LAB MANUAL
NETWORKING LAB

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

SKDAV GOVT .POLYTECHNIC ROURKELA

S.No	Experiment
1	Study of different types of Network cables(coaxial,OFC,UTP,stp) and Practically implement the cross-wired cable and straight through cable using clamping tool.
2	Study of Network Devices in Detail.
3	Study of network IP.
4	Create network of at least 6 computers in Local Area Network.
5	Study of basic network command and configuring network commands.
6	Performing an Initial Switch Configuration
7	Performing an Initial Router Configuration
8	Configuring and Troubleshooting a Switched Network
9	Connecting a Switch
10	Configuring a Wireless Router
11	Using the Cisco IOS Show Commands
12	Study WAN cncept and configure and forward traffic in WAN
13	Connectivity troubleshooting using PING ,IPCONFIG
14	Demonstrating Distribution Layer Functions
15	Study of scaling of networks ,design verities of LAN and forward of traffic
16	Implementing an IP Addressing Scheme
17	Examining Network Address Translation (NAT)
18	Study of Static and Dynamic Routing
19	Install and configure a network interfacecard in work station
20	Configuring a Default Route
21	Configuring Static and Default Routes
22	Configuring RIP
23	Configuring a Cisco Router as a DHCP Server and troubles shoot network

Experiment-1

AIM OF EXPT: Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.

Apparatus (Components): RJ-45 connector, Climping Tool, Twisted pair Cable

Procedure: To do these practical following steps should be done:

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	

CONCLUSION:-

Experiment - 2

AIM OF EXPERIMENT: Study of following Network Devices in Detail

- Repeater
- Hub
- Switch
- Bridge
- Router
- Gate Way

Apparatus (Software): No software or hardware needed.

Procedure: Following should be done to understand this practical.

1. **Repeater:**Functioning at Physical Layer.A**repeater** is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeater have two ports ,so cannot be use to connect for more than two devices

2. Hub: An **Ethernet hub**, **active hub**, **network hub**, **repeater hub**, **hub** or **concentrator** is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

3. **Switch:**A**network switch** or **switching hub** is a computer networking device that connects network segments.The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

4. **Bridge:** A **network bridge** connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term *bridge* formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. *Switch* or *Layer 2 switch* is often used interchangeably with *bridge* .Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

5. **Router:** A **router** is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

6. **Gate Way:** In a communications network, a network node equipped for interfacing with

another network that uses different protocols.

- A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.
- A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

CONCLUSION:-

Experiment - 3

AIM OF EXPERIMENT: Study of network IP

- Classification of IP address
- Sub netting
- Super netting

Apparatus (Software): NA

Procedure: Following is required to be study under this practical.

- Classification of IP address

As show in figure we teach how the ip addresses are classified and when they are used.

Class	Address Range	Supports
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.

- **Sub netting**

Why we Develop sub netting and How to calculate subnet mask and how to identify subnet address.

- **Super netting**

Why we develop super netting and How to calculate supernet mask and how to identify supernet address.

CONCLUSION:-

Experiment-4

AIM OF EXPERIMENT: Create network of at least 6 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.

CONCLUSION:-

Experiment-5

AIM OF EXPERIMENT: Study of basic network command and configuring netwok commands.

Apparatus (Software): Command Prompt And Packet Tracer.

Procedure: To do this EXPERIMENT- follows these steps:

In this EXPERIMENT- students have to understand basic networking commands e.g ping, tracert etc.

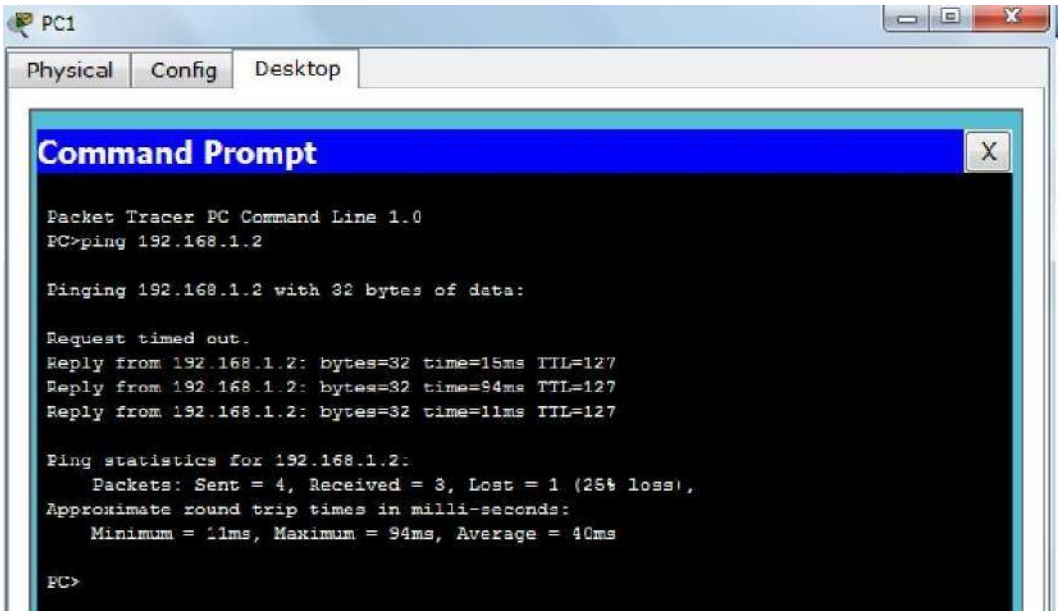
All commands related to Network configuration which includes how to switch to privilege mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.

This commands includes

- Configuring the Router commands
- General Commands to configure network
- Privileged Mode commands of a router
- Router Processes & Statistics
- IP Commands
- Other IP Commands e.g. show ip route etc.

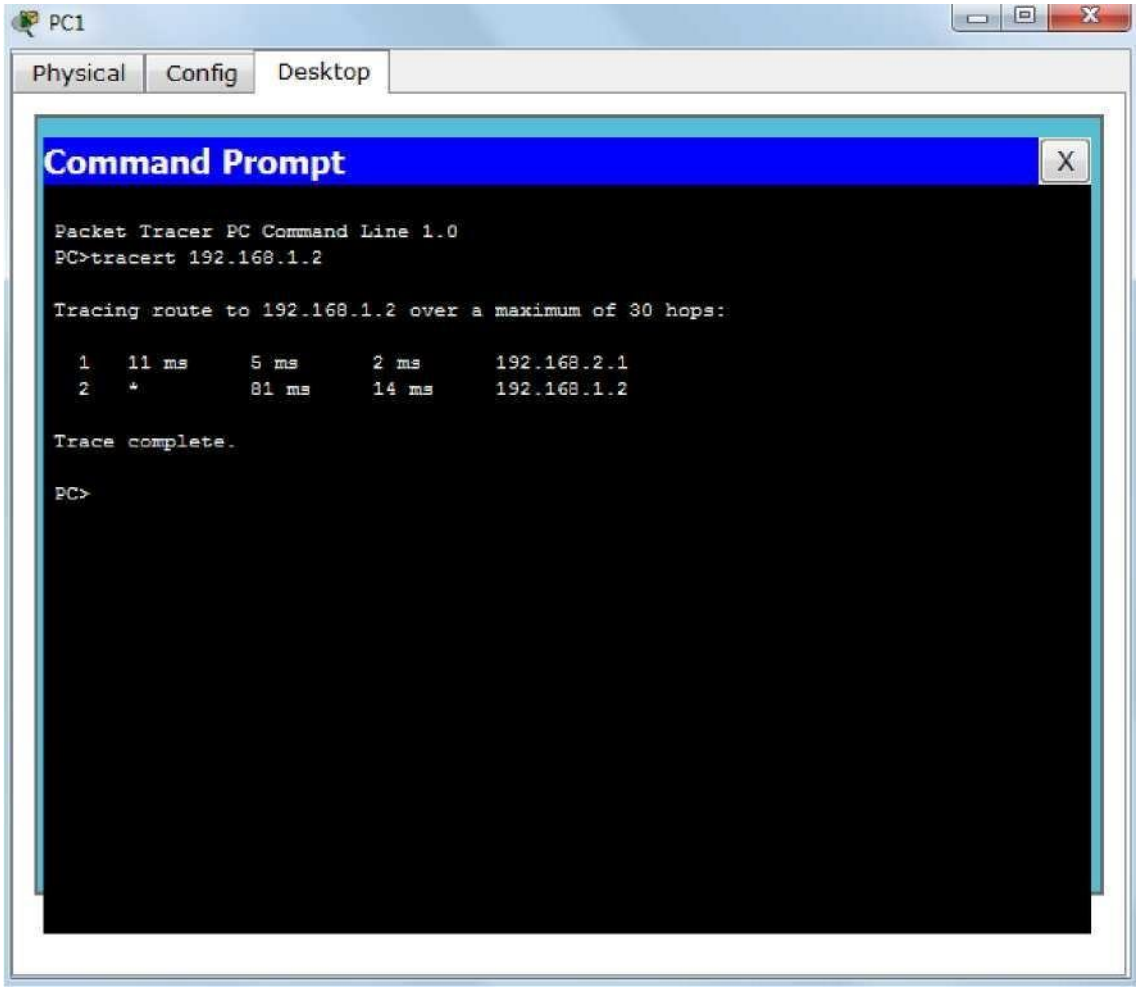
ping:

ping(8) sends an ICMP ECHO_REQUEST packet to the specified host. If the host responds, you get an ICMP packet back. Sound strange? Well, you can "ping" an IP address to see if a machine is alive. If there is no response, you know something is wrong.



Traceroute:

Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.

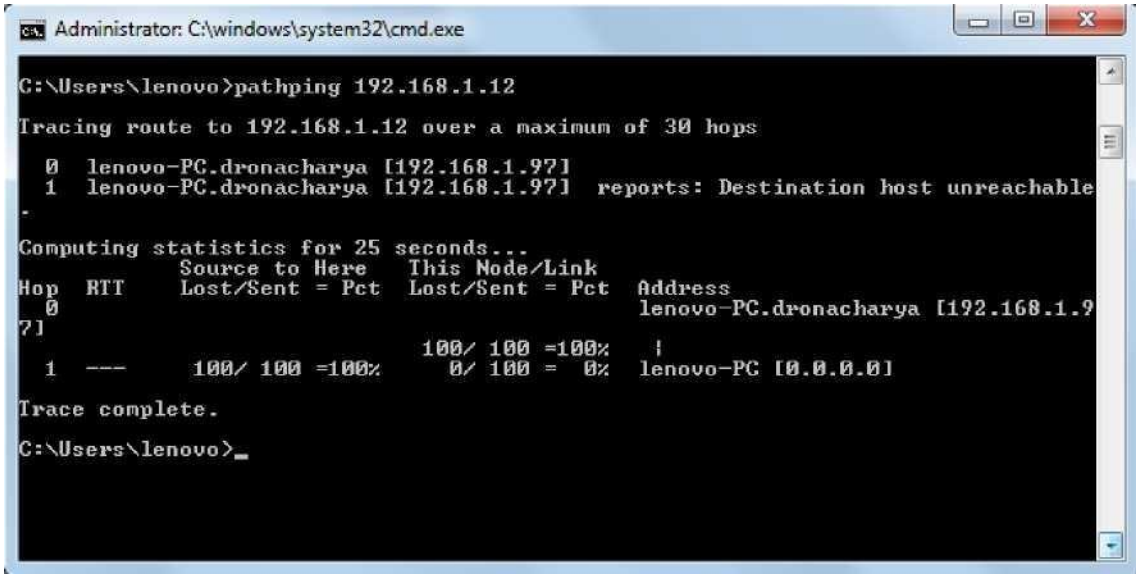


nslookup:

Displays information from Domain Name System (DNS) name servers.
NOTE :If you write the command as above it shows as default your pc's server name firstly.

pathping:

A better version of tracert that gives you statics about packet lost and latency.



Getting Help

In any command mode, you can get a list of available commands by entering a question mark (?).

