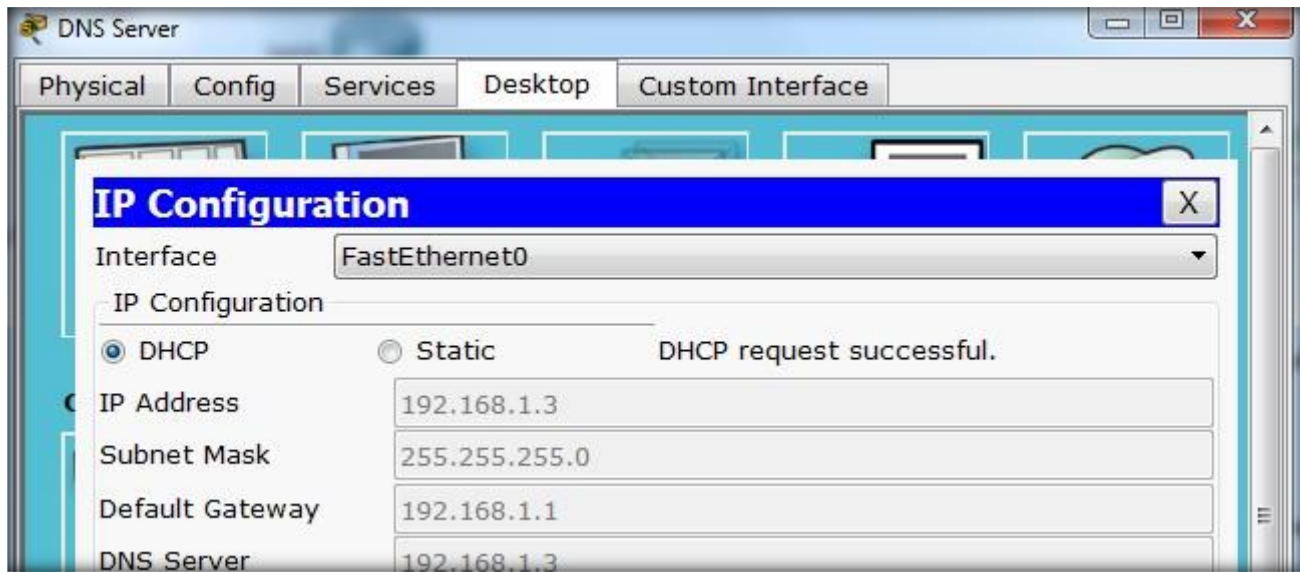


Fig-9: DNS server getting IP through DHCP server

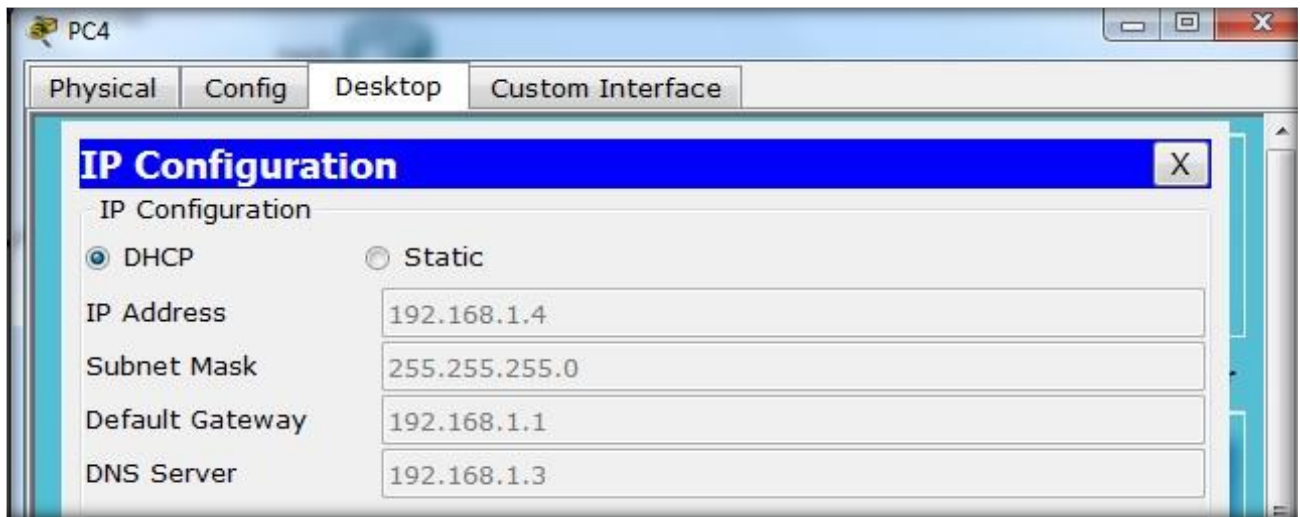


Fig-10: PC4 getting IP through DHCP server

**SIMULATION:**

- a) Now click on simulation icon in the right bottom of packet Tracer.
- b) Now click on auto capture /play icon for packet capturing.
- c) Click on the PC and go to Desktop → IP configuration → DHCP

Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC5	DHCP	
	0.000	--	PC5	DHCP	
	0.001	PC5	Switch4	DHCP	
	0.001	--	PC5	DHCP	
	0.002	PC5	Switch4	DHCP	
	0.002	Switch4	Router1	DHCP	
	0.002	Switch4	PC6	DHCP	
	0.002	Switch4	Server0	DHCP	
	0.003	Switch4	Router1	DHCP	

*Fig-11: DHCP packets in simulation*

Now click on the DHCP packet see how it lease IP address.

**Requesting**

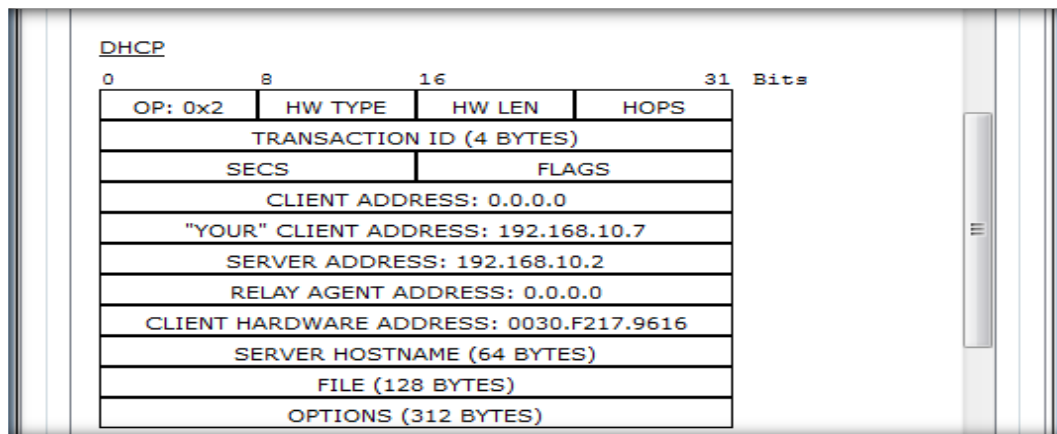
PDU Information at Device: Server0	
OSI Model    Inbound PDU Details	
At Device: Server0 Source: PC5 Destination: 255.255.255.255	
<b>In Layers</b>	
Layer 7: DHCP Frame Server: 0.0.0.0, Client: 0.0.0.0	
Layer6	
Layer5	
Layer 4: UDP Src Port: 68, Dst Port: 67	
Layer 3: IP Header Src. IP: 192.168.10.5, Dest. IP: 255.255.255.255	
Layer 2: Ethernet II Header 0030.F217.9616 >> FFFF.FFFF.FFFF	
Layer 1: Port FastEthernet0	
<b>Out Layers</b>	
Layer7	
Layer6	
Layer5	
Layer4	
Layer3	
Layer2	
Layer1	

