**BASIC DEVICE CONFIGURATION**

Why should I take this module?

Welcome to Basic Device Configuration!

Welcome to the first module in **CCNA Switching, Routing, and Wireless Essentials**! You know that switches and routers come with some built-in configuration, so why would you need to learn to further configure switches and routers?

Imagine that you purchased a model train set. After you had set it up, you realized that the track was just a simple oval shape and that the train cars only ran clockwise. You might want the track to be a figure eight shape with an overpass.

You might want to have two trains that operate independently of each other and are able to move in different directions. How could you make that happen? You would need to reconfigure the track and the controls. It is the same with network devices. As a network administrator you need detailed control of the devices in your network. This means precisely configuring switches and routers so that your network does what you want it to do. This module has many Syntax Checker and Packet Tracer activities to help you develop these skills. Let’s get started!

What will I learn to do in this module?

**Module Title:** Basic Device Configuration

**Module Objective**: Configure devices using security best practices.

| Table caption | |
| --- | --- |
| **Topic Title** | **Topic Objective** |
| **Configure a Switch with Initial Settings** | Configure initial settings on a Cisco switch. |
| **Configure Switch Ports** | Configure switch ports to meet network requirements. |
| **Secure Remote Access** | Configure secure management access on a switch. |
| **Basic Router Configuration** | Configure basic settings on a router to route between two directly-connected networks, using CLI. |
| **Verify Directly Connected Networks** | Verify connectivity between two networks that are directly connected to a router. |

## Video - Download and Install Packet Tracer

This video will show you how to download and install Packet Tracer. You will use Packet Tracer to simulate creating and testing networks on your computer. Packet Tracer is a fun, take-home, flexible software program that will give you the opportunity to use the network representations and theories that you have just learned to build network models and explore relatively complex LANs and WANs.

Students commonly use Packet Tracer to:

* Prepare for a certification exam.
* Practice what they learn in networking courses.
* Sharpen their skills for a job interview.
* Examine the impact of adding new technologies into existing network designs.
* Build their skills for jobs in the Internet of Things.
* Compete in Global Design Challenges (take a look at the 2017 PT 7 Design Challenge on Facebook).

Packet Tracer is an essential learning tool used in many Cisco Networking Academy courses.

To obtain and install your copy of Cisco Packet Tracer follow these steps:

**Step 1**. Log into your Cisco Networking Academy “I'm Learning” page.  
**Step 2**. Select Resources.  
**Step 3**. Select Download Packet Tracer.  
**Step 4**. Select the version of Packet Tracer you require.  
**Step 5**. Save the file to your computer.  
**Step 6**. Launch the Packet Tracer install program.

Video - Getting Started in Cisco Packet Tracer

Packet Tracer is a tool that allows you to simulate real networks. It provides three main menus:

* You can add devices and connect them via cables or wireless.
* You can select, delete, inspect, label, and group components within your network.
* You can manage your network by opening an existing/sample network, saving your current network, and modifying your user profile or preferences.

If you have used any program such as a word processor or spreadsheet, you are already familiar with the File menu commands located in the top menu bar. The Open, Save, Save As, and Exit commands work as they would for any program, but there are two commands that are special to Packet Tracer.

The Open Samples command will display a directory of prebuilt examples of features and configurations of various network and Internet of Things devices included within Packet Tracer.

The Exit and Logout command will remove the registration information for this copy of Packet Tracer and require the next user of this copy of Packet Tracer to do the login procedure again.

Click Play in the video to learn how to use the menus and how to create your first Packet Tracer network.

1.0.5

## Packet Tracer - Logical and Physical Mode Exploration (pending 1.0.5)

The network model in this Packet Tracer Physical Mode (PTPM) activity incorporates many of the technologies that you can master in Cisco Networking Academy courses. It represents a simplified version of how a small to medium-sized business network might look.

Most of the devices in the Seward branch office and Warrenton data center are already deployed and configured. You have just been hired to review the devices and networks deployed. It is not important that you understand everything you see and do in this activity. Feel free to explore the network on your own. If you wish to proceed more systematically, follow the steps below. Answer the questions to the best of your ability.

**CONFIGURE A SWITCH WITH INITIAL SETTINGS**

## Switch Boot Sequence

Before you can configure a switch, you need to turn it on and allow it to go through the five-step boot sequence. This topic covers the basics of configuring a switch and includes a lab at the end.

After a Cisco switch is powered on, it goes through the following five-step boot sequence:

**Step 1**: First, the switch loads a ***power-on self-test (POST***) program stored in ***ROM.***

POST checks the CPU subsystem. It tests the CPU, DRAM, and the portion of the flash device that makes up the flash file system.

**Step 2**: Next, the switch loads the ***boot loader software***. The boot loader is a small program stored in ROM that is run immediately after POST successfully completes.

**Step 3**: The boot loader performs ***low-level CPU initialization***. It initializes the CPU registers, which control where physical memory is mapped, the quantity of memory, and its speed.

**Step 4**: The boot loader initializes the ***flash file system*** on the system board.

**Step 5**: Finally, the boot loader locates and loads a default IOS operating system software image into memory and gives control of the switch over to the IOS.

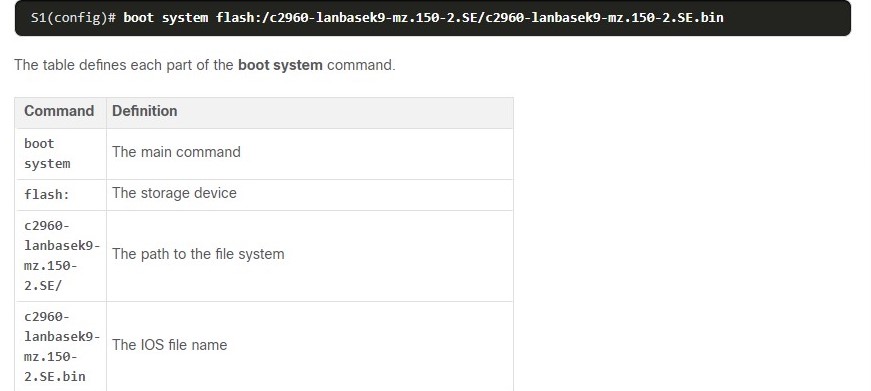
## The boot system Command

The switch attempts to automatically boot by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable file it can find.

On Catalyst 2960 Series switches, the image file is normally contained in a directory that has the same name as the image file (excluding the .bin file extension).

The IOS operating system then initializes the interfaces using the Cisco IOS commands found in the startup-config file. The startup-config file is called **config.text** and is located in flash.

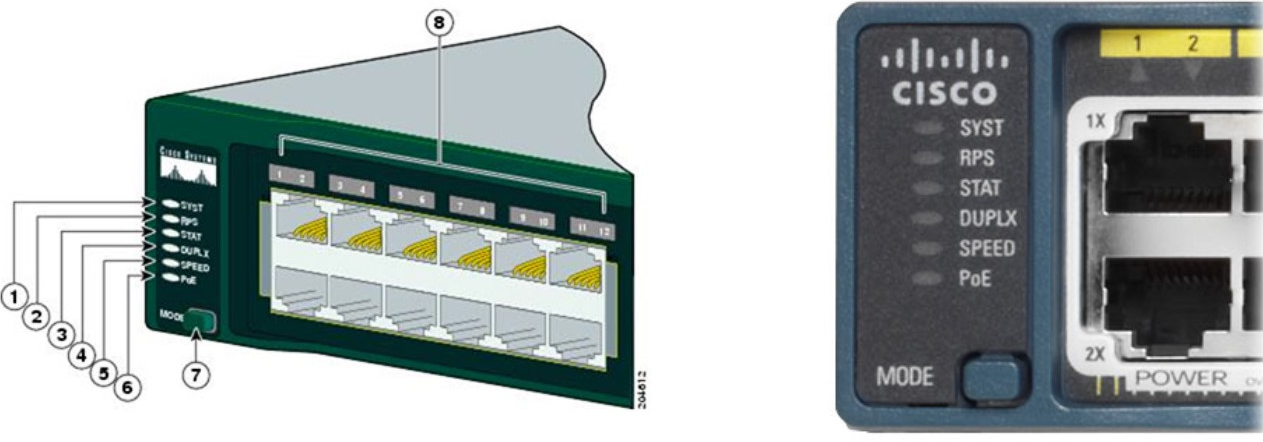
In the example, the BOOT environment variable is set using the **boot system** global configuration mode command. Notice that the IOS is located in a distinct folder and the folder path is specified. Use the command **show boot** to see what the current IOS boot file is set to.



## Switch LED Indicators

Cisco Catalyst switches have several status LED indicator lights. You can use the switch LEDs to quickly monitor switch activity and performance. Switches of different models and feature sets will have different LEDs and their placement on the front panel of the switch may also vary.

