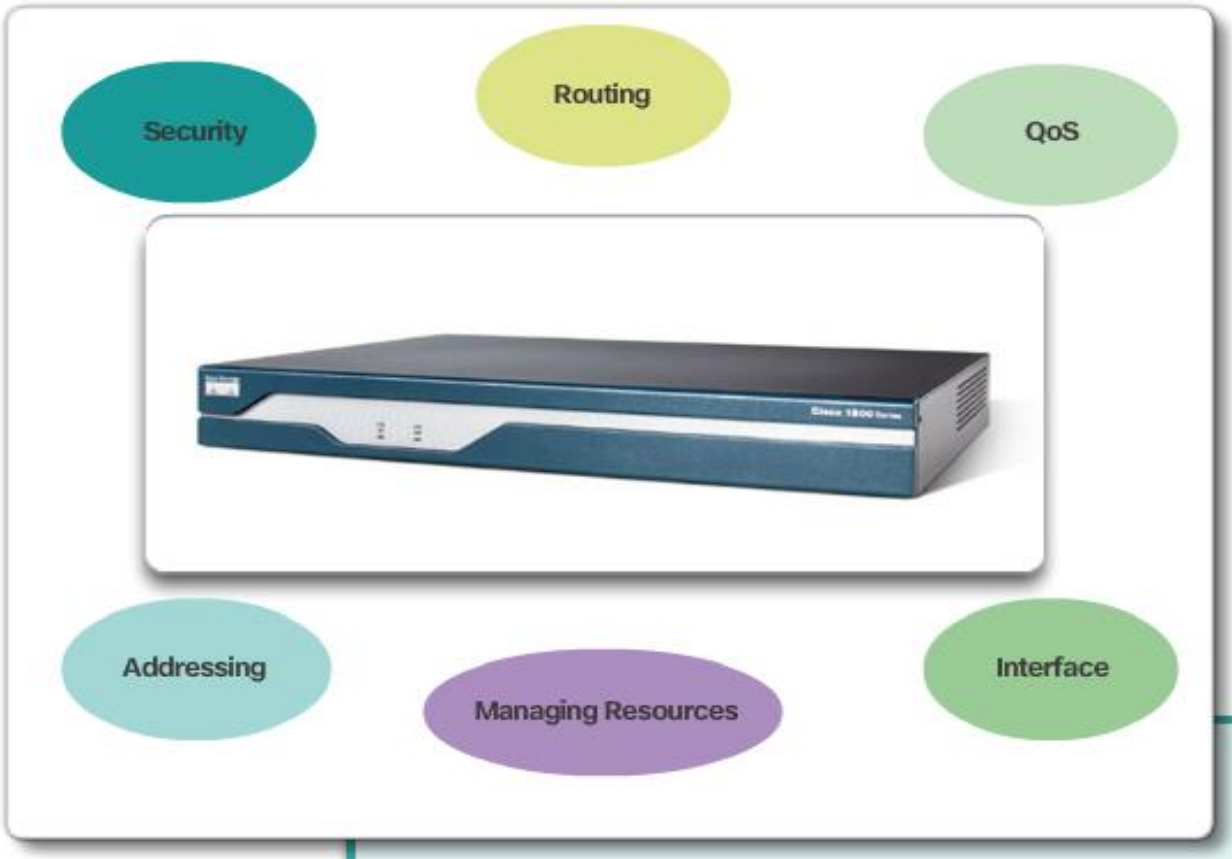
2.0.1.1 Chapter 2: Configure a Network Operating System

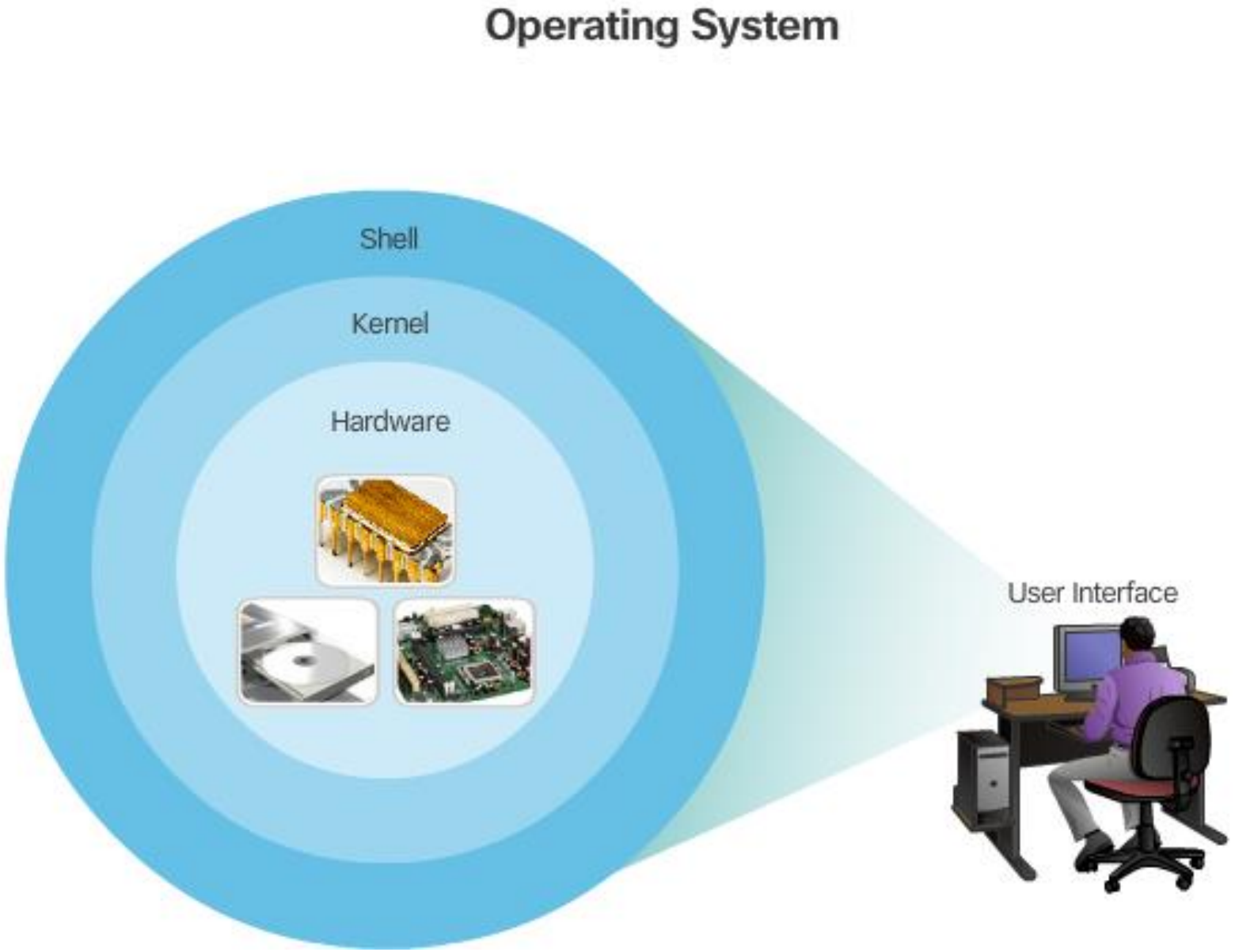
Every computer requires an operating system to function, including computer-based network devices such as switches, routers, access points, and firewalls. These network devices use an operating system called a network operating system.

