Elk Technologies
https://elktech.org
Scott Stephenson

Module 2: Basic Switch and End Device Configuration

Introductions to Networks

Cisco | Networking Academy®
Mind Wide Open™

Module Objectives

- 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
2.1 Cisco IOS Access	Explain how to access a Cisco IOS device for configuration purposes.
2.2 IOS Navigation	Explain how to navigate Cisco IOS to configure network devices.
2.3 The Command Structure	Describe the command structure of Cisco IOS software.
2.4 Basic Device Configuration	Configure a Cisco IOS device using CLI.
2.5 Save Configurations	Use IOS commands to save the running configuration.
2.6 Ports and Addresses	Explain how devices communicate across network media.
2.7 Configure IP Addressing	Configure a host device with an IP address.
2.8 Verify Connectivity	Verify connectivity between two end devices.

2.1 Cisco IOS Access

Key Components of a 2950 or 2960 Switches

- 12, 24, or 48 10/100 Ethernet Ports
- Port Status LEDs
- Mode Button (SYST, RPS, Port)
- Console port
- Dual Purpose 10/100/1000 or SFP port(s)
- Cisco IOS software

- Port Status:
  - **Off**: No link, or port was administratively shut down
  - **Green**: Link present
  - **Blinking green**: Port is transmitting or receiving data
  - **Alternating green/amber**: Link fault
  - **Amber**: Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data
  - **Blinking amber**: Port Is blocked by STP and is transmitting or receiving packets

SYST LED:

- Shows whether the system is receiving wer nd is functioning properly.
- Green: The system is working normally.
- Amber: The system is receiving power but is not working properly.

Routers

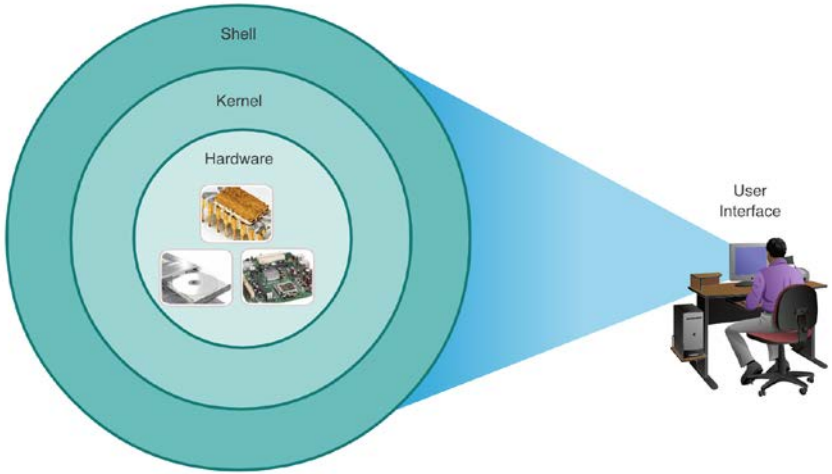
- Cisco 1841

- Cisco 1941

- Cisco 4321

Operating Systems

- **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.



GUI

- A GUI allows the user to interact with the system using an environment of graphical icons, menus, and windows.
- A GUI is more user-friendly and requires less knowledge of the underlying command structure that controls the system.
- Examples of these are: Windows, macOS, Linux KDE, Apple iOS and Android.
- GUIs can fail, crash, or simply not operate as specified. For these reasons, network devices are typically accessed through a CLI.

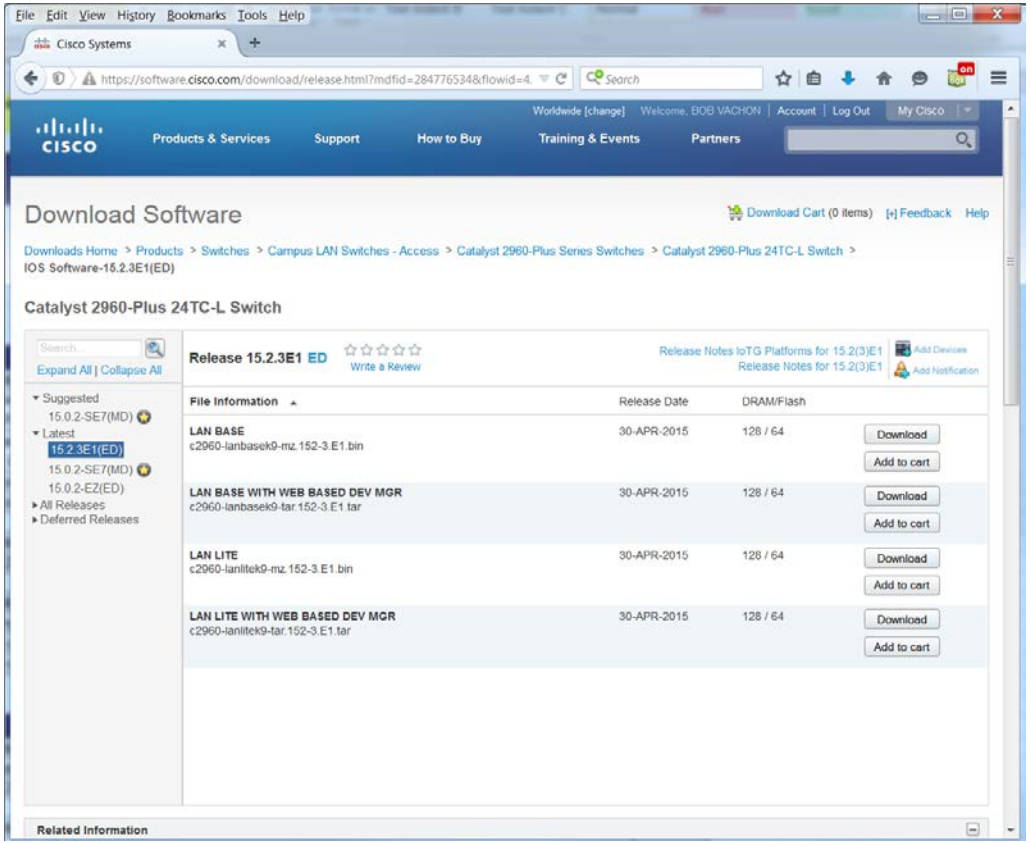
Purpose of an OS

- 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
- CLI-based network operating system 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

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

Purpose of OS

- 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.



