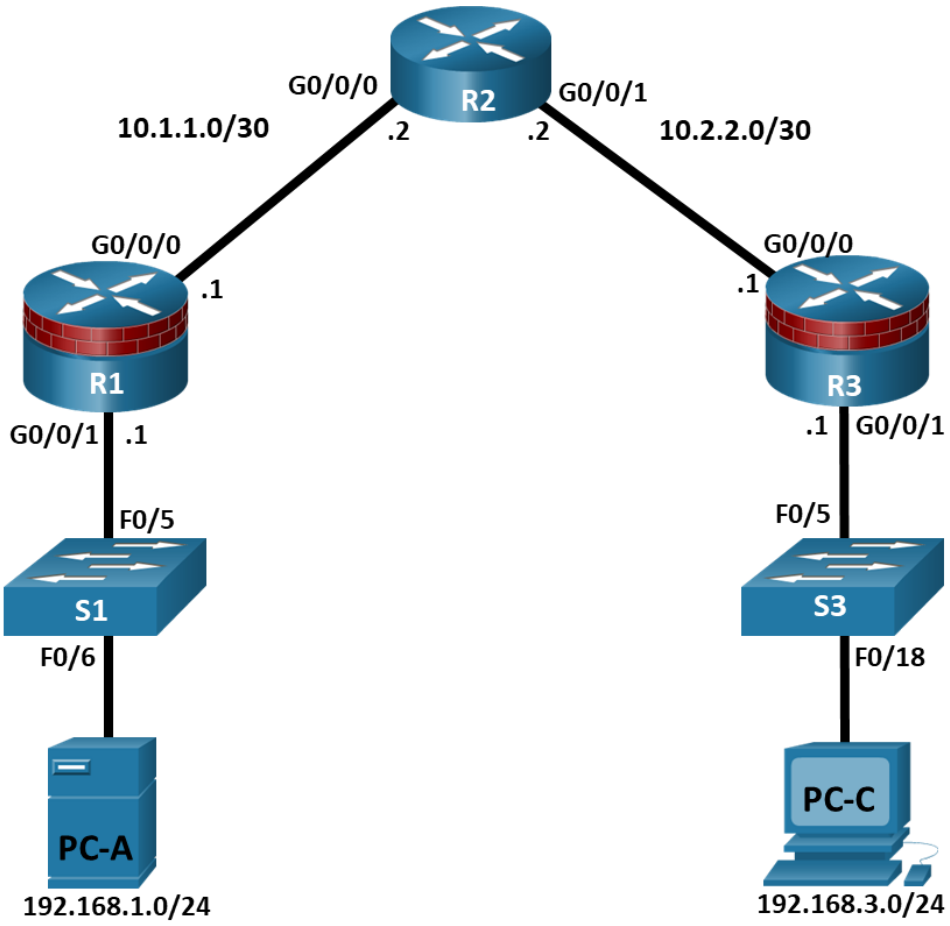
Lab - Configure Local AAA Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

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

Part 2: Configure Local Authentication for Console Access

- Configure a local database user and local access for the console line.
- Test the configuration.

Part 3: Configure Local Authentication for Remote Access

- Configure domain name
- Configure encryption key
- Enable SSH on vty

Part 4: Configure Local Authentication Using AAA on R3

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

Part 5: Observe AAA Authentication Using Cisco IOS Debug

Background / Scenario

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

In addition to basic passwords, specific usernames or accounts with varying privilege levels can be defined in the local router database that can apply to the router as a whole. When the console, vty, or aux lines are configured to refer to this local database, the user is prompted for a username and a password when using any of these lines to access the router.

Additional control over the login process can be achieved using authentication, authorization, and accounting (AAA). For basic authentication, AAA can be configured to access the local database for user logins, and fallback procedures can also be defined. However, this approach is not very scalable because it must be configured on every router. 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.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

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

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

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

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

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology.

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

c. 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.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

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

```
R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1
```

Step 4: Configure PC host IP settings.

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

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

a. Ping from R1 to R3.

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

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

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

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

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

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

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

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

a. Configure a minimum password length.

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

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

b. Configure a password for the privileged EXEC mode on both routers. Use the type 8 (PDKDF2) hashing algorithm.

```
R1(config)# enable algorithm-type sha256 secret cisco12345
```

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

a. 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
```

b. 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
```

c. 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
```

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

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

e. Issue the **show run | section line** command.

Can you read the console, aux, and vty passwords? Explain.

nop the password encryption service was enabled

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

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

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

Step 10: Save the basic configurations on all routers.

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

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

Part 2: Configure Local Authentication for Console Access

In this part of 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 using the type 8 (PDKDF2) hashing algorithm to encrypt the password.

```
R1(config)# username user01 algorithm-type sha256 secret user01pass
```

b. Exit global configuration mode and display the running configuration.

Can you read the user's password?

Nop, sha256 encrypted

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

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

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

b. Exit to the initial router screen that displays:

```
R1 con0 is now available.

Press RETURN to get started.
```

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

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

different user

d. After logging in, issue the **show run** command.

Were you able to issue the command? Explain.

e. Enter privileged EXEC mode using the **enable** command.

Were you prompted for a password? Explain.

Part 3: Configure Local Authentication for Remote Access

In this part, you will use SSH for remote access to R1 using local user database.

Step 1: Configure a domain name for the device.

Step 2: Configure the encryption key method.

Step 3: Enable SSH on the vty lines.

a. Enable SSH on the inbound vty lines using the **transport input** command.

b. Change the login method to use the local database for user verification.

c. From PC-A, establish an SSH session with R1.

Were you prompted for a user account? Explain.

used username user01

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

What password did you use?

user01pass

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

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

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.

Part 4: Configure Local Authentication Using AAA on R3

Step 1: Configure the local user database.

a. Create a local user account with PDKDF2 hashing to encrypt the password.

