Welcome to Switching, Routing, and Wireless Essentials v7.0 (SRWE)

Welcome to the Switching, Routing, and Wireless Essentials (SRWE) course. This is the second course in the CCNA curriculum series. It focuses on switching technologies and router operations that support small-to-medium business networks and includes wireless local area networks (WLAN) and security concepts. In addition to learning, key switching and routing concepts, learners will be able to perform basic network configuration and troubleshooting, identify and mitigate LAN security threats, and configure and secure a basic WLAN.

Welcome to Switching, Routing, and Wireless Essentials v7.0 (SRWE)

These course materials will assist you in developing the skills necessary to do the following:

- **Configure devices using security best practices.**
- **Explain how Layer 2 switches forward data.**
- **Implement VLANs and trunking in a switched network.**
- **Troubleshoot inter-VLAN routing on Layer 3 devices.**
- **Explain how STP enables redundancy in a layer 2 network.**
- **Troubleshoot EtherChannel on switched networks.**
- **Implement DHCPv4 to operate across multiple LANs.**
- **Configure dynamic address allocation in IPv6 networks.**
- **Explain how FHRPs provide default gateway services in a redundant network.**
- **Explain how vulnerabilities compromise LAN security.**
- **Configure switch security to mitigate LAN attacks.**
- **Explain how WLANs enable network connectivity.**
- **Implement a WLAN using a wireless router and a WLC.**
- **Explain how routers use information in packets to make forwarding decisions.**
- **Configure IPv4 and IPv6 static routes.**
- **Troubleshoot static and default routes.**

CCNA: Switching, Routing, and Wireless Essentials

Course Overview

The second course in the CCNA curriculum focuses on switching technologies and router operations that support small-to-medium business networks and includes wireless local area networks (WLAN) and security concepts.

Benefits

Students learn key switching and routing concepts. They can perform basic network configuration and troubleshooting, identify and mitigate LAN security threats, and configure and secure a basic WLAN.

Learning Components

- 16 modules
- 14 hands-on labs
- 31 Cisco Packet Tracer activities
- 15 videos
- 19 syntax checkers
- 1 interactive activity
- 36 CYU quizzes
- 16 module exams
- 5 module group exams
- 1 final exam

Features

Target Audience: Secondary vocational students, 2-year and 4-year college students in Networking or Engineering

Prerequisites: None

Instructor Training Required: Yes

Languages: English

Course Delivery: Instructor-led

Course Recognitions: Certificate of Completion, Letter of Merit, Digital Badge

Estimated Time to Complete: 70 hours

Recommended Next Course: CCNA: Enterprise Networking, Security, and Automation

Module 1: Basic Device Configuration

Introduction

Welcome to Basic Device Configuration!

Welcome to the first module in CCNA Switching, Routing, and Wireless Essentials! You know that switches and routers come with some built-in configuration, so why would you need to learn to further configure switches and routers?

Imagine that you purchased a model train set. After you had set it up, you realized that the track was just a simple oval shape and that the train cars only ran clockwise. You might want the track to be a figure eight shape with an overpass. You might want to have two trains that operate independently of each other and are able to move in different directions. How could you make that happen? You would need to reconfigure the track and the controls. It is the same with network devices. As a network administrator you need detailed control of the devices in your network. This means precisely configuring switches and routers so that your network does what you want it to do. This module has many Syntax Checker and Packet Tracer activities to help you develop these skills. Let's get started!

Module Objectives

Configure devices using security best practices.

Topic Title	Topic Objective
Configure a Switch with Initial Settings	Configure initial settings on a Cisco switch.
Configure Switch Ports	Configure switch ports to meet network requirements.
Secure Remote Access	Configure secure management access on a switch.
Basic Router Configuration	Configure basic settings on a router to route between two directly-connected networks, using CLI.
Verify Directly Connected Networks	Verify connectivity between two networks that are directly connected to a router.

Module 1: Basic Device Configuration

TOPIC 1.1: Configure a Switch with Initial Settings
1.1.1 Switch Boot Sequence

After a Cisco switch is powered on, it goes through the following five-step boot sequence:

Step 1: First, the switch loads a power-on self-test (POST) program stored in ROM. POST checks the CPU subsystem. It tests the CPU, DRAM, and the portion of the flash device that makes up the flash file system.

Step 2: Next, the switch loads the boot loader software. The boot loader is a small program stored in ROM that is run immediately after POST successfully completes.

Step 3: The boot loader performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, the quantity of memory, and its speed.

Step 4: The boot loader initializes the flash file system on the system board.

Step 5: Finally, the boot loader locates and loads a default IOS operating system software image into memory and gives control of the switch over to the IOS.

1.1 Configure a Switch with Initial Settings
1.1.2 The boot system Command

- The switch attempts to automatically boot by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable file it can find.
- The IOS operating system then initializes the interfaces using the Cisco IOS commands found in the startup-config file. The startup-config file is called **config.text** and is located in flash.
- In the example, the BOOT environment variable is set using the **boot system** global configuration mode command. Notice that the IOS is located in a distinct folder and the folder path is specified. Use the command **show boot** to see what the current IOS boot file is set to.

