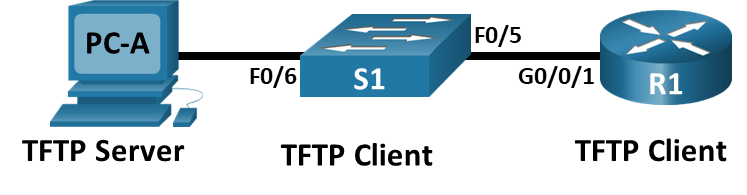
Lab - Use TFTP, Flash, and USB to Manage Configuration Files (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

# Topology



# Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | G0/0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |

# Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Use TFTP to Back Up and Restore the Switch Running Configuration

Part 3 Use TFTP to Back Up and Restore the Router Running Configuration

Part 4: Back Up and Restore Running Configurations Using Router Flash Memory

Part 5: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration

# Background / Scenario

Cisco networking devices are often upgraded or swapped out for a number of reasons. It is important to maintain backups of the latest device configurations, as well as a history of configuration changes. A TFTP server is often used to backup configuration files and IOS images in production networks. A TFTP server is a centralized and secure method used to store the backup copies of the files and restore them as necessary. Using a centralized TFTP server, you can back up files from many different Cisco devices.

In addition to a TFTP server, most of the current Cisco routers can back up and restore files locally from CompactFlash (CF) memory or a USB flash drive. The CF is a removable memory module that has replaced the limited internal flash memory of earlier router models. The IOS image for the router resides in the CF memory, and the router uses this IOS Image for the boot process. With the larger size of the CF memory, additional files can be stored for backup purposes. A removable USB flash drive can also be used for backup purposes.

In this lab, you will use TFTP server software to back up the Cisco device running configuration to the TFTP server. You can edit the file using a text editor and copy the new configuration back to a Cisco device. The instructions here for the TFTP server configuration and operation are generic and there may be some differences in terminology with your TFTP server software.

**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**: Ensure that the routers and switches have been erased and have no startup configurations. If you are unsure contact your instructor.

**Instructor Note**: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices

# Required Resources

* 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.3 universal image or comparable)
* 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
* 1 PC (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
* USB flash drive (Optional)

# Instructions

## Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses for router R1, switch S1 and PC-A.

### Cable the network as shown in the topology.

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

### Configure basic settings for the router.

Open configuration window

* + - 1. Assign a device name to the router.

router(config)# **hostname R1**

* + - 1. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

R1(config)# **no ip domain-lookup**

* + - 1. Assign **class** as the privileged EXEC encrypted password.

R1(config)# **enable secret class**

* + - 1. Assign **cisco** as the console password and enable login.

R1(config)# **line console 0**

R1(config-line)# **password cisco**

R1(config-line)# **login**

* + - 1. Assign **cisco** as the VTY password and enable login.

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco**

R1(config-line)# **login**

* + - 1. Encrypt the plaintext passwords.

R1(config)# **service password-encryption**

* + - 1. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

R1(config)# **banner motd $ Authorized Users Only! $**

* + - 1. Configure interfaces as listed in the table above.

R1(config-if)# **interface g0/0/1**

R1(config-if)# **ip address 192.168.1.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

* + - 1. Save the running configuration to the startup configuration file.

R1# **copy running-config startup-config**

**Note**: Use the question mark (**?**) to help with the correct sequence of parameters needed to execute this command.

Close configuration window

### Configure basic settings for the switch.

Open configuration window

* + - 1. Assign a device name to the switch.

switch(config)# **hostname S1**

* + - 1. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

S1(config)# **no ip domain-lookup**

* + - 1. Assign **class** as the privileged EXEC encrypted password.

S1(config)# **enable secret class**

* + - 1. Assign **cisco** as the console password and enable login.

S1(config)# **line console 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

* + - 1. Assign **cisco** as the VTY password and enable login.

S1(config)# **line vty 0 4**

S1(config-line)# **password cisco**

S1(config-line)# **login**

* + - 1. Encrypt the plaintext passwords.

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

* + - 1. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# **banner motd $ Authorized Users Only! $**

* + - 1. Shut down all unused interfaces.

S1(config)# **interface range f0/1-4, f0/7-24, g0/1-2**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

* + - 1. Configure interface VLAN 1 as specified in the table above.