The figure shows the switch LEDs and the Mode button for a Cisco Catalyst 2960 switch.

****

The ***Mode button*** (7 in the figure) is used to ***toggle through port status***, port duplex, port speed, and if supported, the Power over Ethernet (PoE) status of the port LEDs (8 in the figure).

**System LED**

Shows whether the ***system is receiving power and is functioning properly***. If the LED is off, it means the system is not powered on. If the ***LED is green***, the system is operating normally. If the ***LED is amber***, the system is receiving power but is not functioning properly.

**Redundant Power System (RPS) LED**

Shows the RPS status. If the LED is off, the RPS is off, or it is not properly connected.

If the ***LED is green***, the RPS is connected and ready to provide backup power. If the ***LED is blinking green,*** the RPS is connected but is unavailable because it is providing power to another device.

If the ***LED is amber,*** the RPS is in standby mode, or in a fault condition.

If the ***LED is blinking amber***, the internal power supply in the switch has failed, and the RPS is providing power.

**Port Status LED**

Indicates that the port status mode is selected when the LED is green.

This is the default mode. When selected, the port LEDs will display colors with different meanings. If the LED is off, there is no link, or the port was administratively shut down.

If the LED is green, a link is present. If the LED is blinking green, there is activity and the port is sending or receiving data.

If the LED is alternating green-amber, there is a link fault. If the LED is amber, the port is blocked to ensure that a loop does not exist in the forwarding domain and is not forwarding data (typically, ports will remain in this state for the first 30 seconds after being activated).

If the LED is blinking amber, the port is blocked to prevent a possible loop in the forwarding domain.

**Port Duplex LED**

Indicates that the port duplex mode is selected when the LED is green. When selected, port LEDs that are off are in half-duplex mode. If the port LED is green, the port is in full-duplex mode.

**Port Speed LED**

Indicates that the port speed mode is selected. When selected, the port LEDs will display colors with different meanings. If the LED is off, the port is operating at 10 Mbps. If the LED is green, the port is operating at 100 Mbps. If the LED is blinking green, the port is operating at 1000 Mbps.

**Power over Ethernet (PoE) Mode LED**

If PoE is supported, a PoE mode LED will be present. If the LED is off, it indicates the PoE mode is not selected and that none of the ports have been denied power or placed in a fault condition.

If the LED is blinking amber, the PoE mode is not selected but at least one of the ports has been denied power or has a PoE fault.

If the LED is green, it indicates the PoE mode is selected and the port LEDs will display colors with different meanings.

If the port LED is off, the PoE is off. If the port LED is green, the PoE is on. If the port LED is alternating green-amber, PoE is denied because providing power to the powered device will exceed the switch power capacity. If the LED is blinking amber, PoE is off because of a fault. If the LED is amber, PoE for the port has been disabled.

## Recovering from a System Crash

The boot loader provides access into the switch if the operating system cannot be used because of missing or damaged system files. The boot loader has a command-line that provides access to the files stored in flash memory.

The boot loader can be accessed through a console connection following these steps:

**Step 1**. Connect a PC by console cable to the switch console port. Configure terminal emulation software to connect to the switch.

**Step 2**. Unplug the switch power cord.

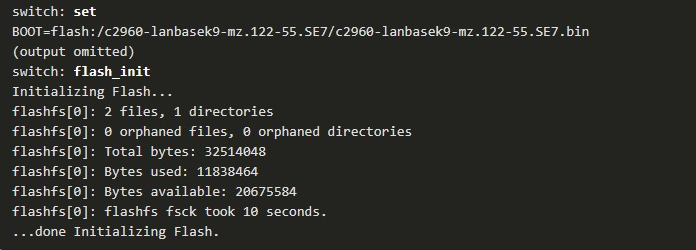
**Step 3**. Reconnect the power cord to the switch and, within 15 seconds, press and hold down the **Mode** button while the System LED is still flashing green.

**Step 4**. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; then release the **Mode** button.

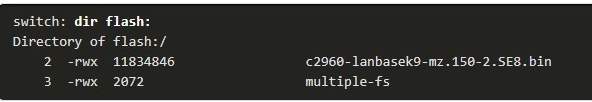
**Step 5**. The boot loader **switch:** prompt appears in the terminal emulation software on the PC.

Type the **help** or? At the boot loader prompt to view a list of available commands.

By default, the switch attempts to automatically boot up by using information in the BOOT environment variable. To view the path of the switch BOOT environment variable type the **set** command. Then, initialize the flash file system using the **flash\_init** command to view the current files in flash, as shown in the output.



After flash has finished initializing you can enter the **dir flash:** command to view the directories and files in flash, as shown in the output.



Enter the **BOOT=flash** command to change the BOOT environment variable path the switch uses to load the new IOS in flash. To verify the new BOOT environment variable path, issue the **set** command again. Finally, to load the new IOS type the **boot** command without any arguments, as shown in the output.

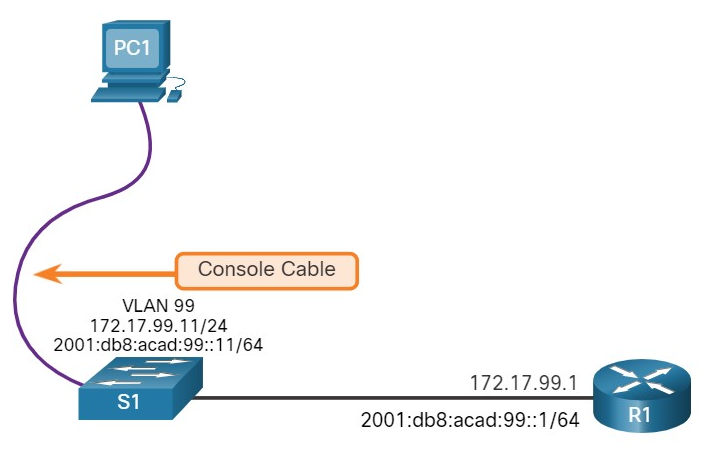


The boot loader commands support initializing flash, formatting flash, installing a new IOS, changing the BOOT environment variable and recovery of lost or forgotten passwords.

## Switch Management Access

To prepare a switch for remote management access, the switch must have a ***switch virtual interface (SVI)*** configured with an IPv4 address and subnet mask or an IPv6 address and a prefix length for IPv6.

The SVI is a virtual interface, not a physical port on the switch. Keep in mind that to manage the switch from a remote network, the switch must be configured with a default gateway. This is very similar to configuring the IP address information on host devices.



## Switch SVI Configuration Example

By default, the switch is configured to have its management controlled through VLAN 1. All ports are assigned to VLAN 1 by default. For security purposes, it is considered a best practice to use a VLAN other than VLAN 1 for the management VLAN, such as VLAN 99 in the example.

**Step 1**

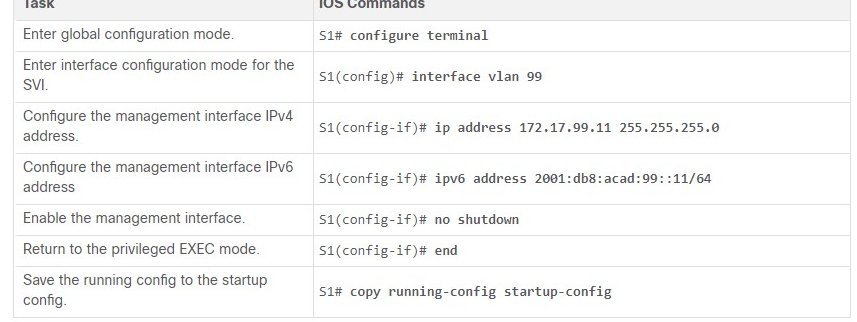
**Configure the Management Interface**

From VLAN interface configuration mode, an IPv4 address and subnet mask is applied to the management SVI of the switch.

Specifically, SVI VLAN 99 will be assigned the 172.17.99.11/24 IPv4 address and the 2001:db8:acad:99::1/64 IPv6 address as shown.

**Note**: The SVI for VLAN 99 will not appear as “up/up” until VLAN 99 is created and there is a device connected to a switch port associated with VLAN 99.

**Note**: The switch may need to be configured for IPv6. For example, before you can configure IPv6 addressing on a Cisco Catalyst 2960 running IOS version 15.0, you will need to enter the global configuration command **sdm prefer dual-ipv4-and-ipv6 default** and then **reload** the switch.

