BANNER MOD !! and Password Setting for switch ..

Asst. Prof. Ashwini Mathur

Different Banners

Cisco IOS routers and Switch support a number of banners, here they are:

- **MOTD banner:** the “message of the day” banner is presented to everyone that connects to the router.
- **Login banner:** this one is displayed just before the authentication prompt.
- **Exec banner:** displayed before the user sees the exec prompt.
- **Incoming banner:** used for users that connect through reverse telnet.

A *banner* is a message that is presented to someone using the router. The type of banner you configure determines when this message is shown to the user. You can configure three main types of banners on a Cisco router.

- **Message of the Day (MOTD):** This type of logon message has been around for a long time on Unix and mainframe systems. The idea was to display a temporary notice to users, such as issues with system availability.

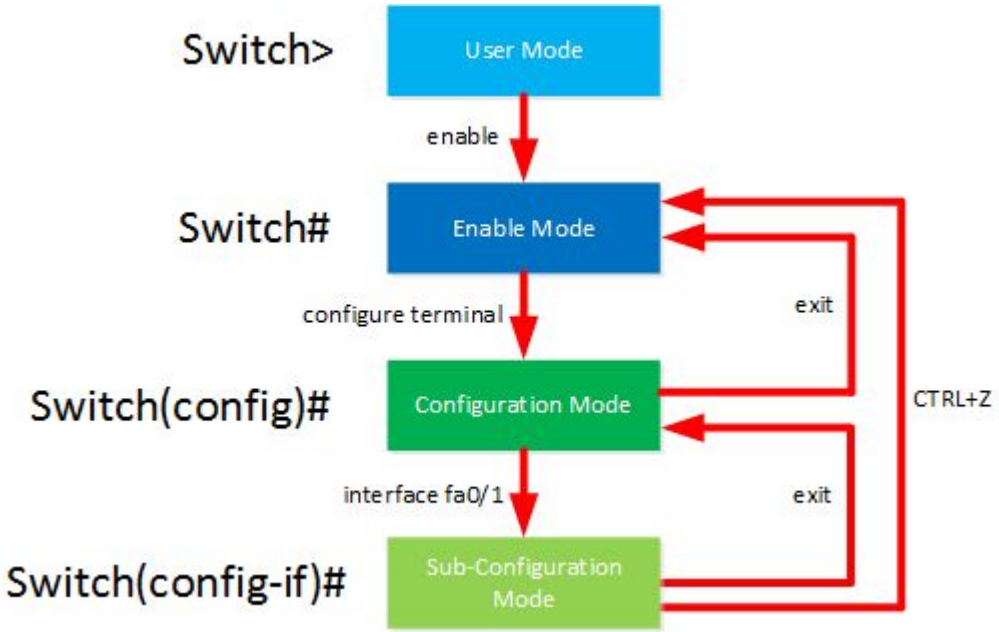
  However, because it displays when you connect to the device prior to login, most network administrators now use it to display legal notices regarding access to the router, such as *unauthorized access to this device is prohibited and violators will be prosecuted to the full extent of the law*.

- **Login:** This banner displays before login to the system but after the MOTD banner is displayed. Typically, this banner displays a permanent message to users.

- **Exec:** This banner displays after the login is completed when the connecting user enters User EXEC mode. Whereas the other banners are seen by all people who attempt to connect to the router, this banner is seen only by users who successfully log on to the router. This banner can be used to post reminders to network administrators.

```
Switch1>enable
Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#banner motd #
Enter TEXT message. End with the character '#'.
This device is for authorized personnel only.
If you have not been provided with permission to
access this device - disconnect at once.
#
Switch1(config)#banner login #
Enter TEXT message. End with the character '#'.
*** Login Required. Unauthorized use is prohibited ***
#
Switch1(config)#banner exec #
Enter TEXT message.  End with the character '#'.
*** Ensure that you update the system configuration ***
*** documentation after making system changes.      ***
#
Switch1(config)#exit
```

```
Switch1 Con0 is now available
Press RETURN to get started!
This device is for authorized personnel only.
If you have not been provided with permission to
access this device - disconnect at once.
*** Login Required.  Unauthorized use is prohibited ***
User Access Verification
Password:
*** Ensure that you update the system configuration ***
*** documentation after making system changes.      ***
Switch1>
```


Switch>
User Mode
enable
Switch#
Enable Mode
configure terminal
exit
Switch(config)#
Configuration Mode
CTRL+Z
interface fa0/1
exit
Switch(config-if)#
Sub-Configuration Mode

Password Setting ...

Table 1 Default Password and Privilege Levels

Feature	Default Setting
Enable password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.
Enable secret password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	No password is defined.

The enable password is used when you move from User EXEC mode to Privileged EXEC mode on a Cisco device. This condition gives you security on your switch because Privileged EXEC mode is where all the dangerous commands are, including Global Configuration mode. To set an enable password you would use the following command:

```
Switch1>enable
Switch1#configure terminal
Switch1(config)#enable password mypass
```

This command creates an enable password that is stored in the configuration file. To view this password, show your running configuration using the following command:

```
Switch1>enable
Password:
Switch1#show running-config | include enable password
enable password mypass
```

The problem with the enable password is that it is stored in plain text in the configuration file. Anyone with access to your configuration file can read your password without any trouble. Cisco's solution to this problem was to create a new type of password called the *secret password*.

When you configure both an enable and a secret password, the secret password is the password that will be used to change from User EXEC mode to Privileged EXEC mode, instead of the weaker enable password. The following code sets both passwords for your switch:

```
Switch1>enable
Switch1#configure terminal
Switch1(config)#enable password mypass
Switch1(config)#enable secret mysecret
```

To see this in your configuration, use the following command:

```
Switch1>enable
Password:
Switch1#show running-config | include enable
enable secret 5 $1$BSX4$FZp.ZFvYSAGUEDn8dvr140
enable password mypass
```