CISCO CCNA1

CCNA Routing and Switching: Introduction to Networks

# HOOFDSTUK 2

## Configure a Network Operating System

DE HOGESCHOOL
MET HET NETWERK

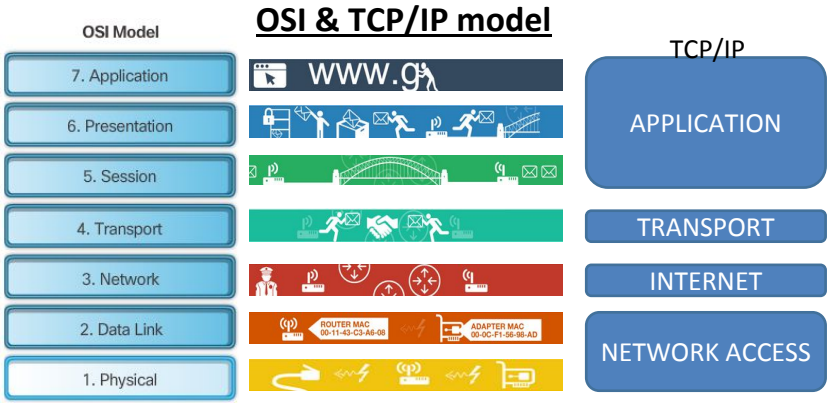
Hogeschool PXL – Elfde-Liniestraat 24 – B-3500 Hasselt
www.pxl.be - www.pxl.be/facebook

# CCNA1 - Overzicht

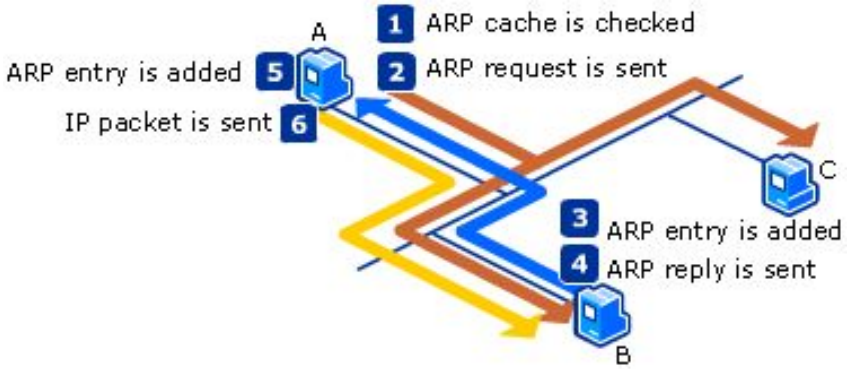
- OSI model en de belangrijkste (LAN) protocollen.
- Data Flow in een LAN
  (verklaring volgens het OSI model).
- IP en subnetting.
- Het toepassen en onderzoeken van bovenstaande 3 in Packettrace oefeningen.

# CCNA1 - Overzicht

1. OSI model en de belangrijkste (LAN) protocollen.




2. Data Flow in een LAN (verklaring volgens het OSI model)




3. IP en subnetting

# Situering hoofdstuk 2

Dit hoofdstuk beschrijft het operation system (OS) gebruikt in Cisco netwerkapparatuur. Een aantal **basis instructies** worden uitgebreid verklaard, en standaard netwerkinstellingen overlopen. Adressering en het testen van connectiviteit komen kort aan bod. Een basis-netwerktopologie wordt bekeken, bestaande uit twee switches en twee pc's, om het gebruik van het Cisco IOS te tonen.

**Doelstellingen:**

- Ken het gebruikte vakjargon. (Console, Telnet, AUX, SSH, Putty, Ping, IP address, DHCP, ..)
- Weet op welke verschillende manieren je een netwerktoestel kan aansluiten om te configureren.
- Ken de gebruikte commando's voor een basis configuratie. De packettrace oefening 2.4.1.2 is hierbij een goede herhaling.
- Werken met packettracer.
- Basisconfiguratie van CISCO netwerkapparatuur. (Accessing, navigatie, paswoorden, MOTD, helpfunctie, testen van connectivty, ..)
- Basis netwerkinstellingen aanpassen en controleren. (IP adressen instellen + gebruik van het ping commando.)

**Activity en PT:**

- 2.1.2.3 Accessing devices
- 2.2.3.4 Configuring initial switch settings
- 2.3.2.5 Implementing basic connectivity
- 2.1.4.6 PT navigating the IOS
- 2.4.1.2 Skills integration challenge

**Zie leerpad op blackboard!**

**Leertip:**

**Packet trace oefening 2.4.1.2 is een totale samenvatting van dit hoofdstuk!** Als je deze PT kan/begrijpt, beheers je een groot deel van het hoofdstuk.

Cisco Networking Academy
Mind Wide Open

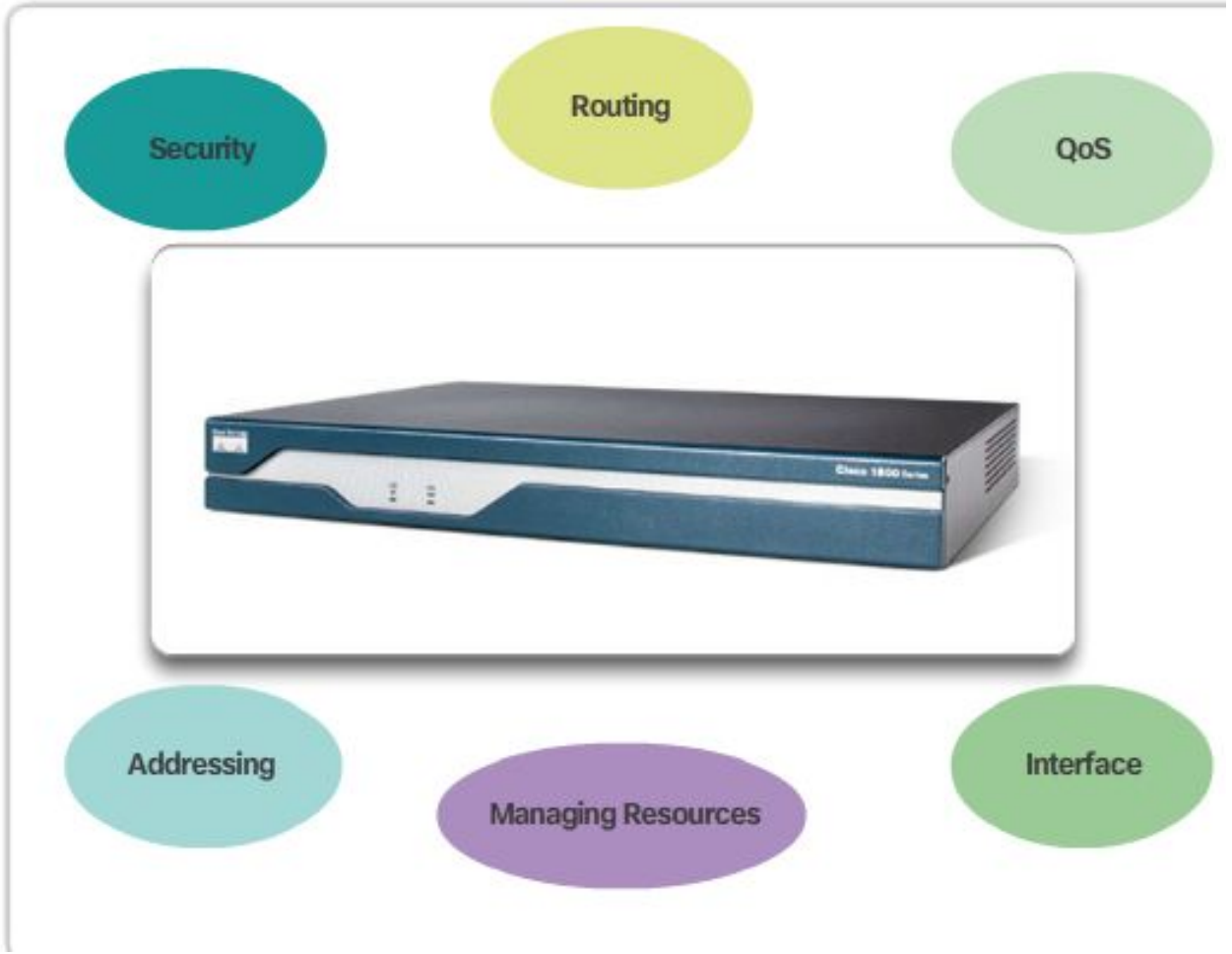
# Chapter 2: Configure a Network Operating System