2.0.1.2 Class Activity - It Is Just an Operating System



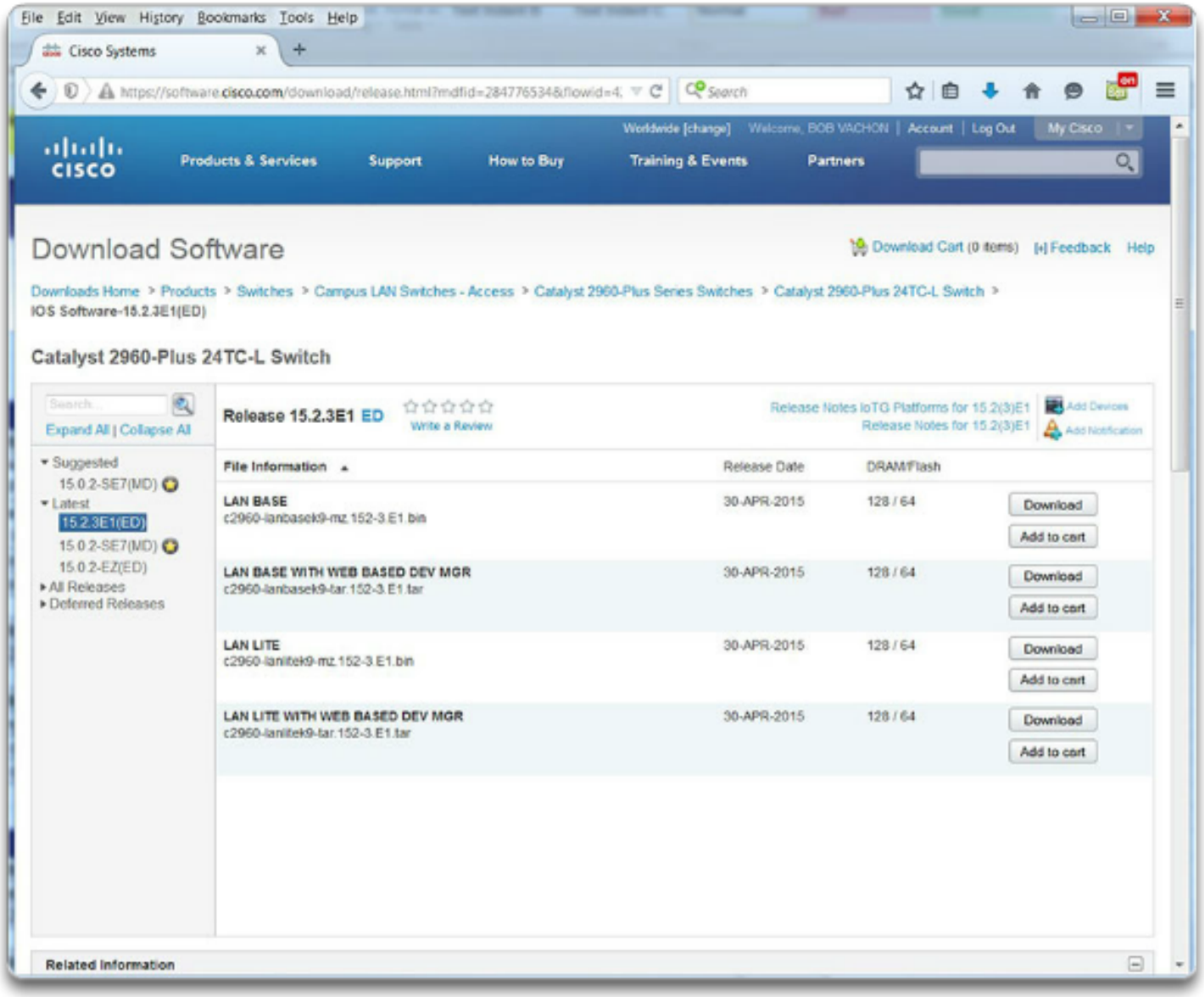
All Cisco network devices use an operating system otherwise known as an internetwork operating system or IOS.

2.1.1.1 Operating Systems



All end devices and network devices require an operating system (OS). As shown in Figure 1, 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).

2.1.1.2 Purpose of OS



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

- 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 like the Cisco IOS on a switch or router enables a network technician to:

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

2.1.2.1 Access Methods

Console

The advantage of using a console port is that the device is accessible even if no networking services have been configured, such as when performing an initial configuration of the networking device. When performing an initial configuration, a computer running terminal emulation software is connected to the console port of the device using a special cable. Configuration commands for setting up the switch or router can be entered on the connected computer.

SSH

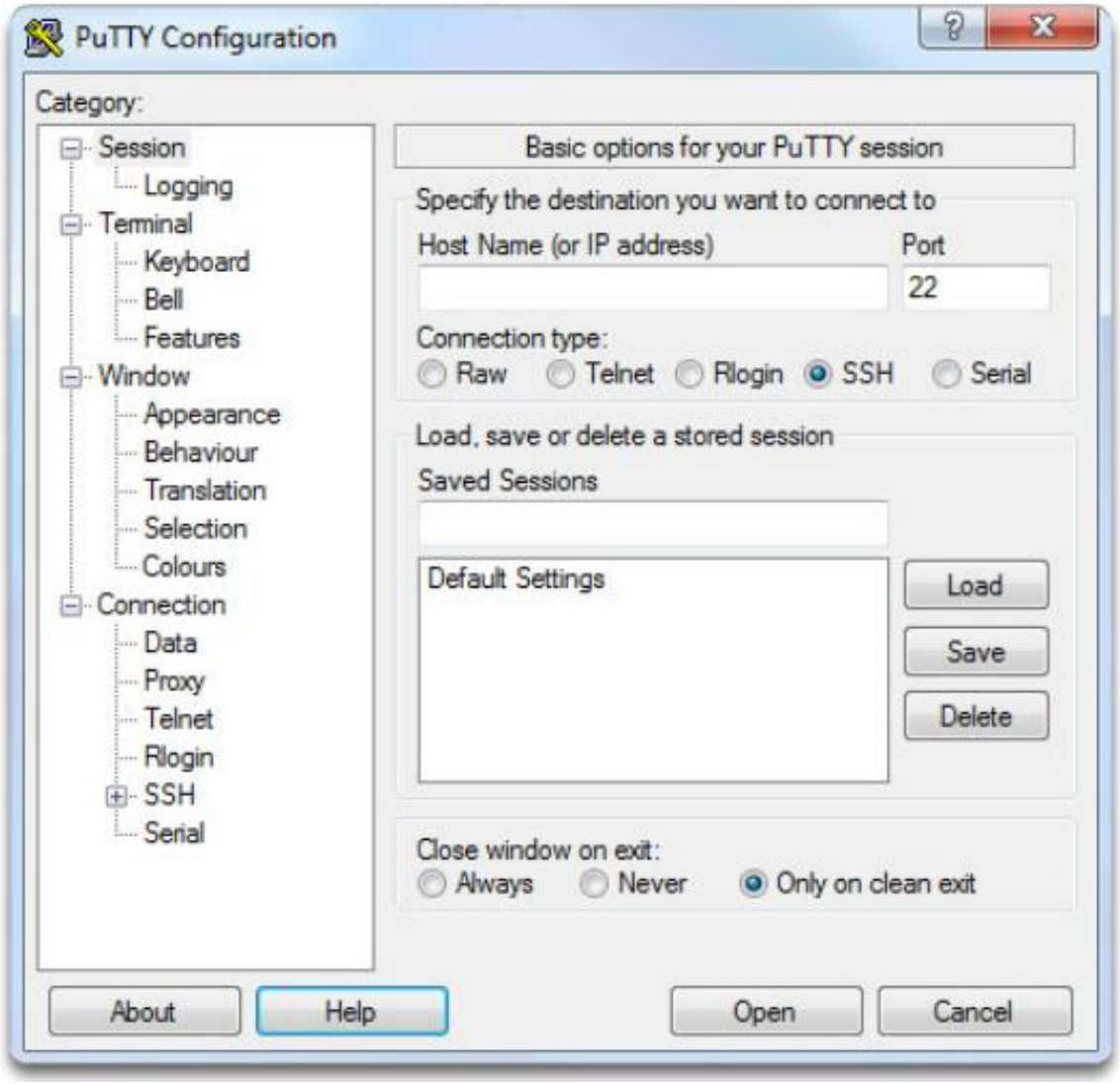
SSH is the recommended method for remote management because it provides a secure connection. SSH provides encrypted password authentication and transport of session data. This keeps the user ID, password, and the details of the management session private. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.

Telnet

Best practice dictates to use SSH instead of Telnet for remote management CLI connections. Cisco IOS includes a Telnet server and a Telnet client that can be used to establish Telnet sessions with other devices.

2.1.2.2 Terminal Emulation Programs

PuTTY



There are a number of excellent terminal emulation programs available for connecting to a networking device either by a serial connection over a console port or by a SSH/Telnet connection. Some of these include:

- PuTTY
- Tera Term
- SecureCRT
- OS X Terminal

2.1.2.3 Activity - Accessing Devices

	Console	Telnet/SSH	AUX
1. You are in the equipment room with a new switch that needs to be configured.	✓		
2. Your manager gives you a special cable and tells you to use it to configure the switch.	✓		
3. You access the IOS by using another intermediary device over a network connection.		✓	
4. You call your manager to tell him you cannot access your router in another city over the Internet. He provides you with the information to access the switch through a telephone connection.			✓

2.1.3.1 Cisco IOS Modes of Operation

Click Play in the figure to view a video demonstration of how to establish a console connection with a switch.

