



Lab 6.1.3 Configure Local AAA on Cisco Router

Objective

In this lab, the students will complete the following tasks:

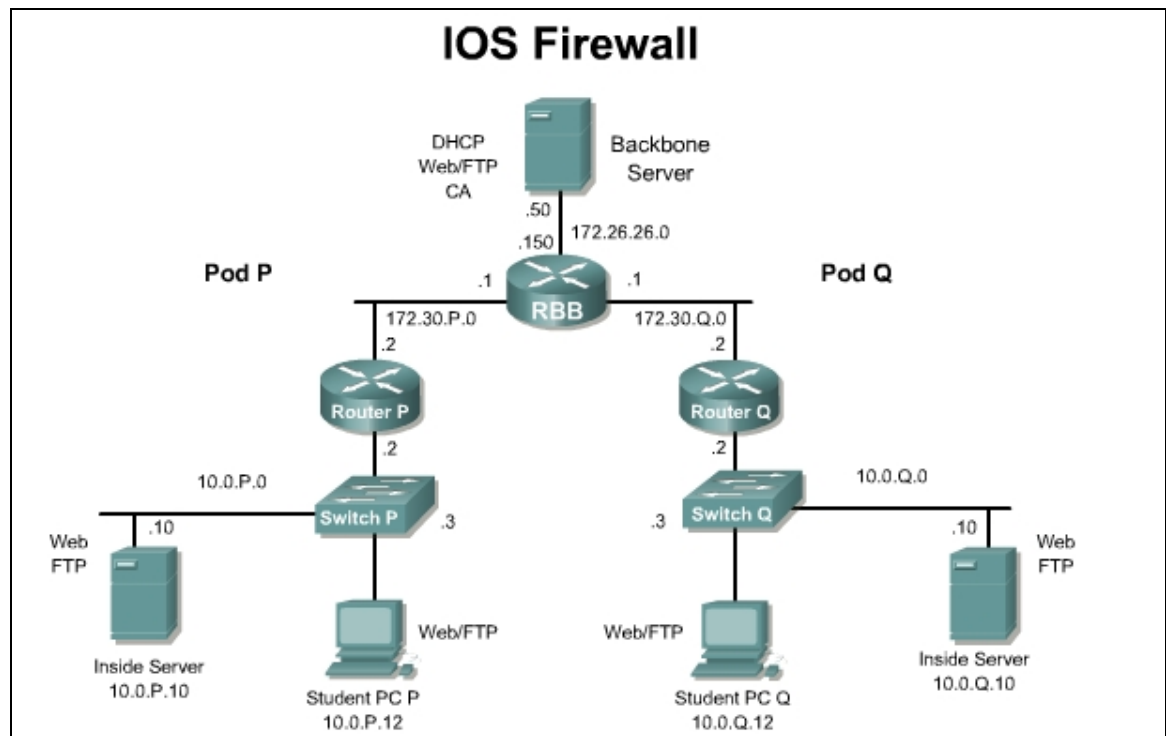
- Securing and testing access to the privileged EXEC, VTY, and console
- Configuring local database authentication using AAA
- Verify and test the AAA configuration

Scenario

Access control is a means network administrators can use to control who is allowed access key network devices and what services they are allowed to use once they have access. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which network administrators can set up access control.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the student PC. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

Additional Materials

The following websites provide additional information on AAA:

- http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d980f.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d9811.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d9810.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d9813.html

Command list

In this lab exercise the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
<code>aaa authentication</code>	Defines authentication parameters.
<code>aaa new-model</code>	Enables AAA.
<code>debug aaa authentication</code>	Enables AAA authentication debugging.
<code>enable</code>	Enters privileged EXEC mode.
<code>enable password <i>password</i></code>	Sets a local password to control access to various privilege levels.
<code>enable secret <i>password</i></code>	Specifies an additional layer of security over the <code>enable password</code> command.
<code>enable secret level <i>level</i> <i>password</i></code>	Sets a password for the privilege level.

Command	Description
<code>privilege level level</code>	Configures a new privilege level for users and associate commands with that privilege level. <i>level</i> - Privilege level associated with the specified line.
<code>privilege mode {level level / reset} command-string</code>	<i>mode</i> - Configuration mode for the specified command. level level - Specifies the privilege level configured for the specified command or commands. The level argument must be a number from 0 to 15. reset - Resets the privilege level of the specified command or commands to the default and removes the privilege level configuration from the running-config file. Note If the no form of this command is used to reset the privilege level to the default, the default form of this command will still appear in the configuration file. To completely remove a privilege configuration, use the reset keyword. <i>command-string</i> - Command associated with the specified privilege level. If the all keyword is used, specifies the command and subcommands associated with the privilege level.
<code>service password-encryption</code>	Encrypts all passwords in the configuration files.
<code>show privilege</code>	Displays the current level of privilege.
<code>username username password password</code>	Defines a local user and password combination.

