

INDEX

SR. NO.	EXPERIMENT	PAGE NO.	REMARK
1.	Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.	1-4	
2.	Study of Network Devices such as Switch, Router, Gateway, Servers etc.	4-5	
3.	To study and design network/subnet using subnet masking and IP addressing.	5	
4.	To study of basic network command and Network configuration commands.	5-7	
5.	Performing an Initial Switch Configuration.	8-10	
6.	Performing an Initial Router Configuration.	11-13	
7.	Configuring and Troubleshooting a Switched Network.	13-18	
8.	Connecting and configuring Switch.	19-20	
9.	Configuring Ethernet and Serial Interfaces	20-23	
10.	To design Local Area Network for a laboratory.	23-24	
11	Configuring WEP on a Wireless Router.	24-26	
12	Using the Cisco IOS Show Commands.	27-28	
13	Examining WAN Connections Output using commands such as Ping, Traceroute, ipconfig.	29-35	
14	Implementing various LAN configurations using LAN kit (Benchmark).	35-37	
15	Study and configure Firewall such as Cyberoam.	37	

Experiment-1

Aim: Study of different types of Network cables and Connectors and making the cross-wired cable and straight through cable using clamping tool.

Apparatus (Components): RJ-45 connector, Clamping 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.

Types of Connectors in Computer Networks

RJ45 Connector

The common interface for terminating Ethernet cables is the RJ45 connector, sometimes referred to as an Ethernet or network connector. These modular jack connectors with eight pins provide rapid and simple connections between switches, routers, and PCs that are part of a network. RJ45 connectors, which are widely used and compatible with several Ethernet standards, are the foundation of wired computer networks, guaranteeing uninterrupted communication and data transfer in residences, workplaces, and data centers.



USB Connectors

There are many different sizes and forms of USB connectors, and each is designed for a particular kind of device or use. USB connectors offer a flexible solution for connecting various devices in computer networks. They range from the standard USB Type-A connector found on computers and peripherals to the adaptable [USB](#) Type-C connector with its reversible design and support for high-speed data transfer and power delivery. USB connectors are now essential in modern cable networking environments due to their extensive compatibility and plug-and-play capability, facilitating smooth interaction and communication between devices.

Types of Internet Cables for Computer Network

Ethernet Cables

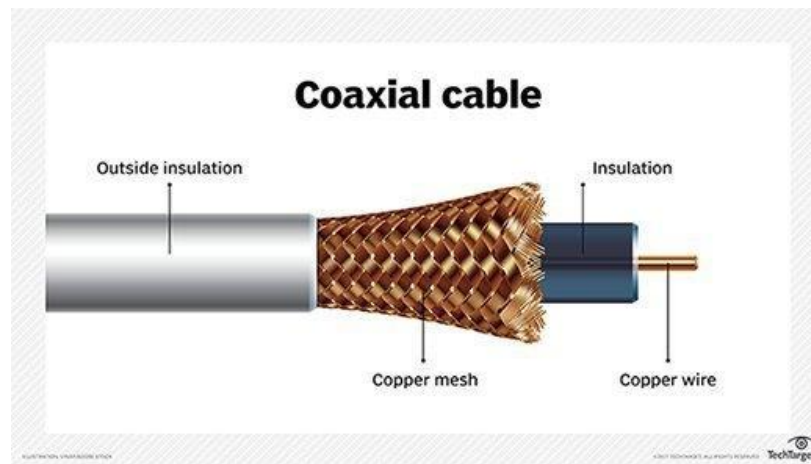
Ethernet connections, which offer dependable and fast connectivity between devices, are the foundation of wired computer networks. In order to provide reliable and secure data transmission in homes, workplaces, and data centers, these cables use twisted pairs of copper wires by the Ethernet protocol. Ethernet cables provide ever higher data transfer speeds and greater bandwidth due to the development of Ethernet standards like [Cat5e Wiring](#), Cat7 wiring, and [Cat6 wiring](#). This allows the seamless transmission of big files, multimedia material, and real-time data streams.



