Lab Manual
For
Computer Networks Lab

(BCAE592B)

(BCA 5th semester)

INDEX

Experiment-1

Aim of the experiment: Recognize the physical topology and cabling (coaxial, OFC, UTP, STP) of a network.

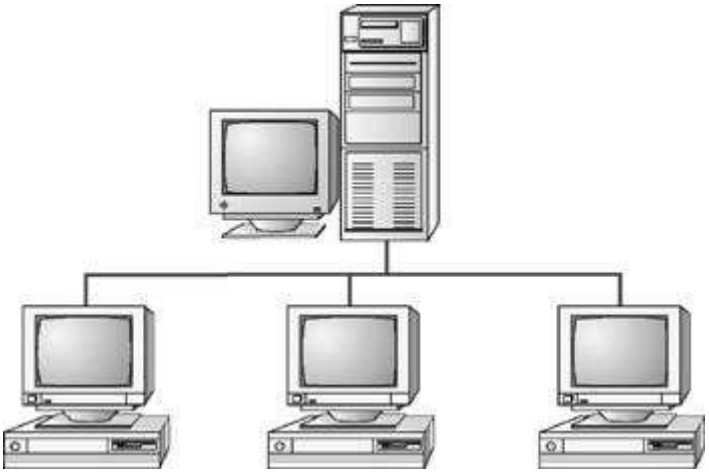
Apparatus Required: Twisted pair cable (STP&UTP), Coaxial and OFC

Theory:

Physical Topology: Every LAN has a topology, or the way that the devices on a network are arranged and how they communicate with each other. It is the physical layout of deviceson a network. The way that the workstations are connected to the network through the actual cables that transmit data the physical structure of the network is called the physical topology. We can form four basic types of network topology.

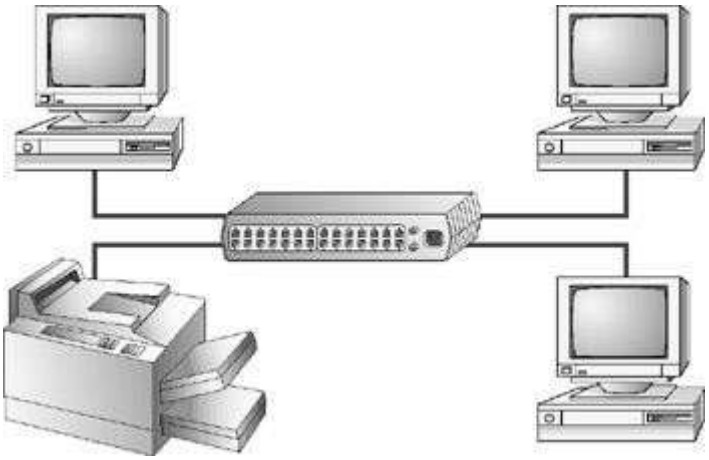
A. Bus:

A single cable to which all network nodes are directly connected.



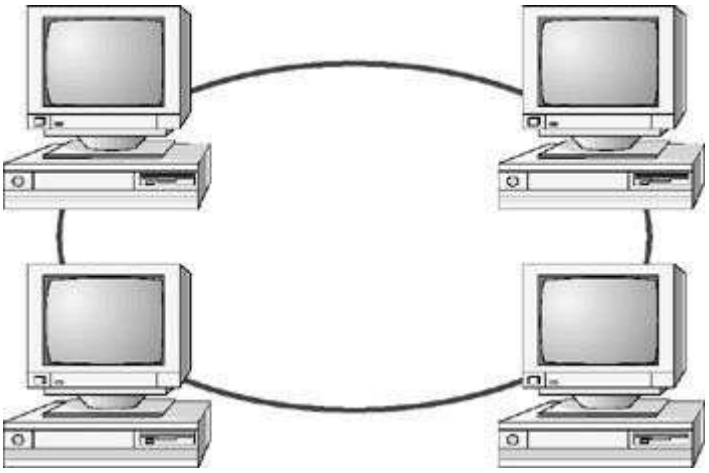
B. Star:

A topology with a single access point or a switch at the center of the topology; all the other nodes are connected directly to this point.



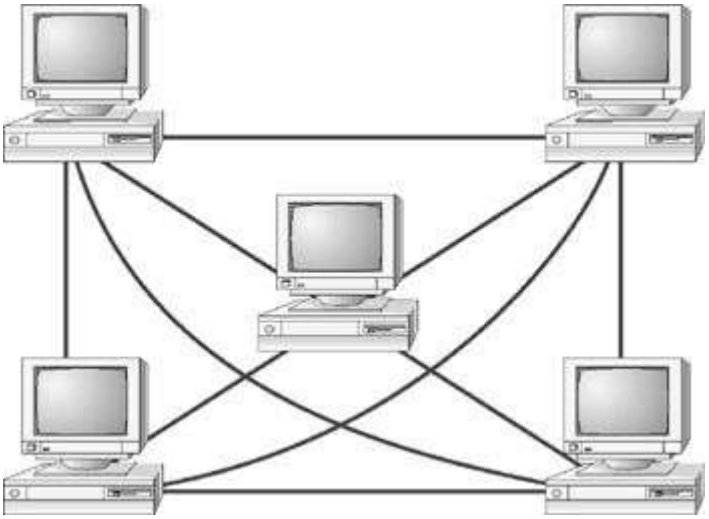
C. Ring:

Each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it.



D. Mesh:

Each device is connected to every other device on the network through a dedicated point-to-point link.



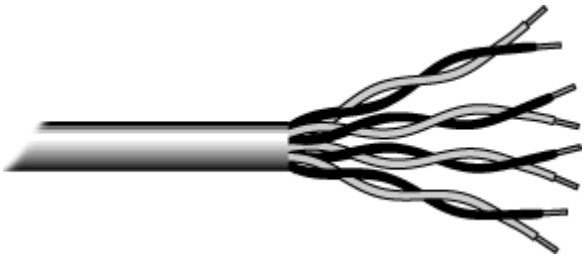
Study of cables:

The following cables are used in the network.

i. UTP
ii. STP
iii. Coaxial
iv. OFC

UTP:

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular.



The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. It has six categories.

STP:

STP stands for Shielded twisted pair. STP is similar to unshielded twisted pair (UTP); however, it contains an extra foil wrapping or copper braid jacket to help shield the cable signals from interference. In STP grounding cable is required.

Coaxial:

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

OFC:

Fibre optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fibre optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair.

Result:

In the above experiments, different physical topology and different network cables are recognized successfully and understood the function of each topology as well as network cables.

Experiment-2

Aim of the experiment: Recognition and use of various types of connectors RJ-45, RJ-11, BNC and SCST.

Apparatus Required: RJ-45, RJ-11, BNC and SCST connectors

Theory:

RJ-45:

The standard connector for UPT and STP cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (RJ-11). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

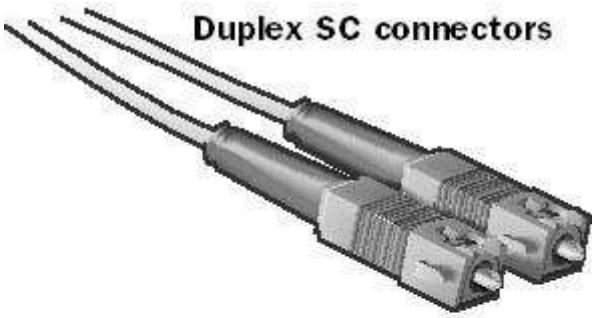
BNC Connector:

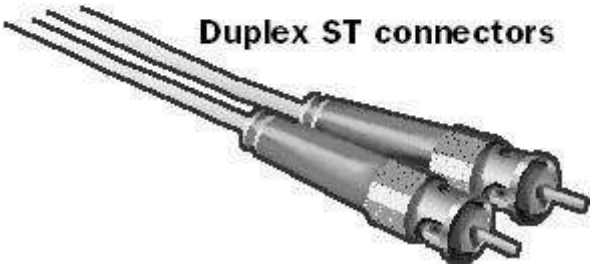
The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

SC and ST Connector:

SC stands for subscriber connector and is a standard-duplex fiber-optic connector with a square moulded plastic body and push-pull locking features. SC connectors are typically used in data communication, CATV, and telephony environments.

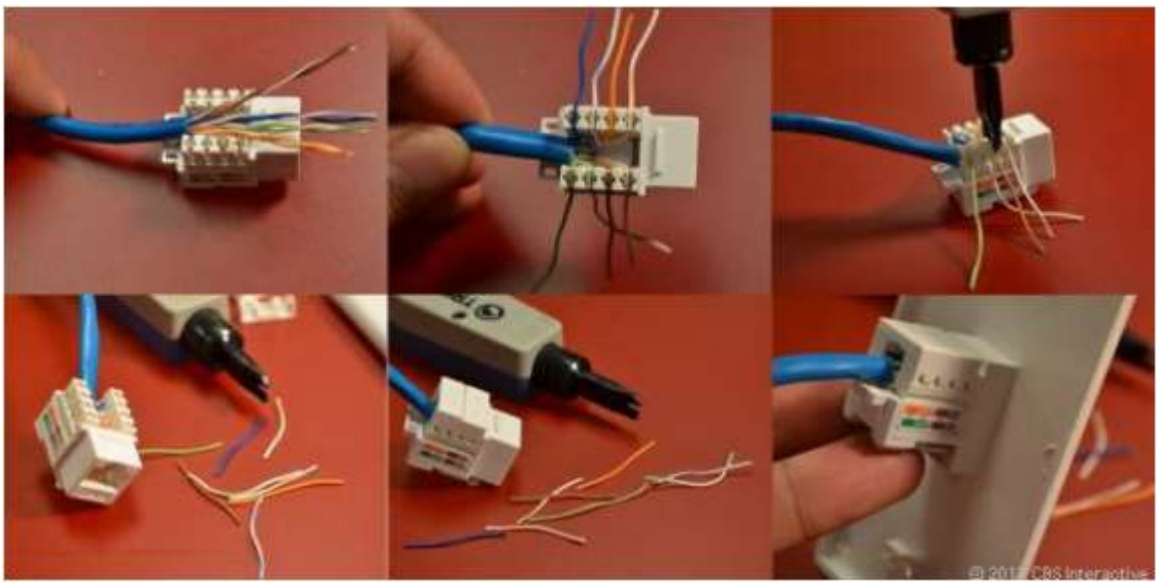
ST stands for straight tip, a high-performance fiber-optic connector with round ceramic ferrules and bayonet locking features. ST connectors are more common than SC connectors. Generally the SC and ST connectors used with either single-mode or multimode fiber-optic cabling.





Result:
In the above experiments, different connectors are used in different network cables are recognized successfully.

IO connector crimping: Run the full length of Ethernet cable in place, from endpoint to endpoint,
making sure to leave excess.
At one end, cut the wire to length leaving enough length to work, but not too much excess.
Strip off about 2 inches of the Ethernet cable sheath.
Align each of the colored wires according to the layout of the jack.
Use the punch down tool to insert each wire into the jack.
Repeat the above steps for the second RJ45 jack.



Testing the crimped cable using a cable tester:

Step 1 : Skin off the cable jacket 3.0 cm long cable stripper up to cable

Step 2: Untwist each pair and straighten each wire 190 0 1.5 cm long.

Step 3 : Cut all the wires

Step 4 : Insert the wires into the RJ45 connector right white orange left brown the pins facing up

Step 5 : Place the connector into a crimping tool, and squeeze hard so that the handle reaches its full swing.

Step 6: Use a cable tester to test for proper continuity.

Result:

Cable Crimping, Standard Cabling and Cross Cabling, IO connector crimping and testing the crimped cable using a cable tester are done successfully

Experiment-3

Aim of the experiment: Making of cross cable and straight cable.

Apparatus/Tools/Equipments/Components Required:

1. RJ-45 connector,
2. Crimping Tool,
3. Twisted pair Cable,
4. Cable Tester.

Procedure:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.

2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

3. You have 2 end jacks, which must be installed on your cable. If you are using a pre- made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

Diagram shows you how to prepare Cross wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Diagram shows you how to prepare straight through wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Cable Crimping Steps:

1. Remove the outmost vinyl shield for 12mm at one end of the cable (we call this side A-side).
2. Arrange the metal wires in parallel
3. Insert the metal wires into RJ45 connector on keeping the metal wire arrangement.

4. Set the RJ45 connector (with the cable) on the pliers, and squeeze it tightly.
5. Make the other side of the cable (we call this side B-side) in the same way.

Testing the crimped cable using a cable tester:

Step 1: Skin off the cable jacket 3.0 cm long cable stripper up to cable

Step 2: Untwist each pair and straighten each wire 190 0 1.5 cm long.

Step 3: Cut all the wires.

Step 4: Insert the wires into the RJ45 connector right white orange left brown the pins facing up

Step 5: Place the connector into a crimping tool, and squeeze hard so that the handle reaches its full swing.

Step 6: Use a cable tester to test for proper continuity.

Result:

Cable Crimping, straight Cabling and Cross Cabling, and testing the crimped cable using a cable tester are done successfully.

Experiment-4

Aim of the experiment: Install and configure a network interface card in a workstation.

Apparatus/ Equipment Required:

1. NIC card
2. Desktop/PC
3. Computer Screw driver set
4. Driver Software

Theory:

NICs (Network Interface Card): Network Interface Card, or NIC is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable.

Every networked computer must also have a network adapter driver, which controls the network adapter.

Each network adapter driver is configured to run with a certain type of network adapter.

Procedure:

1. Install the network card:
2. Disconnect all cables connected to the computer and open the case. Locate an available PCI slot (white slots) and insert the network card and secure the card with the screw that came with it. Once the adapter has been installed and secured close the computer case, connect all the cables and turn it on.
3. After installing the adapter driver it should be working find, now let's configure the card for use on a network.
4. Click on the Start button and select Settings then Control Panel. Double click on the System icon
5. Click on the Hardware tab.
6. Click on Device Manager.

You will see a list of devices installed in your computer.

7. If necessary, click on the + sign next to Network Adapters to expand the list.
8. Ensure that there is no yellow exclamation mark (!) next to the Network Adapter. This indicates a possible problem with the card or configuration.
9. Double click on your network driver (e.g. NE2000 Compatible). In the Device Status box you should see the message:
10. This Device is working correctly.

If you do not see this message or if there is no Network Adapter displayed, then your Ethernet card will probably need configuring.

Result:

Installation and configuration of NIC card and transfer files between systems in a LAN have been done successfully.

Experiment-5

Aim of the experiment: Identify the IP address of a workstation and the class of the address and configure the IP Address on a workstation.

Apparatus/ Equipment Required:

PC connected to internet.

Theory:

Identification of IP Address:

An IPv4 address is a 32-bit address that uniquely and universally identifies the connection of a host or a router to the Internet.

The dotted decimal notation an IPv4 address shown below.

Ex: 192.68.12.1

Classification of IP address:

Class A

1.0.0.1 to 126.255.255.254 Supports 16 million hosts on each of 127 networks.

Class B

128.1.0.1 to 191.255.255.254 Supports 65,000 hosts on each of 16,000 networks.

Class

C 192.0.1.1 to 223.255.254.254 Supports 254 hosts on each of 2 million networks.

Class D

224.0.0.0 to 239.255.255.255 Reserved for multicast groups.

Class E

240.0.0.0 to 254.255.255.254 Reserved.

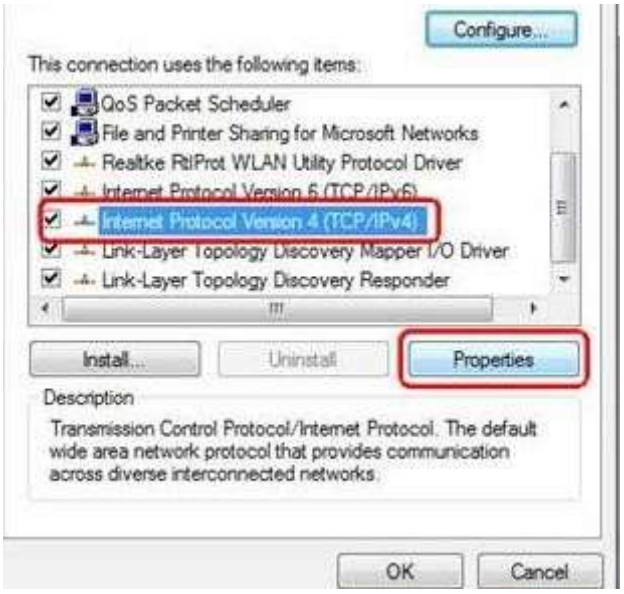
Procedure:

Steps to configure IP address:

Step 1:
1. Click on the Start button and select Control Panel.
2. To check the IP address of the computer, please click on "Network and Internet→ Network and Sharing Center → Change Adapter Settings (on the left)".
3. Then right click on "Ethernet" (right click on Wi-Fi if you want to check the wireless IP address), and go to Status→ Details.
There you will see all the TCP/IP details of this computer.

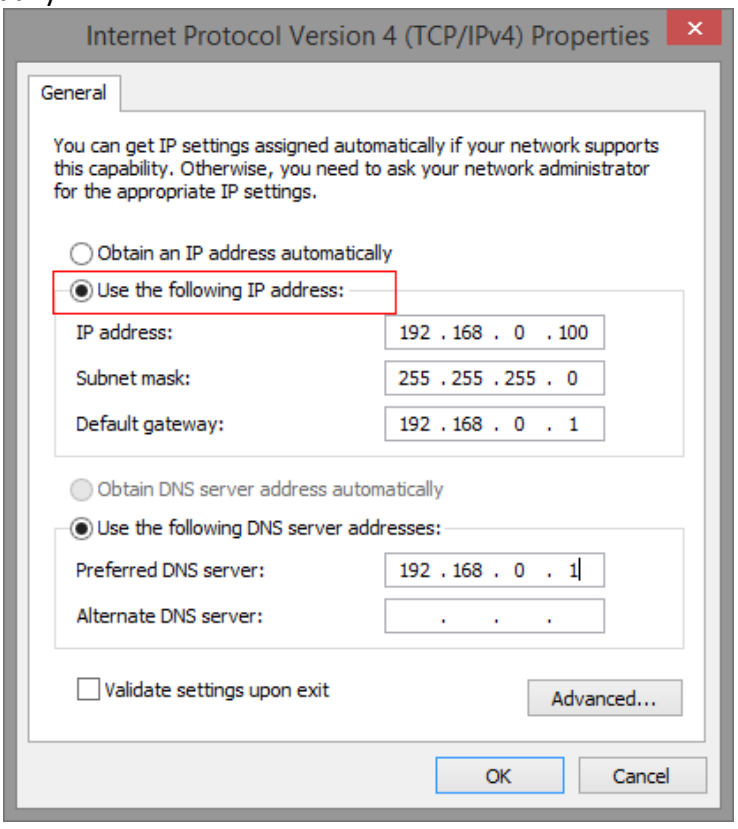
Step 2:

Right click on “Ethernet”, go to “Properties”, and then choose “Internet Protocol Version 4”, click on Properties;



Step 3:

To set manual IP address, please select “Use the following IP address”, and input the IP or DNS address manually.



9. Click OK, then Close to close all boxes.

Result:

Configuration of IP Address in a system in LAN (TCP/IP Configuration) have been done successfully

Experiment-6

Aim of the experiment: Managing user accounts in windows and LINUX

Apparatus/ Equipment Required:

PC with windows OS installed and Linux OS installed.

