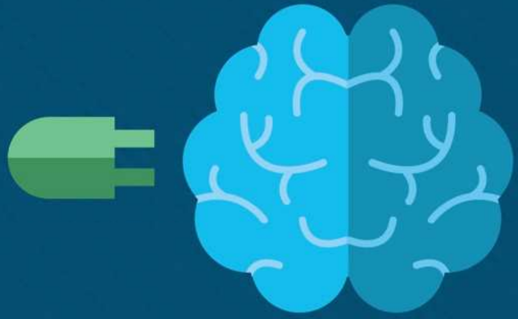


Module 1: Basic Device Configuration

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

Module Objectives

Module Title: Basic Device Configuration

Module Objective: 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.

1.1 Configure a Switch with Initial Settings

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.

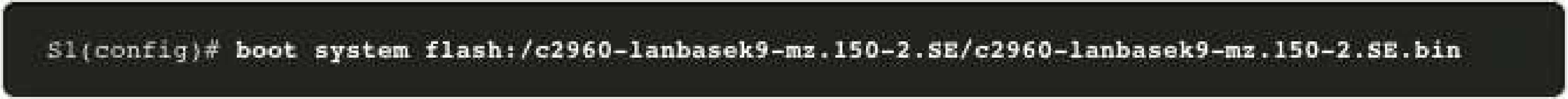
Step 4: The boot loader initializes the flash file system on the system board.

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.

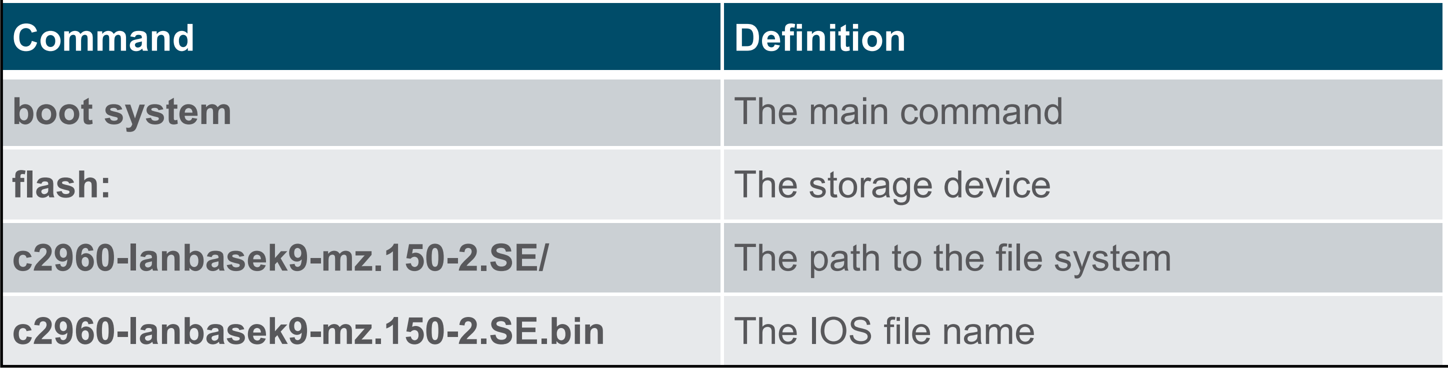
The boot system Command

- 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

Adresář musí být

Kde je operační systém

```
Router#show version | include image
System image file is "flash:c2800nm-adventerprisek9-mz.151-4.M10.bin"
```

Bootovat můžeme od kdekud

```
Router(config)#boot system ?
  WORD   TFTP filename or URL
  flash  Boot from flash memory
  ftp    Boot from a server via ftp
  mop    Boot from a Decnet MOP server
  rcp    Boot from a server via rcp
  rom    Boot from rom
  tftp   Boot from a tftp server
```

Kde hledat bootovací příkazy

```
Router1#show running-config | include ^boot
boot-start-marker
boot system slot0:c3745-ipbasek9-mz.124-6.T.bin
boot system slot0:c3745-ipbasek9-mz.124-7.bin
boot system flash:
boot-end-marker
Router1#
```

Příště hledej v síti

```
Router(config)#config-register 0x210F
```

Přesun IOS z TFTP serveru do flash

```
Router1#copy tftp://172.25.1.1/c2600-ik9o3s-mz.122-12a.bin flash:
Destination filename [c2600-ik9o3s-mz.122-12a.bin]? <enter>
Accessing tftp://172.25.1.1/c2600-ik9o3s-mz.122-12a.bin...
Erase flash: before copying? [confirm] <enter>
Erasing the flash filesystem will remove all files! Continue? [confirm] <enter>
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of flash: complete
Loading c2600-ik9o3s-mz.122-12a.bin from 172.25.1.1 (via FastEthernet0/0.1):
    !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
    !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 11135588 bytes]

Verifying checksum...  OK (0xE643)
11135588 bytes copied in 82.236 secs (135410 bytes/sec)
Router1# reload
Proceed with reload? [confirm]<enter>
```

Bootování IOS image ze sítě přes ROMMON

```
rommon 1 > IP_ADDRESS=192.168.1.1
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=192.168.1.254
rommon 4 > TFTP_SERVER=192.168.1.2
rommon 5 > TFTP_FILE=c2800nm-adventerprisek9-mz.151-4.M12a.bin
rommon 6 > tftpdnld -r
```

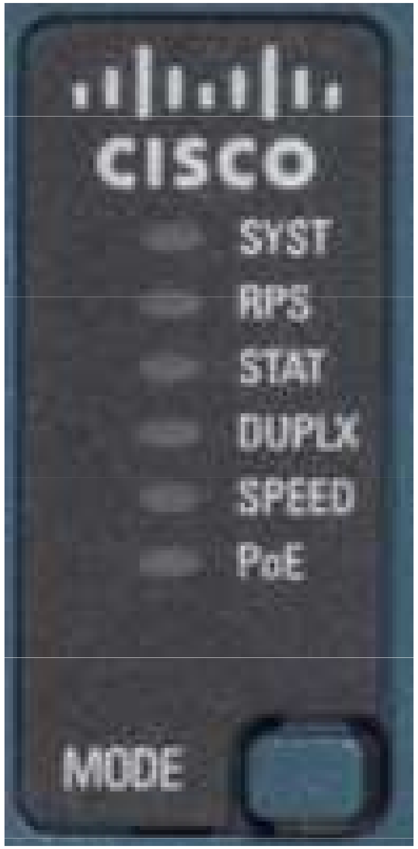
Co dělat když se do paměti nevejdou oba (starý i nový IOS) – starý smažeme

```
Router1#copy tftp://172.25.1.1/c2600-ik9o3s-mz.122-12a.bin flash:
Destination filename [c2600-ik9o3s-mz.122-12a.bin]? <enter>
Accessing tftp://172.25.1.1/c2600-ik9o3s-mz.122-12a.bin...
Erase flash: before copying? [confirm] n
Loading c2600-ik9o3s-mz.122-12a.bin from 172.25.1.1 (via FastEthernet0/0.1): !
%Error copying tftp://172.25.1.1/c2600-ik9o3s-mz.122-12a.bin (Not enough space on device)
Router1#
```

