NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE

Computer Networks Lab (CL3001)

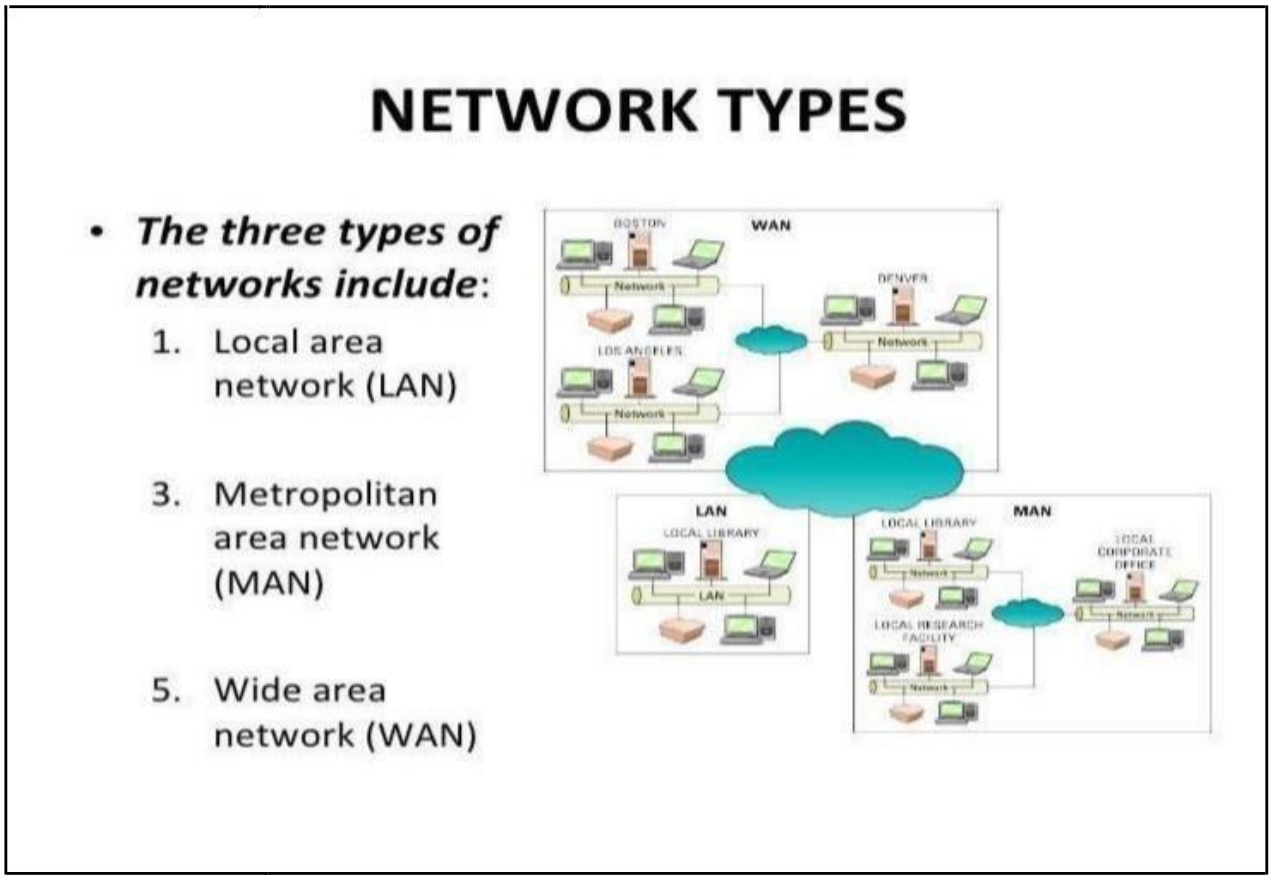
Lab Session 01

To get started with the lab activities, some basic terms to be familiarized with:

Network: **a group or system of interconnected people or things.**

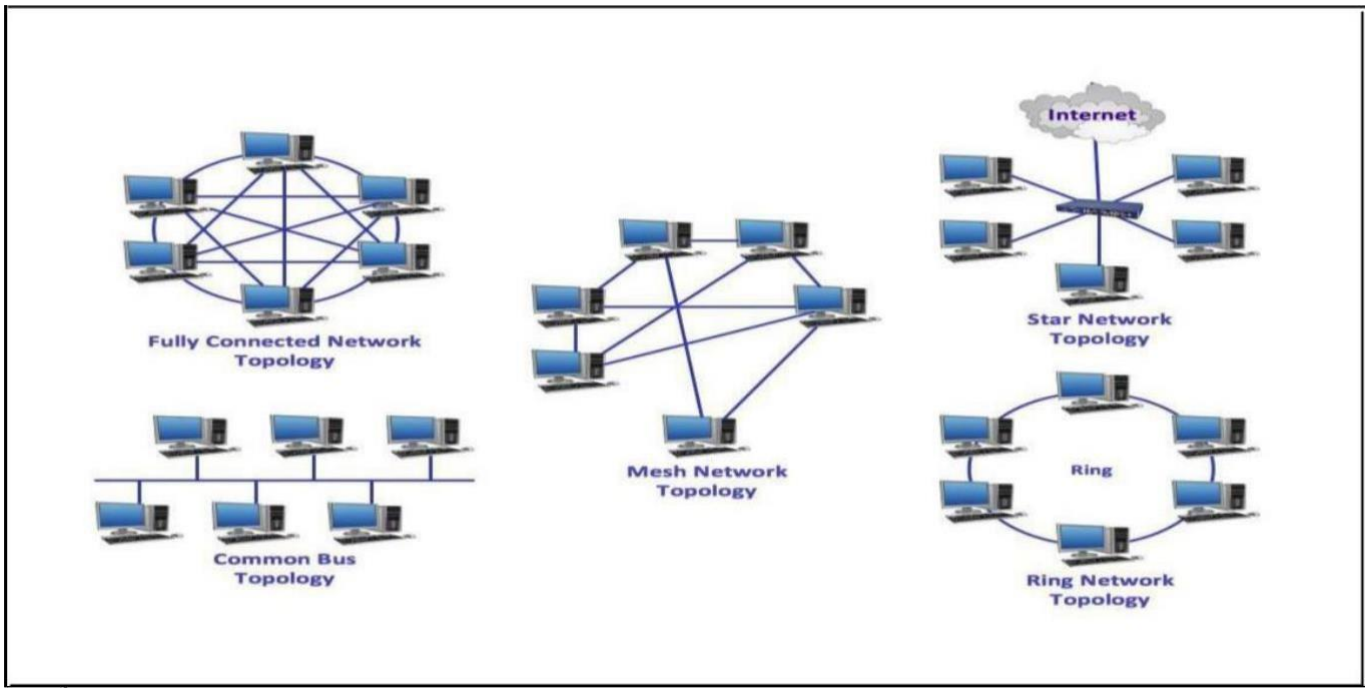
Computer Network: **A computer network or data network is a telecommunications network which allows nodes to share resources. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media.**

Types of Network: **Some of the different networks based on size are LAN, MAN, WAN.**

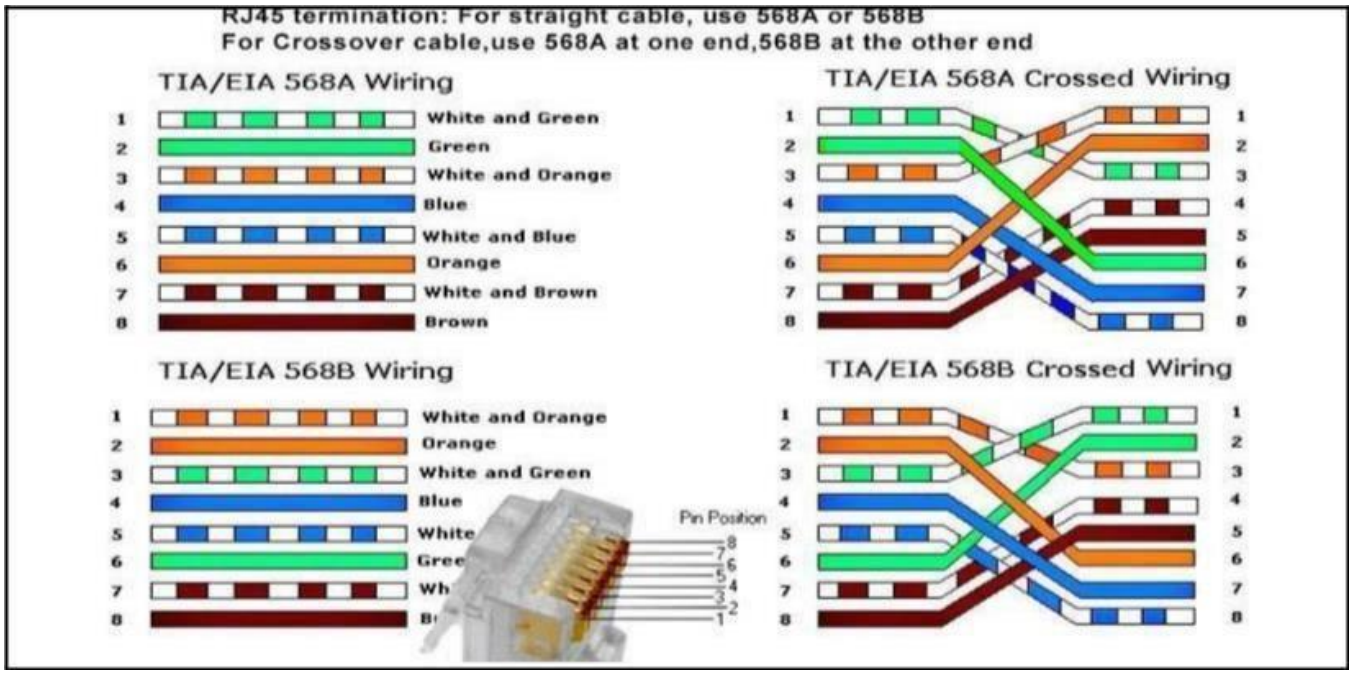


Host: **computer to be connected to a network.**

Topology: **Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted physically or logically. The basic examples of network topologies used in local area networks include bus, ring, star, and tree and mesh topologies as shown below.**



RJ45 Connector: **An 8-pin/8-position plug or jack is commonly used to connect computers onto Ethernet-based local area networks (LAN). Two wiring schemes–T568A and T568B–are used to terminate the twisted-pair cable onto the connector interface as shown below.**

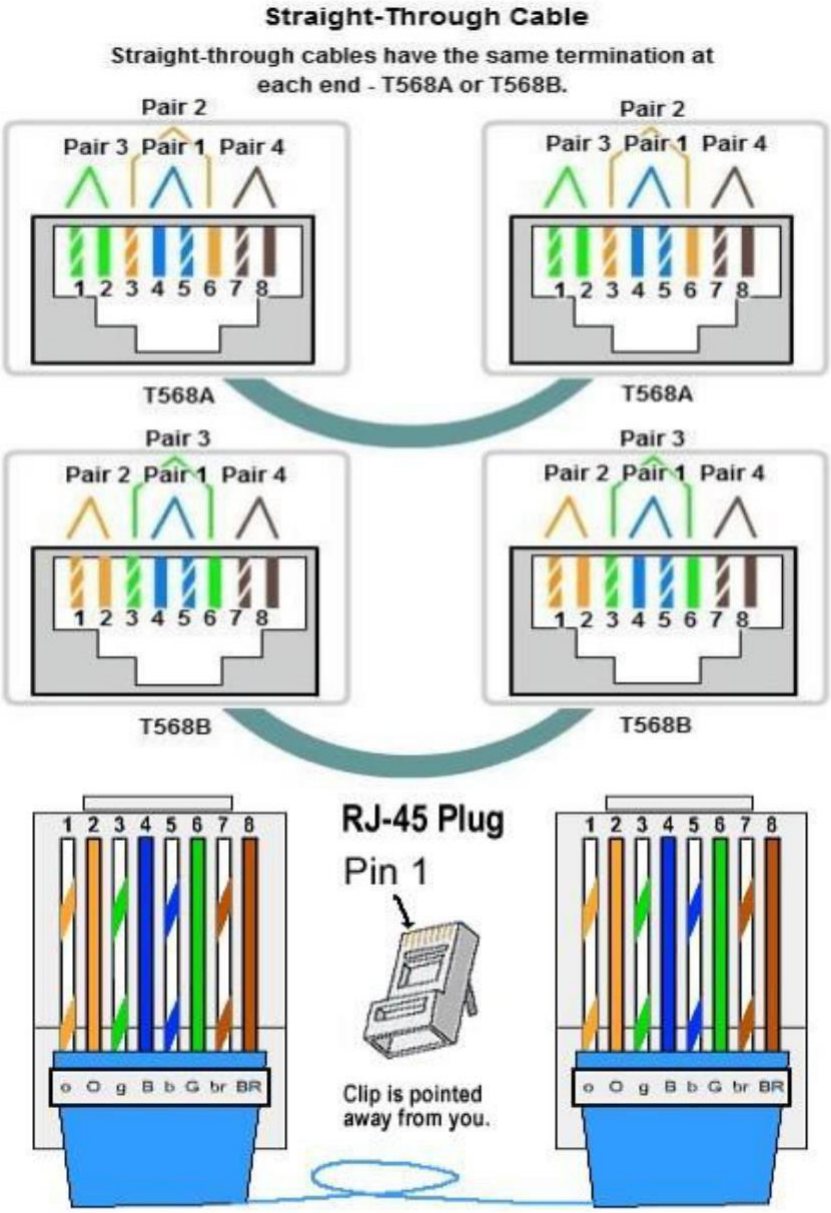


Straight cable:

You usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:

1) **Connect a computer to a switch/hub's normal port.**
2) **Connect a computer to a cable/DSL modem's LAN port.**
3) **Connect a router's WAN port to a cable/DSL modem's LAN port.**
4) **Connect a router's LAN port to a switch/hub's uplink port (normally used for expanding network).**
5) **Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.**

If you need to check how straight cable looks like, it's easy. Both sides (side A and side B) of cable have wire arrangement with same color

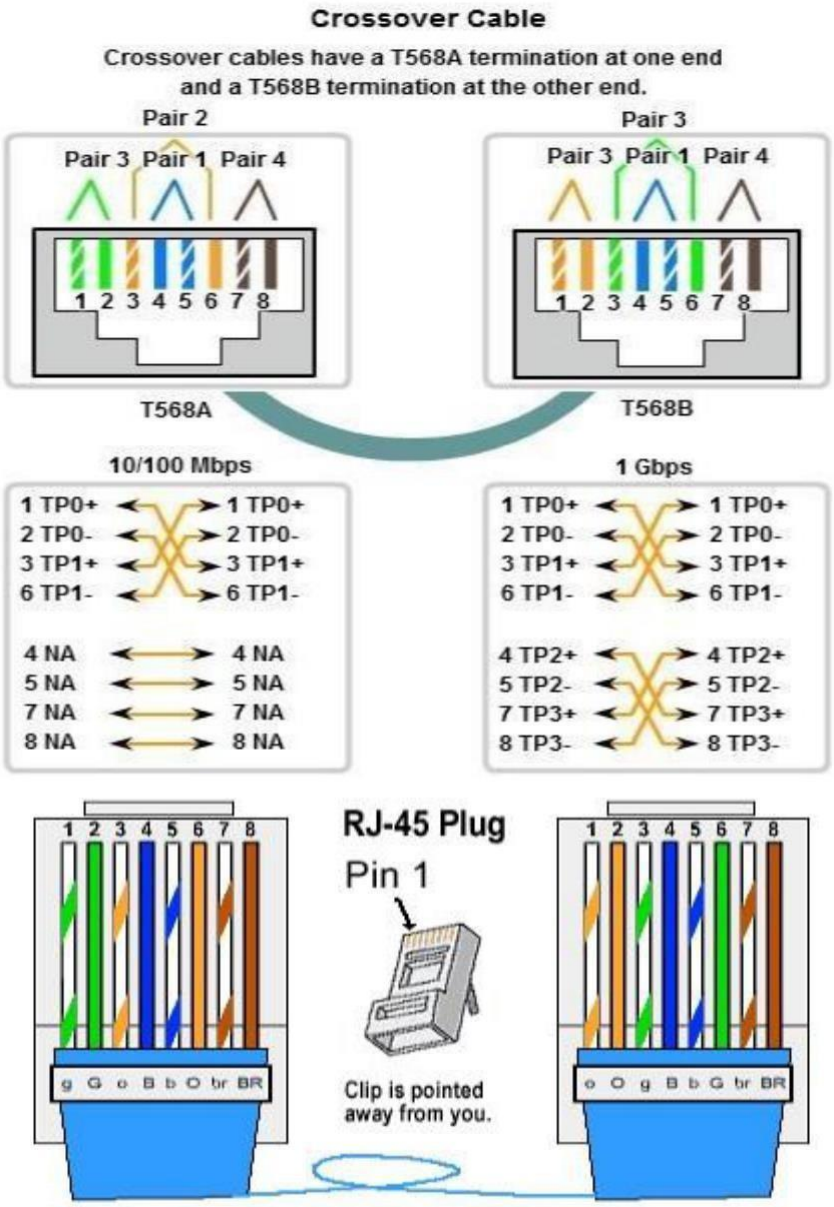


Crossover Cable:

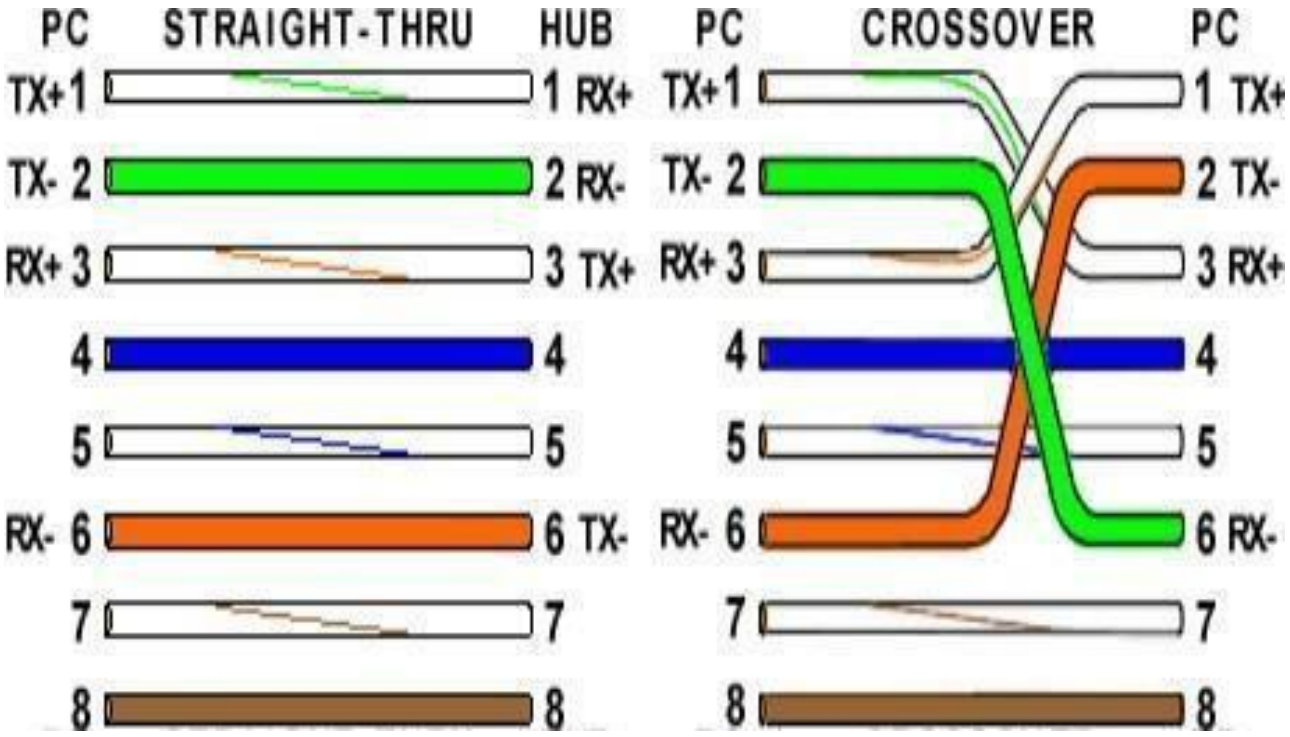
Sometimes you will use crossover cable, it's usually used to connect same type of devices. A crossover cable can be used to:

1) **Connect 2 computers directly.**
2) **Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)**
3) **Connect 2 switches/hubs by using normal port in both switches/hubs.**

In you need to check how crossover cable looks like; both sides (side A and side B) of cable have wire arrangement with following different color.



Note: If there is auto MDI/MDI-X feature support on the switch, hub, network card or other network devices, you don't have to use crossover cable in the situation which is mentioned above. This is because crossover function would be enabled automatically when it's needed.



NIC: Network Interface Card. The hardware interface from a host to the network.

MAC: Medium Access Control is a six hexit number that uniquely defines the NIC in the entire world. For example: 00:C0:9F:9B:D5:46

Hub: a hub is the most basic networking device that connects multiple computers or other network devices together. Unlike a network switch or router, a network hub has no routing tables or intelligence on where to send information and broadcasts all network data across each connection.

Switch: is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

Router: A device that decides where a packet should be sent in order to get to a destination outside a network. Routers range from simple gateways between your home PC and backbone routers of the Internet proper.

IP address: All hosts and routers have an IP address consisting of four decimal numbers. For example: 192.168.0.1 and 131.170.40.33

Port address: every host has 65,535 ports each of which can be connected to a specific application that sends and receives data packets from the network.

Gateway address: every host needs to know the address of the router which connects a network to other networks and the Internet.

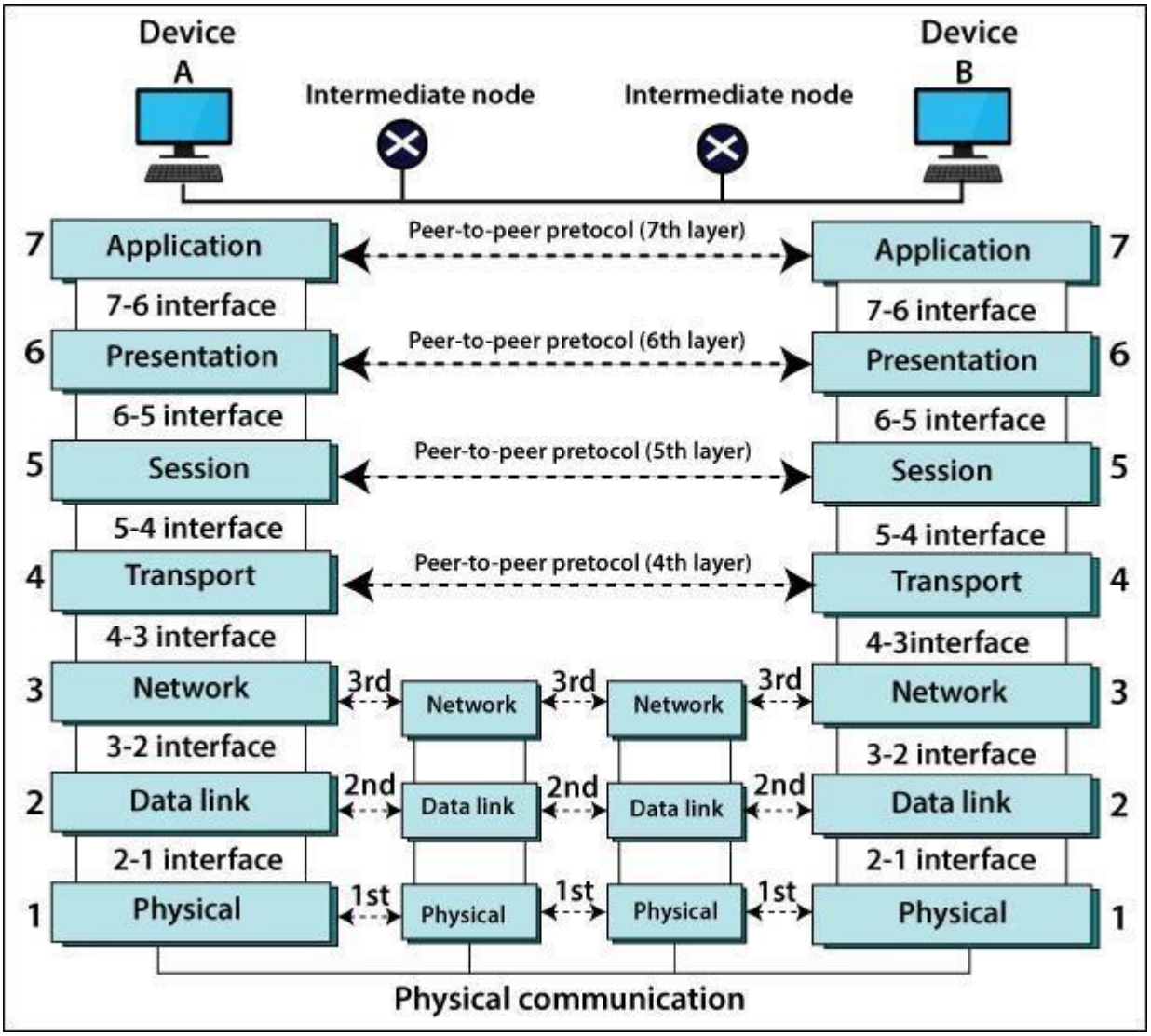
Domain name: hosts may have a domain name which maps onto an IP address. For example, www.google.com is mapped to IP address 66.102.7.104.

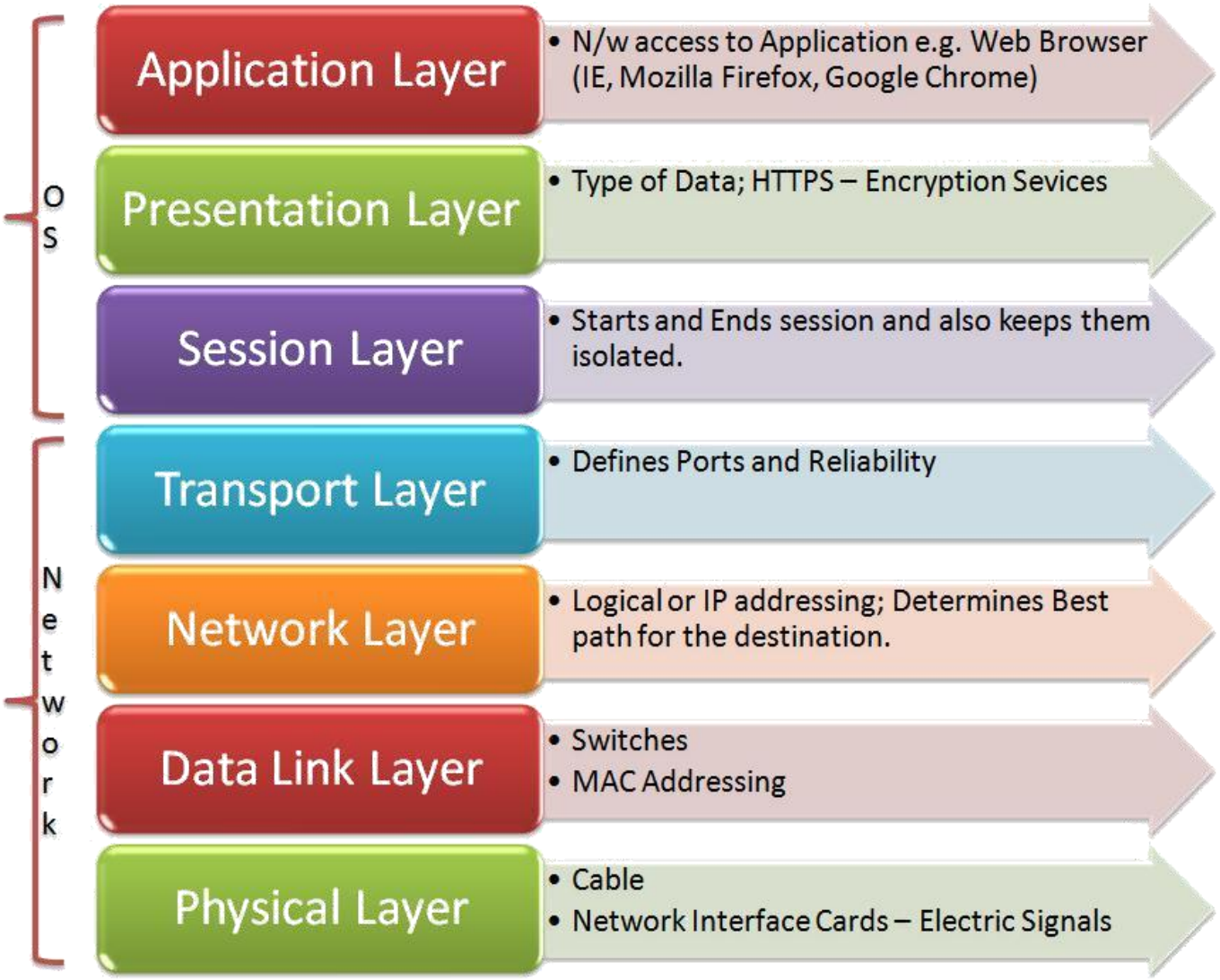
DNS Server: Domain Name System Server. Every host needs access to a DNS server so it can convert between IP address and domain name.

DHCP: Dynamic Host Configuration Protocol. A DHCP can give a host a unique IP address whenever the host restarts thus saving IP addresses. A DNS address is also provided.

OSI model:

To define the OSI model in one sentence: the OSI model is a concept-based model that defines, and sets standards for, the way in which a computing or telecommunication system functions. The goal of the OSI model is to achieve interoperability, through the use of standards, amongst a diverse set of communications. A Layer-Based System. There are seven distinct layers in the OSI model. They are:




OS
Application Layer
• N/w access to Application e.g. Web Browser (IE, Mozilla Firefox, Google Chrome)
Presentation Layer
• Type of Data; HTTPS – Encryption Sevices
Session Layer
• Starts and Ends session and also keeps them isolated.
Network
Transport Layer
• Defines Ports and Reliability
Network Layer
• Logical or IP addressing; Determines Best path for the destination.
Data Link Layer
• Switches
• MAC Addressing
Physical Layer
• Cable
• Network Interface Cards – Electric Signals

Network Command

OBJECTIVES

1. **To learn how to use Windows/Linux networking commands.**
2. **To test networking commands.**
3. **To solve networking problems using networking commands.**

INTRODUCTION

Most computers will be running Linux or MS Windows operating systems (OS).

LINUX is an excellent vehicle to understand and play with networks for several reasons:

Free and open source. Open source lessens the likelihood of deliberate security weaknesses.
Dominates the web server market and it is the basis of many networking boxes such as routers.
More powerful command line than Windows thus making script file operations more powerful and flexible.

WINDOWS:

Dominates the desktop market.
More users are familiar with Windows. (95% of desktop PCs run on Windows)
Has GUI which provides easier usage. However, recent KDE and GNOME desktops under Linux have been shown to be equivalently easy to use.

Notes – Every engineer with networking knowledge should be familiar with both OS.

In LINUX:

There are a number of simple commands that can be used to examine, debug and play with a network. To see all, use the manual pages (eg man ping) of the info pages (info ping).

ROOT PRIVILEGES – many commands require root privileges, or the programs reside in paths that root knows about but not users. It may be easier to log onto Linux as a user and open a root terminal.

In Windows:

Windows has a number of command line programs and GUI programs that can be used to view and alter network configuration. To see all, type hh ntcmds.chm in your terminal window, and to see all options for a command line, type –h, /?, -help, or ?

Some common commands used in Linux and Windows:

Linux Command	Windows Command	Usage / Effect
ifconfig	ipconfig	to find ip address of the computer
hostname	hostname	to display host name
nmap	nmap	To scan what hosts are available on a network and what ports they have open.
nslookup	nslookup	to list variety of info about DNS and the computers that have joined the domain
ping	ping	to check if a host can be accessed (by IP or name)
traceroute	tracert	to trace route from a host through internet router to a destination. Useful to discover why a network cannot get access to internet, and internet routing problems.
netstat	netstat	to print status of network ports, routing tables and more

TASKS

Use the appropriate networking commands to solve these networking problems.

1. **Find the IP address of the computer you are currently using.**

   Command: _____

   IP address: _____

2. **Find the IP address of the computer you are currently using, plus MAC address, plus whether DHCP is turned on.**

   Command: _____

   Answer: _____

3. **Display the host name of the computer.**

   Command: _____

   Hostname: _____

4. **Check for basic IP connectivity between two computers by name and IP address. How can basic IP connectivity be checked? What are the reasons why there is no connectivity?**

   Command: _____

   Reason: _____

5. **Show the MAC address of the host.**

   Command: _____

   MAC address: _____

6. **Show what shared resources are available on the host.**

   Command: _____

   Answer: _____

7. **Find out which ports on your host are connected to applications. Connect the browser to some external web page before running the appropriate command.**

   Command: _____

   Answer: _____

8. **Find all other hosts available on the network.**

   Command: _____

   Answer: _____

9. **Show the address of the gateway.**

   Command: _____

   Answer: _____

10. **Find the path of routers to www.google.com.What is its IP address? How many hops involved in the path?**

    Command: _____

    Answer: _____

11. **A ping to 192.168.0.2 works but a ping to the machine's name "blue machine" fails. What could be wrong?**

Reason:

_____

_____

12. Which type of cable will you use to connect in a normal home installation? Give reasons.

Answer:

_____

_____

13. Can you connect a Switch to another Switch or a router to a PC using a straight-through cable? Explain your answer.

Answer:

_____

_____

14. Write a brief report on your home network or any organizational network including topology, 1 page max).

Answer:

_____

_____

15. Find the path of routers to www.yahoo.com.my. What is its IP address? How many hops involved in the path?

Answer:

_____

_____

NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 04

Objective:

- Implementation & understanding of HTTP/HTTPS.
- Network traffic analysis of HTTP/S protocol headers, cookies using Wireshark

HTTP/HTTPS

1. Hypertext Transfer Protocol (HTTP):

Hypertext Transfer Protocol (HTTP) is a protocol used in networking. When you type any web address in your web browser, your browser acts as a client, and the computer having the requested information acts as a server. When client requests for any information from the server, it uses HTTP protocol to do so. The server responds back to the client after the request completes. The response comes in the form of web page which you see just after typing the web address and press "Enter".

2. Hypertext Transfer Protocol Secure (HTTPS):

Hypertext Transfer Protocol Secure (HTTPS) is a combination of two different protocols. It is more secure way to access the web. It is combination of Hypertext Transfer Protocol (HTTPS) and SSL/TLS protocol. It is more secure way to sending request to server from a client, also the communication is purely encrypted which means no one can know what you are looking for. This kind of communication is used for accessing those websites where security is required. Banking websites, payment gateway, emails (Gmail offers HTTPS by default in Chrome browser), and corporate sector websites are some great examples where HTTPS protocols are used.

For HTTPS connection, public key trusted and signed certificate is required for the server. Thesecertificates come either free or it costs few dollars depends on the signing authority. There is one other method for distributing certificates. Site admin creates certificates and loads in the browser of users. Now when user requests information to the web server, his identity can be verified easily.

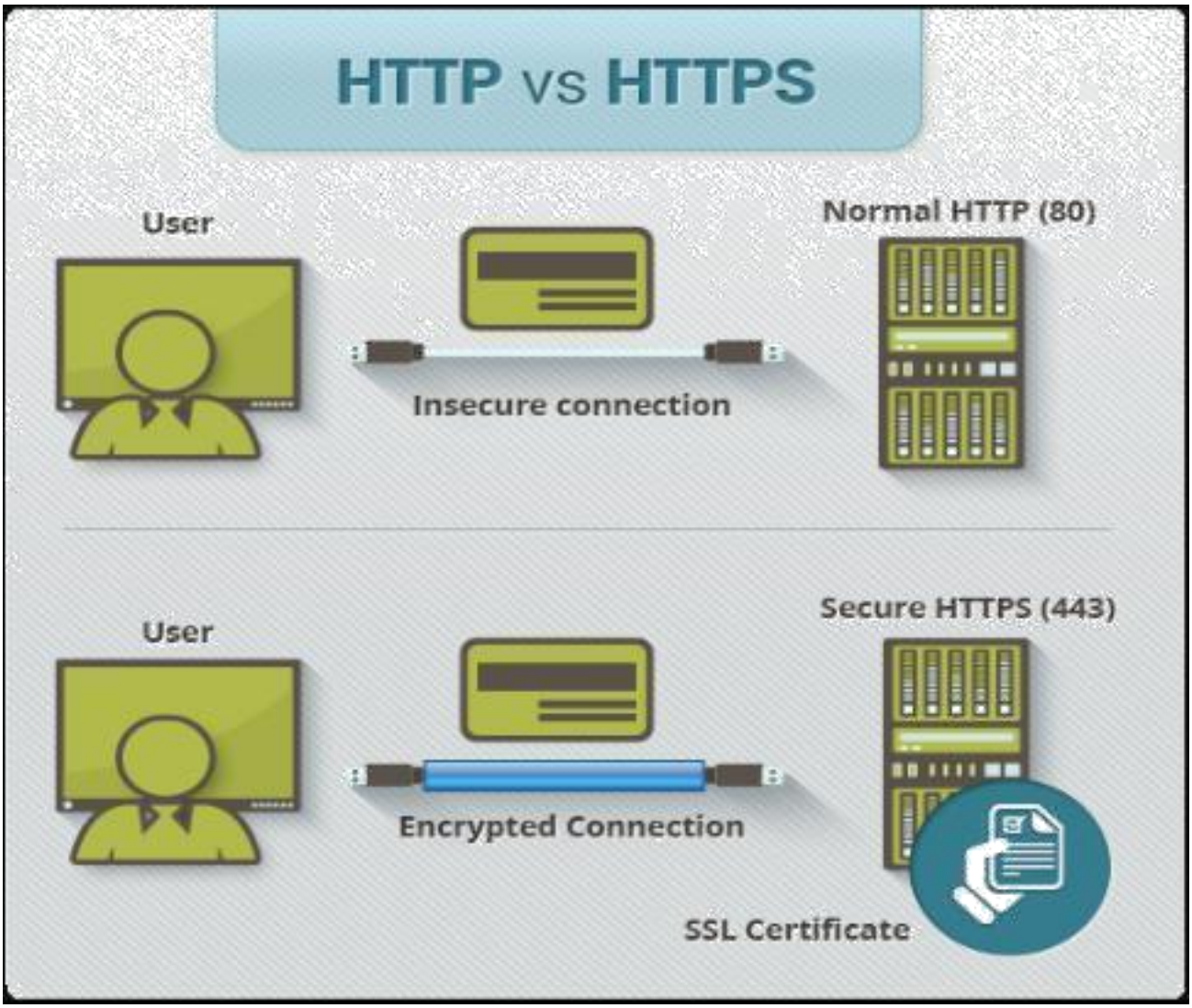


Fig-1: HTTP & HTTPS difference

3. HTTP & HTTPS Differences:

Here are some major difference between HTTP & HTTPS

HTTP	HTTPS
URL begins with "http://"	URL begins with "https://"
It uses port 80 for communication	It uses port 443 for communication
Unsecured	Secured
Operates at Application Layer	Operates at Transport Layer
No encryption	Encryption is present
No certificates required	Certificates required

4a. Client Error:

The 4xx class of status code is intended for cases in which the client seems to have erred. Exceptwhen responding to a HEAD request, the server should include an entity containing an explanation of the error situation, and whether it is a temporary or permanent condition. These status codes are applicable to any request method. User agents should display any included entity to the user.

400 Bad Request:

The server cannot or will not process the request due to something that is perceived tobe a client error (e.g., malformed request syntax, invalid request message framing, or deceptive request routing).

401 Unauthorized (RFC 7235):

Similar to 403 Forbidden, but specifically for use when authentication is required and hasfailed or has not yet been provided. The response must include a WWW -Authenticate header field containing a challenge applicable to the requested resource. See Basic accessauthentication and Digest access authentication.

403 Forbidden:

The request was a valid request, but the server is refusing to respond to it. Unlike a 401 unauthorized response, authenticating will make no difference**.**

404 Not Found:

The requested resource could not be found but may be available again in the future.Subsequent requests by the client are permissible.

408 Request Timeout:

The server timed out waiting for the request. According to HTTP specifications: "The client did not produce a request within the time that the server was prepared to wait. Theclient MAY repeat the request without modifications at any later time."

4b. Server Error:

The server failed to fulfill an apparently valid request.

Response status codes beginning with the digit "5" indicate cases in which the server is aware that it has encountered an error or is otherwise incapable of performing the request. Except when responding to a HEAD request, the server should include an entity containing an explanation of the error situation, and indicate whether it is a temporary or permanent condition. Likewise, user agents should display any included entity to the user. These response codes are applicable to any request method.

500 Internal Server Error:

A generic error message, given when an unexpected condition was encountered andno more specific message is suitable.

501 Not Implemented:

The server either does not recognize the request method, or it lacks the ability to fulfil the request. Usually this implies future availability (e.g., a new feature of a web-service API).

502 Bad Gateway:

The server was acting as a gateway or proxy and received an invalid response from the upstream server.

503 Service Unavailable:

The server is currently unavailable (because it is overloaded or down for maintenance). Generally, this is a temporary state.

5. Implementation:

Design the given topology shown in figure 2. Assign IP address to PC using static through as done in pervious lab.

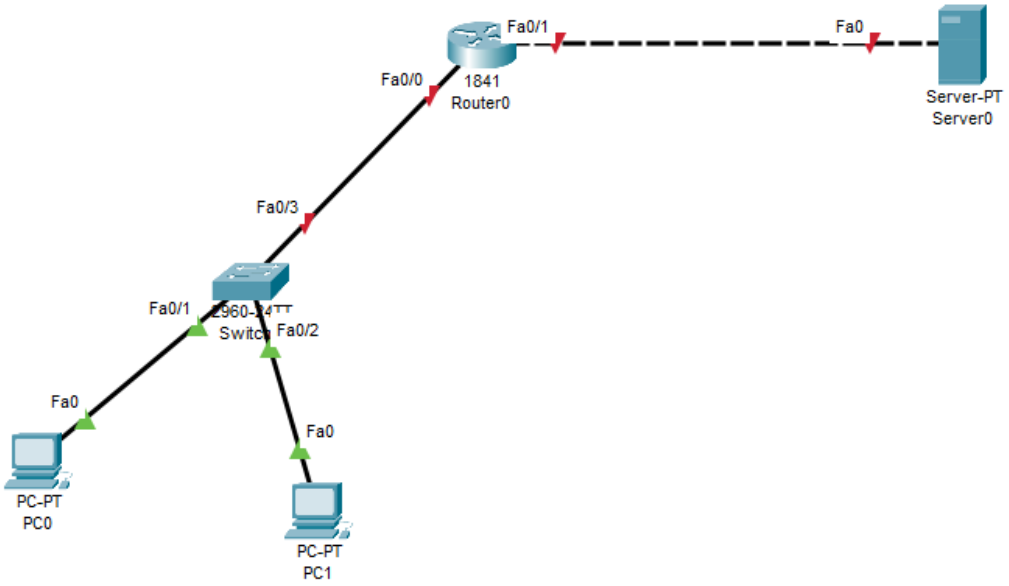


Fig-2: Lab 4 network topology

The above topology configured as “one server room”, “one IT room: and “Lab#01 environment having three systems”. On our server we have enabled web services as well as DNS services. Click on the web server, go to config --->services—HTTP
Here you can see HTTP & HTTPS services are on.

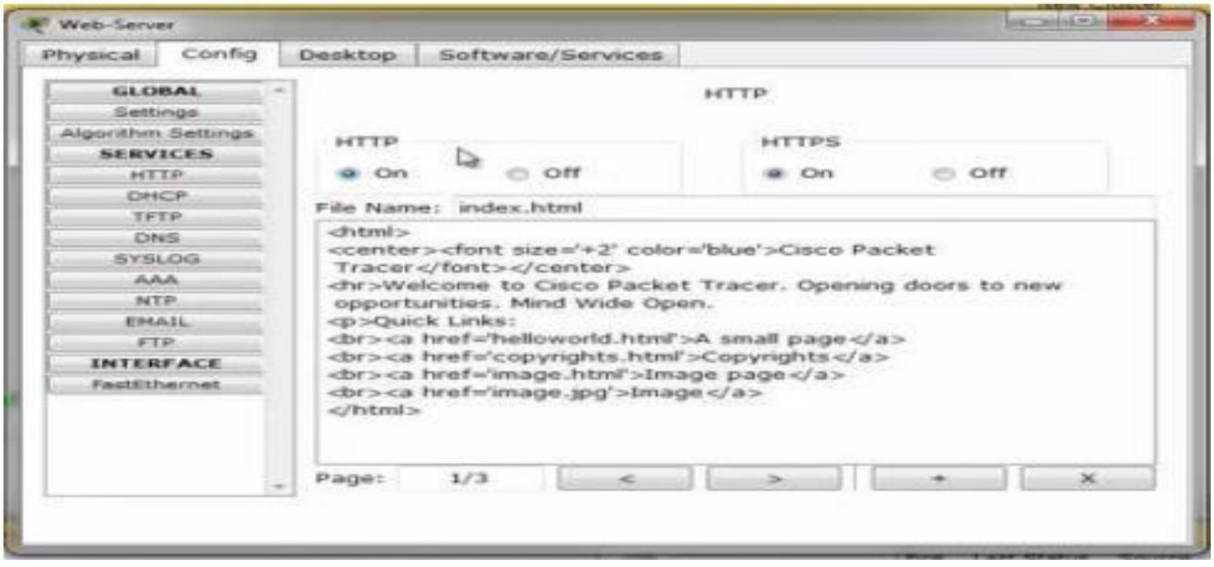


Fig-3: HTTP services on server interface in Packet Tracer

Now click on PC0 and go to Desktop -> Web Browser. Now type web-server IP which you have assign or the website name which you have store in the DNS server record.

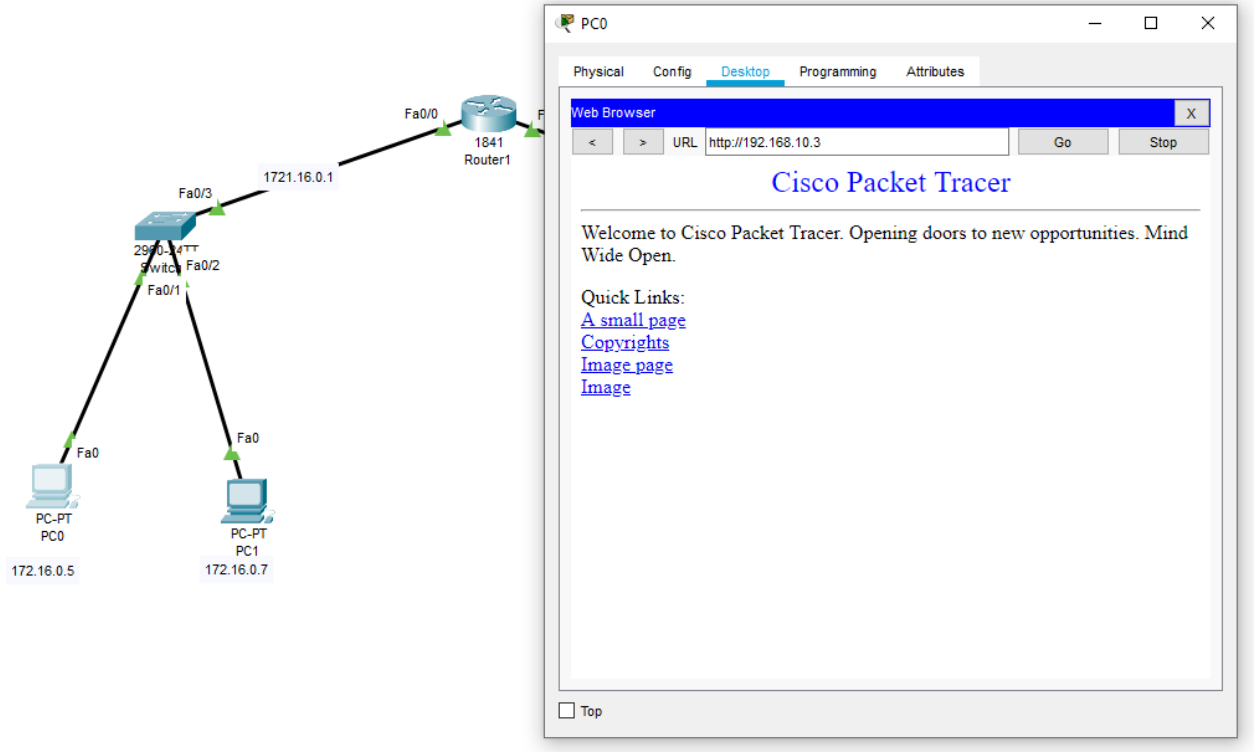


Fig-4: HTTP services on server interface in Packet Tracer

To note the http header format information, go to simulation mode edit filters and clickon http check box then click on capture/forward button.