Procedure:

To go to your user accounts:

1. Go to the Control Panel from the Start Menu.
2. Click Add or remove user accounts.

3. The Manage Accounts pane will appear. You will see all of the user accounts here, and you can add more accounts or manage existing ones.

To create a new account:

1. From the Manage Accounts pane, click Create a new account.
2. Type an account name.

3. Select Standard user or Administrator.
4. Click Create Account.

Changing an account's settings

Once you've created a new account, you may want to add a password or make other changes to the account's settings.

To create a password:

1. From the Manage Accounts pane, click the account name or picture.

2. Click Create a password.

3. Type a password in the New password field, and retype it in the Confirm new password field.

4. If you want, you can type a password hint to help you remember your password.
5. Click Create password.
6. To go back to the Manage Accounts pane, click Manage another account.

Account passwords are case sensitive, which means capital and lowercase letters are treated as different characters. For example, aBc1 is not the same as abc1.

To change your account picture:

You can also change the picture for any account. This picture appears next to the account name and helps you easily identify the account.

1. From the Manage Accounts pane, click the account name or picture.
2. Click Change the picture.

3. Select a picture, or click Browse for more pictures to select one of your own.

4. Click Change Picture.

Result:

Managing user accounts in Windows has successfully done.

Experiment-7

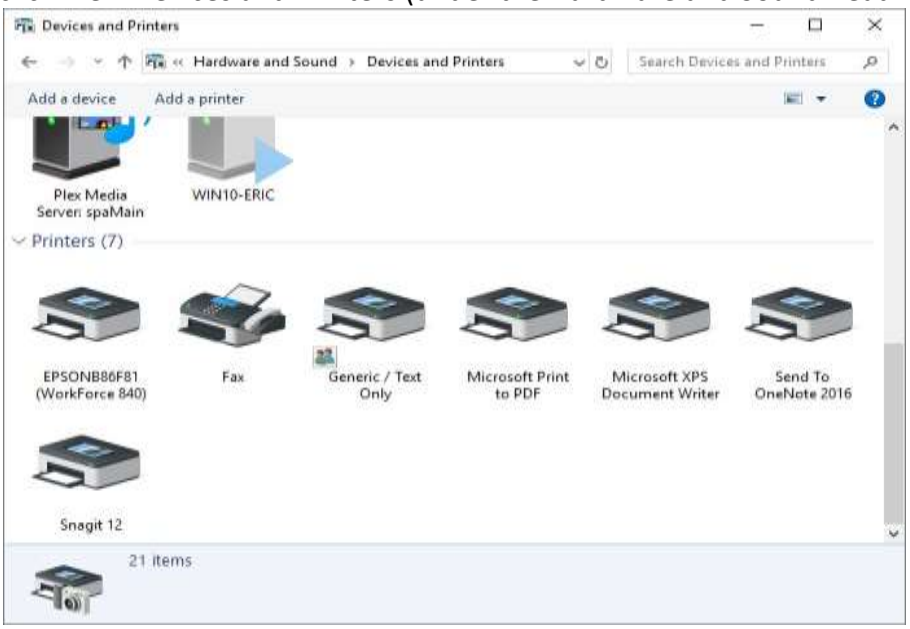
Aim of the experiment: Sharing of Hardware resources in the network.

Apparatus/ Equipment Required:

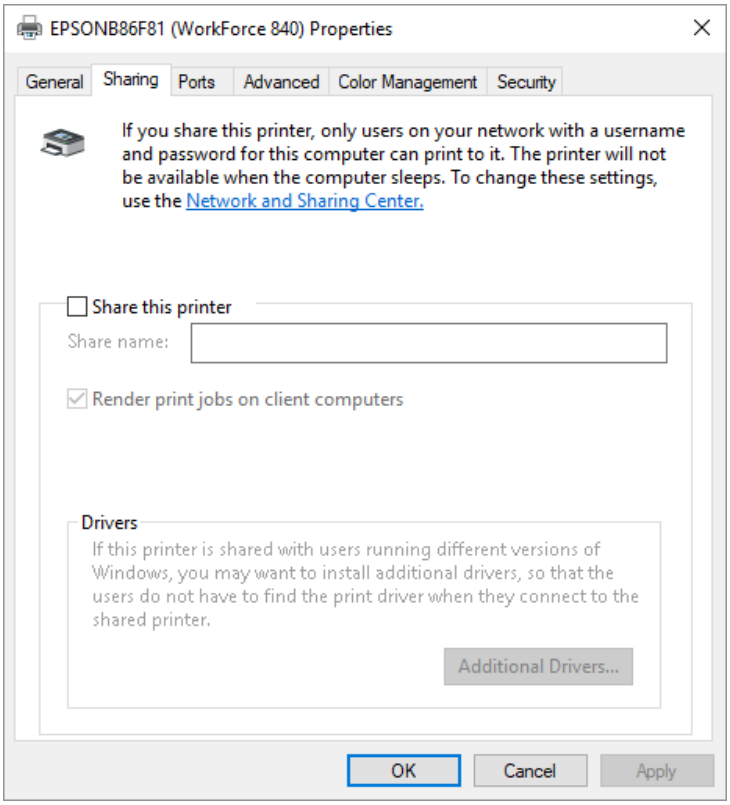
1. Minimum 02 nos. of PCs
2. Printer

Procedure:

1. Network printer can be configured as shared devices so that others on the network can use them.
2. Follow the steps to share printer.
3. Go to the Control Panel from the Start Menu.
4. click View Devices and Printers (under the Hardware and Sound heading).



5. click the printer you want to share from Devices and Printers dialog box.
6. select Printer Properties from the Context menu.

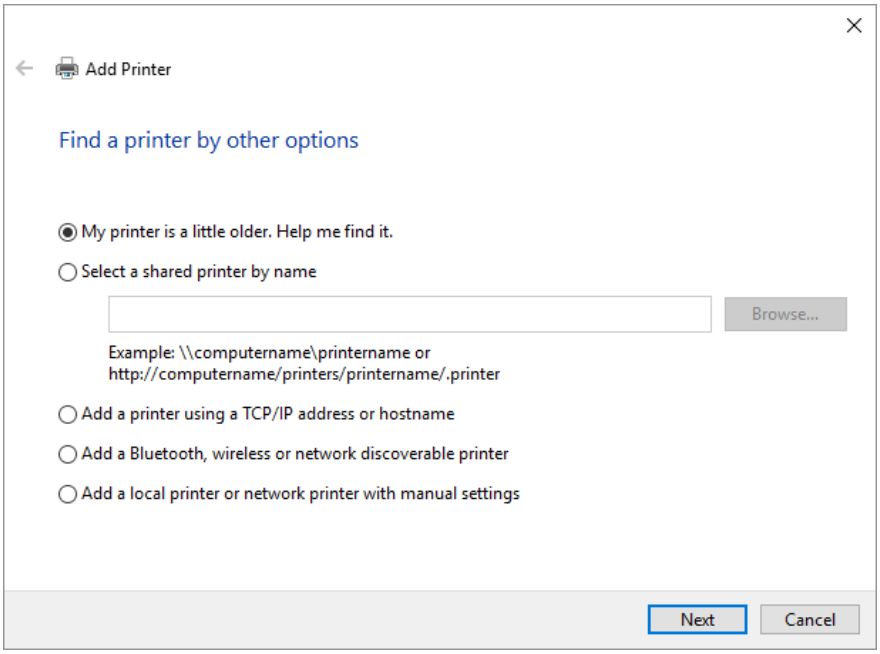


7. Click on the Sharing tab of the printer's Properties dialog box.
8. Click the Share this Printer check box and optionally change the Share Name of the printer.
9. click OK to close the printer's Properties dialog box.

How to access the shared printer:

Now the shared printer is made available to others on your network. In order to access the shared printer from a different system, go to that system

1. Go to the Control Panel from the Start Menu.
2. click View Devices and Printers (under the Hardware and Sound heading).
3. click the Add a Printer option, at the top of the dialog box.
4. Click on The Printer I want isn't Listed if our printer isn't found. Windows displays the Find a Printer by Other Options section of the Add Printer wizard.



5. Click the second option, starts scanning the network for available printers.
6. After all of the printers have been found, select the printer name that you want to use and click Next.
7. The network printer is added to the computer's list of available printers. Click Finish to finish the process.

Result:

Sharing of hardware resources (Network Printer) successfully done in a network among devices connected to it.

Experiment-8

Aim of the experiment: Use of Netstat and its options.
Apparatus/ Equipment Required:

PC connected with internet connection.

Theory:

The **netstat** command is used to display the TCP/IP network protocol statistics and information.

Procedure:

1. **Netstat is a command for checking network and Internet connections.**
2. **Netstat command uses following syntax and switches.**

Syntax and switches:

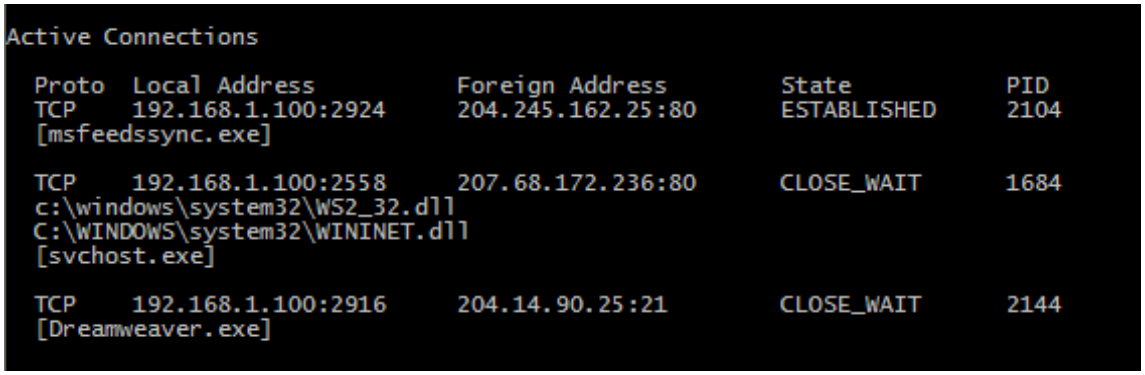
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

Switches	Description
-a	Displays all connections and listening ports.
-b	Displays the executable involved in creating each connection or listening port. In some cases, well-known executables host multiple independent components, and in these cases, the sequence of components involved in creating the connection or listening port is displayed. In this case, the executable name is in [] at the bottom. Note that this option can be time-consuming and fails unless you have sufficient permissions.
-e	Displays Ethernet statistics. This option may be combined with the -s option.
-f	Displays FQDN (fully qualified domain names) for foreign addresses.
-n	Displays addresses and port numbers in numerical form.
-o	Displays the owning process ID associated with each connection.
-p proto	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may

	be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-t	Displays the current connection offload state.
-x	Displays NetworkDirect connections, listeners, and shared endpoints.
-y	Displays the TCP connection template for all connections. Cannot be combined with the other options.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics. If omitted, netstat prints the current configuration information once.

Command:

C:\>NETSTAT



Command:

C:\>NETSTAT -S

```
C:\Windows\system32>netstat -s | findstr Errors
 Received Header Errors = 0
 Received Address Errors = 0
 Received Header Errors = 0
 Received Address Errors = 0
 Errors 0 0
```

```
 Errors  0 0
 Receive Errors = 0
 Receive Errors = 0
C:\Windows\system32>
```

Command:

C:\>NETSTAT -E

```
C:\Windows\system32>netstat -e
Interface Statistics
 Received Sent
Bytes 8988576 2105244
Unicast packets 12972 11880
Non-unicast packets 0 0
Discards 0 0
Errors 0 0
Unknown protocols 0
C:\Windows\system32>
```

Result:

All the option of netstat command used and executed successfully.

Experiment-9

Aim of the experiment: Connectivity troubleshooting using PING, IPCONFIG

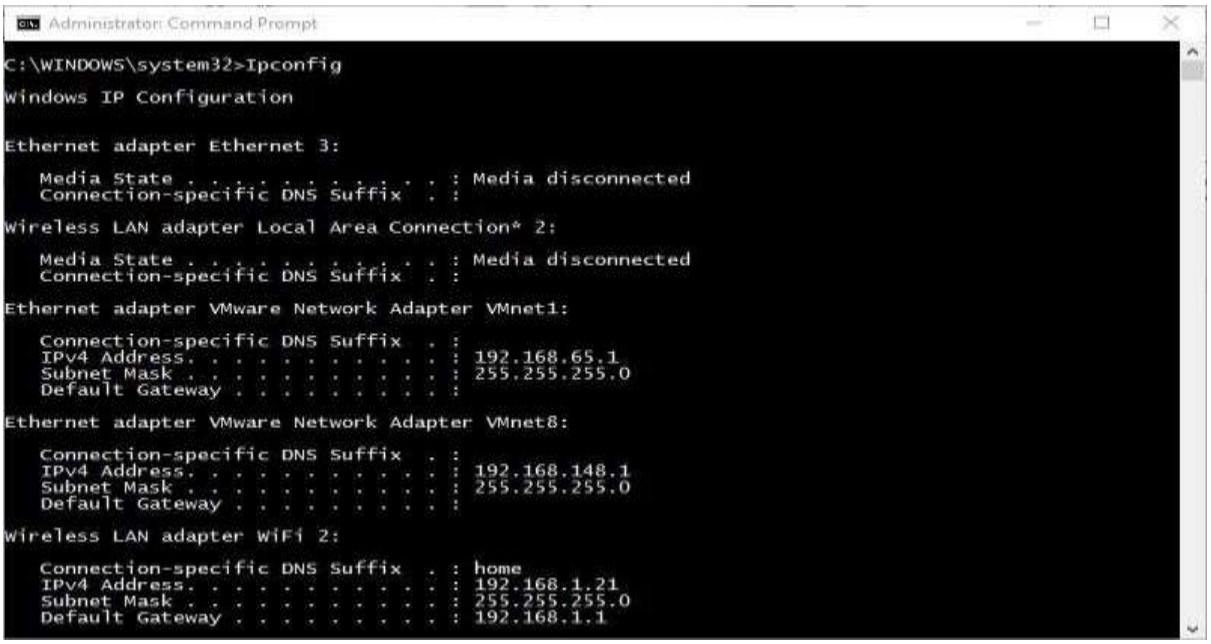
Apparatus/ Equipment Required:

PC connected with internet connection.

Procedure:

Troubleshoot the internet connectivity by using PING and IPCONFIG.

1. Open Command Prompt, and then type ipconfig. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.



3. At the command prompt, ping the loopback address by typing ping 127.0.0.1.

Command:

C:\>ping 127.0.0.1

4. Ping the IP address of the computer.

Command:

C:\> ping 192.168.1.1

5. Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.

6. Ping the IP address of a remote host (a host that is on a different subnet).

If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.

7. Ping the IP address of the DNS server.

If the ping command fails, verify that the DNS server IP address is correct that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

Result:

Troubleshoot the internet connectivity by using IPCONFIG and PING command successfully.

Experiment-10

Aim: Connect the computers in Local Area Network.
Procedure: On the host computer

On the host computer, follow these steps to share the Internet connection:

1. Log on to the host computer as Administrator or as Owner.
2. Click Start, and then click Control Panel.
3. Click Network and Internet Connections.
4. Click Network Connections.
5. Right-click the connection that you use to connect to the Internet. For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other network available.
6. Click Properties.
7. Click the Advanced tab.
8. Under Internet Connection Sharing, select the Allow other network users to connect through this computer's Internet connection check box.
9. If you are sharing a dial-up Internet connection, select the Establish a dial-up connection whenever a computer on my network attempts to access the Internet check box if you want to permit your computer to automatically connect to the Internet.
10. Click OK. You receive the following message:

When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0. 1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

11. Click Yes. The connection to the Internet is shared to other computers on the local area network (LAN).

The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0. 1 and a subnet mask of 255.255.255.0

On the client computer

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client computer. To confirm the LAN adapter IP configuration, follow these steps:

1. Log on to the client computer as Administrator or as Owner.

2. Click Start, and then click Control Panel.

3. Click Network and Internet Connections.

4. Click Network Connections.

5. Right-click Local Area Connection and then click Properties.

6. Click the General tab, click Internet Protocol (TCP/IP) in the connection uses the following items list, and then click Properties.

7. In the Internet Protocol (TCP/IP) Properties dialog box, click Obtain an IP address automatically (if it is not already selected), and then click OK. Note: You can also assign a unique static IP address in the range of 192.168.0.2 to 254. For example, you can assign the following static IP address, subnet mask, and default gateway:

8. IP Address 192.168.31.202

9. Subnet mask 255.255.255.0

10. Default gateway 192.168.31.1

11. In the Local Area Connection Properties dialog box, click OK.

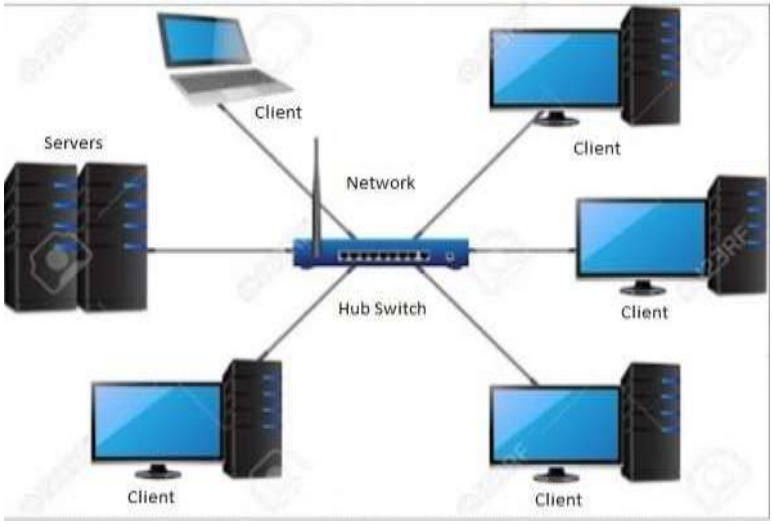
12. Quit Control Panel

Experiment-11

Aim of the experiment: Create a network of at least 6 computers.
Apparatus/ Equipment Required:

1. 06 no's of computers (01 server and 05 clients)
2. Switch
3. Required Cables

Procedure:



1. Take the computer for which you are making server, insert the second LAN in that computer.
2. Connect your internet connection into the first LAN (inbuilt) on that computer.
3. Enter the IP address which you got from your ISP and check whether you can able to use internet on that system.
4. Now make sure that the second LAN is detected and is showing Unplugged.
5. Open properties of the first LAN (inbuilt LAN) and then go to "Advanced" option which is available on the top, then check both the boxes and say ok. and close everything.
6. Now take an Internet cable which is crimped on both the sides with same colours of wires.
7. Connect one end to the second LAN and the other end to the switch.
8. Now open your second LAN properties and go to the TCP/IP properties and there enter IP address as (192.168.0.1) or anything you wish Subnet Mask (255.255.255.0) and the gateway as (192.168.0.1).
9. Now open click on the switch and you will get a notification on your server saying that "Local Area Connection 2" is connected.
10. Now take another Internet cable and one end of that cable should be in any one port of the Switch and the other should be in the second computer.
11. Now you will get a notification that you are connected to internet, open the LAN properties and enter the IP address as (192.168.0.2) subnet mask and gateway should be same as server.