Router>**?**
To obtain a list of commands that begin with a particular character sequence, type in those haracters followed immediately by the question mark (?).

Router#**co?**

configure connect copy
To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark.

Router#**configure ?**

memory Configure from NV memory network Configure from a TFTP network host terminal Configure from the terminal
You can also abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh**.

Configuration Files

Any time you make changes to the router configuration, you must save the changes to memory because if you do not they will be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the startup configuration.
Use the following privileged mode commands to work with configuration files.

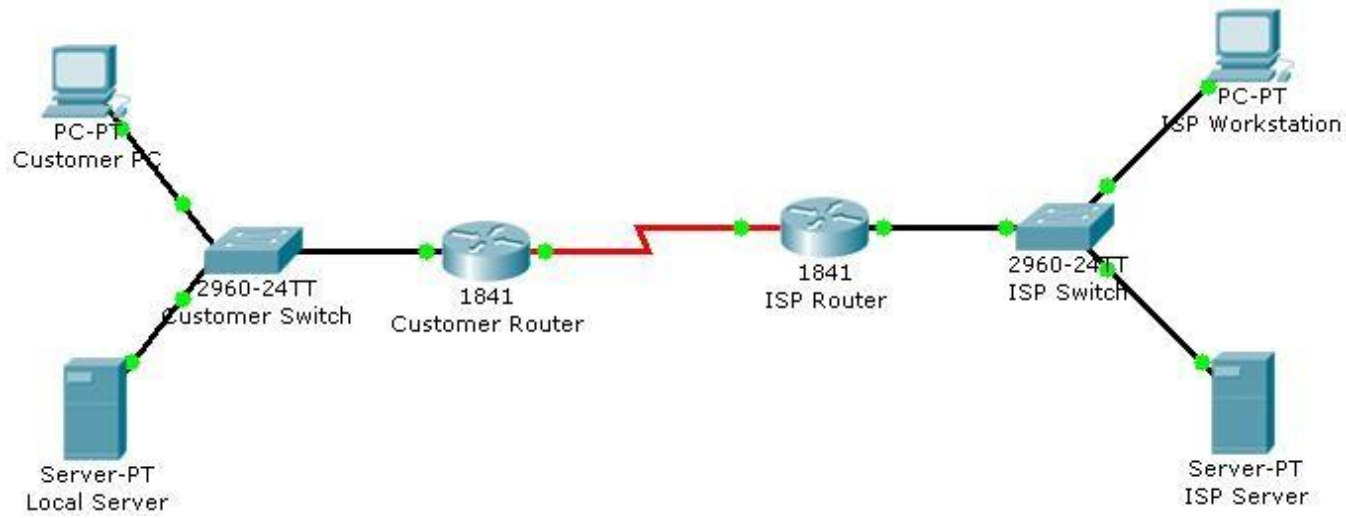
CONCLUSION:-

Experiment-6

AIM:Performing an Initial Switch Configuration

Apparatus (Software): Command Prompt And Packet Tracer.

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. Fromthe 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 **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 3: Configure the console password.

a. From global configuration mode, switch to configuration mode to configure the console line.

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

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

CustomerSwitch(config-line)#**password cisco**
CustomerSwitch(config-line)#**login**
CustomerSwitch(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.

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

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

CustomerSwitch(config-line)#**password cisco**
CustomerSwitch(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 address 192.168.1.5 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 pings may 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 ms

CustomerSwitch#
```

Reflection

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?

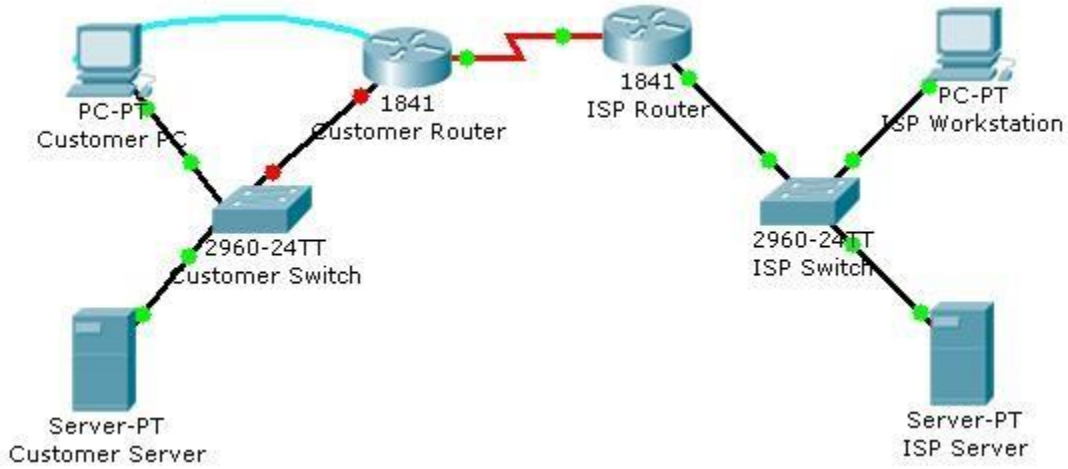
CONCLUSION:-

Experiment-7

AIM:-Performing an Initial Router Configuration

Apparatus (Software): Command Prompt And Packet Tracer.

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 host name, 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 Cisco 1841 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 showthe running 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, encrypt all 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 before the 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 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.

```
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 router CLI.

```
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.

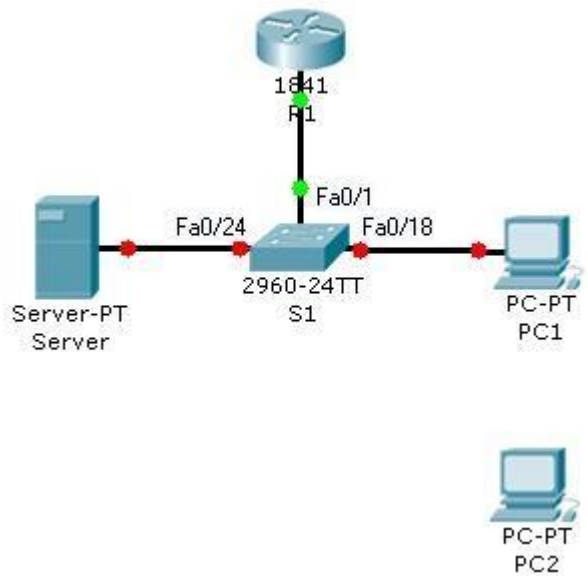
CONCLUSION:-

Experiment-8

AIM:-Configuring and Troubleshooting a Switched Network

Apparatus (Software): Command Prompt And Packet Tracer.

Topology Diagram



Objectives

- Establish console connection to the switch.
- Configure the host name and VLAN1.
- Use the help feature to configure the clock.
- Configure passwords and console/Telnet access.
- Configure login banners.
- Configure the router.
- Solve duplex and speed mismatch problems.
- Configure port security.
- Secure unused ports.
- Manage the switch configuration file.

Background / Preparation

In this Packet Tracer Skills Integration Challenge activity, you will configure basic switch management, including general maintenance commands, passwords, and port security. This activity provides you an opportunity to review previously acquired skills.

Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	172.17.99.1	255.255.255.0
S1	Fa0/1	172.17.99.11	255.255.255.0
PC1	NIC	172.17.99.21	255.255.255.0
PC2	NIC	172.17.99.22	255.255.255.0
Server	NIC	172.17.99.31	255.255.255.0

Step 1: Establish a console connection to a switch.

For this activity, direct access to the S1 Config and CLI tabs is disabled. You must establish a console session through PC1.

a. Connect a console cable from PC1 to S1.

b. From PC1, open a terminal window and use the default terminal configuration. You should now have access to the CLI for S1.

c. Check results.

Your completion percentage should be 8%. If not, click **Check Results** to see which required components are not yet completed.

Step 2: Configure the host name and VLAN 1.

a. Configure the switch host name as S1.

b. Configure port Fa0/1. Set the mode on Fast Ethernet 0/1 to access mode.

i. S1(config)#**interface fastethernet 0/1**
ii. S1(config-if)#**switchport mode access**

c. Configure IP connectivity on S1 using VLAN 1.

i. S1(config)#**interface vlan 1**
ii. S1(config-if)#**ip address 172.17.99.11 255.255.255.0**
iii. S1(config-if)#**no shutdown**

d. Configure the default gateway for S1 and then test connectivity. S1 should be able to ping R1.

e. Check results.

Your completion percentage should be 31%. If not, click **Check Results** to see which required components are not yet completed. Also, make sure that interface VLAN 1 is active.

Step 3: Configure the current time using Help.

a. Configure the clock to the current time. At the privileged EXEC prompt, enter clock ?.

b. Use Help to discover the steps required to set the current time.

c. Use the show clock command to verify that the clock is now set to the current time. Packet Tracer may not correctly simulate the time you entered.

Packet Tracer does not grade this command, so the completion percentage does not change.

Step 4: Configure passwords.

a. Use the encrypted form of the privileged EXEC mode password and set the password to class.

b. Configure the passwords for console and Telnet. Set both the console and vty password to cisco and require users to log in.

c. View the current configuration on S1. Notice that the line passwords are shown in clear text. Enter the command to encrypt these passwords.

d. Check results.

Your completion percentage should be 42%. If not, click **Check Results** to see which required components are not yet completed.

Step 5: Configure the login banner.

If you do not enter the banner text exactly as specified, Packet Tracer does not grade your command correctly. These commands are case-sensitive. Also make sure that you do not include any spaces before or after the text.

a. Configure the message-of-the-day banner on S1 to display as Authorized Access Only. (Do not include the period.)

b. Check results.

Your completion percentage should be 46%. If not, click **Check Results** to see which required components are not yet completed.

Step 6: Configure the router.

Routers and switches share many of the same commands. Configure the router with the same basic commands you used on S1.

a. Access the CLI for R1 by clicking the device.

b. Do the following on R1:

- Configure the hostname of the router as R1.
- Configure the encrypted form of the privileged EXEC mode password and set the password to class.
- Set the console and vty password to cisco and require users to log in.
- Encrypt the console and vty passwords.
- Configure the message-of-the-day as **Authorized Access Only**. (Do not include the period.)

c. Check results.

Your completion percentage should be 65%. If not, click **Check Results** to see which required components are not yet completed.

Step 7: Solve a mismatch between duplex and speed.

a. PC1 and Server currently do not have access through S1 because the duplex and speed are mismatched. Enter commands on S1 to solve this problem.

b. Verify connectivity.

c. Both PC1 and Server should now be able to ping S1, R1, and each other.

d. Check results.

Your completion percentage should be 73%. If not, click **Check Results** to see which required components are not yet completed.

Step 8: Configure port security.

a. Use the following policy to establish port security on the port used by PC1:

- Enable port security
- Allow only one MAC address
- Configure the first learned MAC address to "stick" to the configuration

Note: Only enabling port security is graded by Packet Tracer and counted toward the completion percentage. However, all the port security tasks listed above are required to complete this activity successfully.

b. Verify that port security is enabled for Fa0/18. Your output should look like the following output. Notice that S1 has not yet learned a MAC address for this interface. What command generated this output?

S1#_____

```
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

c. Force S1 to learn the MAC address for PC1. Send a ping from PC1 to S1. Then verify that S1 added the MAC address for PC1 to the running configuration.

```
!
interface FastEthernet0/18
 <output omitted>
 switchport port-security mac-address sticky 0060.3EE6.1659
 <output omitted>
!
```

d. Test port security. Remove the FastEthernet connection between S1 and PC1. Connect PC2 to Fa0/18. Wait for the link lights to turn green. If necessary, send a ping from PC2 to S1 to cause the port to shut down. Port security should show the following results: (the Last Source Address may be different)

```
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
```

Configured MAC Addresses : 1
Sticky MAC Addresses 0
Last Source Address:Vlan : 00D0.BAD6.5193:99
Security Violation Count 1

e. Viewing the Fa0/18 interface shows that line protocol is down (err-disabled), which also indicates a security violation.

