CCNA 1 v7.0 Curriculum: Module 2 – Basic Switch and End Device Configuration

itexamanswers.net/ccna-1-v7-0-curriculum-module-2-basic-switch-and-end-device-configuration.html

April 1, 2020

Contents

2.0. Introduction

2.0.1. Why should I take this module?

Welcome to Basic Switch and End Device Configuration!

As part of your career in networking, you might have to set up a new network or maintain and upgrade an existing one. In either case, you'll configure switches and end devices so that they are secure and perform effectively based on your requirements.

Out of the box, switches and end devices come with some general configuration. But for your particular network, switches and end devices require your specific information and instructions. In this module, you will learn how to access Cisco IOS network devices. You will learn basic configuration commands and use them to configure and verify a Cisco IOS device and an end device with an IP address.

Of course, there is much more to network administration, but none of that can happen without first configuring switches and end devices. Let's get started!

2.0.2. What will I learn to do in this module?

Module Title: Basic Switch and End Device Configuration

Module Objective: Implement initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices.

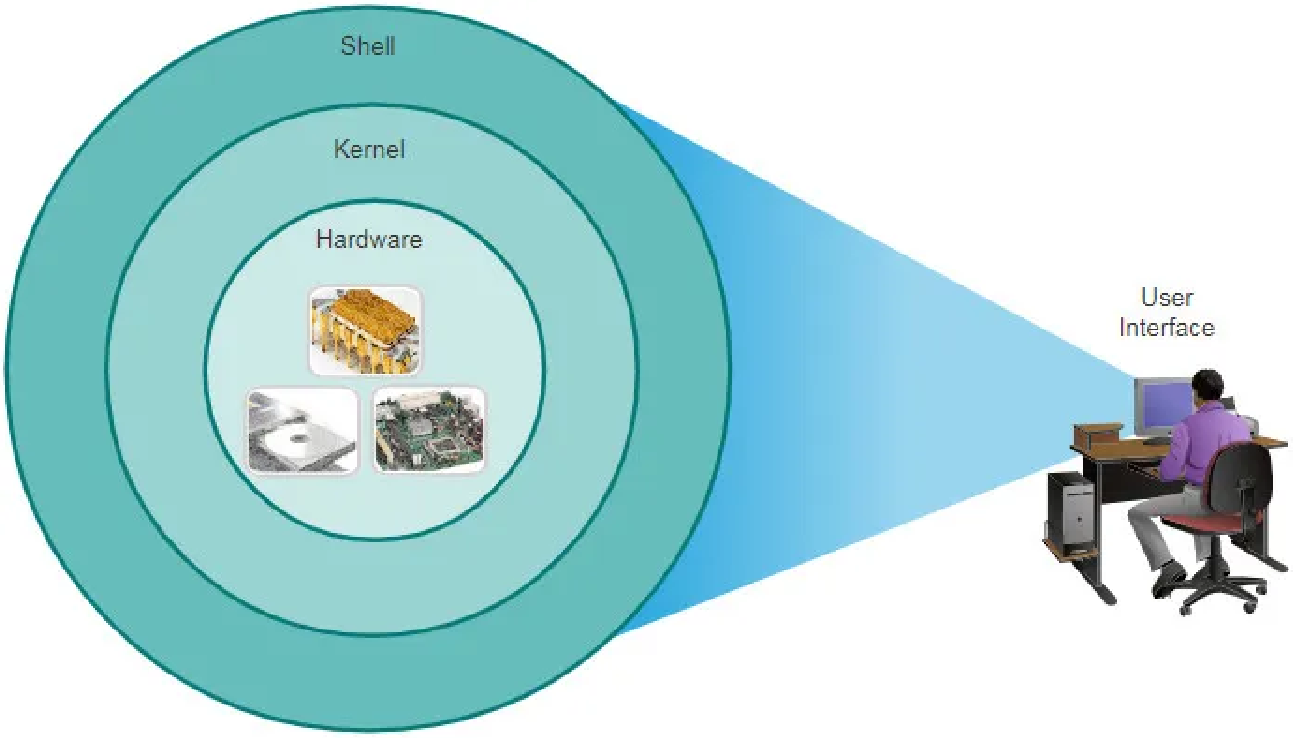
Topic Title	Topic Objective
Cisco IOS Access	Explain how to access a Cisco IOS device for configuration purposes.
IOS Navigation	Explain how to navigate Cisco IOS to configure network devices.
The Command Structure	Describe the command structure of Cisco IOS software.

Topic Title	Topic Objective
Basic Device Configuration	Configure a Cisco IOS device using CLI.
Save Configurations	Use IOS commands to save the running configuration.
Ports and Addresses	Explain how devices communicate across network media.
Configure IP Addressing	Configure a host device with an IP address.
Verify Connectivity	Verify connectivity between two end devices.

2.1. Cisco IOS Access

2.1.1. Operating Systems

All end devices and network devices require an operating system (OS). As shown in the figure, the portion of the OS that interacts directly with computer hardware is known as the kernel. The portion that interfaces with applications and the user is known as the shell. The user can interact with the shell using a command-line interface (CLI) or a graphical user interface (GUI).



- **Shell** – The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.

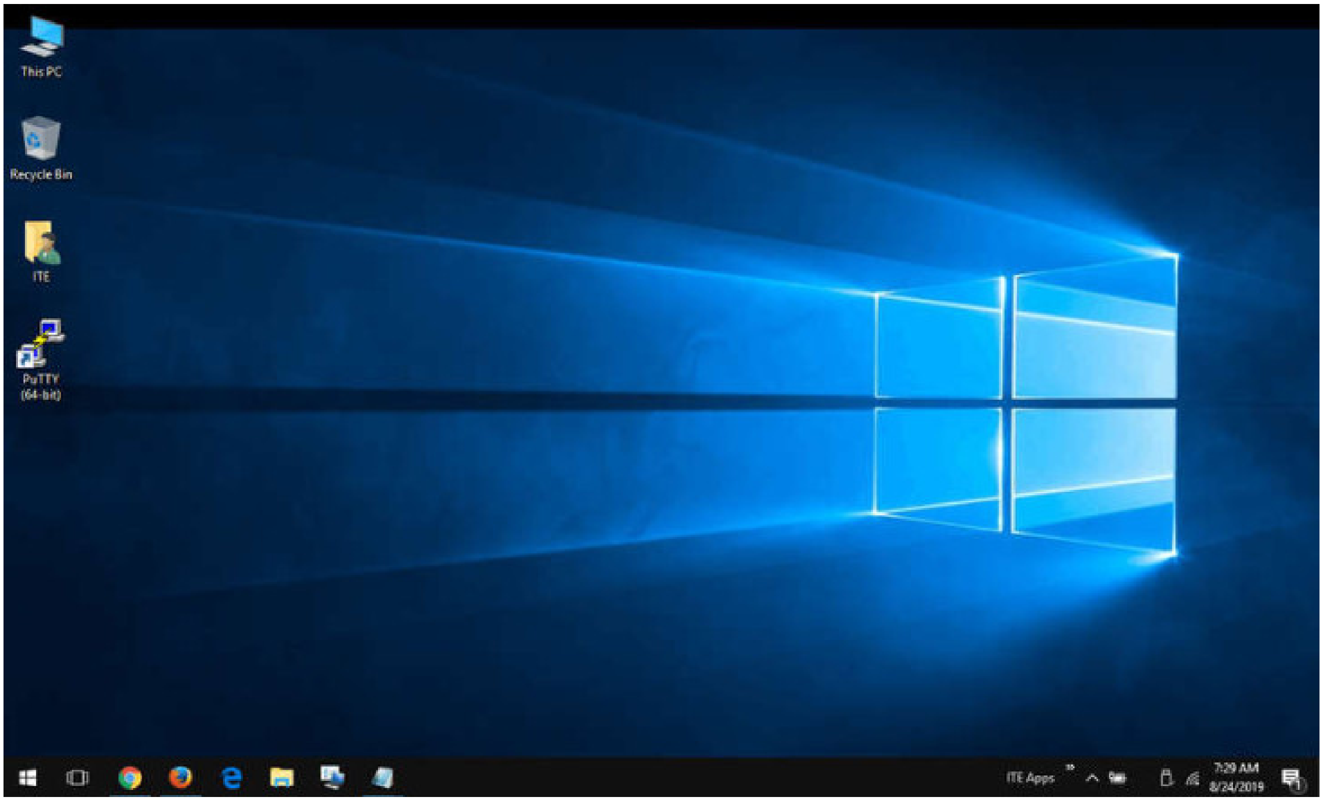
- **Kernel** – Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.
- **Hardware** – The physical part of a computer including underlying electronics.

When using a CLI, the user interacts directly with the system in a text-based environment by entering commands on the keyboard at a command prompt, as shown in the example. The system executes the command, often providing textual output. The CLI requires very little overhead to operate. However, it does require that the user have knowledge of the underlying command structure that controls the system.

```
analyst@secOps ~]$ ls
Desktop Downloads lab.support.files second_drive
[analyst@secOps ~]$
```

2.1.2. GUI

A GUI such as Windows, macOS, Linux KDE, Apple iOS, or Android allows the user to interact with the system using an environment of graphical icons, menus, and windows. The GUI example in the figure is more user-friendly and requires less knowledge of the underlying command structure that controls the system. For this reason, most users rely on GUI environments.



However, GUIs may not always be able to provide all the features available with the CLI. GUIs can also fail, crash, or simply not operate as specified. For these reasons, network devices are typically accessed through a CLI. The CLI is less resource intensive and very stable when compared to a GUI.

The family of network operating systems used on many Cisco devices is called the Cisco Internetwork Operating System (IOS). Cisco IOS is used on many Cisco routers and switches regardless of the type or size of the device. Each device router or switch type uses a different version of Cisco IOS. Other Cisco operating systems include IOS XE, IOS XR, and NX-OS.

Note: The operating system on home routers is usually called firmware. The most common method for configuring a home router is by using a web browser-based GUI.

