Introduction to Networking

CT043-3-1

Version VE1

0002 - Basic Switch and End Device Configuration (2)

Ports and Addresses

1. IP Addresses

Congratulations, you have performed a basic device configuration! Of course, the fun is not over yet. If you want your end devices to communicate with each other, you must ensure that each of them has an appropriate IP address and is correctly connected. You will learn about IP addresses, device ports and the media used to connect devices in this topic.

The use of IP addresses is the primary means of enabling devices to locate one another and establish end-to-end communication on the internet. Each end device on a network must be configured with an IP address. Examples of end devices include these:

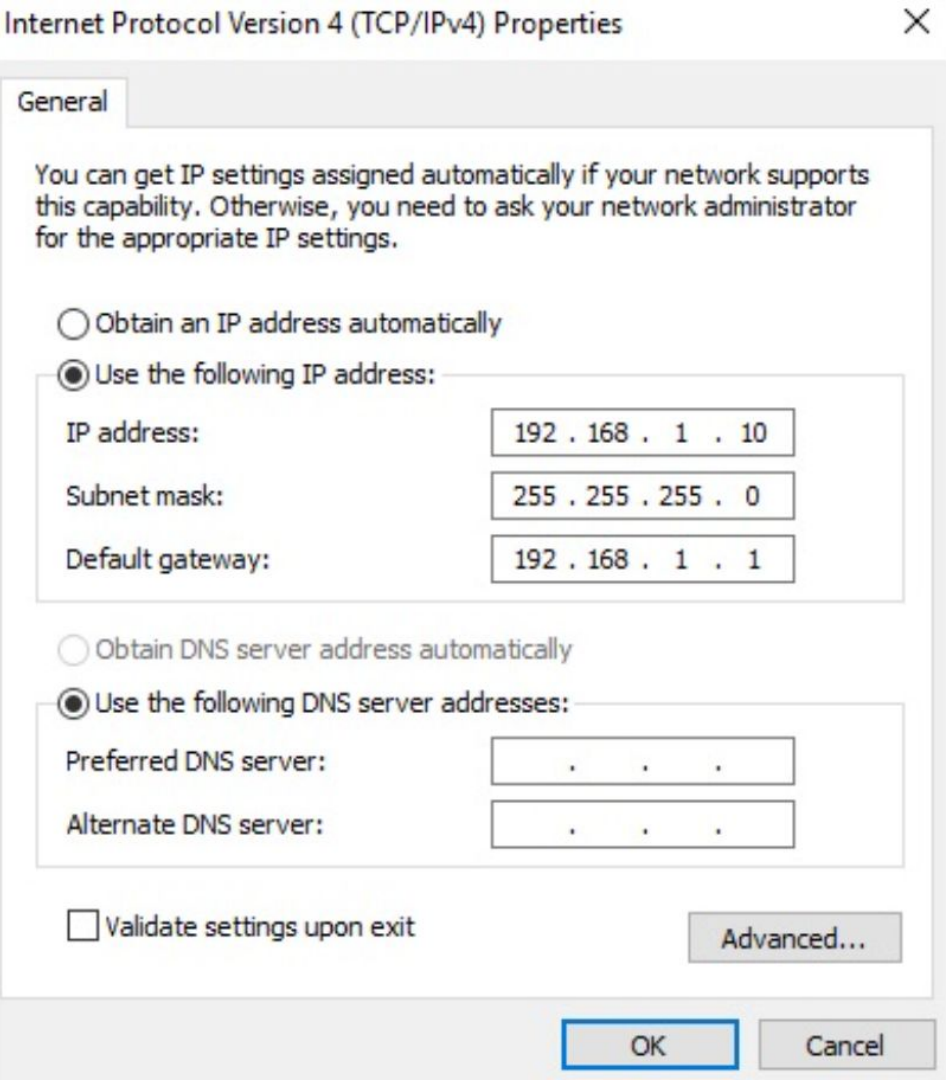
- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Smart phones
- Mobile handheld devices (such as wireless barcode scanners)

The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255. IPv4 addresses are assigned to individual devices connected to a network.

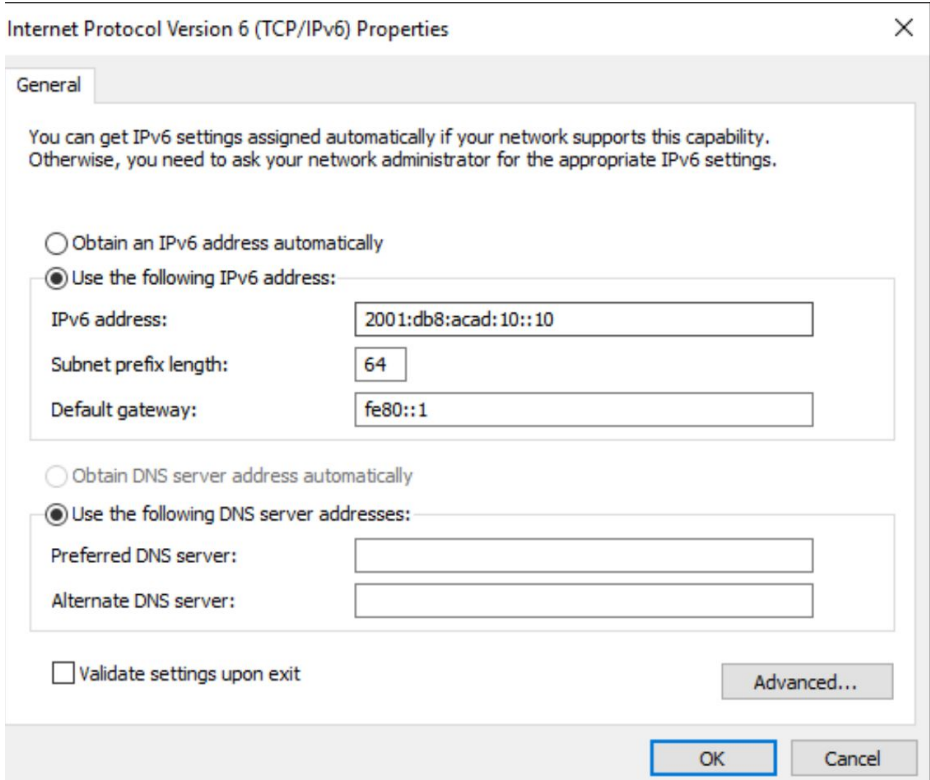
Note: IP in this course refers to both the IPv4 and IPv6 protocols. IPv6 is the most recent version of IP and is replacing the more common IPv4.

With the IPv4 address, a subnet mask is also necessary. An IPv4 subnet mask is a 32-bit value that differentiates the network portion of the address from the host portion. Coupled with the IPv4 address, the subnet mask determines to which subnet the device is a member.

The example in the figure displays the IPv4 address (192.168.1.10), subnet mask (255.255.255.0), and default gateway (192.168.1.1) assigned to a host. The default gateway address is the IP address of the router that the host will use to access remote networks, including the internet.

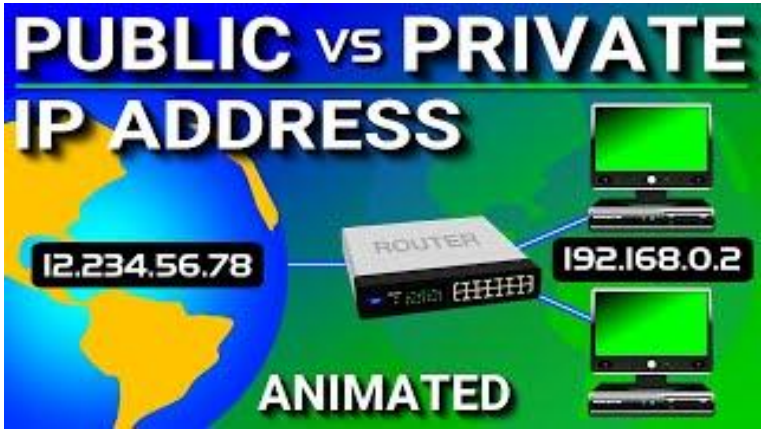


IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every four bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. Groups of four hexadecimal digits are separated by a colon (:) . IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.



YouTube: [Network Ports Explained]

YouTube: [Public vs Private IP Address]



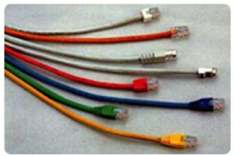
YouTube: [Basics of Port Addressing]

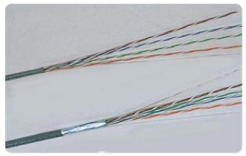
2. Interfaces and Ports

Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them. Each physical interface has specifications, or standards, that define it.

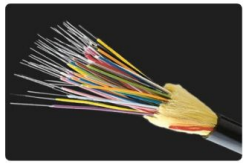
A cable connecting to the interface must be designed to match the physical standards of the interface. Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless, as shown in the figure.

Copper





Fiber-optics



Wireless

Different types of network media have different features and benefits. Not all network media have the same characteristics. Not all media are appropriate for the same purpose. These are some of the differences between various types of media:

- Distance the media can successfully carry a signal
- Environment in which the media is to be installed
- Amount of data and the speed at which it must be transmitted
- Cost of the media and installation

Not only does each link on the internet require a specific network media type, but each link also requires a particular network technology. For example, Ethernet is the most common local-area network (LAN) technology used today. Ethernet ports are found on end-user devices, switch devices, and other networking devices that can physically connect to the network using a cable.

Cisco IOS Layer 2 switches have physical ports for devices to connect. These ports do not support Layer 3 IP addresses. Therefore, switches have one or more switch virtual interfaces (SVIs). These are virtual interfaces because there is no physical hardware on the device associated with it. An SVI is created in software.

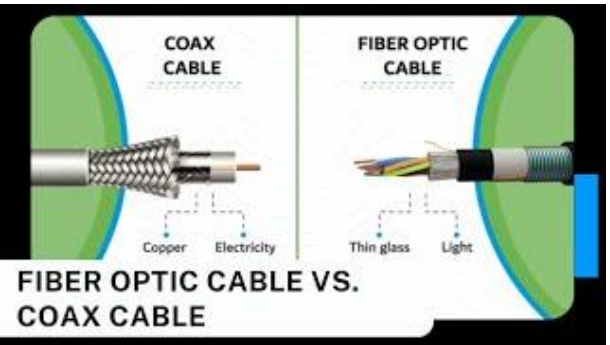
The virtual interface lets you remotely manage a switch over a network using IPv4 and IPv6. Each switch comes with one SVI appearing in the default configuration "out-of-the-box." The default SVI is interface VLAN1.

Note: A Layer 2 switch does not need an IP address. The IP address assigned to the SVI is used to remotely access the switch. An IP address is not necessary for the switch to perform its operations.