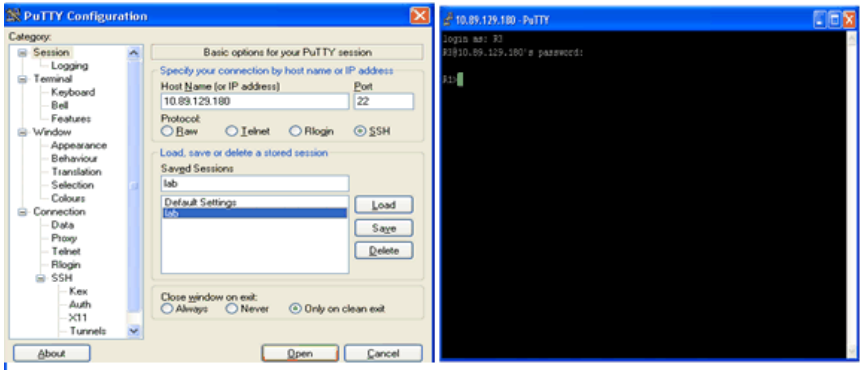
Access Methods

- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.
- Used for initial configuration, use the console port to locally access the switch or router from a serial or USB interface of the PC

- Device is accessible even if no networking services have been configured (out-of-band)
- Need a special console cable
- Should be configured with passwords to prevent unauthorized access
- Device should be located in a secure room so console port can not be easily accessed
- Displays startup, debugging, and error messages by default

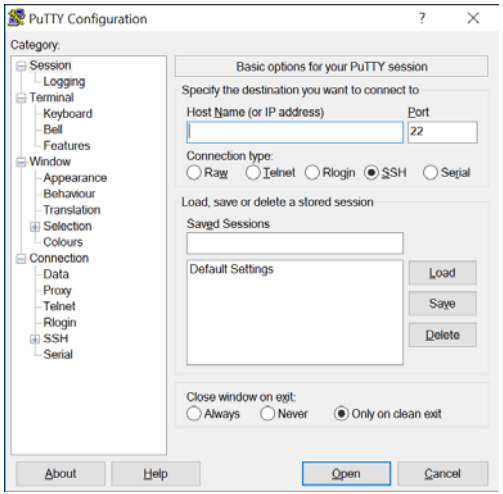
Access Methods

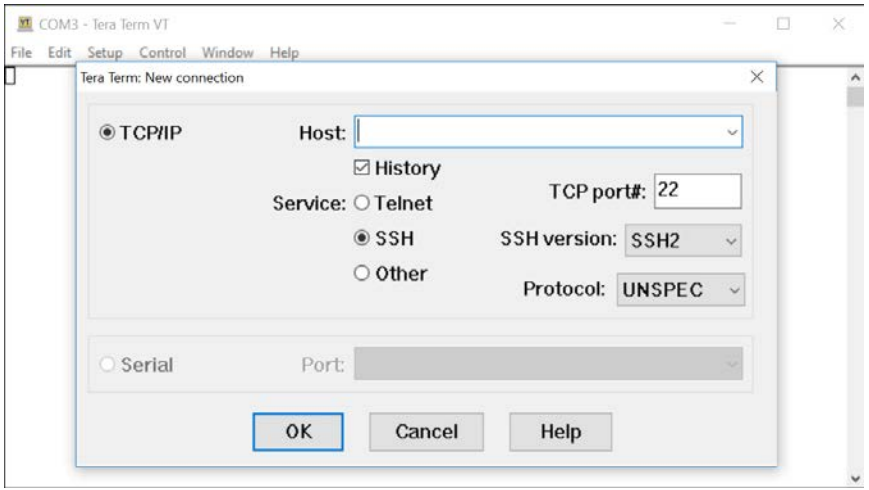
- **Telnet** – Establishes an insecure remote CLI connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext).
  - Requires active networking services and one active interface that is configured
- **Secure Shell** (SSH) – Establishes a secure remote CLI connection to a device, through a virtual interface, over a network.
  - This is the recommended method for remotely connecting to a device.
  - Stronger password authentication
  - Uses encryption when transporting data
- **Auxiliary Port**
  - Out-of-band connection
  - Uses telephone line (dialup)
  - Can be used like console port
  - Not supported on Catalyst switches



Terminal Emulation Programs

- Terminal emulation programs are used to connect to a network device by either a console port or by an SSH/Telnet connection.
- There are several terminal emulation programs to chose from such as PuTTY, Tera Term, HyperTerminal, Solar-PuTTY, and SecureCRT.



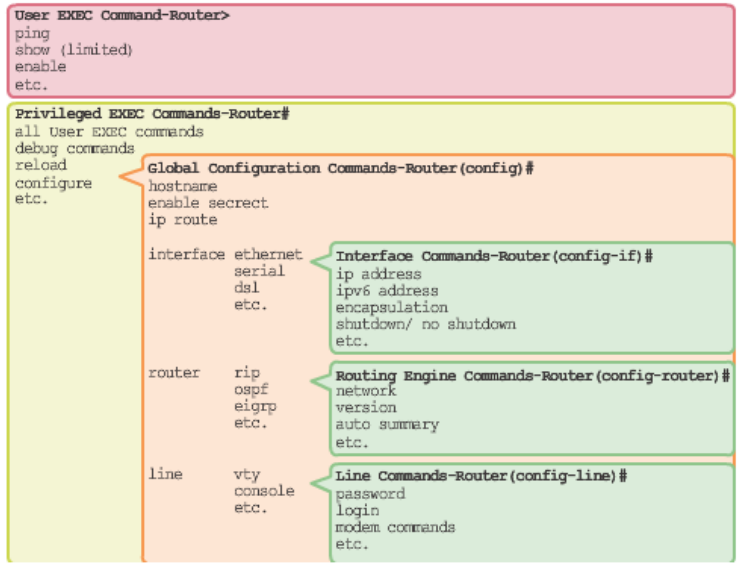


2.2 IOS Navigation

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.
- Initial configuration must be done via console connection, locally accessed through a serial or USB interface of a PC
- Configuration is then done via various CLI command modes

IOS Mode Hierarchical Structure



Primary Command Modes

- **User EXEC Mode**:
  - Allows access to only a limited number of basic monitoring commands
  - The first entrance into the CLI of an IOS device
  - Identified by the CLI prompt that ends with the **>** symbol

```
Router>

Switch>
```

- **Privileged EXEC Mode:**
  - Allows access to all commands and features
  - accessed by entering the enable command
  - Identified by the CLI prompt that ends with the **#** symbol

```
Router#

Switch#
```

Configuration Mode and Subconfiguration Modes

- **Global Configuration Mode**:
  - Used to access configuration options on the device
  - changes made affect the operation of the device as a whole
  - accessed by entering the **`configure terminal`** command
- **Line Configuration Mode**:
  - Used to configure console, SSH, Telnet or AUX access
- **Interface Configuration Mode**:
  - Used to configure a switch port or router interface

```
Switch(config)#
```

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

```
Switch(config-if)#
```

Navigation Between IOS Modes

- **Privileged EXEC Mode:**
  - To move from user EXEC mode to privilege EXEC mode, use the **enabled** command.

```
Switch> enable
Switch#
```

- **Global Configuration Mode:**
  - To move in and out of global configuration mode, use the **configure terminal** command. To return to privilege EXEC mode, use the **exit** command.

```
Switch(config)#
Switch(config)#exit
Switch#
```

- **Line Configuration Mode:**
  - To move in and out of line configuration mode, use the **line** command followed by the management line type. To return to global configuration mode, use the **exit** command.