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.11 255.255.255.0**

S1(config-if)# **no shutdown**

S1(config-if)# **exit**

S1(config)# **ip default-gateway 192.168.1.1**

* + - 1. Save the running configuration to the startup configuration file.

S1# **copy running-config startup-config**

**Note**: Use the question mark (**?**) to help with the correct sequence of parameters needed to execute this command.

Close configuration window

### Verify connectivity from PC-A.

* + - 1. Ping from PC-A to S1.
      2. Ping from PC-A to R1.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

## Use TFTP to Back Up and Restore the Switch Running Configuration

### Verify connectivity to switch S1 from PC-A.

The TFTP application uses the UDP Layer 4 transport protocol, which is encapsulated in an IP packet. For TFTP file transfers to function, there must be Layer 1 and 2 (Ethernet, in this case) and Layer 3 (IP) connectivity between the TFTP client and the TFTP server. The LAN topology in this lab uses only Ethernet at Layers 1 and 2. However, TFTP transfers can also be accomplished over WAN links that use other Layer 1 physical links and Layer 2 protocols. As long as there is IP connectivity between the client and server, as demonstrated by ping, the TFTP transfer can take place. If the pings are not successful, troubleshoot the basic device configurations before continuing.

**Note**: A common misconception is that you can TFTP a file over the console connection. This is not the case because the console connection does not use IP. The TFTP transfer can be initiated from the client device (router or switch) using the console connection, but there must be IP connectivity between the client and server for the file transfer to take place.

### Start the TFTP server.

Start the TFTP program on PC-A. Ensure that the TFTP program is using a directory that you have WRITE permission for, such as a folder on your desktop.

### Explore the copy command on a Cisco device.

* + - 1. Console into switch S1 and, from the privileged EXEC mode prompt, enter **copy ?** to display the options for source or “from” location and other available copy options. You can specify **flash:** or **flash0:** as the source. However, if you simply provide a filename as the source, **flash0:** is assumed and is the default. Note that **running-config** is also an option for the source location.

Open configuration window

S1# **copy ?**

/erase Erase destination file system.

/error Allow to copy error file.

/noverify Don't verify image signature before reload.

/verify Verify image signature before reload.

bs: Copy from bs: file system

cns: Copy from cns: file system

flash: Copy from flash: file system

ftp: Copy from ftp: file system

http: Copy from http: file system

https: Copy from https: file system

logging Copy logging messages

null: Copy from null: file system

nvram: Copy from nvram: file system

rcp: Copy from rcp: file system

running-config Copy from current system configuration

scp: Copy from scp: file system

startup-config Copy from startup configuration

system: Copy from system: file system

tar: Copy from tar: file system

tftp: Copy from tftp: file system

tmpsys: Copy from tmpsys: file system

vb: Copy from vb: file system

xmodem: Copy from xmodem: file system

ymodem: Copy from ymodem: file system

* + - 1. Use the **?** to display the destination options after a source file location is chosen. The **flash:** file system for S1 is the source file system in this example.

S1# **copy flash: ?**

flash: Copy to flash: file system

ftp: Copy to ftp: file system

http: Copy to http: file system

https: Copy to https: file system

null: Copy to null: file system

nvram: Copy to nvram: file system

rcp: Copy to rcp: file system

running-config Update (merge with) current system configuration

scp: Copy to scp: file system

startup-config Copy to startup configuration

system: Copy to system: file system

tftp: Copy to tftp: file system

tmpsys: Copy to tmpsys: file system

vb: Copy to vb: file systesystem

### Transfer the running-config file from switch S1 to TFTP server on PC-A.

* + - 1. From the privileged EXEC mode on the switch, enter the **copy running-config tftp:** command. Provide the remote host address of the TFTP server (PC-A), 192.168.1.3. Press Enter to accept default destination filename (**s1-confg**) or provide your own filename. The exclamation marks (**!!**) indicate the transfer process is in progress and is successful.

S1# **copy running-config tftp:**

Address or name of remote host []? **192.168.1.3**

Destination filename [s1-confg]?

!!

1465 bytes copied in 0.663 secs (2210 bytes/sec)

S1#

The TFTP server may also displays transfer progress.

**Note**: If you do not have permission to write to the current directory that is used by the TFTP server, the following error message displays:

S1# **copy running-config tftp:**

Address or name of remote host []? **192.168.1.3**

Destination filename [s1-confg]?