2.1.3. Purpose of an OS

Network operating systems are similar to a PC operating system. Through a GUI, a PC operating system enables a user to do the following:

- Use a mouse to make selections and run programs
- Enter text and text-based commands
- View output on a monitor

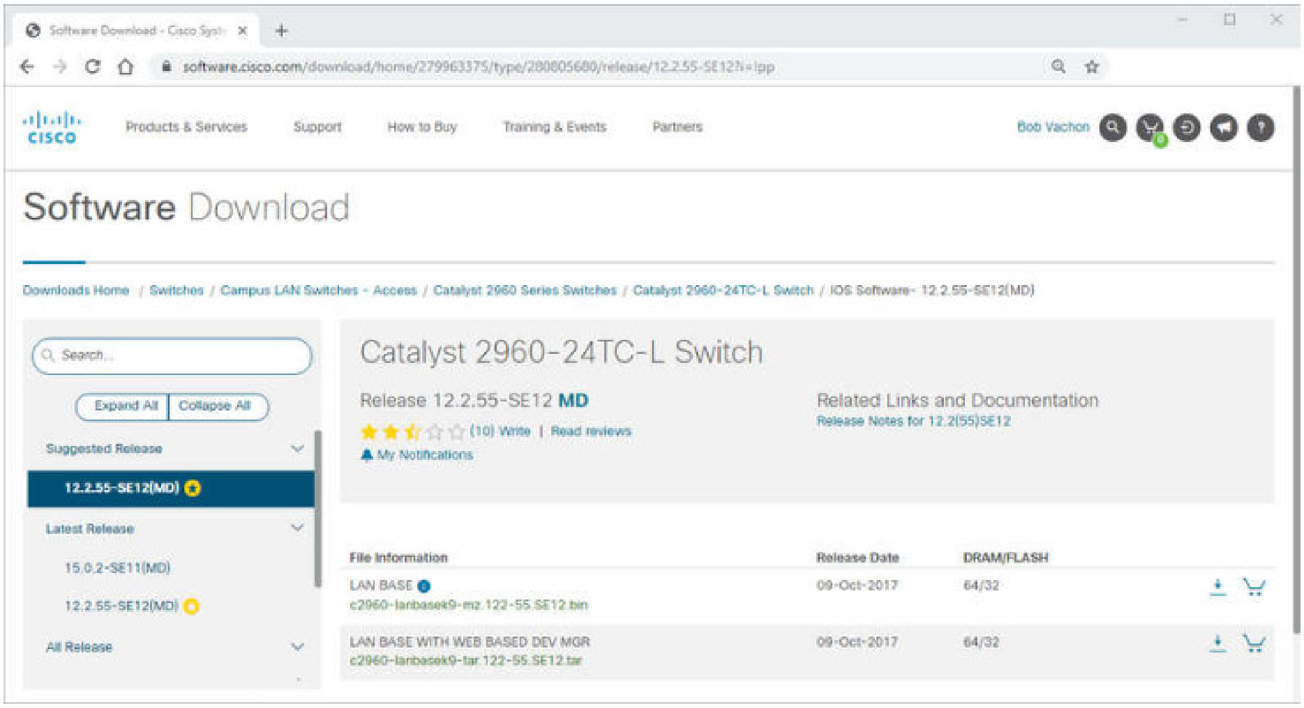
A CLI-based network operating system (e.g., the Cisco IOS on a switch or router) enables a network technician to do the following:

- Use a keyboard to run CLI-based network programs
- Use a keyboard to enter text and text-based commands
- View output on a monitor

Cisco networking devices run particular versions of the Cisco IOS. The IOS version is dependent on the type of device being used and the required features. While all devices come with a default IOS and feature set, it is possible to upgrade the IOS version or feature set to obtain additional capabilities.

The figure displays a list of IOS software releases for a Cisco Catalyst 2960 Switch.

Cisco Software Download Example



Software Download

Downloads Home / Switches / Campus LAN Switches - Access / Catalyst 2960 Series Switches / Catalyst 2960-24TC-L Switch / IOS Software- 12.2.55-SE12(MD)

Catalyst 2960-24TC-L Switch

Release 12.2.55-SE12 **MD**

(10) Write | Read reviews

My Notifications

Related Links and Documentation

Release Notes for 12.2(55)SE12

File Information	Release Date	DRAM/FLASH
LAN BASE c2960-lanbasek9-mz.122-55.SE12.bin	09-Oct-2017	64/32
LAN BASE WITH WEB BASED DEV MGR c2960-lanbasek9-tar.122-55.SE12.tar	09-Oct-2017	64/32

2.1.4. Access Methods

A switch will forward traffic by default and does not need to be explicitly configured to operate. For example, two configured hosts connected to the same new switch would be able to communicate.

Regardless of the default behavior of a new switch, all switches should be configured and secured.

Method	Description
Console	This is a physical management port that provides out-of-band access to a Cisco device. Out-of-band access refers to access via a dedicated management channel that is used for device maintenance purposes only. The advantage of using a console port is that the device is accessible even if no networking services are configured, such as performing the initial configuration. A computer running terminal emulation software and a special console cable to connect to the device are required for a console connection.
Secure Shell (SSH)	SSH is an in-band and recommended method for remotely establishing a secure CLI connection, through a virtual interface, over a network. Unlike a console connection, SSH connections require active networking services on the device, including an active interface configured with an address. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.

Method	Description
Telnet	Telnet is an insecure, in-band method of remotely establishing a CLI session, through a virtual interface, over a network. Unlike SSH, Telnet does not provide a secure, encrypted connection and should only be used in a lab environment. User authentication, passwords, and commands are sent over the network in plaintext. The best practice is to use SSH instead of Telnet. Cisco IOS includes both a Telnet server and Telnet client.

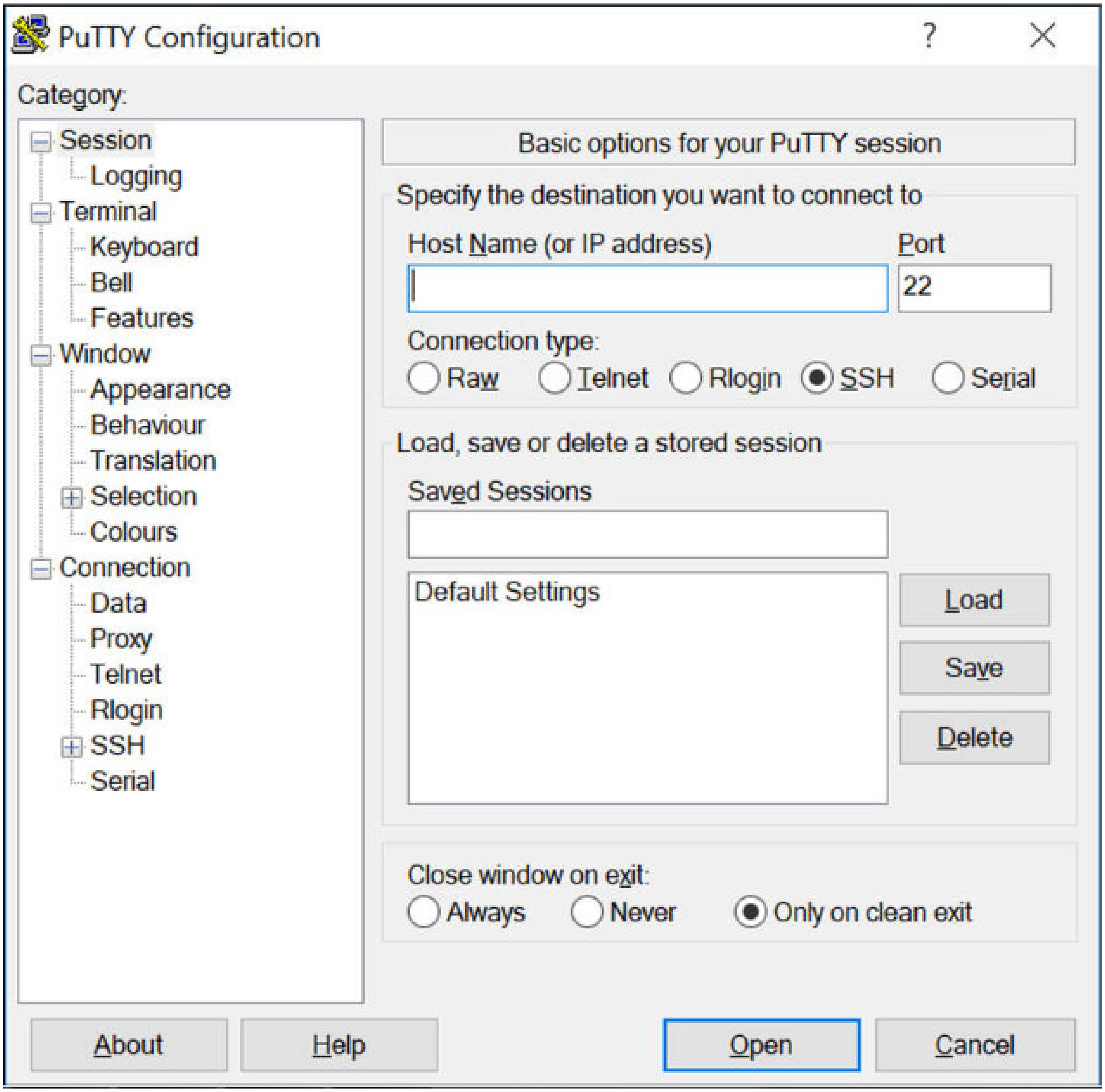
Note: Some devices, such as routers, may also support a legacy auxiliary port that was used to establish a CLI session remotely over a telephone connection using a modem. Similar to a console connection, the AUX port is out-of-band and does not require networking services to be configured or available.

2.1.5. Terminal Emulation Programs

There are several terminal emulation programs you can use to connect to a networking device either by a serial connection over a console port, or by an SSH/Telnet connection. These programs allow you to enhance your productivity by adjusting window sizes, changing font sizes, and changing color schemes.

