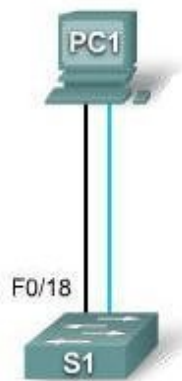# Lab 2.5.2: Managing Switch Operating System and Configuration Files

Topology Diagram

Addressing Table

Device	Hostname	Interface	IP Address	Subnet Mask	Default Gateway
PC1	Host-A	NIC	172.17.99.21	255.255.255.0	172.17.99.1
S1	ALSwitch	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Create and save a basic switch configuration
- Set up a TFTP server on the network
- Back up the switch Cisco IOS software to a TFTP server and then restore it
- Back up the switch configuration to a TFTP server
- Configure a switch to load a configuration from a TFTP server
- Upgrade the Cisco IOS software from a TFTP server
- Recover the password for a 2960 switch (2900 series)

Scenario

In this lab, you will examine and configure a standalone LAN switch. Although a switch performs basic functions in its default out-of-the-box condition, there are a number of parameters that a network administrator should modify to ensure a secure and optimized LAN. This lab introduces you to the basics of switch configuration.

Task 1: Cable and Initialize the Network

Step 1: Cable a network.

Cable a network that is similar to the one in the topology diagram. Create a console connection to the switch. If necessary, refer to Lab 1.3.1. The output shown in this lab is from a 2960 switch. If you use other switches, the switch outputs and interface descriptions may appear different.

Step 2: Clear the configuration on the switch.

Set up a console connection to the switch and erase the existing configuration. If necessary, refer to lab 2.5.1, Appendix 1.

Step 3: Create a basic configuration.

Use the following commands to configure a hostname, line access passwords, and the enable secret password.

```
Switch#configure terminal
Switch(config)#hostname ALSwitch
ALSwitch(config)#line con 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#exit
```

Create VLAN 99 and assign user ports to this VLAN using the commands shown below. Return to privileged EXEC mode when finished.

```
ALSwitch(config)#vlan 99
ALSwitch(config-vlan)#name user
ALSwitch(config-vlan)#exit
ALSwitch(config)#interface vlan 99
ALSwitch(config-if)#ip address 172.17.99.11 255.255.255.0
ALSwitch(config-if)#exit
ALSwitch(config)#interface fa0/18
ALSwitch(config-if)#switchport access vlan 99
ALSwitch(config-if)#end
ALSwitch#
```

Step 4: Configure the host attached to the switch.

Configure the host to use the IP address, mask, and default gateway identified in the addressing table at the beginning of the lab. This host acts as the TFTP server in this lab.

Step 5: Verify connectivity.

To verify that the host and switch are correctly configured, ping the switch IP address that was configured for VLAN 99 from the host.

Was the ping successful? _____

If the answer is no, troubleshoot the host and switch configurations.

Task 2: Starting and Configuring the TFTP Server

Step 1: Start up and configure the TFTP server.

The TFTP server that is shown in this lab is the SolarWinds server, available at
http://www.solarwinds.com/products/freetools/free_tftp_server.aspx. If this URL is out of date, then use
your favorite search engine and search for "solar winds free tftp download".

It may not be like the one that is used in this lab. Please check with your instructor for the operating
instructions for the TFTP server used in place of the Solar Winds TFTP server.

Start the server on the host **Start > All Programs > SolarWinds 2003 Standard Edition > TFTP Server.**

The server should start up and acquire the IP address of the Ethernet interface, and use the C:\TFTP-
Root directory by default.

When the TFTP server is running and shows the correct address configuration on the workstation, copy
the Cisco IOS file from the switch to the TFTP server.

Step 2: Verify connectivity to the TFTP server.

Verify that the TFTP server is running and that it can be pinged from the switch.

What is the IP address of the TFTP server? _____

```
ALSwitch#ping 172.17.99.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.21 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006
ms
ALSwitch#
```

Task 3: Save the Cisco IOS File to a TFTP Server

Step 1: Identify the Cisco IOS filename.