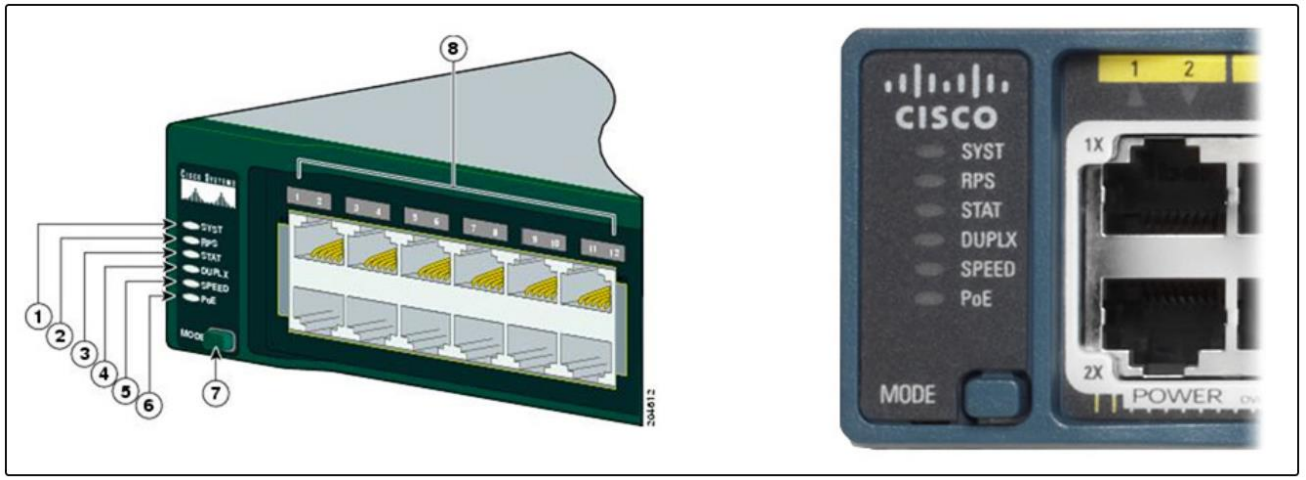
```
S1(config)# boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

Command	Definition
boot system	The main command
flash:	The storage device
c2960-lanbasek9-mz.150-2.SE/	The path to the file system
c2960-lanbasek9-mz.150-2.SE.bin	The IOS file name

1.1 Configure a Switch with Initial Settings
1.1.3 Switch LED Indicators

Cisco Catalyst switches have several status LED indicator lights. You can use the switch LEDs to quickly monitor switch activity and performance. Switches of different models and feature sets will have different LEDs and their placement on the front panel of the switch may also vary.

The figure shows the switch LEDs and the Mode button for a Cisco Catalyst 2960 switch.



1.System LED (SYST): Shows whether the system is receiving power and functioning properly.

2.Redundant Power Supply LED (RPS): Shows the RPS status.

3.Port Status LED (STAT): When green, indicates port status mode is selected, which is the default. Port status can then be understood by the light associated with each port.

4.Port Duplex LED (DUPLX): When green, indicates port duplex mode is selected. Port duplex can then be understood by the light associated with each port.

5.Port Speed LED (SPEED): When green, indicates port speed mode is selected. Port speed can then be understood by the light associated with each port.

6.Power over Ethernet LED (PoE): Present if the switch supports PoE. Indicates the PoE status of ports on the switch.

7.The **Mode button** is used to move between the different modes – STAT, DUPLX, SPEED, and PoE

1.1 Configure a Switch with Initial Settings
1.1.4 Recovering from a System Crash

The boot loader provides access into the switch if the operating system cannot be used because of missing or damaged system files. The boot loader has a command line that provides access to the files stored in flash memory. The boot loader can be accessed through a console connection following these steps:

Step 1. Connect a PC by console cable to the switch console port. Configure terminal emulation software to connect to the switch.

Step 2. Unplug the switch power cord.

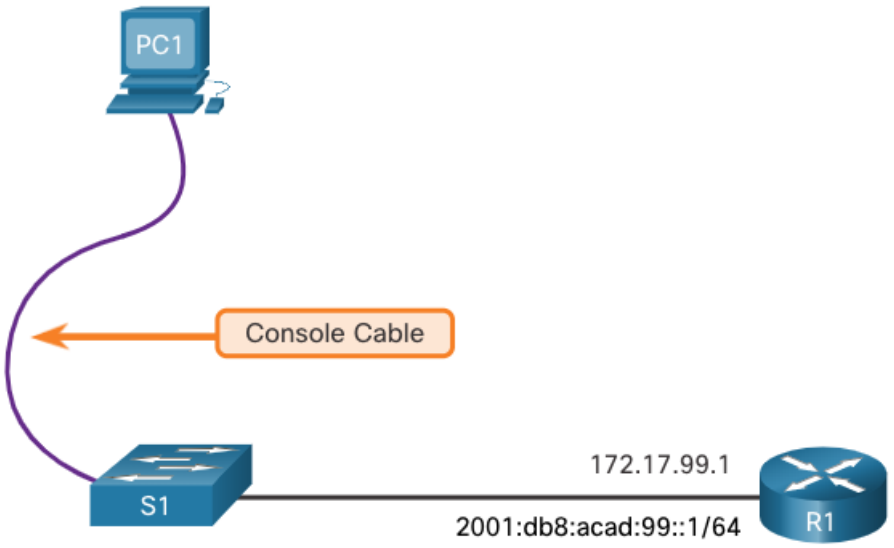
Step 3. Reconnect the power cord to the switch and, within 15 seconds, press and hold down the **Mode** button while the System LED is still flashing green.

Step 4. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; then release the **Mode** button.

Step 5. The boot loader **switch:** prompt appears in the terminal emulation software on the PC.

The boot loader command line supports commands to format the flash file system, reinstall the operating system software, and recover a lost or forgotten password. For example, the **dir** command can be used to view a list of files within a specified directory.

1.1 Configure a Switch with Initial Settings
1.1.5 Switch Management Access



To prepare a switch for remote management access, the switch must be configured with an IP address and a subnet mask.

- To manage the switch from a remote network, the switch must be configured with a default gateway. This is very similar to configuring the IP address information on host devices.
- In the figure, the switch virtual interface (SVI) on S1 should be assigned an IP address. The SVI is a virtual interface, not a physical port on the switch. A console cable is used to connect to a PC so that the switch can be initially configured.

1.1 Configure a Switch with Initial Settings
1.1.6 Switch SVI Configuration Example

By default, the switch is configured to have its management controlled through VLAN 1. All ports are assigned to VLAN 1 by default. For security purposes, it is considered a best practice to use a VLAN other than VLAN 1 for the management VLAN,

Step 1: **Configure the Management Interface:** From VLAN interface configuration mode, an IPv4 address and subnet mask is applied to the management SVI of the switch.

Note: The SVI for VLAN 99 will not appear as "up/up" until VLAN 99 is created and there is a device connected to a switch port associated with VLAN 99.

Note: The switch may need to be configured for IPv6. For example, before you can configure IPv6 addressing on a Cisco Catalyst 2960 running IOS version 15.0, you will need to enter the global configuration command **sdm prefer dual-ipv4-and-ipv6 default** and then **reload** the switch.

Task	IOS Commands
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI.	S1(config)# **interface vlan 99**
Configure the management interface IPv4 address.	S1(config-if)# **ip address 172.17.99.11 255.255.255.0**
Configure the management interface IPv6 address	S1(config-if)# **ipv6 address 2001:db8:acad:99::1/64**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

1.1 Configure a Switch with Initial Settings
1.1.6 Switch SVI Configuration Example (Cont.)

Step 2: Configure the Default Gateway

- The switch should be configured with a default gateway if it will be managed remotely from networks that are not directly connected.
  - **Note**: Because, it will receive its default gateway information from a router advertisement (RA) message, the switch does not require an IPv6 default gateway.

Task	IOS Commands
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.1**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Step 3: **Verify Configuration**

- The **show ip interface brief** and **show ipv6 interface brief** commands are useful for determining the status of both physical and virtual interfaces. The output shown confirms that interface VLAN 99 has been configured with an IPv4 and IPv6 address.

Note: An IP address applied to the SVI is only for remote management access to the switch; this does not allow the switch to route Layer 3 packets.

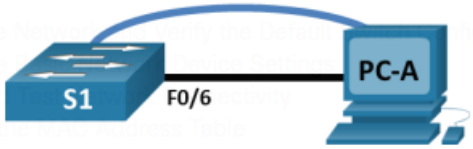
```
S1# show ip interface brief
Interface      IP-Address      OK? Method   Status     Protocol
Vlan99         172.17.99.11    YES manual   down       down
(output omitted)
S1# show ipv6 interface brief
Vlan99                  [down/down]
    FE80::C27B:BCFF:FEC4:A9C1
    2001:DB8:ACAD:99::1
(output omitted)
```

TOPIC 1.1: Configure a Switch with Initial Settings
Packet Tracer Activity 1.1.7 – Basic Switch Configuration

In this laboratory activity 1.1.7, you will complete the following objectives:

- Part 1: Cable the Network and Verify the Default Switch Configuration
- Part 2: Configure Basic Network Device Settings
- Part 3: Verify and Test Network Connectivity
- Part 4: Manage the MAC Address Table

Topology



Addressing Table

Device	Interface	IP Address / Prefix
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad::2 /64
		fe80::2
PC-A	NIC	192.168.1.10 /24
		2001:db8:acad:3 /64
		fe80::3

Required Resources

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Windows with terminal emulation program, such as Tera Term)
- 1 Console cable to configure the Cisco IOS device via the console port
- 1 Ethernet cable as shown in the topology

Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure Basic Network Device Settings

- Configure basic switch settings.
- Configure the PC IP address.

Part 3: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capabilities with Telnet.

Part 4: Manage the MAC Address Table

- Record the MAC address of the host.
- Determine the MAC addresses that the switch has learned.
- List the **show mac address-table** command options.
- Set up a static MAC address.

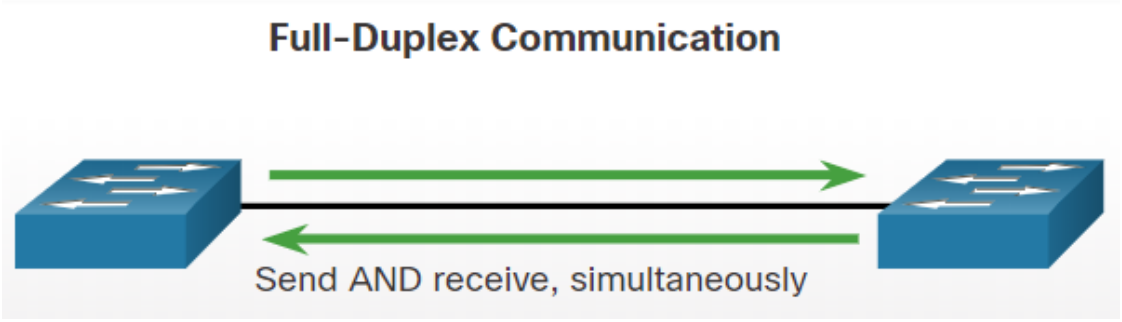
Reflection Questions

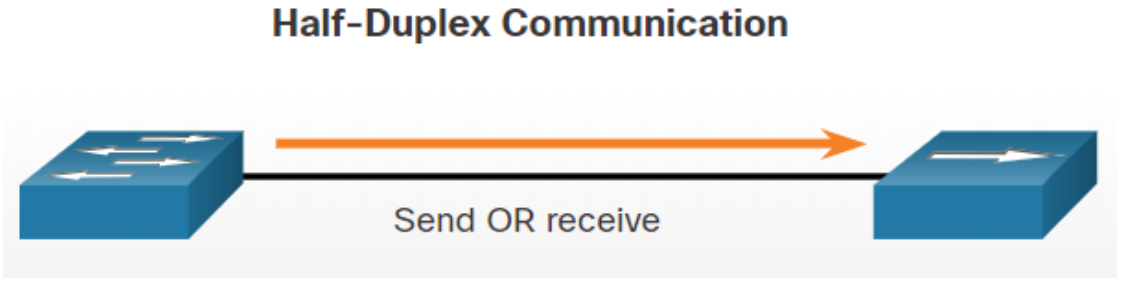
1. Why should you configure the vty password for the switch?
2. Why change the default VLAN 1 to a different VLAN number?
3. How can you prevent passwords from being sent in plain text?
4. Why configure a static MAC address on a port interface?

NOTE: You need to install the latest packet tracer 7.3 simulation to run this packet tracer activity and you need to log in your **NETACAD Account** before doing the PT activity. Please refer to the reading resources and packet tracer resources.

TOPIC 1.2: Configure Switch Ports
1.2.1 Duplex Communication

- Full-duplex communication increases bandwidth efficiency by allowing both ends of a connection to transmit and receive data simultaneously. This is also known as bidirectional communication and it requires microsegmentation.
- A microsegmented LAN is created when a switch port has only one device connected and is operating in full-duplex mode. There is no collision domain associated with a switch port operating in full-duplex mode.
- Unlike full-duplex communication, half-duplex communication is unidirectional. Half-duplex communication creates performance issues because data can flow in only one direction at a time, often resulting in collisions.
- Gigabit Ethernet and 10 Gb NICs require full-duplex connections to operate. In full-duplex mode, the collision detection circuit on the NIC is disabled. Full-duplex offers 100 percent efficiency in both directions (transmitting and receiving). This results in a doubling of the potential use

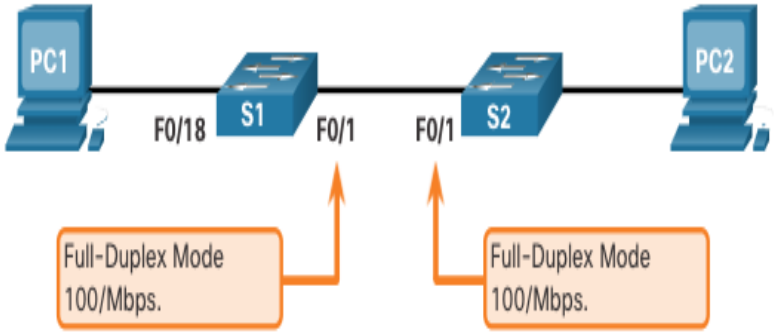




1.2 Configure Switch Ports
1.2.2 Configure Switch Ports at the Physical Layer

- Switch ports can be manually configured with specific duplex and speed settings. The respective interface configuration commands are **duplex** and **speed**.
- The default setting for both duplex and speed for switch ports on Cisco Catalyst 2960 and 3560 switches is auto. The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps and operate only in full-duplex mode when it is set to 1000 Mbps (1 Gbps).
- Autonegotiation is useful when the speed and duplex settings of the device connecting to the port are unknown or may change. When connecting to known devices such as servers, dedicated workstations, or network devices, a best practice is to manually set the speed and duplex settings.
- When troubleshooting switch port issues, it is important that the duplex and speed settings are checked.

Note: Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues. Autonegotiation failure creates



Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface FastEthernet 0/1**
Configure the interface duplex.	S1(config-if)# **duplex full**
Configure the interface speed.	S1(config-if)# **speed 100**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

1.2 Configure Switch Ports
1.2.3 Auto-MDIX

- When automatic medium-dependent interface crossover (auto-MDIX) is enabled, the switch interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.
- When connecting to switches without the auto-MDIX feature, straight-through cables must be used to connect to devices such as servers, workstations, or routers. Crossover cables must be used to connect to other switches or repeaters.
- With auto-MDIX enabled, either type of cable can be used to connect to other devices, and the interface automatically adjusts to communicate successfully.
- On newer Cisco switches, the **mdix auto** interface configuration mode command enables the feature. When using auto-MDIX on an interface, the interface speed and duplex must be set to **auto** so that the feature operates correctly.

```
S1(config-if)# mdix auto
```

Note: The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches but is not available on the older Catalyst 2950 and Catalyst 3550 switches.

To examine the auto-MDIX setting for a specific interface, use the **show controllers ethernet-controller** command with the **phy** keyword. To limit the output to lines referencing auto-MDIX, use the **include Auto-MDIX** filter.