Introduction to Networks v5.1

# Chapter 2:

# Configure a Network Operating

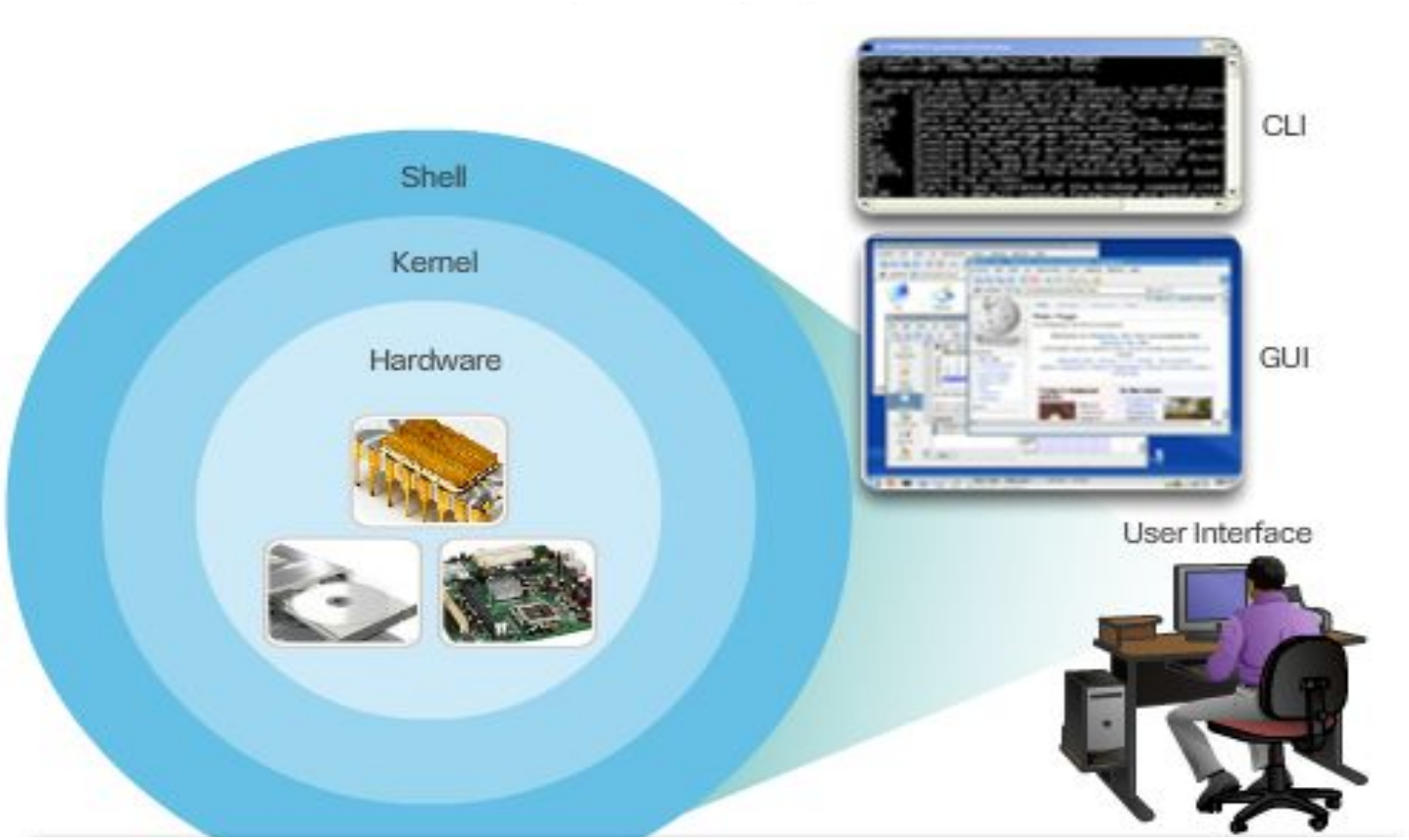
# 2.1.1.1 A Network Operating System



# Section 2.1:
# IOS Bootcamp

2.1.1: Cisco IOS
2.1.2: Cisco IOS Access
2.1.3: Navigate the IOS
2.1.4: The Command Structure

# 2.1.1.1 Operating Systems



# 2.1.1.2 Purpose of OS

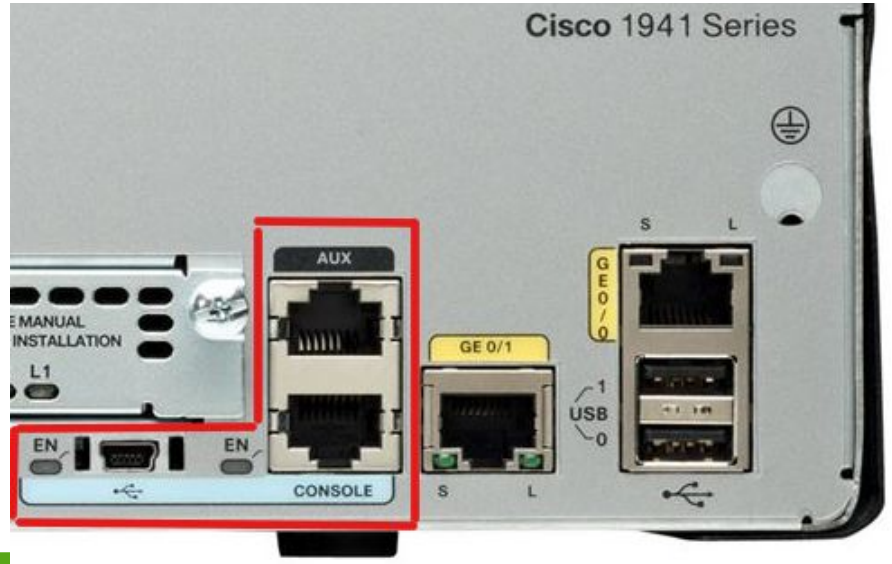
- PC operating systems enable a user to:
  - Use a mouse to make selections and run programs.
  - Enter text and text-based commands via a keyboard.
  - View output on a monitor.
  - ....
- Cisco IOS enables a network technician to:
  - Use a keyboard to run CLI-based network programs.
  - Use a keyboard to enter text and text-based commands.
  - View output on a monitor.
  - ….
- All networking devices come with a default IOS.  (remark: Update)

# 2.1.2.1 Access Methods

Console
- No networking services required.
- Initial configuration
- connection to the console port

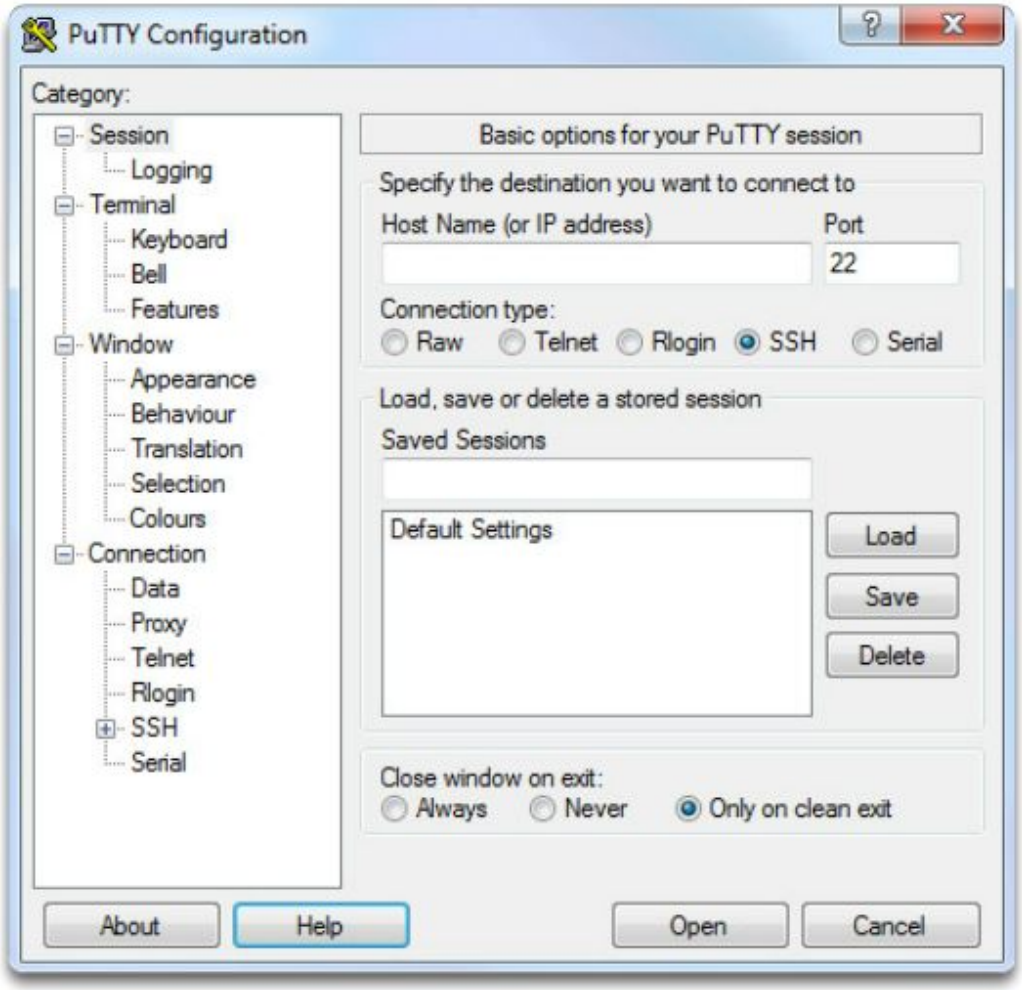
SSH
- Remote management
- secure connection (encrypted password)