Click each program name to see a screen capture of the interface.

PuTTY



Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

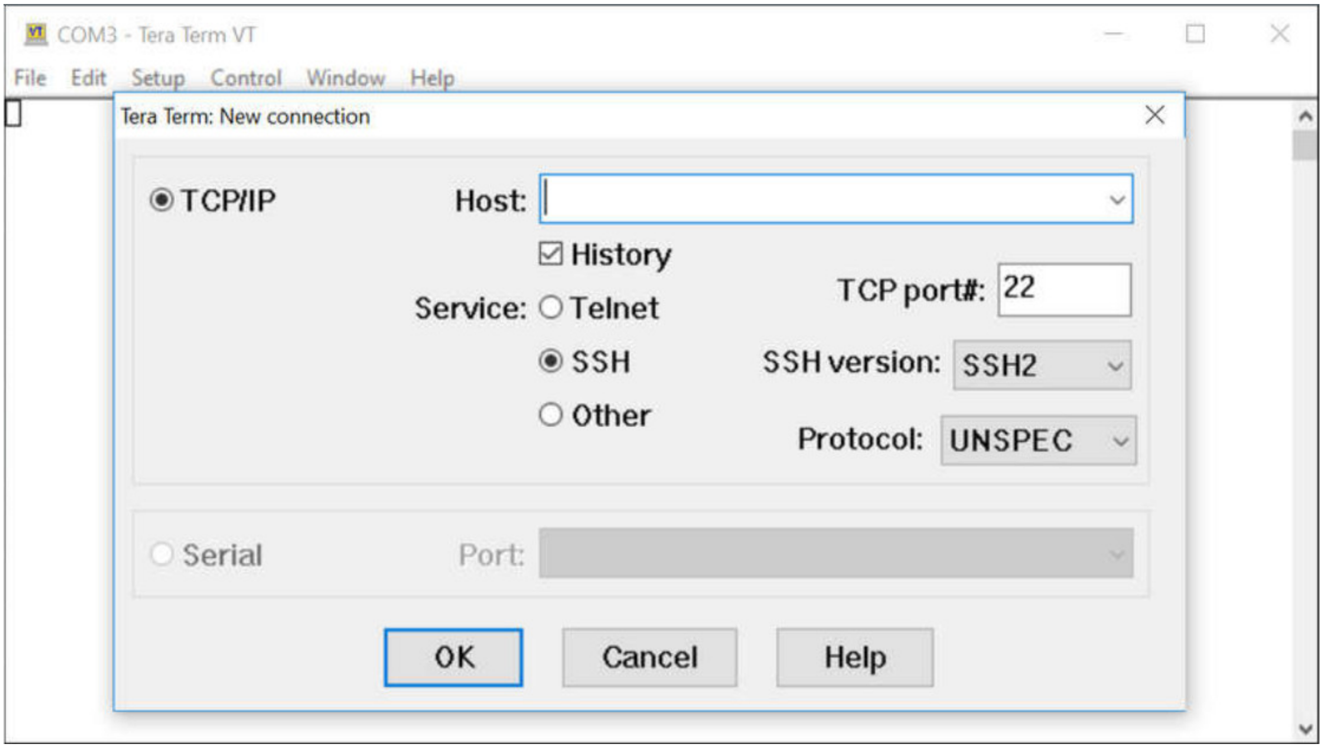
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit

Tera Term



Tera Term: New connection

● TCP/IP   Host:

☑ History

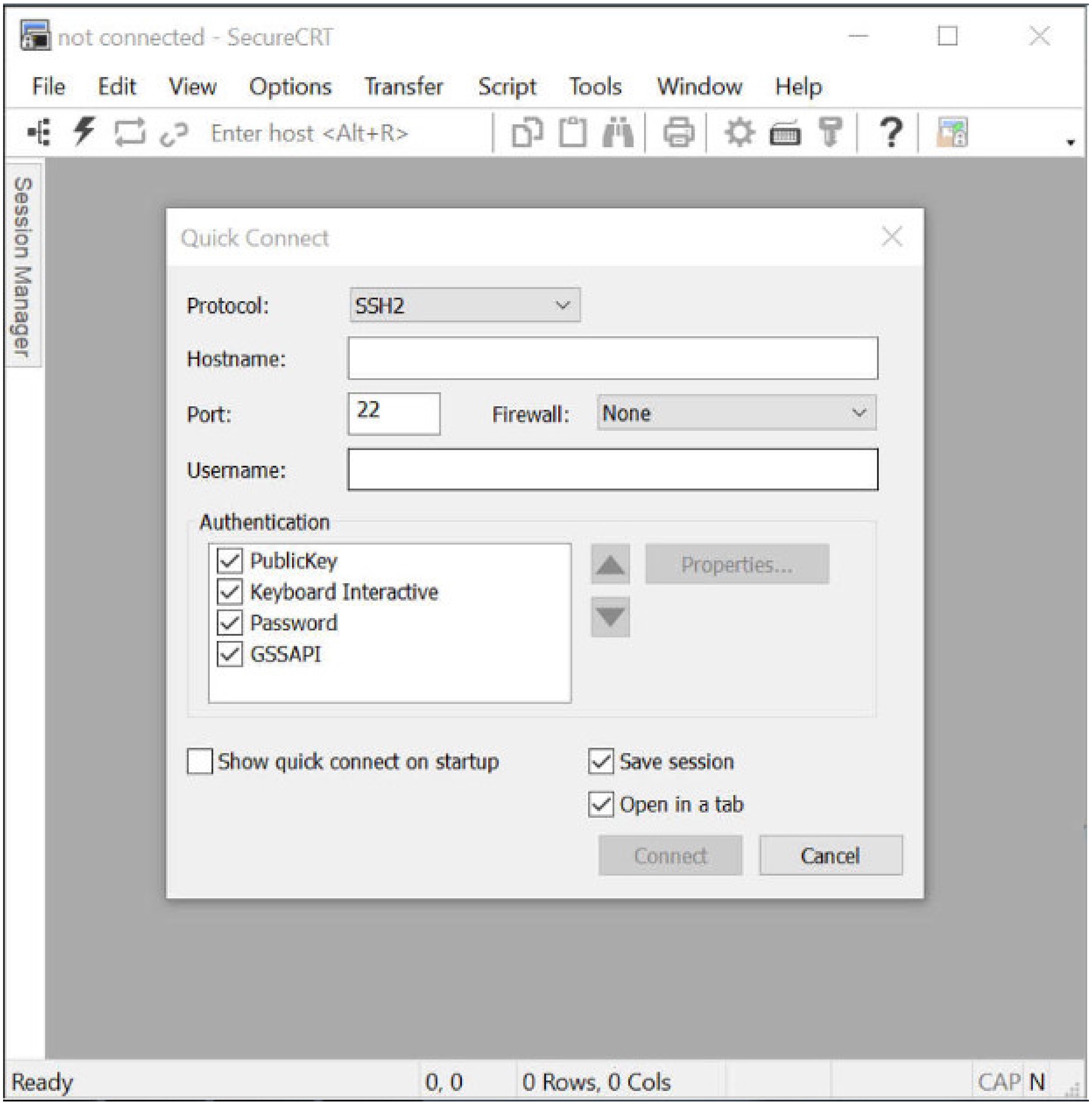
Service: ○ Telnet   TCP port#: 22

● SSH   SSH version: SSH2

○ Other   Protocol: UNSPEC

○ Serial   Port:

SecureCRT



Protocol: SSH2

Hostname:

Port: 22

Firewall: None

Username:

Authentication

☑ PublicKey
☑ Keyboard Interactive
☑ Password
☑ GSSAPI

□ Show quick connect on startup

☑ Save session

☑ Open in a tab

2.2. IOS Navigation

2.2.1. Primary Command Modes

In the previous topic, you learned that all network devices require an OS and that they can be configured using the CLI or a GUI. Using the CLI may provide the network administrator with more precise control and flexibility than using the GUI. This topic discusses using CLI to navigate the Cisco IOS.

As a security feature, the Cisco IOS software separates management access into the following two command modes:

- **User EXEC Mode** – This mode has limited capabilities but is useful for basic operations. It allows only a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device. The user EXEC mode is identified by the CLI prompt that ends with the > symbol.
- **Privileged EXEC Mode** – To execute configuration commands, a network administrator must access privileged EXEC mode. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the # symbol.

The table summarizes the two modes and displays the default CLI prompts of a Cisco switch and router.

Command Mode	Description	Default Device Prompt

User Exec Mode	Mode allows access to only a limited number of basic monitoring commands.
	It is often referred to as “view-only” mode.
		`Switch>`
		`Router>`

Privileged EXEC Mode	Mode allows access to all commands and features. The user can use any monitoring commands and execute configuration and management commands.	`Switch#` `Router#`

2.2.2. Configuration Mode and Subconfiguration Modes

To configure the device, the user must enter global configuration mode, which is commonly called global config mode.

From global config mode, CLI configuration changes are made that affect the operation of the device as a whole. Global configuration mode is identified by a prompt that ends with (config)# after the device name, such as Switch(config)#.

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

- **Line Configuration Mode** – Used to configure console, SSH, Telnet, or AUX access.
- **Interface Configuration Mode** – Used to configure a switch port or router network interface.

When the CLI is used, the mode is identified by the command-line prompt that is unique to that mode. By default, every prompt begins with the device name. Following the name, the remainder of the prompt indicates the mode. For example, the default prompt for line configuration mode is **Switch(config-line)#** and the default prompt for interface configuration mode is **Switch(config-if)#**.

2.2.3. Video – IOS CLI Primary Command Modes

2.2.4. Navigate Between IOS Modes

Various commands are used to move in and out of command prompts. To move from user EXEC mode to privileged EXEC mode, use the **enable** command. Use the **disable** privileged EXEC mode command to return to user EXEC mode.

Note: Privileged EXEC mode is sometimes called enable 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.

