

# Chapter 2: Configure a Network Operating System

CCNA Routing and Switching

Introduction to Networks v6.0



# Chapter 2 - Sections & Objectives

- 2.1 IOS Bootcamp
  - Explain the features and functions of the Cisco IOS Software.
  - Explain the purpose of Cisco IOS.
  - Explain how to access a Cisco IOS device for configuration purposes.
  - Explain how to navigate Cisco IOS to configure network devices.
  - Describe the command structure of Cisco IOS software.
- 2.2 Basic Device Configuration
  - Configure initial settings on a network device using the Cisco IOS Software.
  - Configure hostnames on a Cisco IOS device using the CLI.
  - Use Cisco IOS commands to limit access to device configurations.
  - Use IOS commands to save the running configuration.

# Chapter 2 - Sections & Objectives (Cont.)

## ▪ 2.3 Address Schemes

- Given an IP addressing scheme, configure IP address parameters on devices to provide end-to-end connectivity in a small to medium-sized business network.
- Explain how devices communicate across network media.
- Configure a host device with an IP address.
- Verify connectivity between two end devices.

# 2.1 IOS Bootcamp

# Cisco IOS

## Operating System

Cisco devices use the Cisco **Internetwork Operating System (IOS)**.

- Although used by Apple, iOS is a registered trademark of Cisco in the U.S. and other countries and is used by Apple under license.

- All electronic devices require an operating system.
  - Windows, Mac, and Linux for PCs and laptops
  - Apple iOS and Android for smart phones and tablets
  - Cisco IOS for network devices (e.g., switches, routers, wireless AP, firewall, ...).

### OS Shell

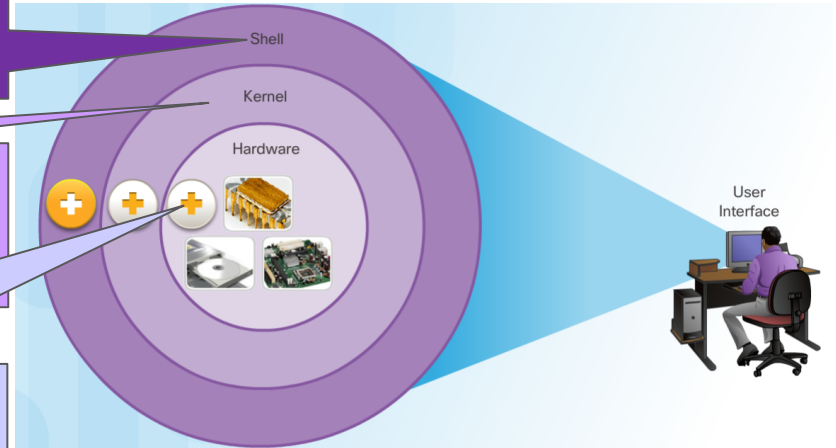
- The OS shell is either a command-line interface (CLI) or a graphical user interface (GUI) and enables a user to interface with applications.

### OS Kernel

- The OS kernel communicates directly with the hardware and manages how hardware resources are used to meet software requirements.

### Hardware

- The physical part of a computer including underlying electronics.