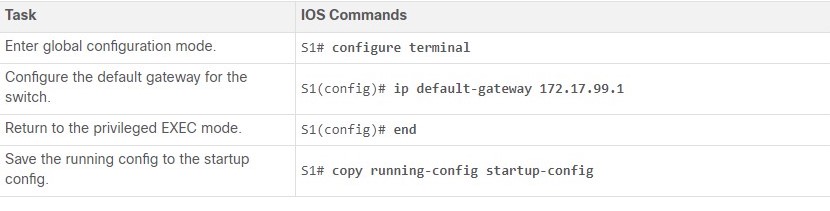


**Step 2**

**Configure the Default Gateway**

The switch should be configured with a default gateway if it will be managed remotely from networks that are not directly connected.

**Note**: Because, it will receive its default gateway information from a router advertisement (RA) message, the switch does not require an IPv6 default gateway.

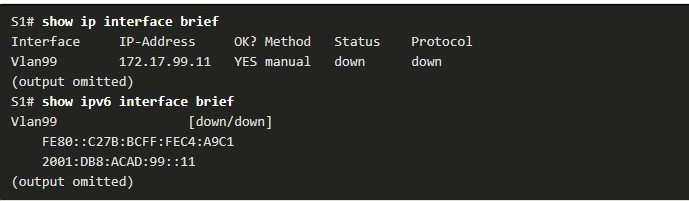


**Step 3**

**Verify Configuration**

The **show ip interface brief** and **show ipv6 interface brief** commands are useful for determining the status of both physical and virtual interfaces. The output shown confirms that interface VLAN 99 has been configured with an IPv4 and IPv6 address.

**Note**: An IP address applied to the SVI is only for remote management access to the switch; this does not allow the switch to route Layer 3 packets.



## Lab - Basic Switch Configuration(pending1.1.7)

##### **Skills Practice Opportunity**

You have the opportunity to practice the following skills:

* Part 1: Cable the Network and Verify the Default Switch Configuration
* Part 2: Configure Basic Network Device Settings
* Part 3: Verify and Test Network Connectivity

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

**CONFIGURING SWITCH PORTS**

## Duplex Communication

The ports of a switch can be configured independently for different needs. This topic covers how to configure switch ports, how to verify your configurations, common errors, and how to troubleshoot switch configuration issues.

***Full-duplex communication*** increases bandwidth efficiency by allowing both ends of a connection to transmit and receive data simultaneously. This is also known as ***bidirectional communication*** and it requires microsegmentation.

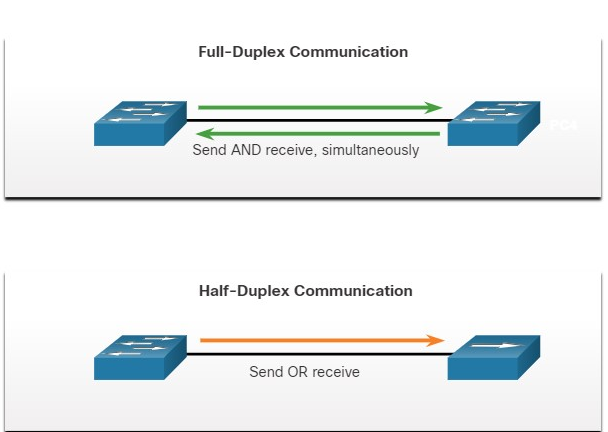
A microsegmented LAN is created when a switch port has only one device connected and is operating in full-duplex mode. There is no collision domain associated with a switch port operating in full-duplex mode.

Unlike full-duplex communication, ***half-duplex communication*** is unidirectional.

Half-duplex communication creates performance issues because data can flow in only one direction at a time, often resulting in collisions.

Half-duplex connections are typically seen in older hardware, such as hubs. Half-duplex hubs have been replaced by switches that use full-duplex communications by default.

The figure illustrates full-duplex and half-duplex communication.

****

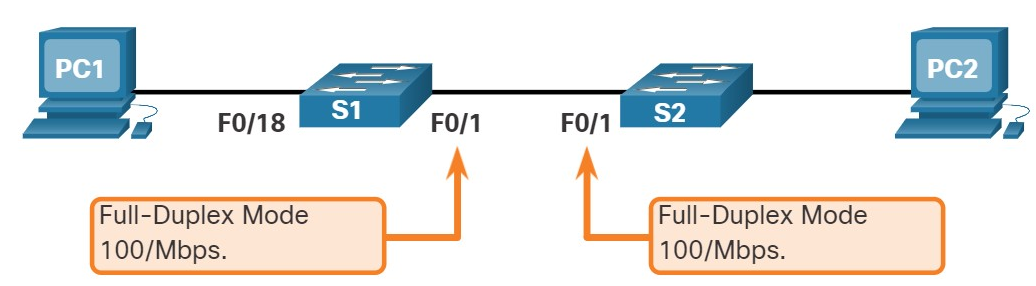
Gigabit Ethernet and 10 Gb NICs require full-duplex connections to operate.

In full-duplex mode, the collision detection circuit on the NIC is disabled. Full-duplex offers 100 percent efficiency in both directions (transmitting and receiving). This results in a doubling of the potential use of the stated bandwidth.

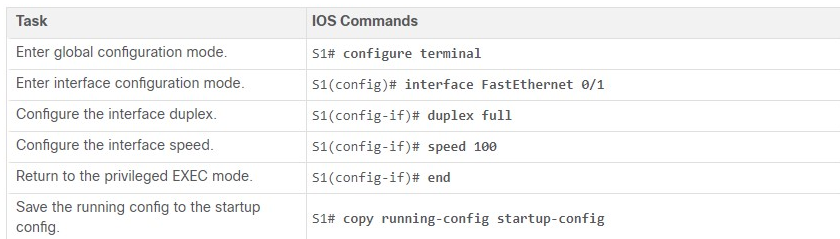
## Configure Switch Ports at the Physical Layer

Switch ports can be manually configured with specific duplex and speed settings.

Use the **duplex** interface configuration mode command to manually specify the duplex mode for a switch port. Use the **speed** interface configuration mode command to manually specify the speed. For example, both switches in the topology should always operate in full-duplex at 100 Mbps.

****

The table shows the commands for S1. The same commands can be applied to S2.

****

The default setting for both duplex and speed for switch ports on Cisco Catalyst 2960 and 3560 switches is auto.

The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps and operate only in full-duplex mode when it is set to 1000 Mbps (1 Gbps).

Autonegotiation is useful when the speed and duplex settings of the device connecting to the port are unknown or may change. When connecting to known devices such as servers, dedicated workstations, or network devices, a best practice is to manually set the speed and duplex settings.

When troubleshooting switch port issues, it is important that the duplex and speed settings should be checked.

**Note**: Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues. Autonegotiation failure creates mismatched settings.

All fiber-optic ports, such as 1000BASE-SX ports, operate only at one preset speed and are always full-duplex.

1.2.3

Auto-MDIX

Until recently, certain cable types (straight-through or crossover) were required when connecting devices.

Switch-to-switch or switch-to-router connections required using different Ethernet cables. Using the ***automatic medium-dependent interface crossover (auto-MDIX)*** feature on an interface eliminates this problem.

When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. When connecting to switches without the auto-MDIX feature, straight-through cables must be used to connect to devices such as servers, workstations, or routers. Crossover cables must be used to connect to other switches or repeaters.

With auto-MDIX enabled, either type of cable can be used to connect to other devices, and the interface automatically adjusts to communicate successfully.

On newer Cisco switches, the **mdix auto** interface configuration mode command enables the feature. When using auto-MDIX on an interface, the interface speed and duplex must be set to **auto** so that the feature operates correctly.

The command to enable auto-MDIX is issued in interface configuration mode on the switch as shown:

****

**Note**: The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches but is not available on the older Catalyst 2950 and Catalyst 3550 switches.

To examine the auto-MDIX setting for a specific interface, use the **show controllers ethernet-controller** command with the **phy** keyword.

To limit the output to lines referencing auto-MDIX, use the **include MDIX** filter. As shown the output indicates On or Off for the feature.

****

## Switch Verification Commands

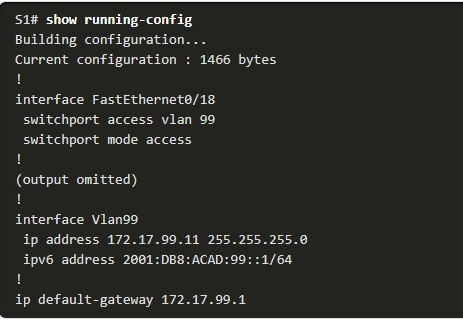
The table summarizes some of the more useful switch verification commands.