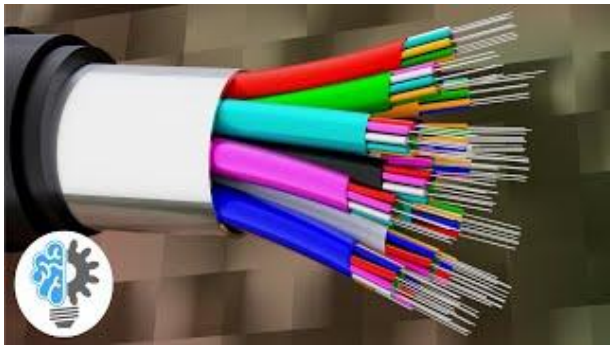
YouTube: [Interfaces, Connections and Ports]

YouTube: [Network Connectors Explained]

YouTube: [Fiber Optic Cable Vs. Coax Cable]



YouTube: [Optical fiber cables, how do they work? | ICT #3]



3. Check Your Understanding - Ports and Addresses

Check your understanding of ports and addresses by choosing the BEST answer to the following questions.

Question 1: What is the structure of an IPv4 address called?

(a) dotted-binary format

(b) dotted-decimal format

(c) dotted-hexadecimal format

Answer: **(b) dotted-decimal format -** IPv4 addresses are written in dotted-decimal format. For example: 192.168.1.1.

Question 2: How is an IPv4 address represented?

(a) four binary numbers between 0 and 1 separated by colons.

(b) four decimal numbers between 0 and 255 separated by periods.

(c) thirty-two hexadecimal numbers separated by colons.

(d) thirty-two hexadecimal numbers separated by periods.

Answer: **(b) -** IPv4 addresses are written as four groups of decimal numbers separated by periods. For example: 192.168.1.1.

Question 3: What type of interface has no physical port associated with it?

(a) Console

(b) Ethernet

(c) serial

(d) switch virtual interface (SVI)

Answer: **(d) switch virtual interface (SVI) -** Switch virtual interfaces (SVIs) are virtual and have no physical port. Layer 2 switches use SVIs for remote management.

Configure IP Addressing

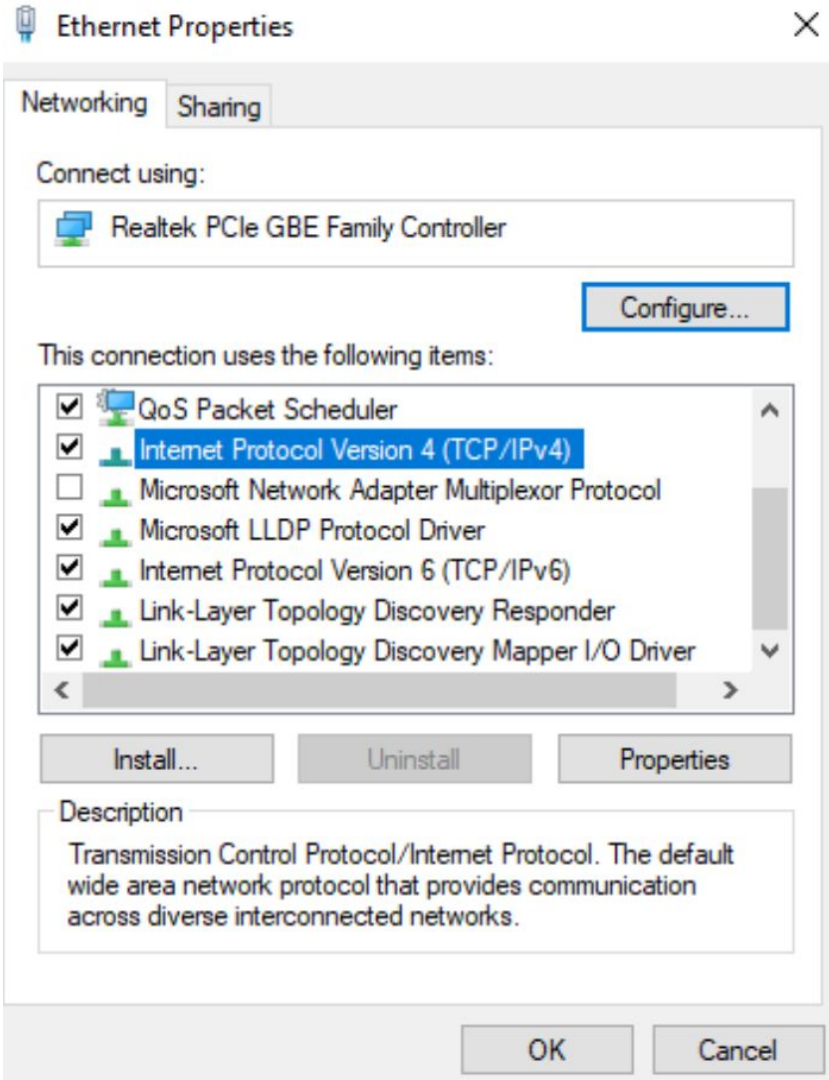
1. Manual IP Address Configuration for End Devices

Much like you need your friends' telephone numbers to text or call them, end devices in your network need an IP address so that they can communicate with other devices on your network. In this topic, you will implement basic connectivity by configuring IP addressing on switches and PCs.

IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP).

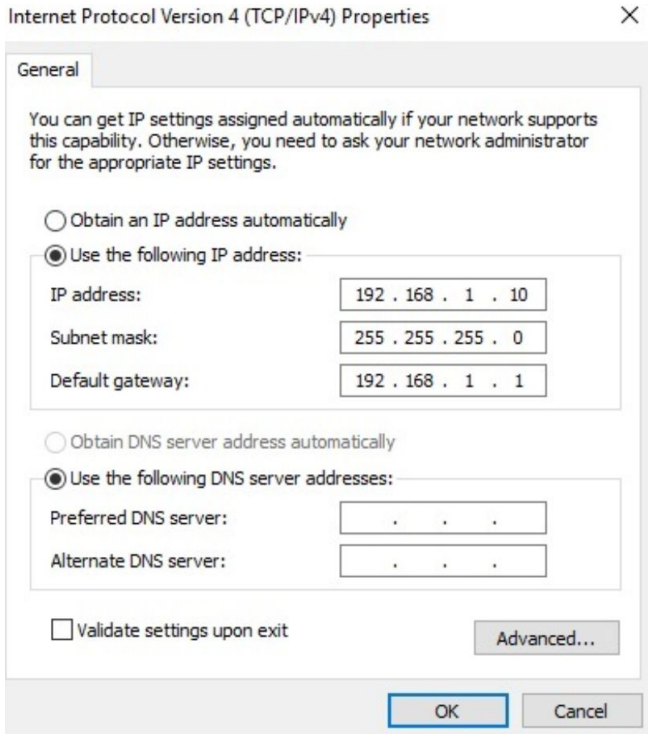
To manually configure an IPv4 address on a Windows host, open the **Control Panel > Network Sharing Center > Change adapter settings** and choose the adapter.

Next right-click and select **Properties** to display the **Local Area Connection Properties**, as shown in the figure.



Highlight Internet Protocol Version 4 (TCP/IPv4) and click **Properties** to open the **Internet Protocol Version 4 (TCP/IPv4)** Properties window, shown in the figure. Configure the IPv4 address and subnet mask information, and default gateway.

Note: IPv6 addressing and configuration options are similar to IPv4.



Note: The DNS server addresses are the IPv4 and IPv6 addresses of the Domain Name System (DNS) servers, which are used to translate IP addresses to domain names, such as www.cisco.com.

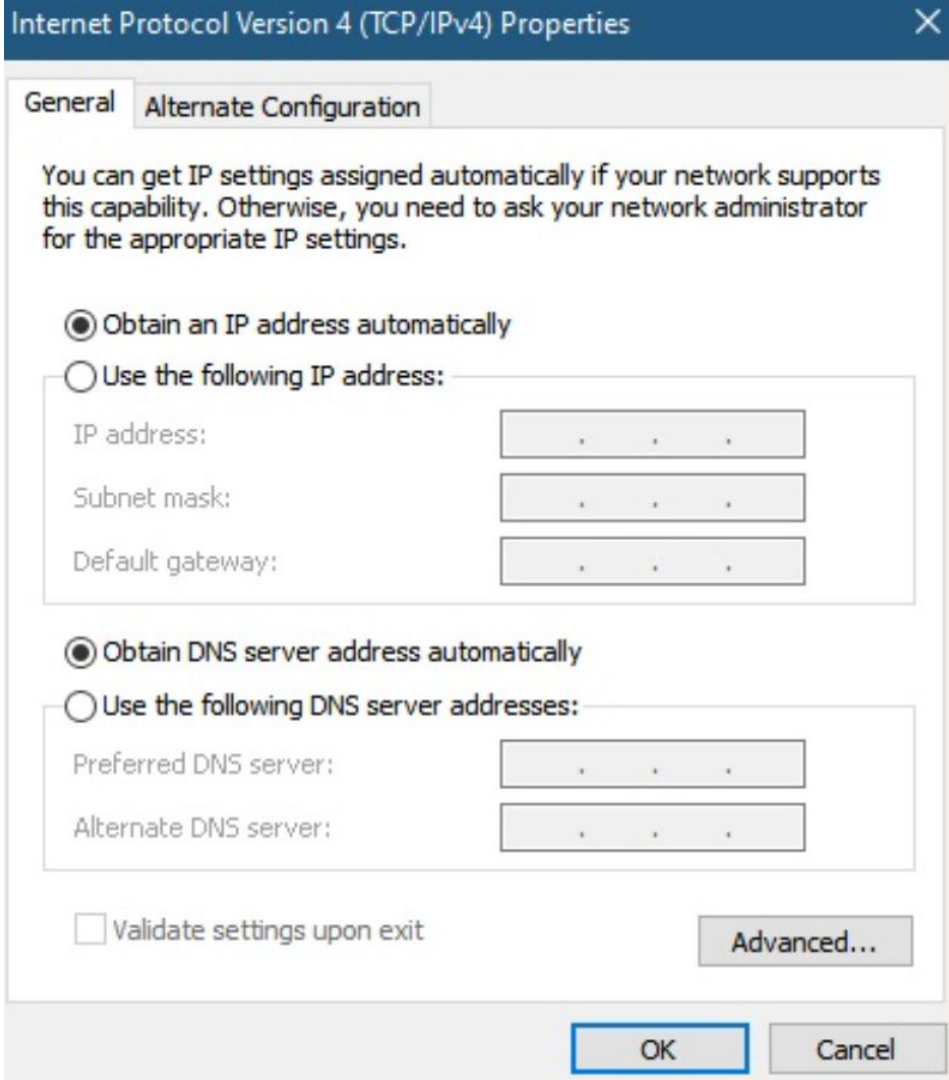
2. Automatic IP Address Configuration for End Devices

End devices typically default to using DHCP for automatic IPv4 address configuration. DHCP is a technology that is used in almost every network. The best way to understand why DHCP is so popular is by considering all the extra work that would have to take place without it.

In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. Imagine the amount of time it would take if every time you connected to the network, you had to manually enter the IPv4 address, the subnet mask, the default gateway, and the DNS server. Multiply that by every user and every device in an organization and you see the problem. Manual configuration also increases the chance of misconfiguration by duplicating another device's IPv4 address.

As shown in the figure, to configure DHCP on a Windows PC, you only need to select **Obtain an IP address automatically and Obtain DNS server address automatically**. Your PC will search out a DHCP server and be assigned the address settings necessary to communicate on the network.

Note: IPv6 uses DHCPv6 and SLAAC (Stateless Address Autoconfiguration) for dynamic address allocation.



