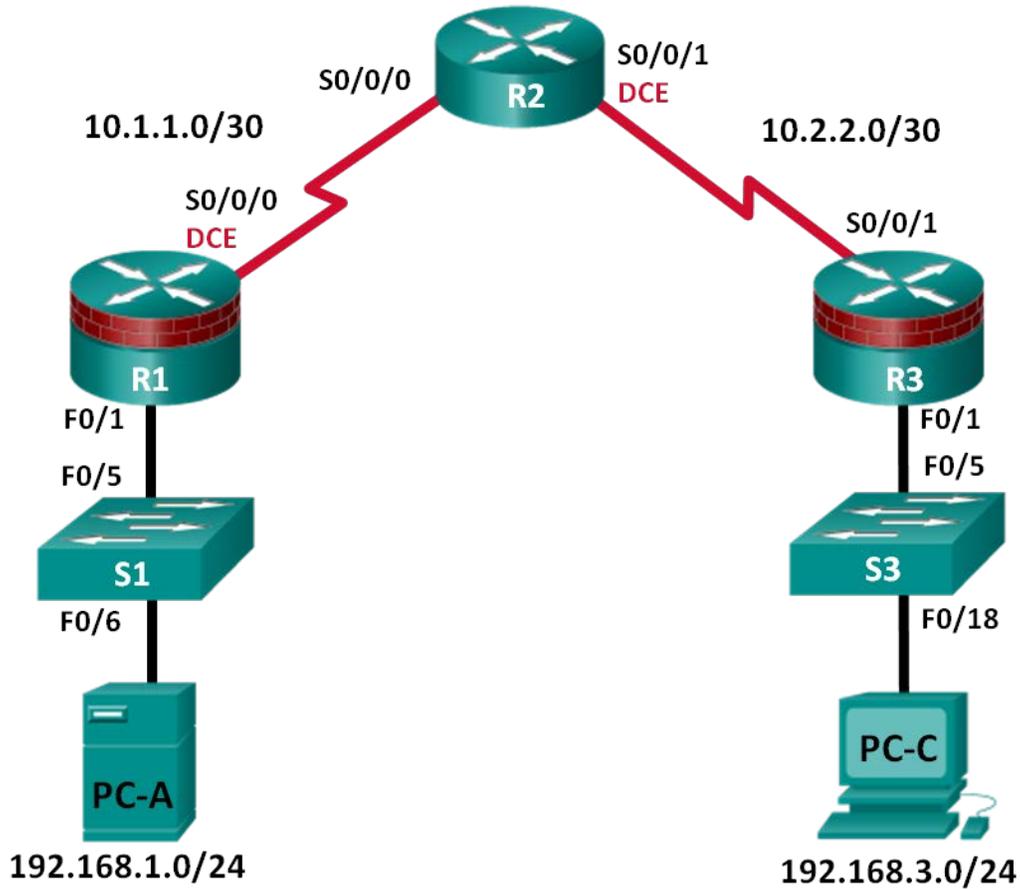**CCNA Security**

Lab - Securing Administrative Access Using AAA and RADIUS

Topology

Note: ISR G2 devices use GigabitEthernet interfaces instead of FastEthernet Interfaces.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Objectives

Part 1: Configure Basic Device Settings

- Configure basic settings such as host name, interface IP addresses, and access passwords.
- Configure static routing.

Part 2: Configure Local Authentication

- Configure a local database user and local access for the console, vty, and aux lines.
- Test the configuration.

Part 3: Configure Local Authentication Using AAA

- Configure the local user database using Cisco IOS.
- Configure AAA local authentication using Cisco IOS.
- Configure AAA local authentication using CCP.
- Test the configuration.

Part 4: Configure Centralized Authentication Using AAA and RADIUS

- Install a RADIUS server on a computer.
- Configure users on the RADIUS server.
- Use Cisco IOS to configure AAA services on a router to access the RADIUS server for authentication.
- Use CCP to configure AAA services on a router to access the RADIUS server for authentication.
- Test the AAA RADIUS configuration.

Background / Scenario

The most basic form of router access security is to create passwords for the console, vty, and aux lines. A user is prompted for only a password when accessing the router. Configuring a privileged EXEC mode enable secret password further improves security, but still only a basic password is required for each mode of access.

In addition to basic passwords, specific usernames or accounts with varying privilege levels can be defined in the local router database that can apply to the router as a whole. When the console, vty, or aux lines are

configured to refer to this local database, the user is prompted for a username and a password when using any of these lines to access the router.

Additional control over the login process can be achieved using authentication, authorization, and accounting (AAA). For basic authentication, AAA can be configured to access the local database for user logins, and fallback procedures can also be defined. However, this approach is not very scalable because it must be configured on every router. To take full advantage of AAA and achieve maximum scalability, AAA is used in conjunction with an external TACACS+ or RADIUS server database. When a user attempts to log in, the router references the external server database to verify that the user is logging in with a valid username and password.