```
S1# show controllers ethernet-controller fa0/1 phy | include MDIX
 Auto-MDIX           :  On    [AdminState=1   Flags=0x00052248]
```

1.2 Configure Switch Ports
1.2.4 Switch Verification Commands

Task	IOS Commands
Display interface status and configuration.	S1# **show interfaces** [*interface-id*]
Display current startup configuration.	S1# **show startup-config**
Display current running configuration.	S1# **show running-config**
Display information about flash file system.	S1# **show flash**
Display system hardware and software status.	S1# **show version**
Display history of command entered.	S1# **show history**
Display IP information about an interface.	S1# **show ip interface** [*interface-id*] OR S1# **show ipv6 interface** [*interface-id*]
Display the MAC address table.	S1# **show mac-address-table** OR S1# **show mac address-table**

1.2 Configure Switch Ports
1.2.5 Verify Switch Port Configuration

The **show running-config** command can be used to verify that the switch has been correctly configured. From the sample abbreviated output on S1, some important information is shown in the figure:

- Fast Ethernet 0/18 interface configured with the management VLAN 99
- VLAN 99 configured with an IPv4 address of 172.17.99.11 255.255.255.0
- Default gateway set to 172.17.99.1

```
S1# show running-config
Building configuration...
Current configuration : 1466 bytes
!
(output omitted)
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 ipv6 address 2001:DB8:ACAD:99::1/64
!
ip default-gateway 172.17.99.1
```

1.2 Configure Switch Ports
1.2.5 Verify Switch Port Configuration (Cont.)

The **show interfaces** command is another commonly used command, which displays status and statistics information on the network interfaces of the switch. The **show interfaces** command is frequently used when configuring and monitoring network devices.

The first line of the output for the **show interfaces fastEthernet 0/18** command indicates that the FastEthernet 0/18 interface is up/up, meaning that it is operational. Further down, the output shows that the duplex is full and the speed is 100 Mbps.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
```

1.2 Configure Switch Ports
1.2.6 Network Access Layer Issues

The output from the **show interfaces** command is useful for detecting common media issues. One of the most important parts of this output is the display of the line and data link protocol status, as shown in the example.

The first parameter (FastEthernet0/18 is up) refers to the hardware layer and indicates whether the interface is receiving a carrier detect signal. The second parameter (line protocol is up) refers to the data link layer and indicates whether the data link layer protocol keepalives are being received. Based on the output of the **show interfaces** command, possible problems can be fixed as follows:

- If the interface is up and the line protocol is down, a problem exists. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.
- If the line protocol and the interface are both down, a cable is not attached, or some other interface problem exists. For example, in a back-to-back connection, the other end of the connection may be administratively down.
- If the interface is administratively down, it has been manually disabled (the **shutdown** command has been issued) in the active configuration.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)MTU 1500 bytes, BW
100000 Kbit/sec, DLY 100 usec,
```

1.2 Configure Switch Ports
1.2.6 Network Access Layer Issues (Cont.)

The **show interfaces** command output displays counters and statistics for the FastEthernet0/18 interface, as shown here:

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2295197 packets input, 305539992 bytes, 0 no buffer
     Received 1925500 broadcasts (74 multicasts)
     0 runs, 0 giants, 0 throttles
     3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 74 multicast, 0 pause input
     0 input packets with dribble condition detected
     3594664 packets output, 436549843 bytes, 0 underruns
     8 output errors, 1790 collisions, 10 interface resets
     0 unknown protocol drops
     0 babbles, 235 late collision, 0 deferred
```

Some media errors are not severe enough to cause the circuit to fail but do cause network performance issues. The table explains some of these common errors which can be detected using the **show interfaces** command.

Error Type	Description
Input Errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1,518 bytes is considered a giant.
CRC	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output Errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	Number of messages retransmitted because of an Ethernet collision.
Late Collisions	A collision that occurs after 512 bits of the frame have been transmitted

1.2 Configure Switch Ports
1.2.7 Interface Input and Output Errors

"Input errors" is the sum of all errors in datagrams that were received on the interface being examined. This includes runts, giants, CRC, no buffer, frame, overrun, and ignored counts. The reported input errors from the **show interfaces** command include the following:

- **Runt Frames** - Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts. Malfunctioning NICs are the usual cause of excessive runt frames, but they can also be caused by collisions.
- **Giants** - Ethernet frames that are larger than the maximum allowed size are called giants.
- **CRC errors** - On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or incorrect cabling. If you see many CRC errors, there is too much noise on the link and you should inspect the cable. You should also search for and eliminate noise sources.

"Output errors" is the sum of all errors that prevented the final transmission of datagrams out the interface that is being examined. The reported output errors from the **show interfaces** command include the following:

- **Collisions** - Collisions in half-duplex operations are normal. However, you should never see collisions on an interface configured for full-duplex communication.
- **Late collisions** - A late collision refers to a collision that occurs after 512 bits of the frame have been transmitted. Excessive cable lengths are the most common cause of late collisions. Another common cause is duplex misconfiguration.

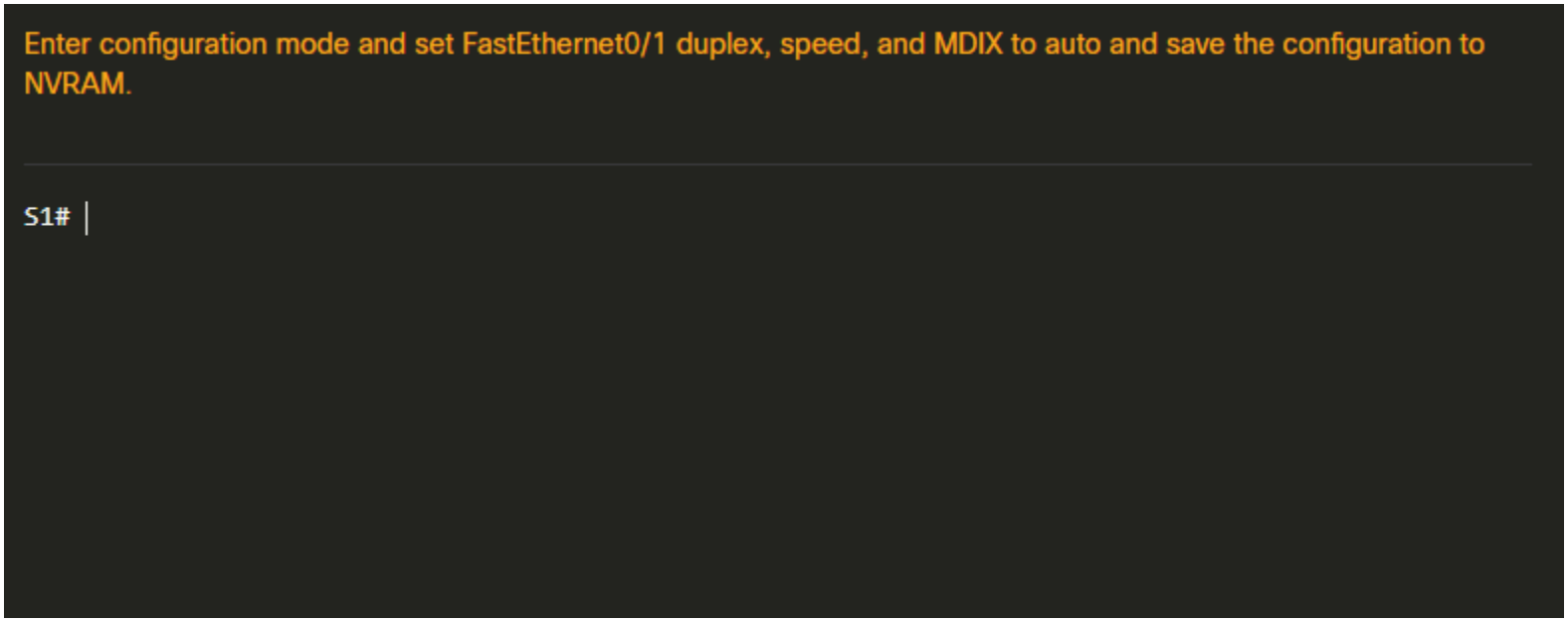
1.2 Configure Switch Ports
1.2.8 Troubleshooting Network Access Layer Issues

To troubleshoot scenarios involving no connection, or a bad connection, between a switch and another device, follow the general process shown in the figure.

TOPIC 1.2: Configure Switch Ports

Written Activity / Syntax Checker 1.2.9 – Configure Switch Port

Configure a switch interface based on the specified requirements. The prompt mut be included before the command.



TOPIC 1.3: Secure Remote Access

1.3 Secure Remote Access
1.3.1 Telnet Operation

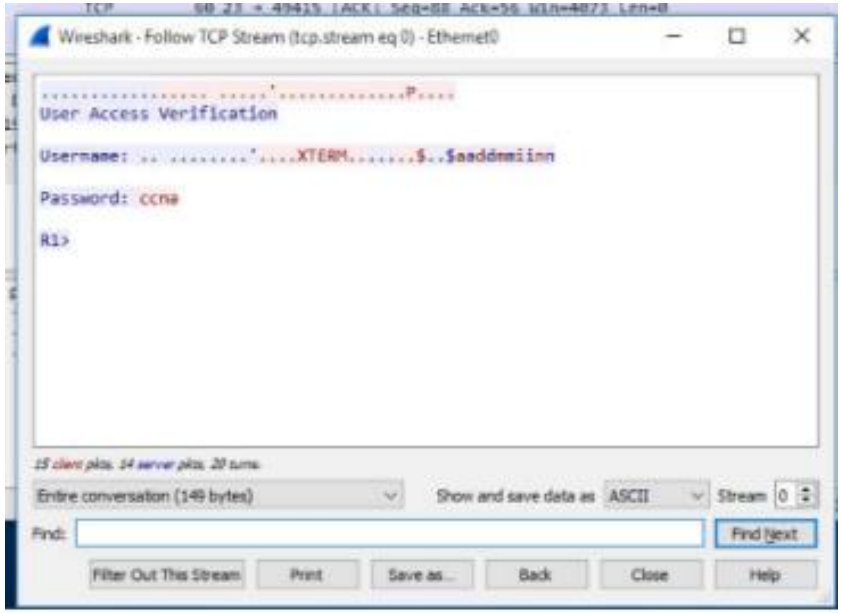
Telnet uses TCP port 23. It is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.

A threat actor can monitor packets using Wireshark. For example, in the figure the threat actor captured the username **admin** and password **ccna** from a Telnet session.

1.3 Secure Remote Access
1.3.2 SSH Operation

Secure Shell (SSH) is a secure protocol that uses TCP port 22. It provides a secure (encrypted) management connection to a remote device. SSH should replace Telnet for management connections. SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices.

The figure shows a Wireshark capture of an SSH session. The threat actor can track the session using the IP address of the administrator device. However, unlike Telnet, with SSH the username and password are encrypted.



1.3 Secure Remote Access
1.3.3 Verify the Switch Supports SSH

To enable SSH on a Catalyst 2960 switch, the switch must be using a version of the IOS software including cryptographic (encrypted) features and capabilities. Use the **show version** command on the switch to see which IOS the switch is currently running. An IOS filename that includes the combination "k9" supports cryptographic (encrypted) features and capabilities. The example shows the output of the **show version** command.

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE SOFTWARE
(fc1)
```

1.3 Secure Remote Access
1.3.4 Configure SSH

Before configuring SSH, the switch must be minimally configured with a unique hostname and the correct network connectivity settings.

Step 1: Verify SSH support - Use the show ip ssh command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

```
S1# show ip ssh
```

Step 2: Configure the IP domain - Configure the IP domain name of the network using the ip domain-name domain-name global configuration mode command.

```
S1(config)# ip domain-name cisco.com
```

Step 3: Generate RSA key pairs - Generating an RSA key pair automatically enables SSH. Use the crypto key generate rsa global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. **Note:** To delete the RSA key pair, use the crypto key zeroize rsa global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

```
S1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
```

Step 4: Configure user authentication - The SSH server can authenticate users locally or using an authentication server. To use the local authentication method, create a username and password pair using the username username secret password global configuration mode command.