Telnet
- Remote management



# 2.1.2.2 Terminal Emulation Programs

PuTTY



# 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. | | | |

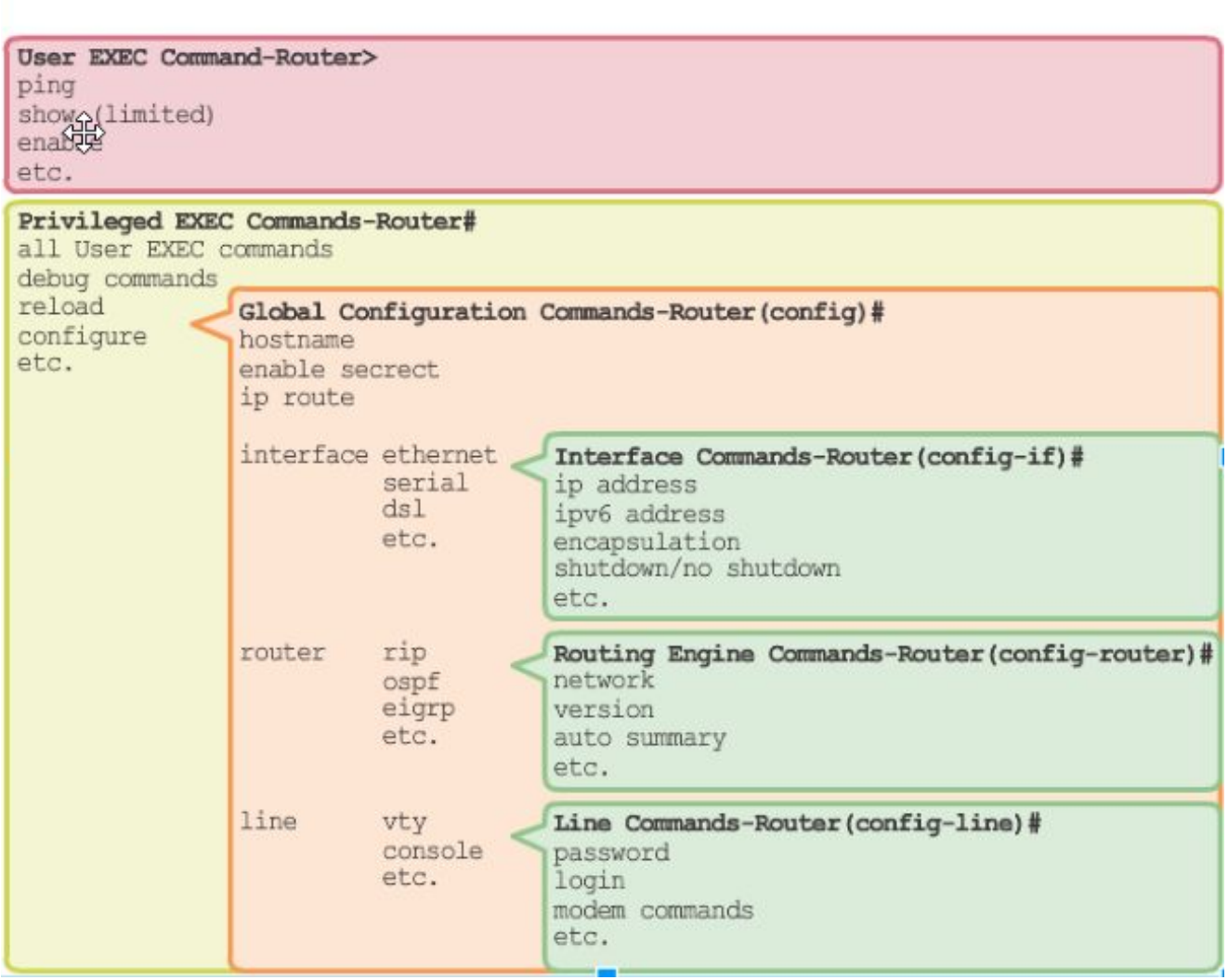
# 2.1.2.3 Activity: Accessing Devices

| | 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. | | | ✓ |

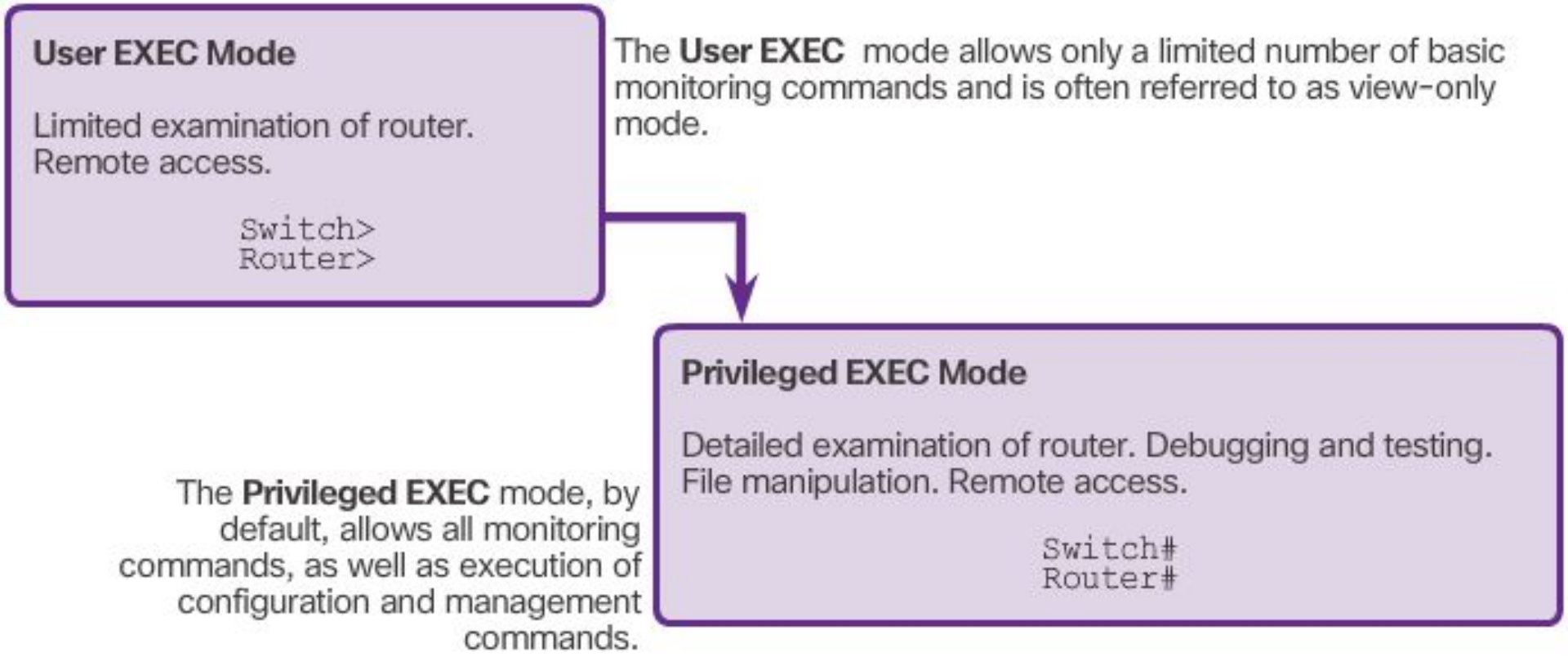
# 2.1.3.1 Cisco IOS Modes of Operation

- A console connection must be established before initial configuration of a Cisco device.
- After being consoled in, the network technician will have to navigate through various command modes of the IOS CLI.
- The Cisco IOS modes use a hierarchical structure and are quite similar for both switches and routers.
- Video Available

# 2.1.3.1 Cisco IOS Modes of Operation (cont)



# 2.1.3.2 Primary Command Modes



# 2.1.3.3 Configuration Command Modes

Global Configuration Mode

- **Configure terminal** → configure the device → exmp: **Switch(config)#**

Two common sub-configuration modes include:

- **Line Configuration Mode -**

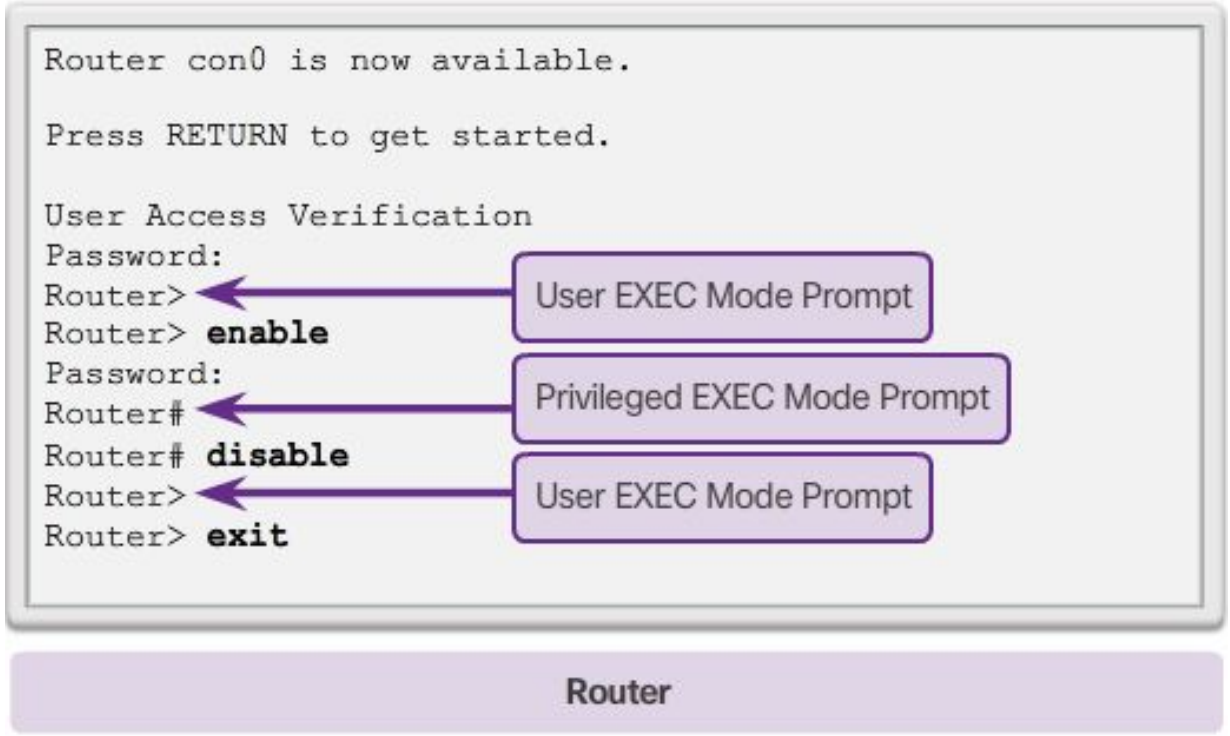
  Used to configure console, SSH, Telnet, or AUX access.
  Example: **Switch(config-line)#**

- **Interface Configuration Mode**

  Used to configure a switch port or router network interface.
  Example: **Switch(config-if)#**