In this lab, you build a multi-router network and configure the routers and hosts. You will then use CLI commands and CCP tools to configure routers with basic local authentication by means of AAA. You will install RADIUS software on an external computer and use AAA to authenticate users with the RADIUS server.

Note: The router commands and output in this lab are from a Cisco 1841 router with Cisco IOS Release 15.1(4)M8 (Advanced IP Services image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 1841 with Cisco IOS Release 15.1(4)M8 advanced IP services image or comparable)
- 2 switches (Cisco 2960 or comparable)
- 2 PCs (Windows Vista or Windows 7 with CCP 2.5, latest version of Java, Internet Explorer, and Flash Player and RADIUS server)
- Serial and Ethernet cables, as shown in the topology
- Console cables to configure Cisco networking devices

CCP Notes:

- If the PC on which CCP is installed is running Windows Vista or Windows 7, it may be necessary to right-click on the CCP icon or menu item, and choose **Run as administrator**.
- In order to run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure that all pop-up blockers are turned off in the browser.

Part 1: Configure Basic Device Settings

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

All steps should be performed on routers R1 and R3. Only steps 1, 2, 3 and 6 need to be performed on R2. The procedure for R1 is shown here as an example.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table.

c. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.

```
R1(config)# no ip domain-lookup
```

Step 3: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

b. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

Step 5: Verify connectivity between PC-A and R3.

a. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that static routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Step 6: Save the basic running configuration for each router.

Step 7: Configure and encrypt passwords on R1 and R3.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

For this step, configure the same settings for R1 and R3. Router R1 is shown here as an example.

a. Configure a minimum password length.

Use the **security passwords** command to set a minimum password length of 10 characters.

```
R1(config)# security passwords min-length 10
```

b. Configure the enable secret password on both routers.

```
R1(config)# enable secret cisco12345
```

c. Configure the basic console, auxiliary port, and vty lines.

d. Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after **5** minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the exec timeout can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

```
R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
```

```
R1(config-line)# login
R1(config-line)# logging synchronous
```

e. Configure a password for the aux port for router R1.

```
R1(config)# line aux 0
R1(config-line)# password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

f. Configure the password on the vty lines for router R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

g. Encrypt the console, aux, and vty passwords.

```
R1(config)# service password-encryption
```

h. Issue the **show run** command. Can you read the console, aux, and vty passwords? Explain.

_____

_____

Step 8: Configure a login warning banner on routers R1 and R3.

a. Configure a warning to unauthorized users using a message-of-the-day (MOTD) banner with the **banner motd** command. When a user connects to the router, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit
```

b. Exit privileged EXEC mode by using the **disable** or **exit** command and press **Enter** to get started.

If the banner does not appear correctly, re-create it using the **banner motd** command.

Step 9: Save the basic configurations on all routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1# copy running-config startup-config
```

Part 2: Configure Local Authentication

In Part 2 of this lab, you configure a local username and password and change the access for the console, aux, and vty lines to reference the router's local database for valid usernames and passwords. Perform all steps on R1 and R3. The procedure for R1 is shown here.

Step 1: Configure the local user database.

a. Create a local user account with MD5 hashing to encrypt the password.

```
R1(config)# username user01 secret user01pass
```

b. Exit global configuration mode and display the running configuration. Can you read the user's password?

_____

Step 2: Configure local authentication for the console line and login.

a. Set the console line to use the locally defined login usernames and passwords.

```
R1(config)# line console 0
R1(config-line)# login local
```

b. Exit to the initial router screen that displays:

```
R1 con0 is now available. Press RETURN to get started.
```

c. Log in using the **user01** account and password previously defined.

What is the difference between logging in at the console now and previously?

_____

_____

d. After logging in, issue the **show run** command. Were you able to issue the command? Explain.

_____

_____

Enter privileged EXEC mode using the **enable** command. Were you prompted for a password? Explain.

_____

_____

Step 3: Test the new account by logging in from a Telnet session.

a. From PC-A, establish a Telnet session with R1.

```
PC-A> telnet 192.168.1.1
```

b. Were you prompted for a user account? Explain.

_____

_____

c. What password did you use to login? _____

d. Set the vty lines to use the locally defined login accounts.

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

e. From PC-A, telnet R1 to R1 again.

```
PC-A> telnet 192.168.1.1
```

Were you prompted for a user account? Explain.

_____

_____

f. Log in as **user01** with a password of **user01pass**.

g. While connected to R1 via Telnet, access privileged EXEC mode with the **enable** command.

What password did you use?

_____

h. For added security, set the aux port to use the locally defined login accounts.

```
R1(config)# line aux 0
```

```
R1(config-line)# login local
```

i.   End the Telnet session with the **exit** command.

Step 4: Save the configuration on R1.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1# copy running-config startup-config
```

Step 5: Perform steps 1 through 4 on R3 and save the configuration.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

Part 3: Configure Local Authentication Using AAA on R3

Task 1: Configure the Local User Database Using Cisco IOS.

Note: To configure AAA using CCP, skip to Task 3.