Co dělat, když se nový IOS nevejde do flash

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#boot system tftp c2500-io-l.122-7a.bin 172.25.1.1
Router1(config)#boot system flash
Router1(config)#end
Router1#
```

Switch LED Indicators



System LED (SYST): Shows whether the system is receiving power and functioning properly.
Redundant Power Supply LED (RPS): Shows the RPS status.
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.
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.
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.
Power over Ethernet LED (PoE): Present if the switch supports PoE. Indicates the PoE status of ports on the switch.

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

Switch LED Indicators (Cont.)

	Off	Green	Blinking Green	Amber	Blinking Amber	Alternating Green/Amber
RPS	Off/No RPS	RPS ready	RPS up but not available	RPS standby or fault	Internal PS failed, RPS providing power	N/A
PoE	Not selected, no issues	Selected	N/A	N/A	Not selected, port issues present	N/A
When the named mode is selected, the light associated with each physical port indicates:						
STAT	No link or shutdown	Link Up	Activity	Port blocked preventing loop	Port blocked preventing loop	Link fault
DUPLEX	Half-duplex	Full-duplex	N/A	N/A	N/A	N/A
SPEED	10Mbps	100Mbps	1000Mbps	N/A	N/A	N/A
PoE	PoE off	PoE on	N/A	PoE disabled	PoE off due to fault	PoE denied (over budget)

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.

Tradiční Password Recovery

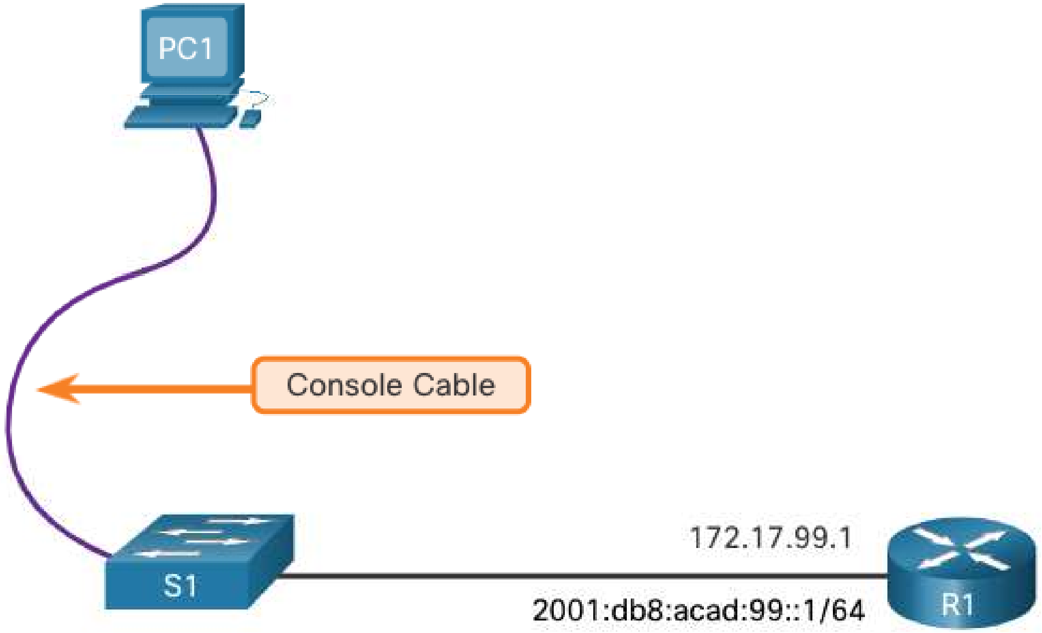
- Vypnout a zapnout switch/router.
- Do jedné minuty zmáčkni Break a zařízení přejde do ROMmon (záleží na typu zařízení).
- **rommon 1> confreg 0x2142** a začne bootování z flashe. Obejde se tím starovací sekvence.
- **rommon 2> reset**
- **hostname(config)#enable secret cisco**
- **no shutdown** na použitá rozhraní
- **hostname(config)#config-register 0x2102**
- **write memory** nebo **copy running-config startup-config**

Configure a Switch with Initial Settings

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.



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.

Switch SVI Configuration Example (Cont.)

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**

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.

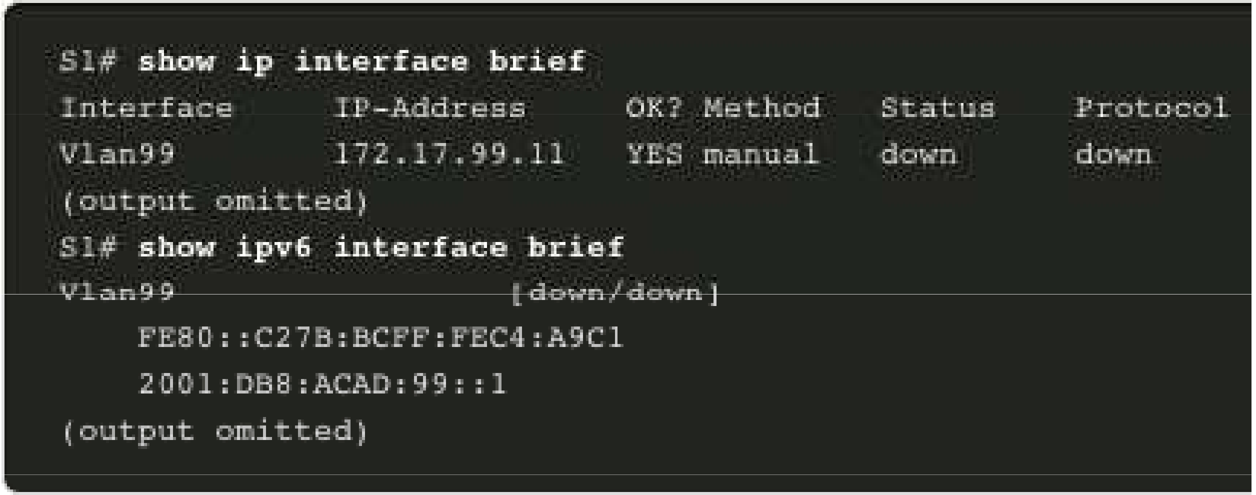
Task	IOS Commands
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.1**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config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

Switch SVI Configuration Example (Cont.)

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)
```

Lab – Basic Switch Configuration

In this lab, 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

1.2 Configure Switch Ports

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 of the stated bandwidth.

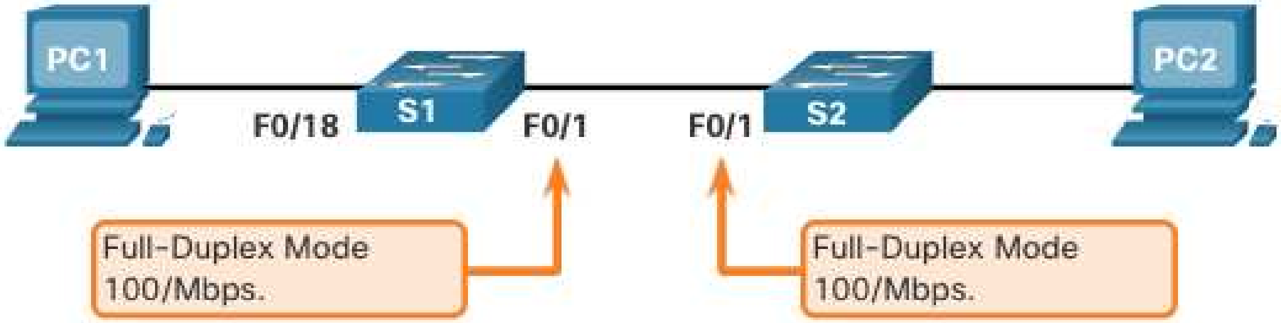
Configure Switch Ports at the Physical Layer

- 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 mismatched settings.

All fiber-optic ports, such as 1000BASE-SX ports, operate only at one preset speed and are always full-duplex

Configure Switch Ports at the Physical Layer (Cont.)



Full-Duplex Mode 100/Mbps.

Full-Duplex Mode 100/Mbps.

Task	IOS Commands
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**

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.

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.

Switch Verification Commands

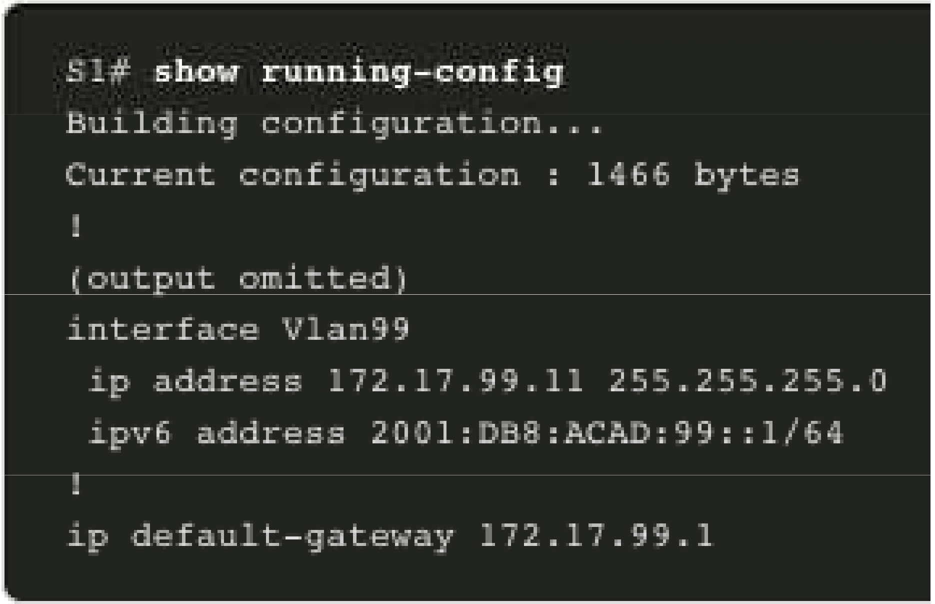
Máme rádi show ☺

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**

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

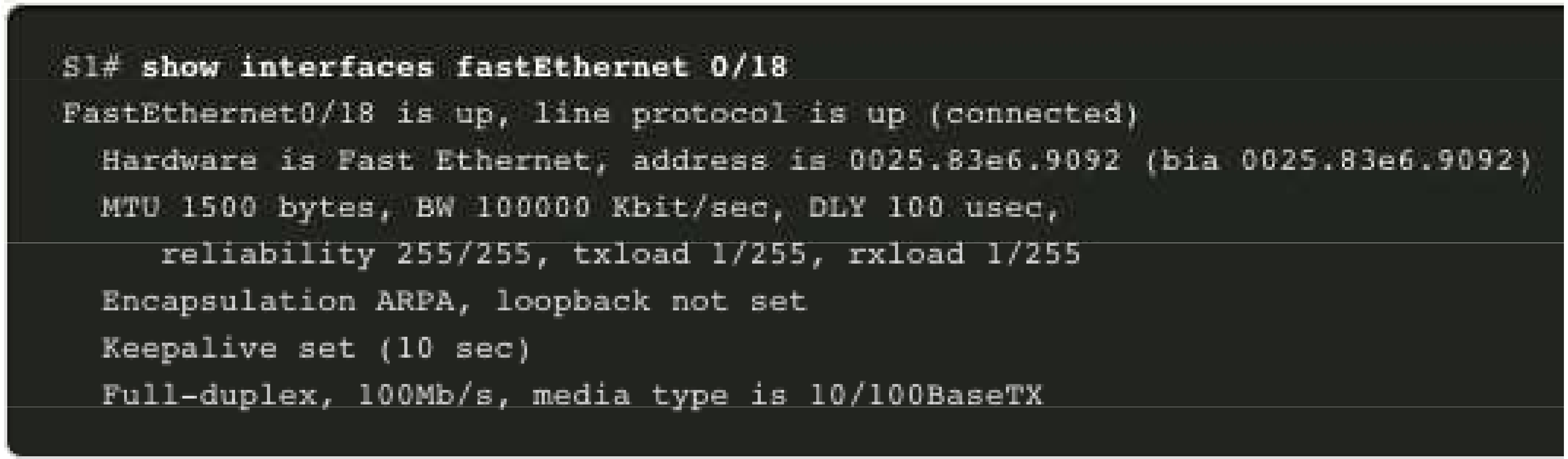


```
S1# show running-config
Building configuration...
Current configuration : 1466 bytes
!
(output omitted)
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 ipv6 address 2001:DB8:ACAD:99::1/64
!
ip default-gateway 172.17.99.1
```

