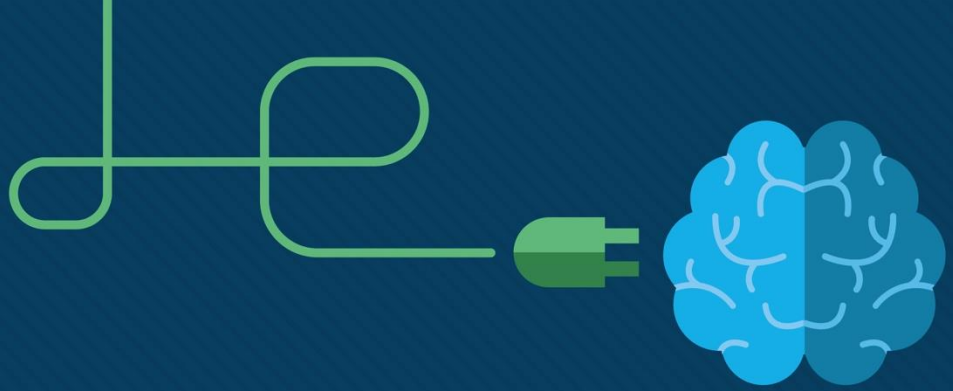
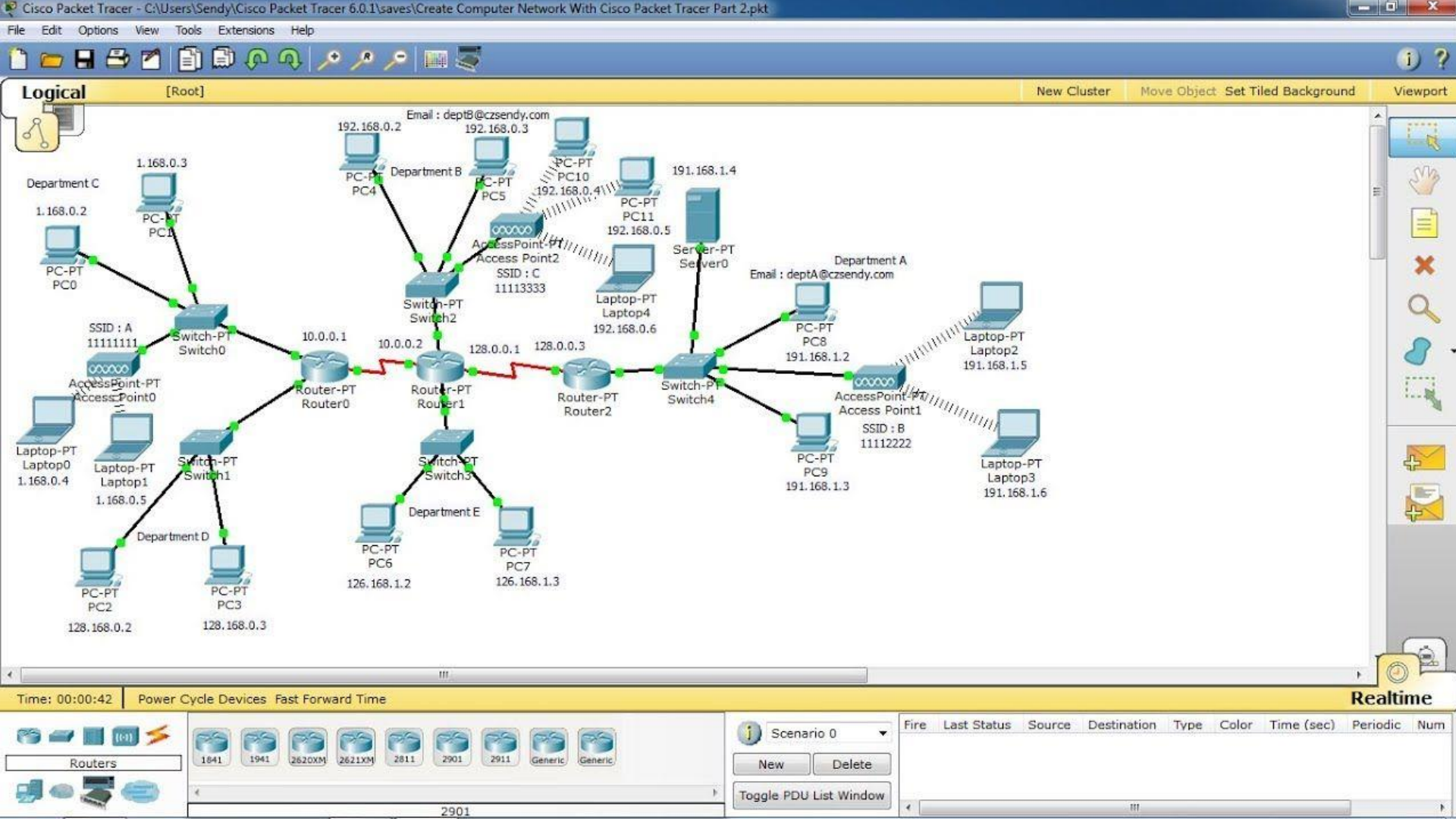