%Error opening tftp://192.168.1.3/s1-confg (Permission denied)

**Note**: Other issues, such as a firewall blocking TFTP traffic, can prevent the TFTP transfer. Please check with your instructor for further assistance.

* + - 1. Check the directory on the TFTP server (usually the default directory for the TFTP server software) to verify that the file was transferred successfully. Your TFTP server may have a dialog for this, or you can simply use the File Explorer provided by your Operating System.

### Create a modified switch running configuration file.

The saved running configuration file, **s1-confg**, can also be restored to the switch by using the **copy** command from the switch. The original or a modified version of the file can be copied to the flash file system of the switch.

* + - 1. Navigate to the TFTP directory on PC-A by using the file system of PC-A, and then locate the **s1-confg** file. Open this file using a text editor program, such as WordPad.
      2. With the file open, locate the **hostname S1** line. Replace **S1** with **Switch1**. Delete all the self-generated crypto keys, as necessary. A sample of the keys is displayed below. These keys are not exportable and can cause errors while updating the running configuration.

crypto pki trustpoint TP-self-signed-1566151040

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-1566151040

revocation-check none

rsakeypair TP-self-signed-1566151040

!

!

crypto pki certificate chain TP-self-signed-1566151040

certificate self-signed 01

3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

<output omitted>

E99574A6 D945014F B6FE22F3 642EE29A 767EABF7 403930CA D2C59E23 102EC12E

02F9C933 B3296D9E 095EBDAF 343D17F6 AF2831C7 6DA6DFE3 35B38D90 E6F07CD4

40D96970 A0D12080 07A1C169 30B9D889 A6E2189C 75B988B9 0AF27EDC 6D6FA0E5

CCFA6B29 729C1E0B 9DADACD0 3D7381

quit

* + - 1. Save this file as a plain text file with a new filename, **Switch1-confg.txt**, in this example.

**Note**: When saving the file, an extension, such as **.txt**, may be added to the filename automatically.

* + - 1. If your TFTP software has the option, use it to show the contents of its directory to verify that the file is present.

### Copy the modified running configuration file from the TFTP server to switch S1.

* + - 1. From the privileged EXEC mode on the switch, enter the **copy tftp running-config** command. Provide the remote host address of the TFTP server, 192.168.1.3. Enter the new filename, **Switch1-confg.txt**. The exclamation mark (!) indicates the transfer process is in progress and is successful.

S1# **copy tftp: running-config**

Address or name of remote host []? **192.168.1.3**

Source filename []? **Switch1-confg.txt**

Destination filename [running-config]?

Accessing tftp://192.168.1.3/Switch1-confg.txt...

Loading Switch1-confg.txt from 192.168.1.3 (via Vlan1): !

[OK - 1580 bytes]

[OK]

1580 bytes copied in 9.118 secs (173 bytes/sec)

\*Mar 1 00:21:16.242: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue "write memory" to save new certificate

\*Mar 1 00:21:16.251: %SYS-5-CONFIG\_I: Configured from tftp://192.168.1.3/Switch1-confg.txt by console

Switch1#

After the transfer has completed, the prompt has changed from S1 to Switch1, because the running configuration is updated with the **hostname Switch1** command in the modified running configuration.

* + - 1. Enter the **show running-config** command to examine running configuration file.

Switch1# **show running-config**

Building configuration...

Current configuration : 3062 bytes

!

! Last configuration change at 00:09:34 UTC Mon Mar 1 1993

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Switch1

!

boot-start-marker

boot-end-marker

<output omitted>

close configuration window

**Note**: This procedure merges the running-config from the TFTP server with the current running-config in the switch or router. If changes were made to the current running-config, the commands in the TFTP copy are added. Alternatively, if the same command is issued, it updates the corresponding command in the switch or router current running-config.

If you want to completely replace the current running-config with the one from the TFTP server, you must erase the switch startup-config and reload the device. You will then need to configure the VLAN 1 management address, so there is IP connectivity between the TFTP server and the switch.

## Use TFTP to Back Up and Restore the Router Running Configuration

The backup and restore procedure from Part 3 can also be performed with a router. In Part 4, the running configuration file will be backed up and restored using a TFTP server.

### Verify connectivity to router R1 from PC-A.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

### Transfer the running configuration from router R1 to TFTP server on PC-A.

Open configuration window

* + - 1. From the privileged EXEC mode on R1, enter the **copy running-config tftp** command. Provide the remote host address of the TFTP server, 192.168.1.3, and accept the default filename.
      2. Verify that the file has been transferred to the TFTP server.