Step 1: Configure the local user database.

a.   Create a local user account with MD5 hashing to encrypt the password.

```
R3(config)# username Admin01 privilege 15 secret Admin01pass
```

b.   Exit global configuration mode and display the running configuration. Can you read the user's password?

_____

_____

Task 2: Configure AAA Local Authentication Using Cisco IOS.

On R3, enable services with the global configuration **aaa new-model** command. Because you are implementing local authentication, use local authentication as the first method, and no authentication as the secondary method.

If you were using an authentication method with a remote server, such as TACACS+ or RADIUS, you would configure a secondary authentication method for fallback if the server is unreachable. Normally, the secondary method is the local database. In this case, if no usernames are configured in the local database, the router allows all users login access to the device.

Step 1: Enable AAA services.

```
R3(config)# aaa new-model
```

Step 2: Implement AAA services for console access using the local database.

a.   Create the default login authentication list by issuing the **aaa authentication login default** *method1[method2][method3]* command with a method list using the **local** and **none** keywords.

```
R3(config)# aaa authentication login default local none
```

Note: If you do not set up a default login authentication list, you could get locked out of the router and be forced to use the password recovery procedure for your specific router.

b.   Exit to the initial router screen that displays:

```
R3 con0 is now available


Press RETURN to get started.
```

Log in to the console as **Admin01** with a password of **Admin01pass**. Remember that passwords are case-sensitive. Were you able to log in? Explain.

_____

_____

Note: If your session with the console port of the router times out, you might have to log in using the default authentication list.

c. Exit to the initial router screen that displays:

```
R3 con0 is now available


Press RETURN to get started.
```

d. Attempt to log in to the console as **baduser** with any password. Were you able to log in? Explain.

_____

_____

e. If no user accounts are configured in the local database, which users are permitted to access the device?

_____

_____

Step 3: Create an AAA authentication profile for Telnet using the local database.

a. Create a unique authentication list for Telnet access to the router. This does not have the fallback of no authentication, so if there are no usernames in the local database, Telnet access is disabled. To create an authentication profile that is not the default, specify a list name of TELNET_LINES and apply it to the vty lines.

```
R3(config)# aaa authentication login TELNET_LINES local
R3(config)# line vty 0 4
R3(config-line)# login authentication TELNET_LINES
```

b. Verify that this authentication profile is used by opening a Telnet session from PC-C to R3.

```
PC-C> telnet 192.168.3.1
Trying 192.168.3.1 ... Open
```

c. Log in as **Admin01** with a password of **Admin01pass**. Were you able to login? Explain.

_____

_____

d. Exit the Telnet session with the **exit** command, and Telnet to R3 again.

e. Attempt to log in as **baduser** with any password. Were you able to login? Explain.

_____

_____

Task 3: (Optional) Configure AAA Local Authentication Using Cisco CCP.

a. .

b. In the Deliver Configuration to Router window, click **Deliver**.

c. In the Commands Delivery Status window, click **OK**.

Task 4: Observe AAA Authentication Using Cisco IOS Debug.

In this task, you use the **debug** command to observe successful and unsuccessful authentication attempts.

Step 1: Verify that the system clock and debug time stamps are configured correctly.

a. From the R3 user or privileged EXEC mode prompt, use the **show clock** command to determine what the current time is for the router. If the time and date are incorrect, set the time from privileged EXEC mode with the command **clock set HH:MM:SS DD month YYYY.** An example is provided here for R3.

```
R3# clock set 14:15:00 26 December 2008
```

b. Verify that detailed time-stamp information is available for your debug output using the **show run** command. This command displays all lines in the running config that include the text "timestamps".

```
R3# show run | include timestamps

service timestamps debug datetime msec
service timestamps log datetime msec
```

c. If the **service timestamps debug** command is not present, enter it in global config mode.

```
R3(config)# service timestamps debug datetime msec
R3(config)# exit
```

d. Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R3# copy running-config startup-config
```

Step 2: Use debug to verify user access.

a. Activate debugging for AAA authentication.

```
R3# debug aaa authentication
AAA Authentication debugging is on
```

b. Start a Telnet session from PC-C to R3.

c. Log in with username **Admin01** and password **Admin01pass**. Observe the AAA authentication events in the console session window. Debug messages similar to the following should be displayed.

```
R3#
Dec 26 14:36:42.323: AAA/BIND(000000A5): Bind i/f
Dec 26 14:36:42.323: AAA/AUTHEN/LOGIN (000000A5): Pick method list 'default'
```

d. From the Telnet window, enter privileged EXEC mode. Use the enable secret password of **cisco12345**. Debug messages similar to the following should be displayed. In the third entry, note the username (Admin01), virtual port number (tty194), and remote Telnet client address (192.168.3.3). Also note that the last status entry is "PASS."