Lab1: Configure a Network Operating System

Instructor Materials

CCNA Routing and Switching

Introduction to Networks v6.0


Cisco Packet Tracer - C:\Users\Sendy\Cisco Packet Tracer 6.0.1\saves\Create Computer Network With Cisco Packet Tracer Part 2.pkt
File Edit Options View Tools Extensions Help
Logical [Root]
New Cluster Move Object Set Tiled Background Viewport
Department C
1.168.0.2
PC-PT PC0
1.168.0.3
PC-PT PC1
SSID : A
11111111
Switch-PT Switch0
AccessPoint-PT Access Point0
Laptop-PT Laptop0
1.168.0.4
Laptop-PT Laptop1
1.168.0.5
Department D
PC-PT PC2
128.168.0.2
PC-PT PC3
128.168.0.3
Switch-PT Switch1
10.0.0.1
Router-PT Router0
10.0.0.2
Router-PT Router1
128.0.0.1
128.0.0.3
Router-PT Router2
Switch-PT Switch3
Department E
PC-PT PC6
126.168.1.2
PC-PT PC7
126.168.1.3
192.168.0.2
PC-PT PC4
Department B
Email : deptB@czsendy.com
192.168.0.3
PC-PT PC5
PC-PT PC10
192.168.0.4
PC-PT PC11
192.168.0.5
191.168.1.4
Server-PT Server0
AccessPoint-PT Access Point2
SSID : C
11113333
Switch-PT Switch2
Laptop-PT Laptop4
192.168.0.6
Switch-PT Switch4
Department A
Email : deptA@czsendy.com
PC-PT PC8
191.168.1.2
Laptop-PT Laptop2
191.168.1.5
AccessPoint-PT Access Point1
SSID : B
11112222
PC-PT PC9
191.168.1.3
Laptop-PT Laptop3
191.168.1.6
Time: 00:00:42
Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811 2901 2911 Generic Generic
2901
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time (sec) Periodic Num

Cisco IOS
Operating System

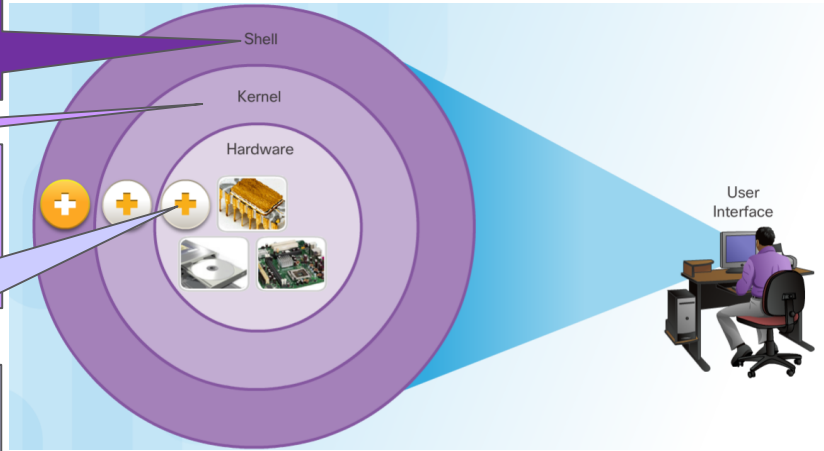
Cisco devices use the Cisco **Internetwork Operating System (IOS)**.
- Although used by Apple, iOS is a registered trademark of Cisco in the U.S. and other countries and is used by Apple under license.