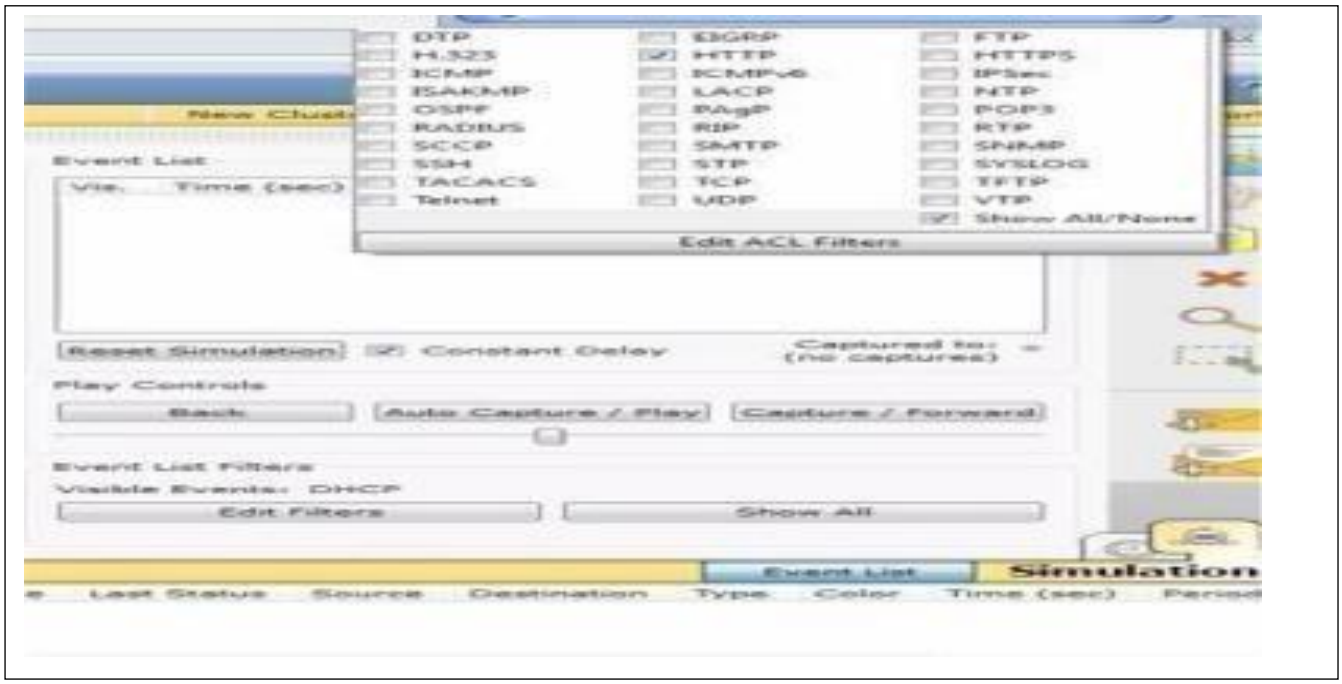


Fig-5: Packet Tracer Simulation Mode Interface

Now click on the http packet, you can note that the destination port is 80.

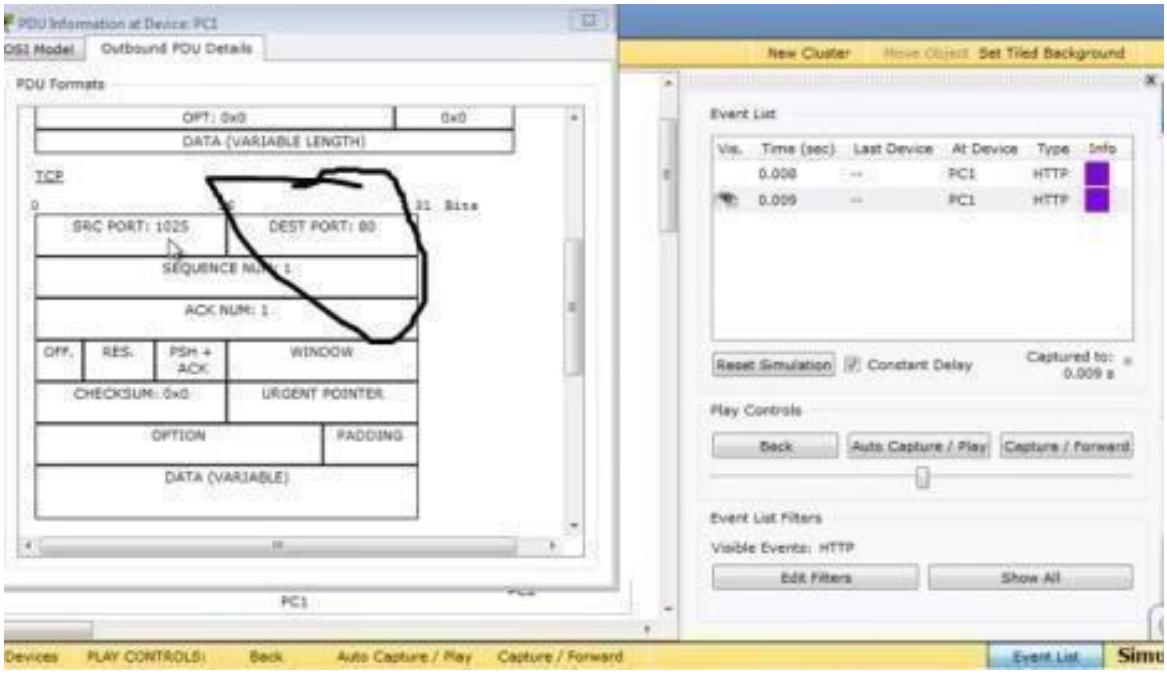


Fig-6: HTTP PDU in Packet Tracer

Now scroll the Outbound PDU Details, you can see the http protocol information.

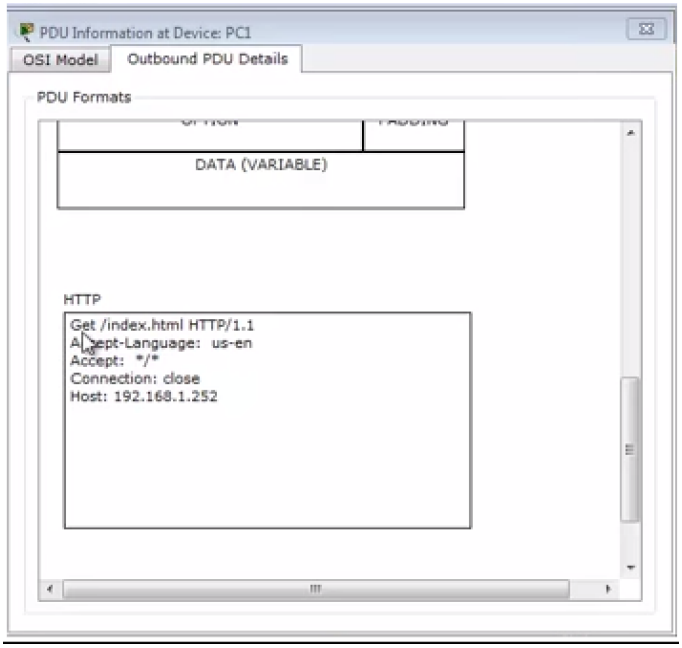


Fig-7: HTTP details in PDU

For HTTPS:

Now click on PC and go to Desktop---- >Web Browser. Now type web-server IP 192.168.1.252

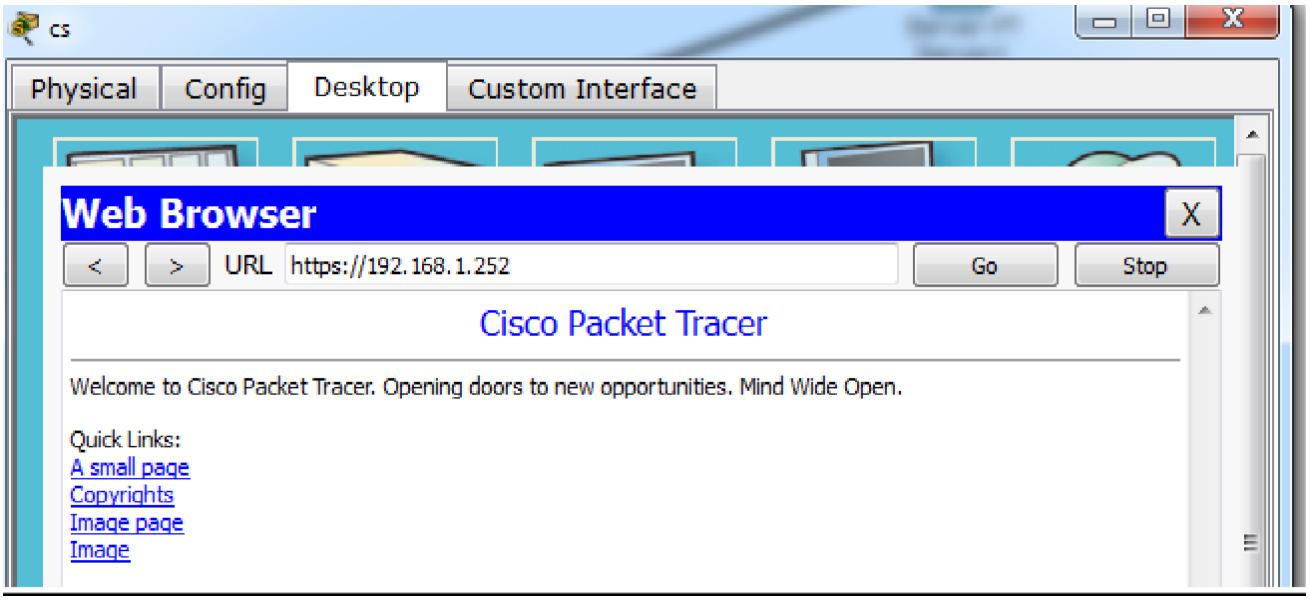


Fig-8: Web page using HTTPS

Now to note the https header format information go to simulation mode ----- > editfilters and click on https check box then click on capture/forward button.

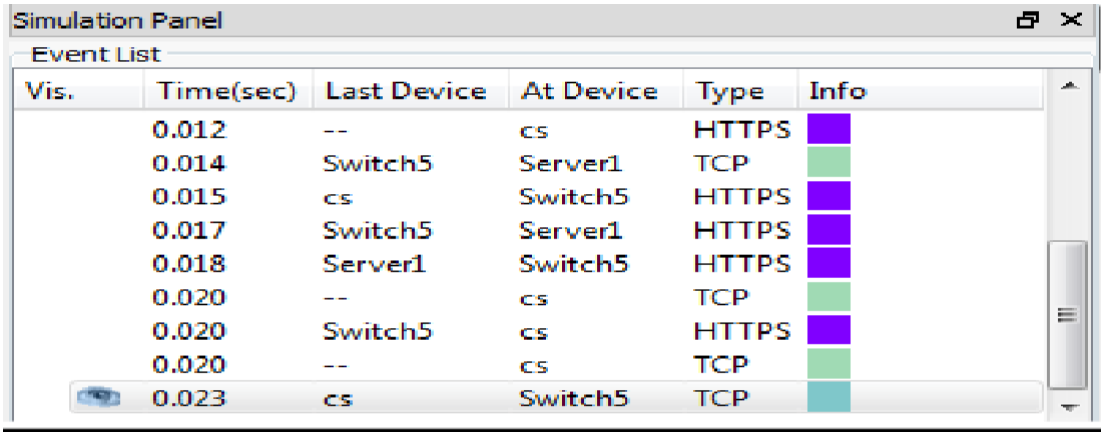


Fig-9: Packets flow in simulation

Now click on the https packet, you can note that the destination port is 443.

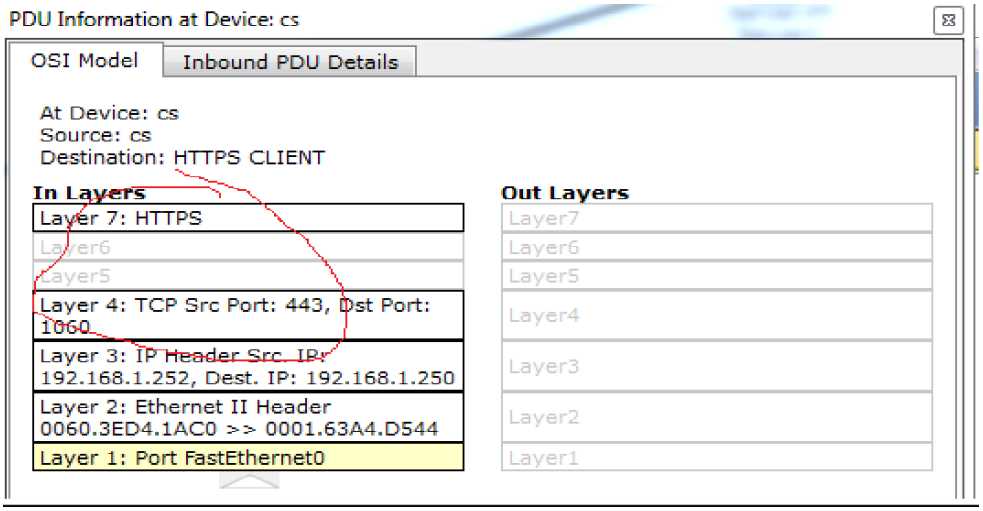


Fig-10: Packet information

Now scroll the Outbound PDU Details, you can see the https PDU.

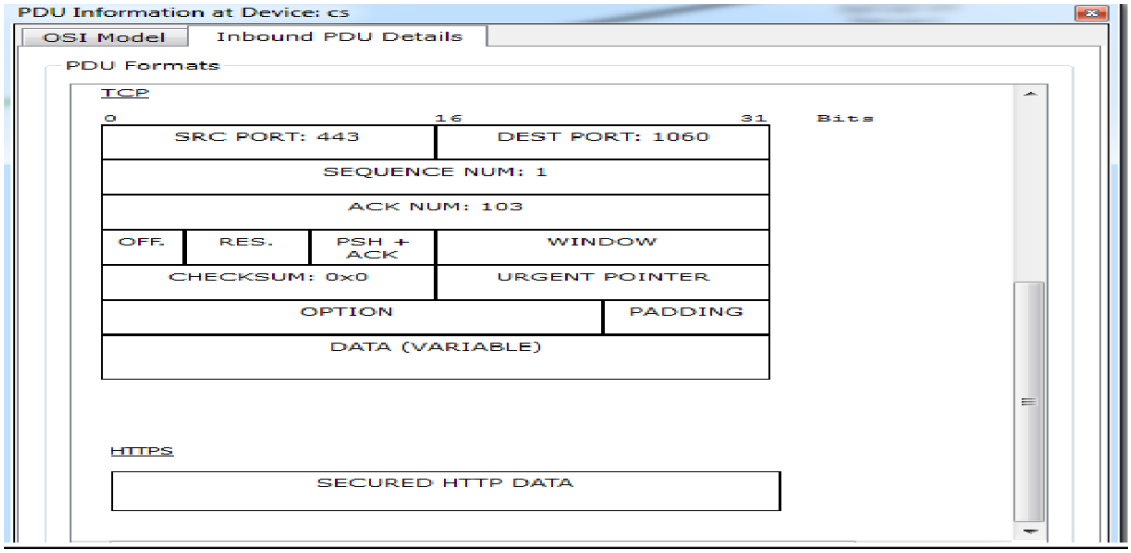


Fig-11: HTTPs PDU details

5. Lab Exercise:

Q1) In caching, what is the difference between the age header and expires?
Q2) What are the four groupings of HTTP headers?

What is Wireshark?

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Figure 12 Wireshark

Why we use Wireshark?

Wireshark has many uses, including **troubleshooting networks that have performance issues**. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

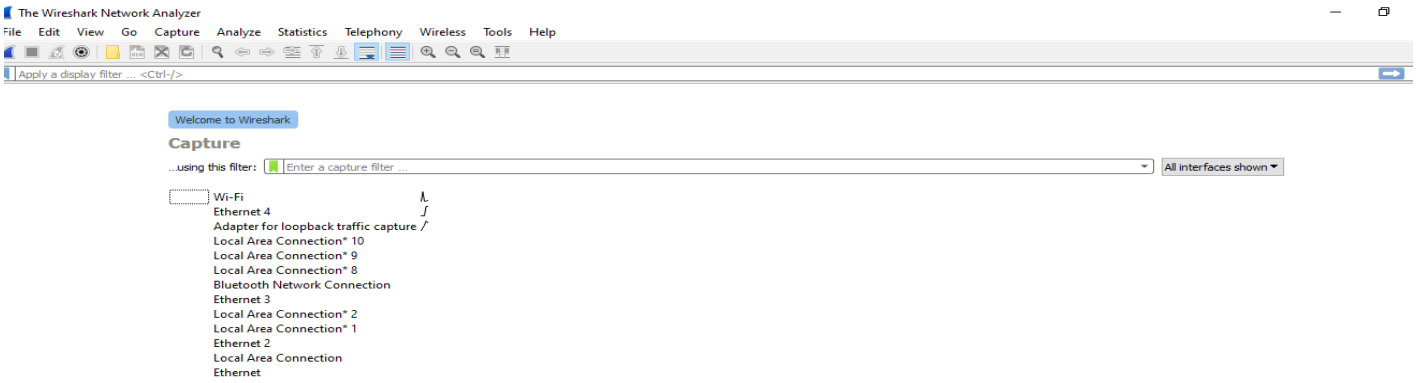


Figure 13 1Wireshark workspace

Open Wireshark

Figure 13 2 Wireshark logo

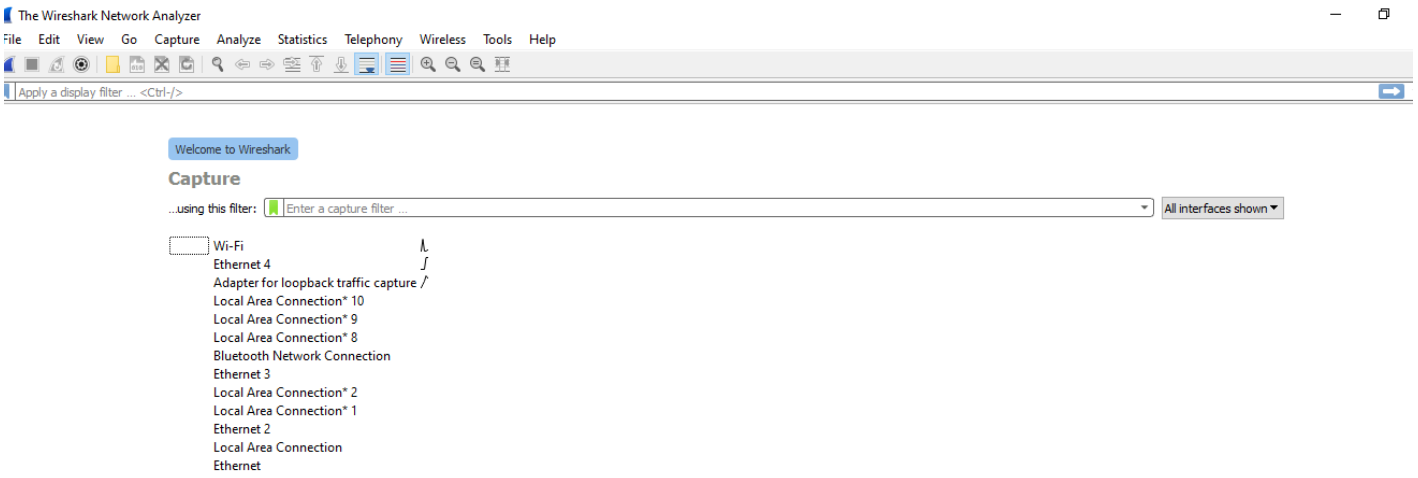


Figure 13 3 Select connected Network

Select the technology you used for packet analysis

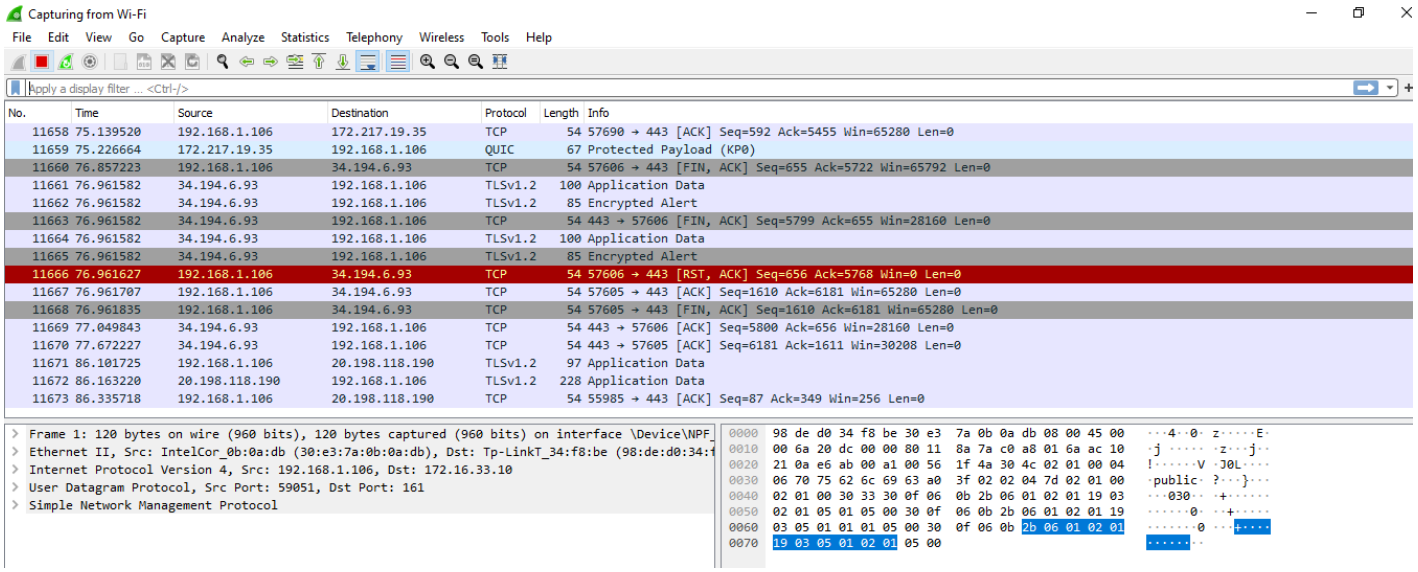


Figure 13 4 Use filter Http for observation

6. Lab Exercise:

TASKs

Goto website below:
http://testphp.vulnweb.com/login.php
Username: your name
Password: you roll number
Take Snapshot of each Step, and Submit in Docx file/pdf with one line answer, what you understand here?

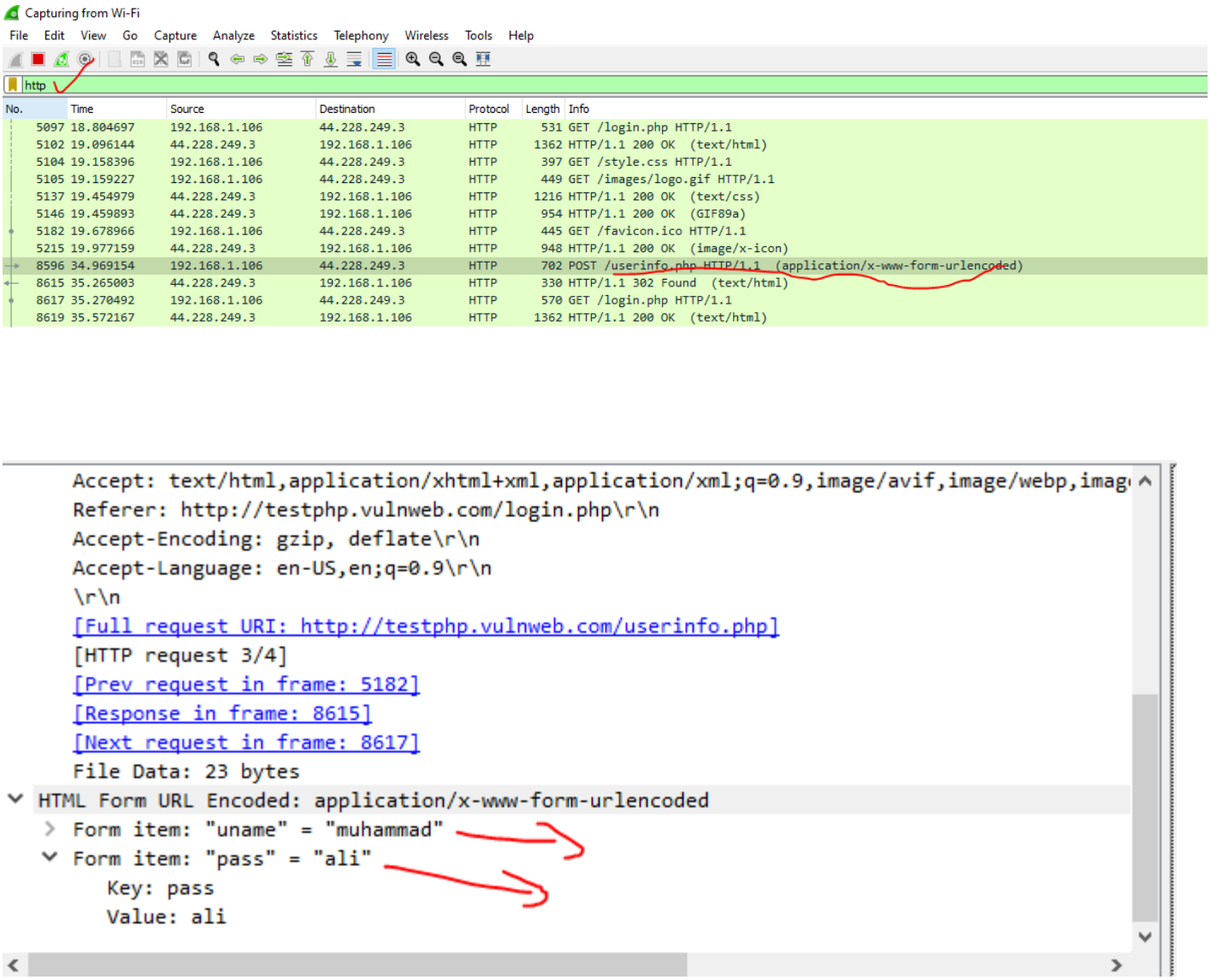


Figure 13 5find the username and password via Wireshark

7. Lab Exercise:

TASK

Follow the above step for HTTPS
Take Snapshot of each Step, and Submit in Docx file/pdf with one line answer, what you understand here?
Observe the difference between HTTP and HTTPS and answer in one line with proper snapshots?

Tasks:

1. Show the packet header format of ARP in Cisco Packet tracer.
2. Identify the differences between Switch and Hub.
3. **Take two PCs, connect them and assign them an ip addresses and check theirconnectivity with the help of PING command.**
4. Take two PCs, connect them with suitable wire and also describe the reason of selection of wire. Assign them IP addresses and check their connectivity by using PINGcommand. (Use Packet tracer for this task).
5. **What are the main command modes? Compare them. Test basic commands on your designed network?**
6. Design and configure the network given in Figure-1 and check the connectivity byPING command. Also describe the functionality of devices in given scenario.

Private Address Space	
Class A	10.0.0.0 to 10.255.255.255
Class B	172.16.0.0 to 172.31.255.255
Class C	192.168.0.0 to 192.168.255.255

NATIONAL UNIVERSITY OF COMPUTER & EMERGINGSCIENCE
Computer Network
Lab (CL3001) Lab

Session 05

Objective:

- Introduction to DNS & configuration of DNS in Cisco Packet Tracer
- Introduction to SMTP & FTP in Cisco Packet Tracer

DNS in Cisco Packet Tracer

1. Introduction to DNS:

The Domain Name System (DNS) is a hierarchical and distributed naming system for computers, services, and other resources in the Internet or other Internet Protocol (IP) networks. It associates various information with domain names assigned to each of the associated entities. Most prominently, it translates readily memorized domain names to the numerical IP addresses needed

for locating and identifying computer services and devices with the underlying network protocols.[1] The Domain Name System has been an essential component of the functionality of the Internet since 1985.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over sub domains to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database.
Some common DNS record types are:

a) A record:

The A record is one of the most commonly used record types in any DNS system. An A record is actually an address record, which means it maps a fully qualified domain name (FQDN) to an IP address. For example, an A record is used to point a domain name, such as "google.com", to the IP address of Google's hosting server, "74.125.224.147". This allows the end user to type in a human- readable domain, while the computer can continue working with numbers. The name in the A record is the host for your domain, and the domain name is automatically attached to your name.

b) CNAME record:

Canonical name records, or CNAME records, are often called alias records because they map an alias to the canonical name. When a name server finds a CNAME record, it replaces the name with the canonical name and looks up the new name. This allows pointing multiple systems to one IP without assigning anA record to each host name. It means that if you decide to change your IP address, you will only have to change one A record.

c) NS record:

An NS record identifies which DNS server is authoritative for a particular zone. The "NS" stands for "name server". NS records that do not exist on the apex of a domain are primarily used for splitting up the management of records on sub-domains.

d) SOA record:

The SOA or Start of Authority record for a domain stores information about the name of the server that supplies the data for the zone, the administrator of the zone and the current version of the data. It also provides information about the number of seconds a secondary name server should wait before checking for updates or before retrying a failed zone transfer.

Assigning IP to DNS server & PCs.

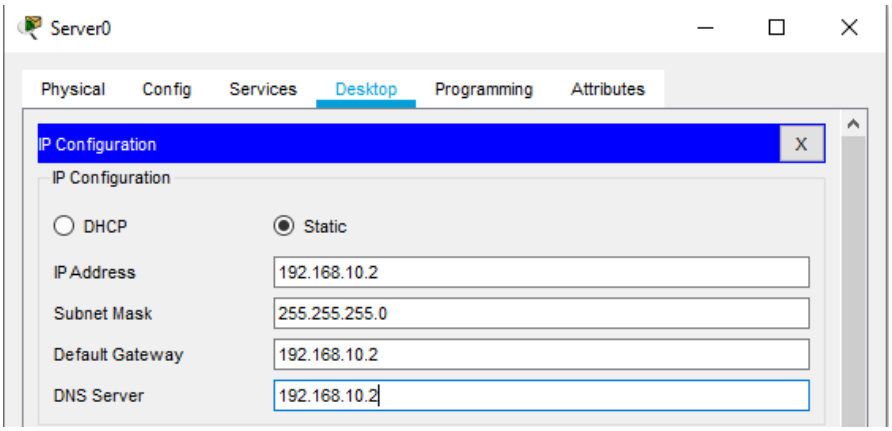


Fig-1: DNS server

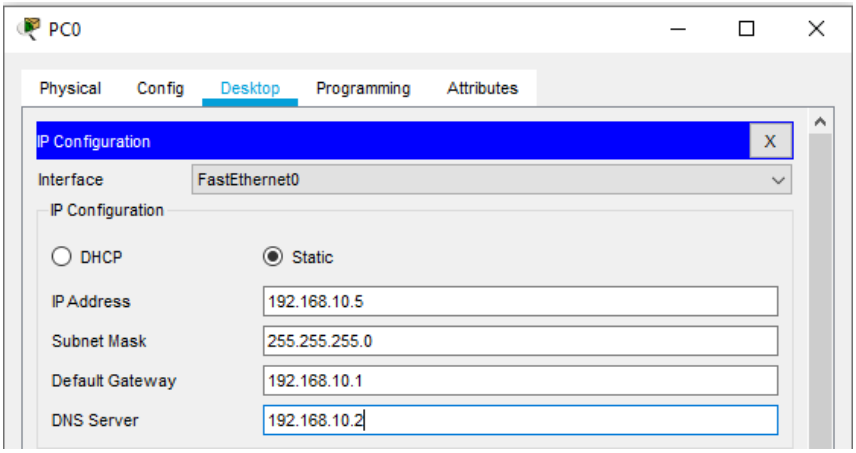


Fig-1: Provide IP to system through static IP

2. DNS Configuration & Simulation:

Now using the DNS service on DNS Server. Go to server services DNS.
First, we add A record. We assign the web server IP against our Domain name

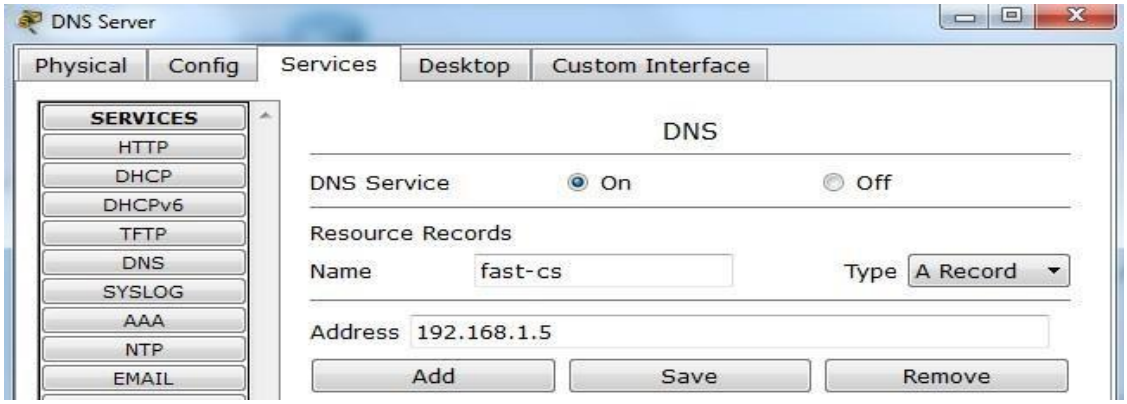


Fig-3: DNS server configuration adding a record

Now click on Add.

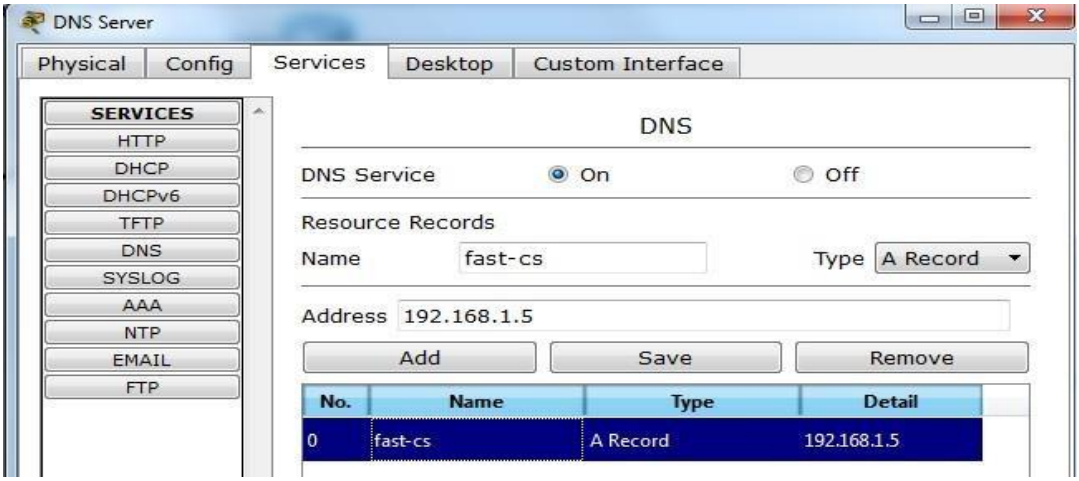


Fig-3: Record is added in DNS server

Now add Cname record.

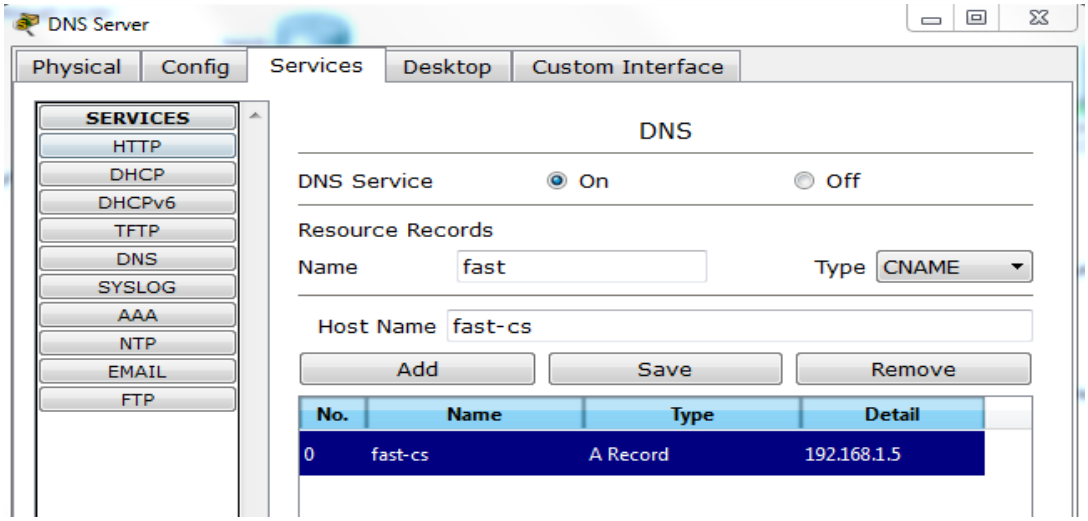


Fig-4: Adding CNAME record in DNS server

Now click on Add

Fig-5: CNAME record is added in DNS server

Now go to PC4 →Desktop →web browser → type fast-cs and see how DNS works.

Fig-6: Opening website

Start simulation.

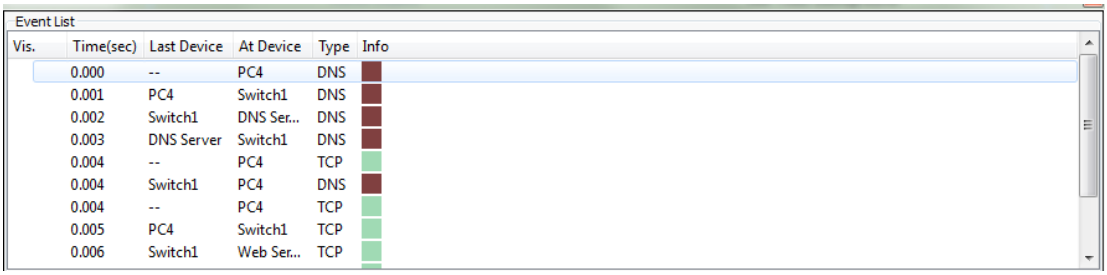


Fig-7: Packets exchange in DNS simulation

Click on DNS packet. See how DNS server resolved the name.

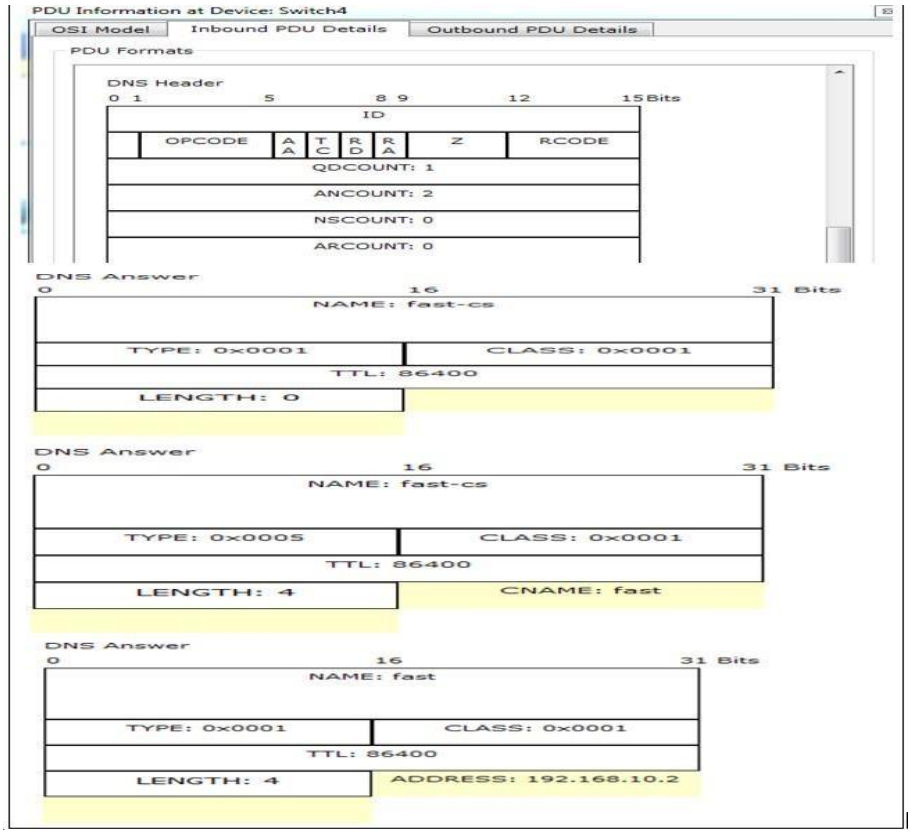


Fig-8: DNS header request & reply to resolve domain name

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 whatchanges will occur at each layer (use next and previous buttons to trace each layer content).

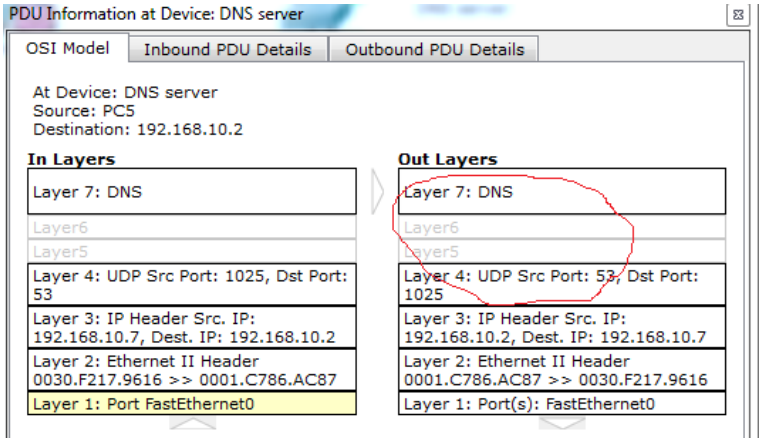


Fig-9: Showing OSI layer involvement in DNS

LAB EXERCISE:

1. Implement the given topology.
2. Add some web servers in your network.
3. Implement DNS & add records of your web servers.

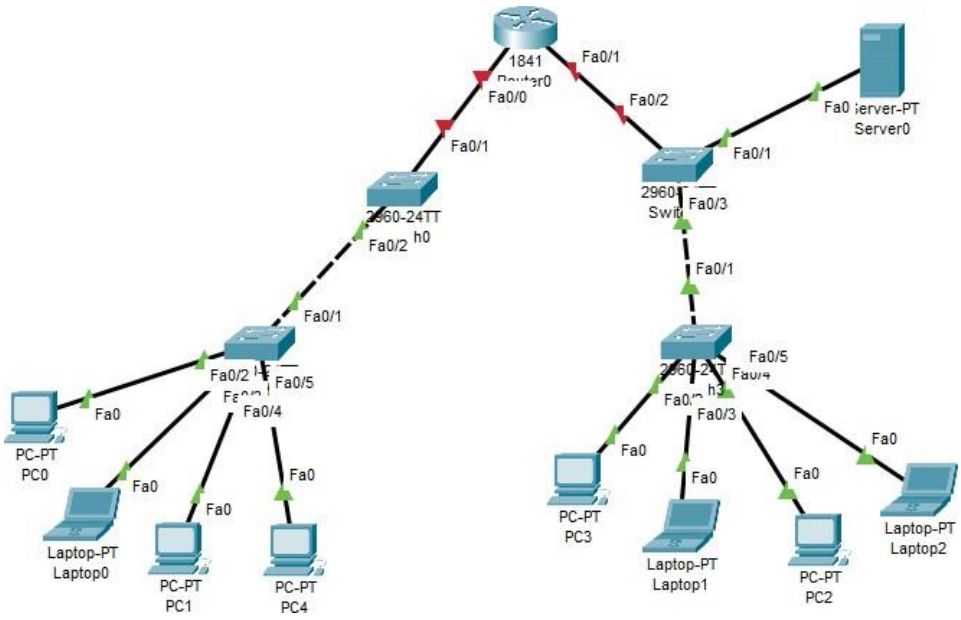


Fig-10: Network topology for task

SMTP

1. Introduction:

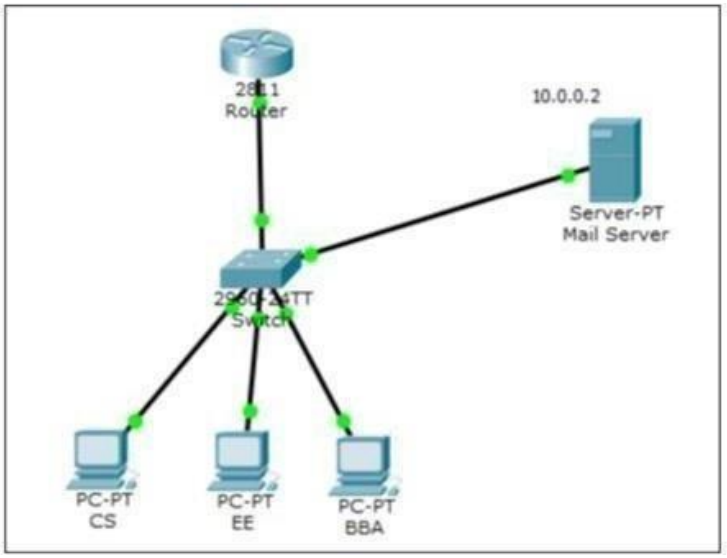
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with Extended SMTP additions by RFC 5321,which is the protocol in widespread use today. Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTPonly for sending messages to a mail server for relaying. For retrieving messages, client applications usuallyuse either IMAP or POP3.

SMTP communication between mail servers uses port 25. Mail clients on the other hand, often submit theoutgoing emails to a mail server on port 587. Despite being deprecated, mail providers sometimes still permit the use of nonstandard port 465 for this purpose. SMTP runs over TCP.

2. Implementation:

Topology:

Construct thetopology shown in figure 1. Turn on router interface& assign IP's to PC using DHCP throughrouter as done in pervious lab. Assign static IP to email server.



Configure and Verify Email Services

- Click on Mail server
- Go to services & then email services
- Enable SMTP & POP3 Service
- Set Domain name fast.com
- Add following users

Username	Password
CS	123
BBA	456
EE	789

Table-1: User name & their passwords

Now configure user email account.
Goto PC → Desktop → Email
Fill the following fields as shown in figure 3.
Click "Save" to save the configurations and do the same for EE and BBA.