Coaxial Cables

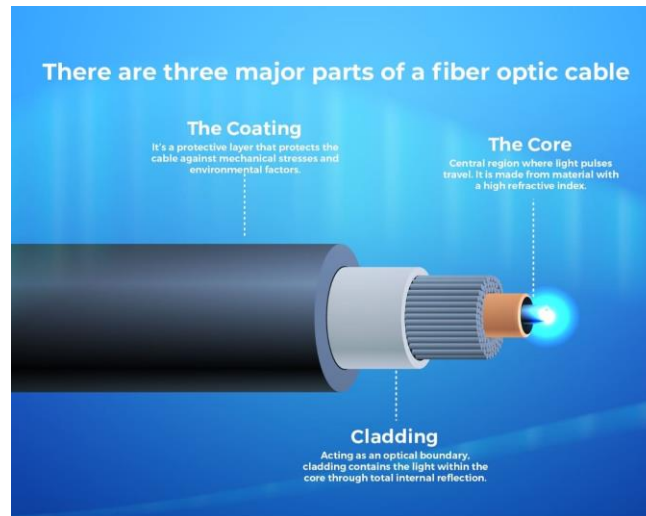
Coaxial cables are widely utilized in networking, cable television, and broadband internet applications because of their strong design and effective signal transfer. These

cables insulate against electromagnetic interference and signal deterioration via an outer sheath, insulation, and shielding layers surrounding the center conductor. Coaxial cables are ideal for data transmission in residential, commercial, and industrial environments because they can transport high-frequency signals over great distances. This capability enables dependable and fast connectivity to a variety of devices and services.



Fiber Optic Cables

Fiber optic cables are the ultimate in high-speed data transmission because they use light signals to send data across great distances with low delay and loss. Large volumes of data may be transmitted at extremely fast speeds thanks to these cables, which are made of tiny glass or plastic fiber strands covered in protective jackets. High-performance networking applications, such as telecommunications, data centers, and long-distance internet connections, are best suited for fiber optic cables due to their exceptional capacity, resilience to electromagnetic interference, and minimal signal attenuation. Fiber optic connections provide unparalleled speed, dependability, and scalability, making them essential in contemporary networking infrastructures despite their initial higher cost than conventional copper-based cables.



Crimping Tool:-

A crimping tool is a device that is used to make cold weld joints between wires and a connector through deforming one or both of them to hold the other. A special connector is used to join metals together. The weld joint properties (mechanical and electrical) are strong as the parent materials when the tool works and offer some result, which is known as crimp. An instance of crimping is to affixing a connector to the end of a wire. For example, a crimping tool is used to create phone cable and network cables to combine RJ-11 and RJ-45 connectors to both ends of the phone or Cat 5 cable. The below picture is an example of RJ-11 (6-pin) and RJ-45 (8-pin) crimping tools.



How to use a Crimping Tool?

First of all, the wire that you want to crimp, bandage it and attach the connector. Then, with the help of matching wire gauge ratings, the right die head for the connector will have to select for crimping tools with interchangeable dies. The groove must be properly matched for die less crimpers. In the last, take out the newly crimped connector with the help of applying pressure. And, for checking your connection is secure or not, give a few tugs.

Experiment - 2

Aim: Study of following Network Devices in Detail

- Switch
- Router

- Gate Way

Apparatus (Software): No software or hardware needed.

Procedure: Following should be done to understand this practical.

1. 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.

2. 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.

3. 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.

Servers:-

A server is a hardware device or software that processes requests sent over a network and replies to them. A client is the device that submits a request and waits for a response from the server. The computer system that accepts requests for online files and transmits those files to the client is referred to as a "server" in the context of the Internet.

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

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.

Experiment-4

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.