- 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

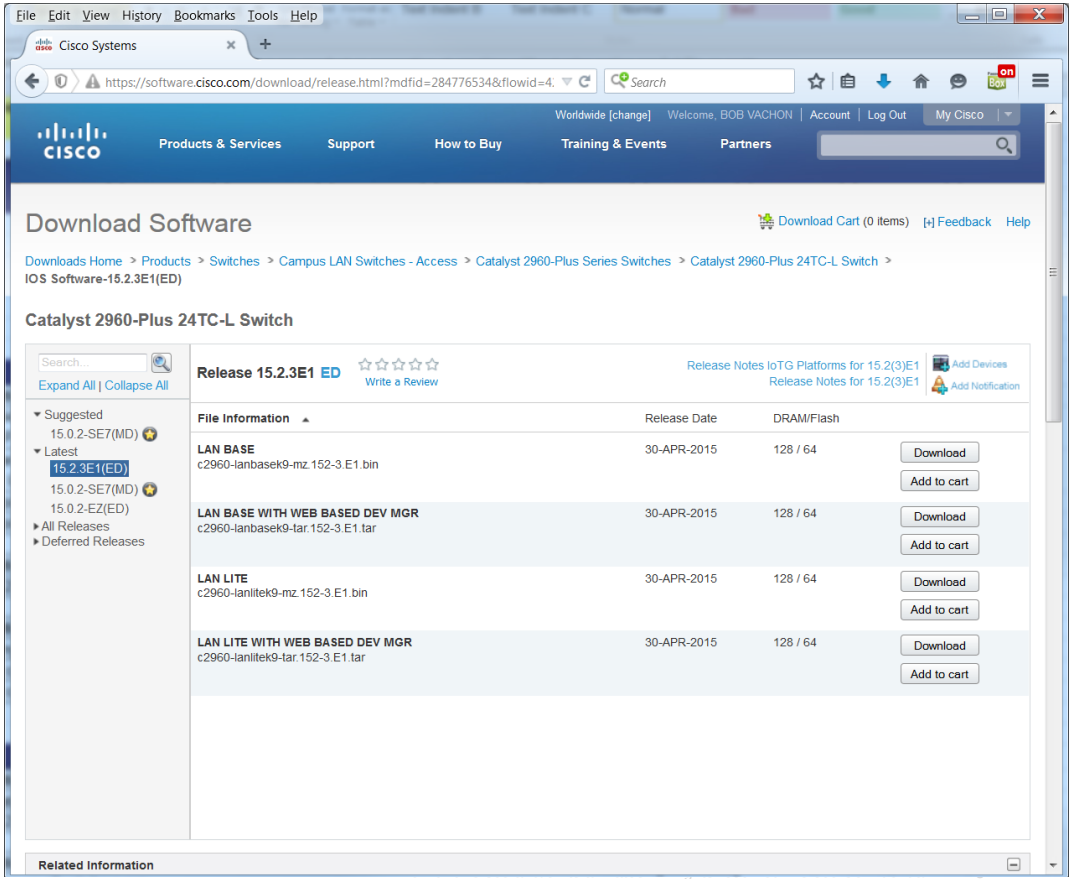
- Using a CLI on a Cisco IOS switch or router enables a network technician to:
  - Use a keyboard to run CLI-based network programs
  - Use a keyboard to enter text and text-based commands

- 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.

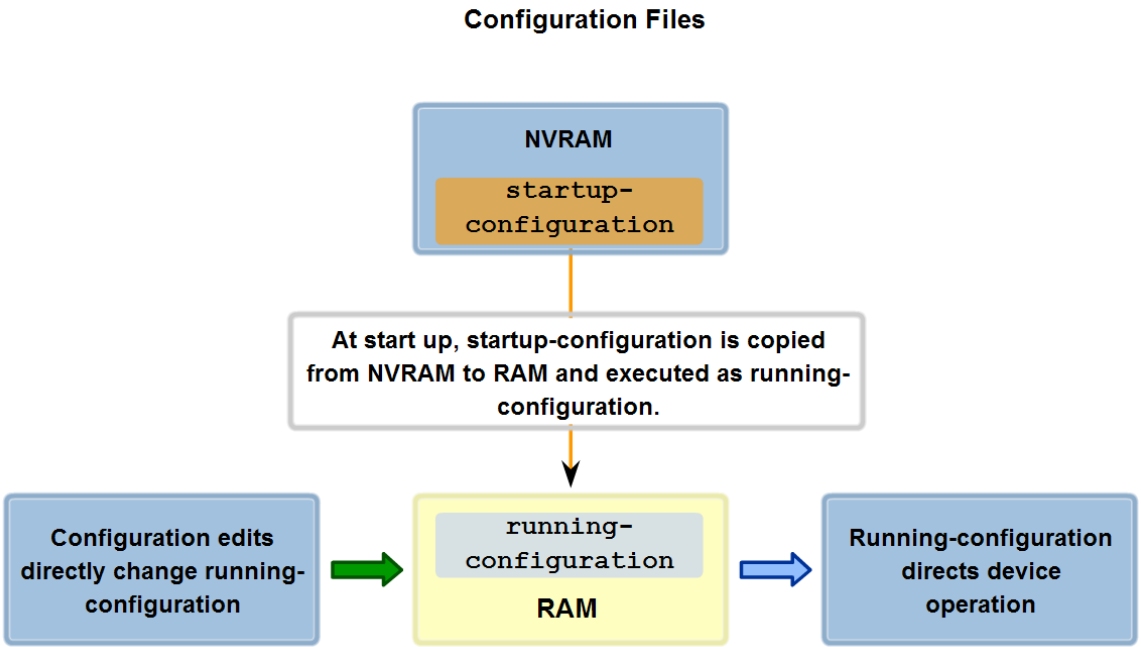


Role of Internetwork Operating System (IOS)

- IOS Provides :

