

Lab – Managing Device Configuration Files Using TFTP, Flash, and USB (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	G0/1	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: (Optional) Download TFTP Server Software

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

Part 4: Use TFTP to Back Up and Restore the Router Running Configuration

Part 5: Back Up and Restore Running Configurations Using Router Flash Memory

Part 6: (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 or flash memory. You can edit the file using a text editor and copy the new configuration back to a Cisco device.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(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 output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure 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.

Instructor Note: If time is limited, the lab can be divided up and performed over multiple sessions. For example, after building the network in Part 1, any combination of the remaining lab parts can be performed in any order.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and a TFTP server)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology
- USB flash drive (Optional)

Part 1: 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.

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

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

Step 2: Initialize and reload the router and switch.

Step 3: Configure basic settings for each device.

- Configure basic device parameters as shown in the Addressing Table.
- To prevent the router and switch from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.
- Assign **class** as the privileged EXEC encrypted password.
- Configure the passwords and allow login for console and vty lines using the **cisco** as the password.
- Configure the default gateway for the switch.
- Encrypt the clear text passwords.
- Configure the IP address, subnet mask, and default gateway for PC-A.

Step 4: Verify connectivity from PC-A.

- Ping from PC-A to S1.
- Ping from PC-A to R1.

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

Part 2: (Optional) Download TFTP Server Software

A number of free TFTP servers are available on the Internet for download. The Tftpd32 server is used with this lab.

Note: Downloading a TFTP server from a website requires Internet access.

Step 1: Verify availability of a TFTP server on PC-A.

- Click the **Start** menu and select **All Programs**.
- Search for a TFTP server on PC-A.
- If a TFTP server is not found, a TFTP server can be downloaded from the Internet.

Step 2: Download a TFTP server.

- Tftpd32 is used in this lab. This server can be downloaded from the following link:
http://tftpd32.jounin.net/tftpd32_download.html
- Choose the appropriate version for your system and install the server.

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

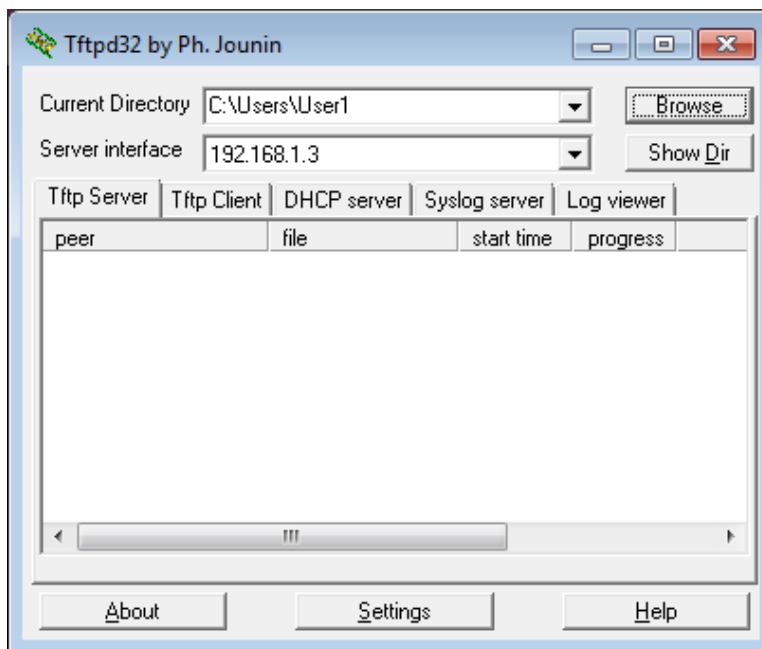
Step 1: Verify connectivity to switch S1 from PC-A.

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.

Step 2: Start the TFTP server.

- Click the **Start** menu and select **All Programs**.
- Find and select **Tftpd32** or **Tftpd64**. The following window displays that the TFTP server is ready.



- c. Click **Browse** to choose a directory where you have write permission, such as C:\Users\User1, or the Desktop.

Step 3: Explore the copy command on a Cisco device.

