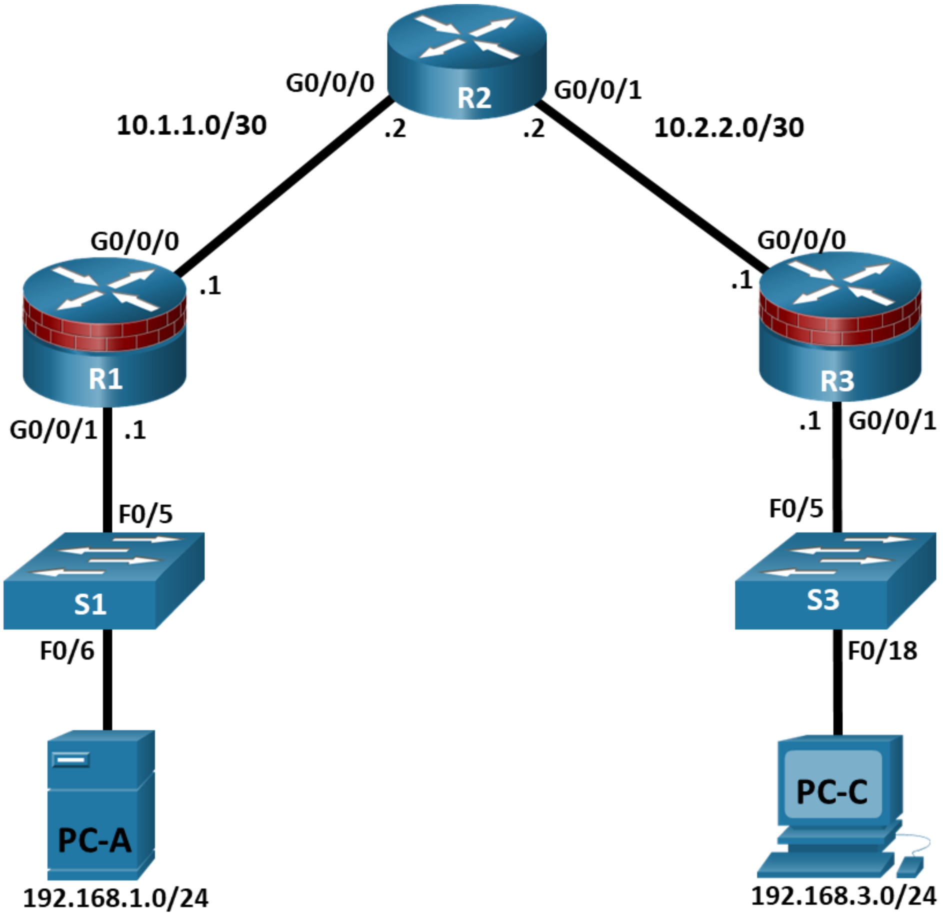
Lab - Configure Server-Based Authentication with RADIUS

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
RADIUS Server on PC-A	NIC	192.168.1.11	255.255.255.0	192.168.1.1	N/A
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

Part 2: Configure Centralized Authentication Using AAA and RADIUS

- Enable AAA.
- Configure the default login authentication list.
- Specify a RADIUS server.

Part 3: Configure Centralized Authentication Using AAA and RADIUS

- Test the AAA RADIUS configuration.
- Change the RADIUS port numbers

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 secret password further improves security, but still only a basic password is required for each mode of access. Local databases with usernames with varying privilege levels can also be used and the users will be prompted for usernames and passwords to access the devices.

In addition to basic passwords and local authentication, 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 access RADIUS software on an external computer and use AAA to authenticate users with the RADIUS server.

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 application and virtualization software, such as VirtualBox installed)

- 1 Security Workstation Virtual Machine with RADIUS server already 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, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

The initial router configurations are provided and the configurations for the switches are optional.

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: Load the configurations.

In this step, you will copy and paste the configurations into each router.

Router R1

```
enable
config terminal
no ip domain lookup
enable algorithm-type sha256 secret cisco12345
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
host R1
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 10.1.1.2
line con 0
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
```

```
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
end
```

Router R2

```
enable
config terminal
no ip domain lookup
host R2
enable algorithm-type sha256 secret cisco12345
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
interface GigabitEthernet0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
ip address 10.2.2.2 255.255.255.252
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 192.168.1.0 255.255.255.0 10.1.1.1
ip route 192.168.3.0 255.255.255.0 10.2.2.1
line con 0
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
end
```

Router R3

```
enable
config terminal
no ip domain lookup
enable algorithm-type sha256 secret cisco12345
```

```
username user01 algorithm-type sha256 secret user01pass
username admin privilege 15 algorithm-type sha256 secret cisco12345
ip domain-name netsec.com
host R3
interface GigabitEthernet0/0/0
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface GigabitEthernet0/0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
router ospf 1
 passive-interface GigabitEthernet0/0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 10.2.2.2
line con 0
 login local
 logging synchronous
 exec-timeout 5 0
line aux 0
 login local
 exec-timeout 5 0
line vty 0 4
 login local
 exec-timeout 5 0
 transport input ssh
crypto key generate rsa general-key modulus 1024
end
```

Step 3: Configure the PCs.