2.1.3.2 Primary Command Modes

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#`

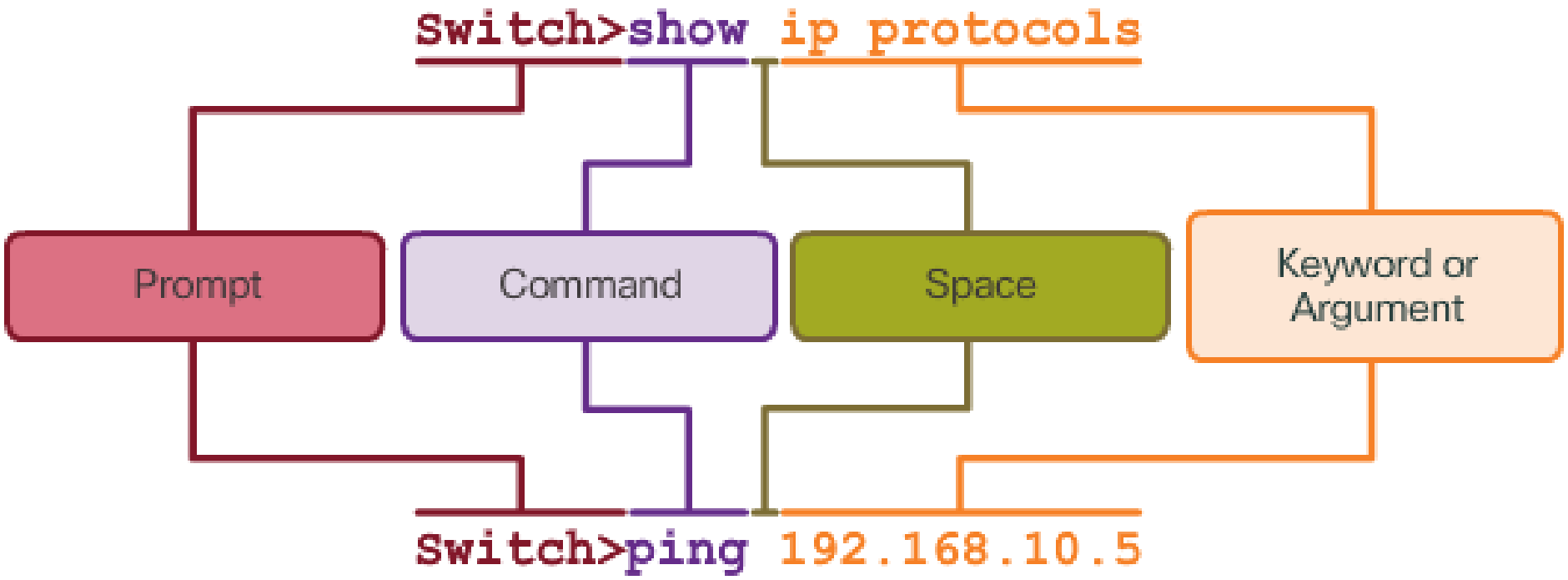
2.1.3.3 Configuration Command Modes

2.1.3.4 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.

2.1.4.1 Basic IOS Command Structure

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 is the command followed by any appropriate keywords and arguments.



2.1.4.2 IOS Command Syntax

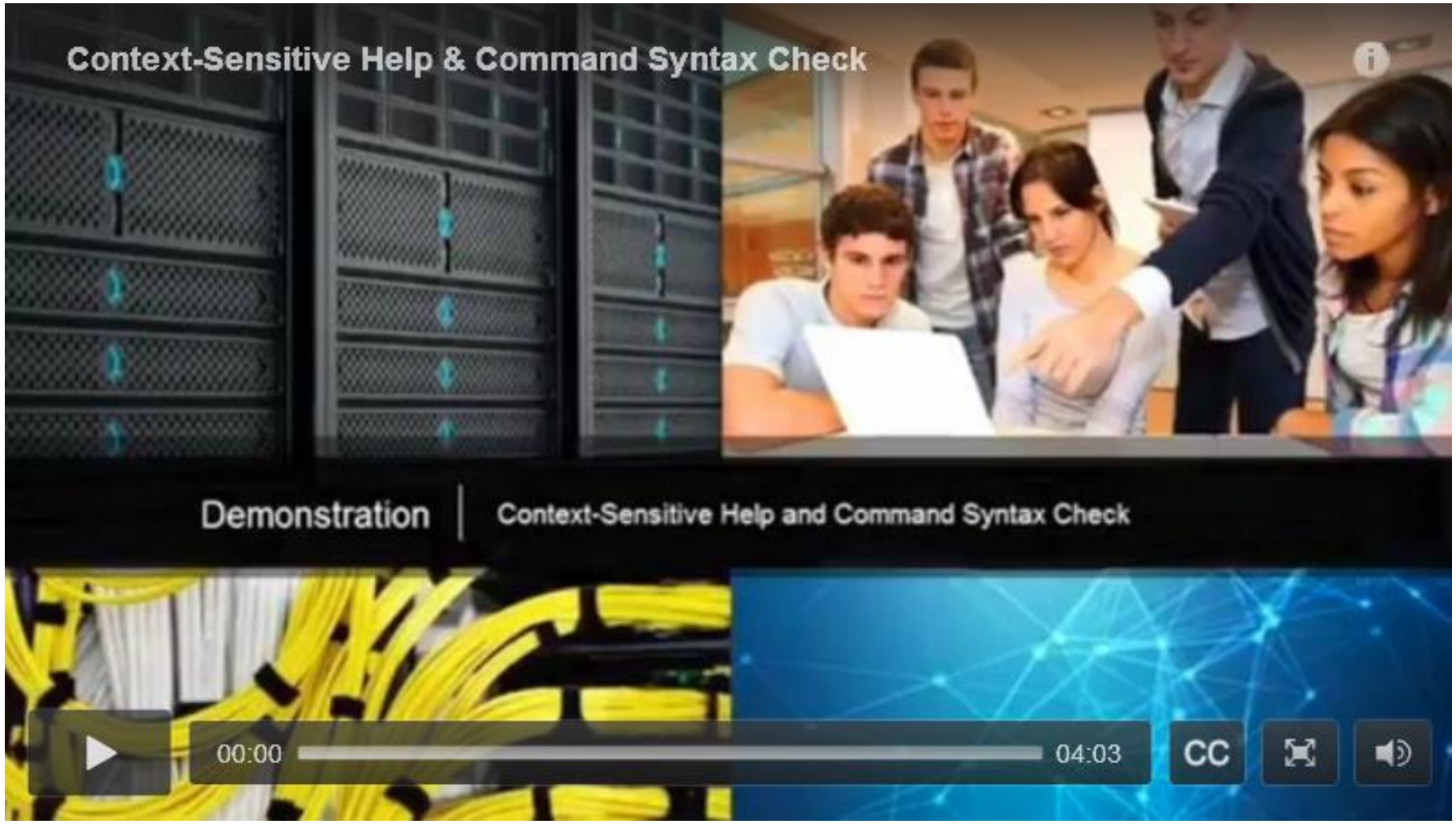
When describing the use of commands, we generally use these conventions.

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.
[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.

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**.

2.1.4.3 IOS Help Features



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

2.1.4.4 Hotkeys and Shortcuts

CLI Hot Keys and Shortcuts

CLI Line Editing	
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.

(NOTE: "**Delete**", the key to erase to the right of the cursor, is not recognized by terminal emulation programs.)

At the "-----More-----" prompt	
Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any Key	Ends the display string, returning to privileged EXEC mode.

Break Keys	
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. Use to abort DNS lookups, traceroutes, pings.

NOTE: **Control** keys - Press and hold the <Ctrl> key and then press the specified letter key.
Escape sequences - Press and release the <Esc> key, and then press the letter key.