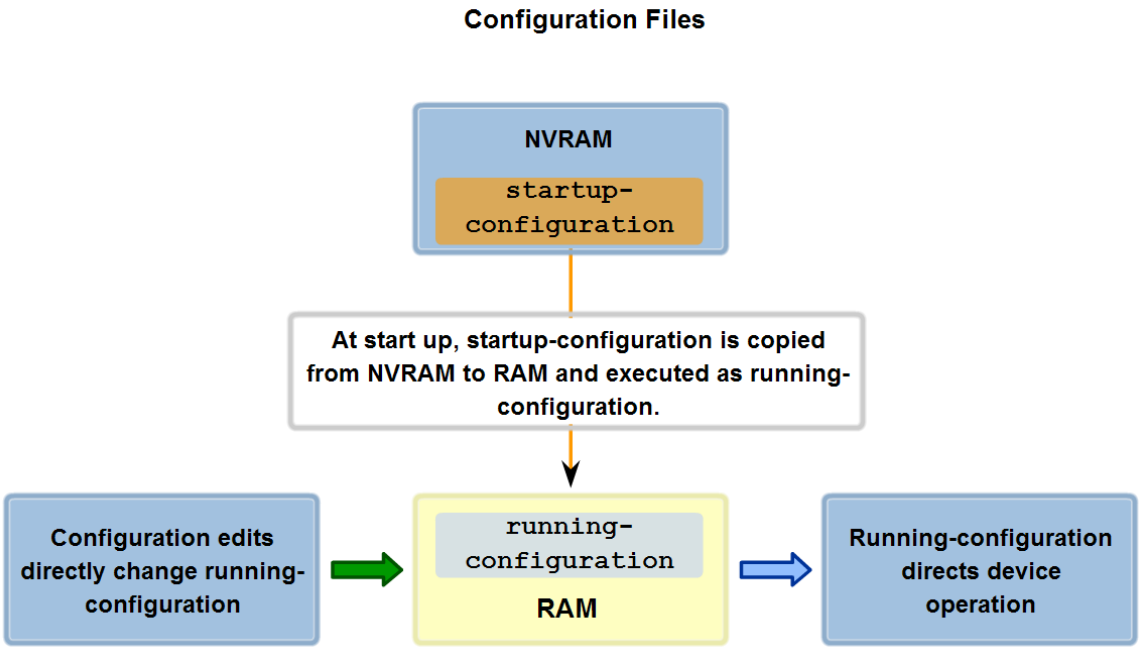
Role of Internetwork Operating System (IOS)

- Define of startup config.



Role of Internetwork Operating System (IOS)

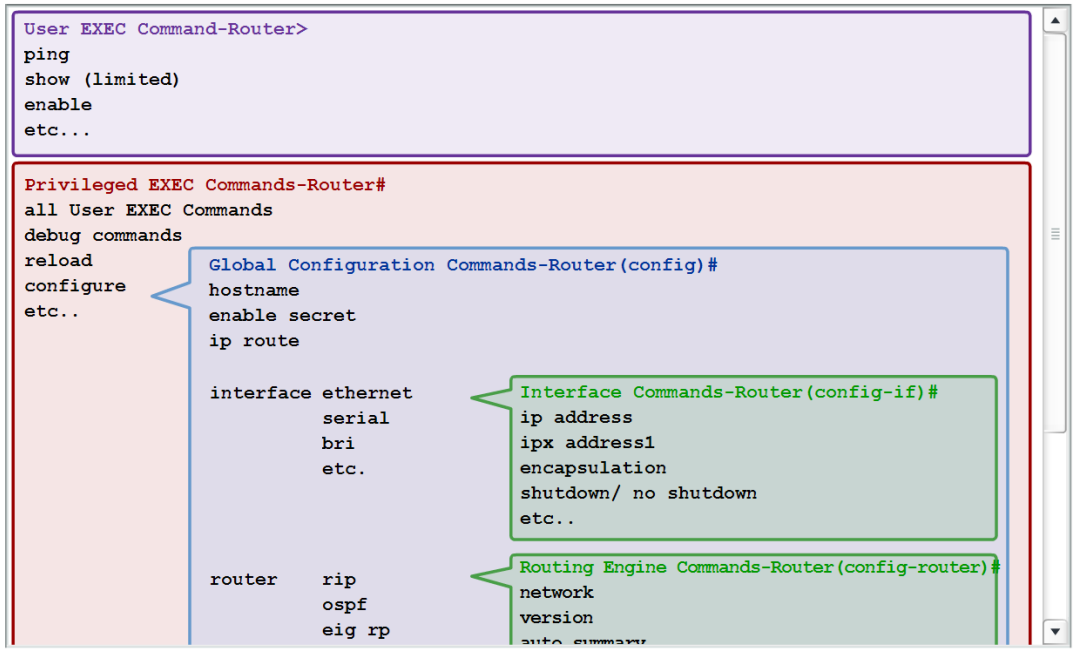
- Identify the relationship between IOS and config



Role of Internetwork Operating System (IOS)