Result:
Successfully created a network using 06 nos of computers.

Experiment-12

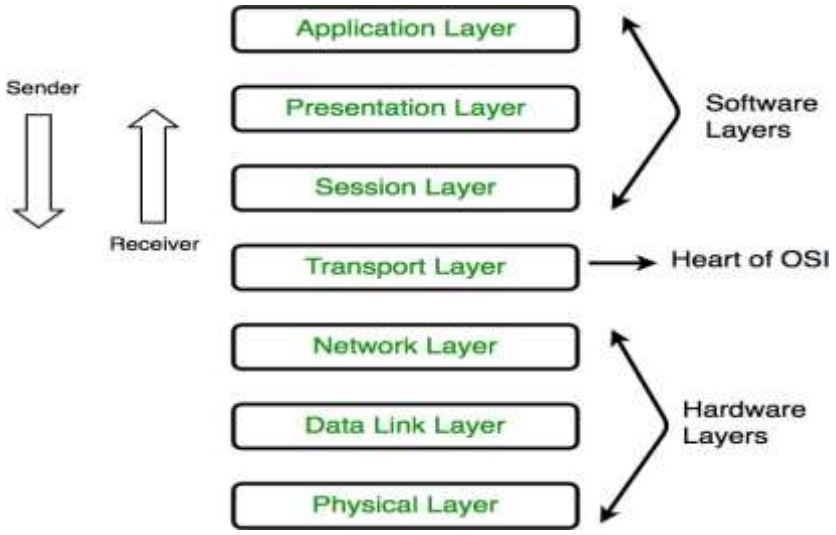
Aim of the experiment: Study of Layers of Network and Configuring Network Operating System.

Apparatus/ Equipment Required:

PC connected with internet connection.

Theory:

Layers of Network:



1. Physical Layer (Layer 1):

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. This layer is responsible for Bit synchronization, Bit rate control, Physical topologies, Transmission mode.

2. Data Link Layer (DLL) (Layer 2):

The data link layer is responsible for the node to node delivery of the message. This layer is responsible for Framing, Physical addressing, Error control, Flow Control, Access control.

3. Network Layer (Layer 3):

Network layer works for the transmission of data from one host to the other located in different networks. This layer is responsible for Routing, Logical Addressing.

4. Transport Layer (Layer 4):

Transport layer provides services to application layer and takes services from network layer. This layer is responsible for Segmentation and Reassembly, Service Point Addressing.

5. Session Layer (Layer 5):

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

6. Presentation Layer (Layer 6):

Presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

7. Application Layer (Layer 7):

At the very top of the OSI Reference Model stack of layers is Application layer which produce the data, which has to be transferred over the network.

Ex: Application – Browsers, Skype Messenger etc.

Procedure:

Configuring Network Operating System.

Basic Task:

- Check for System update
- Setup time zone
- Assign Static IP Address
- Enable Remote Desktop
- Rename server

Configuration steps:

1. Open server manger on virtual box.
2. Click on local server and download windows update and update the window.
3. Click on the Time zone to set the time accordingly.
4. Click on the Ethernet, it will redirect to the network connection wizard (Control panel→network and internet→ network connection)
5. Right click on the Ethernet, go to properties, select internet protocol version4(TCP/IP4).
6. Click on the properties, select the second option
   "Use the following IP address"
   IP Address 172.16.72.5
   Subnet mask 255.255.255.0
   Default gateway 172.16.72.1
   "Use the following DNS server address"
   Preferred DNS server 172.16.72.5
   Alternate DNS server 8.8.8.8
7. Click on ok and close all the console.
8. Click on the remote desktop and turn it to enable and click on refresh button.
9. Close all the open window and restart the computer.

Result:

Network operating system "Windows server 2019" successfully configured.

Experiment-13

Aim of the experiment: Study of Routing and Switching, configuring of Switch and Routers, troubleshooting of networks.

Apparatus/ Equipment Required:

CISCO Packet Tracer software

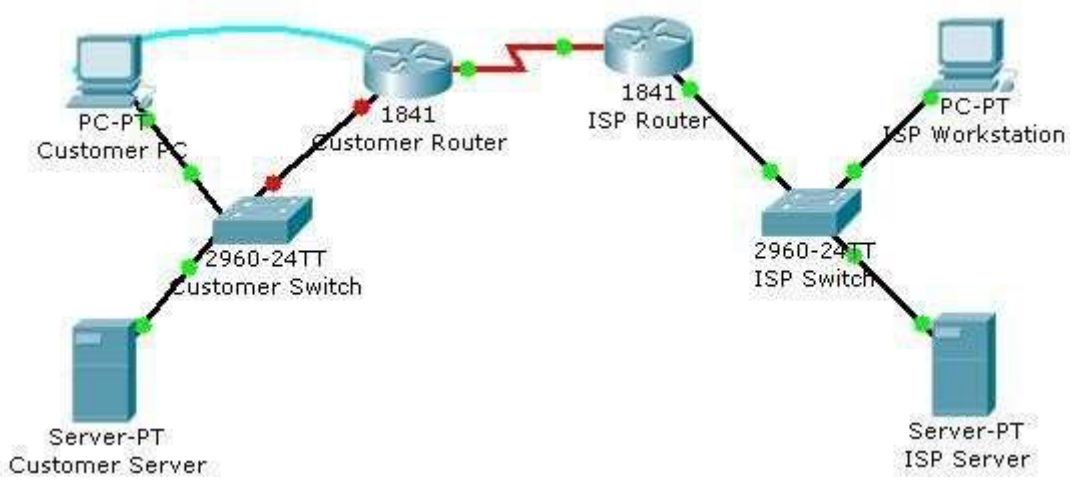
Theory:

Routing and Switching:

Routing and switching are the basic functions of network communication. Routing and Switching are different functions of network communications. The function of Switching is to switch data packets between devices on the same network (or same LAN - Local Area Network). The function of Routing is to Route packets between different networks (between different LANs - Local Area Networks).

Procedure:

Switch configuration (configuration of Cisco Catalyst 2960 switch.):



Topology Diagram

Step 1: Configure the switch host name.

a. From the Customer PC, use a console cable and terminal emulation software to connect to the console of the customer Cisco Catalyst 2960 switch.

b. Set the host name on the switch to **GpblsSwitch** using these commands.

Switch>**enable**
Switch#**configure terminal**
Switch(config)#**hostname GpblsSwitch**

Step 2: Configure the privileged mode password and secret.

a. From global configuration mode, configure the password as **cisco**.

GpblsSwitch (config)#**enable password gpbls**

b. From global configuration mode, configure the secret as **gpbls123**.

GpblsSwitch (config)#**enable secret gpbls123**

Step 3: Configure the console password.

a. From global configuration mode, switch to configuration mode to configure the console line. GpblsSwitch (config)#**line console 0**

b. From line configuration mode, set the password to **cisco** and require the password to be entered at login.

```
GpblsSwitch (config-
line)#password gpbls
GpblsSwitch (config-line)#login
GpblsSwitch (config-line)#exit
```

Step 4: Configure the vty password.

a. From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

GpblsSwitch (config)#**line vty 0 15**

b. From line configuration mode, set the password to **cisco** and require the password to be entered at login.

```
GpblsSwitch (config-
line)#password gpbls
GpblsSwitch (config-line)#login
GpblsSwitch (config-line)#exit
```

Step 5: Configure an IP address on interface VLAN1.

a. From global configuration mode, switch to interface configuration mode for VLAN1, and assign the IP address 192.168.1.5 with the subnet mask of 255.255.255.0.

```
GpblsSwitch (config)#interface vlan 1
GpblsSwitch (config-if)#ip address 192.168.1.5 255.255.255.0
GpblsSwitch (config-if)#no shutdown
GpblsSwitch (config-if)#exit
```

Step 6: Configure the default gateway.

a. From global configuration mode, assign the default gateway to 192.168.1.1.

GpblsSwitch (config)#**ip default-gateway 192.168.1.1**

b. Click the **Check Results** button at the bottom of this instruction window to check your work.

Step 7: Verify the configuration.

a. The Customer Switch should now be able to ping the ISP Server at 209.165.201.10. The first one or two pings may fail while ARP converges.

GpblsSwitch (config)#**end**
GpblsSwitch #**ping 209.165.201.10**

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.10, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 181/189/197 ms
GpblsSwitch #

b. Router configuration (Cisco Router 1841 ISR)

Step 1: Configure the router host name.

a. On Customer PC, use the terminal emulation software to connect to the console of the customer Cisco

1841 ISR.

b. Set the host name on the router to **GpblsRouter** by using these commands.

Router>**enable**
Router#**configure terminal**
Router(config)#**hostname**
GpblsRouter

Step 2: Configure the privileged mode and secret passwords.

a. In global configuration mode, set the password to **cisco**.
b. GpblsRouter(config)#**enable password gpbls**
c. Set an encrypted privileged password to **gpbls123** using the **secret** command.
d. GpblsRouter (config)#**enable secret gpbls123**

Step 3: Configure the console password.

a. In global configuration mode, switch to line configuration mode to specify the console line.

GpblsRouter (config)#**line console 0**

Set the password to **gpbls123**, require that the password be entered at login, and then exit line configuration mode.

GpblsRouter (config-line)#**password gpbls123**
GpblsRouter (config-
line)#**login** GpblsRouter
(config-line)#**exit**
GpblsRouter (config)#

Step 4: Configure the vty password to allow Telnet access to the router.

a. In global configuration mode, switch to line configuration mode to specify the vty lines.

GpblsRouter (config)#**line vty 0 4**

Set the password to **gpbls123**, require that the password be entered at login, exit line configuration mode, and then

exit the configuration session.

```
GpblsRouter (config-line)#password gpbls123
GpblsRouter (config-
line)#login GpblsRouter
(config-line)#exit
GpblsRouter (config)#
```

Step 5: Configure password encryption, a MOTD banner, and turn off domain server lookup.

a. Currently, the line passwords and the enable password are shown in clear text when you show the running configuration. Verify this now by entering the **show running-config** command.
b. To avoid the security risk of someone looking over your shoulder and reading the passwords, encrypt all clear text passwords.

```
GpblsRouter (config)#service password-encryption
```

c. Use the **show running-config** command again to verify that the passwords are encrypted. To provide a warning when someone attempts to log in to the router, configure a MOTD banner.

```
GpblsRouter (config)#banner motd $Authorized Access Only!
```

d. Test the banner and passwords. Log out of the router by typing the **exit** command twice. The banner displays before the prompt for a password. Enter the password to log back into the router.
e. You may have noticed that when you enter a command incorrectly at the user or privileged EXEC prompt, the router pauses while trying to locate an IP address for the mistyped word you entered. For example, this output shows what happens when the **enable** command is mistyped.

```
GpblsRouter >emable
```

f. Translating "enable"...domain server (255.255.255.255)
g. To prevent this from happening, use the following command to stop all DNS lookups from the router CLI.

```
GpblsRouter(config)#no ip domain-lookup
```

h. Save the running configuration to the startup configuration.

```
GpblsRouter(config)#end
GpblsRouter#copy run start
```

Step 6: Verify the configuration.

a. Log out of your terminal session with the Cisco 1841 customer router.
b. Log in to the Cisco 1841 Customer Router. Enter the console password when prompted.
c. Navigate to privileged EXEC mode. Enter the privileged EXEC password when prompted.

d. Click the **Check Results** button at the bottom of this instruction window to check your work

Result:

configuration of Cisco Catalyst 2960 switch and 1841 Router successfully done.

Experiment-14

Aim of the experiment: Study of Scaling of Networks, Design verities of LAN and forward of Traffic.

Apparatus/ Equipment Required:

CISCO Packet Tracer software

Theory:

The Scaling Networks defines the architecture, components, and operations of routers and switches in a larger and more complex network. It includes how to configure routers and switches for advanced functionality. It also includes configuration and troubleshoot routers and switches and resolve common issues with OSPF, EIGRP, STP, and VTP in both IPv4 and IPv6 networks.

Procedure:

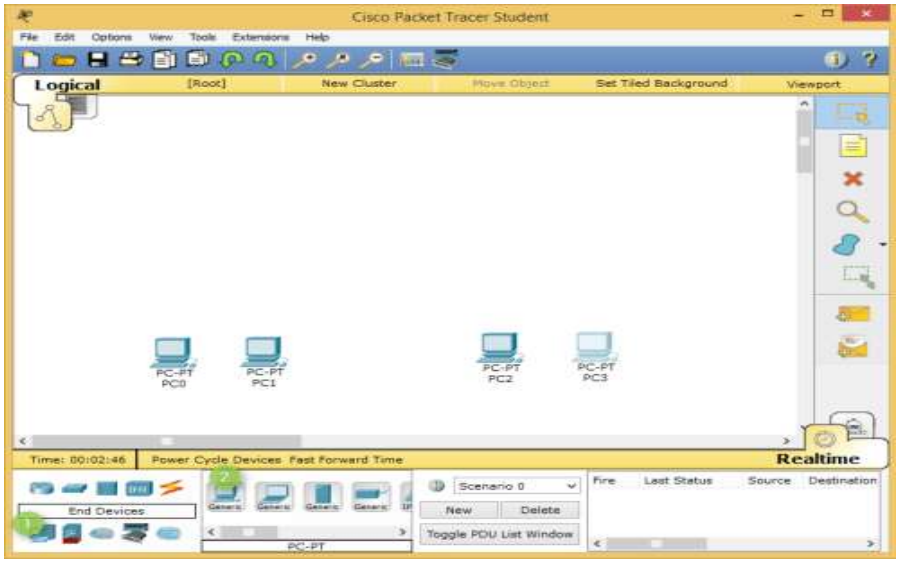
Design varieties of LAN and forward of Traffic:

Adding PCs in Cisco Packet Tracer

To add PCs in Cisco Packet Tracer, you need to perform the following steps:

In the Cisco Packet Tracer console, click on the PC icon, click Generic, and then click in the logical view area to add a Generic PC.

Repeat the same step to add three more Generic PCs in the logical view area, as shown in the following figure.



Adding Switches in Cisco Packet Tracer

To add a switch in Cisco Packet Tracer, click the Switch icon, select a switch type, such as 2960, and then add the selected switch in the logical view area.

Repeat the same step to add one more switch.

Adding Routers in Cisco Packet Tracer

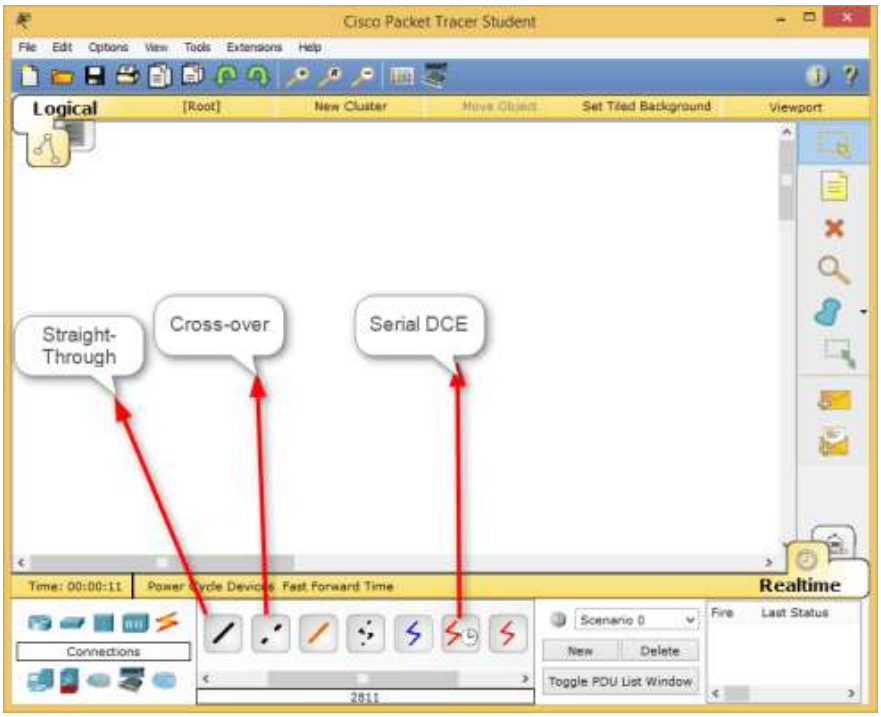
To add a router in Cisco Packet Tracer, click the Router icon, select a router type, such as 2811, and then add the selected router in the logical view area.

Repeat the same step to add one more router.

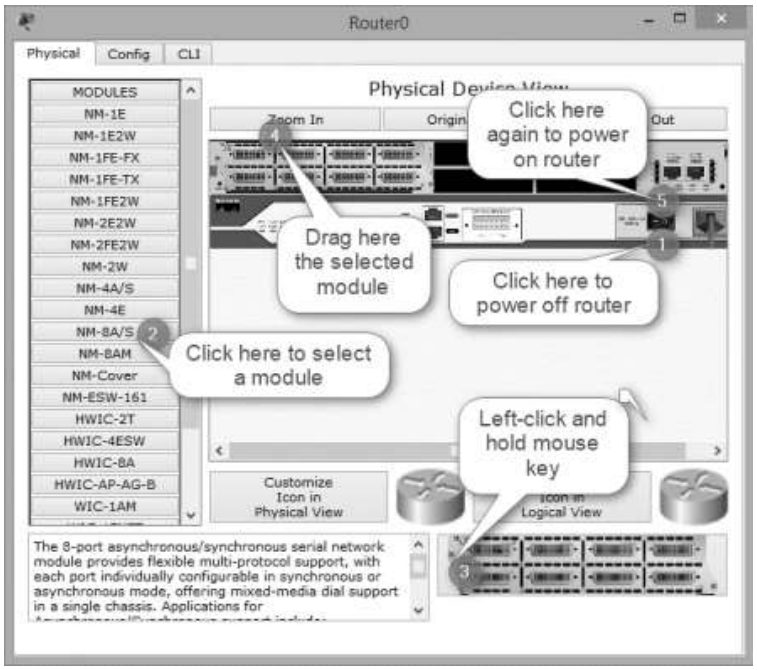
Types of Connection in Cisco Packet Tracer

Straight-through: Used to connect different types of devices (devices that use different wiring standards), such as Router-to-Switch and Switch-to-PC.

Cross-over: Used to connect same types of devices, such as router-to-router, PC-to-PC, and switch-to-switch.
Serial DCE: Used to connect router-to-router in a WAN network.
Console: Used to take console (using hyper terminal) of a router on a PC.