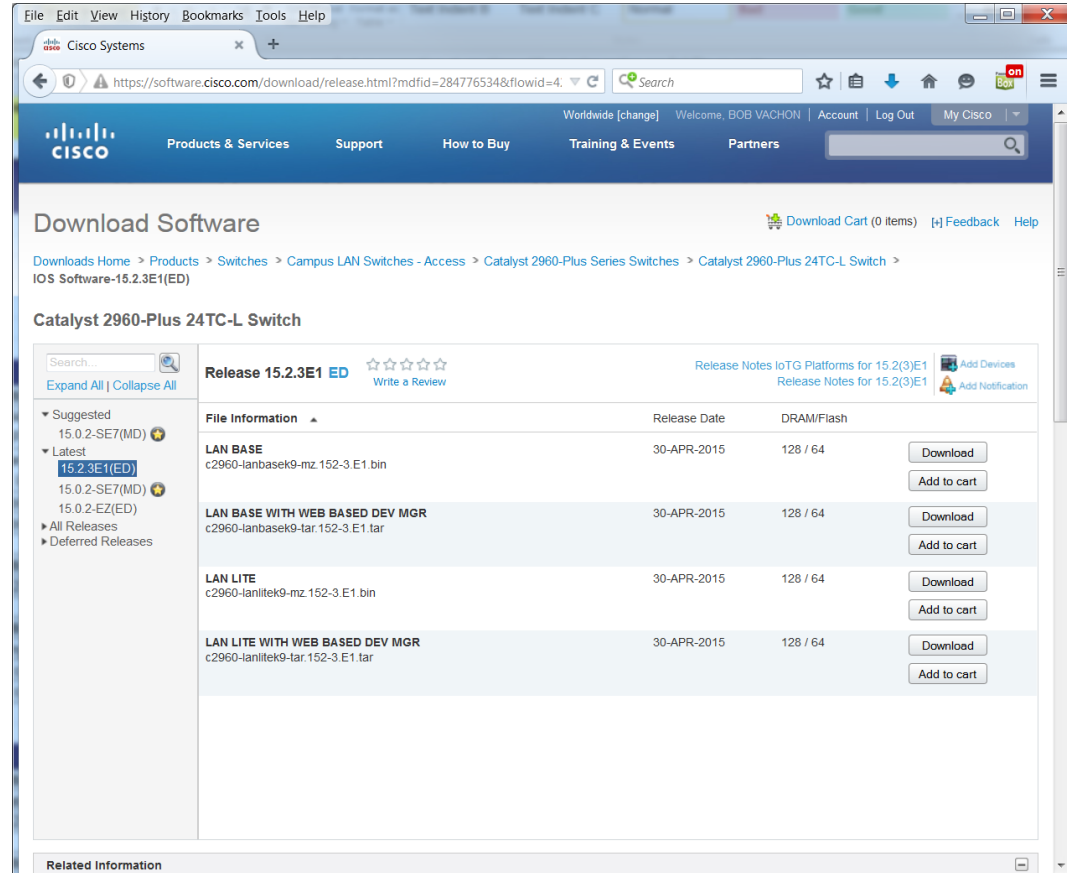
# Purpose of OS

- Using a GUI enables a user to:
  - Use a mouse to make selections and run programs
  - Enter text and text-based commands
  
- Using a CLI on a Cisco IOS 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
  
- There are many distinct variations of Cisco IOS:
  - IOS for switches, routers, and other Cisco networking devices
  - IOS numbered versions for a given Cisco networking devices

## Purpose of OS (Cont.)

- All devices come with a default IOS and feature set. It is possible to upgrade the IOS version or feature set.
- An IOS can be downloaded from cisco.com. However, a Cisco Connection Online (CCO) account is required.

**Note:** The focus of this course will be on Cisco IOS Release 15.x.



The screenshot shows the Cisco Software Download page for the Catalyst 2960-Plus 24TC-L Switch. The page is titled "Download Software" and includes a navigation menu with options like "Products & Services", "Support", "How to Buy", "Training & Events", and "Partners". The main content area displays the "Catalyst 2960-Plus 24TC-L Switch" and lists the available releases. The current release is "Release 15.2.3E1(ED)", which is highlighted in blue. Below the release information, there is a table of files for download, including "LAN BASE", "LAN BASE WITH WEB BASED DEV MGR", "LAN LITE", and "LAN LITE WITH WEB BASED DEV MGR". Each file entry includes the file name, release date (30-APR-2015), and DRAM/Flash requirements (128 / 64). There are "Download" and "Add to cart" buttons for each file.

File Information	Release Date	DRAM/Flash	
<b>LAN BASE</b> c2960-lanbasek9-mz.152-3.E1.bin	30-APR-2015	128 / 64	<a href="#">Download</a> <a href="#">Add to cart</a>
<b>LAN BASE WITH WEB BASED DEV MGR</b> c2960-lanbasek9-tar.152-3.E1.tar	30-APR-2015	128 / 64	<a href="#">Download</a> <a href="#">Add to cart</a>
<b>LAN LITE</b> c2960-lanlitek9-mz.152-3.E1.bin	30-APR-2015	128 / 64	<a href="#">Download</a> <a href="#">Add to cart</a>
<b>LAN LITE WITH WEB BASED DEV MGR</b> c2960-lanlitek9-tar.152-3.E1.tar	30-APR-2015	128 / 64	<a href="#">Download</a> <a href="#">Add to cart</a>

## Access Methods

- The three most common ways to access the IOS are:
  - **Console port** – Out-of-band serial port used primarily for management purposes such as the initial configuration of the router.
  - **Secure Shell (SSH)** - Inband method for remotely and securely establishing a CLI session over a network. User authentication, passwords, and commands sent over the network are encrypted. As a best practice, use SSH instead of Telnet whenever possible.
  - **Telnet** – Inband interfaces remotely establishing a CLI session through a virtual interface, over a network. User authentication, passwords, and commands are sent over the network in plaintext.

