

Securing Administrative Access Using AAA and RADIUS

Objectives

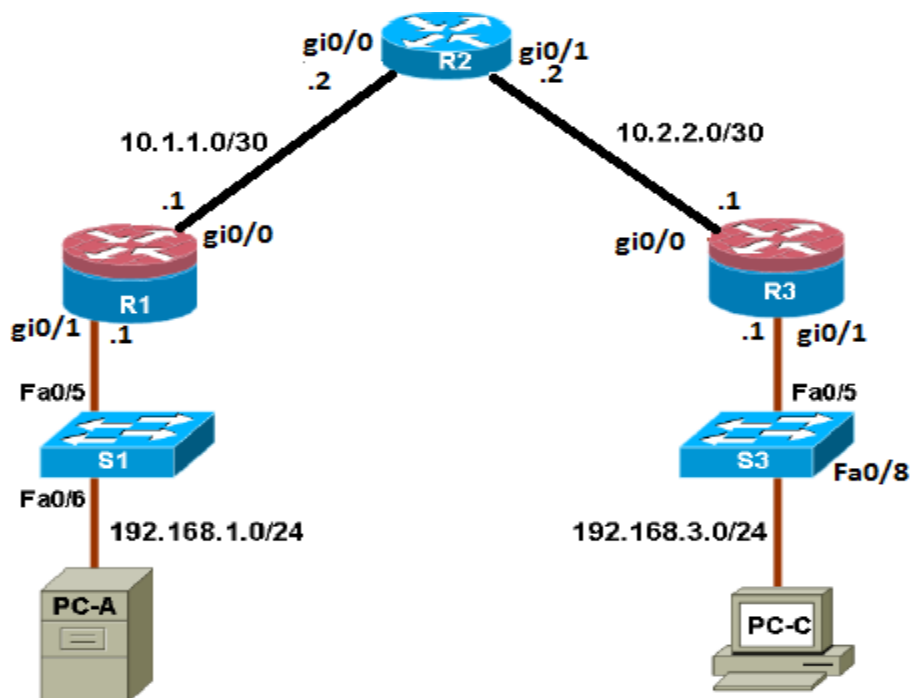
Part 1: Basic Network Device Configuration

Part 2: Configure Local Authentication

Part 3: Configure Local Authentication Using AAA

Part 4: Configure Centralized Authentication Using AAA and RADIUS

Topology



Part 1: Basic Network Device Configuration

Step1: Read and analyze the network map. Set physical links and apply IP settings on routers and PCs. Apply static routes on routers. Test IP connectivity between PCs.

Step 2: 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.

- 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 lab1234567
```

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 conlinepass
```

```
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 auxlinepass
```

```
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 vtylinepass
```

```
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?

No, it was encrypted.

```
R1
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****^C
!
line con 0
  exec-timeout 5 0
  password 7 00071C08085205031F205F5D
  logging synchronous
  login
line aux 0
  exec-timeout 5 0
  password 7 1218100F1E0202013A2A373B
  login
line vty 0 4
  exec-timeout 5 0
  password 7 15041F150823252138322631
  login
  transport input none
!
no scheduler allocate
!
end

R1#
```

Part 2: Configure Local Authentication

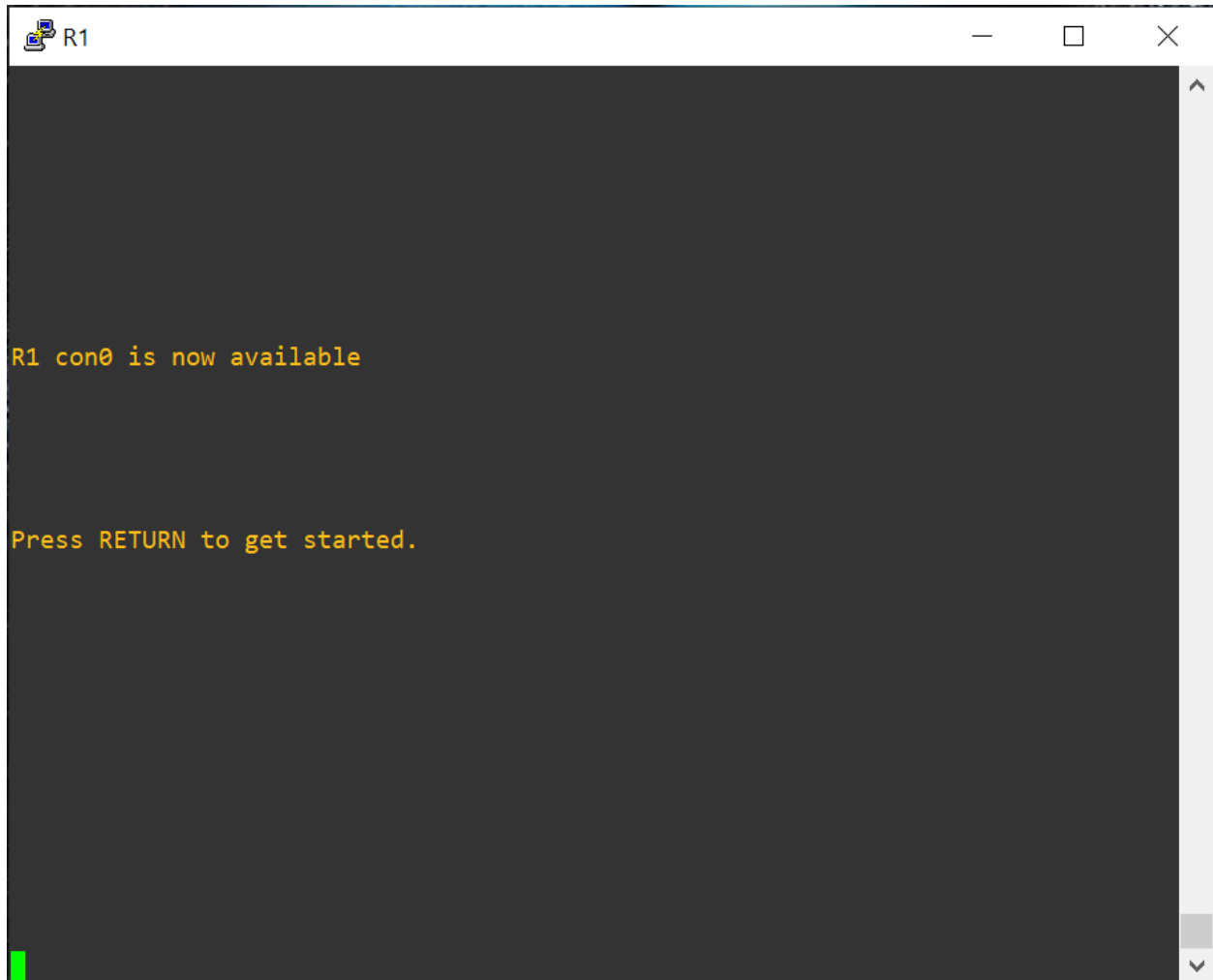
Configure a local username and password and change the access for the console, aux, and vty lines to reference the router's local database for valid usernames and passwords. Perform all steps on R1 and R3. The procedure for R1 is shown here.

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?



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