- a. 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.

```
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.
archive:        Copy from archive: file system
cns:            Copy from cns: file system
flash0:         Copy from flash0: file system
flash1:         Copy from flash1: 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
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
xmodem:        Copy from xmodem: file system
ymodem:        Copy from ymodem: file system
```

- b. 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: ?
```

```
archive:       Copy to archive: file system
flash0:        Copy to flash0: file system
flash1:        Copy to flash1: file system
flash:         Copy to flash: file system
ftp:           Copy to ftp: file system
http:          Copy to http: file system
https:         Copy to https: file system
idconf         Load an IDConf configuration file
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
syslog:        Copy to syslog: file system
system:        Copy to system: file system
tftp:          Copy to tftp: file system
tmpsys:        Copy to tmpsys: file system
xmodem:        Copy to xmodem: file system
ymodem:        Copy to ymodem: file system
```

Step 4: Transfer the running-config file from switch S1 to TFTP server on PC-A.

- a. 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
```

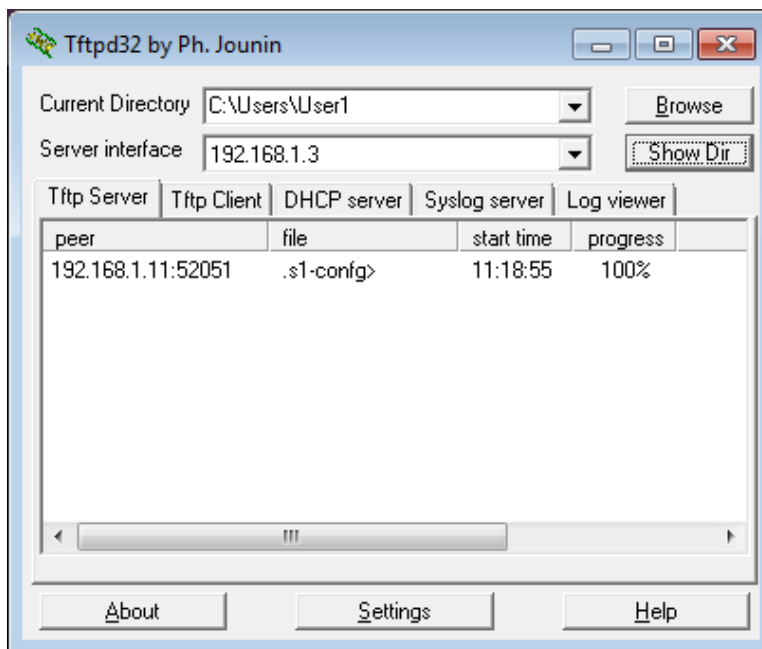
```
Destination filename [s1-confg]?
```

```
!!
```

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

```
S1#
```

The TFTP server also displays the progress during the transfer.



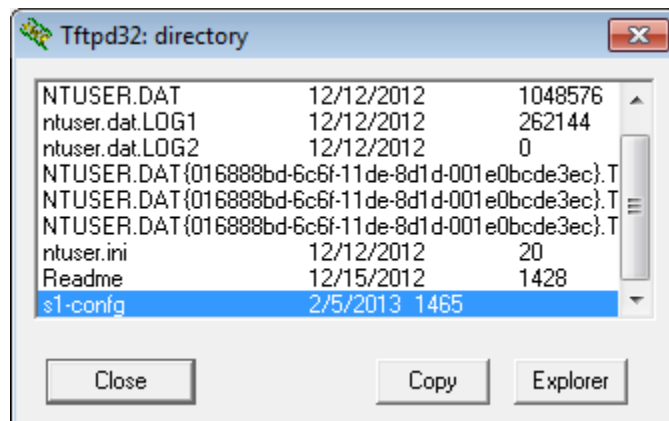
Note: If you do not have permission to write to the current directory that is used by the TFTP server, the following error message displays:

```
S1# copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [s1-config]?
%Error opening tftp://192.168.1.3/s1-config (Permission denied)
```

You can change the current directory in TFTP server by clicking **Browse** and choosing a different folder.

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

- b. In the Tftpd32 server window, click **Show Dir** to verify that the **s1-config** file has been transferred to your current directory. Click **Close** when finished.



Step 5: Create a modified switch running configuration file.

The saved running configuration file, **s1-config**, 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.