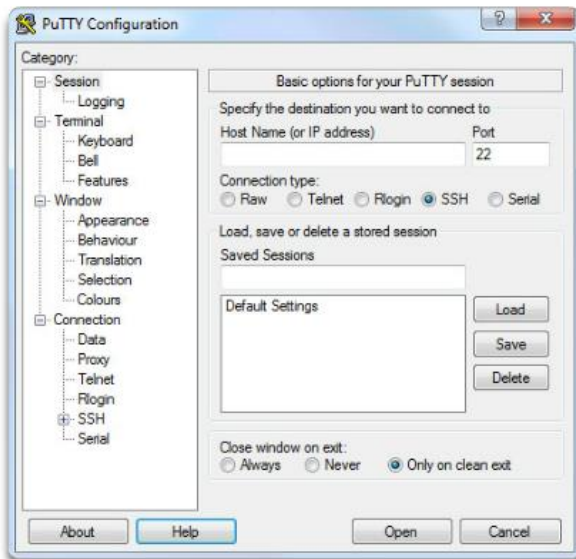
**Note:** The AUX port is an on older method of establishing a CLI session remotely via a telephone dialup connection using a modem.



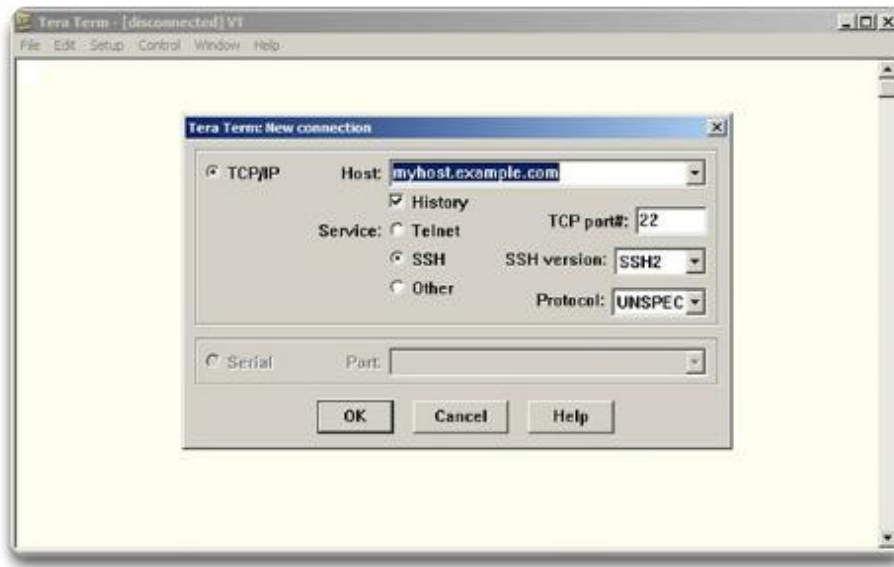
# Terminal Emulation Program

- Regardless of access method, a terminal emulation program will be required. Popular terminal emulation programs include PuTTY, Tera Term, SecureCRT, and OS X Terminal.

PuTTY



Tera Term



# Cisco IOS Modes of Operation

- The Cisco IOS modes use a hierarchical command structure.
- Each mode has a distinctive prompt and is used to accomplish particular tasks with a specific set of commands that are available only to that mode.



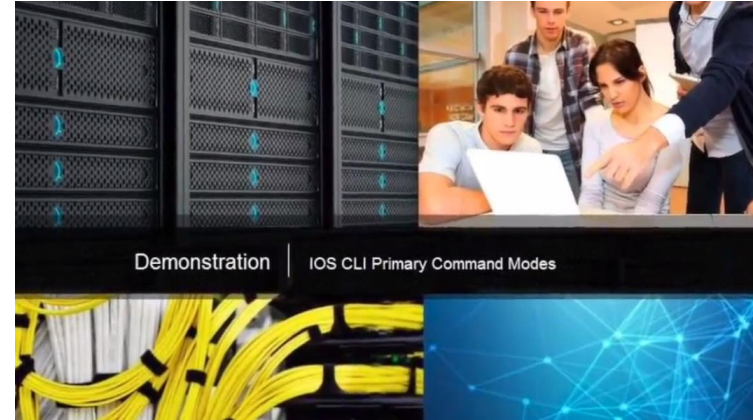
# Primary Command Modes

- The user EXEC mode allows only a limited number of basic monitoring commands.
  - Often referred to as “view-only” mode.
  - By default, there is no authentication required to access the user EXEC mode but it should be secured.
- The privileged EXEC mode allows the execution of configuration and management commands.
  - Often referred to as “enable mode” because it requires the **enable** user EXEC command.
  - By default, there is no authentication required to access the user EXEC mode but it should be secured.

Command Mode	Description	Default Device Prompt
User Exec Mode	<ul style="list-style-type: none"><li>▪ Mode allows access to only a limited number of basic monitoring commands.</li><li>▪ It is often referred to as “view-only” mode.</li></ul>	Switch> Router>
Privileged EXEC Mode	<ul style="list-style-type: none"><li>▪ Mode allows access to all commands and features.</li><li>▪ The user can use any monitoring commands and execute configuration and management commands.</li></ul>	Switch# Router#

# Configuration Command Modes

- The primary configuration mode is called **global configuration** or simply, **global config**.
  - Use the **configure terminal** command to access.
  - Changes made affect the operation of the device.
- Specific sub configuration modes can be accessed from global configuration mode. Each of these modes allows the configuration of a particular part or function of the IOS device.
  - **Interface mode** - to configure one of the network interfaces.
  - **Line mode** - to configure the console, AUX, Telnet, or SSH access.