```
S1(config)# username admin secret ccna
```

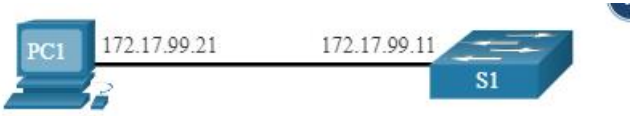
Step 5: Configure the vty lines - Enable the SSH protocol on the vty lines by using the transport input ssh line configuration mode command. Use the line vty global configuration mode command and then the login local line configuration mode command to require local authentication for SSH connections from the local username database.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

Step 6: Enable SSH version 2 - By default, SSH supports both versions 1 and 2. When supporting both versions, this is shown in the show ip ssh output as supporting version 2. Enable SSH version using the ip ssh version 2 global configuration command.

```
S1(config)# ip ssh version 2
```

1.3 Secure Remote Access
1.3.5 Verify SSH is Operational

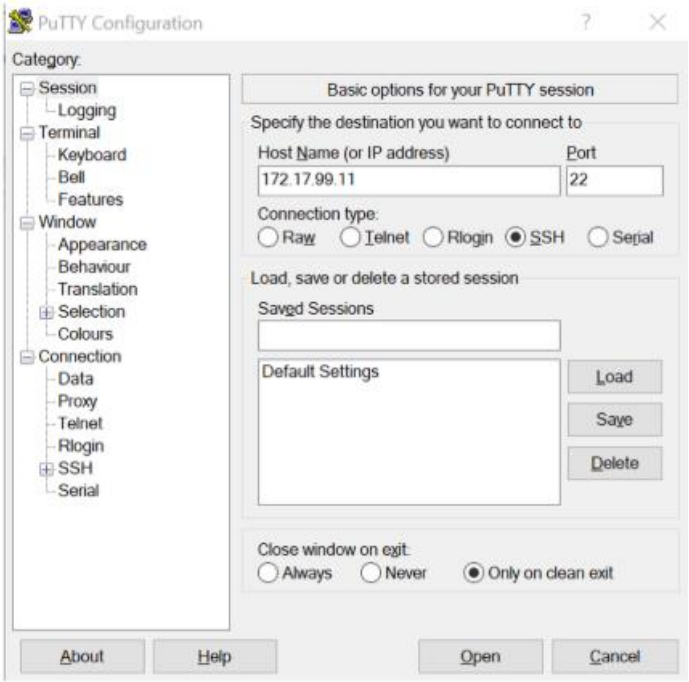


On a PC, an SSH client such as PuTTY, is used to connect to an SSH server. For example, assume the following is configured:

- SSH is enabled on switch S1
- Interface VLAN 99 (SVI) with IPv4 address 172.17.99.11 on switch S1
- PC1 with IPv4 address 172.17.99.21

Using a terminal emulator, initiate an SSH connection to the SVI VLAN IPv4 address of S1 from PC1.

When connected, the user is prompted for a username and password as shown in the example. Using the configuration from the previous example, the username **admin** and password **ccna** are entered. After entering the correct combination, the user is connected via SSH to the command line interface (CLI) on the Catalyst 2960 switch.




```
Login as: admin
Using keyboard-interactive
Authentication.
Password:
S1> enable
Password:
S1#
```

To display the version and configuration data for SSH on the device that you configured as an SSH server, use the **show ip ssh** command. In the example, SSH version 2 is enabled.

```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
To check the SSH connections to the device, use the show ssh command as shown.
S1# show ssh
%No SSHv1 server connections running.
Connection Version Mode Encryption  Hmac         State                 Username
0          2.0   IN   aes256-cbc   hmac-sha1    Session started       admin
0          2.0   OUT  aes256-cbc   hmac-sha1    Session started       admin
S1#
```

TOPIC 1.3: Secure Remote Access

Packet Tracer Activity 1.3.6 – Configure SSH

Packet Tracer - Configure SSH

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objectives

Part 1: Secure Passwords

Part 2: Encrypt Communications

Part 3: Verify SSH Implementation

Background

SSH should replace Telnet for management connections. Telnet uses insecure plain text communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

NOTE: You need to install the latest packet tracer 7.3 simulation to run this packet tracer activity and you need to log in your **NETACAD Account** before doing the PT activity. Please refer to the reading resources and packet tracer resources.

Instructions

Part 1: Secure Passwords

a. Using the command prompt on **PC1**, Telnet to **S1**. The user EXEC and privileged EXEC password is **cisco**.

b. Save the current configuration so that any mistakes you might make can be reversed by toggling the power for **S1**.

c. Show the current configuration and note that the passwords are in plain text. Enter the command that encrypts plain text passwords:

```
S1(config)# service password-encryption
```

d. Verify that the passwords are encrypted.

Part 2: Encrypt Communications

Step 1: Set the IP domain name and generate secure keys.

It is generally not safe to use Telnet, because data is transferred in plain text. Therefore, use SSH whenever it is available.

a. Configure the domain name to be **netacad.pka**.

b. Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

Step 2: Create an SSH user and reconfigure the VTY lines for SSH-only access.

a. Create an **administrator** user with **cisco** as the secret password.

b. Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access. Remove the existing vty line password.

Step 3: Verify SSH Implementation

a. Exit the Telnet session and attempt to log back in using Telnet. The attempt should fail.

b. Attempt to log in using SSH. Type **ssh** and press **Enter** without any parameters to reveal the command usage instructions. **Hint**: The `-l` option is the letter "L", not the number 1.

c. Upon successful login, enter privileged EXEC mode and save the configuration. If you were unable to successfully access **S1**, toggle the power and begin again at Part 1.

TOPIC 1.4: Basic Router Configuration

1.4.1 Configure Basic Router Settings

Cisco routers and Cisco switches have many similarities. They support a similar modal operating system, similar command structures, and many of the same commands. In addition, both devices have similar initial configuration steps. For example, the following configuration tasks should always be performed. Name the device to distinguish it from other routers and configure passwords, as shown in the example.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)#
```

Configure a banner to provide legal notification of unauthorized access, as shown in the example.

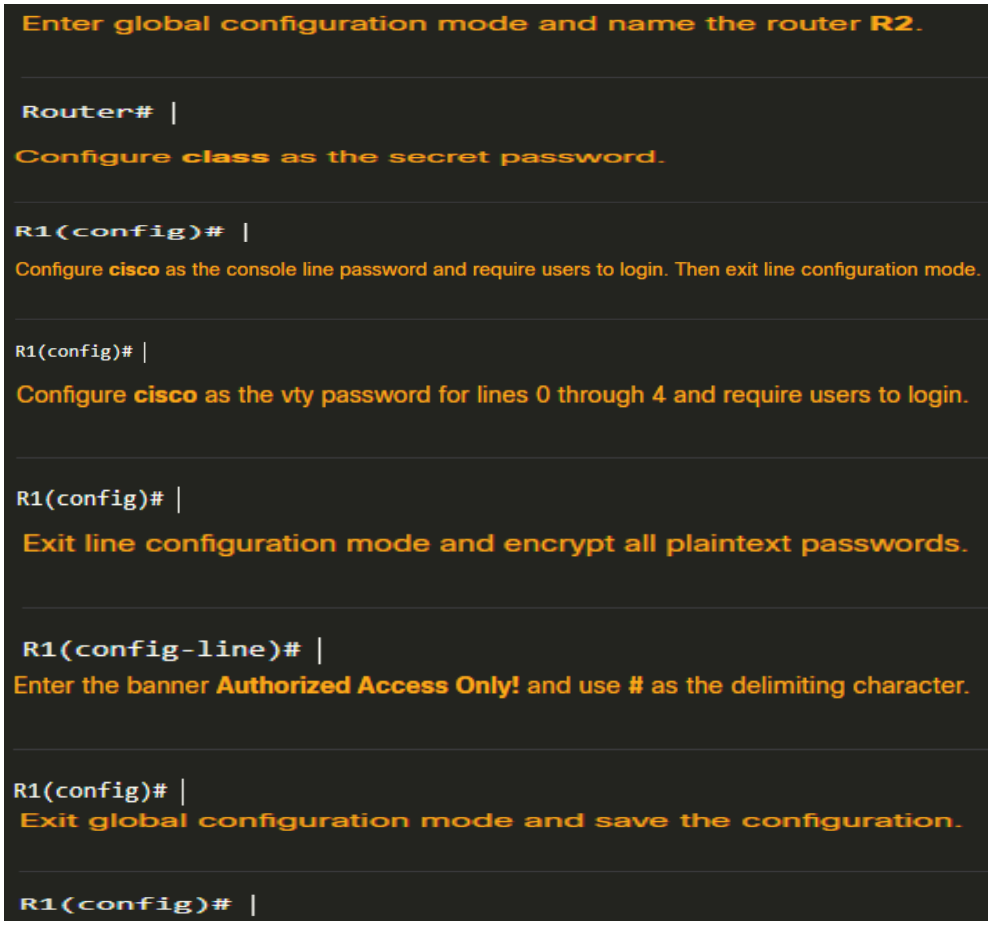
```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

Save the changes on a router, as shown in the example.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

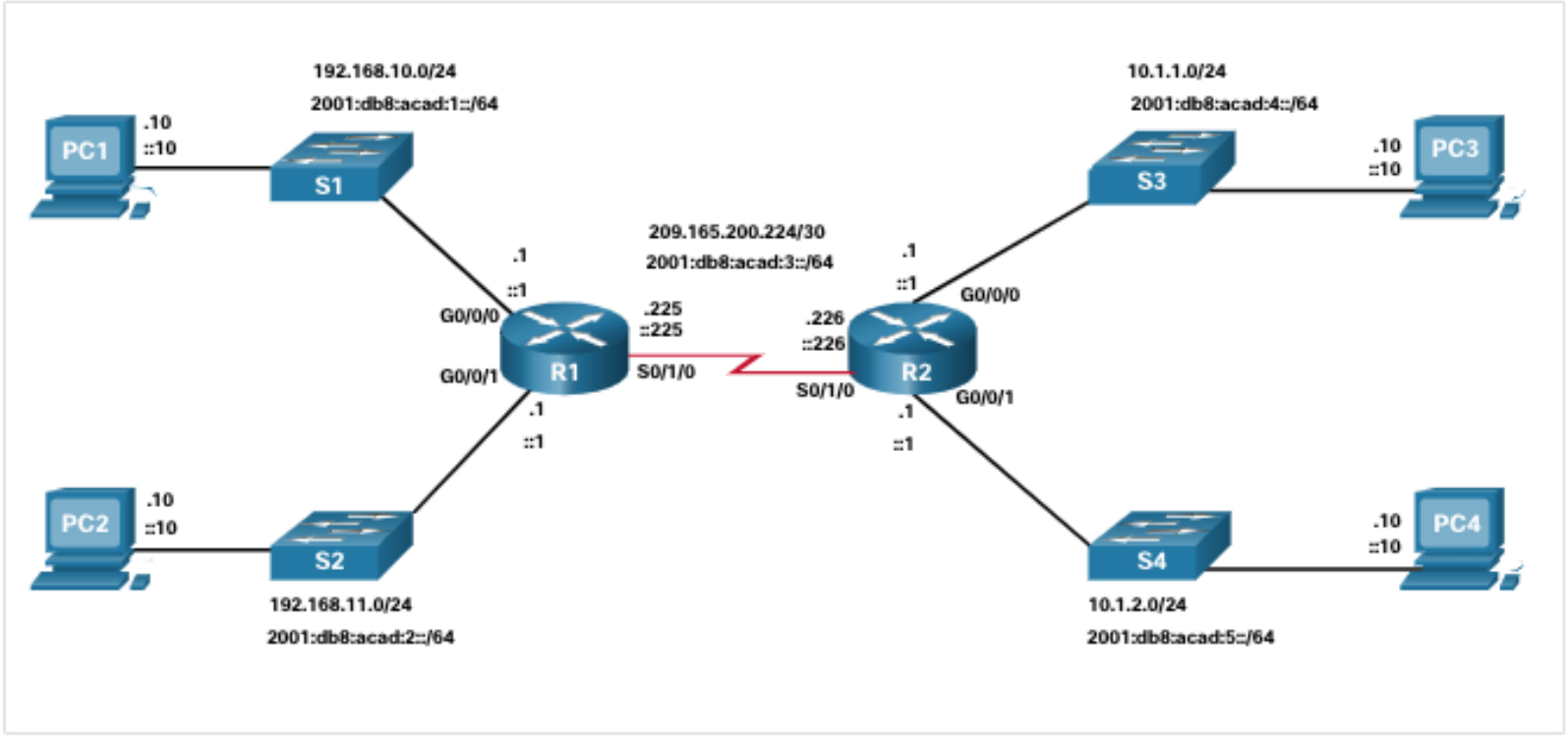
TOPIC 1.4: Basic Router Configuration
Written Activity / Syntax Checker 1.4.2- Configure Basic Router Settings

In this syntax activity, you will configure basic settings for R2.



1.4 Basic Router Configuration
1.4.3 Dual Stack Topology

One distinguishing feature between switches and routers is the type of interfaces supported by each. For example, Layer 2 switches support LANs; therefore, they have multiple FastEthernet or Gigabit Ethernet ports. The dual stack topology in the figure is used to demonstrate the configuration of router IPv4 and IPv6 interfaces.



1.4 Basic Router Configuration
1.4.4 Configure Router Interfaces

Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces. For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and High-Speed WAN Interface Card (HWIC) slots to accommodate other types of network interfaces, including serial, DSL, and cable interfaces.

To be available, an interface must be:

- **Configured with at least one IP address** - Use the **ip address** *ip-address subnet-mask* and the **ipv6 address** *ipv6-address/prefix* interface configuration commands.
- **Activated** - By default, LAN and WAN interfaces are not activated (**shutdown**). To enable an interface, it must be activated using the **no shutdown** command. (This is similar to powering on the interface.) The interface must also be connected to another device (a hub, a switch, or another router) for the physical layer to be active.
- **Description** - Optionally, the interface could also be configured with a short description of up to 240 characters. It is good practice to configure a description on each interface. On production networks, the benefits of interface descriptions are quickly realized as they are helpful in troubleshooting and in identifying a third-party connection and contact information.

The example shows the configure

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Link to LAN 1
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description Link to LAN 2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:acad:3::225/64
R1(config-if)# description Link to R2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

TOPIC 1.4: Basic Router Configuration

Written Activity / Syntax Checker 1.4.5- Configure Basic Router Settings

In this syntax activity, you will configure R2 with its IPv4 and IPv6 interfaces.

Configure GigabitEthernet 0/0/0.

- Use **g0/0/0** to enter interface configuration mode.
- Configure the IPv4 address **10.1.1.1** and subnet mask **255.255.255.0**.
- Configure the IPv6 address **2001:db8:acad:4::1/64**.
- Describe the link as **Link to LAN 3**.
- Activate the interface.