```
R1

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

User Access Verification

Username: user01
Password:
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

R1>
```

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

It was login directly without asking for credential.

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

No, it cannot run. Because the current user (user01) is not a privileged user.

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

Yes. The current user is not a privileged user.

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

a. From PC-A, establish a Telnet session with R1. (transport input telnet)

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

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

Nope. Username for telnet is not defined on (R1). Only password is defined in line tty part.

```
PC-A
Router#telnet 192.168.1.1
Trying 192.168.1.1 ... Open

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

User Access Verification

Password:
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

R1>
```

c. What password did you use to login?

vtlinepass

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?

Yes. Login local means using the local user database on R1.

```
PC-A
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****
R1>
[Connection to 192.168.1.1 closed by foreign host]
Router#telnet 192.168.1.1
Trying 192.168.1.1 ... Open

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

User Access Verification

Username: user01
Password:
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****
R1>
```

- 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?
lab1234567

Step 4: Let other group member perform steps 1 through 3 on R3.

Notes:

Part 3: Configure Local Authentication Using AAA on R3

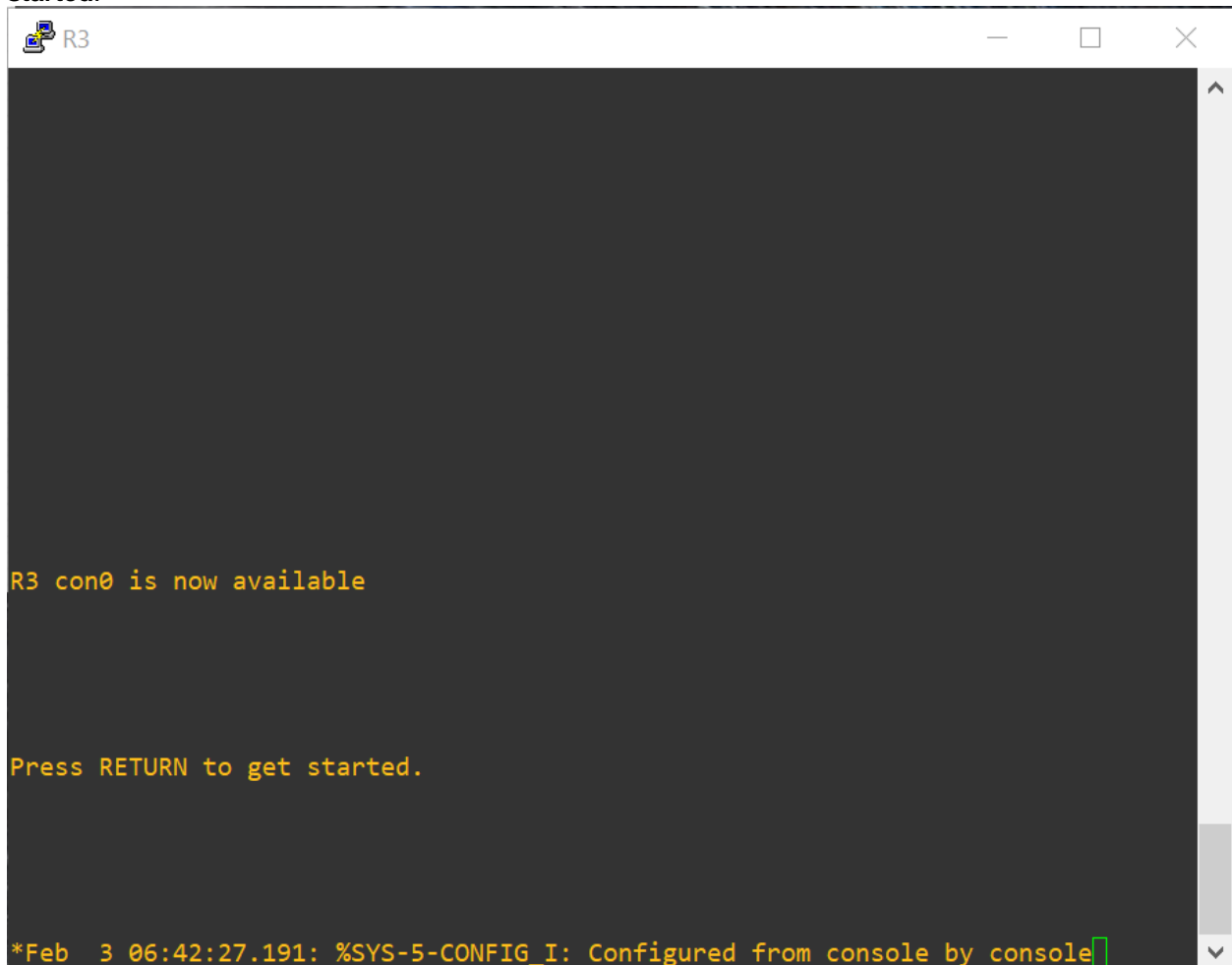
Task 1: Configure the Local User Database Using Cisco IOS

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?
No.

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.**



```
R3  
R3 con0 is now available  
  
Press RETURN to get started.  
  