There are many different subconfiguration modes. For example, to enter line subconfiguration mode, you use the line command followed by the management line type and number you wish to access. Use the exit command to exit a subconfiguration mode and return to global configuration mode.

```
Switch(config)# line console 0
Switch(config-line)# exit
Switch(config)#
```

To move from any subconfiguration mode of the global configuration mode to the mode one step above it in the hierarchy of modes, enter the **exit** command.

To move from any subconfiguration mode to the privileged EXEC mode, enter the **end** command or enter the key combination **Ctrl+Z.**

```
Switch(config-line)# end
Switch#
```

You can also move directly from one subconfiguration mode to another. Notice how after selecting an interface, the command prompt changes from **(config-line)#** to **(config-if)#.**

```
Switch(config-line)# interface FastEthernet 0/1
Switch(config-if)#
```

2.2.5. Video – Navigate Between IOS Modes

2.2.6. A Note About Syntax Checker Activities

When you are learning how to modify device configurations, you might want to start in a safe, non-production environment before trying it on real equipment. NetAcad gives you different simulation tools to help build your configuration and troubleshooting skills. Because these are simulation tools, they typically do not have all the functionality of real equipment. One such tool is the Syntax Checker. In each Syntax Checker, you are given a set of instructions to enter a specific set of commands. You cannot progress in Syntax Checker unless the exact and full command is entered as specified. More advanced simulation tools, such as Packet Tracer, let you enter abbreviated commands, much as you would do on real equipment.

2.2.7. Syntax Checker – Navigate Between IOS Modes

Use the Syntax Checker activity to navigate between IOS command lines on a switch.

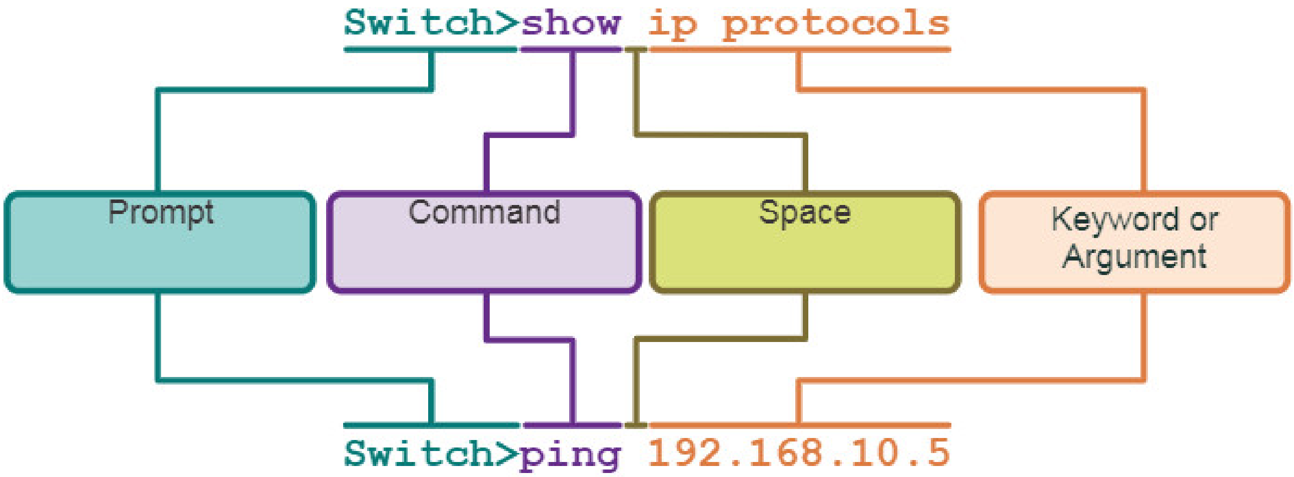
```
Enter privileged EXEC mode using the enable command.

Switch>enable
Return to user EXEC mode using the disable command.

Switch#disable
Re-enter privileged EXEC mode.

Switch>enable
Enter global configuration mode using the configure terminal command.

Switch#configure terminal
Exit global configuration mode and return to privileged EXEC mode using the exit
command.

Switch(config)#exit
Re-enter global configuration mode.

Switch#configure terminal
Enter line subconfiguration mode for the console port using the line console 0
command.

Switch(config)#line console 0
Return to global configuration mode using the exit command.

Switch(config-line)#exit
Enter VTY line subconfiguration mode using the line vty 0 15 command.

Switch(config)#line vty 0 15
Return to global configuration mode.

Switch(config-line)#exit
Enter the VLAN 1 interface subconfiguration mode using the interface vlan 1 command.

Switch(config)#interface vlan 1
From interface configuration mode, switch to line console subconfiguration mode using
the line console 0 global configuration command.

Switch(config-if)#line console 0
Return to privileged EXEC mode using the end command.

Switch(config-line)#end
You successfully navigated between the various IOS command line modes.
```

2.3. The Command Structure

2.3.1. Basic IOS Command Structure

This topic covers the basic structure of commands for the Cisco IOS. A network administrator must know the basic IOS command structure to be able to use the CLI for device configuration.

A Cisco IOS device supports many commands. Each IOS command has a specific format, or syntax, and can only be executed in the appropriate mode. The general syntax for a command, shown in the figure, is the command followed by any appropriate keywords and arguments.



- **Keyword** – This is a specific parameter defined in the operating system (in the figure, **ip protocols**).
- **Argument** – This is not predefined; it is a value or variable defined by the user (in the figure, **192.168.10.5).**

After entering each complete command, including any keywords and arguments, press the Enter key to submit the command to the command interpreter.

2.3.2. IOS Command Syntax Check

A command might require one or more arguments. To determine the keywords and arguments required for a command, refer to the command syntax. The syntax provides the pattern, or format, that must be used when entering a command.

As identified in the table, boldface text indicates commands and keywords that are entered as shown. Italic text indicates an argument for which the user provides the value.

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.

Convention	Description
[x**]**	Square brackets indicate an optional element (keyword or argument).
{x**}**	Braces indicate a required element (keyword or argument).
[x **{**y **|** z **}]**	Braces and vertical lines within square brackets indicate a required choice within an optional element. Spaces are used to clearly delineate parts of the command.

For instance, the syntax for using the **description** command is **description** *string*. The argument is a *string* value provided by the user. The **description** command is typically used to identify the purpose of an interface. For example, entering the command, **description Connects to the main headquarter office switch**, describes where the other device is at the end of the connection.

The following examples demonstrate conventions used to document and use IOS commands:

- **ping** *ip-address* – The command is **ping** and the user-defined argument is the ip-address of the destination device. For example, **ping 10.10.10.5**.
- **traceroute** *ip-address* – The command is **traceroute** and the user-defined argument is the *ip-address* of the destination device. For example, **traceroute 192.168.254.254**.

If a command is complex with multiple arguments, you may see it represented like this:

```
Switch(config-if)# switchport port-security aging { static | time time | type
{absolute | inactivity}}
```

The command will typically be followed we a detailed description of the command and each argument.

The Cisco IOS Command Reference is the ultimate source of information for a particular IOS command.

2.3.3. IOS Help Features

The IOS has two forms of help available: context-sensitive help and command syntax check.

Context-sensitive help enables you to quickly find answers to these questions:

- Which commands are available in each command mode?
- Which commands start with specific characters or group of characters?
- Which arguments and keywords are available to particular commands?

To access context-sensitive help, simply enter a question mark, **?**, at the CLI.

Command syntax check verifies that a valid command was entered by the user. When a command is entered, the command line interpreter evaluates the command from left to right. If the interpreter understands the command, the requested action is executed, and the CLI returns to the appropriate prompt. However, if the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

2.3.4. Video – Context Sensitive Help and Command Syntax Check

2.3.5. Hot Keys and Shortcuts

The IOS CLI provides hot keys and shortcuts that make configuring, monitoring, and troubleshooting easier.

Commands and keywords can be shortened to the minimum number of characters that identify a unique selection. For example, the **configure** command can be shortened to **conf** because **configure** is the only command that begins with **conf.** An even shorter version, **con,** will not work because more than one command begins with con. Keywords can also be shortened.

The table lists keystrokes to enhance command line editing.

Keystroke	Description
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Ctrl+D	Erases the character at the cursor.
Ctrl+K	Erases all characters from the cursor to the end of the command line.
Esc D	Erases all characters from the cursor to the end of the word.
Ctrl+U or **Ctrl+X**	Erases all characters from the cursor back to the beginning of the command line.
Ctrl+W	Erases the word to the left of the cursor.
Ctrl+A	Moves the cursor to the beginning of the line.
Left Arrow or **Ctrl+B**	Moves the cursor one character to the left.
Esc B	Moves the cursor back one word to the left.
Esc F	Moves the cursor forward one word to the right.

Keystroke	Description
Right Arrow or **Ctrl+F**	Moves the cursor one character to the right.
Ctrl+E	Moves the cursor to the end of command line.
Up Arrow or **Ctrl+P**	Recalls the commands in the history buffer, beginning with the most recent commands.
Ctrl+R or **Ctrl+I** or **Ctrl+L**	Redisplays the system prompt and command line after a console message is received.

Note: While the **Delete** key typically deletes the character to the right of the prompt, the IOS command structure does not recognize the Delete key.

When a command output produces more text than can be displayed in a terminal window, the IOS will display a **"–More–"** prompt. The following table describes the keystrokes that can be used when this prompt is displayed.

Keystroke	Description
Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any other key	Ends the display string, returning to privileged EXEC mode.

This table lists commands used to exit out of an operation.

Keystroke	Description
Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode. When in setup mode, aborts back to the command prompt.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Shift-6	All-purpose break sequence used to abort DNS lookups, traceroutes, pings, etc.

2.3.6. Video – Hot Keys and Shortcuts

2.3.7. Packet Tracer – Navigate the IOS

In this activity, you will practice skills necessary for navigating the Cisco IOS, including different user access modes, various configuration modes, and common commands used on a regular basis. You will also practice accessing the context-sensitive help by configuring the clock command.