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
```

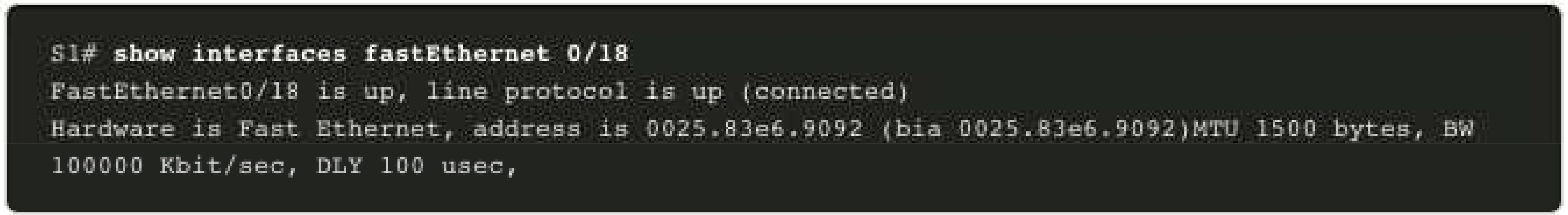
Network Access Layer Issues

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:

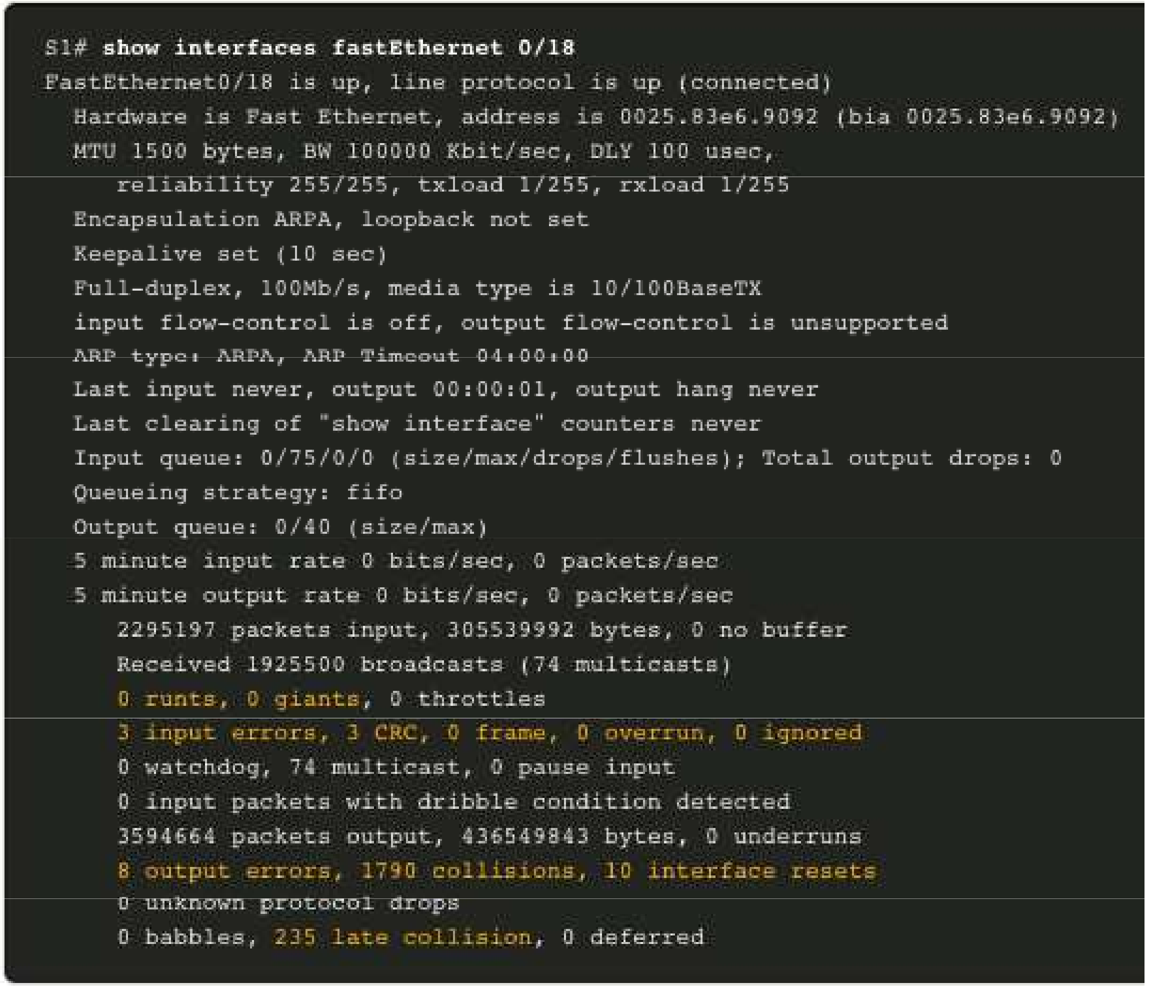
- If the interface is up and the line protocol is down, a problem exists. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.
- If the line protocol and the interface are both down, a cable is not attached, or some 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,
```