*Feb 3 06:42:27.191: %SYS-5-CONFIG_I: Configured from console by console
```

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?

Yes. The server defined the local login user and password in the config.

```
R3

*Feb  3 06:42:27.191: %SYS-5-CONFIG_I: Configured from console by console
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

User Access Verification

Username: Admin01
Password:

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

R3>
```

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

Yes. The key words "local none" allow anyone can login.

```
R3
Press RETURN to get started.

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

User Access Verification

Username: baduser

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

R3>
```

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?

Yes. TELNET_LINKS is defined for remote telnet login

```
PC-C
* Cisco in writing.
*****
PC-C>
PC-C>ena
PC-C#telnet 192.168.3.1
Trying 192.168.3.1 ... Open

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing.
*****

User Access Verification

Username: Admin01
Password:

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing.
*****
R3>
```

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?
No. Server is configured to need local credential to login for telnet.

```
PC-C
* education. IOSv is provided as-is and is not supported by Cisco's
* Technical Advisory Center. Any use or disclosure, in whole or in part,
* of the IOSv Software or Documentation to any third party for any
* purposes is expressly prohibited except as otherwise authorized by
* Cisco in writing.
*****
R3>exit

[Connection to 192.168.3.1 closed by foreign host]
PC-C#telnet 192.168.3.1
Trying 192.168.3.1 ... Open

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS
* education. IOSv is provided as-is and is not supported by Cisco's
* Technical Advisory Center. Any use or disclosure, in whole or in part,
* of the IOSv Software or Documentation to any third party for any
* purposes is expressly prohibited except as otherwise authorized by
* Cisco in writing.
*****

User Access Verification

Username: baduser
Password:

% Authentication failed

Username:
Username: [ ]
```

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

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.

- Connect to the R1 console, and log in with the username **Admin01(user01)** and password **Admin01pass(user01pass)**.
- Enter privileged EXEC mode with the password **cisco12345(lab1234567)**.
- Erase the startup config and then issue the **reload** command to restart the router (Type **no**, so not to save running-config before reloading).

Task 2: Install a RADIUS Server on PC-A

Step 1: Install and configure a RADIUS Server on PC-A

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**.

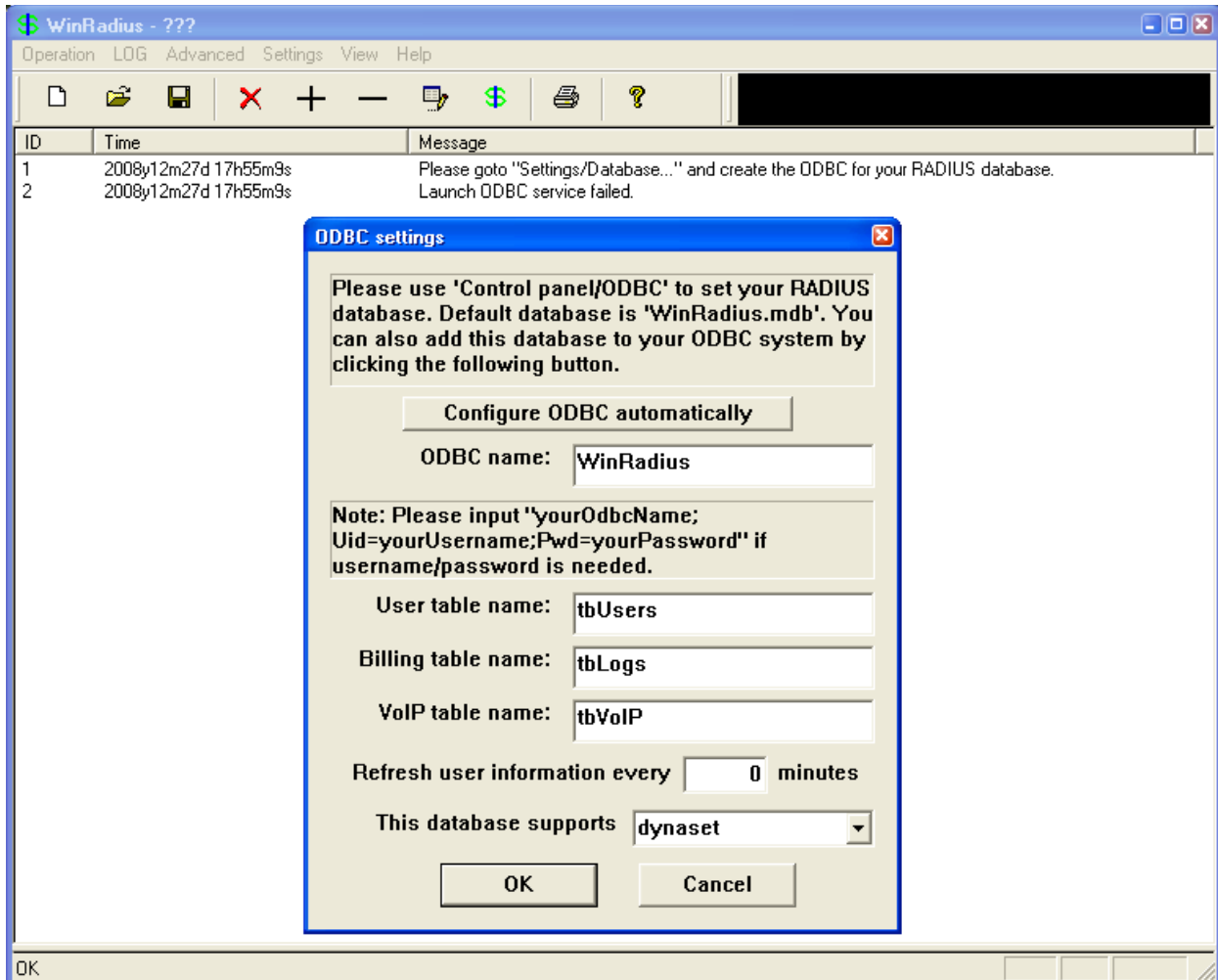
3. Run as Administration for each launch:

- 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.

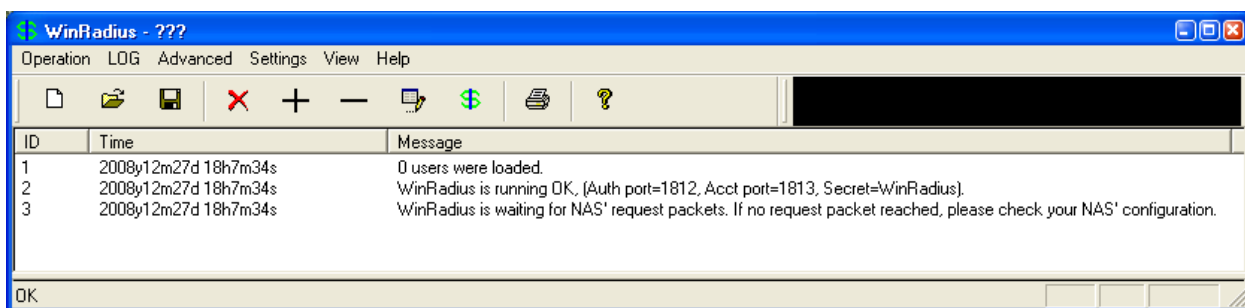
Step 2: Configure the WinRadius server database.

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.



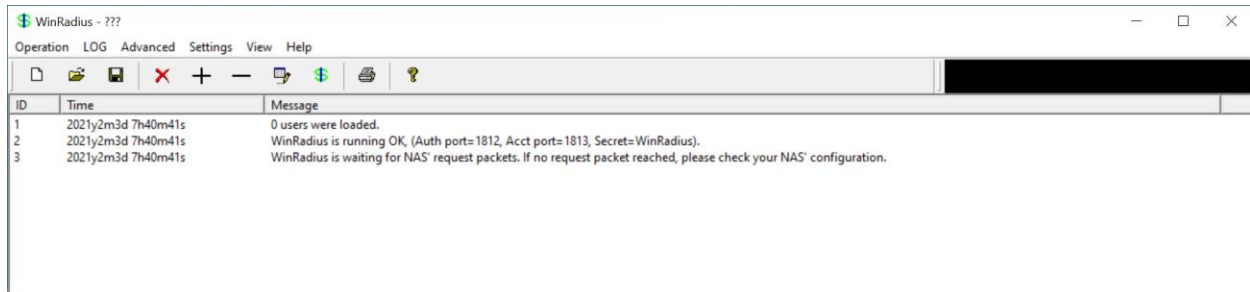
c. When WinRadius starts again, you should see messages similar to the following displayed.