3. Syntax Checker - Verify Windows PC IP Configuration

It is possible to display the IP configuration settings on a Windows PC by using the ipconfig command at the command prompt. The output will show the IPv4 address, subnet mask, and gateway information received from the DHCP server.

Enter the command to display the IP configuration on a Windows PC.

Enter the command to display the IP configuration on a Windows PC.

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : cisco.com
Link-local IPv6 Address . . . . . : fe80::b0ef:ca42:af2c:c6c7%16
IPv4 Address. . . . . . . . . . . : 192.168.1.10
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```

You successfully displayed the IP configuration on a Windows PC.

4. Switch Virtual Interface Configuration

To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch, use the **interface vlan 1** global configuration command. Vlan 1 is not an actual physical interface but a virtual one.

Next assign an IPv4 address using the **ip address** *ip-address subnet-mask* interface configuration command. Finally, enable the virtual interface using the **no shutdown** interface configuration command.

After these commands are configured, the switch has all the IPv4 elements ready for communication over the network.

Note: Similar to a Windows hosts, switches configured with an IPv4 address will typically also need to have a default gateway assigned. This can be done using the **ip default-gateway** *ip-address* global configuration command.

The *ip-address parameter* would be the IPv4 address of the local router on the network, as shown in the example. However, in this module you will only be configuring a network with switches and hosts. Routers will be introduced later.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

5. Syntax Checker - Configure a Switch Virtual Interface

Enter interface configuration mode for VLAN 1.

```
Switch(config)#interface vlan 1
```

Configure the IPv4 address as 192.168.1.20 and the subnet mask as 255.255.255.0.

```
Switch(config-if)#ip address 192.168.1.20 255.255.255.0
```

Enable the interface.

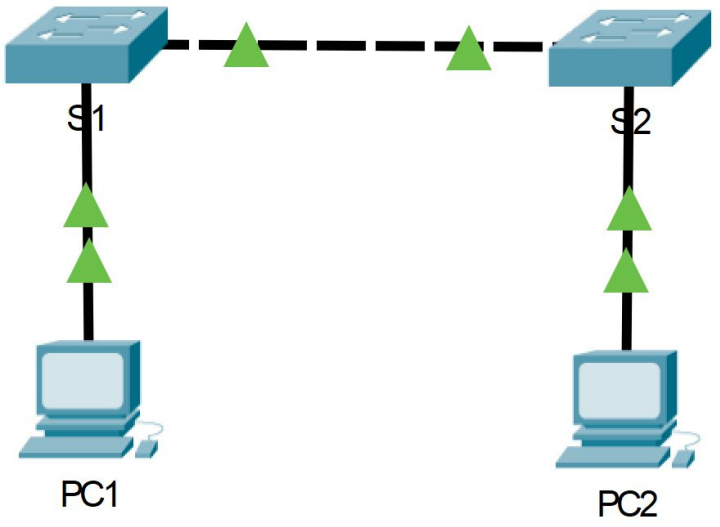
```
Switch(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

You have successfully configured the switch virtual interface for VLAN 1.

6. Packet Tracer - Implement Basic Connectivity

In this activity, you will first perform basic switch configurations. Then you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various **show** commands to verify configurations and use the **ping** command to verify basic connectivity between devices.

- Download Packet Tracer (.pka) file



6A. Packet Tracer - Implementing Basic Connectivity

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

6B. Objectives

- Part 1: Perform a Basic Configuration on S1 and S2
- Part 2: Configure the PCs
- Part 3: Configure the Switch Management Interface

6C. Background

In this activity, you will first perform basic switch configurations. Then, you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various show commands to verify configurations and use the ping command to verify basic connectivity between devices.

6E. Part 1: Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

Step 1: Configure S1 With A Hostname.

a. Click **S1**, and then click the **CLI** tab.

b. Enter the correct command to configure the hostname as **S1**.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
```

Step 2: Configure The Console And Encrypted Privileged Exec Mode Passwords.

a. Use **cisco** for the console password.

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

b. Use **class** for the privileged EXEC mode password.

```
S1(config)#enable secret class
S1(config)#
```

Step 3: Verify The Password Configurations For S1

Question: How can you verify that both passwords were configured correctly?

- After you exit user EXEC mode, the switch will prompt you for a password to access the console interface and will prompt you a second time when accessing the privileged EXEC mode. You can also use the show run command to view the passwords.

S1#show running-config

```
S1#show running-config
Building configuration...

Current configuration : 1148 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
```

```
!
line con 0
 password cisco
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

Step 4: Configure An Motd Banner

Use an appropriate banner text to warn unauthorized access. The following text is an example:

- **Authorized access only. Violators will be prosecuted to the full extent of the law.**

S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#banner motd $Authorized access only. Violators will be prosecuted to the full extent of the law.$
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#exit

```
Press RETURN to get started!

Authorized access only. Violators will be prosecuted to the full extent of the
law.

User Access Verification

Password:
```

Step 5: Save The Configuration File To Nvram.

Question: Which command do you issue to accomplish this step?

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Step 6: Repeat Steps 1 To 5 For S2.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S2

S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit

S2(config)#enable secret class

S2(config)#banner motd $Authorized access only. Violators will be prosecuted to the full extent of the law.$

S2#exit

S2#copy running-config startup-config
```

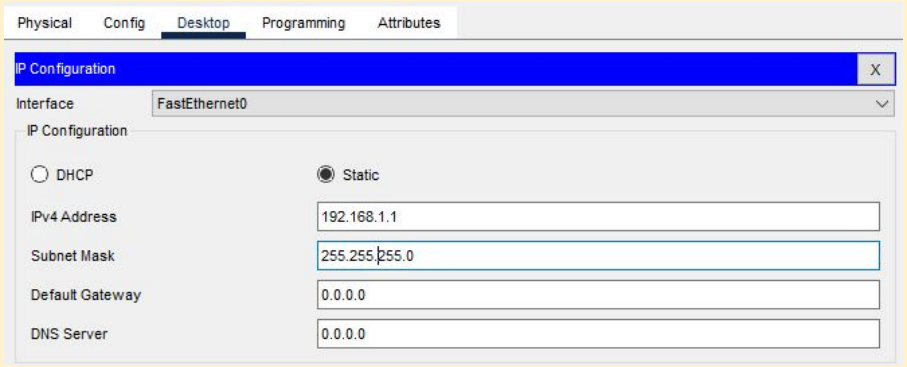
6F. Part 2: Configure The PCs

Configure PC1 and PC2 with IP addresses.

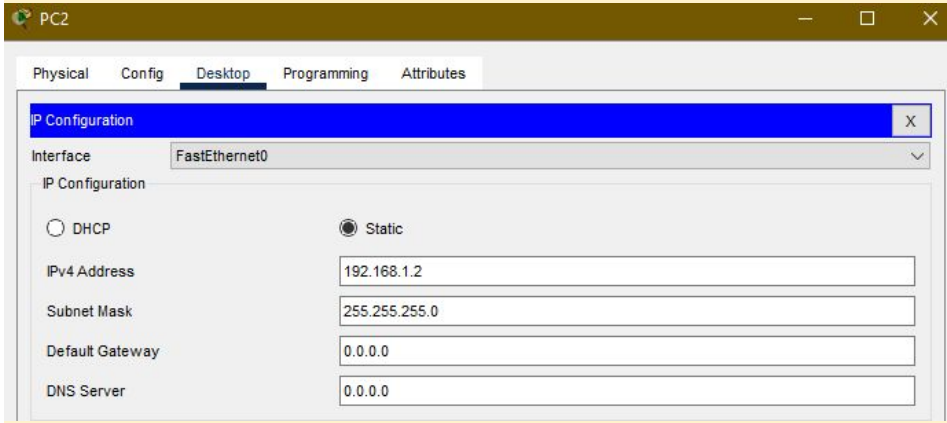
Step 1: Configure Both PCs With Ip Addresses.

a. Click PC1 and then click the **Desktop** tab.

b. Click **IP Configuration**. In the Addressing Table above, you can see that the IP address for PC1 is 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the **IP Configuration** window.

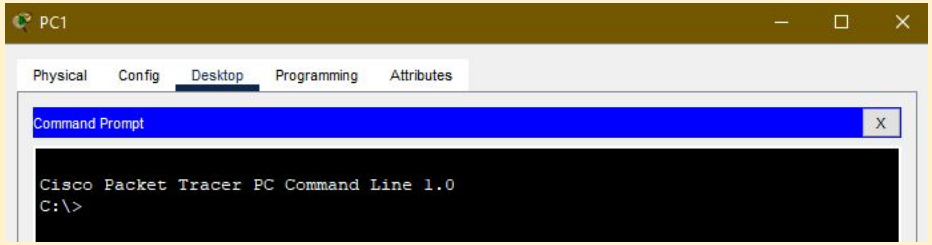


c. Repeat steps 1a and 1b for PC2.



Step 2: Test Connectivity To Switches.

a. Click PC1. Close the **IP Configuration** window if it is still open. In the **Desktop** tab, click **Command Prompt**.



b. Type the **ping** command and the IP address for S1 and press Enter.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:
```

- Were you successful? Explain.
    - Your ping should have been unsuccessful because the switches have not been configured with an IP address.

6G. Part 3: Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 1: Configure S1 With An Ip Address.

a. Switches can be used as plug-and-play devices. This means that they do not need to be configured for them to work. Switches forward information from one port to another based on MAC addresses.

Question:

- If this is the case, why would we configure it with an IP address?
    - In order for you to connect remotely to a switch, you need to assign it an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1.

b. Use the following commands to configure S1 with an IP address.

```
S1 #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)# exit
S1#
```

Question:

- Why do you need to enter the **no shutdown** command?
    - The **no shutdown** command administratively places the interface in an active state.

Step 2: Configure S2 With An Ip Address.

a. Use the information in the Addressing Table to configure S2 with an IP address.

```
S2>enable

S2#configure terminal

S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.254 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#
```

Step 3: Verify The IP Address Configuration On S1 And S2.

S1. Use the **show ip interface brief** command to display the IP address and status of all the switch ports and interfaces. You can also use the **show running-config command**.

```
S1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.253   YES manual up                    up
S1#
```

S2. Use the **show ip interface brief** command to display the IP address and status of all the switch ports and interfaces. You can also use the **show running-config command**.

```
S2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.254   YES manual up                    up
```

Step 4: Save Configurations For S1 And S2 to NVRAM.

a. Which command is used to save the configuration file in RAM to NVRAM?

- copy running-config startup-config

Step 5: Verify Network Connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1's and S2's IP address from PC1 and PC2.

a. Click **PC1**, and then click the **Desktop** tab.

b. Click **Command Prompt**.

c. Ping the IP address for PC2.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=11ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

d. Ping the IP address for S1.