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

Navigation Between IOS Modes

Subconfiguration Modes:

- To move out of any subconfiguration mode to get back to global configuration mode, use the **exit** command. To return to privilege EXEC mode, use the **end** command or key combination **Ctrl +Z**.

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

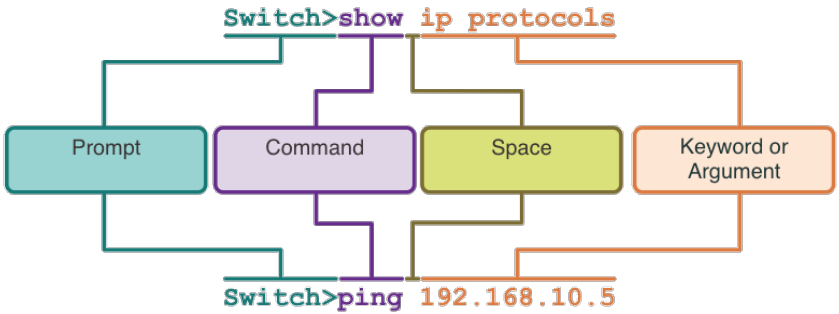
- To move directly from one subconfiguration mode to another, type in the desired subconfiguration mode command. In the example, the command prompt changes from **(config-line)#** to **(config-if)#**.

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

2.3 The Command Structure

Basic IOS Command Structure

- 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 general syntax for a command is the command followed by any appropriate keywords and arguments.
  - **Prompt** – This specifies the mode you are currently in.
  - **Command** – This specifies the action to be performed.
  - **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**).



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.
  - Boldface text indicates commands and keywords that are entered as shown.
  - Italic text indicates an argument for which the user provides the value.
- Commands and keywords can be shortened to the minimum number of characters that identify a unique selection.

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. Spaces are used to clearly delineate parts of the command.

IOS Command Syntax Check

- The command syntax provides the pattern, or format, that must be used when entering a command.
- The command is **ping** and the user-defined argument is the *ip-address* of the destination device. For example, **`ping 10.10.10.5`**

```
ping 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`**

```
traceroute ip-address
```

- 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}}
```

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?
  - Command syntax check verifies that a valid command was entered by the user.
    - If the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

```
Router#ping ?
  WORD  Ping destination address or hostname
  ip    IP echo
  ipv6  IPv6 echo
```

```
Switch#interface fastEthernet 0/1
                 ^
% Invalid input detected at '^' marker.
```