*Fig-12: DHCP request packet*

DHCP				31 Bits
0	8	16		
OP: 0x1		HW TYPE	HW LEN	HOPS
TRANSACTION ID (4 BYTES)				
SECS		FLAGS		
CLIENT ADDRESS: 0.0.0.0				
"YOUR" CLIENT ADDRESS: 0.0.0.0				
SERVER ADDRESS: 0.0.0.0				
RELAY AGENT ADDRESS: 0.0.0.0				
CLIENT HARDWARE ADDRESS: 0030.F217.9616				
SERVER HOSTNAME (64 BYTES)				
FILE (128 BYTES)				
OPTIONS (312 BYTES)				

*Fig-13: DHCP request packet heade*

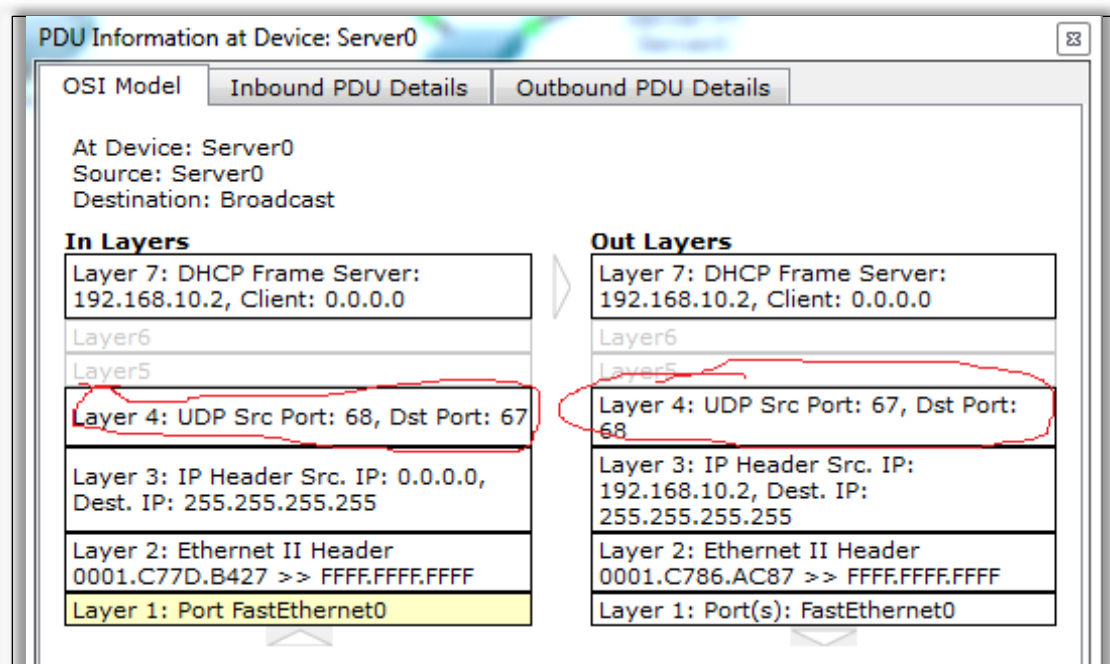
## Leased



*Fig-14: DHCP leased packet header*

## 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).



*Fig-15: DHCP all OSI layers packets*



## DHCP in Wireshark

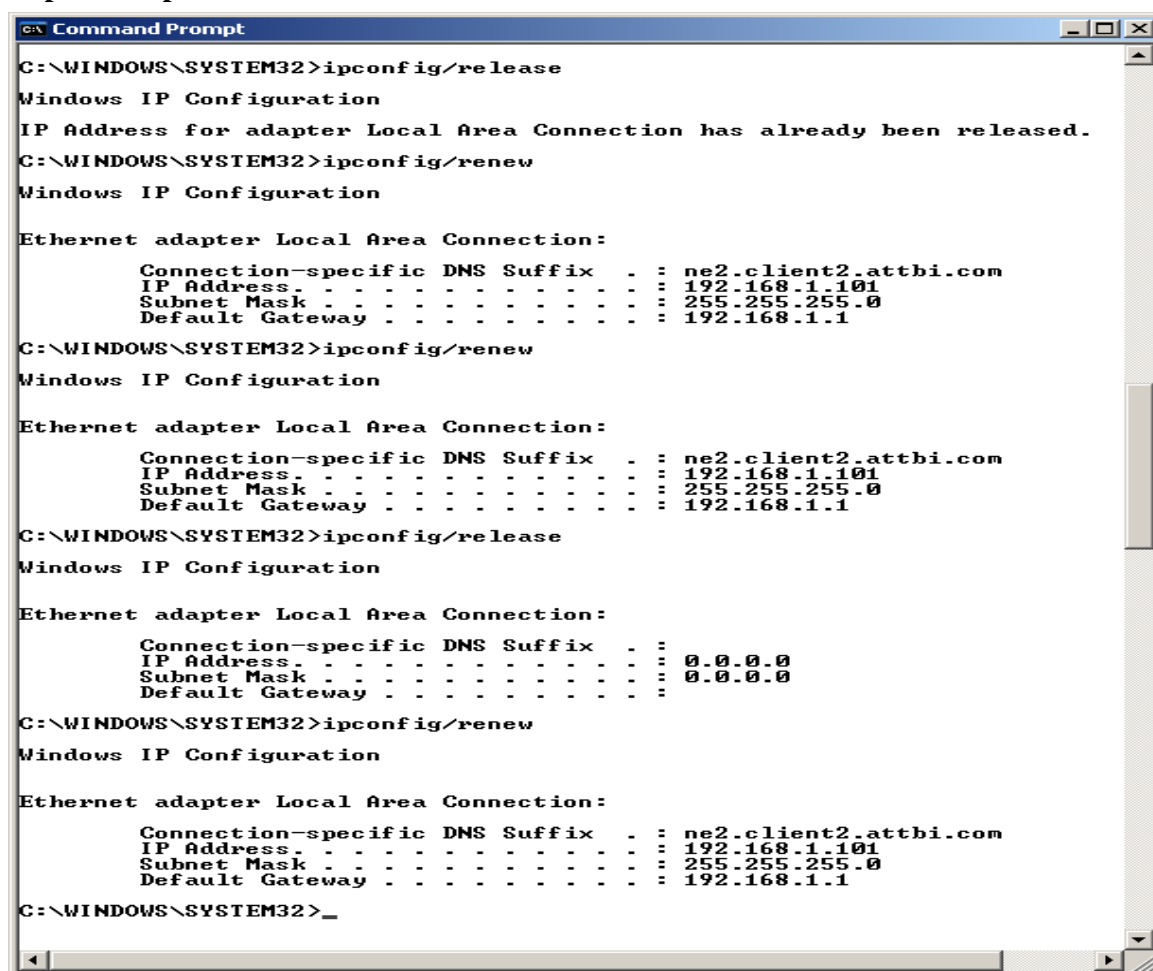
Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). As shown in Figure 1, enter “ipconfig /release”. The executable for ipconfig is in C:\windows\system32. This command releases your current IP address, so that your host’s IP address becomes 0.0.0.0.

Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.

Now go back to the Windows Command Prompt and enter “ipconfig /renew”. This instructs your host to obtain a network configuration, including a new IP address. In Figure 1, the host obtains the IP address 192.168.1.108. Wait until the “ipconfig /renew” has terminated. Then enter the same command “ipconfig /renew” again.

When the second “ipconfig /renew” terminates, enter the command “ipconfig/release” to release the previously-allocated IP address to your computer.

Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.  
**Stop Wireshark packet capture.**



```
C:\WINDOWS\SYSTEM32>ipconfig/release
Windows IP Configuration
IP Address for adapter Local Area Connection has already been released.
C:\WINDOWS\SYSTEM32>ipconfig/renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address . . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>ipconfig/renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address . . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>ipconfig/release
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :

C:\WINDOWS\SYSTEM32>ipconfig/renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address . . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>
```

*Fig-25: Command Prompt window showing sequence of ipconfig commands that you should enter.*

Now let's take a look at the resulting Wireshark window. To see only the DHCP packets, enter into the filter field "bootp". (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68.