2.1.4.5 Video Demonstration – Hotkeys and Shortcuts

2.1.4.6 Packet Tracer - Navigating the IOS

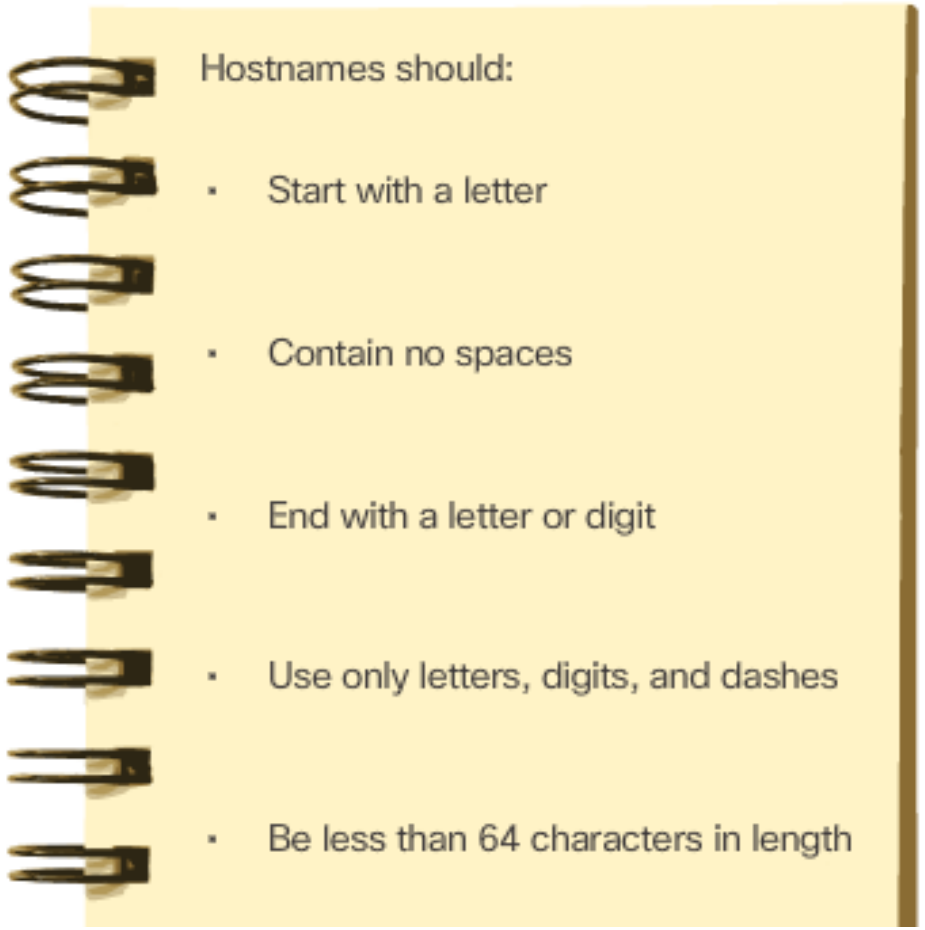
2.1.4.7 Lab - Establishing a Console Session with Tera Term

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

2.2.1.1 Device Names

Guidelines to Choosing a Hostname



2.2.1.2 Configure Hostnames

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

2.2.2.1 Secure Device Access

Limiting Device Access

Securing Administrative Access

- Secure privileged EXEC access with a password
- Secure user EXEC access with a password
- Secure remote Telnet access with a password

Other tasks

- Encrypt all passwords
- Provide legal notification

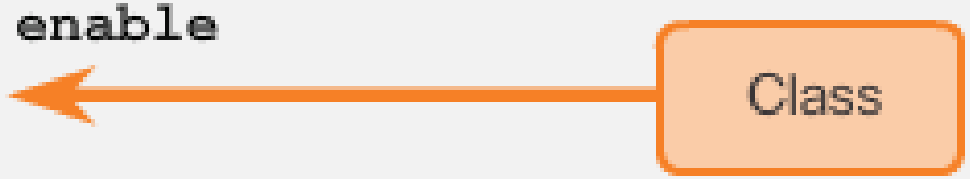
Password Choosing Guidelines

When Choosing Passwords:

- Use passwords that are more than 8 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.
- Don't use common words because these are easily guessed.

2.2.2.2 Configure Passwords

```
Sw-Floor-1> enable
Sw-Floor-1#
Sw-Floor-1# conf terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
Sw-Floor-1# disable
Sw-Floor-1> enable
Password:
Sw-Floor-1#
```



2.2.2.3 Encrypt Passwords

Enter the command to encrypt the plaintext passwords.

```
Switch(config)# service password-encryption
```

Exit global configuration mode and view the running configuration.

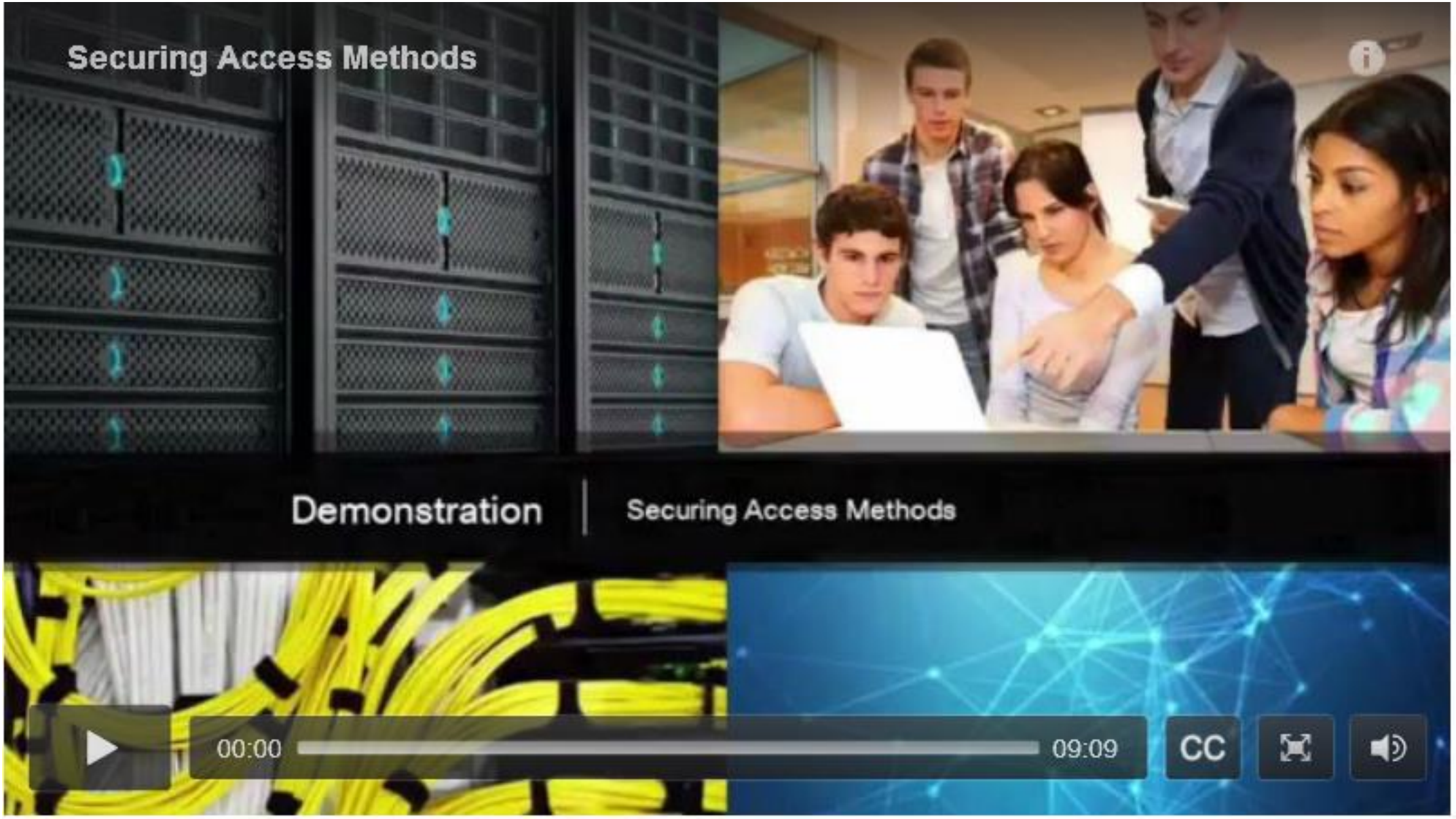
```
Switch(config)# exit

Switch# show running-config
!
<output omitted>
!
line con 0
 password 7 094F471A1A0A
 login
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 login
!
!
end

Switch#
```

You successfully encrypted the plaintext passwords.

2.2.2.4 Banner Messages



2.2.2.5 Syntax Checker - Limiting Access to a Switch

Limit access to a switch.