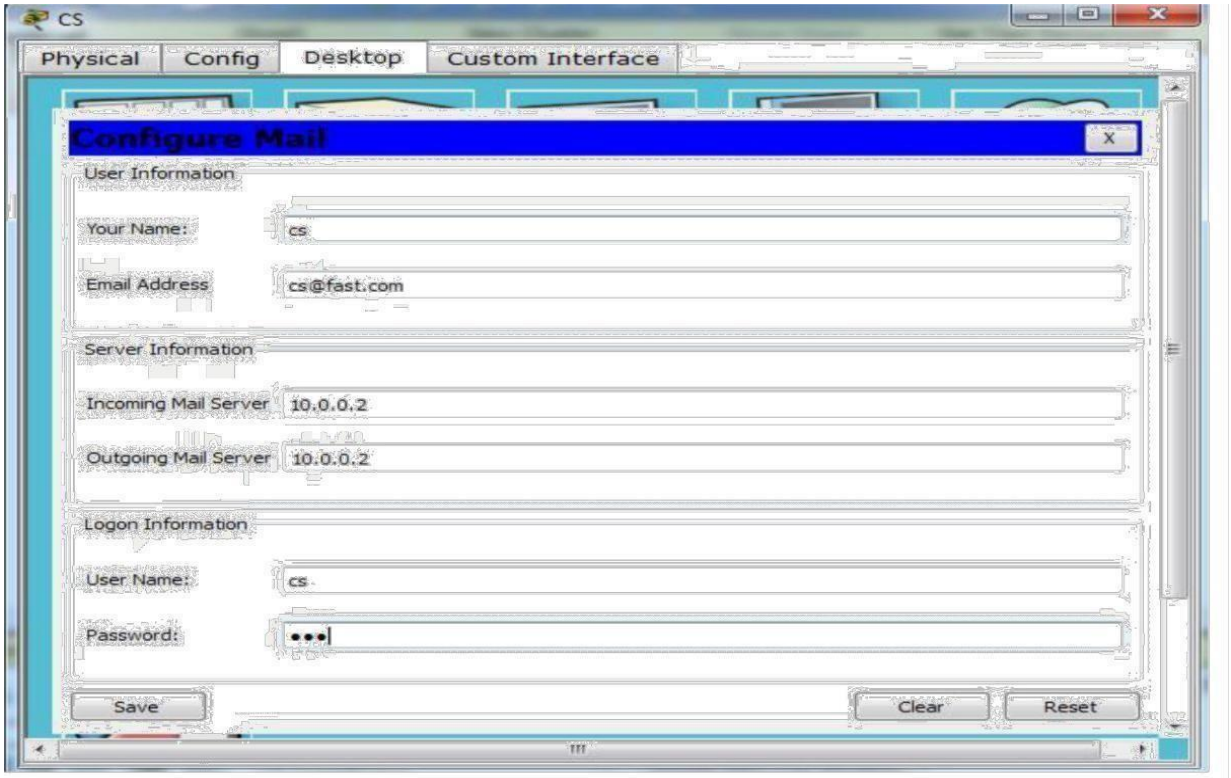


Fig-3: User Email configuration

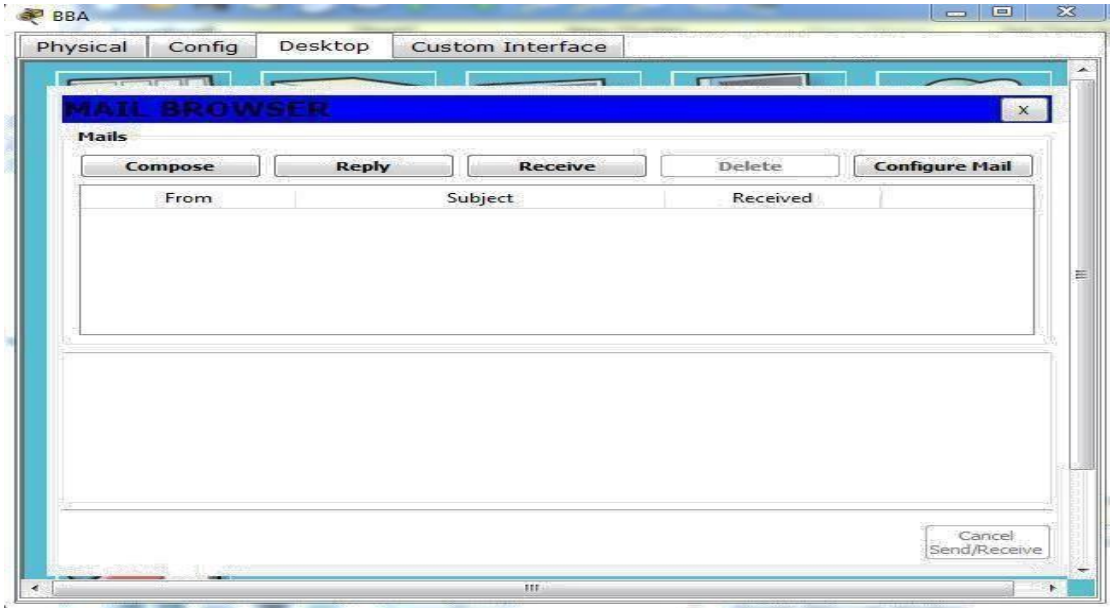
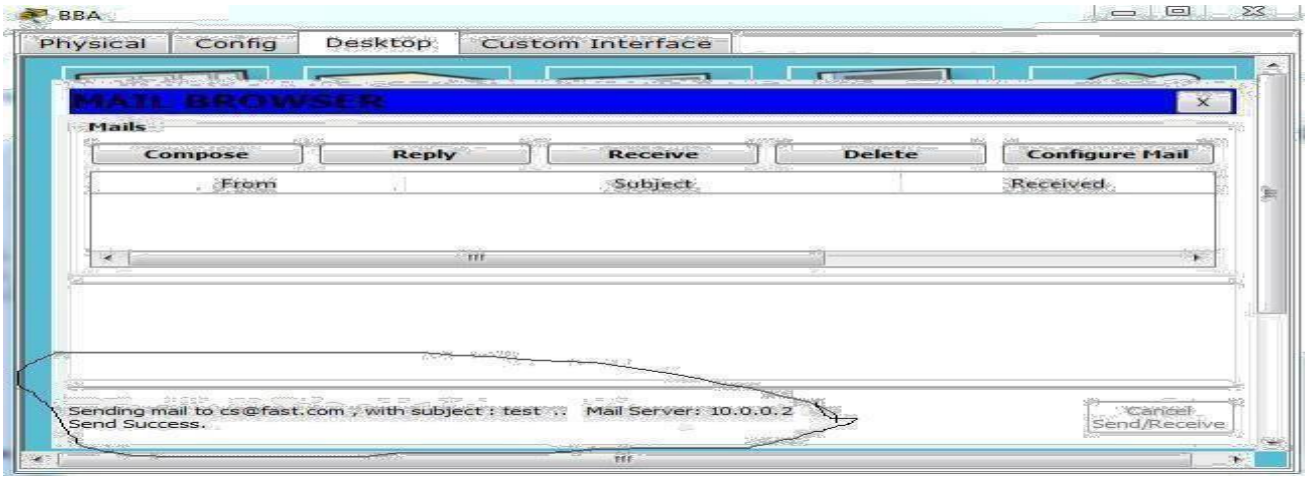


Fig-4: Mail browser view of user PC after mail configuration

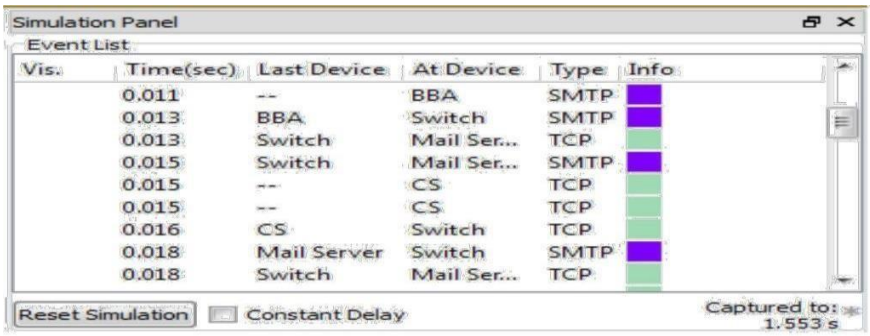
Now compose email **cs@fast.com**

Click on “Send” to send Email.



Simulation:

To note POP 3 header format information, go to simulation mode edit filters & check SMTP & POP 3 boxes. After that click on capture/forward button. Now see how mail server works



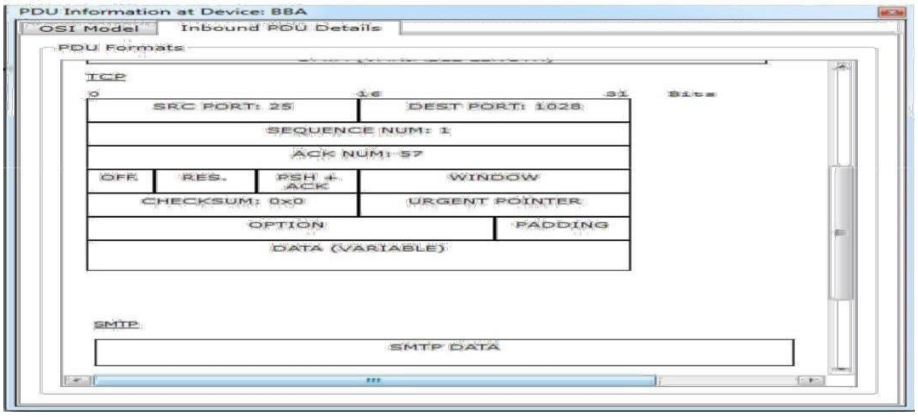


Fig-7: Packets capture in simulation mode & their PDU detail

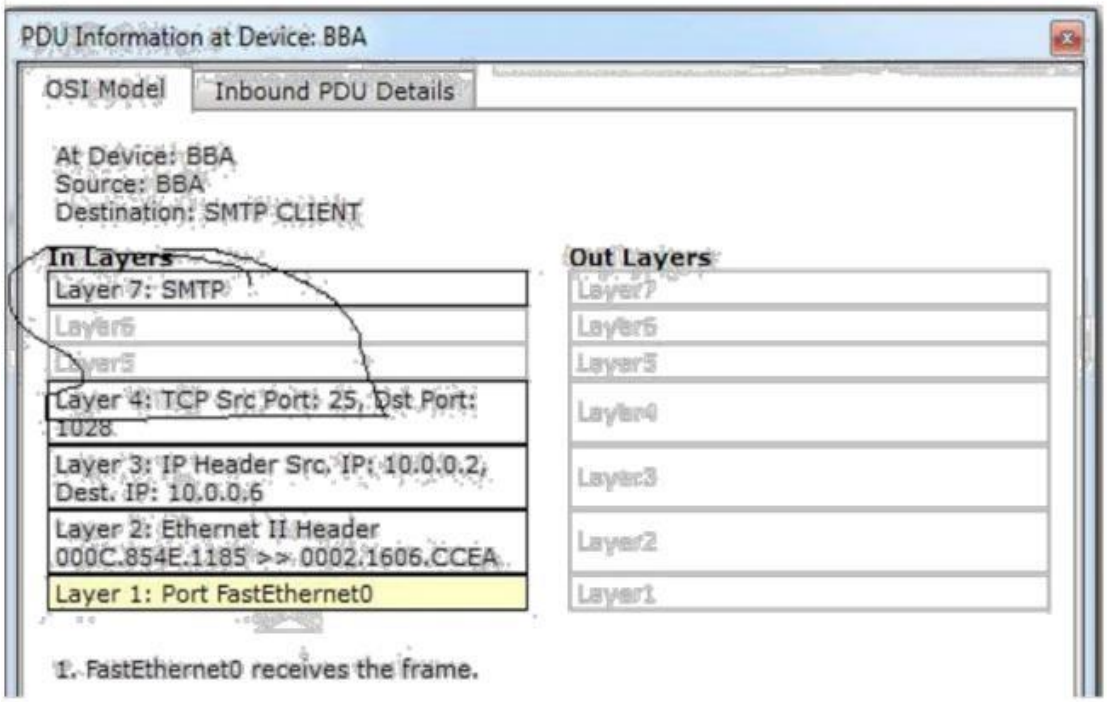
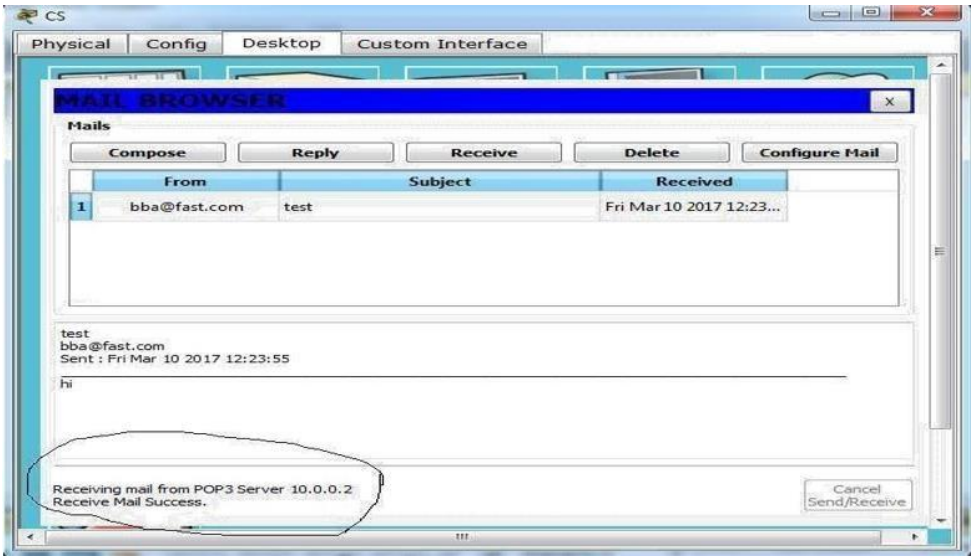


Fig-8: OSI layer information about protocols at each layer in sending mail packet.



FTP

Introduction:

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP). FTP uses TCP as its under layer transport protocol for data reliability transfer. It uses port 21.

FTP may run in active or passive mode, which determines how the data connection is established.

- In active mode, the client starts listening for incoming data connections from the server on port M. It sends the FTP command PORT M to inform the server on which port it is listening. The server then initiates a data channel to the client from its port 20, the FTP server data port.
- In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server, which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received.

Both modes were updated in September 1998 to support IPv6. Further changes were introduced to the passive mode at that time, updating it to extended passive mode.

Implementation:

In this activity, you will configure FTP server in Cisco Packet Tracer. After configuration you will transferfile between client & server. This activity is divided into 3 parts. First Construct the figure 10 topology & repeat all essential steps which we are done in pervious section.

Part 1: Configure FTP services on server

a) Click Server > Config tab > FTP.

b) Click On to enable FTP service.

c) In User Setup, create the following user accounts. Click the + button to add the account:

Username	Password	Permissions
Fast	123	limited to Read, write and List

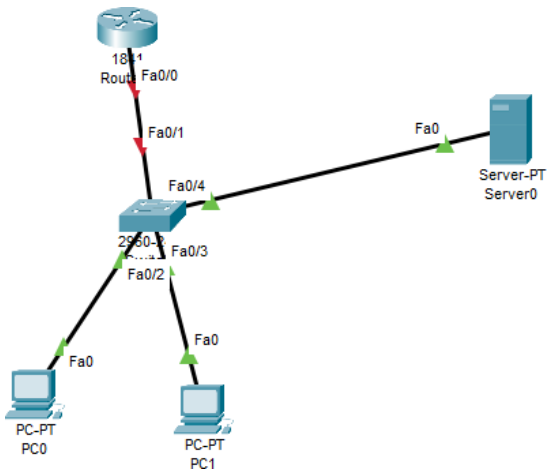


Fig-10: Topology

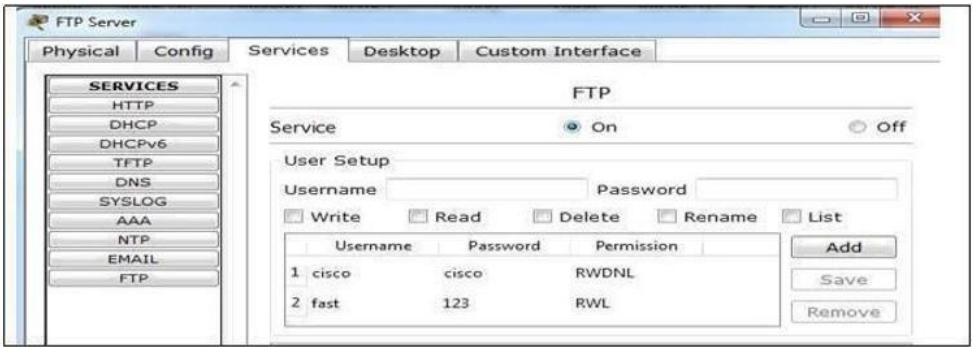


Fig-11: Enabling STP services on server

Now go to PC Desktop command prompt. Connect with the FTP server using username & password assignto FTP server.

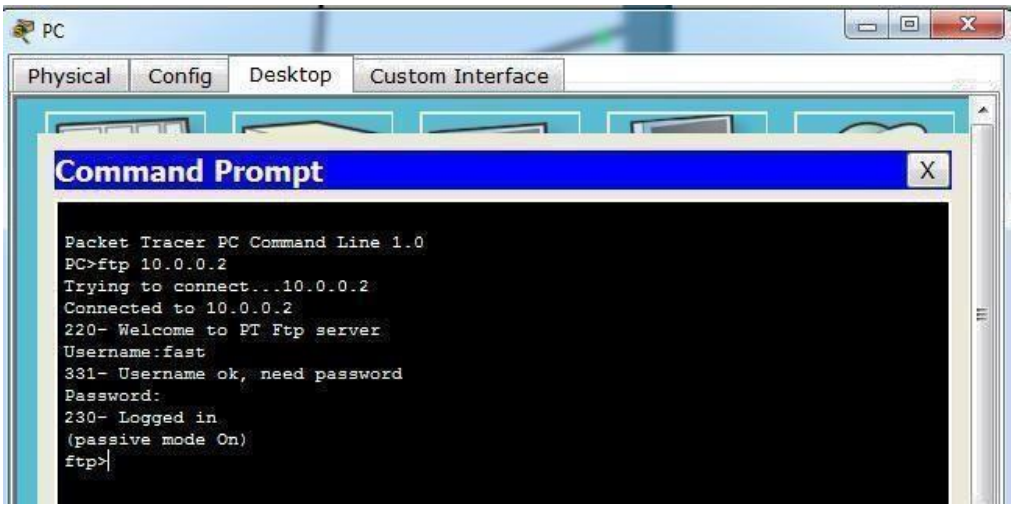


Fig-12: PC established connection with FTP server

Part 2: Upload the file to FTP server

Go to PC Desktop text editor create file named test.bin

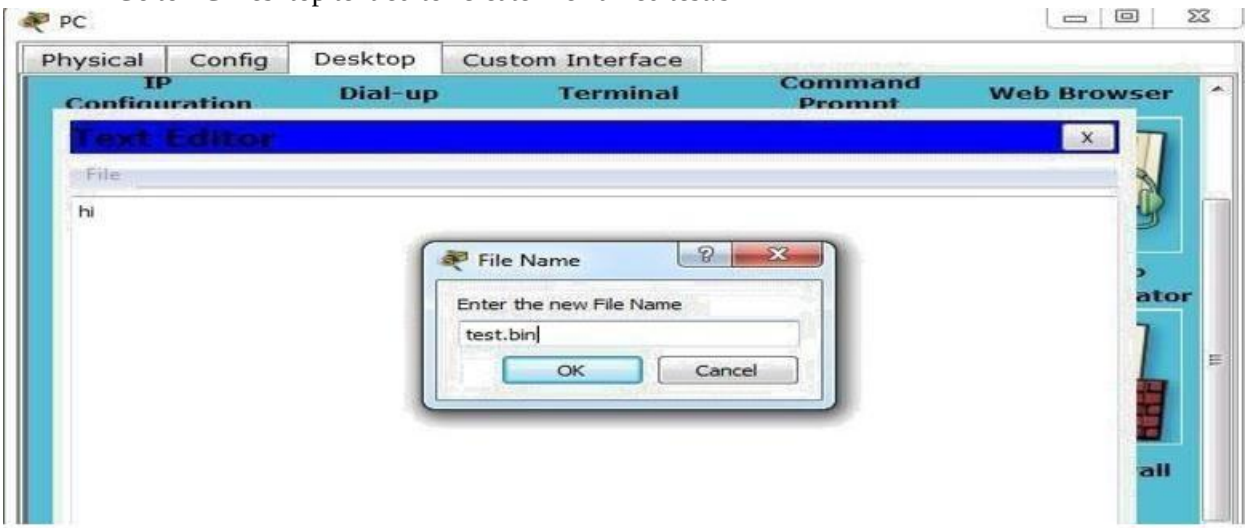


Fig-13: Creating text file in PC

After creating the file go to PC Desktop command prompt and write the following command to transfer filefrom PC to FTP server.

PUT test.bin

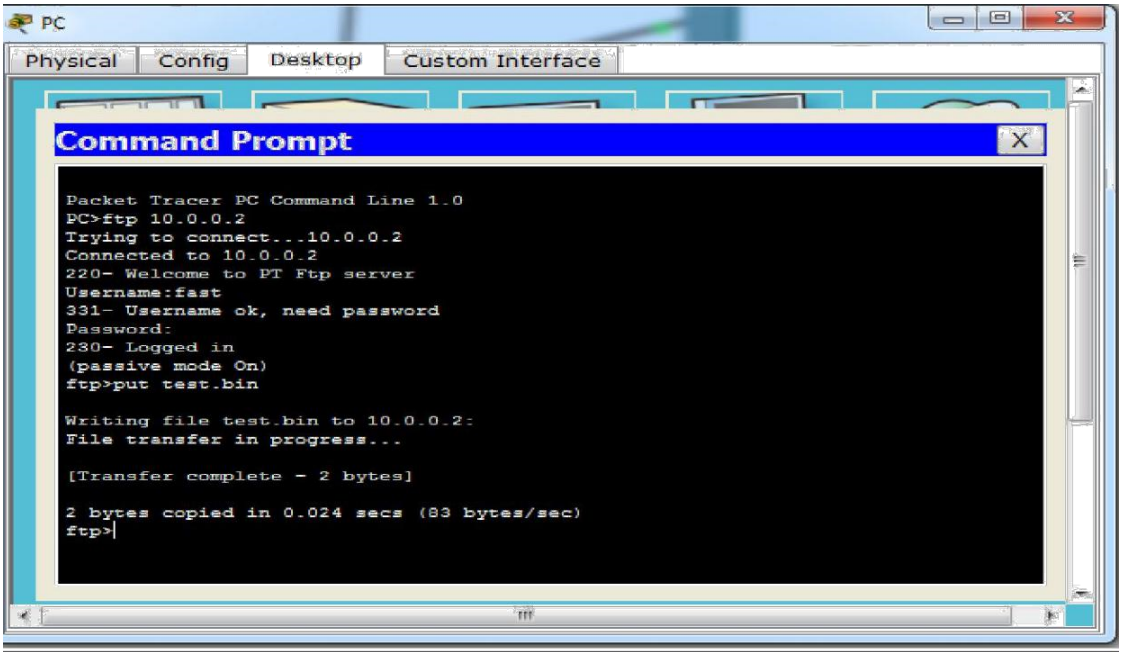


Fig-14: transfer of file from PC to FTP server

Part 3: Download the file from FTP server

Now go to other PC desktop command prompt. Established connection with FTP server and then write the ***dir*** command to see the files in FTP server.

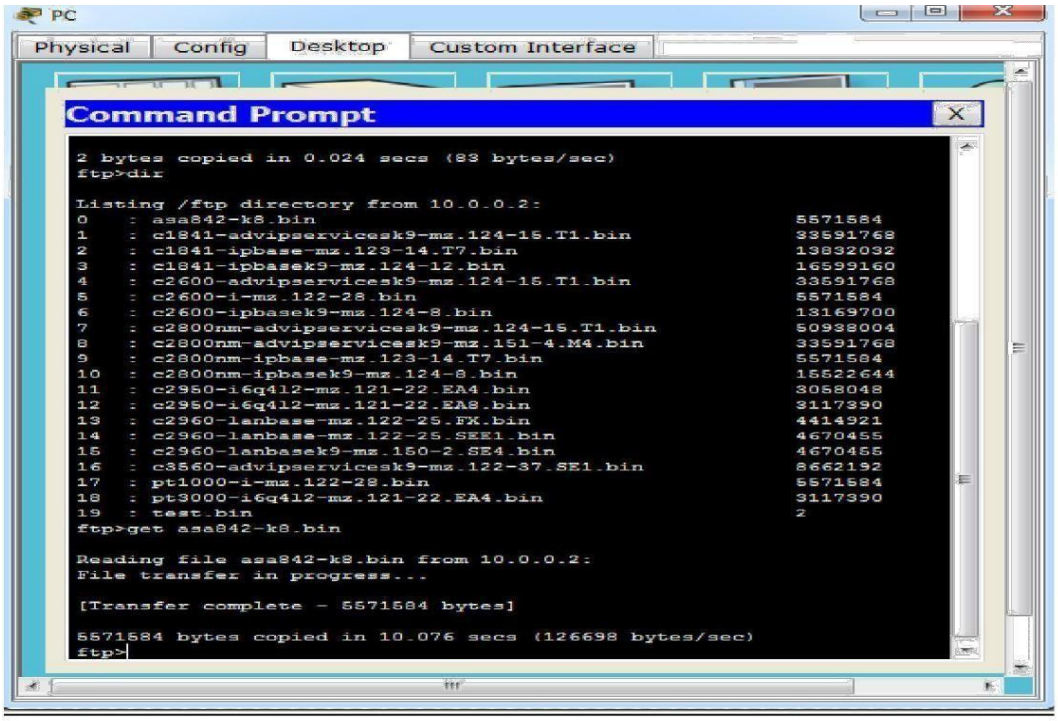
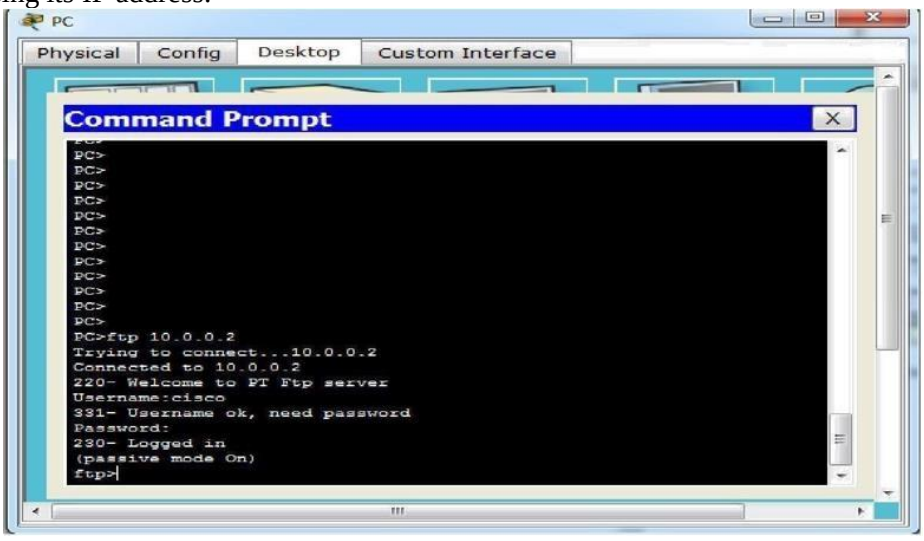


Fig-15: List of current Files in FTP server

Simulation

Select the simulation mode. Go to PC desktop command prompt again make connection with FTP serverusing its IP address.



Now to note the FTP header format information go to simulation mode edit filters and click on FTP check boxthen click on capture/forward button.

How FTP server resolves the login request.

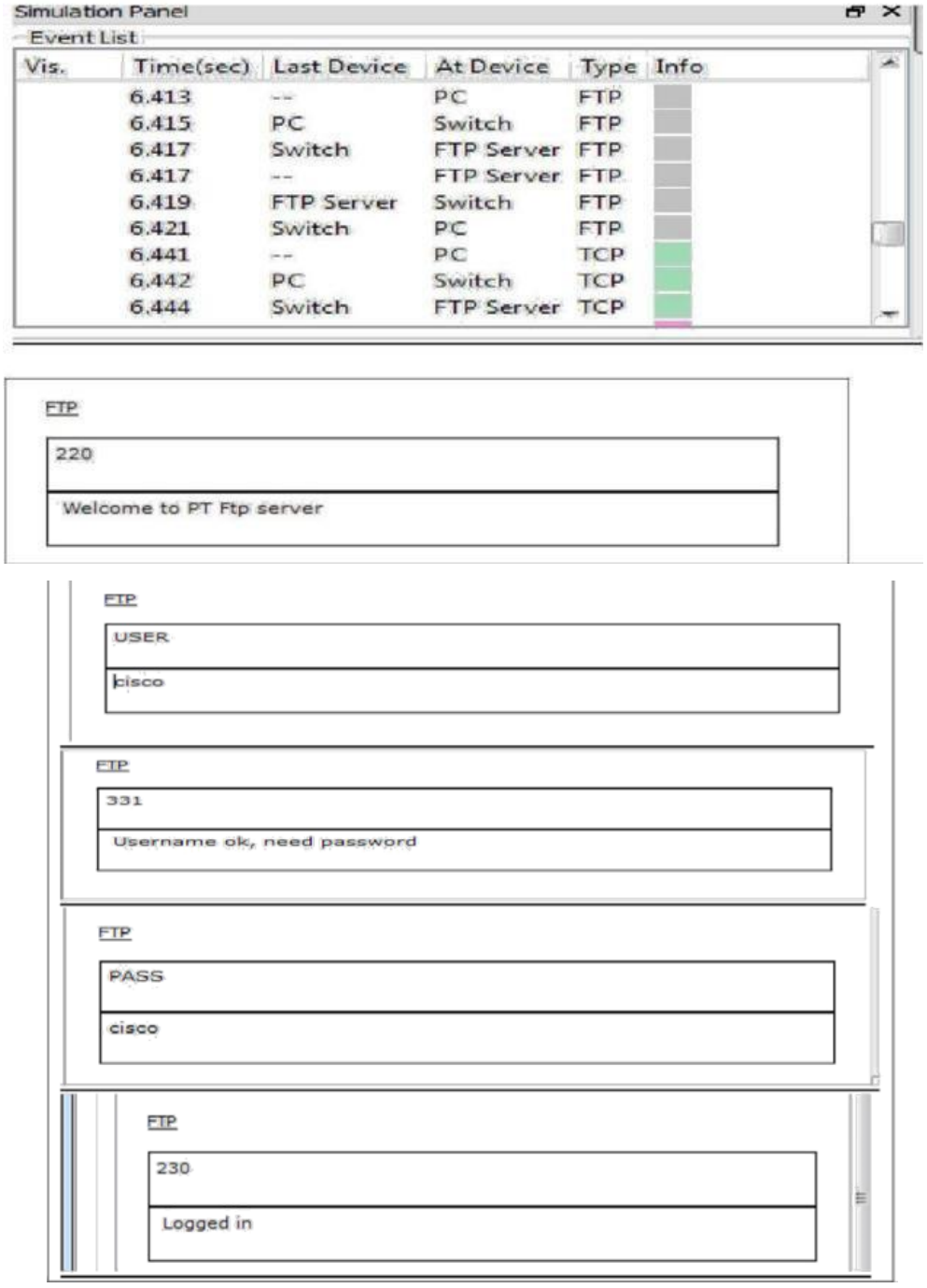


Fig-17: Packets capture in simulation mode

Now click on the FTP packet, you can note that the destination port is 21.

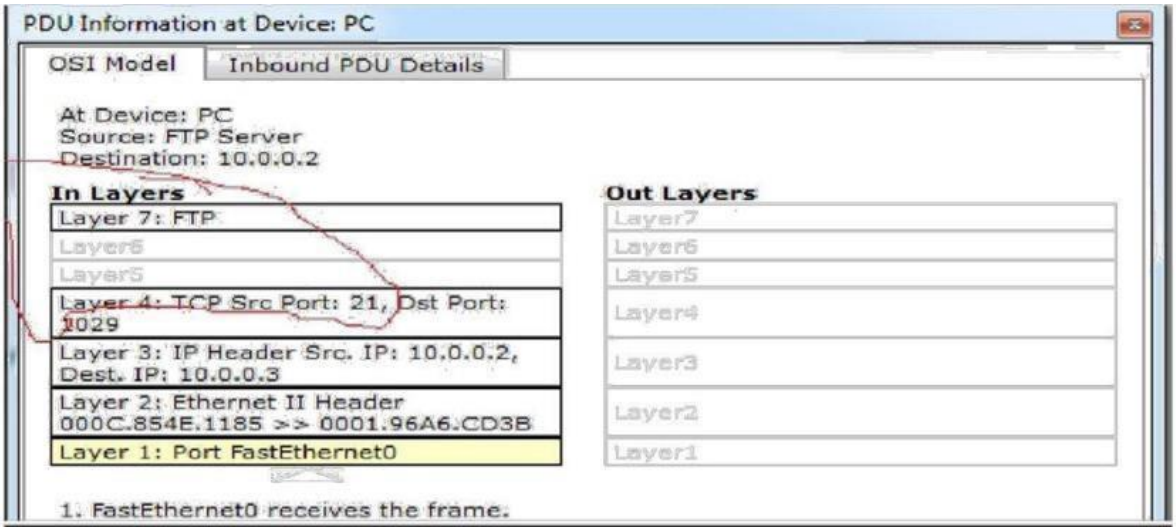


Fig-18: PDU information at PC

Now scroll the Outbound PDU Details, you can see the FTP PDU

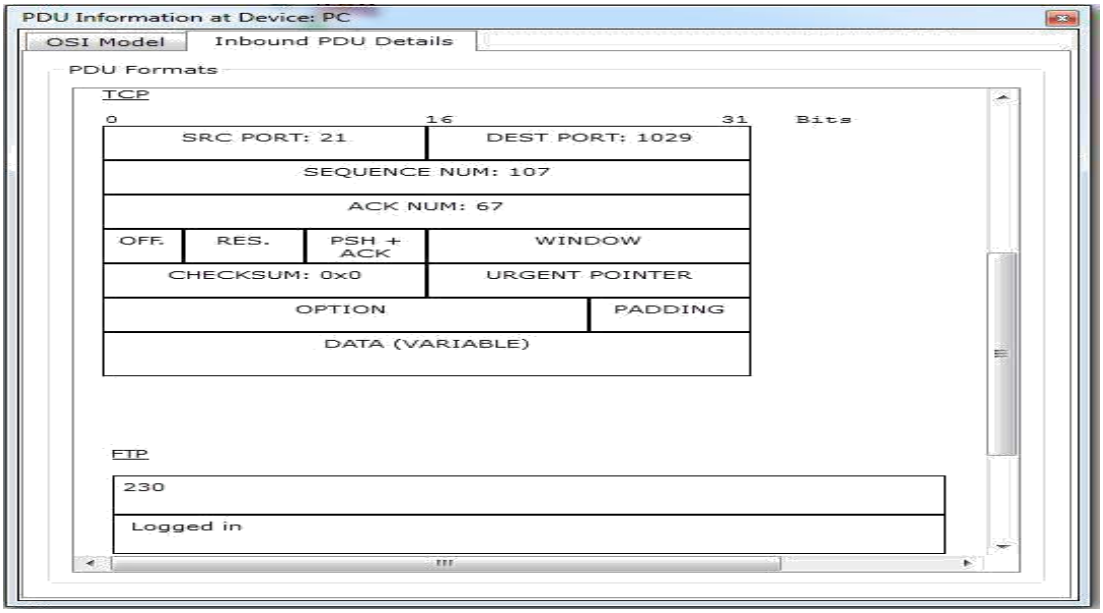


Fig-19: PDU details

1. nslookup In this lab, we'll make extensive use of the nslookup tool, which is available in most Linux/Unix and Microsoft platforms today. To run nslookup in Linux/Unix, you just type the nslookup command on the command line. To run it in Windows, open the Command Prompt and run nslookup on the command line. In it is most basic operation, nslookup tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

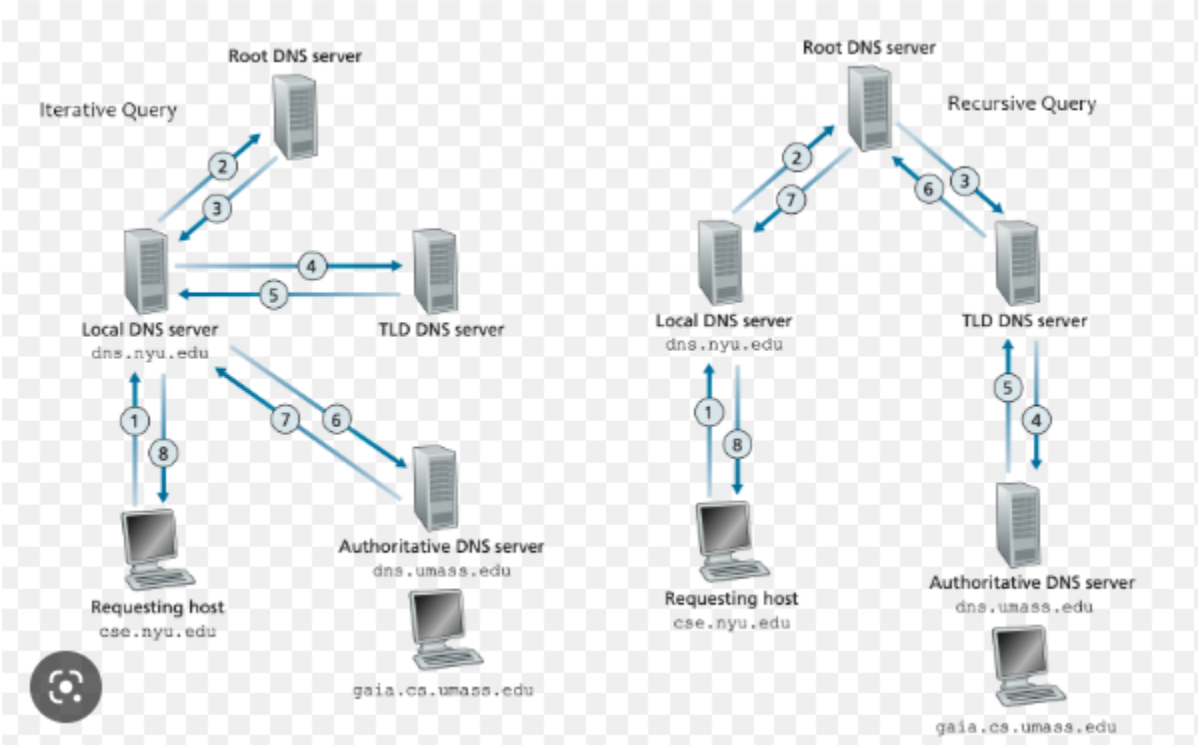
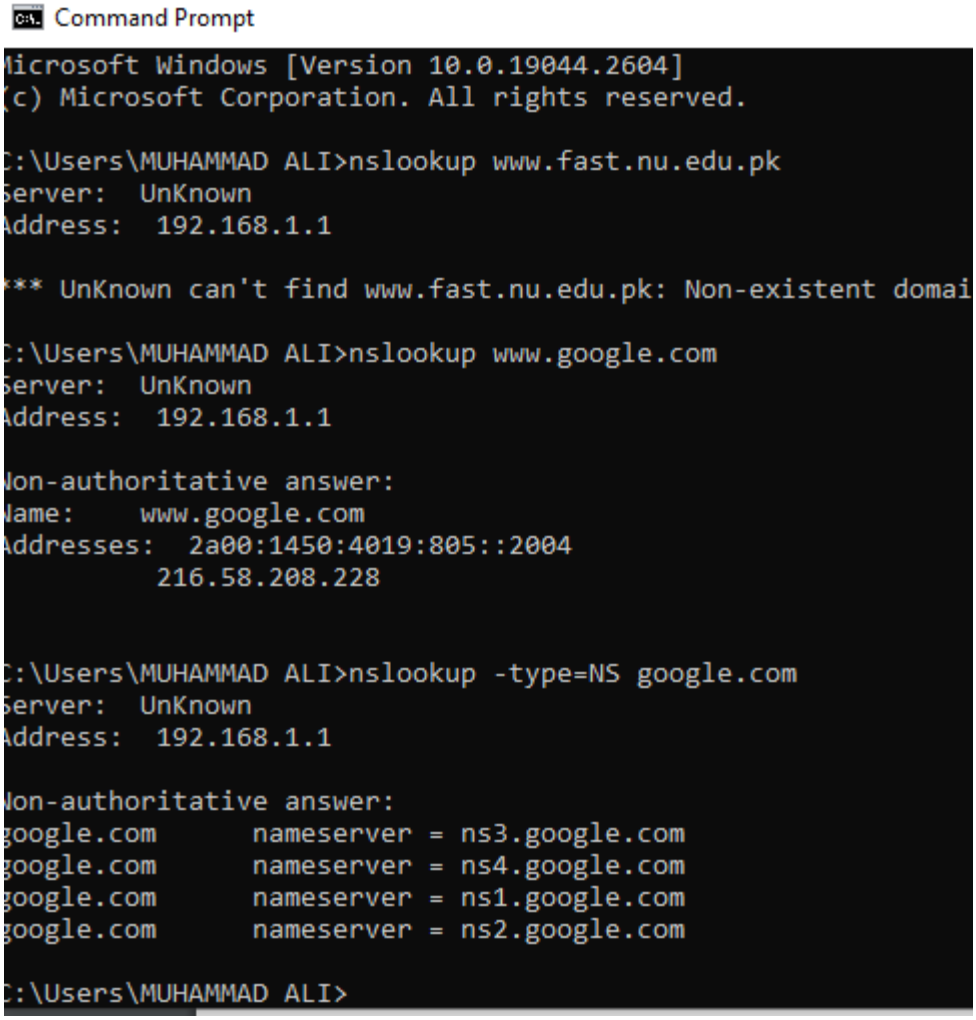
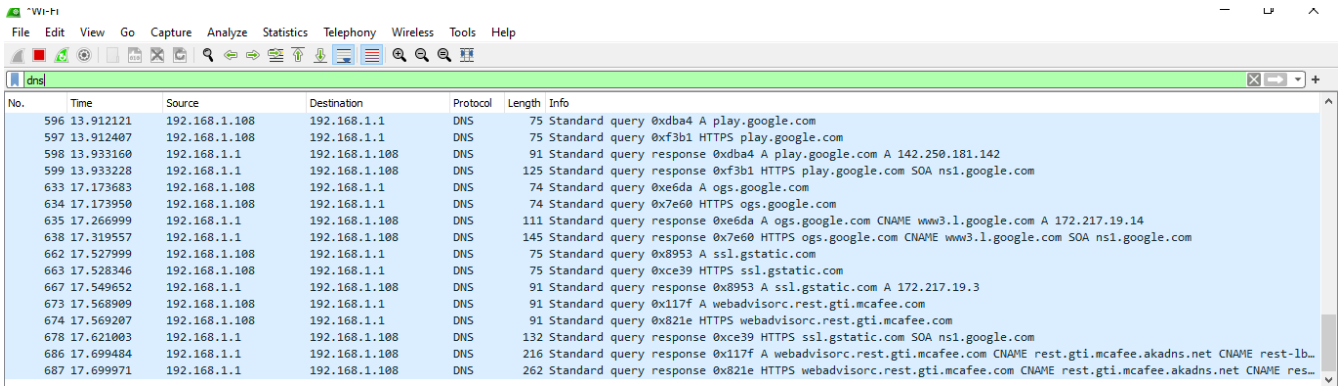


Figure 1 DNS


Command Prompt
Microsoft Windows [Version 10.0.19044.2604]
(c) Microsoft Corporation. All rights reserved.
C:\Users\MUHAMMAD ALI>nslookup www.fast.nu.edu.pk
Server: UnKnown
Address: 192.168.1.1
*** UnKnown can't find www.fast.nu.edu.pk: Non-existent domai
C:\Users\MUHAMMAD ALI>nslookup www.google.com
Server: UnKnown
Address: 192.168.1.1
Non-authoritative answer:
Name: www.google.com
Addresses: 2a00:1450:4019:805::2004
          216.58.208.228
C:\Users\MUHAMMAD ALI>nslookup -type=NS google.com
Server: UnKnown
Address: 192.168.1.1
Non-authoritative answer:
google.com   nameserver = ns3.google.com
google.com   nameserver = ns4.google.com
google.com   nameserver = ns1.google.com
google.com   nameserver = ns2.google.com
C:\Users\MUHAMMAD ALI>

```
C:\Users\MUHAMMAD ALI>ipconfig /all
```

Wireshark DNS lab:



No.	Time	Source	Destination	Protocol	Length	Info
596	13.912121	192.168.1.108	192.168.1.1	DNS	75	Standard query 0xdba4 A play.google.com
597	13.912407	192.168.1.108	192.168.1.1	DNS	75	Standard query 0xf3b1 HTTPS play.google.com
598	13.933160	192.168.1.1	192.168.1.108	DNS	91	Standard query response 0xdba4 A play.google.com A 142.250.181.142
599	13.933228	192.168.1.1	192.168.1.108	DNS	125	Standard query response 0xf3b1 HTTPS play.google.com SOA ns1.google.com
633	17.173683	192.168.1.108	192.168.1.1	DNS	74	Standard query 0xe6da A ogs.google.com
634	17.173950	192.168.1.108	192.168.1.1	DNS	74	Standard query 0x7e60 HTTPS ogs.google.com
635	17.266999	192.168.1.1	192.168.1.108	DNS	111	Standard query response 0xe6da A ogs.google.com CNAME www3.l.google.com A 172.217.19.14
638	17.319557	192.168.1.1	192.168.1.108	DNS	145	Standard query response 0x7e60 HTTPS ogs.google.com CNAME www3.l.google.com SOA ns1.google.com
662	17.527999	192.168.1.108	192.168.1.1	DNS	75	Standard query 0x8953 A ssl.gstatic.com
663	17.528346	192.168.1.108	192.168.1.1	DNS	75	Standard query 0xce39 HTTPS ssl.gstatic.com
667	17.549652	192.168.1.1	192.168.1.108	DNS	91	Standard query response 0x8953 A ssl.gstatic.com A 172.217.19.3
673	17.568909	192.168.1.108	192.168.1.1	DNS	91	Standard query 0x117f A webadvisorc.rest.gti.mcafee.com
674	17.569207	192.168.1.108	192.168.1.1	DNS	91	Standard query 0x821e HTTPS webadvisorc.rest.gti.mcafee.com
678	17.621003	192.168.1.1	192.168.1.108	DNS	132	Standard query response 0xce39 HTTPS ssl.gstatic.com SOA ns1.google.com
686	17.699484	192.168.1.1	192.168.1.108	DNS	216	Standard query response 0x117f A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net CNAME rest-lb…
687	17.699971	192.168.1.1	192.168.1.108	DNS	262	Standard query response 0x821e HTTPS webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net CNAME res…

Lab Exercise:

Let's suppose your organization need to create it's on small server (for provide some services) basednetwork. With bellow mentioned topology and instructions:

a) Configure SMTP (create account with your last name) send mail from PC-A to PC-B.
b) Configure FTP server create account with your first name, password with your roll number and filename with your last name (.bin extension) show all connection results.

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?
2. Run nslookup to determine the authoritative DNS servers for a university in Europe.
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

11. What is the destination port for the DNS query message? What is the source port of DNS response message?
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
15. Provide a screenshot.

Now repeat the previous experiment, but instead issue the command: nslookup –type=NS mit.edu Answer the following questions5 :
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?
19. Provide a screenshot. Now repeat the previous experiment, but instead issue the command: nslookup www.aiit.or.kr bitsy.mit.edu Answer the following questions6:
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
23. Provide a screenshot. 5 If you are unable to run Wireshark and capture a trace file, use t

NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 07

Objective:

- Introduction to NS3 network simulator
- Simple network simulation in NS3
- Implementation of TCP congestion control & simulation in NS3

NS3

1. Introduction:

NS3 is a discrete event simulator targeted at networking research. NS3 provides substantial support for simulation of TCP, UDP, routing & multicast protocols over wired & wireless (local & satellite) networks. This simulator is primarily UNIX based & the NS commands can either be entered via UNIX command prompt or by running a scripting language file, but scripting language is preferred way. NS3 uses Tcl (pronounced as 'tickle') as it's scripting language, which is edited using a text editor & in this example we will use **vi**.

2. Introduction to vi:

vi is a text editor that is available in all UNIX systems, other editors such pico & emacs can also be used instead. Before you start for the first time, you must note that vi is modal editor. A mode is like an environment. Different modes in vi interpret the same key differently. For example, if you're in insert mode, typing a adds an a to the text, whereas in command mode, typing a put you in insert mode because a is the key abbreviation for the append command. If you get confused about what mode you're in, press the Escape key. Pressing Escape key always returns you to the command mode & if you are already in command mode, it simply beeps to remind you of the fact.

When you are in command mode, you can manage your document; this includes the capability to change text, rearrange it, & delete it. Insert mode is when you are maneuver the text area using the arrows keys.

For starting a new document, simply type vi after the command prompt to the start the vi editor. The cursor will be located in the top left corner & each of the following lines will start with a tilde (~) denoting empty lines. Note that the vi editor is currently in command mode. In order to edit an existing file, type the name of the file along with the extension after typing vi & a space in the UNIX command prompt. To enter into insert mode simply press a on the keyboard. Then to save the edited document, type a colon (:) & the cursor will be located in the bottom left corner after the colon, followed by a w & then press enter. In order to quit vi editor type a colon followed by a q (:q), this will take you back to the UNIX prompt. You can also choose to quit editing without saving by typing :q!, & if you forget the exclamation mark (!) the system will issue a warning.