```
R3#
Dec 26 14:40:54.431: AAA: parse name=tty194 idb type=-1 tty=-1
Dec 26 14:40:54.431: AAA: name=tty194 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=194 channel=0
Dec 26 14:40:54.431: AAA/MEMORY: create_user (0x64BB5510) user='Admin01' ruser=' NULL'
ds0=0 port='tty194' rem_addr='192.168.3.3' authen_type=ASCII service=ENABLE priv=15
initial_task_id='0', vrf= (id=0)
```

```
Dec 26 14:40:54.431: AAA/AUTHEN/START (2467624222): port='tty194' list='' action=LOGIN
service=ENABLE
Dec 26 14:40:54.431: AAA/AUTHEN/START (2467624222): non-console enable - default to
enable password
Dec 26 14:40:54.431: AAA/AUTHEN/START (2467624222): Method=ENABLE
R3#
Dec 26 14:40:54.435: AAA/AUTHEN(2467624222): Status=GETPASS
R3#
Dec 26 14:40:59.275: AAA/AUTHEN/CONT (2467624222): continue_login (user='(undef)')
Dec 26 14:40:59.275: AAA/AUTHEN(2467624222): Status=GETPASS
Dec 26 14:40:59.275: AAA/AUTHEN/CONT (2467624222): Method=ENABLE
Dec 26 14:40:59.287: AAA/AUTHEN(2467624222): Status=PASS
Dec 26 14:40:59.287: AAA/MEMORY: free_user (0x64BB5510) user='NULL' ruser='NULL'
port='tty194' rem_addr='192.168.3.3' authen_type=ASCII service=ENABLE priv=15 vrf=
(id=0)
```

e. From the Telnet window, exit privileged EXEC mode using the **disable** command. Try to enter privileged EXEC mode again, but use a bad password this time. Observe the debug output on R3, noting that the status is "FAIL" this time.

```
Dec 26 15:46:54.027: AAA/AUTHEN(2175919868): Status=GETPASS
Dec 26 15:46:54.027: AAA/AUTHEN/CONT (2175919868): Method=ENABLE
Dec 26 15:46:54.039: AAA/AUTHEN(2175919868): password incorrect
Dec 26 15:46:54.039: AAA/AUTHEN(2175919868): Status=FAIL
Dec 26 15:46:54.039: AAA/MEMORY: free_user (0x6615BFE4) user='NULL' ruser='NULL'
port='tty194' rem_addr='192.168.3.3' authen_type=ASCII service=ENABLE priv=15 vrf=
(id=0)
```

f. From the Telnet window, exit the Telnet session to the router. Then try to open a Telnet session to the router again, but this time try to log in with the username **Admin01** and a bad password. From the console window, the debug output should look similar to the following.

```
Dec 26 15:49:32.339: AAA/AUTHEN/LOGIN (000000AA): Pick method list 'default'
```

What message was displayed on the Telnet client screen?

_____

_____

g. Turn off all debugging using the **undebug all** command at the privileged EXEC prompt.

Part 4: Configure Centralized Authentication Using AAA and RADIUS

In Part 4 of the lab, you install RADIUS server software on PC-A. You then configure R1 to access the external RADIUS server for user authentication. The freeware server WinRadius is used for this section of the lab.

Task 1: Restore R1 to the Basic Configuration.

To avoid confusion as to what was already entered and the AAA RADIUS configuration, start by restoring router R1 to its basic configuration as performed in Parts 1 and 2 of this lab.

Step 1: Reload and restore saved configuration on R1.

In this step, restore the router back to the basic configuration saved in Parts 1 and 2.

a. Connect to the R1 console, and log in with the username **Admin01** and password **Admin01pass**.

b. Enter privileged EXEC mode with the password **cisco12345**.

c.   Reload the router and enter **no** when prompted to save the configuration.

```
R1# reload


System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

Step 2: Verify connectivity.

a.   Test connectivity by pinging from host PC-A to PC-C. If the pings are not successful, troubleshoot the router and PC configurations until they are.

b.   If you are logged out of the console, log in again as **user01** with password **user01pass**, and access privileged EXEC mode with the password **cisco12345**.

Task 2: Download and Install a RADIUS Server on PC-A.

There are a number of RADIUS servers available, both freeware and for cost. This lab uses WinRadius, a freeware standards-based RADIUS server that runs on Windows operating systems. The free version of the software can support only five usernames.

Note: A zipped file containing the WinRadius software can be obtained from your instructor.

Step 1: Download the WinRadius software.

a.   Create a folder named **WinRadius** on your desktop or other location in which to store the files.

b.   Extract the WinRadius zipped files to the folder you created in Step 1a. There is no installation setup. The extracted **WinRadius.exe** file is executable.

c.   You may create a shortcut on your desktop for WinRadius.exe.

Note: If WinRadius is used on a PC that uses the Microsoft Windows Vista operating system or the Microsoft Windows 7 operating system, ODBC may fail to create successfully because it cannot write to the registry.

Possible solutions:

a.   Compatibility settings:

1)   Right click on the **WinRadius.exe** icon and select **Properties**.

2)   While in the **Properties** dialog box, select the **Compatibility** tab. In this tab, select the checkbox for **Run this program in compatibility mode for**. Then in the drop down menu below, choose **Windows XP (Service Pack 3)** for example, if it is appropriate for your system.