```
C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

e. Ping the IP address for S2.

```
C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Note:

- You can also use the same ping command on the switch CLI and on PC2.

- All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

Verify Connectivity

1. Video Activity - Test the Interface Assignment

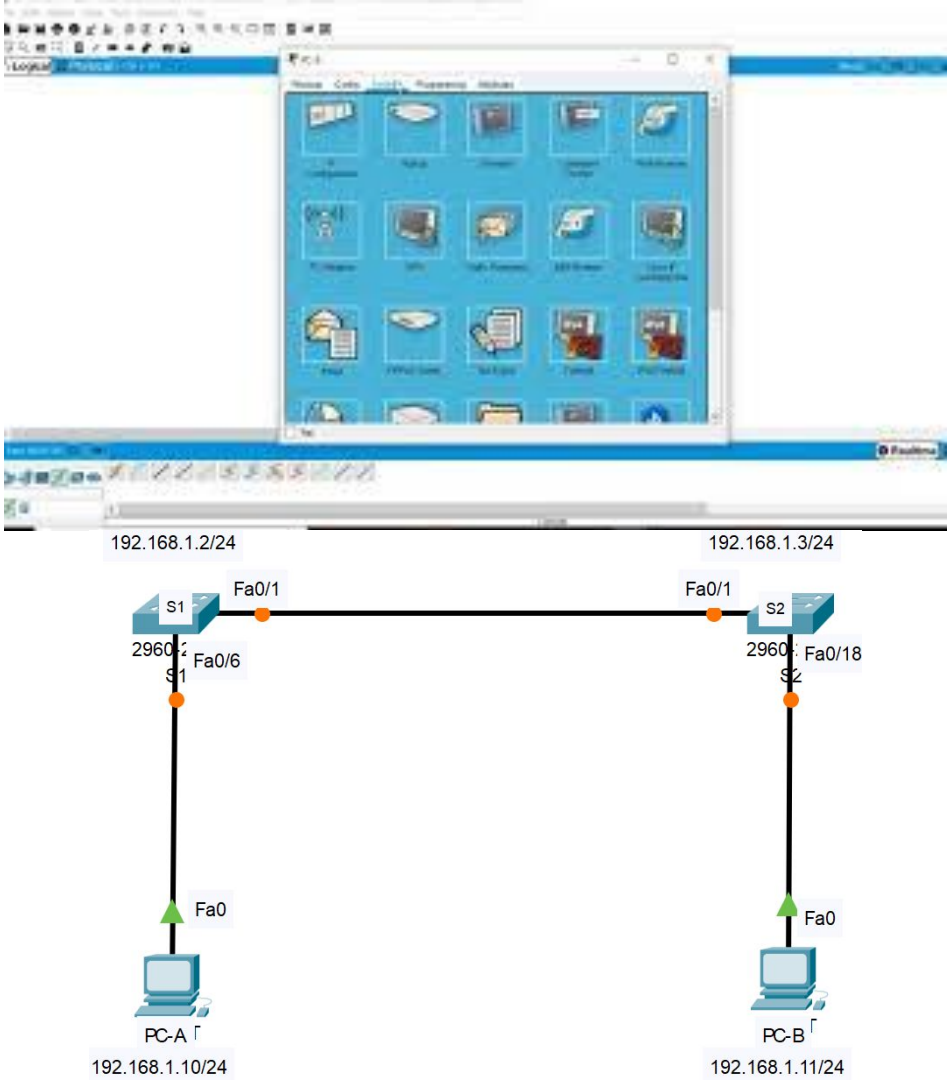
In the previous topic, you implemented basic connectivity by configuring IP addressing on switches and PCs. Then you verified your configurations and connectivity, because, what is the point of configuring a device if you do not verify that the configuration is working? You will continue this process in this topic. Using the CLI, you will verify the interfaces and the addresses of the switches and routers in your network.

In the same way that you use commands and utilities like **ipconfig** to verify the network configuration of a PC host, you also use commands to verify the interfaces and address settings of intermediary devices like switches and routers.

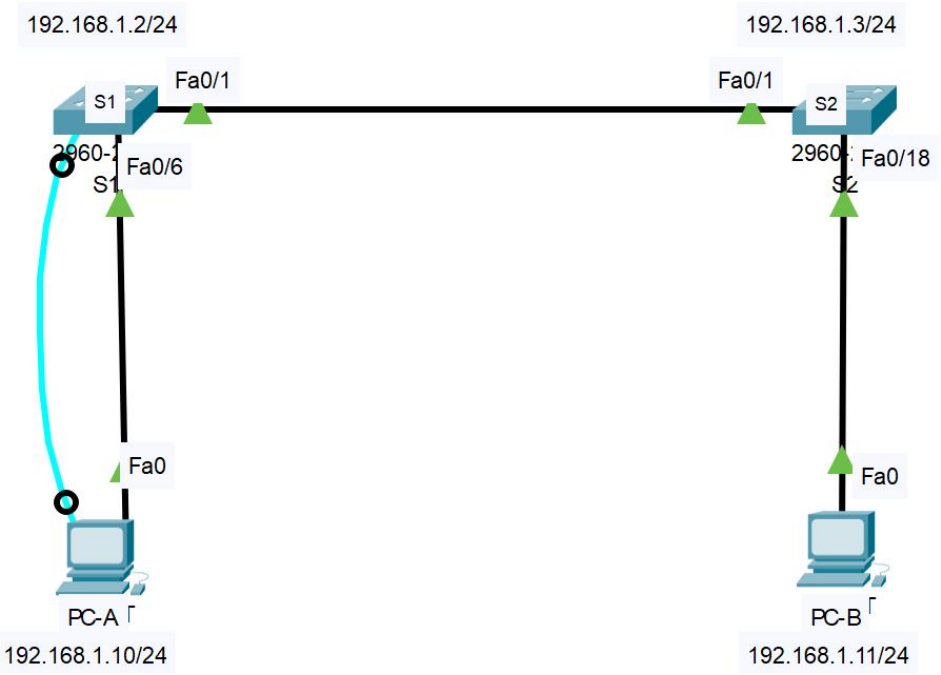
Click Play in the figure to view a video demonstration of the **show ip interface brief** command. This command is useful for verifying the condition of the switch interfaces.

Follow Along in Packet Tracer

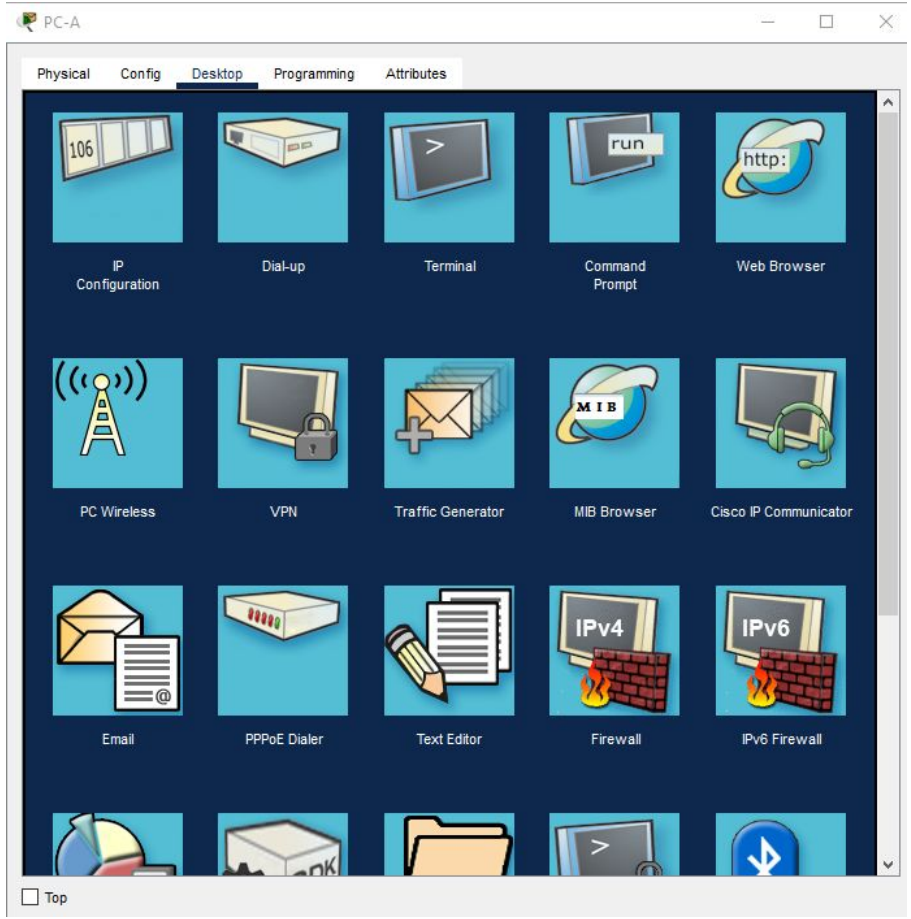
Download the same PKT file that is used in the video. Practice using the **ipconfig** and **show ip interface brief commands**, as shown in the video.



1A. Connect Console Cable From PC To Switch



1B. Use Terminal Emulation Program & Accept Defaults To Bring You To Command Line



1C. Use Enable To Enter Privileged EXEC Mode

```
Sl>enable
Sl#show ip interface
Sl#show ip interface b
Sl#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.2     YES manual administratively down down
Sl#
```

1D. Use Global Configuration Mode & Then Interface Configuration Mode To Enter No Shutdown Command

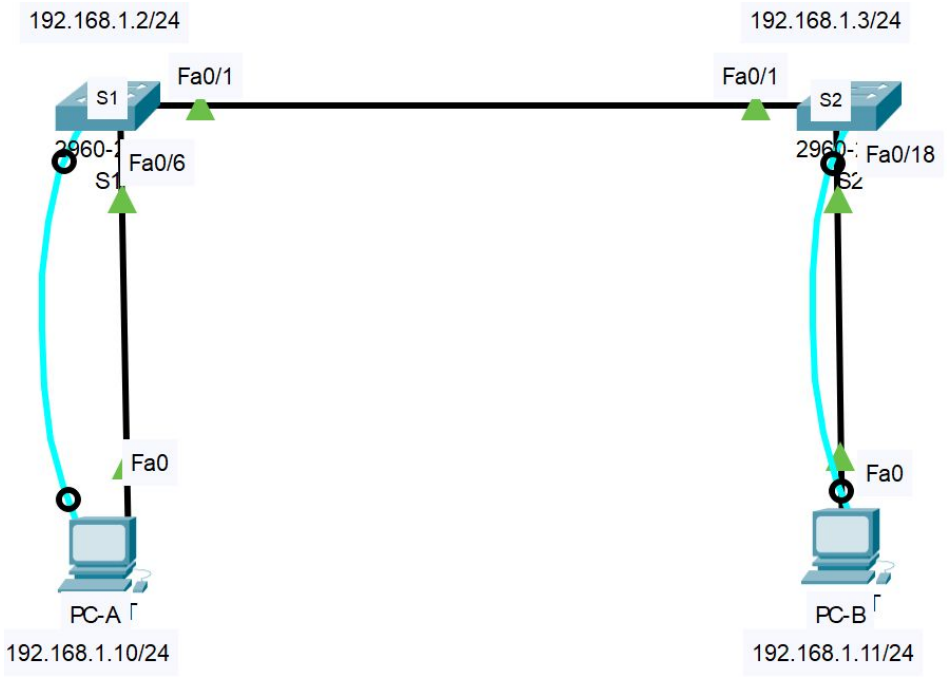
```
Sl#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sl(config)#interface vlan 1
Sl(config-if)#no shutdown

Sl(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Sl(config-if)#^Z
Sl#
%SYS-5-CONFIG_I: Configured from console by console

Sl#
```

Note: No Shutdown Command is to activate the Interface vlan1

1E. Verify The Interface is UP & UP

```
S1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.2     YES manual up                    up
S1#
```

1F. Verify The Switch Virtual Configuration On S2



1G.

- **Use Terminal Emulation Program (PC-B) & Accept Defaults To Bring You To Command Line**
- **Use Enable To Enter Privileged EXEC Mode**

Note: As you can see at the end of the output we have interface vlan1 and has not yet been assigned an IP Address.