```
R3(config)# username Admin01 privilege 15 algorithm-type sha256 secret
Admin01pass
```

b. Exit global configuration mode and display the running configuration.

Can you read the user's password?

Step 2: Enable AAA services.

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.

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

Step 3: 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.

yes

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:

d. Attempt to log in to the console as **baduser** with any password.

Were you able to log in? Explain.

yes

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

any user is allowed.

Step 4: Create an AAA authentication profile for SSH using the local database.

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

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

```
R3(config-line)# login authentication SSH_LINES
```

b. Verify that this authentication profile is used by opening an SSH session from PC-C to R3. Log in as **Admin01** with a password of **Admin01pass**.

Were you able to login? Explain.

yes router accessed local database.

c. Exit the SSH session.

d. Attempt to log in as **baduser** with any password.

Were you able to login? Explain.

no. if username is not found in local db, there is no fallback method.

Part 5: Observe AAA Authentication Using Cisco IOS Debug

In this part, 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 03 February 2021
```

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 an SSH session from R2 to R3. Log in with username **Admin01** and password **Admin01pass**.

```
R2# ssh -l Admin01 10.2.2.1
```

c. Navigate back R3. Observe the AAA authentication events in the console session window. Debug messages similar to the following should be displayed.

```
R3#
Feb  3 14:15:57.653: AAA/BIND(00000FB5): Bind i/f
Feb  3 14:15:57.653: AAA/AUTHEN/LOGIN (00000FB5): Pick method list 'SSH_LINES'
R3#
```

```
Feb  3 14:16:01.966: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Admin01]
[Source: 10.2.2.2] [localport: 22] at 14:16:01 UTC Wed Feb 3 2021
```

d. From the SSH window on R2, 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 (tty866), and remote SSH client address (10.2.2.2). Also note that the last status entry is "PASS."

```
Feb  3 14:19:51.146: AAA: parse name=tty866 idb type=-1 tty=-1
Feb  3 14:19:51.146: AAA: name=tty866 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=866 channel=0
Feb  3 14:19:51.146: AAA/MEMORY: create_user (0x7FD084CE0FF0) user='Admin01'
ruser='NULL' ds0=0 port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE
priv=15 initial_task_id='0', vrf= (id=0)
Feb  3 14:19:51.146: AAA/AUTHEN/START (402765494): port='tty866' list='' action=LOGIN
service=ENABLE
Feb  3 14:19:51.146: AAA/AUTHEN/START (402765494): non-console enable - default to
enable password
Feb  3 14:19:51.147: AAA/AUTHEN/START (402765494): Method=ENABLE
R3#
Feb  3 14:19:51.147: AAA/AUTHEN (402765494): status = GETPASS
R3#
Feb  3 14:19:54.156: AAA/AUTHEN/CONT (402765494): continue_login (user='(undef)')
Feb  3 14:19:54.156: AAA/AUTHEN (402765494): status = GETPASS
Feb  3 14:19:54.156: AAA/AUTHEN/CONT (402765494): Method=ENABLE
Feb  3 14:19:54.259: AAA/AUTHEN (402765494): status = PASS
Feb  3 14:19:54.259: AAA/MEMORY: free_user (0x7FD084CE0FF0) user='NULL' ruser='NULL'
port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
```

e. From the SSH 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  3 14:24:20.274: AAA: parse name=tty866 idb type=-1 tty=-1
Feb  3 14:24:20.274: AAA: name=tty866 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=866 channel=0
Feb  3 14:24:20.274: AAA/MEMORY: create_user (0x7FD08991D130) user='Admin01'
ruser='NULL' ds0=0 port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE
priv=15 initial_task_id='0', vrf= (id=0)
Feb  3 14:24:20.274: AAA/AUTHEN/START (1943266075): port='tty866' list='' action=LOGIN
service=ENABLE
Feb  3 14:24:20.274: AAA/AUTHEN/START (1943266075): non-console enable - default to
enable password
Feb  3 14:24:20.274: AAA/AUTHEN/START (1943266075): Method=ENABLE
R3#
Feb  3 14:24:20.275: AAA/AUTHEN (1943266075): status = GETPASS
R3#
Feb  3 14:24:22.276: AAA/AUTHEN/CONT (1943266075): continue_login (user='(undef)')
Feb  3 14:24:22.276: AAA/AUTHEN (1943266075): status = GETPASS
Feb  3 14:24:22.276: AAA/AUTHEN/CONT (1943266075): Method=ENABLE
Feb  3 14:24:22.379: AAA/AUTHEN(1943266075): password incorrect
Feb  3 14:24:22.379: AAA/AUTHEN (1943266075): status = FAIL
Feb  3 14:24:22.379: AAA/MEMORY: free_user (0x7FD08991D130) user='NULL' ruser='NULL'
port='tty866' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
R3#
```

f. Exit the SSH session to the router R3. Then try to open an SSH 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  3 14:26:40.960: AAA/BIND(00000FB9): Bind i/f
Feb  3 14:26:40.960: AAA/AUTHEN/LOGIN (00000FB9): Pick method list 'SSH_LINES'
```

What message was displayed on the SSH client screen?

[Connection to 10.2.2.1 closed by foreign host]

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

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.

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
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)
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)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

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.