Determine the exact name of the image file that is to be saved. From the console session, enter **show flash**.

```
ALSwitch#show flash
Directory of flash:/
    2  -rwx         556   Mar 8 1993 22:46:45 +00:00  vlan.dat
    5  drwx         192   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX
    32514048 bytes total (26527232 bytes free)
```

Note: If the file is in a subdirectory, as is the case in the output shown above, you cannot initially see the filename. To see the Cisco IOS filename, use the **cd** command to change the switch working directory to the Cisco IOS directory:

```
ALSwitch#cd flash:/c2960-lanbase-mz.122-25.FX
ALSwitch#show flash
Directory of flash:/c2960-lanbase-mz.122-25.FX/
    6  drwx        4160   Mar 1 1993 00:03:36 +00:00  html
  368  -rwx     4414921   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX.bin
  369  -rwx         429   Mar 1 1993 00:04:53 +00:00  info

    32514048 bytes total (26527232 bytes free)
```

What is the name and size of the Cisco IOS image stored in flash? _____

_____

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

_____

From privileged EXEC mode, enter the **copy flash tftp** command. At the prompts, first enter the filename of the Cisco IOS image file, then the IP address of the TFTP server. Make sure to include the complete path if the file is in a subdirectory.

```
ALSwitch#copy flash tftp
Source filename []?c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin
Address or name of remote host []? 172.17.99.21
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? [enter]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
4414921 bytes copied in 10.822 secs (407958 bytes/sec)
ALSwitch#
```

Step 2: Verify the transfer to the TFTP server.

Verify the transfer to the TFTP server by checking the log file. On the SolarWinds TFTP server, the transfer can be verified from the command window, as shown in the following figure:
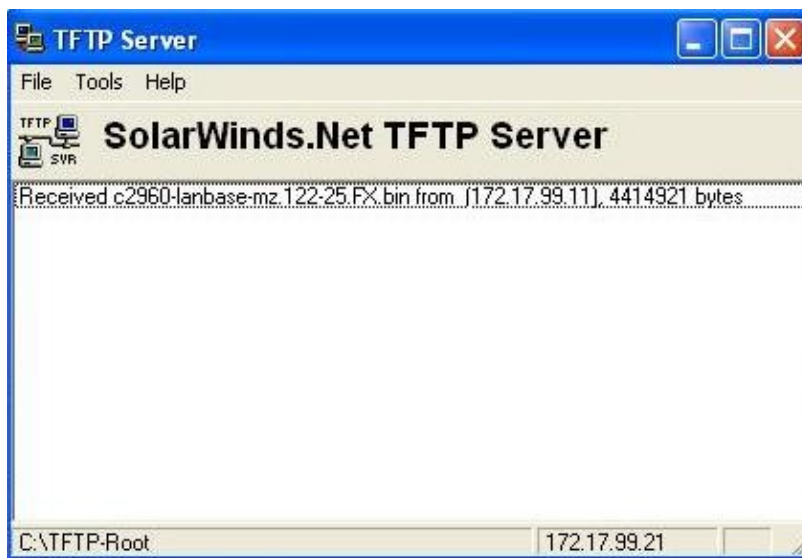
Verify the flash image size in the server root directory. The path for the root server is shown on the server command window—C:\TFTP-root.

Locate this directory on the server using the File Manager and 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 in size, check with your instructor.

Task 4: Restore the Cisco IOS File to the Switch from a TFTP Server

Step 1: Verify connectivity.

Verify that the TFTP server is running, and ping the TFTP server IP address from the switch.

What is the IP address of the TFTP server? _____

```
ALSwitch#ping 172.17.99.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.21 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006
ms
ALSwitch#
```

If the pings fail, troubleshoot the switch and server configurations.

Step 2: Identify Cisco IOS filename on the server and the entire path name of the destination for the switch.

What is the name of the file on the TFTP server root directory that will be copied to the switch?

_____

What is the destination path name for the Cisco IOS file on the switch?
_____

What is the IP address of the TFTP server? _____

**Step 3: Upload the Cisco IOS software from the server to the switch.**

Note: It is important that this process is not interrupted.