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

Hint: The authentication port is 1812, and the accounting port is 1813.

1812 for Authentication and 1813 for 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.

Add user

User name:

Password:

Group:

Address:

Cash prepaid: Cents

Expiry date:

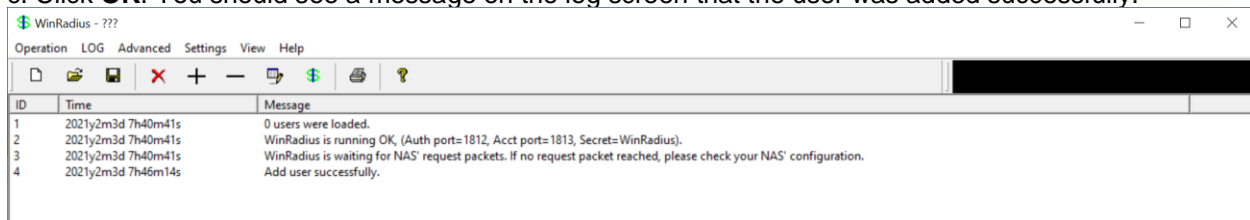
Note: yyyy/mm/dd means expiry date; digit means valid days since first login; empty means never expired.

Others:

Prepaid user Postpaid user

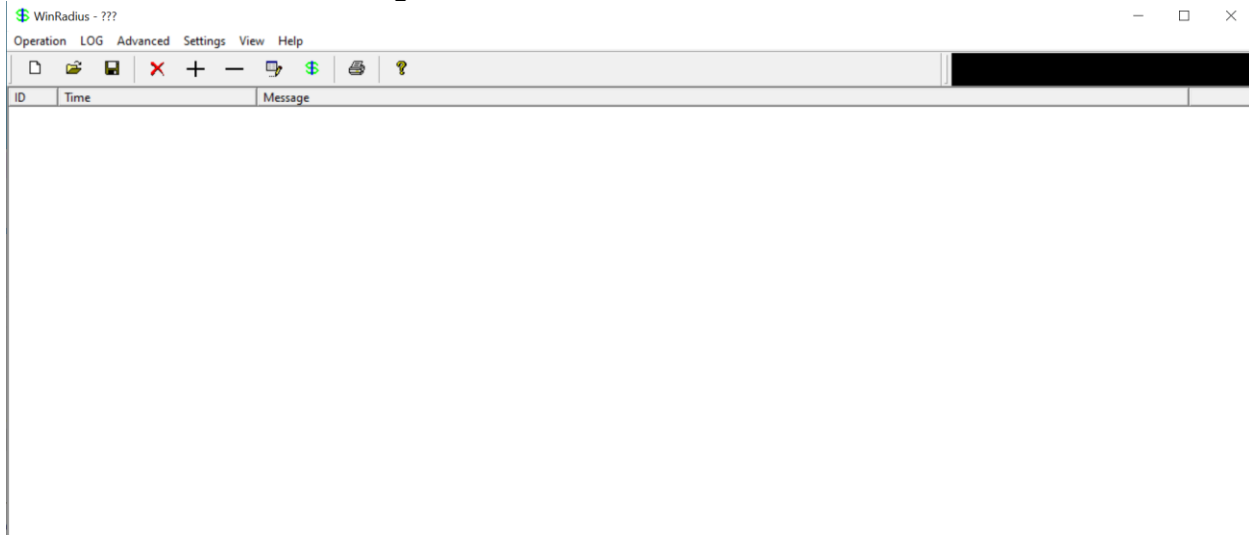
Accounting method:

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



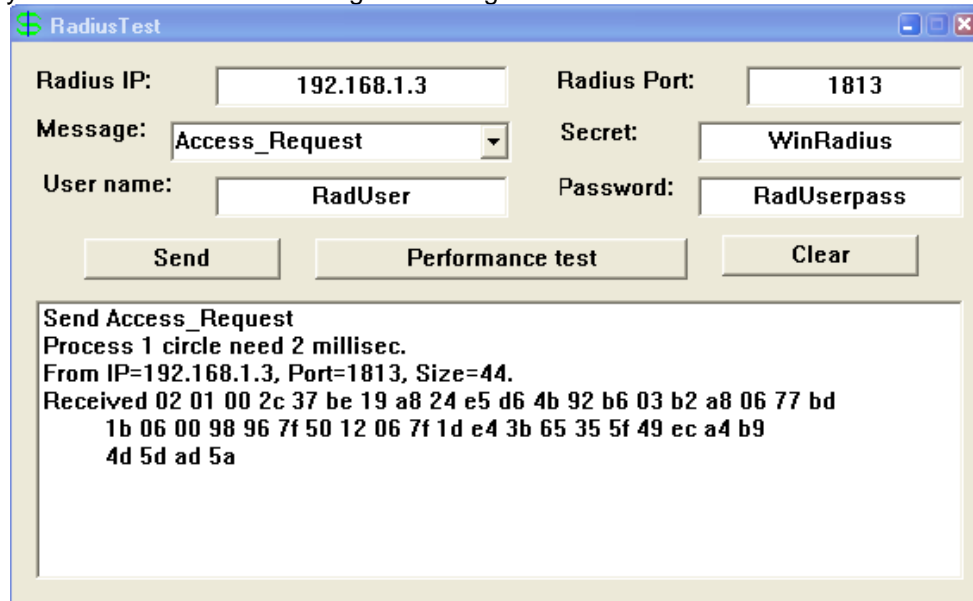
Step 4: Clear the log display.

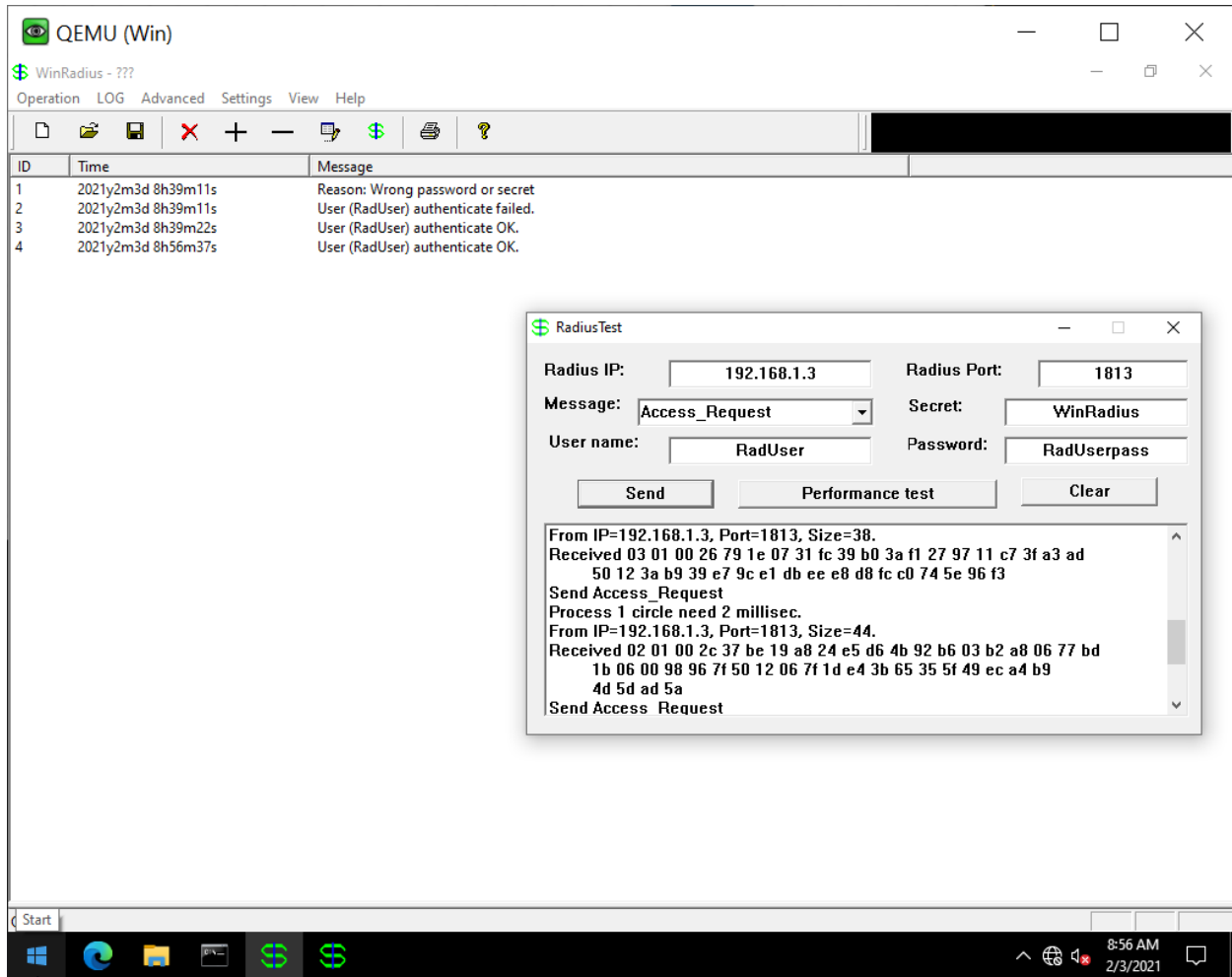
From the main menu, choose **Log > Clear**.



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.





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

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 (please note that it is not recommended in production environment). This is a safeguard measure in case the router starts up without connectivity to an active RADIUS server in this lab.

