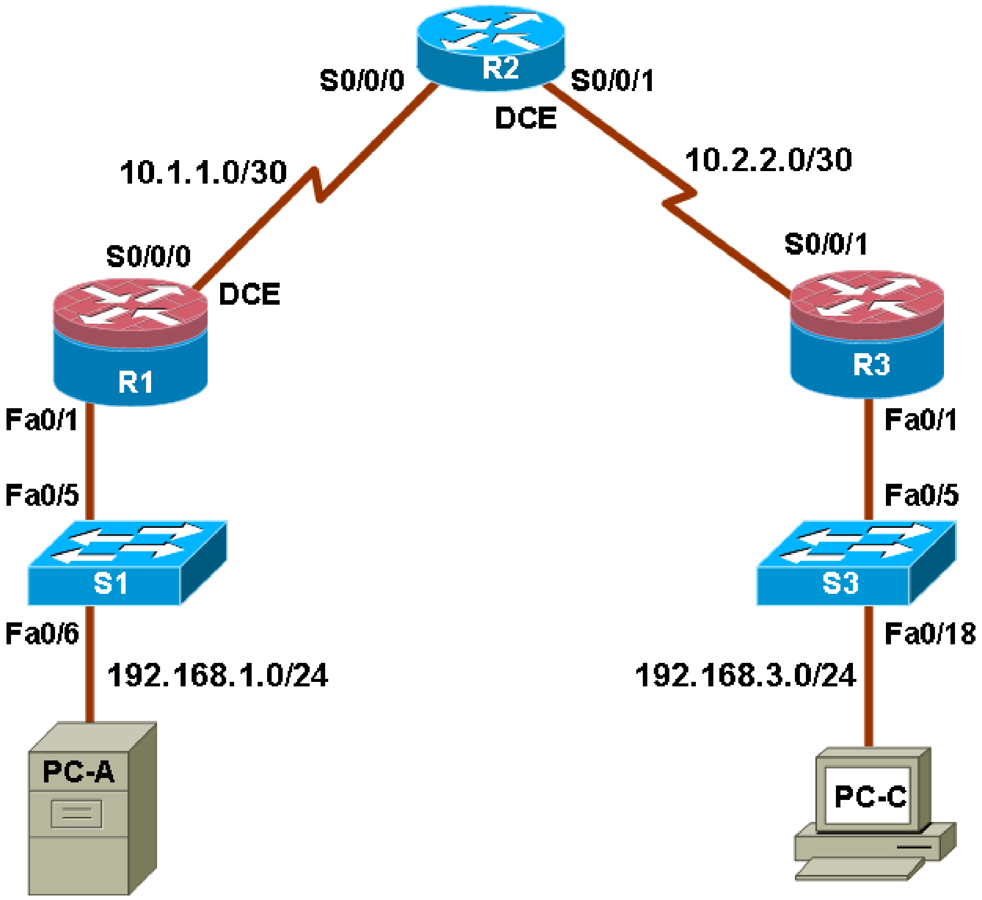
Chapter 3 Lab A: Securing Administrative Access Using AAA and RADIUS

Topology



Note: ISR G2 devices have Gigabit Ethernet interfaces instead of Fast Ethernet Interfaces.

IP 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: Basic Network Device Configuration

- 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

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 with Cisco IOS Release 12.4(20)T (Advance IP 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 12.4(20)T1 or comparable)
- 2 switches (Cisco 2960 or comparable)
- PC-A: Windows XP, Vista or Windows 7 with CCP 2.5 & RADIUS server software available
- PC-C: Windows XP, Vista or Windows 7 with CCP 2.5
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

CCP Notes:

- Refer to Chp 00 Lab A for instructions on how to install and run CCP. Hardware/software recommendations for CCP include Windows XP, Vista, or Windows 7 with Java version 1.6.0_11 up to 1.6.0_21, Internet Explorer 6.0 or above and Flash Player Version 10.0.12.36 and later.
- 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: Basic Network Device Configuration

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 shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router.

Configure host names as shown in the topology.

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

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
```

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.

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.

   Were the ping results successful? _____

   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.

   Were the ping results successful? _____

   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.

Use the **Transfer > Capture text** option in HyperTerminal or some other method to capture the running configs for each router. Save the three files so that they can be used to restore configs later in the lab.

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? Why or why not? ____

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 $Unauthorized access strictly prohibited and
prosecuted to the full extent of the law$
R1(config)# exit
```

b. Issue the **`show run`** command. What does the $ convert to in the output?

____

c. Exit privileged EXEC mode by using the **`disable`** or **`exit`** command and press **Enter** to get started. Does the MOTD banner look like what you expected? ______

Note: If it does not, just re-create it using the **`banner motd`** command.

Step 9: Save the basic configurations.

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.

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

____

e. After logging in, issue the **show run** command. Were you able to issue the command? Why or why not? ____

f. Enter privileged EXEC mode using the **enable** command. Were you prompted for a password? Why or why not? ____

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? Why or why not?

____

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
```

f. Were you prompted for a user account? Why or why not? ________________________________

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

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

i. What password did you use? ____

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

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

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

Step 4: Save the configuration on R1.

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

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

b. Use HyperTerminal or another means to save the R1 running configuration from Parts 1 and 2 of this lab and edit it so that it can be used to restore the R1 config later in the lab.

Note: Remove all occurrences of "- - More - -." Remove any commands that are not related to the items you configured in Parts 1 and 2 of the lab, such as the Cisco IOS version number, no service pad, and so on. Many commands are entered automatically by the Cisco IOS software. Also replace the encrypted passwords with the correct ones specified previously.

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

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

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

b. Use HyperTerminal or another means to save the R3 running configuration from Parts 1 and 2 of this lab and edit it so that it can be used to restore the R3 config later in the lab.

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

Step 1: Enable AAA services.

a. On R3, enable services with the global configuration command **aaa new-model**. 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.

b. 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**.

c. Log in to the console as **Admin01** with a password of **Admin01pass**. Remember that passwords are case-sensitive. Were you able to log in? Why or why not?

____

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

d. Exit to the initial router screen that displays: **`R3 con0 is now available, Press RETURN to get started.`**

e. Attempt to log in to the console as **baduser** with any password. Were you able to log in? Why or why not? ____

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

Step 3: Create a 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? Why or why not?

____

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? Why or why not?

____

____

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

You can also use CCP to configure the router to support AAA.

Note: If you configured R3 AAA authentication using Cisco IOS commands in Tasks 1 and 2, you can skip this task. If you performed Tasks 1 and 2 and you want to perform this task, you should restore R3 to its basic configuration. See Part 4, Step 1 for the procedure to restore R3 to its basic configuration.

Even if you do not perform this task, read through the steps to become familiar with the CCP process.

Step 1: Implement AAA services and HTTP router access prior to starting CCP.

a. From the CLI global config mode, enable a new AAA model.

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

b. Enable the HTTP server on R3 for CCP access.