```
Router(config)#
```

Configure GigabitEthernet 0/0/1.

- Use **g0/0/1** to enter interface configuration mode.
- Configure the IPv4 address **10.1.2.1** and subnet mask **255.255.255.0**.
- Configure the IPv6 address **2001:db8:acad:5::1/64**.
- Describe the link as **Link to LAN 4**.
- Activate the interface.

```
Router(config-if)#
```

Configure Serial 0/0/0.

- Use **s0/0/0** to enter interface configuration mode.
- Configure the IPv4 address **209.165.200.226** and subnet mask **255.255.255.252**.
- Configure the IPv6 address **2001:db8:acad:3::226/64**.
- Describe the link as **Link to R1**.
- Activate the interface.

```
Router(config-if)#
```

1.4 Basic Router Configuration
1.4.6 IPv4 Loopback Interfaces

Another common configuration of Cisco IOS routers is enabling a loopback interface.

- The loopback interface is a logical interface that is internal to the router. It is not assigned to a physical port and can never be connected to any other device. It is considered a software interface that is automatically placed in an "up" state, as long as the router is functioning.
- The loopback interface is useful in testing and managing a Cisco IOS device because it ensures that at least one interface will always be available. For example, it can be used for testing purposes, such as testing internal routing processes, by emulating networks behind the router.
- Loopback interfaces are also commonly used in lab environments to create additional interfaces. For example, you can create multiple loopback interfaces on a router to simulate more networks for configuration practice and testing purposes. The IPv4 address for each loopback interface must be unique and unused by any other interface. In this curriculum, we often use a loopback interface to simulate a link to the internet.
- Enabling and assigning a loopback address is simple:

```
Router(config)# interface loopback number
Router(config-if)# ip address ip-address subnet-mask
```

Multiple loopback interfaces can be enabled on a router. The IPv4 address for each loopback interface must be unique and unused by any other interface, as shown in the example configuration of loopback interface 0 on R1.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# exit
R1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```

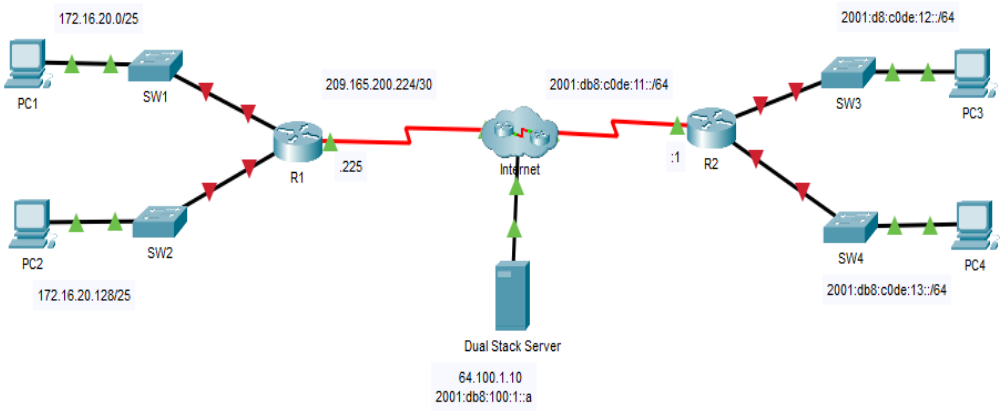
TOPIC 1.4: Basic Router Configuration

Packet Tracer Activity 1.4.7- Configure Basic Router Settings

Packet Tracer - Configure Router Interfaces

Addressing Table

Device	Interface	IP Address/Prefix	Default Gateway
R1	G0/0	172.16.20.1 /25	N/A
	G0/1	172.16.20.129 /25	N/A
	S0/0/0	209.165.200.225 /30	N/A
PC1	NIC	172.16.20.10 /25	172.16.20.1
PC2	NIC	172.16.20.138 /25	172.16.20.129
R2	G0/0	2001:db8:c0de:12::1/64	N/A
	G0/1	2001:db8:c0de:13::1/64	N/A
	S0/0/1	2001:db8:c0de:11::1/64	N/A
		fe80::2	N/A
PC3	NIC	2001:db8:c0de:12::a/64	fe80::2
PC4	NIC	2001:db8:c0de:13::a/64	fe80::2



Objectives

Part 1: Configure IPv4 Addressing and Verify Connectivity

Part 2: Configure IPv6 Addressing and Verify Connectivity

Background

Routers R1 and R2 each have two LANs. Your task is to configure the appropriate addressing on each device and verify connectivity between the LANs.

Note: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

Instructions

Part 1: Configure IPv4 Addressing and Verify Connectivity

Step 1: Assign IPv4 addresses to R1 and LAN devices.

Referring to the **Addressing Table**, configure IP addressing for **R1** LAN interfaces, **PC1** and **PC2**. The serial interface has already configured.

Step 2: Verify connectivity.

PC1 and **PC2** should be able to ping each other and the **Dual Stack Server**.

Part 2: Configure IPv6 Addressing and Verify Connectivity

Step 1: Assign IPv6 addresses to R2 and LAN devices.

Referring to the **Addressing Table**, configure IP addressing for **R2 LAN interfaces**, **PC3** and **PC4**. The serial interface is already configured.

Step 2: Verify connectivity.

PC3 and **PC4** should be able to ping each other and the **Dual Stack Server**.

NOTE: You need to install the latest packet tracer 7.3 simulation to run this packet tracer activity and you need to log in your **NETACAD Account** before doing the PT activity. Please refer to the reading resources and packet tracer resources.

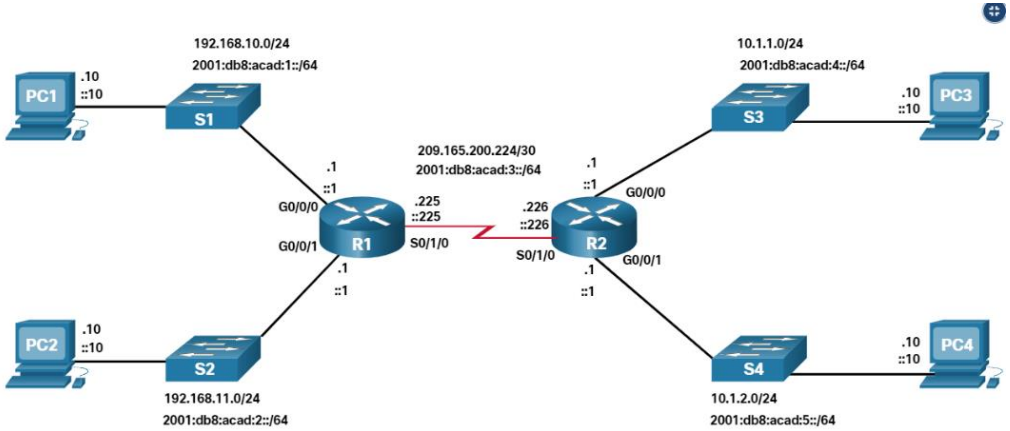
TOPIC 1.5- Verify Directly Connected Networks

1.5 Verify Directly Connected Networks
1.5.1 Interface Verification Commands

There are several **show** commands that can be used to verify the operation and configuration of an interface.

The following commands are especially useful to quickly identify the status of an interface:

- **show ip interface brief** and **show ipv6 interface brief** - These display a summary for all interfaces including the IPv4 or IPv6 address of the interface and current operational status.
- **show running-config interface** *interface-id* - This displays the commands applied to the specified interface.
- **show ip route** and **show ipv6 route** - These display the contents of the IPv4 or IPv6 routing table stored in RAM. In Cisco IOS 15, active interfaces should appear in the routing table with two related entries identified by the code '**C**' (Connected) or '**L**' (Local). In previous IOS versions, only a single entry with the code '**C**' will appear.



1.5 Verify Directly Connected Networks
1.5.2Verify Interface Status

The output of the **show ip interface brief** and **show ipv6 interface brief** commands can be used to quickly reveal the status of all interfaces on the router. You can verify that the interfaces are active and operational as indicated by the Status of "up" and Protocol of "up", as shown in the example. A different output would indicate a problem with either the configuration

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
R1# show ipv6 interface brief
GigabitEthernet0/0/0   [up/up]
    FE80::7279:B3FF:FE92:3130
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1   [up/up]
    FE80::7279:B3FF:FE92:3131
    2001:DB8:ACAD:2::1
Serial0/1/0            [up/up]
    FE80::7279:B3FF:FE92:3130
    2001:DB8:ACAD:3::1
Serial0/1/1            [down/down]     Unassigned
```

