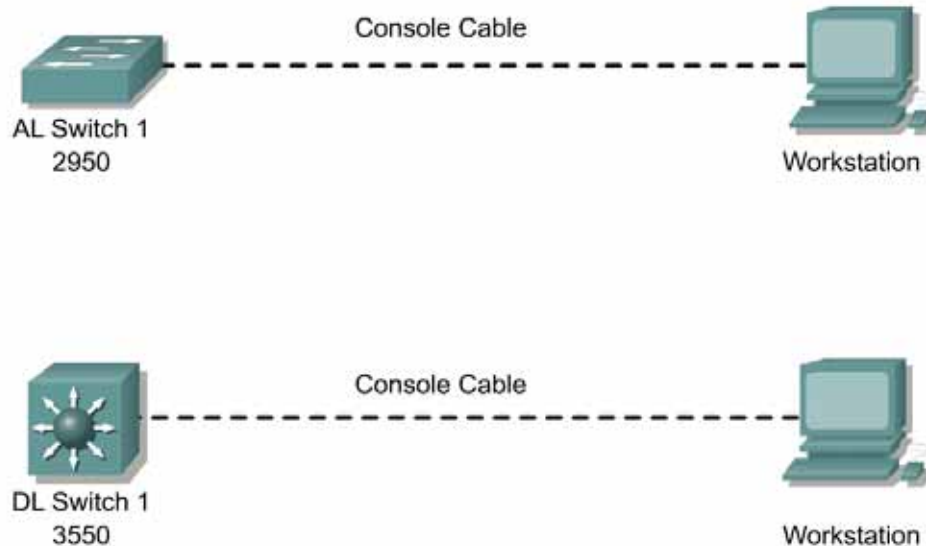


Lab 1.2.9.3 Catalyst 2950T and 3550 Series Password Recovery



Objective

Recover passwords while retaining configurations for the Cisco Catalyst 2950T and 3550 series of Ethernet switches.

Scenario

Access to a network device may be denied because of an incorrect password and sometimes there is no password documentation available for reference. The device will usually contain configurations that should not be changed. Therefore, it is very important to learn the password recovery procedure for devices in the network. This lab will cover the password recovery procedure for the Cisco Catalyst 2950T and 3550 series of Ethernet switches. The password recovery procedure for the 2950T and the 3550 switch is the same.

Step 1

Establish a HyperTerminal console connection with a 2950T or a 3550 switch. Set the privileged EXEC mode secret password to **lostpassword**, save the configuration to Flash memory, and exit from both privileged and user mode.

```
Switch>enable
Switch#configure terminal
Switch(config)#enable secret lostpassword
Switch(config)#exit
Switch#copy running-config startup-config
Switch#exit
```

Log into the switch again. Access to the user mode should be successful. Attempt to access the privileged mode using the password **cisco**. The privileged mode cannot be accessed without knowing the correct password.

Step 2

Begin the password recovery procedure by unplugging the switch power cord.

Step 3

Hold down the **MODE** button located on the left side of the front panel while reconnecting the power cord to the switch.

On the 2950T switch, release the **MODE** button after instructions similar to the sample output appear. On the 3550 switch, release the **MODE** button after the FastEthernet 0/1 light goes out.

<Output omitted>

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

```
flash_init
load_helper
boot
```

Switch:

Step 4

Finish initializing flash by issuing the **flash_init** command.

```
switch: flash_init
Initializing Flash...
flashfs[0]: 14 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 3972096
flashfs[0]: Bytes available: 3769344
flashfs[0]: flashfs fsck took 6 seconds.
...done initializing flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
switch:
```

Step 5

Load the default configuration by issuing the **load_helper** command. This is similar to changing the configuration register on a router to boot into the ROM Monitor mode. Then issue the **dir flash:** command to identify the configuration file that contains the password definition. A sample output is as follows.

```
switch: load_helper
switch: dir flash:
Directory of flash:/
2      -rwx  2253443  <date>                c2950-i6q412-mz.121-6.EA2c.bin
```

```

3      -rwx  269      <date>          env_vars
4      -rwx  109      <date>          info
6      -rwx  698      <date>          config.text
7      drwx  640      <date>          html
18     -rwx  109      <date>          info.ver

3767808 bytes available (3973632 bytes used)
switch:

```

The config.text file contains the password definitions.

Step 6

Rename the original configuration file containing the password definitions and then reboot the switch. The switch will not find the config.text file and will continue with the default boot process. The **Enter** key may need to be pressed a few times during the boot process. The switch will go into the setup mode and present the System Configuration Dialog prompt. Respond with no at the prompt.

```

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

<Output omitted>

--- System Configuration Dialog ---

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

Press RETURN to get started!

Switch>

```

This enables access into the switch and bypasses any passwords.

Step 7

Enter the privileged EXEC mode and restore the name of the configuration file to its original. Then copy the configuration file to running-config to retain any previously entered switch configurations.

```

Switch>enable
Switch#rename flash:config.old flash:config.text
Destination filename [config.text]? <press ENTER>
Switch#copy flash:config.text system:running-config
Destination filename [running-config]? <press ENTER>
698 bytes copied in 0.576 secs
Switch#

```

Step 8

All passwords can now be reassigned and documented without losing any switch configuration from the original configuration file. Be sure to save the configuration after changing the passwords.

```

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password cisco
Switch(config)#enable secret class
Switch(config)#line con 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login

```

```
Switch(config-line)#exit
Switch(config)#exit
Switch#copy running-config startup-config
Destination filename [startup-config]? <press ENTER>
Building configuration...
[OK]
Switch#
```

The process of bypassing passwords to access a 2950T or 3550 series switch is now complete. Passwords have also been changed while retaining all other switch configurations that may have been previously entered. The new passwords should be documented and placed in a secure location for future reference.