Note: direct link for NS 3 image https://www.nsnam.com/2020/04/download-vm-image-of-ns3-and-contiki-ng.html

3. Simple Simulation in NS3:

First.cc

```
/* -*- Mode:C++; c-file-style:"gnu"; indent-tabs-mode:nil; -*- */
/*
 * This program is free software; you can redistribute it and/or modify
 * it under the terms of the GNU General Public License version 2 as
 * published by the Free Software Foundation;
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
 * along with this program; if not, write to the Free Software
 * Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
 */

#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/internet-module.h"
#include "ns3/point-to-point-module.h"
#include "ns3/applications-module.h"

using namespace ns3;

NS_LOG_COMPONENT_DEFINE ("FirstScriptExample");
```

```
int
main (int argc, char *argv[])
{
 CommandLine cmd;
 cmd.Parse (argc, argv);

 Time::SetResolution (Time::NS);
 LogComponentEnable ("UdpEchoClientApplication", LOG_LEVEL_INFO);
 LogComponentEnable ("UdpEchoServerApplication", LOG_LEVEL_INFO);

 NodeContainer nodes;
 nodes.Create (2);

 PointToPointHelper pointToPoint;
 pointToPoint.SetDeviceAttribute ("DataRate", StringValue ("5Mbps"));
 pointToPoint.SetChannelAttribute ("Delay", StringValue ("2ms"));

 NetDeviceContainer devices;
 devices = pointToPoint.Install (nodes);

 InternetStackHelper stack;
 stack.Install (nodes);

 Ipv4AddressHelper address;
 address.SetBase ("10.1.1.0", "255.255.255.0");

 Ipv4InterfaceContainer interfaces = address.Assign (devices);

 UdpEchoServerHelper echoServer (9);

 ApplicationContainer serverApps = echoServer.Install (nodes.Get (1));
 serverApps.Start (Seconds (1.0));
 serverApps.Stop (Seconds (10.0));
```

```
  UdpEchoClientHelper echoClient (interfaces.GetAddress (1), 9);
  echoClient.SetAttribute ("MaxPackets", UintegerValue (1));
  echoClient.SetAttribute ("Interval", TimeValue (Seconds (1.0)));
  echoClient.SetAttribute ("PacketSize", UintegerValue (1024));

  ApplicationContainer clientApps = echoClient.Install (nodes.Get (0));
  clientApps.Start (Seconds (2.0));
  clientApps.Stop (Seconds (10.0));

  Simulator::Run ();
  Simulator::Destroy ();
  return 0;
}
```

Table 1First.cc [Dr. par deep kumar]

Second.cc

```
/* -*- Mode:C++; c-file-style:"gnu"; indent-tabs-mode:nil; -*- */
/*
* This program is free software; you can redistribute it and/or modify
* it under the terms of the GNU General Public License version 2 as
* published by the Free Software Foundation;
*
* This program is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
* GNU General Public License for more details.
*
* You should have received a copy of the GNU General Public License
* along with this program; if not, write to the Free Software
* Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
*/
```

```
#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/csma-module.h"
#include "ns3/internet-module.h"
#include "ns3/point-to-point-module.h"
#include "ns3/applications-module.h"
#include "ns3/ipv4-global-routing-helper.h"
#include "ns3/netanim-module.h"


// Default Network Topology
//
//     10.1.1.0
// n0 ---------- n1   n2   n3   n4
//   point-to-point |   |   |   |
//                  ================
//                    LAN 10.1.2.0


using namespace ns3;

NS_LOG_COMPONENT_DEFINE ("SecondScriptExample");

int
main (int argc, char *argv[])
{
 bool verbose = true;
 uint32_t nCsma = 3;

 CommandLine cmd;
 cmd.AddValue ("nCsma", "Number of \"extra\" CSMA nodes/devices",
    nCsma);
```

```
cmd.AddValue ("verbose", "Tell echo applications to log if true", verbose);

cmd.Parse (argc,argv);

if (verbose)
 {
  LogComponentEnable ("UdpEchoClientApplication", LOG_LEVEL_INFO);
  LogComponentEnable ("UdpEchoServerApplication", LOG_LEVEL_INFO);
 }

nCsma = nCsma == 0 ? 1 : nCsma;

NodeContainer p2pNodes;
p2pNodes.Create (2);

NodeContainer csmaNodes;
csmaNodes.Add (p2pNodes.Get (1));
csmaNodes.Create (nCsma);

PointToPointHelper pointToPoint;
pointToPoint.SetDeviceAttribute ("DataRate", StringValue ("5Mbps"));
pointToPoint.SetChannelAttribute ("Delay", StringValue ("2ms"));

NetDeviceContainer p2pDevices;
p2pDevices = pointToPoint.Install (p2pNodes);

CsmaHelper csma;
csma.SetChannelAttribute ("DataRate", StringValue ("100Mbps"));
csma.SetChannelAttribute ("Delay", TimeValue (NanoSeconds (6560)));

NetDeviceContainer csmaDevices;
csmaDevices = csma.Install (csmaNodes);
```

```
InternetStackHelper stack;
stack.Install (p2pNodes.Get (0));
stack.Install (csmaNodes);

Ipv4AddressHelper address;
address.SetBase ("10.1.1.0", "255.255.255.0");
Ipv4InterfaceContainer p2pInterfaces;
p2pInterfaces = address.Assign (p2pDevices);

address.SetBase ("10.1.2.0", "255.255.255.0");
Ipv4InterfaceContainer csmaInterfaces;
csmaInterfaces = address.Assign (csmaDevices);

UdpEchoServerHelper echoServer (9);

ApplicationContainer serverApps = echoServer.Install (csmaNodes.Get
  (nCsma));
serverApps.Start (Seconds (1.0));
serverApps.Stop (Seconds (10.0));

UdpEchoClientHelper echoClient (csmaInterfaces.GetAddress (nCsma), 9);
echoClient.SetAttribute ("MaxPackets", UintegerValue (1));
echoClient.SetAttribute ("Interval", TimeValue (Seconds (1.0)));
echoClient.SetAttribute ("PacketSize", UintegerValue (1024));

ApplicationContainer clientApps = echoClient.Install (p2pNodes.Get (0));
clientApps.Start (Seconds (2.0));
clientApps.Stop (Seconds (10.0));

Ipv4GlobalRoutingHelper::PopulateRoutingTables ();

pointToPoint.EnablePcapAll ("second");
csma.EnablePcap ("second", csmaDevices.Get (1), true);
```

```
        AnimationInterface anim ("second.xml");
        Simulator::Run ();
        Simulator::Destroy ();
        return 0;
}
```

Table 2 Secondt.cc [Dr. par deep kumar]

4. Code Explanation:

The following is the explanation of the script above. In general, an NS script starts with making aSimulator object instance.

- **set *ns* [new Simulator]:** generates an NS simulator object instance, and assigns it to variable *ns* (italics is used for variables and values in this section). What this line does is the following: Initialize the packet format (ignore this for now)
  - Create a scheduler (default is calendar scheduler)
  - Select the default address format (ignore this for now)

The "Simulator" object has member functions that do the following:

- Create compound objects such as nodes and links (described later)
- Connect network component objects created (ex. attach-agent)
- Set network component parameters (mostly for compound objects)
- Create connections between agents (ex. make connection between a "tcp" and "sink")
- Specify NAM display options
- Etc.

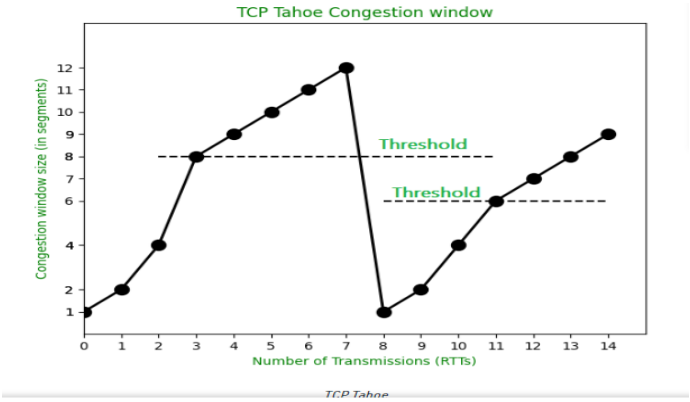
Most of member functions are for simulation setup (referred to as plumbing functions) and scheduling, however some of them are for the NAM display. The "Simulator" object memberfunction implementations are located in the "ns-2/tcl/lib/ns-lib.tcl" file.

TCP Congestion Control Simulation:

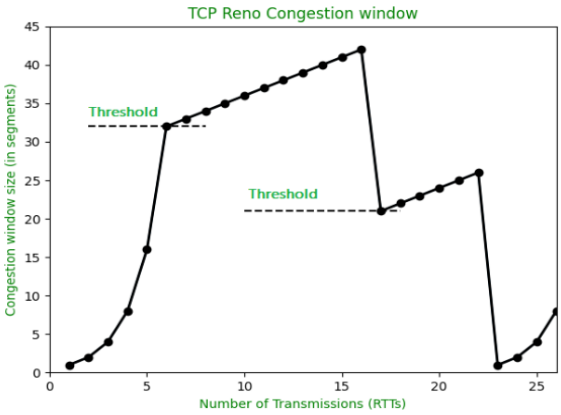
In this example we will implement & simulate congestion control mechanism of TCP between two nodes. It consists of three parts which are as follow.

1. Slow start threshold (exponential increase of packets) ssthresh
2. Congestion avoidance (additive increase)

3. Congestion detection (multiplicative decrease)



TCP Tohe



TCP Reno

Task 1

Q1. Apply TCP Congestion control mechanism in NS3 & plot the congestion window graph.

Helpful link for TCP congestion Task

https://www.youtube.com/watch?v=9rkN3FtOkaQ&t=885s

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.

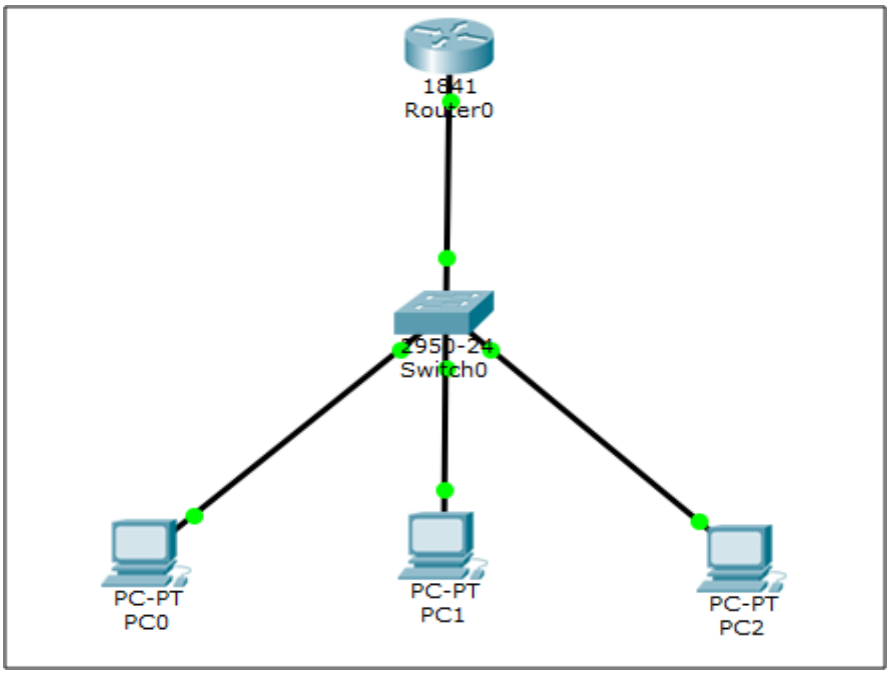


Fig-1: Network Topology

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

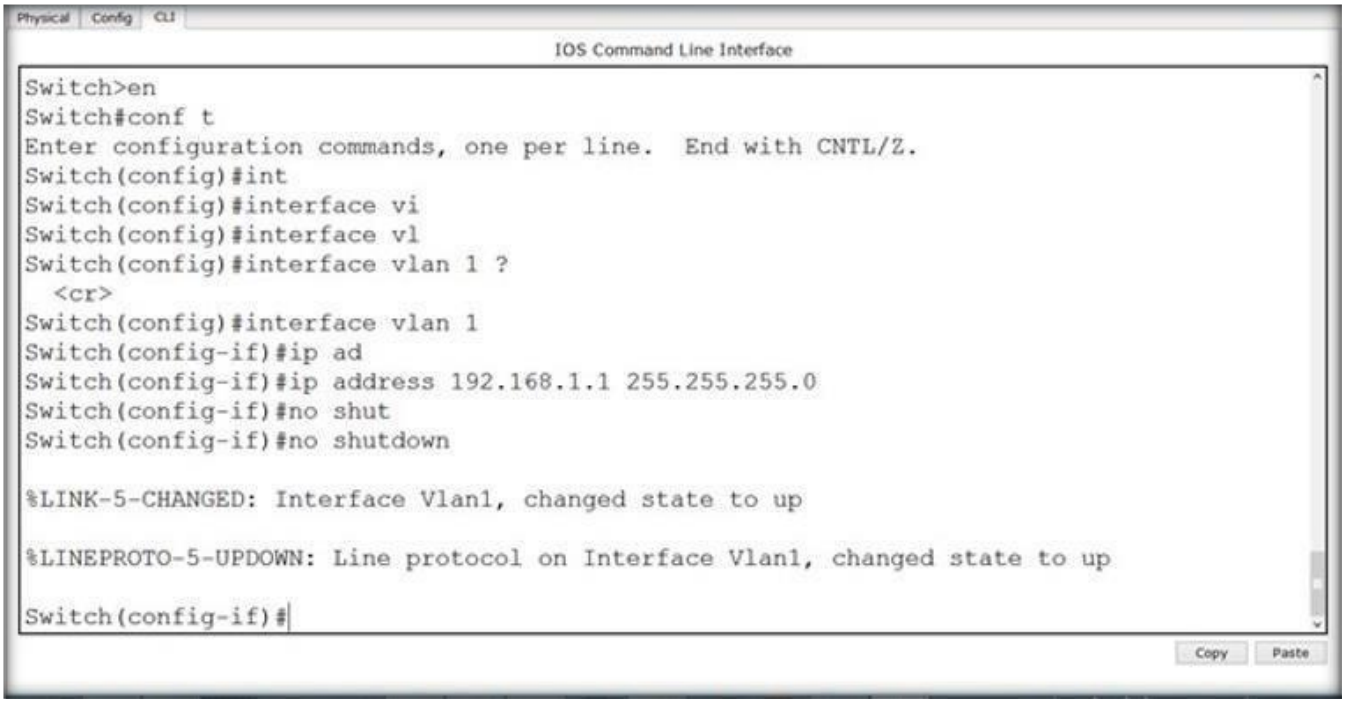


Fig-2: Configuring VLAN Connection

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

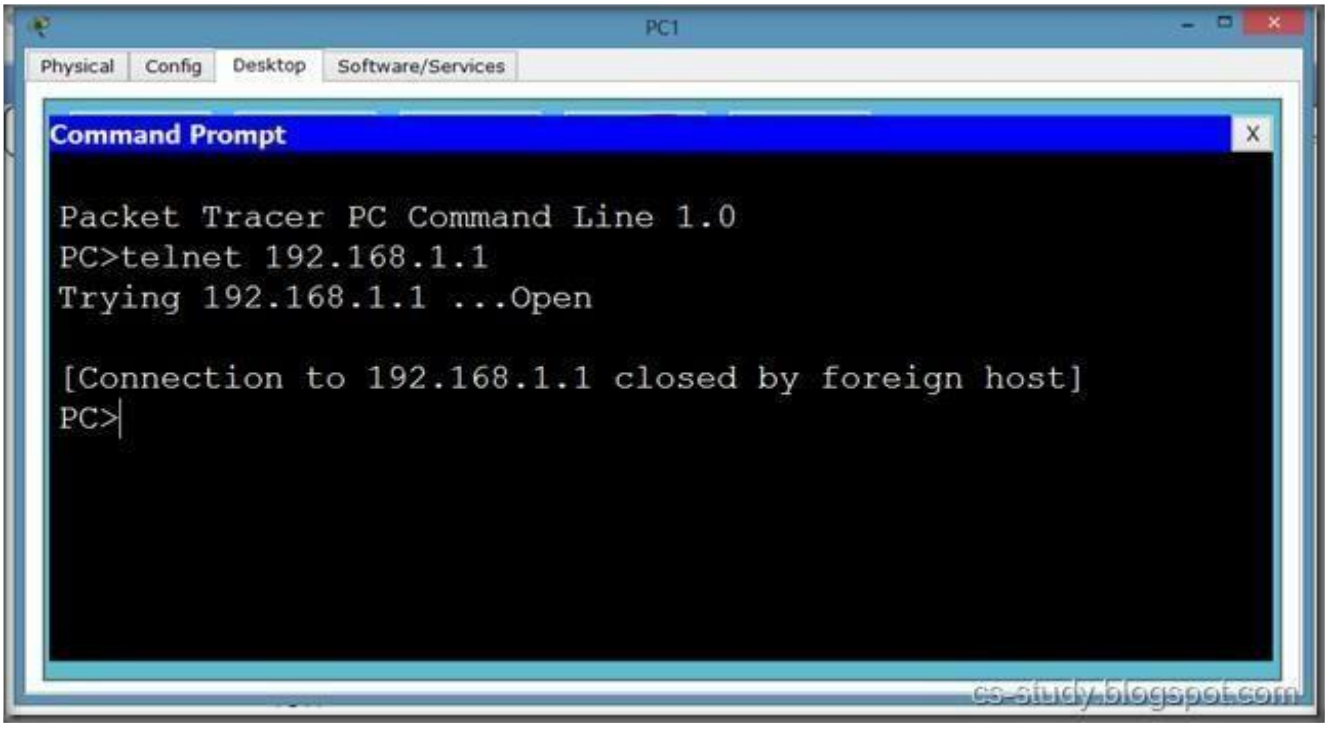


Fig-3: Initial Checking of VLAN

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.

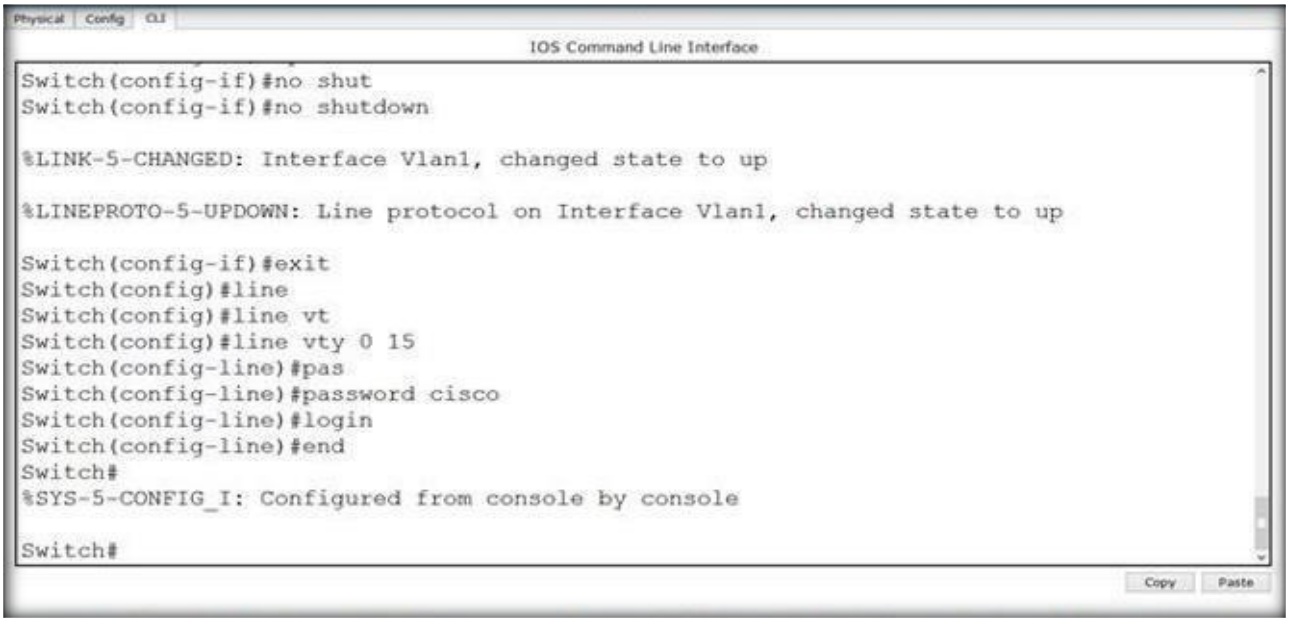


Fig-4: Creating Vty-line connection for Telnet

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

Fig-5: Checking Vty-line connection for Telnet

Let’s apply password on the switch enabled mode.

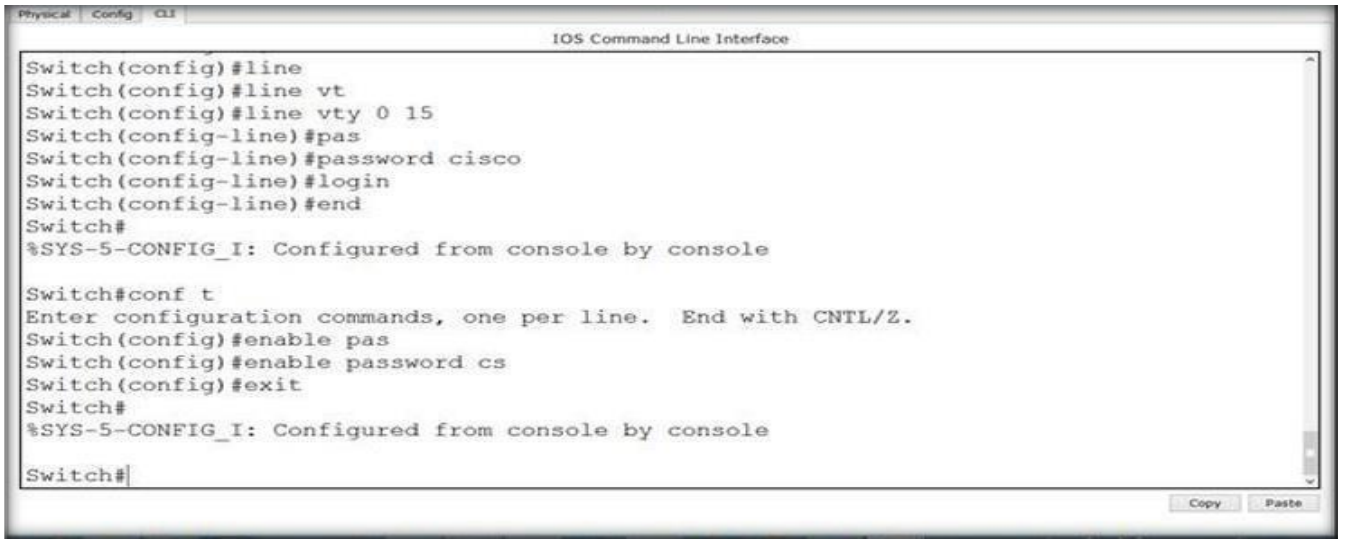


Fig-6: Adding password in enable mode

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

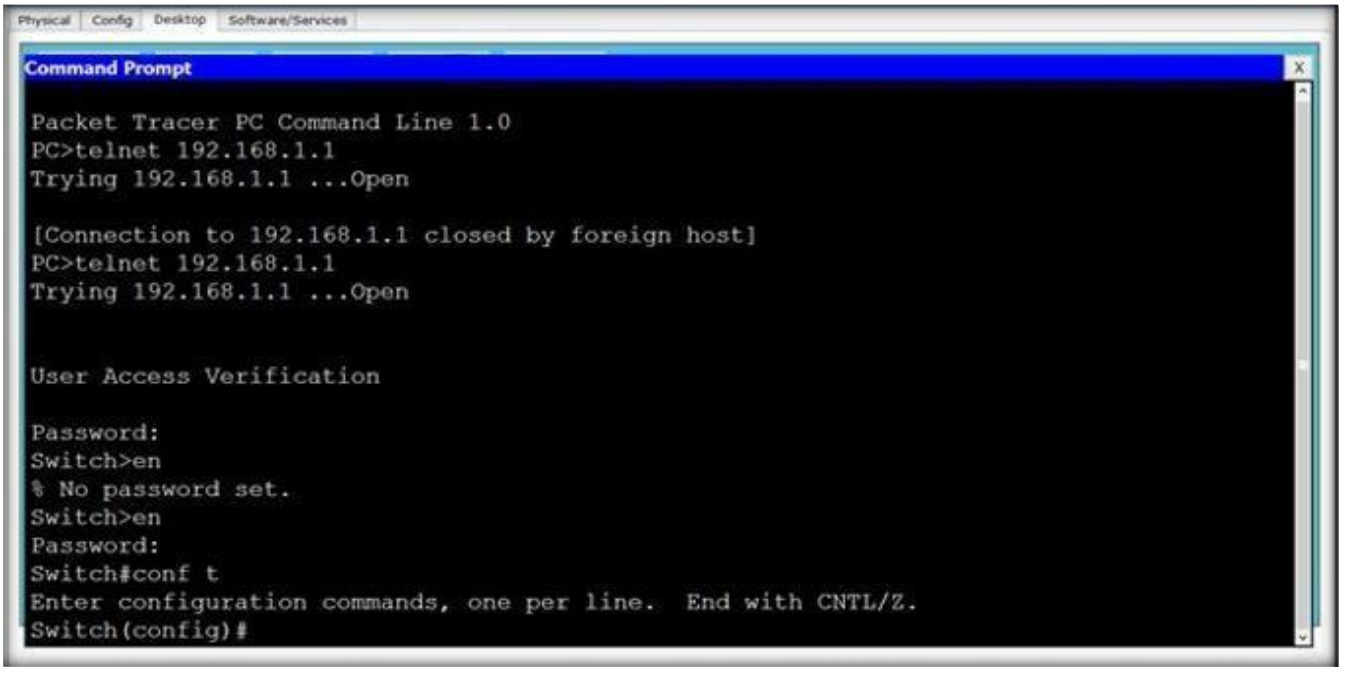


Fig-7: Checking by it using command

Introduction to SSH:

Secure Shell or Secure Socket Shell is a network protocol. It is an application layer protocol that is in the7th later of the Open Systems Interconnection (OSI) network model. It also refers to the suite of utilitiesthat 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 authenticationallows 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 thefigure 9 till figure 14 for the configuration of SSH Protocol.

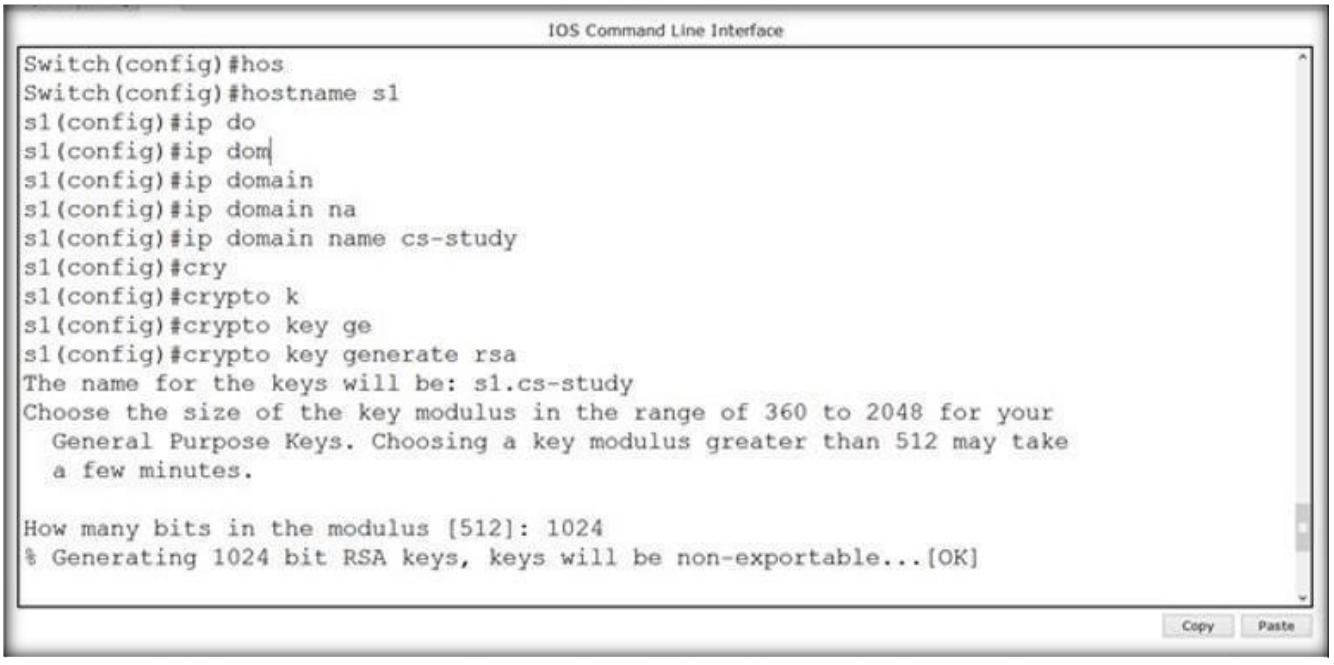


Fig-8: Creating Domain & RSA key

Commands continued.

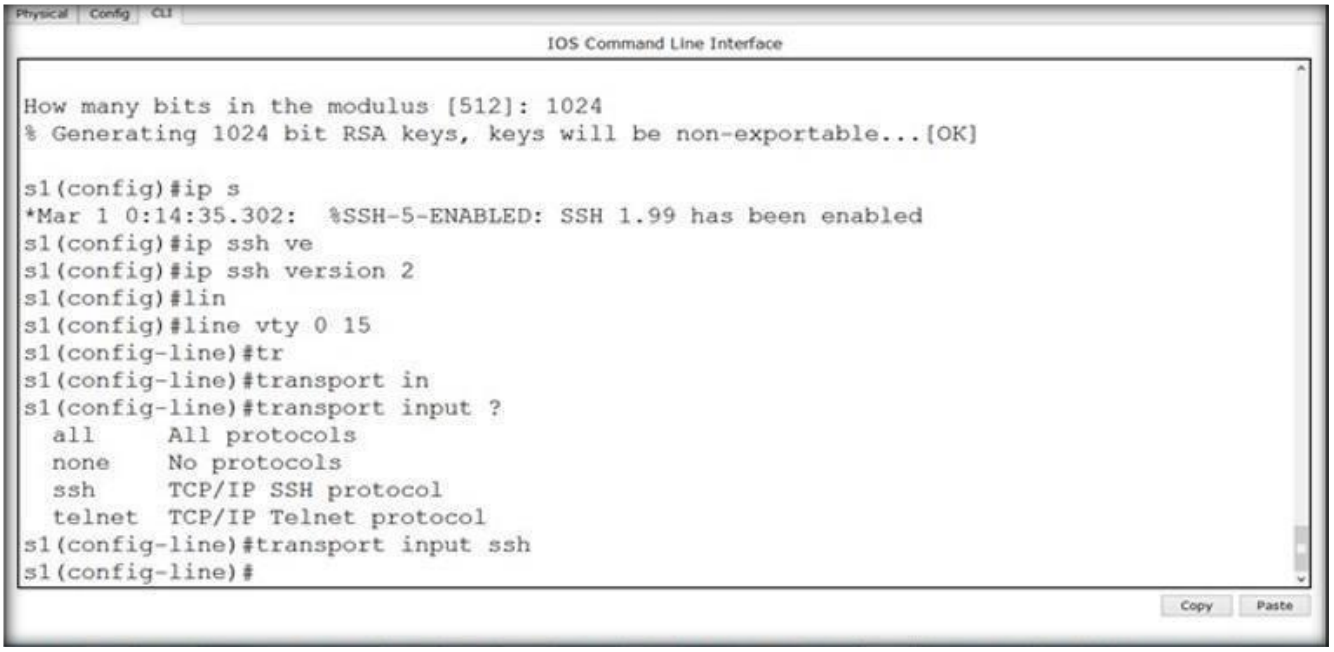


Fig-9: Creating SSH connection

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

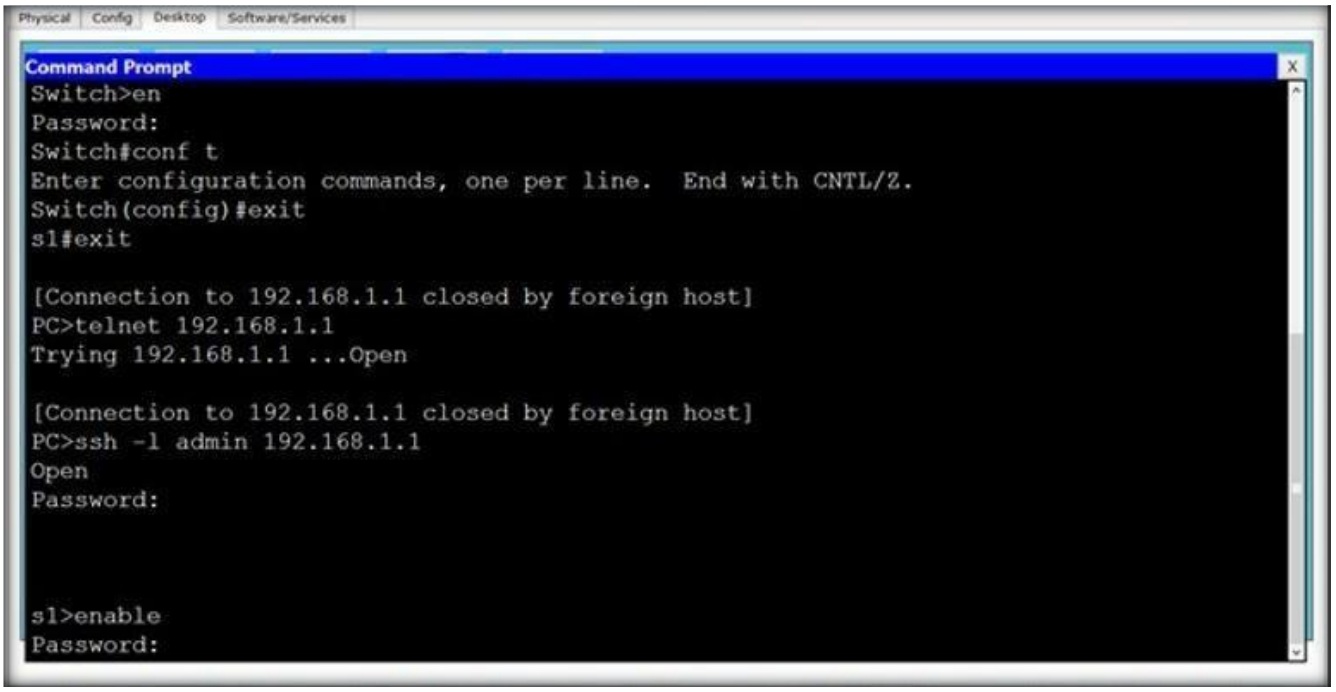


Fig-10: Checking SSH connection of Admin user

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

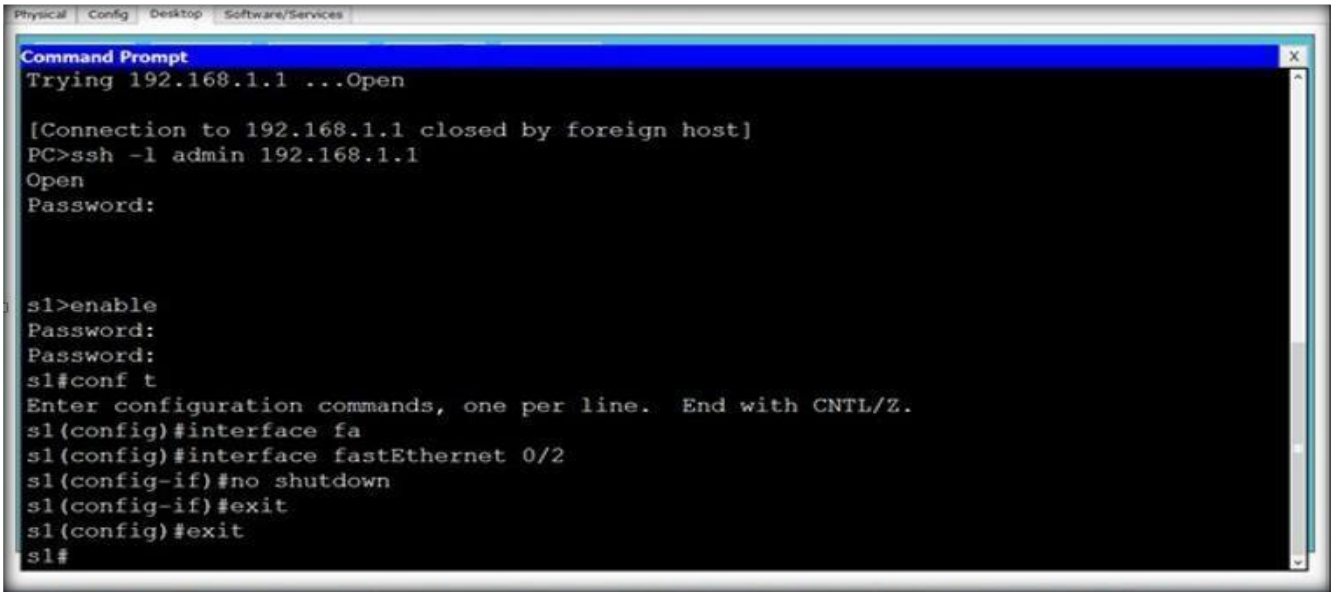


Fig-11: Moving to enable mode using specific computer

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

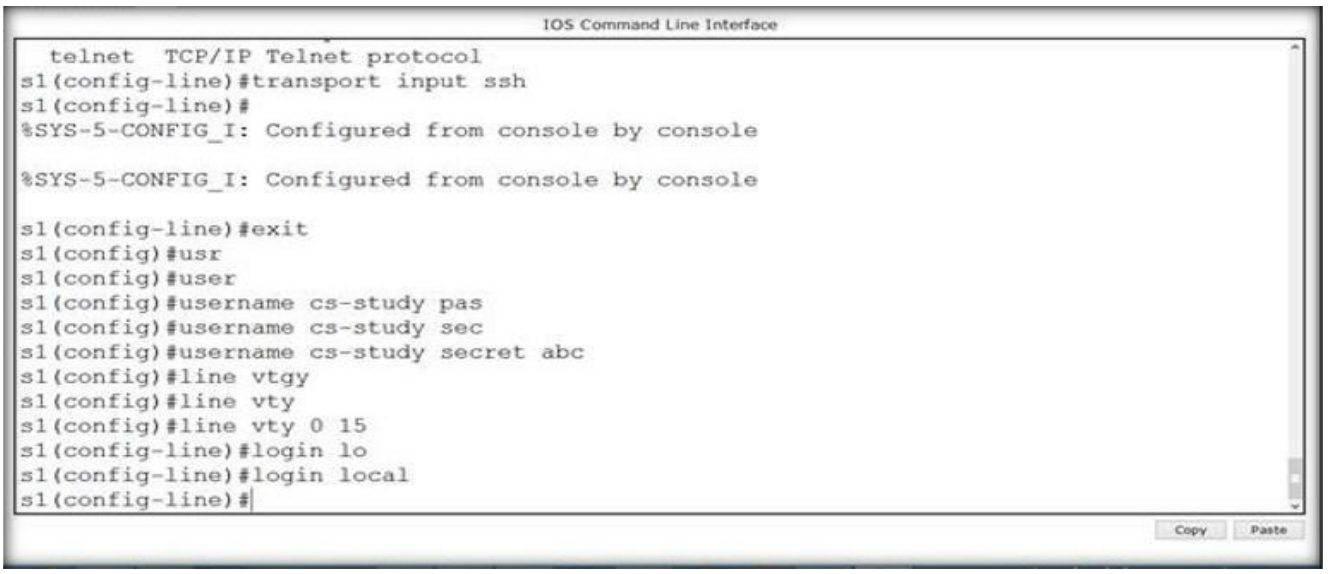


Fig-12: Creating Vty connection on specific domain

and from our pc as follows.

Fig-13: Checking the connection

Lab Exercise SSH & Telnet

Question # 1

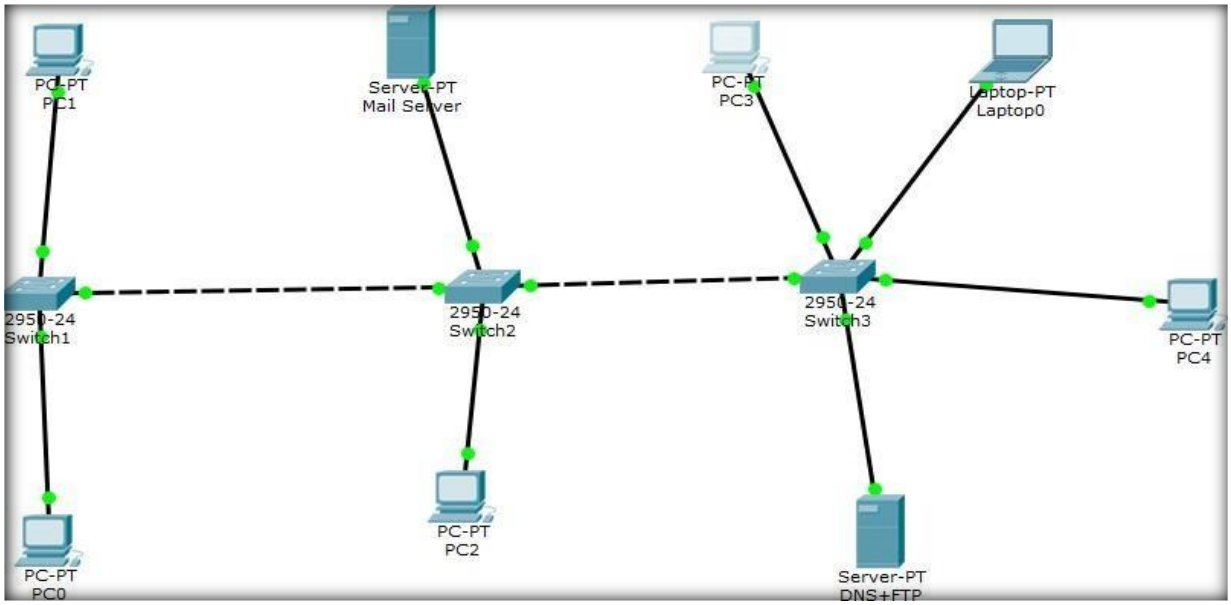


Fig-14a: Network Topology

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

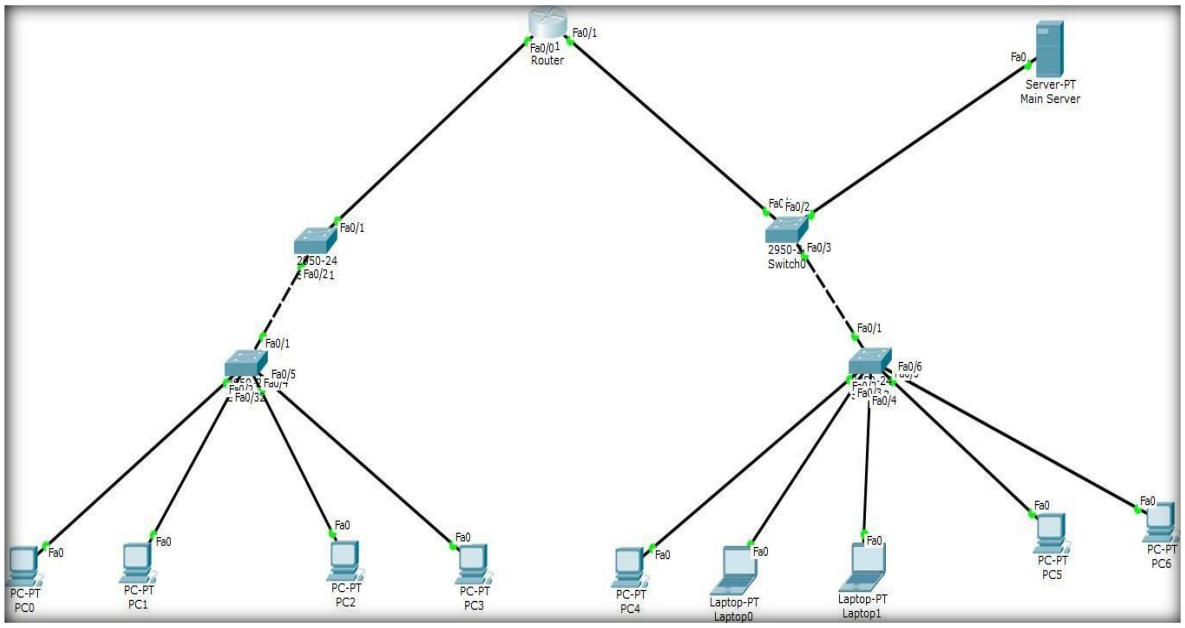


Fig-14b: Network Topology

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, itinitially 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 onrouter 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 oninterface Fa0/0 is implemented on router & for network on Fa0/1 we have DHCP server. First construct given network in packet tracer.

