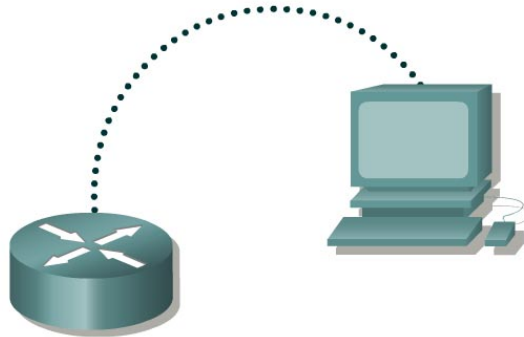




Lab 5.2.5 Managing IOS Images with TFTP



Router designation	Router name	Fast Ethernet 0 address	Subnet mask all addresses
Router 1	GAD	192.168.14.1	255.255.255.0

Straight-through cable	—————
Serial cable	————— <del> </del>
Console (Rollover)	
Crossover cable	- - - - -

Objective

- Backup a copy of a router IOS from flash to a TFTP server.
- Reload the backup IOS software image from a TFTP server into flash on a router.

Background/Preparation

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.

Cable a network similar to the one in the previous diagram. Any router that meets the interface requirements may be used. Possible routers include 800, 1600, 1700, 2500, 2600 routers, or a combination. Refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. The following steps are intended to be executed on each router unless specifically instructed otherwise.

Start a HyperTerminal session as performed in the Establishing a HyperTerminal session lab.

Step 1 Configure the Gadsden router

- If there are any difficulties configuring hostname, refer to the Configuring router passwords lab. If there are any difficulties configuring interfaces, refer to the Configuring host tables lab.
- Verify the routers configurations by performing a `show running-config` on each router. If not correct, fix any configuration errors and verify.

Step 2 Configure the workstation

- a. The configuration for the host connected to the Gadsden Router is:

IP Address	192.168.14.2
IP subnet mask	255.255.255.0
Default gateway	192.168.14.1

Step 3 Login to the router in user mode

- a. Connect to the Gadsden router and login.

Step 4 Collect information to document the new router

- a. Issue the `show version` command.
- b. What is the current value of the config-register? ____ 0x _____
- c. How much flash memory does this router have? _____
- d. Is there at least 4mb (4096K) of flash? _____
- e. What is the version number of boot ROM? _____
- f. Is the boot ROM version 5.2 or later? _____

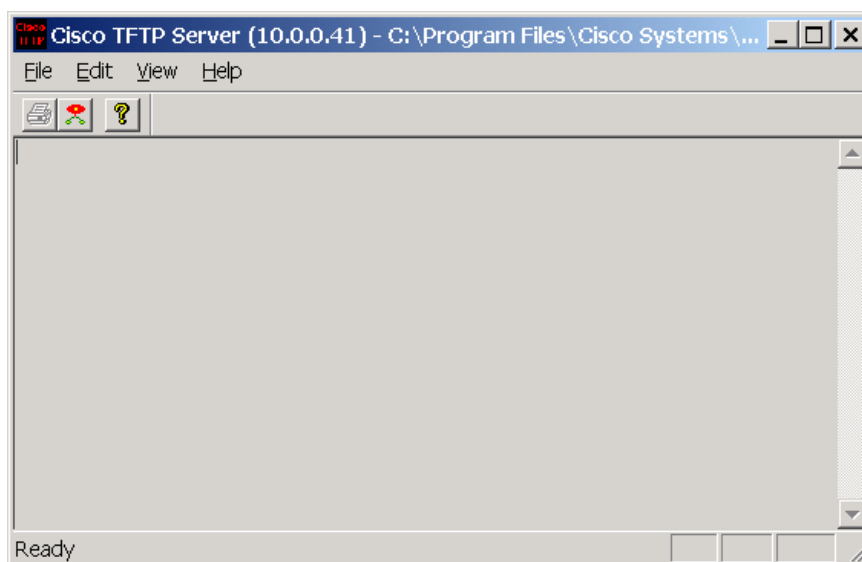
Step 5 Collect more information to document the new router

- a. Issue the `show flash` command.
- b. Is there a file already stored in flash? _____
- c. If so, what is the exact name of that file? _____
- d. How much of flash is available or unused? _____

Note: If there is a file in flash, it will probably need to be erased before a new one is loaded. That choice will be offered in the `copy tftp flash` command in a later step. However, it is possible to save a copy of that file with the command `copy flash tftp`. If there is a possibility of ever having to revert to that software version, follow the instructions in the Copy IOS to TFTP server section.