To see DHCP packets in the current version of Wireshark, you need to enter "bootp" and not "dhcp" in the filter.) We see from Figure 2 that the first ipconfig renew command caused four DHCP packets to be generated: a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.

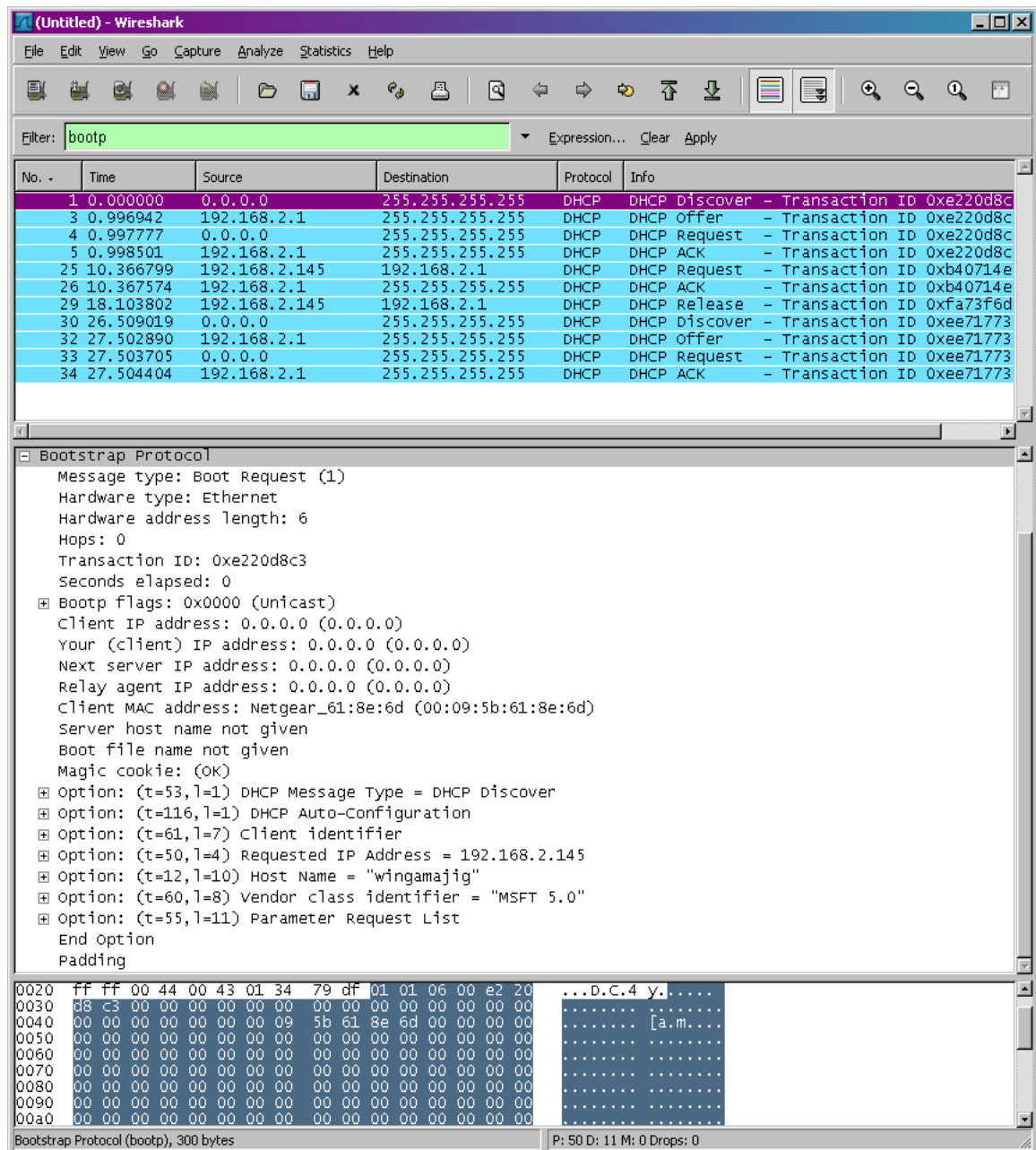


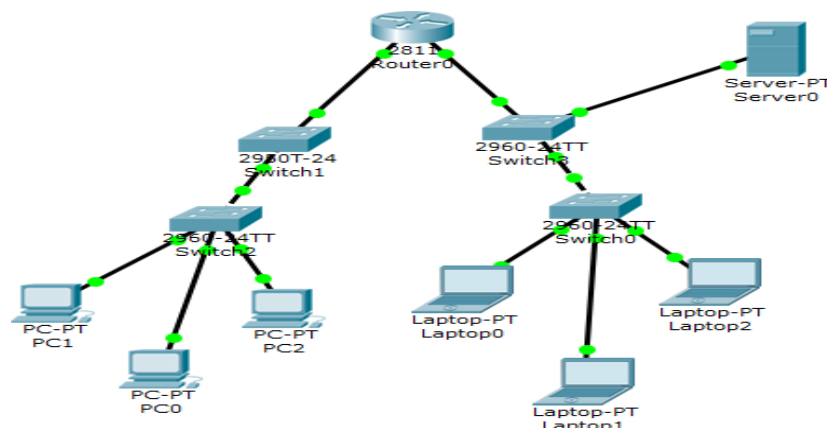
Fig-26: Wireshark window with first DHCP packet – the DHCP Discover packet – expanded.

### Answer the following questions:

1. Are DHCP messages sent over UDP or TCP?
2. What is the link-layer (e.g., Ethernet) address of your host?
3. What values in the DHCP discover message differentiate this message from the DHCP request message?
4. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?
5. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
6. What is the IP address of your DHCP server?
7. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
8. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?
9. Explain the purpose of the lease time. How long is the lease time in your experiment?

### Lab Exercise DHCP

1. Implement the given topology.
2. Implement DHCP on router.
3. Add some web servers in your network.
4. Implement DNS & add records of your web servers.
5. Exclude a certain range of IP and assign those IPs to web server & DNS server.



*Fig-24: Network topology for task*



## Objective:

- Introduction to Subnets & Subnetting
- Purpose of Subnetting
- Subnet tables of different IPv4 classes.
- Introduction of CIDR
- Implementation of Subnetting

## SUBNETTING

### 1. What is Subnet:

A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through Subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.

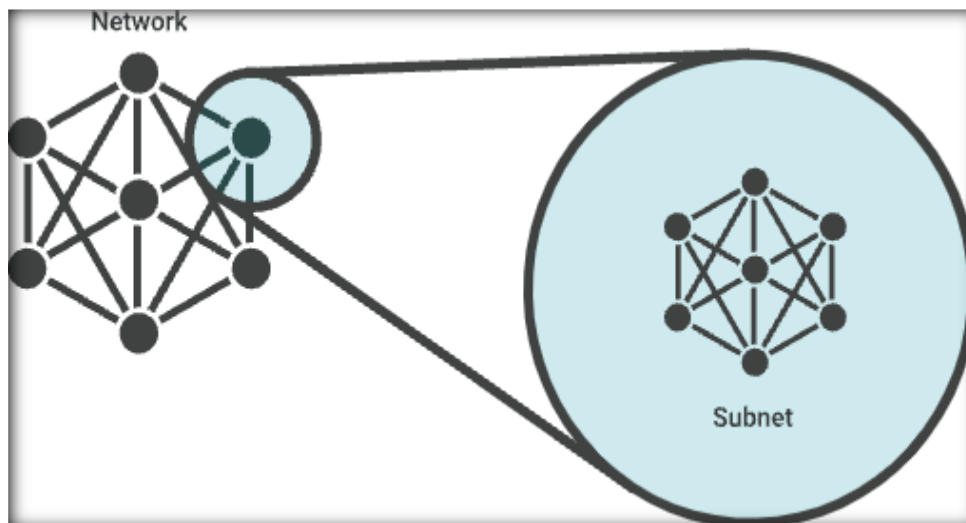


Fig-1: Subnet in network

Imagine Alice puts a letter in the mail that is addressed to Bob, who lives in the town right next to hers. For the letter to reach Bob as quickly as possible, it should be delivered right from Alice's post office to the post office in Bob's town, and then to Bob. If the letter is first sent to post office hundreds of miles away, Alice's letter could take a lot longer to reach Bob.