Step 1 Secure and Test Access to Privileged EXEC, Line, VTY, AUX, and Console

Configure the current password protection by protecting access points into the router with passwords. Complete the following steps on the pod router:

- Set the security of the privileged EXEC mode by configuring an enable secret password of **rouge7fox**.
- Configure the VTY password of all VTYS to **echo9**.
- Configure a console password of **front door**. Yes, there is a space in the password.
- Look at the running configuration. Note that all passwords except “enable secret” are clear text. Use the **service password-encryption** command to correct this.
- Show the running configuration again to ensure all passwords are now encrypted.
 - What happens to the passwords when the **no service password-encryption** command is used?

Step 2 Configure the Local Database Authentication Using AAA

In this section, configure the local database authentication using AAA for the enable, line, and local methods.

Now that the NAS access points are protected, use the AAA commands to prepare for migration to a Cisco Secure Access Control Server (CSACS) environment. The goal of this task is to illustrate that each router access point can be secured using unique methods.

In this lab, there are two access points or lines to protect: VTY and console.

Complete the following steps to configure login authentication.

- a. Turn on AAA features. Note that on command examples, spaces are added at times for readability only:

```
RouterP(config)# aaa new-model
```

- b. Configure the login authentication to use the enable password using the default list:

```
RouterP(config)# aaa authentication login default enable
```

This protects all logins access instantly.

- c. Test the model. Exit from the privilege mode and then exit from user mode. Then try to access the router on the console port. A password prompt will appear.

1. Which password will be valid, **front door** or **rouge7fox**? Why?

- d. Protect the console specifically. Enter the following commands so the IS group can access the console. Be aware that some passwords contain spaces.

```
RouterP(config)# username admin password back door
```

```
RouterP(config)# aaa authentication login console-in local
```

```
RouterP(config)# line con 0
```

```
RouterP(config-line)# login authentication console-in
```

- e. Using the local database, students have just given the console a different login method from all the others. Cisco recommends never using **admin** as a username because it is too easy to guess.

- f. Exit the configuration, enable, and user modes, and test the method.

- g. Secure the VTY access for the IS personnel by using the following commands:

```
RouterP(config)# username isgroup password other door
```

```
RouterP(config)# aaa authentication login is-in local
```

```
RouterP(config)# line vty 0 4
```

```
RouterP(config-line)# login authentication is-in
```

- h. This is the same idea as the console protection, but on the Telnet access via the vty ports. Test by telneting into the NAS from the student PC. Do not use any of the Telnet icons on the desktop. They may be mapped to a specific server. Use the Telnet applet from MS-DOS instead.

1. What is prompted for at the beginning of the Telnet session?

Step 3 Test the Connection with Debug

In this task, use debug to look at the indicators for successful and unsuccessful authentication attempts. Before beginning this section, ensure that all Telnet sessions are disconnected, except for the console session. It is important in debugging to ensure the proper time is set to reference messages, especially if logging multiple devices to a central logging system.

Check the NAS clock by logging in to user mode and typing **show clock**. If the time and date are incorrect, enter the following command: **clock set HH:MM:SS DD month YYYY**. For example, **clock set 17:00:00 21 March 2005**.

To look at the indicators for successful and unsuccessful authentication attempts, complete the following steps:

- a. Log in to privileged mode and use the following command to verify the correct timestamp information for the debug output. Enable console logging of debug messages:

```
RouterP(config)# service timestamps debug datetime msec
```

```
RouterP(config)# logging on
```

```
RouterP(config)# logging console debugging
```

- b. Turn on debugging for AAA authentication:

```
RouterP# debug aaa authentication
```

- c. Trigger an AAA authentication event by exiting the console connection and then logging in using **admin** and **back door** as the username and password.