# 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 return to user EXEC mode, use the **disable** command.
- Various methods can be used to exit / quit configuration modes:
  - **exit** - Used to move from a specific mode to the previous more general mode, such as from interface mode to global config.
  - **end** - Can be used to exit out of global configuration mode regardless of which configuration mode you are in.
  - **^z** - Works the same as **end**.



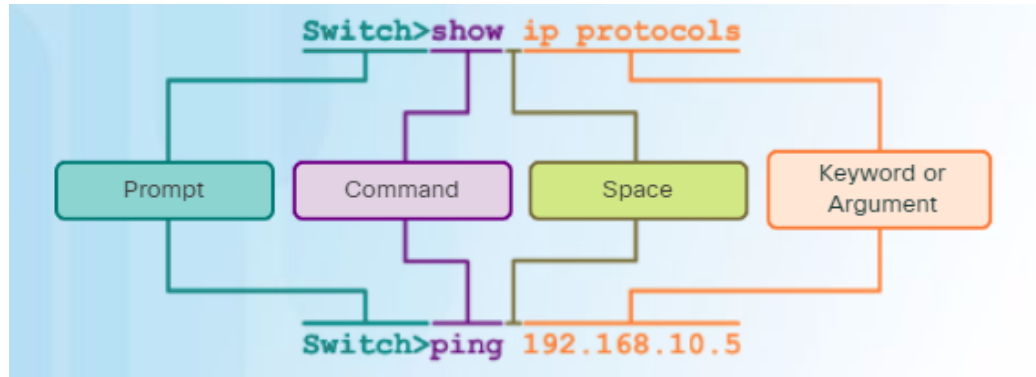
# Navigate Between IOS Modes (Cont.)

- The following provides an example of navigating between IOS modes:
  - Enter privileged EXEC mode using the **enable** command.
  - Enter global config mode using the **configure terminal** command.
  - Enter interface sub-config mode using the **interface fa0/1** command.
  - Exit out of each mode using the **exit** command.
  - The remainder of the configuration illustrates how you can exit a sub-config mode and return to privileged EXEC mode using either the **end** or **^Z** key combination.



# 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 at the appropriate mode.



- The syntax for a command is the command followed by any appropriate keywords and arguments.
  - **Keyword** - a specific parameter defined in the operating system (in the figure, **ip protocols**)
  - **Argument** - not predefined; 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.



# IOS Command Syntax

- To determine the keywords and arguments required for a command, refer to the command syntax
  - Refer to the following table when looking at command syntax.

Convention	Description
<b>boldface</b>	Boldface text indicates commands and keywords that you enter literally as shown.
<i>italics</i>	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.

- Examples:
  - **description** *string* - The command is used to add a description to an interface. The *string* argument is text entered by the administrator such as **description** *Connects to the main headquarter office switch.*
  - **ping** *ip-address* - The command is **ping** and the user-defined argument is the *ip-address* of the destination device such as in **ping** *10.10.10.5*



# The Command Structure

## IOS Help Features

- IOS Context-Sensitive Help:
  - Context-sensitive help provides a list of commands and the arguments associated with those commands within the context of the current mode.
  - To access context-sensitive help, enter a question mark ?, at any prompt.



# IOS Help Features (Cont.)

- IOS Command Syntax Check:
  - The command line interpreter checks an entered command from left to right to determine what action is being requested.
  - If the interpreter understands the command, the requested action is executed and the CLI returns to the appropriate prompt.
  - If the interpreter discovers an error, the IOS generally provides feedback such as “Ambiguous command”, “Incomplete command”, or “Incorrect command”.



# Hot Keys and Shortcuts

- 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 of **con** will not work because more than one command begins with **con**.
  - Keywords can also be shortened.

# Video Demonstration - Hotkeys and Shortcuts

The IOS CLI support the following hotkeys:

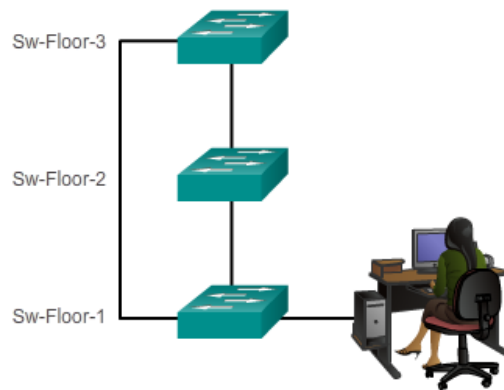
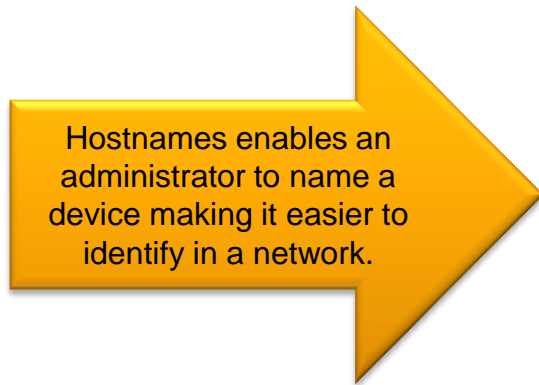
- **Down Arrow** – Allows the user to scroll through command history.
- **Up Arrow** - Allows the user to scroll backward through commands.
- **Tab** - Completes the remainder of a partially entered command.
- **Ctrl-A** - Moves to the beginning of the line.
- **Ctrl-E** – Moves to the end of the line.
- **Ctrl-R** – Redisplays a line.
- **Ctrl-Z** – Exits the configuration mode and returns to user EXEC.
- **Ctrl-C** – Exits the configuration mode or aborts the current command.
- **Ctrl-Shift-6** – Allows the user to interrupt an IOS process (e.g., ping).



# 2.2 Basic Device Configuration

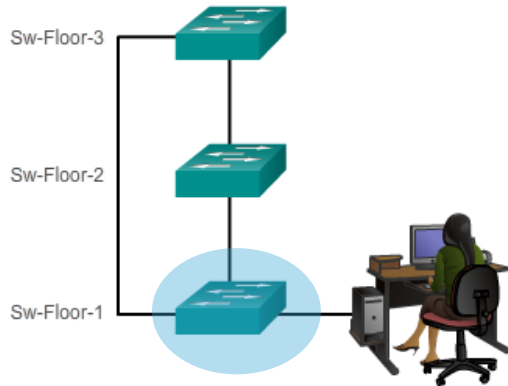
# Device Names

- The first step when configuring a switch is to assign it a unique device name, or hostname.
- Hostnames appear in CLI prompts, can be used in various authentication processes between devices, and should be used on topology diagrams.
- Without a hostname, network devices are difficult to identify for configuration purposes.



# Configure Hostnames

- Once the naming convention has been identified, the next step is to apply the names to the devices using the CLI.
- The **hostname** *name* global configuration command is used to assign a name.



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

# Limit Access to Device Configurations

## Limiting Device Access

- **Step 1** - Secure network devices to physically limit access by placing them in wiring closets and locked racks.
- **Step 2** - Enforce secure passwords as passwords are the primary defense against unauthorized access to network devices.
- Limit administrative access as follows.
- Use strong password as suggested.

### 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

### 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.

For convenience, most labs and examples in this course use the simple but weak passwords **cisco** or **class**.



# Limit Access to Device Configurations

## Configure Passwords

- Secure privileged EXEC access using the **enable secret** *password* global config command.
- Secure user EXEC access by configuring the line console as follows:

Securing User EXEC Mode	Description
Switch(config)# <b>line console 0</b>	Command enters line console configuration mode.
Switch(config-line)# <b>password</b> <i>password</i>	Command specifies the line console password.
Switch(config-line)# <b>login</b>	Command makes the switch require the password.

- Secure remote Telnet or SSH access by configuring the Virtual terminal (VTY) lines as follows:

Securing Remote Access	Description
Switch(config)# <b>line vty 0 15</b>	Cisco switches typically support up to 16 incoming VTY lines numbered 0 to 15.
Switch(config-line)# <b>password</b> <i>password</i>	Command specifies the VTY line password.
Switch(config-line)# <b>login</b>	Command makes the switch require the password.

# Limit Access to Device Configurations

## Configure Passwords (Cont.)

<b>Secure Privileged EXEC</b>	<pre>Sw-Floor-1 (config) # enable secret class Sw-Floor-1 (config) # exit Sw-Floor-1 # Sw-Floor-1 # disable Sw-Floor-1 &gt; enable Password: Sw-Floor-1 #</pre>
<b>Securing User EXEC</b>	<pre>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 Sw-Floor-1 (config) #</pre>
<b>Securing Remote Access</b>	<pre>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) #</pre>

# Encrypt Passwords

- The **startup-config** and **running-config** files display most passwords in plaintext. This is a security threat because anyone can see the passwords if they have access to these files.
  