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**.

```
Router#con
% Ambiguous command: "con"
Router#con?
configure  connect
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Hot Keys and Shortcuts

- The table below is a brief list of 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.
Left Arrow or Ctrl+B	Moves the cursor one character to the left.
Right Arrow or Ctrl+F	Moves the cursor one character to the right.
Up Arrow or Ctrl+P	Recalls the commands in the history buffer, beginning with the most recent commands.
Ctrl-A	Moves cursor to the beginning of the line.
Ctrl-E	Moves to the end of the line.

Hot Keys and Shortcuts

- When a command output produces more text than can be displayed in a terminal window, the IOS will display a “--More--” prompt. The table below 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.

Note: To see more hot keys and shortcuts refer to 2.3.5.

Hot Keys and Shortcuts

- Commands that can be 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.
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.

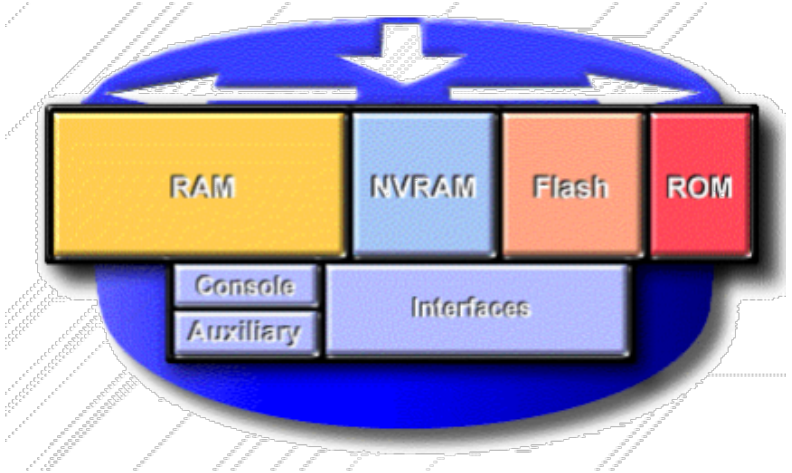
Command	Description
exit	allows a user to return to the previous level in the command hierarchy
end	Allows a user to directly return to Privileged Exec mode

Note: To see more hot keys and shortcuts refer to 2.3.5.

2.4 Basic Device Configuration

Switch/Router Configuration Sources

- **RAM** – holds active/running configuration. Contents are lost with power down.
- **NVRAM** – holds startup configuration. Retains contents when power is removed.
- **Flash** – holds IOS images. Similar to NVRAM.
- **ROM** – holds bootstrap and POST. Has basic IOS in case no full IOS is found.



Location of the Cisco IOS

- IOS stored in Flash
- Non-volatile storage – not lost when power is lost
- Can be changed or overwritten as needed
- Can be used to store multiple versions of IOS
- IOS copied from flash to volatile RAM
- Quantity of flash and RAM memory determines IOS that can be used

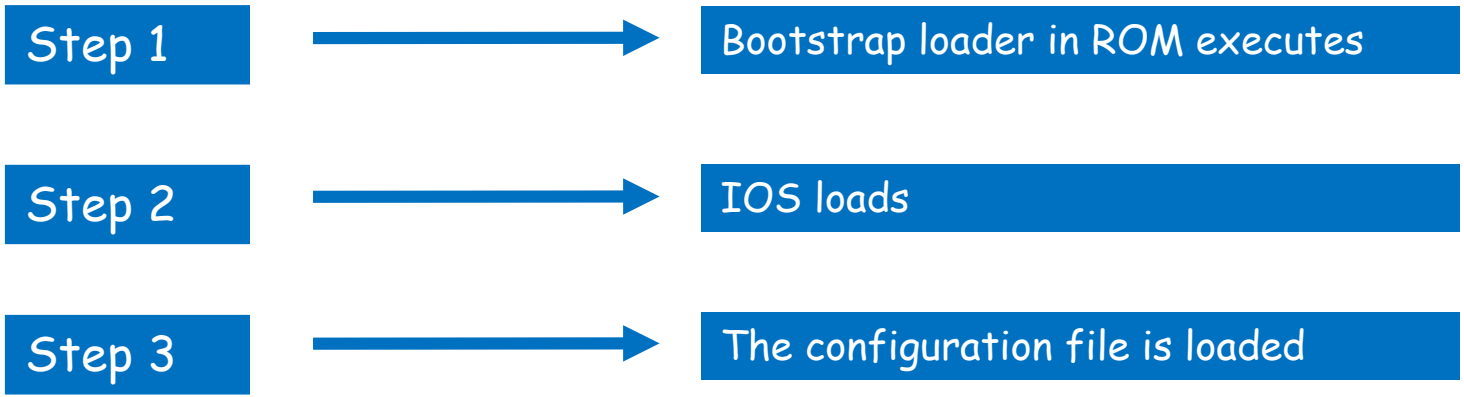
3 Modes in the IOS

- The ROM modes allow a user to recover a password by changing the registry settings, to replace the Cisco IOS image file, or recover from system failures

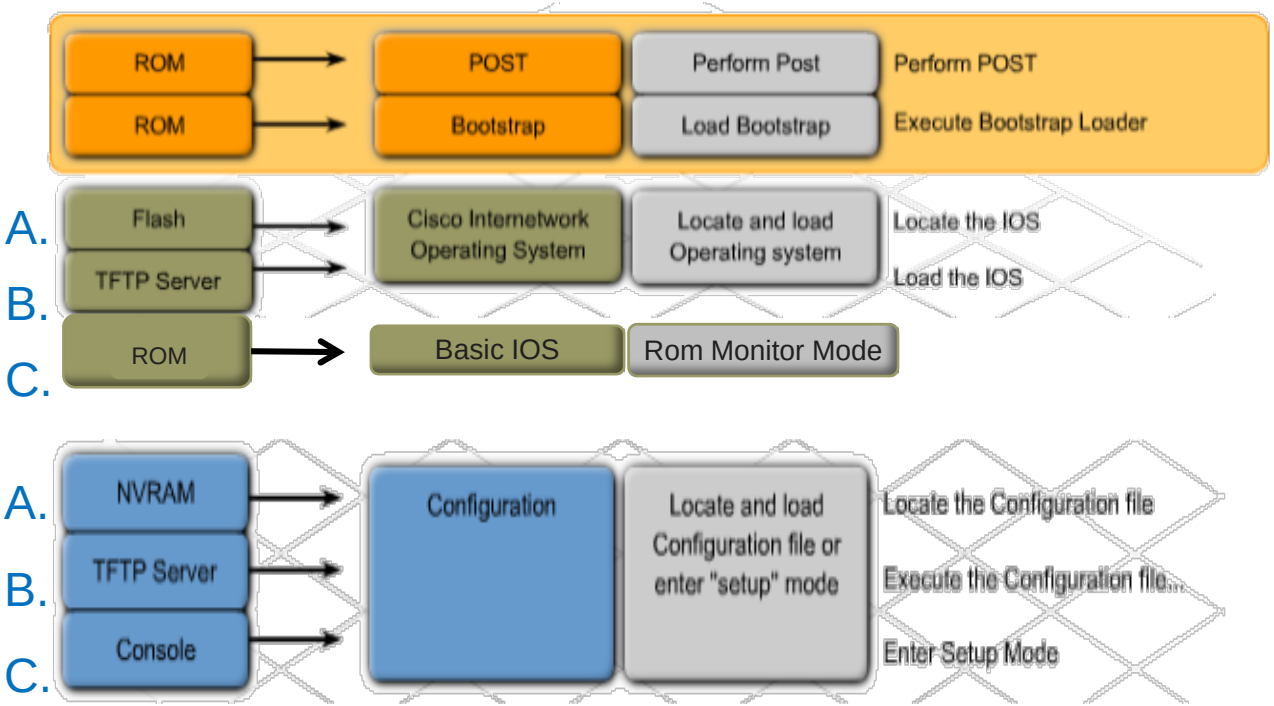
Operating Environment	Prompt	Usage
ROM monitor	> or ROMMON>	Failure or password recovery
Boot ROM	Router(boot)>	Flash image upgrade
Cisco IOS	Router>	Normal operation

A Switch/Router Starts Up

- Before anything else happens, there is a Power On Self-Test (POST)



Steps in Switch/Router Initialization



Device Names

- The first configuration command on any device should be to give it a unique hostname.
- By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."
- Guideline for naming devices:
  - 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

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

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

Password Guidelines

- The use of weak or easily guessed passwords are a security concern.
- 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.
- Password Guidelines:
  - 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.

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.

Configure Passwords

- Securing **Console line** access:
  - First enter line console configuration mode using the **`line console 0`** command in global configuration mode.
  - 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#
```

- Securing **privileged EXEC** mode access:
  - First enter global configuration mode.
  - Next, use the **`enable secret`** ***`password`*** command.

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

Configure Passwords

- Securing **VTY line** access:
  - First enter line VTY configuration mode using the **`line vty 0 15`** command in global configuration mode.

```
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#
```

  - Next, specify the VTY password using the **`password`** ***`password`*** command.
  - Finally, enable VTY access using the **`login`** command.
  - Note: 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.

Encrypt Passwords

- The startup-config and running-config files display most passwords in plaintext.
- To encrypt all plaintext passwords, use the **service password-encryption** global config command.
  - All passwords in the running-config are encrypted.
- Use the **show running-config** command to verify that the passwords on the device are now encrypted.

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

```
Sw-Floor-1# show running-config
!

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

Banner Messages

- A banner message is important to warn unauthorized personnel from attempting to access the device.
- To create a banner message of the day on a network device, use the **banner motd # *the message of the day* #** global config command.
- Note: The "**#**" in the command syntax is called the **delimiting character**. It is entered before and after the message.
- The banner will be displayed on attempts to access the device.

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

```
Press RETURN to get started.



Authorized Access Only!

