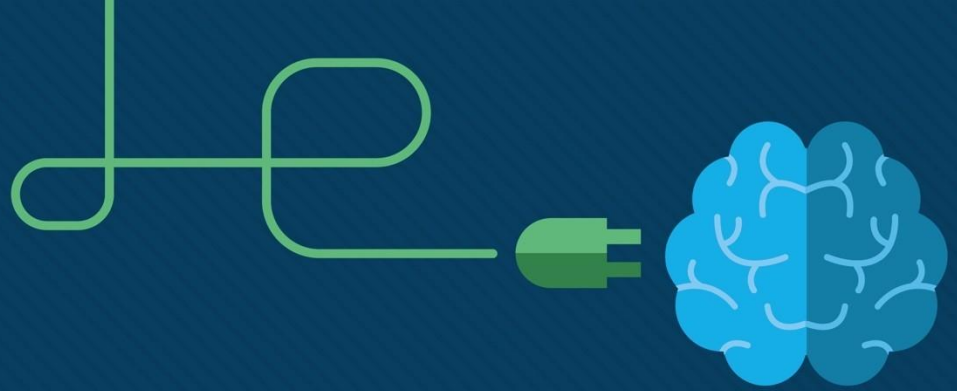


Module 2: Basic Switch and End Device Configuration

Introductions to Networks v7.0
(ITN)

Module Objectives

Topic Title	Topic Objective
Cisco IOS Access	Explain how to access a Cisco IOS device for configuration purposes.
IOS Navigation	Explain how to navigate Cisco IOS to configure network devices.
The Command Structure	Describe the command structure of Cisco IOS software.
Basic Device Configuration	Configure a Cisco IOS device using CLI.
Save Configurations	Use IOS commands to save the running configuration.
Ports and Addresses	Explain how devices communicate across network media.
Configure IP Addressing	Configure a host device with an IP address.

Verify Connectivity	Verify connectivity between two end devices.

Module Title: Basic Switch and End Device Configuration

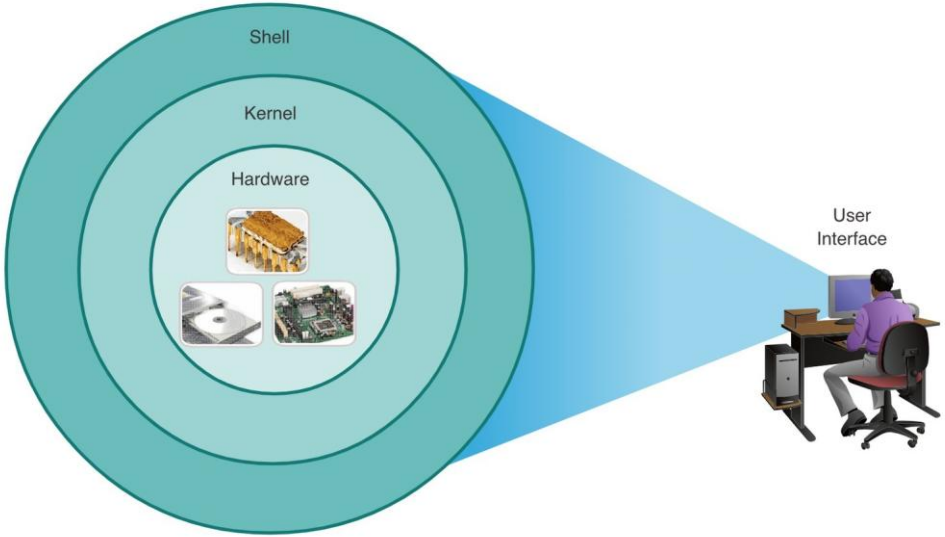
Module Objective: Implement initial settings including passwords, IP addressing, and default gateway parameters on a network switch and end devices.