```
R3(config)# ip http server
```

Note: For maximum security, enable secure http server by using the `ip http secure-server` command.

c. Add a user named **admin** to the local database.

```
R3(config)# username admin privilege 15 secret cisco12345
```

d. Have CCP use the local database to authenticate web sessions.

```
R3(config)# ip http authentication local
```

Step 2: Access CCP and discover R3.

a. Start CCP on PC-C. In the Manage Devices window, add R3 IP address 192.168.3.1 in the first IP address field. Enter **admin** in the Username field, and **cisco12345** in the Password field.

b. At the CCP Dashboard, click the **Discover** button to discover and connect to R3. If discovery fails, click the **Discovery Details** button to determine the problem.

Step 3: Use CCP to create an administrative user.

a. Click the **Configure** button at the top of the screen.

b. Choose **Router > Router Access > User Accounts/View**.

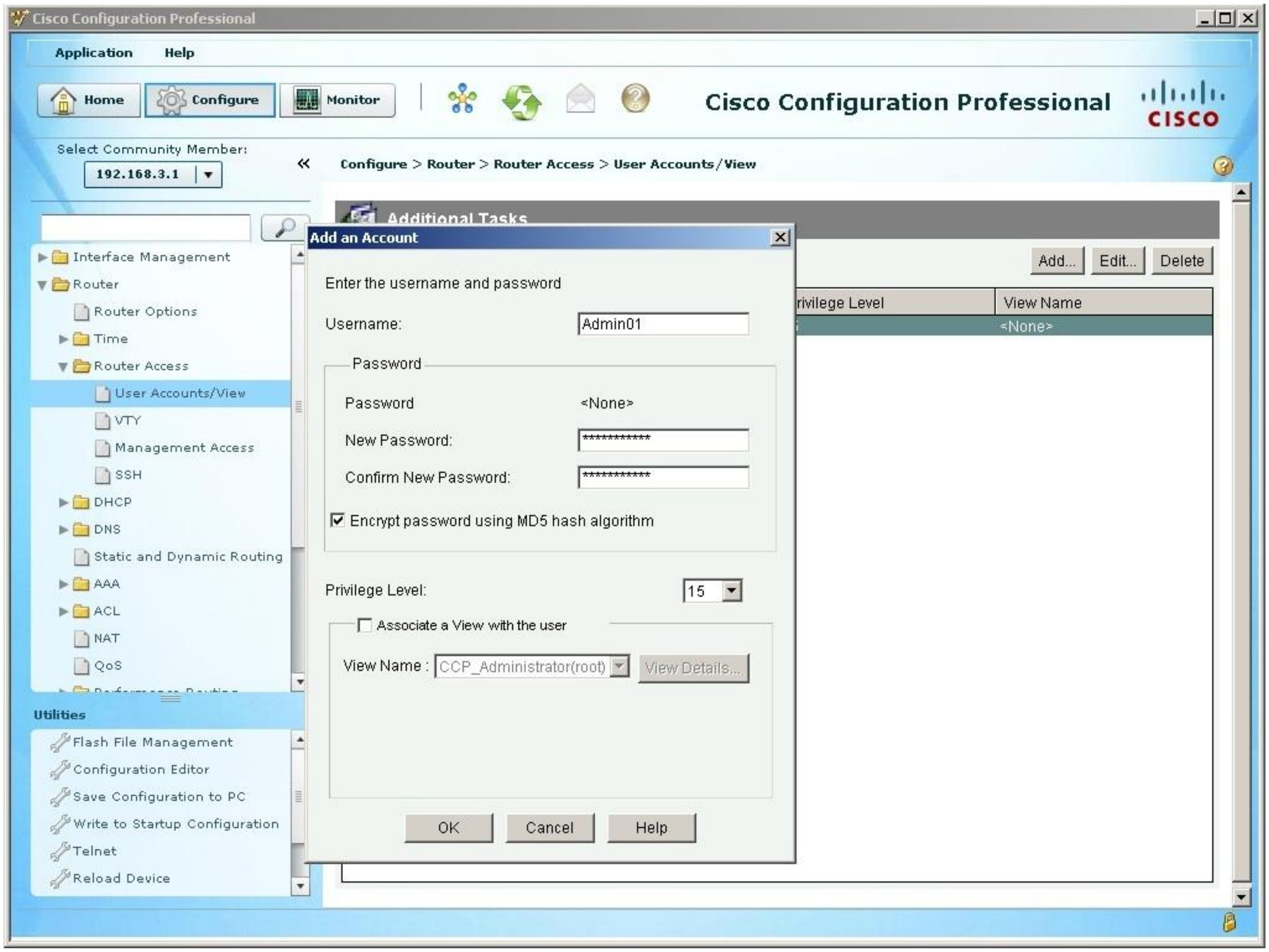
c. In the User Accounts/View window, click **Add**.

d. In the Add an Account window, enter **Admin01** in the Username field.

e. Enter the password **Admin01pass** in the New Password and Confirm New Password fields. (Remember, passwords are case-sensitive.)

f. Confirm that the **Encrypt password using MD5 hash algorithm** check box is checked.

g. Select **15** from the Privilege Level drop-down list and click **OK**.



Configure > Router > Router Access > User Accounts/View

Add an Account

Enter the username and password

Username: Admin01

Password

Password <None>

New Password: ************

Confirm New Password: ************

☑ Encrypt password using MD5 hash algorithm

Privilege Level: 15

☐ Associate a View with the user

View Name : CCP_Administrator(root)

h. In the Deliver Configuration to Router window, make sure that the Save Running Config to Router's Startup Config check box is checked, and click **Deliver**.