```
S2#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual up                    up
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  unassigned      YES manual administratively down down
S2#
```

1H. Use Global Configuration Mode & Then Interface Configuration Mode To Enter No Shutdown Command

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.3 255.255.255.0

S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show ip interface brief
```

```
S2#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual up                    up
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.3     YES manual up                    up
S2#
```

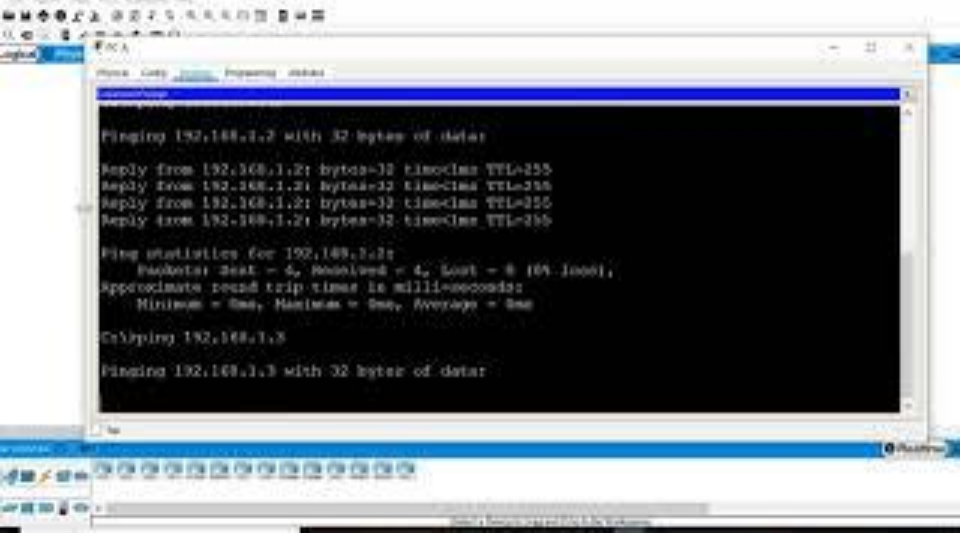
1I. Video Activity - Test End-to-End Connectivity

The ping command can be used to test connectivity to another device on the network or a website on the internet.

Click Play in the figure to view a video demonstration using the ping command to test connectivity to a switch and to another PC.

Follow Along in Packet Tracer

Download the same PKT file that is used in the video. Practice using the ping command, as shown in the video.

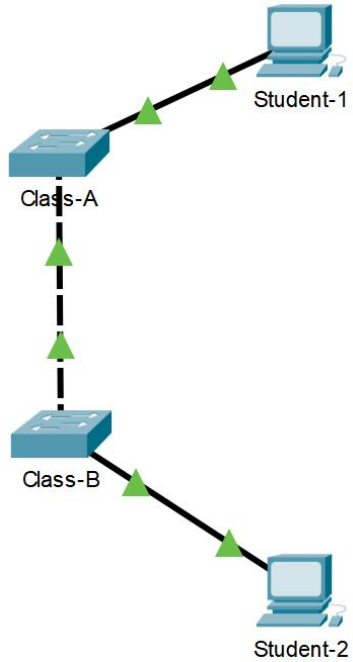


Module Practice and Quiz

1. Packet Tracer - Basic Switch and End Device Configuration

As a recently hired LAN technician, you have been asked by your network manager to demonstrate your ability to configure a small LAN. Your tasks include configuring initial settings on two switches by using the Cisco IOS and configuring IP address parameters on host devices to provide end-to-end connectivity. You are to use two switches and two hosts on a cabled and powered network.

- Download Packet Tracer (.pka) file



1A. Addressing Table

Device	Interface	IP Address	Subnet Mask
Class-A	VLAN 1	128.107.20.10	255.255.255.0
Class-B	VLAN 1	128.107.20.15	255.255.255.0
Student-1	NIC	128.107.20.25	255.255.255.0
Student-2	NIC	128.107.20.30	255.255.255.0

1B. Objectives

- Configure hostnames and IP addresses on two Cisco Internetwork Operating System (IOS) switches using the command-line interface (CLI).
- Use Cisco IOS commands to specify or limit access to the device configurations.
- Use IOS commands to save the running configuration.
- Configure two host devices with IP addresses.
- Verify connectivity between the two PC end devices.

1C. Scenario

As a recently hired LAN technician, your network manager has asked you to demonstrate your ability to configure a small LAN. Your tasks include configuring initial settings on two switches using the Cisco IOS and configuring IP address parameters on host devices to provide end-to-end connectivity. You are to use two switches and two hosts/PCs on a cabled and powered network.

1D. Instructions

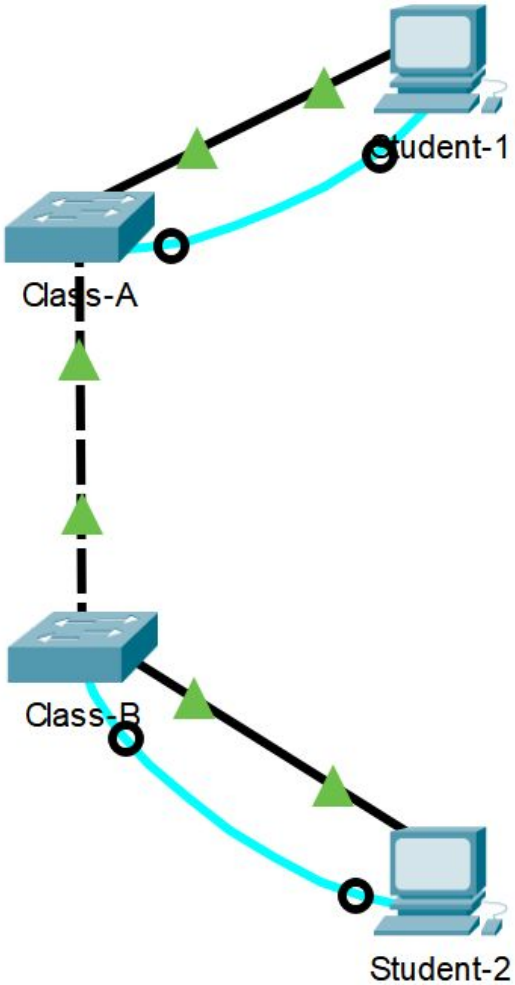
Configure the devices to fulfill the requirements below.

1E. Requirements

- Use a console connection to access each switch.
- Name **Class-A** and **Class-B** switches.
- Use the **R4Xe3** password for all lines.
- Use the **C4aJa** secret password.
- Encrypt all clear text passwords.
- Configure an appropriate message-of-the-day (MOTD) banner.
- Configure addressing for all devices according to the Addressing Table.
- Save your configurations.
- Verify connectivity between all devices.

Note: Click **Check Results** to see your progress. Click **Reset Activity** to generate a new set of requirements. If you click on this before you complete the activity, all configurations will be lost.

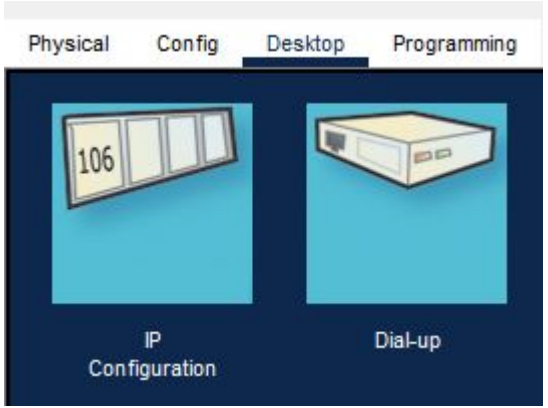
Step 1:

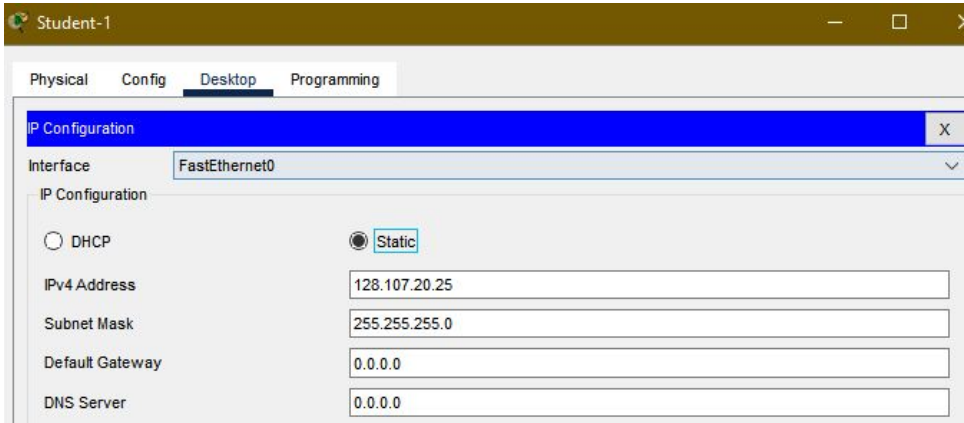


Step 2: Student-1 (Terminal)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Class-A
Class-A(config)#line console 0
Class-A(config-line)#password R4Xe3
Class-A(config-line)#exit
Class-A(config)#line vty 0 15
Class-A(config-line)#password R4Xe3
Class-A(config-line)#login
Class-A(config-line)#exit
Class-A(config)#enable secret C4aJa
Class-A(config)#service password-encryption
Class-A(config)#banner motd #Unauthorized access is strictly Prohibited#
```

Step 3: Student-1 (IP Configuration)





```
Class-A(config)#interface vlan 1
Class-A(config-if)#ip address 128.107.20.10 255.255.255.0
Class-A(config-if)#no shutdown
Class-A(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up

^Z
Class-A#

Class-A#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Class-A#
```

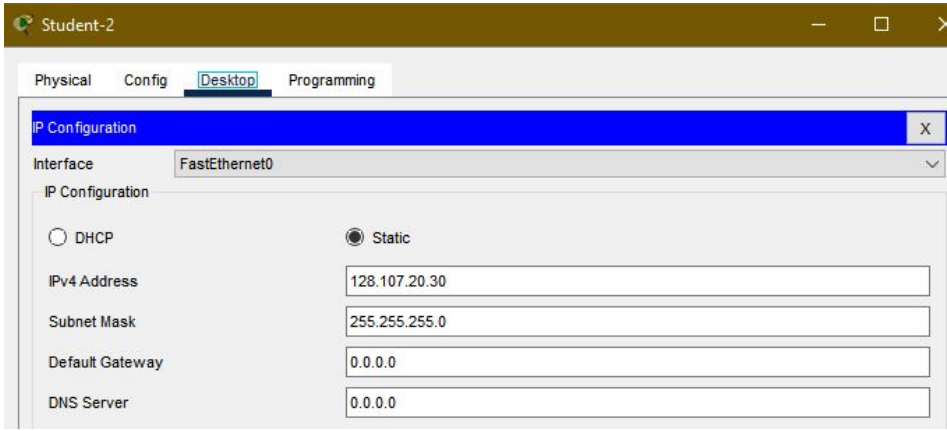
Step 4: Student-1 (Command Prompt)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 128.107.20.30

Pinging 128.107.20.30 with 32 bytes of data:

Reply from 128.107.20.30: bytes=32 time<1ms TTL=128
Reply from 128.107.20.30: bytes=32 time<1ms TTL=128
Reply from 128.107.20.30: bytes=32 time<1ms TTL=128
Reply from 128.107.20.30: bytes=32 time<1ms TTL=128

Ping statistics for 128.107.20.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Step 5: Student-2 (Terminal)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Class-B
Class-B(config)#line console 0
Class-B(config-line)#password R4Xe3
Class-B(config-line)#login
Class-B(config-line)#exit
Class-B(config)#line vty 0 15
Class-B(config-line)#password R4Xe3
Class-B(config-line)#login
Class-B(config-line)#exit
Class-B(config)#enable secret C4aJa
Class-B(config)#banner motd #Warning! Unauthorized access is strictly
Prohibited#
```