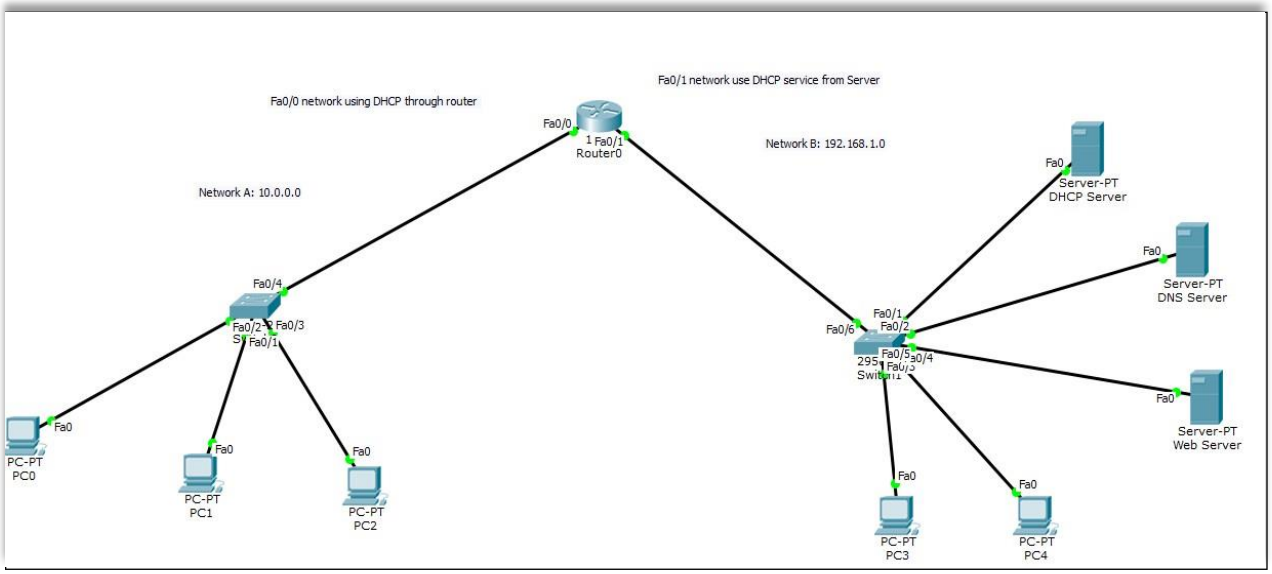


Fig-1: Network Topology

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

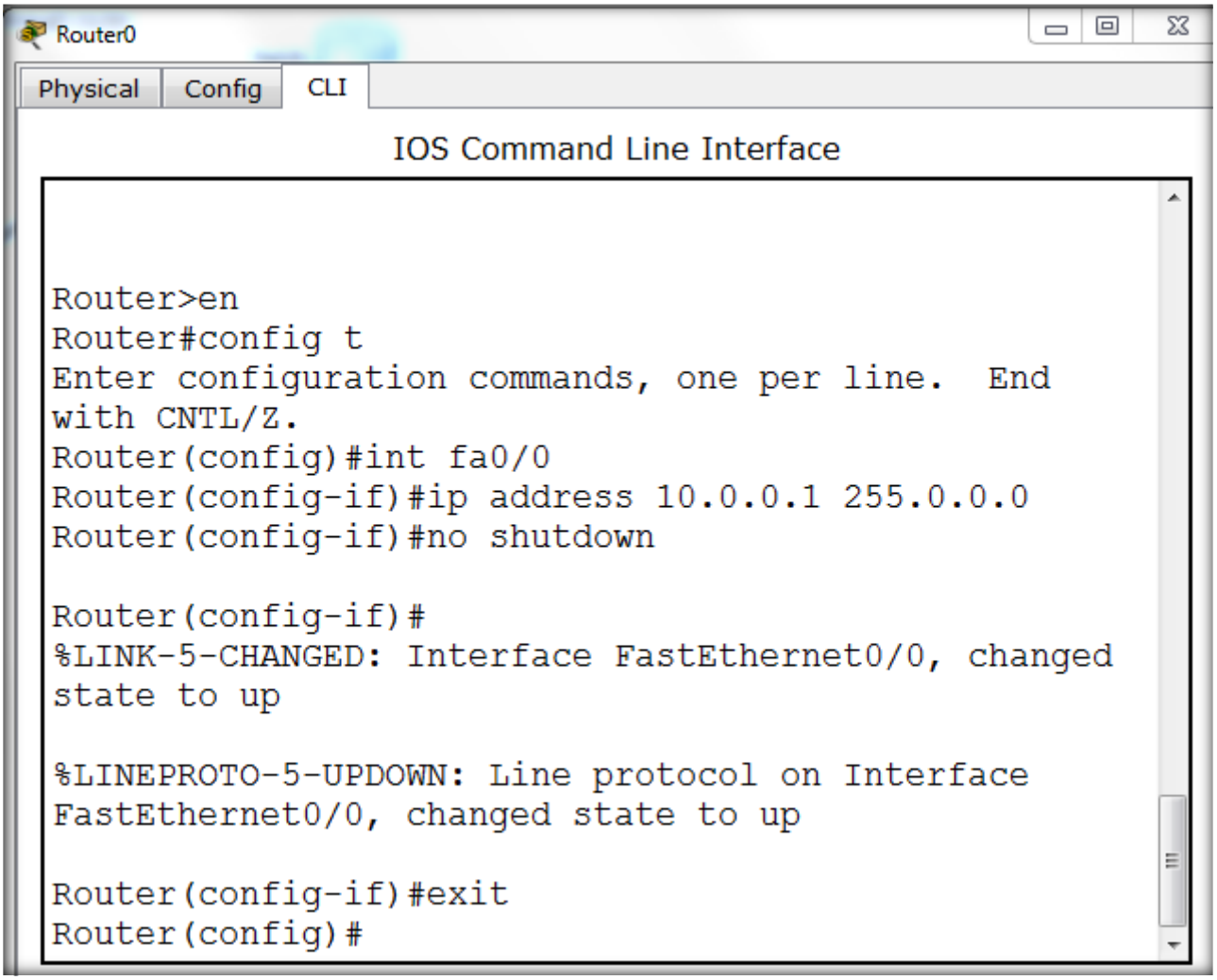


Fig-2: Assigning IP on Fa0/0 interface

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

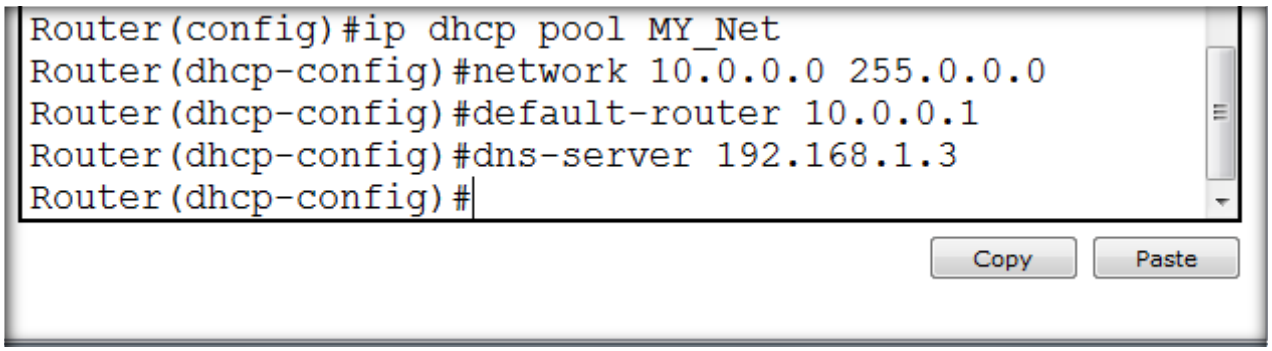


Fig-3: Implementing DHCP on router

Now assigning IP to PC0, PC1 & PC2

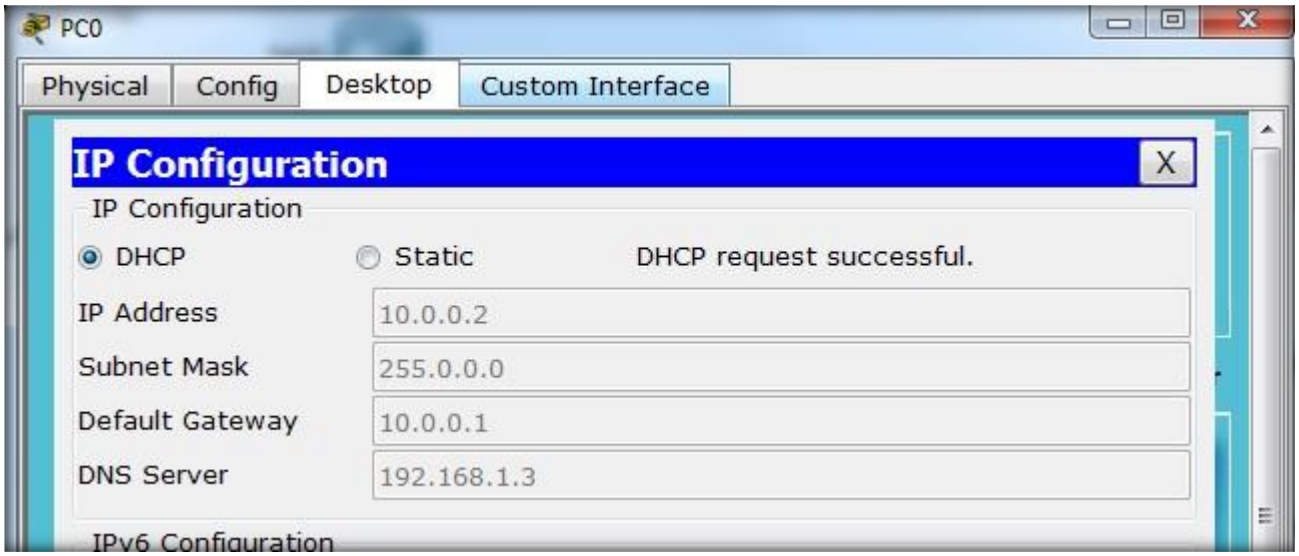


Fig-4: PC0 getting IP through DHCP

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

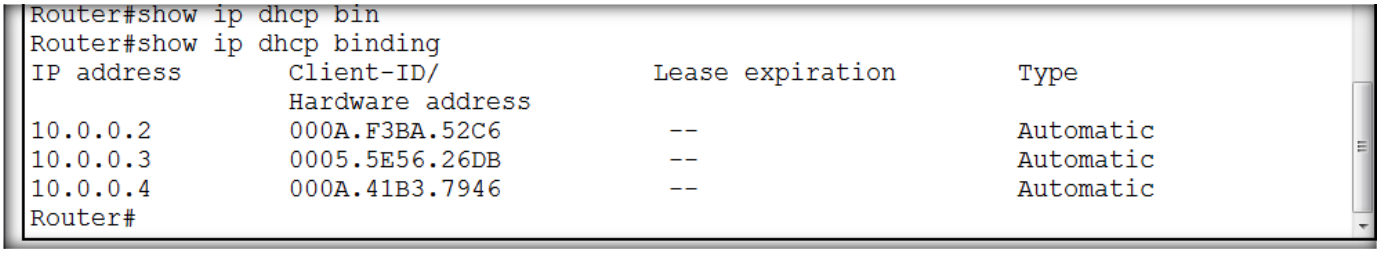


Fig-5: Checking DHCP binding status in router

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.

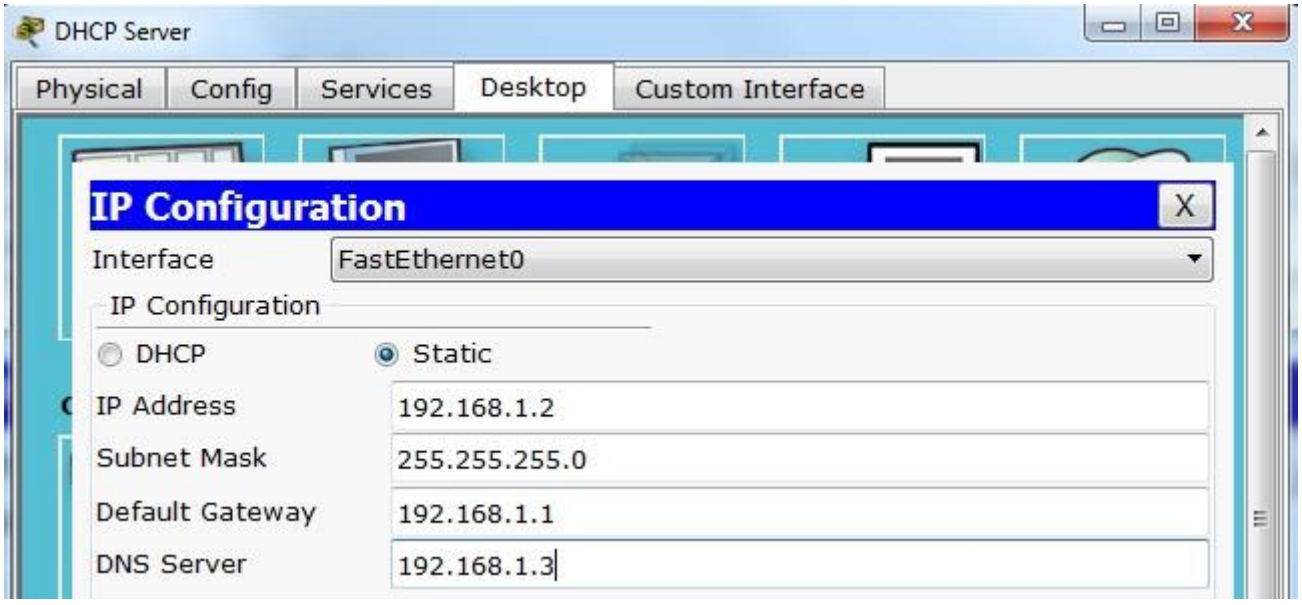


Fig-7: Assigning IP address to DHCP server

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

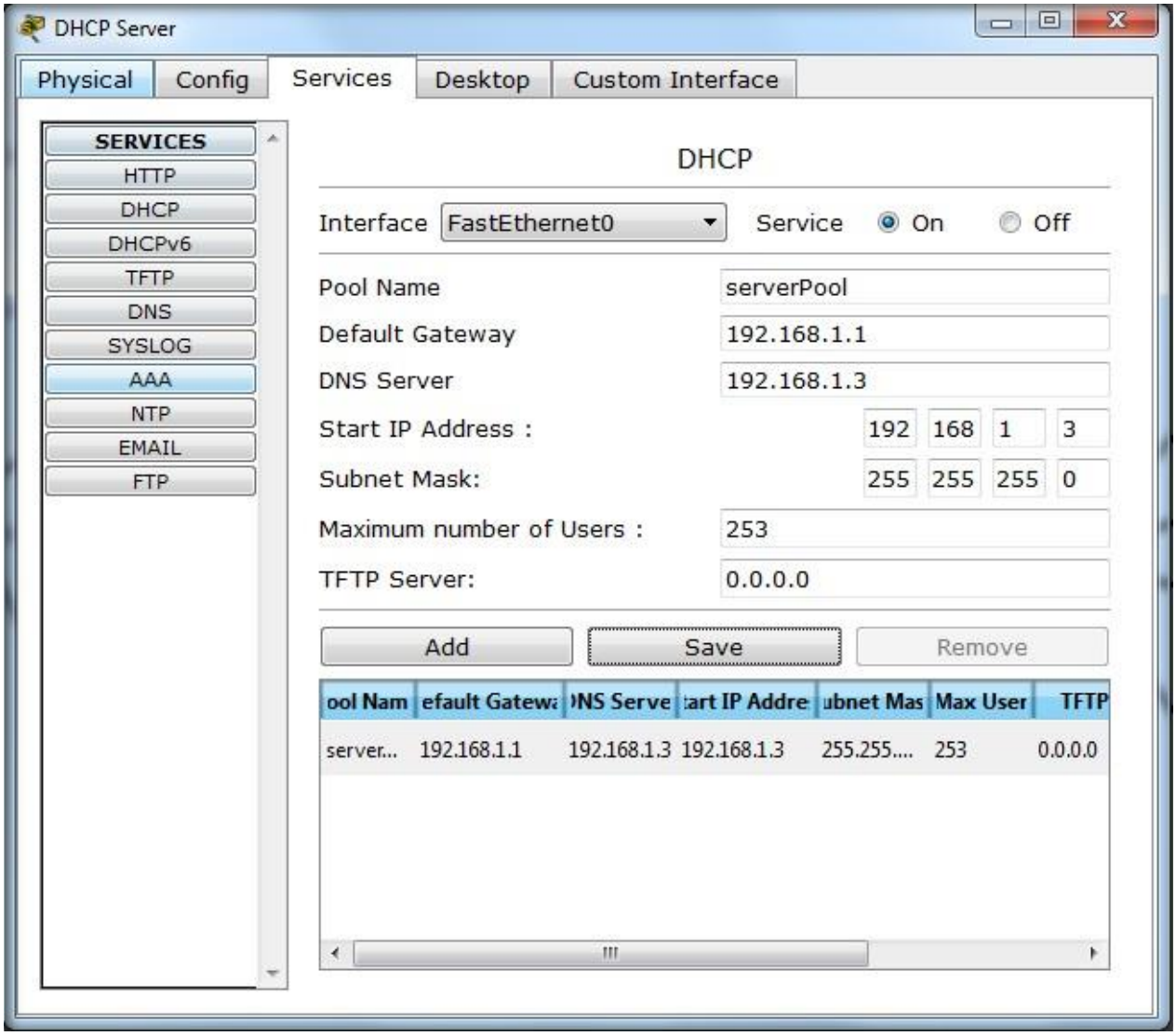


Fig-8: Configuring DHCP server

Now assigning IP to DNS server & PCs

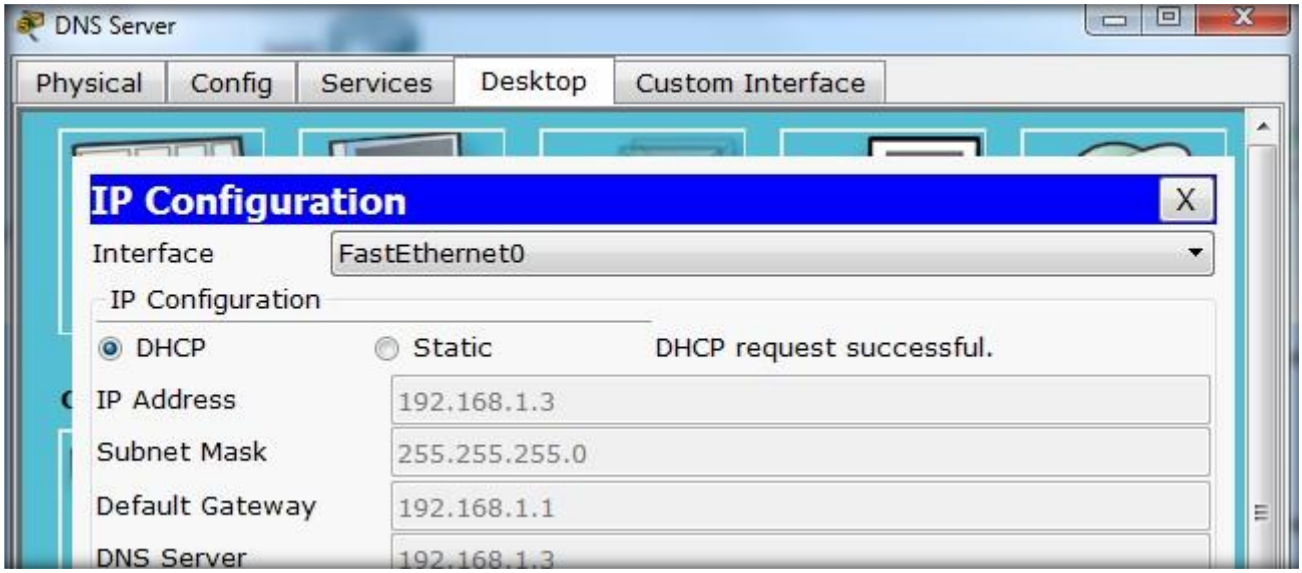


Fig-9: DNS server getting IP through DHCP server

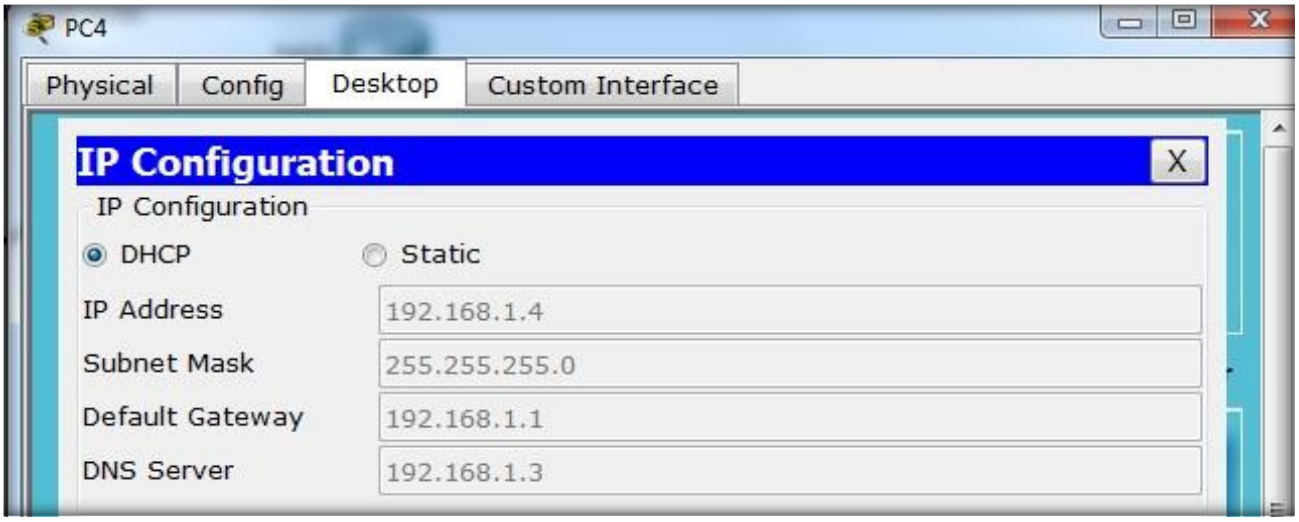


Fig-10: PC4 getting IP through DHCP server

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

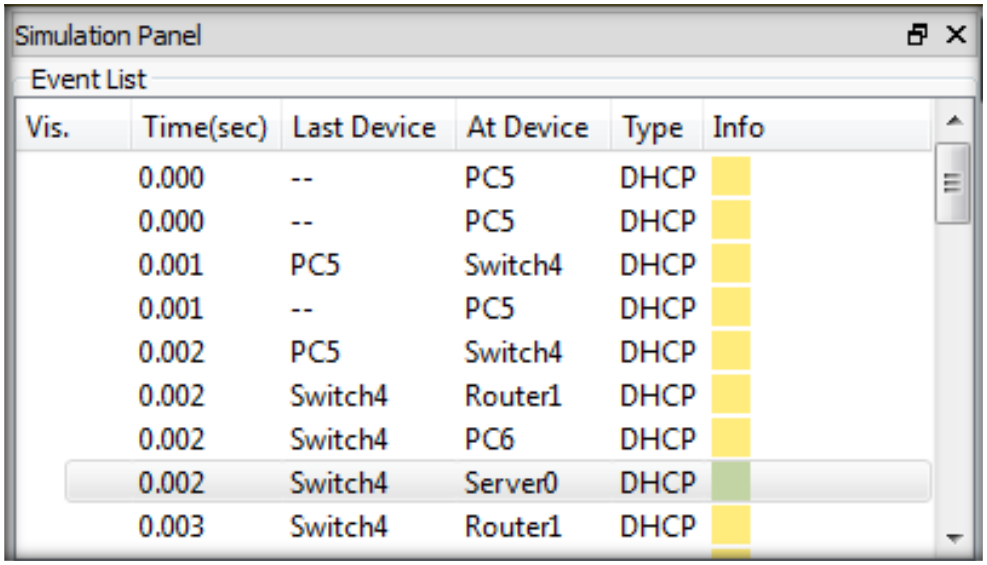


Fig-11: DHCP packets in simulation

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

Requesting

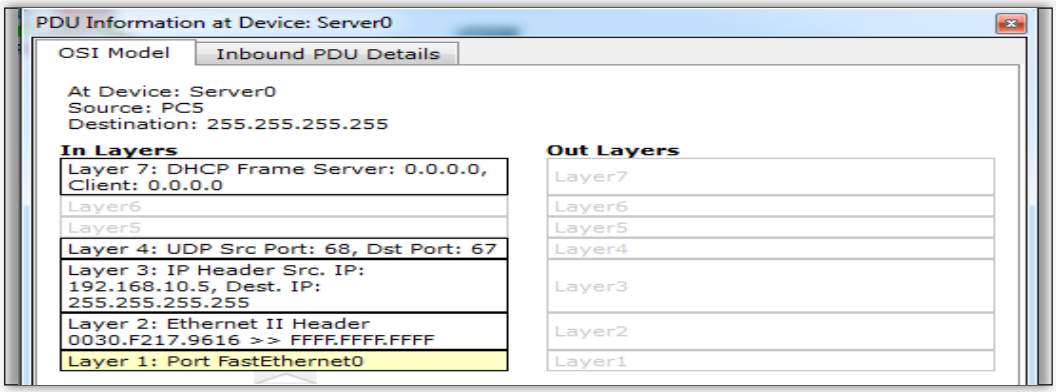


Fig-12: DHCP request packet

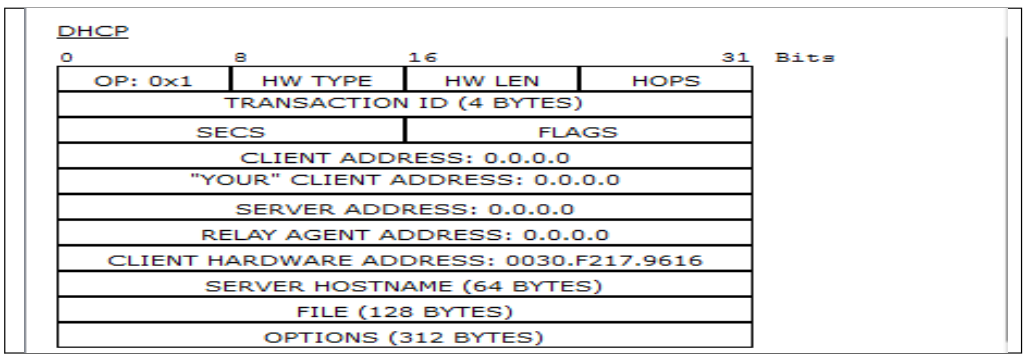


Fig-13: DHCP request packet heade

Leased

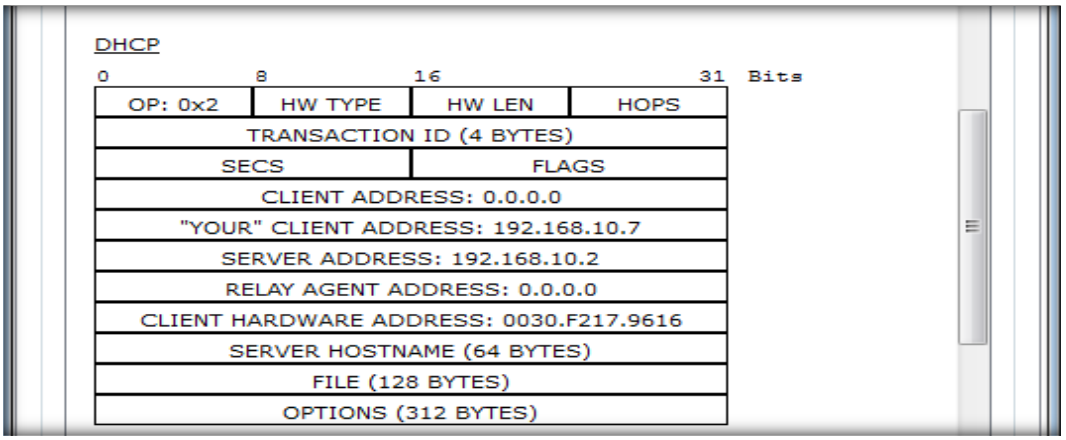


Fig-14: DHCP leased packet header

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).

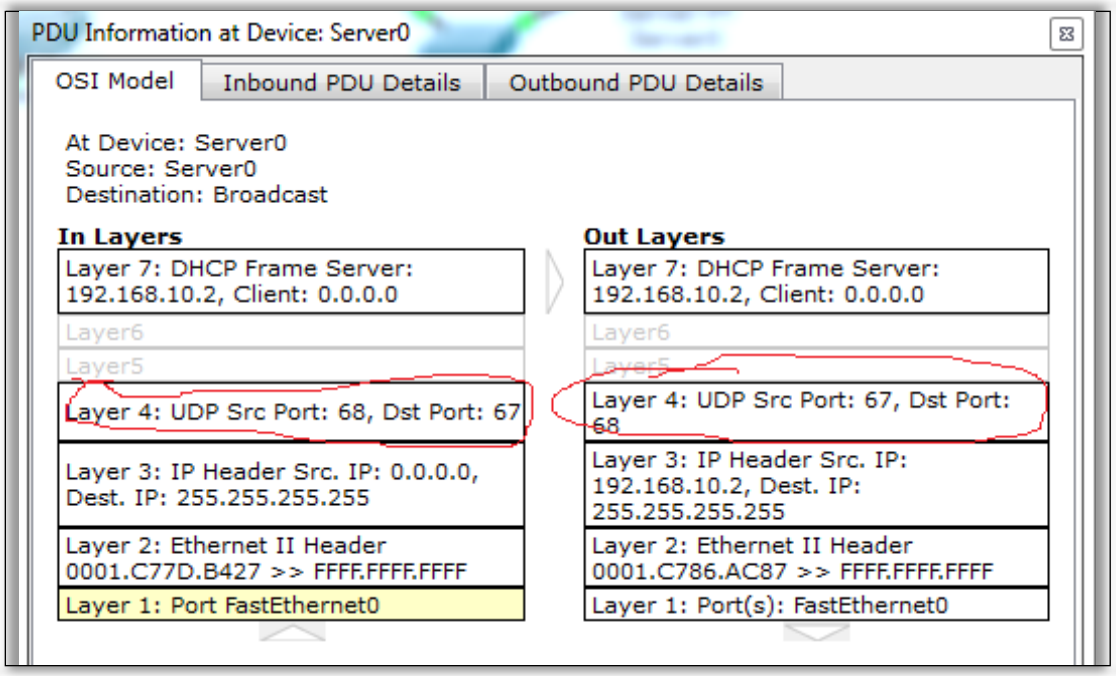


Fig-15: DHCP all OSI layers packets

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.

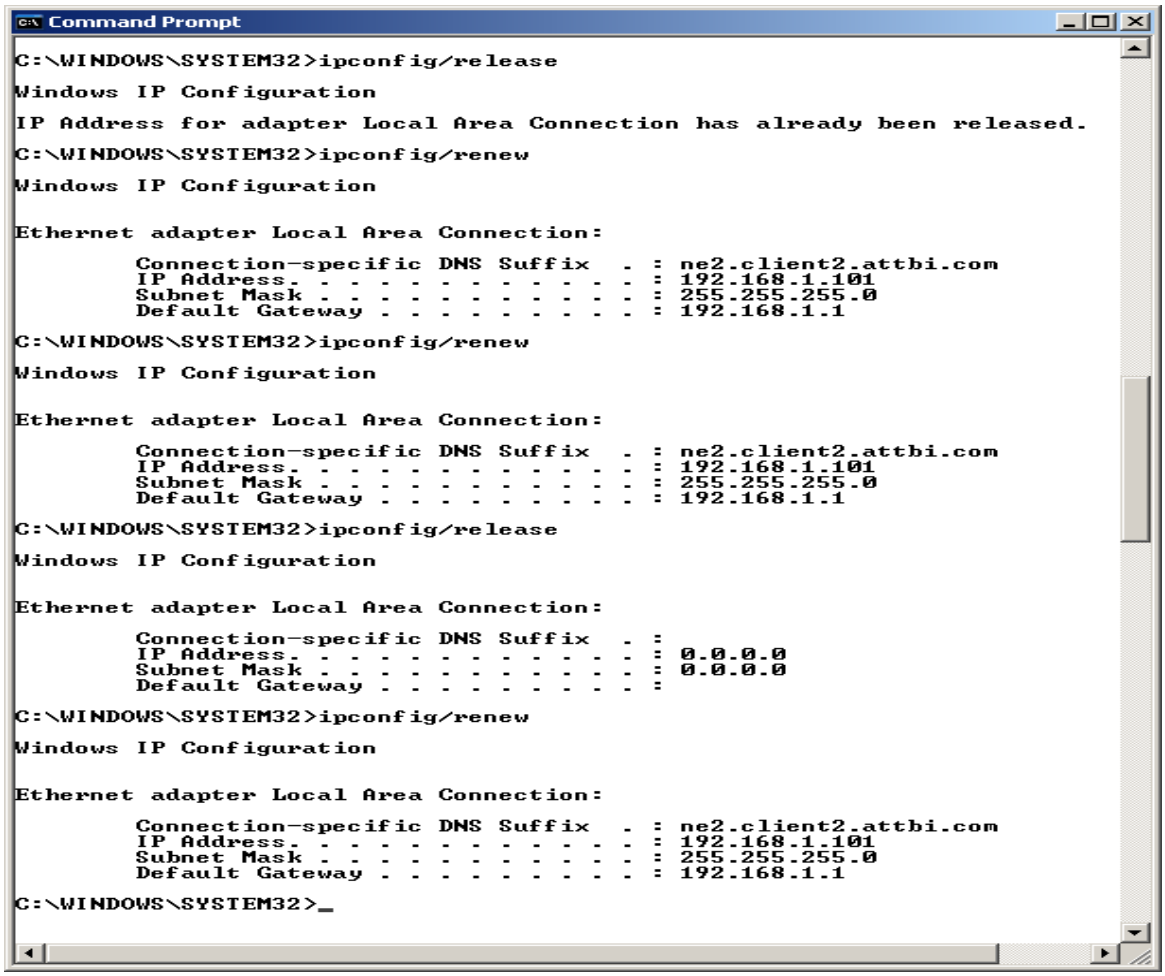


Fig-25: Command Prompt window showing sequence of ipconfig commands that you should enter.

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.

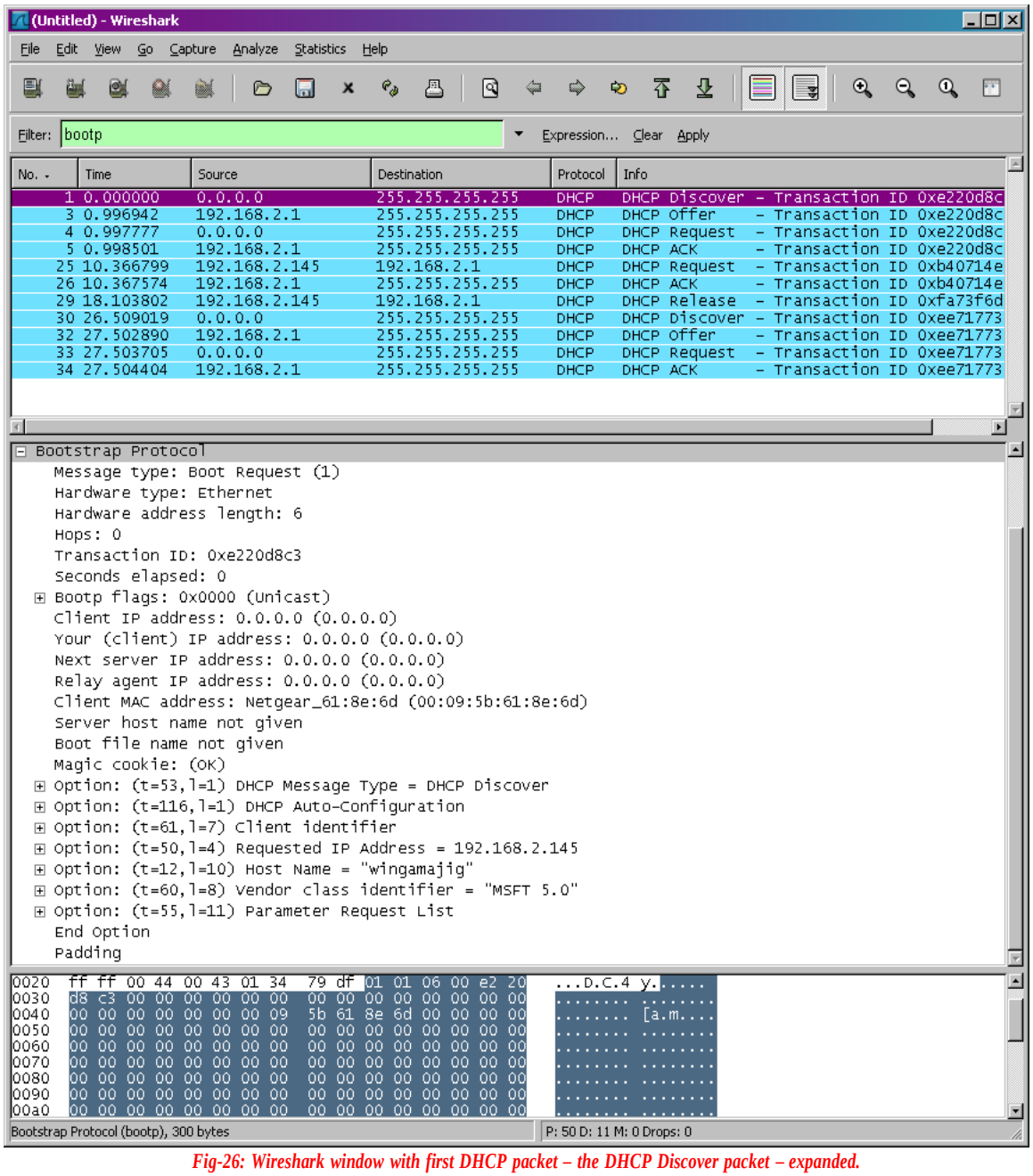


Fig-26: Wireshark window with first DHCP packet – the DHCP Discover packet – expanded.

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.

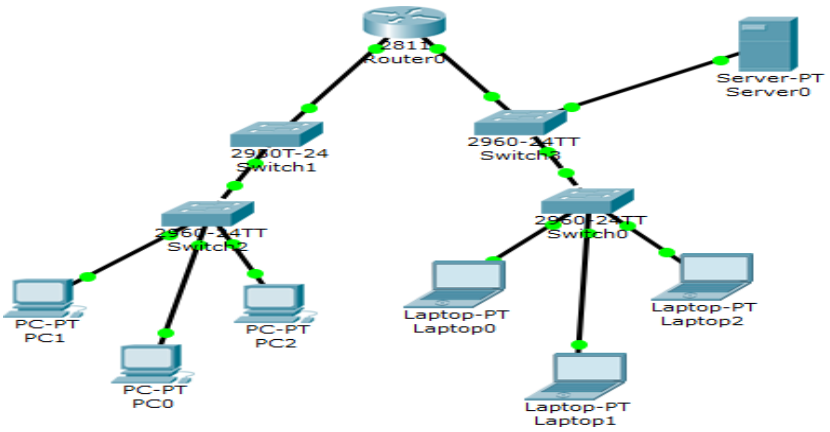


Fig-24: Network topology for task

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.

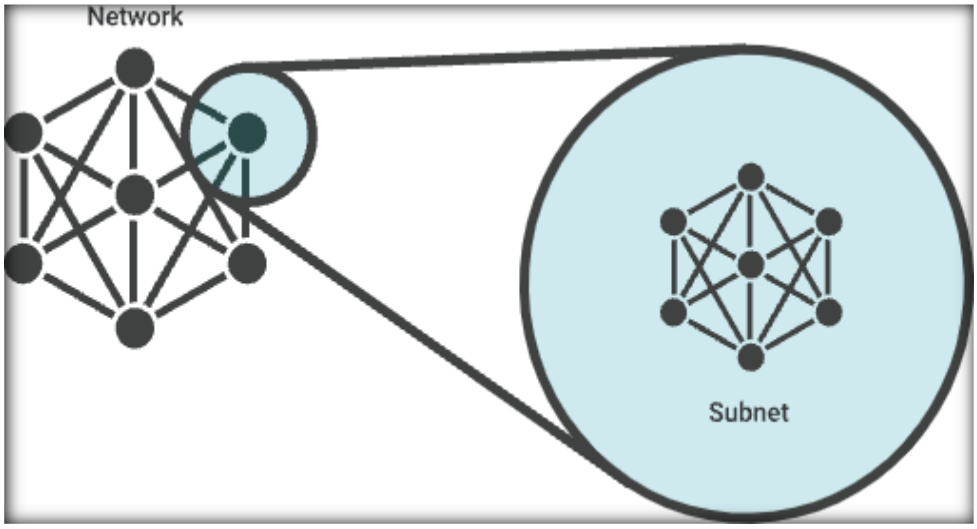


Fig-1: Subnet in network

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.

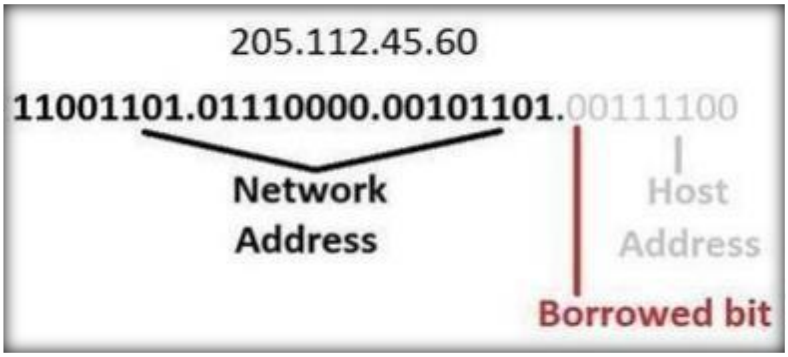


Fig-2: Bits concept of IP

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.

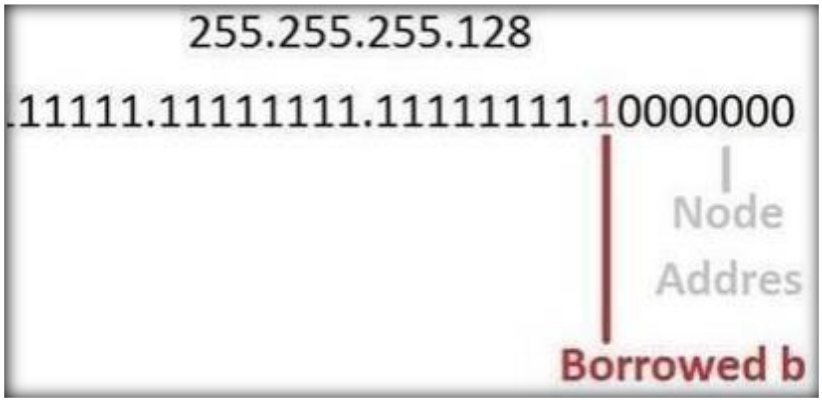


Fig-3: Borrowed bit from host section to network section

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

ass A Host/Subnet Table

lass 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

ass B Host/Subnet Table

lass 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

ass C Host/Subnet Table

lass 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 inreality 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 addressin 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 x 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 Address Blocks

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 scenarioin Cisco Packet Tracer.

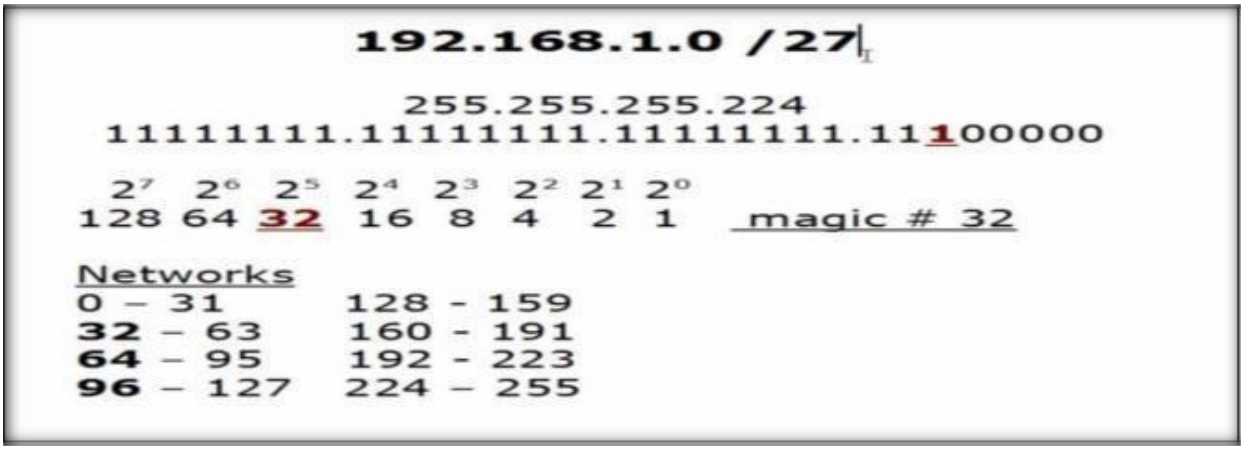


Fig-9: Logical Subnets

Calculation:

From above figure 3, we have:
Possible Subnets:2n = 23 =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.

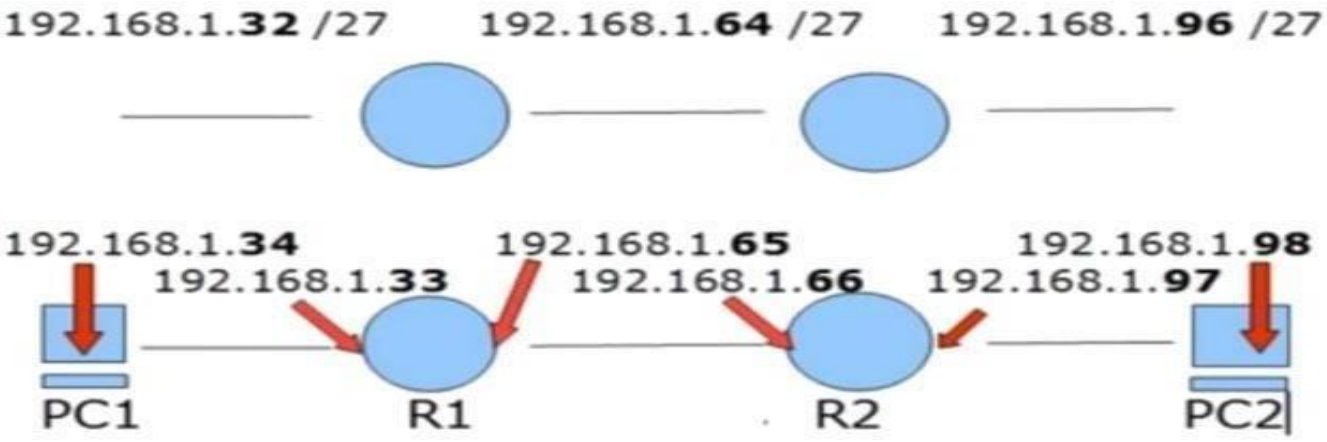


Fig-10: Scenario to implement

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.

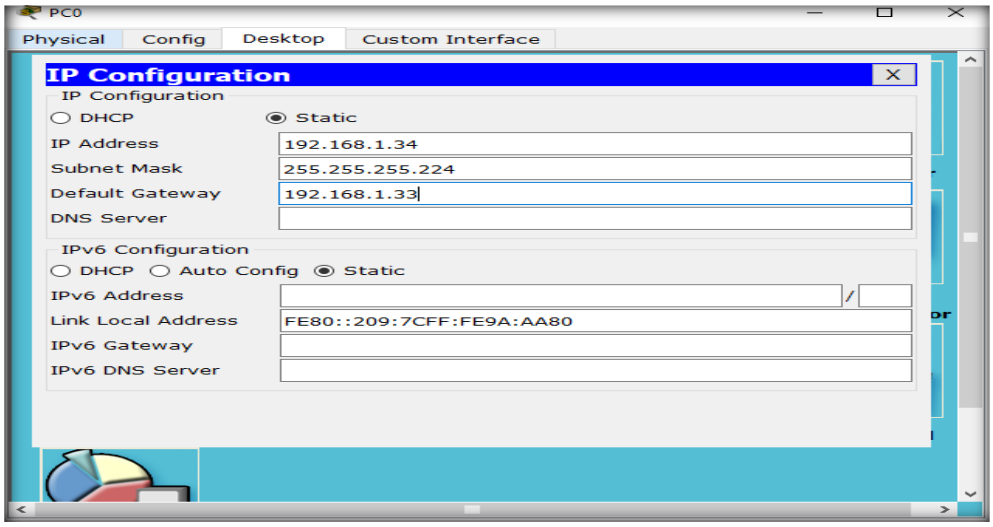


Fig-12: Assigning IP to PC0

Now configure the Interface FastEthernet0/0 of Router R0.

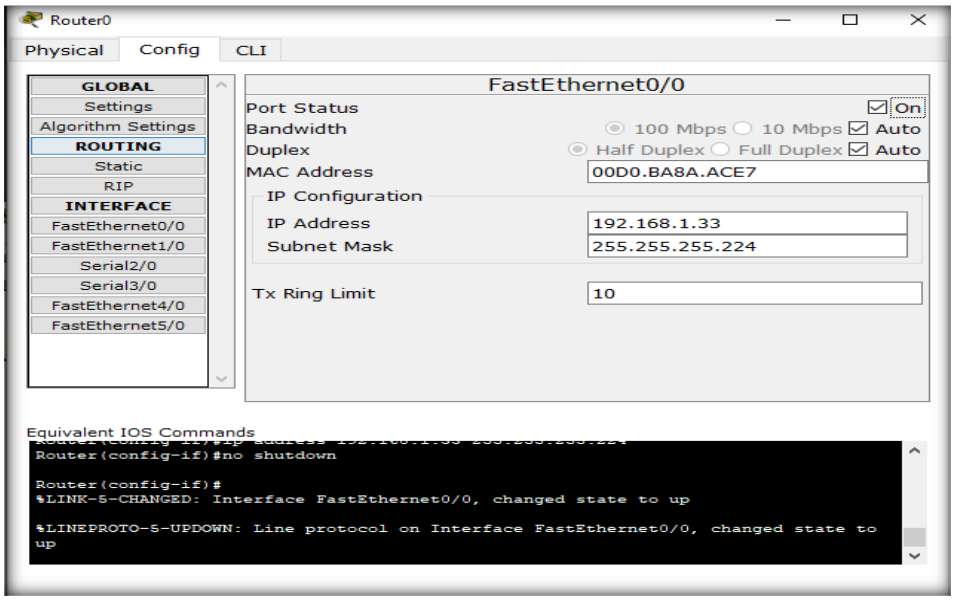


Fig-13: Interfacing Router 0 FastEthernet0/0

Configure the Interface Serial2/0 of Router R1

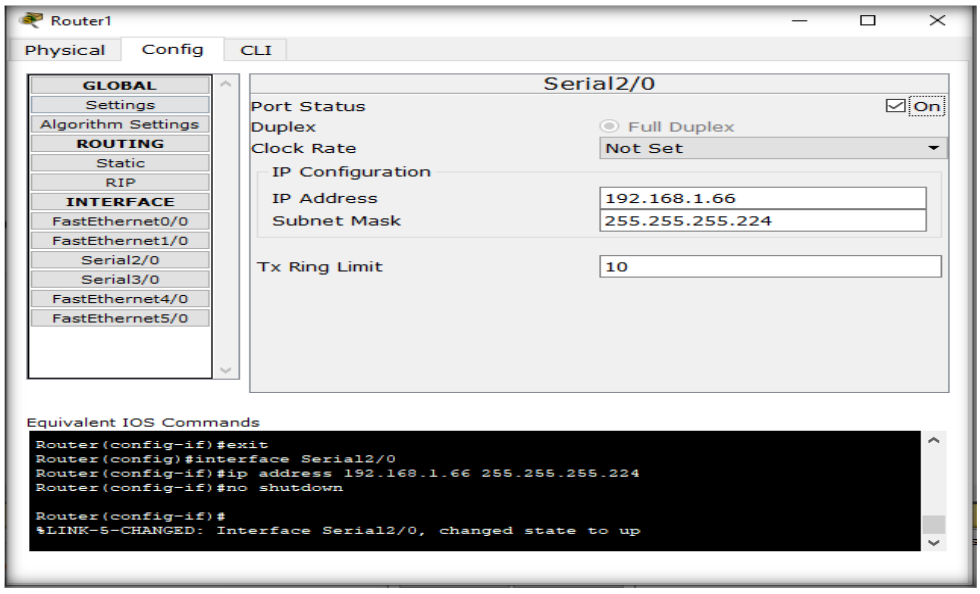


Fig-14: Interfacing Serial interface of Router 0

Now configuring PC1.

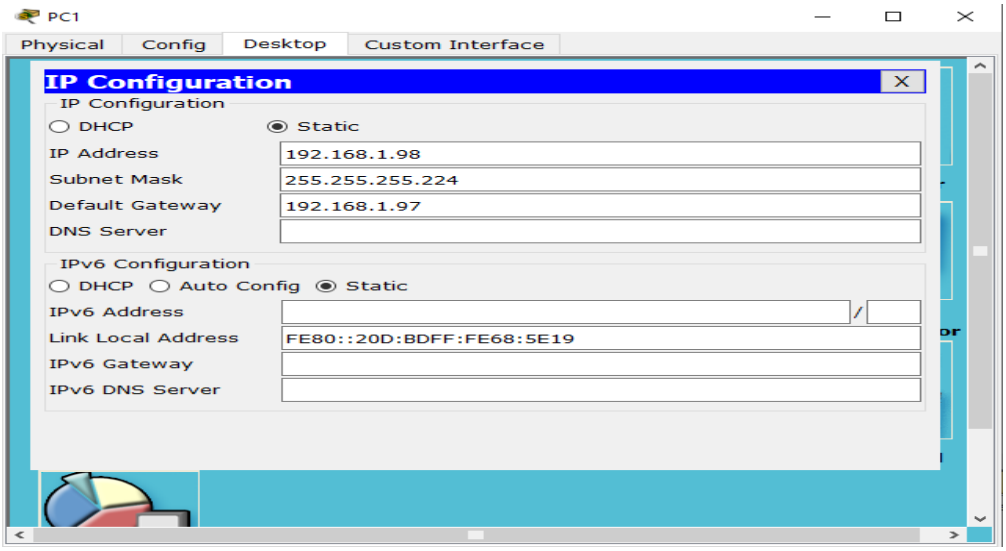


Fig-15: Assigning IP to PC1

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

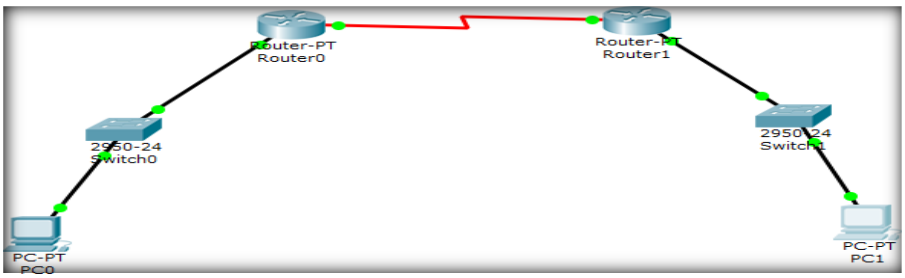


Fig-16: All links are up in network

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.