3)   Click **OK**.

b.   Run as Administrator settings:

1)   Right click on the WinRadius.exe icon and select **Properties**.

2)   While in the **Properties** dialog box, select the **Compatibility** tab. In this tab, select the checkbox for **Run this program as administrator** in the Privilege Level section.

3)   Click **OK**.

c.   Run as Administration for each launch:

1)   Right click on the WinRadius.exe icon and select **Run as Administrator**.

2)   When WinRadius launches, click **Yes** in the User Account Control dialog box.

Step 2: Configure the WinRadius server database.

a. Start the WinRadius.exe application. WinRadius uses a local database in which it stores user information. When the application is started for the first time, the following messages are displayed:

    ```
    Please go to "Settings/Database and create the ODBC for your RADIUS database.
    Launch ODBC failed.
    ```

b. Choose **Settings > Database** from the main menu. The following screen is displayed. Click the **Configure ODBC Automatically** button and then click **OK**. You should see a message that the ODBC was created successfully. Exit WinRadius and restart the application for the changes to take effect.
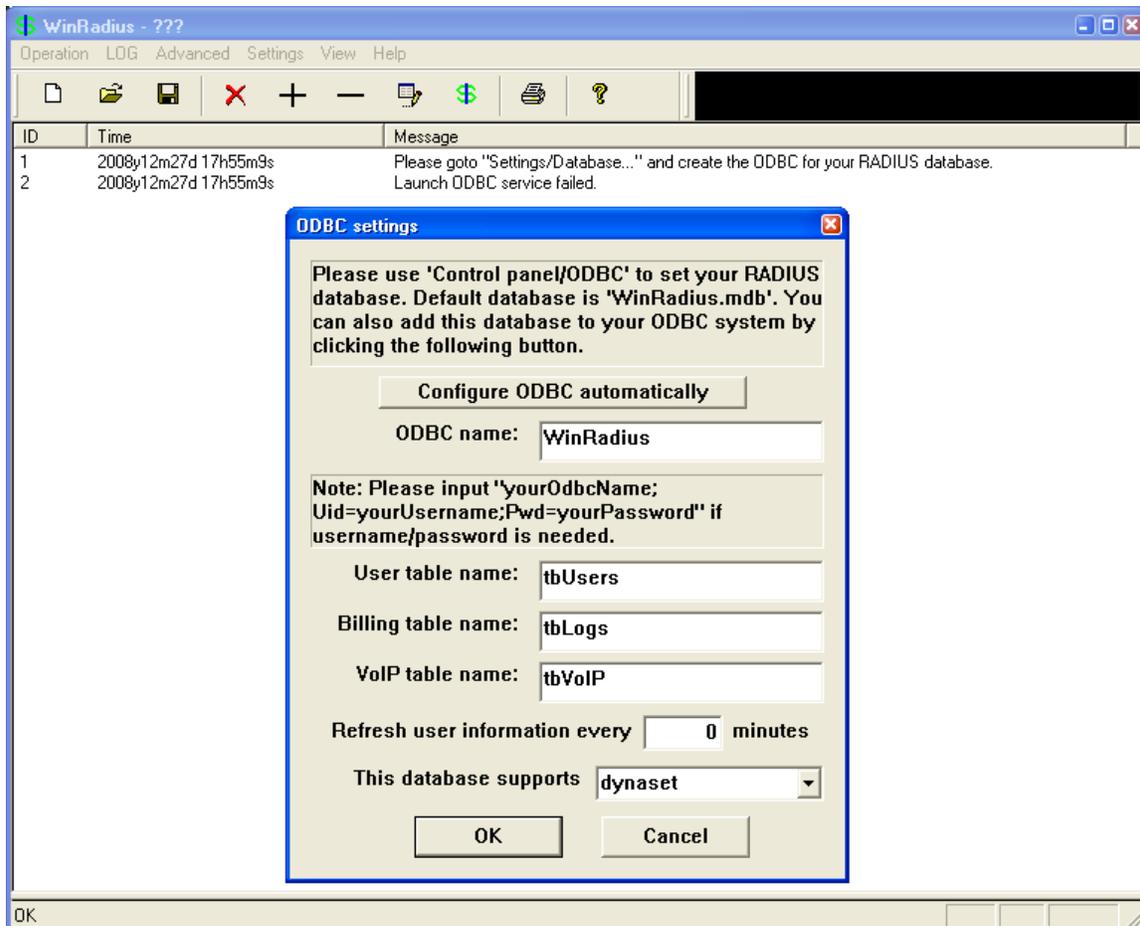
c. When WinRadius starts again, you should see messages similar to the following displayed.
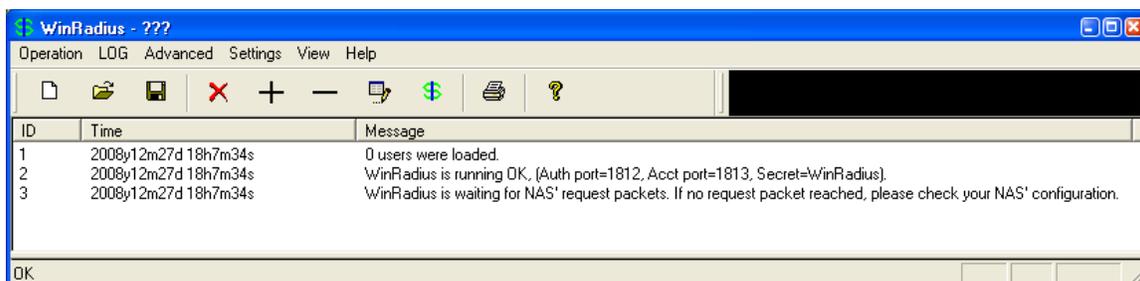
==**Note about WinRadius Server**==:

<mark>The free version of WinRadius only supports five usernames. If the first message in the above screen shows something other than 0 users were loaded, then you will need to remove the previously added users from the WinRadius database.</mark>

<mark>To determine what usernames are in the database, click on **Operation** > **Query** then click **OK**. A list of usernames contained in the database is displayed in the bottom section of the WinRadius window.</mark>

<mark>To delete a user, click **Operation** > **Delete User**, and then enter the username exactly as listed. Usernames are case sensitive.</mark>

    d.   On which ports is WinRadius listening for authentication and accounting?

_____

_____

Step 3: Configure users and passwords on the WinRadius server.

    a.   From the main menu, select **Operation** > **Add User**.

    b.   Enter the username **RadUser** with a password of **RadUserpass**. Remember that passwords are case-sensitive.
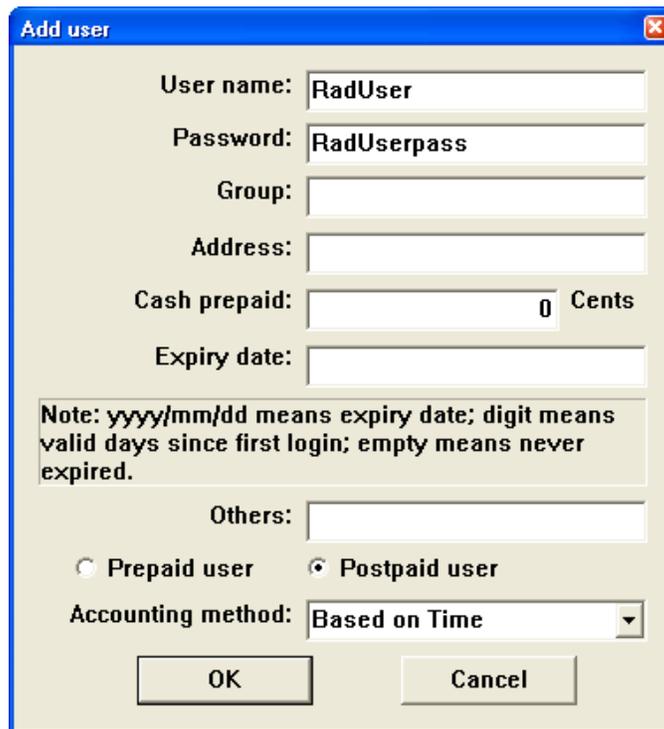
    c.   Click **OK**. You should see a message on the log screen that the user was added successfully.

Step 4: Clear the log display.

From the main menu, choose **Log** > **Clear**.

## Step 5: Test the new user added using the WinRadius test utility.

    a.   A WinRadius testing utility is included in the downloaded zip file. Navigate to the folder where you unzipped the WinRadius.zip file and locate the file named RadiusTest.exe.

b. Start the RadiusTest application, and enter the IP address of this RADIUS server (**192.168.1.3**), username **RadUser**, and password **RadUserpass** as shown. Do not change the default RADIUS port number of 1813 and the RADIUS password of WinRadius.