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

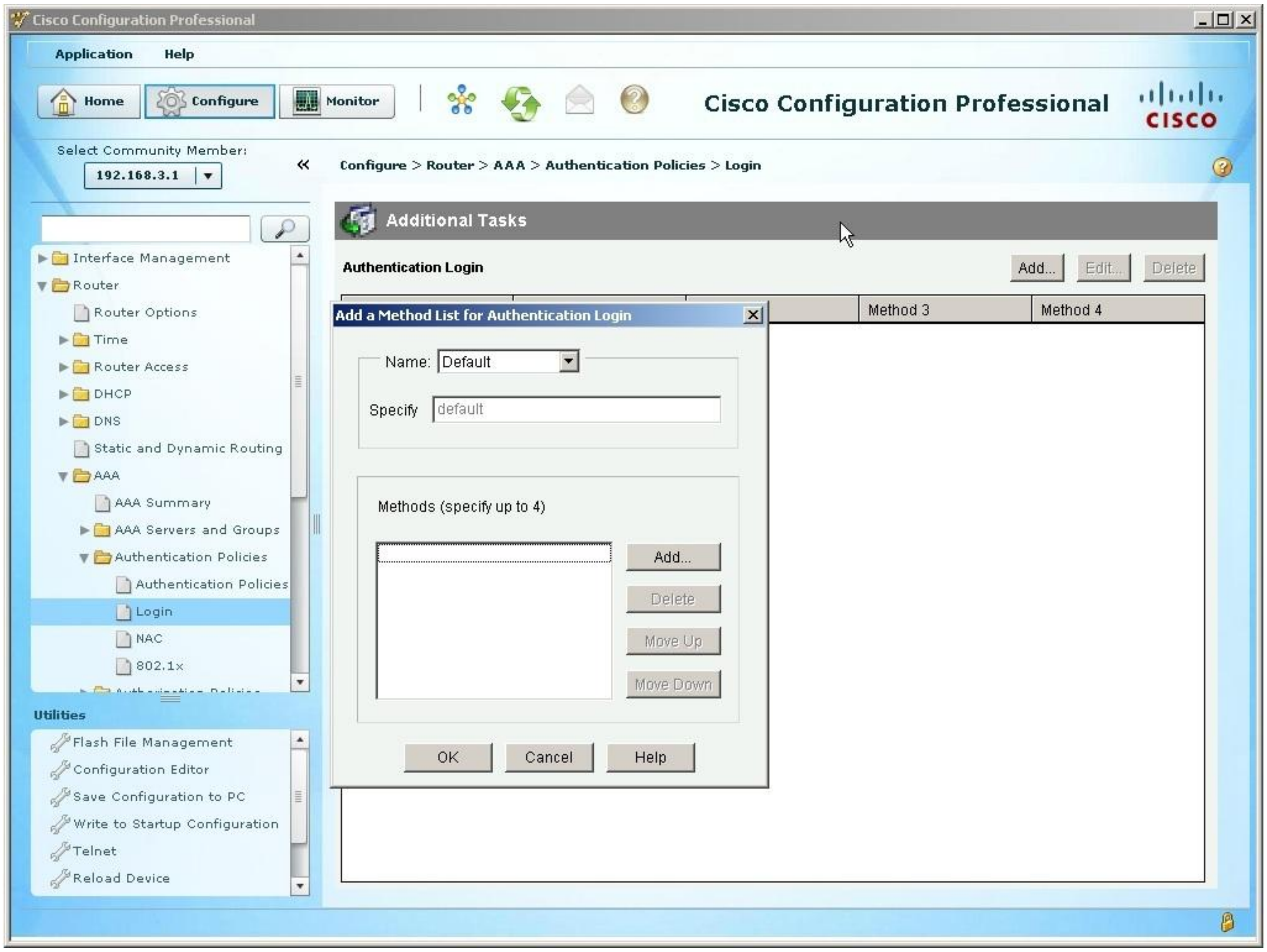
Step 4: Create AAA method list for login.

a. Click the **Configure** button at the top of the screen.

b. Choose **Router > AAA > Authentication Policies > Login**.

c. In the Authentication Login window, click **Add**.

d. In the Add a Method List for Authentication Login window, verify that **Default** is in the Name field.



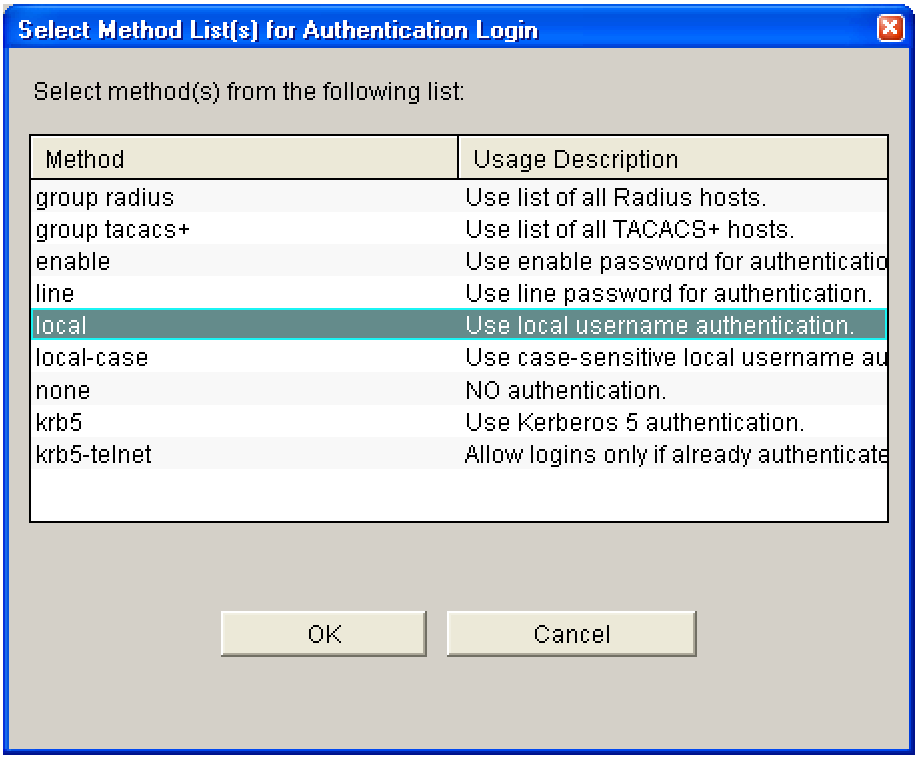
Name: Default

Specify: default

Methods (specify up to 4)

e. Click **Add** in the Methods section.

f. In the Select Method List(s) for Authentication Login window, choose **local** and click **OK**. Take note of the other methods listed, which include RADIUS (group radius) and TACACS+ (group tacacs+).



Select Method List(s) for Authentication Login

Select method(s) from the following list:

Method	Usage Description
group radius	Use list of all Radius hosts.
group tacacs+	Use list of all TACACS+ hosts.
enable	Use enable password for authenticatio
line	Use line password for authentication.
local	Use local username authentication.
local-case	Use case-sensitive local username au
none	NO authentication.
krb5	Use Kerberos 5 authentication.
krb5-telnet	Allow logins only if already authenticate

g. Click **OK** to close the window.

h. Repeat steps 4f and 4g. Choose **none** as a second authentication method and click the **OK** button when done.

i. In the Deliver Configuration to Router window, make sure that the Save Running Config to Router's Startup Config checkbox is checked, and click **Deliver**. In the Commands Delivery Status window, click **OK**.

j. What command was delivered to the router?

____

Step 5: Verify the AAA username and profile for console login.

a. Exit to the initial router screen that displays:

```
R3 con0 is now available, Press RETURN to get started.
```

b. Log in to the console as **Admin01** with a password of **Admin01pass**. Were you able to login? Why or why not? ____

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**. Were you able to login? Why or why not?

____

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

e. Log in to the console as **Admin01** with a password of **Admin01pass**. Access privileged EXEC mode using the enable secret password **cisco12345** and then show the running config. What commands are associated with the CCP session?

____

____

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 v
rf= (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 v
rf= (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? ________________________________

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 router 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 Router R1 to Its Basic Settings

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: Erase and reload the router.

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. Erase the startup config and then issue the **reload** command to restart the router.

Step 2: Restore the basic configuration.

a. When the router restarts, enter privileged EXEC mode with the **enable** command, and then enter global config mode. Use the HyperTerminal **Transfer > Send File** function, cut and paste or use another method to load the basic startup config for R1 that was created and saved in Part 2 of this lab.

b. 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.

c. 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**.

d. Save the running config to the startup config using the `copy run start` command.

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 XP and most other Windows operating systems. The free version of the software can support only five usernames.

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. Download the latest version from http://www.suggestsoft.com/soft/itconsult2000/winradius/, http://winradius.soft32.com, http://www.brothersoft.com/winradius-20914.html**.**

c. Save the downloaded zip file in the folder you created in Step 1a, and extract the zipped files to the same folder. There is no installation setup. The extracted WinRadius.exe file is executable.

d. 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:

1. Compatibility settings:

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

    b. 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.

    c. Click **OK**.

2. **Run as Administrator** settings:

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

    b. 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.

    c. Click **OK**.

3. **Run as Administration** for each launch:

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

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

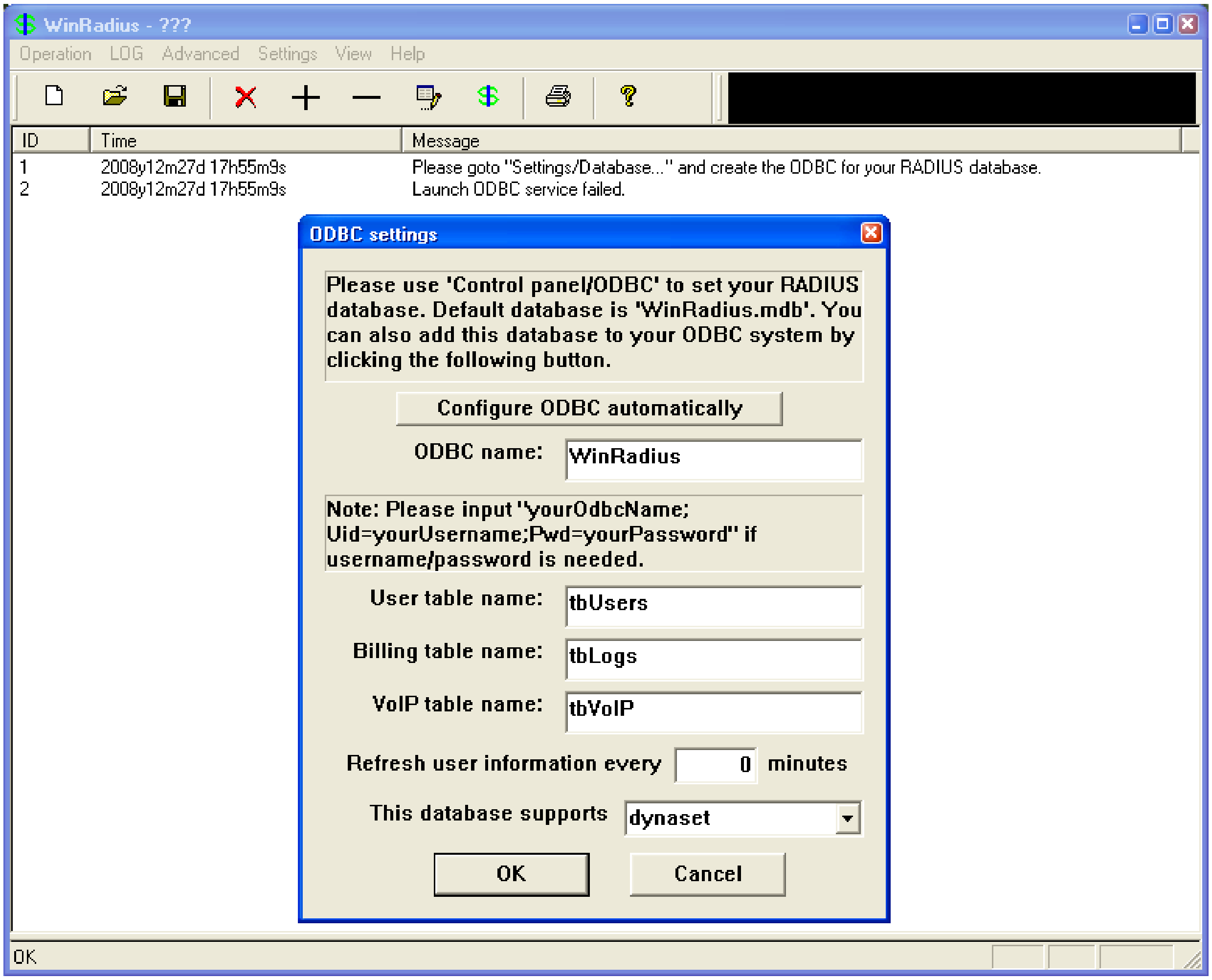
Step 2: Configure the WinRadius server database.

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.


WinRadius - ???
Operation LOG Advanced Settings View Help
ODBC settings
Configure ODBC automatically
OK
Cancel