- d. After logging in and being presented the user mode prompt, continue with privileged mode. The debug information should be similar to the following:

```
Username:
```

```
Mar 21 17:05:00.461: AAA/AUTHEN/LOGIN (00000053): Pick method list  
'console-in'
```

```
Username: admin
```

```
Password:
```

```
RouterP>enable
```

```
Password:
```

```
Mar 21 17:05:11.656: AAA: parse name=tty0 idb type=-1 tty=-1
```

```
Mar 21 17:05:11.656: AAA: name=tty0 flags=0x11 type=4 shelf=0 slot=0  
adapter=0 port=0 channel=0
```

```
Mar 21 17:05:11.656: AAA/MEMORY: create_user (0x82B2138C)  
user='admin' ruser='NU
```

```
LL' ds0=0 port='tty0' rem_addr='async' authen_type=ASCII  
service=ENABLE priv=15 initial_task_id='0'
```

```
Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): port='tty0'  
list='' action=LOGIN service=ENABLE
```

```
Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): console enable -  
default to enable password (if any)
```

```
Mar 21 17:05:11.656: AAA/AUTHEN/START (3254755694): Method=ENABLE
```

```
Mar 21 17:05:11.660: AAA/AUTHEN(3254755694): Status=GETPASS
```

```
RouterP#
```

```
Mar 21 17:05:18.671: AAA/AUTHEN/CONT (3254755694): continue_login  
(user='(undef)')
```

```

Mar 21 17:05:18.671: AAA/AUTHEN(3254755694): Status=GETPASS
Mar 21 17:05:18.671: AAA/AUTHEN/CONT (3254755694): Method=ENABLE
Mar 21 17:05:18.755: AAA/AUTHEN(3254755694): Status=PASS
Mar 21 17:05:18.755: AAA/MEMORY: free_user (0x82B2138C) user='NULL'
ruser='NULL'

port='tty0' rem_addr='async' authen_type=ASCII service=ENABLE
priv=15

RouterP#

```

- e. Log out of the router before continuing.
- f. Log in to the router and enter an invalid enable password:

```

Username:

Mar 21 17:07:40.612: AAA/AUTHEN/LOGIN (000000054): Pick method list
'console-in'

Username: admin

Password:

RouterP>enable

Password:

Mar 21 17:07:52.103: AAA: parse name=tty0 idb type=-1 tty=-1
Mar 21 17:07:52.103: AAA: name=tty0 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=0 channel=0

Mar 21 17:07:52.107: AAA/MEMORY: create_user (0x82CE62E0)
user='admin' ruser='NULL' ds0=0 port='tty0' rem_addr='async'
authen_type=ASCII service=ENABLE priv=15 initial_task_id='0'

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): port='tty0'
list='' action=LOGIN service=ENABLE

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): console enable -
default to enable password (if any)

Mar 21 17:07:52.107: AAA/AUTHEN/START (2358711356): Method=ENABLE
Mar 21 17:07:52.107: AAA/AUTHEN(2358711356): Status=GETPASS

% Access denied

RouterP>

Mar 21 17:07:55.180: AAA/AUTHEN/CONT (2358711356): continue_login
(user='(undef)')

Mar 21 17:07:55.180: AAA/AUTHEN(2358711356): Status=GETPASS
Mar 21 17:07:55.180: AAA/AUTHEN/CONT (2358711356): Method=ENABLE
Mar 21 17:07:55.260: AAA/AUTHEN(2358711356): password incorrect
Mar 21 17:07:55.260: AAA/AUTHEN(2358711356): Status=FAIL
Mar 21 17:07:55.260: AAA/MEMORY: free_user (0x82CE62E0) user='NULL'
ruser='NULL'

port='tty0' rem_addr='async' authen_type=ASCII service=ENABLE
priv=15

RouterP>

```

Step 4 Telnet from the Student PC to the NAS

- a. Telnet from the student PC to the NAS and enter a username and password. After a successful Telnet authentication, enter the privileged EXEC mode. The students should use the following passwords:

- Telnet username **isgroup**
- Telnet password **other door**
- Enable password **rouge7fox**

The **debug aaa authentication** and **debug aaa authorization** output should be similar to the output below:

```
RouterP#
Mar 21 17Mar 21 17:42:18.065: AAA/AUTHEN/LOGIN (00000011): Pick
method list 'is-in'
Mar 21 17Mar 21 17:42:25.890: AAA/AUTHOR (00000011): Method list
id=0 not configured. Sk ip author
Mar 21 17Mar 21 17:42:29.817: AAA: parse name=tty67 idb type=-1
tty=-1
Mar 21 17:42:29.817: AAA: name=tty67 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=67 channel=0
Mar 21 17:42:29.817: AAA/MEMORY: create_user (0x82D1B690)
user='isgroup' ruser=
'NULL' ds0=0 port='tty67' rem_addr='10.0.1.12' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0'
Mar 21 17:42:29.817: AAA/AUTHEN/START (3905120739): port='tty67'
list='' action=LOGIN service=ENABLE
Mar 21 17:42:29.821: AAA/AUTHEN/START (3905120739): non-console
enable - default to enable password
Mar 21 17:42:29.821: AAA/AUTHEN/START (3905120739): Method=ENABLE
Mar 21 17:42:29.821: AAA/AUTHEN(3905120739): Status=GETPASS
Mar 21 17:42:34.064: AAA/AUTHEN/CONT (3905120739): continue_login
(user='(undef)')
Mar 21 17:42:34.068: AAA/AUTHEN(3905120739): Status=GETPASS
Mar 21 17:42:34.068: AAA/AUTHEN/CONT (3905120739): Method=ENABLE
Mar 21 17:42:34.152: AAA/AUTHEN(3905120739): Status=PASS
Mar 21 17:42:34.152: AAA/MEMORY: free_user (0x82D1B690) user='NULL'
ruser='NULL'
' port='tty67' rem_addr='10.0.1.12' authen_type=ASCII service=ENABLE
priv=15
```