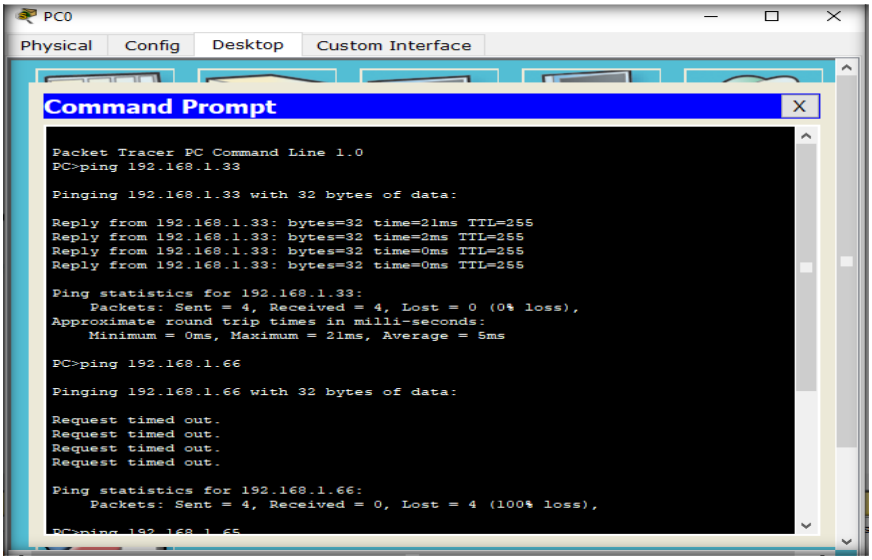


Fig-17: Ping result of before routing is applied

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

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

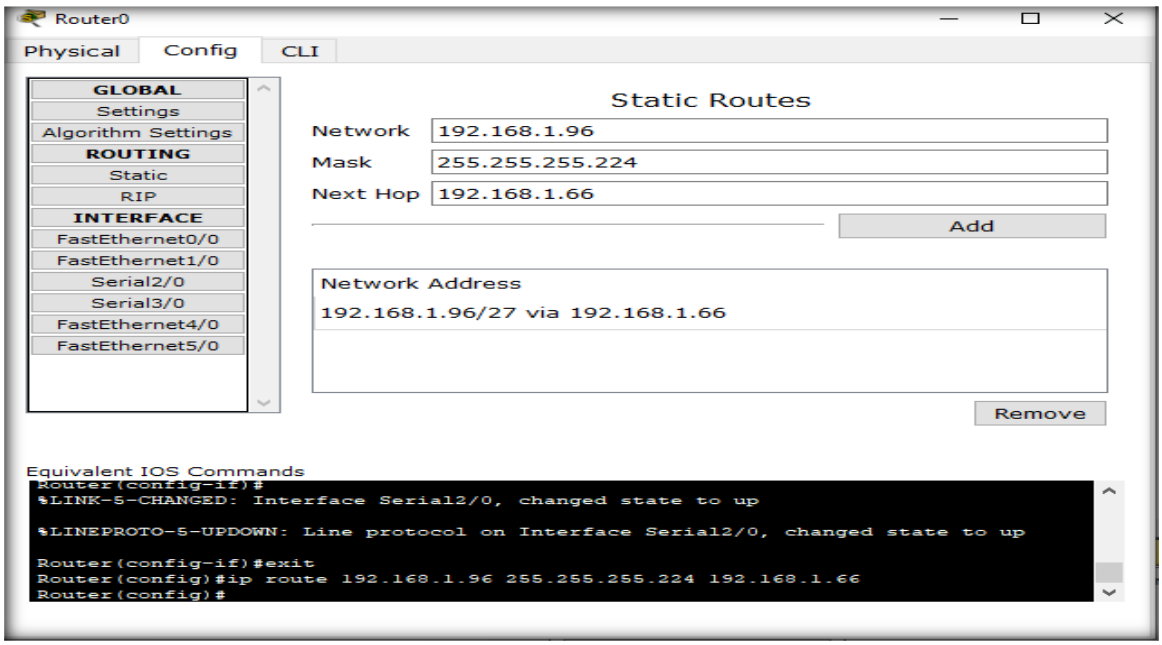


Fig-18: Applying Static Routing on Router 0

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

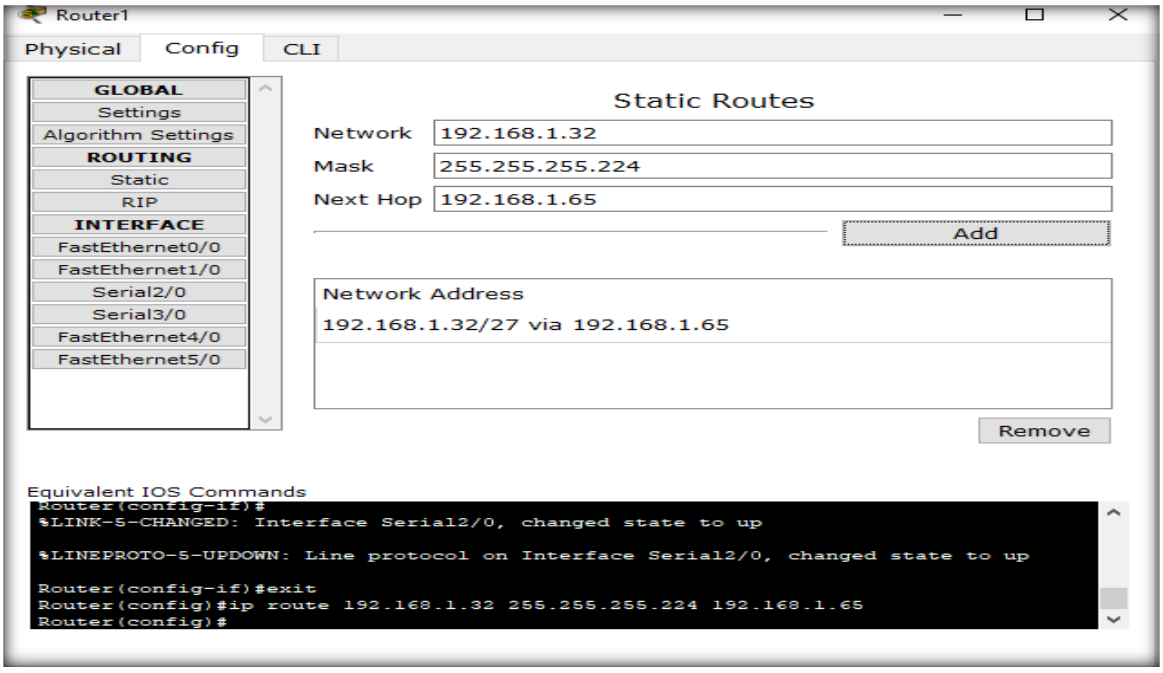


Fig-19: Applying Static Routing on Router 1

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

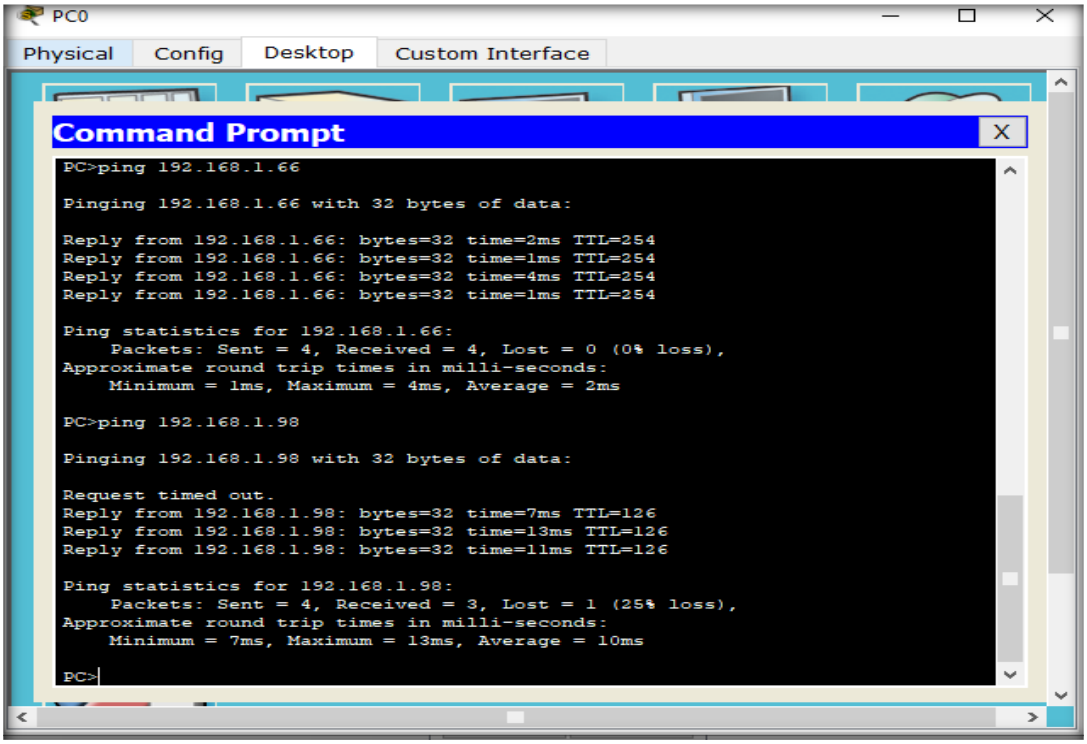


Fig-20: Ping is successful after static routing is applied

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

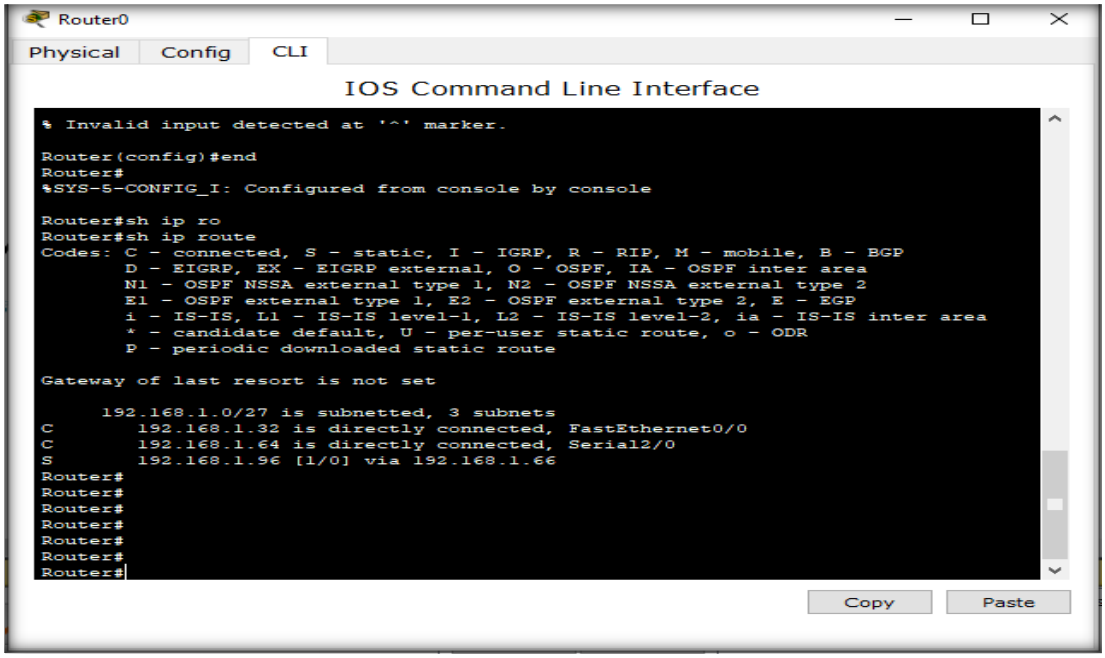


Fig-21: IP routes detail of router R0

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.

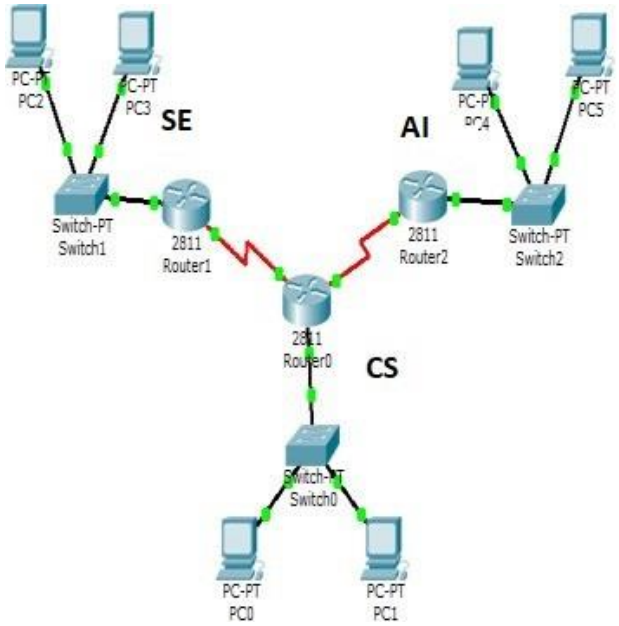
There are 4 departments with the following number of hosts:

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.



NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 9

Objective:

- Introduction to Routing protocol & Routed protocol
- Introduction to Routing Basis
- Introduction to Static Routing
- Default Routing
- Administrative Distance
- Classes of Routing protocol
- Introduction to Dynamic Routing
- Types of Dynamic Routing & its configuration (RIP & OSPF)

Routing Protocol

1. Introduction to Routing Protocol & Routed Protocol:

Routing protocols are mechanisms by which routing information is exchanged between routers so that routing decisions can be made. In the Internet, there are three types of routing protocols commonly used. They are: distance vector, link state, and path vector. You must understand the difference between a routing protocol and a routed protocol. A routing protocol is used by routers to dynamically find all the networks in the internetwork and to ensure that all routers have the same routing table. Basically, a routing protocol determines the path of a packet through an internetwork.

Examples of routing protocols are RIP, RIPv2, EIGRP, and OSPF.

Once all routers know about all networks, a routed protocol can be used to send user data (packets) through the established enterprise. Routed protocols are assigned to an interface and determine the method of packet delivery.

Examples of routed protocols are IP and IPv6.

2. Routing Basis:

The term routing is used for taking a packet from one device and sending it through the network to another device on a different network. Routers do not really care about hosts - they only care about networks and the best path to each network.

The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host.

If a network is not directly connected to the router, then the router must use one of two ways to learn how to get to the remote network: static routing, meaning that someone must hand-type all network locations into the routing table, or something called dynamic routing.

3. Introduction to Static Routing:

Before identifying the benefits of dynamic routing protocols, consider the reasons why network professionals use static routing. Dynamic routing certainly has several advantages over static routing; however, static routing is still used in networks today. In fact, networks typically use a combination of both static and dynamic routing.

Static routing has several primary uses, including:

- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from a stub network, which is a network with only one default route out and no knowledge of any remote networks.
- Accessing a single default route (which is used to represent a path to any network thatdoes not have a more specific match with another route in the routing table).

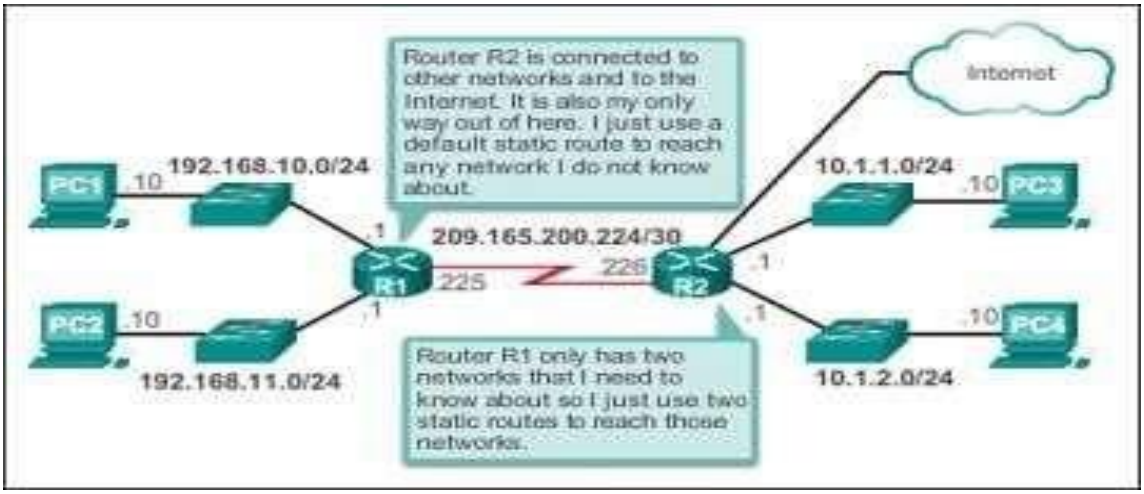


Fig-1: Simple scenario for static routing

Static routing is easy to implement in a small network. Static routes stay the same, which makesthem fairly easy to troubleshoot. Static routes do not send update messages and, therefore, require very little overhead.

Advantages	Disadvantages
Easy to implement in a small network.	Suitable for simple topologies or for special purposes such as a default static route.
Very secure. No advertisements are sent,unlike with dynamic routing protocols.	Configuration complexity increases dramatically as the network grows. Managingthe static configurations in large networks can become time consuming.
It is very predictable, as the route to thedestination is always the same.	If a link fails, a static route cannot reroute traffic. Therefore, manual intervention isrequired to re-route traffic.
No routing algorithm or update mechanisms are required. Therefore, extra resources (CPU and memory) are not required.	

Table-1: Advantages & Disadvantages of Static Routing

4. Default Route:

We use default routing to send packets with a remote destination network not in the routing table to the next-hop router.You should only use default routing on stub networks—those with only one exit path out of the network.

5. Configuration of Static & Default Route:

Using Cisco Packet Tracer software, we simulate the following network mentioned in figure 1 which has4 networks and 10 subnetworks and assign each host an IP. Also we have to assign an IP for each interfaceon the router. We assign an IP for the Router interface and start it up using the following commands:

Router(config)#interface fa0/0
Router(config-if)#ip address 192.168.1.129 255.255.255.192Router(config-if)#no shutdown

Where:
fa0/0: is the name of the interface.
192.168.1.129: is the IP address for interface fa0/0.
255.255.255.192: is the subnet mask being used on the network that connected directly to the interface.
no shutdown: to start up the interface.

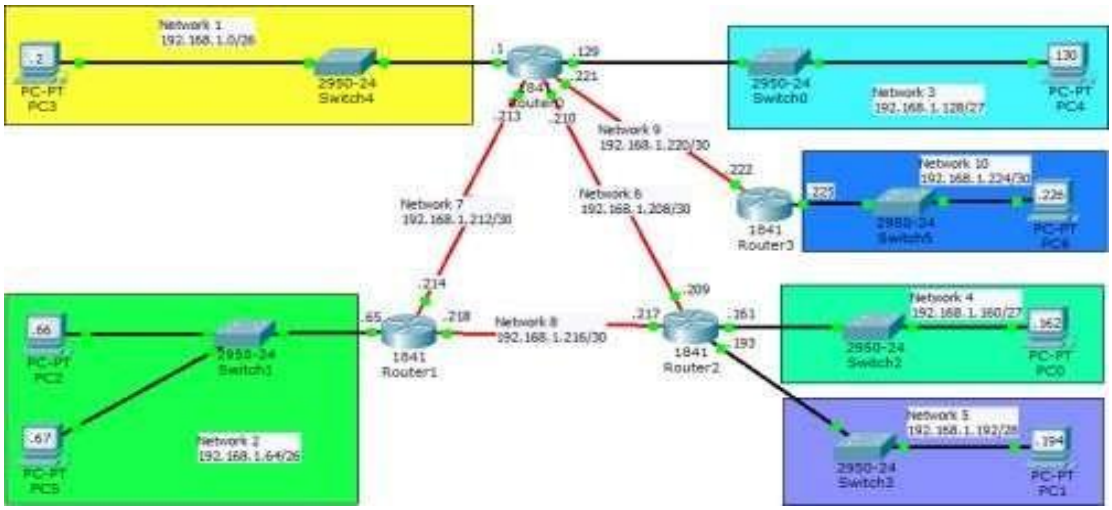


Fig-2: Network Topology

Run the same commands for all routers interfaces and assign each interface an appropriate IP/mask pair.

Now we start routing
Network 10 is connected directly to Router 3 and no other subnets is connected to Router 3, so we can configure default route on it using the following command:
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.221Where:
0.0.0.0: is the destination network IP [0.0.0.0 in case of default routing]
0.0.0.0: is the subnet mask being used on the destination network.
192.168.1.221: is the address of the next-hop router that will receive the packet and forward it to the destination network.

For the other routers, we cannot implement default routing since each of them is connected to more than one network. In this case, we use static routing. We can configure static route on router0 as follow:

Router(config)#ip route 192.168.1.64 255.255.255.192 192.168.1.214

Where:
192.168.1.64: is the destination network we want to send packets to it.
255.255.255.192: is the subnet mask being used on the destination network.
192.168.1.214: is the address of the next-hop router that will receive the packet and forward it to the destination network.

Configuring all other static routes on router0:

Router(config)#ip route 192.168.1.160 255.255.255.224 192.168.1.209
Router(config)#ip route 192.168.1.192 255.255.255.240 192.168.1.209
Router(config)#ip route 192.168.1.224 255.255.255.252 192.168.1.222

And do the same thing for the other routers. To review routing table on a router, use command "show ip route" as shown in figure 2

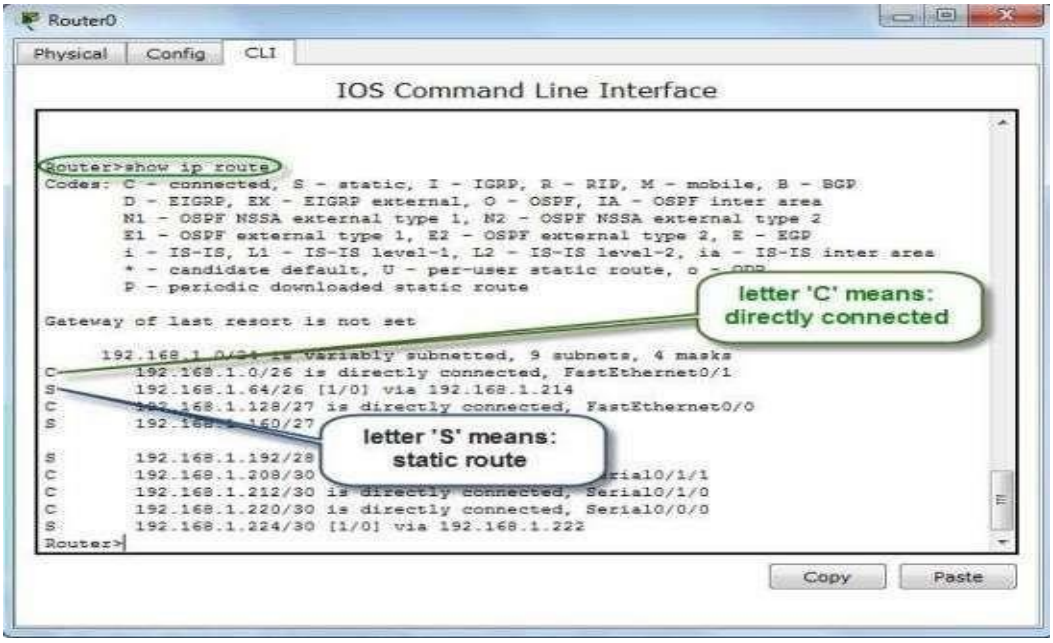


Fig-3: Routing Table

Alternatively, by using the Inspect tool from the right panel, and select "Routing Table" from the menu:

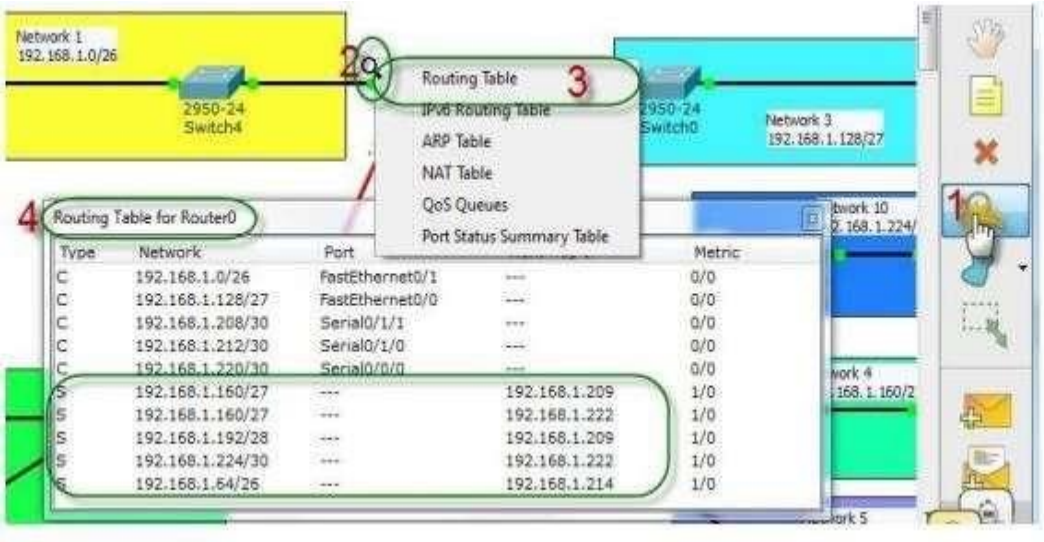


Fig-4: Alternate way of routing table

Another quick note: to mention that when (if) the packet is lost on the way back to the originating host, you will typically see a "Request timed out" message because it is an unknown error shown in figure 4. If the error occurs because of a known issue, such as if a route is not in the routing table on the way to the destination device, you will see a "Destination host unreachable" message as shown in figure 5. This should help you determine if the problem occurred on the way to the destination or on the way.

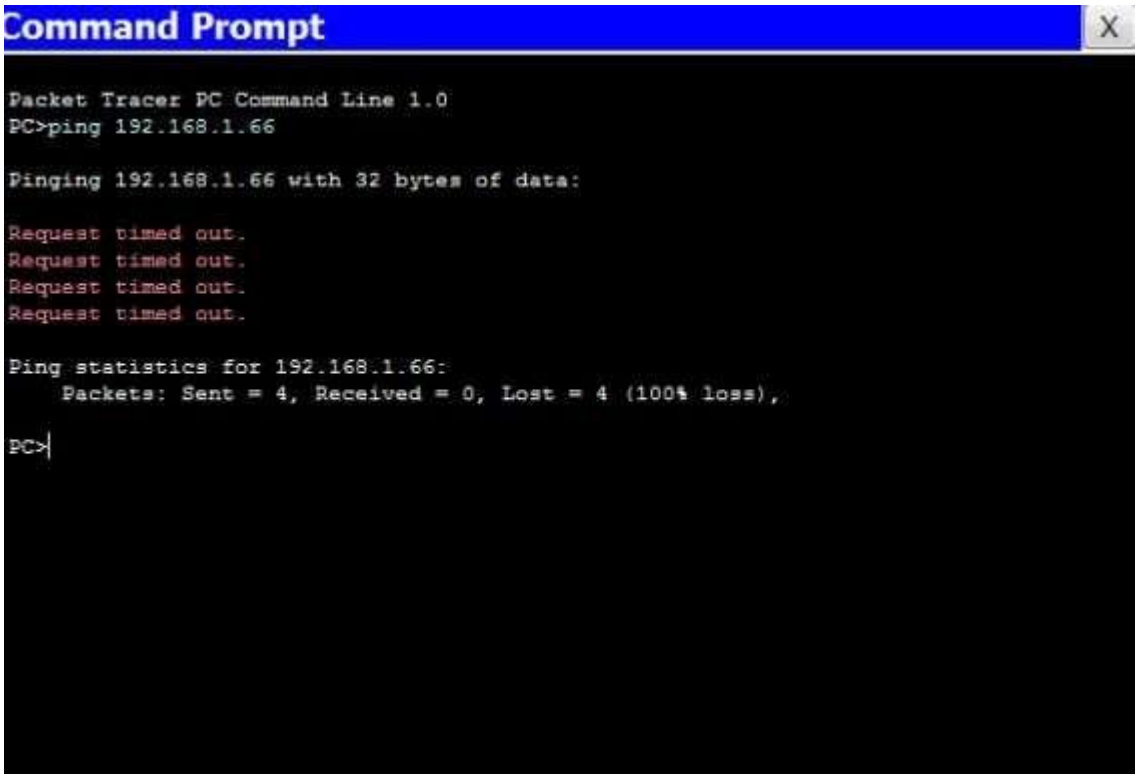


Fig-5: Request Timed out Error

Destination host unreachable message:

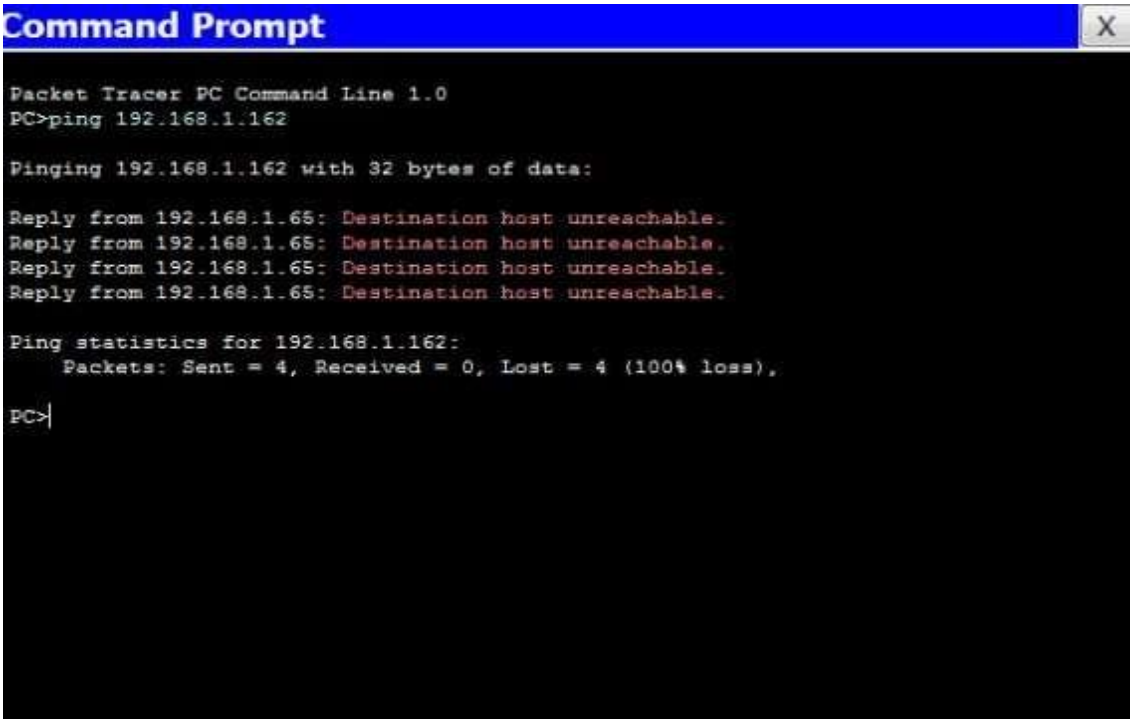


Fig-6: Destination Host Unreachable Error

6. Administrative Distances:

The administrative distance (AD) is used to rate the trustworthiness of routing information received on a router from a neighbor router. An administrative distance is an integer from 0 to 255, where 0 is the most trusted and 255 means no traffic will be passed via this route.

If a router receives two updates listing the same remote network, the first thing the router checks is the AD.

If one of the advertised routes has a lower AD than the other, then the route with the lowest AD will be placed in the routing table. If both advertised routes to the same network have the same AD, then routing protocol metrics (such as hop count or bandwidth of the lines) will be used to find the best path to the remote network. The advertised route with the lowest metric will be placed in the routing table.

But if both advertised routes have the same AD as well as the same metrics, then the routing protocol will load-balance to the remote network (which means that it sends packets down each link). Table 1 below shows default AD

Route Source	Default AD
Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP 1	120
External EIGRP	170

Table-2: Administrative Distances

The smaller the AD is, the more preferable to route is.

7. Classes of Routing Protocol:

Following are the classes of routing protocols:

Distance vector:

The distance-vector protocols find the best path to a remote network by judging distance. Each time a packet goes through a router, that's called a hop. The route with the least number of hops to the network is determined to be the best route. The vector indicates the direction to the remote network. Both RIP and IGRP are distance-vector routing protocols. They send the entire routing table to directly connected neighbors.

Link state:

In link-state protocols, also called shortest-path-first protocols. Link-state routers know more about the internetwork than any distance vector routing protocol. OSPF is an IP routing protocol that is completely link state. Link-state protocols send updates containing the state of their own links to all other routers on the network.

Hybrid:

Hybrid protocols use aspects of both distance vector and link state—for example, EIGRP. There's no set way of configuring routing protocols for use with every business. This is something you really have to do on a case- by-case basis. If you understand how the different routing protocols work, you can make good, solid decisions that truly meet the individual needs of any business.

8. Introduction to Dynamic Routing:

Dynamic routing is when protocols are used to find networks and update routing tables on routers. True, this is easier than using static or default routing, but it'll cost you in terms of router CPU processes and bandwidth on the network links.

A routing protocol defines the set of rules used by a router when it communicates routing information between neighbor routers. The routing protocol includes Routing Information Protocol (RIP) versions 1 and 2, with a bit of Interior Gateway Routing Protocol (IGRP) thrown in.

Two types of routing protocols are used in internetworks: interior gateway protocols (IGPs) and exterior gateway protocols (EGPs).

IGPs are used to exchange routing information with routers in the same autonomous system (AS). An AS is a collection of networks under a common administrative domain, which basically means that all routers sharing the same routing table information are in the same AS.

EGPs are used to communicate between ASes. An example of an EGP is Border Gateway Protocol (BGP), which is beyond the scope of our lab.

9. Dynamic Routing Types & Their Configuration:

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a true distance-vector routing protocol. RIP sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it's inefficient on large networks with slow WAN links or on networks with a large number of routers installed.
What will happen using RIP?

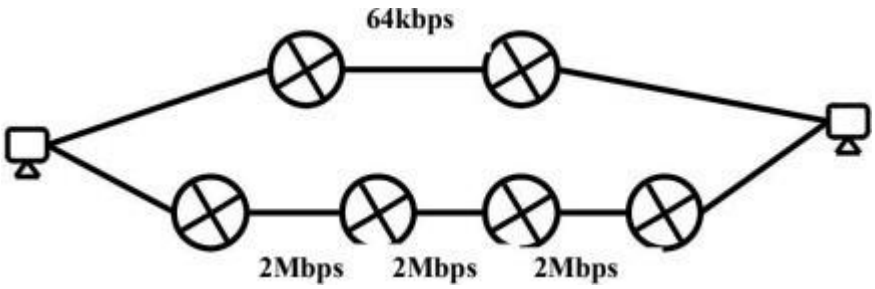


Fig-7: Topology with RIP

RIP Versions

	RIP V1	RIP V2
AD	**120**	**120**
Metric	**Hope count**	**Hope count**
Sending update per sec	**30 sec**	**30 sec**
Sending updates using	**Broadcast**	**multicast**
VLSM\CIDR	**Not supported**	**Supported**

Table-3: RIP V1 vs V2 characteristics

RIP practical part

RIPV1

Lab_A#config t Lab_A(config)#router rip
Lab_A(config-router)#network 192.168.10.0 (only net without mask)
Lab_A(config-router)#passive-interface serial 0/0 (This command prevents RIP update broadcasts from being sent out a specified interface, yet that same interface can still receive RIP updates.)

RIPV2

RIPv2 is considered classless because subnet information is sent with each route update

Lab_C(config)#router rip
Lab_C(config-router)#network 192.168.40.0
Lab_C(config-router)#network 192.168.50.0
Lab_C(config-router)#version 2

Open Shortest Path First (OSPF)

OSPF works by using the Dijkstra algorithm. First, a shortest path tree is constructed, and then the routing table is populated with the resulting best paths. OSPF converges quickly, although perhaps not as quickly as EIGRP, and it supports multiple, equal-cost routes to the same destination. Like EIGRP, it does support both IP and IPv6 routed protocols.

OSPF provides the following features:

- Consists of areas and autonomous systems
- Minimizes routing update traffic
- Allows scalability
- Supports VLSM/CIDR
- Has unlimited hop count
- Allows multi-vendor deployment (open standard)

OSPF Terminology

- Router ID
- Neighbor
- Adjacency
- Hello protocol
- Neighborship database
- Link State Advertisement
- Topological database
- OSPF areas
- Loopback Address
- Link costs

OSPF Practical Part

Lab_A#config t Lab_A(config)#router ospf 1

1: is OSPF process number: out of scope for CCNA, range: <1-65535>

Lab_A(config-router)#network 10.0.0.0 0.255.255.255 area 0 0.255.255.255 : an example of wildcard

Wildcard

The wildcard mask can be configured as the inverse of a subnet mask. For example, IP 172.16.1.16/28 network. The subnet mask for this interface is /28 or 255.255.255.240. The inverse of the subnet mask results in the wildcard mask.

255.255.255.255
- 255.255.255.240 (Subtract the subnet mask)
---

0. 0. 0. 15 Wildcard mask

255.255.255.255
255.255.255.0 (Subtract the subnet mask)
---

0. 0. 0. 255 Wildcard mask

255.255.255.255
255.255.0.0 (Subtract the subnet mask)
---

0. 0. 255. 255 Wildcard mask

10. Lab Exercise:

Q1: Implement Subnetting with IP address of XX.XX.0.0/24. where xx is your roll no same are midterm. Then assign ip address in such a way that very less ip address should waste. Last run RIP routing protocol in such a way that all devices can communicate easily. What will be the administrative distance of the routing? Use figure 8 for your reference.

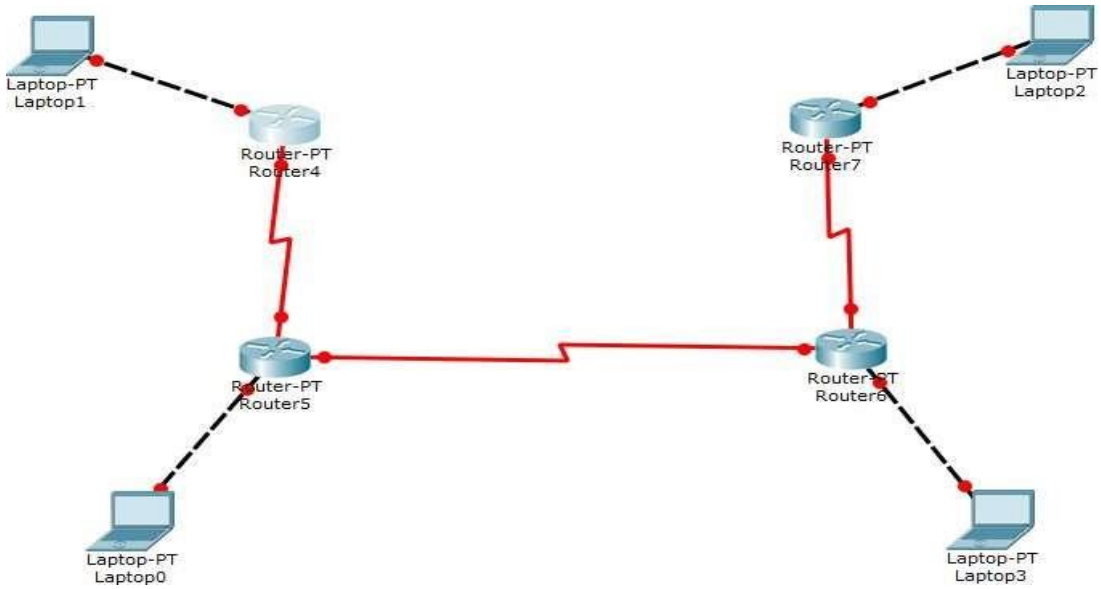


Fig-8: Network Topology for Q1

Q2: Implement Subnetting with IP address of 172.168.1.0/24. All the assignment of IP should be done dynamically in such a way that there should be less waste of Ips. Run the dynamic routing protocol with less administrative distance. What will be the administrative distance of the routing? Use Figure 9 as reference.

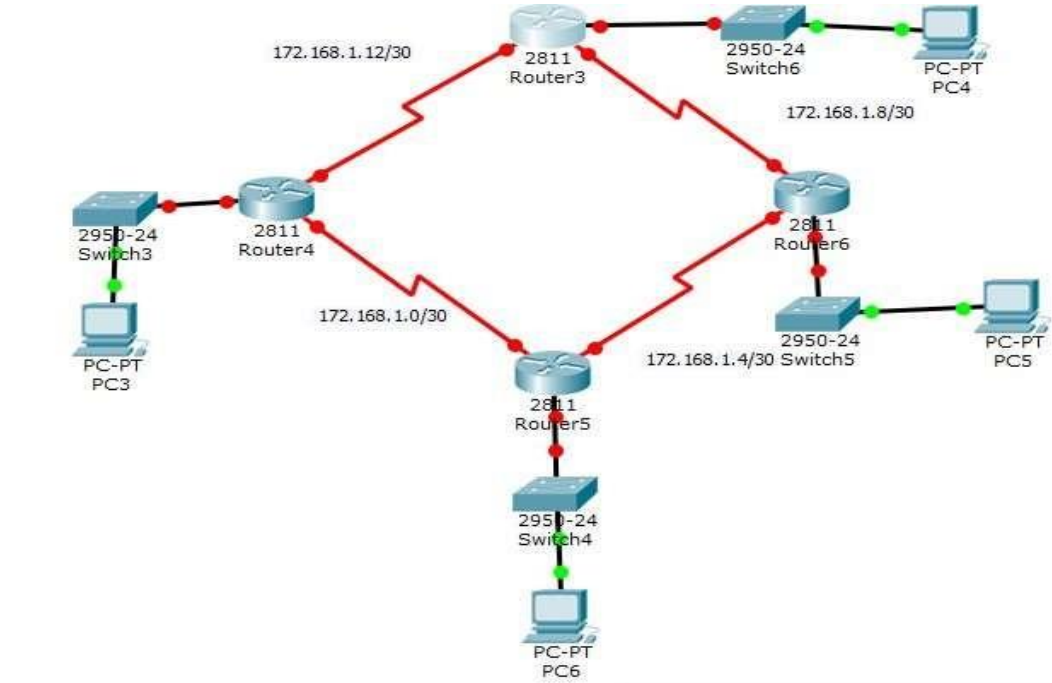


Fig-9: Network Topology for Q2

Q3: Implement the subnetting on the given scenario of figure 10. You have to implement the static routing on the same. What will be the administrative distance of the routing?
Use Network Address as follows: 192.168.4.0/24.

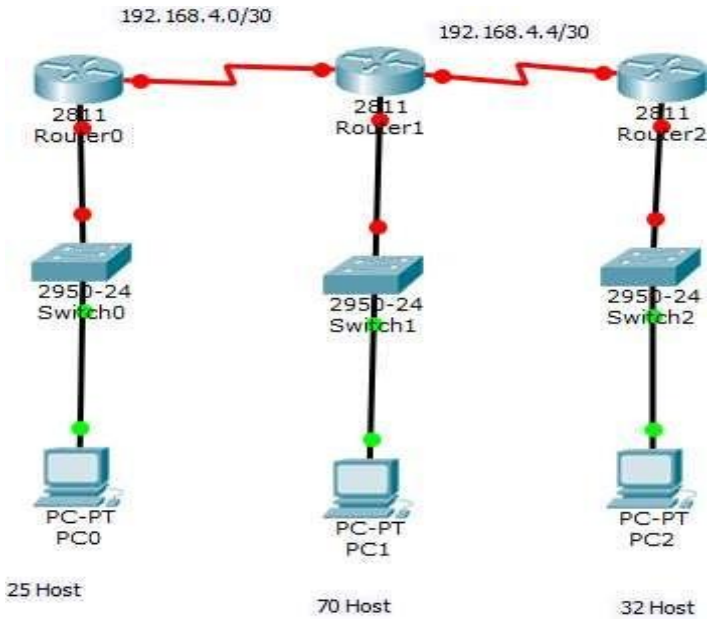


Fig-10: Network Topology for Q3

Q4: In what case we use static routing or dynamic routing given a topological reason for this question.

National University of Computer & Emerging Sciences, Karachi
FAST School of Computing
Spring 2023, Lab Manual 11

Course Code: CL-3001	Course: Computer Networks Lab
Instructor(s):	Mr. Muhammad Ali, Mr. Muhammad Nadeem, Mr. Shaheer Ahmad and Miss Hania Usman

Contents:

1. Introduction to Virtual Area Network

A traditional LAN comprising of workstations connected to each other by means of a hub or a repeater form a single collision and broadcast domains. Due to this, these devices propagate any incoming data throughout the network. To prevent collisions from traveling through all the workstations in the network, a bridge or a switch can be used. These devices will not forward collisions, but still will allow broadcasts and multicasts to pass through. A router, therefore, may be used to prevent broadcasts and multicasts from traveling through different networks. To stop broadcasts in a same LAN segment, VLAN's allow a network manager to logically segment a LAN into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.

A Virtual Local Area Network can be defined as a group of networking devices in the same broadcast domain, logically. Since this is a logical segmentation and not a physical one, it means that the devices in the same VLAN may be widely separated in the network; both by geography and location, workstations do not have to be physically located together.

VLAN helps you group users together according to their function rather than their physical location. This means Users on different floors of the same building, or even in different buildings can now belong to the same LAN. This makes the management much simpler.

Some of the benefits of VLANs are:

1. They improve network performance by reducing the size of broadcast domains. In a broadcast domain, every device can send packets to every other device, and every packet must be received and processed. When a broadcast domain becomes very large, this can degrade the performance of switches on the network due to the high volumes of broadcast data

2. VLANs allow for the adding of additional layers of security. For example, a specific VLAN can be created for users with specific security clearances.

3. VLANs make device management easier. If a user moves to a new physical location, the physical workstation of that user does not need to be reconfigured. Also, if a user stays in the same location but changes jobs, only the VLAN membership of the workstation needs to be changed.

For multiple VLANs to communicate with each other, a router is required. Routers between VLANs filter broadcast traffic, enhance network security, perform address summarization, and mitigate network congestion.