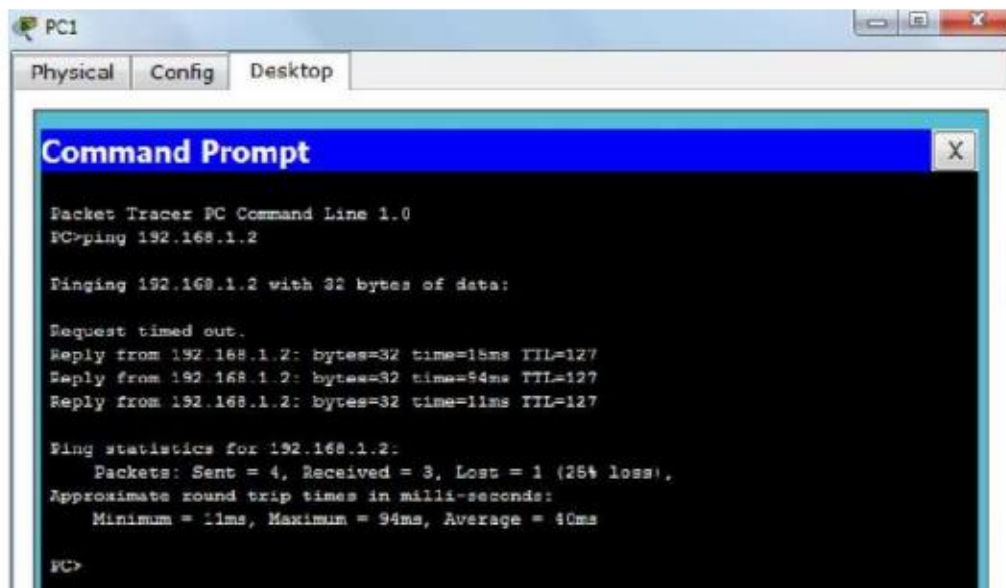
All commands related to Network configuration which includes how to switch to privilege mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.

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.



```
PC1
Physical Config Desktop
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

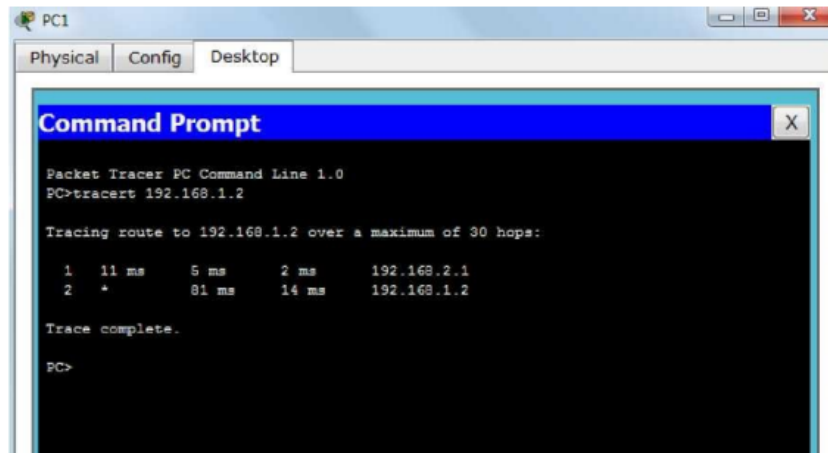
Request timed out.
Reply from 192.168.1.2: bytes=32 time=18ms TTL=127
Reply from 192.168.1.2: bytes=32 time=94ms TTL=127
Reply from 192.168.1.2: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 94ms, Average = 40ms

PC>
```

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.

```
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  ---      Lost/Sent = Pct  Lost/Sent = Pct  lenovo-PC.dronacharya [192.168.1.97]
  1  ---      100/ 100 =100%   100/ 100 =100%   1
                                0/ 100 = 0%      lenovo-PC [0.0.0.0]

Trace complete.

C:\Users\lenovo>
```

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 characters 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

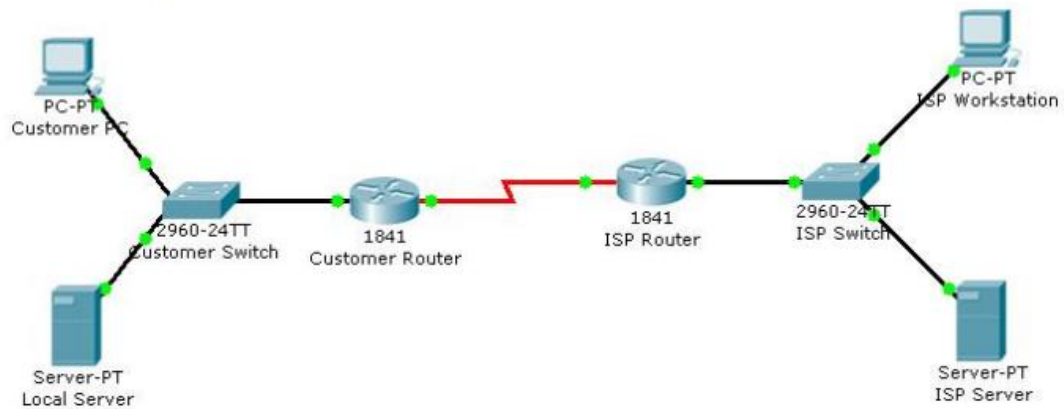
Any time you make changes to the router configuration, you must save the changes to memory because if you do not they will be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the startup configuration.

