IT NE 2006
Securing Administrative Access Using AAA and RADIUS

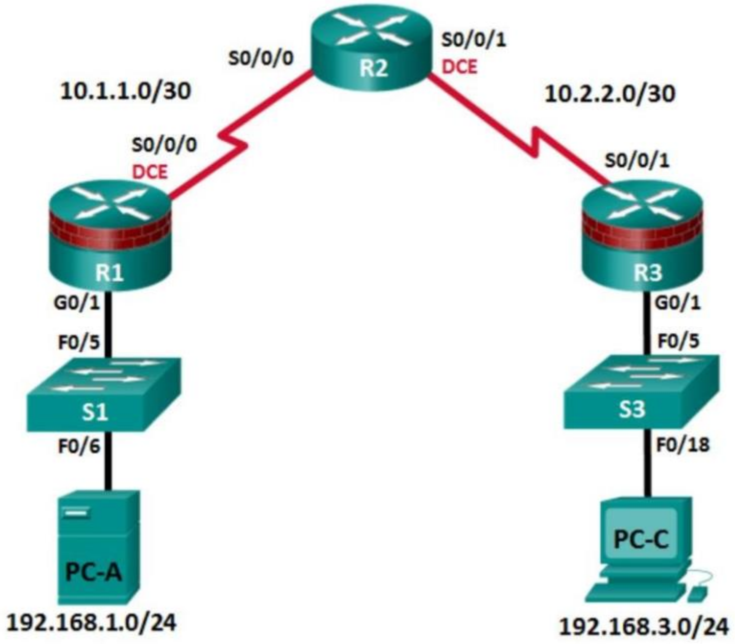
LAB 4

WEEK - 5

CONTENTS

Objective: Securing Administrative Access Using AAA and RADIUS

Topology



Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1-S0000	F0/1	192.168.1.1	255.255.255.0	N/A	S1-S0000 F0/1
	S0/0 (DEC)	10.1.1.1	255.255.255.252	N/A	N/A
R2-S0000	S0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3-S0000	F0/1	192.168.3.1	255.255.255.0	N/A	S3-S0000 F0/1
	S0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A-S0000	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-C-S0000	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S2 F0/3

In this lab, you will perform the following tasks:

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.
- 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.
- 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 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: Before beginning, ensure that the routers and switches have been erased and have no startup configurations.

Task 1: Configure Basic Device Settings

The desktop system assigned to you serves as an end-user terminal. You access and manage the lab environment from the student desktop system using GNS3 Software.

Students should perform the steps in this task individually.

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: Deploy router in GNS3 network.

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

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology plus your student ID.

b. Configure interface IP addresses as shown in the IP Addressing Table.

R1 Config – *Copy page the commands in bold text*

```
R1-S0000# conf t interface f0/1
ip address 192.168.1.1 255.255.255.0
no shutdown
exit interface
s0/0
ip address 10.1.1.1 255.255.255.252
no shutdown
exit exit
copy running-config startup-config
Destination filename [startup-config]?
```

R3 Config - *Copy page the commands in bold text*

```
R3-S0000# conf t interface f0/1
ip address 192.168.3.1 255.255.255.0
no shutdown
exit interface
s0/1 ip
address
10.2.2.1
255.255.255.
252
no shutdown
exit exit
copy running-config startup-config
Destination filename [startup-config]?
```

R2 Config - *Copy page the commands in bold text*

```
R2-S0000# conf t interface s0/0
ip address 10.1.1.2 255.255.255.252
no shutdown
exit interface
s0/1
```

```
ip address 10.2.2.2 255.255.255.252
no shutdown
exit exit
copy running-config startup-config
Destination filename [startup-config]?
```

c. Configure a clock rate for routers with a DCE serial cable attached to their serial interface. R1-STUDENTID is shown here as an example.

Copy page the commands in bold text

```
R1-S0000#  Conf

t  interface S0/0

clock rate 64000

 Exit

 Exit

R3:

R3-S000 #  Conf t

interface S0/1

clock rate 64000

 Exit

 Exit

R2:

R2-S000 #  Conf t

interface S0/0

clock rate 64000

exit  interface

S0/1  clock rate

64000

 Exit
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1-STUDENTID is shown here as an example.

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

R2-STUDENTID(config)# no ip domain-lookup
```

R3-STUDENTID(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.