### Restore the running configuration file to the router.

* + - 1. Erase the startup-config file on the router.
      2. Reload the router.
      3. Configure the G0/0/1 interface on the router with an IP address 192.168.1.1.
      4. Verify connectivity between the router and PC-A.
      5. Use the **copy** command to transfer the running-config file from the TFTP server to the router. Use **running-config** as the destination.
      6. Verify the router has updated the running-config.

Close configuration window

## Back Up and Restore Configurations Using Router Flash Memory

Current generation Cisco routers do not have internal flash memory. The flash memory for these routers uses CompactFlash (CF) memory. The use of CF memory allows for more available flash memory and easier upgrades without the need to open the router case. Besides storing the necessary files, such as IOS images, the CF memory can store other files, such as a copy of the running configuration. In Part 5, you will create a backup copy of the running configuration file and save it on the USB memory on the router.

**Note**: If the router does not use CF, the router may not have enough flash memory for storing the backup copy of running configuration file. You should still read through the instructions and become familiar with the commands.

### Display the router file systems.

The **show file systems** command displays the available file systems on the router. The **flash0:** file system is the default file system on this router as indicated by the asterisk (\*) symbol (at the beginning of the line). The **flash0:** file system can also be referenced using the name **flash:**. The total size of the **flash0:** is approximately 7GB with about 6GB available. Currently **flash0:** and **nvram:** are the only available file systems.

Open configuration window

R1# **show file systems**

File Systems:

Size(b) Free(b) Type Flags Prefixes

- - opaque rw system:

- - opaque rw tmpsys:

\* 7194652672 6299918336 disk rw bootflash: flash:

1804468224 1723789312 disk ro webui:

- - opaque rw null:

- - opaque ro tar:

- - network rw tftp:

- - opaque wo syslog:

33554432 33543116 nvram rw nvram:

- - network rw rcp:

- - network rw ftp:

- - network rw http:

- - network rw scp:

- - network rw sftp:

- - network rw https:

- - opaque ro cns:

#### Question:

Where is the startup-config file located?

Type your answers here.

nvram:

**Note**: Verify there is at least 1 MB (1,048,576 bytes) of free space. If there is not enough space in the flash memory, please contact your instructor for further instructions. You can determine the size of flash memory and space available using the **show flash** or **dir flash:** command at the privileged EXEC prompt.

### Copy the router running configuration to flash.

A file can be copied to flash by using the **copy** command at the privileged EXEC prompt. In this example, the file is copied into **flash0:**, because there is only one flash drive available as displayed in the previous step, and it is also the default file system. The **R1-running-config-backup** file is used as the filename for the backup running configuration file.

**Note**: Remember that filenames are case-sensitive in the IOS file system.

* + - 1. Copy the running configuration to flash memory.

R1# **copy running-config flash:**

Destination filename [running-config]? **R1-running-config-backup**

2169 bytes copied in 0.968 secs (2241 bytes/sec)

* + - 1. Use **dir** command to verify the running-config has been copied to flash.

R1# **dir flash:**

Directory of bootflash:/

11 drwx 16384 Aug 2 2019 04:15:13 +00:00 lost+found

370945 drwx 4096 Sep 25 2019 20:17:11 +00:00 .installer

338689 drwx 4096 Aug 2 2019 04:15:55 +00:00 .ssh

217729 drwx 4096 Aug 2 2019 04:17:59 +00:00 core

379009 drwx 4096 Sep 25 2019 20:19:13 +00:00 .prst\_sync

80641 drwx 4096 Aug 2 2019 04:16:09 +00:00 .rollback\_timer

161281 drwx 4096 Aug 2 2019 04:16:11 +00:00 gs\_script

112897 drwx 77824 Sep 25 2019 20:23:03 +00:00 tracelogs

362881 drwx 4096 Aug 23 2019 17:19:54 +00:00 .dbpersist

298369 drwx 4096 Aug 2 2019 04:16:41 +00:00 virtual-instance

12 -rw- 30 Sep 25 2019 20:19:13 +00:00 throughput\_monitor\_params

8065 drwx 4096 Aug 2 2019 04:17:55 +00:00 onep

13 -rw- 35 Sep 25 2019 20:20:19 +00:00 pnp-tech-time

249985 drwx 4096 Aug 20 2019 17:40:11 +00:00 Archives

14 -rw- 64414 Sep 25 2019 20:20:28 +00:00 pnp-tech-discovery-summary

15 -rw- 3509 Sep 25 2019 20:24:32 +00:00 R1-running-config-backup

17 -rw- 5032908 Sep 19 2019 14:16:23 +00:00 isr4200\_4300\_rommon\_1612\_1r\_SPA.pkg