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 runts, 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
```

Network Access Layer Issues (Cont.)

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

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.

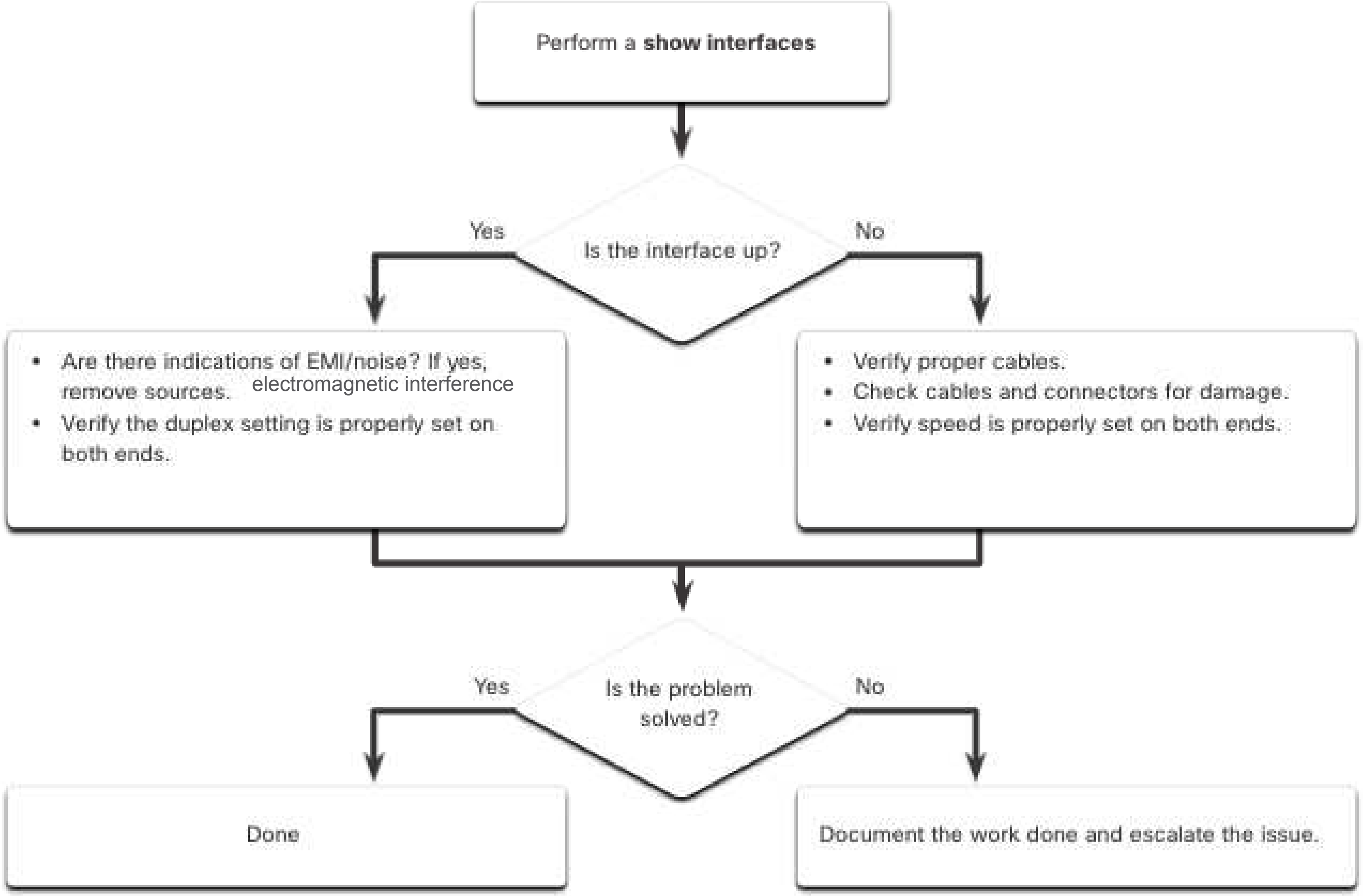
Interface Input and Output Errors (Cont.)

“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.

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.



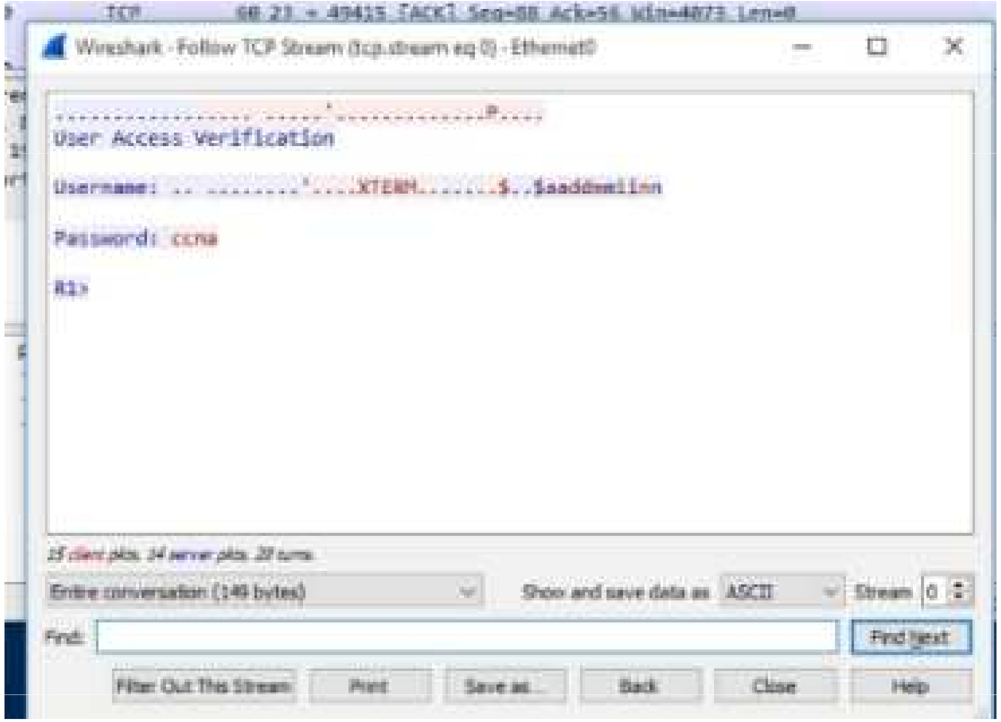
Perform a **show interfaces**
Is the interface up?
Yes
No
• Are there indications of EMI/noise? If yes, remove sources.
electromagnetic interference
• Verify the duplex setting is properly set on both ends.
• Verify proper cables.
• Check cables and connectors for damage.
• Verify speed is properly set on both ends.
Is the problem solved?
Yes
No
Done
Document the work done and escalate the issue.

1.3 Secure Remote Access

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.



```
TCP    60 23 → 49415 [ACK] Seq=88 Ack=56 Win=4073 Len=0
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ethernet0

```
..................... ......'..............P....
User Access Verification

Username: .. .........'....XTERM.......$..$aaddmmiinn

Password: ccna

R1>
```

15 client pkts, 14 server pkts, 28 turns.

Entire conversation (149 bytes)

Show and save data as: ASCII

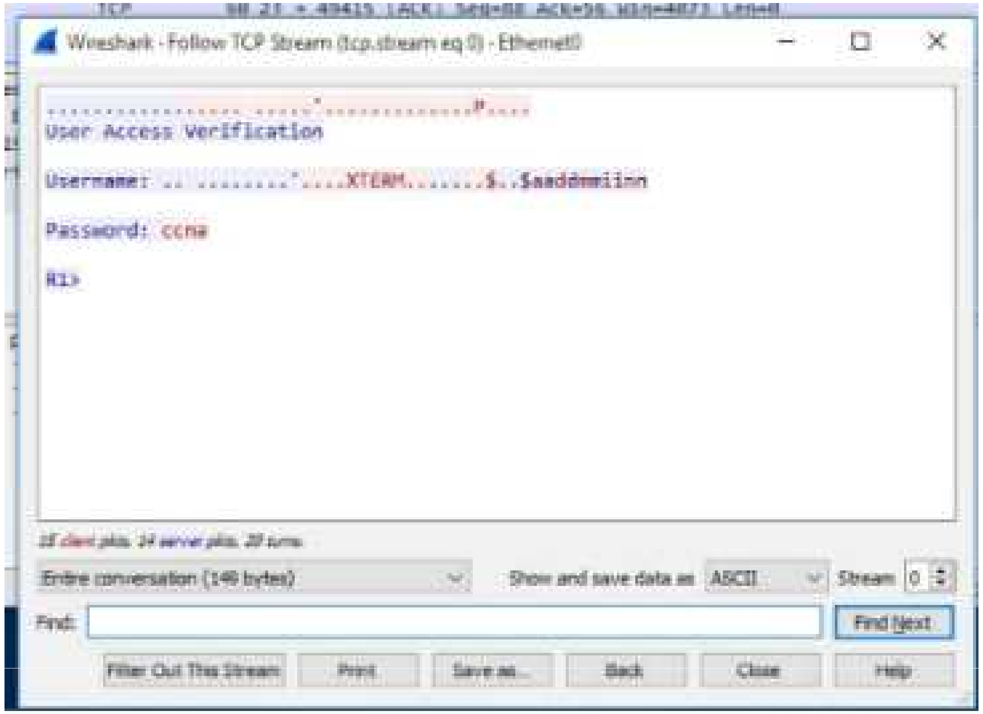
Stream: 0

Find:

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.



```
.................. .....'..............P....
User Access Verification

Username: .. .........'.....XTERM.......$..$aaddmmiinn

Password: ccna

R1>
```

15 client pkts, 24 server pkts, 20 turns.

Entire conversation (149 bytes)

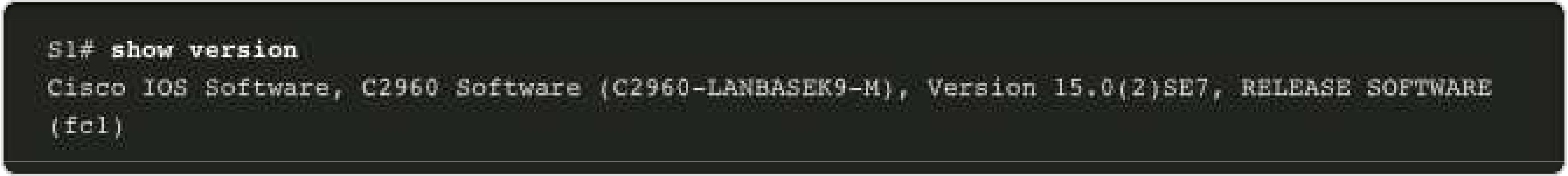
Show and save data as: ASCII

Stream: 0

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)
```

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.

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 (my píšeme no ip-domain lookup.)

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.

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.

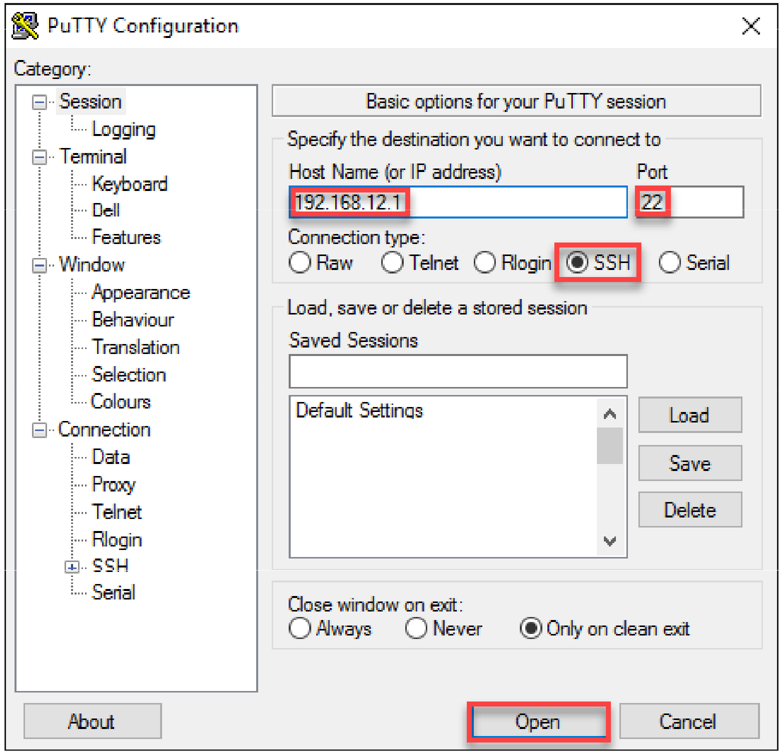
Step 5: Configure the vty lines - Enable the SSH protocol on the vty lines by using the transport input ssh line configuration mode command. Use the line vty global configuration mode command and then the login local line configuration mode command to require local authentication for SSH connections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

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.

Konfigurace SSH na serveru