```
ID  Time               Message
1   2008y12m27d 17h55m9s   Please goto "Settings/Database..." and create the ODBC for your RADIUS database.
2   2008y12m27d 17h55m9s   Launch ODBC service failed.
```

Please use 'Control panel/ODBC' to set your RADIUS database. Default database is 'WinRadius.mdb'. You can also add this database to your ODBC system by clicking the following button.

ODBC name: WinRadius

Note: Please input 'yourOdbcName; Uid=yourUsername;Pwd=yourPassword" if username/password is needed.

User table name: tbUsers

Billing table name: tbLogs

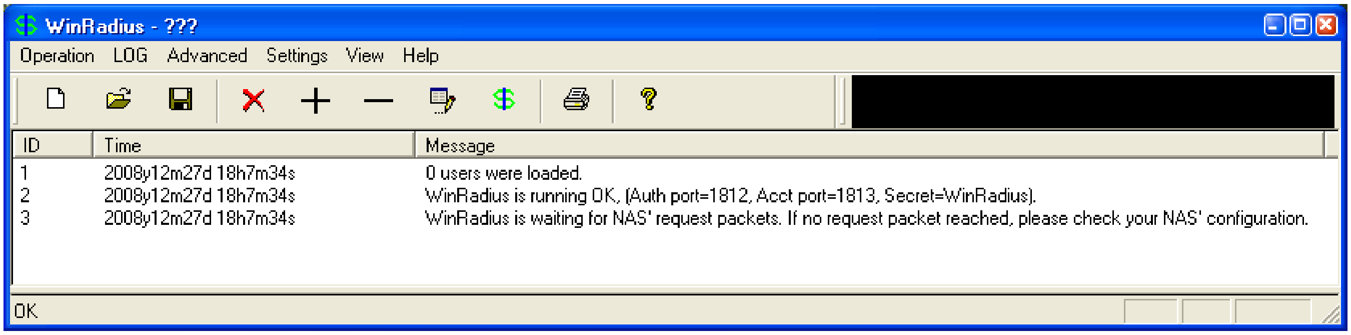
VoIP table name: tbVoIP

Refresh user information every 0 minutes

This database supports dynaset

OK

c. When WinRadius starts again, you should see messages similar to the following displayed.