Like the postal service, networks are more efficient when messages travel as directly as possible. When a network receives data packets from another network, it will sort and route those packets by subnet so that the packets do not take an inefficient route to their destination.

### 2. What is Subnetting:

A subnet is just a range of IP addresses. All the devices in the same subnet can communicate directly with one another without going through any routers. In IPv4, a network interface is connected to only one subnet and has only one IP address. In IPv6 things are slightly more complicated, so we'll save IPv6 Subnetting for another article. But it's useful to understand IPv4 first because the basic concepts are the same.

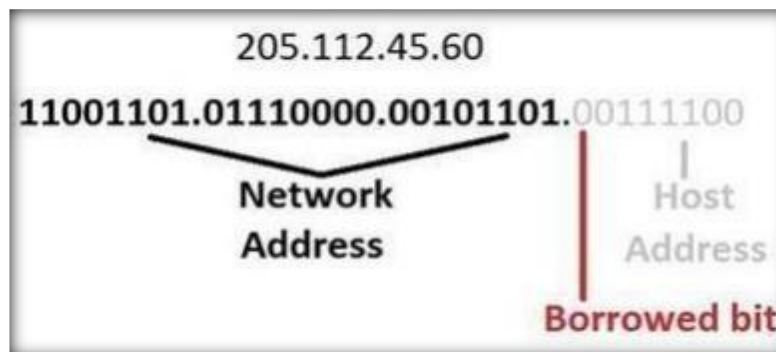
My laptop is on a subnet that also includes a server, a printer, a couple of other workstations, and a router. If I want to communicate with another device in my subnet, I can send packets to it directly. If it's not on my subnet, I need to forward the packet to a router first. That router also needs to be on my subnet. My computer knows that another device is in my subnet by looking at my own IP address and my subnet mask.

Suppose my IP address is 192.168.101.15 and my subnet mask is 255.255.255.0. There are 32 bits in the IP address and the same number in the mask. We always write those 32 bits as four 8-bit numbers, often called octets. The thing that can make it confusing is that we use decimal notation for each of those 8-bit numbers, but the mechanics of Subnetting are really going on in binary.

### 3. Purpose of Subnetting:

To subnet a network means to create logical divisions of the network. Subnetting, therefore, involves dividing the network into smaller portions called subnets. Subnetting applies to IP addresses because this is done by borrowing bits from the host portion of the IP address. In a sense, the IP address then has three components - the network part, the subnet part and, finally, the host part.

We create a subnet by logically grabbing the last bit from the network component of the address and using it to determine the number of subnets required. In the following example, a Class C address normally has 24 bits for the network address and eight for the host, but we are going to borrow the left- most bit of the host address and declare it as identifying the subnet.



*Fig-2: Bits concept of IP*

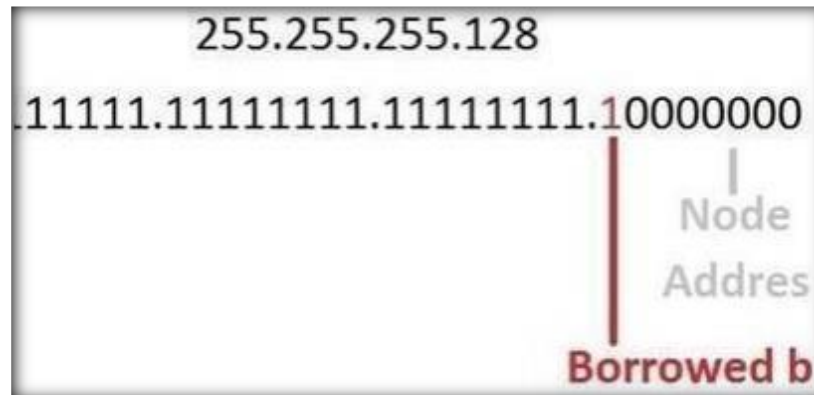
If the bit is a 0, then that will be one subnet; if the bit is a 1 that would be the second subnet. Of course, with only one borrowed bit we can only have two possible subnets. By the same token, that also reduces the number of hosts we can have on the network to 127 (but actually 125 useable addresses given all zeros and all ones are not recommended addresses), down from 255.

So how can you tell how many bits should be borrowed, or, in other words, how many subnets we want to

have on our network? The answer is with a subnet mask.

Subnet masks sound a lot scarier than they really are. All that a subnet mask does is indicate how many bits are being “borrowed” from the host component of an IP address.

If you can’t remember anything about Subnetting, remember this concept. It is the foundation of all Subnetting. The reason a subnet mask has this name is that it literally masks out the host bits being borrowed from the host address portion of the IP address. In the following diagram, there is a subnet mask for a Class C address. The subnet mask is 255.255.255.128 which, when translated into bits, indicates which bits of the host part of the address will be used to determine the subnet number.



*Fig-3: Borrowed bit from host section to network section*

More bits borrowed means fewer individually addressable hosts that can be on the network. Sometimes, all the combinations and permutations can be confusing, so here are some tables of subnet possibilities.

#### **4. Subnet Tables of IPv4:**

In pervious lab we study the default subnet mask for each class IPv4. In this section we provided the subnet tables of class A, B & C when we create subnet from these IP address.

Address Class	Value in First Octet	Classful Mask (Dotted Decimal)	Classful Mask (Prefix Notation)
Class A	1–126	255.0.0.0	/8
Class B	128–191	255.255.0.0	/16
Class C	192–223	255.255.255.0	/24
Class D	224–239	—	—
Class E	240–255	—	—

*Fig-4: Default Subnet mask of each IPv4 class*

## CLASS A HOST/Subnet Table

**Class A Host/Subnet Table**

Class A bits	Subnet Mask	Effective Subnets	Effective Hosts	Number of Subnet Mask bits
1	255.128.0.0	2	8388606	/9
2	255.192.0.0	4	4194302	/10
3	255.224.0.0	8	2097150	/11
4	255.240.0.0	16	1048574	/12
5	255.248.0.0	32	524286	/13
6	255.252.0.0	64	262142	/14
7	255.254.0.0	128	131070	/15
8	255.255.0.0	256	65534	/16
9	255.255.128.0	512	32766	/17
10	255.255.192.0	1024	16382	/18
11	255.255.224.0	2048	8190	/19
12	255.255.240.0	4096	4094	/20
13	255.255.248.0	8192	2046	/21
14	255.255.252.0	16384	1022	/22
15	255.255.254.0	32768	510	/23
16	255.255.255.0	65536	254	/24
17	255.255.255.128	131072	126	/25
18	255.255.255.192	262144	62	/26
19	255.255.255.224	524288	30	/27
20	255.255.255.240	1048576	14	/28
21	255.255.255.248	2097152	6	/29
22	255.255.255.252	4194304	2	/30
23	255.255.255.254	8388608	2	/31

*Fig-5: Class A subnet table*

## Class B Host / Subnet Table

### Class B Host / Subnet Table

Class B bits	Subnet Mask	Effective Subnets	Effective Hosts	Number of Subnet Mask bits
1	255.255.128.0	2	32766	/17
2	255.255.192.0	4	16382	/18
3	255.255.224.0	8	8190	/19
4	255.255.240.0	16	4094	/20
5	255.255.248.0	32	2046	/21
6	255.255.252.0	64	1022	/22
7	255.255.254.0	128	510	/23
8	255.255.255.0	256	254	/24
9	255.255.255.128	512	126	/25
10	255.255.255.192	1024	62	/26
11	255.255.255.224	2048	30	/27
12	255.255.255.240	4096	14	/28
13	255.255.255.248	8192	6	/29
14	255.255.255.252	16384	2	/30
15	255.255.255.254	32768	2	/31

*Fig-6: Class B subnet table*

## Class C Host / Subnet Table

### Class C Host / Subnet Table

Class C bits	Subnet Mask	Effective Subnets	Effective Hosts	Number of Subnet Mask bits
1	255.255.255.128	2	126	/25
2	255.255.255.192	4	62	/26
3	255.255.255.224	8	30	/27
4	255.255.255.240	16	14	/28
5	255.255.255.248	32	6	/29
6	255.255.255.252	64	2	/30
7	255.255.255.254	128	2	/31

*Fig-7: Class C subnet table*

## 5. CIDR:

Having spent a whole bunch of time learning about IP addresses and classes, you might be surprised that in reality they are not used anymore other than to understand the basic concepts of IP addressing.

