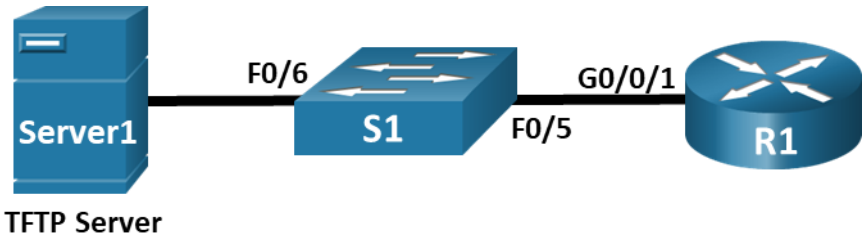
Packet Tracer - Use TFTP and Flash to Manage Configuration Files - Physical Mode

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
Server1	F0	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Cable 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

Background / Scenario

Cisco networking devices are often upgraded or replaced 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 back up configuration files and IOS images in production networks. A TFTP server is a centralized and secure method used to store file backups 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 back up purposes. A removable USB flash drive can also be used for back up purposes.

In this Packet Tracer Physical Mode (PTPM) activity, you will use TFTP server software to back up the running configuration of Cisco devices to the TFTP server. You will also back up the running configuration to Flash.

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will cable the network topology and configure basic settings, such as the interface IP addresses for R1, S1, and Server1.

Note: There are two PCs available so that you can establish a console connection from one PC to the router and the other PC to the switch. That way, you will not have to change the cables during the activity.

Step 1: Cable the network.

Cable the devices as shown in the topology. Connect a console cable from **PC1** to **R1**. Connect a console cable from **PC2** to **S1**.

Step 2: Use the CLI tab on the router to configure basic settings for the router.

a. Open a terminal to R1 from PC1. Click **PC1** > **Desktop** tab > **Terminal**, and then click **OK**.

b. Assign a device name to the router.

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

d. Assign **class** as the privileged EXEC encrypted password.

e. Assign **cisco** as the console password and enable login.

f. Assign **cisco** as the vty password and enable login.

g. Encrypt the plaintext passwords.

h. Create a banner that warns anyone accessing the device that Authorized Users Only are permitted.

i. Configure interfaces as listed in the **Addressing Table**.

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

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

Step 3: Use the CLI tab on the switch to configure basic settings for the switch.

a. Open a terminal to S1 from PC2. Click **PC2** > **Desktop** tab > **Terminal**, and then click **OK**.

b. Assign a device name to the switch.

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

d. Assign **class** as the privileged EXEC encrypted password.

e. Assign **cisco** as the console password and enable login.

f. Assign **cisco** as the vty password and enable login.

g. Encrypt the plaintext passwords.

h. Shut down all unused interfaces.

i. Configure interface VLAN 1 as specified in the **Addressing Table**.

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

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

Step 4: Using the Desktop tab, configure the IP addressing information for Server1 and verify connectivity with S1 and R1.

a. Ping from **Server1** to **S1**.

b. Ping from **Server1** to **R1**.

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

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

In this part, you will back up and restore the configuration for S1 to and from a TFTP server.

Step 1: Start the TFTP server application on Server1.

From the Services tab of **Server1**, turn on the TFTP application.

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 activity 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 the output of the **ping** command, 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: Explore the copy command on a Cisco device.

a. From the privileged EXEC mode prompt of **S1**, 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 ?
  flash:          Copy from flash: file system
  ftp:            Copy from ftp: file system
  running-config  Copy from current system configuration
  scp:            Copy from scp: file system
  startup-config  Copy from startup configuration
  tftp:           Copy from tftp: file system
S1# copy
```

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: ?
  ftp:            Copy to ftp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
  startup-config  Copy to startup configuration
  tftp:           Copy to tftp: file system
S1# copy flash:
```

Step 3: Transfer the running-config file from S1 to the TFTP server on Server1.

a. From the privileged EXEC mode of **S1**, enter the **copy running-config tftp:** command. Provide the remote host address of the TFTP server, 192.168.1.3. Press **Enter** to accept the 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]?