Use the following privileged mode commands to work with configuration files.

Experiment-5

Performing an Initial Switch Configuration

Topology Diagram



Objectives

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

Background / Preparation

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

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

Note: Not all commands are graded by Packet Tracer.

Step 1: Configure the switch host name.

- From the Customer PC, use a console cable and terminal emulation software to connect to the console of the customer Cisco Catalyst 2960 switch.
- Set the host name on the switch to **CustomerSwitch** using these commands.

```
Switch>enable
Switch#configure terminal
```

Step 2: Configure the privileged mode password and secret.

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

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

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

```
CustomerSwitch(config)#enable secret cisco123
```

Step 3: Configure the console password.

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

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

- 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.

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

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

- 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#
```

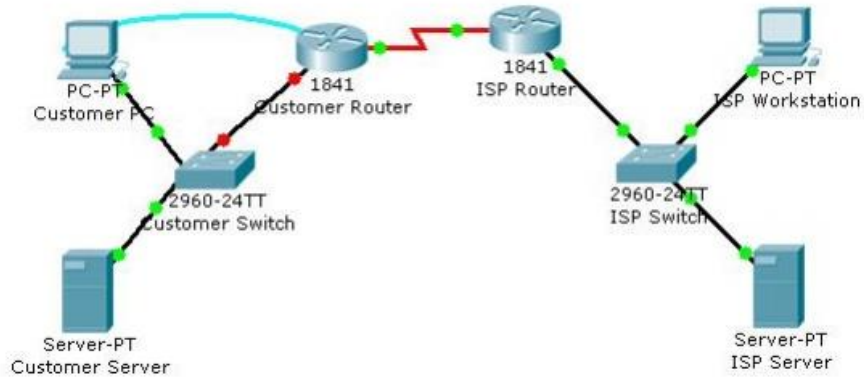
Reflection

- 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?
-

Experiment-6

Performing an Initial Router Configuration

Topology Diagram



Objectives

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

Background / Preparation

In this activity, you will use the Cisco IOS CLI to apply an initial configuration to a router, including 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.

- 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.

- 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
```

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.

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

Reflection

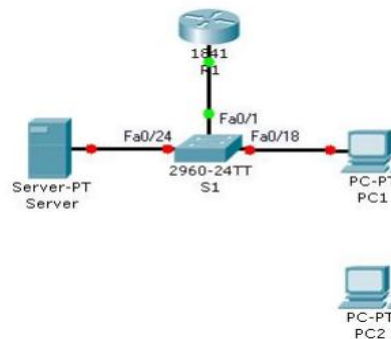
Which Cisco IOS CLI commands did you use most?

How can you make the customer router passwords more secure?

Experiment-7

Configuring and Troubleshooting a Switched Network

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 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.

- Connect a console cable from PC1 to S1.
- From PC1, open a terminal window and use the default terminal configuration. You should now have access to the CLI for S1.
- 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.

- Configure the switch host name as S1.
- Configure port Fa0/1. Set the mode on Fast Ethernet 0/1 to access mode.
 - S1(config)#**interface fastethernet 0/1**
 - 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.

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

- 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.

- 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.

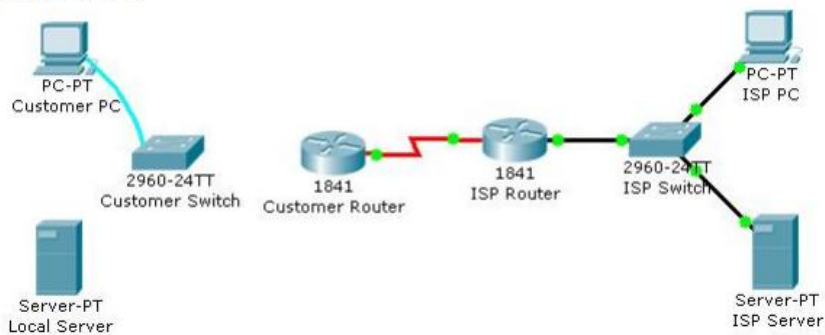
- a. Save the current configuration for S1 and R1 to NVRAM.
- b. Back up the startup configuration file on S1 and R1 by uploading them to Server. Verify that Server has the R1-config and S1-config files.
- c. Check results.