```
Router(config)#hostname R1
R1(config)#ip domain-name UO.LOCAL
R1(config)#crypto key generate rsa
R1(config)#ip ssh version 2

R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config)#username admin password moje_heslo
```

Konfigurace SSH na klientovi



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.12.1

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Nastavení SSH na Packet Traceru

```
R2#ssh -l admin 192.168.12.1
Password:
```

Jiná Cisco zařízení

```
R2#ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

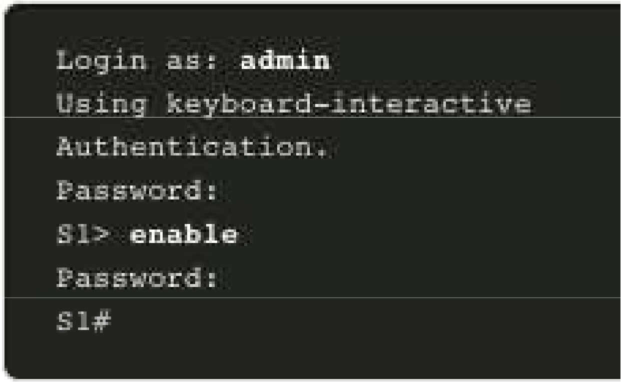
Verify SSH is Operational

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.

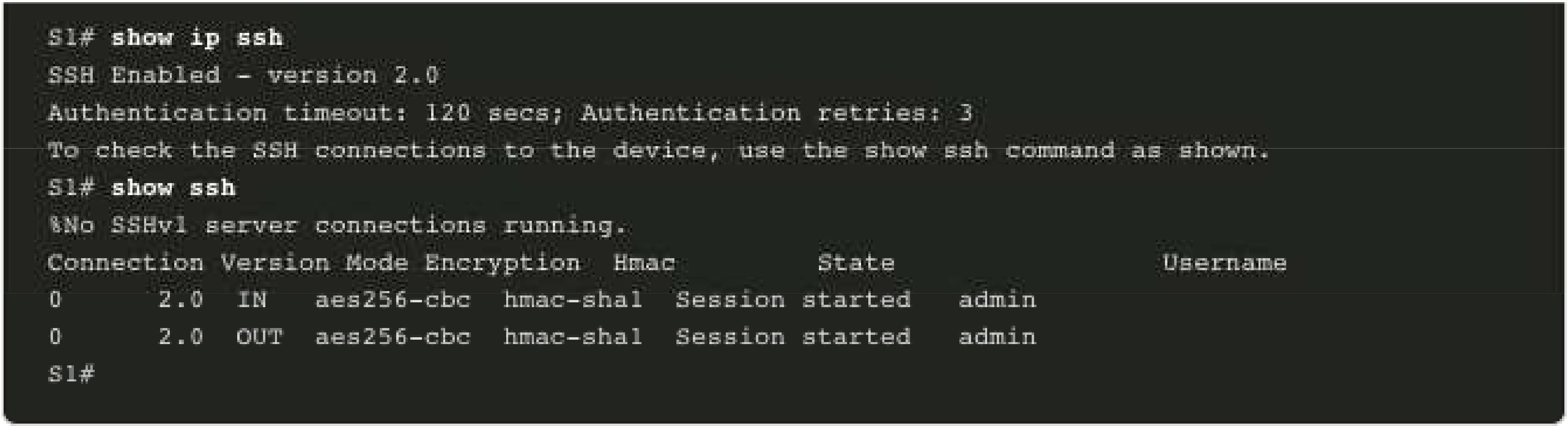
When connected, the user is prompted for a username and password as shown in the example. Using the configuration from the previous example, the username **admin** and password **ccna** are entered. After entering the correct combination, the user is connected via SSH to the command line interface (CLI)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



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

Verify SSH is Operational (Cont.)

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#
```

Packet Tracer – Configure SSH

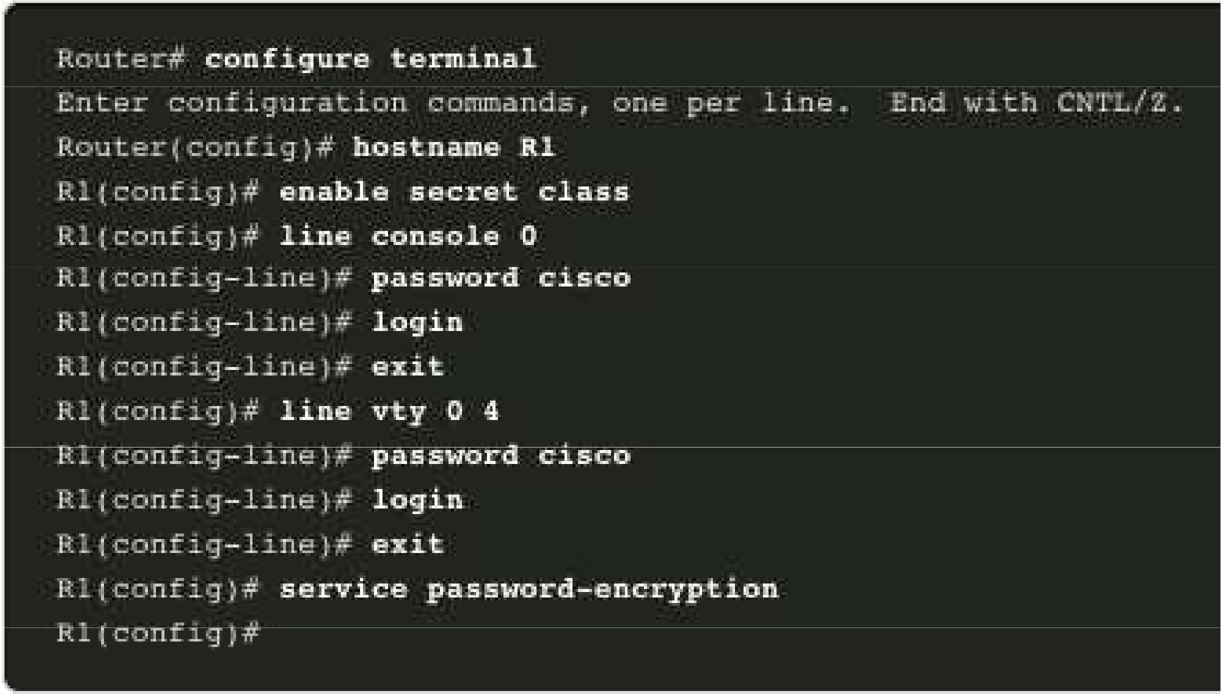
In this Packet Tracer, you will do the following:

- Secure passwords
- Encrypt communications
- Verify SSH implementation

1.4 Basic Router Configuration

Configure Basic Router Settings

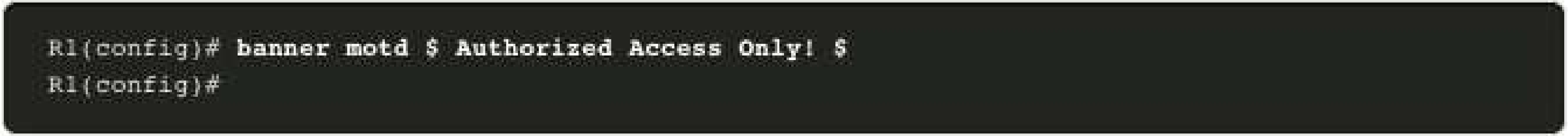
Cisco routers and Cisco switches have many similarities. They support a similar modal operating system, similar command structures, and many of the same commands. In addition, both devices have similar initial configuration steps. For example, the following configuration tasks should always be performed. 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)#
```

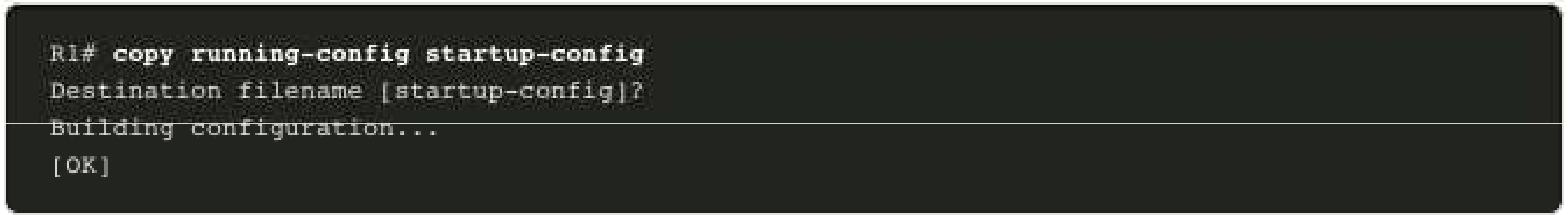
Configure Basic Router Settings (Cont.)