****

## Verify Switch Port Configuration

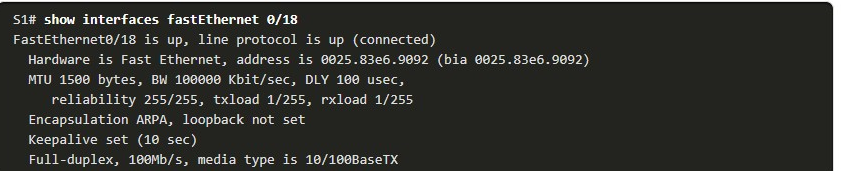
The **show running-config** command can be used to verify that the switch has been correctly configured. From the sample abbreviated output on S1, some important information is shown in the figure:

* Fast Ethernet 0/18 interface is configured with the management VLAN 99
* VLAN 99 is configured with an IPv4 address of 172.17.99.11 255.255.255.0
* The default gateway is set to 172.17.99.1

****

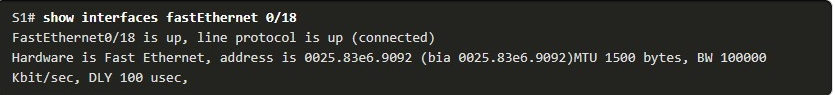
The **show interfaces** command is another commonly used command, which displays status and statistics information on the network interfaces of the switch. The **show interfaces** command is frequently used when configuring and monitoring network devices.

The first line of the output for the **show interfaces fastEthernet 0/18** command indicates that the FastEthernet 0/18 interface is up/up, meaning that it is operational. Further down, the output shows that the duplex is full and the speed is 100 Mbps.

****

## Network Access Layer Issues

The output from the **show interfaces** command is useful for detecting common media issues. One of the most important parts of this output is the display of the line and data link protocol status, as shown in the example.

****

The first parameter (FastEthernet0/18 is up) refers to the hardware layer and indicates whether the interface is receiving a carrier detect signal.

The second parameter (line protocol is up) refers to the data link layer and indicates whether the data link layer protocol keepalives are being received.

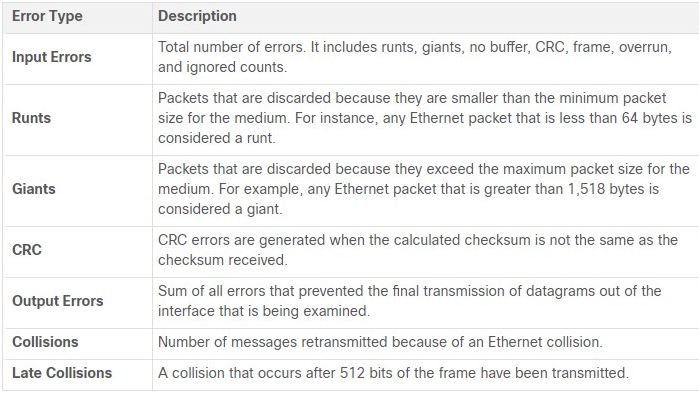
Based on the output of the **show interfaces** command, possible problems can be fixed as follows:

* If the interface is up and the line protocol is down, a problem exists. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.
* If the line protocol and the interface are both down, a cable is not attached, or some other interface problem exists. For example, in a back-to-back connection, the other end of the connection may be administratively down.
* If the interface is administratively down, it has been manually disabled (the **shutdown** command has been issued) in the active configuration.

The **show interfaces** command output displays counters and statistics for the FastEthernet0/18 interface, as highlighted in the example.

****

Some media errors are not severe enough to cause the circuit to fail but do cause network performance issues. The table explains some of these common errors which can be detected using the **show interfaces** command.

****

## Interface Input and Output Errors

“Input errors” is the sum of all errors in datagrams that were received on the interface being examined.

This includes runts, giants, CRC, no buffer, frame, overrun, and ignored counts. The reported input errors from the **show interfaces** command include the following:

* **Runt Frames** - Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts. Malfunctioning NICs are the usual cause of excessive runt frames, but they can also be caused by collisions.
* **Giants** - Ethernet frames that are larger than the maximum allowed size are called giants.
* **CRC errors** - On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or incorrect cabling. If you see many CRC errors, there is too much noise on the link and you should inspect the cable. You should also search for and eliminate noise sources.

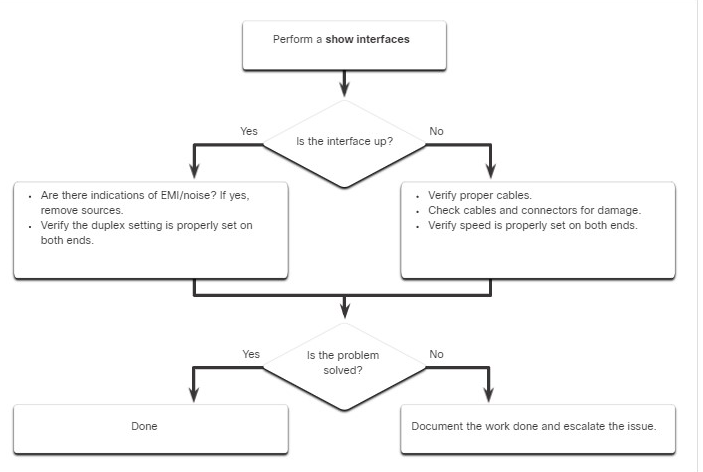
“Output errors” is the sum of all errors that prevented the final transmission of datagrams out the interface that is being examined. The reported output errors from the **show interfaces** command include the following:

* **Collisions** - Collisions in half-duplex operations are normal. However, you should never see collisions on an interface configured for full-duplex communication.
* **Late collisions** - A late collision refers to a collision that occurs after 512 bits of the frame have been transmitted. Excessive cable lengths are the most common cause of late collisions. Another common cause is duplex misconfiguration. For example, you could have one end of a connection configured for full-duplex and the other for half-duplex. You would see late collisions on the interface that is configured for half-duplex. In that case, you must configure the same duplex setting on both ends. A properly designed and configured network should never have late collisions.

## Troubleshooting Network Access Layer Issues

Most issues that affect a switched network are encountered during the original implementation. Theoretically, after it is installed, a network continues to operate without problems. However, cabling gets damaged, configurations change, and new devices are connected to the switch that require switch configuration changes. Ongoing maintenance and troubleshooting of the network infrastructure is required.

To troubleshoot scenarios involving no connection, or a bad connection, between a switch and another device, follow the general process shown in the figure.

****

Use the **show interfaces** command to check the interface status.

If the interface is down:

* Check to make sure that the proper cables are being used. Additionally, check the cable and connectors for damage. If a bad or incorrect cable is suspected, replace the cable.
* If the interface is still down, the problem may be due to a mismatch in speed setting. The speed of an interface is typically autonegotiated; therefore, even if it is manually applied to one interface, the connecting interface should autonegotiate accordingly. If a speed mismatch does occur through misconfiguration, or a hardware or software issue, then that may result in the interface going down. Manually set the same speed on both connection ends if a problem is suspected.

If the interface is up, but issues with connectivity are still present:

* Using the **show interfaces** command, check for indications of excessive noise. Indications may include an increase in the counters for runts, giants, and CRC errors. If there is excessive noise, first find and remove the source of the noise, if possible. Also, verify that the cable does not exceed the maximum cable length and check the type of cable that is used.
* If noise is not an issue, check for excessive collisions. If there are collisions or late collisions, verify the duplex settings on both ends of the connection. Much like the speed setting, the duplex setting is usually autonegotiated. If there does appear to be a duplex mismatch, manually set the duplex to full on both ends of the connection.

**SECURE REMOTE ACCESS**

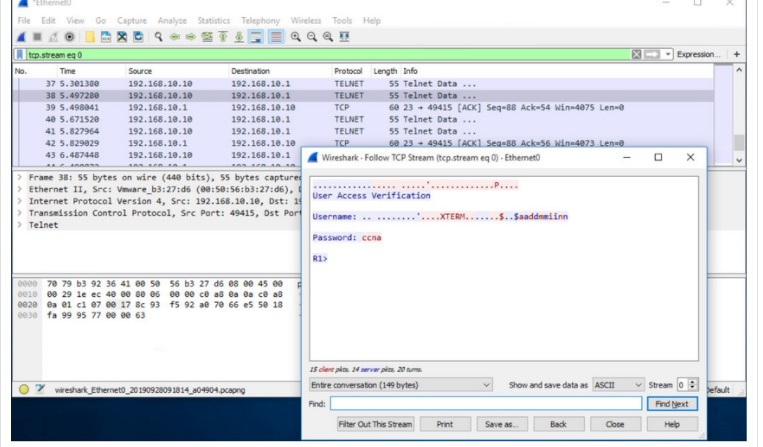
## Telnet Operation

You might not always have direct access to your switch when you need to configure it. You need to be able to access it remotely and it is imperative that your access is secure.