2.3.7 Packet Tracer – Navigate the IOS

2.3.8. Lab – Navigate the IOS by Using Tera Term for Console Connectivity

In this lab, you will complete the following objectives:

- Part 1: Access a Cisco Switch through the Serial Console Port
- Part 2: Display and Configure Basic Device Settings
- Part 3: (Optional) Access a Cisco Router Using a Mini-USB Console Cable

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

Packet Tracer – Physical Mode (PTPM)

2.3.8 Packet Tracer – Navigate the IOS Using a Terminal Client for Console Connectivity – Physical Mode

Lab Equipment

2.3.8 Lab – Navigate the IOS by Using Tera Term for Console Connectivity

2.4. Basic Device Configuration

2.4.1. Device Names

You have learned a great deal about the Cisco IOS, navigating the IOS, and the command structure. Now, you are ready to configure devices! The first configuration command on any device should be to give it a unique device name or hostname. By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."

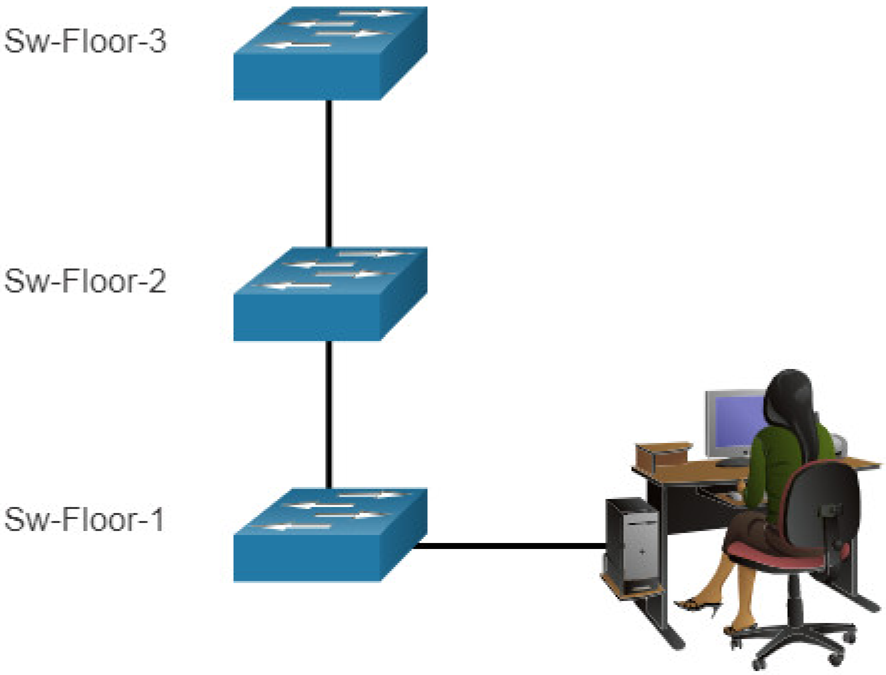
The problem is if all switches in a network were left with their default names, it would be difficult to identify a specific device. For instance, how would you know that you are connected to the right device when accessing it remotely using SSH? The hostname provides confirmation that you are connected to the correct device.

The default name should be changed to something more descriptive. By choosing names wisely, it is easier to remember, document, and identify network devices. Here are some important naming guidelines for hosts:

- Start with a letter

- Contain no spaces
- End with a letter or digit
- Use only letters, digits, and dashes
- Be less than 64 characters in length

An organization must choose a naming convention that makes it easy and intuitive to identify a specific device. The hostnames used in the device IOS preserve capitalization and lowercase characters. For example, the figure shows that three switches, spanning three different floors, are interconnected together in a network. The naming convention that was used incorporated the location and the purpose of each device. Network documentation should explain how these names were chosen so additional devices can be named accordingly.



When network devices are named, they are easy to identify for configuration purposes.

When the naming convention has been identified, the next step is to use the CLI to apply the names to the devices. As shown in the example, from the privileged EXEC mode, access the global configuration mode by entering the configure terminal command. Notice the change in the command prompt.

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

From global configuration mode, enter the command **hostname** followed by the name of the switch and press **Enter.** Notice the change in the command prompt name.

Note: To return the switch to the default prompt, use the **no hostname** global config command.

Always make sure the documentation is updated each time a device is added or modified. Identify devices in the documentation by their location, purpose, and address.

2.4.2. Password Guidelines

The use of weak or easily guessed passwords continues to be the biggest security concern of organizations. Network devices, including home wireless routers, 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.

All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.

When choosing passwords, use strong passwords that are not easily guessed. There are some key points to consider when choosing passwords:

- Use passwords that are more than eight characters in length.
- Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
- Avoid using the same password for all devices.
- Do not use common words because they are easily guessed.

Use an internet search to find a password generator. Many will allow you to set the length, character set, and other parameters.

Note: Most of the labs in this course use simple passwords such as **cisco** or **class.** These passwords are considered weak and easily guessable and should be avoided in production environments. We only use these passwords for convenience in a classroom setting, or to illustrate configuration examples.

2.4.3. Configure Passwords

When you initially connect to a device, you are in user EXEC mode. This mode is secured using the console.

To secure user EXEC mode access, enter line console configuration mode using the **line console 0** global configuration command, as shown in the example. The zero is used to represent the first (and in most cases the only) console interface. Next, specify the user EXEC mode password using the **password** *password* command. Finally, enable user EXEC access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Console access will now require a password before allowing access to the user EXEC mode.

To have administrator access to all IOS commands including configuring a device, you must gain privileged EXEC mode access. It is the most important access method because it provides complete access to the device.

To secure privileged EXEC access, use the **enable secret** *password* global config command, as shown in the example.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Virtual terminal (VTY) lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

To secure VTY lines, enter line VTY mode using the **line vty 0 15** global config command. Next, specify the VTY password using the **password** *password* command. Lastly, enable VTY access using the **login** command.

An example of securing the VTY lines on a switch is shown.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

2.4.4. Encrypt Passwords

The startup-config and running-config files display most passwords in plaintext. This is a security threat because anyone can discover the passwords if they have access to these files.

To encrypt all plaintext passwords, use the **service password-encryption** global config command as shown in the example.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

The command applies weak encryption to all unencrypted passwords. This encryption applies only to passwords in the configuration file, not to passwords as they are sent over the network. The purpose of this command is to keep unauthorized individuals from viewing passwords in the configuration file.

Use the **show running-config** command to verify that passwords are now encrypted.

```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
password 7 03095A0F034F38435B49150A1819
login
!
!
end
```

2.4.5. Banner Messages

Although requiring passwords is one way to keep unauthorized personnel out of a network, it is vital to provide a method for declaring that only authorized personnel should attempt to access the device. To do this, add a banner to the device output. Banners can be an important part of the legal process in the event that someone is prosecuted for breaking into a device. Some legal systems do not allow prosecution, or even the monitoring of users, unless a notification is visible.

To create a banner message of the day on a network device, use the **banner motd #** the message of the day **#** global config command. The "#" in the command syntax is called the delimiting character. It is entered before and after the message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols such as the "#" are often used. After the command is executed, the banner will be displayed on all subsequent attempts to access the device until the banner is removed.

The following example shows the steps to configure the banner on Sw-Floor-1.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only#
```

2.4.6. Video – Secure Administrative Access to a Switch

2.4.7. Syntax Checker – Basic Device Configuration

Secure management access to a switch.

- Assign a device name.
- Secure user EXEC mode access.
- Secure privileged EXEC mode access.
- Secure VTY access.
- Encrypt all plaintext passwords.
- Display a login banner.

```
Enter global configuration mode.

Switch#configure terminal
Name the switch “Sw-Floor-1”.

Switch(config)#hostname Sw-Floor-1
Secure user EXEC mode access by entering line console 0, assign the password cisco,
enable login, and return to the global configuration mode using exit.

Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Secure privileged EXEC mode access using the password class.

Sw-Floor-1(config)#enable secret class
Secure the VTY lines 0 through 15, assign the password cisco, enable login, and
return to the global configuration mode using exit.

Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Encrypt all plaintext passwords.

Sw-Floor-1(config)#service password-encryption
Create a banner message using the “#” symbol as the delimiter. The banner should
display exactly: Warning! Authorized access only!

Sw-Floor-1(config)#banner motd #Warning! Authorized access only!#
You successfully completed the basic requirements to access and secure a device.
```

2.5. Save Configurations

2.5.1. Configuration Files

You now know how to perform basic configuration on a switch, including passwords and banner messages. This topic will show you how to save your configurations.

There are two system files that store the device configuration:

- **startup-config** – This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.
- **running-config** – This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.

The **show running-config** privileged EXEC mode command is used to view the running config. As shown in the example, the command will list the complete configuration currently stored in RAM.

```
Switch# show running-config
Building configuration...
Current configuration : 1351 bytes
!
! Last configuration change at 00:01:20 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

To view the startup configuration file, use the **show startup-config** privileged EXEC command.

If power to the device is lost, or if the device is restarted, all configuration changes will be lost unless they have been saved. To save changes made to the running configuration to the startup configuration file, use the **copy running-config startup-config** privileged EXEC mode command.

2.5.2. Alter the Running Configuration

If changes made to the running config do not have the desired effect and the running-config has not yet been saved, you can restore the device to its previous configuration. Remove the changed commands individually, or reload the device using the **reload** privileged EXEC mode command to restore the startup-config.

The downside to using the **reload** command to remove an unsaved running config is the brief amount of time the device will be offline, causing network downtime.

When a reload is initiated, the IOS will detect that the running config has changes that were not saved to the startup configuration. A prompt will appear to ask whether to save the changes. To discard the changes, enter **n** or **no.**

Alternatively, if undesired changes were saved to the startup config, it may be necessary to clear all the configurations. This requires erasing the startup config and restarting the device. The startup config is removed by using the **erase startup-config** privileged EXEC mode command. After the command is issued, the switch will prompt you for confirmation. Press **Enter** to accept.