```
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
```

```
R1(config)#radius-server host
R1(config)#radius-server host
R1(config)#radius-server host
R1(config)#radius-server host 192.168.1.3 key WinRadius
Warning: The CLI will be deprecated soon
'radius-server host 192.168.1.3 key WinRadius'
Please move to 'radius server <name>' CLI.
R1(config)#
!
!
radius-server host 192.168.1.3 key WinRadius
!
radius server 192.168.1.3
address ipv4 192.168.1.3 auth-port 1645 acct-port 1646
key WinRadius
!
!
!
radius-server host 192.168.1.3 key WinRadius
!
radius server 192.168.1.3
address ipv4 192.168.1.3 auth-port 1812 acct-port 1813
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**.

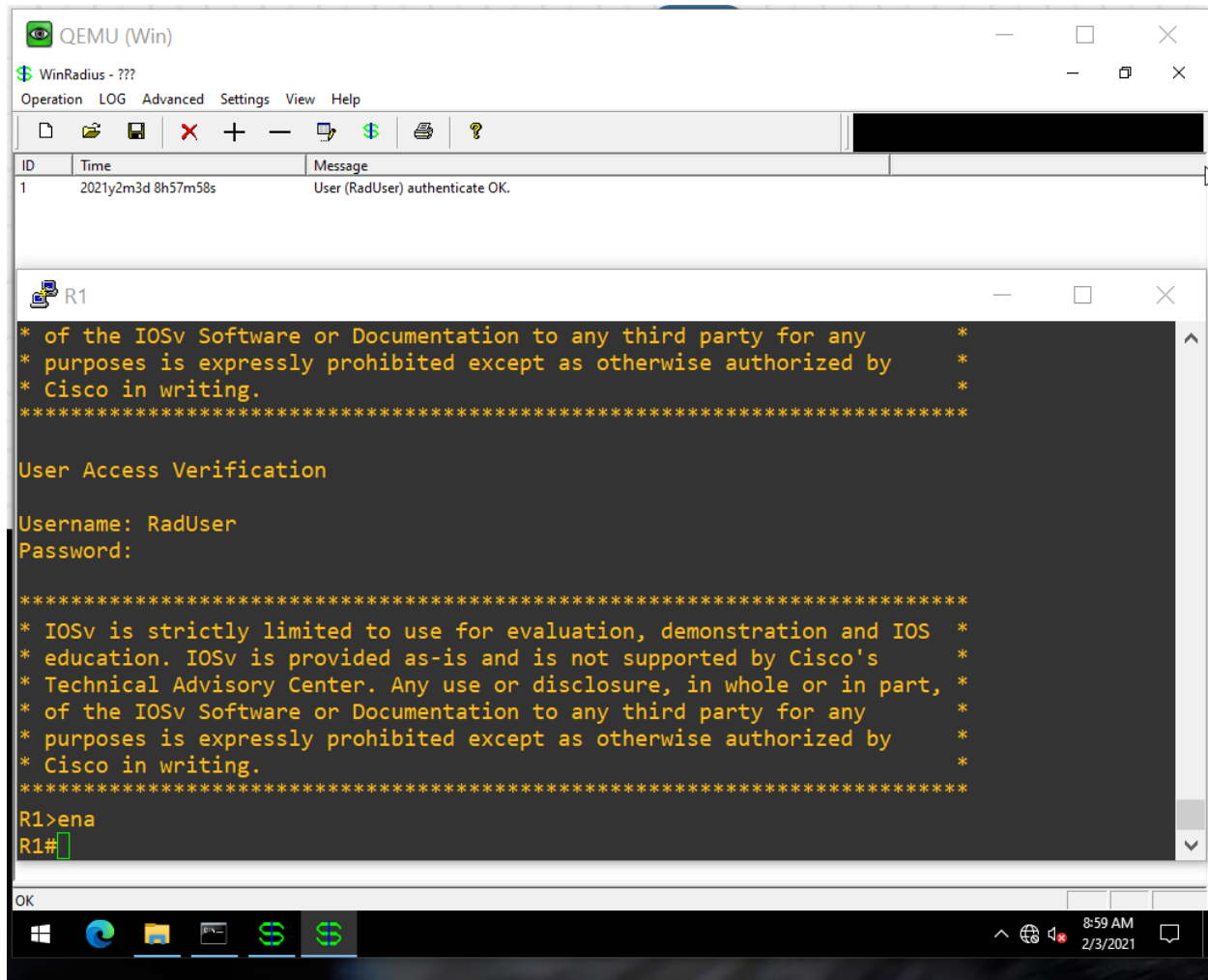
b. Clear the log on the WinRadius server by choosing **Log > Clear** from the main menu.

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?

Yes, I can login and gain access to user EXEC prompt. There was around 30 sec of 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?

I cannot login.

QEMU (Win) WinRadius - ???

Operation LOG Advanced Settings View Help

ID	Time	Message
1	2021y2m3d 8h57m58s	User (RadUser) authenticate OK.
2	2021y2m3d 9h4m9s	Reason: Unknown username
3	2021y2m3d 9h4m9s	User (uasdd) authenticate failed.