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



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

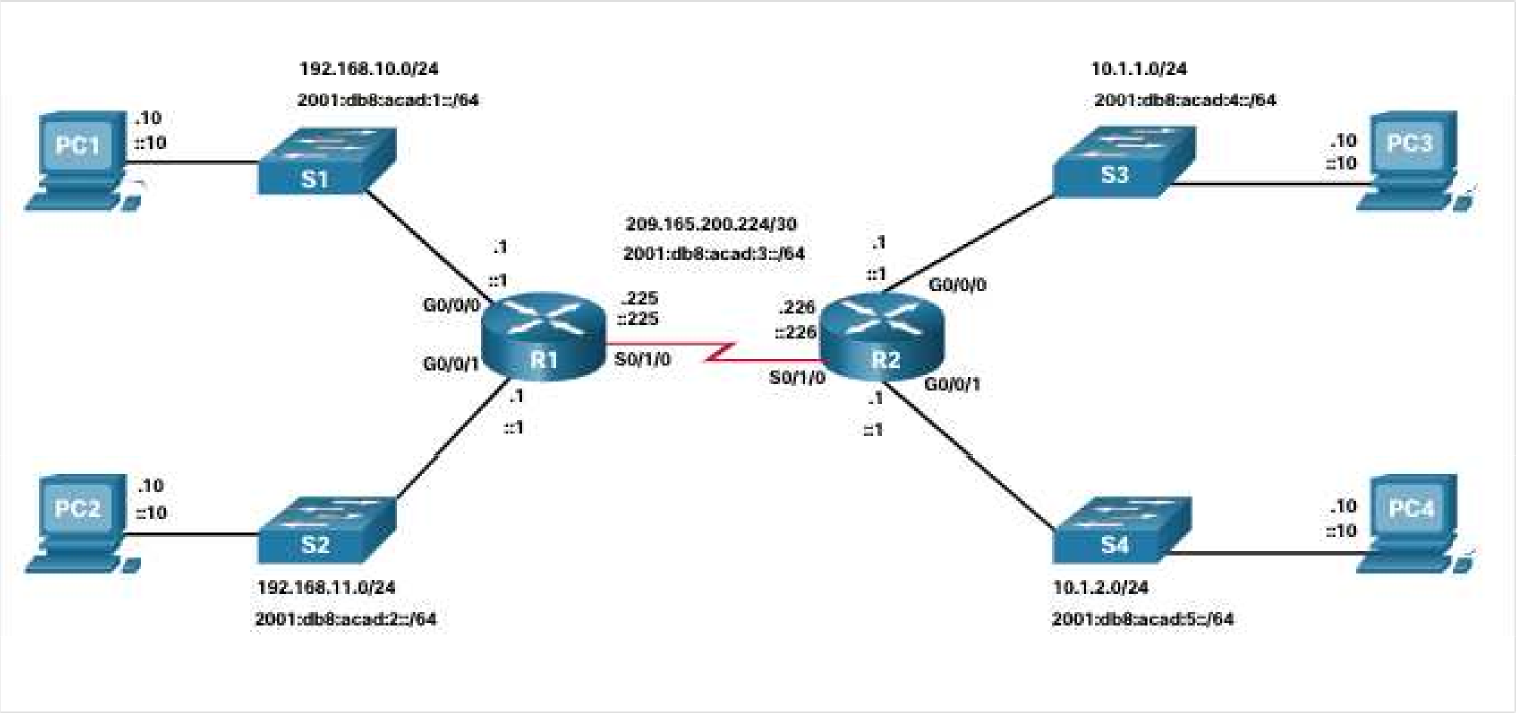
Save the changes on a router, as shown in the example.



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

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.



Configure Router Interfaces

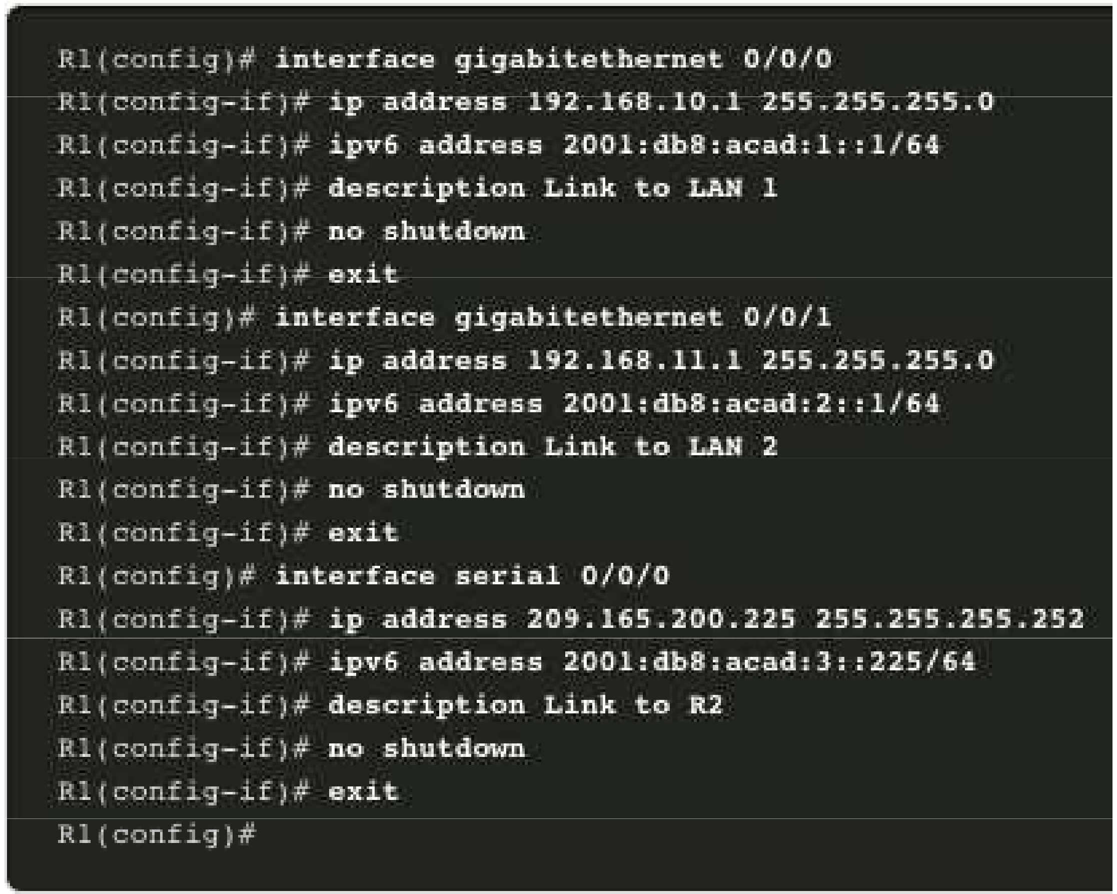
Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces. For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and High-Speed WAN Interface Card (HWIC) slots to accommodate other types of network interfaces,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

Configure Router Interfaces (Cont.)

The example shows the configure for the interfaces on R1:



```
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)#
```