After removing the startup config from NVRAM, reload the device to remove the current running config file from RAM. On reload, a switch will load the default startup config that originally shipped with the device.

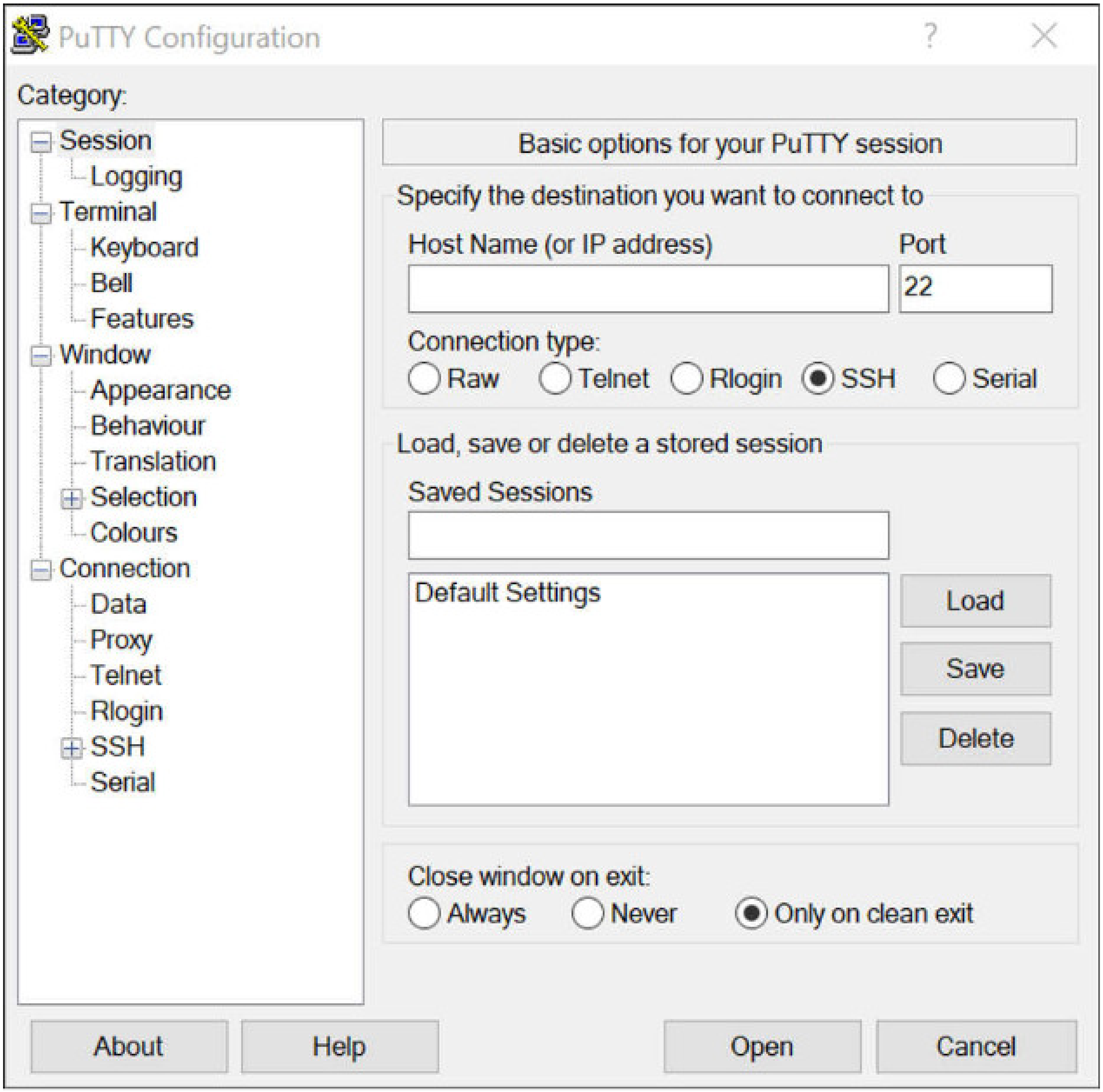
2.5.3. Video – Alter the Running Configuration

2.5.4. Capture Configuration to a Text File

Configuration files can also be saved and archived to a text document. This sequence of steps ensures that a working copy of the configuration file is available for editing or reuse later.

For example, assume that a switch has been configured, and the running config has been saved on the device.

Step 1. Open terminal emulation software, such as PuTTY or Tera Term, that is already connected to a switch.



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

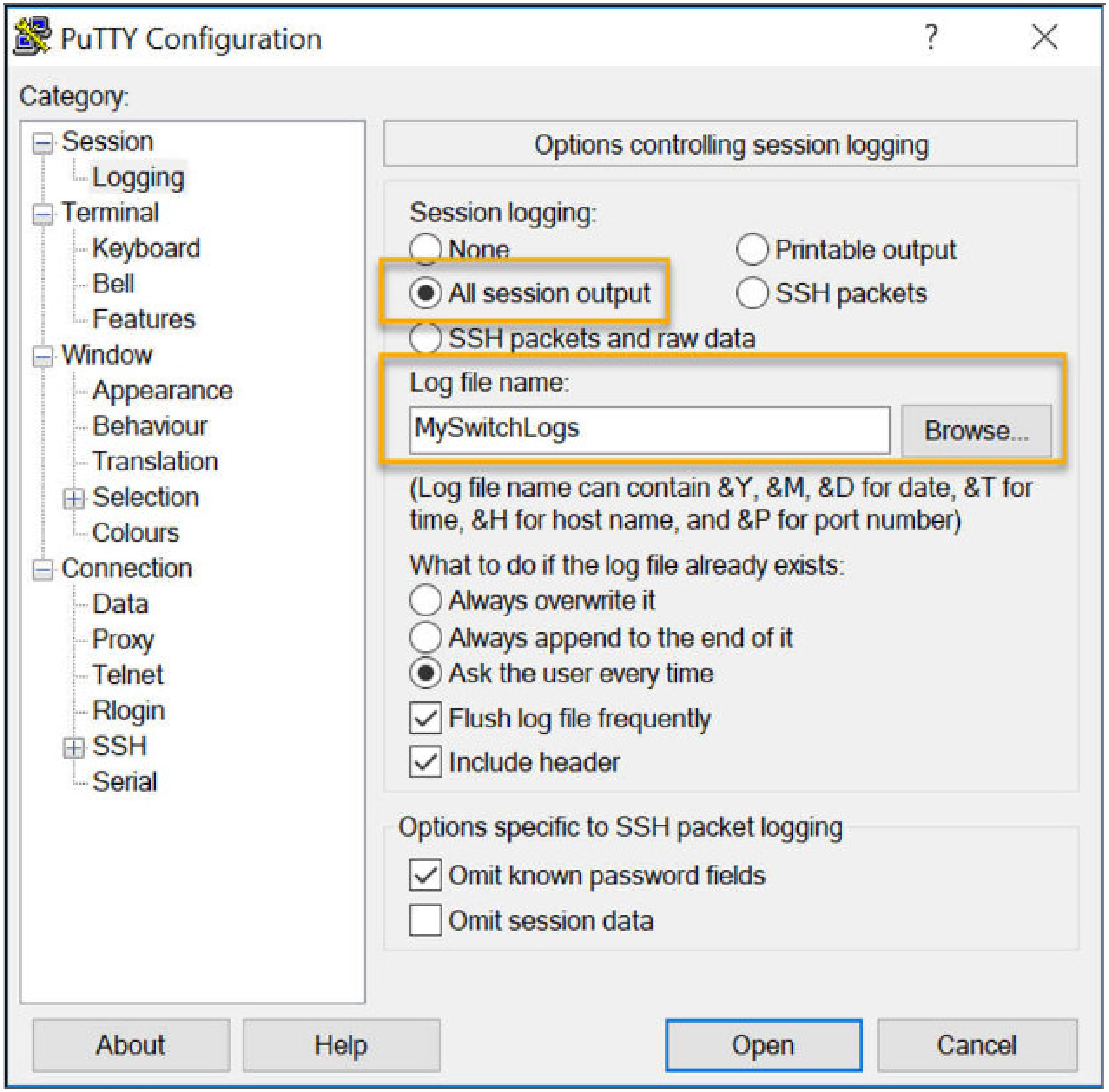
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit

Step 2. Enable logging in the terminal software and assign a name and file location to save the log file. The figure displays that **All session output** will be captured to the file specified (i.e., MySwitchLogs).



Options controlling session logging

Session logging:

○ None ○ Printable output

● All session output ○ SSH packets

○ SSH packets and raw data

Log file name:

MySwitchLogs Browse...