- Video Available

# 2.1.3.4 Navigate Between IOS Modes



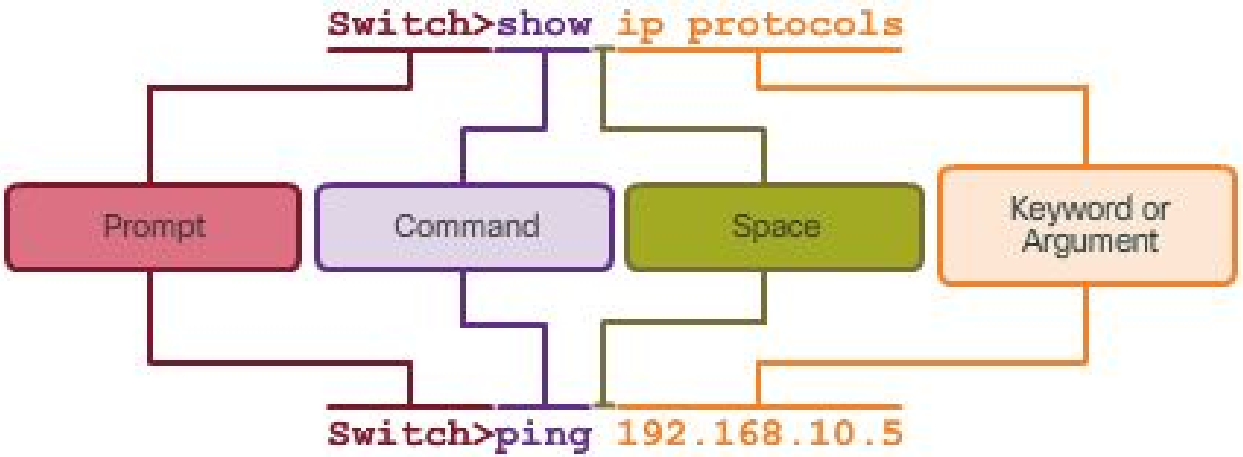
# 2.1.3.4 Navigate Between IOS Modes (cont.)

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

**Exit**
**End** or **Ctrl+Z**
Video Available

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
```

# 2.1.4.1 Basic IOS Command Structure

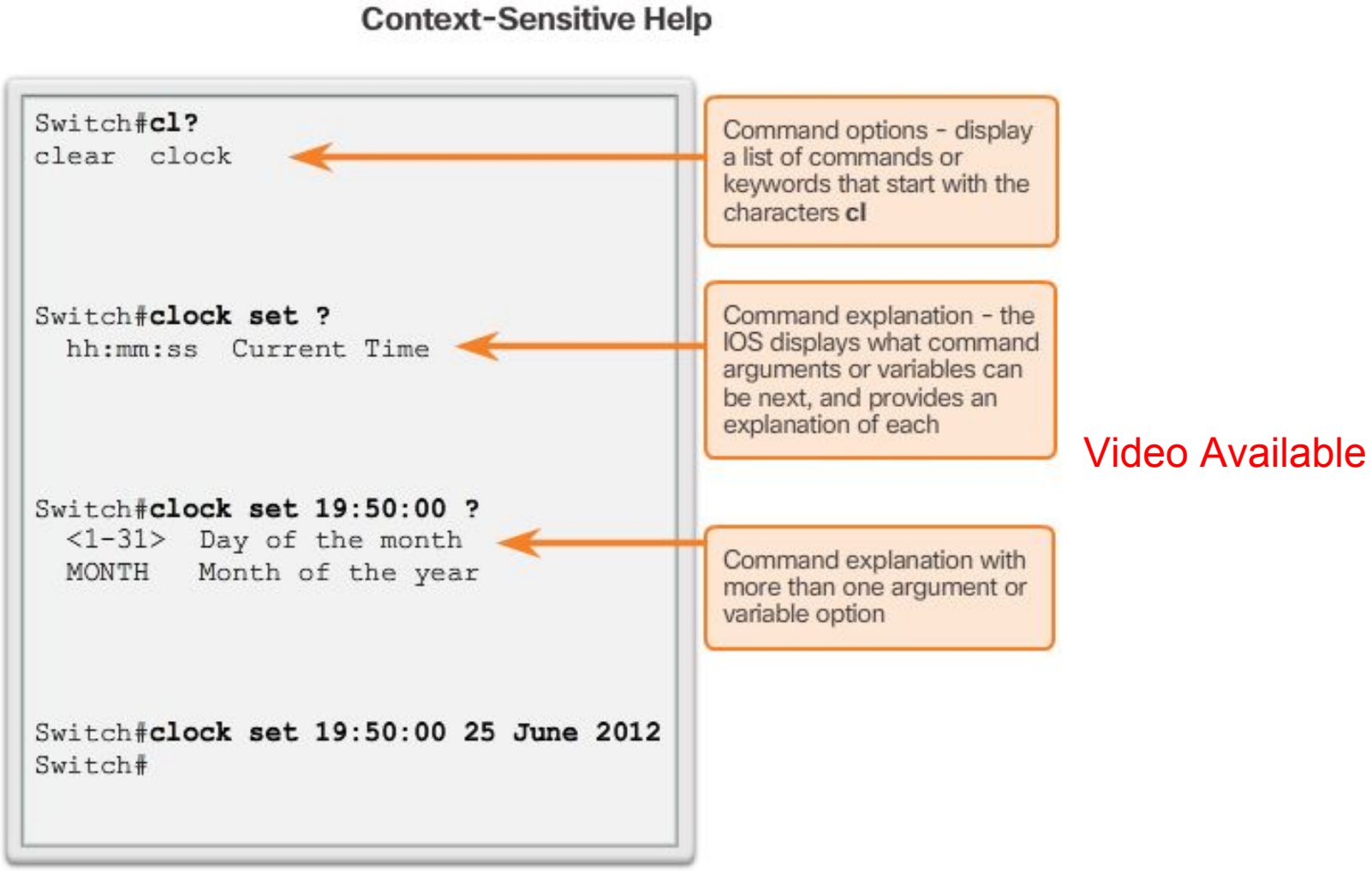


# 2.1.4.2 IOS Command Syntax

**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. |

# 2.1.4.3 IOS Help Features




Video Available

# 2.1.4.3 IOS Help Features (cont.)

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

The IOS returns a help message indicating that required keywords or arguments were left off the end of the command.

```
Switch#c
% Ambiguous command:'c'
```

The IOS returns a help message to indicate that there were not enough characters entered for the command interpreter to recognize the command.

Video Available

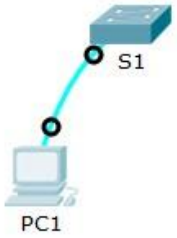
```
Switch#clock set 19:50:00 25 6
                           ^
% Invalid input detected at '^'
marker.
```

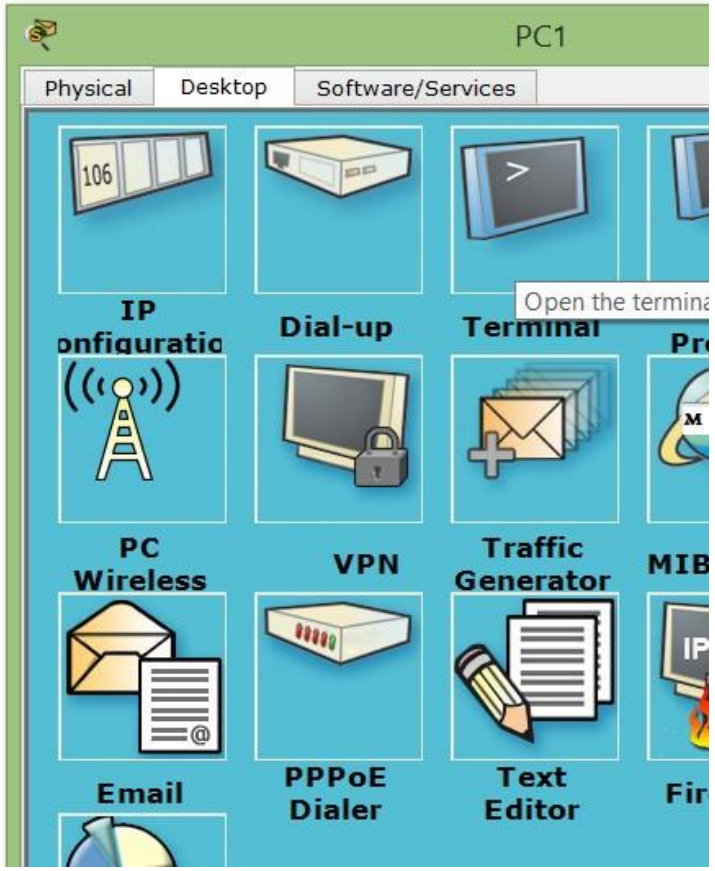
The IOS returns a "^" to indicate where the command interpreter can not decipher the command.

# 2.1.4.4 Hotkeys and Shortcuts

- **Tab –** Completes the remainder of a partially typed command or keyword
- **Ctrl-R –** Redisplays a line
- **Ctrl-A –** Moves cursor to the beginning of the line
- **Ctrl-Z –** Exits configuration mode and returns to user EXEC
- **Down Arrow –** Allows the user to scroll forward through former commands
- **Up Arrow –** Allows the user to scroll backward through former commands
- **Ctrl-Shift-6 –** Allows the user to interrupt an IOS process such as **ping** or **traceroute.**
- **Ctrl-C –** Aborts the current command and exits the configuration mode

# 2.1.4.6 Packet Tracer - Navigating the IOS



# 2.1.4.6 Packet Tracer - Navigating the IOS

1. Connect PC1 en S1 (console)
2. Terminal session
3. Explore IOS (use help)
4. Enter privileged EXEC mode
5. Enter Global config mode
6. Set the Clock

# Section 2.2:
# Basic Device Configuration

2.2.1: Hostnames
2.2.2: Limit Access to Device Configurations
2.2.3: Save Configurations

# 2.1.1.1 Device Names

## Guidelines to Choose a Hostname

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

Hostnames allow devices to be identified by network administrators over a network or the Internet.

# 2.2.1.2 Configure Hostnames

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

Syntax Checker Available

# 2.2.2.1 Secure Device Access

Securing Administrative Access

- Privileged EXEC → password
- User EXEC → password
- Remote Telnet → Password

Other

- Encrypt passwords
- Provide legal notification via motd

# 2.2.2.2 Configure Passwords

## Privileged EXEC Password Example

```
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#
```

Class

## User EXEC Password Example

```
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)#
```

## VTY Line Password

```
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)#
```

# 2.2.2.2 Configure Passwords (cont.)

- Use the **enable secret** command, not the older **enable** password command.
- The **enable secret** command provides greater security because the password is encrypted.