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

Experiment-8

Connecting a Switch

Topology Diagram



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.

- 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
-

- 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.

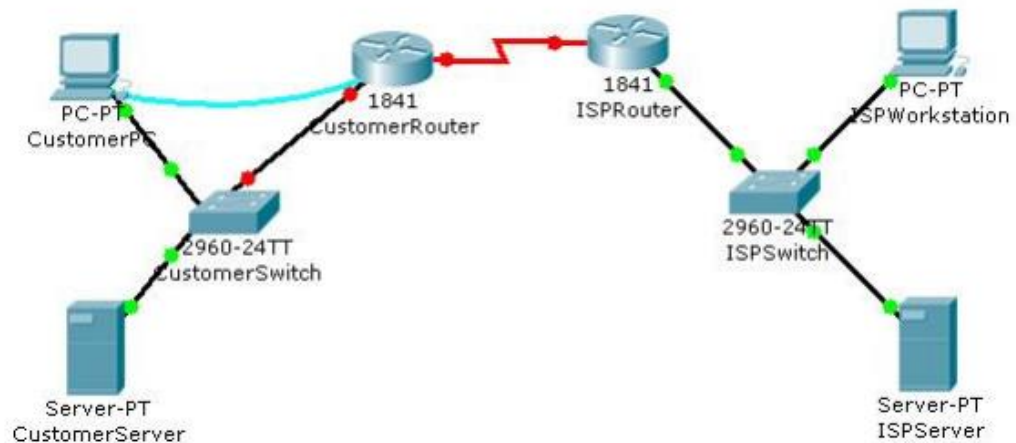
Reflection

- 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-9

Configuring Ethernet and Serial Interfaces

Topology Diagram



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.

- Enter global configuration mode.
- Identify the serial interface to configure.
- Describe the interface. (Connected to ISP)
- Specify the interface IP address and subnet mask. (209.165.200.225 255.255.255.224)
- Ensure that the interface is enabled.
- 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.

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

```

CustomerRouter#copy run start

```

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

Reflection

- When you ping the LAN IP address of the ISP router, what happens and why?
 - Which of the following Cisco IOS 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 happened.

Experiment-10

To design Local area network for a laboratory

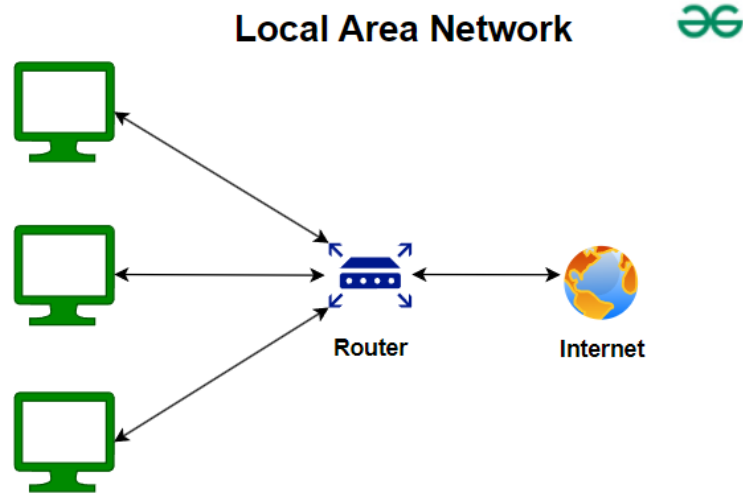
A Local Area Network (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.

Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and Ethernet.

Several experimental and early commercial LAN technologies were developed in the 1970s. Cambridge Ring is a type of LAN that was developed at Cambridge University in 1974.



Local Area Network

How do LANs Work?