R1: - *Copy page the commands in bold text* R1-

```
S0000#
conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ip route 0.0.0.0 0.0.0.0 S0/0 end
```

R3: *Copy page the commands in bold text* R3-S0000#

```
conf t
Enter configuration commands, one per line.  End with
CNTL/Z. ip route 0.0.0.0 0.0.0.0 S0/1 end
```

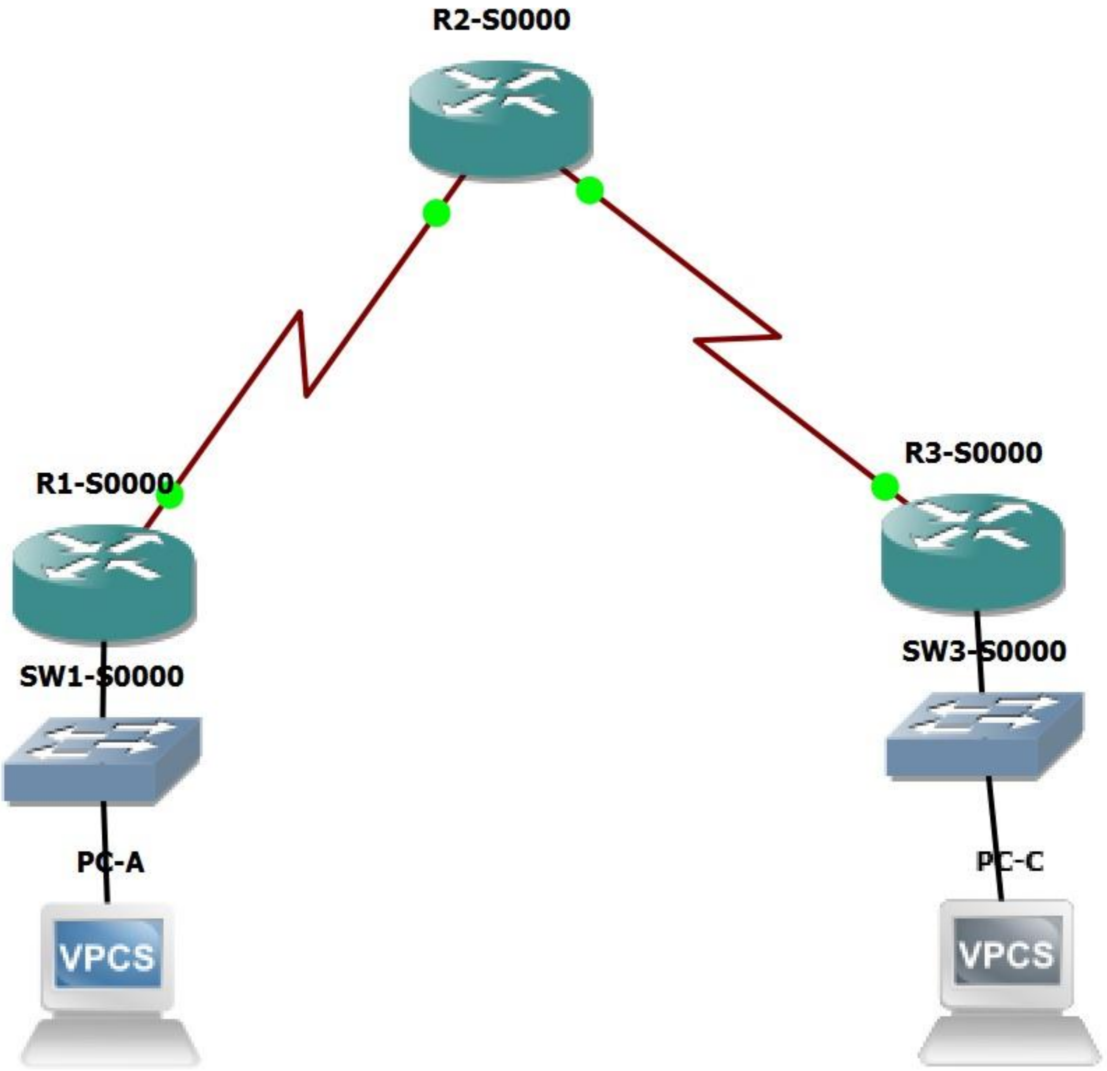
b. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

R2: *Copy page the commands in bold text* R2-S0000#

```
conf t ip route 192.168.1.0
255.255.255.0 S0/0 ip route
192.168.3.0 255.255.255.0 S0/1 end
```

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.



Deploy VPCS A: Connect Switch Port 8 to R1 f0/1

Deploy VPCS C: Connect Switch Port 8 to R3 f0/1

PCA> ip 192.168.1.2/24 192.168.1.1

PCA> Save

Deploy VPCS C: Connect to R3 f0/1

PCA> ip 192.168.3.2/24 192.168.3.1

PCA> Save

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-S0000 and R3. Router R1-S0000 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-S0000(config)# security passwords min-length 10

R3-S0000(config)# security passwords min-length 10
```

b. Configure the enable secret password on both routers. Use the type 9 (SCRYPT) hashing algorithm.