Instead, network administrators use **Classless Internet Domain Routing (CIDR)**, pronounced "cider", to represent IP addresses. The idea behind CIDR is to adapt the concept of Subnetting to the entire Internet. In short, classless addressing means that instead of breaking a particular network into subnets, we can aggregate networks into larger supernets.

CIDR is therefore often referred to as supernetting, where the principles of subnetting are applied to largernetworks. CIDR is written out in a network/mask format, where the mask is tacked onto the network address in the form of the number of bits used in the mask. An example would be 205.112.45.60/25. What is mostimportant to understand about the CIDR method of subnetting is the use the network prefix (the /25 of 205.112.45.60/25), rather than the classful way of using the first three bits of the IP address to determine the dividing point between the network number and the host number.

### **The process for understanding what this mean is**

1. The "205" in the first octet means this IP address would normally contain 24 bits to represent the network portion of the address. With eight bits to an octet, the arithmetic is  $3 \times 8 = 24$ , or looking at itthe other way around, "/24" means no bits are being borrowed from the last octet.
2. But this is "/25," which indicates it is "borrowing" one bit from the host portion of the address.
3. With only one bit, there can only be two unique subnets.
4. So, this is the equivalent of a net mask of 255.255.255.128, where there is a maximum of 126 host addresses addressable on each of the two subnets.

So why did CIDR become so popular? Because it's a much more efficient allocator of the IP address space. Using CIDR, a network admin can carve out a number of host addresses that's closer to what is required than with the class approach.

For example, say a network admin has an IP address of 207.0.64.0/18 to work with. This block consists of 16,384 IP addresses. But if only 900 host addresses are required, this wastes scarce resources, leaving 15,484 ( $16,384 - 900$ ) addresses unused. By using a subnet CIDR of 207.0.68.0/22 though, the network would address 1,024 nodes, which is much closer to the 900 host addresses required.

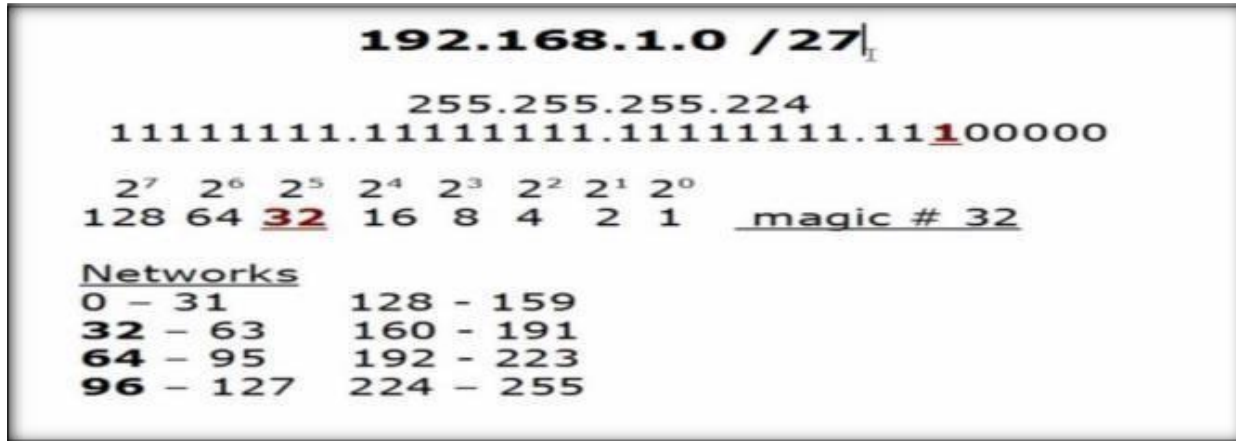
CIDR Prefix	Dotted Decimal Notation	# Node Addresses	# of Traditional Class Networks
/13	255.248.0.0	512K	8 B or 2048 C class
/14	255.252.0.0	256K	4 B or 1024 C class
/15	255.254.0.0	128K	2 B or 512 C class
/16	255.255.0.0	64K	1 B or 256 C class
/17	255.255.128.0	32K	128 C class
/18	255.255.192.0	16K	64 C class
/19	255.255.224.0	8K	32 C class
/20	255.255.240.0	4K	16 C class
/21	255.255.248.0	2K	8 C class
/22	255.255.252.0	1K	4 C class
/23	255.255.254.0	512	2 C class
/24	255.255.255.0	256	1 C class
/25	255.255.255.128	128	1/2 C class
/26	255.255.255.192	64	1/4 C class
/27	255.255.255.224	32	1/8 C class



**Fig-8: CIDR Address table**

## 6. Implementation of Subnetting on Packet Tracer:

Consider an IP of Class C 192.168.1.0/27, using above IP calculate the subnets and implement the scenario in Cisco Packet Tracer.



**Fig-9: Logical Subnets**

**Calculation:**

From above figure 3, we have:

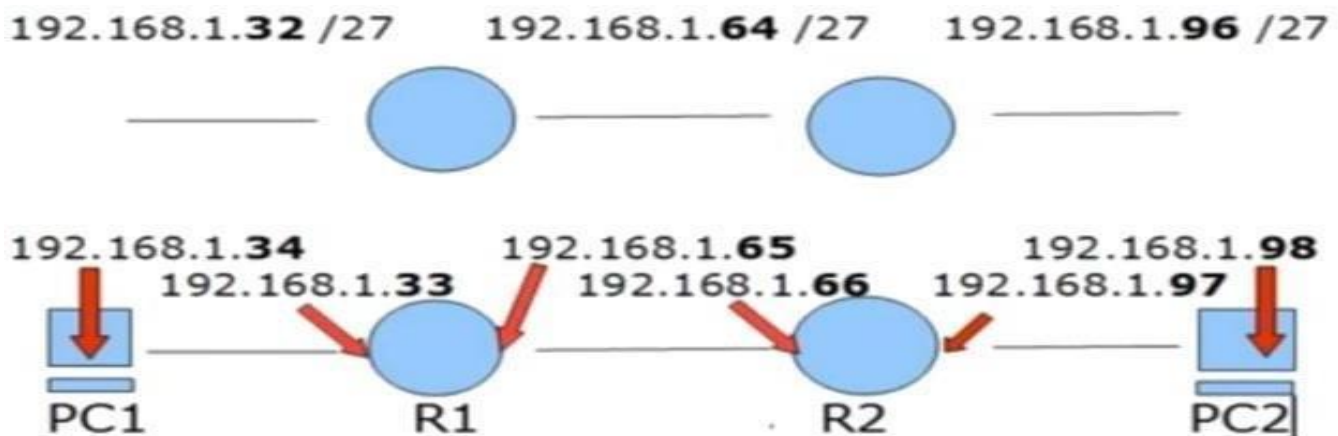
Possible Subnets:  $2^n = 2^3 = 8$  Possible Hosts = 32

Usable Hosts in each Subnet =  $32 - 2 = 30$

Note: 1st address of every subnet shows network address and last address shows Broadcast address. e.g., 0,32,64 & 96 represent Network address where 31,63,95 & 127 represent Broadcast address.