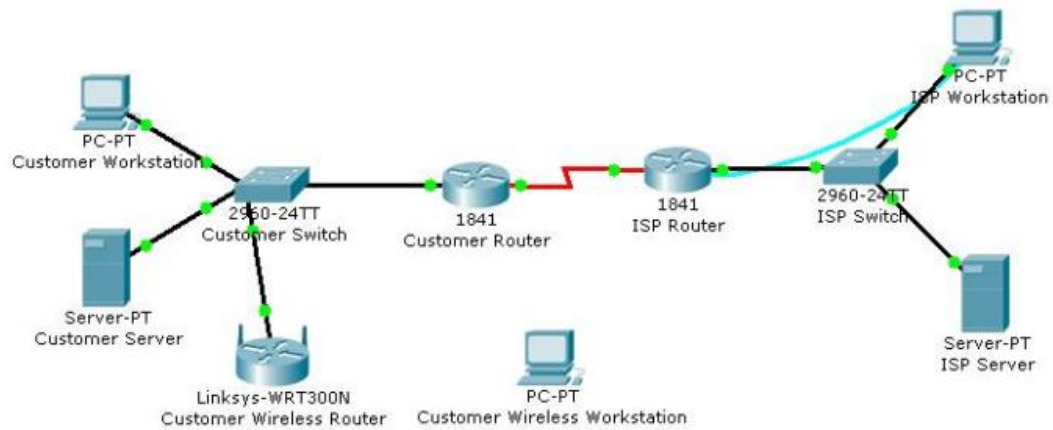
A router serves as the hub where the majority of LANs connect to the Internet. Home LANs often utilise a single router, but bigger LANs may also use network switches to transmit packets more effectively.

LANs nearly always connect devices to the network via [Ethernet](#), WiFi, or both of these technologies. Ethernet is a way to connect devices to the Local Area Network ethernet define the physical and data link layer of the OSI model. WiFi is a protocol that is used to connect devices to the Local Area Network wirelessly.

Experiment-11

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.

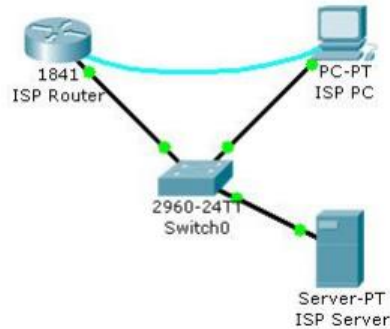
After you configure the correct WEP key and SSID on the customer wireless workstation, notice that there is a wireless connection between the workstation and the wireless router.

- 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.
-

Experiment-12

Using the Cisco IOS Show Commands

Topology Diagram



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#** prompt indicates 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.

- Type **show arp**.
 - Type **show flash**.
 - Type **show ip route**.
 - Type **show interfaces**.
 - Type **show protocols**.
 - Type **show users**.
 - 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?

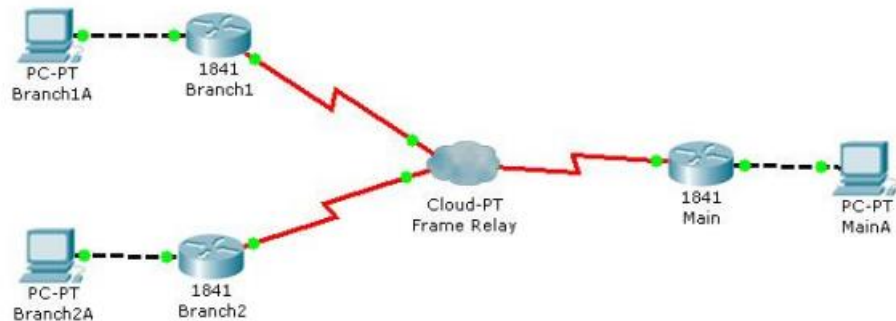
- 209.165.201.0
- 209.165.201.1
- 209.165.201.10

Which interface is up and running?

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

Experiment-13

Examining WAN Connections



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.

- Click on Branch1 and use various **show** commands to view the connectivity to the network.
 - Use the **show running-configuration** command to view the router configuration.
 - Use the **show ip interface brief** command to view the status of the interfaces.
 - 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.
 - Click on Branch 2 and use various **show** commands to view the connectivity to the network.
 - Use the **show running-configuration** command to view the router configuration.
 - Use the **show ip interface brief** command to view the status of the interfaces.
 - 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.