Writing running-config...!!
[OK - 1549 bytes]

1549 bytes copied in 0 secs
S1#
```

b. Check the directory in the TFTP application on **Server1** to verify that the file was transferred successfully. Click **Server1** > **Services** tab > **TFTP**. You should see the **S1-confg** file listed at the top of the **File** list.

Step 4: Modify the running configuration on the switch and copy the running configuration file from the TFTP server to the switch.

a. On **S1**, create a banner that warns anyone accessing the device that unauthorized access is prohibited.

b. From the privileged EXEC mode on **S1**, enter the **copy tftp running-config** command. Provide the remote host address of the TFTP server, 192.168.1.3. Enter the filename, **S1-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 []? S1-confg
Destination filename [running-config]?

Accessing tftp://192.168.1.3/S1-confg...
Loading S1-confg from 192.168.1.3: !
[OK - 1525 bytes]

1525 bytes copied in 0 secs
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

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

```
S1# show running-config
<output omitted>
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
ip default-gateway 192.168.1.1
!
banner motd ^CAuthorized Users Only! ^C
!
```

```
!
!
line con 0
 password 7 0822455D0A16
 login
!
<output omitted>
S1#
```

Note: Notice that the **banner motd** command was added after the running configuration was copied to the TFTP server. It is still present after the running configuration was copied back from the TFTP server.

If you do not erase the startup configuration, the 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 current running-config of the switch or router.

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

The backup and restore procedure from Part 2 can also be performed with a router. In Part 3, the running configuration file will be backed up and restored using a TFTP server.

Step 1: Transfer the running configuration from R1 to the TFTP server.

a. Open the **Terminal** program on **PC1** for **R1**.

b. 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 **R1-confg** as the default filename.

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

Step 2: Restore the running configuration file to the router.

Note: If you want to completely replace the current running-config with the one from the TFTP server, you must erase the router startup-config and reload the device. You will then need to configure the G0/0/1 interface address, so there is IP connectivity between the TFTP server and the router.

a. Erase the startup-config file on the router.

b. Reload the router.

Note: Your completion percentage will temporarily be lower until you restore the configuration.

c. Configure the **G0/0/1** interface on the router with an IP address 192.168.1.1. Wait until the Spanning Tree Protocol (STP) converges on **S1**.

d. Verify connectivity between the router and **Server1**. You may need to ping a few times before connectivity is re-established.

e. Use the **copy** command to transfer the **R1-confg** file from the TFTP server to the router. Use **running-config** as the destination.

f. Verify that the router has updated the running configuration. The router prompt should be changed back to **R1#** and your completion percentage should reflect that all your configurations are now restored.

Part 4: 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.

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 **flash0:** file system can also be referenced using the name **flash:**. The total size of the **flash0:** is approximately 3GB with about 2.5GB available. Currently **flash0:** and **nvram:** are the only available file systems.

Note: Verify that there is at least 1 MB (1,048,576 bytes) of free space. You can determine the size of flash memory and space available using the **show flash** or **dir flash:** command at the privileged EXEC prompt.

```
R1# show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
*   3249049600    2761893177     flash     rw  flash:
         29688         23590     nvram     rw  nvram:
```

Where is the startup-config file located?

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
Building configuration...
[OK]
R1#
```

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

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

    6  -rw-         732           <no date>  R1-running-config-backup
    3  -rw-   486899872           <no date>  isr4300-universalk9.03.16.05.S.155-3.S5-
ext.SPA.bin
    2  -rw-       28282           <no date>  sigdef-category.xml
    1  -rw-      227537           <no date>  sigdef-default.xml


3249049600 bytes total (2761893177 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

interface. 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.

a. Erase the startup-config file on the router.

b. Reload the router.

Note: Your completion percentage will temporarily be lower until you restore the configuration.

c. Verify the router has the default initial configuration.

Step 4: Restore the running configuration from flash.

a. Copy the saved running-config file from flash to update the running-config.

```
Router# copy flash: running-config
Source filename []? R1-running-config-backup
Destination filename [running-config]?

732 bytes copied in 0.416 secs (1759 bytes/sec)
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

b. Use the **show ip interface brief** command to view the status of the interfaces.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/1   192.168.1.1     YES manual administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
R1#
```

c. In Packet Tracer, the G0/0/1 interface will be administratively down. Enter interface configuration mode and reactivate the interface. Your completion percentage should now be 100%.