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
```

Packet Tracer – Configure Router Interfaces

In this Packet Tracer activity, you will do the following:

- Configure IPv4 addressing and verify connectivity
- Configure IPv6 addressing and verify connectivity

1.5 Verify Directly Connected Networks

Interface Verification Commands

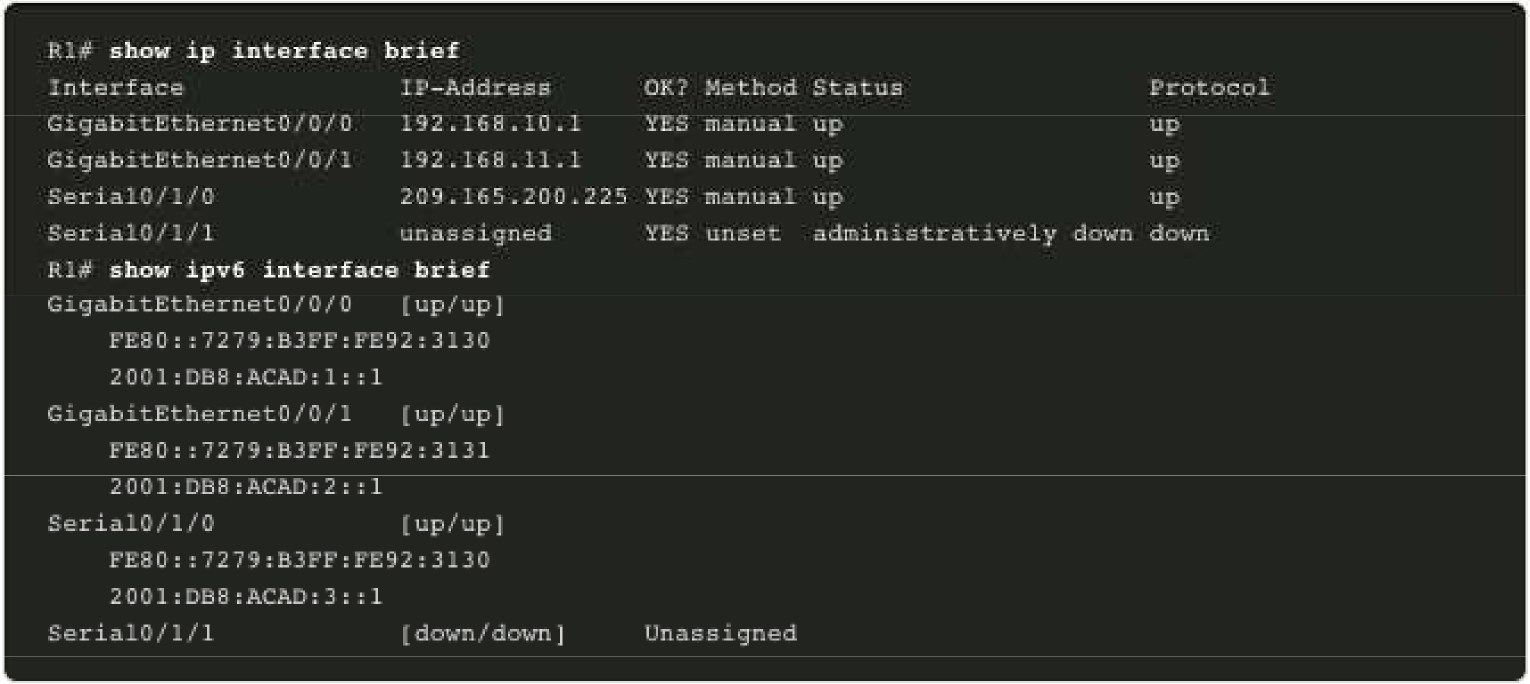
There are several **show** commands that can be used to verify the operation and configuration of an interface.

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.

Verify 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

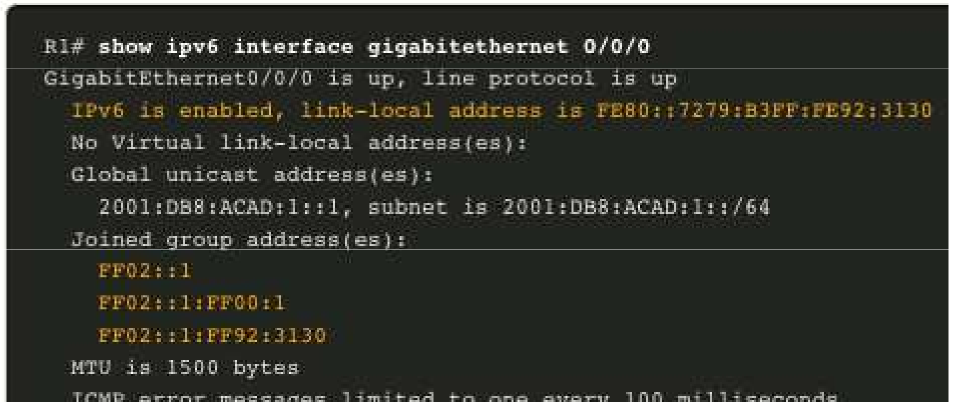


```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225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

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.



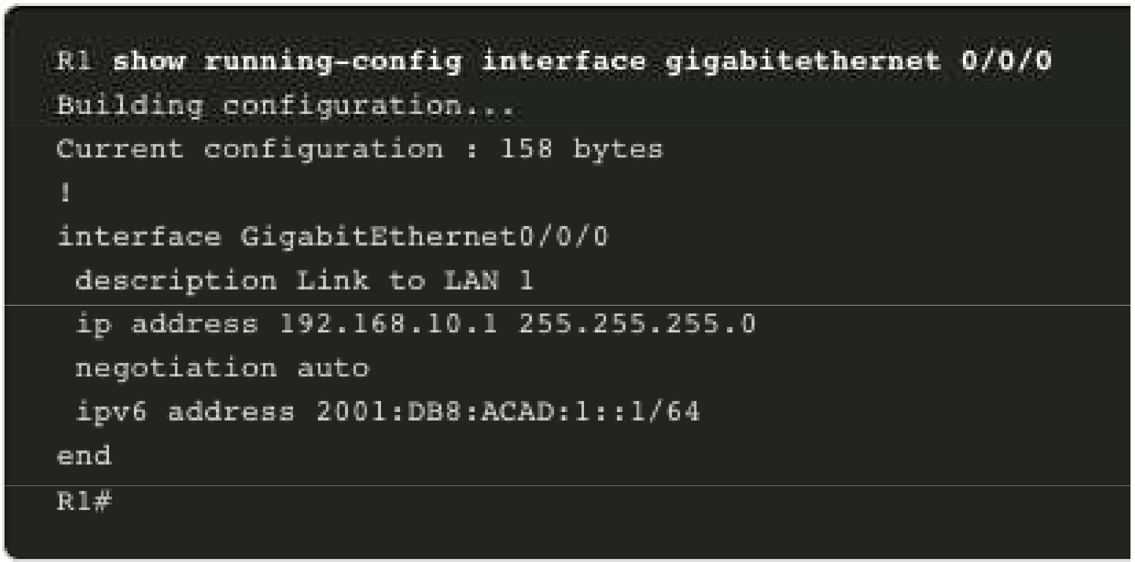
```
R1# show ipv6 interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::7279:B3FF:FE92:3130
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF92:3130
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
```

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

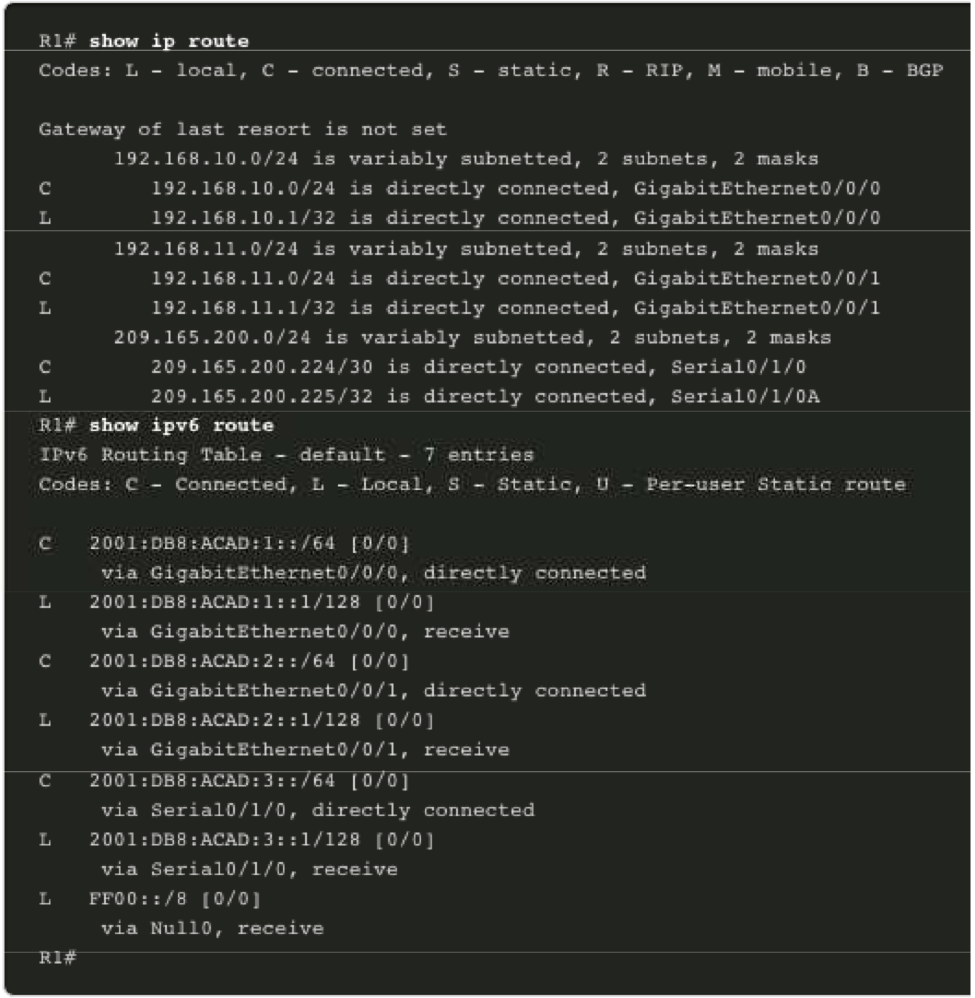


```
R1 show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 158 bytes
!
interface GigabitEthernet0/0/0
 description Link to LAN 1
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:ACAD:1::1/64
end
R1#
```

Verify Routes

The output of the **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.