This topic discusses how to configure ***Secure Shell (SSH)*** for remote access. A Packet Tracer activity gives you the opportunity to try this yourself.

Telnet ***uses TCP port 23***. It is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.

A threat actor can monitor packets using Wireshark. For example, in the figure the threat actor captured the username **admin** and password **ccna** from a Telnet session.

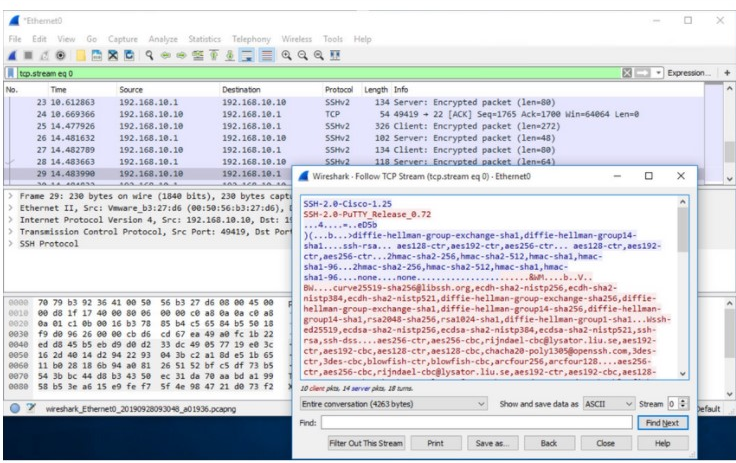
****

## SSH Operation

***Secure Shell (SSH)*** is a secure protocol that uses ***TCP port 22***. It provides a secure (encrypted) management connection to a remote device.

SSH should replace Telnet for management connections. SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices.

For example, the figure shows a Wireshark capture of an SSH session. The threat actor can track the session using the IP address of the administrator device. However, unlike Telnet, with SSH the username and password are encrypted.

****

## Verify the Switch Supports SSH

To enable SSH on a Catalyst 2960 switch, the switch must be using a version of the IOS software including cryptographic (encrypted) features and capabilities.

Use the **show version** command on the switch to see which IOS the switch is currently running. An IOS filename that includes the combination “k9” supports cryptographic (encrypted) features and capabilities. The example shows the output of the **show version** command.

## Configure SSH

Before configuring SSH, the switch must be minimally configured with a unique hostname and the correct network connectivity settings.

**Step 1**

**Verify SSH support.**

Use the **show ip ssh** command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

S1# **show ip ssh**

**Step 2**

**Configure the IP domain.**

Configure the IP domain name of the network using the **ip domain-name** domain-name global configuration mode command. In the figure, the domain-name value is **cisco.com**.

S1(config)# **ip domain-name cisco.com**

**Step 3**

**Generate RSA key pairs.**

Not all versions of the IOS default to SSH version 2, and SSH version 1 has known security flaws. To configure SSH version 2, issue the **ip ssh version 2** global configuration mode command. Generating an RSA key pair automatically enables SSH.

Use the **crypto key generate rsa** global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. The sample configuration in the figure uses a modulus size of 1,024 bits. A longer modulus length is more secure, but it takes longer to generate and to use.

**Note**: To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

S1(config)# **crypto key generate rsa** How many bits in the modulus [512]: **1024**

**Step 4**

**Configure user authentication.**

The SSH server can authenticate users locally or using an authentication server. To use the local authentication method, create a username and password pair using the **username** username **secret** password global configuration mode command. In the example, the user admin is assigned the password ccna.

S1(config)# **username admin secret ccna**

**Configure the vty lines.**

Enable the SSH protocol on the vty lines by using the **transport input ssh** line configuration mode command.

The Catalyst 2960 has vty lines ranging from 0 to 15. This configuration prevents non-SSH (such as Telnet) connections and limits the switch to accept only SSH connections. Use the **line vty** global configuration mode command and then the **login local** line configuration mode command to require local authentication for SSH connections from the local username database.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

S1(config-line)# **login local** S1(config-line)# **exit**

**Step 6**

**Enable SSH version 2.**

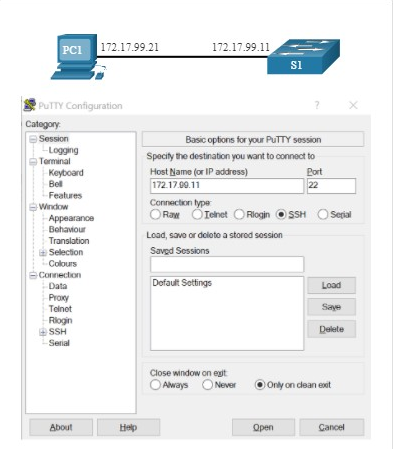
By default, SSH supports both versions 1 and 2. When supporting both versions, this is shown in the **show ip ssh** output as supporting version 2. Enable SSH version using the **ip ssh version 2** global configuration command.

## Verify SSH is Operational

On a PC, an SSH client such as PuTTY, is used to connect to an SSH server. For example, assume the following is configured:

* SSH is enabled on switch S1
* Interface VLAN 99 (SVI) with IPv4 address 172.17.99.11 on switch S1
* PC1 with IPv4 address 172.17.99.21

The figure shows the PuTTY settings for PC1 to initiate an SSH connection to the SVI VLAN IPv4 address of S1.

****

When connected, the user is prompted for a username and password as shown in the example. Using the configuration from the previous example, the username **admin** and password **ccna** are entered.

After entering the correct combination, the user is connected via SSH to the command line interface (CLI) on the Catalyst 2960 switch.

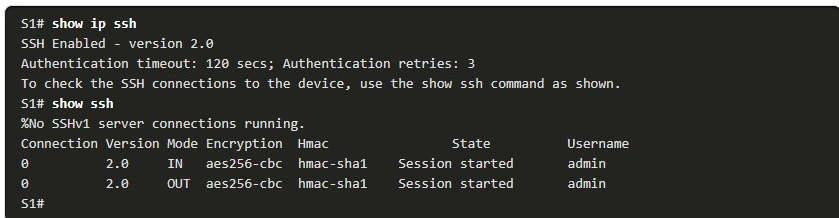
Login as: **admin**

Using keyboard-interactive Authentication.

Password:

S1> **enable** Password: S1#

To display the version and configuration data for SSH on the device that you configured as an SSH server, use the **show ip ssh** command. In the example, SSH version 2 is enabled.

****

## Packet Tracer - Configure SSH(pending 1.3.6)

SSH should replace Telnet for management connections. Telnet uses insecure plaintext communications.

SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

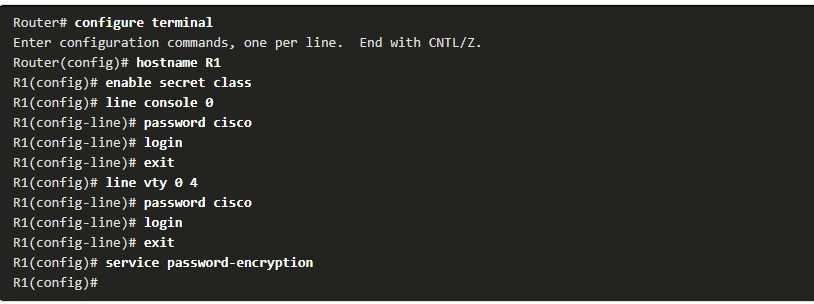
**BASIC ROUTER CONFIGURATIONS**

## Configure Basic Router Settings

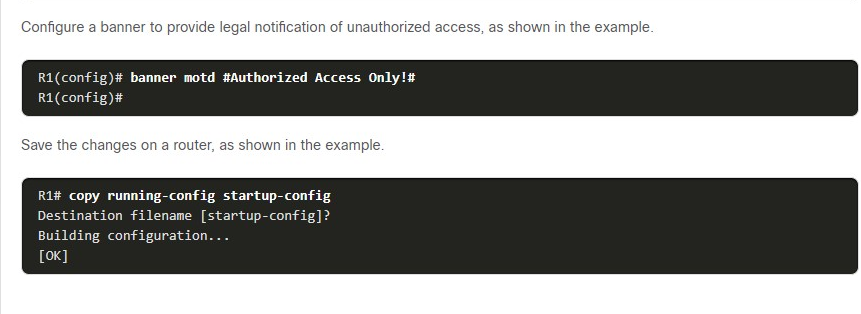
Up to now, this module has only covered switches. If you want devices to be able to send and receive data outside of your network, you will have to configure routers. This topic teaches you basic router configuration and provides two Syntax Checkers and a Packet Tracer activity so you can practice these skills.

**Cisco routers** and **Cisco switches** have many similarities. They support a similar modal operating system, similar command structures, and many of the same commands.