1.5 Verify Directly Connected Networks
1.5.3 Verify IPv6 Link Local and Multicast Addresses

The output of the **show ipv6 interface brief** command displays two configured IPv6 addresses per interface. One address is the IPv6 global unicast address that was manually entered. The other address, which begins with FE80, is the link-local unicast address for the interface. A link-local address is automatically added to an interface whenever a global unicast address is assigned. An IPv6 network interface is required to have a link-local address, but not necessarily a global unicast address.

The **show ipv6 interface gigabitethernet 0/0/0 c**ommand displays the interface status and all of the IPv6 addresses belonging to the interface. Along with the link local address and global unicast address, the output includes the multicast addresses assigned to the interface, beginning with prefix FF02, as shown in the example.

```
R1# show ipv6 interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::7279:B3FF:FE92:3130
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF92:3130
  MTU is 1500 bytes
```

1.5 Verify Directly Connected Networks
1.5.4 Verify Interface Configuration

The output of the **show running-config interface** command displays the current commands applied to the specified interface, as shown.

The following two commands are used to gather more detailed interface information:

- **show interfaces**- Displays interface information and packet flow count for all interfaces on the device.
- **show ip interface** and **show ipv6 interface** - Displays the IPv4 and IPv6 related information for all interfaces on a router..

```
R1 show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 158 bytes
!
interface GigabitEthernet0/0/0
 description Link to LAN 1
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:ACAD:1::1/64
end
R1#
```

1.5 Verify Directly Connected Networks
1.5.5 Verify Routes

The output of **show ip route** and **show ipv6 route** commands reveal the three directly connected network entries and the three local host route interface entries, as shown in the example.

The local host route has an administrative distance of 0. It also has a /32 mask for IPv4, and a /128 mask for IPv6. The local host route is for routes on the router that owns the IP address. It is used to allow the router to process packets destined to that IP.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0A
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

A '**C**' next to a route within the routing table indicates that this is a directly connected network. When the router interface is configured with a global unicast address and is in the "up/up" state, the IPv6 prefix and prefix length are added to the IPv6 routing table as a connected route.

The IPv6 global unicast address applied to the interface is also installed in the routing table as a local route. The local route has a /128 prefix. Local routes are used by the routing table to efficiently process packets with the interface address of the router as the destination.

The **ping** command for IPv6 is identical to the command used with IPv4 except that an IPv6 address is used. As shown in the example, the **ping** command is used to verify Layer 3 connectivity between R1 and PC1.

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

1.5 Verify Directly Connected Networks
1.5.6 Filter Show Command Output

Commands that generate multiple screens of output are, by default, paused after 24 lines. At the end of the paused output, the --More-- text displays. Pressing **Enter** displays the next line and pressing the spacebar displays the next set of lines. Use the **terminal length** command to specify the number of lines to be displayed. A value of 0 (zero) prevents the router from pausing between screens of output.

Another very useful feature that improves the user experience in the CLI is the filtering of **show** output. Filtering commands can be used to display specific sections of output. To enable the filtering command, enter a pipe (**|**) character after the **show** command and then enter a filtering parameter and a filtering expression.

There are four filtering parameters that can be configured after the pipe:

- section - Shows the entire section that starts with the filtering expression.
- include - Includes all output lines that match the filtering expression.
- exclude - Excludes all output lines that match the filtering expression.
- begin - Shows all the output lines from a certain point, starting with the line that matches the filtering expression

```
R1# show running-config | section line vty
line vty 0 4
 password 7 110A1016141D
 login
 transport input all
```

```
R1# show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
```

```
R1# show ip interface brief | include up
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
```

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0
```

TOPIC 1.5: Verify Directly Connected Networks
Written Activity / Syntax Checker 1.5.7- Filter Show Command Output

In this Syntax Checker activity, you will filter output for show commands.

Enter the command to filter the show running-config output for the 'line con' section.

```
R1#
```

Enter the command to filter for 'down' interfaces in the brief listing.

```
R1#
```

Enter the command to exclude 'up' interfaces in the brief listing.

```
R1#
```

Enter the command to filter the show running-config output to begin at the word 'line'.

```
R1#
```

1.5 Verify Directly Connected Networks
1.5.8 Command History Feature

The command history feature is useful because it temporarily stores the list of executed commands to be recalled.

- To recall commands in the history buffer, press **Ctrl**+**P** or the **Up Arrow** key. The command output begins with the most recent command. Repeat the key sequence to recall successively older commands. To return to more recent commands in the history buffer, press **Ctrl**+**N** or the **Down Arrow** key. Repeat the key sequence to recall successively more recent commands.
- By default, command history is enabled and the system captures the last 10 command lines in its history buffer. Use the **show history** privileged EXEC command to display the contents of the buffer.
- It is also practical to increase the number of command lines that the history buffer records during the current terminal session only. Use the **terminal history size** user EXEC command to increase or decrease the size of the buffer.

An example of the **terminal history size** and **show history** commands is shown in the figure.

```
R1# terminal history size 200
R1# show history
  show ip int brief
  show interface g0/0/0
  show ip route
  show running-config
  show history
  terminal history size 200
```

TOPIC 1.5: Verify Directly Connected Networks
Written Activity / Syntax Checker 1.5.9- Command History Feature

In this Syntax Checker activity, you will use the command history feature.

Enter the command to set the number of lines in command history to 200.

```
R1>
```

Enter the command to display command history.

```
R1>
```

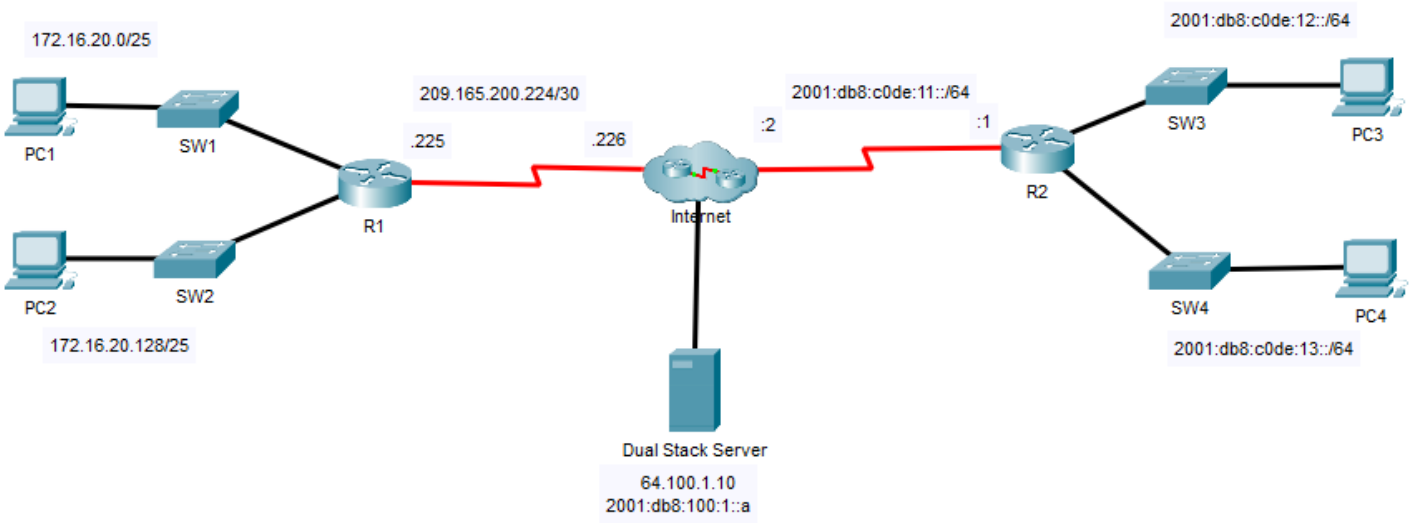
TOPIC 1.5: Verify Directly Connected Networks

Packet Tracer Activity 1.5.10- Verify Directly Connected Networks

Packet Tracer - Verify Directly Connected Networks

Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	172.16.20.1/25	N/A
	G0/0/1	172.16.20.129/25	N/A
	S0/1/0	209.165.200.225/30	N/A
PC1	NIC	172.16.20.10/25	172.16.20.1
PC2	NIC	172.16.20.138/25	172.16.20.129
R2	G0/0/0	2001:db8:c0de:12::1/64	N/A
	G0/0/1	2001:db8:c0de:13::1/64	N/A
	S0/1/1	2001:db8:c0de:11::1/64	N/A
		fe80::2	N/A
PC3	NIC	2001:db8:c0de:12::a/64	fe80::2
PC4	NIC	2001:db8:c0de:13::a/64	fe80::2



TOPIC 1.5: Verify Directly Connected Networks
Packet Tracer Activity 1.5.10- Verify Directly Connected Networks

Objectives

- Verify IPv4 Directly Connected Networks
- Verify IPv6 Directly Connected Networks
- Troubleshoot connectivity issues.

Background

Routers R1 and R2 each have two LANs. Your task is to verify the addressing on each device and verify connectivity between the LANs.

Note: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

Instructions

Part 1: Verify IPv4 Directly Connected Networks

Step 1: Verify IPv4 addresses and port status on R1.

a. Check the status of the configured interfaces by filtering the output.

```
R1# show ip interface brief | exclude unassigned
```

b. Based on the output, correct any port status problems that you see.

c. Refer to the **Addressing Table** and verify the IP addresses configured on R1. Make any corrections to addressing if necessary.

d. Display the routing table by filtering to start the output at the word **Gateway**.

Note: Terms that are used to filter output can be shortened to match text as long as the match is unique. For example, Gateway, Gate, and Ga will have the same effect. G will not Filtering is case-sensitive

```
R1# show ip route | begin Gate
```

What is the Gateway of last resort address?

f. Display specific interface information for G0/0/0 by filtering for **duplex**.

What is the duplex setting, speed, and media type?

Step 2: Verify connectivity.

PC1 and **PC2** should be able to ping each other and the **Dual Stack Server**. If not, verify the status of the interfaces and the IP address assignments.

Part 2: Verify IPv6 Directly Connected Networks

Step 1: Verify IPv6 addresses and port status on R2.

a. Check the status of the configured interfaces.