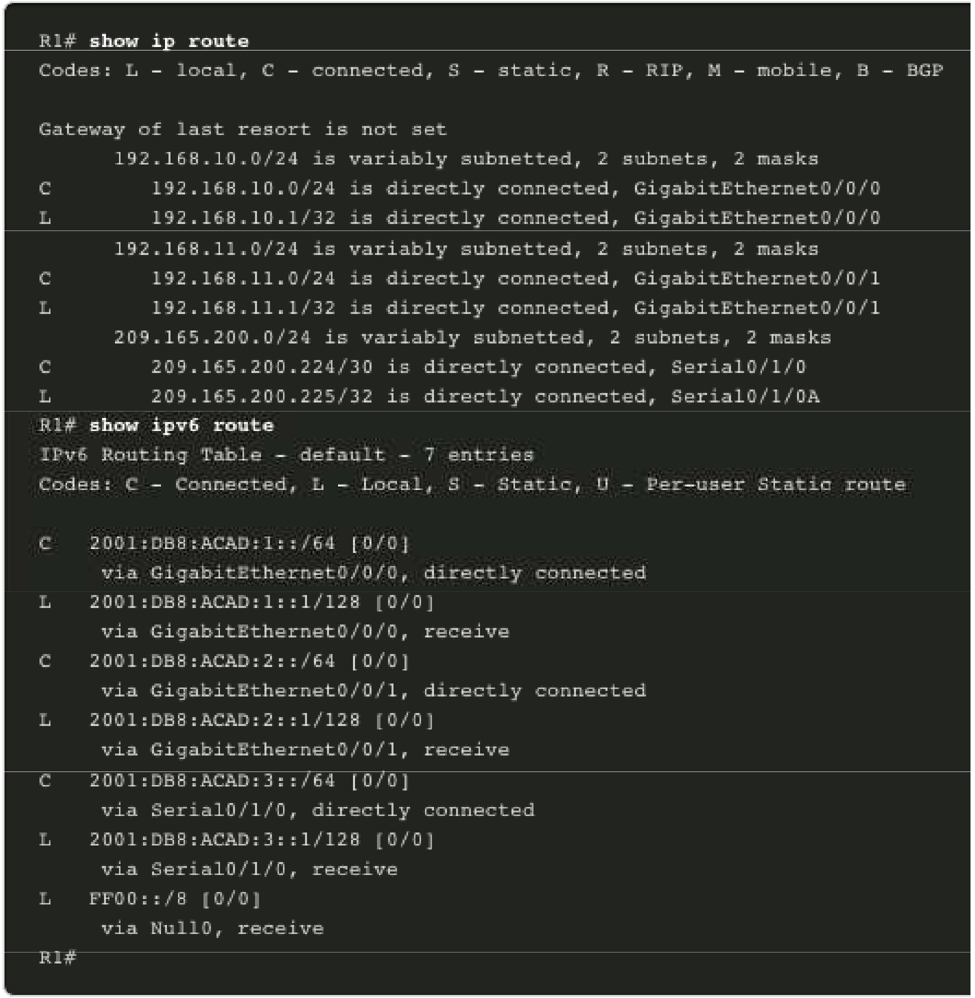


```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

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#
```

Verify Routes (Cont.)

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.



```
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#
```

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

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.

Packet Tracer – Verify Directly Connected Networks

In this Packet Tracer activity, you will complete the following objectives:

- Verify IPv4 directly connected networks
- Verify IPv6 directly connected networks
- Troubleshoot connectivity issues

1.6 Module Practice and Quiz

Packet Tracer – Implement a Small Network

In this Packet Tracer activity, you will do the following:

- Create a network topology
- Configure devices and verify connectivity

Lab– Configure Basic Router Settings

In this lab, you will complete the following objectives:

- Set up the topology and initialize devices
  - Cable equipment to match the network topology
  - Initialize and restart the router and switch
- Configure devices and verify connectivity
  - Assign static IPv4 and IPv6 information to the PC interface
  - Configure basic router settings
  - Configure the router for SSH
  - Verify network connectivity

What Did I Learn In This Module?

- 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.
- 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.
- 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.
- Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously.
- 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.

What Did I Learn In This Module? (Cont.)

- There are several show commands to use when verifying switch configurations.
- 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) 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.
- 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.
- 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.

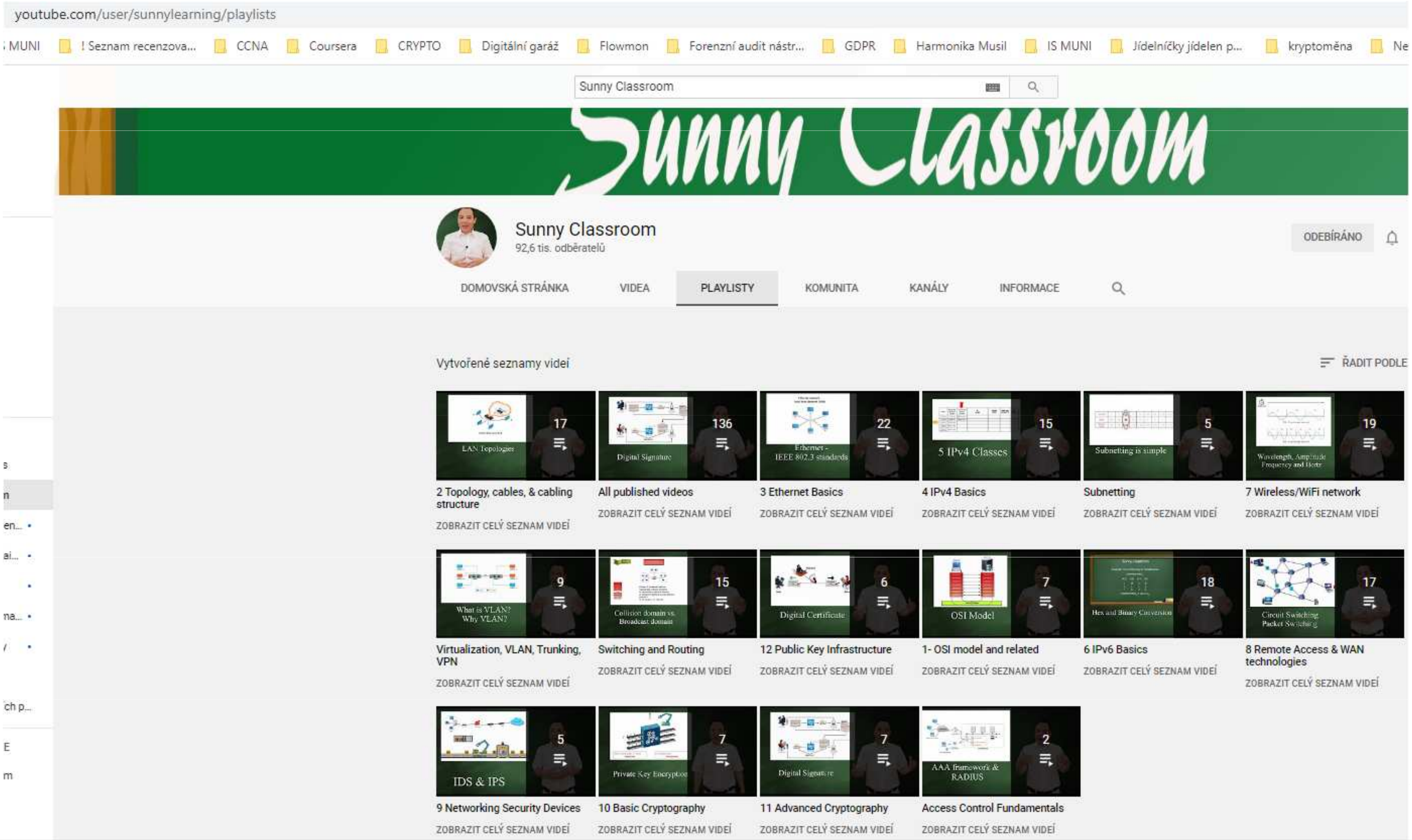
What Did I Learn In This Module? (Cont.)

- One distinguishing feature between switches and routers is the type of interfaces supported by each.
- Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of 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.
- 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.
- 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.

New Terms and Commands

- **boot system flash**
- Power over Ethernet (PoE)
- **duplex**
- **speed**
- auto-mdix
- **show controllers ethernet controller X**
- **phy**
- **show flash**
- **show history**
- **show ip ssh**
- **ip ssh version 2**
- Loopback Interface
- **interface loopback x**
- **include**
- **exclude**
- **section**
- **show history**
- **terminal history size**

Sunny Classroom: https://www.youtube.com/user/sunnylearning/videos



youtube.com/user/sunnylearning/playlists

Sunny Classroom

92,6 tis. odběratelů

Vytvořené seznamy videí

- 2 Topology, cables, & cabling structure — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- All published videos — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 3 Ethernet Basics — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 4 IPv4 Basics — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- Subnetting — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 7 Wireless/WiFi network — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- Virtualization, VLAN, Trunking, VPN — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- Switching and Routing — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 12 Public Key Infrastructure — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 1- OSI model and related — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 6 IPv6 Basics — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 8 Remote Access & WAN technologies — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 9 Networking Security Devices — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 10 Basic Cryptography — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- 11 Advanced Cryptography — ZOBRAZIT CELÝ SEZNAM VIDEÍ
- Access Control Fundamentals — ZOBRAZIT CELÝ SEZNAM VIDEÍ