- Use the **service password-encryption** global config command to encrypt all passwords.
  - The command applies weak encryption to all unencrypted passwords.
  - However, it does stop “shoulder surfing”.

```
Sw-Floor-1(config)# service password-encryption
S1(config)# exit
S1# show running-config
<output omitted>
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
<Output omitted>
line con 0
  password 7 0822455D0A16
  login
!
line vty 0 4
  password 7 0822455D0A16
  login
line vty 5 15
  password 7 0822455D0A16
  login!
```

# Banner Messages

- Banners are messages that are displayed when someone attempts to gain access to a device. Banners are an important part of the legal process in the event that someone is prosecuted for breaking into a device.
- Configured using the **banner motd delimiter message delimiter** command from global configuration mode. The delimiting character can be any character as long as it is unique and does not occur in the message (e.g., # \$ % ^ & \* )



# Syntax Checker – Limiting Access to a Switch

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 and allow login.

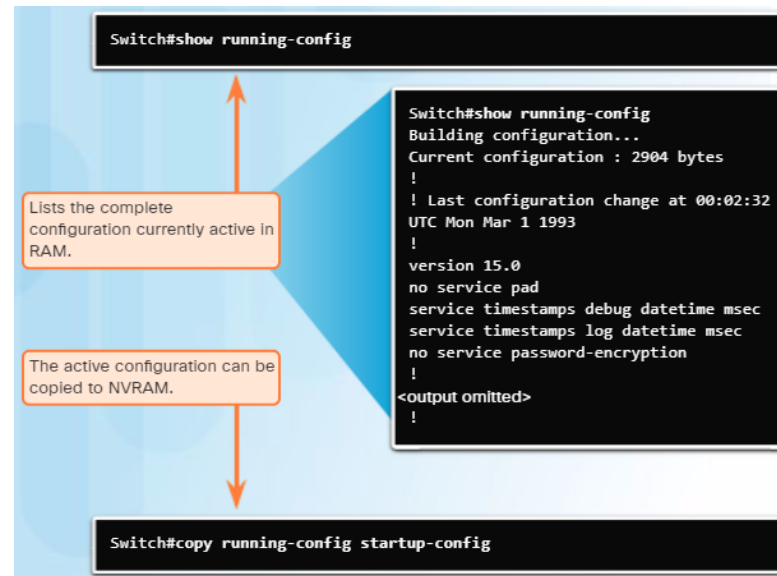
```
Sw-Floor-1(config)# line console 0  
Sw-Floor-1(config-line)# password Cisc0  
Sw-Floor-1(config-line)# login  
Sw-Floor-1(config-line)# exit  
Sw-Floor-1(config)#
```

