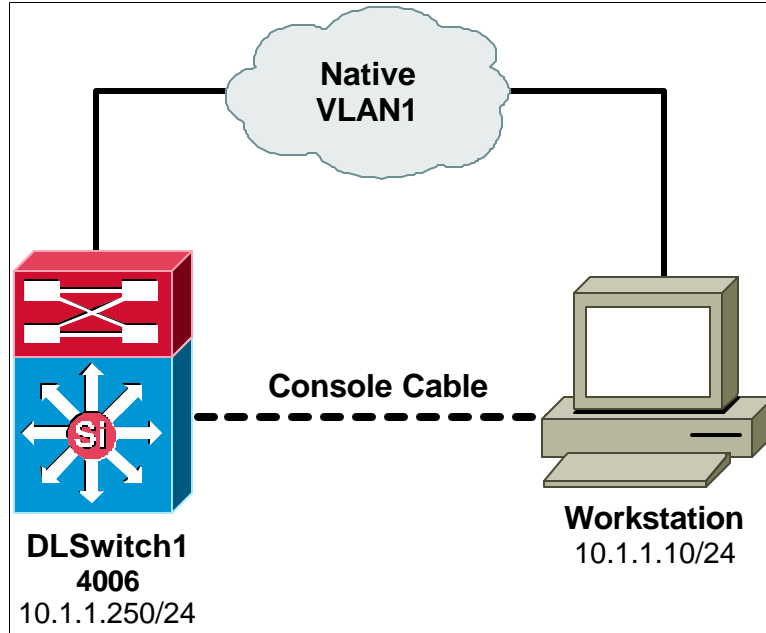


### Lab 3.3.4.1: Catalyst 4000 Password Recovery



#### Objective:

Regain control of a Cisco Catalyst 4000 Ethernet switch after you have lost the passwords.

#### Scenario:

You have just taken a job at a company that uses Catalyst 4000 Ethernet switches for their backbone. The person who managed the network before you did not leave any documentation containing the passwords. Perform password recovery on the Catalyst 4000 - change the user exec password to "cisco" and the privileged exec mode password to "class".

#### Lab Tasks:

1. First, configure your 4000 switch to the diagram above. You can skip this step if you already have the Lab 3.1.3 (4000 initial setup) configured.

```
Console> enable
Console> (enable) set system name DLSwitch1
System name set.
DLSwitch1> (enable)
```

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.

```
DLSwitch1> (enable) set password
Enter old password: (Because you do not currently have a password, just hit enter)
Enter new password:
```

Retype new password:  
Password changed.

```
DLSwitch1> (enable) set enablepass  
Enter old password: (Because you do not currently have a password, just hit enter)  
Enter new password:  
Retype new password:  
Password changed.
```

```
DLSwitch1> (enable) set interface sc0 10.1.1.250 255.255.255.0  
DLSwitch1> (enable) set interface sc0 1
```

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 4000 series of switches deals with password recovery much differently than the other Cisco IOS based devices.

To sum it up, the Catalyst 4000 series switch does not require a password when logging in from the console port during the first 30 seconds after it has booted up. A password is still required during this time if you are trying to log in via telnet.

This is a great example of why physical security of your devices is so important. Anyone who can get access to your console port will have the ability to change your passwords.

3. Make sure you are connected to the console port and power off your Catalyst 4000 switch. Read through the rest of this step, as you will have to complete it within 30 seconds after the switch comes back up. It is important to power off your switch, as a warm reset will not allow you to enter without a password, it must be a full power off.

Turn on the power to your Catalyst 4000 switch by plugging in the power cords.

Watch the start-up messages. As soon as you see:

```
Cisco Systems, Inc. Console
```

```
Enter password:
```

Hit enter immediately. Remember, you will not need a password to log in.

```
DLSwitch1>
```

Enter privileged mode. You will also not need a password so just hit enter.

```
DLSwitch1> enable  
DLSwitch1> (enable)
```

Now you will reset the password using the **set password** and **set enablepass** commands. When prompted for the current passwords, hit enter.

```
DLSwitch1> (enable) set password  
Enter old password: (just hit enter)
```

```
Enter new password: ("cisco" hit enter)
Retype new password: ("cisco" hit enter)
Password changed.
```

```
DLSwitch1> (enable) set enablepass
Enter old password: (just hit enter)
Enter new password: ("class" hit enter)
Retype new password: ("class" hit enter)
Password changed.
```

Your password change is now complete.

If you were fast enough, your new passwords are part of the saved config. The rest of the switches configuration is unchanged.

Why is the Catalyst 4000 password recovery better or worse than other IOS based devices?

---

---

---

---