S1#**show interface fa0/18**
FastEthernet0/18 is down, line protocol is down (err-disabled)
<output omitted>

f. Reconnect PC1 and re-enable the port. To re-enable the port, disconnect PC2 from Fa0/18 and reconnect PC1. Interface Fa0/18 must be manually reenabled with the no shutdown command before returning to the active state.

g. Check results.

Your completion percentage should be 77%. If not, click **Check Results** to see which required components are not yet completed.

Step 9: Secure unused ports.

a. Disable all ports that are currently not used on S1. Packet Tracer grades the status of the following ports: Fa0/2, Fa0/3, Fa0/4, Gig 1/1, and Gig 1/2.

b. Check results.

Your completion percentage should be 96%. If not, click **Check Results** to see which required components are not yet completed.

Step 10: Manage the switch configuration file.

a. Save the current configuration for S1 and R1 to NVRAM.

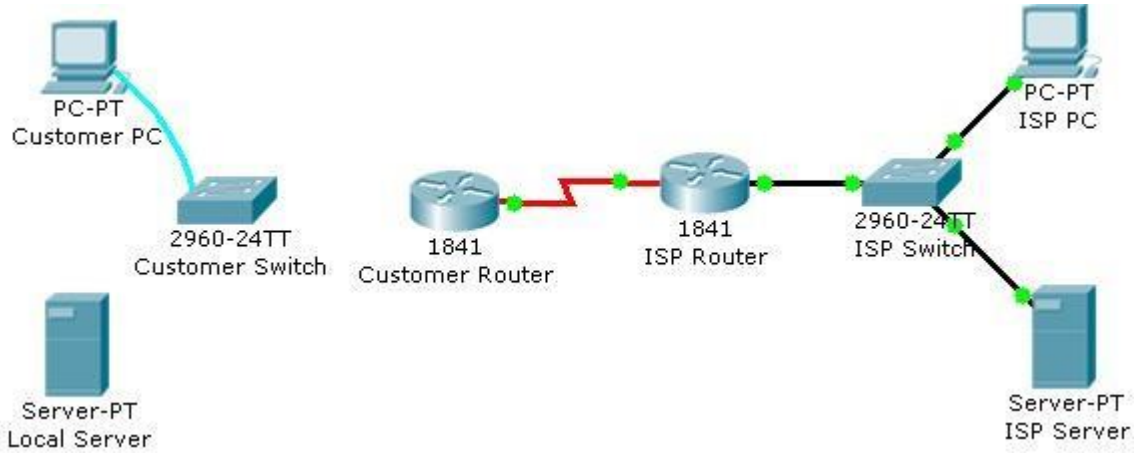
b. Back up the startup configuration file on S1 and R1 byuploading them to Server. Verify that Server has the R1-confg and S1-confg files.

c. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Experiment-9

AIM OF EXPERIMENT:- **Connecting a Switch**



Objectives

- Connect a switch to the network.
- Verify the configuration on the switch.

Background / Preparation

In this activity, you will verify the configuration on the customer Cisco Catalyst 2960 switch. The switch is already configured with all the basic necessary information for connecting to the LAN at the customer site. The switch is currently not connected to the network. You will connect the switch to the customer workstation, the customer server, and customer router. You will verify that the switch has been connected and configured successfully by pinging the LAN interface of the customer router.

Step 1: Connect the switch to the LAN.

a. Using the proper cable, connect the FastEthernet0/0 on Customer Router to the FastEthernet0/1 on Customer Switch.

b. Using the proper cable, connect the Customer PC to the Customer Switch on port FastEthernet0/2.

c. Using the proper cable, connect the Local Server to the Customer Switch on port FastEthernet0/3.

Step 2: Verify the switch configuration.

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

b. Use the console connection and terminal utility on the Customer PC to verify the configurations. Use **cisco** as the console password.

c. Enter privileged EXEC mode and use the **show running-config** command to verify the following configurations. The password is **cisco123**.

   a. VLAN1 IP address = 192.168.1.5

   b. Subnet mask = 255.255.255.0

c. Password required for console access

d. Password required for vty access

e. Password enabled for privileged EXEC mode

f. Secret enabled for privileged EXEC mode

d. Verify IP connectivity between the Cisco Catalyst 2960 switch and the Cisco 1841 router by initiating a ping to 192.168.1.1 from the switch CLI.

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

Reflection

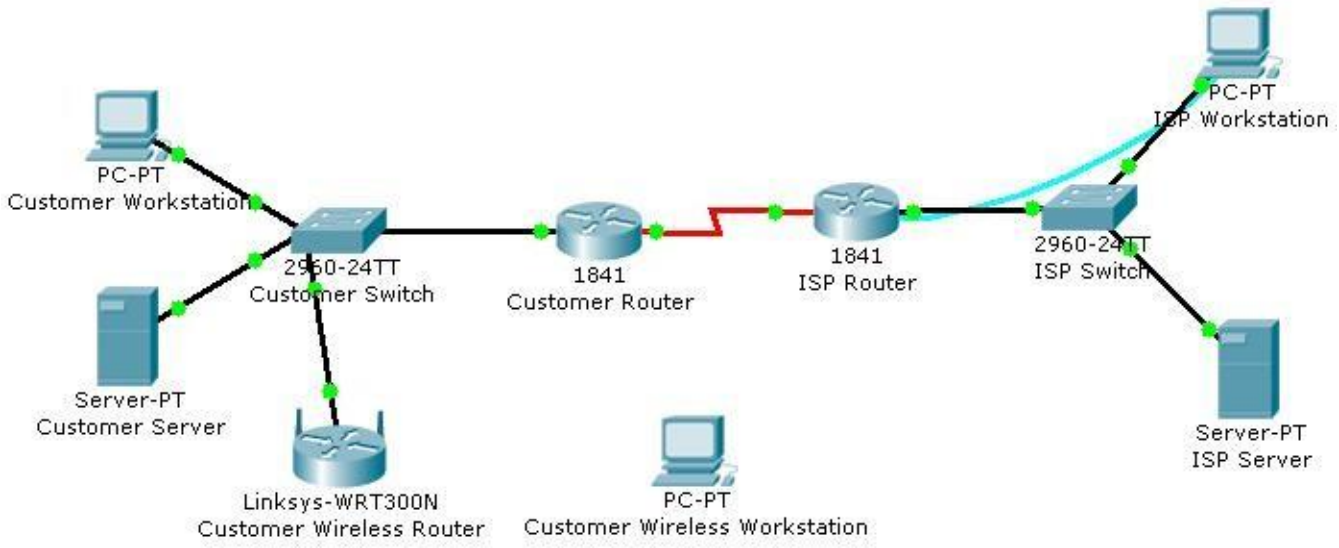
a. What is the significance of the enable secret command compared to the enable password?

b. If you want to remove the requirement to enter a password to access the console, what commands do you issue from your starting point in privileged EXEC mode?

Experiment-10

AIM OF EXPT:- Configuring WEP on a Wireless Router

Topology Diagram



Objectives

- Configure WEP security between a workstation and a Linksys wireless router.

Background / Preparation

You have been asked to go back to a business customer and install a new Linksys wireless router for the customer office. The company has some new personnel who will be using wireless computers to save money on adding additional wired connections to the building. The business is concerned about the security of the network because they have financial and highly classified data being transmitted over the network. Your job is to configure the security on the router to protect the data.

In this activity, you will configure WEP security on both a Linksys wireless router and a workstation.

Step 1: Configure the Linksys wireless router to require WEP.

a. Click the **Customer Wireless Router** icon. Then, click the **GUI** tab to access the router web management interface.

b. Click the **Wireless** menu option and change the **Network Name (SSID)** from **Default** to **CustomerWireless**. Leave the other settings with their default options.

c. Click the **Save Settings** button at the bottom of the **Basic Wireless Settings** window.

d. Click the **Wireless Security** submenu under the **Wireless** menu to display the current wireless security parameters.

e. From the **Security Mode** drop-down menu, select **WEP**.

f. In the **Key1** text box, type **1a2b3c4d5e**. This will be the new WEP pre-shared key to access the wireless network.

g. Click the **Save Settings** button at the bottom of the **Wireless Security** window.

Step 2: Configure WEP on the customer wireless workstation.

a. Click the **Customer Wireless Workstation**.

b. Click the **Config** tab.

c. Click the **Wireless** button to display the current wireless configuration settings on the workstation.

d. Change the **SSID** to **CustomerWireless**.

e. Change the **Security Mode** to **WEP**. Enter **1a2b3c4d5e** in the **Key** text box, and then close the window.

Step 3: Verify the configuration.

After you configure the correct WEP key and SSID on the customer wireless workstation, notice that there is a wireless connection between the workstation and the wireless router.

a. Click the Customer Wireless Workstation.

b. Click the **Desktop** tab to view the applications that are available.

c. Click on the **Command Prompt** application to bring up the command prompt.

d. Type **ipconfig /all** and press **Enter** to view the current network configuration settings.

e. Type **ping 192.168.2.1** to verify connectivity to the LAN interface of the customer wireless router.

f. Close the command prompt window.

g. Open a web browser.

h. In the address bar of the web browser window, type **http://192.168.1.10**. Press **Enter**. The Intranet web page that is running on the customer server appears. You have just verified that the customer wireless workstation has connectivity to the rest of the customer network.

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

Reflection

a. What is the purpose of using WEP on a wireless network?

b. What is the significance of the key that you used to secure WEP?

c. Is WEP the best choice for wireless security?

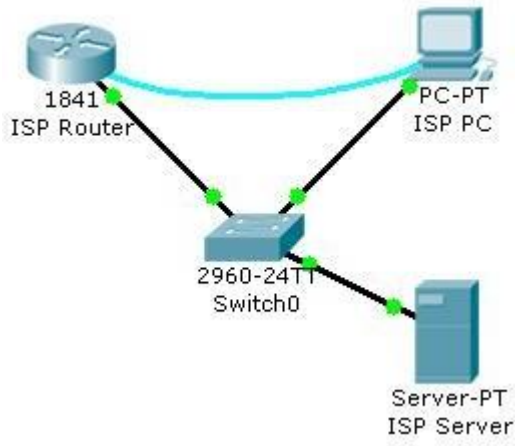
CONCLUSION:-

Experiment-11

AIM OF EXP:- Using the Cisco IOS Show Commands

Topology Diagram

Apparatus (Software): Command Prompt And Packet Tracer.



Objectives

- Use the Cisco IOS **show** commands.

Background / Preparation

The Cisco IOS **show** commands are used extensively when working with Cisco equipment. In this activity, you will use the **show** commands on a router that is located at an ISP.

Note: This activity begins by showing 100% completion, because the purpose is only to explore the Cisco IOS **show** commands. This activity is not graded.

Step 1: Connect to the ISP Cisco 1841 router.

Use the terminal emulation software on ISP PC to connect to the Cisco 1841 router. The **ISPRouter>** prompt indicates that you are in user EXEC mode. Now type **enable** at the prompt. The **ISPRouter#** promptindicates that you are in privileged EXEC mode.

Step 2: Explore the show commands.

Use the information displayed by these **show** commands to answer the questions in the Reflection section.

a. Type **show arp**.

b. Type **show flash**.

c. Type **show ip route**.

d. Type **show interfaces**.

e. Type **show protocols**.

f. Type **show users**.

g. Type **show version**.

Reflection

a. Why do you need to be in privileged EXEC mode to explore the Cisco IOS **show** commands that were used in this activity?

How much flash memory is reported?

Which of the following is subnetted?

- 209.165.201.0
- 209.165.201.1
- 209.165.201.10

Which interface is up and running?