- Click on Main and use a variety of **show** commands to view the connectivity to the network.
- Use the **show running-configuration** command to view the router configuration.
- Use the **show ip interface brief** command to view the status of the interfaces.
- 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.

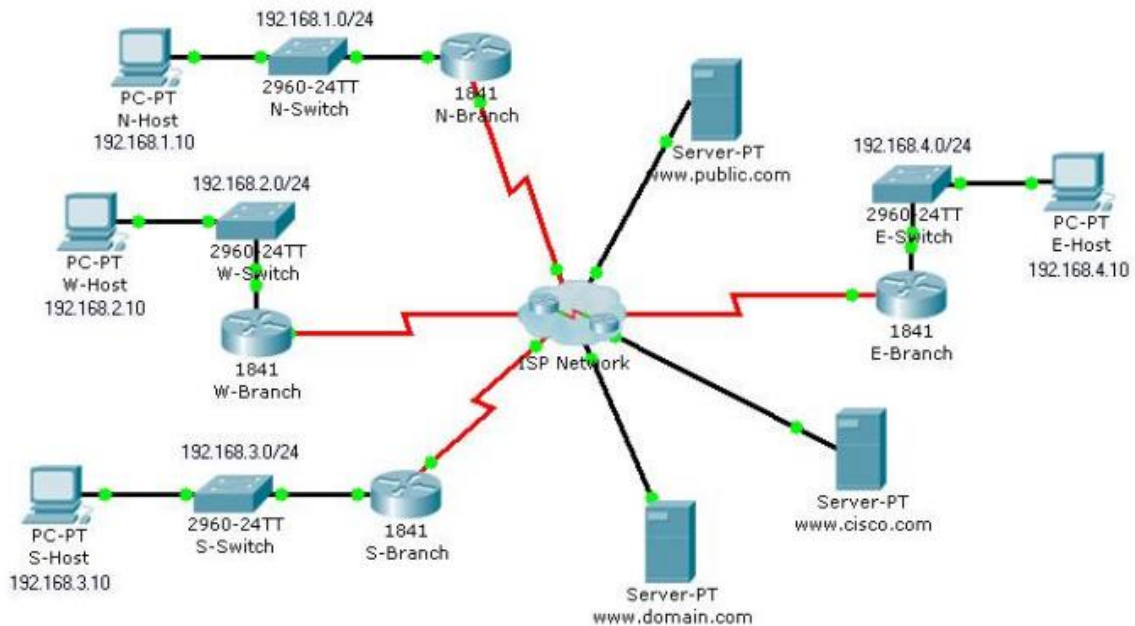
Reflection

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

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

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),
```

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:

```
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>
```

```

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>tracert 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>tracert 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-14

8 steps to LAN setup and configuration

Here's a quick walkthrough of how to set up and configure your LAN in eight simple steps.

1. Identify network services and resources

Start by listing all the services and resources that will be shared across the network. This could include file servers, printers, and internet access.

Knowing what needs to be shared helps in selecting the right hardware and software, ensuring that all networking needs are met. You can use a spreadsheet to organize these resources, noting their locations and access requirements.

2. Select and prepare networking devices

[Choosing the right switch](#) and router is crucial. Make sure these devices have enough ports for all your workstations and other hardware. Update the firmware to the latest versions to ensure you're getting the best performance and security features.

3. Plan your network architecture

Before you start connecting cables, you can either use network design software such as [Cisco Packet Tracer](#) (**Figure A**) or pen and paper to sketch out a network diagram. This will serve as your blueprint for device placement, cable lengths, and types. A well-planned architecture minimizes potential issues and simplifies troubleshooting down the line.