R1

```

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing.
*****

User Access Verification

Username: uasdd
Password:

% Authentication failed

Username: [

```

OK

9:04 AM 2/3/2021

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

Operation LOG Advanced Settings view Help

ID	Time	Message
1	2021y2m3d 8h57m58s	User (RadUser) authenticate OK.
2	2021y2m3d 9h4m9s	Reason: Unknown username
3	2021y2m3d 9h4m9s	User (uasdd) authenticate failed.

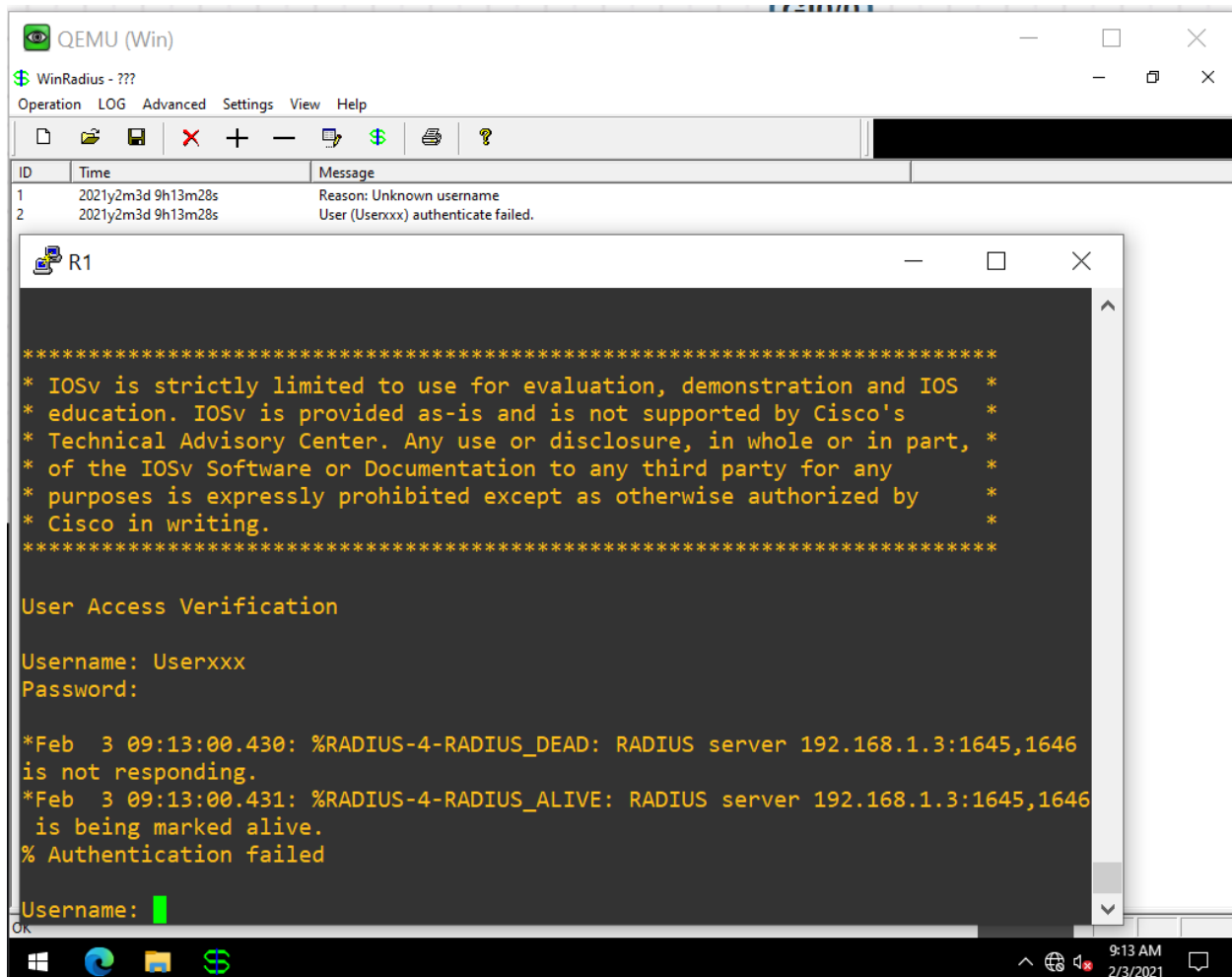
h. Why was a nonexistent username able to access the router and no messages are displayed on the RADIUS server log screen?

Cannot login anymore they fixed it in 15.6(T)

```

R1#sh ver
Cisco IOS Software, IOSv Software (VIOS-ADVENTERPRISEK9-M), Version 15.6(1)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 20-Nov-15 13:39 by prod_rel_team

```



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 ? →enter
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 >
```

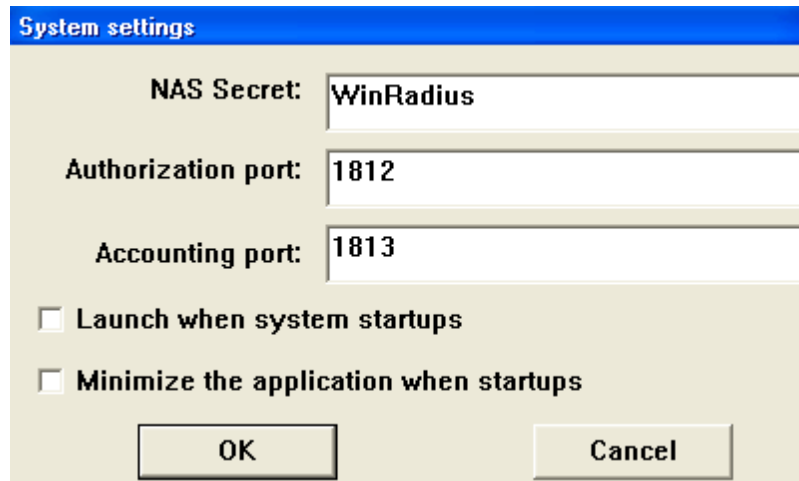
b. Check the R1 running configuration for lines containing the command **radius**. The following command displays all running config lines that include the text "radius".