(Log file name can contain &Y, &M, &D for date, &T for time, &H for host name, and &P for port number)

What to do if the log file already exists:

○ Always overwrite it

○ Always append to the end of it

● Ask the user every time

☑ Flush log file frequently

☑ Include header

Options specific to SSH packet logging

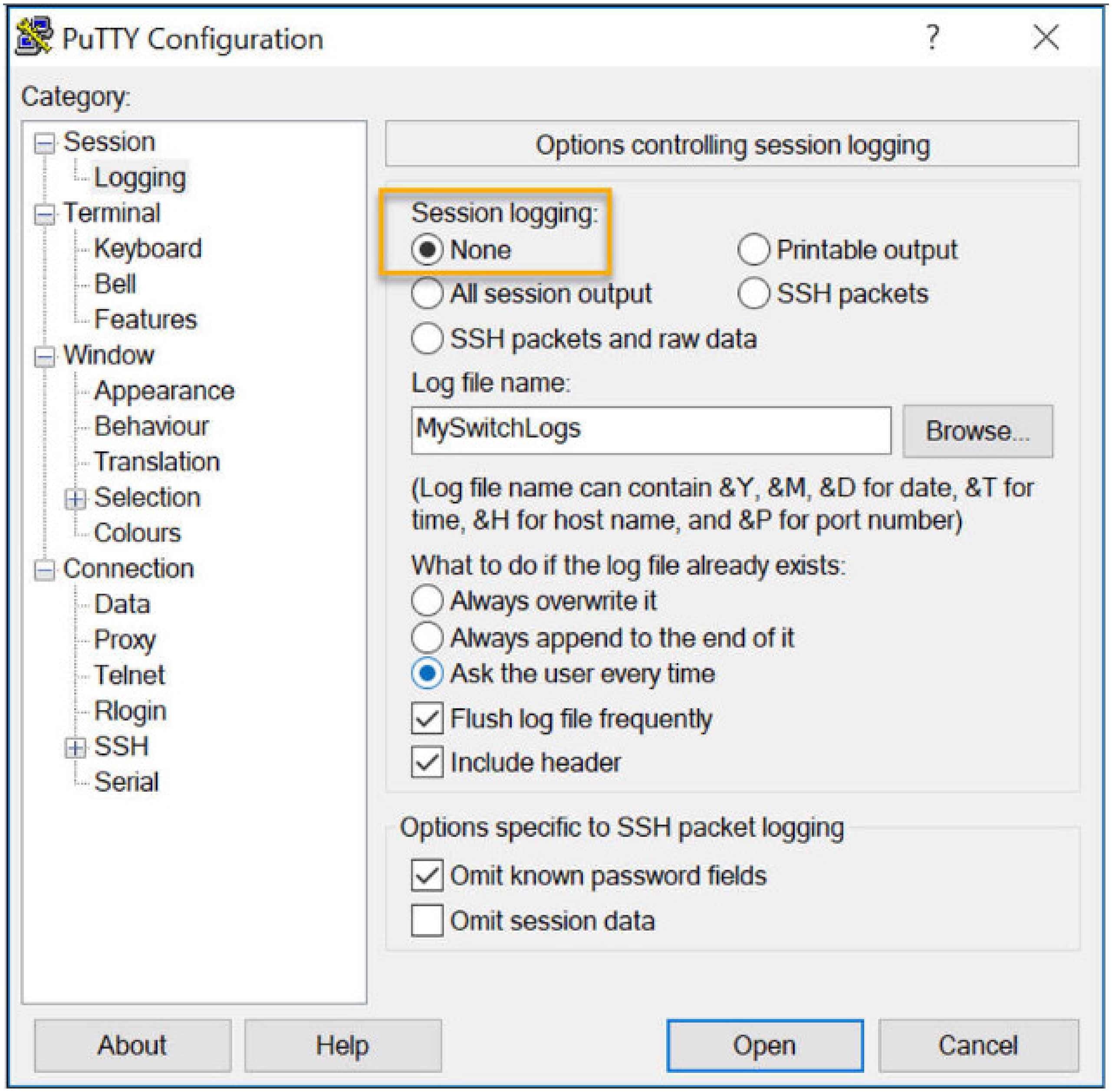
☑ Omit known password fields

□ Omit session data

Step 3. Execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.

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

Step 4. Disable logging in the terminal software. The figure shows how to disable logging by choosing the **None** session logging option.



Session logging:
● None ○ Printable output
○ All session output ○ SSH packets
○ SSH packets and raw data

Log file name:
MySwitchLogs

(Log file name can contain &Y, &M, &D for date, &T for time, &H for host name, and &P for port number)

What to do if the log file already exists:
○ Always overwrite it
○ Always append to the end of it
● Ask the user every time

☑ Flush log file frequently
☑ Include header

☑ Omit known password fields
□ Omit session data

The text file created can be used as a record of how the device is currently implemented. The file could require editing before being used to restore a saved configuration to a device.

To restore a configuration file to a device:

- **Step 1.** Enter global configuration mode on the device.
- **Step 2.** Copy and paste the text file into the terminal window connected to the switch.

The text in the file will be applied as commands in the CLI and become the running configuration on the device. This is a convenient method of manually configuring a device.

2.5.5. Packet Tracer – Configure Initial Switch Settings

In this activity, you will perform basic switch configurations. You will secure access to the CLI and console ports using encrypted and plaintext passwords. You will learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited.

2.5.5 Packet Tracer – Configure Initial Switch Settings

2.6. Ports and Addresses

2.6.1. 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)

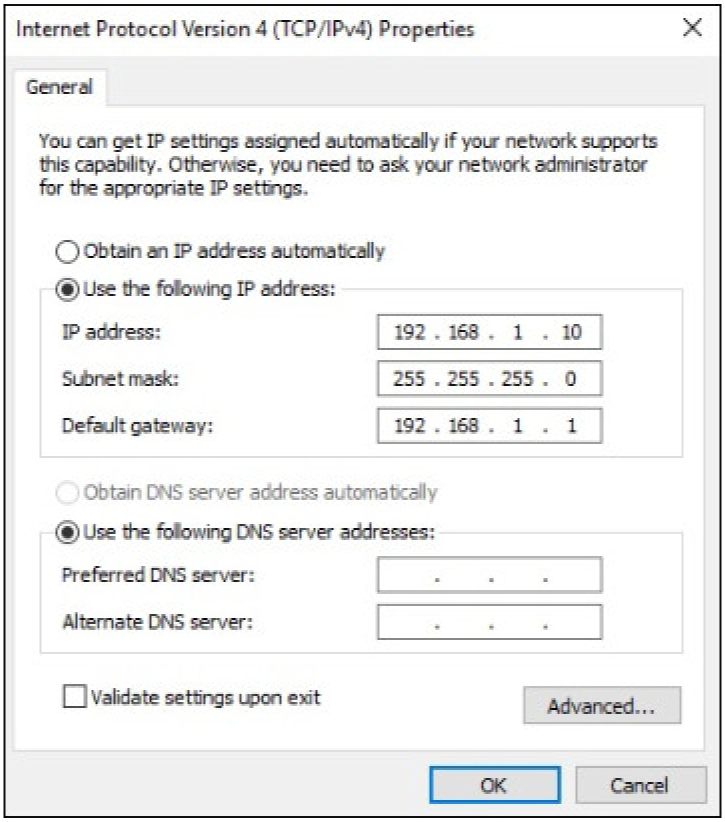
The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255. IPv4 addresses are assigned to individual devices connected to a network.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

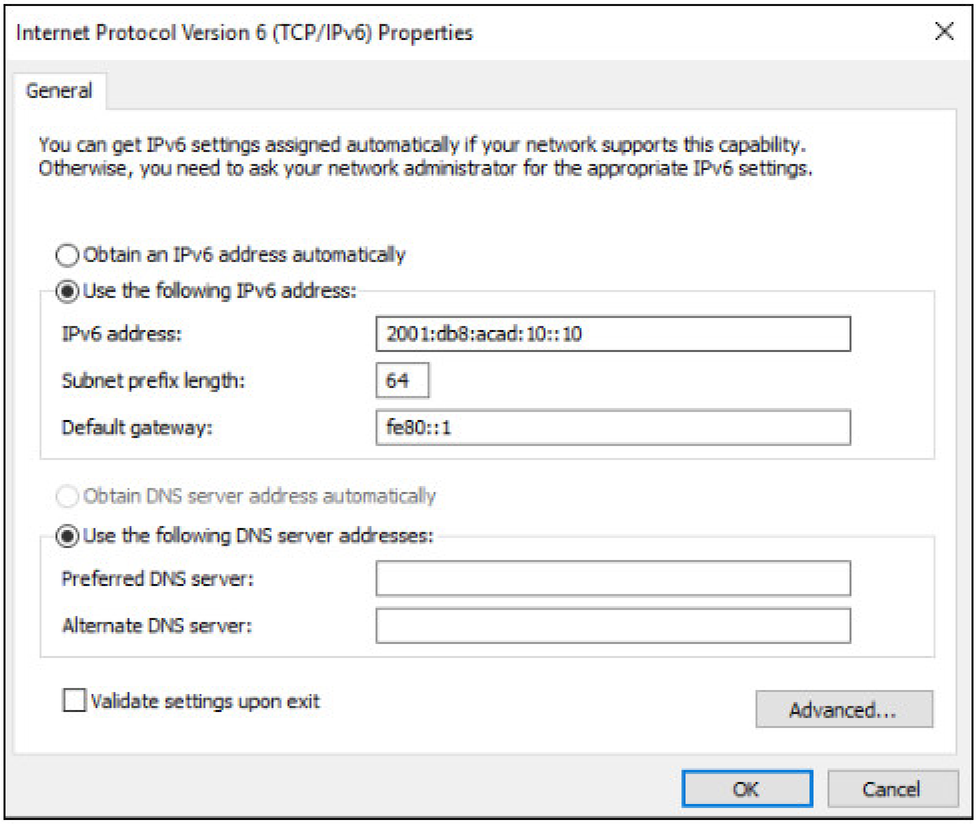
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address: 2001:db8:acad:10::10