Step 6: Student-1 (IP Configuration)



```
Class-B(config)#interface vlan 1
Class-B(config-if)#ip address 128.107.20.15 255.255.255.0
Class-B(config-if)#no shutdown

Class-B(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%IP-4-DUPADDR: Duplicate address 128.107.20.15 on Vlan1, sourced by 0001.64E6.6436

^Z
Class-B#
%SYS-5-CONFIG_I: Configured from console by console

Class-B#copy running-config st
Destination filename [startup-config]?
Building configuration...
[OK]
Class-B#
```

2. Lab - Basic Switch and End Device Configuration

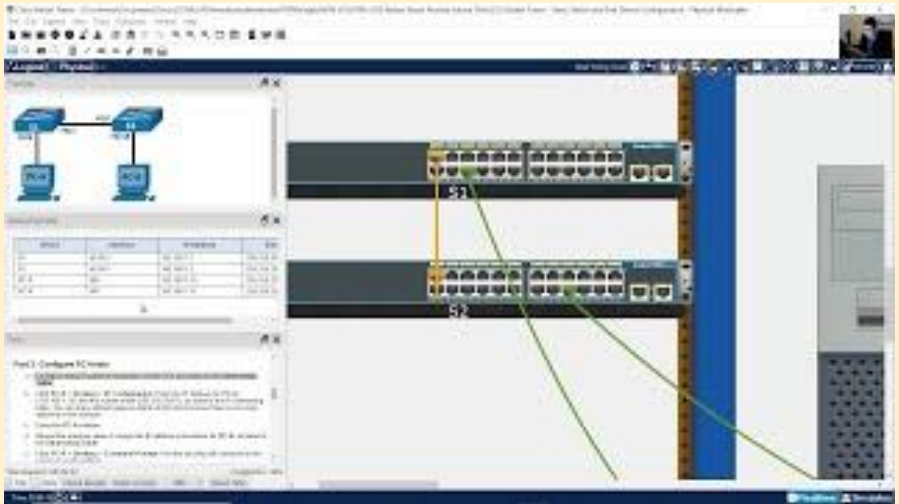
Skills Practice Opportunity

You have the opportunity to practice the following skills:

- Part 1: Set Up the Network Topology
- Part 2: Configure PC Hosts
- Part 3: Configure and Verify Basic Switch Settings

You can practice these skills using the Packet Tracer or lab equipment, if available.

Packet Tracer - Physical Mode (PTPM)



2A. Objectives

- Part 1: Set Up the Network Topology
- Part 2: Configure PC Hosts
- Part 3: Configure and Verify Basic Switch Settings

2B. Background / Scenario

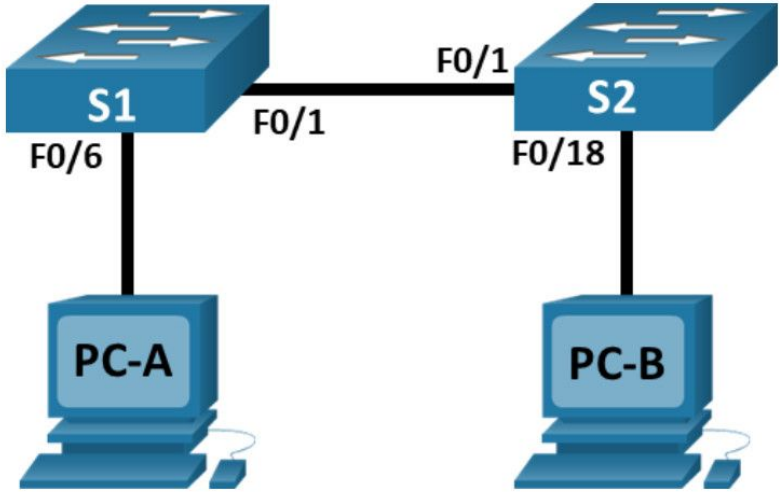
In this Packet Tracer Physical Mode (PTPM) activity, you will build a simple network with two hosts and two switches. You will also configure basic settings including hostname, local passwords, and login banner. Use show commands to display the running configuration, IOS version, and interface status. Use the copy command to save device configurations.

You will apply IP addressing for to the PCs and switches to enable communication between the devices. Use the ping utility to verify connectivity.

2C. Addressing Table

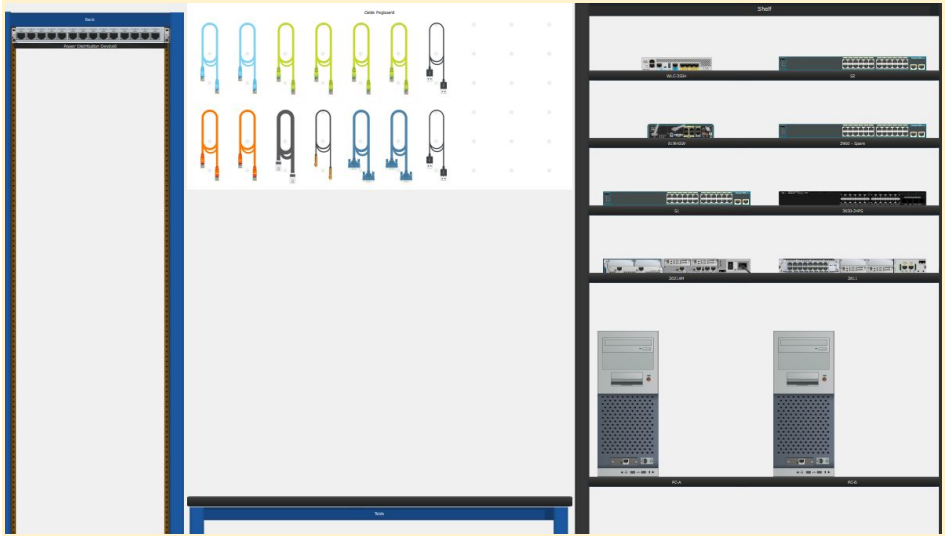
Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

2D. Topology



2E. Part 1: Set Up the Network Topology

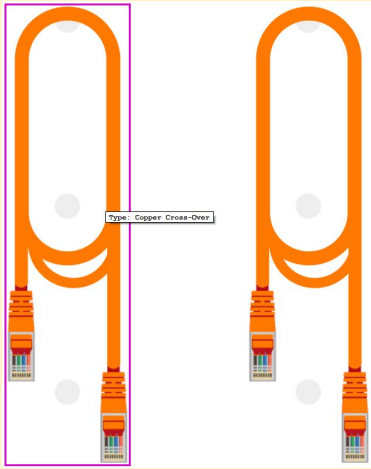
Power on the PCs and cable the devices according to the topology. To select the correct port on a switch, right click and select **Inspect Front**. Use the Zoom tool, if necessary. Float your mouse over the ports to see the port numbers. Packet Tracer will score the correct cable and port connections.

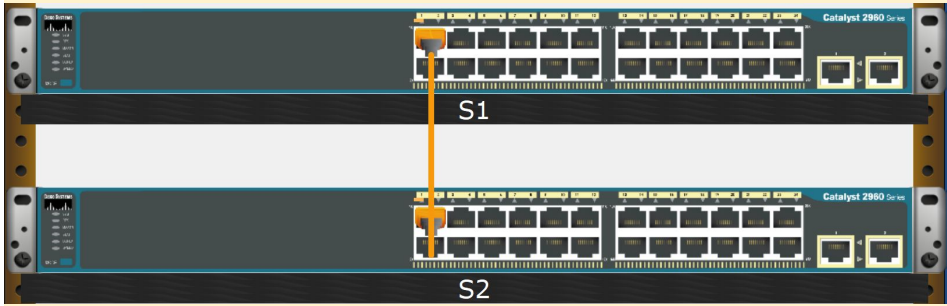


a. There are several switches, routers, and other devices on the **Shelf**. Click and drag switches **S1** and **S2** to the Rack. Click and drag two PCs to the **Table**.

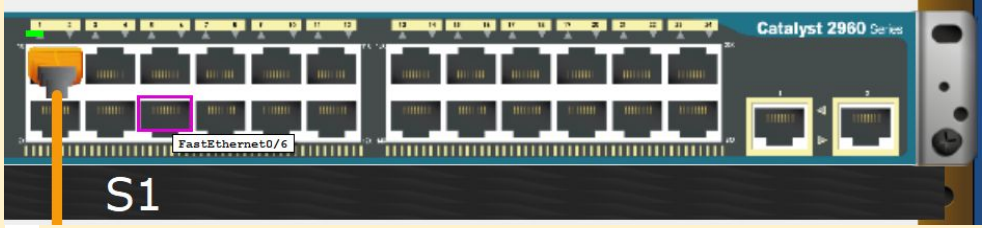
b. Power on the PCs.

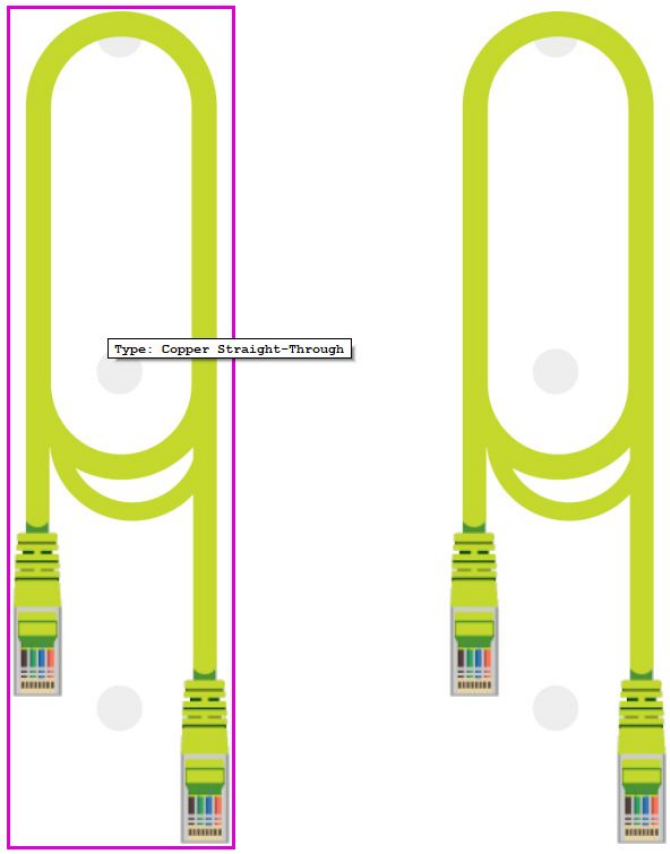
c. On the **Cable Pegboard**, click a **Copper Cross-Over** cable. Click the **FastEthernet0/1** port on **S1** and then click the **FastEthernet0/1** port on **S2** to connect them. You should see the cable connecting the two ports.