User Access Verification

Password:
```

2.5 Save Configurations

Configuration Files

- 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.
- To save changes made to the running configuration to the startup configuration file, use the **`copy running-config startup-config`** privileged EXEC mode command.
  - It will be loaded if the switch is restarted.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

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

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

Alter the Running Configurations

- 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. To do this you can:
  - Remove the changed commands individually.
  - Reload the device using the **reload** command in privilege EXEC mode.
    Note: This will cause the device to briefly go offline, leading to network downtime.

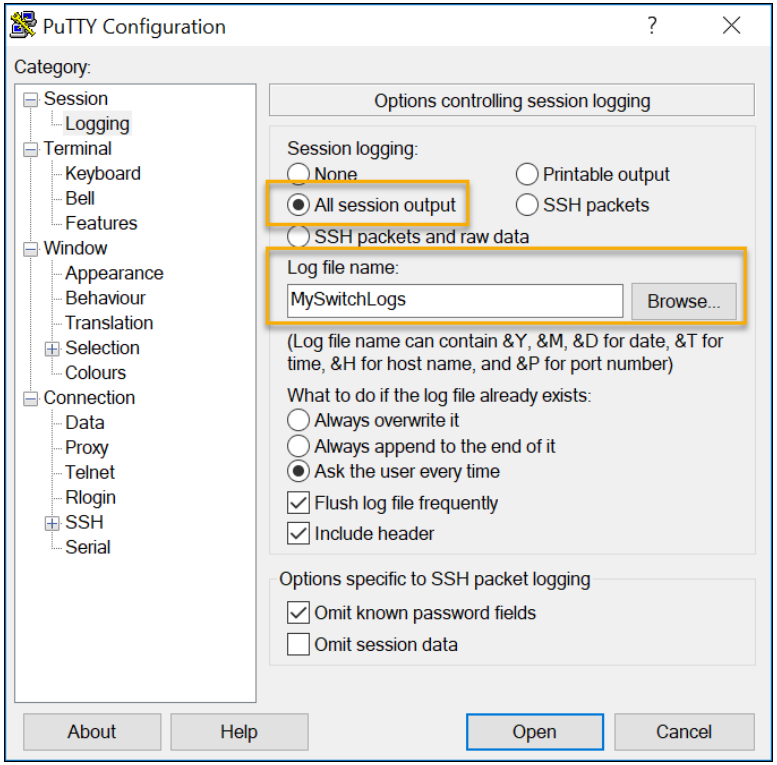
```
Router# reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

- If the undesired changes were saved to the startup-config, it may be necessary to clear all the configurations using the **erase startup-config** command in privilege EXEC mode.
  - After erasing the startup-config, reload the device to clear the running-config file from RAM.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

Capture Configuration to a Text File

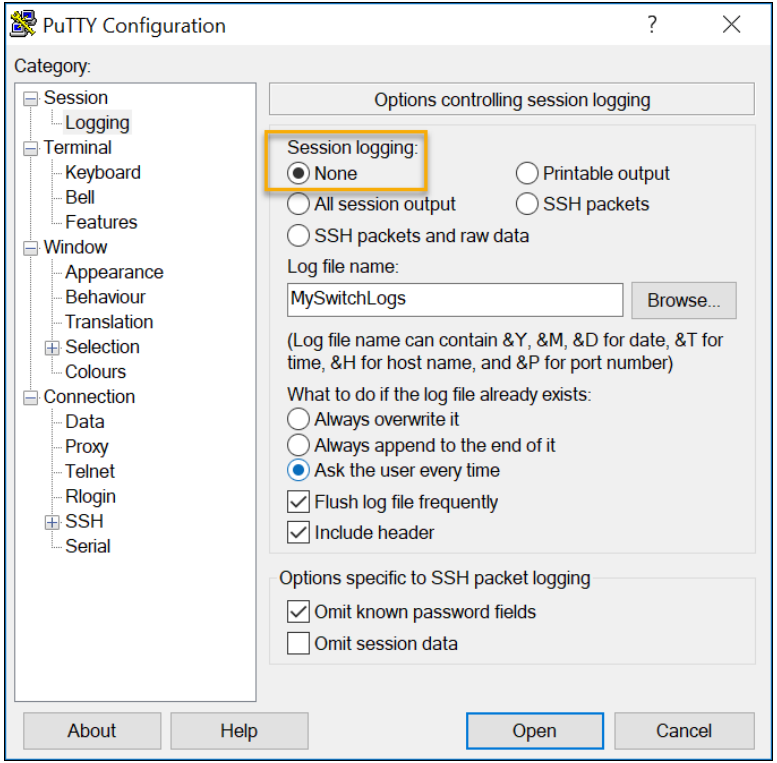
- Configuration files can also be saved and archived to a text document.
  - Step 1. Open terminal emulation software, such as PuTTY or Tera Term, that is already connected to a switch.
  - Step 2. Enable logging in to the terminal software and assign a name and file location to save the log file. The figure displays that **All session output** will be captured to the file specified (i.e., MySwitchLogs).



Capture Configuration to a Text File

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

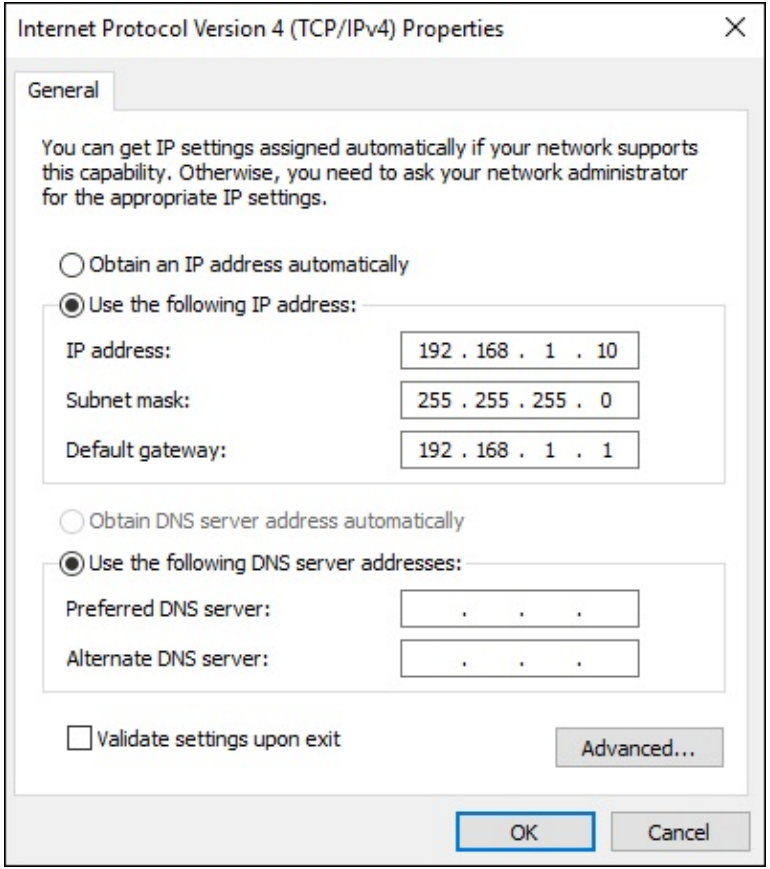
```
Switch# show running-config
Building configuration...
```