2.1 Cisco IOS Access

(IOS – Internetwork Operating System)

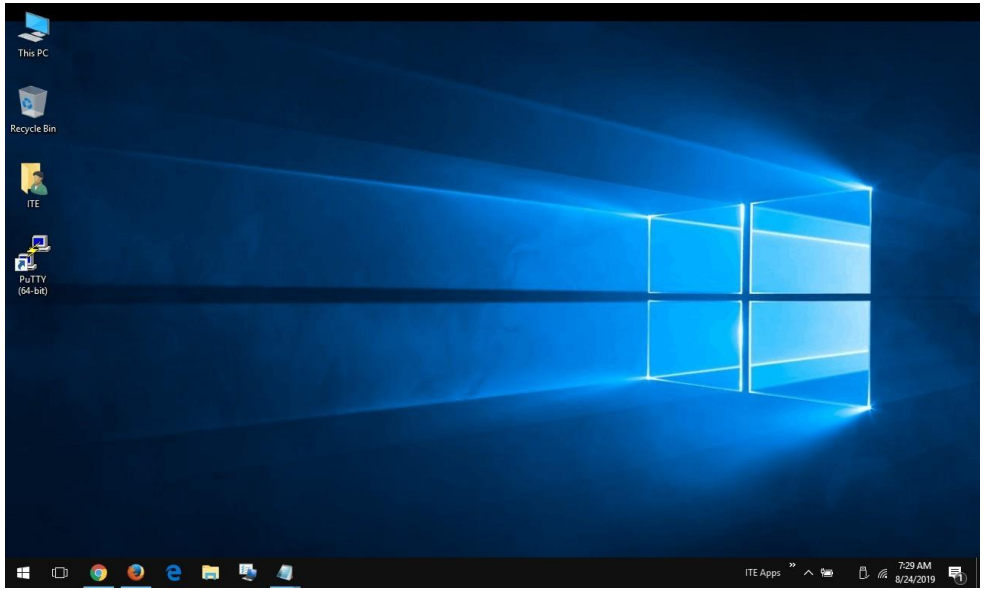
Operating Systems

- **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 following:

- Use a mouse to make selections programs
- Enter text and text-based commands
- View output on a monitor

CLI-based network operating system enables a the network technician to do the following:

- Use a keyboard to run CLI-based and run network programs
- Use a keyboard to enter text and commands text-based

Cisco IOS Access

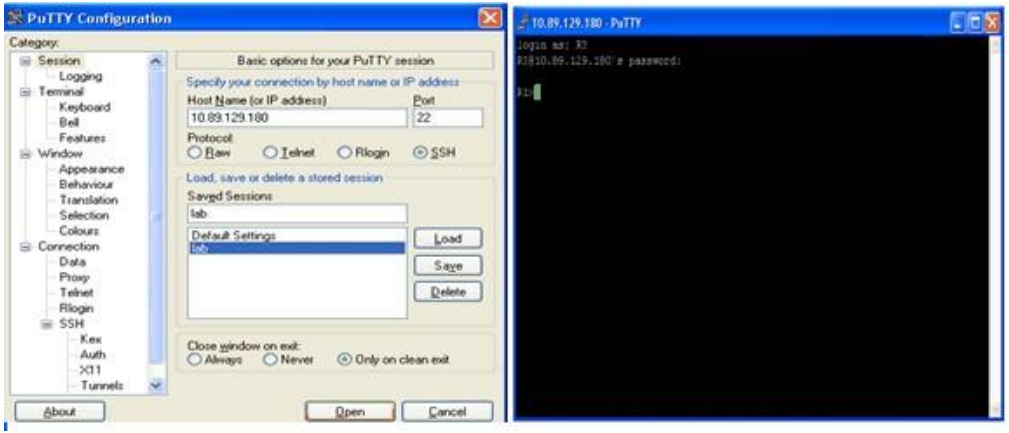
```
analyst@secOps ~]$ ls
Desktop  Downloads  lab.support.files  second_drive
[analyst@secOps ~]$
```

Access Methods

- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.

Cisco IOS Access

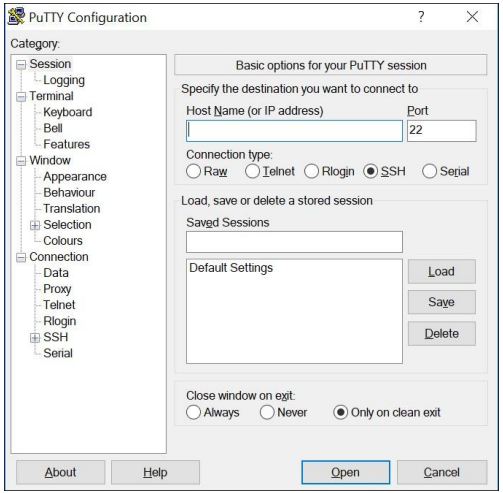
- **Secure Shell (SSH)** – Establishes a secure remote CLI connection to a device, through a virtual interface, over a network. (Note: This is the recommended method for remotely connecting to a device.)
- **Telnet** – Establishes an insecure remote CLI connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext.)