Secure the first 16 VTY lines. Use the password Cisc0 and 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)# end  
Sw-Floor-1#
```

# Save the Running Configuration File

- Cisco devices use a **running configuration** file and a **startup configuration** file.
- The running configuration file is stored in RAM and contains the current configuration on a Cisco IOS device.
  - Configuration changes are stored in this file.
  - If power is interrupted, the running config is lost.
  - Use the **show startup-config** command to display contents.
- The startup config file is stored in NVRAM and contains the configuration that will be used by the device upon reboot.
  - Typically the running config is saved as the startup config.
  - If power is interrupted, it is not lost or erased.
  - Use the **show running-config** command to display contents.
- Use the **copy running-config startup-config** command to save the running configuration.



# Alter the Running Configuration

- If configuration changes do not have the desired effect, they can be removed individually or the device can be rebooted to the last saved configuration using the **reload** privileged EXEC mode command.
  - The command restores the startup-config.
  - 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 configuration, it may be necessary to clear all the configurations using the **erase startup-config** privileged EXEC mode command.



## Save Configurations

# Capture Configuration to a Text File

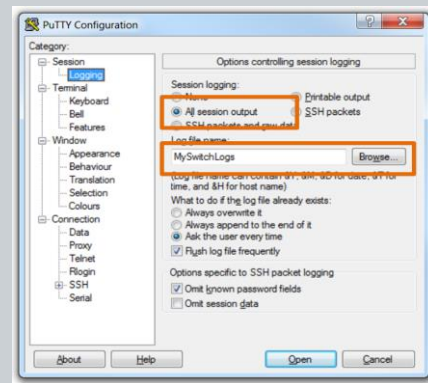
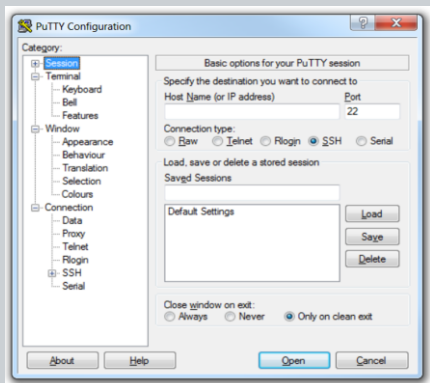
- Configuration files can also be saved and archived to a text document for editing or reuse later. For example, assume a switch has been configured and the running config has been saved.

Connect to the switch using PuTTY or Tera Term.

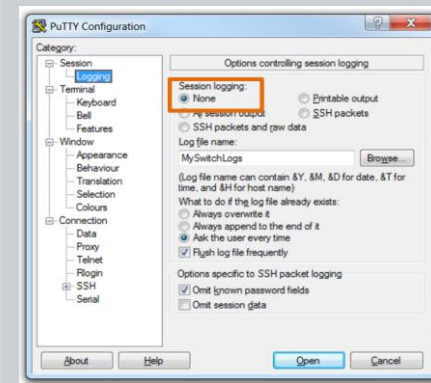
Enable logging and assign a name and file location to save the log file.

Generate text to be captured as text displayed in the terminal window will also be placed into the chosen file.

Disable logging in the terminal software by choosing **None** in the Session logging option.



Execute the **show running-config** or **show startup-config** command at the privileged EXEC prompt.





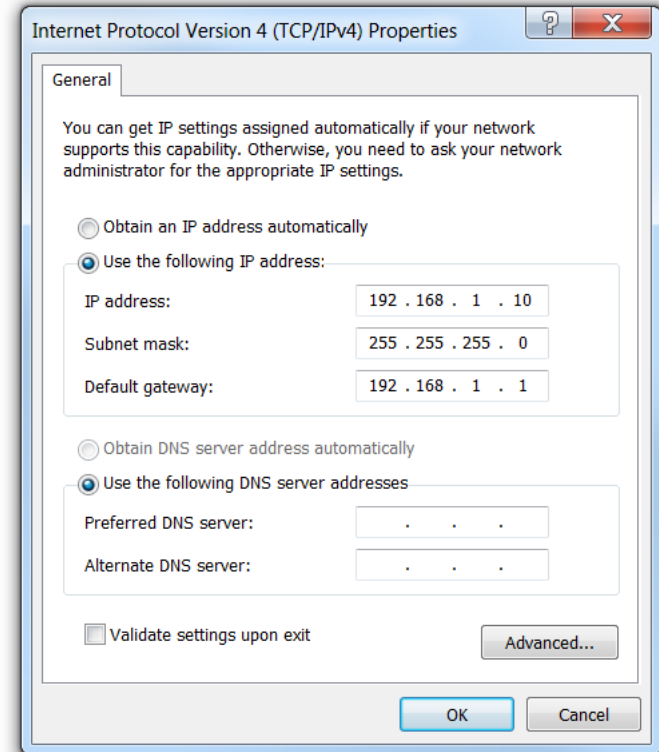
# Capture Configuration to a Text File (Cont.)

- The text file created can be used as a record of how the device is currently implemented and be used to restore a configuration. The file would require editing before being used to restore a saved configuration to a device.
- To restore a configuration file to a device:
  - Enter global configuration mode on the device.
  - 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.

# 2.3 Address Schemes

# IP Addressing Overview

- Each end device on a network (e.g., PCs, laptops, servers, printers, VoIP phones, security cameras, ...) require an IP configuration consisting of:
  - **IP address**
  - **Subnet mask**
  - **Default gateway** (optional for some devices)
  
- IPv4 addresses are displayed in dotted decimal format consisting of:
  - 4 decimal numbers 0 and 255
  - Separated by decimal points (dots)
  - E.g., 192.168.1.10, 255.255.255.0, 192.168.1.1