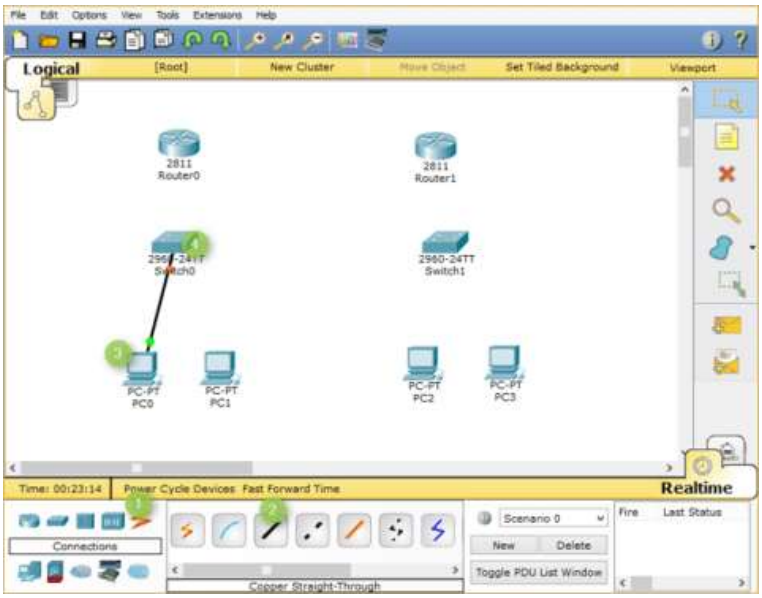
Customize the interfaces before it can be used to connect other network devices. To do this, double-click Router0, on the Router0 properties dialog box, click the Power button to power off Router0.



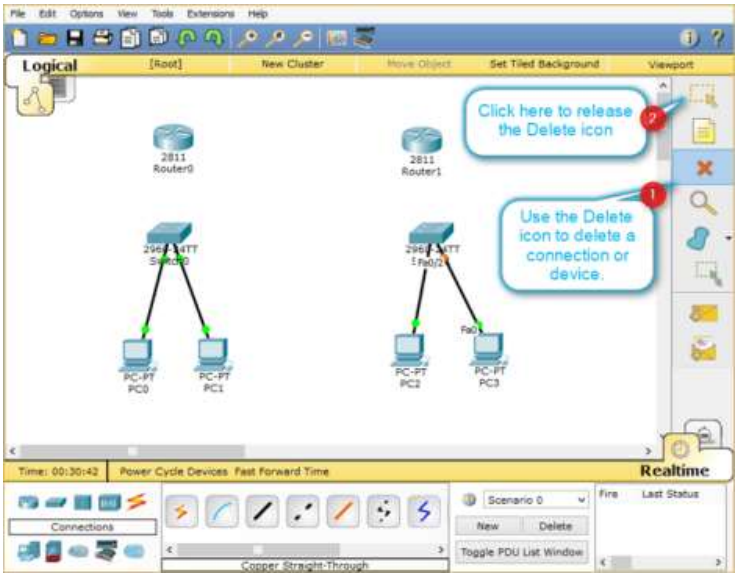
Now, open the Router1 properties dialog box, add the same module to Router1 also, and then close the Router1 properties dialog box.

Connecting Devices in Cisco Packet Tracer

To connect devices in Cisco Packet Tracer, click the connection type icon, and select an appropriate cable. For example, to connect PC0 to Switch0, select the straight-through cable, click on PC0, select the FastEthernet0 interface.
Next, click on Switch0, and then select the FastEthernet0/1 interface. The following figure displays how to connect a PC to a switch in Cisco Packet Tracer.

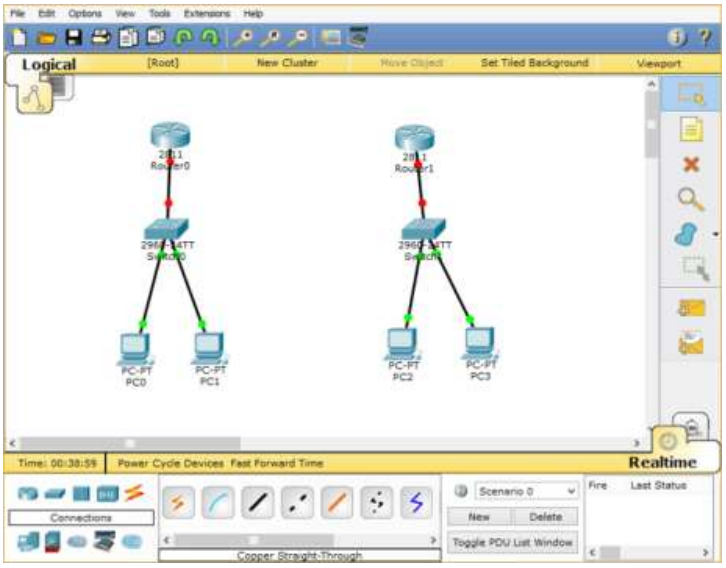


Now, add PC1 to Switch0 using the FastEthernet0/2 interface. Also, add PC2 and PC3 to the FastEthernet0/1 and FastEthernet0/2 interfaces of Switch1, respectively.
If you have connected a wrong device to a wrong interface, you can use the Delete option to delete a connection or device. The following figure displays how to use the Delete option to delete a device or connection in Cisco Packet Tracer.



Once, you have connected all the PCs to switches, now, connect Switch0 to Router0, and Switch1 to Router1 using the straight-through cables.
Select the straight-through cable, click on Switch0, and then select FastEthernet0/3 interface.
Click Router0 and select the FastEthernet0/0 interface.
Select again the straight-through cable, click on Switch1, and select FastEthernet0/3 interface.

Next, click Router1 and then select the FastEthernet0/0 interface.

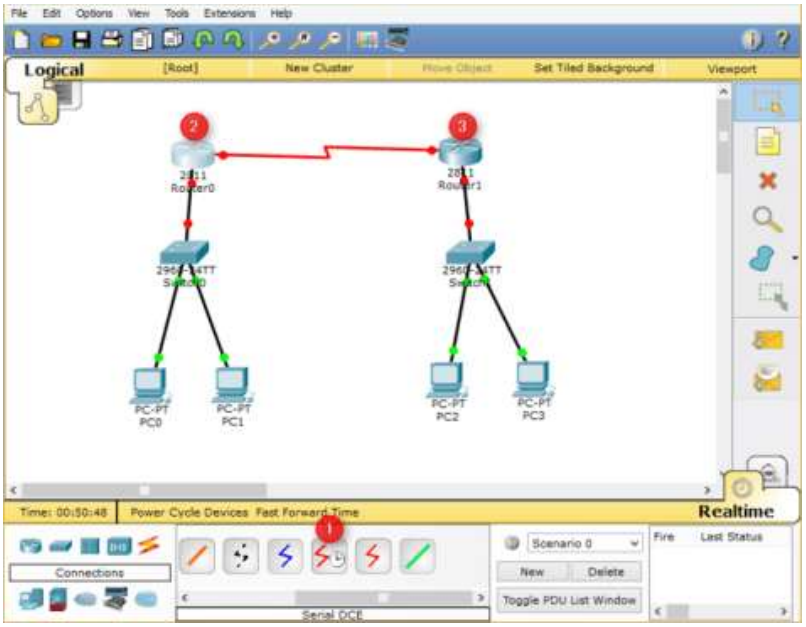


Interconnecting Routers in Cisco Packet Tracer

Now, connect Router0 to Router1 using the serial connection. To do this, you need to perform the following steps:

Select the Serial DCE cable, click on Router0, and select the Serial1/0 interface.

Click on Router1 and select the Serial1/0 interface, as shown in the following figure.



Result:

Verities of LAN is created successfully.

Experiment-15

Aim of the experiment: Study WAN concepts and Configure and forward Traffic in WAN.

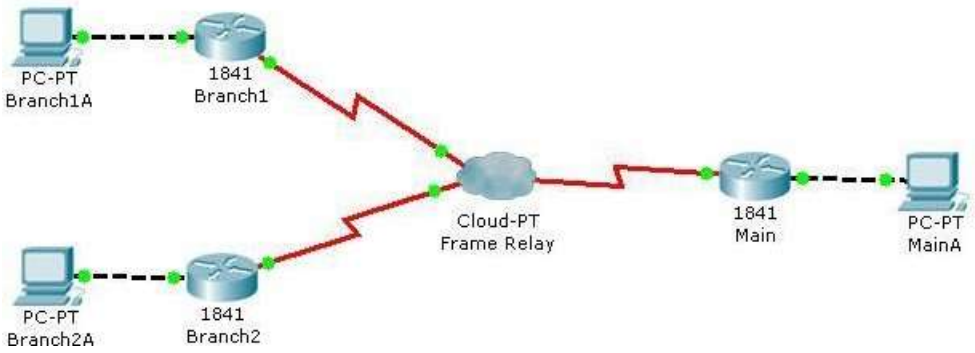
Apparatus/ Equipment Required:

CISCO Packet Tracer software

Theory:

Wide Area Network, or WAN, is used to connect physically separated locations on a network. WANs can connect buildings that are across town or across the world on the same network. There are various techniques to do this, but two of the most common are hub and spoke and full mesh networks topologies.

Configure and forward Traffic in WAN:



Step 1: Configuration of Branch1 and Branch2 (Switch).

a. Click on Branch1 and use various show commands to view the connectivity to the network. b. Use the show running-configuration command to view the router configuration.

c. Use the show ip interface brief command to view the status of the interfaces.

d. Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi commands to see the status of the Frame-relay circuit.

e. Click on Branch 2 and use various show commands to view the connectivity to the network. f. Use the show running-configuration command to view the router configuration.

g. Use the show ip interface brief command to view the status of the interfaces.

h. Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi commands to see the status of the Frame-relay circuit.

Step 2: Configuration of Main (Router).

a. Click on Main and use a variety of show commands to view the connectivity to the network. b. Use the show running-configuration command to view the router configuration.

c. Use the show ip interface brief command to view the status of the interfaces.

d. To view the status of the frame-relay configurations use the show frame-relay lmi, show frame- relay map, and show frame-relay pvc commands.

Result:

Configuration of WAN done successfully.

Experiment-16

Aim of the experiment: Configure IPv4 and IPv6 and learn Quality, security and other services.

Procedure:

Configure IPv4:

Configure IPv4 DHCP

Step 1. Log in to the web-based utility and choose LAN > IPv4 Setting or LAN > VLAN and IPv4 Address depending on the WAP model you have.

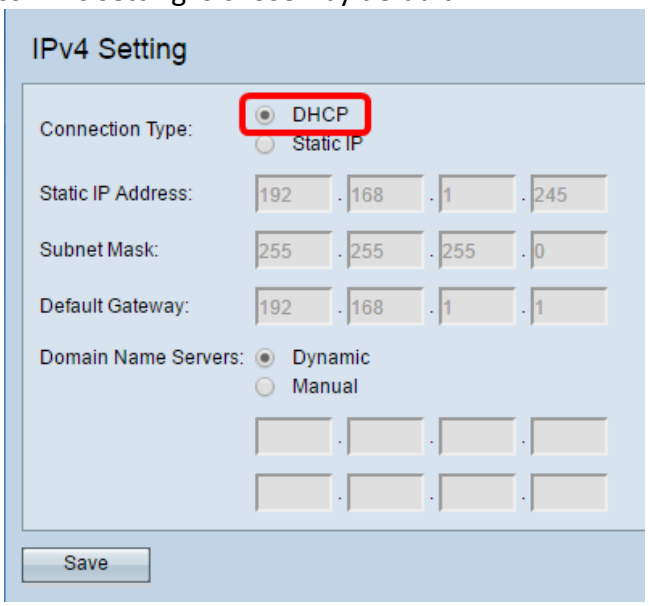
Configure IPv4

Configure IPv4 DHCP

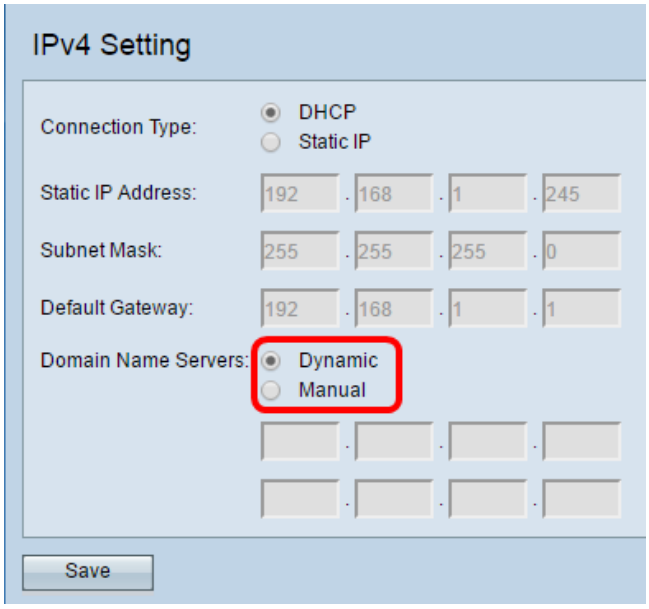
Step 1. Log in to the web-based utility and choose LAN > IPv4 Setting or LAN > VLAN and IPv4 Address depending on the WAP model you have.

WAP131, WAP150, WAP351, WAP361, WAP571, WAP571E	WAP121, WAP321, WAP371, WAP551, WAP561
	

Step 2. In the Connection Type area, click **DHCP** radio button to automatically obtain an IP address. This setting is chosen by default.



Step 3. Choose your preferred DNS configuration from the Domain Name Servers radio buttons.



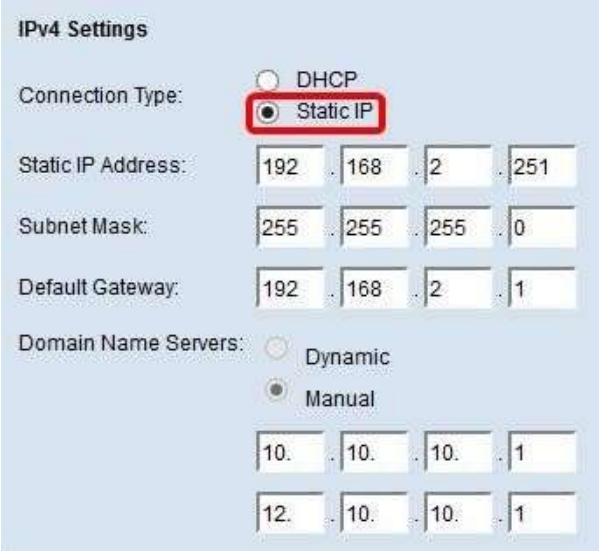
The available options are defined as follows:

- Dynamic — WAP acquires the Domain Name Server (DNS) addresses from a DHCP server on the Local Area Network (LAN). If you choose this option, skip to Step 4.
- Manual — Allows you to manually configure one or more DNS server addresses in the Domain Name Servers fields.

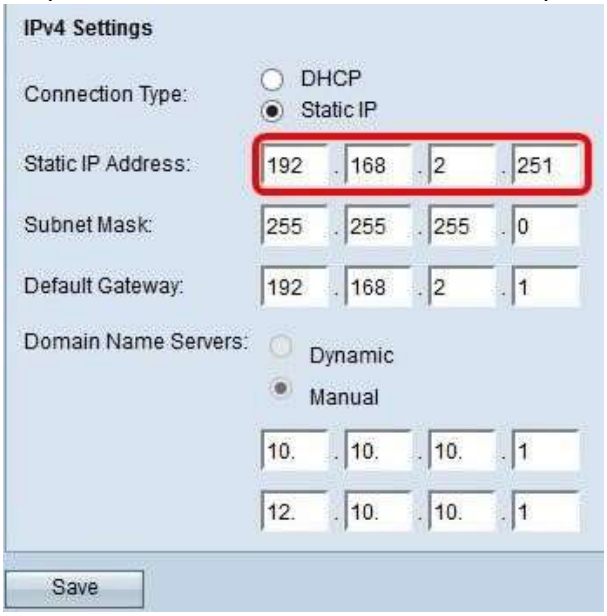
Step 4. Click Save.

Configure Static IPv4 Address

Step 1. Click the radio button for Static IP.

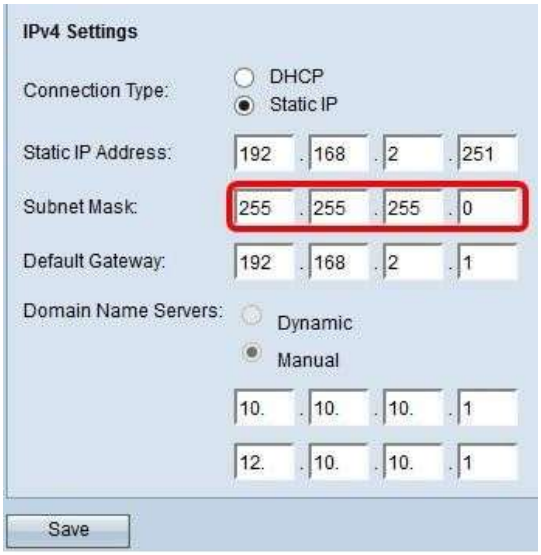


Step 2. Enter an IP address for the access point in the Static IP Address field.

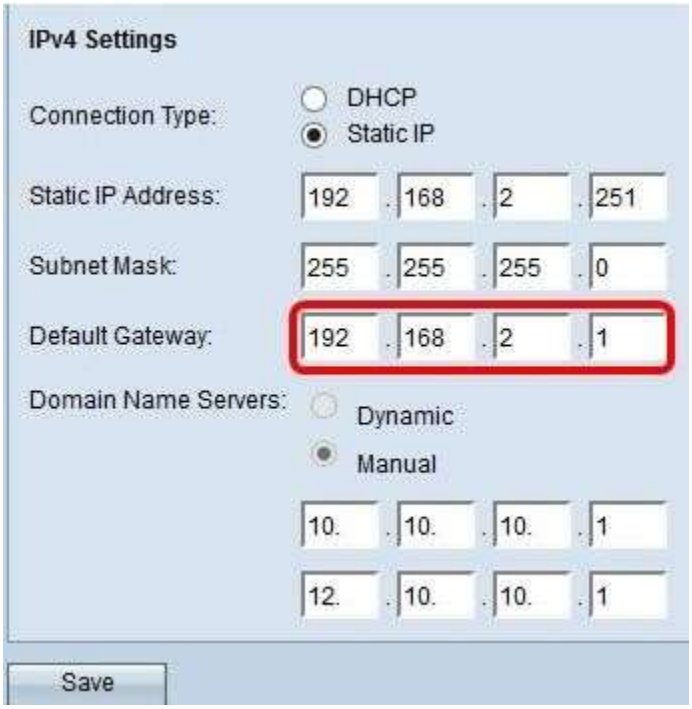


Step 3. Enter the subnet mask of the network in the *Subnet Mask* field.