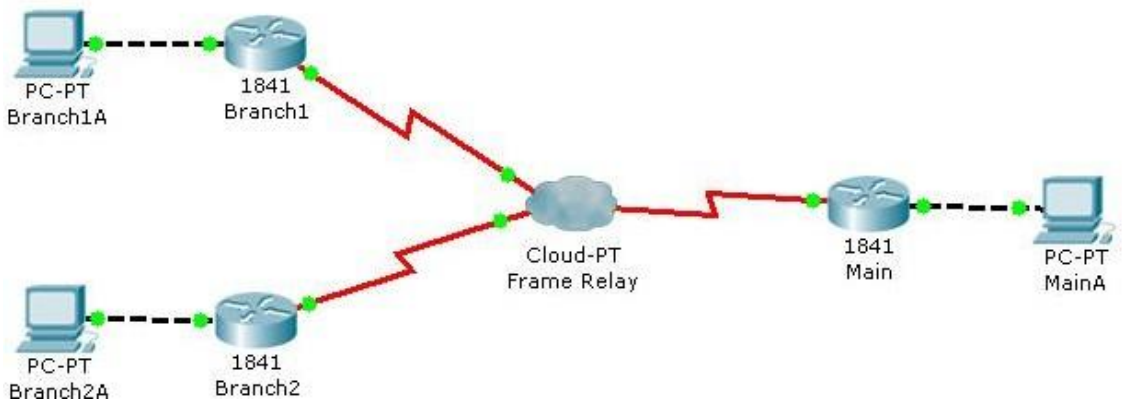
- Serial0/1/0
- FastEthernet0/1
- FastEthernet0/0
- VLAN1

CONCLUSION:-

Experiment-12

Aim of experiment: Study WAN concepts and Configure and forward traffic in WAN

Apparatus (Software): Command Prompt And Packet Tracer.



Objective

The **show** commands are very powerful commands for troubleshooting and monitoring networks. They give a static image of the network at a given time. The use of a variety of **show** commands will give a clear picture of how the networking is communicating and transferring data.

Background / Preparation

The physical topology of the network has been designed using Frame Relay. To test the network connectivity, use a variety of **show** commands.

Required file: Examining WAN Connections.pka

Step 1: Examine the configuration of Branch1 and Branch2.

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: Examine the configuration of Main.

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.

Reflection

a. In what situations would it be beneficial to use the various **show** commands?

_____
_____
____

b. What beneficial information can be obtained from the various **show** commands?

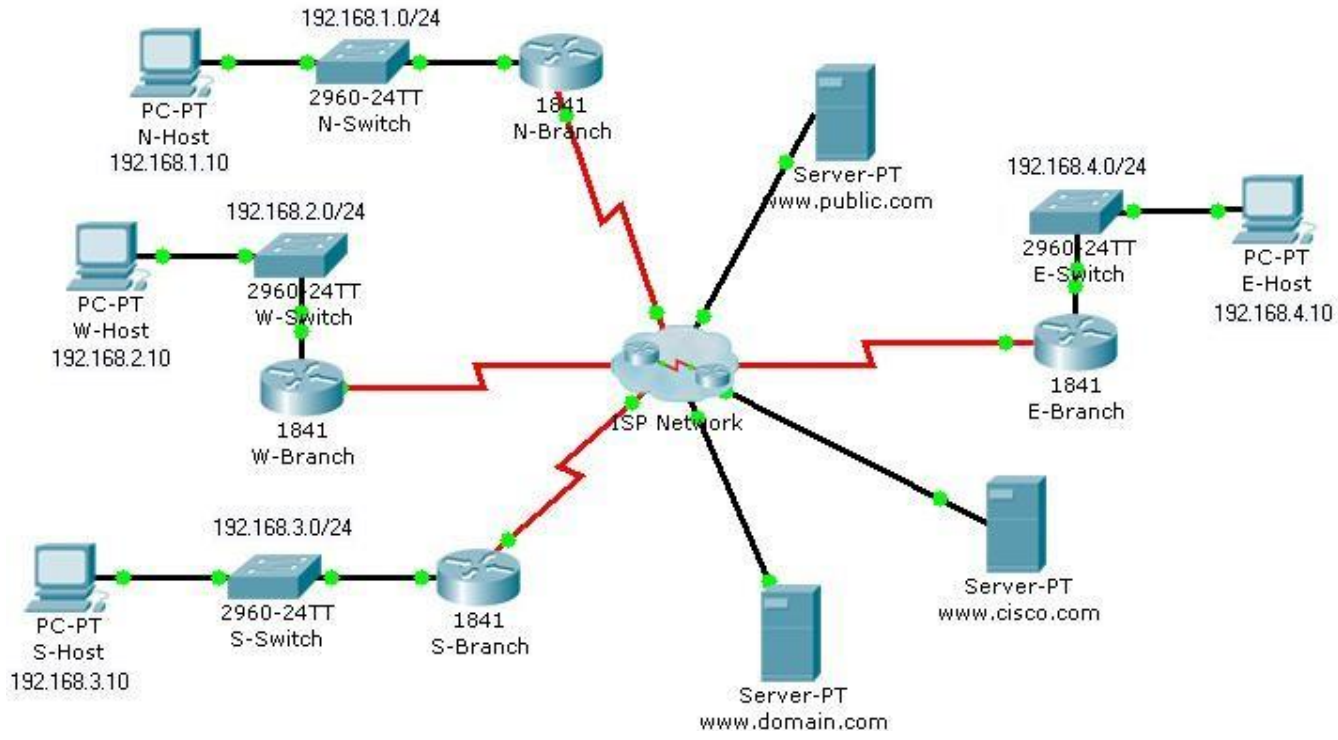
_____
_____
____

CONCLUSION:-

Experirment-13

EXPERIMENT-Connectivity troubleshooting using PING ,IPCONFIG

Apparatus (Software): Command Prompt And Packet Tracer.



Objectives

- Distinguish the difference between successful and unsuccessful ping attempts.
- Distinguish the difference between successful and unsuccessful traceroute attempts.

Background / Preparation

In this activity, you will test end-to-end connectivity using ping and traceroute. At the end of this activity, you will be able to distinguish the difference between successful and unsuccessful ping and traceroute attempts.

Note: Before beginning this activity, make sure that the network is converged. To converge the network quickly, switch between Simulation mode and Realtime mode until all the link lights turn green.

Step 1: Test connectivity using ping from a host computer and a router.

Click N-Host, click the **Desktop** tab, and then click **Command Prompt**. From the Command Prompt window, ping the Cisco server at www.cisco.com.

Packet Tracer PC Command Line 1.0
PC>**ping www.cisco.com**

Pinging 64.100.1.185 with 32 bytes of data:

Request timed out.

```
Reply from 64.100.1.185: bytes=32 time=185ms TTL=123
Reply from 64.100.1.185: bytes=32 time=281ms TTL=123
Reply from 64.100.1.185: bytes=32 time=287ms TTL=123

Ping statistics for 64.100.1.185:
   Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
   Minimum = 185ms, Maximum = 287ms, Average = 251ms

PC>
```

From the output, you can see that N-Host was able to obtain an IP address for the Cisco server. The IP address was obtained using (DNS). Also notice that the first ping failed. This failure is most likely due to lack of ARP convergence between the source and destination. If you repeat the ping, you will notice that all pings succeed.

From the Command Prompt window on N-Host, ping E-Host at 192.168.4.10. The pings fail. If you do not want to wait for all four unsuccessful ping attempts, press **Ctrl+C** to abort the command, as shown below.

```
PC>ping 192.168.4.10

Pinging 192.168.4.10 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 192.168.4.10:
   Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
PC>
```

Click the N-Branch router, and then click the **CLI** tab. Press **Enter** to get the router prompt. From the router prompt, ping the Cisco server at www.cisco.com.

```
N-Branch>ping www.cisco.com
Translating "www.cisco.com"...domain server (64.100.1.242)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.100.1.185, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 210/211/213 ms

N-Branch>
```

As you can see, the ping output on a router is different from a PC host. Notice that the N-Branch router resolved the domain name to the same IP address that N-Host used to send its pings. Also notice that the first ping fails, which is indicated by a period (.), and that the next four pings succeed, as shown with an exclamation point (!).

From the CLI tab on N-Branch, ping E-Host at 192.168.4.10. Again, the pings fail. To not wait for all the failures, press **Ctrl+C**.

```
N-Branch>ping 192.168.4.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.10, timeout is 2 seconds:
...
Success rate is 0 percent (0/4)

N-Branch>
```

Step 2: Test connectivity using traceroute from a host computer and a router.

a. Click N-Host, click the **Desktop tab**, and then click **Command Prompt**. From the Command Prompt window, trace the route to the Cisco server at www.cisco.com.

```
PC>tracert www.cisco.com

Tracing route to 64.100.1.185 over a maximum of 30 hops:

  1   92 ms     77 ms     86 ms     192.168.1.1
  2 91 ms       164 ms    84 ms     64.100.1.101
  3 135 ms      168 ms    151 ms    64.100.1.6
  4 185 ms      261 ms    161 ms    64.100.1.34
  5 257 ms      280 ms    224 ms    64.100.1.62
  6 310 ms      375 ms    298 ms    64.100.1.185

Trace complete.

PC>
```

The above output shows that you can successfully trace a route all the way to the Cisco server at 64.100.1.185. Each hop in the path is a router responding three times to trace messages from N-Host. The trace continues until the destination for the trace (64.100.1.185) responds three times.

From the Command Prompt window on N-Host, trace a route to E-Host at 192.168.4.10. The trace fails, but notice that the **tracert** command traces up to 30 hops. If you do not want to wait for all 30 attempts to time out, press **Ctrl+C**.

```
PC>tracert 192.168.4.10

Tracing route to 192.168.4.10 over a maximum of 30 hops:

  1 103 ms      45 ms     91 ms     192.168.1.1
  2 56 ms       110 ms    125 ms    64.100.1.101
  3 174 ms      195 ms    134 ms    64.100.1.6
  4 246 ms      183 ms    179 ms    64.100.1.34
  5 217 ms      285 ms    226 ms    64.100.1.62
  6 246 ms      276 ms    245 ms    64.100.1.154
  7   *         *         *         Request timed out.
  8   *         *         *         Request timed out.
  9   *         *         *         Request timed out.
 10
Control-C
^C
PC>
```

The **tracert** command can be helpful in finding the potential source of a problem. The last device to respond was 64.100.1.154, so you would start troubleshooting by determining which device is configured with the IP address 64.100.1.154. The source of the problem might not be that device, but the trace has given you a starting point, whereas a ping simply tells you that the destination is either reachable or unreachable.

Click the N-Branch router, and then click the **CLI** tab. Press **Enter** to get the router prompt. From the router prompt, trace the route to the Cisco server at www.cisco.com.

```
N-Branch>traceroute www.cisco.com
Translating "www.cisco.com"...domain server (64.100.1.242)
Type escape sequence to abort.
Tracing the route to 64.100.1.185

  1 64.100.1.101     60 msec 32 msec 59 msec
  2 64.100.1.6       98 msec 65 msec 65 msec
  3 64.100.1.34      138 msec 147 msec 147 msec
  4 64.100.1.62      189 msec 148 msec 145 msec
  5 64.100.1.185     219 msec 229 msec 293 msec
N-Branch>
```

As you can see, traceroute output on a router is very similar to the output on a PC host. The only difference is that on a PC host, the IP address is listed after the three millisecond outputs.

From the **CLI** tab on N-Branch, trace the route to E-Host at 192.168.4.10. The trace fails at the same IP address as it failed when tracing from N-Host. Again, you can use **Ctrl+C** to abort the command.

```
N-Branch>traceroute 192.168.4.10
Type escape sequence to abort.
Tracing the route to 192.168.4.10

  1   64.100.1.101    41 msec    19 msec    32 msec
  2   64.100.1.6      33 msec    92 msec    117 msec
  3   64.100.1.34     98 msec 102 msec 102 msec
  4   64.100.1.62     166 msec 172 msec 156 msec
  5   64.100.1.154    157 msec 223 msec 240 msec
  6   *     *     *
  7   *     *     *
  8   *     *     *
  9
N-Branch>
```

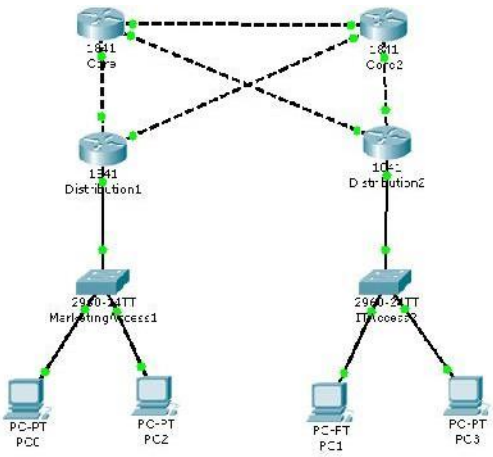
Step 3: Practice the ping and trace route commands.