In addition, both devices have similar initial configuration steps. For example, the following configuration tasks should always be performed. Name the device to distinguish it from other routers and configure passwords, as shown in the example.

****

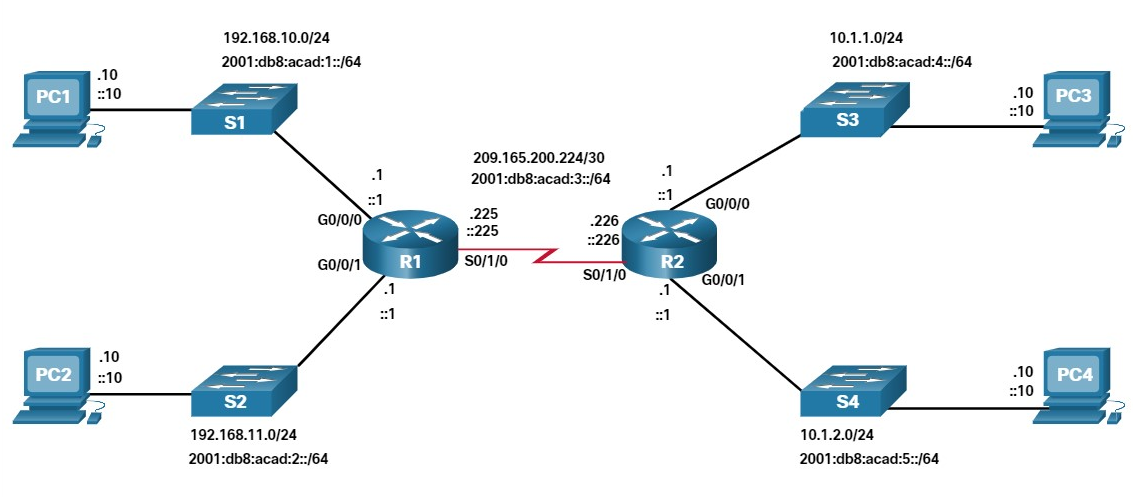
Configure a banner to provide legal notification of unauthorized access, as shown in the example.

****

## Dual Stack Topology

One distinguishing feature between switches and routers is the type of interfaces supported by each. For example, Layer 2 switches support LANs; therefore, they have multiple FastEthernet or Gigabit Ethernet ports.

The dual stack topology in the figure is used to demonstrate the configuration of router IPv4 and IPv6 interfaces.

****

Configure Router Interfaces

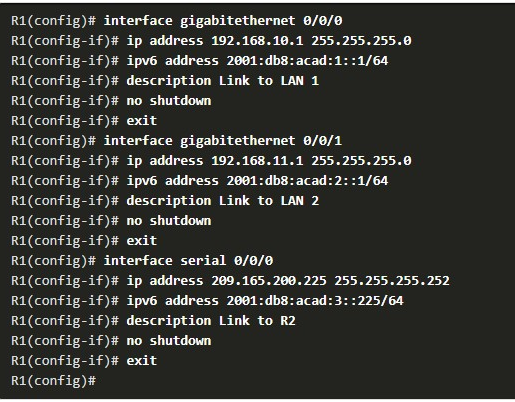
Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces.

For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and High-Speed WAN Interface Card (HWIC) slots to accommodate other types of network interfaces, including serial, DSL, and cable interfaces.

To be available, an interface must be:

* **Configured with at least one IP address** - Use the **ip address** *ip-address subnet-mask* and the **ipv6 address** *ipv6-address/prefix* interface configuration commands.
* **Activated** - By default, LAN and WAN interfaces are not activated (**shutdown**). To enable an interface, it must be activated using the **no shutdown** command. (This is similar to powering on the interface.) The interface must also be connected to another device (a hub, a switch, or another router) for the physical layer to be active.
* **Description** - Optionally, the interface could also be configured with a short description of up to 240 characters. It is good practice to configure a description on each interface. On production networks, the benefits of interface descriptions are quickly realized as they are helpful in troubleshooting and in identifying a third-party connection and contact information.

The following example shows the configuration for the interfaces on R1.

****

## IPv4 Loopback Interfaces

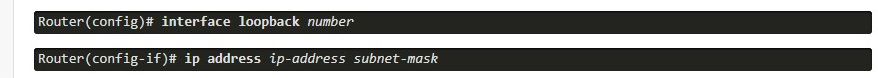
Another common configuration of Cisco IOS routers is enabling a loopback interface.

The loopback interface is a logical interface that is internal to the router. It is not assigned to a physical port and can never be connected to any other device. It is considered a software interface that is automatically placed in an “up” state, as long as the router is functioning.

The loopback interface is useful in testing and managing a Cisco IOS device because it ensures that at least one interface will always be available. For example, it can be used for testing purposes, such as testing internal routing processes, by emulating networks behind the router.

Loopback interfaces are also commonly used in lab environments to create additional interfaces. For example, you can create multiple loopback interfaces on a router to simulate more networks for configuration practice and testing purposes. In this curriculum, we often use a loopback interface to simulate a link to the internet.

Enabling and assigning a loopback address is simple:

****

Multiple loopback interfaces can be enabled on a router. The IPv4 address for each loopback interface must be unique and unused by any other interface, as shown in the example configuration of loopback interface 0 on R1.

## Packet Tracer- Configure Router Interfaces (pending 1.4.7)

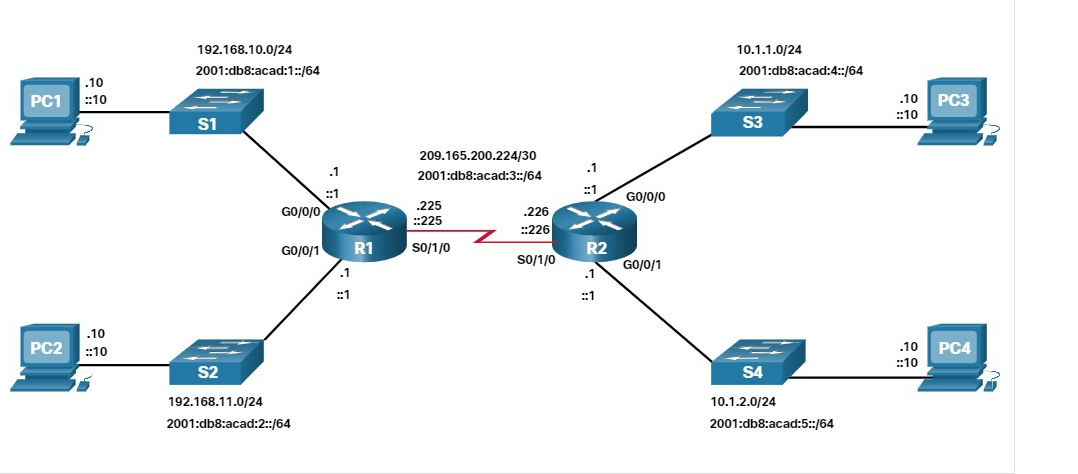
In this Packet Tracer activity, you will configure routers with IPv4 and IPv6 addressing.

**VERIFY DIRECTLY CONNECTED NETWORKS**

## Interface Verification Commands

There is no point in configuring your router unless you verify the configuration and connectivity. This topic covers the commands to use to verify directly connected networks. It includes two Syntax Checkers and a Packet Tracer.

There are several **show** commands that can be used to verify the operation and configuration of an interface. The topology in the figure is used to demonstrate the verification of router interface settings.

****

The following commands are especially useful to quickly identify the status of an interface:

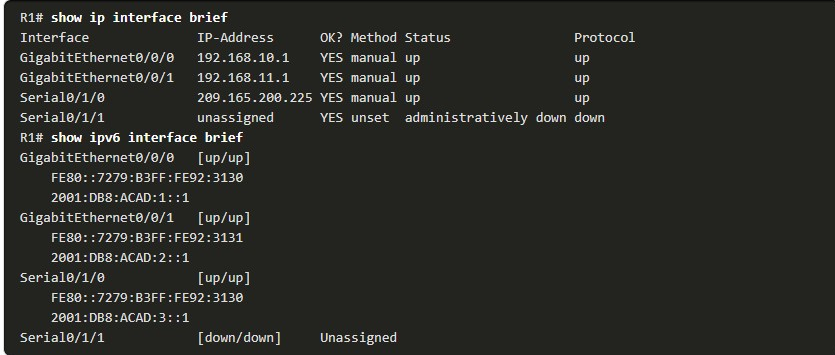
* **Show ip interface brief** and **show ipv6 interface brief** - These display a summary for all ***interfaces*** including the IPv4 or IPv6 address of the interface and current operational status.
* **show running-config interface** *interface-id* - This displays the commands applied to the specified interface.
* **show ip route** and **show ipv6 route** - These display the contents of the IPv4 or IPv6 routing table stored in RAM.

