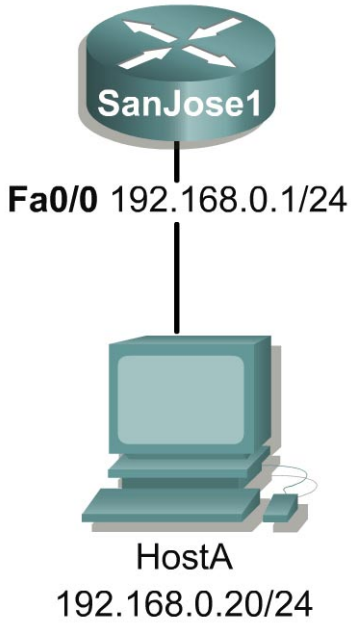
# Lab 11.3.2 AAA Authorization and Accounting




## Objective

In this lab, the student will use the **exec-timeout** command to control the amount of time before an idle telnet or console session is terminated.

The student will also be introduced to the Cisco IOS AAA security authorization and accounting features. These can be implemented to limit the EXEC commands that a user is permitted to use.

## Scenario

The International Travel Agency (ITA) is becoming concerned about the security of its routers and switches. A prototype of Cisco's login security features including AAA and Cisco Secure is to be created.

## Step 1

Before beginning this lab, it is recommended that the routers be reloaded after erasing their startup configurations. Configure the router's FastEthernet interface and the host's IP address, subnet mask and default gateway. This prevents problems that may be caused by residual configurations.

Build and configure the network according to the diagram. Use the following commands to configure SanJose1:

```
SanJose1(config)#line con 0
SanJose1(config-line)#exec-timeout 0 0
SanJose1(config-line)#password cisco
SanJose1(config-line)#logging synchronous
SanJose1(config-line)#enable password cisco
SanJose1(config-line)#line vty 0 4
```

```
SanJose1(config-line)#login
SanJose1(config-line)#password cisco
SanJose1(config-line)#exec-timeout 0 0
SanJose1(config-line)#line aux 0
SanJose1(config-line)#exec-timeout 0 0
SanJose1(config-line)#login
SanJose1(config-line)#password cisco
```

The **exec-timeout 0 0** commands configure the amount of time a router will wait before terminating an idle EXEC session. The first number specifies the number of minutes, and the second number specifies the number of seconds. Therefore, the command **exec-timeout 0 45** would configure the idle timer to 45 seconds. Using two zeros, as shown, will configure the router so that the EXEC sessions never time out. Such a configuration is a security risk, because unattended sessions will remain open and a malicious user could potentially exploit this. While configuring **exec-timeout 0 0** is uncommon on production routers, it is a useful configuration when performing lab exercises.

It is possible to set different timeout values for each of the CON, VTY, and AUX sessions. The default timeout for all three of these lines is 10 minutes.

## Step 2

The AAA feature can be used to limit a user's options based on the username/password entered during login.

By default, there are three privilege levels on the router, as follows:

| Privilege Level | Result |
|---|---|
| 1 | User level only (prompt is router>), the default level for login |
| 15 | Privileged level (prompt is router#), the level after going into enable mode |
| 0 | Seldom used, but includes five commands: disable, enable, exit, help, and logout |

Levels 2 through 14 can be defined by "moving" commands from one of the default privilege levels to the new level. Configuring custom privilege levels can involve significant administration on the router.

To determine the current privilege level, type the show privilege command as follows:

```
SanJose1#show privilege
Current privilege level is 15
```

1. While in user EXEC mode, what is the privilege level?

---

2. While in privileged EXEC mode, what is the privilege level?

---

Configure custom privilege levels, by adding the following entries to the authentication database on SanJose1:

```
SanJose1(config)#username cisco0 privilege 0 password cisco0
SanJose1(config)#username cisco15 privilege 15 password cisco15
SanJose1(config)#username cisco7 privilege 7 password cisco7
```

```
SanJose1(config)#aaa new-model
SanJose1(config)#aaa authentication login default local
```

When login in as **cisco0**, a user will only have access to the disable, enable, exit, help, and logout commands. When login in as **cisco15**, a user will have regular EXEC privilege access. The **cisco7** login will be used to custom define which commands a user will have access to.

It is important to realize that we have only created the local database. No restrictions have been applied to those usernames yet.

To prevent a lock out on the router when the configuration for AAA authorization is started, exit out completely from EXEC mode and log back into the router using the username **cisco15** and password **cisco15**.

> **Note:** It is important to log in as a user with privilege level 15 in order to modify the default privilege level of IOS commands. Failure to do so will result in console session lockout when the **aaa authorization exec default local** command is entered.