Subnet prefix length: 64

Default gateway: fe80::1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

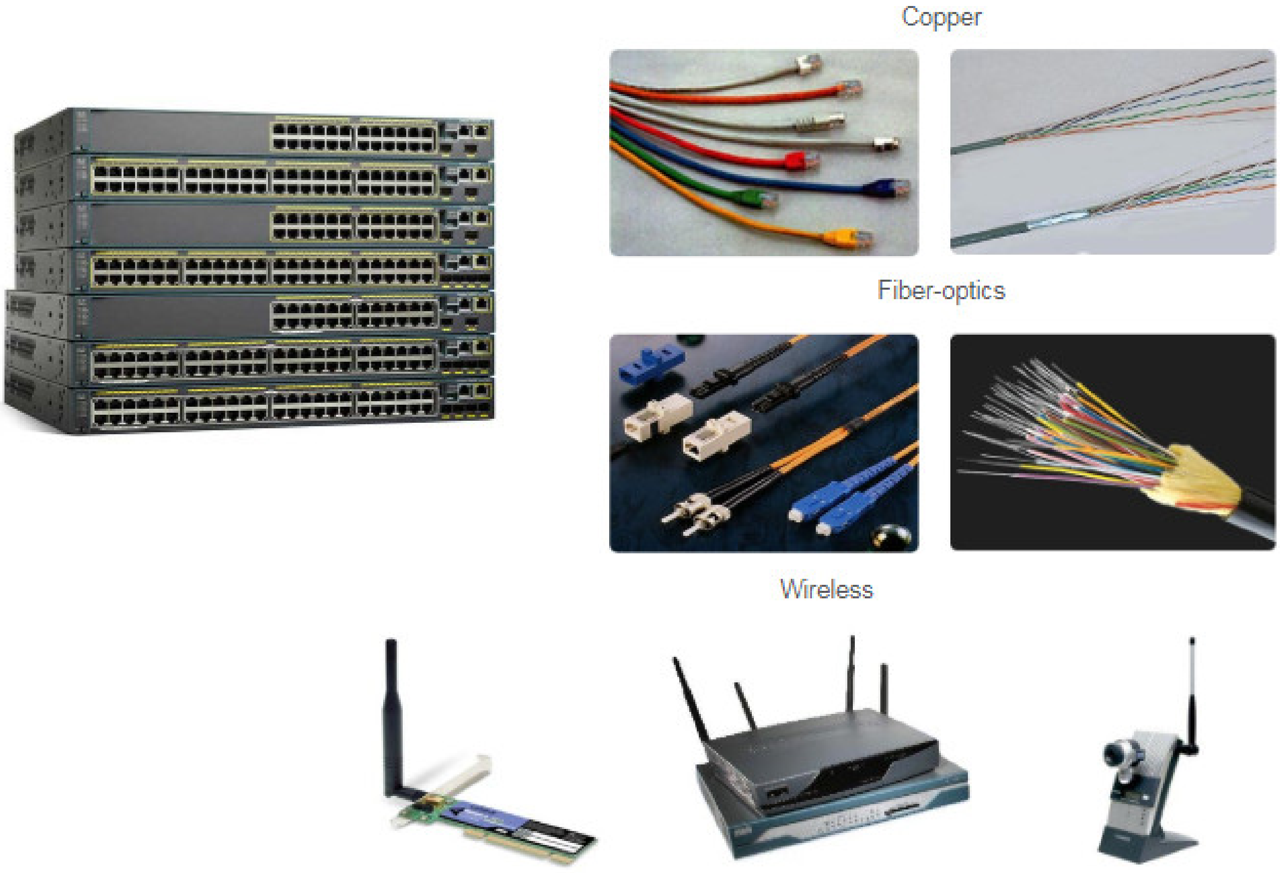
Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

2.6.2. 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.



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.

2.7. Configure IP Addressing

2.7.1. Manual IP Address Configuration for End Devices

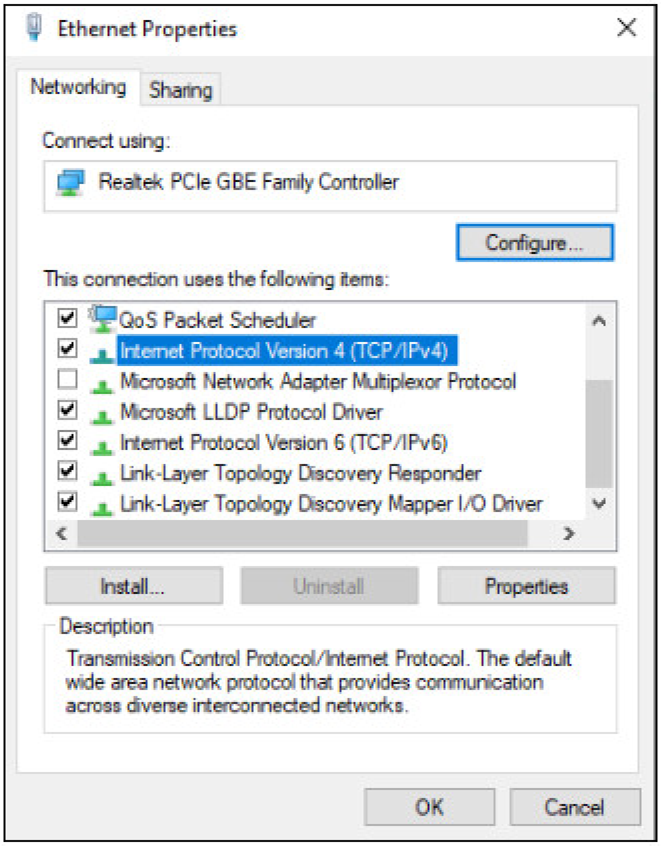
Much like you need your friends' telephone numbers to text or call them, end devices in your network need an IP address so that they can communicate with other devices on your network. In this topic, you will implement basic connectivity by configuring IP addressing on switches and PCs.

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.



Ethernet Properties

Networking | Sharing

Connect using:

Realtek PCIe GBE Family Controller

Configure...

This connection uses the following items:

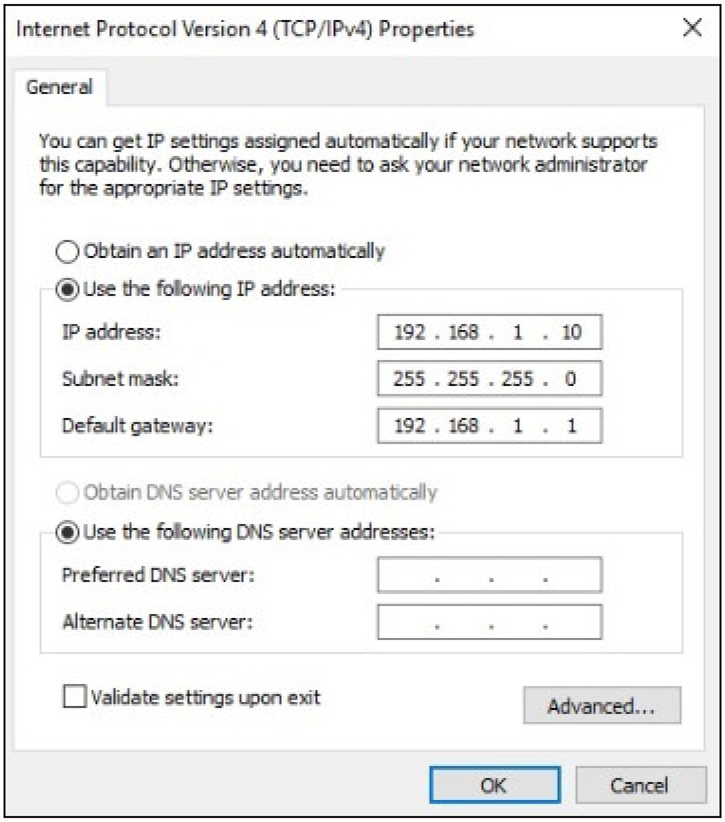
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

Advanced...

OK | Cancel

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.

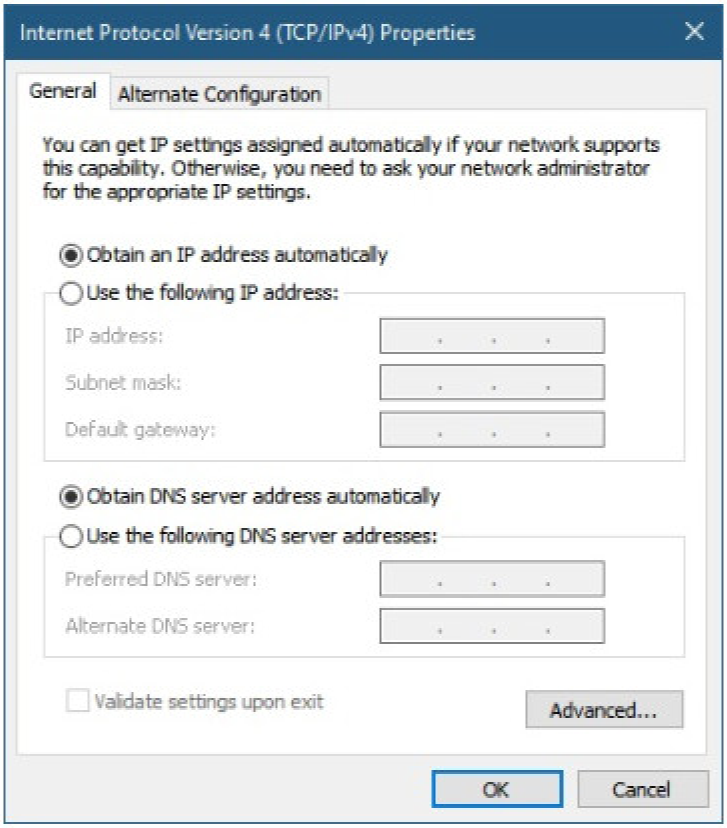
2.7.2. Automatic IP Address Configuration for End Devices

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

2.7.3. 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.

```
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.
```

2.7.4. 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.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

2.7.5. 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.
```

2.7.6. 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.

2.7.6 Packet Tracer – Implement Basic Connectivity

2.8. Verify Connectivity

2.8.1. 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.

2.8.2. 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.

2.9. Module Practice and Quiz

2.9.1. 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.

2.9.1 Packet Tracer – Basic Switch and End Device Configuration

2.9.2. Lab – Basic Switch and End Device Configuration

In this lab, you will complete the following objectives:

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)

2.9.2 Packet Tracer – Basic Switch and End Device Configuration – Physical Mode

Lab Equipment

2.9.2 Lab – Basic Switch and End Device Configuration

2.9.3. 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 subconfiguration modes. Each of these modes allows the configuration of a particular part or function of the IOS device. Two common subconfiguration 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 global configuration** command. Vlan 1 is not an actual physical interface but a virtual one.

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.

2.9.4 Module Quiz – Basic Switch and End Device Configuration

Download Slide Powerpoint (PPT)

PPT

CCNA 1 v7.0 Curriculum: Module 2 - Basic Switch and End Device Configuration.pptx

1 file(s) 30.15 MB

Download