```
R2# show ipv6 int brief
```

What is the status of the configured interfaces?

b. Refer to the **Addressing Table** and make any corrections to addressing as necessary.

Note: When changing an IPv6 address it is necessary to remove the incorrect address since an interface is capable of supporting multiple IPv6 networks.

```
R2(config)# int g0/0/1
R2(config-if)# no ipv6 address 2001:db8:c0de:14::1/64
```

Configure the correct address on the interface.

c. Display the IPv6 routing table.

Note: Filtering commands do not presently work with the IPv6 commands.

d. Display all IPv6 addressing configured on interfaces by filtering the output of the **running-config**.

Filter the output on **R2** for **ipv6** or **interface**.

```
R2# sh run | include ipv6|interface
```

How many addresses are configured on each Gigabit interface?

Step 2: Verify connectivity.

PC3 and **PC4** should be able to ping each other and the **Dual Stack Server**. If not, verify the interface status and IPv6 address assignments.

NOTE: You need to install the latest packet tracer 7.3 simulation to run this packet tracer activity and you need to log in your **NETACAD Account** before doing the PT activity. Please refer to the reading resources and packet tracer resources.

TOPIC 1.5: Verify Directly Connected Networks
Quiz 1.5- Verify Directly Connected Networks

Check your understanding of verifying directly connected networks by choosing the BEST answer to the following questions.

1. Which command will display a summary of all IPv6-enabled interfaces on a router that includes the IPv6 address and operational status?

- **show ip interface brief**
- **show ipv6 route**
- **show running-config interface**
- **show ipv6 interface brief**

2. When verifying routes, what code is used to identify directly connected routes in the routing table?

- C
- D
- L
- R

3. Which command will display packet flow counts, collisions, and buffer failures on an interface?

- **show interface**
- **show ip interface**
- **show running-config interface**

4. An IPv6-enabled interface is required to have which type of address?

- loopback
- global unicast
- link-local
- static

5. What character is used to enable the filtering of commands?

- pipe |
- comma ,
- colon :
- semi colon ;

6. Which filtering expression will show all output lines starting from the line matching the filtering expression?

- section
- begin
- include

MODULE 1: BASIC DEVICE CONFIGURATION
Packet Tracer Activity 1.6.1 – Implement a Small Network

Packet Tracer - Implement a Small Network

Addressing Table

Device	Interface	Address	Subnet Mask	Default Gateway
RTA	G0/0	10.10.10.1	255.255.255.0	N/A
	G0/1	10.10.20.1	255.255.255.0	N/A
SW1	VLAN1	10.10.10.2	255.255.255.0	
SW2	VLAN1	10.10.20.2	255.255.255.0	
PC-1	NIC		255.255.255.0	
PC-2	NIC		255.255.255.0	

Objectives

Part 1: Create the Network Topology

Part 2: Configure Devices and Verify Connectivity

Instructions

Part 1: Create the Network Topology

Step 1: Obtain the required devices.

a. Click the **Network Devices** icon in the bottom tool bar.
b. Click the router icon in the submenu.
c. Locate the **1941** router icon. Click and drag the icon for the 1941 router into the topology area.
d. Click the switch entry in the submenu.
e. Locate the **2960** switch icon. Click and drag the icon for the 2960 switch into the topology area.
f. Repeat the step above so that there are **two** 2960 switches in the topology area.
g. Click the **End Devices** icon.
h. Locate the PC icon. Drag **two** PCs to the topology area.
i. Arrange the devices into a layout that you can work with by clicking and dragging.

Step 2: Name the devices.

The devices have default names that you will need to change. You will name the devices as shown in the Addressing Table. You are changing the display names of the devices. This is the text label that appears below each device. Your display names must match the information in the Addressing Table **exactly**. If a display name does not match, you will not be scored for your device configuration.

a. Click the device display name that is below the device icon. A text field should appear with a flashing insertion point. If the configuration window for the device appears, close it and try again, clicking a little further away from the device icon.
b. Replace the current display name with the appropriate display name from the Addressing Table.
c. Repeat until all devices are named.

Step 3: Connect the devices.

a. Click the orange lightning bolt connections icon in the bottom toolbar.
b. Locate the Copper Straight-Through cable icon. It looks like a solid black diagonal line.
c. To connect the device, click the Copper Straight-Through cable icon and then click the first device that you want to connect. Select the correct port and then click the second device. Select the correct port and the devices will be connected.
d. Connect the devices as specified in the table below.

From Device	Port	To Device	Port
RTA	G0/0	SW1	G0/1
	G0/1	SW2	G0/1
SW1	F0/1	PC-1	Fastethernet0
SW2	F0/1	PC-2	Fastethernet0

NOTE: You need to install the latest packet tracer 7.3 simulation to run this packet tracer activity and you need to log in your **NETACAD Account** before doing the PT activity. Please refer to the reading resources and packet tracer resources.

MODULE 1: BASIC DEVICE CONFIGURATION
Packet Tracer Activity 1.6.1 – Implement a Small Network

Part 2: Configure Devices

Record the PC addressing and gateway addresses in the addressing table. You can use any available address in the network for PC-1 and PC-2.

Step 1: Configure the router.

a. Configure basic settings.
   1) Hostname as shown in the Addressing Table.
   2) Configure **Ciscoenpa55** as the encrypted password.
   3) Configure **Ciscolinepa55** as the password on the lines.
   4) All lines should accept connections.
   5) Configure an appropriate message of the day banner.

b. Configure interface settings.
   1) Addressing.
   2) Descriptions on the interfaces.
   3) Save your configuration.

Step 2: Configure switch SW1 and SW2.

a. Configure the default management interface so that it will accept connections over the network from local and remote hosts. Use the values in the addressing table.

b. Configure an encrypted password using the value in step 1a above.

c. Configure all lines to accept connections using the password from step 1a above.

d. Configure the switches so that they can send data to hosts on remote networks.

e. Save your configuration.

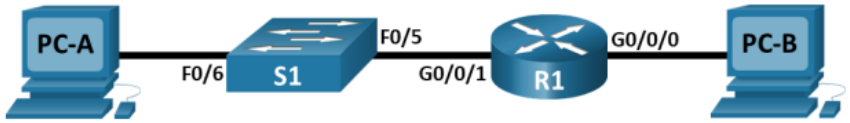
Step 3: Configure the hosts.

Configure addressing on the hosts. If your configurations are complete, you should be able to ping all devices in the topology.

MODULE 1: BASIC DEVICE CONFIGURATION
Packet Tracer Activity 1.6.2 – Configure Basic Router Settings

Lab - Configure Basic Router Settings

Topology



Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	192.168.0.1 /24	N/A
		2001:db8:acad::1 /64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	
		2001:db8:acad:1::1 /64	
		fe80::1	
	Loopback0	10.0.0.1 /24	
		2001:db8:acad:2::1 /64	
		fe80::1	
PC-A	NIC	192.168.1.10 /24	192.168.1.1
		2001:db8:acad:1::10 /64	fe80::1
PC-B	NIC	192.168.0.10 /24	192.168.0.1
		2001:db8:acad::10 /64	fe80::1

Objectives

Part 1: Set Up the Topology and Initialize Devices

- Cable equipment to match the network topology.
- Initialize and restart the router and switch.

Part 2: Configure Devices and Verify Connectivity

- Assign static IPv4 and IPv6 information to the PC interfaces.
- Configure basic router settings.
- Configure the router for SSH.
- Verify network connectivity.

Part 3: Display Router Information

- Retrieve hardware and software information from the router.
- Interpret the output from the startup configuration.
- Interpret the output from the routing table.
- Verify the status of the interfaces.

NOTE: You need to install the latest packet tracer 7.3 simulation to run this packet tracer activity and you need to log in your **NETACAD Account** before doing the PT activity. Please refer to the reading resources and packet tracer resources.

MODULE 1: BASIC DEVICE CONFIGURATION
Packet Tracer Activity 1.6.2 – Configure Basic Router Settings

Background / Scenario

This is a comprehensive lab to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and interface settings on the router.

In Part 3, you will use SSH to connect to the router remotely and utilize the IOS commands to retrieve information from the device to answer questions about the router.

For review purposes, this lab provides the commands necessary for specific router configurations.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the router and switch have been erased and have no startup configurations. Consult with your instructor for the procedure to initialize and reload a router and switch.

Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 4221 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Instructions

Part 1: Set Up the Topology and Initialize Devices

Step 1: Cable the network as shown in the topology.

a. Attach the devices as shown in the topology diagram, and cable as necessary.

b. Power on all the devices in the topology.

Step 2: Initialize and reload the router and switch.

Part 2: Configure Devices and Verify Connectivity

Step 1: Configure the PC interfaces.

a. Configure the IP address, subnet mask, and default gateway settings on PC-A.

b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: Configure the router.

a. Console into the router and enable privileged EXEC mode.

b. Enter configuration mode.

c. Assign a device name to the router.

d. Set the router's domain name as ccna-lab.com.

e. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

f. Encrypt the plaintext passwords.

g. Configure the system to require a minimum 12-character password.

h. Configure the username **SSHadmin** with an encrypted password of **55Hadm!n2020**.

i. Generate a set of crypto keys with a 1024 bit modulus

j. Assign the privileged EXEC password to **$cisco!PRIV***

k. Assign **$cisco!!CON*** as the console password, configure sessions to disconnect after four minutes of inactivity, and enable login.

l. Assign **$cisco!!VTY*** as the vty password, configure the vty lines to accept SSH connections only, configure sessions to disconnect after four minutes of inactivity, and enable login using the local database.

m. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

n. Enable IPv6 Routing

o. Configure all three interfaces on the router with the IPv4 and IPv6 addressing information from the addressing table above. Configure all three interfaces with descriptions. Activate all three interfaces.

p. The router should not allow vty logins for two minutes if three failed login attempts occur within 60 seconds.

q. Set the clock on the router.

r. Save the running configuration to the startup configuration file.

What would be the result of reloading the router prior to completing the **copy running-config startup-config** command?

Step 3: Verify network connectivity.

a. Using the command line at PC-A, ping the IPv4 and IPv6 addresses for PC-B.

Note: It may be necessary to disable the PCs firewall.

Were the pings successful?

MODULE 1: BASIC DEVICE CONFIGURATION
Packet Tracer Activity 1.6.2 – Configure Basic Router Settings

b. Remotely access R1 from PC-A using the Tera Term SSH client.

Using Tera Term on PC-A, open an SSH session to the R1 Loopback interface IPv4 address. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router. Log in as **SSHadmin** with the password **55Hadm!n2020**.

Was remote access successful?

Using Tera Term on PC-A, open an SSH session to the R1 Loopback interface IPv6 address. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router. Log in as **SSHadmin** with the password **55Hadm!n2020**. **Note**: The IPv6 address should be surrounded with square brackets, i.e. [*IPv6 address*]

Was remote access successful?

Why is the Telnet protocol considered to be a security risk?

Part 3: Display Router Information

In Part 3, you will use **show** commands from an SSH session to retrieve information from the router.

Step 1: Establish an SSH session to R1.

Using Tera Term on PC-B, open an SSH session to the R1 Loopback interface IPv6 address and log in as **SSHadmin** with the password **55Hadm!n2020**.

Step 2: Retrieve important hardware and software information.

a. Use the **show version** command to answer questions about the router.

What is the name of the IOS image that the router is running?

How much non-volatile random-access memory (NVRAM) does the router have?

How much Flash memory does the router have?