```
ID  Time                Message
1   2008y12m27d 18h7m34s  0 users were loaded.
2   2008y12m27d 18h7m34s  WinRadius is running OK, (Auth port=1812, Acct port=1813, Secret=WinRadius).
3   2008y12m27d 18h7m34s  WinRadius is waiting for NAS' request packets. If no request packet reached, please check your NAS' configuration.
OK
```

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

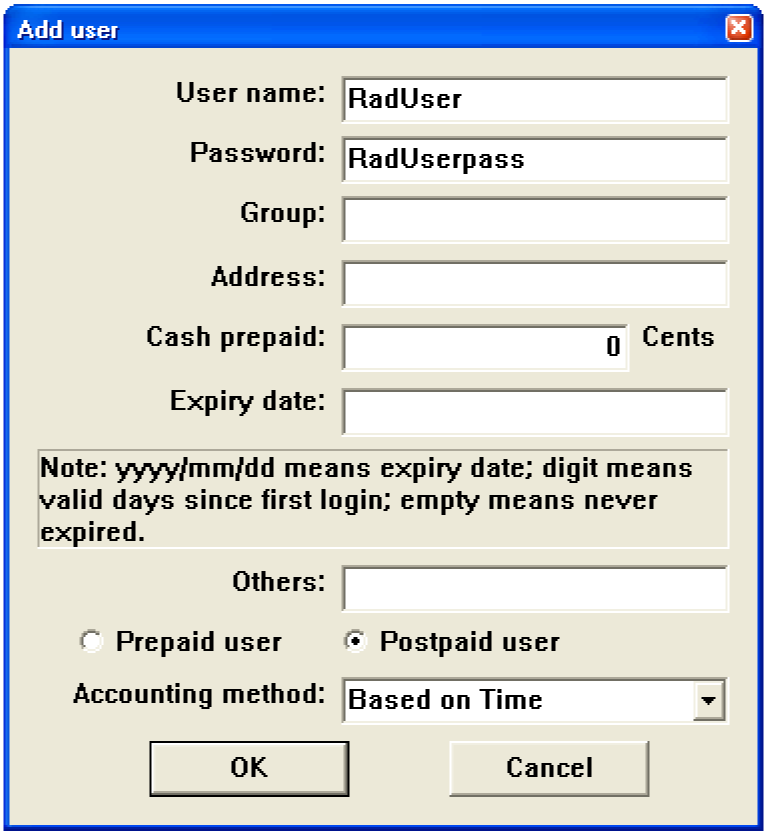
____

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

Note: The free version of WinRadius can support only five usernames. The usernames are lost if you exit the application and restart it. Any usernames created in previous sessions must be re-created. Note that the first message in the previous screen shows that zero users were loaded. No users had been created prior to this, but this message is displayed each time WinRadius is started, regardless of whether users were created or not.

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.



User name: RadUser

Password: RadUserpass

Group:

Address:

Cash prepaid: 0 Cents

Expiry date:

Note: yyyy/mm/dd means expiry date; digit means valid days since first login; empty means never expired.

Others:

○ Prepaid user ● Postpaid user

Accounting method: Based on Time

c. Click **OK**. You should see a message on the log screen that the user was added successfully.

Step 4: Clear the log display.

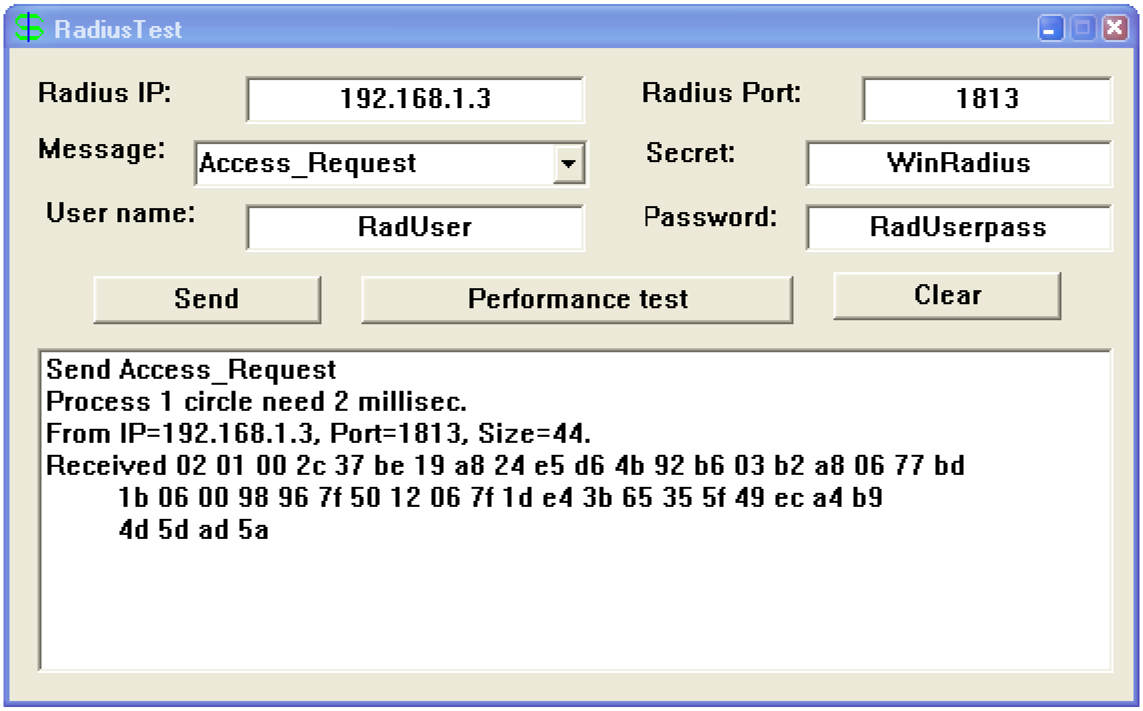
From the main menu, choose **Log > Clear**.

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. On the WinRadius log display, you should also see a message indicating that user RadUser was authenticated successfully.



Radius IP: 192.168.1.3
Radius Port: 1813
Message: Access_Request
Secret: WinRadius
User name: RadUser
Password: RadUserpass