In privileged EXEC mode, copy the file from the TFTP server to flash memory.

```
ALSwitch#copy tftp flash
Address or name of remote host []? 172.17.99.21
Source filename []? c2960-lanbase-mz.122-25.FX.bin
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? c2960-lanbase-
mz.122-25.F
X/c2960-lanbase-mz.122-25.FX.bin
%Warning:There is a file already existing with this name
Do you want to over write? [confirm] [enter]
Accessing tftp://172.17.99.21 /c2960-lanbase-mz.122-25.FX.bin...
Loading c2960-lanbase-mz.122-25.FX.bin from 172.17.99.21  (via
Vlan1):!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4414921 bytes]

4414921 bytes copied in 43.964 secs (100421 bytes/sec)
ALSwitch#
```

The server output screen should look something like the following:
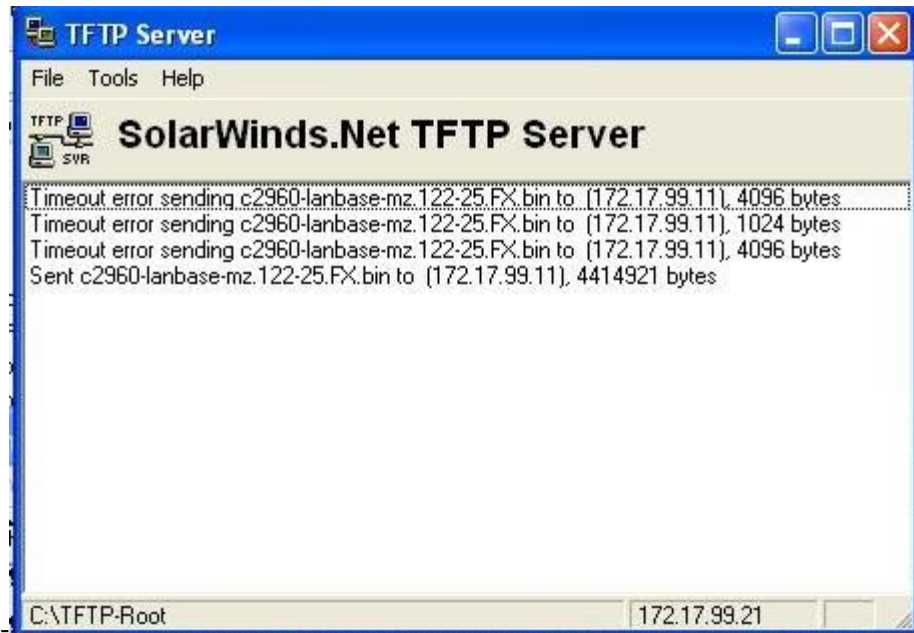
Is the file size of the uploaded file the same as that of the saved file on the TFTP root directory? _____

Step 4: Test the restored Cisco IOS image.

Verify that the switch image is correct. To do this, reload the switch and observe the startup process to confirm that there are no flash errors. If there are none, the Cisco IOS software on the switch should have started correctly. To further verify the Cisco IOS image in flash, issue the **show version** command, which will show output similar to the following:

```
System image file is "flash:c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin"
```

Task 5: Back Up and Restore a Configuration File from a TFTP Server

Step 1: Copy the startup configuration file to the TFTP server.

Verify that the TFTP server is running and that it can be pinged from the switch.

What is the IP address of the TFTP server? _____

In privileged EXEC mode, enter the **copy running-config startup-config** command to make sure that the running configuration file is saved to the startup configuration file.

```
ALSwitch#copy running-config startup-config
Destination filename [startup-config]?[enter] Building configuration...
[OK]
```

Back up the saved configuration file to the TFTP server with the command **copy startup-config tftp**. At the prompt, enter the IP address of the TFTP server:

```
AlSwitch#copy startup-config tftp
Address or name of remote host []? 172.17.99.21
Destination filename [alswitch-confg]? [enter]
!!
1452 bytes copied in 0.445 secs (3263 bytes/sec)#
```

Step 2: Verify the transfer to the TFTP server.