```
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#
```

# 2.2.2.2 Configure Passwords (cont.)

Console port must be secured.

- Reduces the chance of unauthorized personnel physically plugging a cable into the device and gaining device access.

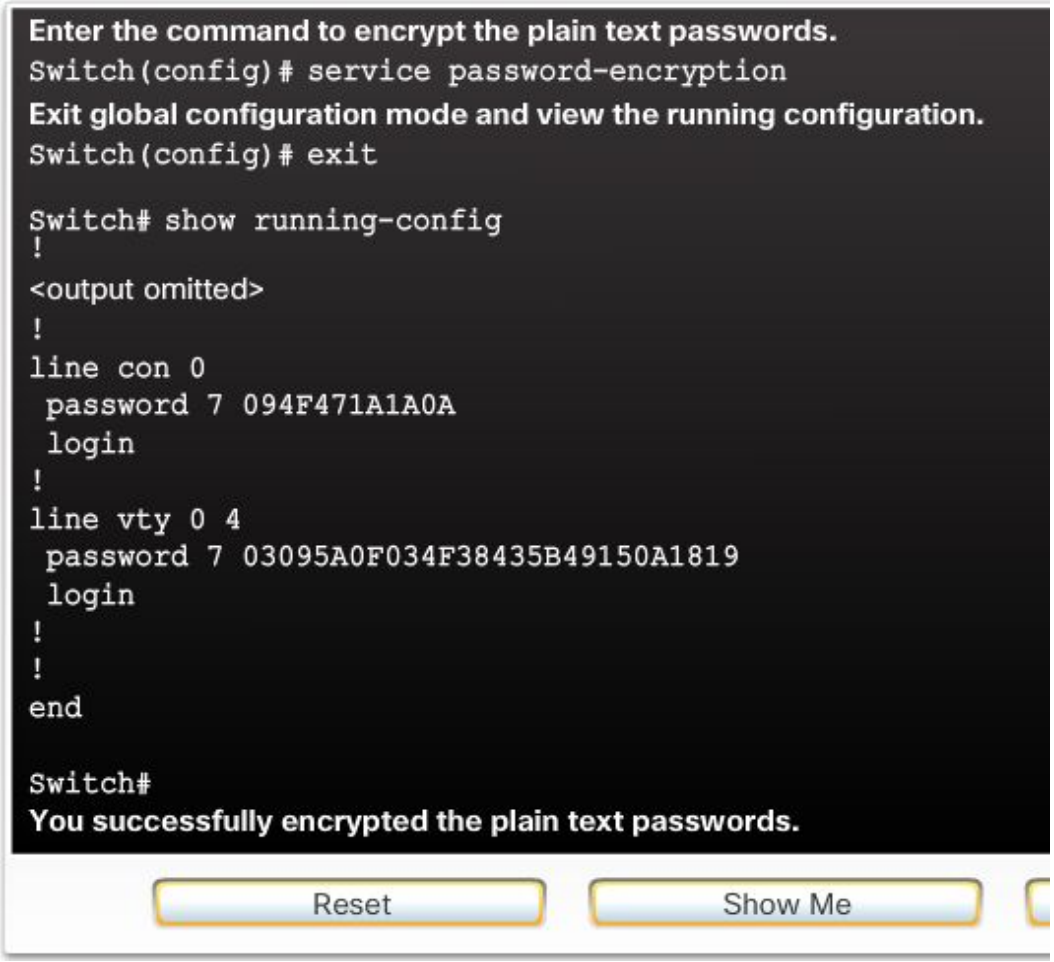
VTY lines allow access to a Cisco device via Telnet.

- The number of VTY lines supported varies with the type of device and the IOS version.

