

Experiment-1

Aim: 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, Clipping 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 it 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	

Experiment - 2

Aim: 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.

Experiment - 3

Aim: Study of network IP

- Classification of IP address
- Sub netting
- Super netting

Apparatus (Software): NA

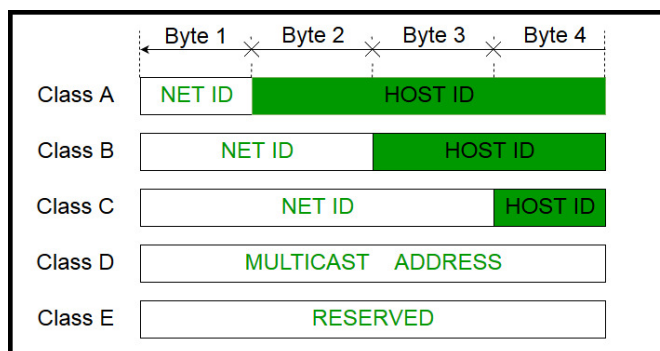
Procedure: Following is required to be study under this practical.

- Classification of IP address

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.

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.



- **Subnetting:** A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses.
- **Supernetting:** Supernetting is the process of aggregating routes to multiple smaller networks, thus saving storage space in the routing table and simplifying routing decisions and reducing routing advertisements to neighboring gateways.

Experiment-4

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-5

Aim: Study of basic network command and Network configuration 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.

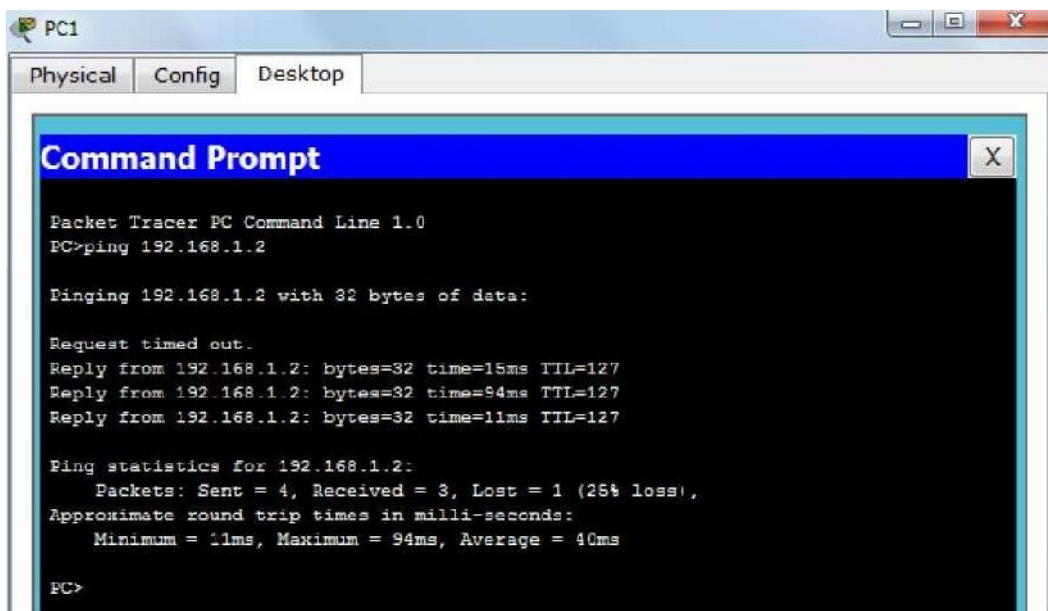
This commands includes

- 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:

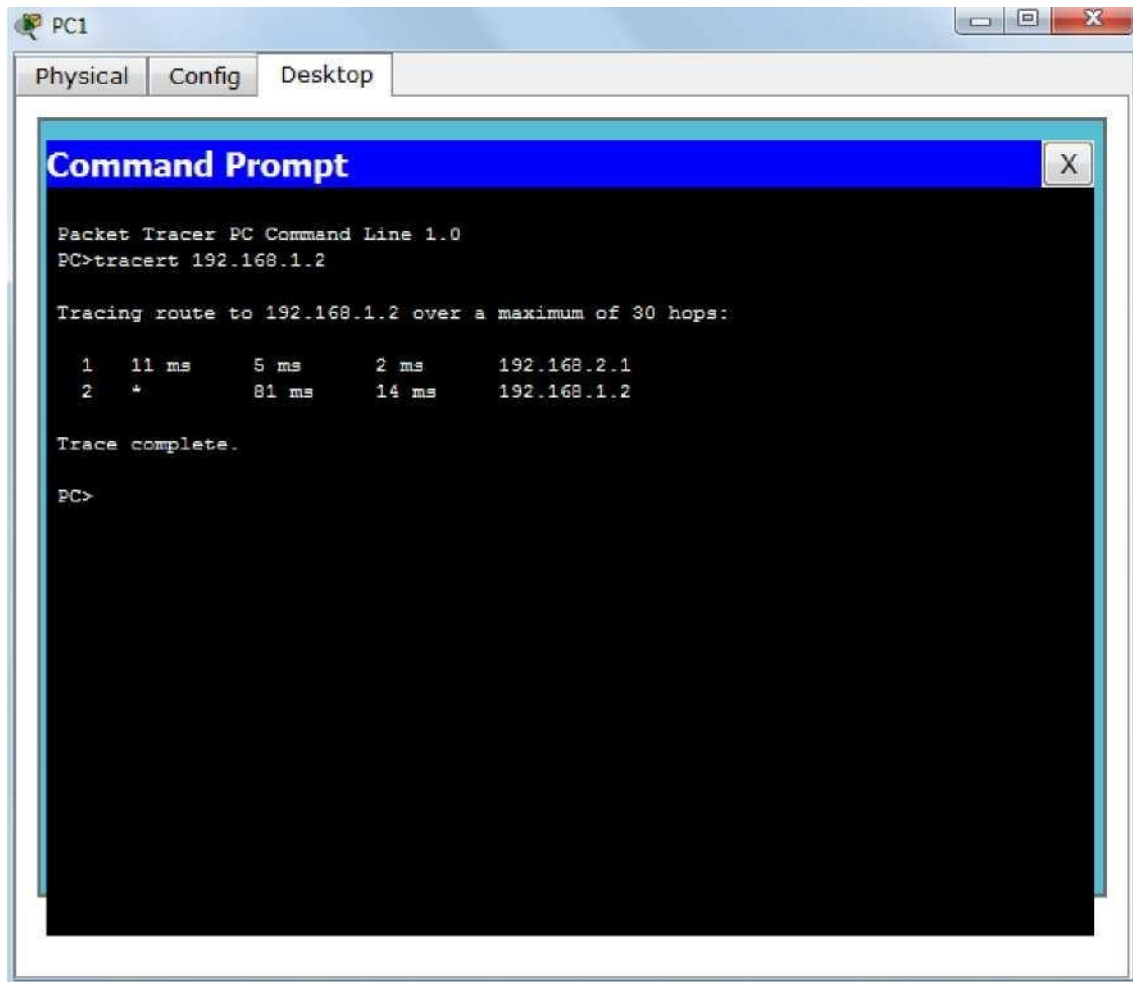
•

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.



The screenshot shows a Packet Tracer PC Command Line window for PC1. The window has tabs for Physical, Config, and Desktop. The Command Prompt is open, displaying the output of the 'tracert 192.168.1.2' command. The output shows a successful trace to 192.168.1.2 over 2 hops. The first hop is to 192.168.2.1 with a total time of 11 ms. The second hop is to 192.168.1.2 with a total time of 81 ms. The trace is complete.

```
Packet Tracer PC Command Line 1.0
PC>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  0  11 ms    5 ms     2 ms     192.168.2.1
  1  *        81 ms    14 ms    192.168.1.2

Trace complete.

PC>
```