- Encrypt all passwords.
- Secure the privileged EXEC access.
- Secure the console access.
- Secure the VTY access.

Encrypt all passwords.

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

Secure the privileged EXEC access with the password. Cla55.

```
Sw-Floor-1(config)#  enable secret Cla55
Sw-Floor-1(config)#
```

Secure the console line.

- Use the password Cisc0.
- Allow login.

```
Sw-Floor-1(config)#  line console 0
Sw-Floor-1(config-line)#  password Cisc0
Sw-Floor-1(config-line)#  login
SW-Floor-1(config-line)#
```

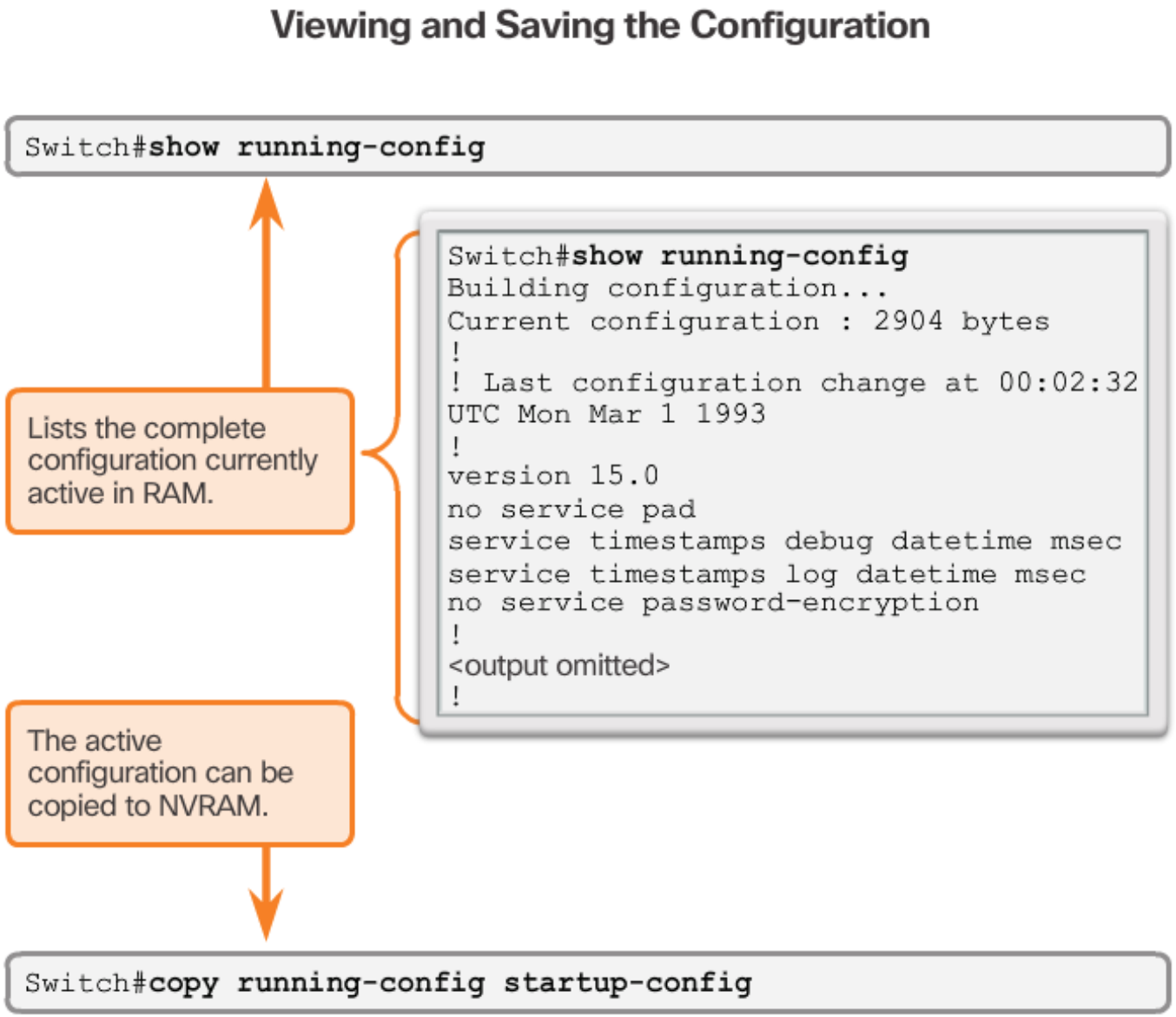
Secure the first 16 VTY lines.

- Use the password Cisc0.
- Allow login.

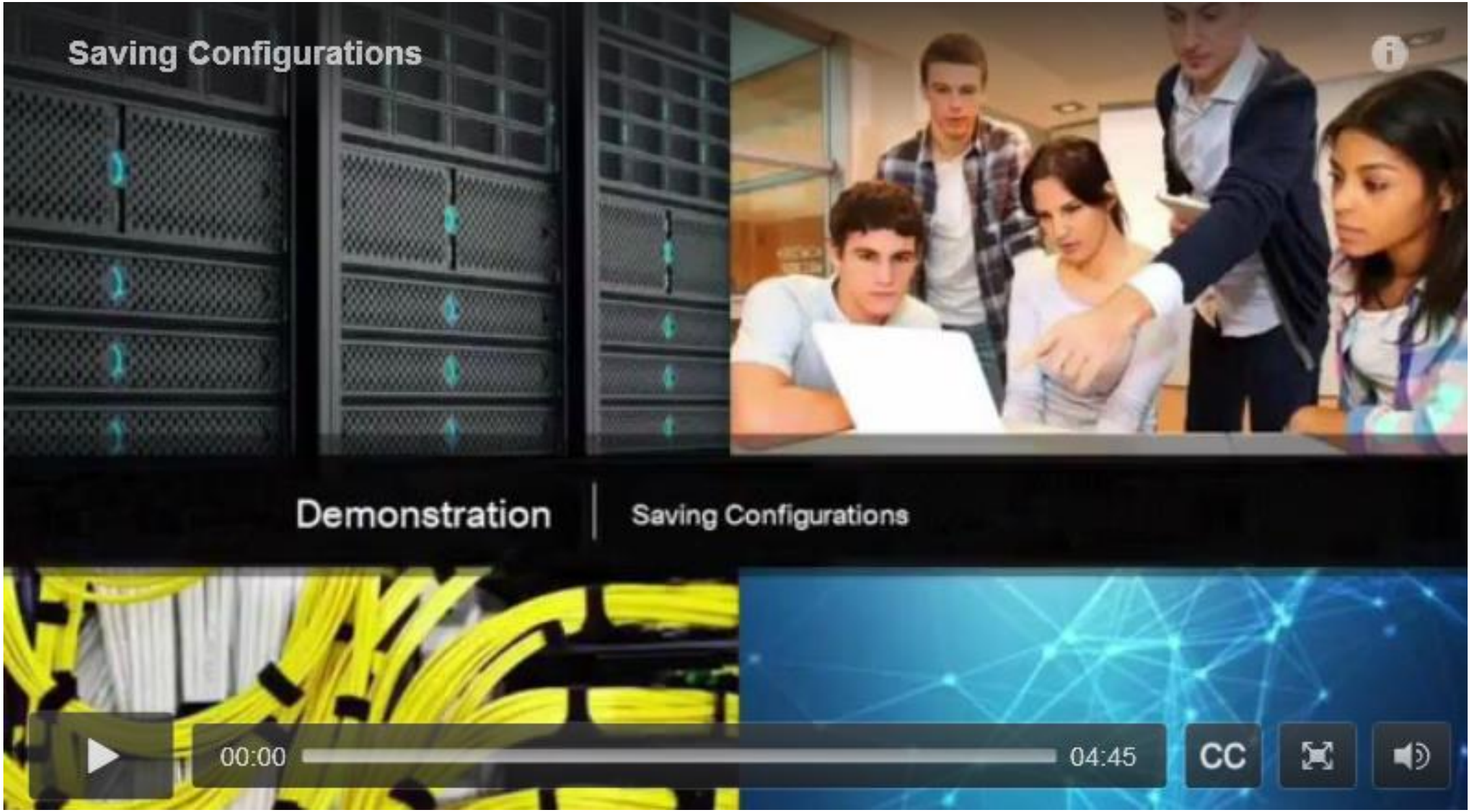
```
Sw-Floor-1(config)#  line vty 0 15
Sw-Floor-1(config-line)#  password Cisc0
Sw-Floor-1(config-line)#  login
Sw-Floor-1(config-line)#
```

You have successfully limited access to a switch.

