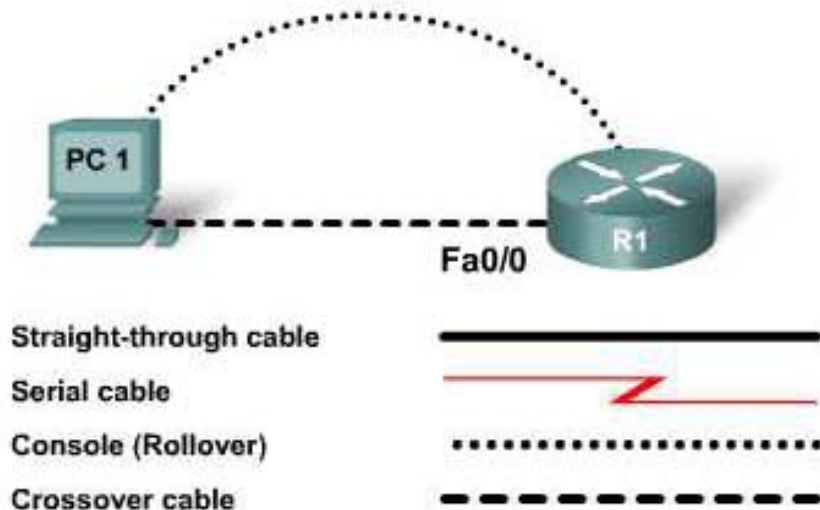


Lab 3.2.4 Installing a Cisco IOS Software Image



Device Designation	Device Name	Fast Ethernet Address	Subnet mask
R1	ACC-CPE-1	10.0.0.1	255.255.255.0
PC	PC1	10.0.0.254	255.255.255.0

Objectives

- Download the correct IOS and transfer the file to the Cisco router.
- Use TFTP to save and restore a Cisco IOS image.

640-802 CCNA Exam Objectives

This lab contains skills that relate to the following CCNA exam objectives:

- Manage IOS configuration files, including: save, edit, upgrade, restore.
- Verify router hardware and software operation using **show** and **debug** commands.

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

How is an understanding of the networking device IOS transfer to and from a TFTP server useful in network administration?

How will a network administrator know if the IOS was transferred and saved correctly?

Background / Preparation

This lab demonstrates backing up a Cisco router IOS image file to a TFTP server and uploading an IOS image to a router.

For recovery purposes, it is important to keep backup copies of router IOS images. These can be stored in a central location, such as a TFTP server, and retrieved if necessary.

Cisco IOS files have a specific name structure that reflects the platform, IOS version, feature set, and file type. It is strongly recommended that Cisco IOS image files not be renamed for any reason.

The configuration output used in this lab matches that of an 1841 series router. The same commands can be used with other Cisco routers but may produce slightly different output.

Task 1: Run and Configure the TFTP Server

Step 1: Configure network connectivity

NOTE: If the PC used in this lab is also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so that these can be restored at the conclusion of the lab.

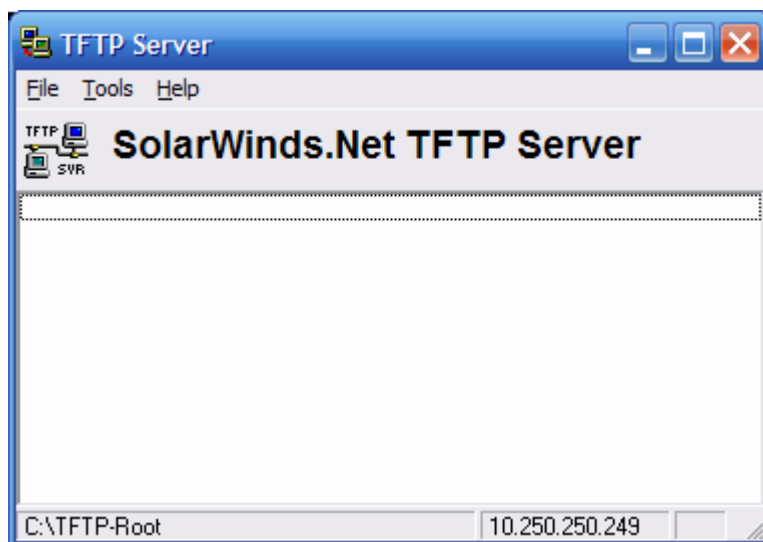
- Referring to the topology diagram, connect the console (or rollover) cable to the console port on the router and the other cable end to the host computer with a DB-9 or DB-25 adapter to the COM 1 port. Use a crossover cable to connect PC1 NIC interface to Router interface Fa0/1. Ensure that power has been applied to both the host computer and router.
- Using the IP address information from the table, configure computer PC1.
- On PC1 establish a console session to the router using HyperTerminal or TeraTerm.
- Configure the router hostname and interface as given in the table.
- Ping PC1 from the CLI prompt to verify connectivity between the router and the PC. Troubleshoot the configuration of the router and PC if connectivity is not verified.