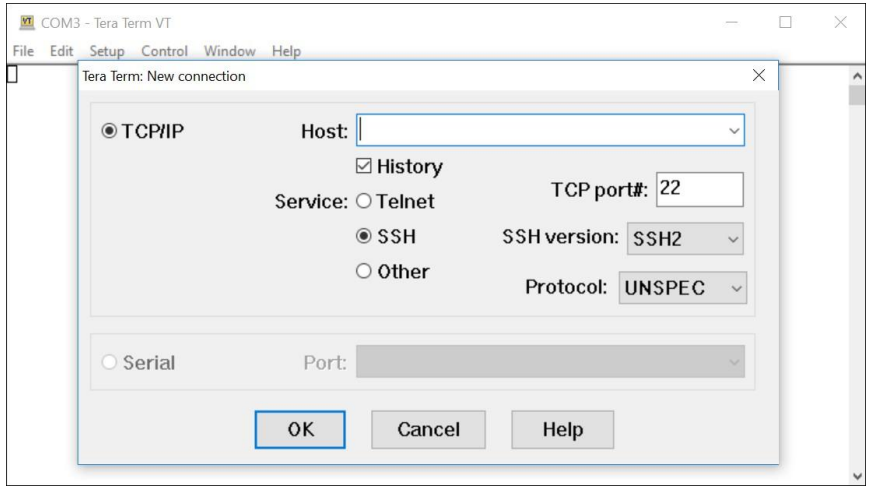


Terminal Emulation Programs

- 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 and SecureCRT.

Cisco IOS Access





2.2 IOS Navigation

Primary Command Modes

User EXEC Mode:

- Allows access to only a limited number of basic monitoring commands
- Identified by the CLI prompt that ends with the > symbol

```
Router>

Switch>
```

Privileged EXEC Mode:

- Allows access to all commands and features
- 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

```
Switch(config)#
```

Line Configuration Mode:

- Used to configure console, SSH, Telnet or AUX access

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

Interface Configuration Mode:

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

IOS Navigation

- Used to configure a switch port or router interface

Navigation Between IOS Modes

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

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

type. To return to global configuration mode, use the **exit** command.

Navigation Between IOS Modes (Cont.)

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**.

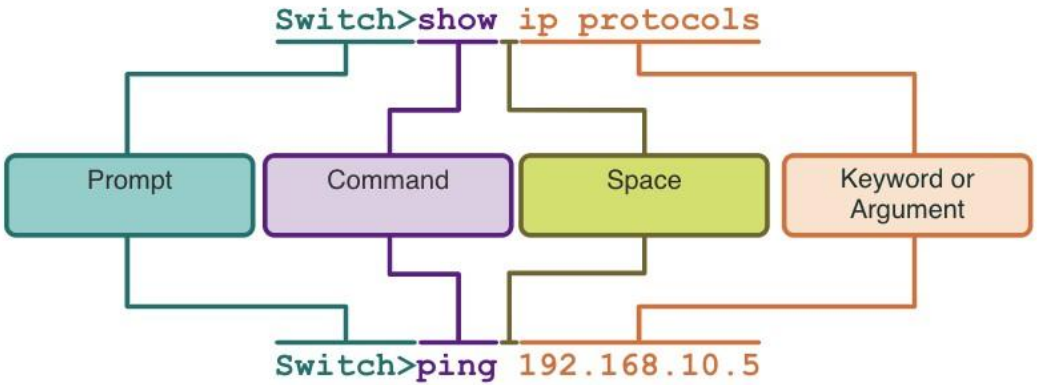
```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

- 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



- **Keyword** – This is a specific parameter defined in the operating system (in the figure, **ip protocols**).

The Command Structure

- **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.

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).

The Command Structure

{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 (Cont.)

- The command syntax provides the pattern, or format, that must be used when entering a command.

- The command is **ping** and the userdefined 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 *ipaddress* of the destination

```
traceroute ip-address
```

The Command Structure

device. For example, **traceroute 192.168.254.254**.

- 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?

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

- Command syntax check verifies that a valid command was entered by the user.

The Command Structure

- If the interpreter cannot understand the command being entered, it will provide feedback describing what is wrong with the command.