c. Click **Send** and you should see a Send Access_Request message indicating the server at 192.168.1.3, port number 1813, received 44 hexadecimal characters.
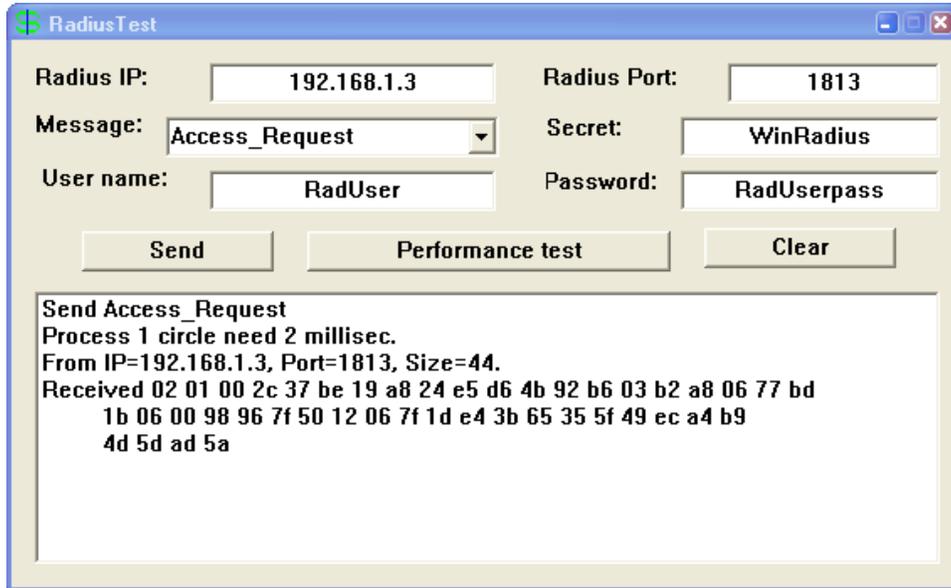
d. Review the WinRadius log to verify that RadUser successfully authenticated.
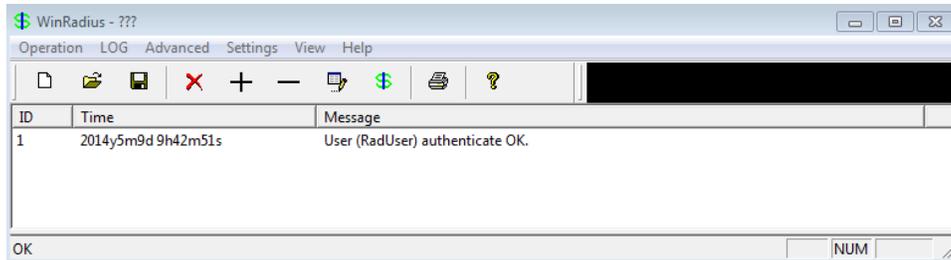
e. Close the RadiusTest application.

Task 3: Configure R1 AAA Services and Access the RADIUS Server Using Cisco IOS

Note: To configure AAA using CCP, proceed to Task 5.

Step 1: Enable AAA on R1.

Use the **aaa new-model** command in global configuration mode to enable AAA.

```
R1(config)# aaa new-model
```

Step 2: Configure the default login authentication list.

a. Configure the list to first use RADIUS for the authentication service, and then none. If no RADIUS server can be reached and authentication cannot be performed, the router globally allows access without authentication. This is a safeguard measure in case the router starts up without connectivity to an active RADIUS server.

```
R1(config)# aaa authentication login default group radius none
```

b. You could alternatively configure local authentication as the backup authentication method instead.

Note: If you do not set up a default login authentication list, you could get locked out of the router and need to use the password recovery procedure for your specific router.

Step 3: Specify a RADIUS server.

a. Use the **radius-server host** *hostname* **key** *key* command to point to the RADIUS server. The *hostname* argument accepts either a host name or an IP address. Use the IP address of the RADIUS server, PC-A (**192.168.1.3**). The key is a secret password shared between the RADIUS server and the RADIUS client (R1 in this case) and used to authenticate the connection between the router and the server before the user authentication process takes place. The RADIUS client may be a Network Access Server (NAS), but router R1 plays that role in this lab. Use the default NAS secret password of **WinRadius** specified on the RADIUS server (see Task 2, Step 5). Remember that passwords are case-sensitive.

```
R1(config)# radius-server host 192.168.1.3 key WinRadius
```

Task 4: Test the AAA RADIUS Configuration.

Step 1: Verify connectivity between R1 and the computer running the RADIUS server.

Ping from R1 to PC-A.

```
R1# ping 192.168.1.3
```

If the pings were not successful, troubleshoot the PC and router configuration before continuing.

Step 2: Test your configuration.

a. If you restarted the WinRadius server, you must re-create the user **RadUser** with a password of **RadUserpass** by choosing **Operation** > **Add User**.

b. Clear the log on the WinRadius server by choosing **Log** > **Clear** from the main menu.

c. On R1, exit to the initial router screen that displays:

```
R1 con0 is now available


Press RETURN to get started.
```

d. Test your configuration by logging in to the console on R1 using the username **RadUser** and the password of **RadUserpass**. Were you able to gain access to the user EXEC prompt and, if so, was there any delay?

    _____

    _____

e. Exit to the initial router screen that displays:

```
R1 con0 is now available


Press RETURN to get started.
```

f. Test your configuration again by logging in to the console on R1 using the nonexistent username of **Userxxx** and the password of **Userxxxpass**. Were you able to gain access to the user EXEC prompt? Explain.

    _____

    _____

_____

_____

g. Were any messages displayed on the RADIUS server log for either login? _____

h. Why was a nonexistent username able to access the router and no messages are displayed on the RADIUS server log screen?