```
Send Access_Request
Process 1 circle need 2 millisec.
From IP=192.168.1.3, Port=1813, Size=44.
Received 02 01 00 2c 37 be 19 a8 24 e5 d6 4b 92 b6 03 b2 a8 06 77 bd
         1b 06 00 98 96 7f 50 12 06 7f 1d e4 3b 65 35 5f 49 ec a4 b9
         4d 5d ad 5a
```

d. 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.

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? Why or why not? ____

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 accounting 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`**. The following command displays all running config lines that include the text “radius”.

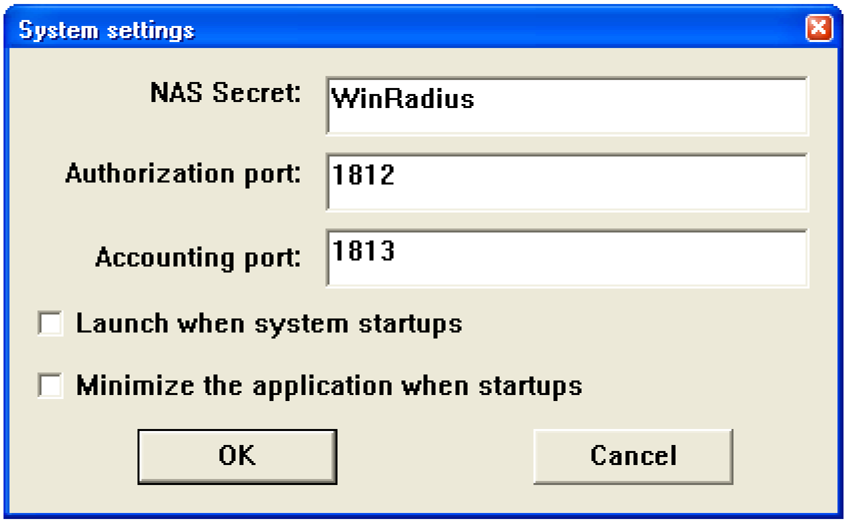
```
R1# show run | incl radius
aaa authentication login default group radius none
radius-server host 192.168.1.3 auth-port 1645 acct-port 1646 key 7
097B47072B04131B1E1F
```

< Output omitted >

c. 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.

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



NAS Secret: WinRadius

Authorization port: 1812

Accounting port: 1813

□ Launch when system startups

□ Minimize the application when startups

b. What are the default WinRadius UDP port numbers? ______________________________________

Note: The early deployment of RADIUS was done using UDP port number 1645 for authentication and 1646 for accounting, which conflicts with the datametrics service. Because of this conflict, 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. In this step, you modify the IOS port numbers to those of the RADIUS server, which are specified in RFC 2865.

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`**.

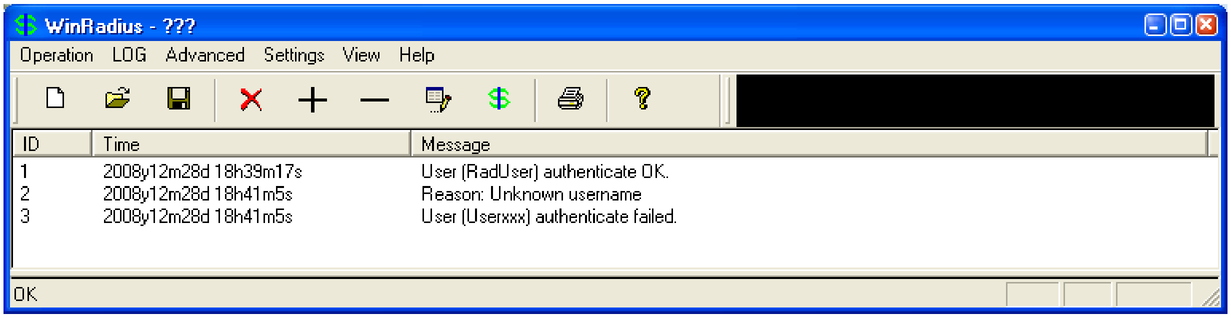
e. Log in again using an invalid username of **Userxxx** and the password of **Userxxxpass**. Were you able to login? ____

What message was displayed on the router? ____

The following messages should display on the RADIUS server log.

```
Reason: Unknown username

User (Userxxx) authenticate failed
```



```
ID  Time                  Message
1   2008y12m28d 18h39m17s User (RadUser) authenticate OK.
2   2008y12m28d 18h41m5s  Reason: Unknown username
3   2008y12m28d 18h41m5s  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
```

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
```

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?

____

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?

____

Task 5: (Optional) Configure R1 AAA Services and Access the RADIUS Server Using CCP

You can also use CCP to configure the router to access the external RADIUS server.

Note: If you configured R1 to access the external RADIUS server using Cisco IOS in Task 3, you can skip this task. If you performed Task 3 and you want to perform this task, restore the router to its basic configuration as described Task 1 of this part, except log in initially as RadUser with the password RadUserpass**.** If the RADIUS server is unavailable at this time, you will still be able to log in to the console.

If you do not perform this task, read through the steps to become familiar with the CCP process.

Step 1: Implement AAA services and HTTP router access prior to starting CCP.

a. From the CLI global config mode, enable a new AAA model.

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

b. Enable the HTTP server on R1.

```
R1(config)# ip http server
```

c. Add a user named **admin** to the local database.

```
R1(config)# username admin privilege 15 secret cisco12345
```

d. Have CCP use the local database to authenticate web sessions.

```
R1(config)# ip http authentication local
```

Step 2: Access CCP and discover R1.

a. Start CCP on PC-C. In the Manage Devices window, add R1 IP address 192.168.1.1 in the first IP address field. Enter **admin** in the Username field, and **cisco12345** in the Password field.

b. At the CCP Dashboard, click the **Discover** button to discover and connect to R3. If discovery fails, click the **Discovery Details** button to determine the problem.

Step 3: Configure R1 AAA to access the WinRADIUS server.

a. Click the **Configure** button at the top of the screen.

b. Choose **Router > AAA > AAA Servers and Groups > Servers**.

c. In the AAA Servers window, click **Add**.

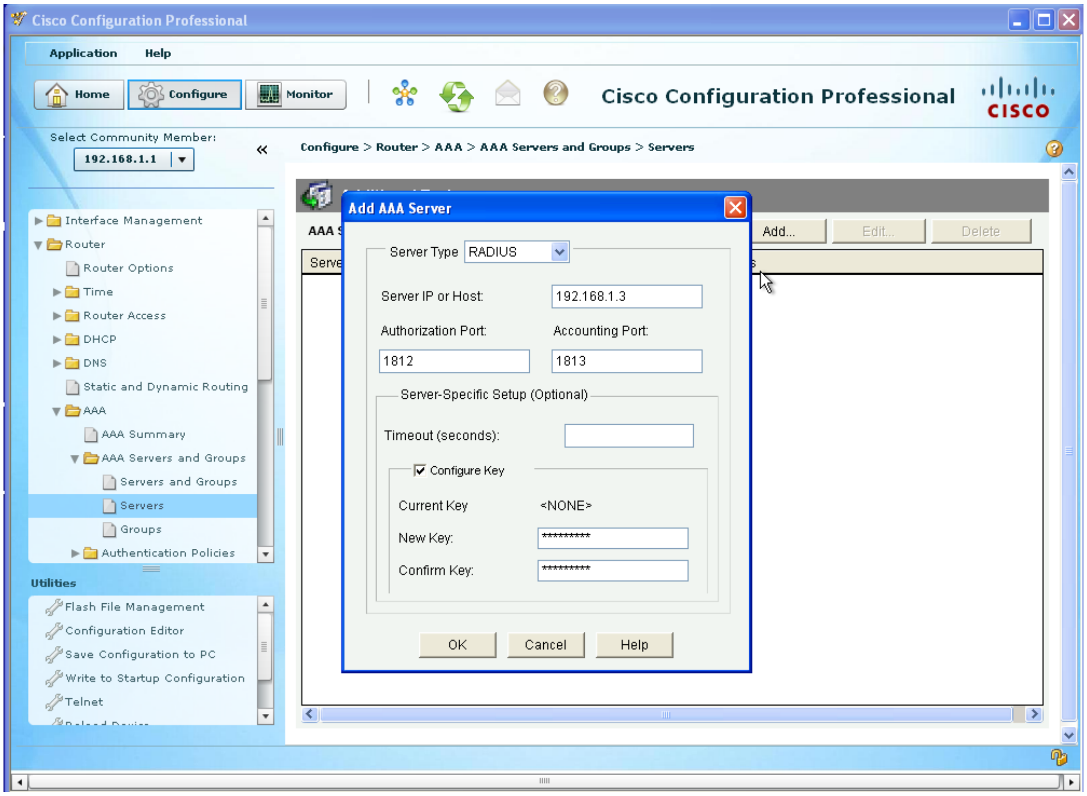
d. In the Add AAA Server window, verify that **RADIUS** is in the Server Type field.