2.2.3.1 Save the Running Configuration File

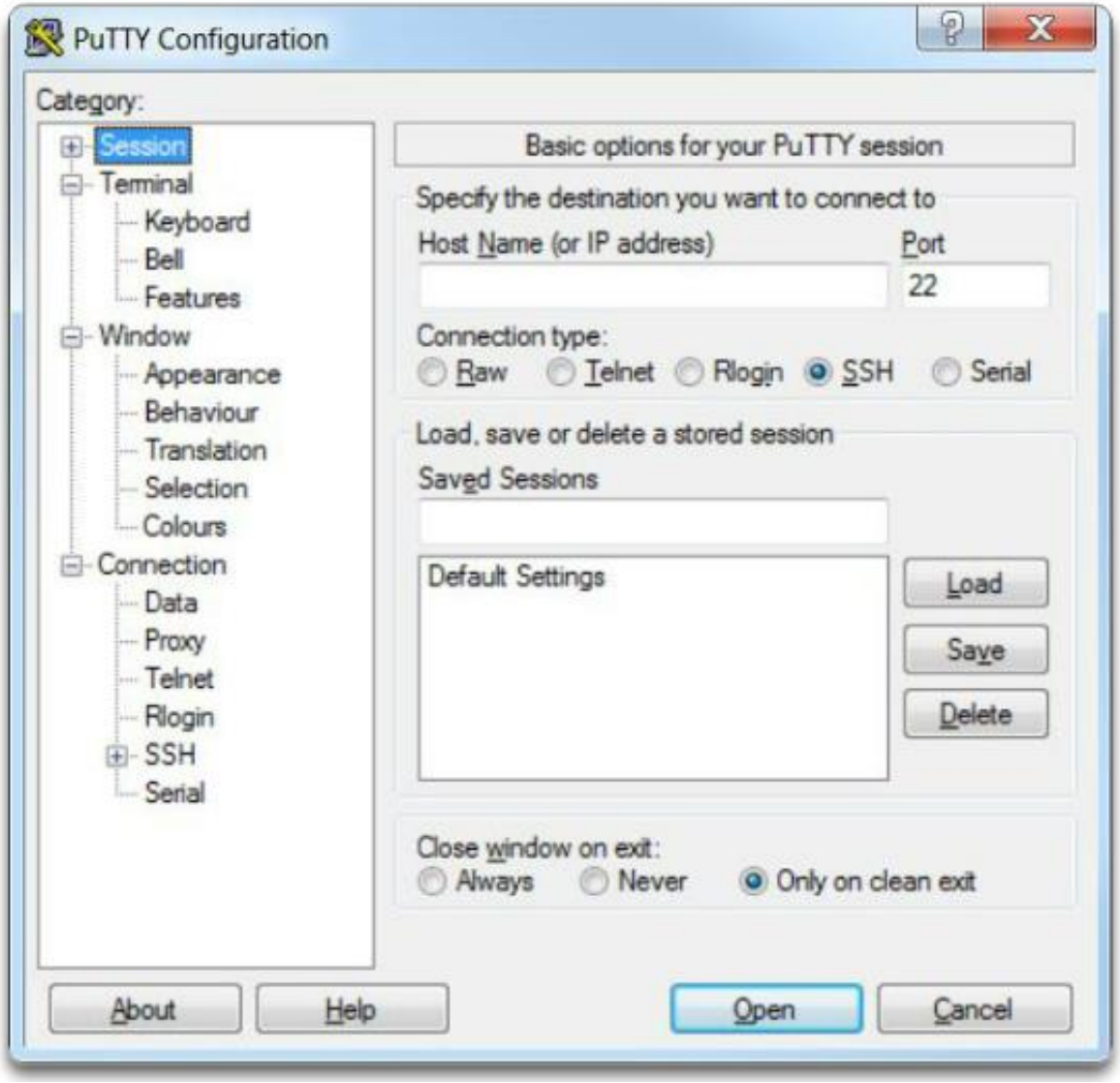


2.2.3.2 Alter the Running Configuration



2.2.3.3 Capture Configuration to a Text File

Using PuTTY to Capture Console Session



2.2.3.4 Packet Tracer - Configuring Initial Switch Settings

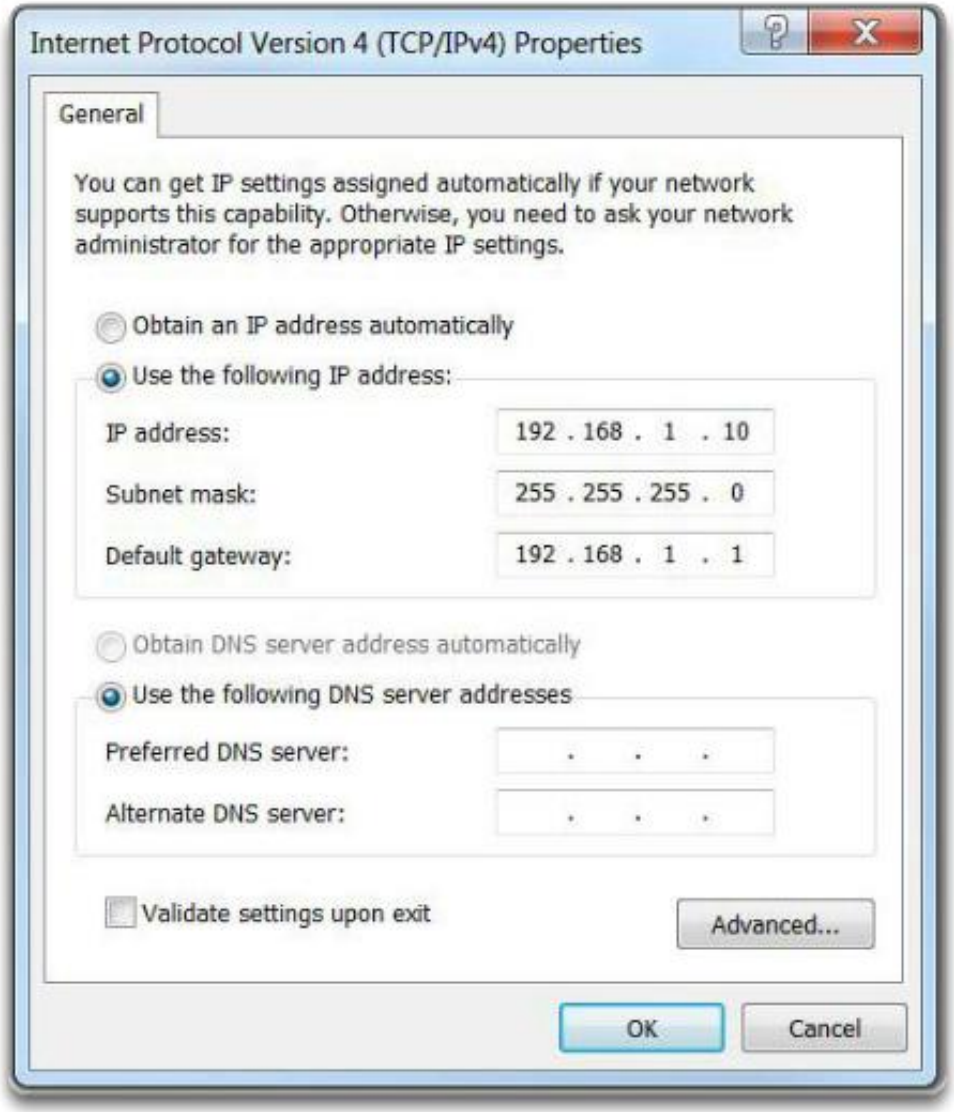
2.3.1.1 IP Addresses

Connecting End Devices

Devices Requiring IP Addresses

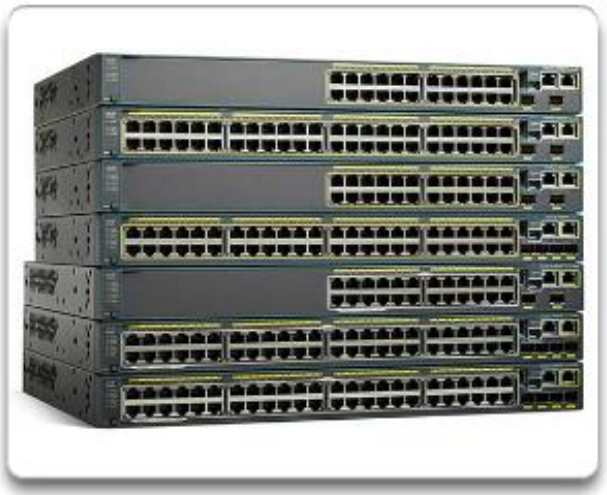
- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Smart phones
- Mobile handheld devices (such as wireless barcode scanners)