```
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)#
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)#
```

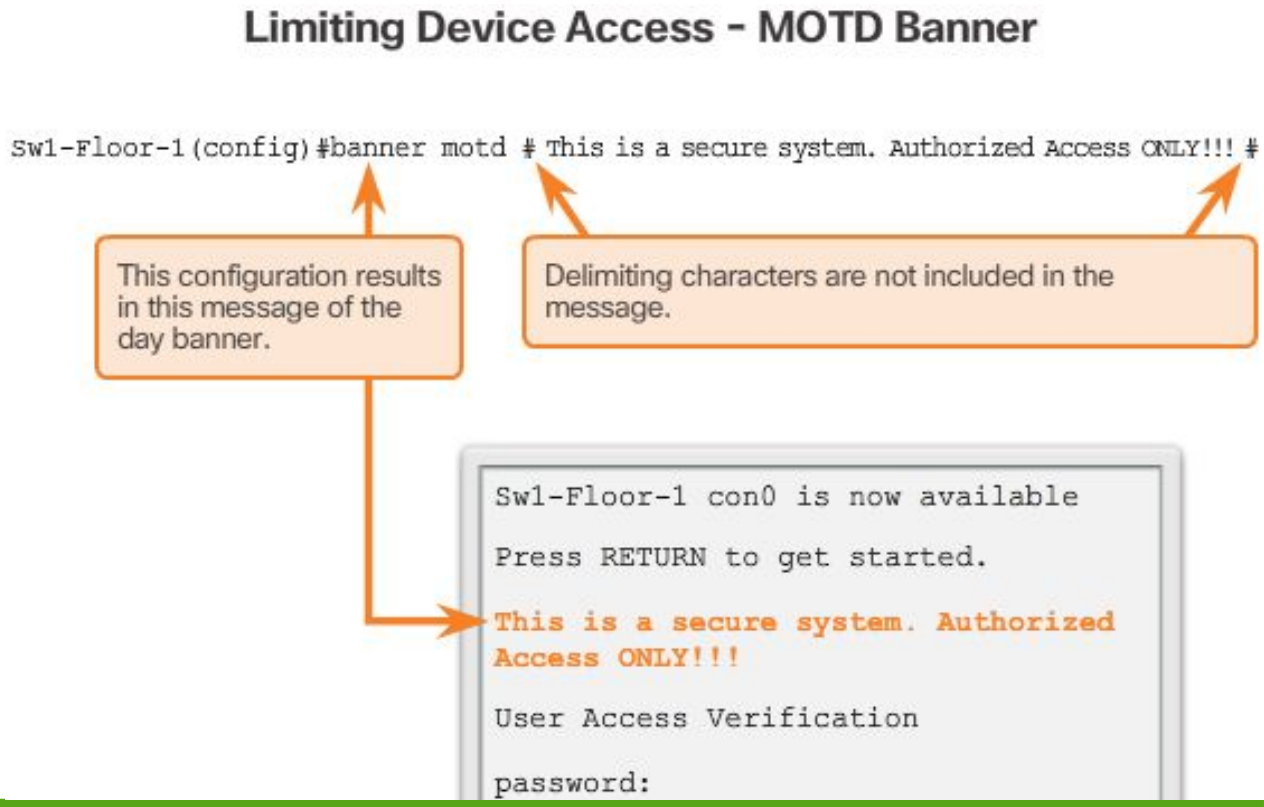
# 2.2.2.3 Encrypt Passwords

## service password-encryption



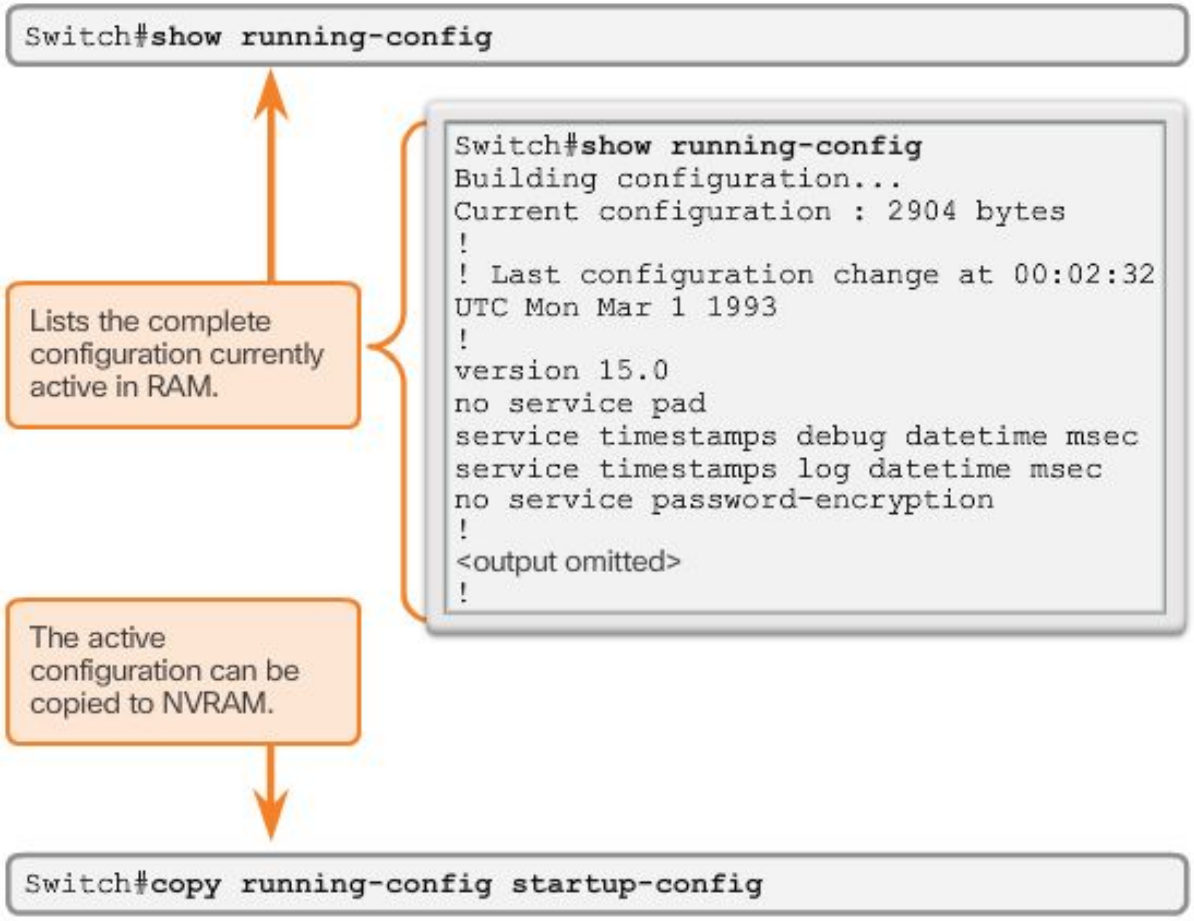
# 2.2.2.4 Banner Messages

- Wording that implies that a login is "welcome" or "invited" is not appropriate.-
- Often used for legal notification because it is displayed to all connected terminals.
- Video Available



# 2.2.3.1 Save the Running Configuration File

- **Startup configuration** –File stored in NVRAM that contains all of the commands that will tents when the device is




ifying affects the operation of
ı the device is powered off or

# 2.2.3.2 Alter the Running Configuration

- Restore the device to its previous configuration by removing the changed commands individually.
- Copy the startup configuration file to the running configuration with the **copy startup-config running-config** privileged EXEC mode command.
- Reload the device with the **reload** command from privileged EXEC mode.
- Switch# **reload**

  System configuration has been modified. Save? [yes/no]: **n**

  Proceed with reload? [confirm]

- Video Available

# 2.2.3.4 Packet Tracer - configuring initial Switch settings

# 2.2.3.4 Packet Tracer - configuring initial Switch settings

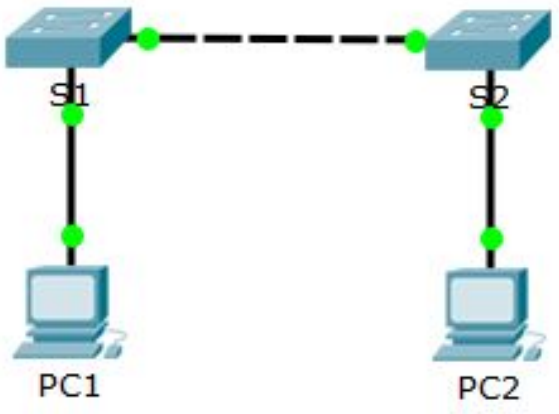
**Part 1: Verify the Default Switch Configuration**

**Part 2: Configure a Basic Switch Configuration**

**Part 3: Configure a MOTD Banner**

**Part 4: Save Configuration Files to NVRAM**

**Part 5: Configure S2**



# 2.2.3.4 Packet Tracer - configuring initial Switch settings

**Part 1: Verify the Default Switch Configuration**

**enable → show running config**

**Part 2: Configure a Basic Switch Configuration**

1. **hostname ⇒**
   **Config t → hostname S1 → exit**
2. **Secure access to console line ⇒**
   **Config t → line console 0 → password letmein → login → exit**
3. **Secure privileged mode access ⇒**
   **enable → config t → enable password c1$c0 → exit**
4. **configure encrypted password (privileged mode) ⇒**
   **config t → enable secret itsasecret → exit**
5. **encrypt the enable and console passwords ⇒**
   **config t → service password-encryption → exit**

# 2.2.3.4 Packet Tracer - configuring initial Switch settings

**Part 3: Configure a message of the day (MOTD) banner**

**config t → banner motd “.....” exit**

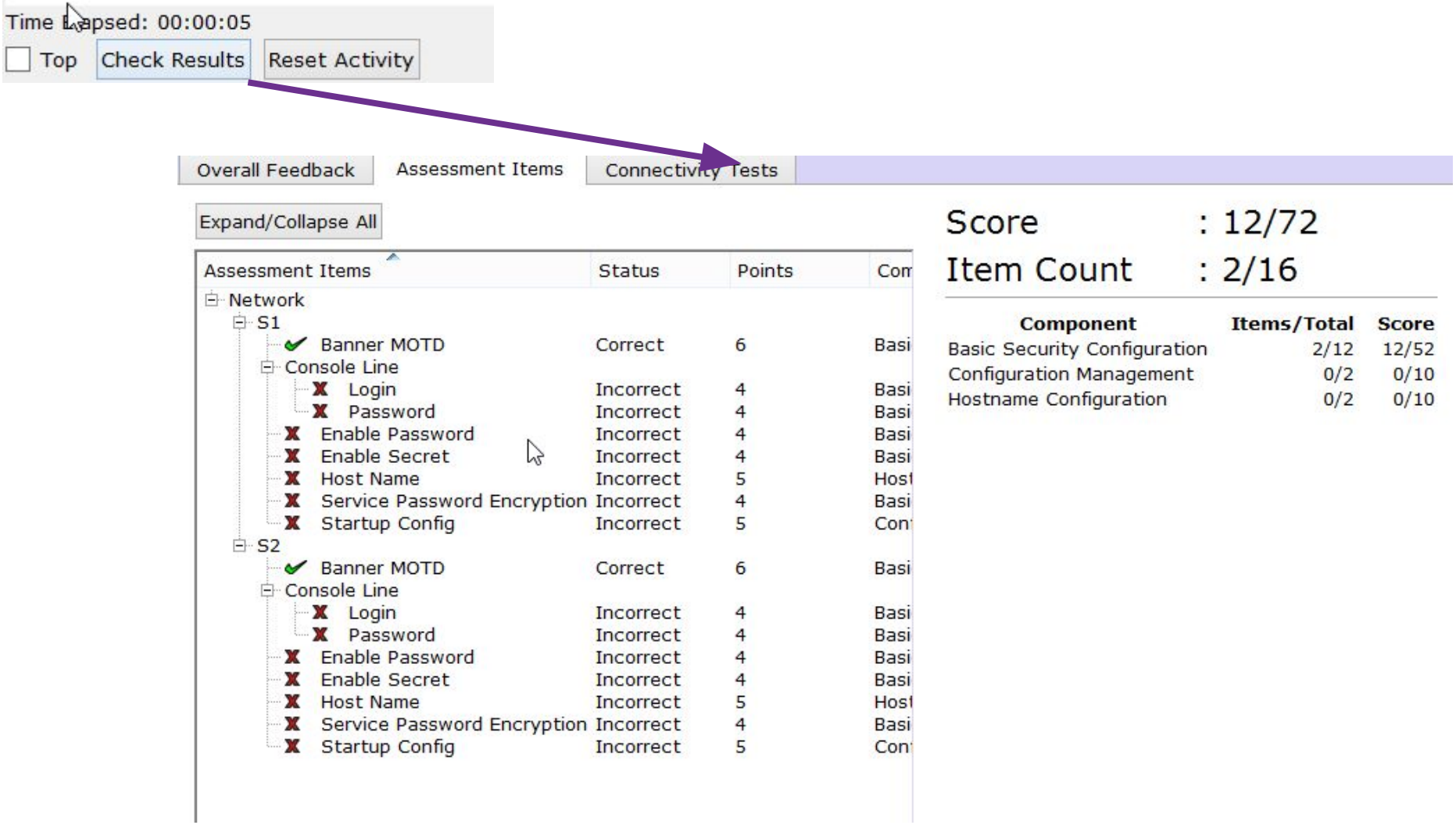