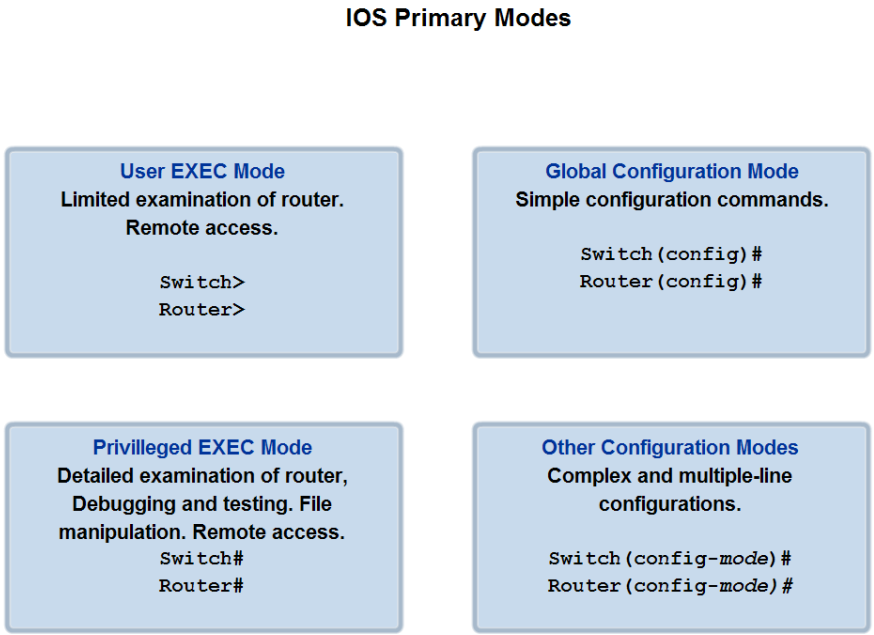
- Recognize that Cisco IOS is modal and describe the implications of modes.

IOS Mode Hierarchical Structure



Role of Internetwork Operating System (IOS)

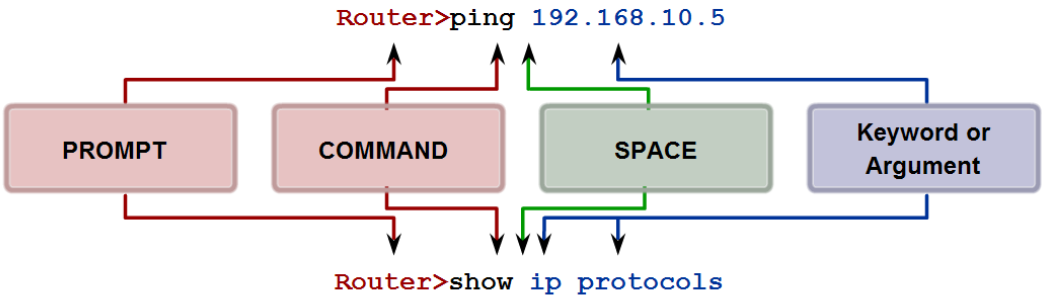
- Define the different modes and identify the mode prompts in the CLI



Role of Internetwork Operating System (IOS)

- Identify the basic command structure for IOS commands

Basic IOS Command Structure



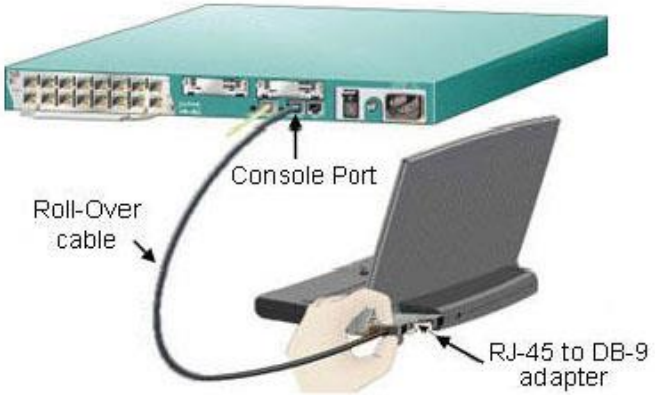
Prompt commands are followed by a space and then the keyword or arguments.

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.