Custom Subnet Mask = 255.255.255.224

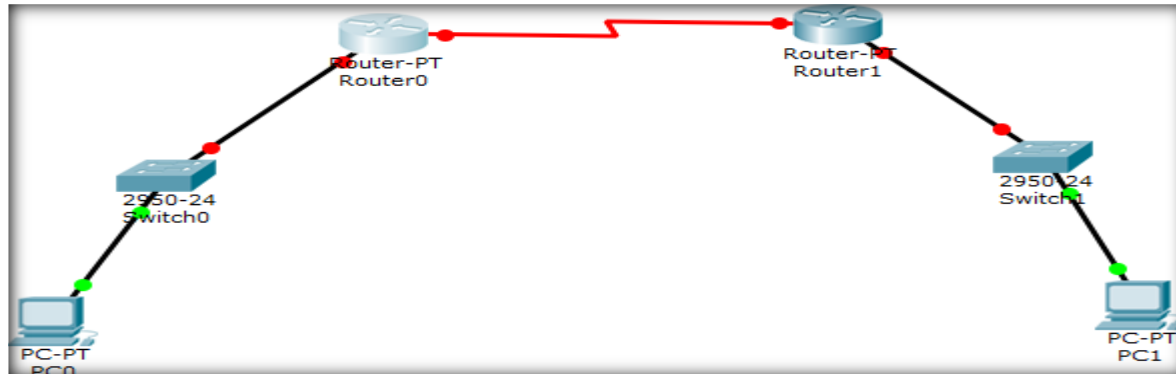
Now implementing below figure 10 scenarios on Cisco packet Tracer.



**Fig-10: Scenario to implement**

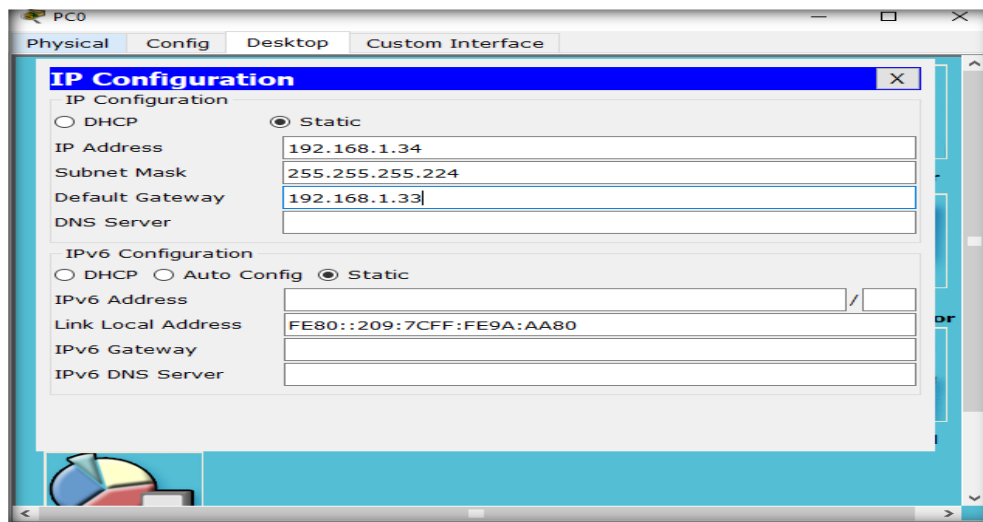


We have taken two routers R1 & R2 and connected their Fast Ethernet interface Fa 0/0 with the switch. While routers connected with their serial interface 2/0.



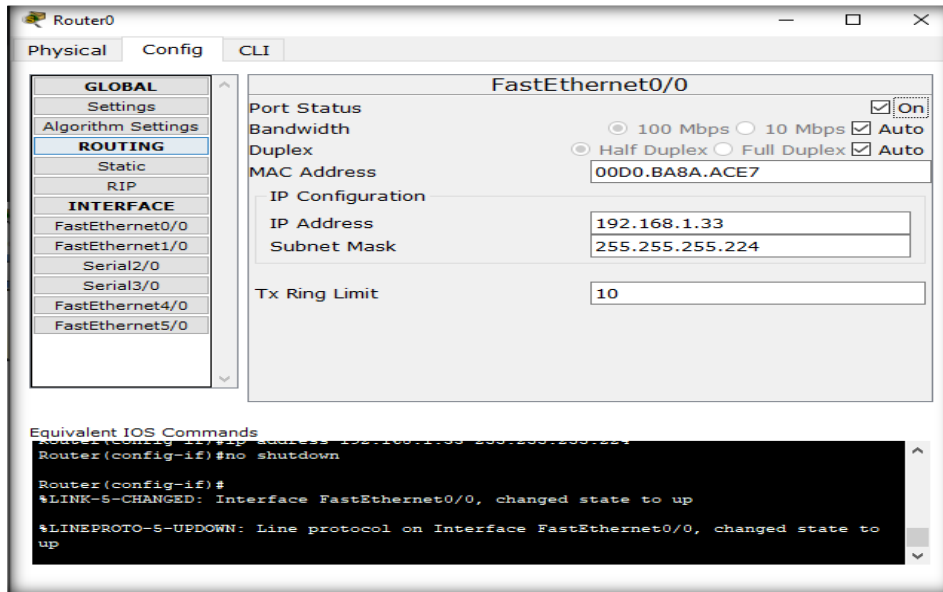
*Fig-11: Network Topology*

Now configuring PC0.



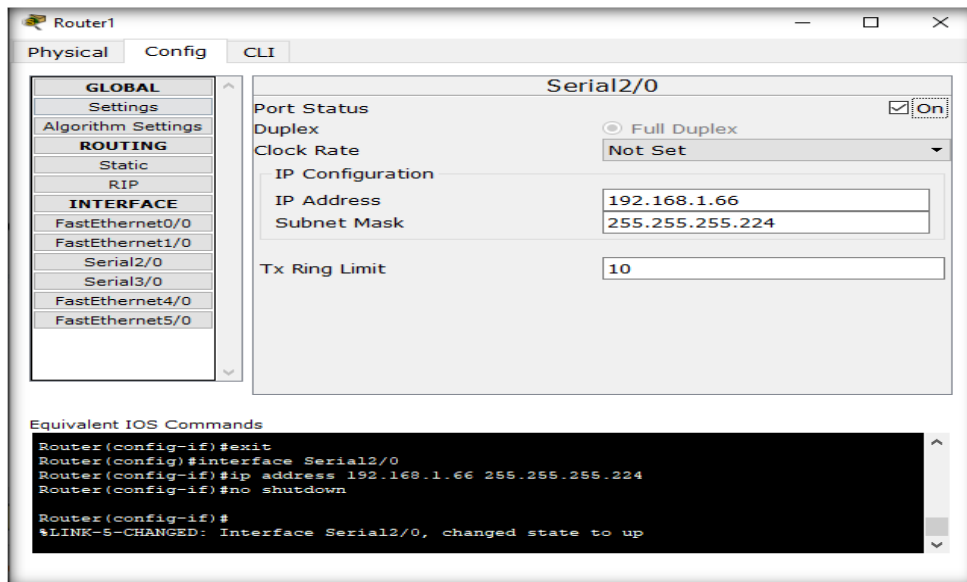
*Fig-12: Assigning IP to PC0*

Now configure the Interface FastEthernet0/0 of Router R0.