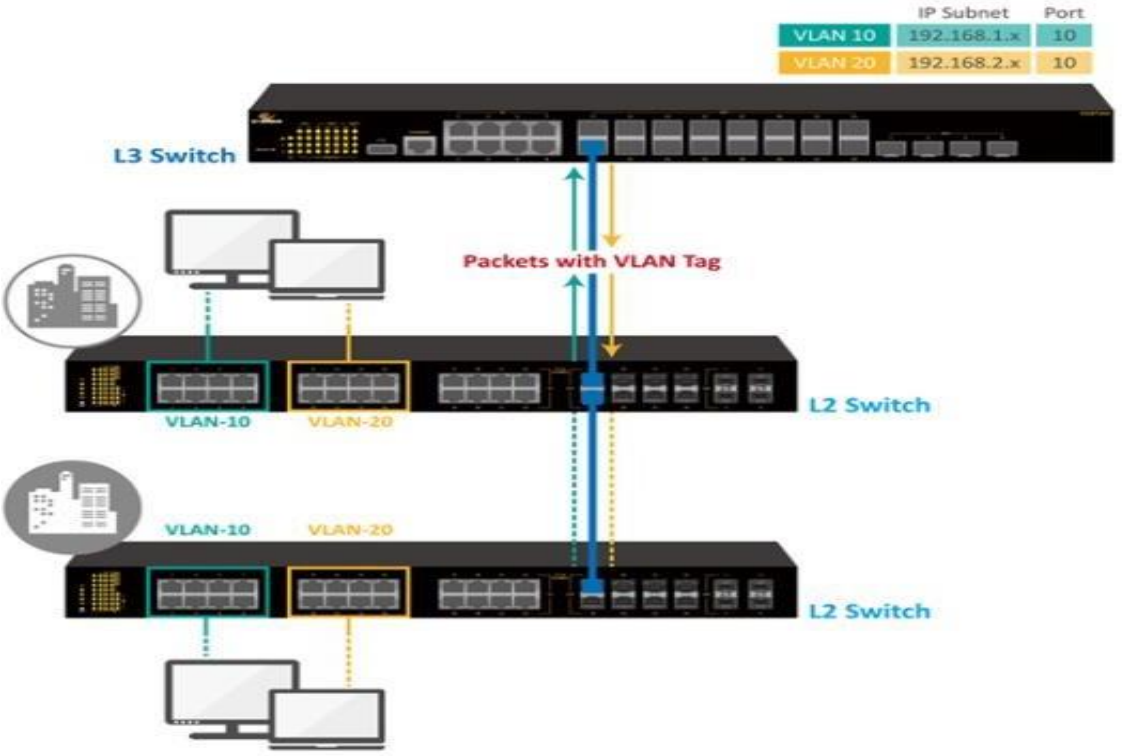


Figure 1 (Multiple Vlans Connection)

Real World Scenario

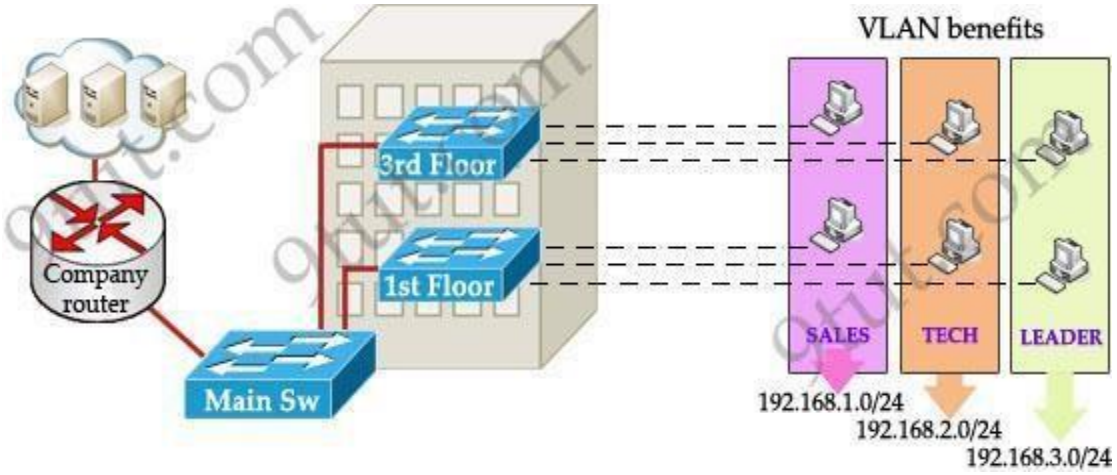


Figure 2 (Departmental Wise Vlan Example)

Take a real-world example as shown in figure 2. As VLANs break up broadcast domains, so now if a computer in ***Sales*** broadcasts, only computers in ***Sales*** will receive that frame.

It is important to point out that you don't have to configure a VLAN until your network gets so large and has so much traffic that you need one. Many times, people are simply using VLAN's because the network they are working on was already using them

You need to consider using VLAN's in any of the following situations:

- You have more than 200 devices on your LAN You have a lot of broadcast traffic on your LAN

- Groups of users need more security or are being slowed down by too many broadcasts? Groups of users need to be on the same broadcast domain because they are running the same applications.

- An example would be a company that has VoIP phones. The users using the phone could be on a different VLAN, not with the regular users. Or, just to make a single switch into multiple virtual switches.

Another important fact is that, on a Cisco switch, VLAN's are enabled by default and ALL devices are already in a VLAN. The VLAN that all devices are already in is VLAN 1. So, by default, you can just use all the ports on a switch and all devices will be able to talk to one another.

2. Types of Connection in Vlan

Devices on a VLAN can be connected in three ways based on whether the connected devices are VLAN-aware or VLAN-unaware. Recall that a VLAN-aware device is one which understands VLAN memberships (i.e. which users belong to a VLAN) and VLAN formats. Below are the types of connection in vlan. They are:

1. Trunk Link

All the devices connected to a trunk link, including workstations, must be VLAN-aware. All frames on a trunk link must have a special header attached. These special frames are called tagged frames as shown in figure 3

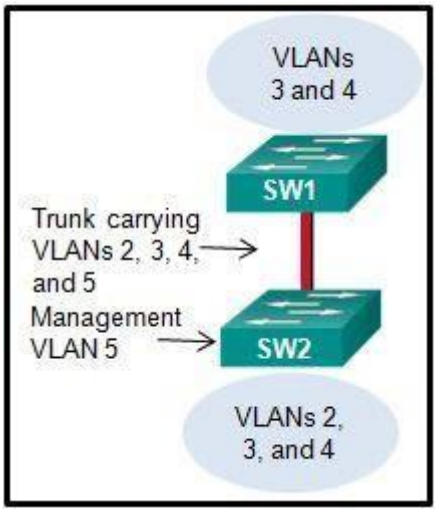


Figure 3(Trunk Link Connection)

2. Access Link

An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged). The VLAN-unaware device can be a LAN segment with VLAN-unaware workstations or it can be a number of LAN segments containing VLAN-unaware devices (legacy LAN).

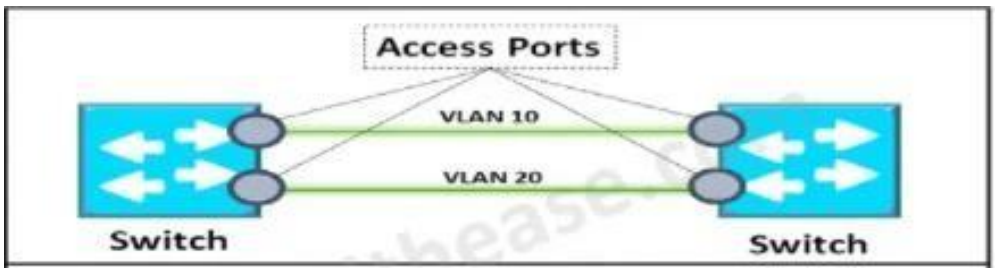


Figure 4(Access Link Connection)

The combine pictural view of Access and Trunk link is given in figure 5

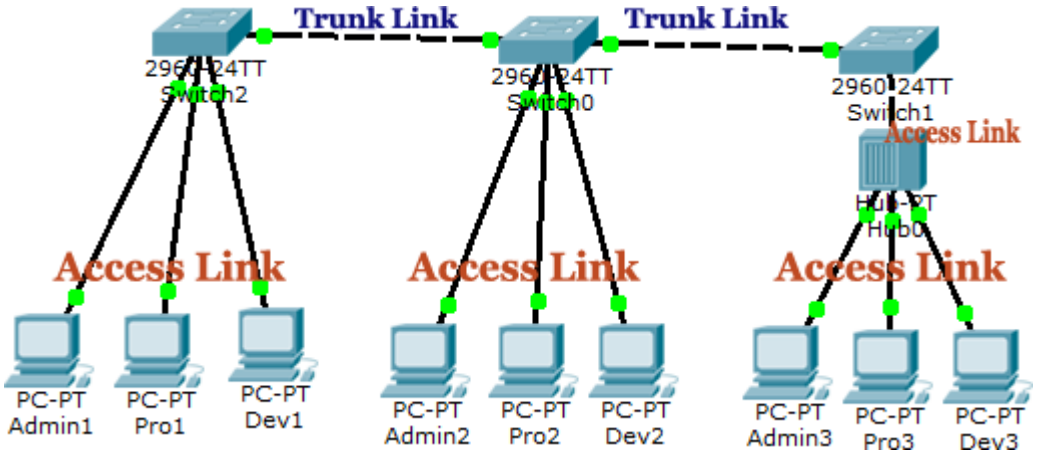


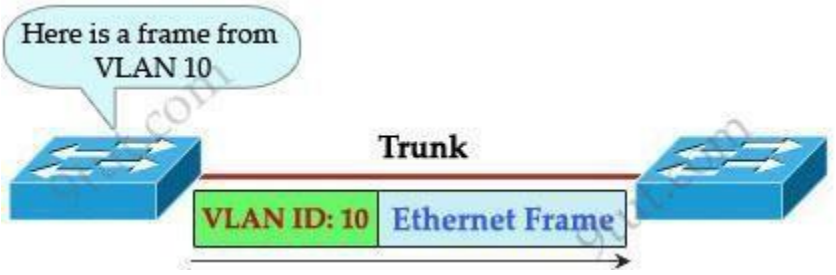
Figure 5(Combine Access and Trunk Link)

Communication in VLAN

Hosts in the same VLAN can communicate normally even they are connecting to 2 or more different switches. When using multiple VLANs in networks that have multiple interconnected switches, we need to use VLAN Trunking between the switches. With VLAN trunking, the switches tag each frame sent between switches so that the receiving switch knows which VLAN the frame belongs to. This tag is known as a VLAN ID. A VLAN ID is a number which is used to identify a VLAN.

3. Introduction to Intervlan Routing

To enable different VLANs to communicate with each other need a router. Without a router, the computers within each VLAN can communicate with each other but not with any other computers in another VLAN. For example, we need a router to transfer file from LEADER to TECH. This is called "*inter-VLAN routing*".



The tag is only added and removed by the switches when frames are sent out on the trunk links. Hosts don't know about this tag because it is added on the first switch and removed on the last switch. The picture below describes the process of a frame sent from PC A to PC B.

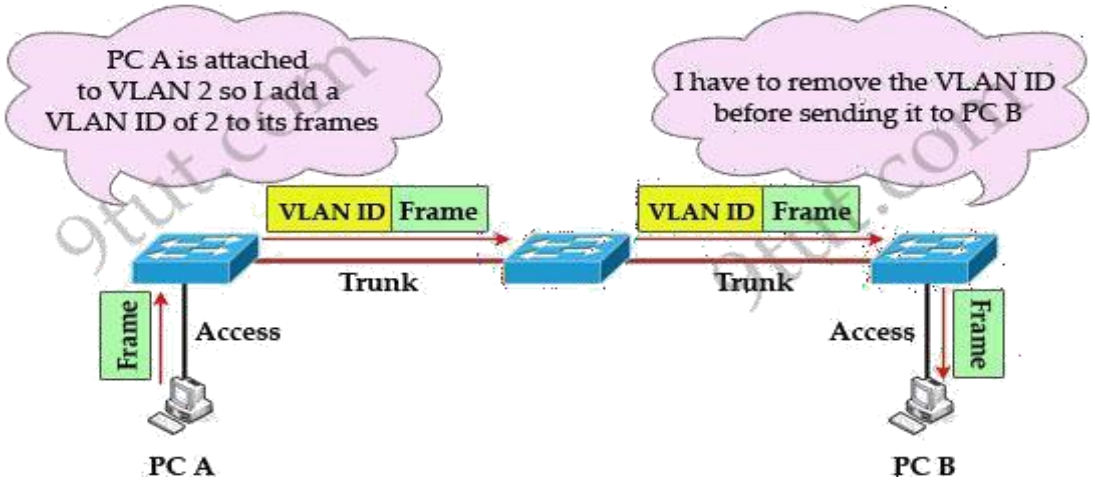


Figure 6(Connection of Vlan ID)

Note: Trunk link does not belong to a specific VLAN; rather it is a conduit for VLANs between switches and routers.

To allow inter-VLAN routing you need to configure trunking on the link between router and switch. Therefore, in our example we need to configure 3 links as "trunk".

Cisco switches support two different trunking protocols, Inter-Switch Link (ISL) and IEEE 802.1q. Cisco created ISL before the IEEE standardized trunking protocol. Because ISL is Cisco proprietary, it can be used only between two Cisco switches. 802.1q is usually used in practical.

In 802.1q encapsulation, there is a concept called native VLAN that was created for backward compatibility with old devices that don't support VLANs. Native VLAN works as follows:

1. Frame belonging to the native VLAN is not tagged when sent out on the trunk links.
2. Frame received untagged on the trunk link is set to the native VLAN.

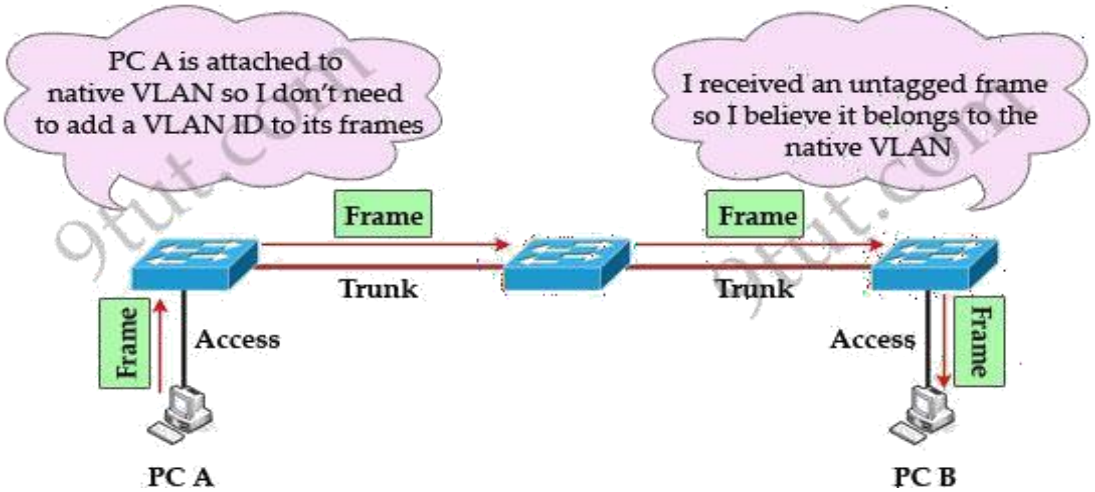


Figure 7 (Understanding of the Vlan Frame)

So if an old switch doesn't support VLAN it can still "understand" that frame and continue sending it (without dropping it).

Every port belongs to at least one VLAN. If a switch receives untagged frames on a trunkport, they are assumed to be part of the native VLAN. By default, VLAN 1 is the default and native VLAN but this can be changed on a per port basis by configuration.

4. Configuration of Vlan

Creating Vlan

Step 1: Enter privileged EXEC mode

Switch>enable

Step 2: Enter global configuration mode.

Switch#config terminal

Step 3: Create VLAN

Switch(config)#vlan X (X can be any natural number)

Step 4: Give name to VLAN

Switch(config-vlan)#name XYZ (Name of VLAN)

Notice that we don't need to exit out of "vlan mode" to create another VLAN.

Set VLAN Membership

Assign VLAN to each port:

Step 5: Enter interface configuration mode.

Switch(config)#interface type port(int fa0/1)

Step 6: Set the mode of port as trunk or access

Switch(config-if) #switchport mode access/trunk (access when pc-switch else trunk)

Step 7: If port is in access mode, assign a VLAN to the port.

Switch(config-if) #switchport access vlan-number

Notice that for port connecting to host we must configure it as access port

5. Configuration InterVlan Routing

Step 8: Enter interface configuration mode.

Router(config)#interface *type port*

Step 9: Enter sub-interface configuration mode.

Router(config-if)#interface *type port.subport*

Step 10. Set the ip address of the subinterface.

Router(config-subif)#ip address X.X.X.X Y.Y.Y.Y

Step 11. Set the encapsulation type and vlan allowed on sub-interface.

Router(config-subif)# encapsulation dot1q*vlan number*

Lab Exercise

Q1: Implement the given topology of figure A on cisco packet tracer. Perform the following task:

1. Create different vlan members on the given switches
2. Create Trunk and Access link connection
3. Create the intervlan routing on the given router

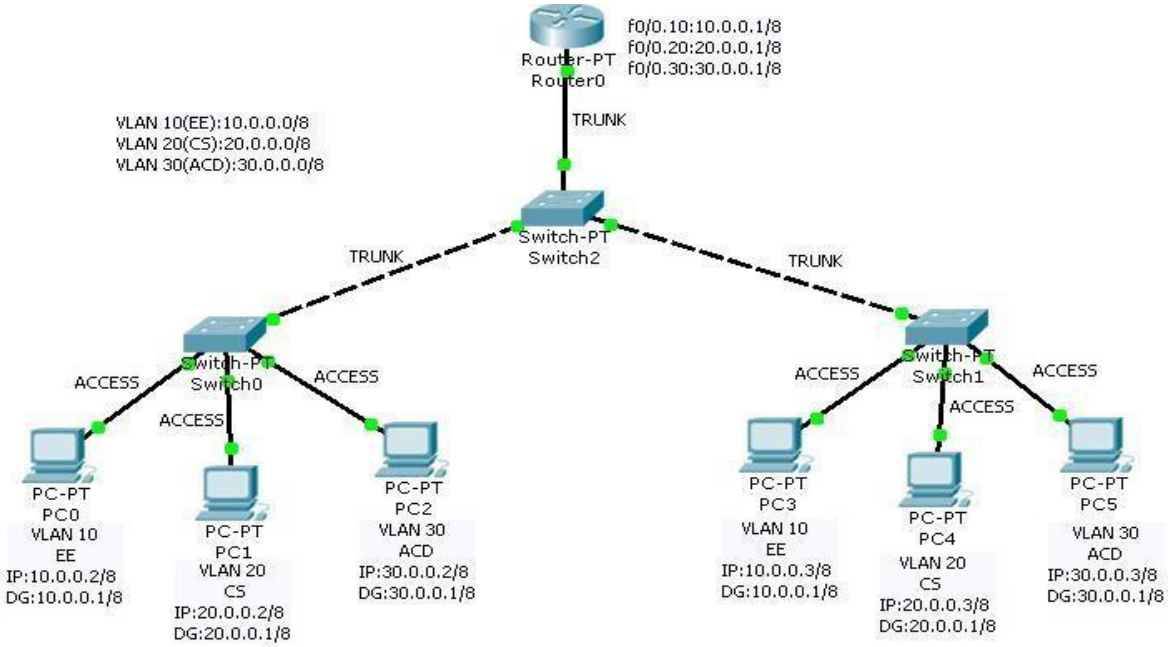


Figure A (Network Topology)

Q2: Implement the given topology of figure B on cisco packet tracer. Perform the following task:

1. Do peform Vlans and InterVlan Routing.
2. Dynamic Ips should be assign to all the end devices.
3. The default gateways should be like XX.XX.1.1, XX.XX.2.1 and so on where XX.XX will be your roll number like 3879 and it will be 38.79.1.1,38.79.2.1 and so on.

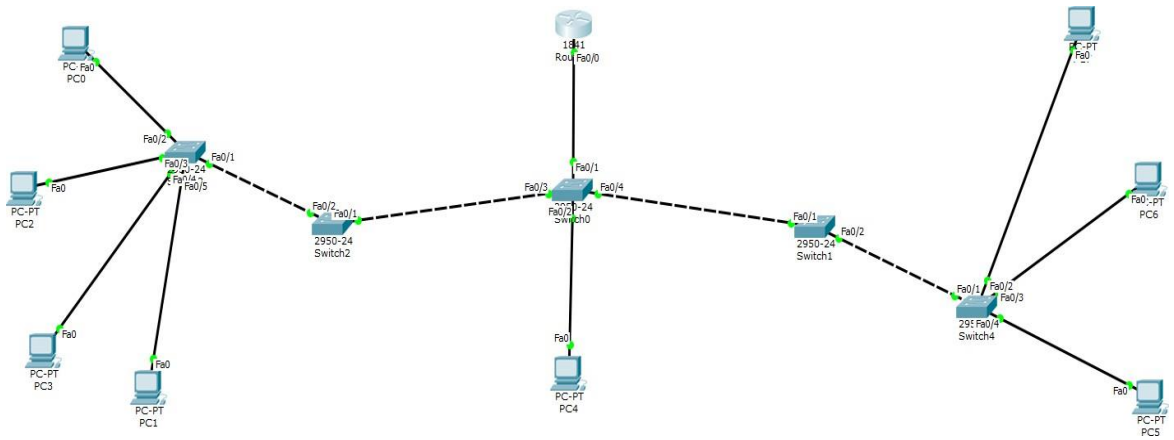


Figure B (Network Topology)

NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 11

Objective:

- Introduction to Wireless Network
- Importance of Wireless Technology
- Working of Wireless Network
- Configuration of Wireless Network
- Introduction to NAT & its Types
- Configuration of NAT
- Wireshark of NAT
- Lab Exercise

Wireless Network

1. Introduction to Wireless Network

A wireless network allows devices to stay connected to the network while roaming without the need for wires. Because access points amplify Wi-Fi signals, a computer may be far away from a router and still be connected to the network. When you connect to a Wi-Fi hotspot at a café or similar public area, you are connecting to that organization's wireless network.

The main difference between a wireless and a wired network is that a wired network requires wires to connect devices, such as laptops or desktop computers, to the Internet or another network. A wired network, as opposed to a wireless network, has numerous disadvantages. The primary disadvantage is that a router is permanently connected to your computer. The most common wired networks employ cables connected to an Ethernet port on the network router and a computer or other equipment on the other end.

2. Importance of Wireless:

However, delving into a specific technology at this point is getting ahead of the tale. Regardless of how the protocols are constructed or what sort of data they carry, wireless networks have some important advantages.

The most obvious benefit of wireless networking is mobility. Users of wireless networks can connect to existing networks and then roam freely. Because the phone connects the user via cell towers, a mobile phone user can travel kilometers in a single call.

Initially, mobile telephone was prohibitively expensive. Due to the exorbitant price, it was only used by highly mobile professionals such as sales managers and important executive decision-makers who needed to be accessible at any time and from any location. Mobile telephone, on the other hand, has proven to be a valuable service that is becoming increasingly popular.

Wireless networks often provide a lot of flexibility, which translates to quick installation. Wireless networks link users to an existing network using a variety of base stations.

3. Working of Wireless Network:

A wireless local area network (WLAN) connects a collection of computers in the same way that a wired network does. Because "wireless" does not require costly cabling, the major benefit is that it is generally easier, faster, and less expensive to set up.

Building a network by dragging cables over an office's walls and ceilings, on the other hand, may be time-consuming and costly. Even if you currently have a wired network, a wireless network might be a cost-effective method to extend or expand it.

Radio Frequency (RF) technology, a frequency related with radio wave transmission within the electromagnetic spectrum, is used to power wireless networks. When an RF current is sent into an antenna, it creates an electromagnetic field that can travel over space.

A wireless network's core is a mechanism known as an access point (AP). The fundamental function of an access point is to transmit a wireless signal that computers can detect and tune into. Because wireless networks are frequently linked to wired networks, access points frequently serve as a portal to the resources of the wired network, such as an Internet connection.

To connect to an access point and join a wireless network, computers must be equipped with wireless network adapters. These are usually incorporated into the device, but if not, any computer or notebook can be turned wireless-capable by connecting an add-on adapter to an empty expansion slot, USB port, or, in the case of notebooks, a PC card slot.

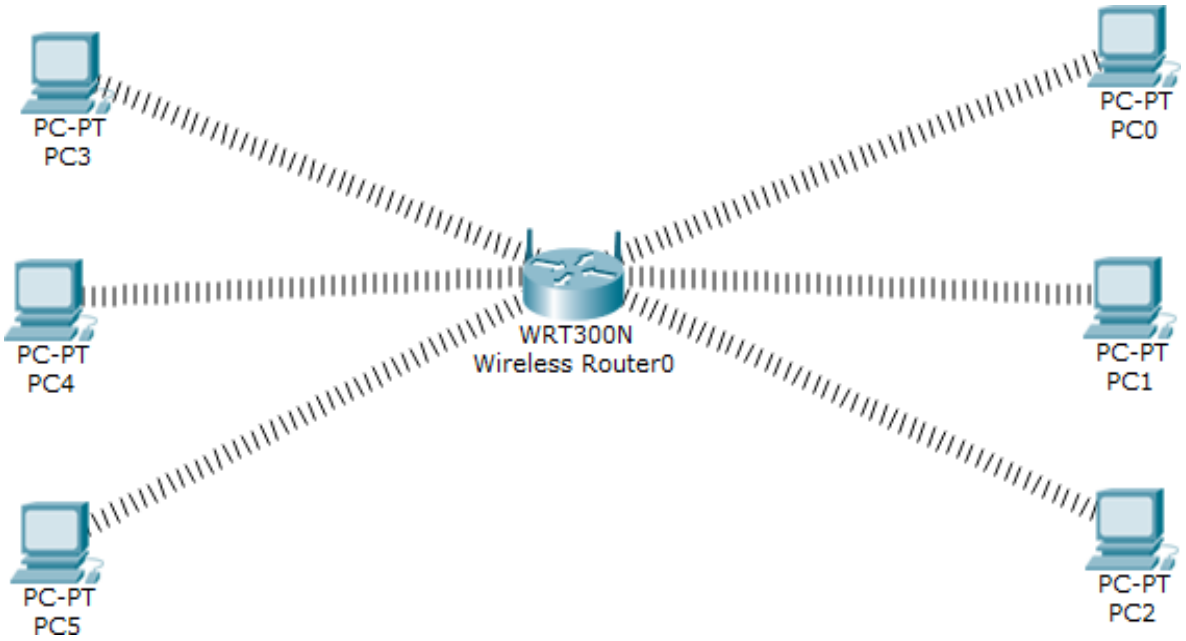


Fig-1: Wireless Network Topology

4. Configuration of Wireless Network:

The above topology mentioned in figure 1 we have six pc connected with Linksys Wireless routers.

1. DHCP is configured and enabled on Wireless router.
2. IP pool for DHCP is 192.168.0.100 to 192.168.0.150.
3. IP pool for DHCP is 192.168.0.100 to 192.168.0.150.
4. PC are configured to receive IP from DHCP Server.
5. No security is configured.
6. Default SSID is configured to Default.
7. Topology is working on infrastructure mode.

8. Default user name and password is admin.
9. IP of wireless is set to 192.168.0.1.

Now we perform some following tasks on the given above topology i.e., Figure 1:

- Configure Static IP on PC and Wireless Router
- Change SSID to Mother Network
- Change IP address of router and end devices
- Secure your network by configuring WAP key on Router
- Connect PC by using WAP key

To complete the above tasks, we will follow this step-by-step guide of how to configure wireless network

As given in question our network is running on 192.168.0.0 network and all PC's are DHCP clients and functioning properly. So, we will first connect to given Wireless router to turn off the DHCP Services.

Double click on PC and select Web Browser. As given in question IP of Wireless router is 192.168.0.1 so give it in Web browser and press enter, now it will ask for authentication which is also given in question. Default username is admin and password is also admin.

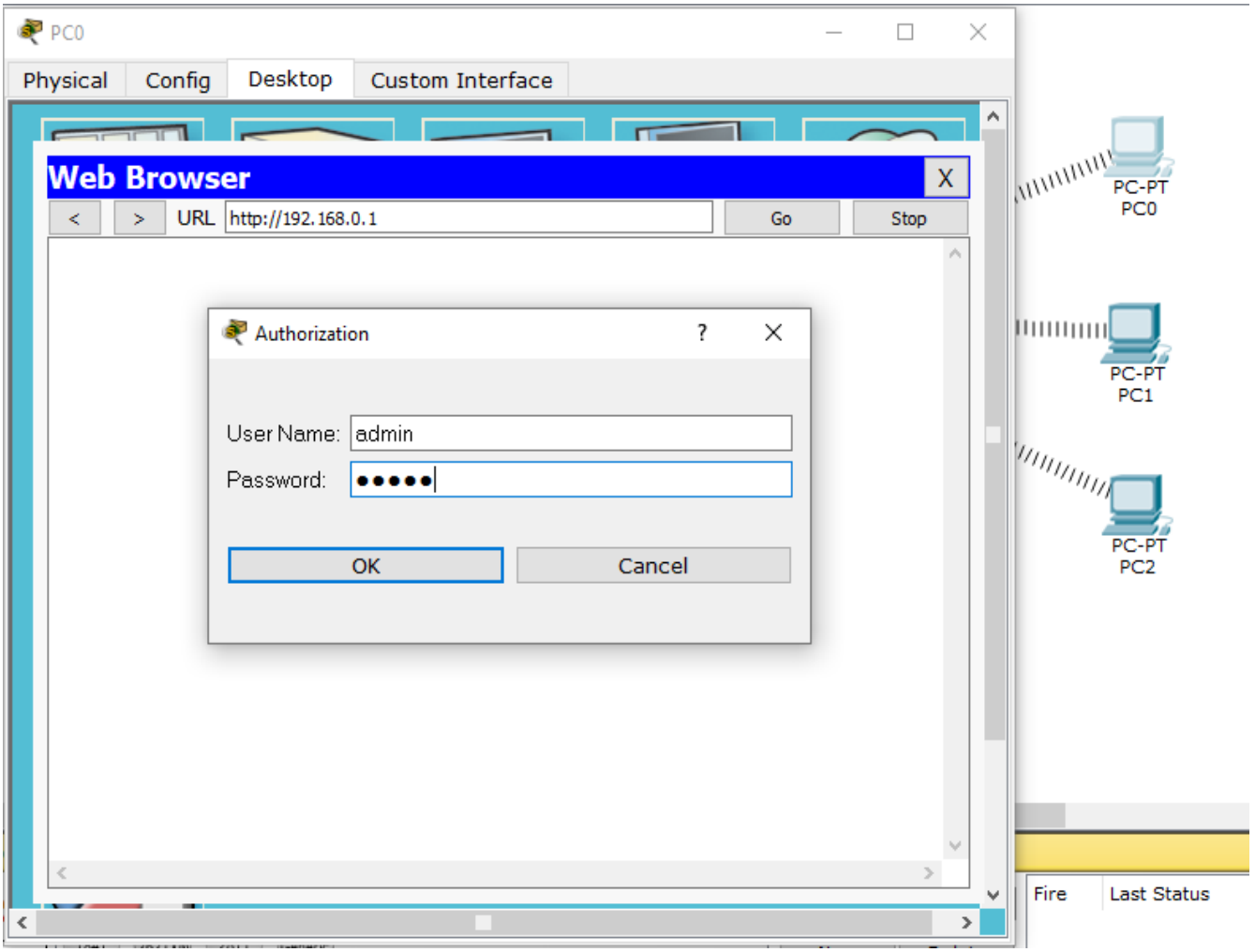


Fig-2: Authentication using username & password

This will bring GUI mode of Wireless router. Scroll down screen to Network Step and Select Disable DHCP.

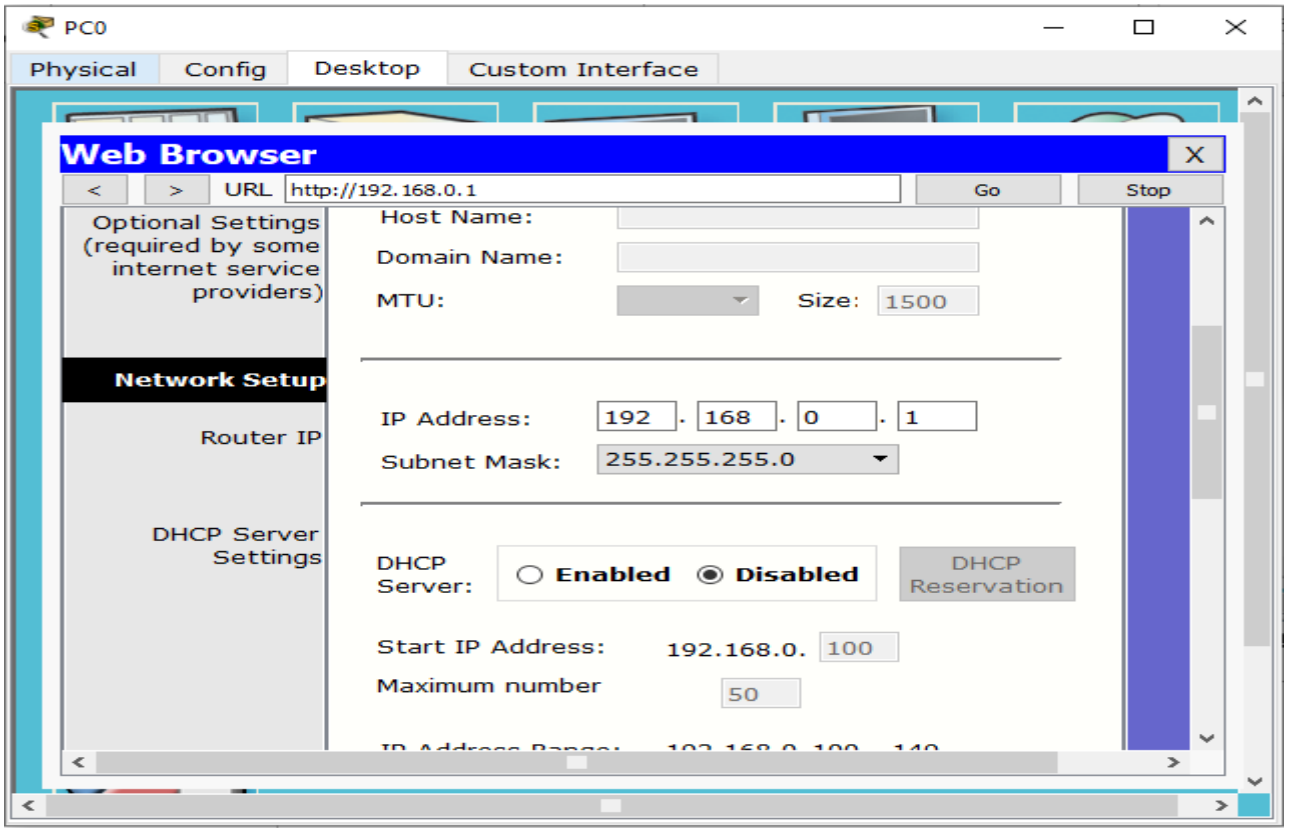


Fig-3: Select disabled option after authentication

Go in end of page and click on save setting this will save setting click on continue for further setting

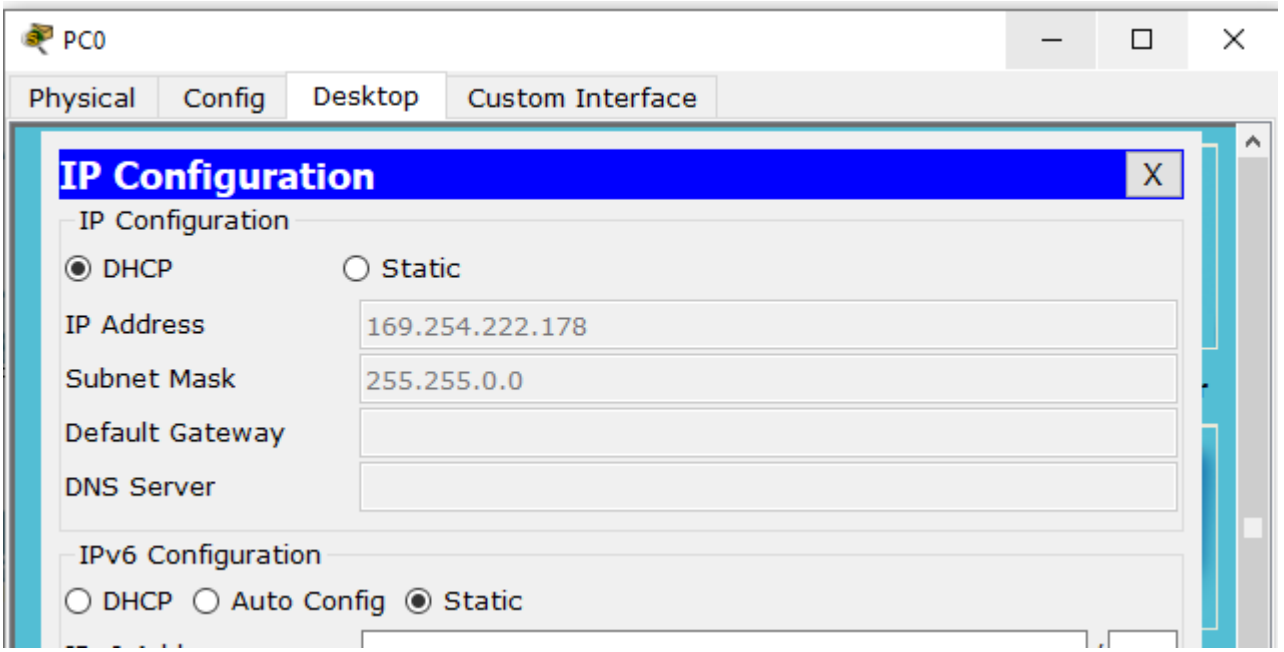


Fig-4: After disabling DHCP, APIPA address is visible

Move to Router directly, select Administration from top Manu and change password to test and go in the end of page and Click on Save Setting.

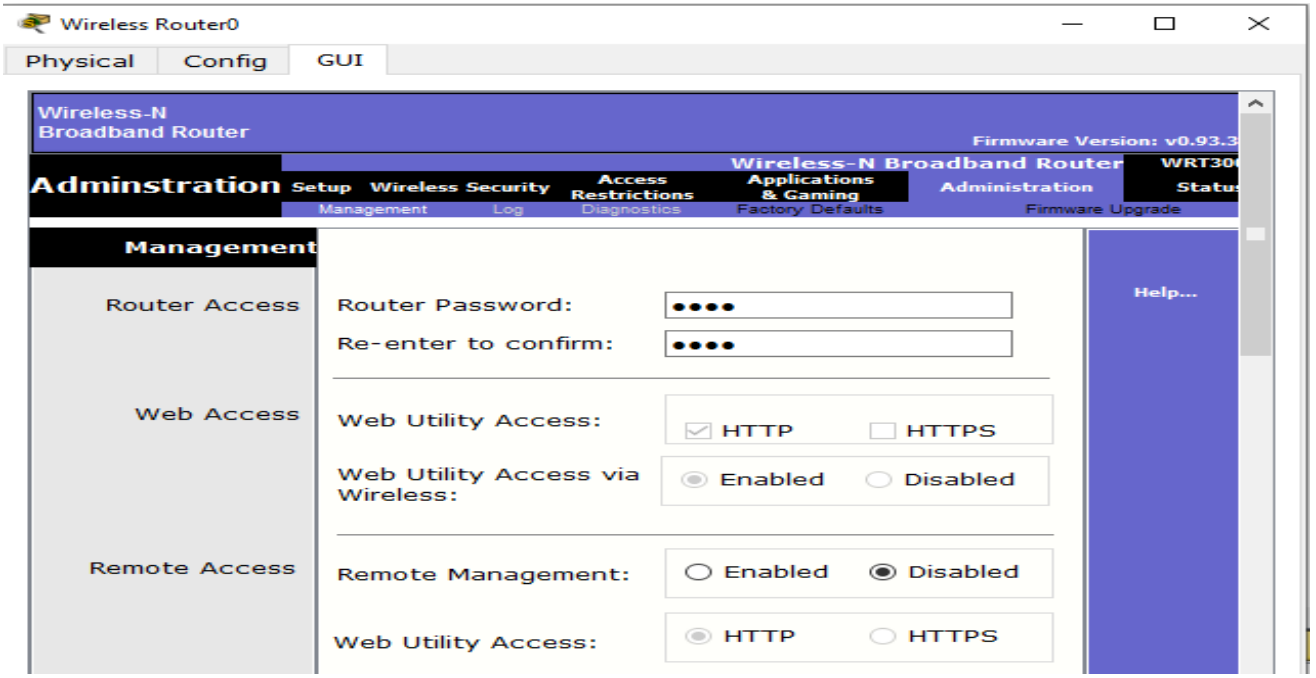


Fig-5: Changing the default password

Click on continue for further setting. This time it will ask you to authenticate again give new password test this time

Fig-6: Authentication of the user with new password

Now click on wireless tab and set default SSID to FastNetwork.

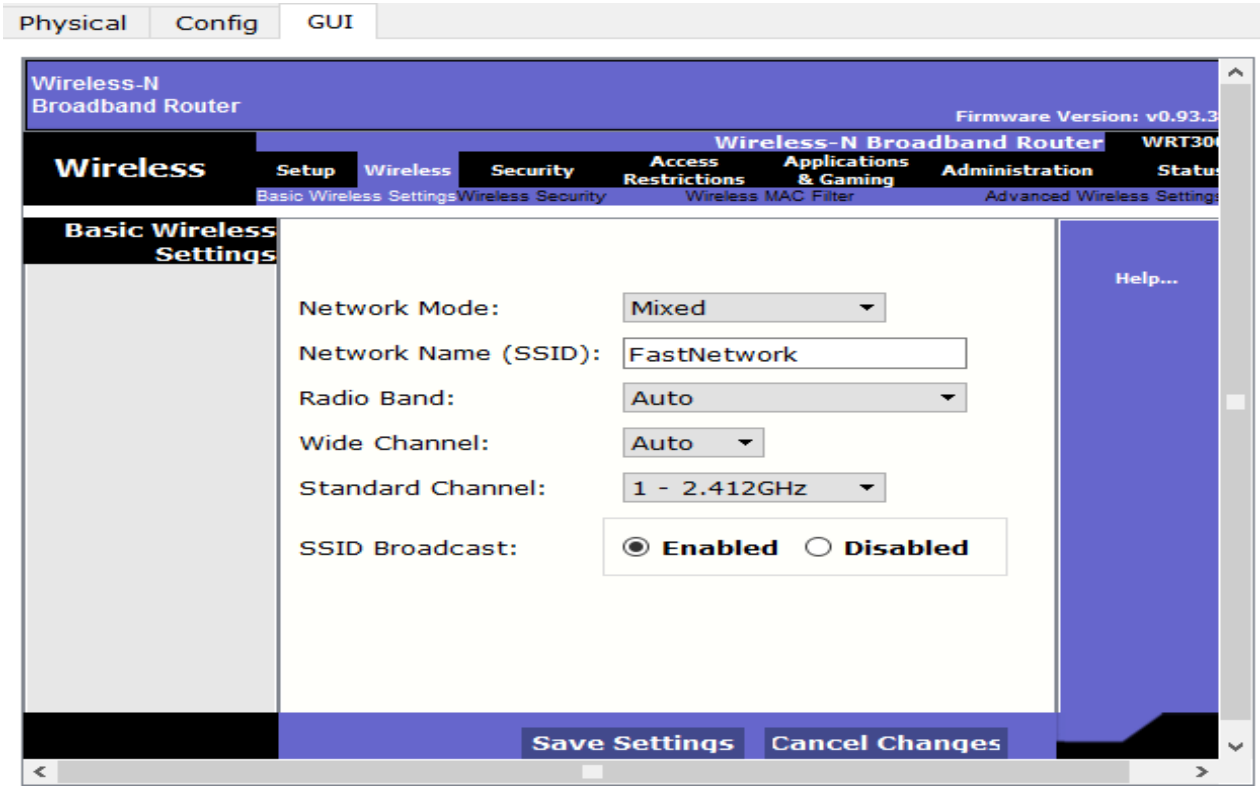


Fig-7: Changing the SSID

Now Select wireless security and change Security Mode to WEP.

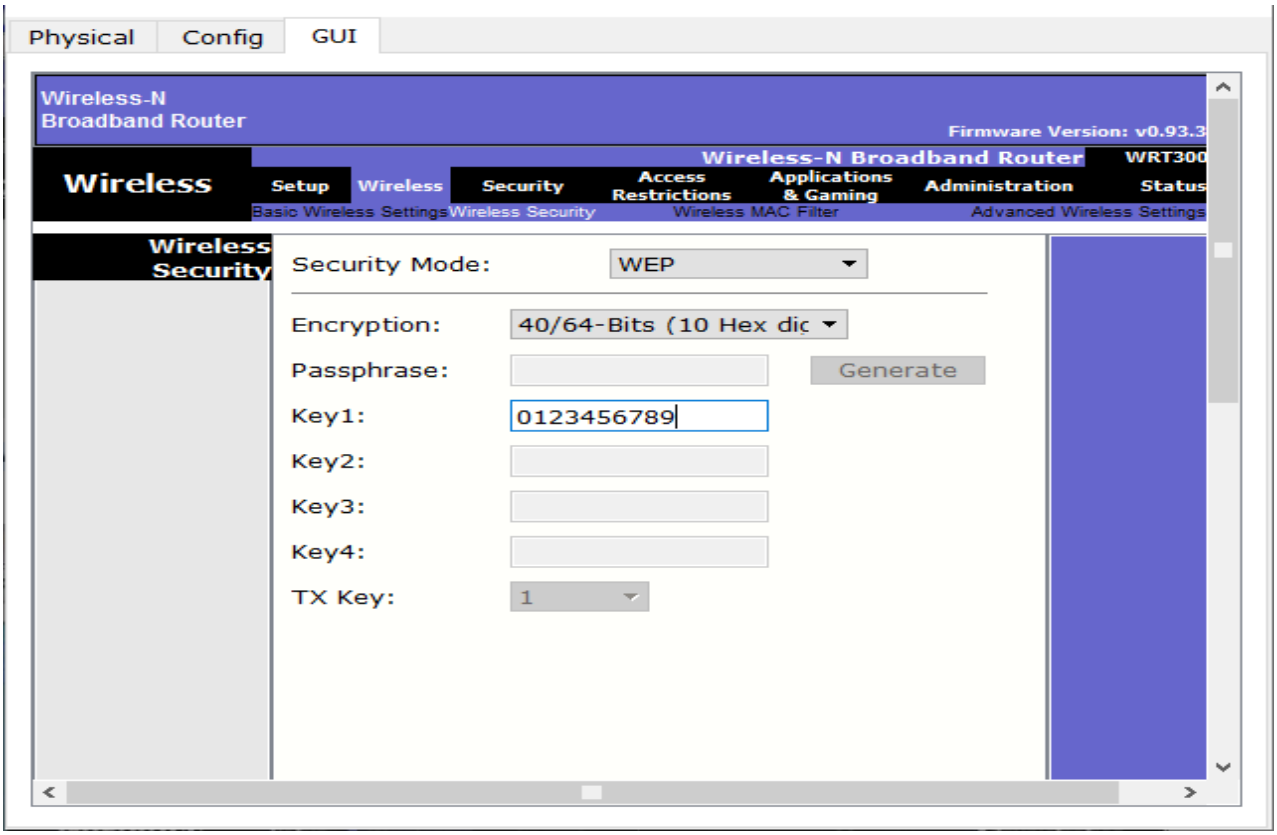


Fig-8: Setting WEP Key

Again, go in the end of page and Click on Save Setting.

Now we have completed all given task on Wireless router. Now configure the static IP on all three PC's Double clicks on pc select Desktop tab click on IP configuration select Static IP and set IP as given below:

PC	IP	Subnet Mask	Default Gateway
PC0	192.168.0.2	255.255.255.0	192.168.0.1
PC1	192.168.0.3	255.255.255.0	192.168.0.1
PC2	192.168.0.4	255.255.255.0	192.168.0.1
PC3	192.168.0.5	255.255.255.0	192.168.0.1
PC4	192.168.0.6	255.255.255.0	192.168.0.1
PC5	192.168.0.7	255.255.255.0	192.168.0.1

Table-1: PC IP Addresses

Now it's time to connect PC's from Wireless router. To do so click PC select Desktop click on PC Wireless.

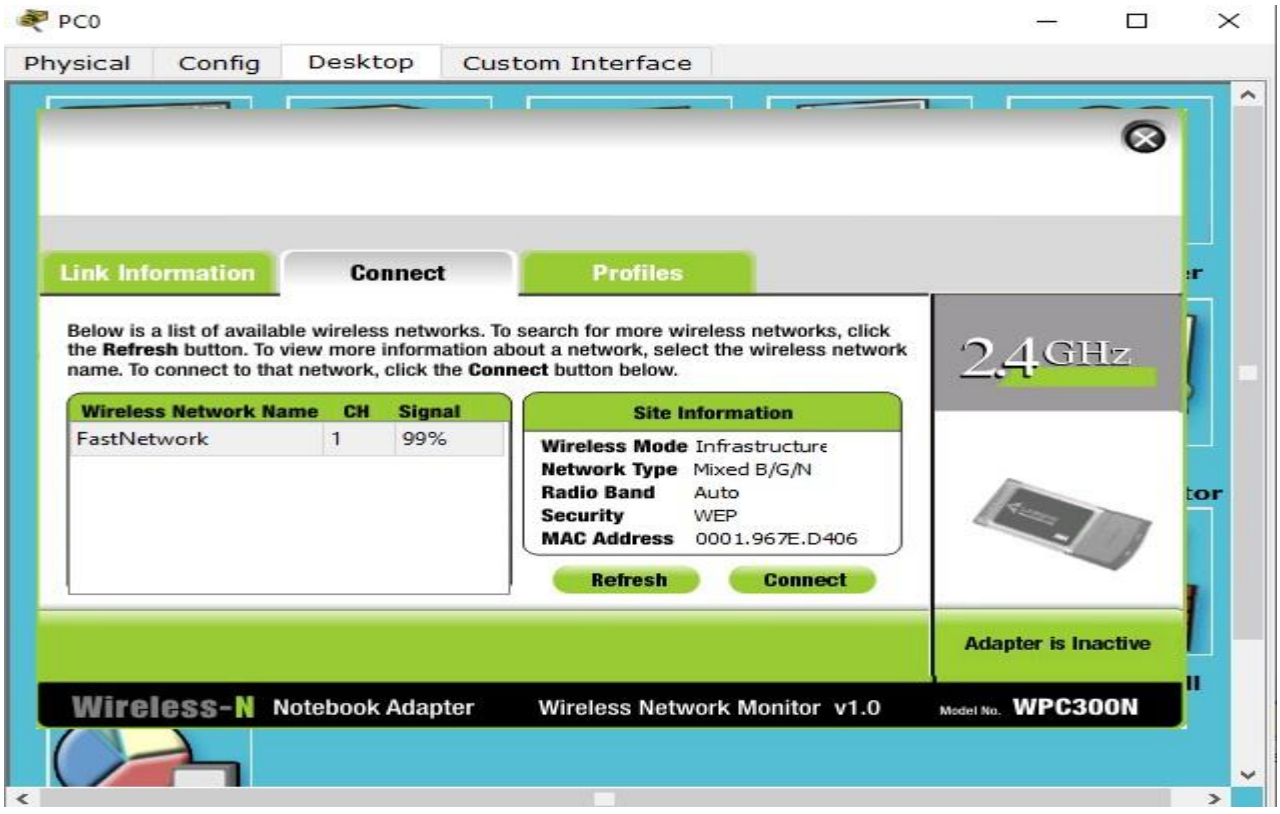


Fig-9: Connecting to Network

Click on connect tab and click on Refresh button. It will ask for WEP key insert 0123456789 and click connect.