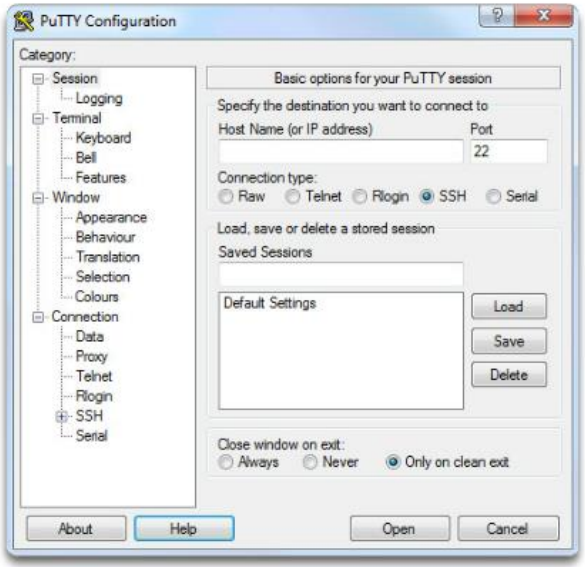
Console Port



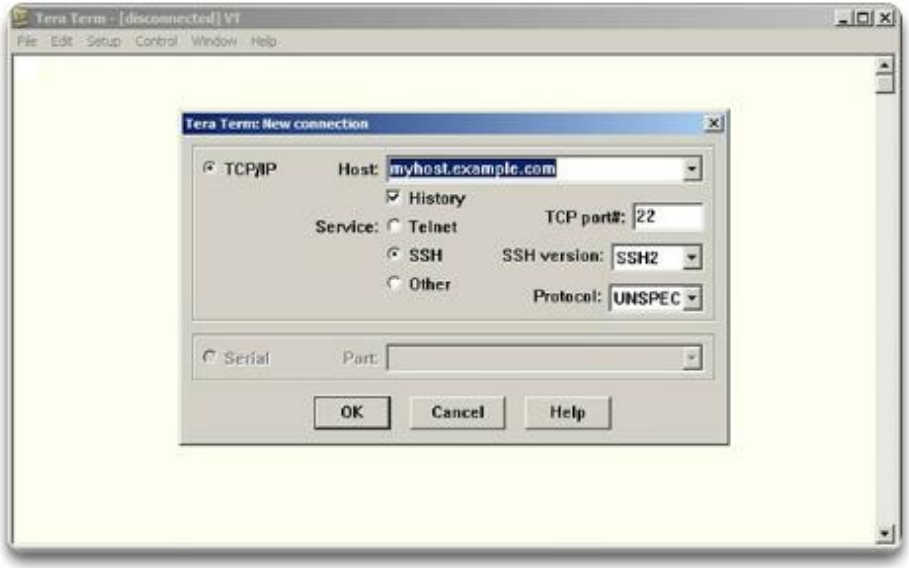
Terminal Emulation Program

- 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	• 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#`

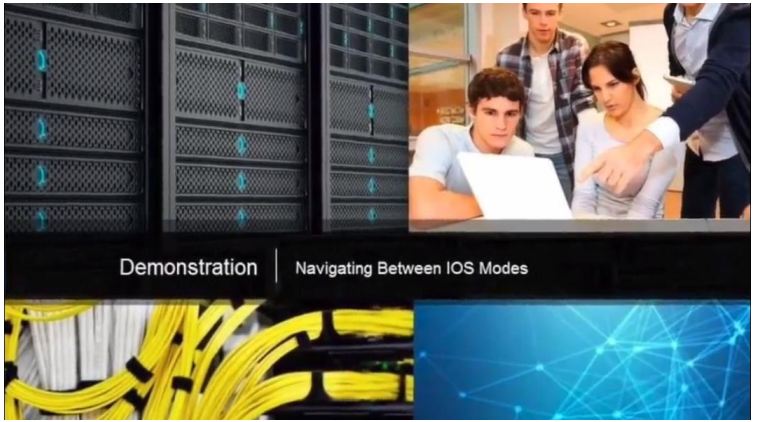
Configuration Command Modes

- 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

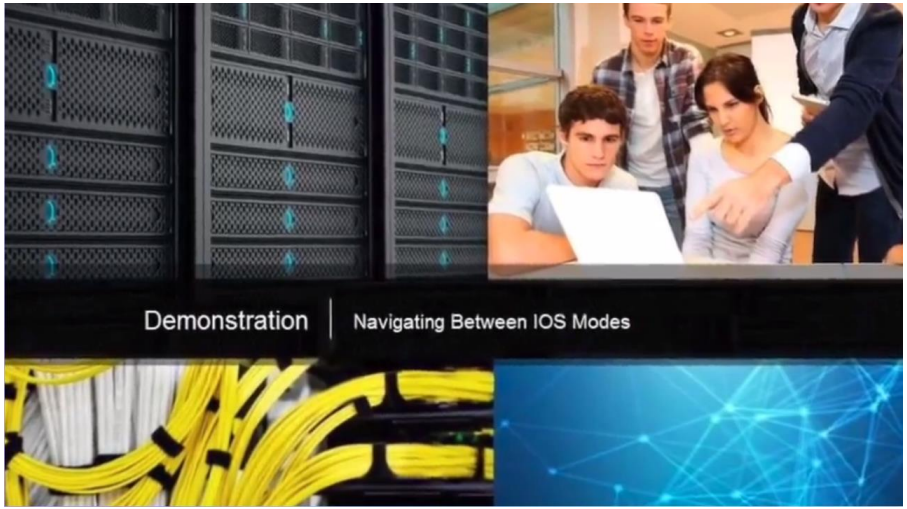
- Various commands are used to move in and out of command prompts:
  - To move from user EXEC mode to privileged EXEC mode, use the **enable** command.
  - Use return to user EXEC mode, use the **disable** command.



- 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**.