Step 2: Start the TFTP server

- Check that a TFTP Server such as Solarwinds is installed on PC1. If not, see your instructor to arrange the installation. This software must be installed and running before the any file transfer can be initiated from the router.

NOTE: For convenience, PC1 is both used both for the terminal session and as a TFTP server in this lab. In a production environment, the server can be any appropriately configured and accessible secure computer on the network.

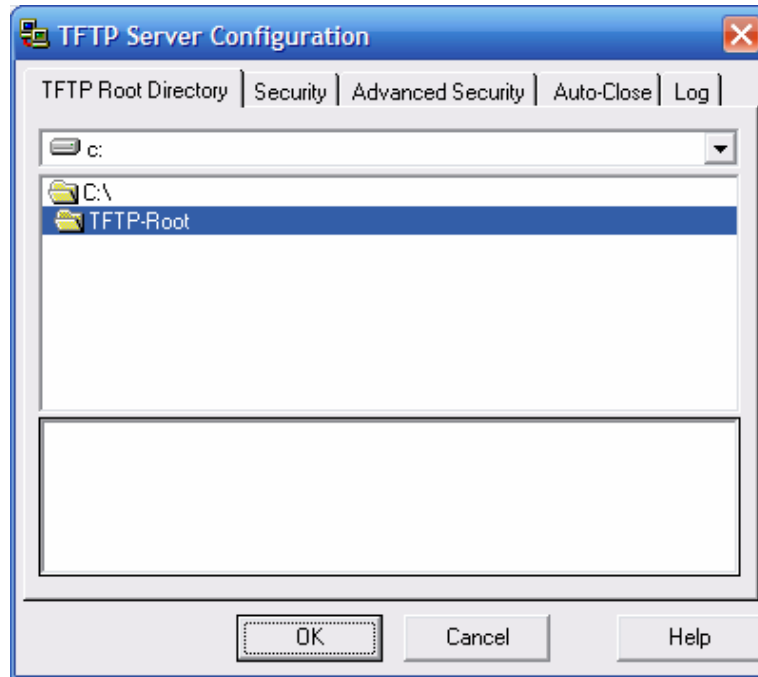
- Start the TFTP program (Solarwinds). The active TFTP Server window will appear as shown.



Step 3: Configure the TFTP server

- a. Go to the **File** menu and select **Configure**.
- b. Verify the following settings in the TFTP Server Configuration window by clicking the appropriate tabs.

Setting	Value
TFTP Root Directory	TFTP-Root
Security	Transmit and Receive Files
Advanced Security	<all IP addresses>
Auto-Close	Never
Log	Enable Log Requests to the Following File. Leave the default file.



- c. When finished, click **OK**.

Task 2: Back up the Current IOS

Step 1: Collect information to document the router

It is important to document the features and information about the router before transferring the IOS file, in case any recovery action has to be taken.

- a. Issue the **show flash** command.

Is there an IOS image file stored in flash? _____

Exact name of that file: _____

Size of that file: _____

Amount of flash that is available or unused? _____

What attributes can be identified from codes in the Cisco IOS filename?

Sample Output:

ACC-CPE-1# **show flash:**

```
-#- --length-- -----date/time----- path
1    13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2      1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3   4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4   833024 May 05 2007 21:30:42 +00:00 es.tar
5   1052160 May 05 2007 21:31:10 +00:00 common.tar
6     1038 May 05 2007 21:31:36 +00:00 home.shtml
7   102400 May 05 2007 21:32:02 +00:00 home.tar
8    491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9   1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10   398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
```

8679424 bytes available (23252992 bytes used)

- b. Issue the **show version** command and record the following information:

Configuration-register value: _____

Size of flash memory: _____

Is there at least 16 MB of flash? _____

Version number of boot ROM: _____

Is the boot ROM version 5.2 or later? _____

Sample Output:

```
ACC-CPE-1#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(1c),
RELEASE SO
FTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 25-Oct-05 17:10 by evmiller
```

```
ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
```

```
R1 uptime is 2 days, 12 hours, 29 minutes
System returned to ROM by reload at 21:21:02 UTC Fri Aug 24 2007
System image file is "flash:c1841-ipbase-mz.124-1c.bin"
```

```
Cisco 1841 (revision 7.0) with 114688K/16384K bytes of memory.
Processor board ID FTX1118X0AB
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)
```

```
Configuration register is 0x2102
```

Step 2: Copy IOS image to the TFTP server

- a. Before copying the files, verify that the TFTP server is running.
- b. Record the IP address of the TFTP server _____
- c. From the privileged EXEC mode, issue the **copy flash tftp** command. At the prompt, enter the filename for your system as reported in Step 1. To ensure accuracy, select the filename as shown in the **show flash:** output and copy and paste it at the source filename prompt. Then enter the IP address of the TFTP server. At the destination filename, press **Enter** to accept the name displayed.