Step 6 Start and configure the Cisco TFTP Server

- a. Check with the instructor as to the IP address of the Cisco TFTP server.



Step 7 Verify connectivity

- Ping the TFTP server from the Gadsden router.

If the ping fails, review host and router configurations to resolve the problem.

Step 8 Copy IOS to TFTP server

- Before copying the files, verify that the TFTP server is running.

b. What is the IP address of the TFTP server? _____

- From the console session, enter **show flash**.

d. What is the name and length of the Cisco IOS image stored in flash?

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

Step 9 Write the configuration

- Write the configuration mode commands to specify what the IOS image should be loaded from:

Flash: _____

TFTP server: _____

ROM: _____ Will this be a full IOS image? _____

Step 10 Copy the IOS image to the TFTP server

- From the console session in the privileged EXEC mode, enter the **copy flash tftp** command. At the prompt enter the IP address of the TFTP server:

```
GAD#copy flash tftp
Source filename []? flash:c1700-y-mz.122-11.T.bin
Address or name of remote host []? 192.168.14.2
Destination filename [c1700-y-mz.122-11.T.bin]? y
```

After entering this command and answering the process requests, the student should see the following output on the console. Do not interrupt this process.

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
4284648 bytes copied in 34.012 secs (125975 bytes/sec)
```

Step 11 Verify the transfer to the TFTP server

- Check the TFTP server log file by clicking **View > Log File**. The output should resemble the following output:

```
Mon Sep 16 14:10:08 2002: Receiving 'c1700-y-mz.122-11.T.bin' in binary
mode
Mon Sep 16 14:11:14 2002: Successful.
```

- b. Verify the flash image size in the TFTP server directory. To locate it, click on **View > Options**. This will show the TFTP server root directory. It should be similar to the following, unless the default directories were changed:

```
C:\Program Files\Cisco Systems\Cisco TFTP Server
```

- c. Locate this directory using the File Manager. Look at the detail listing of the file. The file length in the `show flash` command should be the same file size as the file stored on the TFTP server. If the file sizes are not identical, check with the instructor.

Step 12 Copy the IOS image from the TFTP server

- a. Now that the IOS is backed up, the image must be tested and the IOS restored to the router. Verify again that the TFTP server is running, sharing a network with the router, and can be reached. Ping the TFTP server IP address.

- b. Record the IP address of the TFTP server. _____

- c. Copy from the privileged EXEC prompt.

```
GAD#copy tftp flash
```

```
Address or name of remote host []?192.168.14.2
```

```
Source filename []?c1700-y-mz.122-11.T.bin
```

```
Destination filename [c1700-y-mz.122-11.T.bin]? [Enter]
```

```
Accessing tftp://192.168.14.2/c1700-y-mz.122-11.T.bin...
```

```
Erase flash: before copying? [confirm] [Enter]
```

```
Erasing the flash filesystem will remove all files! Continue?
```

```
[confirm] [Enter]
```

```
Erasing device...
```

```
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
```

```
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
```

```
...erased
```

```
Erase of flash: complete
```

```
Loading c1700-y-mz.122-11.T.bin from 192.168.14.2 (via
```

```
FastEthernet0):!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
[OK - 4284648 bytes]
```

```
Verifying checksum... OK (0x9C8A)
```

```
4284648 bytes copied in 26.584 secs (555739 bytes/sec)
```

- d. The router may prompt to erase flash. Will the image fit in available flash? _____

- e. If the flash is erased, what happened on the router console screen as it was doing so?

- f. What is the size of the file being loaded? _____ Do not interrupt the process.

- g. What happened on the router console screen as the file was being downloaded?

- h. Was the verification successful? _____

- i. Was the whole operation successful? _____

Step 13 Test the restored IOS image

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

System image file is "flash:c1700-y-mz.122-11.T.bin"

Upon completion of the previous steps, logoff by typing `exit`. Turn the router off.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If “class” does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

```
System configuration has been modified. Save? [yes/no]:
```

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm]
```

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

Press **Enter**.

The router is ready for the assigned lab to be performed.

Router Interface Summary					
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2	Interface #5
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	
In order to find out exactly how the router is configured, look at the interfaces. This will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.					