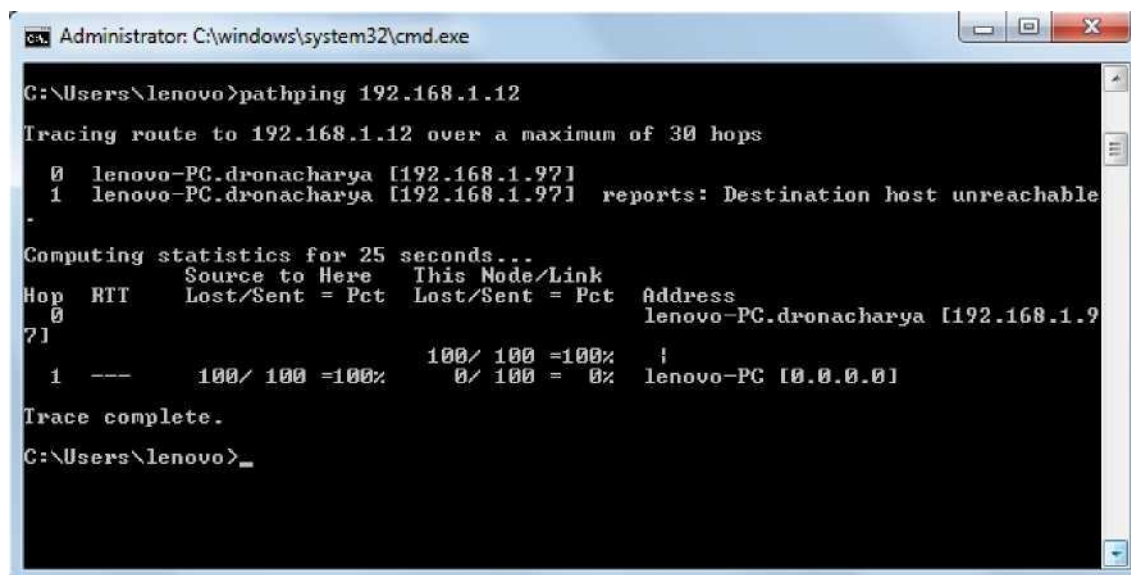
nslookup:

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 statistics about packet lost and latency.



```
Administrator: C:\windows\system32\cmd.exe

C:\Users\lenovo>pathping 192.168.1.12

Tracing route to 192.168.1.12 over a maximum of 30 hops

  0  lenovo-PC.dronacharya [192.168.1.97]
  1  lenovo-PC.dronacharya [192.168.1.97]  reports: Destination host unreachable
-

Computing statistics for 25 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
 0      Source to Here   This Node/Link   Address
 0      100/ 100 =100%    0/ 100 = 0%      lenovo-PC.dronacharya [192.168.1.97]
 1      ---      100/ 100 =100%    0/ 100 = 0%      lenovo-PC [0.0.0.0]

Trace complete.

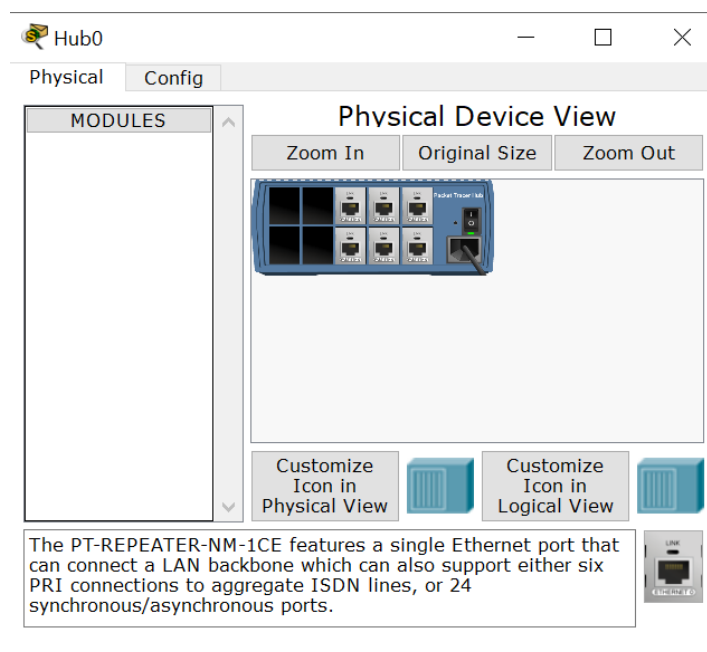
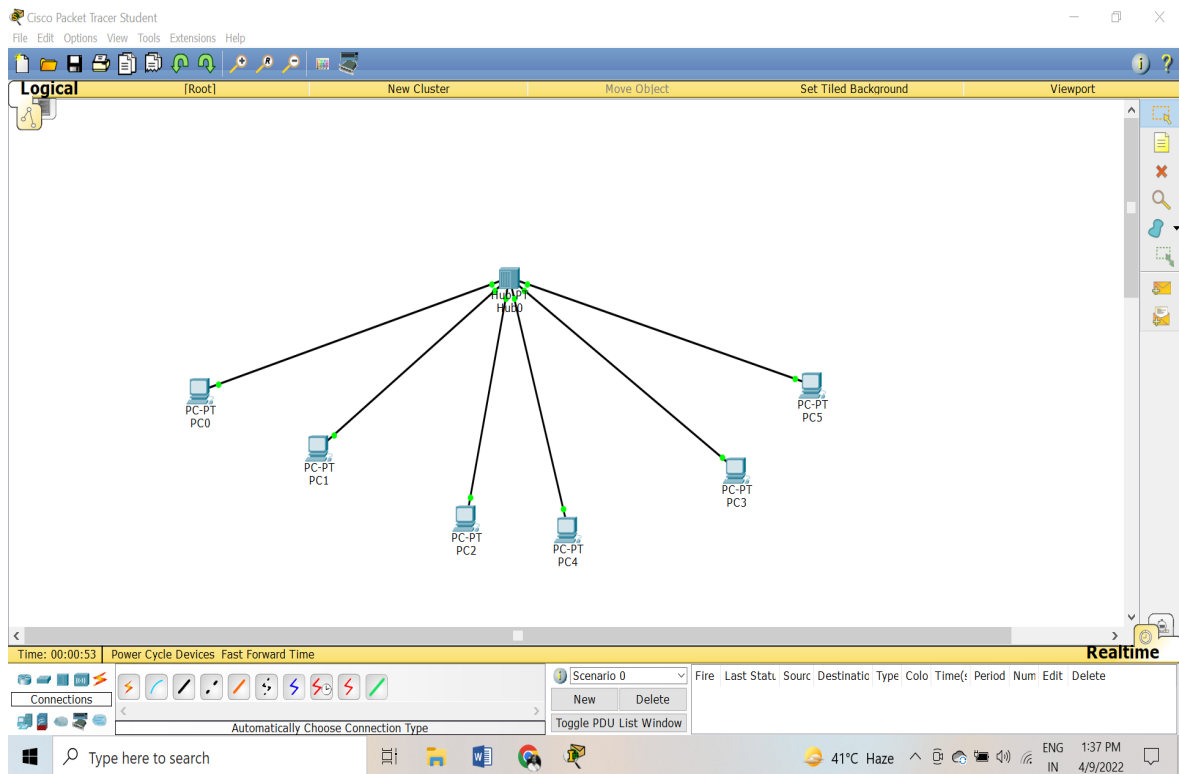
C:\Users\lenovo>
```

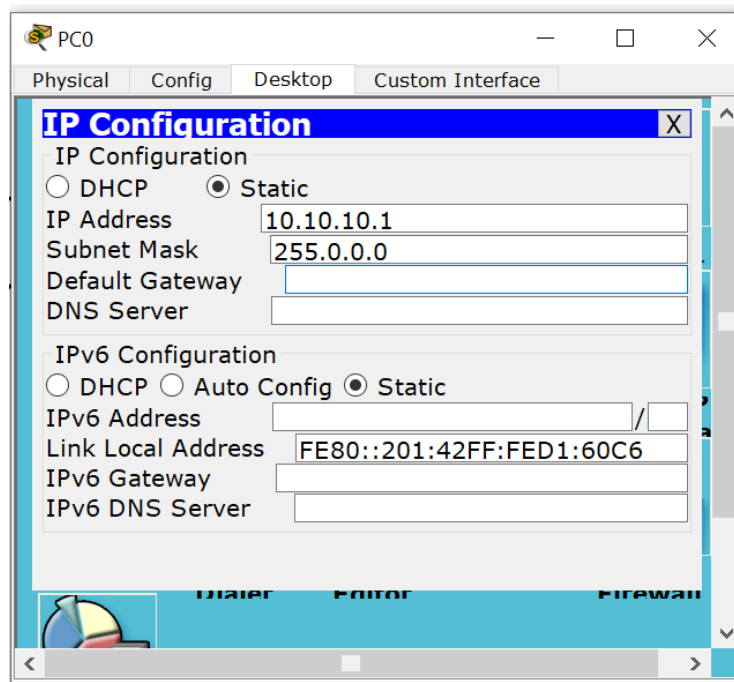
Ipconfig: (Internet Protocol CONFIGuration) A command line utility that is used to display and manage the IP address assigned to the machine. In Windows, typing ipconfig without any parameters displays the computer's currently assigned IP, subnet mask and default gateway addresses.