18 -rw- 517153193 Sep 21 2019 04:24:04 +00:00 isr4200-universalk9\_ias.16.09.04.SPA.bin

7194652672 bytes total (6299643904 bytes free)

* + - 1. Use the **more** command to view the running-config file in flash memory. Examine the file output and scroll to the Interface section. Notice the **no shutdown** command is not included with the GigabitEthernet0/1. The interface is shut down when this file is used to update the running configuration on the router.

R1# **more flash:R1-running-config-backup**

<output omitted>

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

<output omitted>

### Erase the startup configuration and reload the router.

### Restore the running configuration from flash.

* + - 1. Verify the router has the default initial configuration.
      2. Copy the saved running-config file from flash to update the running-config.

Router# **copy flash:R1-running-config-backup running-config**

* + - 1. Use the **show ip interface brief** command to view the status of the interfaces. The interface GigabitEthernet0/1 was not enabled when the running configuration was updated, because it is administratively down.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 unassigned YES unset administratively down down

GigabitEthernet0/0/1 192.168.1.1 YES TFTP administratively down down

Serial0/1/0 unassigned YES unset administratively down down

Serial0/1/1 unassigned YES unset administratively down down

Close configuration window

The interface can be enabled using the **no shutdown** command in the interface configuration mode on the router.

Another option is to add the **no shutdown** command for the GigabitEthernet0/0/1 interface to the saved file before updating the router running configuration file. This will be done in Part 5 using a saved file on a USB flash drive.

**Note**: Because the IP address was configured by using a file transfer, TFTP is listed under the Method heading in the **show ip interface brief** output.

## (Optional) Use a USB Drive to Back Up and Restore the Running Configuration

A USB flash drive can be used to backup and restore files on a router with an available USB port. One USB port is available on the 4221 routers.

**Note**: USB ports are not available on all routers, but you should still become familiar with the commands.

**Note**: Some ISR G1 routers (1841, 2801, or 2811) use File Allocation Table (FAT) file systems, which results in a maximum size limit for the USB flash drives that can be used in this part of the lab. The recommended maximum size for an ISR G1 is 4 GB. If you receive the following message, the file system on the USB flash drive may be incompatible with the router or the capacity of the USB flash drive may have exceeded maximum size of the FAT file system on the router.

\*Feb 8 13:51:34.831: %USBFLASH-4-FORMAT: usbflash0 contains unexpected values in partition table or boot sector. Device needs formatting before use!

### Insert a USB flash drive into a USB port on the router.

Notice the message on the terminal when inserting the USB flash drive.

\*Sep 24 23:00:33.242: %IOSD\_INFRA-6-IFS\_DEVICE\_OIR: Device usb0 added

### Verify that the USB flash file system is available.

Open configuration window

R1# **show file systems**

File Systems:

Size(b) Free(b) Type Flags Prefixes

- - opaque rw system:

- - opaque rw tmpsys:

\* 7194652672 6297677824 disk rw bootflash: flash:

256589824 256577536 disk rw usb0:

1804468224 1723789312 disk ro webui:

- - opaque rw null:

- - opaque ro tar:

- - network rw tftp:

- - opaque wo syslog:

33554432 33543116 nvram rw nvram:

- - network rw rcp:

- - network rw ftp:

- - network rw http:

- - network rw scp:

- - network rw sftp:

- - network rw https:

- - opaque ro cns:

### Copy the running configuration file to the USB flash drive.

Use the **copy** command to copy the running configuration file to the USB flash drive.

R1# **copy running-config usb0:**

Destination filename [running-config]? **R1-running-config-backup.txt**

2198 bytes copied in 0.708 secs (3105 bytes/sec)

### List the file on the USB flash drive.

Use the **dir** command (or **show** command) on the router to list the files on the USB flash drive. In this sample, a flash drive was inserted into USB port 0 on the router.