Throughout this course, you will often use ping and traceroute to test connectivity and troubleshoot problems. To practice these commands, ping and trace from W-Host and S-Host to any other destination in the network. You can also ping and trace from N-Branch to other locations.

CONCLUSION:-

Experirment-14

AIM OF EXPT:-Demonstrating Distribution Layer Functions
Apparatus (Software): Command Prompt And Packet Tracer.



Objective

- Demonstrate the functions performed by the Distribution Layer devices.

Background / Preparation

VLANs can be added to a network for security purposes and traffic control. Devices on separate VLANs are unable to communicate unless a router has been configured to help with this communication. Observe how packet filtering and route summarization traverse the network using simulation mode.

Required file: Demonstrating Distribution Layer Functions

Step 1: Setup Simulation filters to capture routing protocols

a. Enter simulation mode in Packet Tracer.
b. Click on the edit filters button.
c. Select EIGRP
d. Click on the Reset Simulation button.
e. Click Auto Capture/Play
f. Observe the EIGRP updates

Step 2: Test connectivity between the network devices using Realtime mode.

a. From PC0 ping PC1, PC2, PC3, and PC4.
b. From PC1 ping PC0, PC2, PC4, PC3

Step 3: Test connectivity between the network devices using Simulation mode

a. Switch from Realtime mode to Simulation mode.
b. Create a simple PDU from PC0 to PC1. Click Capture/Forward until the PDU has made the complete trip to PC1 and back.
c. In the event list view the PDU events.
d. Create another PDU from PC0 to PC2.

Reflection

c. Why can't PC0 communicate with PC1 but PC1 can communicate with PC0's default gateway?

_____

_____

_____

d. What effect on connectivity would removing the subinterfaces have?

_____

_____

e. Why must a router be in the topology to have communication between the VLANs?

_____

_____

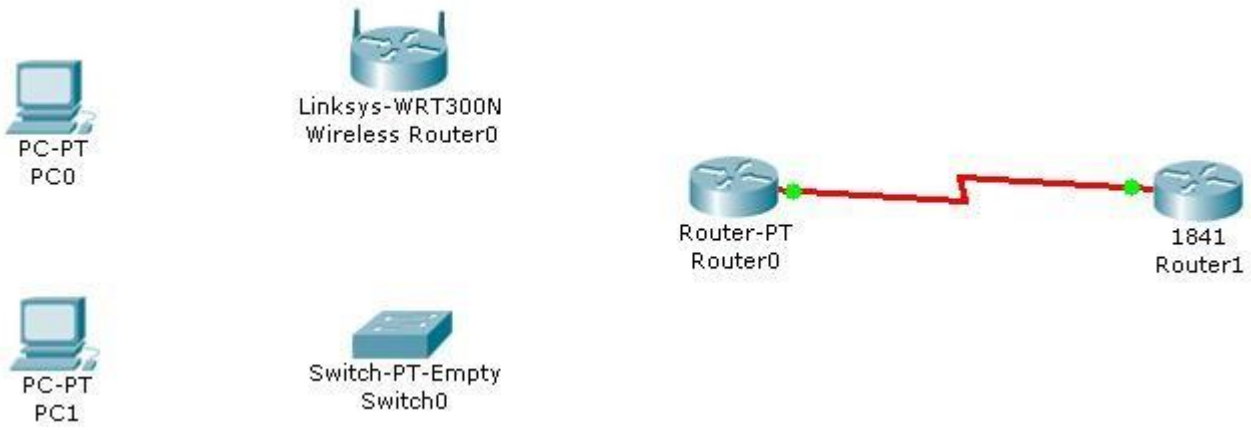
_____

Experirment-15

AIM OF EXPERIMENT: Study of scaling of networks ,design verities of LAN and forward of traffic

Apparatus (Software): Command Prompt And Packet Tracer.

Topology Diagram



Objectives

- Determine the cable types to use to connect all devices to the switch.
- Add appropriate modules to switches and routers.
- Connect the devices to the switch using the appropriate cable types.

Background / Preparation

The results of a site survey for an ISP customer indicate that the customer needs to upgrade the LAN to include a new standalone switch. The network has an existing router (Router0) and a Linksys 300N router. It is necessary to determine which interfaces are needed on the new switch to provide connectivity to the router, the Linksys device, and the customer PCs. The customer wants to use copper cabling.

Note: Links created with the switch may take a minute to change from amber to green. Switch between Simulation mode and Realtime mode to speed up this process.

Step 1: Determine the required connectivity options.

a. Click Router0. Using the information in the Physical Device View window on the Physical tab, determine what type of interface is available on the router to connect to the new switch.

Hint: Place the mouse pointer on the interface to display the interface type. Click on the interface type to display a description of the interface.

Which interface is available on the router to connect to the new switch? What type of cable is required?

_____

Click the Linksys 300N. Using the picture on the **Physical** tab, determine what type of cable is necessary to connect to the new switch.

Which interface is available on the Linksys 300N to connect to the new switch? What type of cable is required?

_____

Step 2: Configure the new switch with the required options.

a. Click Switch0.

On the **Physical** tab, explore each switch module available under the **Modules** option.

Choose the appropriate interfaces to connect to Router0 and the Linksys 300N router.

Choose the appropriate interfaces to connect to the existing PCs.

Power down the switch using the power button in the **Physical Device View** window on the **Physical** tab.

Choose the appropriate modules for the switch. Add the four necessary interfaces to the switch.

Power up the switch using the power button shown in the **Physical Device View** window on the **Physical** tab.

Click the **Config** tab. Select each interface and ensure that the **On** box is checked.

Step 3: Connect the router to the switch.

a. Using the appropriate cable, connect the router port to the first available switch port. Click the **Config** tab on the router. Select the interface and ensure that the **On** box is checked.

b. Verify connectivity. A green light appears on each end of the link if the cabling is correct.

Step 4: Connect the Linksys 300N to the switch.

a. Using the appropriate cable, connect the Linksys 300N to the second available port on the new switch.

Verify connectivity. A green light appears on each end of the link if the cabling is correct.

Step 5: Connect the PCs to the switch.

a. Using the appropriate cable, connect the existing PCs to the new switch.

b. Verify connectivity. A green light appears on each end of the links if the cabling is correct.

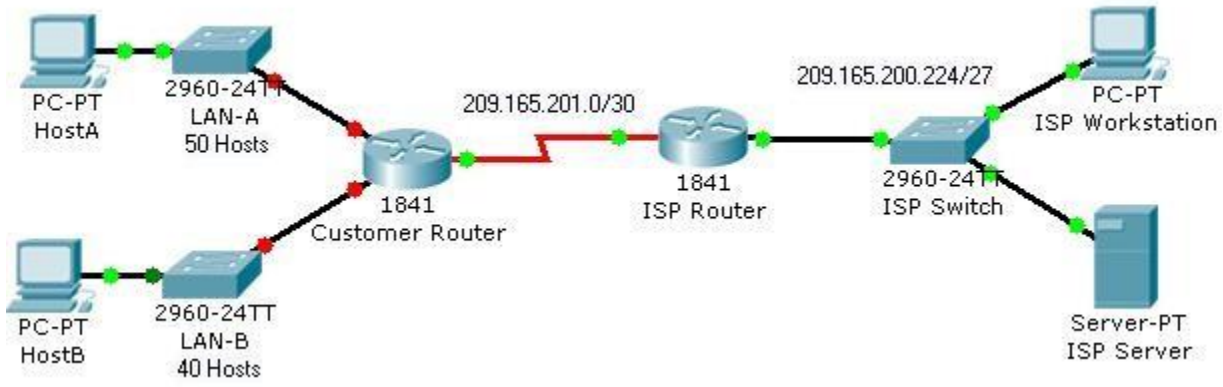
c. Click the Check Results button at the bottom of this instruction window to check your work.

CONCLUSION:

Experirment-16

AIM OF EXPT:- Implementing an IP Addressing Scheme

Topology Diagram



Objectives

- Subnet an address space based on the host requirements.
- Assign host addresses to devices.
- Configure devices with IP addressing.
- Verify the addressing configuration.

Background / Preparation

In this activity, you will subnet the private address space 192.168.1.0/24 to provide enough host addresses for the two LANs attached to the router. You will then assign valid host addresses to the appropriate devices and interfaces. Finally, you will test connectivity to verify your IP address implementation.

Step 1: Subnet an address space based on the host requirements.

a. You are given the private address space 192.168.1.0/24. Subnet this address space based on the following requirements:

- LAN-A needs enough addresses for 50 hosts.
- LAN-B needs enough addresses for 40 hosts.

How many bits must be left for host addresses? _____

How many bits can now be taken from the host portion to make a subnet? _____

How many hosts does each subnet support? _____

How many subnets are created? _____

What is the new subnet mask? _____

Step 2: Assign host addresses to devices.

What is the subnet address for subnet 0? _____

What is the subnet address for subnet 1? _____

Assign subnet 0 to LAN-A, and assign subnet 1 to LAN-B.

What is the first address in subnet 0? _____
This address is assigned the FastEthernet0/0 interface on Customer Router.

What is the first address in subnet 1? _____
This address is assigned the FastEthernet0/1 interface on Customer Router.

What is the last address in subnet 0? _____
This address is assigned to HostA.

What is the last address in subnet 1? _____
This address is assigned to HostB.

What is the default gateway for HostA? _____

What is the default gateway for HostB? _____

Step 3: Configure devices with IP addressing.

Configure HostA and HostB with IP addressing, including the subnet mask and default gateway.

a. Click HostA. On the **Desktop** tab, choose **IP Configuration**. Enter the correct addressing for HostA according to your answers in Step 1 and Step 2.

b. Click HostB. On the **Desktop** tab, choose **IP Configuration**. Enter the correct addressing for HostB according to your answers in Step 1 and Step 2.

c. Check results. On the **Assessment Items** tab, your configurations for HostA and HostB should have green checkmarks. If not, read the provided feedback for a hint on how to correct the problem.

Note: If you cannot see all the feedback, place your mouse pointer over the right side of the **Activity Results** window. When the cursor turns into a double-headed arrow, click and drag to resize the window until you can see all the feedback text.)

Configure the LAN interfaces on Customer Router with IP addresses and a subnet mask.

a. Click Customer Router. Click the Config tab.

b. On the left side under Interface, click FastEthernet0/0. Enter the IP address and subnet mask, and then set the Port Status to On.

c. On the left side under Interface, click FastEthernet0/1. Enter the IP address and subnet mask, and then set the Port Status to On.

d. Notice in the Equivalent IOS Commands window that your actions produced actual commands. You can scroll through the command window. In the next chapter, you will learn how to enter these commands directly into the router instead of using the Config tab.

For a better view of the commands, you can increase the size of the window. To resize the window, place your mouse pointer over the bottom border of the window. When the cursor turns into a double-headed arrow, click and drag.

Check results. On the Assessment Items tab, your configurations for Customer Router should have green checkmarks. If not, read the provided feedback for a hint on how to correct the problem.

Step 4: Verify the addressing configuration.

a. Test connectivity between HostA, HostB, ISP Workstation, and ISP Server. You can use the Add Simple PDU tool to create pings between the devices. You can also click HostA or HostB, then the Desktop tab, and then Command Prompt. Use the ping command to test connectivity to other devices. To obtain the IP address of another device, place your mouse pointer over the device.

b. Check results. On the Connectivity Tests tab, the status of each test should be successful.