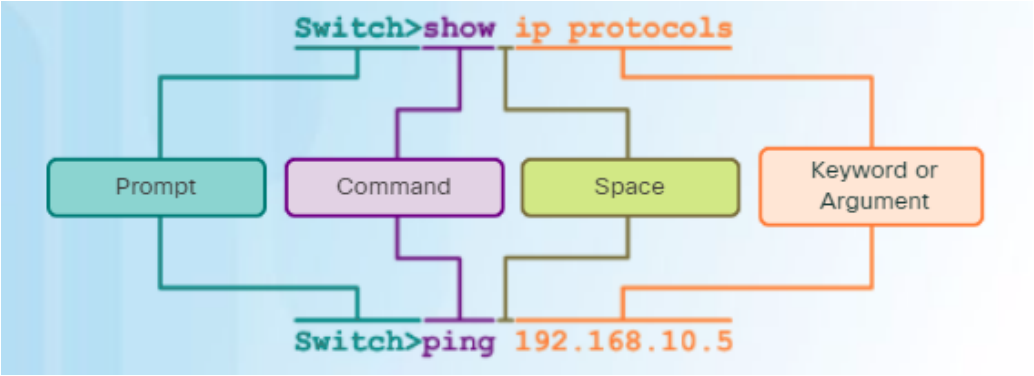
Navigate Between IOS Modes (Cont.)

- 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

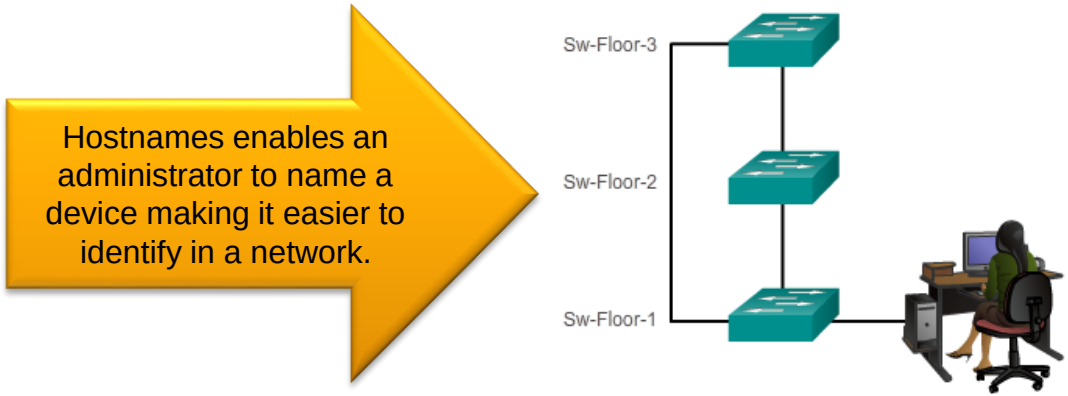
- A Cisco IOS device supports many commands. Each IOS command has a specific format or syntax and can only be executed at the appropriate mode.



- 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.

Device Names

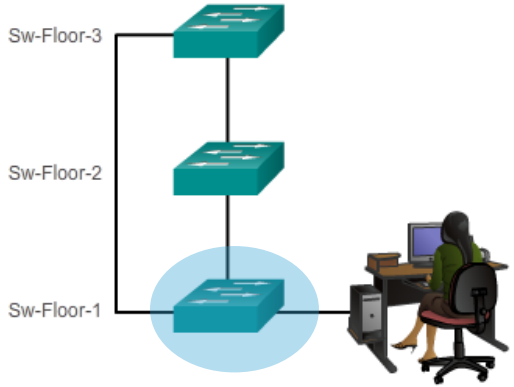
- The first step when configuring a switch is to assign it a unique device name, or hostname.
  - Hostnames appear in CLI prompts, can be used in various authentication processes between devices, and should be used on topology diagrams.
  - Without a hostname, network devices are difficult to identify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