Verify the transfer to the TFTP server by checking the command window on the TFTP server. The output should look similar to the following:

```
Received alswitch-confg from (172.17.99.11), 1452 bytes
```

Verify that the alswitch-confg file is in the TFTP server directory C:\TFTP-root.

Step 3: Restore the startup configuration file from the TFTP server.

To restore the startup configuration file, the existing startup configuration file must be erased and the switch reloaded.

```
AlSwitch#erase nvram
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
AlSwitch#
AlSwitch#reload
Proceed with reload? [confirm] [enter]
```

When the switch has reloaded, you must reestablish connectivity between the switch and the TFTP server before the configuration can be restored. To do this, configure VLAN 99 with the correct IP

address and assign port FastEthernet 0/18 to VLAN 99. When you are finished, return to privileged EXEC mode.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#ip address 172.17.99.11 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/18
Switch(config-if)#switchport access vlan 99
Switch(config-if)#end
Switch#
```

After VLAN 99 is up, verify connectivity by pinging the server from the switch.

```
Switch#ping 172.17.99.21
```

If the ping is unsuccessful, troubleshoot the switch and server configuration. Restore the configuration from the TFTP server with the **copy tftp startup-config** command.

Note: It is important that this process is not interrupted.

```
Switch#copy tftp startup-config
Address or name of remote host []? 172.17.99.21
Source filename []? alswitch-confg
Destination filename [startup-config]? [enter]
Accessing tftp://172.17.99.21 /alswitch-confg...
Loading alswitch-confg from 172.17.99.21  (via Vlan99): !
[OK - 1452 bytes]
1452 bytes copied in 9.059 secs (160 bytes/sec)
Switch#
00:21:37: %SYS-5-CONFIG_NV_I: Nonvolatile storage configured from
tftp://172.17.99.21 /alswitch-confg by console
Switch#
```

Was the operation successful? _____

Step 4: Verify the restored startup configuration file.

In privilege EXEC mode, reload the switch again. When the reload is complete, the switch should show the ALSwitch prompt. Type the command **show startup-config** to verify that the restored configuration is complete, including the line access and enable secret passwords.

Task 6: Upgrade the Cisco IOS Software of the Switch

Note: This lab requires that a combination of a Cisco IOS image and the HTML archive (tar) file be placed in the default TFTP server directory by the instructor or student. This file should be downloaded by the instructor from the Cisco Connection online software center. In this lab, the c2960-lanbase-mz.122-25.FX.tar file is referenced for instructional purposes only. This has the same filename stem as the current image. However, for the purpose of the lab, assume that this is an update. The Cisco IOS software update release includes the binary image and new HTML files to support changes to the web interface.

This lab also requires that there is a saved copy of the current configuration file as a backup.

Step 1: Determine the current boot sequence for the switch.

Use the **show boot** command to display the settings of the boot environment variables.

```
ALSwitch#show boot
BOOT path-list : flash:c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
NVRAM/Config file
     buffer size:   65536
ALSwitch#
```

Determine if there is sufficient memory to hold multiple image files:

```
ALSwitch#sh flash
Directory of flash:/
    2  -rwx        616   Mar 1 1993 06:39:02 +00:00  vlan.dat
    4  -rwx          5   Mar 1 1993 10:14:07 +00:00  private-
config.text
    5  drwx        192   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX
  370  -rwx       1281   Mar 1 1993 10:14:07 +00:00  config.text

32514048 bytes total (26524672 bytes free)
ALSwitch#
```

Note that on this platform, only about 6 MB is in use, and approximately 26.5 MB is free, so there is plenty of memory for multiple images. If there is insufficient space for multiple images, you must overwrite the existing image with the new one, so make sure there is a backup of the existing Cisco IOS file on the TFTP server before beginning the upgrade.

Step 2: Prepare for the new image.

If the switch has enough free memory as shown in the last step, use the **rename** command to rename the existing Cisco IOS file to the same name with the .old extension:

```
ALSwitch#rename flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.old
```

Verify that the renaming was successful:

```
ALSwitch#dir flash:/c2960-lanbase-mz.122-25.FX/

    Directory of flash:/c2960-lanbase-mz.122-25.FX/

    6  drwx       4160   Mar 1 1993 00:03:36 +00:00  html
  368  -rwx    4414921   Mar 1 1993 03:26:51 +00:00  c2960-lanbase-
mz.122-25.FX.old
  369  -rwx        429   Mar 1 1993 00:04:53 +00:00  info
32514048 bytes total (26524672 bytes free)
```

Use the **delete** command to remove existing HTML files. Including an ***** in the command instead of a specific filename deletes all files in the directory.