R1# **dir usb0:**

Directory of usb0:/

6 -rwx 3539 Sep 25 2019 20:41:58 +00:00 R1-running-config-backup.txt

3 drwx 4096 Sep 24 2019 13:32:26 +00:00 System Volume Information

256589824 bytes total (256573440 bytes free)

### Erase the startup-config and reload the router.

### Modify the saved file.

* + - 1. Remove the USB drive from the router.

Router#

\*Sep 24 23:00:27.674: %IOSD\_INFRA-6-IFS\_DEVICE\_OIR: Device usb0 removed

* + - 1. Insert the USB drive into the USB port of a PC.
      2. Modify the file using a text editor. The **no shutdown** command is added to the GigabitEthernet0/0/1 interface. Save the file as a plain text file on to the USB flash drive.

interface GigabitEthernet0/0/1

ip address 192.168.1.1 255.255.255.0

no shutdown

duplex auto

speed auto

* + - 1. Remove the USB flash drive from the PC safely.

### Restore the running configuration file to the router.

* + - 1. Insert the USB flash drive into a USB port on the router. Notice the port number where the USB drive has been inserted if there is more than one USB port available on the router.

\*Sep 24 23:00:33.242: %IOSD\_INFRA-6-IFS\_DEVICE\_OIR: Device usb0 added

* + - 1. List the files on the USB flash drive.

R1# **dir usb0:**

Directory of usb0:/

6 -rwx 3539 Sep 25 2019 20:41:58 +00:00 R1-running-config-backup.txt

3 drwx 4096 Sep 24 2019 13:32:26 +00:00 System Volume Information

256589824 bytes total (256573440 bytes free)

* + - 1. Copy the running configuration file to the router.

Router# **copy usb0:R1-running-config-backup.txt running-config**

Destination filename [running-config]?

2344 bytes copied in 0.184 secs (12739 bytes/sec)

R1#

* + - 1. Verify that the GigabitEthernet0/1 interface is enabled.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 unassigned YES unset administratively down down

GigabitEthernet0/0/1 192.168.1.1 YES TFTP up up

Serial0/1/0 unassigned YES unset administratively down down

Serial0/1/1 unassigned YES unset administratively down down

The G0/1 interface is enabled because the modified running configuration included the **no shutdown** command.

Close configuration window

# Reflection Questions

* 1. What command do you use to copy a file from the flash to a USB drive?

Type your answers here.

copy flash:filename usb0:

* 1. What command do you use to copy a file from the USB flash drive to a TFTP server?

Type your answers here.

copy usb0:filename tftp:

# 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.

End of document

# Device Configs

# Router R1

R1# show run

Building configuration...

Current configuration : 3476 bytes

!

! Last configuration change at 20:51:21 UTC Wed Sep 25 2019

!

version 16.9

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

platform qfp utilization monitor load 80

no platform punt-keepalive disable-kernel-core

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

enable secret 5 $1$dWNi$ZFS7MSiKRPGn7B9nN6mPS/

!

no aaa new-model

!

no ip domain lookup

!

!

!

login on-success log

!

!

subscriber templating

!

!

multilink bundle-name authenticated

!

!

crypto pki trustpoint TP-self-signed-3903873913

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-3903873913

revocation-check none

rsakeypair TP-self-signed-3903873913

!

!

crypto pki certificate chain TP-self-signed-3903873913

certificate self-signed 01

30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

<output omitted>

quit

!

license udi pid ISR4221/K9 sn FGL23313183

no license smart enable

diagnostic bootup level minimal

!

spanning-tree extend system-id

!

!

redundancy

mode none

!

!

interface GigabitEthernet0/0/0

no ip address

shutdown

negotiation auto

!

interface GigabitEthernet0/0/1

ip address 192.168.1.1 255.255.255.0

negotiation auto

!

interface Serial0/1/0

!

interface Serial0/1/1

!

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

!

!

control-plane

!

banner motd ^C Authorized Users Only! ^C

!

line con 0

password 7 00071A150754

login

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

password 7 110A1016141D

login

!

end

# Switch S1

S1#show run

Building configuration...

Current configuration : 1498 bytes

!

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

ip address 192.168.1.11 255.255.255.0

!

ip default-gateway 192.168.1.1

ip http server

ip http secure-server

!

line con 0

password 045802150C2E

login

line vty 0 4

password 045802150C2E

login

line vty 5 15

password 045802150C2E

login

!

end