```
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.

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

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

The Command Structure

- 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**.

Hot Keys and Shortcuts (Cont.)

- 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.

Hot Keys and Shortcuts (Cont.)

- 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.
  - The table below lists commands that can be used to exit out of an operation.

The Command Structure

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.

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.

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

2.4 Basic Device Configuration

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

Basic Device Configuration

```
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:
- Use passwords that are more than eight characters in length.
- Use a combination of upper and lowercase letters, numbers,

assword 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.

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 user EXEC mode access:

Basic Device Configuration

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

- 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.

Configure Passwords (Cont.)

Securing VTY line access:

- First enter line VTY configuration mode using the **line vty 0 15** command in global configuration mode.
- Next, specify the VTY password using the **password** *password* command.
- Finally, enable VTY access using the **login** command.

```
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#
```

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

Basic Device Configuration

```
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.

Basic Device Configuration

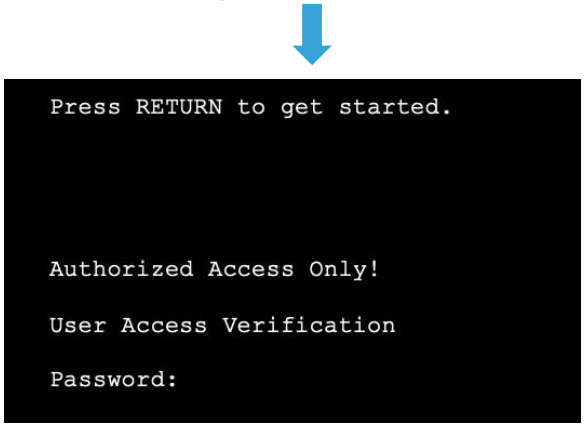
- To create a banner message of the day on a network device, use the **banner motd #** *the message of the day* **#** global config command.

Note: The "#" in the command syntax is called the delimiting character. It is entered before and after the message.

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

The banner will be displayed on attempts to access the device.

Basic Device Configuration



2.5 Save Configurations

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.

Save Configurations

```
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 ...
```

Save Configurations

If the undesired changes were saved to the startup-config, it may be necessary to clear all the configurations using the **erase startupconfig** command in privilege EXEC mode.