```
R1-S0000(config)# enable secret cisco12345

R3-S0000(config)# enable secret cisco12345
```

Step 8: Configure the basic console, auxiliary port, and vty lines.

a. Configure a console password and enable login for router R1-S0000. 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-S0000(config)# line console 0

R1-S0000(config-line)# password ciscoconpass

R1-S0000(config-line)# exec-timeout 5 0

R1-S0000(config-line)# login

R1-S0000(config-line)# logging synchronous

R3-S0000# exit
```

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

```
R1-S0000(config)# line aux 0

R1-S0000(config-line)# password ciscoauxpass

R1-S0000(config-line)# exec-timeout 5 0

R1-S0000(config-line)# login

R1-S0000(config-line)# exit
```

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

```
R1-S0000(config)# line vty 0 4

R1-S0000(config-line)# password ciscovtypass

R1-S0000(config-line)# exec-timeout 5 0

R1-S0000(config-line)# login

R1-S0000(config-line)# exit
```

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

```
R1-S0000(config)# service password-encryption

R1-S0000(config)# exit
```

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

Step 9: 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-S0000(config)# banner motd $Unauthorized access strictly prohibited!$

R1-S0000(config)# exit

R3-S0000(config)# banner motd $Unauthorized access strictly prohibited!$

R3-S0000(config)# exit

R2-S0000(config)# banner motd $Unauthorized access strictly prohibited!$

R2-S0000(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 10: Save the basic configurations on all routers.

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

```
R1-S0000# copy running-config startup-config

R3-S0000# copy running-config startup-config

R2-S0000# 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. Use the type 9 (SCRYPT) hashing algorithm.

```
R1-S0000(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-S0000(config)# conf t

R1-S0000(config)# line console 0

R1-S0000(config-line)# login local
```

b. Exit to the initial router screen that displays: R1-S0000 con0 is now available. Press RETURN to get started.

```
R1-S0000(config-line)# exit

R1-S0000(config)# exit

R3-S0000# exit
```

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.

```
R2-S0000> telnet 10.1.1.1
```

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

____

____

b. Set the vty lines to use the locally defined login accounts and configure the transport input command to allow Telnet.

```
R1-S0000(config)# line vty 0 4

R1-S0000(config-line)# login local

R1-S0000(config-line)# transport input telnet

          R1-S0000(config-line)# exit
```

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

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

Were you prompted for a user account? Explain.

____

d. Log in as user01 with a password of user01pass.

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

What password did you use?

____

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

```
          R1-S0000(config)# line aux 0

          R1-S0000(config-line)# login local
```

g. 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.

Step 1: Configure the local user database.

a. Create a local user account with 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-case 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. Note: The local-case parameter is used to make usernames case-sensitive.

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 usernames and passwords are both case-sensitive now. 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.

____

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

OR

R2-S0000# telnet 192.1683.1

Trying 192.168.3.1 ... Open

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

____

____

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: 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-StudentID 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-S0000# clock set 14:15:00 26 December 2014
```

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-S0000# 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 R2 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#

Feb 20 08:45:49.383: AAA/BIND(0000000F): Bind i/f

Feb 20 08:45:49.383: AAA/AUTHEN/LOGIN (0000000F): Pick method list 'TELNET_LINES'
```

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 (tty132), and remote Telnet client address (10.2.2.2). Also note that the last status entry is "PASS."

```
R3#

Feb 20 08:46:43.223: AAA: parse name=tty132 idb type=-1 tty=-1

Feb 20 08:46:43.223: AAA: name=tty132 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=132

channel=0

Feb 20 08:46:43.223: AAA/MEMORY: create_user (0x32716AC8) user='Admin01' ruser='NULL' ds0=0

port='tty132' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 initial_task_id='0',

vrf= (id=0)

Feb 20 08:46:43.223: AAA/AUTHEN/START (2655524682): port='tty132' list='' action=LOGIN

service=ENABLE

Feb 20 08:46:43.223: AAA/AUTHEN/START (2

R3#655524682): non-console enable - default to enable password

Feb 20 08:46:43.223: AAA/AUTHEN/START (2655524682): Method=ENABLE
Feb 20 08:46:43.223: AAA/AUTHEN (2655524682): status = GETPASS

R3#

Feb 20 08:46:46.315: AAA/AUTHEN/CONT (2655524682): continue_login (user='(undef)')

Feb 20 08:46:46.315: AAA/AUTHEN (2655524682): status = GETPASS

Feb 20 08:46:46.315: AAA/AUTHEN/CONT (2655524682): Method=ENABLE

Feb 20 08:46:46.543: AAA/AUTHEN (2655524682): status = PASS
```

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.

```
Feb 20 08:47:36.127: AAA/AUTHEN (4254493175): status = GETPASS

Feb 20 08:47:36.127: AAA/AUTHEN/CONT (4254493175): Method=ENABLE

Feb 20 08:47:36.355: AAA/AUTHEN(4254493175): password incorrect

Feb 20 08:47:36.355: AAA/AUTHEN (4254493175): status = FAIL

Feb 20 08:47:36.355: AAA/MEMORY: free_user (0x32148CE4) user='NULL' ruser='NULL'

port='tty132' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)

R3#
```

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.

```
Feb 20 08:48:17.887: AAA/AUTHEN/LOGIN (00000010): Pick method list 'TELNET_LINES'
```

What message was displayed on the Telnet client screen?

____

____