```
ALSwitch#delete flash:/c2960-lanbase-mz.122-25.FX/html/*
```

Step 3: Extract the new Cisco IOS image and HTML files into flash memory.

Enter the following to place the new Cisco IOS image and HTML files into the flash memory target directory:

```
ALSwitch#archive tar /x tftp://172.17.99.21/c2960-lanbase-mz.122-
25.FX.tar flash:/c2960-lanbase-mz.122-25.FX
```

Step 4: Associate the new boot file.

Enter the **boot** command with the name of the new image filename at the global configuration mode prompt. When you are finished, return to privileged EXEC mode and save the configuration.

```
ALSwitch(config)#boot system flash:/c2960-lanbase-mz.122-25.FX/c2960-
lanbase-mz.122-25.FX.bin
ALSwitch(config)# end
ALSwitch#copy running-config startup-config
```

Step 5: Restart the switch.

Restart the switch using the **reload** command to see if the new Cisco IOS software loaded. Use the **show version** command to see the Cisco IOS filename.

What was the name of the Cisco IOS file the switch booted from? _____

_____ _____

Was this the proper filename? _____

If the Cisco IOS filename is now correct, remove the backup file from flash memory using this command from privileged EXEC mode:

```
ALSwitch(config)#delete flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-
mz.122-25.FX.old
```

Task 7: Recover Passwords on the Catalyst 2960

Step 1: Reset the console password.

Have a classmate change the console and vty passwords on the switch. Save the changes to the startup-config file and reload the switch.

Now, without knowing the passwords, try to gain access to the switch.

Step 2: Recover access to the switch

Make sure that a PC is connected to the console port and a HyperTerminal window is open. Turn the switch off. Turn it back on while holding down the **MODE** button on the front of the switch at the same time that the switch is powered on. Release the **MODE** button after the SYST LED stops blinking and stays on.

The following output should be displayed:

```
The system has been interrupted prior to initializing the flash
filesystem. The following commands will initialize the flash
filesystem, and finish loading the operating system software:
flash_init
```

```
load_helper
boot
```

To initialize the file system and finish loading the operating system, enter the following commands:

```
switch:flash_init
switch:load_helper
switch:dir flash:
```

Note: Do not forget to type the colon (:) after **flash** in the command **dir flash:**.

Type **rename flash:config.text flash:config.old** to rename the configuration file. This file contains the password definition.

Step 3: Restart the system.

Type the **boot** command to boot the system. Enter **n** when prompted to continue the configuration dialog, and **y** when asked if you want to terminate auto-install.

To rename the configuration file with its original name, type the command **rename flash:config.old flash:config.text** at the privileged EXEC mode prompt.

```
Switch# rename flash:config.old flash:config.text
Destination filename [config.text]? [enter]
```

Copy the configuration file into memory:

```
Switch#copy flash:config.text system:running-config
Destination filename [running-config][enter]
```

The configuration file is now reloaded. Change the old unknown passwords as follows:

```
ALSwitch#configure terminal
ALSwitch(config)#no enable secret
ALSwitch(config)#enable secret class
ALSwitch(config)#line console 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#exit
ALSwitch(config)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#end
ALSwitch#copy running-config startup-config
Destination filename [startup-config]?[enter] Building configuration...
[OK]
ALSwitch#
```

Terminate your console connection and then reestablish it to verify that the new passwords have been configured. If not, repeat the procedure.

Once the steps are completed, log off by typing **exit**, and turn all the devices off. Then remove and store the cables and adapter.