Experiment-6

Connecting Hub in Network

Topology Diagram





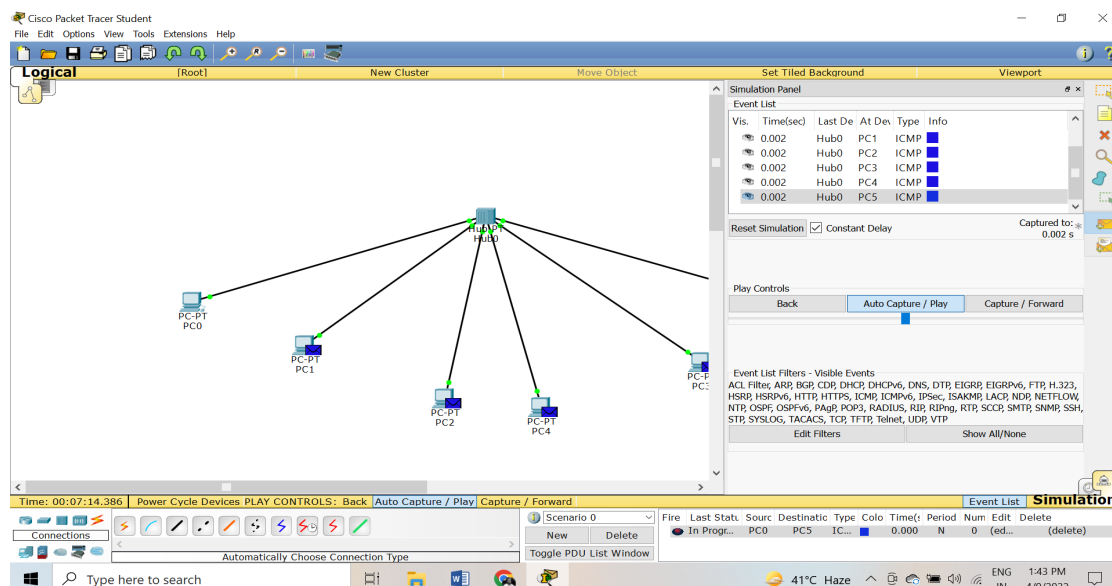
Objectives

- Perform an initial configuration of HUB

Background / Preparation

Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

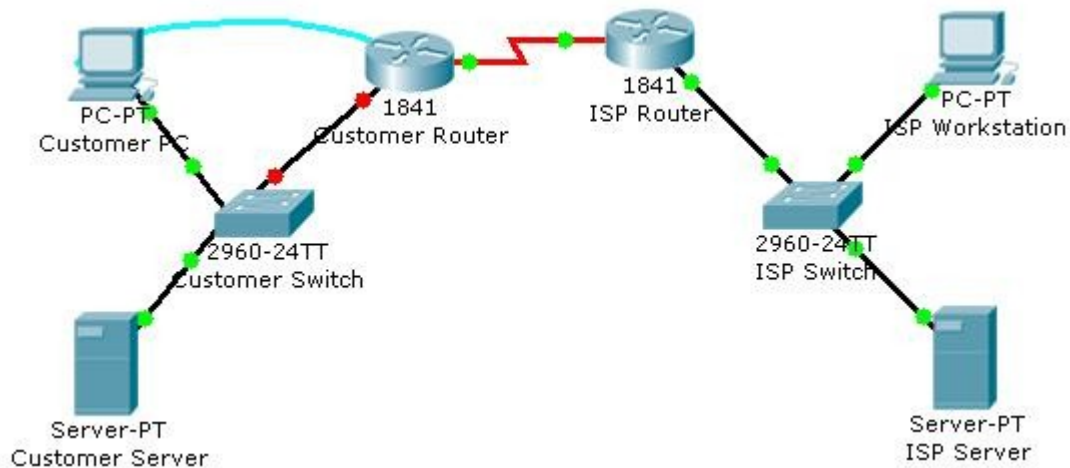
A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.