2.6 Ports and Addresses

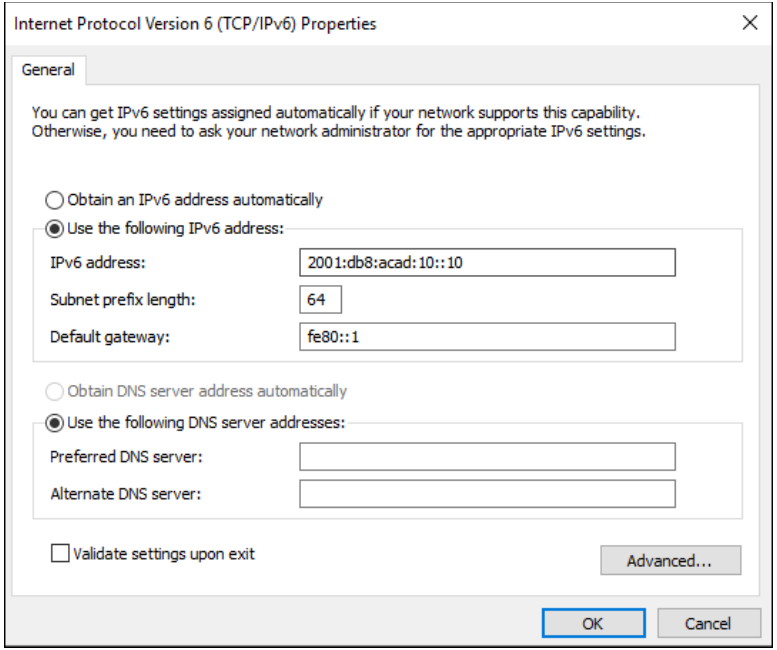
IP Addresses

- 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.
- The structure of an IPv4 address is called **dotted decimal notation** and is represented by four decimal numbers between 0 and 255.
- 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 **default gateway** address is the IP address of the router that the host will use to access remote networks, including the internet.



IP Addresses

- **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.
- 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.



Interfaces and Ports

- Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.
- Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.
- Different types of network media have different features and benefits. Some of the differences between various types of media include:
  - 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

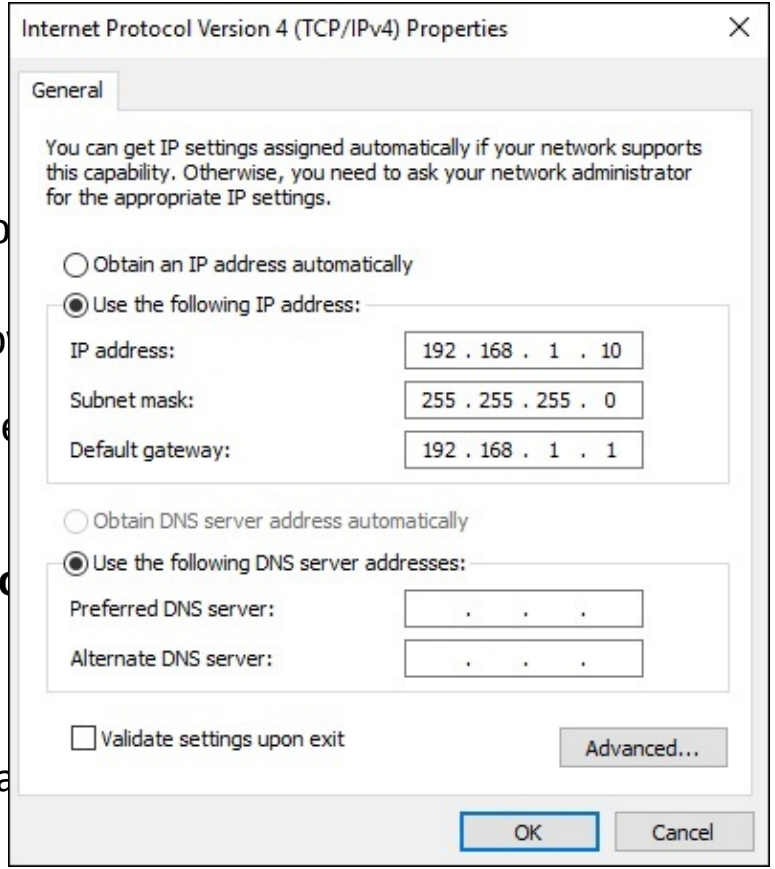
Interfaces and Ports

- Cisco IOS Layer 2 switches have physical ports for devices to connect.
- These ports do not support Layer 3 IP addresses.
- Switches can have one or more switch virtual interfaces (SVIs).
  - An SVI is created in software. These are virtual interfaces because there is no physical hardware on the device associated with it.
  - The SVI 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

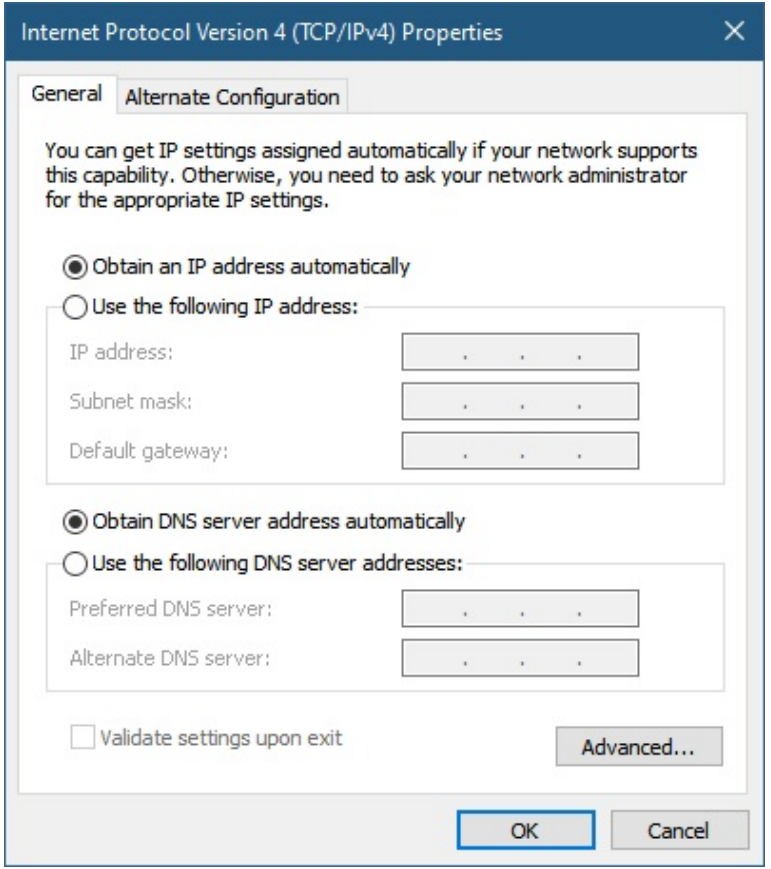
Manual IP Address Configuration for End Devices

- End devices on the network need an IP address in order to communicate with other devices on the network.
- IPv4 address information can be entered into end devices manually, or automatically using Dynamic Ho Configuration Protocol (DHCP).
  - To manually configure an IPv4 address on a Windo PC, 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**.
  - Next, click **Properties** to open the **Internet Protoco Version 4 (TCP/IPv4) Properties** window. Then configure the IPv4 address and subnet mask information, and default gateway.
- **Note**: IPv6 addressing and configuration options are simila to IPv4.



