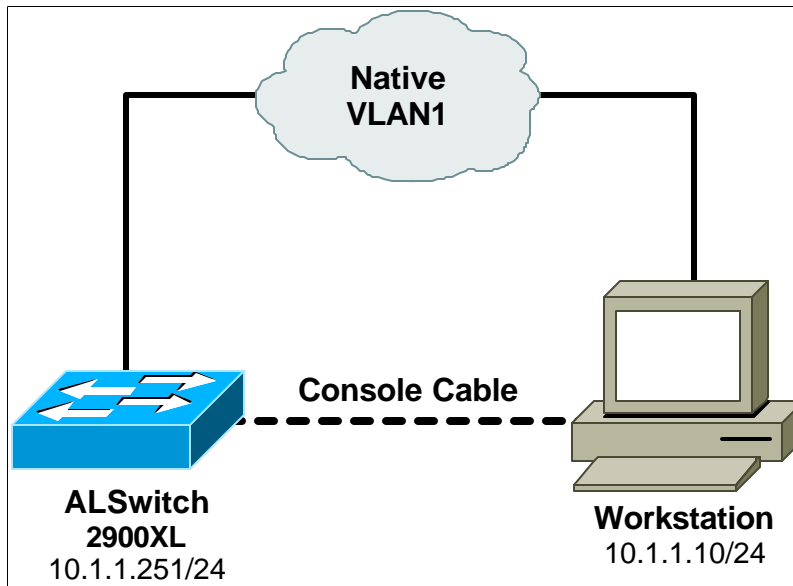


Lab 3.3.4.2: Catalyst 2900 Password Recovery



Objective:

Regain control of a Cisco Catalyst 2900 Ethernet switch after you have lost the passwords.

Scenario:

You have just taken a job at a company that uses Catalyst 2900 Ethernet switches in their IDFs. The person that managed the network before you did not leave any documentation containing the passwords. Perform password recovery on the Catalyst 2900 - change the user exec password to "cisco" and the privileged exec mode password to "class".

Lab Tasks:

1. First, configure your 2900 switch to the diagram above. You can skip this step if you already have the Lab 3.2.3 (2900 initial setup) configured.

```
Switch>enable
Switch#
```

Set the switch name.

```
Switch#config terminal
Switch(config)#host ALSwitch
ALSwitch(config)#
```

Have someone set the passwords in the steps below. Tell them to not use the standard passwords, but to make up some of their own. Make sure they do not tell you what they have set them to.

```
ALSwitch(config)#enable password somethingdifferent
ALSwitch(config)#line con 0
```

```

ALSwitch(config-line)#password somethingelse
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 15
ALSwitch(config-line)#password somethingelse
ALSwitch(config-line)#login

ALSwitch(config)#interface vlan 1
ALSwitch(config-if)#ip address 10.1.1.251 255.255.255.0

```

Configure the IP address of your workstation to 10.1.1.10/24

2. Attempt to telnet into the Catalyst switch. You will not be able to get in because you do not know the passwords.

The Catalyst 2900 series of switches deals with password recovery in a similar fashion to other IOS devices. The idea is to move the current startup config out of the way so that the switch loads the default config, which has no passwords. Once the switch is up and running, we get into enable mode, move the saved startup config into running config, modify the passwords and then move it back into the startup config.

3. Make sure you are connected to the console port and power off your Catalyst 2900 switch.

Hold down the "MODE" button on the front of the Catalyst 2900 switch at the same time that you power on the switch. You can let go of the "MODE" button a second or two after the LED light above port 1 is no longer lit.

Watch the start-up message. When you see:

```

C2900XL Boot Loader (C2900-HBOOT-M) Version 12.0(5)XU, RELEASE
SOFTWARE (fc1)
Compiled Mon 03-Apr-00 17:20 by swati
starting...
Base ethernet MAC Address: 00:02:b9:9a:85:80
Xmodem file system is available.

```

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

```

switch:

Type: **flash_init** and then type **load_helper**

```

switch: flash_init
Initializing Flash...
flashfs[0]: 109 files, 3 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 3612672
flashfs[0]: Bytes used: 2776064
flashfs[0]: Bytes available: 836608
flashfs[0]: flashfs fsck took 8 seconds.

```

```
...done Initializing Flash.  
Boot Sector Filesystem (bs:) installed, fsid: 3  
Parameter Block Filesystem (pb:) installed, fsid: 4  
switch: load_helper
```

This is similar to changing the config-register on a router to boot into rom-monitor mode.

Now, list the contents of the switch's flash memory:

```
switch: dir flash:  
Directory of flash:/  
  
 2    -rwx  1644046    <date>                c2900XL-c3h2s-mz-120.5-  
XU.bin  
 3    -rwx   105961    <date>                c2900XL-diag-mz-120.5-XU  
 4    drwx   6784     <date>                html  
111  -rwx    286     <date>                env_vars  
112  -rwx    648     <date>                config.text  
  
836608 bytes available (2776064 bytes used)
```

We want to rename the **config.txt** file to a temporary name - config.old.

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

Now reboot the switch:

```
Switch: boot
```

When the switch reboots, it will prompt you to enter the Configuration Dialog. Answer no.

When the switch finishes the boot up sequence, enter privileged exec mode and rename the temporary file back into the original name or the startup-config.

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

Now we want to copy the startup-config (config.text) to our running-config.

```
Switch#copy flash:config.text system:running-config  
Destination filename [running-config]? (Press Enter)  
648 bytes copied in 1.206 secs (648 bytes/sec)  
ALSwitch#
```

Because we are currently in privileged mode, we can re-assign the passwords:

```
ALSwitch(config)#enable password class  
ALSwitch(config)#line con 0  
ALSwitch(config-line)#password cisco  
ALSwitch(config-line)#line vty 0 15  
ALSwitch(config-line)#password cisco  
ALSwitch(config-line)#login
```

Now save your changes.

```
ALSwitch#copy running-config startup-config
```

Your password change is now complete.