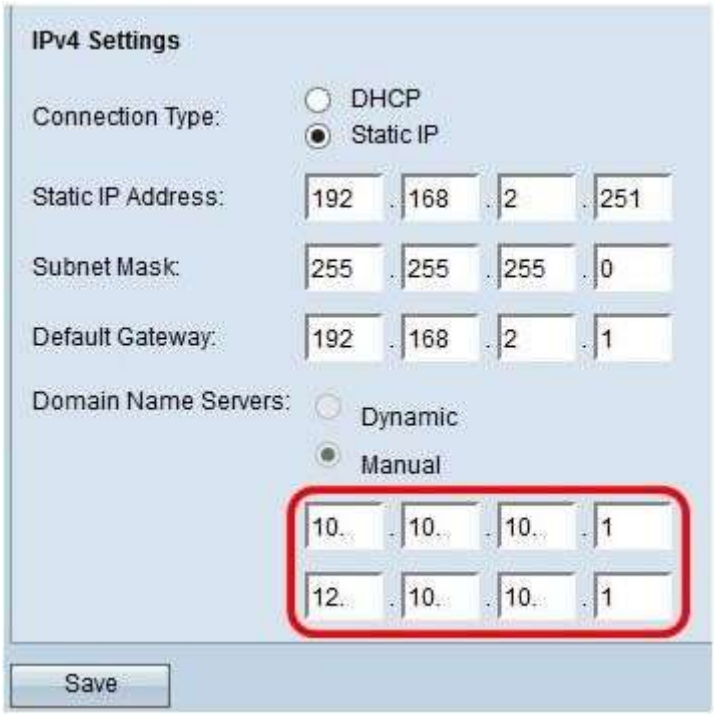
Note: The default mask is 255.255.255.0



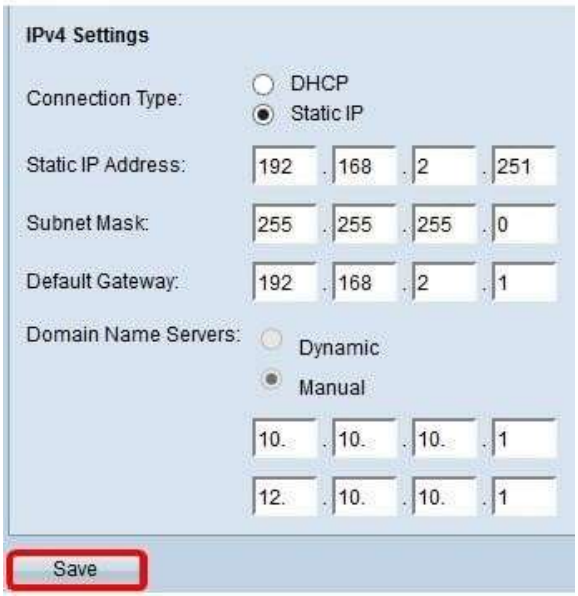
Step 4. Enter the default gateway IP address in the *Default Gateway* field.



Step 5. Enter the IP address of the DNS in the *Domain Name Ser*ver fields.



Step 6. Click **Save**.



Step 7. If you have pre-configured settings before, a pop-up window will appear confirming the wireless settings are about to be updated and that possible disconnections may happen. Click OK.

You should now have statically configured the IPv4 address.

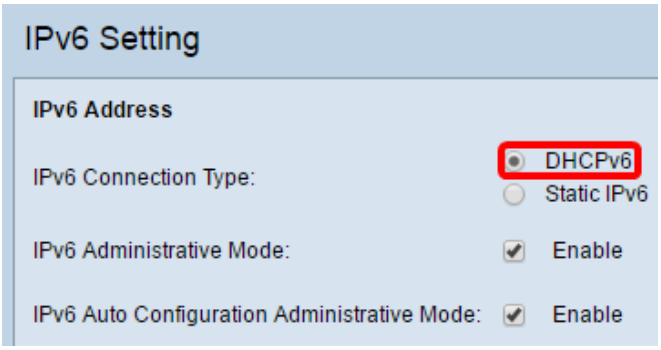
Configure IPv6

Configure IPv6 DHCP

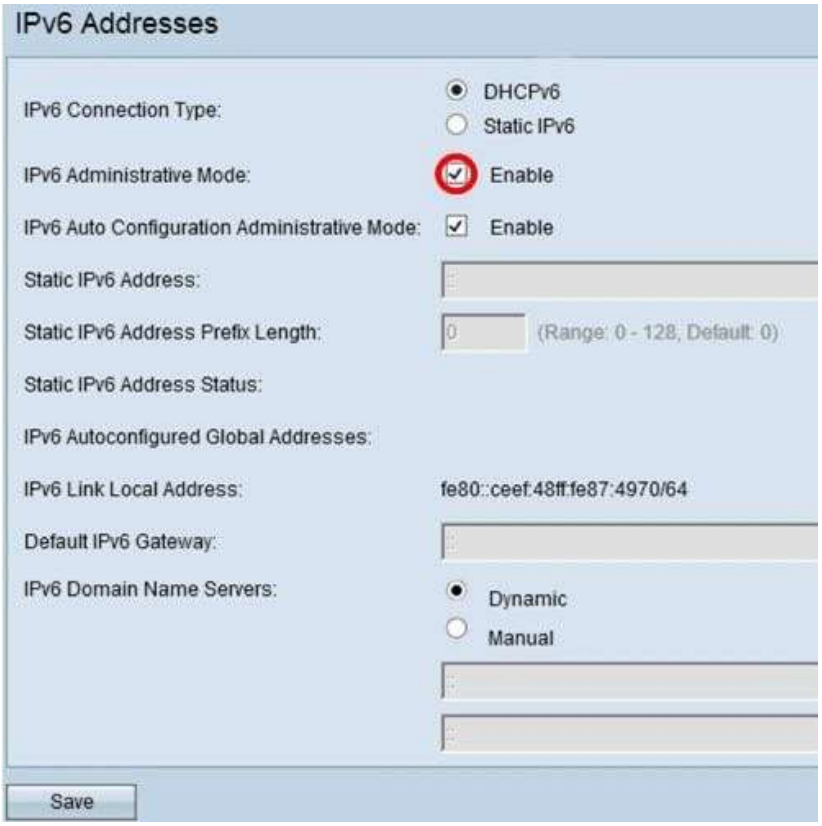
Step 1. Log in to the web-based utility and choose LAN > IPv6 Setting or LAN > IPv6 Addresses.

WAP131, WAP150, WAP351, WAP361, WAP571, and WAP571E	WAP121, WAP321, WAP371, WAP551, and WAP561
	

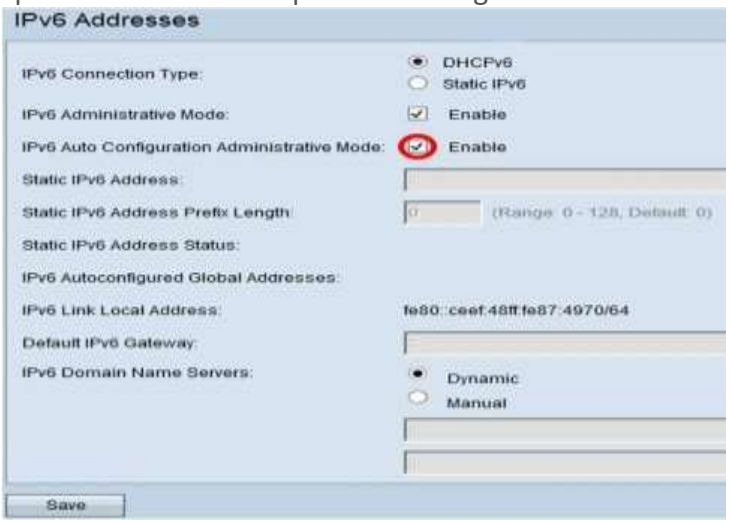
Step 2. Click **DHCPv6** as the IPv6 Connection Type. The IPv6 connection type tells the device how to obtain IPv6 address.



Step 3. To permit IPv6 management access to the access point, check the Enable IPv6 Administrative Mode check box.



Step 4. To learn its IPv6 addresses and gateway through router advertisements received on the LAN port, check the Enable IPv6Auto Configuration Administrative Mode check box. Access points can have multiple auto-configured IPv6 addresses.

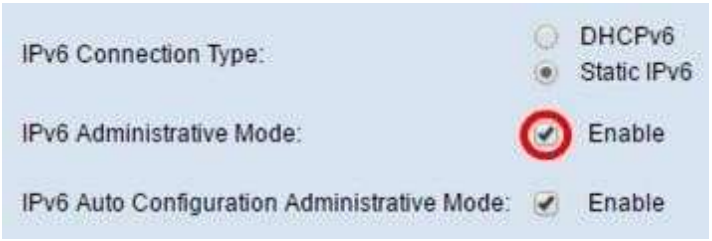


Step 5. Click Save.

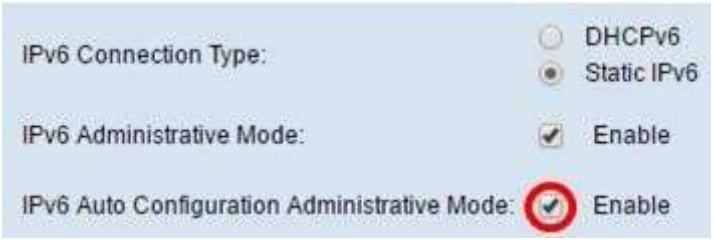
Configure Static IPv6 Address

Step 1. Click Static IPv6 as the IPv6 Connection Type to assign an IPv6 address manually to the access point.

Step 2. Check the IPv6 Administrative Mode check box to enable IPv6 management access. This allows the device management interface to be accessed via an IPv6 address.



Step 3. Check the IPv6 Auto Configuration Administrative Mode check box to enable IPv6 automatic address configuration on the device. This is enabled by default.



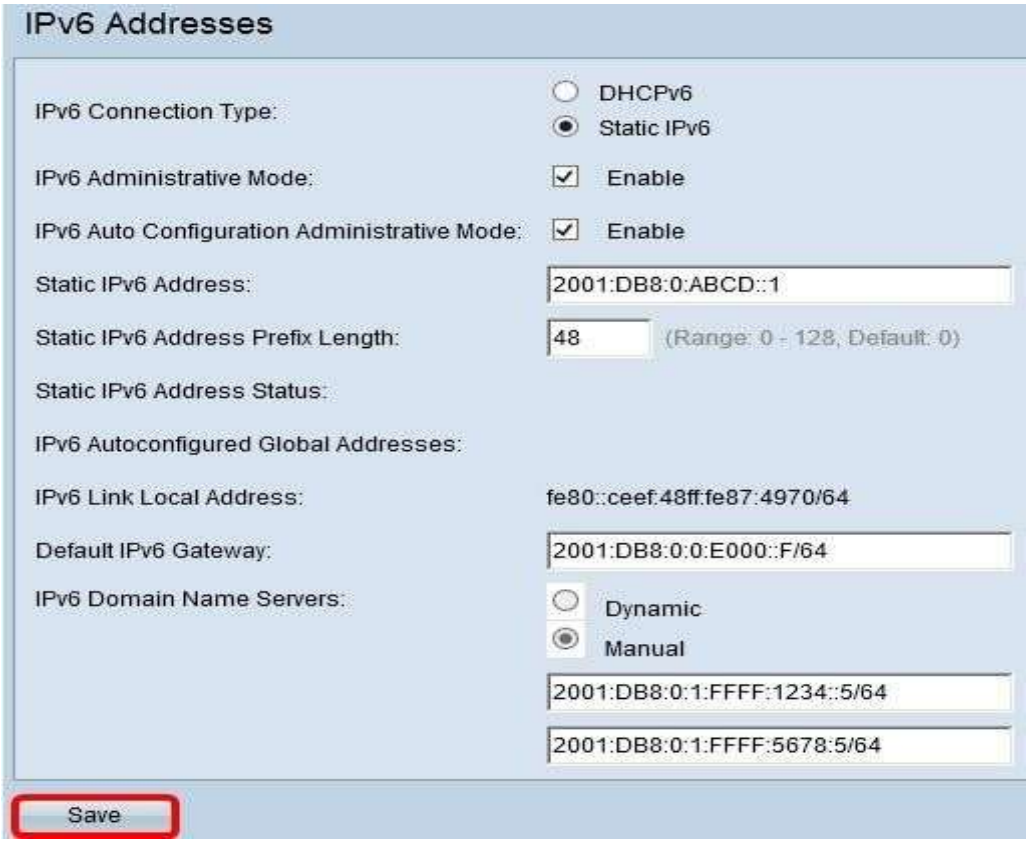
Step 4. Enter the IPv6 address of the access point in the *Static IPv6 Address* field.

Step 5. Enter the prefix length of the static address in the Static IPv6 Address Prefix Length field.

Step 6. Enter the IPv6 address of the default gateway in the Default IPv6 Gateway field.

Step 7. Enter the IPv6 DNS server address in the IPv6 Domain Name Servers fields.

Step 8. Click Save.



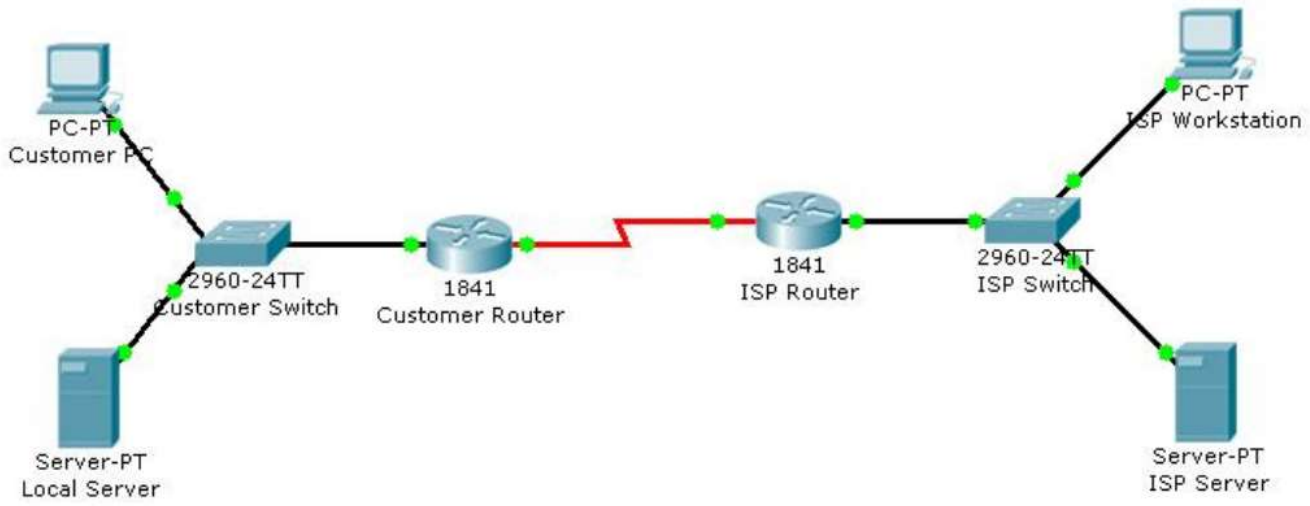
Result:

Configuration of IPv4 and IPv6 successfully done

Experiment: 17

Performing an Initial Switch Configuration

Topology Diagram



Objectives

- Perform an initial configuration of a Cisco Catalyst 2960 switch.

Background / Preparation

In this activity, you will configure these settings on the customer Cisco Catalyst 2960 switch:

- Host name
- Console password
- vty password
- Privileged EXEC mode password
- Privileged EXEC mode secret
- IP address on VLAN1 interface
- Default gateway

Note: Not all commands are graded by Packet Tracer.

Step 1: Configure the switch host name.

a. From the Customer PC, use a console cable and terminal emulation software to connect to the consoleof the customer Cisco Catalyst 2960 switch.

b. Set the host name on the switch to **CustomerSwitch** using these commands.

Switch>**enable**
Switch#**configure**
terminal
Switch(config)#**hostname CustomerSwitch**

Step 2: Configure the privileged mode password and secret.

a. From global configuration mode, configure the password as **cisco**.

CustomerSwitch(config)#**enable password cisco**

b. From global configuration mode, configure the secret as **cisco123**.

CustomerSwitch(config)#
enable secret cisco123

Step 4: Configure the vty password.

a. From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

CustomerSwitch(config)#**line vty 0 15**

b. From line configuration mode, set the password to **cisco** and require the password to be entered atlogin.

CustomerSwitch(config-line)#**password**
ciscoCustomerSwitch(config-line)#**login**
CustomerSwitch(config-line)#**exit**

Step 5: Configure an IP address on interface VLAN1.

From global configuration mode, switch to interface configuration mode for VLAN1, and assign the IP address192.168.1.5 with the subnet mask of 255.255.255.0.

CustomerSwitch(config)#**interface vlan 1**
CustomerSwitch(config-if)#**ip address 192.168.1.5 255.255.255.0**
CustomerSwitch(config-if)#**no shutdown**
CustomerSwitch(config-if)#**exit**

Step 6: Configure the default gateway.

a. From global configuration mode, assign the default gateway to 192.168.1.1.

CustomerSwitch(config)#**ip default-gateway 192.168.1.1**

b. Click the **Check Results** button at the bottom of this instruction window to check your work.

Step 7: Verify the configuration.

The Customer Switch should now be able to ping the ISP Server at 209.165.201.10. The first one or two pingsmay fail while ARP converges.

CustomerSwitch(config)#**end**
CustomerSwitch#**ping**
209.165.201.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.10, timeout is 2 seconds:
..!!!

Success rate is 60 percent (3/5), round-trip min/avg/max =

181/189/197 msCustomerSwitch#

Viva Questions:

a. What is the significance of assigning the IP address to the VLAN1 interface instead of any of the Fast Ethernet interfaces?

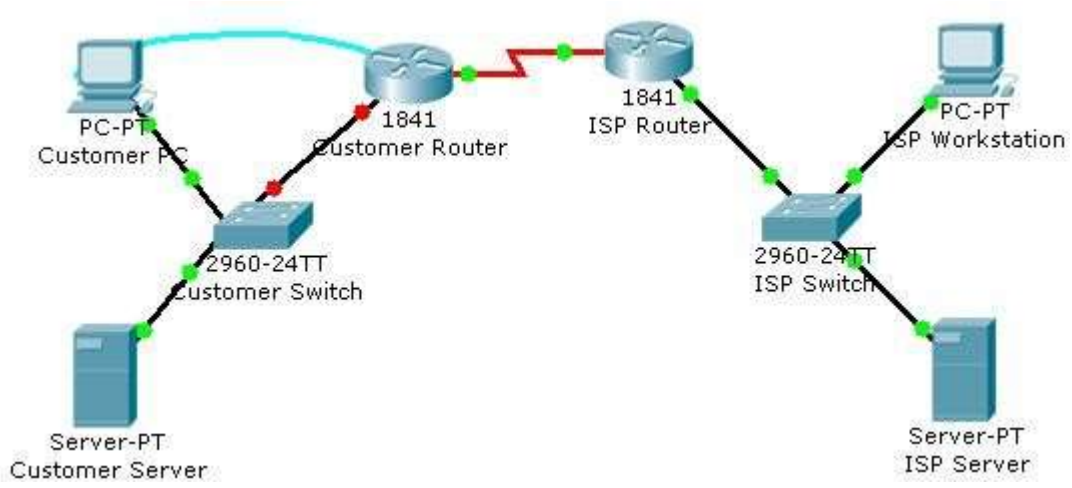
b. What command is necessary to enforce password authentication on the console and vty lines?

c. How many gigabit ports are available on the Cisco Catalyst 2960 switch that you used in the activity?

Experiment: 18

Performing an Initial Router Configuration

Topology Diagram



Objectives

- Configure the router host name.
- Configure passwords.
- Configure banner messages.
- Verify the router configuration.

Background / Preparation

In this activity, you will use the Cisco IOS CLI to apply an initial configuration to a router, including hostname, passwords, a message-of-the-day (MOTD) banner, and other basic settings.

Note: Some of the steps are not graded by Packet Tracer.

Step 1: Configure the router host name.

a. On Customer PC, use the terminal emulation software to connect to the console of the customer Cisco1841 ISR.