In Cisco IOS 15, active interfaces should appear in the routing table with two related entries identified by the code ‘**C**’ (Connected) or ‘**L**’ (Local). In previous IOS versions, only a single entry with the code ‘**C**’ will appear.

## Verify Interface Status

The output of the **show ip interface brief** and **show ipv6 interface brief** commands can be used to quickly reveal the status of all interfaces on the router.

You can verify that the interfaces are active and operational as indicated by the Status of “up” and Protocol of “up”, as shown in the example. A different output would indicate a problem with either the configuration or the cabling.

****

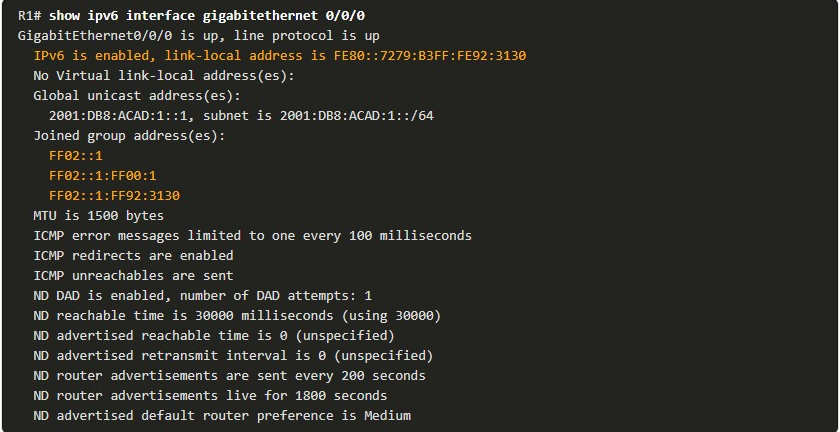
## Verify IPv6 Link Local and Multicast Addresses

The output of the **show ipv6 interface brief** command displays two configured IPv6 addresses per interface. One address is the IPv6 global unicast address that was manually entered.

The other address, which begins with FE80, is the ***link-local unicast*** address for the interface. A link-local address is automatically added to an interface whenever a global unicast address is assigned.

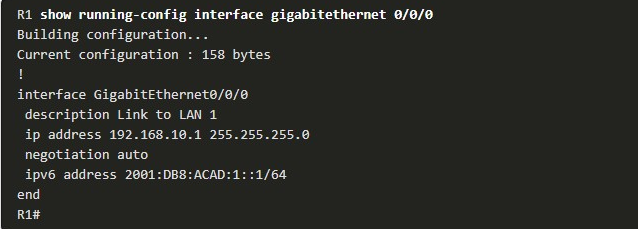
An IPv6 network interface is required to have a link-local address, but not necessarily a global unicast address.

The **show ipv6 interface gigabitethernet 0/0/0 c**ommand displays the interface status and all of the IPv6 addresses belonging to the interface. Along with the link local address and global unicast address, the output includes the multicast addresses assigned to the interface, beginning with prefix FF02, as shown in the example.

****

## Verify Interface Configuration

The output of the **show running-config interface** command displays the current commands applied to the specified interface as shown.

****

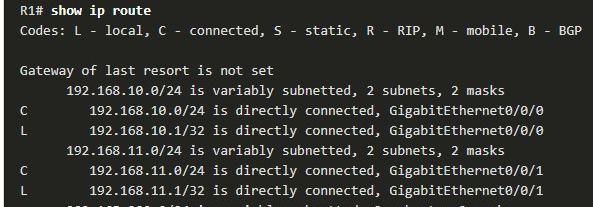
The following two commands are used to gather more detailed interface information:

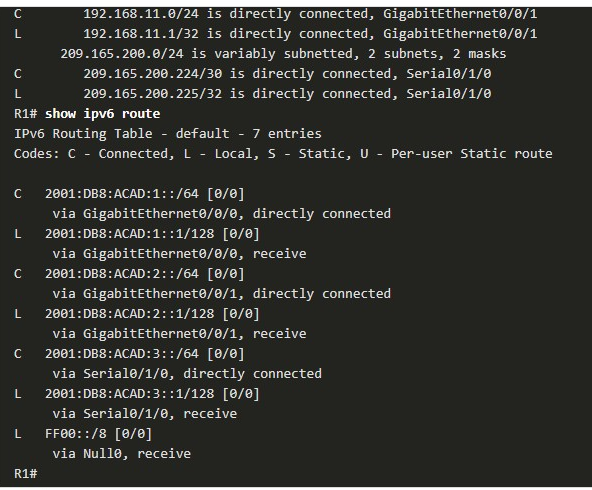
* **show interfaces**- Displays interface information and packet flow count for all interfaces on the device.
* **show ip interface** and **show ipv6 interface** - Displays the IPv4 and IPv6 related information for all interfaces on a router.

## Verify Routes

The output of the **show ip route** and **show ipv6 route** commands reveal the three directly connected network entries and the three local host route interface entries, as shown in the example.

The local host route has an administrative distance of 0. It also has a /32 mask for IPv4, and a /128 mask for IPv6. The local host route is for routes on the router that owns the IP address. It is used to allow the router to process packets destined to that IP.

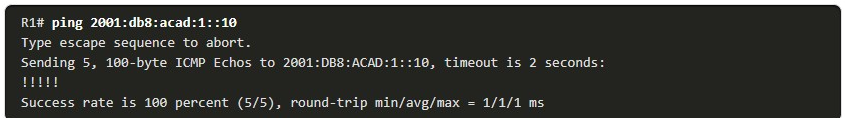


****

A ‘**C**’ next to a route within the routing table indicates that this is a ***directly connected network***. When the router interface is configured with a global unicast address and is in the “up/up” state, the IPv6 prefix and prefix length are added to the IPv6 routing table as a connected route.

The IPv6 global unicast address applied to the interface is also installed in the routing table as a local route. The local route has a /128 prefix. Local routes are used by the routing table to efficiently process packets with the interface address of the router as the destination.

The **ping** command for IPv6 is identical to the command used with IPv4 except that an IPv6 address is used. As shown in the example, the **ping** command is used to verify Layer 3 connectivity between R1 and PC1.



## Filter Show Command Output

Commands that generate multiple screens of output are, by default, paused after 24 lines.

At the end of the paused output, the --More-- text displays. Pressing **Enter** displays the next line and pressing the spacebar displays the next set of lines.

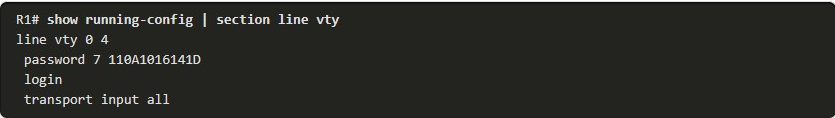
Use the **terminal length** command to specify the number of lines to be displayed. A value of 0 (zero) prevents the router from pausing between screens of output.

Another very useful feature that improves the user experience in the CLI is the filtering of **show** output. Filtering commands can be used to display specific sections of output. To enable the filtering command, enter a pipe (**|**) character after the **show** command and then enter a filtering parameter and a filtering expression.

There are four filtering parameters that can be configured after the pipe.

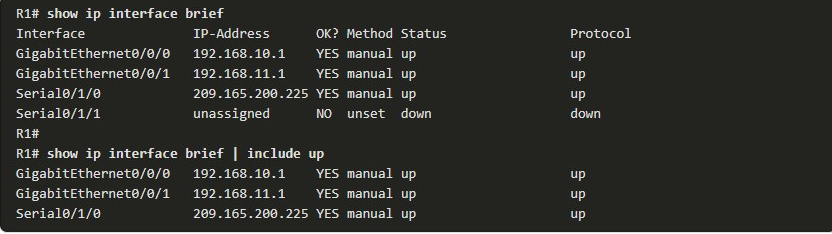
**Section**

Shows the entire section that starts with the filtering expression, as shown in the example.



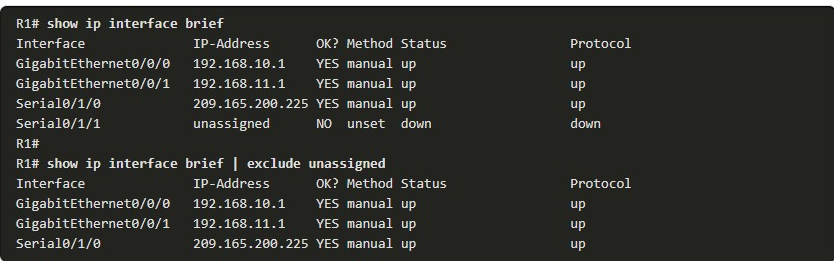
**Include**

Includes all output lines that match the filtering expression, as shown in the example.