Reflection

a. How many subnets are still available for future expansion?

b. What would be the two subnet addresses if the host requirement was 80 hosts per LAN?

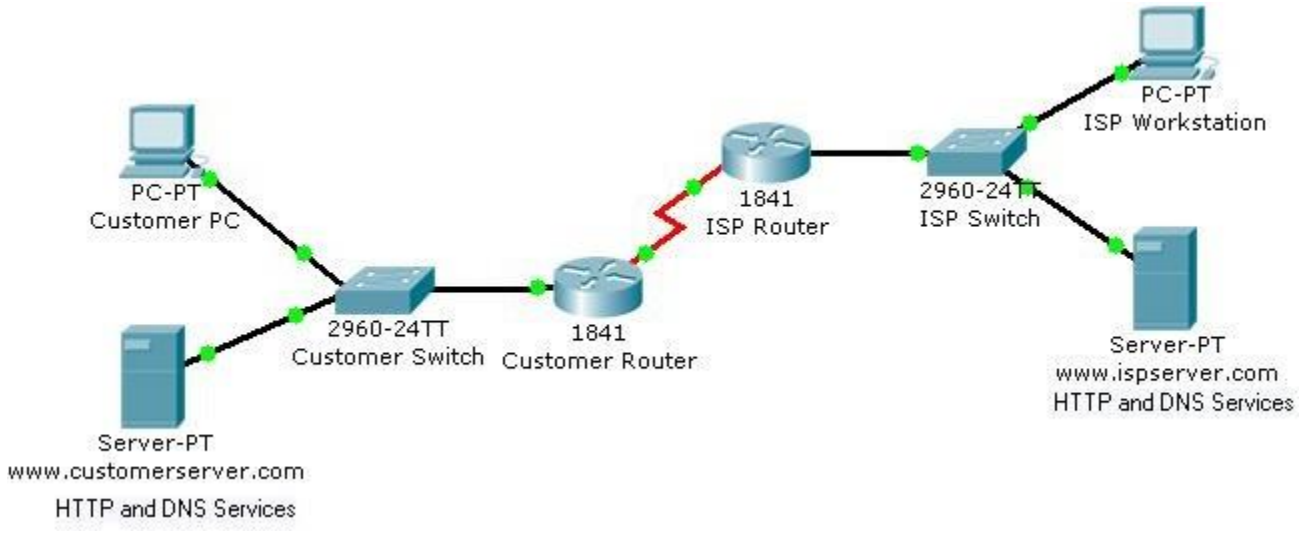
c. Challenge: Create your own Packet Tracer network using the same topology, but implement an addressing scheme based on 80 hosts per LAN. Have another student or your instructor check your work.

CONCLUSION:-

Experirment-17

Examining Network Address Translation (NAT)

Topology Diagram



Objectives

- Examine NAT processes as traffic traverses a NAT border router.

Background / Preparation

In this activity, you will use Packet Tracer Simulation mode to examine the contents of the IP header as traffic crosses the NAT border router.

Step 1: Prepare the network for Simulation mode.

Verify that the network is ready to send and receive traffic. All the link lights should be green. If some link lights are still amber, you can switch between Simulation and Realtime mode several times to force the lights to turn green faster. Switch to Simulation mode before going to the next step.

Step 2: Send an HTTP request from an inside host to an outside web server.

Click Customer PC. Click the Desktop tab and then Web Browser. In the URL field, type the web address for the ISP server (www.ispserver.com). Make sure that you are in Simulation mode, and then click Go.

In the event list, notice that Customer PC queues a DNS request and sends out an ARP request. You can view the contents of the ARP request by either clicking on the packet in the topology or clicking on the packet color under Info in the Event List window.

In the PDU Information at Device: Customer PC window, which IP address is Customer PC attempting to find a MAC address for? _____

In the Event List window, click Capture/Forward twice. Which device answers the ARP request from Customer PC? Which MAC address is placed inside the ARP reply?

_____

In the Event List window, click Capture/Forward twice. Customer PC accepts the ARP replay and then builds another packet. What is the protocol for this new packet? If you click Outbound PDU Details for this packet, you can see the details of the protocol. _____

In the Event List window, click Capture/Forward twice. Click the packet at the www.customerserver.com server. Then click the Outbound PDU Details tab. Scroll down to the bottom to see the Application Layer data. What is the IP address for the ISP server?

_____

In the Event List window, click Capture/Forward twice. Customer PC now formulates another ARP request. Why?

_____

In the Event List window, click Capture/Forward 10 times until Customer PC formulates an HTTP request packet. Customer PC finally has enough information to request a web page from the ISP server.

In the Event List window, click Capture/Forward three times. Click the packet at Customer Router to examine the contents. Customer Router is a NAT border router. What is the inside local address and the inside global address for Customer PC?

_____

In the Event List window, click Capture/Forward seven times until the HTTP reply reaches Customer Router. Examine the contents of the HTTP reply and notice that the inside local and global addresses have changed again as the packet is forwarded on to Customer PC.

Step 3: Send an HTTP request from an outside host to an inside web server.

Customer Server provides web services to the public (outside addresses) through the domain name www.customerserver.com. Follow a process similar to Step 2 to observe an HTTP request on ISP Workstation.

a. Click ISP Workstation. Click the **Desktop** tab, and then **Web Browser**. In the **URL** field, type the Customer Server web address (www.customerserver.com). Make sure that you are in Simulation mode, and then click **Go**.

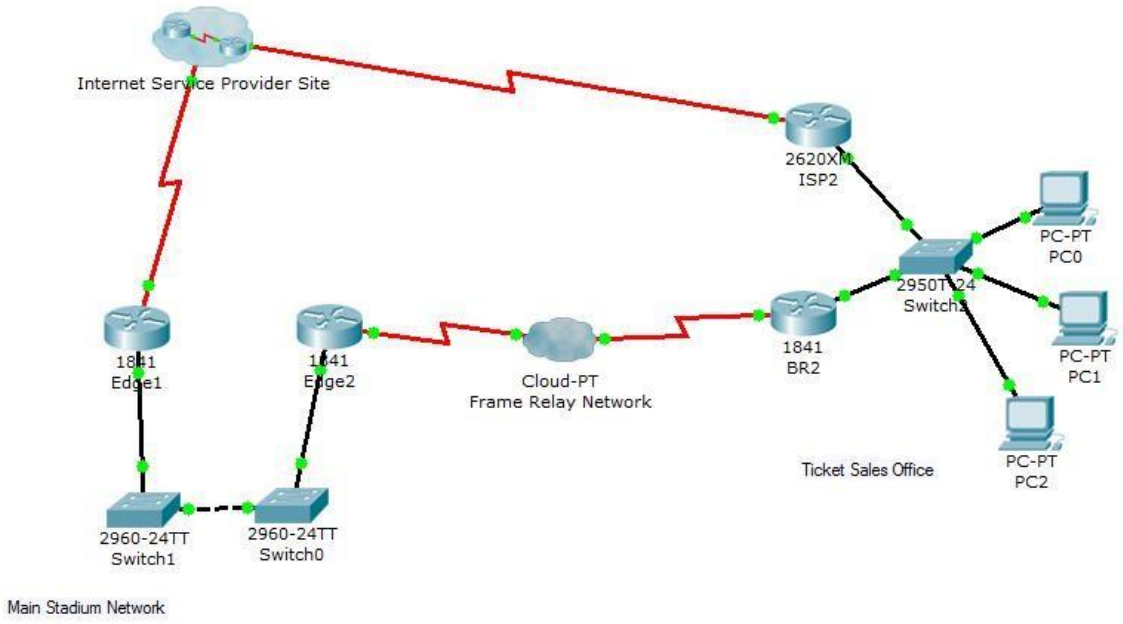
b. You can either click **Auto Capture/Play** or **Capture/Forward** to step through each stage of the process. The same ARP and DNS processes occur before the ISP Workstation can formulate an HTTP request.

c. When the HTTP request arrives at Customer Router, check the packet contents. What is the inside local address? What is the inside global address?

_____

Experirment-18

AIM:-Observing Static and Dynamic Routing



Objective

Observe the network behavior using static and default routing only and compare it to the behavior of dynamic routing.

Background / Preparation

In this exercise, you will observe what the adaptability of dynamic routing compared to static and default routing. The Ticket Sales Office network is currently configured using static and default routing.

Required file: Observing Static and Dynamic Routing.pka

Step 1: Test Connectivity Using Static and Default Routing.

Open a Command Prompt on PC0.

Trace (tracert) a connection to the Edge1 FastEthernet 0/0 address. This should be successful.

Step 2: Bring down Frame Relay Network and Observe Routing.

On the BR2 router, shutdown the link to the Frame Relay network.

Perform a trace from PC0 again to the Edge1 FastEthernet 0/0 address. What happens this time?

_____

_____

Step 3: Configure Dynamic Routing and Observe Routing

a. Configure EIGRP (AS 10) on the BR2 and ISP2 routers. Be sure to include all directly connected networks and turn off auto-summary.
b. Do a third trace from PC0 to the Edge1 FastEthernet 0/0 interface. (It should be successful again.)
c. Did the path change? If so, how?

_____

Reflection

What are the advantages of using dynamic routing? Static and default routing?

_____

_____

The static routes in this lab were set with an administrative distance of 130. What would have happened if they were set at 30? At 230?

_____

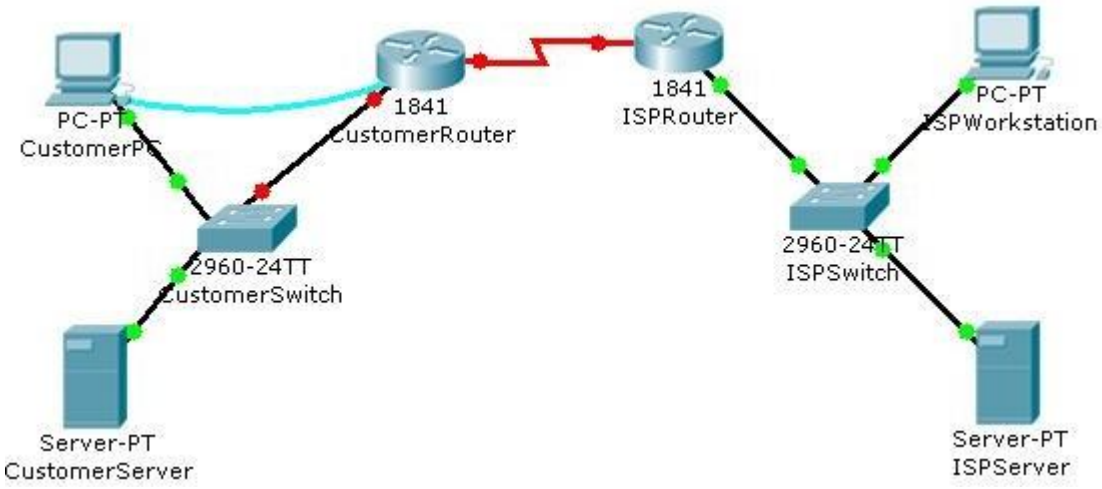
CONCLUSION:-

Experiment-19

AIM OF EXPT:- Configuring Ethernet and Serial Interfaces

Topology Diagram

Apparatus (Software) : Command Prompt And Packet Tracer.



Objectives

- Configure a LAN Ethernet interface.
- Configure a WAN serial interface.
- Verify the interface configurations.

Background / Preparation

In this activity, you will configure the LAN Ethernet interface and the WAN serial interface on the Customer Cisco 1841 router.

Step 1: Configure the LAN Ethernet interface.

a. Use the terminal emulation software on the Customer PC to connect to the Cisco 1841 Customer Router. Enter **cisco** for the console password.

b. Enter privileged EXEC mode using **cisco123** for the privileged EXEC password. The CustomerRouter# prompt indicates that you are in privileged EXEC mode.

c. Enter global configuration mode. The CustomerRouter(config)# prompt indicates that you are in global configuration mode.

d. Identify which LAN interface to configure with an IP address. To configure the Fast Ethernet interface, use this command.