```
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?
Hint: 1645 and 1646

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

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



b. What are the default WinRadius UDP port numbers?
Hint: 1812 and 1813

```
!
!
radius-server host 192.168.1.3 key WinRadius
!
radius server 192.168.1.3
 address ipv4 192.168.1.3 auth-port 1645 acct-port 1646
 key WinRadius
!
```

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?

Yes. I can login and there was about 30 sec of delay.

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?

% Authentication failed

The screenshot shows two windows. The top window is WinRadius, displaying a log table with two entries:

ID	Time	Message
1	2021y2m3d 9h13m28s	Reason: Unknown username
2	2021y2m3d 9h13m28s	User (Userxxx) authenticate failed.

The bottom window is the R1 terminal, showing the following output:

```
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing.
*****

User Access Verification

Username: Userxxx
Password:

*Feb 3 09:13:00.430: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.3:1645,1646
is not responding.
*Feb 3 09:13:00.431: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.3:1645,1646
is being marked alive.
% Authentication failed

Username: █
```

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?

Yes.

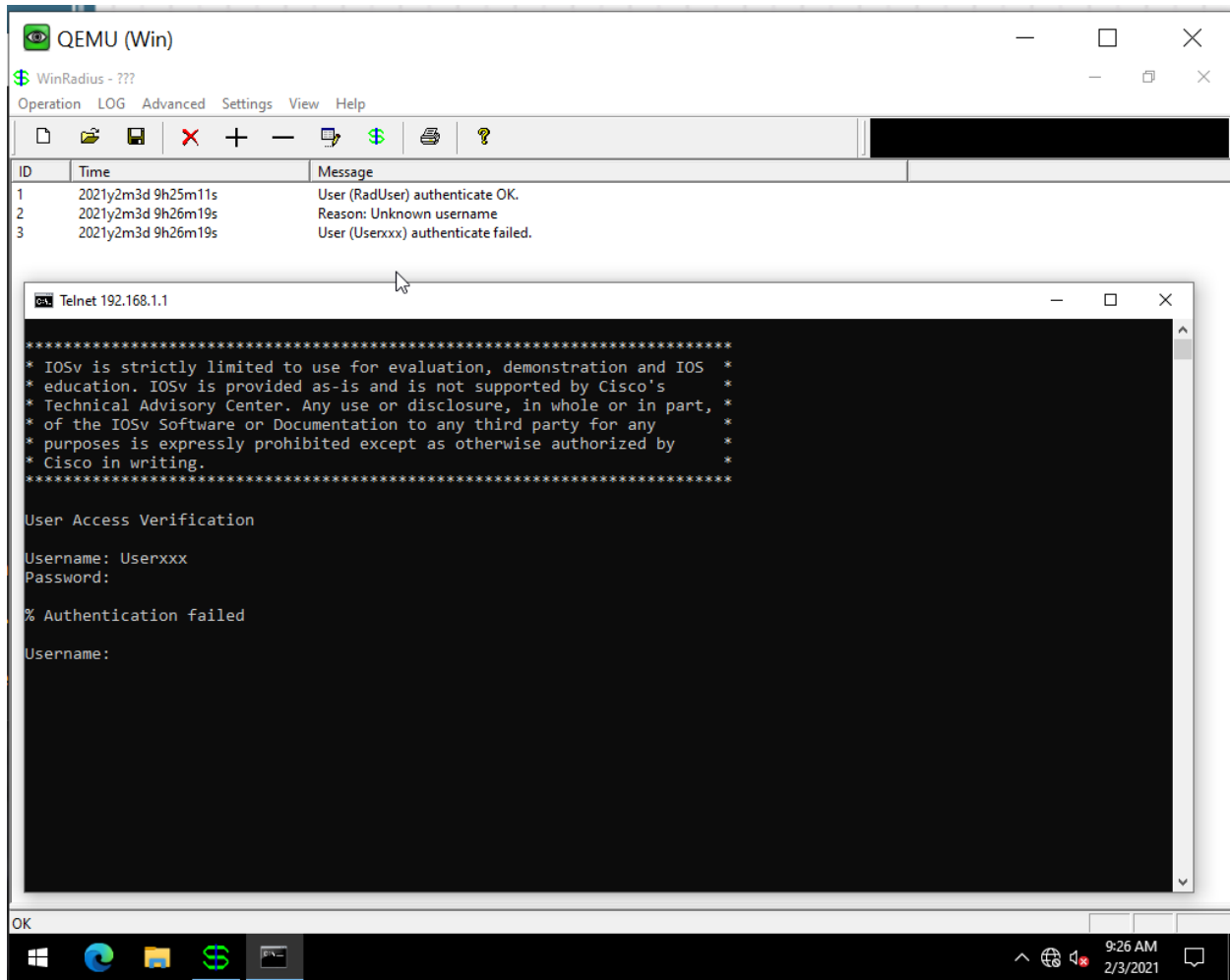
The screenshot shows a QEMU (Win) window titled "WinRadius - ???". The interface includes a menu bar (Operation, LOG, Advanced, Settings, View, Help) and a toolbar with icons for file operations and help. A table displays a log entry:

ID	Time	Message
1	2021y2m3d 9h25m11s	User (RadUser) authenticate OK.

Below the table is a Telnet window titled "Telnet 192.168.1.1". The window displays a Cisco IOSv banner, followed by "User Access Verification". The user enters "RadUser" for the username and "RadUserpass" for the password. The prompt "R1>" is visible at the bottom of the Telnet window.

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?

No.



Step 8: Free lab practice

Step 9: Please submit this lab report.

Note: Please remove all passwords from network devices, and tidy up your group lab environment after you complete this lab. Thanks!

Group members: Hui Zhao 101159615

Date: 2021 Feb 3