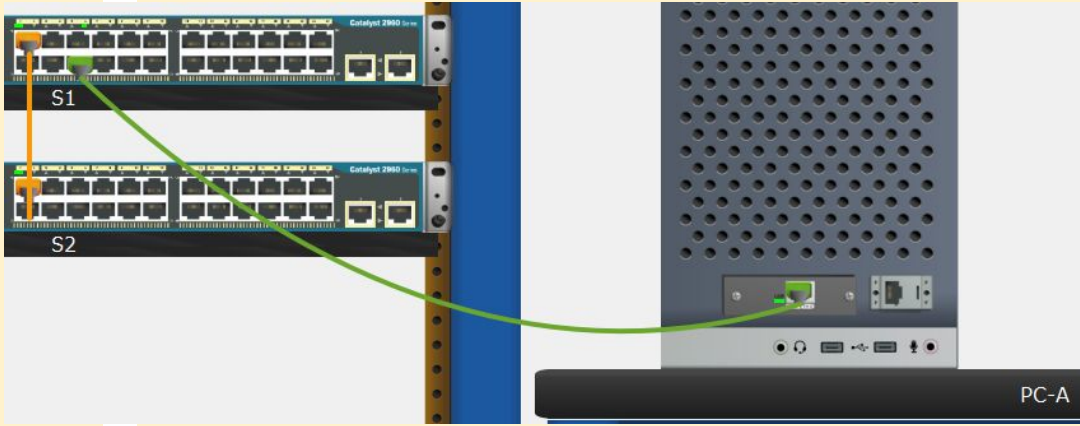




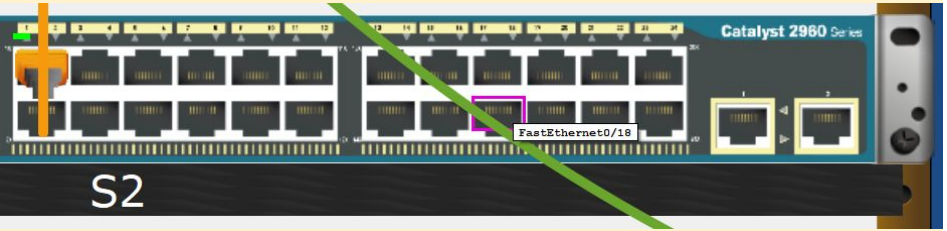
d. On the **Cable Pegboard**, click a **Copper Straight-Through** cable. Click the **FastEthernet0/6** port on **S1** and then click the **FastEthernet0** port on **PC-A** to connect them.



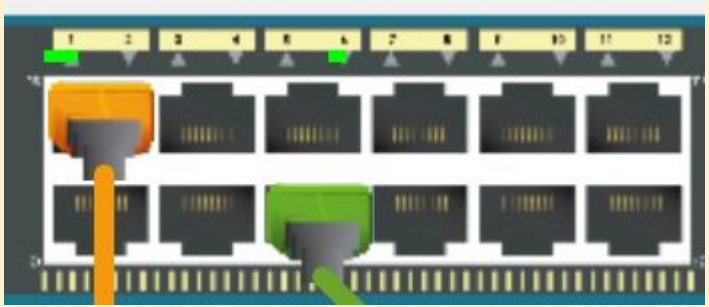




e. On the **Cable Pegboard**, click a **Copper Straight-Through** cable. Click the **FastEthernet0/18** port on **S2** and then click the **FastEthernet0** port on **PC-B** to connect them.



f. Visually inspect network connections. Initially, when you connect devices to a switch port, the link lights will be amber. After a minute or so, the link lights will turn green.

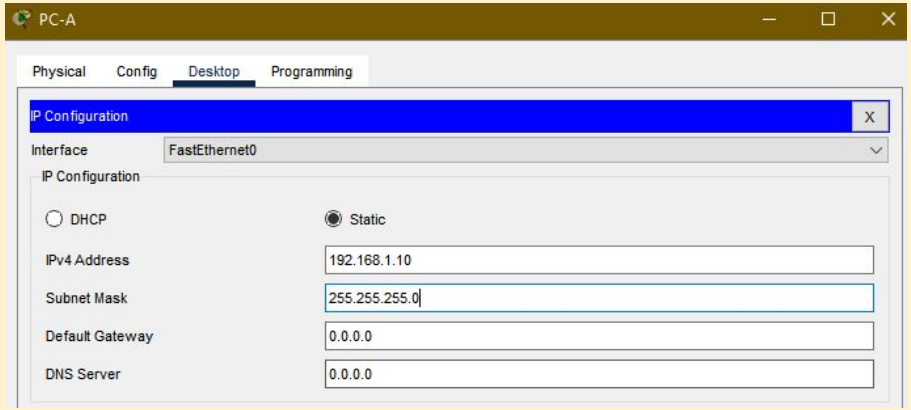


2F. Part 2: Configure PC Hosts

a. Configure static IP address information on the PCs according to the **Addressing Table**.

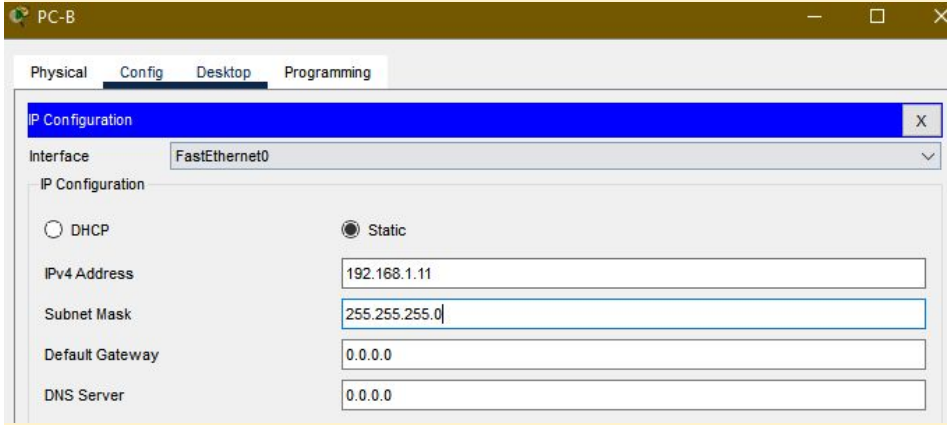
b. Click **PC-A** > **Desktop** > **IP Configuration**. Enter the IP address for **PC-A** (192.168.1.10) and the subnet mask (255.255.255.0), as listed in the IP addressing table. You can leave default gateway blank at this time because there is no router attached to the network.

c. Close the PC-A window.



d. Repeat the previous steps to assign the IP address information for **PC-B**, as listed in the **Addressing Table**.

PC-B → Desktop → IP Configuration



e. Click **PC-A** > **Desktop** > **Command Prompt**. Use the ipconfig /all command at the prompt to verify settings.

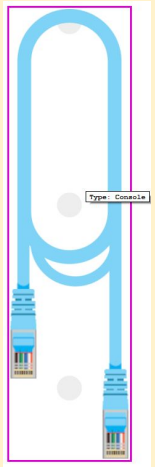
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 000A.F355.6C9E
   Link-local IPv6 Address.....: FE80::20A:F3FF:FE55:6C9E
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.10
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                         0.0.0.0
   DHCP Servers.....: 0.0.0.0
   DHCPv6 IAID.....:
                              DHCPv6          Client          DUID.....:
00-01-00-01-15-DB-75-3D-00-0A-F3-55-6C-9E
   DNS Servers.....: ::
                         0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.....: 0001.42D3.ABE6
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                         0.0.0.0
   DHCP Servers.....: 0.0.0.0
   DHCPv6 IAID.....:
                              DHCPv6          Client          DUID.....:
00-01-00-01-15-DB-75-3D-00-0A-F3-55-6C-9E
   DNS Servers.....: ::
                         0.0.0.0
```

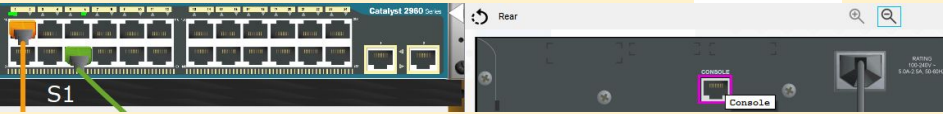
f. Enter **ping 192.168.1.11** at the prompt to test the connectivity to PC-B. The ping should be successful, as shown in the following output. If the ping is not successful, check the configurations on both of the PCs and troubleshoot as necessary.

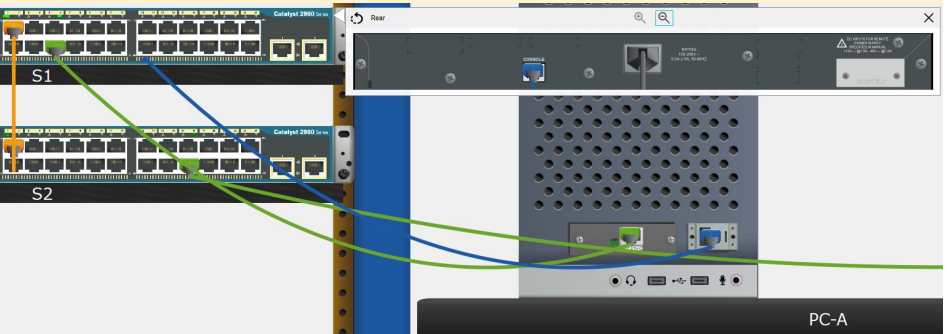
```
Packet Tracer PC Command Line 1.0

C:\> ping 192.168.1.11
Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2G. Part 3: Configure and Verify Basic Switch Settings

a. On the **Cable Pegboard**, click a **Console** cable (**For configuration**). Connect the console cable between S1 and PC-A.







b. Establish a console connection to the switch S1 from PC-A using the Packet Tracer generic Terminal program (**PC-A** > **Desktop** > **Terminal**). Press ENTER to get the **Switch>** prompt.