CustomerRouter(config)#**interface FastEthernet 0/0**

Add a description to the interface.

CustomerRouter(config-if)#**description Connected to CustomerSwitch**

Specify the IP address and subnet mask for the interface.

```
CustomerRouter(config-if)#ip address 192.168.1.1 255.255.255.0
```

Ensure that the interface is enabled.

```
CustomerRouter(config-if)#no shutdown
```

Exit interface configuration mode.

```
CustomerRouter(config-if)#end
```

Step 2: Verify the LAN interface configuration.

Use the **show ip route** command to verify your configuration. This is a partial example of the output.

```
CustomerRouter#show ip route

<output omitted>

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Step 3: Configure the WAN serial interface.

Refer to the diagram in the Packet Tracer workspace area and the commands used in Step 1 to configure the WAN serial interface on Customer Router.

Tip: Remember the Cisco IOS CLI Help commands to configure the interface.

a. Enter global configuration mode.
b. Identify the serial interface to configure.
c. Describe the interface. (Connected to ISP)
d. Specify the interface IP address and subnet mask. (209.165.200.225 255.255.255.224)
e. Ensure that the interface is enabled.
f. End interface configuration mode.

Step 4: Verify the interface configurations.

Use the **show run** command to verify your configuration. This is a partial example of the output.

```
CustomerRouter#show run
...
!
interface FastEthernet0/0
 description Connected to CustomerSwitch
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
```

```
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 description Connected to ISP
 ip address 209.165.200.225 255.255.255.224
!
```

Use the **ping** command to verify connectivity to the WAN interface on the ISP router. This is a partial example of the output.

```
CustomerRouter#ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 35/37/47 ms
```

Use the **ping** command to verify connectivity to the customer switch. This is a partial example of the output.

```
CustomerRouter#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/12 ms
```

Step 5: Save the configuration.

a. In privileged EXEC mode, save the running configuration to the startup configuration.

```
CustomerRouter#copy run start
```

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

Reflection

a. When you ping the LAN IP address of the ISP router, what happens and why?

b. Which of the following Cisco ISO CLI modes do you need to be in to configure the description of an interface?

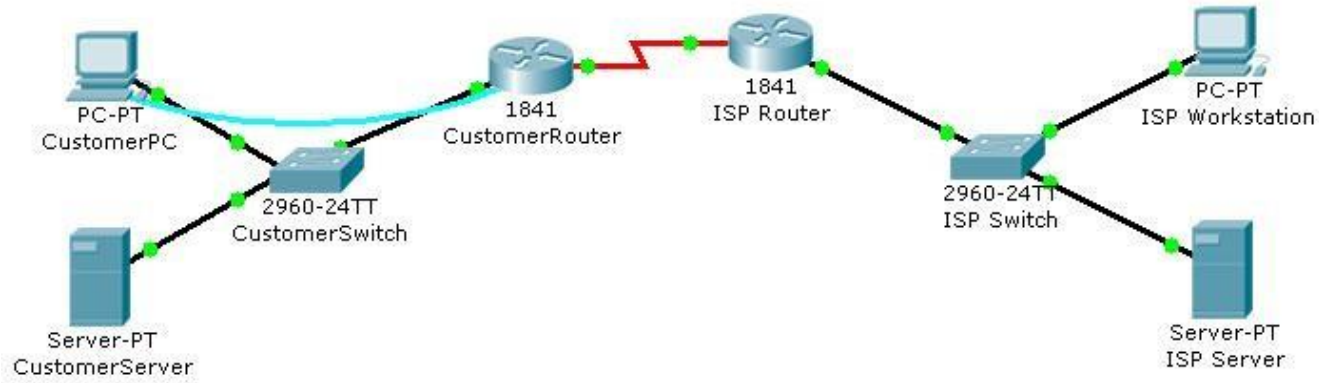
- **CustomerRouter#**
- **CustomerRouter>**
- **CustomerRouter(config)#**
- **CustomerRouter(config-if)#**

c. You configured the Fast Ethernet 0/0 interface with the **no shutdown** command and verified the configuration. However, when you rebooted the router, the interface was shutdown. You reconfigured the Fast Ethernet 0/0 interface and verified that the configuration works. Explain what most likely happened.

Experiment-20

AIM OF EXPT:- Configuring a Default Route

Topology Diagram



Objectives

- Configure a default route on a router.

Background / Preparation

In this activity, you will configure a default route on the Cisco 1841 Customer router. The default route configuration uses the WAN IP address on the Cisco 1841 ISP router. This is the next-hop router from the Cisco 1841 Customer router.

Step 1: Verify reachability from CustomerRouter to the LAN IP address on the ISP router.

a. Use terminal emulation software on the Customer PC to connect to the customer Cisco 1841 router. Use **cisco123** for the console password.

b. Use the **ping** command to verify if the LAN IP address 209.165.201.1 on the ISP router is reachable from the CustomerRouter

CustomerRouter>**ping 209.165.201.1**

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Step 2: Configure the default route.

a. Enter privileged EXEC mode using the password **cisco**. The CustomerRouter# prompt indicates that you are in privileged EXEC mode.

b. Enter global configuration mode. The CustomerRouter(config)# prompt indicates that you are in global configuration mode.

c. Configure a default route using the ISP WAN IP address as the next hop IP address.

```
CustomerRouter(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
CustomerRouter(config)#end
```

Step 3: Verify the default route configuration.

a. Use the **show ip route** command to verify the configuration of the default route. This is a partial example of the output.

```
CustomerRouter#show ip route
Codes: C - connected, S - static,...

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, FastEthernet0/0
     209.165.200.0/27 is subnetted, 1 subnets
C    209.165.200.224 is directly connected, Serial0/1/0
S*  0.0.0.0/0 [1/0] via 209.165.200.226
```

b. Use the **ping** command to verify connectivity to the LAN IP address on the ISP router

```
CustomerRouter#ping 209.165.201.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/25/34 ms
```

Step 4: Save the configuration.

a. From privileged EXEC mode, save the running configuration to the startup configuration.

   i. CustomerRouter#**copy run start**

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

Reflection

You can now access the entire ISP network. Write down some issues and considerations to discuss with your classmates about this configuration. Here are two questions to begin with:

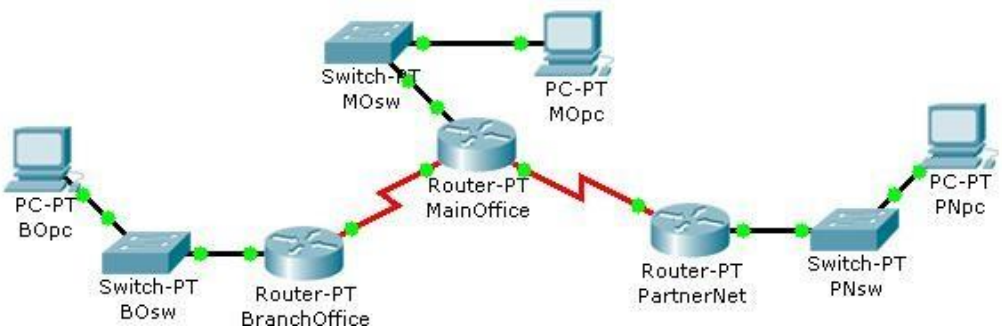
- Is this type of access to the ISP LAN likely to happen in the real world?
- Why has the student activity been configured to allow this type of access?

CONCLUSION:-

Experirment-21

AIM OF EXPT:- Configuring Static and Default Routes

Topology Diagram



Objectives

- Configure static routes on each router to allow communication between all clients.
- Test connectivity to ensure that each device can fully communicate with all other devices.

Background / Preparation

This topology represents a small WAN. Each device in this network has been configured with IP addresses; however, no routing has been configured. The company management wants to use static routes to connect the multiple networks.

Step 1: Test connectivity between the PCs and the default gateway.

To determine if there is connectivity from each PC to its configured gateway, first use a simple ping test.

a. Click BOpc and go to **Desktop > Command Prompt**.

b. From the command prompt, type the **ipconfig** command. Note the IP address for BOpc and the default gateway address. The default gateway address is the IP address for the Fast Ethernet interface on BranchOffice.

c. Ping 192.168.1.1, the default gateway address for the BranchOffice LAN, from the command prompt on BOpc. This ping should be successful.

d. Click PNpc and go to **Desktop > Command Prompt**.

e. From the command prompt, type the **ipconfig** command. Note the IP address for PNpc and the default gateway address. The default gateway address is the IP address for the Fast Ethernet interface on PartnerNet.

f. Ping 192.168.3.1, the default gateway address for the PartnerNet LAN, from the command prompt on PNpc. This ping should be successful.

g. Repeat steps a, b, and c for MOpc and its respective default gateway, the Fast Ethernet interface on MainOffice. Each of these ping tests should be successful.

Step 2: Ping between routers to test connectivity.

Use a console cable and terminal emulation software on BOpc to connect to Branch Office.

a. Test connectivity with MainOffice by pinging 10.10.10.1, the IP address of the directly connected serial 3/0 interface. This ping should succeed.

b. Test connectivity with MainOffice by pinging 10.10.10.5, the IP address of the serial 2/0 interface. This ping should fail.

c. Issue the **show ip route** command from the terminal window of BOpc. Note that only directly connected routes are shown in the BranchOffice routing table. The ping to 10.10.10.5 failed because the BranchOffice router has no routing table entry for 10.10.10.5.

d. Repeat steps a through d on the other two PCs. The pings to directly connected networks will succeed. However, pings to remote networks will fail.

e. What steps must be taken to reach all the networks from any PC in the activity?

Step 3: Viewing the routing tables.

You can view routing tables in Packet Tracer using the Inspect tool. The Inspect tool is in the Common Tools bar to the right of the topology. The Inspect tool is the icon that appears as a magnifying glass.

a. In the **Common Tools** bar, click on the **Inspect** tool.

b. Click the MainOffice router and choose **Routing Table.**

c. Click the BranchOffice router and choose **Routing Table.**

d. Click the PartnerNet router and choose **Routing Table.**

e. Move the routing table windows around so that you can see all three at once.

f. What networks do each of the routers already know about?

g. Does each router know how to route to all networks in the topology? After comparing the routing tables, close the window for each routing table by clicking the **x** in the upper right corner of each window.

Step 4: Configure default routes on the BranchOffice and PartnerNet routers.

To configure static routes for each router, first determine which routes need to be added for each device. For the BranchOffice and the PartnerNet routers, a single default route allows these devices to route traffic for all networks not directly connected. To configure a default route, you must identify the IP address of the next hop router, which in this case is the MainOffice router.

a. From the **Common** toolbar, click the **Select** tool.

b. Move the cursor over the red serial link between the BranchOffice router and the MainOffice router. Notice that the interface of the next hop is S3/0.

c. Move the cursor over the MainOffice router and note that the IP address for Serial 3/0 is 10.10.10.1.

d. Move the cursor over the red serial link between the PartnerNet router and the MainOffice router. Notice that the interface of the next hop is S2/0.

e. Move the cursor over the MainOffice router and note that the IP address for Serial 2/0 is 10.10.10.5.

f. Configure the static routes on both the BranchOffice and PartnerNet routers using the CLI. Click the BranchOffice router, and click the **CLI** tab.

g. At the **BranchOffice>** prompt, type **enable** to enter privileged EXEC mode.

h. At the **BranchOffice#** prompt, type **configure terminal**.

i. The syntax for a default route is **ip route 0.0.0.0 0.0.0.0** ***next_hop_ip_address***. Type **ip route 0.0.0.0 0.0.0.0 10.10.10.1**.

j. Type **end** to get back to the **BranchOffice#** prompt.

k. Type **copy run start** to save the configuration change.

l. Repeat steps f through k on the PartnerNet router, using 10.10.10.5 as the next hop IP address.

Step 5: Configure static routes at Main Office.

The configuration of static routes at the Main Office is a bit more complex because the MainOffice router is responsible for routing traffic to and from the Branch Office and PartnerNet LAN segments.

The MainOffice router knows only about routes to the 10.10.10.0/30, 10.10.10.4/30, and 192.168.2.0/24 networks because they are directly connected. Static routes to the 192.168.1.0/24 and 192.168.3.0/24 networks need to be added so that the MainOffice router can route traffic between the networks behind the BranchOffice and PartnerNet routers.

a. Click the MainOffice router, and then click the **CLI** tab.

b. At the MainOffice> prompt, type **enable** to enter privileged EXEC mode.

c. At the MainOffice# prompt, type **configure terminal**.

d. The syntax for a static route is **ip route** ***network subnet_mask next_hop_ip_address***:

```
ip route 192.168.1.0 255.255.255.0 10.10.10.2
ip route 192.168.3.0 255.255.255.0 10.10.10.6
```

e. Type **end** to return to the MainOffice# prompt.

f. Type **copy run start** to save the configuration change.

g. Repeat steps a through e from Step 3. View the routing tables and notice the difference in the routing tables. The routing table for each router should have an “S” for each static route.

Step 6: Test connectivity.

Now that each router in the topology has static routes configured, all hosts should have connectivity to all other hosts. Use ping to verify connectivity.

a. Click **BOpc** and click the **Desktop** tab.

b. Choose the **Command prompt** option.

c. Type **ping 192.168.3.2.** The ping should be successful, verifying that the static routes are configured properly.

d. Type **ping 192.168.2.2.** Notice that the result is successful even though you did not specifically add the 192.168.2.0 network as a static route into any of the routers. Because a default route was used on the BranchOffice and PartnerNet routers, a route for the 192.168.2.0 network was not needed. The default route sends all traffic destined off network to the MainOffice router. The 192.168.2.0 network is directly connected to the MainOffice router; therefore, no additional routes needed to be added to the routing table

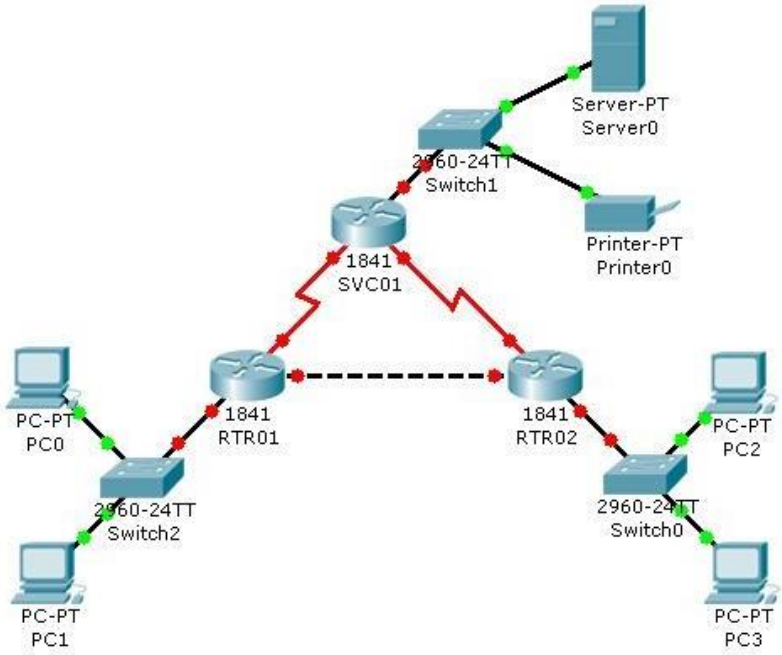
e. Click the **Check Results** button at the bottom of this instruction window to check your work.

CONCLUSION:-

Experiment-22

AIM OF EXPERIMENT:- Configuring RIP

Topology Diagram



Objectives

- Configure routers using basic interface configuration commands.
- Enable RIP.
- Verify the RIP configuration.

Background / Preparation

A simple routed network has been set up to assist in reviewing RIP routing behavior. In this activity, you will configure RIP across the network and set up end devices to communicate on the network.

Step 1: Configure the SVC01 router and enable RIP.

a. From the CLI, configure interface Fast Ethernet 0/0 using the IP address 10.0.0.254 /8.

b. Configure interface serial 0/0/0 using the first usable IP address in network 192.168.1.0 /24 to connect to the RTR01 router. Set the clock rate at 64000.

c. Configure interface serial 0/0/1 using the first usable IP address in network 192.168.2.0 /24 with a clock rate of 64000.

d. Using the **no shutdown** command, enable the configured interfaces.

e. Configure RIP to advertise the networks for the configured interfaces.

f. Configure the end devices.

i. Server0 uses the first usable IP address in network 10.0.0.0 /8. Specifythe appropriate default gateway and subnet mask.

ii. Printer0 uses the second usable IP address in network 10.0.0.0 /8. Specify the appropriate default gateway and subnet mask.

Step 2: Configure the RTR01 router and enable RIP.

a. Configure interface Fast Ethernet 0/0 using the first usable IP address in network 192.168.0.0/24 to connect to the RTR02 router.

b. Configure interface serial 0/0/0 using the second usable IP address in network 192.168.1.0 /24 to connect to the SVC01 router.

c. Configure interface Fast Ethernet 0/1 using the IP address 172.16.254.254 /16.

d. Using the **no shutdown** command, enable the configured interfaces.

e. Configure RIP to advertise the networks for the configured interfaces.

f. Configure the end devices.

i. PC0 uses the first usable IP addresses in network 172.16.0.0 /16.

ii. PC1 uses the second usable IP address in network 172.16.0.0 /16.

iii. Specify the appropriate default gateway and subnet mask on each PC.

Step 3: Configure the RTR02 router and enable RIP.

a. Configure interface Fast Ethernet 0/0 using the second usable IP address in network 192.168.0.0 /24 to connect to the RTR01 router.

b. Configure interface serial 0/0/0 using the second usable IP address in network 192.168.2.0 /24 to connect to the SVC01 router.

c. Configure interface Fast Ethernet 0/1 using the IP address 172.17.254.254 /16.

d. Using the **no shutdown** command, enable the configured interfaces.

e. Configure RIP to advertise the networks for the configured interfaces.

f. Configure the end devices.

i. PC2 uses the first usable IP addresses in network 172.17.0.0 /16.

ii. PC3 uses the second usable IP address in network 172.17.0.0 /16.

iii. Specify the appropriate default gateway and subnet mask on each PC.

Step 4: Verify the RIP configuration on each router.

a. At the command prompt for each router, issue the commands **show ip protocols** and **show ip route** to verify RIP routing is fully converged. The **show ip protocols** command displays the networks the router is advertising and the addresses of other RIP routing neighbors. The **show ip route** command output displays all routes know to the local router including the RIP routes which are indicated by an "R".

b. Every device should now be able to successfully ping any other device in this activity.

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

two preconfigured firewalls. In the two scenarios presented, you will replace the existing routers with the firewalls. The firewalls need to be configured with the appropriate IP address configurations, and the firewalls should be tested to ensure that they are installed and configured correctly.

Scenario 1: Protecting the Network from Hackers

Because the company is concerned about security, you recommend a firewall to protect the network from hackers on the Internet. It is very important that access to the network from the Internet is restricted.

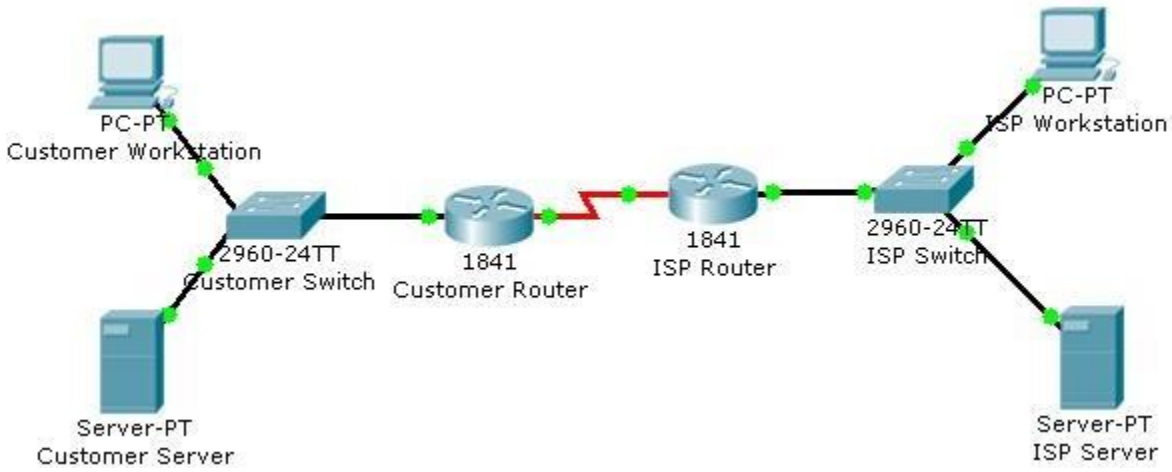
Firewall_1 has been preconfigured with the appropriate rules to provide the security required. You will install it on the network and confirm that it is functioning as expected.

:

EXPERIMENT NUMBER-23

AIM OF EXPT:-Configuring a Cisco Router as a DHCP Server
Apparatus (Software): Command Prompt And Packet Tracer.

Topology Diagram



Objectives

- Configure the customer Cisco 1841 ISR as a DHCP server.

Background / Preparation

In this activity, you will continue to configure the Cisco 1841 ISR router for the customer network by configuring the DHCP service. The customer has several workstations that need to be automatically configured with IP addresses on the local subnet and appropriate DHCP options to allow access to the Internet.

The DHCP pool will use the 192.168.1.0/24 network but the first 49 addresses are excluded. The default gateway and DNS server also need to be configured as 192.168.1.1 and 192.168.1.10.

For this activity, both the user and privileged EXEC passwords are **cisco**.

Note: Packet Tracer does not currently support the domain name and lease period options. These options are not used in this activity.

Step 1: Configure the DHCP service.

a. From the customer workstation, use a console cable and terminal emulation software to connect to the console of the customer Cisco1841 ISR.

b. Log in to the console of the Cisco 1841 ISR and enter global configuration mode.

c. Before creating a DHCP pool, configure the addresses that are excluded. The range is from 192.168.1.1 to 192.168.1.49.

CustomerRouter(config)#**ip dhcp excluded-address 192.168.1.1 192.168.1.49**

d. Create a DHCP pool called pool1.

CustomerRouter(config)#**ip dhcp pool pool1**

e. Define the network address range for the DHCP pool.

CustomerRouter(dhcp-config)#**network 192.168.1.0 255.255.255.0**

f. Define the DNS server as 192.168.1.10.

CustomerRouter(dhcp-config)#**dns-server 192.168.1.10**

g. Define the default gateway as 192.168.1.1.

CustomerRouter(dhcp-config)#**default-router 192.168.1.1**

h. Add an exclusion range of 192.168.1.1 to 192.168.1.49 to the DHCP pool.

CustomerRouter(dhcp-config)#**exit**
CustomerRouter(config)#**ip dhcp excluded-address 192.168.1.1 192.168.1.49**

i. Exit the terminal.

Step 2: Verify the DHCP configuration.

a. From the customer workstation, open the **Command Prompt** window.
b. Type **ipconfig /release** to release the current IP address.
c. Type **ipconfig /renew** to request a new IP address on the local network.
d. Verify that the IP address has been correctly assigned by pinging the LAN IP address of the Cisco 1841 ISR.
e. Click the **Check Results** button at the bottom of this instruction window to check your work.

Reflection

a. What is the purpose of DHCP on the customer network?

b. What IP address is assigned to the workstation after its IP address is renewed?

c. What other DHCP options can be defined on the Cisco 1841 ISR router that are not configured in this activity?

CONCLUSION:-