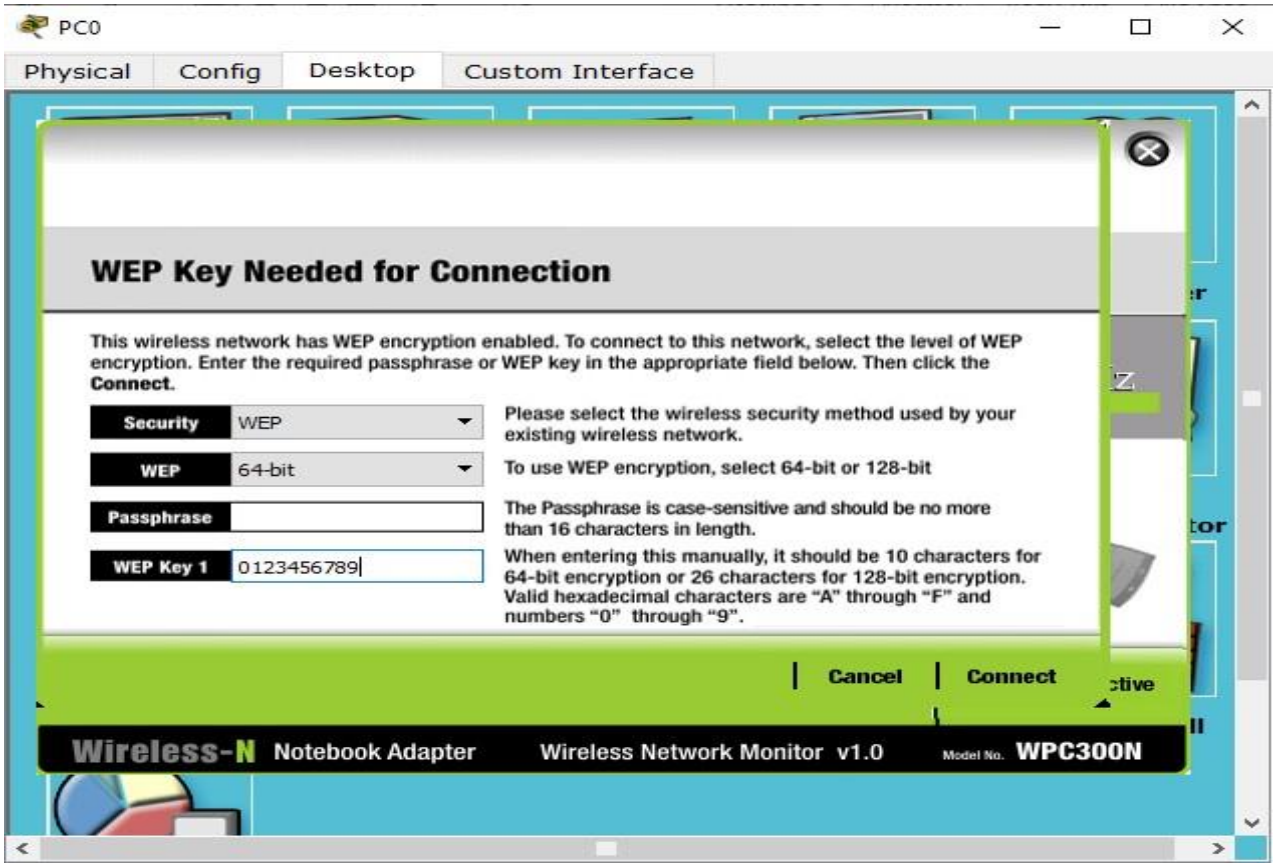


Fig-10: Entering WEP Key

It will connect you with wireless router as shown in figure 11

Fig-11: Connected to the wireless network

NAT

5. Introduction to NAT & Its Types:

Network Address Translation (NAT) is a mechanism by which a device modifies a packet's TCP/IP address/port number and maps the IP address from one realm to another (usually from private IP address to public IP address and vice versa). This is accomplished by the NAT device allocating a temporary port number on the public side of the NAT when forwarding outbound packets from the internal host to the Internet, maintaining this mapping for a predetermined period of time, and forwarding inbound packets received from the Internet on this public port back to the internal host.

NAT devices are used to avoid the exhaustion of IPv4 address space by allowing multiple hosts to share a single public/Internet address. Also due to its mapping nature (i.e., a mapping can only be created by a transmission from an internal host), NAT device is preferred to be installed even when IPv4 address exhaustion is not a problem (for example when there is only one host at home), to provide some sort of security/shield for the internal hosts against threats from the Internet.

Despite the fact that NAT provides some shields for the internal network, one must distinguish NAT solution from firewall solution. NAT is not a firewall solution. A firewall is a security solution designed to enforce the security policy of an organization, while NAT is a connectivity solution to allow multiple hosts to use a single public IP address. Understandably both functionalities are difficult to separate at times, since many (typically consumer) products claims to do both with the same device and simply label the device a "NAT box". But we do want to make this distinction rather clear, as PJNATH is a NAT traversal helper and not a firewall bypass solution (yet).

Following are the types of NAT.

Static NAT (Network Address Translation)- Static NAT (Network Address Translation) is one-to-one mapping of a private IP address to a public IP address. Static NAT (Network Address Translation) is useful when a network device inside a private network needs to be accessible from internet.

Dynamic NAT (Network Address Translation)- Dynamic NAT can be defined as mapping of a private IP address to a public IP address from a group of public IP addresses called as NAT pool. Dynamic NAT establishes a one-to-one mapping between a private IP address to a public IP address. Here the public IP address is taken from the pool of IP addresses configured on the end NAT router. The public to private mapping may vary based on the available public IP address in NAT pool.

PAT (Port Address Translation)- Port Address Translation (PAT) is another type of dynamic NAT which can map multiple private IP addresses to a single public IP address by using a technology known as Port Address Translation.

6. Configuration of NAT:

1. Static NAT Configuration:

Static NAT is used to do a one-to-one mapping between an inside address and an outside address. Static NAT also allows connections from an outside host to an inside host. Usually, static NAT is used for servers inside your network. For example, you may have a web server with the inside IP address 192.168.0.10 and you want it to be accessible when a remote host makes a request to 209.165.200.10. For this to work, you must do a static NAT mapping between those to IPs. In this example, we will use the Fast Ethernet 0/1 as the inside NAT interface, the interface connecting to our network, and the Serial 0/0/0 interface as the outside NAT interface, the one connecting to our service provider.

Working Step on Router:
Router(config)#ip nat inside source static 192.168.0.10 209.165.200.10
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside

2. Dynamic NAT Configuration:

Dynamic NAT is used when you have a "pool" of public IP addresses that you want to assign to your internal hosts dynamically. Don't use dynamic NAT for servers or other devices that need to be accessible from the Internet. In this example, we will define our internal network as 192.168.0.0/24. We also have the pool of public IP addresses from 209.165.200.226 to 209.165.200.240 and our assigned netmask is 255.255.255.224. When you configure dynamic NAT, you have to define an ACL to permit only those addresses that are allowed to be translated.

Working Steps on Router:
Router(config)#ip nat pool NAT-POOL 209.165.200.226 209.165.200.240 netmask 255.255.255.224
Router(config)#access-list 1 permit 192.168.0.0 0.255.255.255
Router(config)#ip nat inside source list 1 pool NAT-POOL
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside Router
(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside

3. NAT Overload (PAT) Configuration:

NAT Overload, sometimes also called PAT, is probably the most used type of NAT. You can configure NAT overload in two ways, depending on how many public IP address you have available. The first case, and one of the most often seen cases, is that you have only one public IP address allocated by your ISP. In this case, you map all your inside hosts to the available IP address. The configuration is almost the same as for dynamic NAT, but this time you specify the outside interface instead of a NAT pool.

Working Steps on Router:
Router(config)#access list 1 permit 192.168.0.0 0.255.255.255
Router(config)#ip nat inside source list 1 interface serial 0/0/0 overload
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside

4. Example:

In this example we configure NAT overload (PAT) on the router which is located in Multan and static NAT is configured on Islamabad router. A simple topology is shown in figure 12.

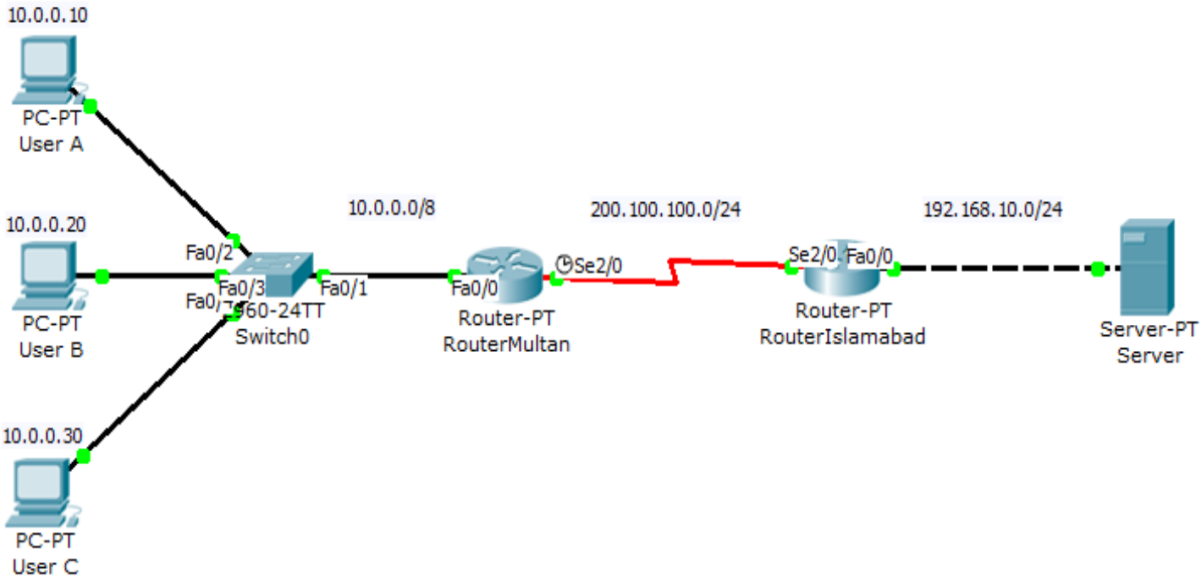


Fig-12: Network topology scenario for NAT

Assigning IP address to Multan router

Router>enable
Router# configure terminal
Router(config)#
Router(config)#hostname R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 100.0.0.1 255.0.0.0
R1(config-if)#clock rate 64000
R1(config-if)#bandwidth 64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#

Assigning IP address to Islamabad router

Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 100.0.0.2 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#exit

Configuring NAT Overload (PAT) on router Multan

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 1 permit 10.0.0.10 0.0.0.0
R1(config)#access-list 1 permit 10.0.0.20 0.0.0.0
R1(config)#access-list 1 deny any
R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.1 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool ccna overload
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface Serial 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit

Configuring Static NAT on router Islamabad

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
R2(config)#interface Serial 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#

Configuring static route on routers

R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2
R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1

Now ping server from a PC or open website through web browser using 200.0.0.10 IP address. To check the connectivity after configuring NAT. Use show "**ip nat translation command"** to verify NAT implementation on router.

```
R1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 50.0.0.1:1        10.0.0.20:1        200.0.0.10:1       200.0.0.10:1
icmp 50.0.0.1:2        10.0.0.20:2        200.0.0.10:2       200.0.0.10:2
icmp 50.0.0.1:3        10.0.0.20:3        200.0.0.10:3       200.0.0.10:3
icmp 50.0.0.1:4        10.0.0.20:4        200.0.0.10:4       200.0.0.10:4
tcp 50.0.0.1:1024      10.0.0.10:1025     200.0.0.10:80      200.0.0.10:80
tcp 50.0.0.1:1025      10.0.0.20:1025     200.0.0.10:80      200.0.0.10:80
```

Fig-13: NAT information of Router 1 (Multan)

7. Wireshark of NAT:

In this section, we'll capture packets from a simple web request from a client PC in a home network to a www.google.com server. Within the home network, the home network router provides a NAT service. Figure 12 shows our Wireshark trace-collection scenario. As in our other Wireshark labs, we collect a Wireshark trace on the client PC in our home network. This file is called NAT_home_side. Because weare also interested in the packets being sent by the NAT router into the ISP, we'll collect a second trace file at a PC (not shown) tapping into the link from the home router into the ISP network, as shown in Figure 12. (The hub device shown on the ISP side of the router is used to tap into the link between the NAT router and the first hop router in the ISP). Client-to-server packets captured by Wireshark at this point will have undergone NAT translation. The Wireshark trace file captured on the ISP side of the home router is called NAT_ISP_side.

Open the NAT_home_side file and answer the following questions. You might find it useful to use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer.To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and selectthe minimum amount of packet detail that you need to answer the given in the Exercise Section of NAT.

Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract thefiles need for this lab.

8. Lab Exercise:

1. Wireless Network

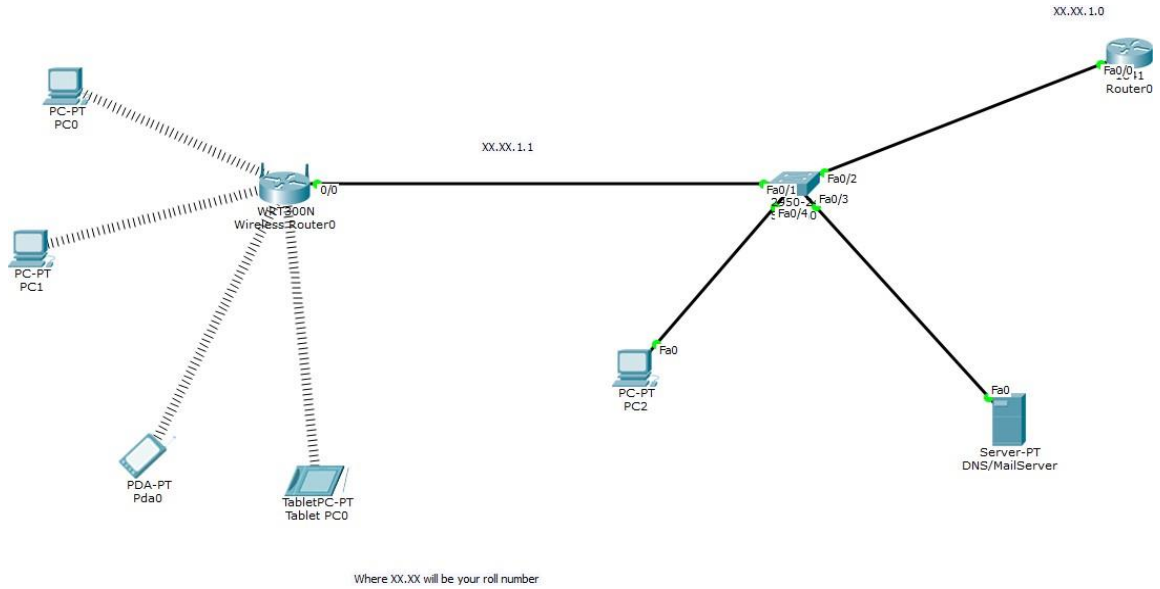


Fig-14: Topology for 1st exercise

1. Do configure the network
2. Change the Network of Wireless Router to your StudentID+Name.
3. Set the key while connecting the wireless router with end devices.
4. Do perform secure communication on Switch0 and Router0 and check it through PC0.
5. Do send mails from Wireless Users to Lan Users by creating different domains.
6. Hit the web browser using CNAME.

7. Show HTTP and HTTPs packet movement by taking screenshots.

2. NAT (Cisco Packet Tracer)

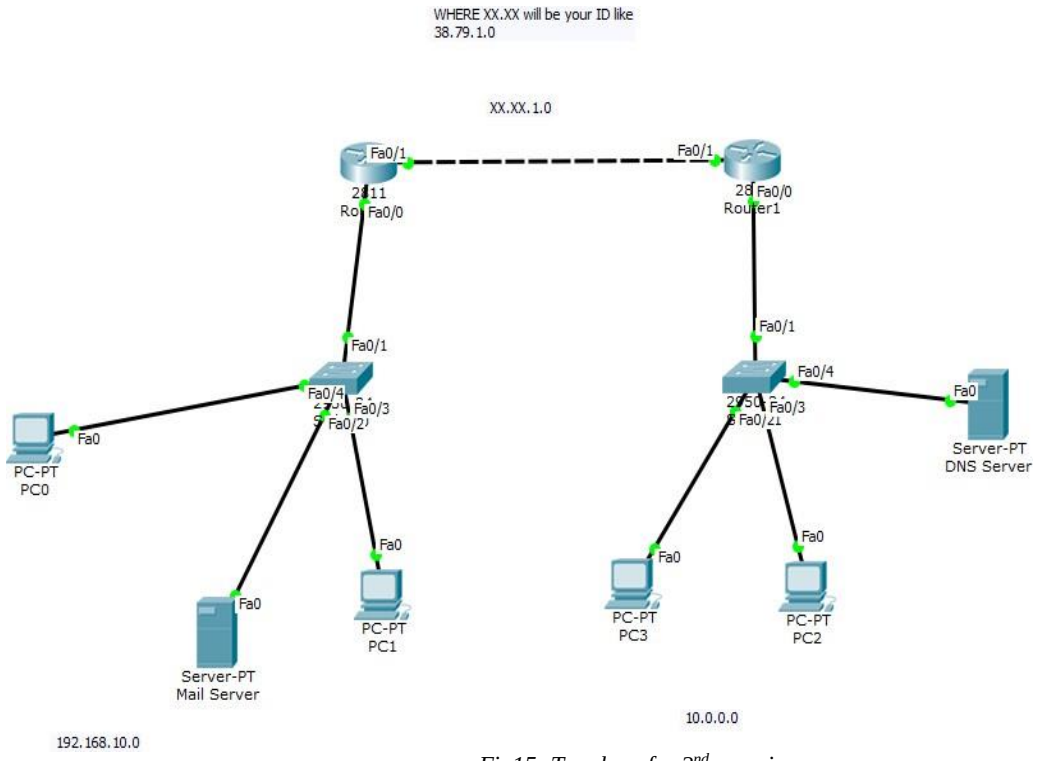


Fig15: Topology for 2nd exercise

1. Perform Static Nat on Router0 and Dynamic Nat on Router1
2. Do send mail from PC1 to PC2
3. Do hit the website from PC0

3. NAT (Wireshark)

1. What is the IP address of the client?
2. The client actually communicates with several different Google servers in order to implement "safe browsing." (See extra credit section at the end of this lab). The main Google server that willserve up the main Google web page has IP address 64.233.169.104. In order to display only thoseframes containing HTTP messages that are sent to/from this Google, server, enter the expression"http && ip.addr == 64.233.169.104" (without quotes) into the Filter: field in Wireshark .
3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses andTCP source and destination ports on the IP datagram carrying this HTTP GET?
4. At what time4 is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IPdatagram carrying this HTTP 200 OK message?
5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What arethe source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client?

NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Network Lab (CL3001)
Lab Session 13

Objective:

- Introduction to Access Control List (ACL)
- Types of ACL
- Advantages of ACL
- Rules of ACL
- ACL Implementation in Packet Tracer
- Lab Exercise

ACCESS CONTROL LIST (ACL)

1. Introduction to Access Control List (ACL):

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network. ACLs are mainly found in network devices with packet filtering capabilities including routers and switches.

Different ACLs have different working mechanisms based on what they do. For File system ACLs, they work by creating tables that inform the operating system of access privileges given for certain system subjects. Each object has a unique security property that acts as an identification factor in its access control list. Some privileges include read/write privileges, file execution, and several others.

Some popular operating systems utilizing this mechanism include Unix-based systems, Windows NT/2000, and Novell's Netware.

In the case of Networking ACLS, they are installed in networking devices (Routers and switches) with the sole purpose of filtering traffic. This is done by using pre-defined rules that decided which packets transferred. Source and destination IP addresses also play a major role in this decision.

Packet filtering improves network security by decreasing network traffic access, restricting device and user access to the involved network.

Access lists are sequential, and are made up of two major components; permit and deny statements. A name and a number are used to identify access lists.

ACL Features

1. The set of rules defined are matched serial wise i.e. matching starts with the first line, then 2nd, then 3rd, and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

Once the access-list is built, then it should be applied to inbound or outbound of the interface:

Inbound access lists –
When an access list is applied on inbound packets of the interface then first the packets will be processed according to the access list and then routed to the outbound interface.

Outbound access lists –
When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.

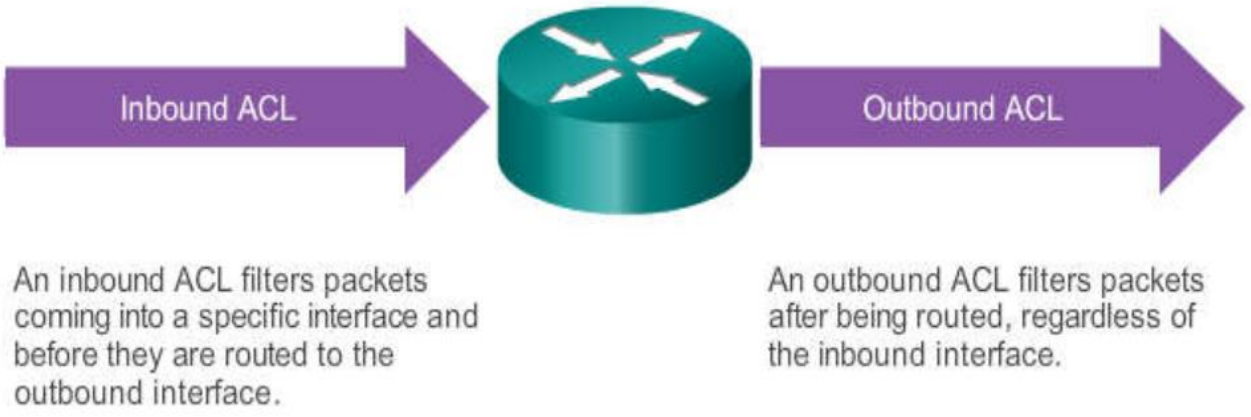


Fig-1: Inbound & Outbound

2. Types of ACL:

There are four types of ACLs that play different roles in a network including, Standard, Reflexive, Extended, and Dynamic:

1. Standard ACL

These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.

2. Extended ACL

These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

3. Reflexive ACL

Also known as IP session ACLs, Reflective ACLs use upper-layer session details to filter traffic.

4. Dynamic ACL

As the term suggests, Dynamic ACLs are reliable on extended ACLs, Telnet, and authentication. They grant users access to a resource only if the user authenticates the device through telnet.

Also, there are two categories of access-list:

1. ***Numbered access-list*** – These are the access list that cannot be deleted specifically once created i.e., if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list then the whole access list will be deleted. The numbered access-list can be used with both standard and extended access lists.

2. ***Named access list*** – In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list, unlike numbered access list. Like numbered access lists, these can be used with both standards and extended access lists.

3. Advantages of ACL:

- Improve network performance.
- Provides security as the administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of the network.

4. Rules of ACL:

1. The standard Access-list is generally applied close to the destination (but not always).
2. The extended Access-list is generally applied close to the source (but not always).
3. We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.
4. We can't remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule then the whole ACL will be removed. If we are using named access lists then we can delete a specific rule.
5. Every new rule which is added to the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.
6. As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.
7. Standard access lists and extended access lists cannot have the same name.

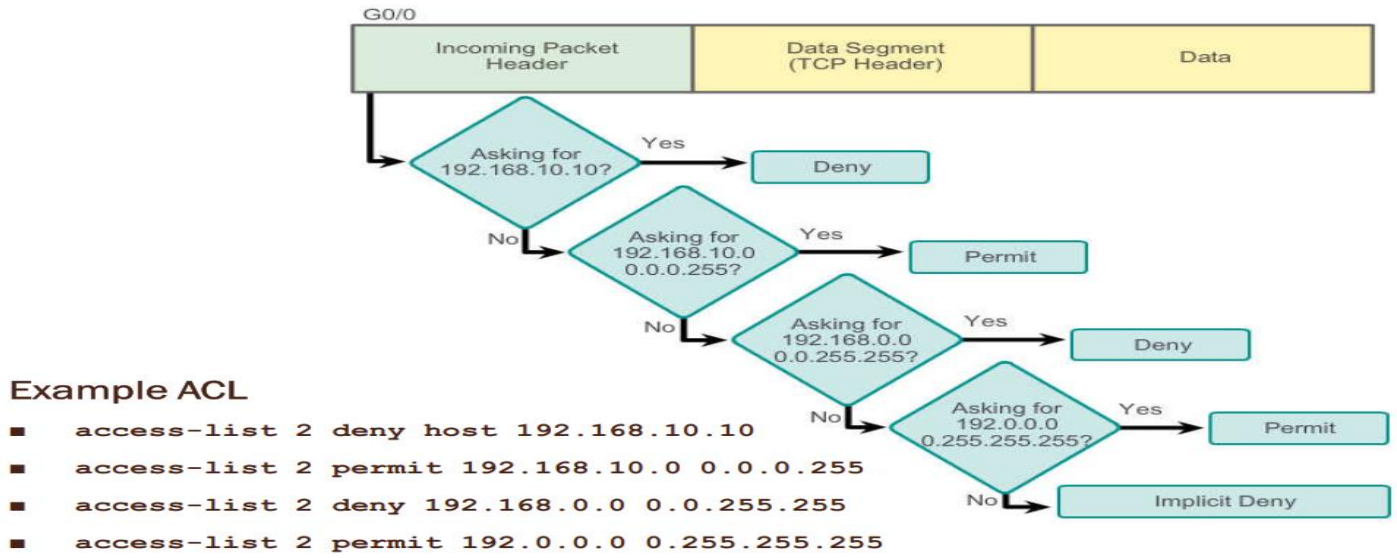


Fig-2: Flow of ACL checking packet

5. ACL Implementation in Packet Tracer:

Create the network topology given in figure 3. Implement IP addresses scheme and configure RIPv2 in routers. Then ping server from laptop 1 to test the connectivity.

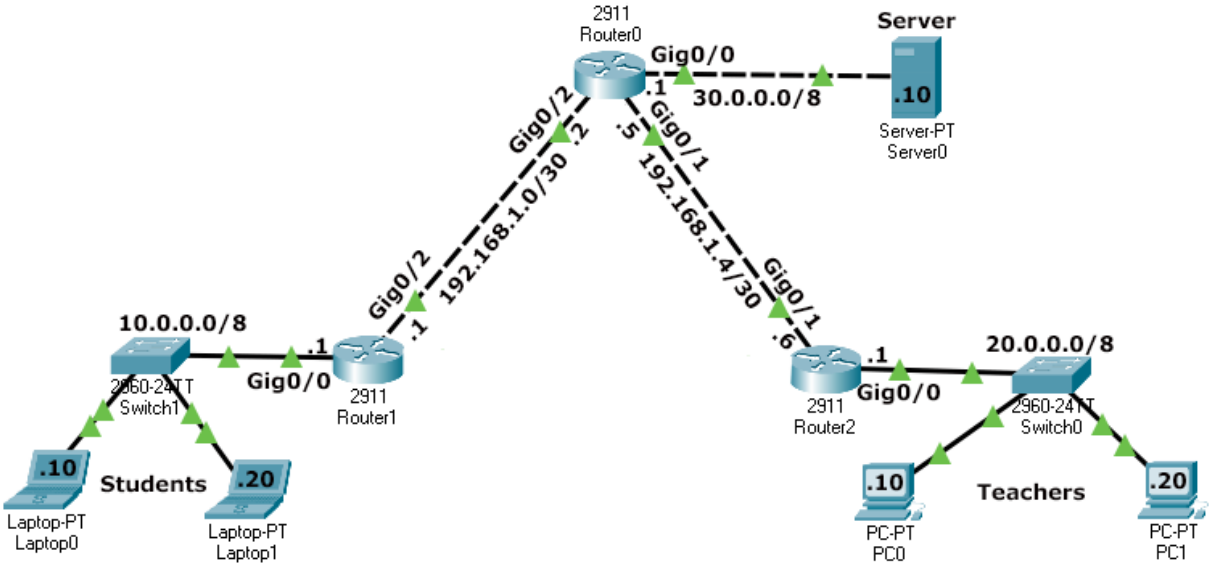


Fig-3: Network Topology showing Student & teacher subnets

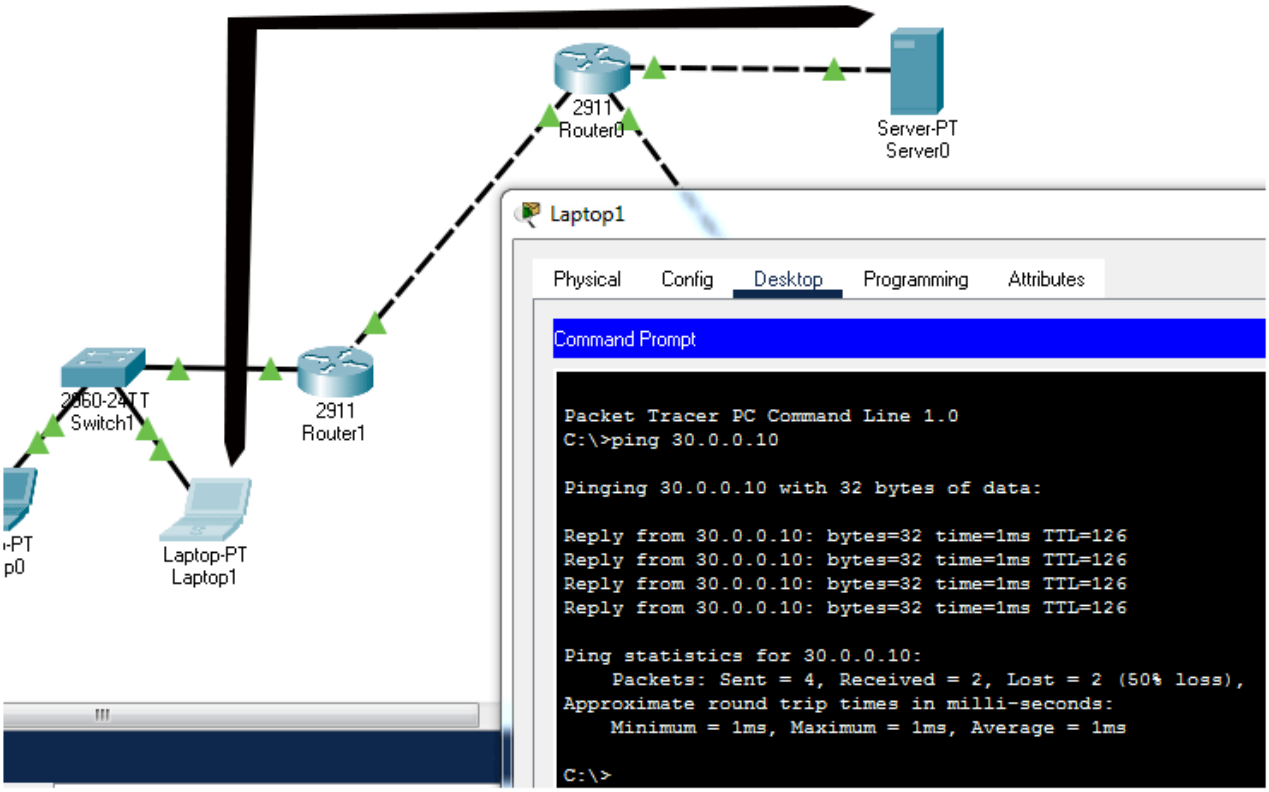


Fig-4: Connectivity between laptop 1 & server

Create and implement a standard access list that blocks the student's section from accessing the Server section.

The students section uses IP subnet 10.0.0.0/8. All packets originating from this section have an IP address from this subnet. If we create a standard ACL with a deny statement for this subnet, all packets having an IP address from this subnet in their source address will be dropped.

A router's interface uses the ACL to filter traffic passing through it. An incorrectly implemented ACL can block entire traffic passing through it. Before creating and implementing an ACL, we have to select the correct interface and the correct direction for the ACL.

In our network, we have seven locations where we can implement the ACL. The following image shows these locations and the direction in which they can be used to filter traffic.

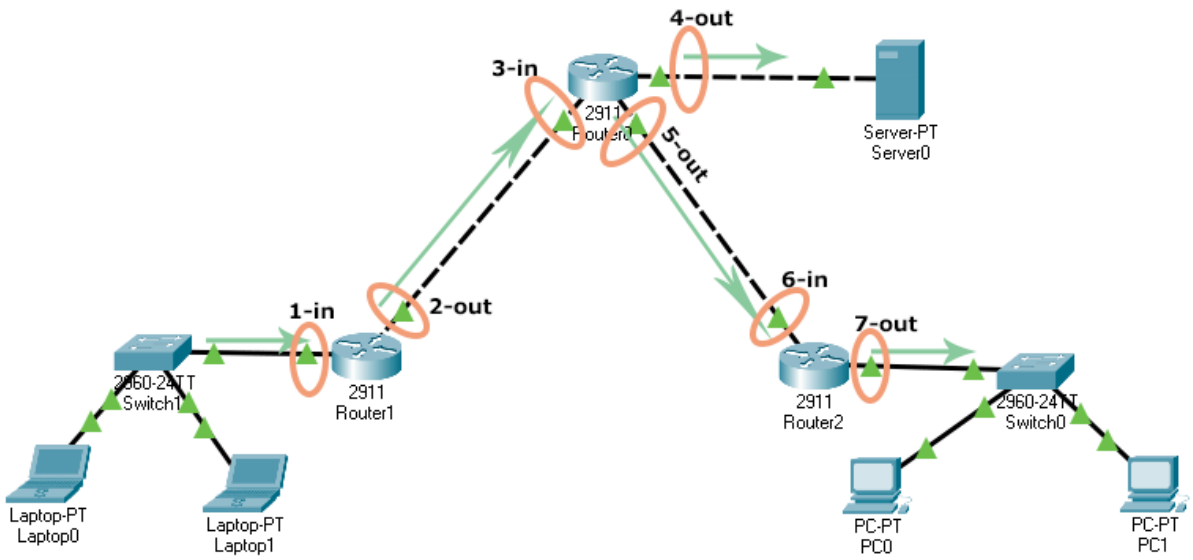


Fig-5: Network Topology showing all inbound & outbound

Location	Interface	Direction	Effect
1	Router1's Gig0/0	In	The student's section will not be able to access the Server and the Teachers section.
2	Router1's Gig0/2	Out	The student's section will not be able to access the Server and Teachers section.
3	Router0's Gig0/2	In	The student's section will not be able to access the Server and Teachers section.
4	**Router0's Gig0/0**	**Out**	**The student's section will not be able to access the Server section but it will be able to access the Teachers section.**
5	Router0's Gig0/1	Out	The student's section will not be able to access the Teachers section but it will be able to access the Server section.
6	Router1's Gig0/1	In	The student's section will not be able to access the Teachers section but it will be able to access the Server section.
7	Router1's Gig0/0	Out	The student's section will not be able to access the Teachers section but it will be able to access the Server section.

Table-1: Shows location & impact of ACL

Standard ACL configuration commands

We have two commands to create a standard access list. These commands are 'access-list' and 'ip access-list'. The 'ip access-list' command has an advantage over the 'access-list' command. It allows us to update or modify statements. We have already learned how to use the 'access-list' command to create a standard access list in the previous part of this tutorial. In this part, let's use the 'ip access-list' command.

The 'ip access-list' is a global configuration mode command. To create a standard access list, it uses the following syntax.

Router(config)# ip access-list standard ACL_#

In the above syntax, the ACL_# is the name or number of the standard ACL. When you hit the enter key after entering this command, the command prompt changes and you enter standard ACL configuration mode.

Router(config-std-acl)#

In standard ACL configuration mode, you can use the following syntax to create statements.

Router(config)# ip access-list standard ACL_name
Router(config-std-acl)# permit|deny source_IP_address [wildcard_mask]

An ACL does nothing until it is applied to an interface. To apply a standard ACL to an interface, enter the interface configuration mode of the interface and use the following command.

Router(config)# interface type [slot_#]port_#
Router(config-if)# ip access-group ACL_# in|out

Once an ACL is activated on an interface, the interface processes all packets through it.

Now applying ACL on Router 0.

Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list standard BlockStudents
Router(config-std-nacl)#deny 10.0.0.0 0.255.255.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip access-group BlockStudents out
Router(config-if)#exit
Router(config)#exit
Router#

Let's discuss the above commands. We used the first two commands to enter global configuration mode. The next command creates a standard ACL named **BlockStudents**. In ACL configuration mode, we added two statements. The first statement denies all traffic from the 10.0.0.0/8 subnet. The second statement allows all other traffic. We used the next commands to exit ACL configuration mode and enter interface configuration mode. The next command applies the **BlockStudents** ACL in the out direction. The last two commands exit interface configuration mode and global configuration mode, respectively.
To verify the ACL, we can test connectivity between sections. The student's section should not be able to access the Server section but it should be able to access the Teachers section. The Teachers section should be able to access both the Server and the Students section. You can use the ping command to test connectivity. The following image shows this testing.

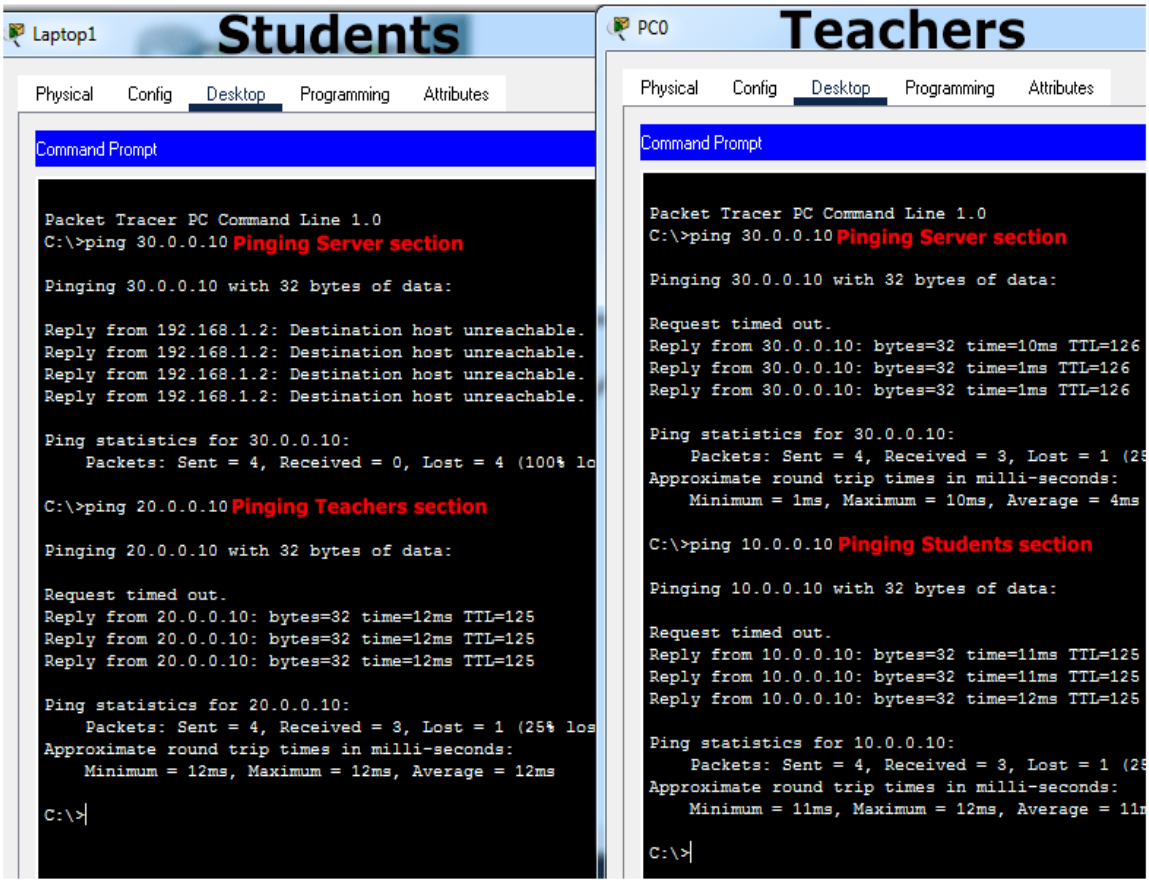


Fig-6: Verifying ACL

To modify or update a standard ACL statement, use the following steps.

- Use the 'show access-lists' command to view the sequence number of the statement.
- Enter standard ACL configuration mode
- Delete the existing statement with the 'no [*sequence number*]' command
- Insert the modified, updated, or the new statement with the sequence number of the old statement

Let's take an example. Suppose, instead of blocking the entire subnet we only want to block a single host (10.0.0.10/8) from the student's section. For this, access the CLI prompt of Router0 and run the following commands.

Router>
Router#show access-lists
Standard IP access list BlockStudents
10 deny 10.0.0.0 0.255.255.255
20 permit any
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list standard BlockStudents
Router(config-std-nacl)#no 10
Router(config-std-nacl)#10 deny 10.0.0.10 0.0.0.0
Router(config-std-nacl)#exit
Router(config)#exit
Router#
Router#show access-lists

Standard IP access list BlockStudents
10 deny host 10.0.0.10
20 permit any
Router#

Let's understand the above commands.

First, we checked the sequence number of the statement that we had used to block the entire Students section. As we can in the above output, the sequence number of the statement is 10. After it, we entered the ACL configuration mode of the ACL. In ACL configuration mode, we deleted the current statement with the 'no *sequence_number_of_statement*' command. In the end, we inserted the new statement at the place of the existing statement.

Since the ACL is already active on the interface, the interface starts using the new statement as soon as it is added. To verify the change, send ping requests again from the blocked host and the allowed host. The following image shows this testing.

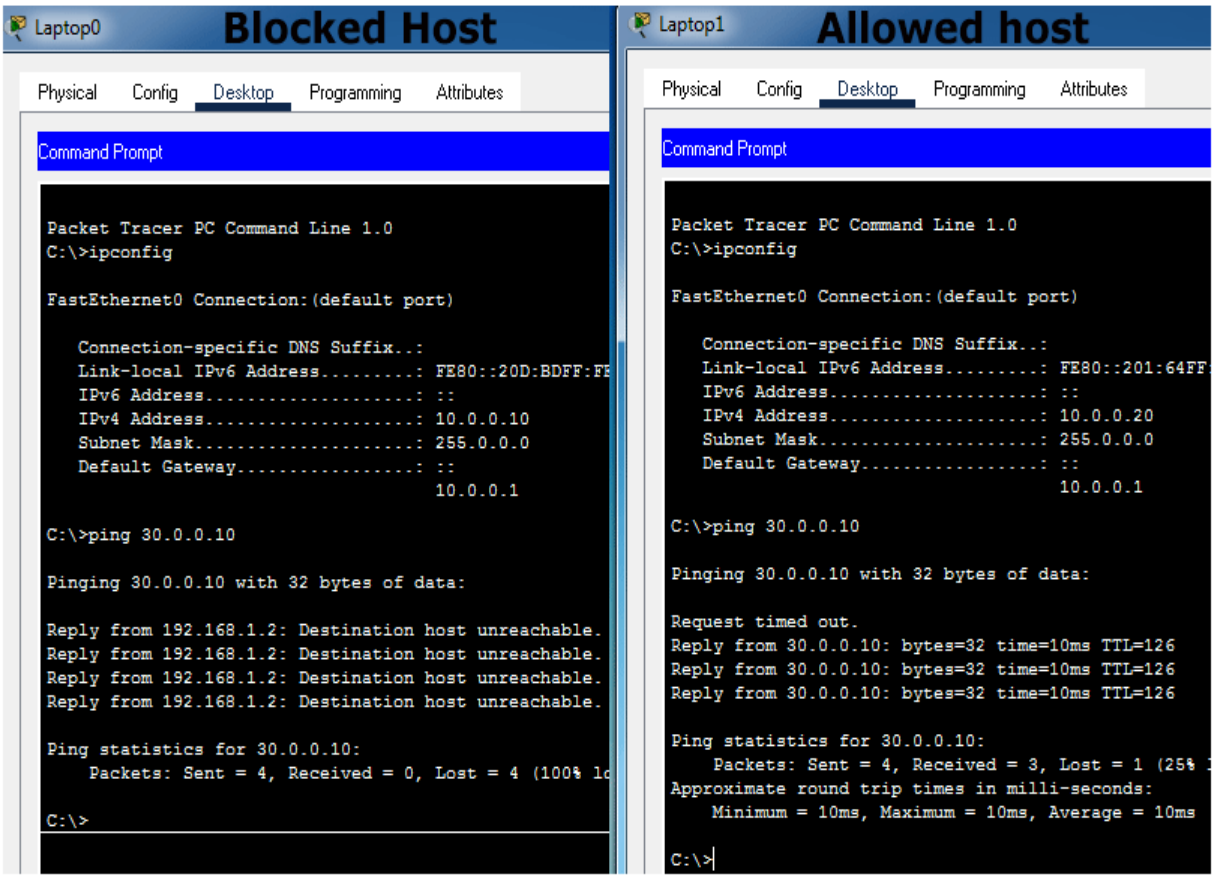


Fig-7: Verifying Modify ACL

6. Lab Exercise:

Create the given network Topology in figure 8. Apply IP given IP scheme which is shown in table II. Where xx are your student ID two digits.

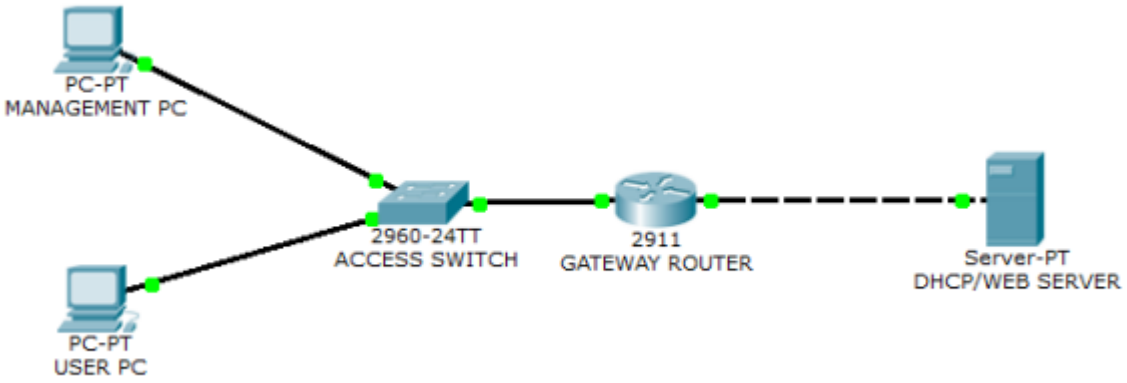


Fig-8: Network Topology for Task

Addressing Table			
Device	**IP Address**	**Subnet Mask**	**Default-Gateway**
Management PC	xx.1.0.1	255.255.255.0	xx.1.0.254
User PC	xx.1.0.2	255.255.255.0	xx.1.0.254
Gateway Router G0/0	xx.1.0.254	255.255.255.0	
Gateway Router G0/1	xx.2.0.254	255.255.255.0	
DHCP / WEB server	xx.2.0.1	255.255.255.0	xx.2.0.254

Table-II: Addressing scheme of above network topology

Q1) Configure the network and verify the connection between PCs & server.

Q2) Create a standard named ACL (such as TEL) to limit access of Telnet of router by any other devices only Management PC can access router Telnet.

Q3) Create an extended ACL to only limit the web traffic to pass and block other services by server.