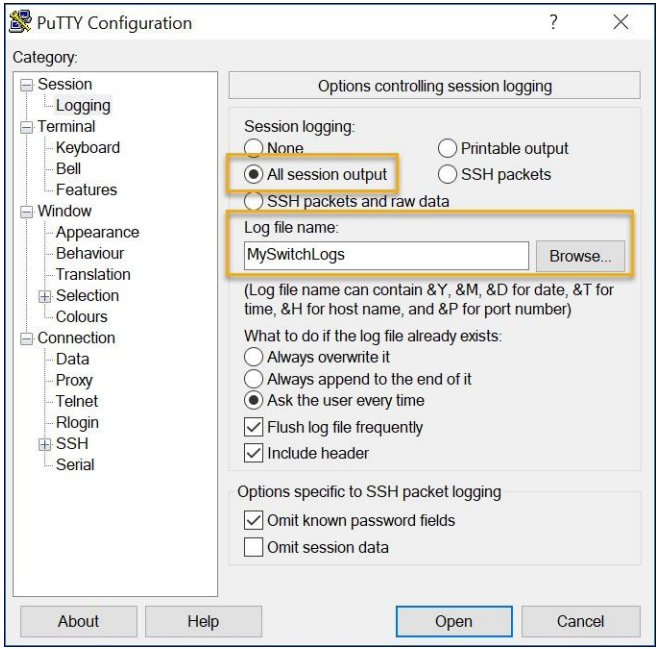
- After erasing the startup-config, reload the device to clear the running-config file from RAM.

```
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).



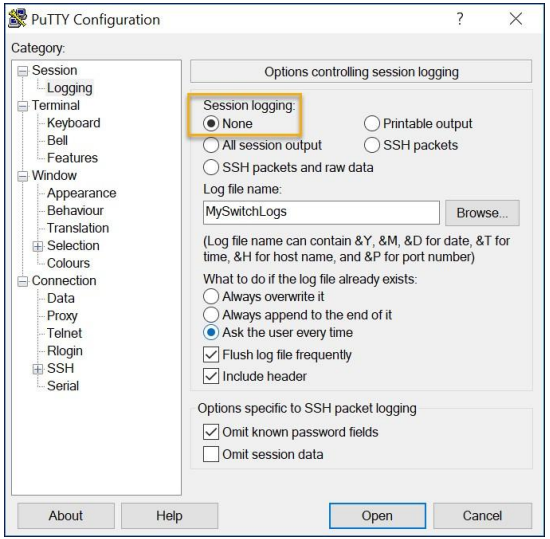
Capture Configuration to a Text File (Cont.)

- **Step 3.** Execute the **show runningconfig** or **show startup-config** command at the privileged EXEC prompt. Text displayed in the terminal window will be placed into the chosen file.

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

Save Configurations

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

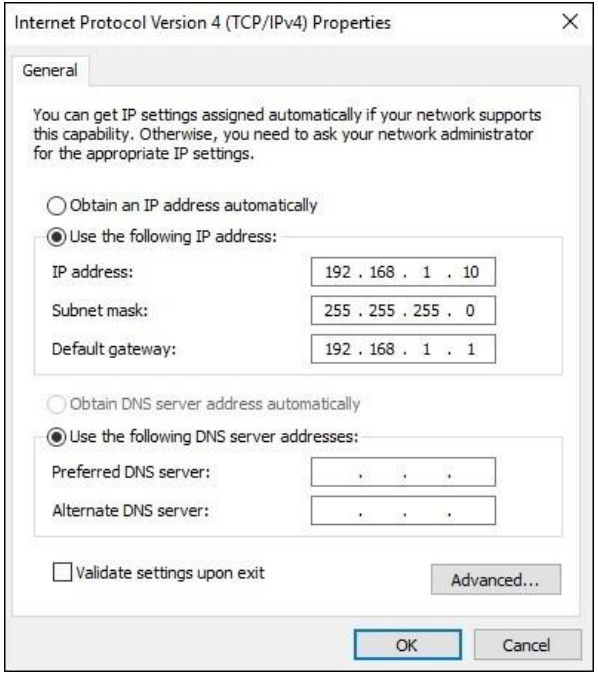


Note: The text file created can be used as a record of how the device is currently implemented. The file could require editing before being used to restore a saved configuration to a device.

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.

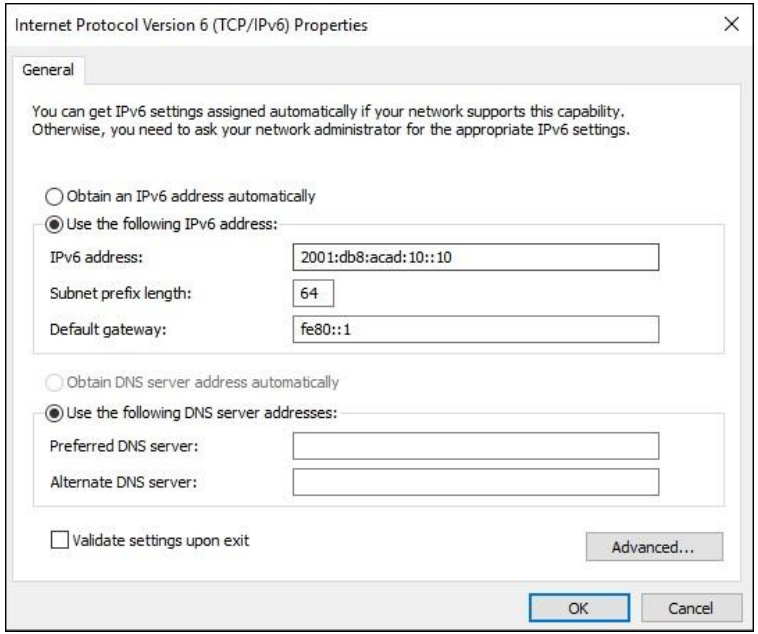


Ports and Addresses

- 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 (Cont.)

- 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.

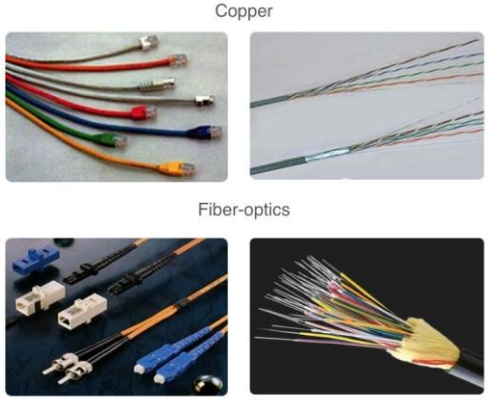


Ports and Addresses