- b. Next, Telnet from the student PC to the pod router but enter a wrong enable password. The **debug aaa authentication** and **debug aaa authorization** output should be similar to the output below:

```
RouterP#
Mar 21 17:43:56.639: AAA/AUTHEN/LOGIN (00000012): Pick method list
'is-in'
Mar 21 17:44:05.129: AAA/AUTHOR (00000012): Method list id=0 not
configured. Sk ip author
```

```

Mar 21 17:44:08.090: AAA: parse name=tty67 idb type=-1 tty=-1
Mar 21 17:44:08.090: AAA: name=tty67 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=67 channel=0
Mar 21 17:44:08.090: AAA/MEMORY: create_user (0x82D1BE74)
user='isgroup' ruser=
'NULL' ds0=0 port='tty67' rem_addr='10.0.1.12' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0'
Mar 21 17:44:08.090: AAA/AUTHEN/START (3951678639): port='tty67'
list='' action=LOGIN service=ENABLE
Mar 21 17:44:08.094: AAA/AUTHEN/START (3951678639): non-console
enable - default to enable password
Mar 21 17:44:08.094: AAA/AUTHEN/START (3951678639): Method=ENABLE
Mar 21 17:44:08.094: AAA/AUTHEN(3951678639): Status=GETPASS
Mar 21 17:44:12.886: AAA/AUTHEN/CONT (3951678639): continue_login
(user='(undef)')
Mar 21 17:44:12.890: AAA/AUTHEN(3951678639): Status=GETPASS
Mar 21 17:44:12.890: AAA/AUTHEN/CONT (3951678639): Method=ENABLE
Mar 21 17:44:12.974: AAA/AUTHEN(3951678639): password incorrect
Mar 21 17:44:12.974: AAA/AUTHEN(3951678639): Status=FAIL
Mar 21 17:44:12.974: AAA/MEMORY: free_user (0x82D1BE74) user='NULL'
ruser='NULL'
' port='tty67' rem_addr='10.0.1.12' authen_type=ASCII service=ENABLE
priv=15

```

1. What syntax indicates the authentication was unsuccessful?

Step 5 View a Sample Configuration for the NAS

At this point, the NAS configuration should look like the one shown in this task.

- a. To view the configuration, log in to privileged mode and enter **show running config**:

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot system flash
boot-end-marker
!

```



```

enable secret 5 $1$0G/5$Q0NZw3aKe7IawIE/LpS9A1
enable password 7 0822455D0A16
!
aaa new-model
!
!
aaa authentication login default enable
aaa authentication login console-in local
aaa authentication login is-in local
!
aaa session-id common
!
resource policy
!
memory-size iomem 15
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.0.1.1 10.0.1.12
!
ip dhcp pool POD1_INSIDE
    network 10.0.1.0 255.255.255.0
    default-router 10.0.1.2
!
!
no ip ips deny-action ips-interface
no ip domain lookup
!
no ftp-server write-enable
!
!
!
username admin password 0 back door
username isgroup password 0 other door
!

```

```

!
!
!
!
interface FastEthernet0/0
  description inside
  ip address 10.0.1.2 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  description outside
  ip address 172.30.1.2 255.255.255.0
  duplex auto
  speed auto
!
router eigrp 1
  network 10.0.0.0
  network 172.30.0.0
  no auto-summary
  no eigrp log-neighbor-changes
!
ip classless
!
ip http server
ip http authentication local
no ip http secure-server
!
!
!
control-plane
!
!
!
!
line con 0
  password 7 08275E41070D45131D041E
  login authentication console-in
line aux 0

```

```
line vty 0 4
  privilege level 15
  password 7 0001100E0B02
  login authentication is-in
  transport input telnet
!
!
end
```