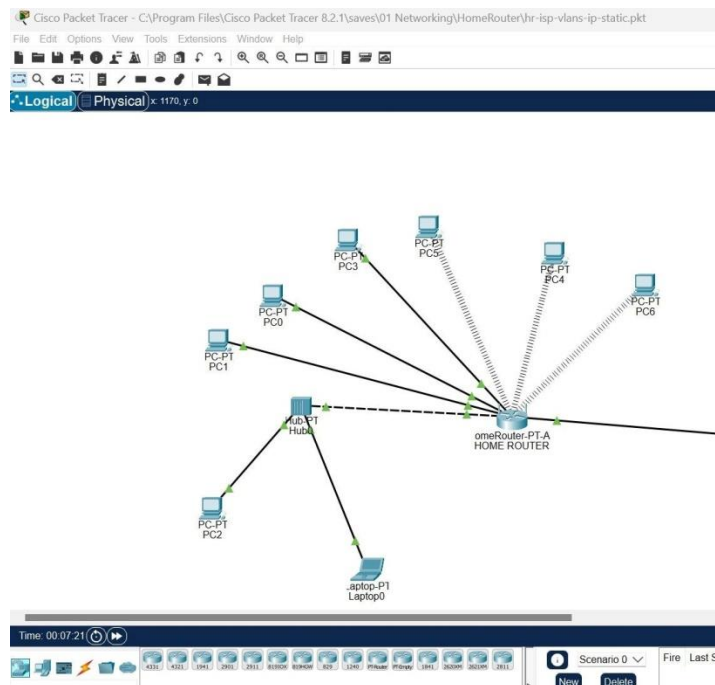


Figure A: Design of a simple network in Cisco Packet Tracer.

4. Configure IP addressing

[IP addressing](#) is a critical aspect of network setup. Decide whether to use static or dynamic IP addresses. Static IPs are often used for servers and network devices, while dynamic IPs can be assigned to workstations through DHCP.

For static IPs, you'll need to manually enter IP addresses for each device. This is often done through each device's settings menu. It's also possible to enable DHCP for dynamic IPs on your router via its admin panel to automatically assign IPs to connected devices.

5. Cable and connect devices

Based on your network diagram, start connecting devices using the appropriate cables. Remember to keep the process neat. Make sure to use quality cables and connectors to minimize signal loss and potential issues. Test each connection as you go along to ensure it's secure and functional.

6. Initial testing

Once all devices are connected, perform an initial round of tests. Check if all devices can communicate with each other, access the internet, and use shared resources. Resolve any issues before moving to the next step.

7. Monitor and manage

While you could stop after Step 6, it will serve you better in the long run to ensure that your LAN is not just up and running, but that it stays that way. This is done by keeping an eye on your network's performance after confirming that it's functional.

Use [network monitoring](#) and [management tools](#) like [Wireshark](#) and [SolarWinds Network Performance Monitor](#) to monitor traffic, bandwidth usage, and any unauthorized access attempts.

8. Document your network

Documentation is often overlooked, but is crucial for effective network management. Keep a record of all configurations, IP addresses, and device placements. This documentation will be invaluable for troubleshooting and future network expansions.

Experiment-15

Configuring Cyberoam Firewall

On the Cyberoam Firewall Web Admin Console do the following.

1. Select **System > Logging > Manage Syslog**
2. Specify unique name for **Syslog server**
3. Specify **IP address** and **port** of the syslog server. Cyberoam will send logs to the configured IP address. The default port is 514
4. Select **Facility**. Facility indicates the source of a log message to the syslog server. You can configure **Facility** to distinguish log messages from different Cyberoam Firewalls
5. Select the **Severity** level of the messages logged. Severity level is the severity of the message that has been generated

Note:	Cyberoam logs all messages at and above the logging severity level you select. For example, select 'ERROR' to log all messages tagged as 'ERROR,' as well as any messages tagged with 'CRITICAL,' 'ALERT' and 'EMERGENCY' and select 'DEBUG' to log all messages. Note: Firewall Analyzer requires the severity level as 'INFORMATIONAL'.
--------------	---

6. Click **Create** to save the configuration.

Also you need to enable logging on each rule to monitor allowed and denied traffic. Please follow the below steps.

- Click **Log Traffic** to enable/disable traffic logging for the rule. Ensure firewall rule logging is in **On/Enable** state in the Logging Management. Refer to Cyberoam Console Guide, Cyberoam Management for more details.
- To log the traffic permitted and denied by the firewall rule, you need to keep **On/Enable** state in the firewall rule logging from the **Web Admin Console > Firewall rule and from the Telnet Console > Cyberoam Management**.
- Specify full description of the rule, displays full description of the rule, modify if required.