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 twistedpair 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



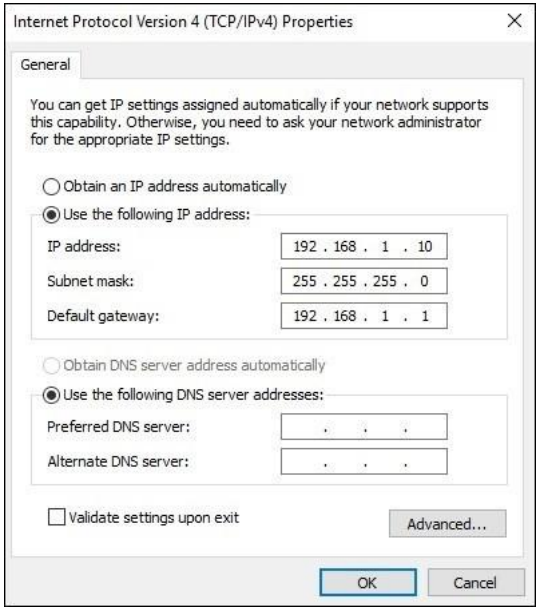
Ports and Addresses

- Amount of data and the speed at which it must be transmitted
- Cost of the media and installation

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 Host Configuration Protocol (DHCP).
- To manually configure an IPv4 address on a Windows PC, open the **Control Panel > Network and 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 configure the IPv4 address and subnet mask



information, and default gateway.

Note: IPv6 addressing and configuration options are similar to IPv4.

Configure IP Addressing 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 and 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.

Configure IP Addressing

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.

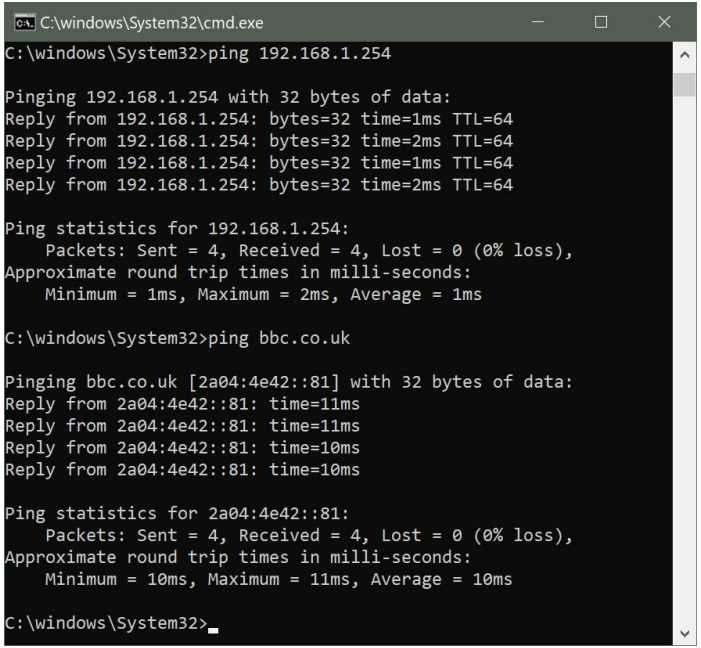
```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

2.8 Verify Connectivity

Verify Connectivity

Ping Command

- The ping command will help to see the connectivity from device A to device B. Once you know the IP address or domain name, we can ping those computing devices.




CISCO