_____

_____

i. When the RADIUS server is unavailable, messages similar to the following are typically displayed after attempted logins.

```
*Dec 26 16:46:54.039: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.3:1645,1646 is
not responding.
*Dec 26 15:46:54.039: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.3:1645,1646 is
being marked alive.
```

Step 3: Troubleshoot router-to-RADIUS server communication.

a. Check the default Cisco IOS RADIUS UDP port numbers used on R1 with the **radius-server host** command and the Cisco IOS Help function.

```
R1(config)# radius-server host 192.168.1.3 ?
  acct-port  UDP port for RADIUS acco/unting server (default is 1646)
  alias        1-8 aliases for this server (max. 8)
  auth-port  UDP port for RADIUS authentication server (default is 1645)
<Output omitted>
```

b. Check the R1 running configuration for lines containing the command **radius**.
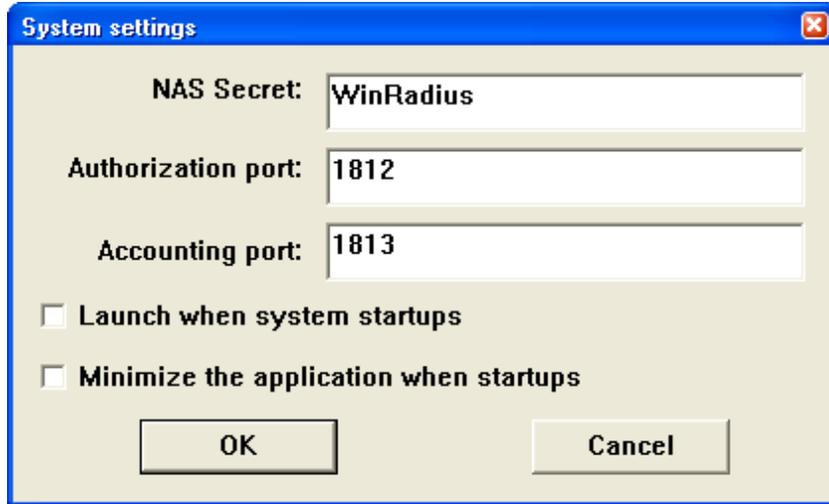
```
R1# show run | include radius
aaa authentication login default group radius none
radius-server host 192.168.1.3 auth-port 1645 acct-port 1646 key 7
097B47072B04131B1E1F
<Output omitted>
```

What are the default R1 Cisco IOS UDP port numbers for the RADIUS server?

_____

Step 4: Check the default port numbers on the WinRadius server on PC-A.

From the WinRadius main menu, choose **Settings** > **System**.

What are the default WinRadius UDP port numbers? _____

Note: RFC 2865 officially assigned port numbers 1812 and 1813 for RADIUS.

Step 5: Change the RADIUS port numbers on R1 to match the WinRadius server.

Unless specified otherwise, the Cisco IOS RADIUS configuration defaults to UDP port numbers 1645 and 1646. Either the router Cisco IOS port numbers must be changed to match the port number of the RADIUS server or the RADIUS server port numbers must be changed to match the port numbers of the Cisco IOS router.

a. Remove the previous configuration using the following command.

```
R1(config)# no radius-server host 192.168.1.3 auth-port 1645 acct-port 1646
```

b. Issue the **radius-server host** command again and this time specify port numbers **1812** and **1813**, along with the IP address and secret key for the RADIUS server.

```
R1(config)# radius-server host 192.168.1.3 auth-port 1812 acct-port 1813 key
WinRadius
```

Step 6: Test your configuration by logging into the console on R1.

a. Exit to the initial router screen that displays: R1 con0 is now available, Press **RETURN** to get started.

b. Log in again with the username of **RadUser** and password of **RadUserpass**. Were you able to login? Was there any delay this time?

_____

_____

_____

_____

c. The following message should display on the RADIUS server log.

```
User (RadUser) authenticate OK.
```

d. Exit to the initial router screen that displays:

```
R1 con0 is now available, Press RETURN to get started.
```

e. Log in again using an invalid username of **Userxxx** and the password of **Userxxxpass**. Were you able to login?

_____

_____

What message was displayed on the router?

_____

The following messages should display on the RADIUS server log.

```
Reason: Unknown username
User (Userxxx) authenticate failed
```


Step 7: Create an authentication method list for Telnet and test it.

a. Create a unique authentication method list for Telnet access to the router. This does not have the fallback of no authentication, so if there is no access to the RADIUS server, Telnet access is disabled. Name the authentication method list **TELNET_LINES**.

```
R1(config)# aaa authentication login TELNET_LINES group radius
```

b. Apply the list to the vty lines on the router using the login authentication command.

```
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET_LINES
```

c. Telnet from PC-A to R1, and log in with the username **RadUser** and the password of **RadUserpass**. Were you able to gain access to log in? Explain.

_____

_____

d. Exit the Telnet session, and telnet from PC-A to R1 again. Log in with the username **Userxxx** and the password of **Userxxxpass**. Were you able to log in? Explain.

_____

_____

Reflection

1. Why would an organization want to use a centralized authentication server rather than configuring users and passwords on each individual router?

_____

_____

_____

_____

_____

_____

_____

_____

2. Contrast local authentication and local authentication with AAA.

_____

_____

_____

_____

_____

_____

_____

_____

3. Based on the Academy online course content, web research, and the use of RADIUS in this lab, compare and contrast RADIUS with TACACS+.

_____

_____

_____

_____

_____

_____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				