# Interfaces and Ports

- Cisco IOS Layer 2 switches have physical ports for devices to connect. However, these ports do not support Layer 3 IP addresses.
- To remotely connect to and manage a Layer 2 switch, it must be configured with one or more switch virtual interfaces (SVIs).
- Each switch has a default VLAN 1 SVI.

**Note:** A Layer 2 switch does not need an IP address to operate. The SVI IP address is only used to remotely manage a switch.

## Configure IP Addressing

# Manual IP Address Configuration for End Devices

- To manually configure an IP address on a Windows host:

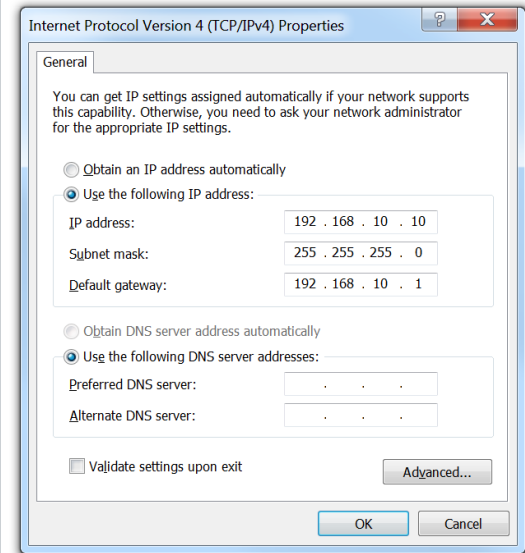
Open the **Control Panel > Network Sharing Center > Change adapter settings** and click on the adapter.

Configure the IPv4 address and subnet mask information, and default gateway and then click **OK**.

Right-click on the adapter and select **Properties** to display the Local Area Connection Properties window.

Highlight Internet Protocol Version 4 (TCP/IPv4) and click **Properties** to open the Internet Protocol Version 4 (TCP/IPv4) Properties window

Click **Use the following IP address** to manually configure the IPv4 address configuration.



Note: Windows 10 manual IPv4 configuration is provided as Supplemental material at the end of this presentation

# Automatic IP Address Configuration for End Devices

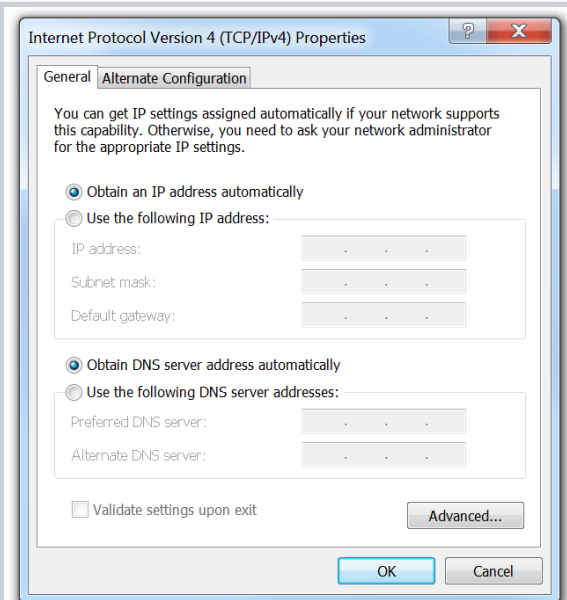
- To assign the IP configuration using a Dynamic Host Configuration Protocol (DHCP) server:

Open the **Control Panel > Network Sharing Center > Change adapter settings** and click on the adapter.

Click **Obtain an IP address automatically** and click on **OK**.

Right-click on the adapter and select **Properties** to display the Local Area Connection Properties window.

Highlight Internet Protocol Version 4 (TCP/IPv4) and click **Properties** to open the Internet Protocol Version 4 (TCP/IPv4) Properties window



# Configure IP Addressing

## Switch Virtual Interface

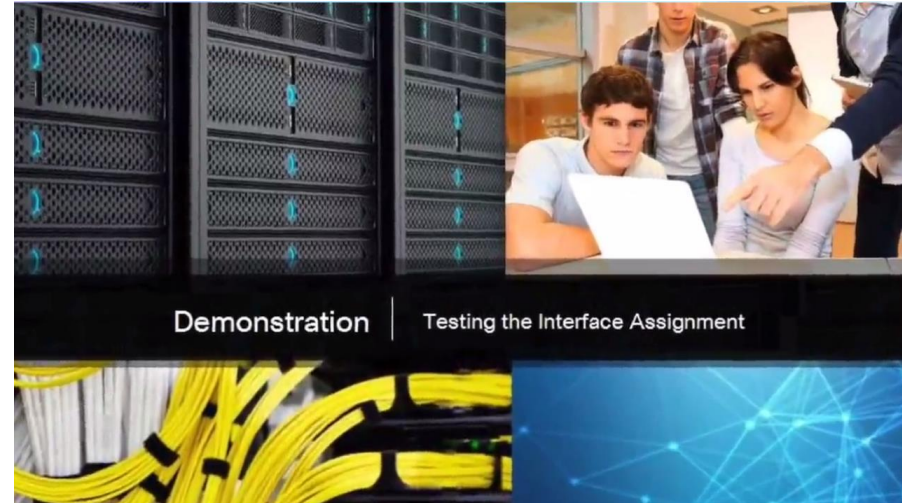
- To remotely manage a switch, it must also be configured with an IP configuration:
  - However, a switch does not have a physical Ethernet interface that can be configured.
  - Instead, you must configure the VLAN 1 **switch virtual interface (SVI)**.
- The VLAN 1 SVI must be configured with:
  - **IP address** - Uniquely identifies the switch on the network
  - **Subnet mask** - Identifies the network and host portion in the IP address
  - **Enabled** - Using the **no shutdown** command.



Use the **show ip interface brief** privileged EXEC command to verify.

# Interface Addressing Verification

- The IP configuration on a Windows host is verified using the **ipconfig** command.
- To verify the interfaces and address settings of intermediary devices like switches and routers, use the **show ip interface brief** privileged EXEC command.





## Verifying Connectivity

# 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.



# 2.4 Chapter Summary

## Chapter 2: Configure a Network Operating System

- Explain the features and functions of Cisco IOS Software.
- Configure initial settings on a network device using the Cisco IOS software.
- Given an IP addressing scheme, configure IP address parameters on end devices to provide end-to-end connectivity in a small to medium-sized business network.