Configuring a Static IP Address on a Host

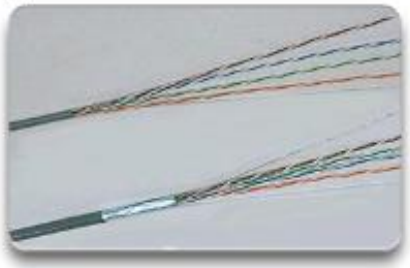


2.3.1.2 Interfaces and Ports

Interfaces and Ports



Copper

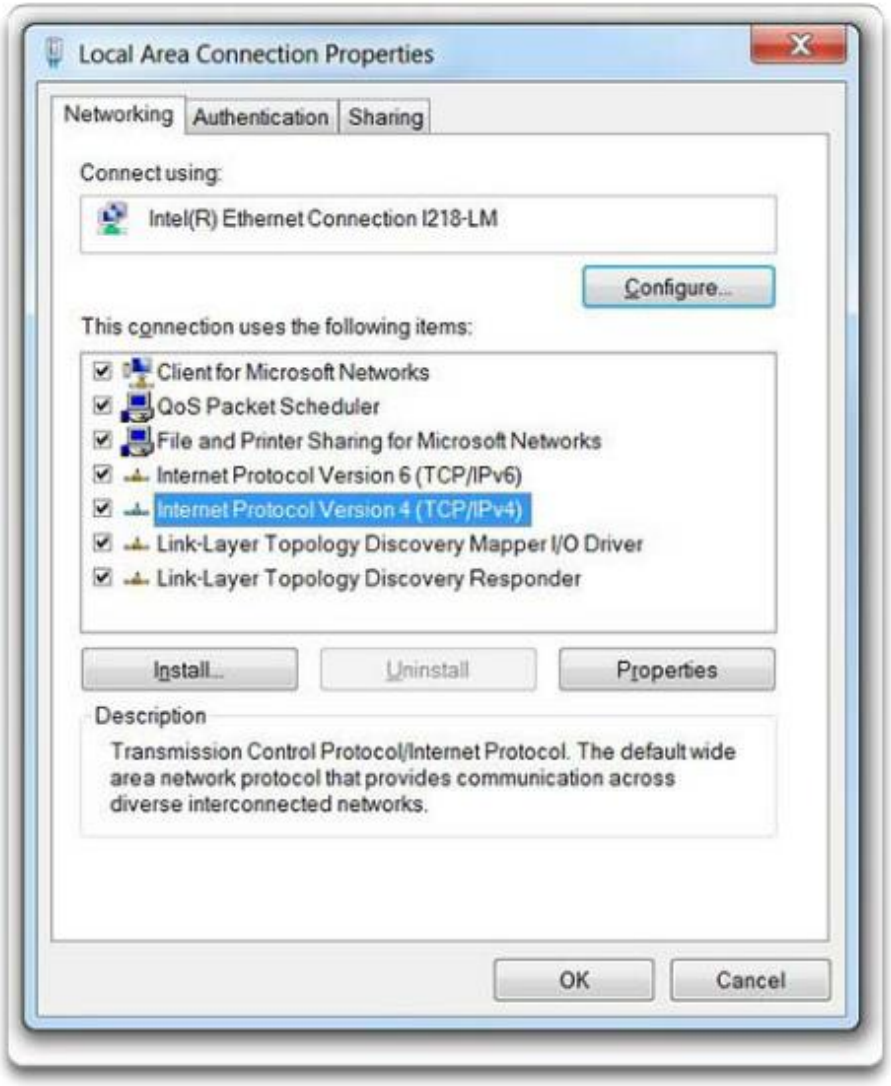


Fiber Optics

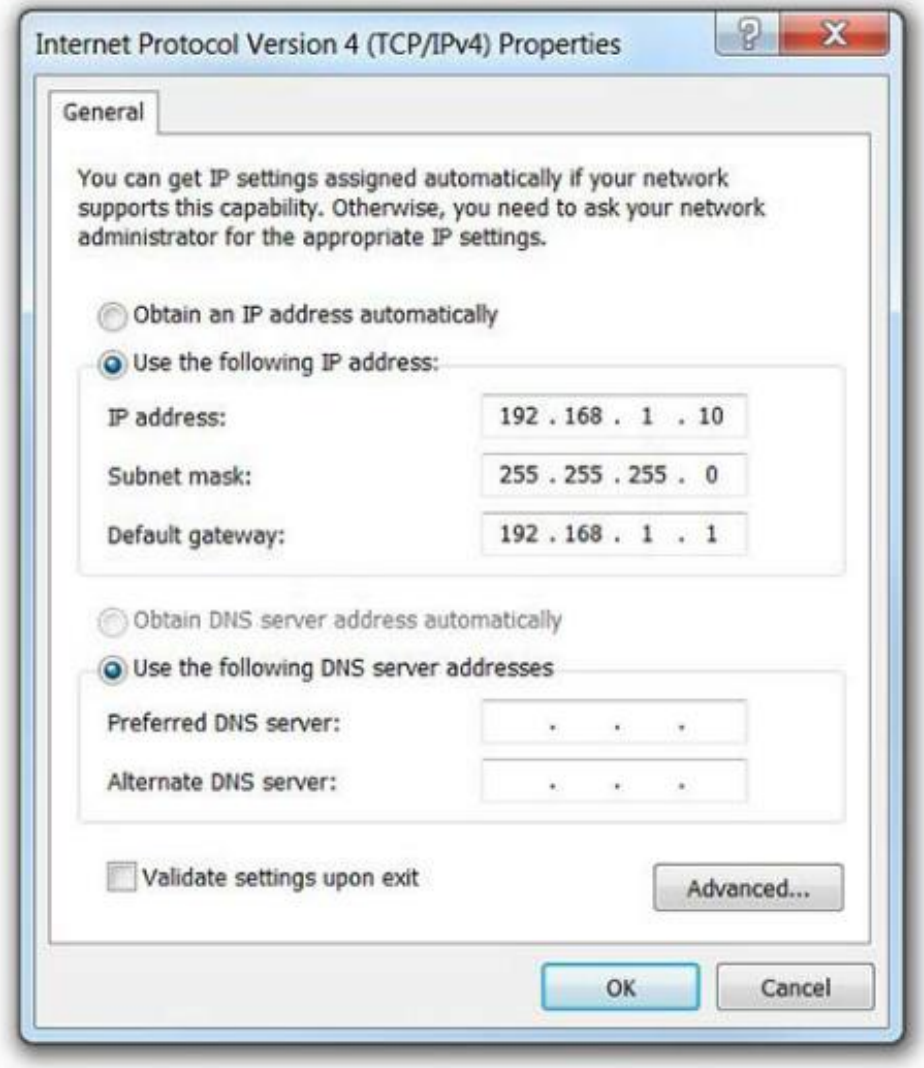
Wireless

2.3.2.1 Manual IP Address Configuration for End Devices

Ethernet Adapter Properties



Manually Assigning IPv4 Address Information



2.3.2.2 Automatic IP Address Configuration for End Devices

Assigning Dynamic Addresses

Verifying Windows PC IP Configuration

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

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
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. . . . . . . . . . . : 10.82.240.197
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.82.240.198