Set the host name on the router to CustomerRouter by using these commands.

```
Router>enable
Router#configure
terminal
Router(config)#hostname CustomerRouter
```

Step 2: Configure the privileged mode and secret passwords.

a. In global configuration mode, set the password to **cisco**.

CustomerRouter(config)#**enable password cisco**

Set an encrypted privileged password to cisco123 using the secret command.

CustomerRouter(config)#**enable secret cisco123**

Step 3: Configure the console password.

a. In global configuration mode, switch to line configuration mode to specify the console line.
CustomerRouter(config)#**line console 0**

Set the password to **cisco123**, require that the password be entered at login, and then exit line configuration mode.

CustomerRouter(config-line)#**password**
cisco123 CustomerRouter(config-line)#**login**
CustomerRouter(config-line)#**exit**
CustomerRouter(config)#

Step 4: Configure the vty password to allow Telnet access to the router.

a. In global configuration mode, switch to line configuration mode to specify the vty lines.
CustomerRouter(config)#**line vty 0 4**

Set the password to **cisco123**, require that the password be entered at login, exit line configuration mode, and then
exit the configuration session.

CustomerRouter(config-line)#**password**
cisco123 CustomerRouter(config-line)#**login**
CustomerRouter(config-line)#**exit**
CustomerRouter(config)#

Step 5: Configure password encryption, a MOTD banner, and turn off domain server lookup.

a. Currently, the line passwords and the enable password are shown in clear text when you show therunning configuration. Verify this now by entering the **show running-config** command.

To avoid the security risk of someone looking over your shoulder and reading the passwords, encryptall clear text passwords.

CustomerRouter(config)#**service password-encryption**

Use the **show running-config** command again to verify that the passwords are encrypted.

To provide a warning when someone attempts to log in to the router, configure a MOTD banner.

CustomerRouter(config)#**banner motd $Authorized Access Only!$**

Test the banner and passwords. Log out of the router by typing the **exit** command twice. The

banner displays beforethe prompt for a password. Enter the password to log back into the router.

You may have noticed that when you enter a command incorrectly at the user or privileged EXEC prompt, the routerpauses while trying to locate an IP address for the mistyped word you entered. For example, this output shows what happens when the **enable** command is mistyped.

```
CustomerRouter>emable
Translating "emable"...domain server (255.255.255.255)
```

To prevent this from happening, use the following command to stop all DNS lookups from the routerCLI.

```
CustomerRouter(config)#no ip domain-lookup
```

Save the running configuration to the startup configuration.

```
CustomerRouter(config)#end
CustomerRouter#copy run
start
```

Step 6: Verify the configuration.

a. Log out of your terminal session with the Cisco 1841 customer router.
b. Log in to the Cisco 1841 Customer Router. Enter the console password when prompted.
c. Navigate to privileged EXEC mode. Enter the privileged EXEC password when prompted.
d. Click the Check Results button at the bottom of this instruction window to check your work.

Viva Questions:

Which Cisco IOS CLI commands did you use most?

How can you make the customer router passwords more secure?

Experiment: 19

Configuration of LAN

Aim:
To analyse the performance of various configurations and protocols in LAN
Requirements

- Windows pc – 3Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

Procedure

- Open the CISCO Packet tracer software
- Drag and drop 3 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Make the connections using Straight through Ethernet cables
- Give IP address of the PC1, PC2 and PC3 as 192.168.1.1, 192.168.1.2 and 192.168.1.3 respectively, ping between PCs and observe the transfer of data packets in real and simulation mode.

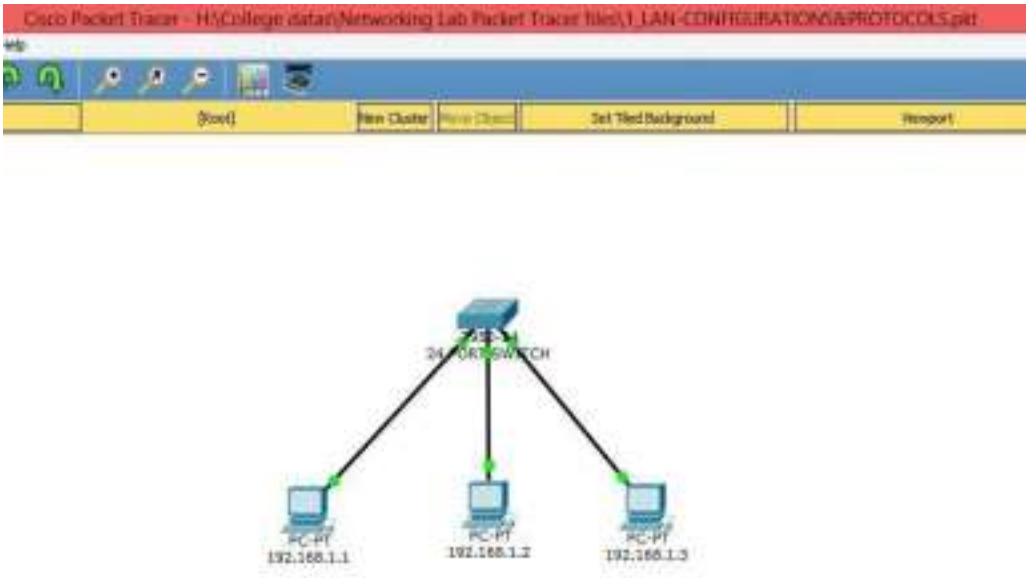
Theory

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.

The advantages of a LAN are the same as those for any group of devices networked together. The devices can use a single Internet connection, share files with one another, print to
shared printers, and be accessed and even controlled by one another.

Network Topology Diagram for LAN



Input Details for LAN

PC0	PC1	PC2
IP Address : 10.0.0.1 Gate way : 10.0.0.50	IP Address : 10.0.0.2 Gate way : 10.0.0.50	IP Address : 10.0.0.3 Gate way : 10.0.0.50

LAN OUTPUT WINDOW: (PINGING FROM PC0-PC1)

Packet Tracer PC Command Line 1.0

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=8ms TTL=128

Reply from 10.0.0.2: bytes=32 time=4ms TTL=128

Reply from 10.0.0.2: bytes=32 time=4ms TTL=128

Reply from 10.0.0.2: bytes=32 time=4ms TTL=128

Ping statistics for 10.0.0.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 4ms, Maximum = 8ms, Average = 5ms

LAN - MAC ADDRESS TABLE:

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0009.7c61.c0d0    DYNAMIC     Fa0/1
   1    000d.bdc2.3317    DYNAMIC     Fa0/2
   1    0090.0ce6.60c9    DYNAMIC     Fa0/3
```

RESULT

Hence, the various configurations and protocols in LAN are analysed and the experiment is performed successfully.

VIVA QUESTIONS

What is LAN and its uses?

A local-area network (LAN) is a computer network that spans a relatively small area. Most often, a LAN is confined to a single room, building or group of buildings, however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

What are the advantages of LAN?

In LAN computers can exchange data and messages in the easy and fast way. It also saves time and makes our work fast. Every user can share messages and data with any other user on LAN. The user can log in from any computer on the network and access the same data placed on the server.

How does LAN work?

Early LAN (Local Area Network) networks were formed using coaxial cable, coax is an electric cable and it is used to carry radio signals. LAN (Local Area Network) setup is developed by connecting two or more than two computers with each other using a physical connection in order to share files and data overtime.

What is a disadvantage of LAN?

Disadvantages of LANs:

The use of email within the network can lead to problems of time wasting as people send messages that do not relate to work. If the dedicated file server fails, work stored on shared hard disk drives will not be accessible and it will not be possible to use network printers either.

Experiment:20

Configuration of VLAN

Aim:

To construct a VLAN and make the PC's communicate among a VLAN

Requirements

- Windows pc – 6 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

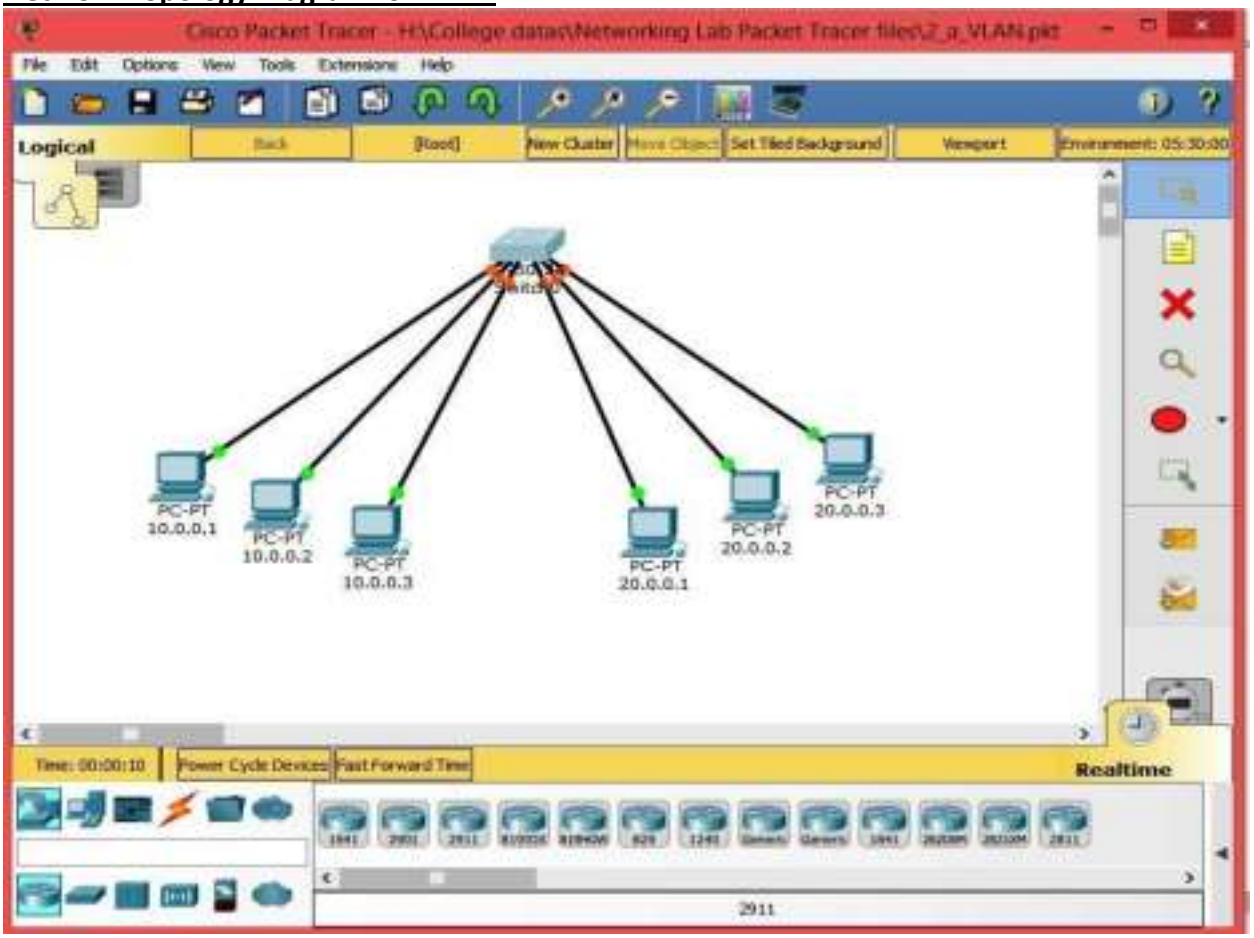
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 6 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Make the connections using Straight through Ethernet cables
- Give IP address of the PCs as per table, ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible. VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.

Network Topology Diagram for VLAN



Input Details for VLAN 10

PC0	PC1	PC2
IP Address : 10.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.3 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50

Input Details for VLAN 20

PC0	PC1	PC2
IP Address : 20.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50	IP Address : 20.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50	IP Address : 20.0.0.3 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50

CONFIGURATION OF THE SWITCHPORT FOR VLAN:

Switch>en
Switch#config
Configuring from terminal, memory, or network [terminal]? Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#vlan 10
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#ex
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#ex
Switch(config)#interface range fastEthernet 0/4-6
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#ex
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

VLAN OUTPUT: (PINGING FROM PC0)

C:\>PING 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

8 | P a g e

C:\>PING 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

MAC- ADDRESS TABLE:

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------
-------------------------------------------

Vlan    Mac Address       Type        Ports Vlan    Mac Address       Type        Ports
----    -----------       --------    ----- ----    -----------       --------    -----

  10    0009.7c61.c0d0    DYNAMIC     Fa0/1   20    0060.3e8d.3936    DYNAMIC     Fa0/5
  10    000d.bdc2.3317    DYNAMIC     Fa0/2   20    00d0.bcb6.54aa    DYNAMIC     Fa0/6
  10    0090.0ce6.60c9    DYNAMIC     Fa0/3   20    00e0.a371.aec7    DYNAMIC     Fa0/4
```

Result

Hence, created VLAN structure and observed the communications of PCs within aVLAN

VIVA QUESTIONS

What is LAN and VLAN?

VLAN and LAN are two terms used frequently in the networking field. ... VLAN is an implementation of a private subset of a LAN in which the computers interact with each other as if they are connected to the same broadcast domain irrespective of their physical locations

What is VLAN? And how it is reduce the broadcast traffic?
A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch. VLAN divides the broadcast domain so, the frames that will be broadcasted onto the network are only the ports logically grouped with in the same VLAN.

What is Inter VLAN Routing?
VLANs divide broadcast domains in a LAN environment so, by default only Hosts that are members of the same VLAN can communicate. Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them. This is known as Inter VLAN Routing.

Give the Command to Create VLAN?
Switch(config)#vlan 10
Switch(config-vlan)#ex

How can we add an interface to a VLAN?
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#ex

Which command is used to see all VLANs information?
Switch # show vlan 10

Experiment: 21

Configuration of Inter VLAN

Aim: To construct a Inter - VLAN and make the PC's communicate among a VLAN

Requirements

- Windows pc – 4 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

Procedure

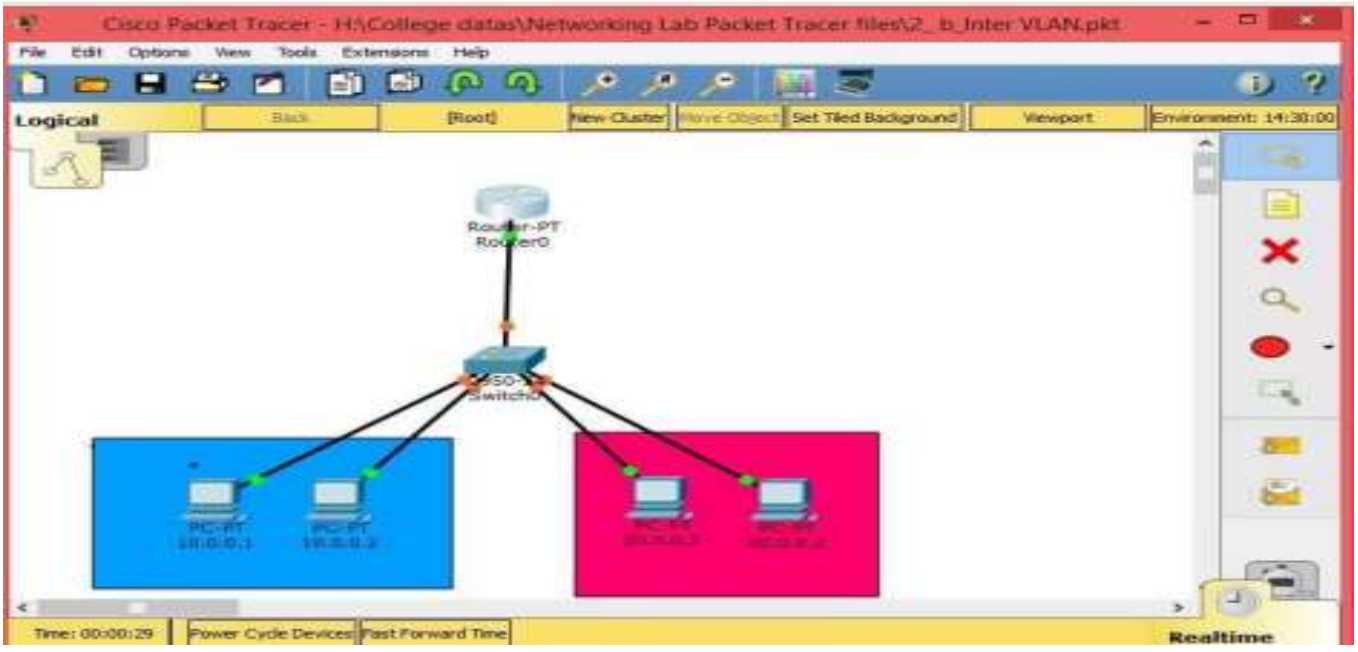
- Open the CISCO Packet tracer software
- Drag and drop 4 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Make the connections using Straight through Ethernet cables
- Give IP address of the PCs as per table, ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

Inter-VLAN routing can be defined as a way to forward traffic between different VLAN by implementing a router in the network. As we learnt previously, VLANs logically segment the switch into different subnets, when a router is connected to the switch, an administrator can configure the router to forward the traffic between the various VLANs configured on the switch. The user nodes in the VLANs forwards traffic to the router which then forwards the traffic to the destination network regardless of the VLAN configured on the switch.

The use of VLANs means that users would not be able to communicate across departments, i.e. a user in FINANCE, would not be able to send a message to a user in SALES since they are on different broadcast domains.

Network Topology Diagram for Inter VLAN



Input Details for VLAN 10

PC0	PC1
IP Address : 10.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50

Input Details for VLAN 20

PC0	PC1
IP Address : 20.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50	IP Address : 20.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 20.0.0.50

CONFIGURING THE TRUNK PORT IN SWITCH:

```
Switch#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/7
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#no shut
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
```

ROUTER CONFIGURATION:

```
Router>en
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.0.0.50 255.0.0.0
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up %LINEPROTO-5-UPDOWN: Line
```

protocol on Interface FastEthernet0/0.20, changed state to up
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 20.0.0.50 255.0.0.0
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E – EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o – ODR P - periodic downloaded static route
Gateway of last resort is not set
C 10.0.0.0/8 is directly connected, FastEthernet0/0.10
C 20.0.0.0/8 is directly connected, FastEthernet0/0.20

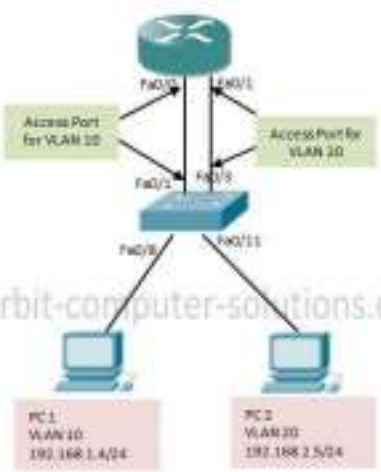
OUTPUT:(PINGING PC3 IN VLAN20 FROM PC0 IN VLAN10)

C:\>ping 20.0.0.1
Pinging 20.0.0.1 with 32 bytes of data:
Request timed out.
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time<1ms TTL=127
Reply from 20.0.0.1: bytes=32 time=4ms TTL=127
Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 4ms, Average = 1ms

Result
Hence, We constructed Inter VLAN and made the communications of PCs between different VLANs.