- Navigate to the TFTP directory on PC-A by using the file system of PC-A, and then locate the **s1-config** file. Open this file using a text editor program, such as WordPad.
- 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
```

- Save this file as a plain text file with a new filename, **Switch1-config.txt**, in this example.
Note: When saving the file, an extension, such as **.txt**, may be added to the filename automatically.
- In the Tftpd32 server window, click **Show Dir** to verify that the **Switch1-config.txt** file is located in the current directory.

Step 6: Upload running configuration file from TFTP server to switch S1.

- 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-config.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-config.txt
Destination filename [running-config]?
Accessing tftp://192.168.1.3/Switch1-config.txt...
Loading Switch1-config.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-  
config.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.

- b. 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>
```

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.

Part 4: 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.

Step 1: Verify connectivity to router R1 from PC-A.

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

Step 2: Transfer the running configuration from router R1 to TFTP server on PC-A.

- 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.
- Verify that the file has been transferred to the TFTP server.

Step 3: Restore the running configuration file to the router.

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

Part 5: Back Up and Restore Configurations Using Router Flash Memory

For the 1941 and other newer Cisco routers, there is no 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 CF 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.

Step 1: 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 hash (#) sign (at the end of the highlighted line) indicates that it is a bootable disk. The **flash0:** file system can also be referenced using the name **flash:**. The total size of the **flash0:** is 256 MB with 62 MB available. Currently the **flash1:** slot is empty as indicated by the — under the headings, Size (b) and Free (b). Currently **flash0:** and **nvr:** are the only available file systems.

```
R1# show file systems
```

```
File Systems:
```

Size (b)	Free (b)	Type	Flags	Prefixes
-	-	opaque	rw	archive:
-	-	opaque	rw	system:
-	-	opaque	rw	tmpsys:
-	-	opaque	rw	null:
-	-	network	rw	tftp:
* 260153344	64499712	disk	rw	flash0: flash:#
-	-	disk	rw	flash1:
262136	242776	nvr:	rw	nvr:
-	-	opaque	wo	syslog:
-	-	opaque	rw	xmodem:
-	-	opaque	rw	ymodem:
-	-	network	rw	rcp:
-	-	network	rw	http:
-	-	network	rw	ftp:
-	-	network	rw	scp:
-	-	opaque	ro	tar:

```
-          - network rw https:
-          - opaque ro  cns:
```

Where is the startup-config file located?

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.

Step 2: 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.

- a. 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)
```

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

```
R1# dir flash:
Directory of flash0:/

 1  drw-          0  Nov 15 2011 14:59:04 +00:00  ipsdir
<output omitted>
20  -rw-      67998028  Aug 7 2012 17:39:16 +00:00  c1900-universalk9-mz.SPA.152-
4.M3.bin
22  -rw-      2169    Feb 4 2013 23:57:54 +00:00  R1-running-config-backup
24  -rw-      5865    Jul 10 2012 14:46:22 +00:00  lpnat
25  -rw-      6458    Jul 17 2012 00:12:40 +00:00  lpIPSec

260153344 bytes total (64503808 bytes free)
```

- c. 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>
```

Step 3: Erase the startup configuration and reload the router.

Step 4: Restore the running configuration from flash.

- Verify the router has the default initial configuration.
- Copy the saved running-config file from flash to update the running-config.
Router# `copy flash:R1-running-config-backup running-config`
- 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
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	TFTP	administratively down	down
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down

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 GigabitEthernet0/1 interface to the saved file before updating the router running configuration file. This will be done in Part 6 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.

Part 6: (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. Two USB ports are available on the 1941 routers.

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

Note: Because some ISR G1 routers (1841, 2801, or 2811) use File Allocation Table (FAT) file systems, there is 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!
```

Step 1: Insert a USB flash drive into a USB port on the router.

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

R1#