-----------------------------------
```

You successfully displayed the IP configuration on a Windows PC.

2.3.2.3 Switch Virtual Interface Configuration

2.3.2.4 Syntax Checker - Configuring a Switch Virtual Interface

Configure a Switch Virtual Interface

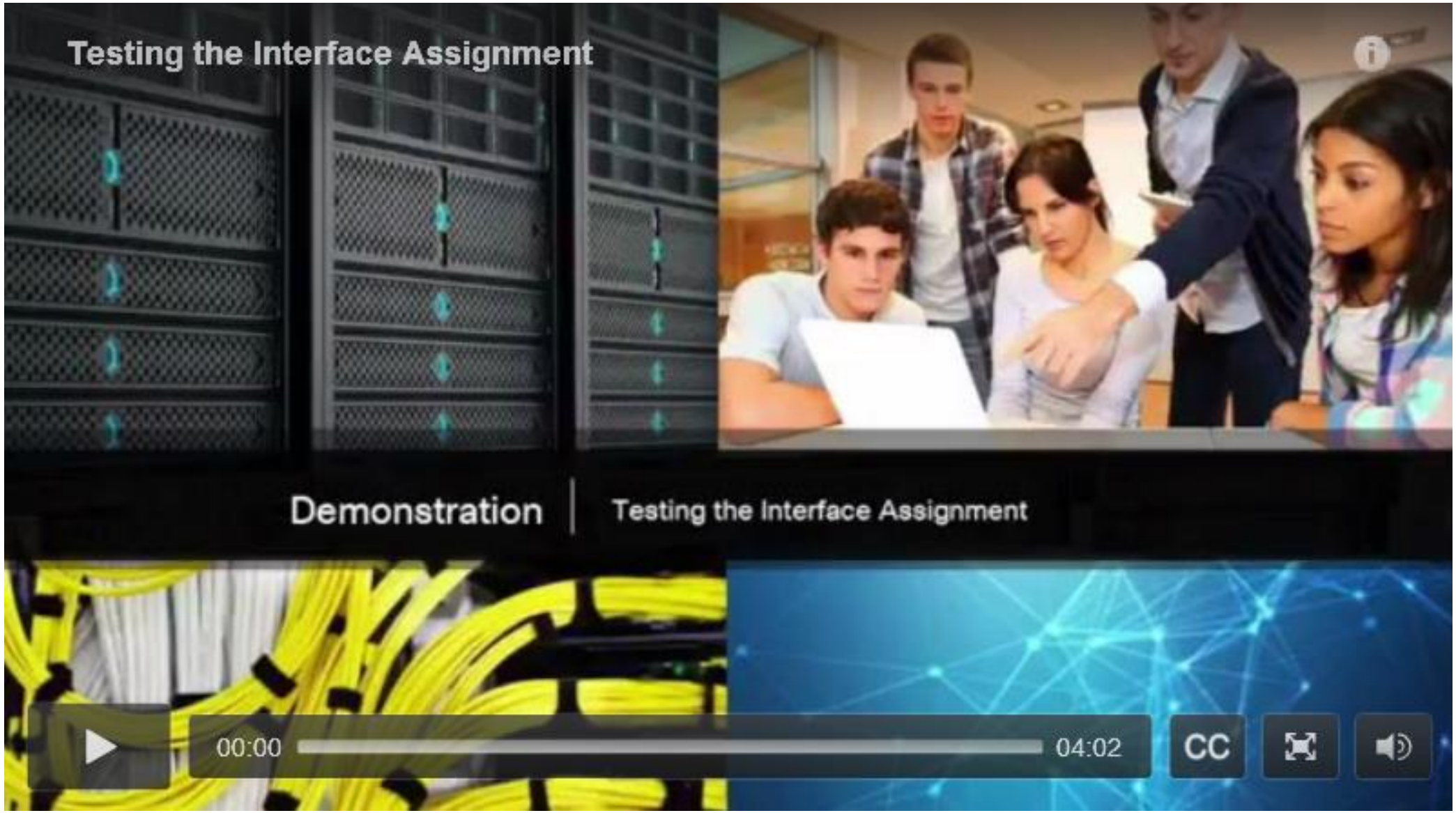
- Enter interface configuration mode for VLAN 1.
- Configure the IPv4 address as 192.168.10.2 and the subnet mask as 255.255.255.0.
- Enable the interface.

```
Switch(config)#  interface vlan 1
Switch(config-if)#  ip address 192.168.10.2 255.255.255.0
Switch(config-if)#  no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Switch(config-if)#
```

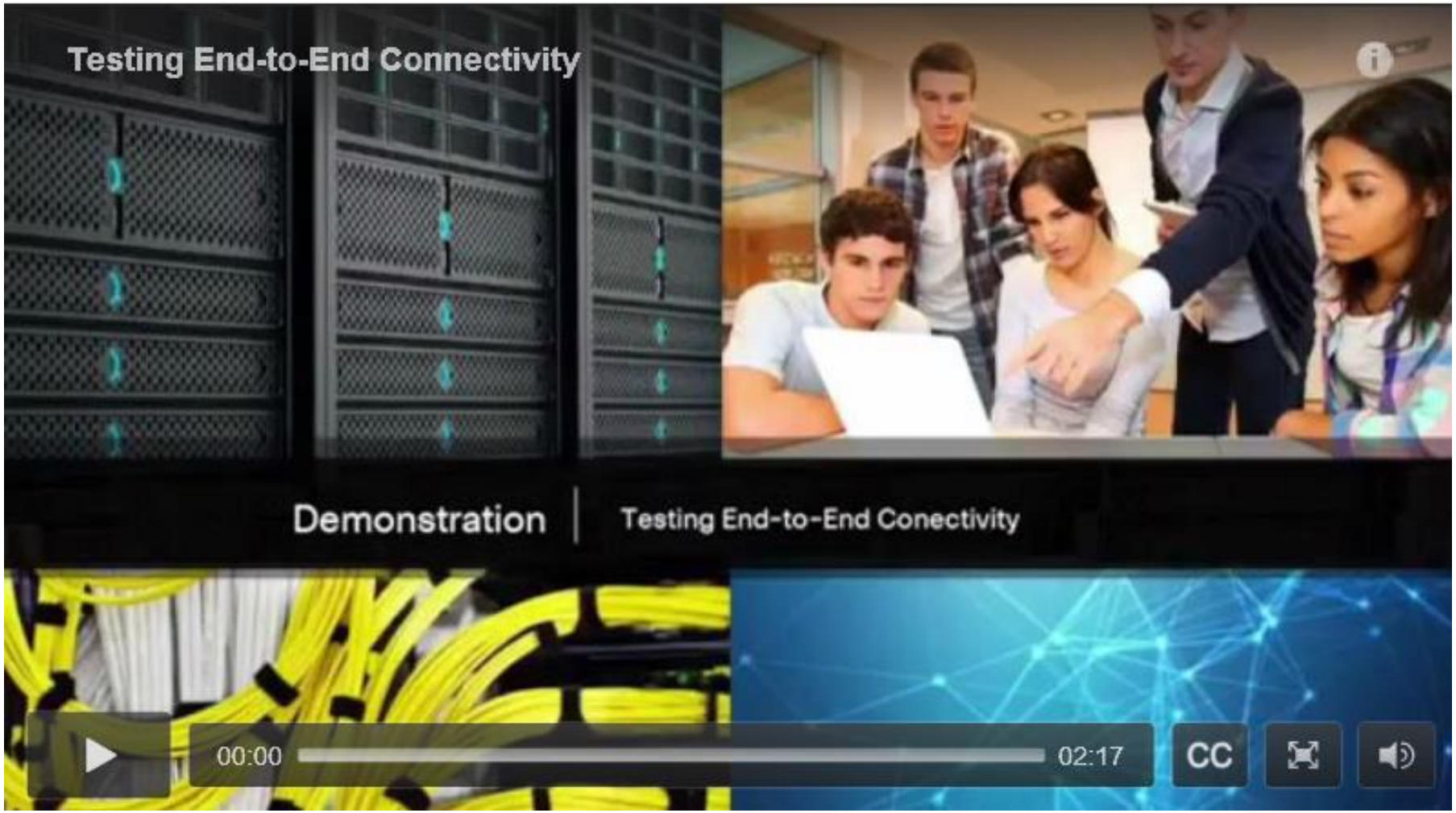
You have successfully configured the switch virtual interface for VLAN 1.

2.3.2.5 Packet Tracer - Implementing Basic Connectivity

2.3.3.1 Interface Addressing Verification



2.3.3.2 End-to-End Connectivity Test



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

2.3.3.3 Lab - Building a Simple Network

In this lab, you will complete the following objectives:

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

2.3.3.4 Lab - Configuring a Switch Management Address

In this lab, you will complete the following objectives:

- Part 1: Configure a Basic Network Device
- Part 2: Verify and Test Network Connectivity

2.4.1.1 Class Activity - Tutor Me

The CLI commands the Cisco IOS!

2.4.1.2 Packet Tracer - Skills Integration Challenge

2.4.1.3 Chapter 2: Configure a Network Operating System