b. The **show** commands often provide multiple screens of outputs. Filtering the output allows a user to display certain sections of the output. To enable the filtering command, enter a pipe (|) character after a **show** command, followed by a filtering parameter and a filtering expression. You can match the output to the filtering statement by using the **include** keyword to display all lines from the output that contain the filtering expression. Filter the **show version** command, using **show version | include register** to answer the following question.

What is the boot process for the router on the next reload?

Step 3: Display the startup configuration.

Use the **show startup-config** command on the router to answer the following questions.

How are passwords presented in the output?

Use the **show startup-config | section vty** command.

What is the result of using this command?

Step 4: Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions.

What code is used in the routing table to indicate a directly connected network?

How many route entries are coded with a C code in the routing table?

Step 5: Display a summary list of the interfaces on the router.

a. Use the **show ip interface brief** command on the router to answer the following question.

What command changed the status of the Gigabit Ethernet ports from administratively down to up?

b. Use the **show ipv6 int brief** command to verify IPv6 settings on R1.

What is the meaning of the [up/up] part of the output?

c. On PC-B, change its configuration so that it no longer has a static IPv6 address. You may have to reboot the machine. Then, issue the **ipconfig** command on PC-B to examine the IPv6 configuration.

What is the IPv6 address assigned to PC-B?

What is the default gateway assigned to PC-B?

Issue a ping from PC-B to the R1 default gateway link local address. Was it successful?

Issue a ping from PC-B to the R1 IPv6 unicast address 2001:db8:acad::1. Was it successful?

MODULE 1: BASIC DEVICE CONFIGURATION
Packet Tracer 1.6.2 Activity – Configure Basic Router Settings

Reflection Questions

1. In researching a network connectivity issue, a technician suspects that an interface was not enabled. What **show** command could the technician use to troubleshoot this issue?

2. In researching a network connectivity issue, a technician suspects that an interface was assigned an incorrect subnet mask. What **show** command could the technician use to troubleshoot this issue?

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

MODULE 1: BASIC DEVICE CONFIGURATION
1.6.3 What Did I Learn in This Module?

Configure a Switch with Initial Settings

- After a Cisco switch is powered on, it goes through a five-step boot sequence.
- The BOOT environment variable is set using the **boot system** global configuration mode command.
- The IOS is located in a distinct folder and the folder path is specified.
- Use the switch LEDs to monitor switch activity and performance: SYST, RPS, STAT, DUPLX, SPEED, and PoE.
- The boot loader provides access into the switch if the operating system cannot be used because of missing or damaged system files.
- The boot loader has a command line that provides access to the files stored in flash memory.
- To prepare a switch for remote management access, the switch must be configured with an IP address and a subnet mask.
- To manage the switch from a remote network, the switch must be configured with a default gateway.
- To configure the switch SVI, you must first configure the management interface, then configure the default gateway, and finally, verify your configuration.

Configure Switch Ports

- Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously.
- Half-duplex communication is unidirectional. Switch ports can be manually configured with specific duplex and speed settings.
- Use autonegotiation when the speed and duplex settings of the device connecting to the port are unknown or may change.
- When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.
- There are several **show** commands to use when verifying switch configurations.
- Use the **show running-config** command and the **show interfaces** command to verify a switch port configuration.
- The output from the **show interfaces** command is also useful for detecting common network access layer issues because it displays the line and data link protocol status.
- The reported input errors from the **show interfaces** command include: runt frames, giants, CRC errors, along with collisions and late collisions.
- Use **show interfaces** to determine if your network has no connection or a bad connection between a switch and another device.

MODULE 1: BASIC DEVICE CONFIGURATION
1.6.3 What Did I Learn in This Module?

Secure Remote Access

- Telnet (using TCP port 23) is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.
- SSH (using TCP port 22) is a secure protocol that provides an encrypted management connection to a remote device.
- SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices.
- Use the **show version** command on the switch to see which IOS the switch is currently running.
- An IOS filename that includes the combination "k9" supports cryptographic features and capabilities.
- To configure SSH you must verify that the switch supports it, configure the IP domain, generate RSA key pairs, configure use authentication, configure the VTY lines, and enable SSH version 2.
- To verify that SSH is operational, use the **show ip ssh** command to display the version and configuration data for SSH on the device.

Basic Router Configuration

- The following initial configuration tasks should always be performed: name the device to distinguish it from other routers and configure passwords, configure a banner to provide legal notification of unauthorized access, and save the changes on a router.
- One distinguishing feature between switches and routers is the type of interfaces supported by each.
- For example, Layer 2 switches support LANs and, therefore, have multiple FastEthernet or Gigabit Ethernet ports.
- The dual stack topology is used to demonstrate the configuration of router IPv4 and IPv6 interfaces.
- Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces.
- For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and High-Speed WAN Interface Card (HWIC) slots to accommodate other types of network interfaces, including serial, DSL, and cable interfaces.
- The IPv4 loopback interface is a logical interface that is internal to the router.
- It is not assigned to a physical port and can never be connected to any other device.

MODULE 1: BASIC DEVICE CONFIGURATION
1.6.3 What Did I Learn in This Module?

Verify Directly Connected Networks

- Use the following commands to quickly identify the status of an interface: **show ip interface brief** and **show ipv6 interface brief** to see summary all interfaces (IPv4 and IPv6 addresses and operational status), **show running-config interface interface-id** to see the commands applied to a specified interface, and **show ip route** and **show ipv6 route** to see the contents of the IPv4 or IPv6 routing table stored in RAM.
- The output of the **show ip interface brief** and **show ipv6 interface brief** commands can be used to quickly reveal the status of all interfaces on the router.
- The **show ipv6 interface gigabitethernet 0/0/0** command displays the interface status and all of the IPv6 addresses belonging to the interface.
- Along with the link local address and global unicast address, the output includes the multicast addresses assigned to the interface.
- The output of the **show running-config interface** command displays the current commands applied to a specified interface.
- The **show interfaces** command displays interface information and packet flow count for all interfaces on the device.
- Verify interface configuration using the **show ip interface** and **show ipv6 interface** commands, which display the IPv4 and IPv6 related information for all interfaces on a router.
- Verify routes using the **show ip route** and **show ipv6 route** commands.
- Filter show command output using the pipe (|) character.
- Use filter expressions: section, include, exclude, and begin.
- By default, command history is enabled, and the system captures the last 10 command lines in its history buffer.
- Use the **show history** privileged EXEC command to display the contents of the buffer.

MODULE 1: BASIC DEVICE CONFIGURATION
1.6.4 MODULE QUIZ

1. Which tasks can be accomplished by using the command history feature? (Choose two.)

- [ ] View a list of commands entered in a previous session.
- [ ] Recall up to 15 command lines by default.
- [ ] Set the command history buffer size.
- [ ] Recall previously entered commands.
- [ ] Save command lines in a log file for future reference.

2. What is the first action in the boot sequence when a switch is powered on?

- ◯ load the default Cisco IOS software
- ◯ load boot loader software
- ◯ low-level CPU initialization
- ◯ load a power-on self-test program

3. What must an administrator have in order to reset a lost password on a router?

- ◯ a TFTP server
- ◯ a crossover cable
- ◯ access to another router
- ◯ physical access to the router

4. When configuring a switch for SSH access, what other command that is associated with the **login local** command is required to be entered on the switch?

- ◯ **enable secret** *password*
- ◯ **password** *password*
- ◯ **username** *username* **secret** *secret*
- ◯ **login block-for** *seconds* **attempts** *number* **within***seconds*

5. Which command will provide information about the status of all interfaces including the number of giants, runts, and collisions on the interface?

- ◯ **show interfaces**
- ◯ **show ip interface brief**
- ◯ **show history**
- ◯ **show running-config**

6. Which statement describes the system LED operation on Cisco Catalyst switches?

- ◯ If the LED is blinking green, the system is operating normally.
- ◯ If the LED is amber, the system is not powered on.
- ◯ If the LED is blinking amber, the switch is performing POST.
- ◯ If the LED is amber, the system is receiving power but it is not functioning properly

7. Which prompt is displayed when a network administrator successfully accesses the boot loader on a switch to recover from a system crash?

- ◯ system:
- ◯ system#
- ◯ switch:
- ◯ switch#

8. What type of Ethernet cable would be used to connect one switch to another switch when neither switch supports the auto-MDIX feature?

- ◯ straight-through
- ◯ crossover
- ◯ coaxial
- ◯ rollover

MODULE 1: BASIC DEVICE CONFIGURATION
1.6.4 MODULE QUIZ

9. Which router bootup sequence is correct?

- 1 - perform the POST and load the Cisco IOS software
  2 - locate and load the startup configuration file or enter setup mode
  3 - locate and load the bootstrap program
- 1 - perform the POST and load the bootstrap program
  2 - locate and load the startup configuration file or enter setup mode
  3 - locate and load the Cisco IOS software
- 1 - perform the POST and load the startup configuration file
  2 - locate and load the bootstrap program
  3 - locate and load the Cisco IOS software
- 1 - perform the POST and load the bootstrap program
  2 - locate and load the Cisco IOS software
  3 - locate and load the startup configuration file or enter setup mode

10. What advantage does SSH offer over Telnet?

- encryption
- more connection lines
- connection-oriented services
- username and password authentication

11. A network administrator has configured VLAN 99 as the management VLAN and has configured it with an IP address and subnet mask. The administrator issues the **show interface vlan 99** command and notices that the line protocol is down. Which action can change the state of the line protocol to up?

- Connect a host to an interface associated with VLAN 99.
- Configure a default gateway.
- Remove all access ports from VLAN 99.
- Configure a transport input method on the vty lines.

12. Which statement describes SVIs?

- An SVI is created automatically for each VLAN on a multilayer switch.
- Creating an SVI automatically creates an associated VLAN.
- A default SVI is created for VLAN 1 for switch administration.
- An SVI can only be created for the management VLAN.

13. An administrator issues the command **confreg 0x2142** at the rommon 1> prompt. What is the effect when this router is rebooted?

- Contents in RAM will be erased.
- Contents in RAM will be ignored.
- Contents in NVRAM will be erased.
- Contents in NVRAM will be ignored.

Reference:

CCNAv7 Switching, Routing and Wireless Essentials
https://www.netacad.com

Contact Information of the Facilitator

Name	:	*Engr. Rochelle Z. Valdulla,LPT*
MS Teams Account (email)	:	*rochelle.valdulla@aics.edu.ph*
Smart Phone Number	:	*09512858859 / 09178469639*