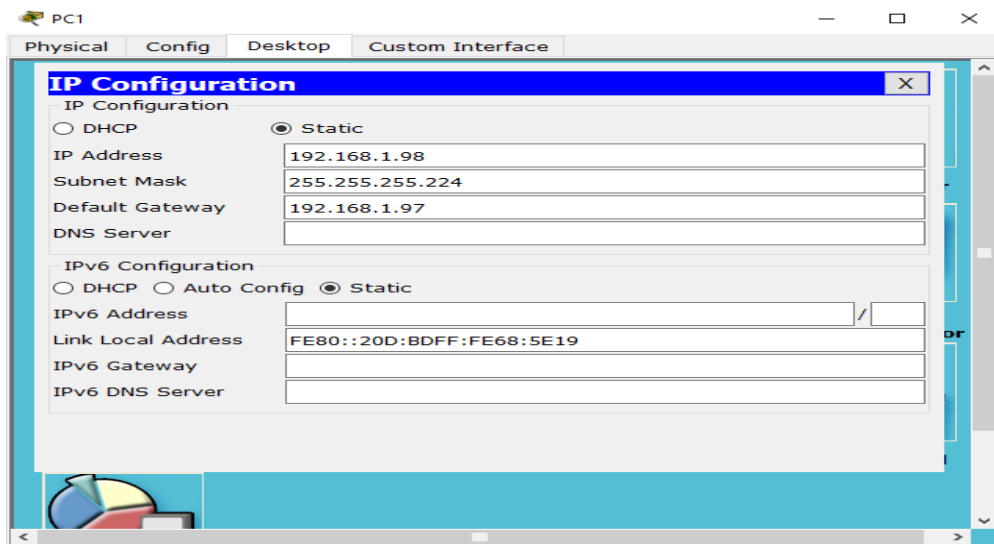
*Fig-13: Interfacing Router 0 FastEthernet0/0*

Configure the Interface Serial2/0 of Router R1



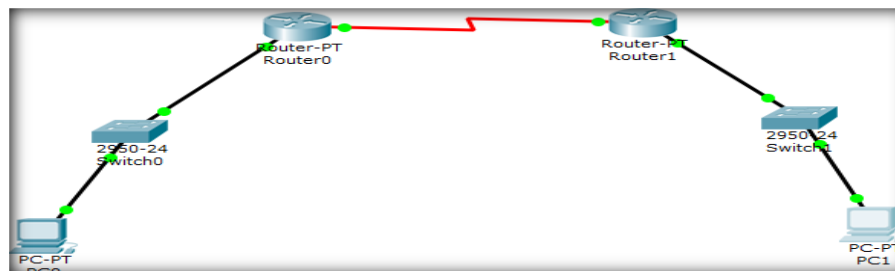
*Fig-14: Interfacing Serial interface of Router 0*

Now configuring PC1.



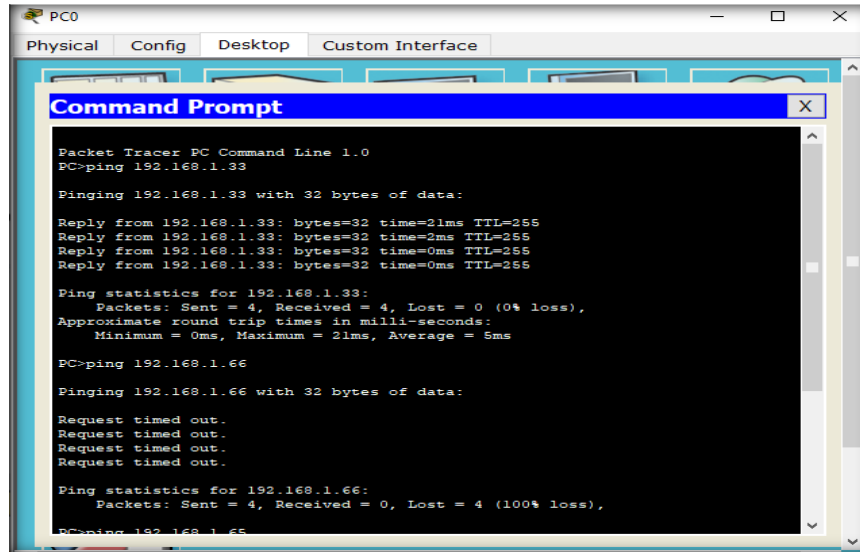
*Fig-15: Assigning IP to PC1*

Now we have gone through the entire configuration, all the interfaces are up as shown in figure 16.



*Fig-16: All links are up in network*

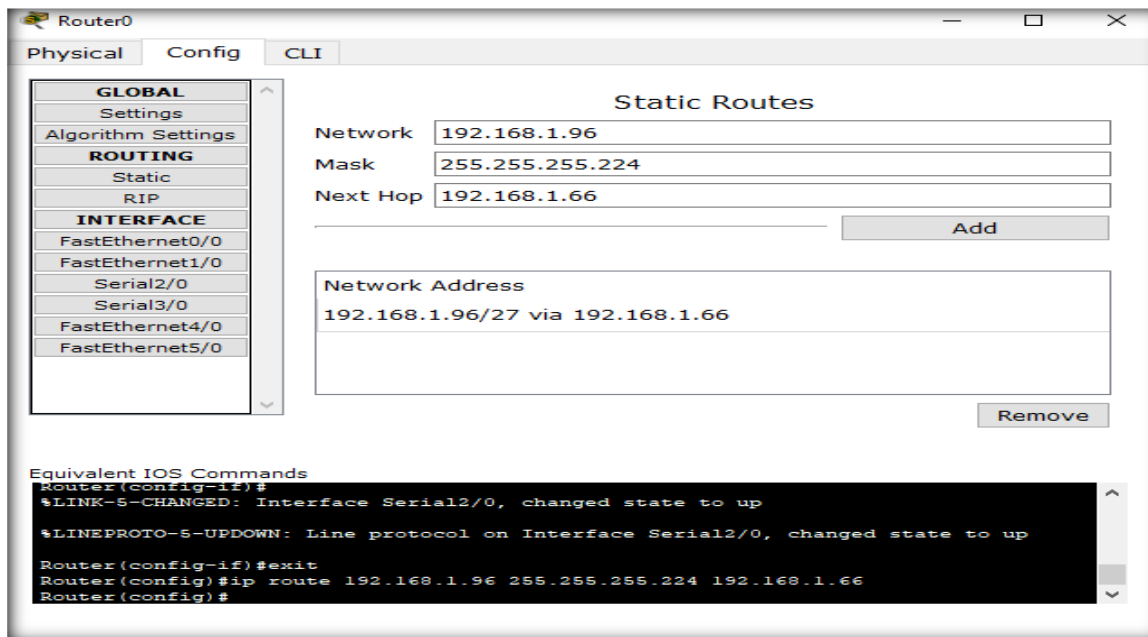
Now let start the pinging the interfaces from PC0. As we ping 192.168.1.33 and 192.168.1.65, we got the reply because these interfaces are directly connected to Router R0.



*Fig-17: Ping result of before routing is applied*

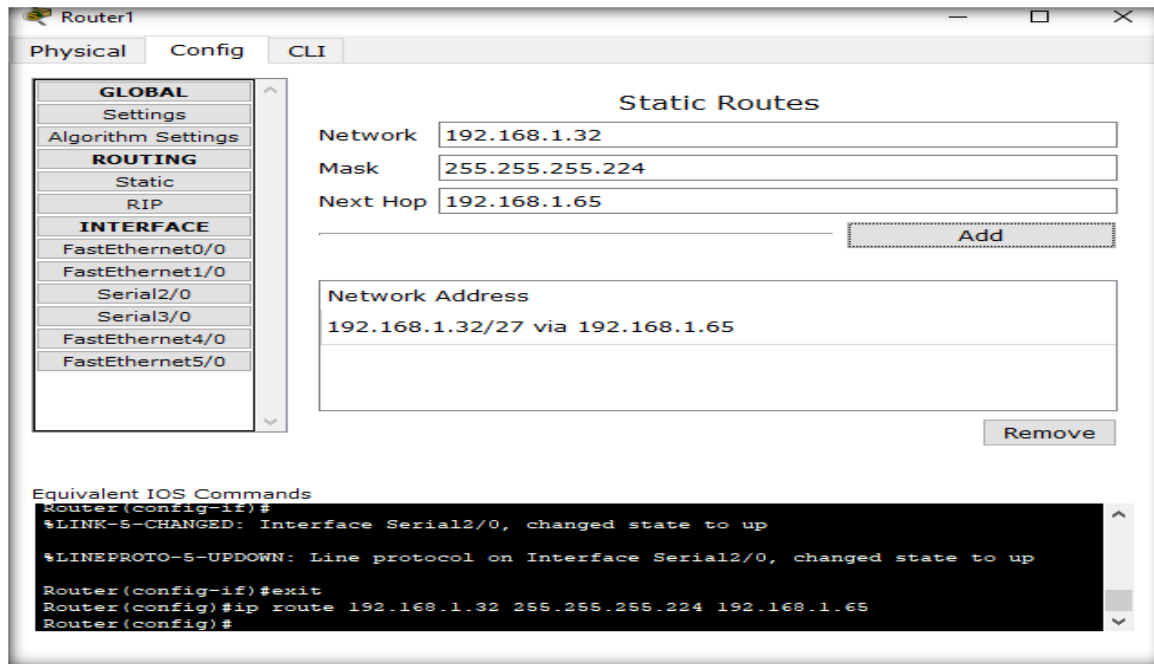
But when we ping 192.168.1.66, we got the Timed out because these interfaces are not directly connected to Router R1 as shown in figure 17.