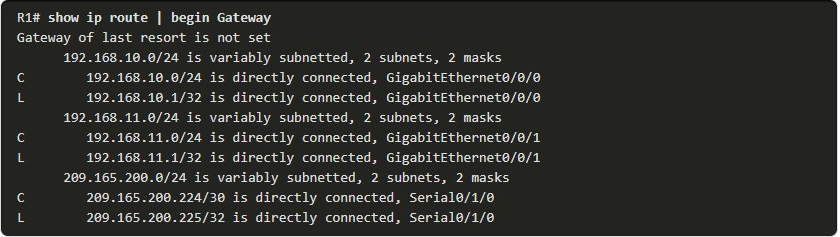
**Exclude**

Excludes all output lines that match the filtering expression, as shown in the example.



**Begin**

Shows all the output lines from a certain point, starting with the line that matches the filtering expression, as shown in the example.



**Note**: Output filters can be used in combination with any **show** command.

## Command History Feature

The command history feature is useful because it temporarily stores the list of executed commands to be recalled.

To recall commands in the history buffer, press **Ctrl**+**P** or the **Up Arrow** key.

The command output begins with the most recent command. Repeat the key sequence to recall successively older commands.

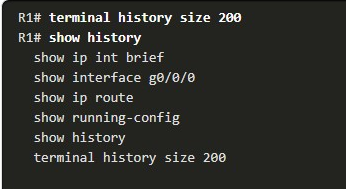
To return to more recent commands in the history buffer, press **Ctrl**+**N** or the **Down Arrow** key. Repeat the key sequence to recall successively more recent commands.

By default, command history is enabled and the system captures the last 10 command lines in its history buffer. Use the **show history** privileged EXEC command to display the contents of the buffer.

It is also practical to increase the number of command lines that the history buffer records during the current terminal session only.

Use the **terminal history size** user EXEC command to increase or decrease the size of the buffer.

An example of the **terminal history size** and **show history** commands is shown in the figure.



1.5.10

## Packet Tracer - Verify Directly Connected Networks(pending 1.5.10)

In this Packet Tracer activity, routers R1 and R2 each have two LANs. Your task is to verify the addressing on each device and verify connectivity between the LANs

1. Which command will display a summary of all IPv6-enabled interfaces on a router that includes the IPv6 address and operational status?



**show ip interface brief**



**show ipv6 route**



**show running-config interface**



**show ipv6 interface brief**

**ANS: The command to view a summary of IPv6-enabled interfaces along with their IPv6 address and operational status is show ipv6 interface brief. show ip interface brief will give the same information but for IPv4. show ip route and show running-config interface will not give the information requested.**

1. When verifying routes, what code is used to identify directly connected routes in the routing table?



C



D



L



R

**ANS: Directly connected routes will have a route code of "C" in the routing table. Routes with "D" indicate an EIGRP learned route. Routes with "L" indicate a local route and "R" indicates a RIP-learned route. RIP stands for Routing Information Protocol, which is one of the first routing protocols.**

1. Which command will display packet flow counts, collisions, and buffer failures on an interface?



**show interface**



**show ip interface**



**show running-config interface**

**ANS: The show interface command will display lots of packet flow information such as counts, collisions, and buffer failures. The show ip interface and show running-config interface commands give a lot of information as well but not packet flow information**.

1. An IPv6-enabled interface is required to have which type of address?



loopback



global unicast



link-local



Static

**ANS: All IPv6-enabled interfaces are required to have at least a link-local address. If one is not manually configured, then the interface will automatically generate one.**

1. What character is used to enable the filtering of commands?



pipe |



comma ,



colon :



semi colon ;

**ANS: The pipe character when used with commands enables filtering of the command output.**

1. Which filtering expression will show all output lines starting from the line matching the filtering expression?



section



begin



include

**ANS: While all three expressions will show matching output lines, the begin expression will show all output lines starting from the line matching the filter expression. The include expression shows all output lines that match the filter expression, and the section expression includes the entire section that starts with the filter expression.**

1.6.1

## Packet Tracer - Implement a Small Network

## (pending 1.6.1)

In this Packet Tracer activity, routers R1 and R2 each have two LANs. Your task is to verify the addressing on each device and verify connectivity between the LANs.

1.6.2

## Lab - Configure Basic Router Settings

##### **Skills Practice Opportunity**

You have the opportunity to practice the following skills:

* Part 1: Set Up the Topology and Initialize Devices
* Part 2: Configure Devices and Verify Connectivity
* Part 3: Display Router Information

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

**Packet Tracer - Physical Mode (PTPM)**

## What did I learn in this module?

**Configure a Switch with Initial Settings**

After a Cisco switch is powered on, it goes through a five-step boot sequence.

The BOOT environment variable is set using the **boot system** global configuration mode command. The IOS is located in a distinct folder and the folder path is specified.

Use the switch LEDs to monitor switch activity and performance: SYST, RPS, STAT, DUPLX, SPEED, and PoE.

The ***boot loader*** provides access into the switch if the operating system cannot be used because of missing or damaged system files.

The boot loader has a command line that provides access to the files stored in flash memory. To prepare a switch for remote management access, the switch must be configured with an IP address and a subnet mask.

To manage the switch from a remote network, the switch must be configured with a default gateway.

To configure the switch SVI, you must first configure the management interface, then configure the default gateway, and finally, verify your configuration.

**Configure Switch Ports**

Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously.

Half-duplex communication is unidirectional. Switch ports can be manually configured with specific duplex and speed settings.

Use autonegotiation when the speed and duplex settings of the device connecting to the port are unknown or may change.

When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.

There are several **show** commands to use when verifying switch configurations. Use the **show running-config** command and the **show interfaces** command to verify a switch port configuration.

The output from the **show interfaces** command is also useful for detecting common network access layer issues because it displays the line and data link protocol status.

The reported input errors from the **show interfaces** command include: runt frames, giants, CRC errors, along with collisions and late collisions. Use **show interfaces** to determine if your network has no connection or a bad connection between a switch and another device.

**Secure Remote Access**

Telnet (using TCP port 23) is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.

SSH (using TCP port 22) is a secure protocol that provides an encrypted management connection to a remote device.

SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices.

Use the **show version** command on the switch to see which IOS the switch is currently running. An IOS filename that includes the combination “k9” supports cryptographic features and capabilities.

To configure SSH you must verify that the switch supports it, configure the IP domain, generate RSA key pairs, configure use authentication, configure the VTY lines, and enable SSH version 2. To verify that SSH is operational, use the **show ip ssh** command to display the version and configuration data for SSH on the device.

**Basic Router Configuration**

The following initial configuration tasks should always be performed: name the device to distinguish it from other routers and configure passwords, configure a banner to provide legal notification of unauthorized access, and save the changes on a router.

One distinguishing feature between switches and routers is the type of interfaces supported by each. For example, Layer 2 switches support LANs and, therefore, have multiple FastEthernet or Gigabit Ethernet ports.

The dual stack topology is used to demonstrate the configuration of router IPv4 and IPv6 interfaces. Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces.

For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and High-Speed WAN Interface Card (HWIC) slots to accommodate other types of network interfaces, including serial, DSL, and cable interfaces. The IPv4 loopback interface is a logical interface that is internal to the router. It is not assigned to a physical port and can never be connected to any other device.

**Verify Directly Connected Networks**

Use the following commands to quickly identify the status of an interface:

* **show ip interface brief** and **show ipv6 interface brief** to see summary all interfaces (IPv4 and IPv6 addresses and operational status),
* **show running-config interface interface-id** to see the commands applied to a specified interface,
* **Show ip route** and **show ipv6 route** to see the contents of the IPv4 or IPv6 routing table stored in RAM.

The output of the **show ip interface brief** and **show ipv6 interface brief** commands can be used to quickly reveal the status of all interfaces on the router.

The **show ipv6 interface gigabitethernet 0/0/0** command displays the interface status and all of the IPv6 addresses belonging to the interface.

Along with the link local address and global unicast address, the output includes the multicast addresses assigned to the interface.

The output of the **show running-config interface** command displays the current commands applied to a specified interface.

The **show interfaces** command displays interface information and ***packet flow count*** for all interfaces on the device.

Verify interface configuration using the **show ip interface** and **show ipv6 interface** commands, which display the IPv4 and IPv6 related information for all interfaces on a router.

Verify routes using the **show ip route** and **show ipv6 route** commands. Filter show command output using the pipe (|) character. Use filter expressions: section, include, exclude, and begin. By default, command history is enabled, and the system captures the last 10 command lines in its history buffer. Use the **show history** privileged EXEC command to display the contents of the buffer.