```
* *Feb  5 20:38:04.678: %USBFLASH-5-CHANGE: usbflash0 has been inserted!
```

Step 2: Verify that the USB flash file system is available.

R1# `show file systems`

File Systems:

	Size (b)	Free (b)	Type	Flags	Prefixes
	-	-	opaque	rw	archive:
	-	-	opaque	rw	system:
	-	-	opaque	rw	tmpsys:
	-	-	opaque	rw	null:
	-	-	network	rw	tftp:
*	260153344	64512000	disk	rw	flash0: flash:#
	-	-	disk	rw	flash1:
	262136	244676	nvr	rw	nvr
	-	-	opaque	wo	syslog:
	-	-	opaque	rw	xmodem:
	-	-	opaque	rw	ymodem:
	-	-	network	rw	rcp:
	-	-	network	rw	http:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:
	-	-	opaque	ro	tar:
	-	-	network	rw	https:
	-	-	opaque	ro	cns:
	7728881664	7703973888	usbflash	rw	usbflash0:

Step 3: 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 usbflash0:
Destination filename [running-config]? R1-running-config-backup.txt
2198 bytes copied in 0.708 secs (3105 bytes/sec)
```

Step 4: 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 usbflash0:
Directory of usbflash0:/

 1  -rw-      16216  Nov 15 2006 09:34:04 +00:00  ConditionsFR.txt
 2  -rw-       2462  May 26 2006 21:33:40 +00:00  Nlm.ico
 3  -rw-    24810439  Apr 16 2010 10:28:00 +00:00  Twice.exe
 4  -rw-        71   Jun 4 2010 11:23:06 +00:00  AUTORUN.INF
 5  -rw-     65327  Mar 11 2008 10:54:26 +00:00  ConditionsEN.txt
 6  -rw-       2198   Feb 5 2013 21:36:40 +00:00  R1-running-config-backup.txt
```

```
7728881664 bytes total (7703973888 bytes free)
```

Step 5: Erase the startup-config and reload the router.

Step 6: Modify the saved file.

- Remove the USB drive from the router.

```
Router#  
*Feb  5 21:41:51.134: %USBFLASH-5-CHANGE: usbflash0 has been removed!
```

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

```
!  
interface GigabitEthernet0/1  
  ip address 192.168.1.1 255.255.255.0  
  no shutdown  
  duplex auto  
  speed auto  
!
```

- d. Remove the USB flash drive from the PC safely.

Step 7: Restore the running configuration file to the router.

- a. 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.

```
*Feb  5 21:52:00.214: %USBFLASH-5-CHANGE: usbflash1 has been inserted!
```

- b. List the files on the USB flash drive.

```
Router# dir usbflash1:  
Directory of usbflash1:/  
  
 1  -rw-          16216  Nov 15 2006 09:34:04 +00:00  ConditionsFR.txt  
 2  -rw-           2462  May 26 2006 21:33:40 +00:00  Nlm.ico  
 3  -rw-       24810439  Apr 16 2010 10:28:00 +00:00  Twice.exe  
 4  -rw-           71    Jun 4 2010 11:23:06 +00:00  AUTORUN.INF  
 5  -rw-       65327    Mar 11 2008 10:54:26 +00:00  ConditionsEN.txt  
 6  -rw-         2344    Feb 6 2013 14:42:30 +00:00  R1-running-config-backup.txt  
  
7728881664 bytes total (7703965696 bytes free)
```

- c. Copy the running configuration file to the router.

```
Router# copy usbflash1:R1-running-config-backup.txt running-config  
Destination filename [running-config]?  
2344 bytes copied in 0.184 secs (12739 bytes/sec)  
R1#
```

- d. Verify that the GigabitEthernet0/1 interface is enabled.

```
R1# show ip interface brief  


| Interface                  | IP-Address  | OK? | Method | Status                | Protocol |
|----------------------------|-------------|-----|--------|-----------------------|----------|
| Embedded-Service-Engine0/0 | unassigned  | YES | unset  | administratively down | down     |
| GigabitEthernet0/0         | unassigned  | YES | unset  | administratively down | down     |
| GigabitEthernet0/1         | 192.168.1.1 | YES | TFTP   | up                    | up       |
| Serial0/0/0                | unassigned  | YES | unset  | administratively down | down     |
| Serial0/0/1                | unassigned  | YES | unset  | administratively down | down     |


```

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

Reflection

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

copy flash:filename usbflash0:

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

copy usbflash0:filename tftp:

Router Interface Summary Table

Router Interface Summary				
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)

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.

Device Configs

Router R1

```
R1# show run
Building configuration...

Current configuration : 1283 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
```

```
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
```

```
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
  password 14141B180F0B
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 070C285F4D06
  login
  transport input all
!
scheduler allocate 20000 1000
!
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
```