VIVA QUESTIONS

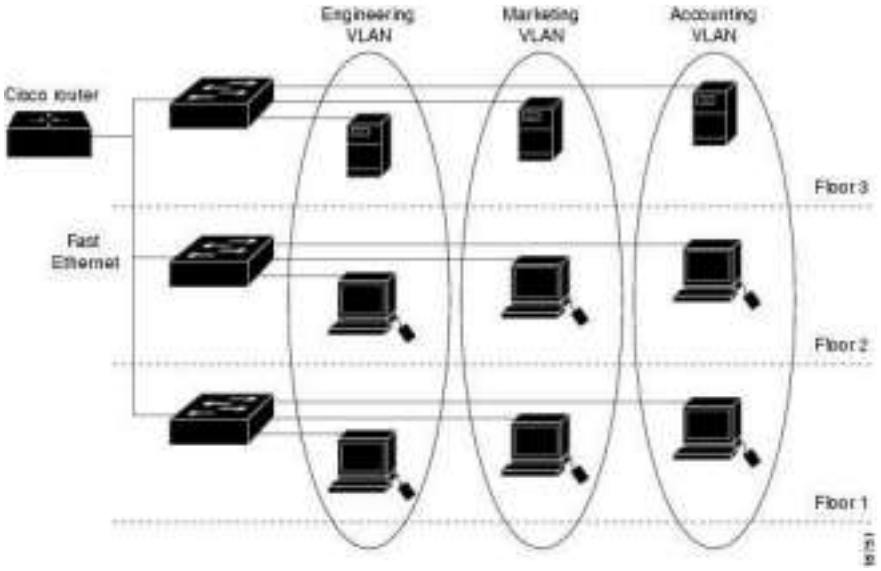
What is Inter VLAN Routing ? Explained with Examples
Inter-VLAN routing using a router on a stick utilizes an external router to pass traffic between VLANs.



The figure above show a traditional inter-VLAN routing:

1 Traffic from PC1 on VLAN10 is routed through router R1 to reach PC3 on VLAN 20. 2. PC1 and PC3 are on different VLANs and have IP addresses on different subnets. 3. Router R1 has a separate interface configured for each of the VLANs.

Sample of VLAN



Experiment: 22

Configuration of Wireless LAN

Aim: To construct a Wireless LAN and make the PC's communicate wirelessly

Requirements

- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

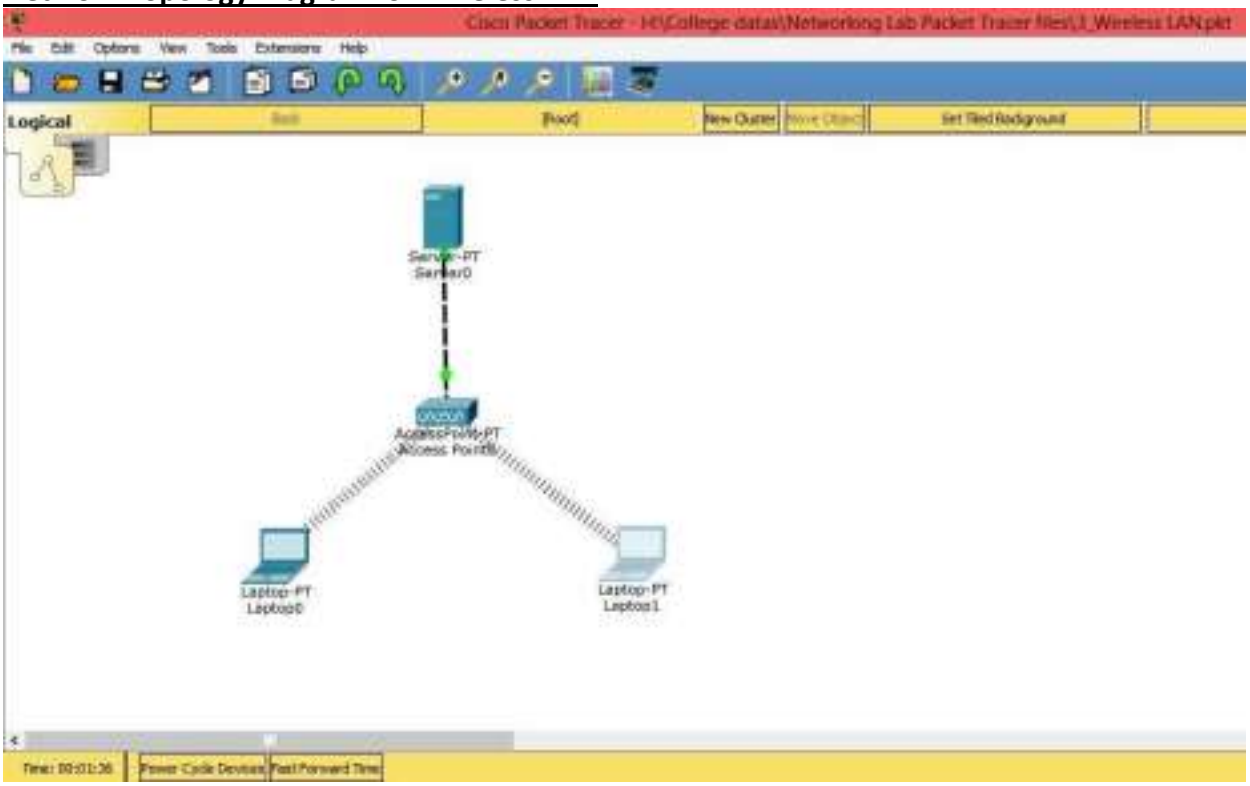
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 2 Laptop pcs using End Device Icons on the left corner • Select Access point and server from wireless devices
- Select laptop-> physical-> OFF laptop-> remove LAN Module & replace WPC 300N Wireless module -> ON Laptop
- Observe the wireless connections between access point and laptops
- Give IP address of the PCs as per table, ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

A Wireless Local Area Network (WLAN) implements a flexible data communication system frequently augmenting rather than replacing a wired LAN within a building or campus. WLANs use radio frequency to transmit and receive data over the air, minimizing the need for wired connections.

Network Topology Diagram for Wireless LAN



WLAN OUTPUT WINDOW:(PINGING FROM laptop 1- laptop 0) C:\>ping 169.254.129.204

Pinging 169.254.129.204 with 32 bytes of data:
Reply from 169.254.129.204: bytes=32 time=30ms TTL=128
Reply from 169.254.129.204: bytes=32 time=16ms TTL=128

Reply from 169.254.129.204: bytes=32 time=15ms TTL=128
Reply from 169.254.129.204: bytes=32 time=13ms TTL=128
Ping statistics for 169.254.129.204:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 13ms, Maximum = 30ms, Average = 18ms

Result:

Thus, constructed a WLAN and made the Laptops communicate wirelessly

VIVA QUESTIONS

What is a Wireless Network?

A wireless local-area network (WLAN) uses radio waves to connect devices, such as laptops, to the Internet and to your business network and applications.

What is mean by wireless LAN?

A wireless local area network (WLAN) is a wireless distribution method for two or more devices that use high-frequency radio waves and often include an access point to the Internet. A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection.

What is the difference between WiFi and wireless LAN?

While wireless LANs refer to any local area network (LAN) that a mobile user can connect to through a wireless (radio) connection; Wi-Fi (short for "wireless fidelity") is a term for certain types of WLANs that use specifications in the 802.11 wireless protocol family.

What are the Benefits of a WLAN?

Small businesses can experience many benefits from a WLAN. A few examples:

• You can access network resources from any location within the wireless network's coverage area. • Wireless access to the Internet and to company resources help your staff be more productive and collaborative.

• You don't have to string cables, as you do with wired networks. Installation can be quick and cost effective.

• You can easily expand WLANs where and as needed, because no wires are involved. • By eliminating or reducing wiring expenses, WLANs can cost less to operate than wired networks.

Who Uses WLANs?

WLANs are frequently offered in public places such as cafes, hotels, and airport lounges. In addition, many businesses have wireless networks throughout their office buildings or campuses for employee and guest use.

Experiment: 23

Configuration of Address Resolution protocol

Aim: To construct simple LAN and understand the concept and operation of Address

Resolution Protocol (ARP)

Requirements

- Windows pc – 5 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Cat-5 LAN cable

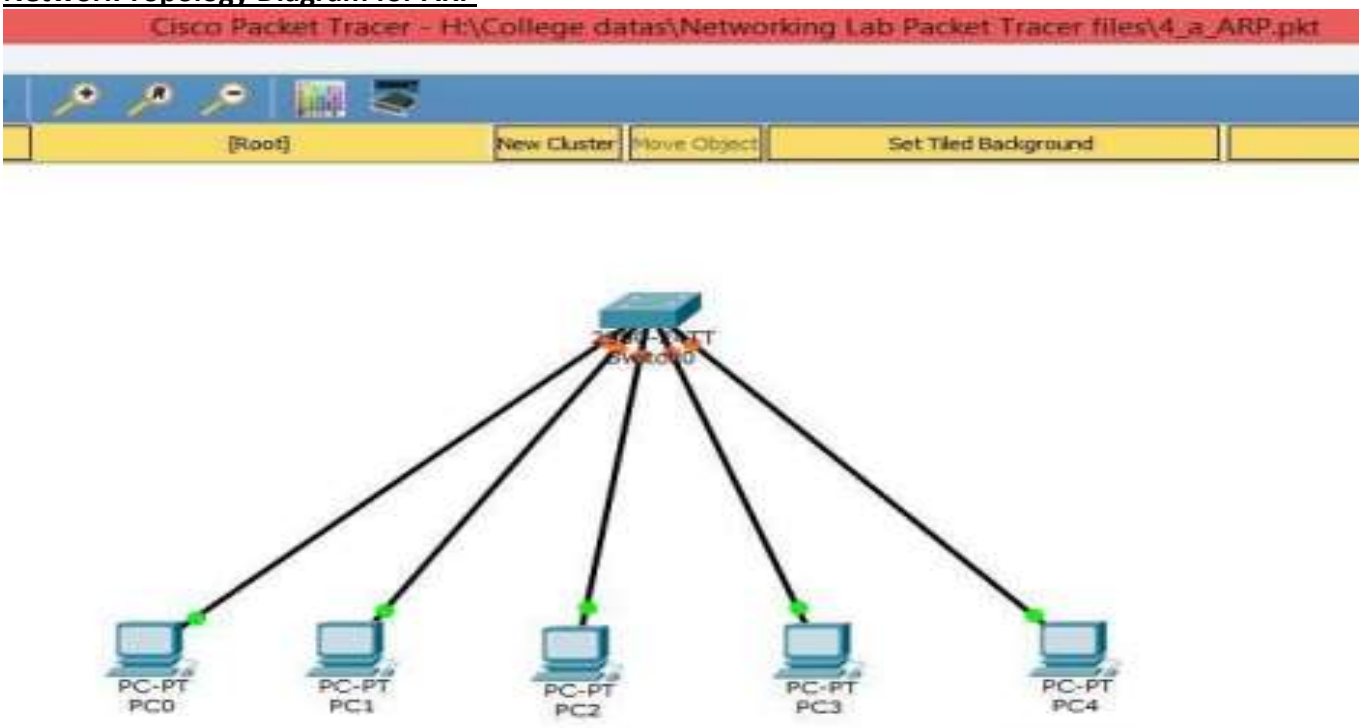
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 5 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Make the connections using Straight through Ethernet cables
- Give IP address of the PC1, PC2, PC3 and PC4 as per the input table respectively, observe the source and destination MAC address of all packets.
- Get cache from switch.

Theory

ARP (Address Resolution Protocol) is a network protocol used to find out the hardware (MAC) address of a device from an IP address. It is used when a device wants to communicate with some other device on a local network (for example on an Ethernet network that requires physical addresses to be known before sending packets). The sending device uses ARP to translate IP addresses to MAC addresses. The device sends an ARP request message containing the IP address of the receiving device. All devices on a local network segment see the message, but only the device that has that IP address responds with the ARP reply message containing its MAC address. The sending device now has enough information to send the packet to the receiving device.

Network Topology Diagram for ARP



Input Details for ARP

PC0	PC1	PC2	PC3	PC4
IP Address : 10.0.0.1 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.2 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.3 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.4 Subnet Mask: 255.255.255.0 Gate way : 10.0.0.50	IP Address : 10.0.0.5 Subnet Mask : 255.255.255.0 Gate way : 10.0.0.50

OUTPUT:

ARP CATCH TABLE OF PC1 (IP: 10.0.0.2):

C:\>arp -a

Internet Address Physical Address Type
10.0.0.1 0001.42c1.0547 dynamic
10.0.0.3 0001.6402.dab3 dynamic
10.0.0.4 0001.43e2.332b dynamic
10.0.0.5 0001.9665.3174 dynamic

SWITCH MAC ADDRESS TABLE:

```
Switch>
Switch>SHOW MAC ADDRESS-TABLE
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.42c1.0547    DYNAMIC     Fa0/1
   1    0001.43e2.332b    DYNAMIC     Fa0/4
   1    0001.6402.dab3    DYNAMIC     Fa0/3
   1    0001.9665.3174    DYNAMIC     Fa0/5
   1    0060.70c9.ba88    DYNAMIC     Fa0/2
```

Result:

Thus, constructed a simple LAN and understand the concept and operation of ARP and got the ARP Cache of given layout.

VIVA QUESTIONS

What is ARP?

Address Resolution Protocol (ARP) is a network protocol, which maps a network layer protocol address to a data link layer hardware address. For example, ARP is used to resolve IP address to the corresponding Ethernet address.

What is ARP process?

ARP (Address Resolution Protocol) is a network protocol used to find out the hardware (MAC) address of a device from an IP address.

What is a Address Resolution Protocol in networking?

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). ARP can also be used for IP over other LAN technologies, such as token ring, fiber distributed data interface (FDDI) and IP over ATM.

Where is ARP protocol used?

This is where ARP comes into the picture, its functionality is to translate IP address to physical address.

The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Network layer in the OSI model.

What is the use of ARP?

A host in an Ethernet network can communicate with another host, only if it knows the Ethernet address (MAC address) of that host. The higher level protocols like IP use a different kind of addressing scheme (like IP address) from the lower level hardware addressing scheme like MAC address. ARP is used to get the Ethernet address of a host from its IP address. ARP is extensively used by all the hosts in an Ethernet network.

What is an ARP cache?

ARP maintains the mapping between IP address and MAC address in a table in memory called ARP cache. The entries in this table are dynamically added and removed.

Can ARP be used in a network other than Ethernet?

ARP is a general protocol, which can be used in any type of broadcast network. The fields in the ARP packet specifies the type of the MAC address and the type of the protocol address. ARP is used with most IEEE 802.x LAN media. In particular, it is also used with FDDI, Token Ring, and Fast Ethernet, in precisely the same way as it is with Ethernet.

Experiment: 24

Configuration of Routing Information protocol

Aim: To understand the concept and operation of Routing Information Protocol (RIP)

Requirements

- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 2 No
- Router – 2 Nos
- Cat-5 LAN cable

Procedure

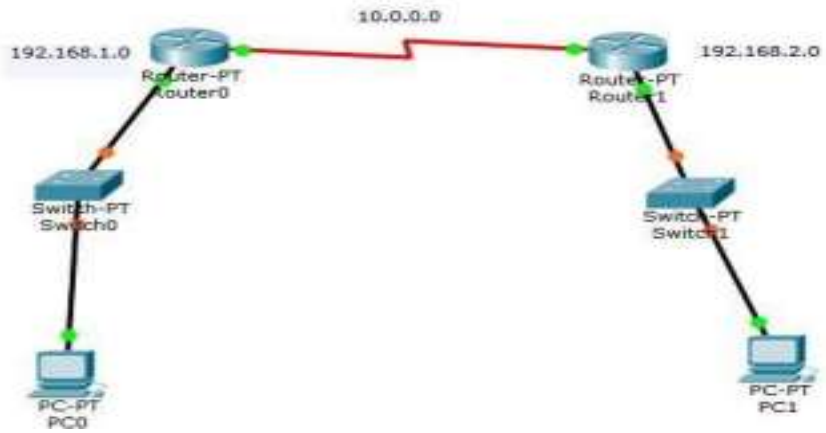
- Open the CISCO Packet tracer software
- Drag and drop 5 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router and apply clock rate as per the table.
- Make the connections using Straight through Ethernet cables
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

RIP (Routing Information Protocol) is one of the oldest distance vector routing protocols. It is usually used on small networks because it is very simple to configure and maintain, but lacks some advanced features of routing protocols like OSPF or EIGRP. Two versions of the protocol exists: version 1 and version 2. Both versions use hop count as a metric and have the administrative distance of 120. RIP version 2 is capable of advertising subnet masks and uses multicast to send routing updates, while version 1 doesn't advertise subnet masks and uses broadcast for updates. Version 2 is backwards compatible with version 1.

RIPv2 sends the entire routing table every 30 seconds, which can consume a lot of bandwidth. RIPv2 uses multicast address of 224.0.0.9 to send routing updates, supports authentication and triggered updates (updates that are sent when a change in the network occurs).

Network Topology Diagram for RIP



Input Details for RIP

PC0	PC1	Router 0	Router 1
IP Address : 192.168.1.2 Gate way : 192.168.1.1	IP Address: 192.168.2.2 Gate way : 192.168.2.1	Fast Ethernet 0/0 IP Address: 192.168.1.1 Serial 2/0 : 10.0.0.1 at 6400 clock rate	Fast Ethernet 0/0 IP Address : 192.168.2.1 Serial 2/0 : 10.0.0.2 no clock rate

OUTPUT:

RIP (PINGING FROM PC0 TO PC1):

C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
Reply from 192.168.2.2: bytes=32 time=13ms TTL=126

Reply from 192.168.2.2: bytes=32 time=11ms TTL=126
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 13ms, Average = 11ms

Result:

Thus, understand the concept and operation of RIP and pinged from PC in are networks to PC to another network.

VIVA QUESTIONS

What is RIP routing?

RIP stand for Routing information Protocol. It is protocol which communicates to one router to another router. It update after 30sec send his routing table to another router. It is distance vector protocol which protocol work on metric hop count after that is transferred the packet from source to destination. It has to follow shortage distance basis transfer the data.

How do we configure rip? Specify the commands.

#Router rip
#network 10.0.0.0

Which command is used to check RIP routing?