Experiment-07

Performing an Initial Router Configuration

Topology Diagram



Objectives

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

Background / Preparation

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

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 show the 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>enable
Translating "enable"...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
```

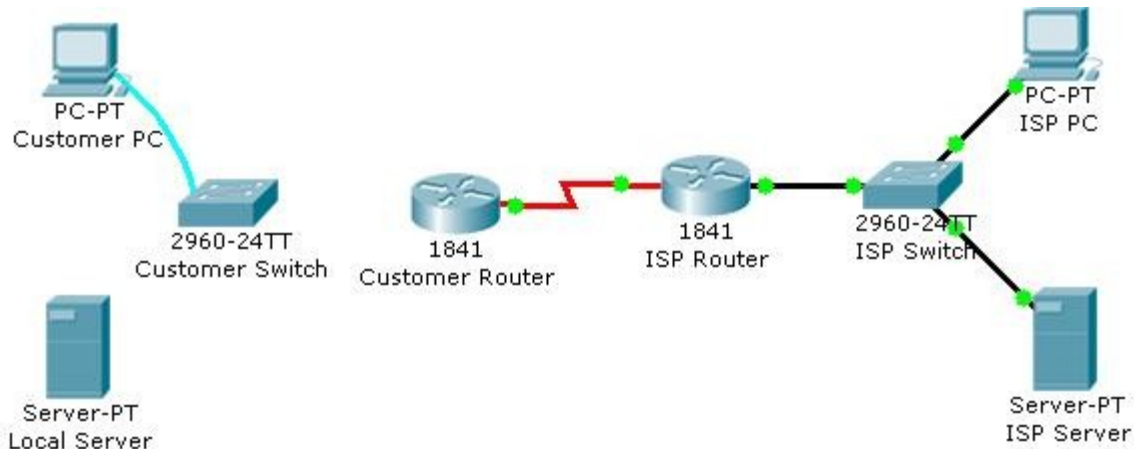
Step 6: Verify the configuration.

- 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.

Experiment-08

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

Topology



Background / Preparation

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s). It supports unicast, multicast as well as broadcast communications.

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.

- Using the proper cable, connect the FastEthernet0/0 on Customer Router to the FastEthernet0/1 on Customer Switch.
- Using the proper cable, connect the Customer PC to the Customer Switch on port FastEthernet0/2.
- Using the proper cable, connect the Local Server to the Customer Switch on port FastEthernet0/3.

Step 2: Verify the switch configuration.

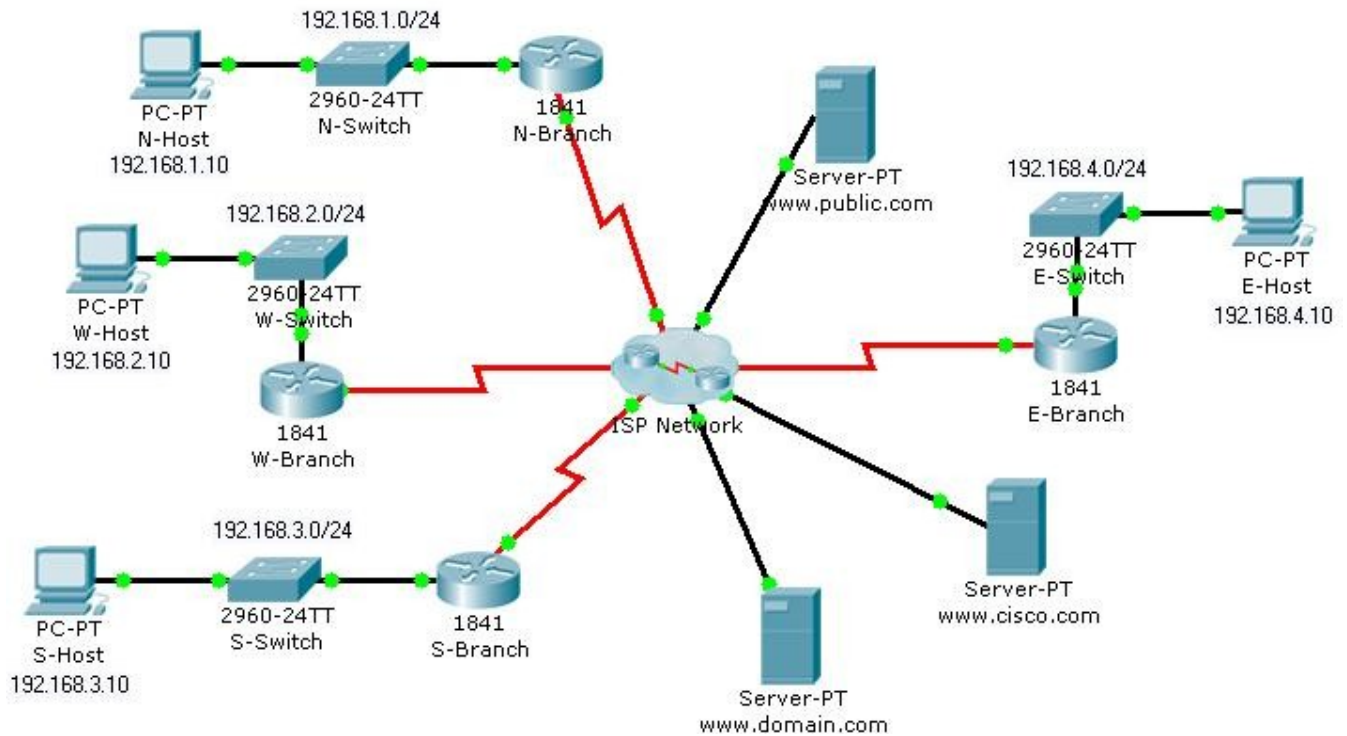
- From the Customer PC, use the terminal emulation software to connect to the console of the customer Cisco Catalyst 2960 switch.
- Use the console connection and terminal utility on the Customer PC to verify the configurations. Use **cisco** as the console password.
- Enter privileged EXEC mode and use the **show running-config** command to verify the following configurations. The password is **cisco123**.
 - VLAN1 IP address = 192.168.1.5
 - Subnet mask = 255.255.255.0
 - 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.

Experiment-9

Interpreting Ping and Traceroute Output

Topology Diagram



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>
```