After authenticating as **cisco15** and entering privilege EXEC mode, configure AAA authorization and create a custom privilege level. First, enter the following configuration command:

```
SanJose1(config)#aaa authorization exec default local
```

Next, specify which commands will be authorized. On SanJose1, issue the following commands from the console:

```
SanJose1(config)#aaa authorization commands 0 default local
SanJose1(config)#aaa authorization commands 15 default local
SanJose1(config)#aaa authorization commands 7 default local
```

After issuing these commands, a user must be "authorized" to use commands in privilege levels 0, 7, and 15.

The following is an example of the command to configure the router to query a TACACS+ server:

```
aaa authorization commands 0 default group tacacs+ local enable
```

The **group** keyword indicates a server group while the **tacacs+** keyword indicates the type of security server. If configured with this command, the local database on SanJose1 would only be used if the TACACS+ server were unavailable.

The final step is to specify which commands will exist in privilege level 7. On SanJose1, issue the following commands from the console:

```
SanJose1(config)#privilege configure level 7 snmp-server host
SanJose1(config)#privilege configure level 7 snmp-server enable
SanJose1(config)#privilege configure level 7 snmp-server
SanJose1(config)#privilege exec level 7 ping
SanJose1(config)#privilege exec level 7 configure terminal
SanJose1(config)#privilege exec level 7 configure
```

Now enter the **debug aaa authorization** command so the authorization process can be observed.

## Step 3

From Host A, Telnet to SanJose1. Log in as **cisco15**. Because privilege level 15 was used, privileged EXEC access is immediately given.

Enter the **show privilege** command and verify the privilege level. Enter global configuration mode and then exit. Make note of the **debug** results on SanJose1's console session.

Exit out of the Telnet session.

Now, again from Host A, Telnet into the router as **cisco0**.

1. After authenticated as **cisco0**, can the privileged EXEC mode be entered?

_____

As **cisco0**, enter the **?** command at the router prompt.

2. How many commands are available to privilege level 0?

_____

Exit out of the Telnet session, and Telnet in as **cisco7** from Host A. Notice that this user, like **cisco15**, begins an EXEC session in privileged mode.

Enter global configuration and use the **?** command to see which commands are available in privilege level 7, as shown in the following:

```
SanJose1#config terminal

SanJose1(config)#?
Configure commands:
  default      Set a command to its defaults
  end          Exit from configure mode
  exit         Exit from configure mode
  help         Description of the interactive help system
  no           Negate a command or set its defaults
  snmp-server  Modify SNMP parameters
```

Notice the **debug** output on SanJose1. Use the **undebug all** command to turn off all debugging.

## Step 4

In this step, configure AAA accounting on SanJose1. Enter privilege EXEC mode by either consoling in or by telnetting in as **cisco15**.

**Note:** If a TACACS+ server is not available, the results will not be stored but the recording will occur.

Enter the following:

```
SanJose1(config)#aaa accounting exec default start-stop group tacacs+
SanJose1(config)#aaa accounting commands 15 default start-stop group tacacs+
SanJose1(config)#aaa accounting network default start-stop group tacacs+
SanJose1(config)#aaa accounting connection default start-stop group tacacs+
SanJose1(config)#aaa accounting system default start-stop group tacacs+
```

The following is a brief description of each of the command options:

| Option | Result |
|---|---|
| **AAA** | Identifies a AAA command |
| **accounting** | Accounting or tracking feature of AAA |
| **exec** | Tracks EXEC commands on the device |
| **commands 15** | Tracks commands by privilege level 15 users, can be 0 through 15 |
| **network** | Tracks network services like PPP |
| **connection** | Tracks outbound Telnet sessions |
| **system** | Tracks system events like reload |
| **start-stop** | Include both Start and Stop recordings (compared to *stop-only*) |
| **default** | Use the default list as compared to a custom list |
| **group** | Use a group of servers |
| **TACACS+** | Use TACACS+ instead of a RADIUS server |

On SanJose1, enable **debug aaa accounting** with the following command:

```
SanJose1#debug aaa accounting
AAA Accounting debugging is on
```

From Host A, Telnet to SanJose1 and authenticate as **cisco15**. In the Telnet session, perform a couple of simple commands like **show run**. Return to the console session on SanJose1 and examine the **debug** output. The following is a partial sample **debug** output that resulted from **cisco15** entering the **show running-config** and **copy running-config startup-config** commands.

**Note:** The output may vary depending on the router platform and IOS used.

```
01:04:59: AAA/ACCT/CMD: User cisco15, Port tty2, Priv 15:"show running-config
<cr>"
01:04:59: AAA/ACCT/CMD: Found list "default"
01:04:59: AAA/ACCT: user cisco15, acct type 3 (3901449983):
Method=tacacs+ (tacacs+)
01:05:20: AAA/ACCT/CMD: User cisco15, Port tty2, Priv 15:"copy running-config
startup-config <cr>"
01:05:20: AAA/ACCT/CMD: Found list "default"
01:05:20: AAA/ACCT: user cisco15, acct type 3 (2545785330):
Method=tacacs+ (tacacs+)
```