Sample Output:

```
ACC-CPE-1#copy flash tftp
Source filename []? c1841-ipbase-mz.124-1c.bin
Address or name of remote host []? 10.0.0.254
Destination filename [c1841-ipbase-mz.124-1c.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
13937472 bytes copied in 37.627 secs (370412 bytes/sec)
```

Step 3: Verify the transfer to the TFTP server

- a. Verify a successful upload transfer. Open Log file c:\Program Files\SolarWinds\Free Tools\TFTP-Server.txt. Contents should be similar to the following example:

```
3/25/2007 12:29 :Receiving c1841-ipbase-mz.124-1c.bin from 10.0.0.1)
3/25/2007 12:29 :Received c1841-ipbase-mz.124-1c.bin from (10.0.0.1),
13937472 bytes
```

- b. Verify the flash image size in the TFTP server directory. Using Windows Explorer or My Computer, locate the TFTP root directory. Display file details and record the file size:

The file size shown in the **show flash:** command output should be the same as the file size of the file stored on the TFTP server. If the file sizes are not identical, check with your instructor.

Task 3: Restore or Upgrade the Current IOS

Step 1: Prepare to restore or update the IOS image

- a. Before copying the files, verify that the TFTP server is running and that the required IOS image file is in the TFTP root directory. Note the exact filename.
- b. Ping PC1 to confirm that connectivity between the router and the PC has been maintained.
- c. Confirm that the flash memory capacity is of sufficient size to hold the IOS image.

Which command is issued to confirm flash memory size?

Step 2: Copy the IOS image from the TFTP server

- a. From the privileged EXEC mode, issue the **copy tftp flash** command.
- b. At the prompt, enter the IP address of the TFTP server.
- c. Enter the filename for your system, as noted in Step 1.
- d. At the destination filename, press **Enter** to accept the name displayed.

NOTE: If prompted to overwrite an existing file with the same name, press **Enter** to confirm. Do not interrupt the process.

Sample Output:

```
ACC-CPE-1#copy tftp flash
Address or name of remote host []? 10.0.0.254
Source filename []? c1841-ipbase-mz.124-1c.bin
Destination filename [c1841-ipbase-mz.124-1c.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing tftp://10.0.0.254/ c1841-ipbase-mz.124-1c.bin...

Loading c1700-y-mz.122-11.T.bin from 10.0.0.254 (via FastEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13937472 bytes]
Verifying checksum... OK (0x9C8A)
13937472 bytes copied in 37.627 secs (370412 bytes/sec)
```

If successful, the checksum OK output is displayed. If the checksum fails, the IOS upload steps will need to be repeated.

Some older systems may require that flash be erased. If the `Erase flash: before copying?` prompt is confirmed, all files in flash will be removed. In contrast, other systems have sufficient capacity to store multiple files. If the router prompts to erase flash, output similar to below will occur before the new image is uploaded to flash.

Sample Output:

```
Erase flash: before copying? [confirm][Enter]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
...erased
Erase of flash: complete
```

Step 3: Test the restored IOS image

- Verify that the router IOS image is correct. Power cycle the router power and observe the startup process to confirm that there were no flash errors. If there are none, the router IOS should have started correctly.
- Further verify the IOS image in flash by issuing the `show version` command, which will show an output similar to this:

```
System image file is "flash: c1841-ipbase-mz.124-1c.bin"
```

Step 4: Clean up

Erase the configurations and reload the router. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), delete the IOS image file from the TFTP directory, reconnect the appropriate cabling and restore the TCP/IP settings.

Task 3: Reflection / Challenge

Step 1: Switch IOS Upgrade

As a challenge lab, research and list the steps required to back up the Cisco IOS image file from a switch to a TFTP server. In addition, list how to restore or upgrade the IOS image from the TFTP server to the switch.

Step 2: Non-operational Device

The performance of IOS image backup and upgrade for routers and switches as described in this lab presumes that the device has a current, fully operational IOS to allow the configuration of IP connectivity prior to copying the image file. However, there may be cases where the current IOS is corrupt or for some other reason the device will not boot with an operational IOS.

- Research and record the ROMMON process that enables a router to be configured and its IOS uploaded if the device has this problem.
- Research and record the X-Modem or similar process that enables the IOS of a switch to be uploaded using the serial (console) connection if the device has this problem.