e. In the Server IP or Host field, enter the IP address of PC-A, **192.168.1.3**.

f. Change the **Authorization Port** from 1645 to 1812, and change the **Accounting Port** from 1646 to 1813 to match the RADIUS server port number settings.

g. Check the **Configure Key** check box.

h. Enter **WinRadius** in both the New Key and Confirm Key fields.



Add AAA Server

Server Type: RADIUS

Server IP or Host: 192.168.1.3

Authorization Port: 1812

Accounting Port: 1813

Server-Specific Setup (Optional)

Timeout (seconds):

☑ Configure Key

Current Key: <NONE>

New Key: **********

Confirm Key: **********

i. In the Deliver Configuration to Router window, click **Deliver**, and in the Commands Delivery Status window, click **OK**.

j. What command was delivered to the router?

____

____

Step 4: Configure the R1 AAA login method list for RADIUS.

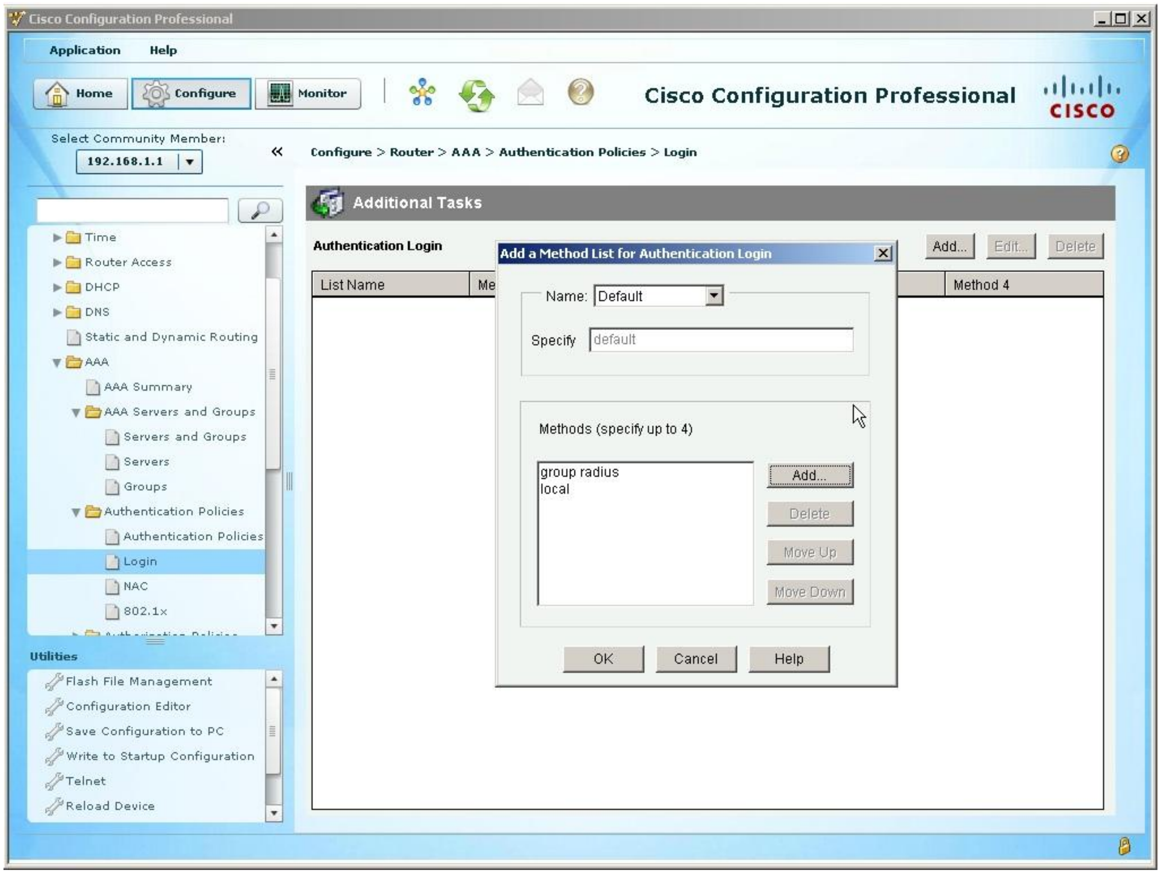
a. Click the **Configure** button at the top of the screen.

b. Choose **Router > AAA > Authentication Policies > Login**.

c. In the Authentication Login window, click **Add**.

d. In the Select Method List(s) for Authentication Login window, choose **group radius** and click **OK**.

e. In the Select Method List(s) for Authentication Login window, choose **local** as a second method and click **OK**.



Name: Default

Specify: default

Methods (specify up to 4)

group radius
local

f. In the Deliver Configuration to Router window, click **Deliver** and in the Commands Delivery Status window, click **OK**.

g. What command(s) were delivered to the router?

____

____

Step 5: Test your configuration.

a. If you restarted the RADIUS 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**.

c. Test your configuration by opening a Telnet session from PC-A to R1.

```
C:> telnet 192.168.1.1
```

d. At the login prompt, enter the username **RadUser** defined on the RADIUS server and a password of **RadUserpass**.

Were you able to login to R1? _____

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)
2800	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.				