**Part 4: Save configuration files to NVRAM**

**copy running-config startup-config**

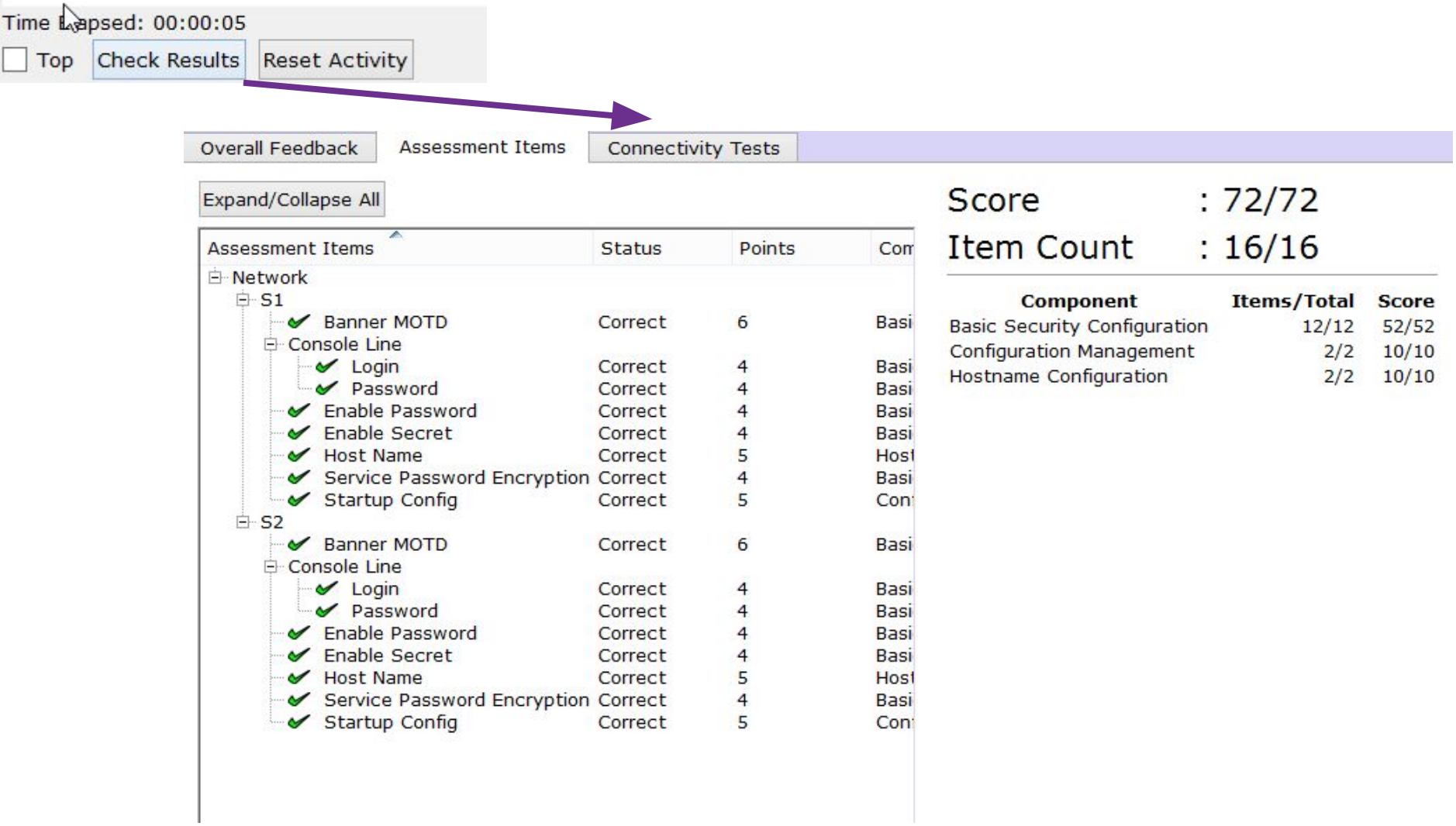
**Part 5: Configure S22**

**...**

# 2.2.3.4 Packet Tracer - configuring initial Switch settings



# 2.2.3.4 Packet Tracer - configuring initial Switch settings



# Section 2.3: Address Schemes

2.3.1: Ports and Addresses
2.3.2: Configure IP Addressing
2.3.3: Verifying Connectivity

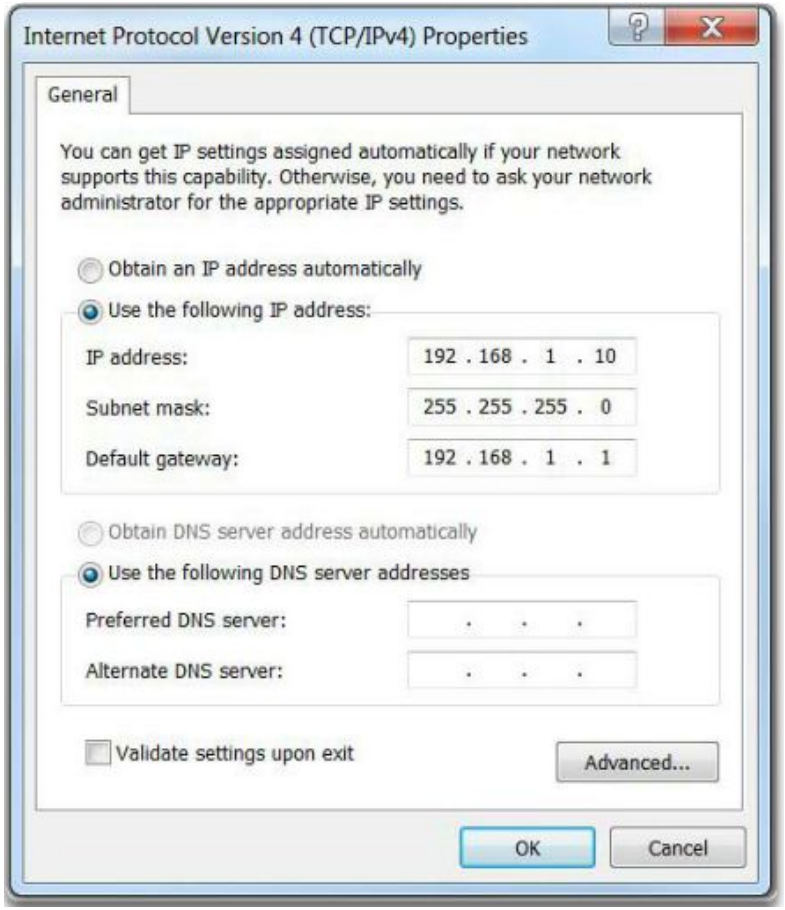
# 2.3.1.1 IP Addresses

## Connecting End Devices

Devices requiring IP addresses:

- Computers
- Network printers
- VoIP phones
- Security cameras
- Smart Phones
- Mobile devices
- ...

## Configuring a Static IP Address on a Host

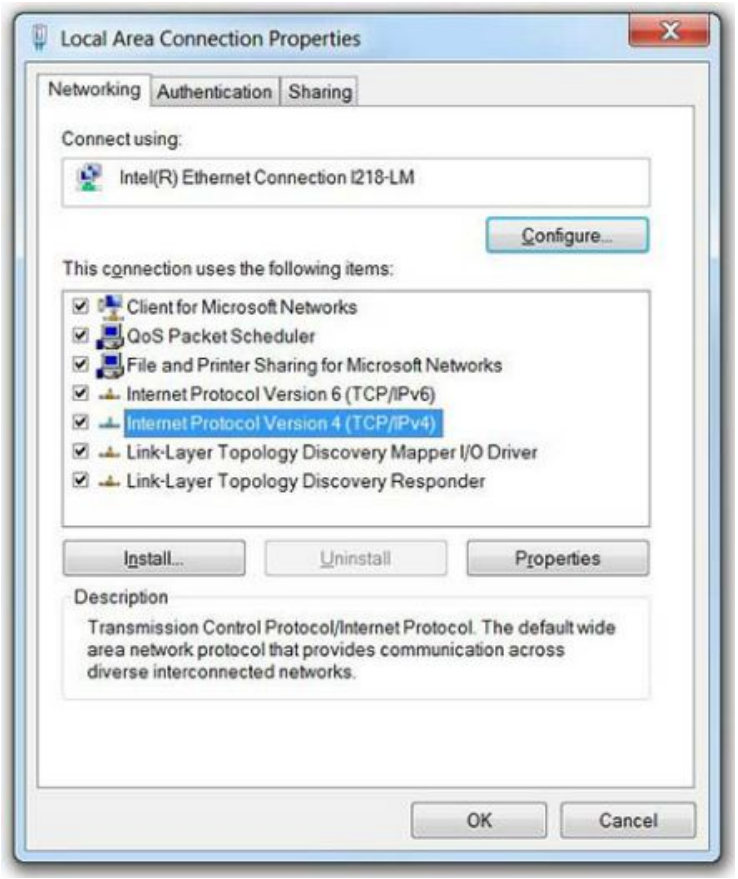


# 2.3.1.2 Interfaces and Ports

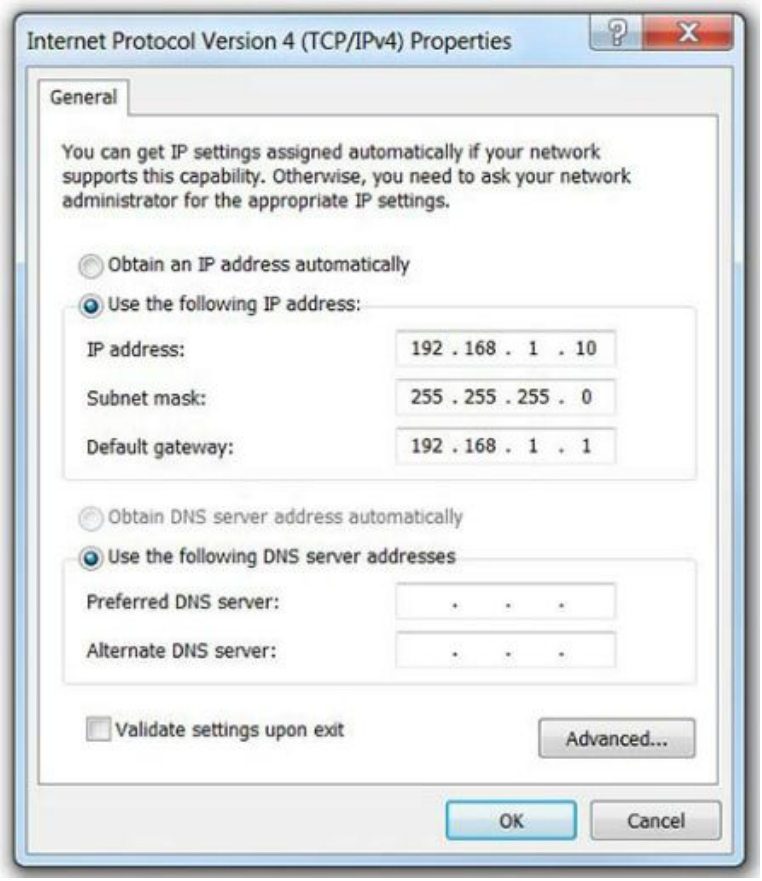
- Network communications depend on end user device interfaces, networking device interfaces, and the cables that connect them.
- Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless.
- Different types of network media have different features and benefits.
- Ethernet is the most common local area network (LAN) technology.
- Ethernet ports are found on end user devices, switch devices, and other networking devices.
- Cisco IOS switches have physical ports for devices to connect to, but they also have one or more switch virtual interfaces (SVIs). No physical hardware on the device is associated with it. It is created in software.
- SVI provides a means to remotely manage a switch over a network.

# 2.3.2.1 Manual IP Address Configuration for End Devices

## Ethernet Adapter Properties

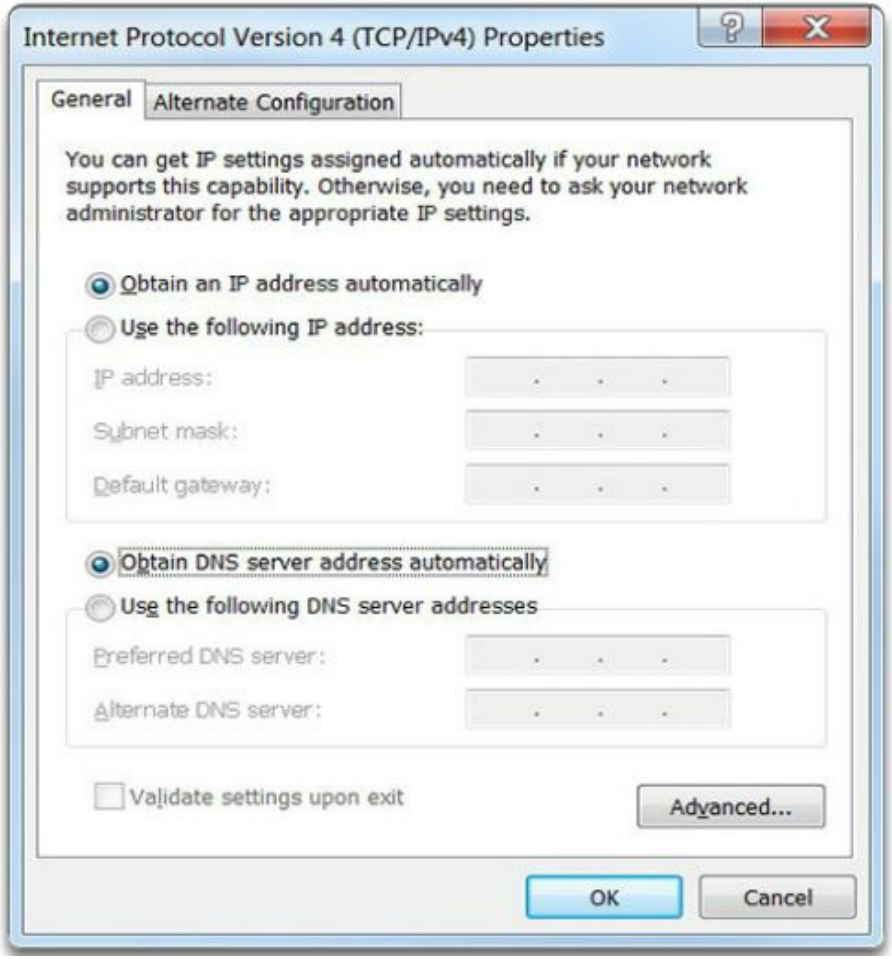



## Manually Assigning IPv4 Address Information



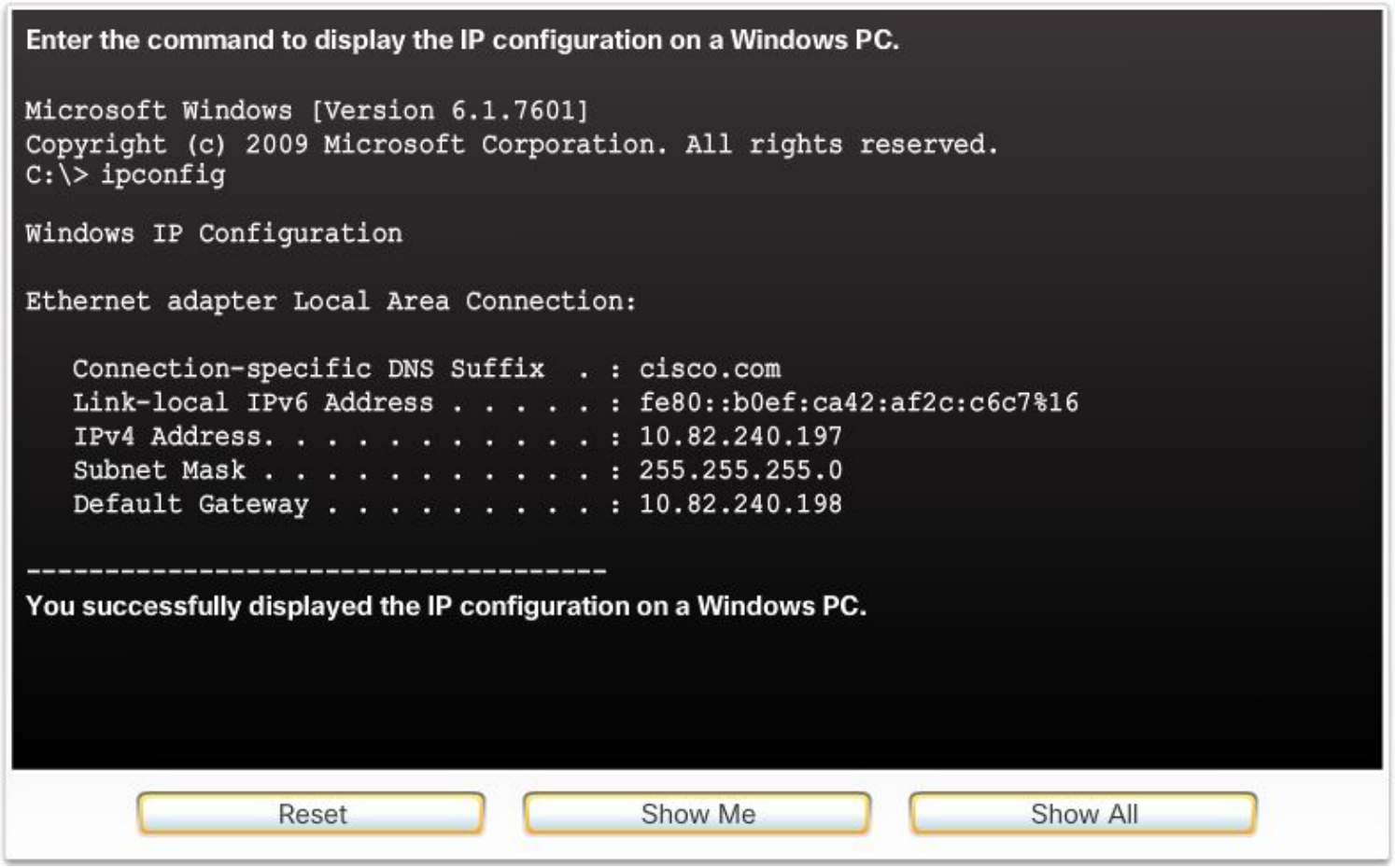
# 2.3.2.2 Automatic IP Address Configuration for End Devices

## Assigning Dynamic Addresses



# 2.3.2.2 Automatic IP Address Configuration for End Devices

## Verifying Windows PC IP Configuration



# 2.3.2.3 Switch Virtual Interface Configuration

- **IP address** - Together with subnet mask, uniquely identifies end device on internetwork
- **Subnet mask** - Determines which part of a larger network is used by an IP address
- **interface VLAN 1** - Interface configuration mode
- **ip address 192.168.10.2 255.255.255.0** - Configures the IP address and subnet mask for the switch
- **no shutdown** - Administratively enables the interface
- Switch still needs to have physical ports configured and VTY lines to enable remote management

Video Available