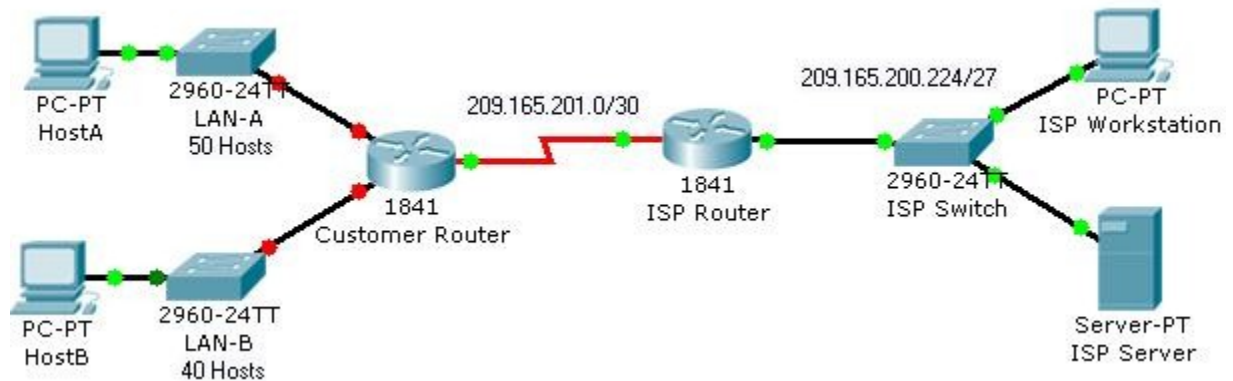
Step 3: Practice the ping and trace route commands.

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.

Experiment-10

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.

- 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.
- 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.
- 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.

- Click Customer Router. Click the Config tab.
- On the left side under Interface, click FastEthernet0/0. Enter the IP address and subnet mask, and then set the Port Status to On.
- On the left side under Interface, click FastEthernet0/1. Enter the IP address and subnet mask, and then set the Port Status to On.
- 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.

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