PC-A

Physical Config Desktop Programming

Terminal

```
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01


Switch    Ports  Model              SW Version            SW Image
------    -----  -----              ----------            ----------
*    1    26     WS-C2960-24TT      12.2                  C2960-LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state
to up


Switch>
```

c. You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the configure command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command. (PC-A)

```
Switch>enable
Switch#
```

d. The prompt changed from **Switch>** to **Switch#** which indicates privileged EXEC mode. Enter global configuration mode. (PC-A)

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

e. The prompt changed to **Switch(config)#** to reflect global configuration mode. Give the switch a name according to the **Addressing Table**. (PC-A)

```
Switch(config)#hostname S1
S1(config)#
```

f. Enter local passwords. Use **class** as the privileged EXEC password and **cisco** as the password for console access. (PC-A)

Note: **Only 1 Console Cable connected between S1 & PC-A so the line console is 0.**

```
S1(config)#line console ?
  <0-0>  First Line number
```

```
S1(config)#enable secret class
S1(config)#line console ?
  <0-0>  First Line number
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

g. Configure and enable the VLAN 1 interface according to the **Addressing Table**. (From VLAN 1 interface configure the S1 IP Address & Subnet Mask)

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.00
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#
```

h. A login banner, known as the message of the day (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated. Configure an appropriate MOTD banner to warn about unauthorized access. (PC-A)

```
S1(config-if)#exit
S1(config)#banner motd $Unauthorized Access is Prohibited!$
S1(config)#
```

i. Save the configuration to the startup file on non-volatile random access memory (NVRAM). (PC-A)

```
S1(config)#^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

j. Display the current configuration. (PC-A)

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#show r
S1#show running-config
Building configuration...

Current configuration : 1210 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
```

```
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
!
banner motd ^CUnauthorized Access is Prohibited!^C
!
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


S1#
```

k. Display the IOS version and other useful switch information. (PC-A)

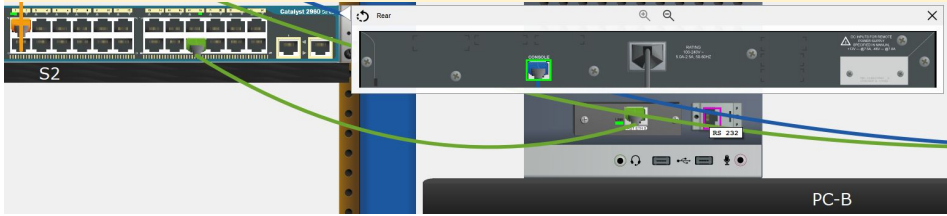
```
S1#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.


24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00E0.F780.A6A8
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01


Switch   Ports  Model          SW Version          SW Image
------   -----  -----          ----------          ----------
*    1   26     WS-C2960-24TT  12.2                C2960-LANBASE-M

Configuration register is 0xF


S1#
```

l. Display the status of the connected interfaces on the switch. (PC-A)

```
S1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.1     YES manual up                    up
S1#
```

m. Close Configuration Window.

n. Repeat the previous steps to configure switch S2. Make sure the hostname is configured as S2.




```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#enable secret class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.1.2 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up

S2(config-if)#exit
S2(config)#banner motd %Unauthorized Access is Prohibited!%
S2(config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

```
S2#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual up                    up
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.2     YES manual up                    up
S2#
```

o. Record the interface status for the following interfaces. (PC-A & PC-B)

S2#show ip interface brief

Interface	S1 Status	S1 Protocol	S2 Status	S2 Protocol
F0/1	Up	Up	Up	Up
F0/6	Up	Up	Down	Down
F0/18	Down	Down	Up	Up
VLAN 1	Up	Up	Up	Up

p. From a PC, ping S1 and S2. The pings should be successful.

PC-B ⟶ Desktop ⟶ Command Prompt

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms


C:\>
```

q. From a switch, ping PC-A (IP: 192.168.1.10) and PC-B. The pings should be successful.

PC-B ⟶ Desktop ⟶ Terminal

```
C:\>ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S2#
```

2H. Part 4: Reflection Question

a. Why are some FastEthernet ports on the switches up while others are down?

- The FastEthernet ports are up when cables are connected to the ports unless they were manually shutdown by the administrators. Otherwise, the ports would be down.

b. What could prevent a ping from being sent between the PCs?

- Wrong IP address, media disconnected, switch powered off or ports administratively down, firewall.

3. What Did I Learn In This Module?

All end devices and network devices require an operating system (OS). The user can interact with the shell using a command-line interface (CLI) to use a keyboard to run CLI-based network programs, use a keyboard to enter text and text-based commands, and view output on a monitor.

As a security feature, the Cisco IOS software separates management access into the following two command modes: User EXEC Mode and Privileged EXEC Mode.

Global configuration mode is accessed before other specific configuration modes. From global config mode, the user can enter different sub configuration modes. Each of these modes allows the configuration of a particular part or function of the IOS device.

Two common sub configuration modes include: Line Configuration Mode and Interface Configuration Mode. To move in and out of global configuration mode, use the configure terminal privileged EXEC mode command. To return to the privileged EXEC mode, enter the exit global config mode command.

Each IOS command has a specific format or syntax and can only be executed in the appropriate mode. The general syntax for a command is the command followed by any appropriate keywords and arguments. The IOS has two forms of help available: context-sensitive help and command syntax check.

The first configuration command on any device should be to give it a unique device name or hostname. Network devices should always have passwords configured to limit administrative access. Cisco IOS can be configured to use hierarchical mode passwords to allow different access privileges to a network device. Configure and encrypt all passwords. Provide a method for declaring that only authorized personnel should attempt to access the device by adding a banner to the device output.

There are two system files that store the device configuration: startup-config and running-config. Running configuration files can be altered if they have not been saved. Configuration files can also be saved and archived to a text document.

IP addresses enable devices to locate one another and establish end-to-end communication on the internet. Each end device on a network must be configured with an IP address. The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255.

IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP). In a network, DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled. To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch, use the interface vlan 1 command in global configuration mode.

In the same way that you use commands and utilities to verify a PC host's network configuration, you also use commands to verify the interfaces and address settings of intermediary devices like switches and routers. The show ip interface brief command verifies the condition of the switch interfaces. The ping command can be used to test connectivity to another device on the network or a website on the internet.

4. Module Quiz - Basic Switch and End Device Configuration

1. Which statement is true about the running configuration file in a Cisco IOS device?

(a) It should be deleted using the **erase running-config** command.

(b) It is automatically saved when the router reboots.

(c) It affects the operation of the device immediately when modified.

(d) It is stored in NVRAM.

Answer: (c) - As soon as configuration commands are entered into a router, they modify the device immediately. Running configuration files can not be deleted nor are they saved automatically.

2. Which two statements are true regarding the user EXEC mode? (Choose two.)

(a) All router commands are available.

(b) Only some aspects of the router configuration can be viewed.

(c) Global configuration mode can be accessed by entering the enable command.

(d) The device prompt for this mode ends with the “>” symbol.

(e) Interfaces and routing protocols can be configured.

Answer: (b & d) - User EXEC mode limits access to some show and debug commands. It is the first level of user interface encountered when configuring a router and is intended for investigation of certain functions of the device. The User EXEC prompt is identified with the “>” symbol.

3. Which type of access is secured on a Cisco router or switch with the enable secret command?

(a) console line

(b) virtual terminal

(c) privileged EXEC

(d) AUX port

Answer: (c) - The enable secret command secures access to the privileged EXEC mode of a Cisco router or switch.

4. What is the default SVI on a Cisco switch?

(a) VLAN1

(b) VLAN99

(c) VLAN100

(d) VLAN999

Answer: (a) - Layer 2 switches use switch virtual interfaces (SVIs) to provide a means for remote access over IP. The default SVI on a Cisco switch is VLAN1.

5. When a hostname is configured through the Cisco CLI, which three naming conventions are part of the guidelines? (Choose three.)

(a) the hostname should end with a special character

(b) the hostname should be written in all lower case characters

(c) the hostname should be fewer than 64 characters in length

(d) the hostname should contain no spaces

(e) the hostname should begin with a letter

Answer: (c, d, e) 255.255.240.0 - A hostname can be configured with upper or lower case characters and should end with a letter or digit, not a special character. A hostname should start with a letter and no space is allowed for a hostname.

6. What is the function of the shell in an OS?

(a) It interacts with the device hardware.

(b) It provides the intrusion protection services for the device.

(c) It provides dedicated firewall services.

(d) It interfaces between the users and the kernel.

Answer: (d) The size of each subnet may be different, depending on requirements. - Most operating systems contain a shell and a kernel. The kernel interacts with the hardware and the shell interfaces between the kernel and the users.

7. A router with a valid operating system contains a configuration file stored in NVRAM. The configuration file has an enable secret password but no console password. When the router boots up, which mode will display?

(a) privileged EXEC mode

(b) user EXEC mode

(c) setup mode

(d) global configuration mode

Answer: (b) - If a Cisco IOS device has a valid IOS and a valid configuration file, it will boot into user EXEC mode. A password will be required to enter privileged EXEC mode.

8. Which memory location on a Cisco router or switch will lose all content when the device is restarted?

(a) ROM

(b) NVRAM

(c) RAM

(d) flash

Answer: (c) - RAM is volatile memory and will lose all contents if the router or switch is restarted or shutdown.

9. An administrator has just changed the IP address of an interface on an IOS device. What else must be done in order to apply those changes to the device?

(a) Nothing must be done. Changes to the configuration on an IOS device take effect as soon as the command is typed correctly and the Enter key has been pressed.

(b) Reload the device and type yes when prompted to save the configuration.

(c) Copy the running configuration to the startup configuration file.

(d) Copy the information in the startup configuration file to the running configuration.

Answer: (a) - Changes to router and switch configurations take effect as soon as the command is entered. For this reason, it is very important that changes to live production devices are always carefully planned before being implemented. If commands are entered that render the device unstable or inaccessible, the device may have to be reloaded, resulting in network downtime.

10. Why would a technician enter the command copy startup-config running-config?

(a) to remove all configurations from the switch

(b) to make a changed configuration the new startup configuration

(c) to save an active configuration to NVRAM

(d) to copy an existing configuration into RAM

Answer: (d) - Usually, changes are made to a running configuration in RAM and copied to NVRAM. However, in this case, the technician wants to copy a previously saved configuration from NVRAM into RAM in order to make changes to it.?

11. Which functionality is provided by DHCP?

(a) translation of IP addresses to domain names

(b) end-to-end connectivity test

(c) remote switch management

(d) automatic assignment of an IP address to each host

Answer: (d) - DHCP provides dynamic and automatic IP address assignment to hosts.

12. Which two functions are provided to users by the context-sensitive help feature of the Cisco IOS CLI? (Choose two.)

(a) displaying a list of all available commands within the current mode

(b) selecting the best command to accomplish a task

(c) providing an error message when a wrong command is submitted

(d) determining which option, keyword, or argument is available for the entered command

(e) allowing the user to complete the remainder of an abbreviated command with the TAB key

Answer: (a & d) - Context-sensitive help provides the user with a list of commands and the arguments associated with those commands within the current mode of a networking device. A syntax checker provides error checks on submitted commands and the TAB key can be used for command completion if a partial command is entered.

13. Which memory location on a Cisco router or switch stores the startup configuration file?

(a) ROM

(b) NVRAM

(c) RAM

(d) flash

Answer: (b) - The startup configuration file of a Cisco router or switch is stored in NVRAM, which is nonvolatile memory.

14. To what subnet does the IP address 10.1.100.50 belong if a subnet mask of 255.255.0.0 is used?

(a) 10.0.0.0

(b) 10.1.100.0

(c) 10.1.100.32

(d) 10.1.0.0

Answer: (d) - The purpose of a subnet mask is to separate the network portion of the address from the host portion of the IP address. The network portion of the IP address is identified by all binary 1s in the subnet mask. Using a subnet mask of 255.255.0.0 identifies the first two octets of the IP address as the network portion.