**Therefore, we have to add static route in Router R0.**



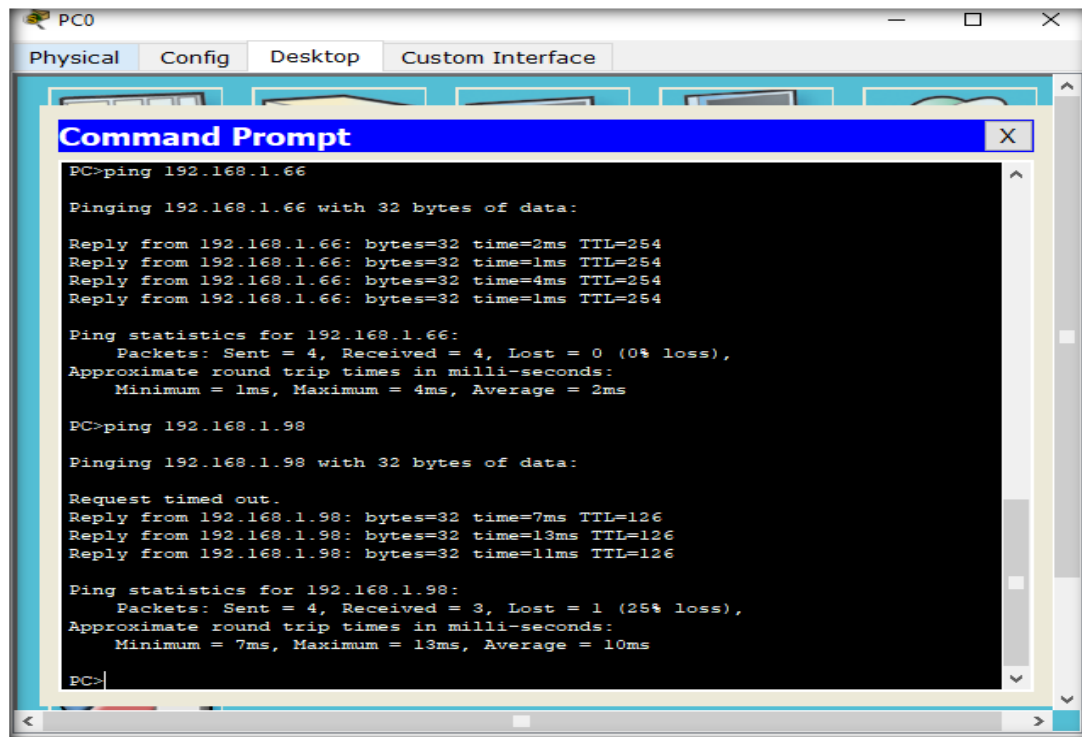
*Fig-18: Applying Static Routing on Router 0*

**Therefore, we have to add static route in Router R1.**



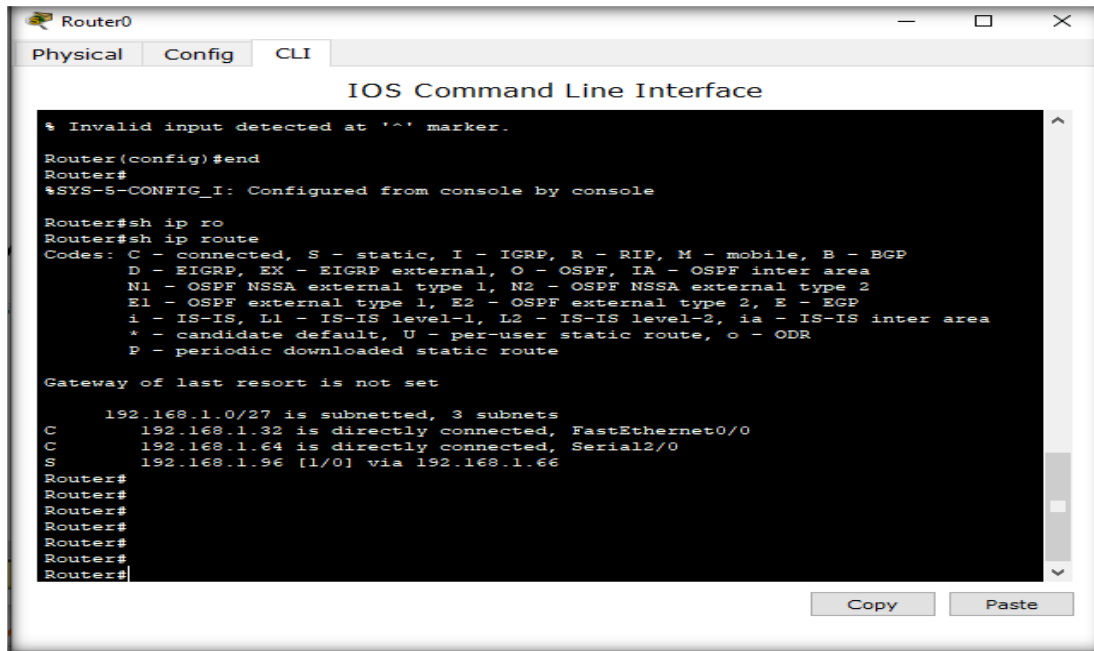
*Fig-19: Applying Static Routing on Router 1*

As you can see that we got the reply after adding the static route in Routers R0 & R1



*Fig-20: Ping is successful after static routing is applied*

Now using show ip route command we can see all the details of routing table saved in R0.



```
Router0
Physical Config CLI
IOS Command Line Interface

% Invalid input detected at '^' marker.

Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#sh ip ro
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      192.168.1.0/27 is subnetted, 3 subnets
C       192.168.1.32 is directly connected, FastEthernet0/0
C       192.168.1.64 is directly connected, Serial12/0
S       192.168.1.96 [1/0] via 192.168.1.66
Router#
Router#
Router#
Router#
Router#
Router#
Router#
```

*Fig-21: IP routes detail of router R0*

## Lab Exercise SUBNETTING

NOTE: In this assignment, your student ID will be used as a reference. For instance, if your ID is 20k-1234, then Id A = 1, Id B = 2, Id C = 3, and Id D = 4. In case any value in your ID is 0, you should consider it as 1.

Your submission will be in two parts, one document and one packet tracer file.

**Task-01** You are given an IP address pool (191.10.2.0 / 24) for your organization.

- I. Create networks (subnetworks),
- II. identify all network and broadcast addresses,
- III. host ranges and unused IP addresses.

There are 4 departments with the following number of hosts:

- I. Marketing: (6 x Id A) hosts
- II. Sales: (4 x Id B) hosts
- III. HR: (2 x Id C) host
- IV. IT: 8 hosts

**Task-02** Let consider an example of subnetting for FAST NUCES. There are 3 departments i.e. CS, EE and BBA. You have to perform subnetting for the allocation of the given requirement

90 PCs for CS  
50 PCs for SE  
20 PCs for AI

The network address for the given scenario is 196.168.10.0/24. Implement it on Cisco Packet Tracer.