#show ip route
#show ip protocols

Experiment: 25

Configuration of Open shortest Path First (OSPF) Algorithm

Aim: To construct multiple router networks and understand the operation of OSPF Protocol

Requirements

- Windows pc – 3 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 3 No
- Router – 3 Nos
- Cat-5 LAN cable

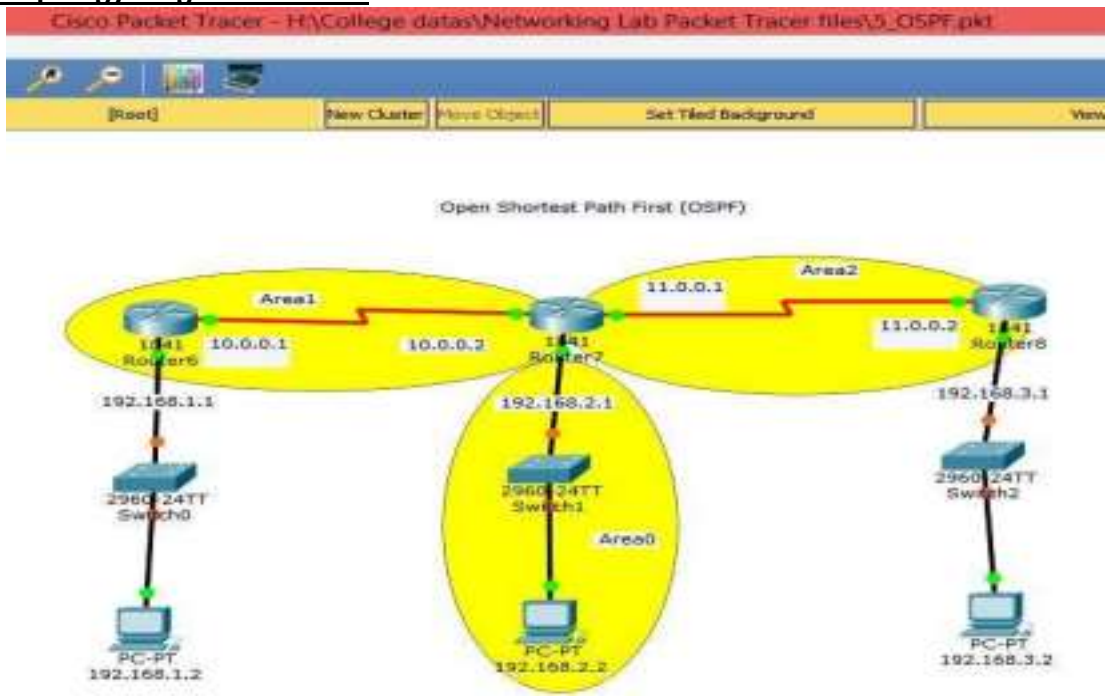
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 5 pcs using End Device Icons on the left corner
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router and apply clock rate • Add HWIC -2T Peripheral to all routers, type CLI's for all routers
- Make the connections using Straight through Ethernet cables
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

The OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks. Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. Unlike RIP, which requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place. When routes change -- sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.

Network Topology Diagram for OSPF



Input Details for OSPF

PC0	PC1	PC2
IP Address : 192.168.1.2 Gate way : 192.168.1.1	IP Address: 192.168.2.2 Gate way : 192.168.2.1	IP Address: 192.168.3.2 Gate way : 192.168.3.1

Router 0	Router 1	Router 2
fa 0/0 IP Address: 192.168.1.1 Serial 0/0/0 : 10.0.0.1 @ 2000000 clock rate Serial 0/0/1 : -	fa 0/0 IP Address : 192.168.2.1 Serial 0/0/0 : 10.0.0.2 Serial 0/0/1 : - @ 2000000 clock rate	Fa 0/0 IP Address : 192.168.3.1 Serial 0/0/0 : 10.0.0.2 @ no clock rate Se 0/0/1 : 11.0.0.1

ROUTER0 CLI:

```
Router#en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 1
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
Router(config-router)#exit
00:19:21: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

ROUTER1 CLI:

```
Router(config)#router ospf 2
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 10.0.0.0 0.255.255.255 area 1
00:19:07: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
Router(config-router)#network 11.0.0.0 0.255.255.255 area 2
Router(config-router)#exit
00:25:52: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done
```

ROUTER2 CLI:

```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 2
Router(config-router)#network 11.0.0.0 0.255.255.255 area 2
```

00:25:19: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL, Loading Done
Router(config)#exit

OUTPUT:

ROUTER0:

Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
C 10.0.0.0/8 is directly connected, Serial0/0/0
O IA 11.0.0.0/8 [110/128] via 10.0.0.2, 00:04:43, Serial0/0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
O IA 192.168.2.0/24 [110/65] via 10.0.0.2, 00:07:42, Serial0/0/0
O IA 192.168.3.0/24 [110/129] via 10.0.0.2, 00:00:53, Serial0/0/0

ROUTER1:

C 10.0.0.0/8 is directly connected, Serial0/0/0
C 11.0.0.0/8 is directly connected, Serial0/0/1
O 192.168.1.0/24 [110/65] via 10.0.0.1, 00:04:50, Serial0/0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
O 192.168.3.0/24 [110/65] via 11.0.0.2, 00:04:45, Serial0/0/1

ROUTER2:

O IA 10.0.0.0/8 [110/128] via 11.0.0.1, 00:06:55, Serial0/0/0
C 11.0.0.0/8 is directly connected, Serial0/0/0
O IA 192.168.1.0/24 [110/129] via 11.0.0.1, 00:06:45, Serial0/0/0
O IA 192.168.2.0/24 [110/65] via 11.0.0.1, 00:06:55, Serial0/0/0
C 192.168.3.0/24 is directly connected, FastEthernet0/0

Result:

Thus, understand the concept and operation of OSPF and obtained the routing table and observe transfer data packets in real and simulation time.

VIVA QUESTIONS

What is the algorithm used by OSPF?

OSPF uses SPF (Shortest Path First) algorithm for calculating the best path and preparing OSPF database. **What are the characteristics of OSPF ?**

1. OSPF supports only IP routing.
2. OSPF routes have an administrative distance i.e. 110.
3. OSPF uses cost as its metric, which is computed based on the bandwidth of the link. OSPF has no hop-count limit.

What are the different OSPF network types and give an example for each ?

Different OSPF network types with their examples are given below:

1) Broadcast Multi-Access – indicates a topology where broadcast occurs.

Examples include Ethernet, Token Ring, and ATM.
2) Point-to-Point – indicates a topology where two routers are directly connected. An example would be a point-to-point T1.
3) Point-to-Multipoint – indicates a topology where one interface can connect to multiple destinations. Each connection between a source and destination is treated as a point-to-point link. An example would be Point-to-Multipoint Frame Relay.
4) Non-broadcast Multi-access Network (NBMA) – indicates a topology where one interface can connect to multiple destinations; however, broadcasts cannot be sent across a NBMA network.

Name tables which OSPF maintain?

The OSPF process builds and maintains three separate tables:
1) A neighbor table – contains a list of all neighboring routers.
2) A topology table – contains a list of all possible routes to all known networks within an area. 3) A routing table – contains the best route for each known network.

Experiment: 26

Configuration of Enhanced Internal Gateway Routing Protocol

Aim: To construct multiple router networks and understand the operation of EIGRP Protocol

Requirements

- Windows pc – 4 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 2 No
- Router – 3 Nos
- Cat-5 LAN cable

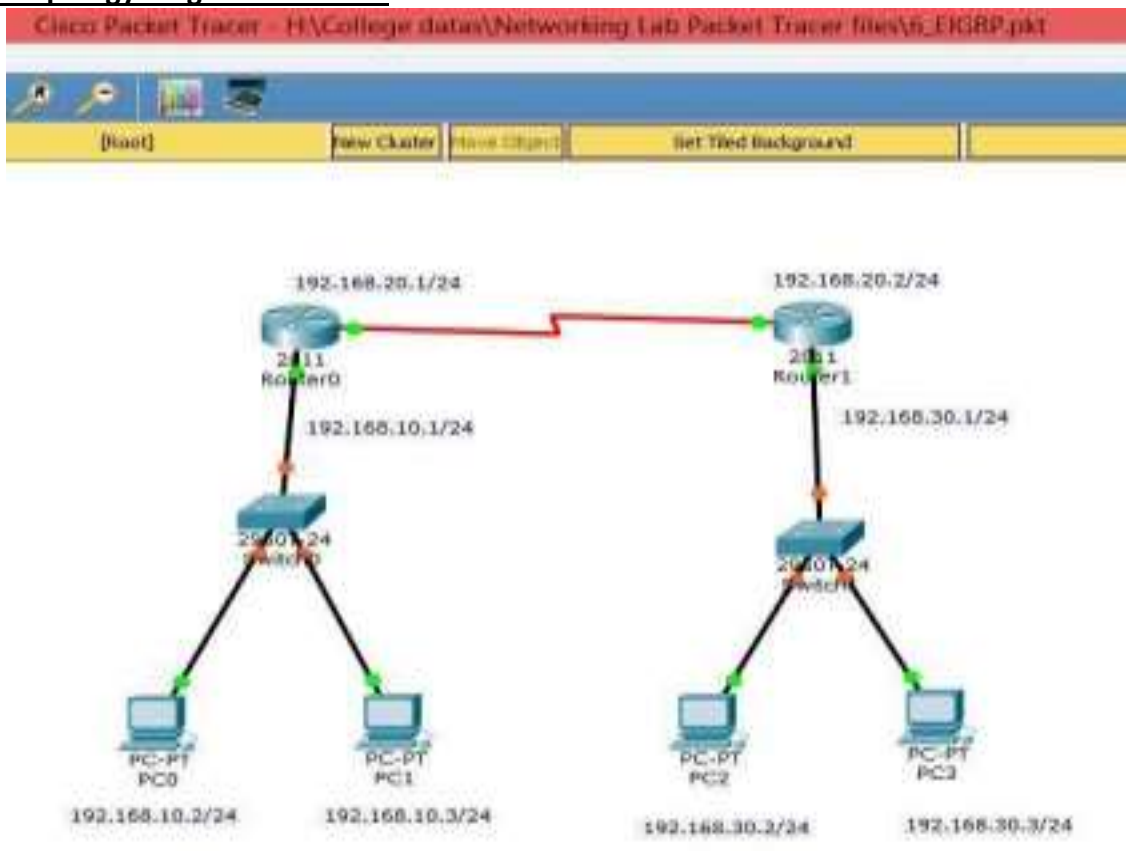
Procedure

- Open the CISCO Packet tracer software
- Drag and drop 4 pcs using End Device Icons on the left corner
- Select TWO 8 port switch from switch icon list in the left bottom corner • Select TWO Routers and Give the IP address for serial ports of router and apply clock rate as per the input table.
- Add WIC -IT Peripheral to all routers, type CLI's for all routers
- Make the connections using Straight through Ethernet cables
- Ping between PCs and observe the transfer of data packets in real and simulation mode. **Theory**

Enhanced Interior Gateway Routing Protocol (EIGRP Protocol) is an enhanced distance vector routing protocol which Uses Diffused Update Algorithm (DUAL) to calculate the shortest path. It is also considered as a Hybrid Routing Protocol because it has characteristics of both Distance Vector and Link State Routing Protocols.

EIGRP supports classless routing and VLSM, route summarization, incremental updates, load balancing and other features.

Network Topology Diagram for EIGRP



Input Details for EIGRP

PC0	PC1	PC2	PC3
IP Address : 192.168.10.2 Gate way : 192.168.10.1	IP Address: 192.168.10.3 Gate way : 192.168.10.1	IP Address: 192.168.30.2 Gate way : 192.168.30.1	IP Address: 192.168.30.3 Gate way : 192.168.30.1

Router 0	Router 1
fa 0/0 IP Address: 192.168.10.1 Serial 0/0/0 : 192.168.20.1 @ 6400 clock rate	fa 0/0 IP Address : 192.168.30.1 Serial 0/0/0 : 192.168.20.2

ROUTER0 CLI:

Router(config)#router eigrp 10
Router(config-router)#network 192.168.10.0 255.255.255.0
Router(config-router)#network 192.168.20.0 255.255.255.0
Router(config-router)#exit

ROUTER1 CLI:

Router(config)#router eigrp 10
Router(config-router)#network 192.168.20.0 255.255.255.0
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.20.1 (Serial0/1/0) is up: new adjacency
Router(config-router)#network 192.168.30.0 255.255.255.0
Router(config-router)#exit

OUTPUT:

ROUTER0:

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
C 192.168.10.0/24 is directly connected, FastEthernet0/0
C 192.168.20.0/24 is directly connected, Serial0/3/0
D 192.168.30.0/24 [90/20514560] via 192.168.20.2, 00:04:51, Serial0/3/0 **ROUTER1:**
D 192.168.10.0/24 [90/20514560] via 192.168.20.1, 00:05:35, Serial0/1/0 C 192.168.20.0/24 is directly connected, Serial0/1/0
C 192.168.30.0/24 is directly connected, FastEthernet0/0

Result:

Thus, understand the concept and operation of EIGRP and obtained the routing table and observe transfer data packets in real and simulation time.

VIVA QUESTIONS

Why EIGRP is called hybrid protocol?

EIGRP is also called hybrid protocol because its metric is not just plain HOP COUNT (max 255, included in pure distance vector protocol) rather includes the links bandwidth, delay, reliability and Load parameter into the calculation. Thats why called Advanced or Hybrid protocol.

What are the different packets or message in EIGRP?

There are Six packets in EIGRP, 1-Hello , 2-Update, 3-Query, 4-Reply, 5-Acknoladgment, 6.Request **What are different route types in EIGRP?**

There are three different types of routes in EIGRP:

• Internal Route—Routes that are originated within the Autonomous System (AS).

• Summary Route—Routes that are summarized in the router (for example, internal paths that have been summarized).

• External Route—Routes that are redistributed to EIGRP.

Experiment: 27

Configuration Telnet

To understand the operation of TELNET by accessing the router in server room from a PC in IT office.

Requirements

- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Router – 1 Nos
- Cat-5 LAN cable

Procedure

- Open the CISCO Packet tracer software
- Drag and drop 1 pc and 1 laptop using End Device Icons on the left corner.
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router
- Type CLI's for the router
- Make and verify the connections from any pc to the server by providing correct password; in command prompt of PC.
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory

Telnet, developed in 1969, is a protocol that provides a command line interface for communication with a remote device or server, sometimes employed for remote management but also for initial device setup like network hardware. Telnet stands for Teletype Network, but it can also be used as a verb; 'to telnet' is to establish a connection using the Telnet protocol. Telnet is a simple, text-based network protocol that is used for accessing remote computers over TCP/IP networks like the Internet.

Network Topology Diagram for TELNET

Input Details for TELNET

Router 0 PC0 PC1

IP Address : 192.168.0.1 IP Address : 192.168.0.2 IP Address : 192.168.0.3

Gate way : - Gate way : 192.168.0.1 Gate way : 192.168.0.2

ROUTER CLI:

```
Router#config
Configuring from terminal, memory, or network [terminal]?
Router(config)#line vty 0 4
Router(config-line)#password sai123
Router(config-line)#login local
Router(config-line)#exit
Router(config)#username sai privilege 4 password sai123
Router(config)#exit
```

OUTPUT:
PINGING FROM PC0 TO SERVER USING TELENET:
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>telnet 192.168.0.1
Trying 192.168.0.1 ...Open
User Access Verification
Username: sai
Password: <type the password---sai123(invisible)>
Router#show ip route(now router can be accessed from pc0)
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
192.168.0.0 /24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
Router#

Result:
Thus, verified the operation of TELNET and accessed the router from Pcs

VIVA QUESTIONS

What are common uses for Telnet?
Telnet can be used to test or troubleshoot remote web or mail servers, as well as for remote access to MUDs (multi-user dungeon games) and trusted internal networks.
How does Telnet work?
Telnet provides users with a bidirectional interactive text-oriented communication system utilizing a virtual terminal connection over 8 byte. User data is interspersed in-band with telnet control information over the transmission control protocol (TCP). Often, Telnet was used on a terminal to execute functions remotely.
The user connects to the server by using the Telnet protocol, which means entering Telnet into a command prompt by following this syntax: telnet hostname port. The user then executes

commands on the server by using specific Telnet commands into the Telnet prompt. To end a session and log off, the user ends a Telnet command with Telnet.

Is Telnet secure?

Because it was developed before the mainstream adaptation of the internet, Telnet on its own does not employ any form of encryption, making it outdated in terms of modern security. It has largely been overlapped by Secure Shell (SSH) protocol, at least on the public internet, but for instances where Telnet is still in use, there are a few methods for securing your communications.

Experiment: 28

Aim: Configuration of Secured Shell (SSH) cryptographic Protocol

To understand the operation of SSH by accessing the routers remotely by PCs
Requirements

- Windows pc – 2 Nos
- CISCO Packet Tracer Software (Student Version)
- 8 port switch – 1 No
- Router – 1 Nos
- Cat-5 LAN cable

Procedure
- Open the CISCO Packet tracer software
- Drag and drop 1 pc and 1 laptop using End Device Icons on the left corner.
- Select 8 port switch from switch icon list in the left bottom corner
- Select Routers and Give the IP address for serial ports of router
- Type CLI's for the router
- Make and verify the SSH operation by pinging in the command prompt of PC
- Ping between PCs and observe the transfer of data packets in real and simulation mode.

Theory
SSH stands for Secure Shell is a network protocol, used to access remote machine in order to execute command-line network services and other commands over a Network. SSH is Known for its high security, cryptographic behavior and it is most widely used by Network Admins to control remote web servers primarily.
Both SSH and Telnet are network Protocol. Both the services are used in order to connect and communicate to another machine over Network. SSH uses Port 22 and Telnet uses port 23 by default. Telnet send data in plain text and non-encrypted format everyone can understand whereas SSH sends data in encrypted format. Not to mention SSH is more secure than Telnet and hence SSH is preferred over Telnet.

Network Topology Diagram for SSH

Input Details for SSH
Router 0 PC0 PC1
IP Address : 192.168.1.1 IP Address : 192.168.1.2 IP Address : 192.168.1.3
Gate way : - Gate way : 192.168.1.1 Gate way : 192.168.1.1
ROUTER CLI:

```
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password sai123
Router(config-line)#login local
Router(config-line)#exit
```

```
Router(config)#username saimukhesh privilege 4 password sai123
Router(config)#hostname r1
r1(config)#ip domain-name cisco
r1(config)#line vty 0 4
r1(config-line)#transport input ssh
r1(config-line)#exit
r1(config)#crypto key generate rsa
The name for the keys will be: r1.cisco
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
0r1(config)#
*Mar 1 0:3:53.842: %SSH-5-ENABLED: SSH 1.99 has been enabled
r1(config)#
```

OUTPUT:

PINGING FROM PC1 TO SERVER USING SSH:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ssh -l saimukhesh 192.168.1.1
Open
Password: <sai123>
r1#
```

(now router can be accessed from pc1)

Result:

Thus, verified the operation of SSH and accessed the router from a remote Pcs.

What is SSH?

VIVA QUESTIONS

Secure Shell protocol is abbreviated as SSH. It is a secure and most commonly using protocol to access remote servers. This protocol uses encryption while transferring data between two hosts.

What is SSH port forwarding ?

SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming.
Syntax : ssh -L localport:host:hostport user@ssh_server –N
where:
-L – port forwarding parameters
localport – local port (chose a port that is not in use by other service)
host – server that has the port (hostport) that you want to forward
hostport – remote port
-N – do not execute a remote command, (you will not have the shell)
user – user that have ssh access to the ssh server (computer)
ssh_server – the ssh server that will be used for forwarding/tunnelling
How to enable debugging in ssh command ?
To enable debugging in ssh command use '-v' option like 'ssh root@www.linuxtechi.com -v'.
To increase the debugging level just increase the number of v's.
What is the difference between ssh & Telnet ?
In ssh communication between client & server is encrypted but in telnet communication between the client & server is in plain text . We can also say SSH uses a public key for authentication while Telnet does not use any authentication.SSH adds a bit more overhead to the bandwidth compared to Telnet. Default port of ssh is 22 and for telnet 23.
How to check SSH server's Version ?
Using the command ' ssh -V ' we can find the ssh server's version.