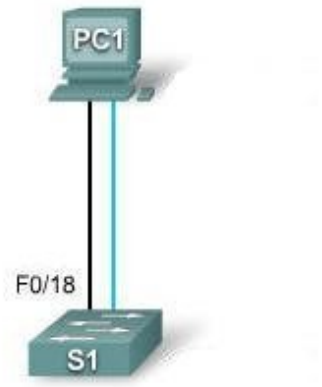
Lab 2.5.3: Managing Switch Operating System and Configuration Files Challenge

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 Cisco 2960 switch (2900 series)

Scenario

In this lab, you will explore file management and password recovery procedures on a Cisco Catalyst switch.

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. Then, 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. Erase the configuration on the switch.

Step 3: Create a basic configuration.

Configure the switch with the following hostname and access passwords. Then enable secret passwords on the switch.

Hostname	Console Password	Telnet Password	Command Password
ALSwitch	cisco	cisco	class

Create VLAN 99. Assign IP address 172.17.99.11 to this interface. Assign the FastEthernet 0/18 port to this VLAN.

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. 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 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 was used in the development of this lab is the SolarWinds server, available at http://www.solarwinds.com.

The labs in your classroom may be using a different TFTP server. If so, check with your instructor for the operating instructions for the TFTP server in use.

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

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

Step 2: Verify connectivity to the TFTP server.

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

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

Step 1: Identify the Cisco IOS filename.

Determine the exact name of the image file that is to be saved.

Note that if the file is in a subdirectory, you cannot initially see the filename. To see the Cisco IOS filename, first change the switch working directory to the Cisco IOS directory.

Examine the output from the switch and then answer these questions.

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

_____

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

_____

Step 2: In privileged EXEC mode, copy the image file to the TFTP server.

Step 3: Verify the transfer to the TFTP server.

Verify the transfer to the TFTP server by checking the log file. With the SolarWinds TFTP server, you can verify the transfer from the command window or from the server log file at:

C:\Program Files\SolarWinds\2003 Standard Edition\TFTP-Server.log.

Verify that the flash image size is in the server root directory. The path for the root server is shown on the server command window:

C:\TFTP-root

Use the File Manager to locate this directory on the server and look at the detail listing of the file. The file length displayed by the **show flash** command should be the same size as the size of 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.

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

Step 2: Identify the 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 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.

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 image and observe the startup process. Confirm that there are no flash errors. If there are no errors, the Cisco IOS software on the switch should have started correctly. To further verify the Cisco IOS image in flash, issue the command that will show the Cisco IOS version.

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. Save the current configuration.

Back up the saved configuration file to the TFTP server.

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, first erase the existing startup configuration file, and then reload the switch.

When the switch has been reloaded, you must reestablish connectivity between the switch and the TFTP server before the configuration can be restored. To do this, reconfigure VLAN 99 with the correct IP address and assign port Fast Ethernet 0/18 to that VLAN (refer to Task 1).

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

If the ping is unsuccessful, troubleshoot the switch and server configuration. Restore the configuration from the TFTP server by copying the alswitch-confg file from the server to the switch.

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

Was the operation successful? _____

Step 4: Verify the restored startup configuration file.

In privilege EXEC mode, reload the router again. When the reload is complete, the switch should show the ALSwitch prompt. Examine the running configuration to verify that the restored configuration is complete, including the 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 file 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 and check memory availability.

Determine if there is sufficient memory to hold multiple image files. Assume that the new files require as much space as the current files in flash memory.

Is there sufficient memory capacity to store additional Cisco IOS and HTML files? _____

Step 2: Prepare for the new image

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

Verify that the renaming was successful.

As a precaution, disable access to the switch HTML pages, and then remove the existing HTML files from flash memory.

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
```

Re-enable the HTTP server on the switch.

Step 4: Associate the new boot file.

Enter the boot system command with the new image filename at the configuration mode prompt, and then save the configuration.

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 file name? _____

If the Cisco IOS filename is now correct, remove the backup file (with the .old extension) from flash memory.

Task 7: Recover Passwords on the Catalyst 2960

Step 1: Reset the console password.

Have a classmate change the console, vty, and enable secret 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 privilege EXEC mode on the switch.

Step 2: Recover access to the switch.

Detailed password recovery procedures are available in the online Cisco support documentation. In this case, they can be found in the troubleshooting section of the Catalyst 2960 Switch Software Configuration Guide. Follow the procedures to restore access to the switch.

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

Appendix 1: Password Recovery for the Catalyst 2960

Recovering a Lost or Forgotten Password

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

These sections describes how to recover a forgotten or lost switch password:

- **Procedure with Password Recovery Enabled**
- **Procedure with Password Recovery Disabled**

You enable or disable password recovery by using the **service password-recovery** global configuration command. Follow the steps in this procedure if you have forgotten or lost the switch password.

Step 1 Connect a terminal or PC with terminal-emulation software to the switch console port.

Step 2 Set the line speed on the emulation software to 9600 baud.

Step 3 Power off the switch. Reconnect the power cord to the switch and, within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; then release the **Mode** button.

Several lines of information about the software appear with instructions, informing you if the password recovery procedure has been disabled or not.

- If you see a message that begins with this:

```
The system has been interrupted prior to initializing the flash
file system.
The following commands will initialize the flash file system
```

proceed to the "Procedure with Password Recovery Enabled" section, and follow the steps.

- If you see a message that begins with this:


```
The password-recovery mechanism has been triggered, but is
currently disabled.
```

proceed to the "Procedure with Password Recovery Disabled" section, and follow the steps.

Step 4 After recovering the password, reload the switch:

```
Switch> reload

Proceed with reload? [confirm] y
```

Procedure with Password Recovery Enabled

If the password-recovery mechanism is enabled, this message appears:

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

flash_init
load_helper
boot
```

Step 1 Initialize the flash file system:

```
switch: flash_init
```

Step 2 If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.

Step 3 Load any helper files:

```
switch: load_helper
```

Step 4 Display the contents of flash memory:

```
switch: dir flash:
```

The switch file system appears:


```
Directory of flash:
   13  drwx         192   Mar 01 1993 22:30:48  c2960-lanbase-
mz.122-25.FX
   11  -rwx        5825   Mar 01 1993 22:31:59  config.text
   18  -rwx         720   Mar 01 1993 02:21:30  vlan.dat

16128000 bytes total (10003456 bytes free)
```

Step 5 Rename the configuration file to config.text.old.

This file contains the password definition.

```
switch: rename flash:config.text flash:config.text.old
```

Step 6 Boot the system:

```
switch: boot
```

You are prompted to start the setup program. Enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

Step 7 At the switch prompt, enter privileged EXEC mode:

```
Switch> enable
```

Step 8 Rename the configuration file to its original name:

```
Switch# rename flash:config.text.old flash:config.text
```

Step 9 Copy the configuration file into memory:

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

Press **Return** in response to the confirmation prompts.

The configuration file is now reloaded, and you can change the password.

Step 10 Enter global configuration mode:

```
Switch# configure terminal
```

Step 11 Change the password:

```
Switch (config)# enable secret password
```

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 12 Return to privileged EXEC mode:

```
Switch (config)# exit
Switch#
```

Step 13 Write the running configuration to the startup configuration file:

```
Switch# copy running-config startup-config
```

The new password is now in the startup configuration.

Note This procedure is likely to leave your switch virtual interface in a shutdown state. You can see which interface is in this state by entering the **show running-config** privileged EXEC command. To re-enable the interface, enter the **interface vlan** *vlan-id* global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the **no shutdown** command.

Step 14 Reload the switch:

```
Switch# reload
```

Procedure with Password Recovery Disabled

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
```



```
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default
configuration (y/n)?
```

Caution Returning the switch to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup switch and VLAN configuration files.

- If you enter **n** (no), the normal boot process continues as if the **Mode** button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:

```
Press Enter to continue........
```

- If you enter **y** (yes), the configuration file in flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

Step 1 Elect to continue with password recovery and lose the existing configuration:

```
Would you like to reset the system back to the default
configuration (y/n)? Y
```

Step 2 Load any helper files:

```
Switch: load_helper
```

Step 3 Display the contents of flash memory:

```
switch: dir flash:
```

The switch file system appears:

```
Directory of flash:
13  drwx         192   Mar 01 1993 22:30:48 c2960-lanbase-
mz.122-25.FX.0

16128000 bytes total (10003456 bytes free)
```


Step 4 Boot the system:

```
Switch: boot
```

You are prompted to start the setup program. To continue with password recovery, enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

Step 5 At the switch prompt, enter privileged EXEC mode:

```
Switch> enable
```

Step 6 Enter global configuration mode:

```
Switch# configure terminal
```

Step 7 Change the password:

```
Switch (config)# enable secret password
```

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 8 Return to privileged EXEC mode:

```
Switch (config)# exit
Switch#
```

Step 9 Write the running configuration to the startup configuration file:

```
Switch# copy running-config startup-config
```

The new password is now in the startup configuration.

Note This procedure is likely to leave your switch virtual interface in a shutdown state. You can see which interface is in this state by entering the **show running-config** privileged EXEC command. To re-enable the interface, enter the **interface vlan** *vlan-id* global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the **no shutdown** command.

Step 10 You must now reconfigure the switch. If the system administrator has the backup switch and VLAN configuration files available, you should use those.