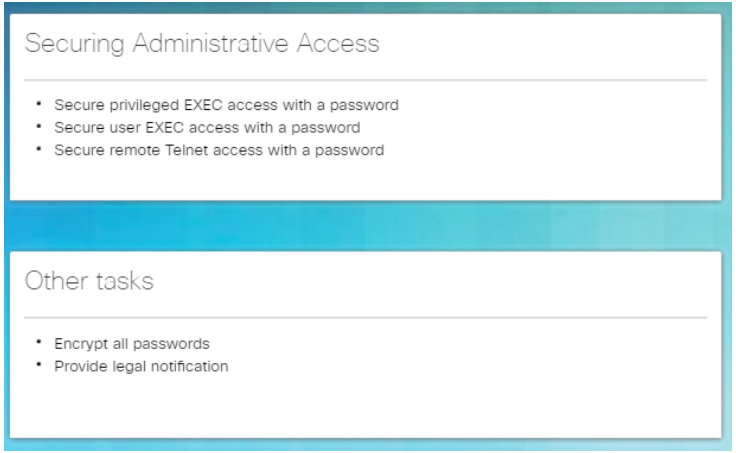



```
Switch>
Switch> enable
Switch#
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

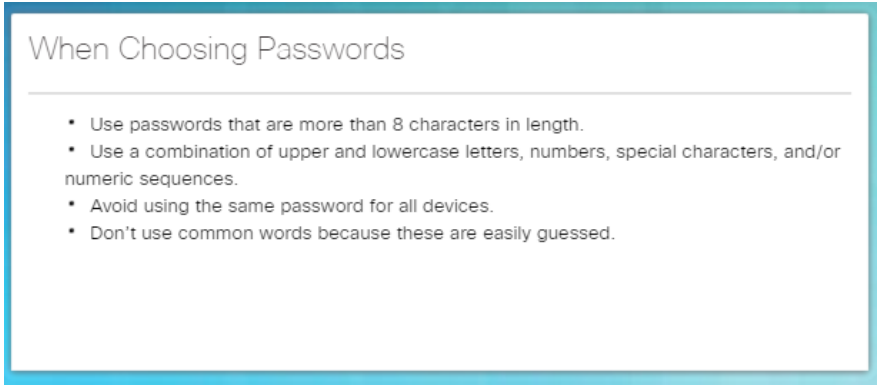
Limiting Device Access

- **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.



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

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)#` **line console 0**	Command enters line console configuration mode.
`Switch(config-line)#` **password** *password*	Command specifies the line console password.
`Switch(config-line)#` **login**	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)#` **line vty 0 15**	Cisco switches typically support up to 16 incoming VTY lines numbered 0 to 15.
`Switch(config-line)#` **password** *password*	Command specifies the VTY line password.
`Switch(config-line)#` **login**	Command makes the switch require the password.

Configure Passwords (Cont.)

Secure Privileged EXEC	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#
Securing User EXEC	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)#
Securing Remote Access	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)#

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 isunique 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.

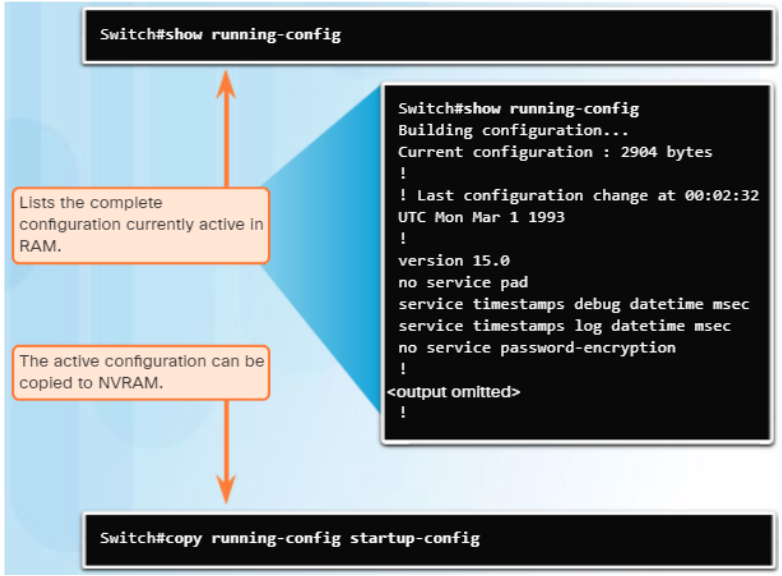
```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password Cisc0
Sw-Floor-1(config-line)# login
SW-Floor-1(config-line)# exit
Sw-Floor-1(config)#
```

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.



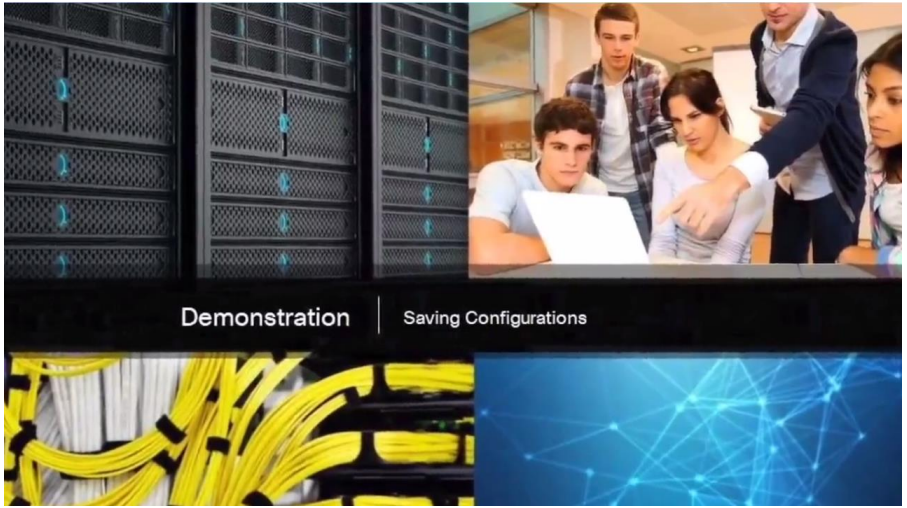
- The startup config file is stored in NVRAM and contains the configuration that will be used by the device upon reboot.
  - Typically the running config is saved as the startup config.
  - If power is interrupted, it is not lost or erased.
  - Use the **show running-config** command to display contents.

- 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.



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