```
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#interface VLAN 1
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#no shutdown
```

# 2.3.2.4 Switch Virtual Interface Configuration

**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.**

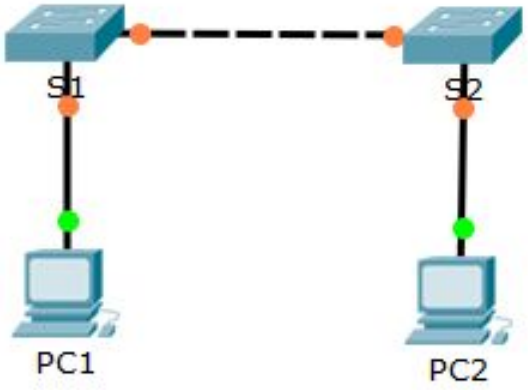
# 2.3.2.5 Packet Tracer - Implementing Basic Connectivity

# 2.3.2.5 Packet Tracer - Implementing Basic Connectivity

**Part 1: Perform a Basic Configuration on S1 and S2**

**Part 2: Configure the PCs**

**Part 3: Configure the Switch Management Interface**



# 2.3.2.5 Packet Tracer - Implementing Basic Connectivity

**Part 1: Perform a Basic Configuration on S1 and S2 ( = repeat)**

- **Hostname** **[ → hostname S1 ]**
- **Console password = cisco** **[ → line console 0 → password cisco → login]**
- **privileged password = class** **[ → enable password class ]**
- **MOTD banner** **[ → banner motd “.....”]**
- **save config** **[ → copy run start]**

**Part 2: Configure the PCs**

- **PC1: IP= 192.168.1.1 subnet mask= 255.255.255.0**
- **PC2: IP= 192.168.1.2 subnet mask= 255.255.255.0**
- **verify using ping command (e.a. On PC2: ping 192.168.1.1)**

# 2.3.2.5 Packet Tracer - Implementing Basic Connectivity

**Part 3: Configure the Switch Management Interface**

**→ configure terminal**

**→ interface vlan 1**

**→ ip address 192.168.1.253 255.255.255.0**

**→ no shutdown**

**verify:**

**show ip interface brief**

**show interfaces vlan 1**

**show running-config**

# 2.3.3.1 Interface Addressing Verification

```
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
```

```
S2#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                  192.168.10.3    YES manual  up        up
```

Video Available

# 2.3.3.4 End-to-End Connectivity Test

```
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:\>
```

Video Available

# CHAPTER 2: Summary

2.0 Introduction

2.1 IOS Bootcamp

2.2 Basic Device Configuration

2.3 Address Schemes

2.4 Summary

# 2.4.1.2 PT → Skills integration challenge

# 2.4.1.2 PT → Skills integration challenge