Automatic IP Address Configuration for End Devices

- DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled.
- End devices are typically by default using DHCP for automatic IPv4 address configuration.
  - To configure DHCP on a Windows PC, 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**.
  - Next, click **Properties** to open the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, then select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Note: IPv6 uses DHCPv6 and SLAAC (Stateless Address Autoconfiguration) for dynamic address allocation.



Switch Virtual Interface Configuration

- Characteristics of a SVI:
  - It is not an actual physical interface but a virtual one.
  - It provides a means to remotely manage a switch.
  - Once assigned the interface becomes an active member of that switch VLAN and can exchange traffic with other VLAN members.
  - It is associated with VLAN 1 by default.
  - It is considered active once it is up.

```
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
```

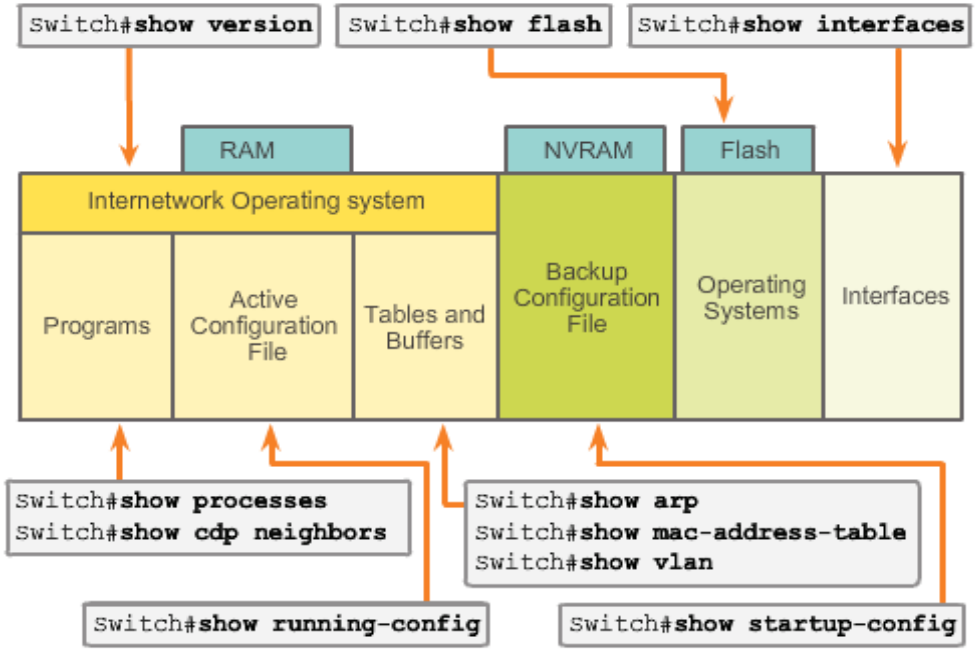
Switch Virtual Interface Configuration

- 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:
  - Enter the **interface vlan 1** command in global configuration mode.
  - Next assign an IPv4 address using the **ip address *ip-address subnet-mask*** command.
  - Finally, enable the virtual interface using the **no shutdown** command.

```
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
```

2.8 Verify Connectivity

IOS Examination Commands



IOS **show** commands can provide information about the configuration, operation and status of parts of a Cisco router.

Verify End Devices

- **ipconfig /all**

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....................: 00E0.8F2E.4CCA
   Link-local IPv6 Address.....: FE80::2E0:8FFF:FE2E:4CCA
   IP Address.....................: 192.168.1.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.....................: 0.0.0.0
   DNS Servers.....................: 0.0.0.0
   DHCP Servers.....................: 0.0.0.0
   DHCPv6 Client DUID.....................: 00-01-00-01-0E-73-B9-24-00-
E0-8F-2E-4C-CA
```

Verify Interfaces

- show interfaces
- show interfaces g0/0/0
- show ip interface
- show ip interface brief

```
S1#show ip interface
Vlan1 is up, line protocol is up
  Internet address is 192.168.1.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are None
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disable
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

```
S1#show ip interface ?
  Vlan   Catalyst Vlans
  brief  Brief summary of IP status and configuration
  |      Output Modifiers
  <cr>
```

```
S1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.2     YES manual up                    up
S1#
```

```
S1#show interfaces ?
  Ethernet         IEEE 802.3
  FastEthernet     FastEthernet IEEE 802.3
  GigabitEthernet  GigabitEthernet IEEE 802.3z
  Port-channel     Ethernet channel port interface
  Vlan             Catalyst Vlans
  etherchannel     Show interface etherchannel information
  status           interface line status
  switchport       Show interface switchport information
  trunk            Show interface trunk information
  |                Output Modifiers
  <cr>
```

Verify Connectivity

- **From a Switch:**
  - **ping**
  - **traceroute**

```
S1#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms



S1#traceroute 192.168.1.11
Type escape sequence to abort.
Tracing the route to 192.168.1.11

  1    *      0 msec     1 msec
S1#
```

- **From a PC:**
  - **ping**
  - **tracert**

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>tracert 192.168.1.11

Tracing route to 192.168.1.11 over a maximum of 30 hops:

  1    0 ms      1 ms      0 ms      192.168.1.11

Trace complete.
```

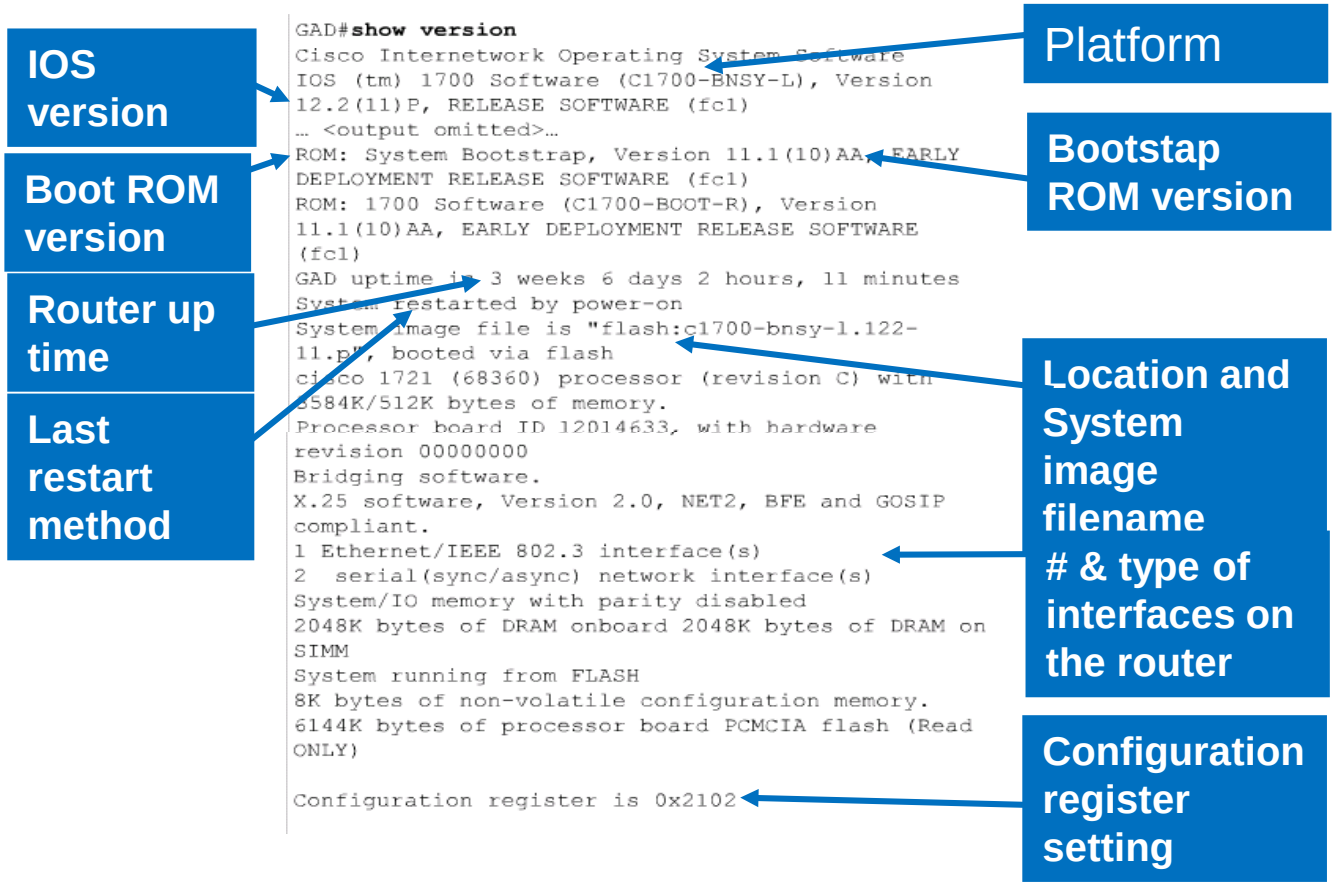
Testing End-to-End Connectivity

- Interface Addressing Verification
  - Cisco IOS supports commands to allow IP configuration verification.
- 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.
- Ping tests connectivity with the destination device
  - Ping 127.0.0.1
  - Ping NIC IP address
  - Ping default gateway
  - Ping next hop
  - Ping next interface
  - Ping end device

```
S1#show ip interface brief
Interface              IP-Address      OK? Method  Status    Protocol
FastEthernet0/1        unassigned      YES manual  up        up
FastEthernet0/2        unassigned      YES manual  up        up

<output omitted>


Vlan1                  192.168.10.2    YES manual  up        up
```

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=838ms TTL=35
Reply from 192.168.10.2: bytes=32 time=820ms TTL=35
Reply from 192.168.10.2: bytes=32 time=883ms TTL=36
Reply from 192.168.10.2: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35
Reply from 192.168.10.11: bytes=32 time=883ms TTL=36
Reply from 192.168.10.11: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms

C:\>
```

The show version Command



The show flash Command

- This command would show all of the Cisco IOS image files – not just the one that the router booted from
- Might compare to a directory listing

```
BHM#show flash
PCMCIA flash directory:
File  Length    Name/status
  1   6007232   c1700-bnsy-l.212-11.p
[6007296 bytes used, 284160 available, 6291456
total]
6144K bytes of processor board PCMCIA flash (Read
ONLY)
BHM#
```

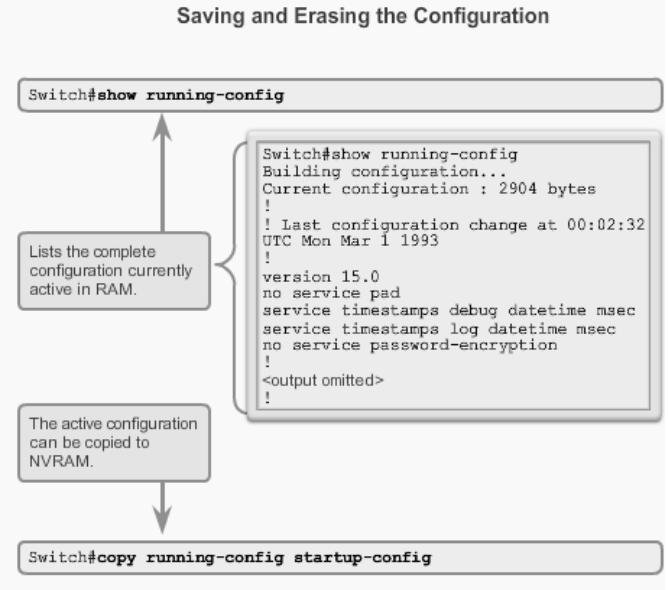
The show cdp neighbors Commands

- Information gathered by CDP includes:
  - Device identifiers - configured host name
  - Address list - Layer 3 address, if configured
  - Port identifier - directly connected port
  - Capabilities list - function or functions provided by the device
  - Platform - hardware platform of the device

```
R3#show cdp neighbors
Capability Codes: R - Router, T- Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Hose, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch           Fas 0/0            133         S I       WS-C2950-2Fas 0/11
R2               Ser 0/0/           149        R S I      Cisco 1841Ser 0/0/1
```

```
R3#show cdp neighbors detail
-------------------------
Device ID: R2
Entry address(es):
  IP address: 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK-9M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco System, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
```

Configuration Files




```
Switch# reload
System configuration has been modified.
Save? [yes/no]: n
Proceed with reload? [confirm]
```

- Startup configuration is removed by using the erase startup-config

```
Switch# erase startup-config
```

- On a switch you must also issue the delete vlan.dat

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
```

- The running configuration (RAM) affects the operation of the device immediately when modified.
- Issue the reload command without saving the running configuration to discard the changes and work with the file in NVRAM.

2.9 Module Practice and Quiz

What did I learn in this module?

- All end devices and network devices require an operating system (OS).
- 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 IOS command has a specific format or syntax and can only be executed in the appropriate mode.

What did I learn in this module?

- Basic device configurations- hostname, password, encrypt passwords and banner.
- There are two system files that store the device configuration: startup-config and running-config.
- 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.

New Terms and Commands

- operating system (OS)
- CLI
- GUI
- shell
- kernel
- hardware
- console
- Secure Shell (SSH)
- Telnet
- terminal emulation programs
- user EXEC mode
- privileged EXEC mode
- line configuration mode
- interface configuration mode
- Enable
- configure terminal
- exit
- end
- argument
- keyword
- command syntax
- ping
- traceroute
- help command ”?”
- hot keys
- hostname
- console
- enable secret
- VTY line
- show running-config
- banner motd
- startup-config
- running-config
- reload
- erase startup-config
- DHCP
- switch virtual interface (SVI)
- ipconfig
- show ip int brief


CISCO


Elk Technologies
https://elktech.org
Scott Stephenson