PC-A will function as the RADIUS server for this lab. A virtual machine with a RADIUS server is setup for use in this course. You can deploy the virtual machine on PC-A by following **Lab - Installing the Virtual Machine** if you have not done so already. You may choose to download, install, and configure a RADIUS server for your use if desired.

a. Assign the IP address and default gateway on PC-C according to the Addressing Table.

b. If you have not already deployed the virtual machine **Security Workstation VM**, please go back to **Lab - Installing the Virtual Machine**.

c. Start VirtualBox and verify that the Security Workstation is using the Bridged Adapter in the Network Settings.

d. Start the Security Workstation VM. Log into the VM as **sec_admin** with the password **net_secPW**. Select the user **sec_admin** from the dropdown list if necessary.

e. From the menu bar at the bottom of the Desktop, click **Terminal Emulator**.

f. Within the terminal emulator window, you will configure this virtual machine with an IP address of 192.168.1.11 by running a script. When prompted for a password, use the password **net_secPW**.

```
[sec_admin@Workstation ~]$ cd ~/lab.support.files/scripts/
```

```
[sec_admin@Workstation scripts]$ ./configure_as_static.sh
[sudo] password for sec_admin:
Configuing the NIC as:
IP: 192.168.1.11/24
GW: 192.168.1.1

IP Configuration successful.
```

g. Enter **ip addr** at the prompt to verify the assigned static IP address on Security Workstation VM.

```
[sec_admin@Workstation scripts]$ ip addr
<output omitted>
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 00:50:56:9c:c5:37 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.11/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe9c:5248/64 scope link
       valid_lft forever preferred_lft forever
```

h. Ping the gateway IP address (R1's G0/0/0, 192.168.1.1) from Security Workstation VM.

```
[sec_admin@Workstation scripts]$ ping -c 4 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.605 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.661 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.654 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.641 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3042ms
rtt min/avg/max/mdev = 0.605/0.640/0.661/0.021 ms
```

Step 4: Verify connectivity.

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

b. From Security Workstation VM terminal, establish an SSH session with R1 using the username **user01** and password **user01pass**. Enter **yes** when prompted if you are sure you want to continue connecting.

```
[sec_admin@Workstation scripts]$ ssh -l user01 192.168.1.1
```

c. Exit the SSH session when finished. Establish another SSH with R1 using the username **admin** and password **cisco12345**.

d. Exit the SSH session when finished. Now you have verified end-to-end connectivity and Security Workstation VM can communicate with router R1.

Part 2: Configure Centralized Authentication Using AAA and RADIUS

In this part, you will configure R1 to use AAA services to authenticate users. The RADIUS server is already configured with one user **RadUser** with the password **RadUserpass** and the secret shared key **$trongKey**.

Step 1: Enable AAA on R1.

Open a console on R1 and 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.

Configure the list to first use RADIUS for the authentication service, and then the fallback, **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
```

Note: You could alternatively configure local authentication as the backup authentication method.

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

Step 3: Specify a RADIUS server.

a. Use the **radius server** command to enter RADIUS server configuration mode.

```
R1(config)# radius server NetSec
```

b. Use the **?** to view the sub-mode commands available for configuring a RADIUS server.

```
R1(config-radius-server)# ?
RADIUS server sub-mode commands:
  address          Specify the radius server address
  automate-tester  Configure server automated testing.
  backoff          Retry backoff pattern(Default is retransmits with constant
                   delay)
  exit             Exit from RADIUS server configuration mode
  key              Per-server encryption key
  no               Negate a command or set its defaults
  non-standard     Attributes to be parsed that violate RADIUS standard
  pac              Protected Access Credential key
  retransmit       Number of retries to active server (overrides default)
  timeout          Time to wait (in seconds) for this radius server to reply
                   (overrides default)
```

c. Use the **address** command to configure the IP address of the RADIUS server.

```
R1(config-radius-server)# address ipv4 192.168.1.11
```

d. The **key** command is used for the secret password that is shared between the RADIUS server and the router (R1 in this case) and is used to authenticate the connection between the router and the server before the user authentication process takes place. Use the secret password of **$trongPass** that has been configured on the Radius server. Remember that passwords are case-sensitive.

```
R1(config-radius-server)# key $trongPass
R1(config-radius-server)# end
```

Note: For the purposes of this lab, an unencrypted password is configured. In the future, IOS will require encrypted passwords.

Part 3: Test the AAA RADIUS Configuration.

Step 1: Start the RADIUS Server and verify operation.

a. At the Security Workstation terminal, start the RADIUS server by entering the **sudo systemctl start freeradius.service** command. Enter the password **net_secPW** as necessary.

```
[sec_admin@Workstation ~]$ sudo systemctl start freeradius.service
```

b. Verify that the server is running, enter the command **sudo systemctl status freeradius.service** at the terminal prompt.

```
[sec_admin@Workstation ~]$ sudo systemctl status freeradius.service
? freeradius.service - FreeRADIUS high performance RADIUS server.
     Loaded: loaded (/usr/lib/systemd/system/freeradius.service; disabled; vendor
preset: disabled)
     Active: active (running) since Sun 2021-02-14 22:14:07 EST; 18min ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             https://wiki.freeradius.org/Home
             https://networkradius.com/freeradius-documentation/
    Process: 890 ExecStartPre=/usr/bin/radiusd -C (code=exited, status=0/SUCCESS)
    Process: 893 ExecStart=/usr/bin/radiusd -d /etc/raddb (code=exited,
status=0/SUCCESS)
   Main PID: 895 (radiusd)
      Tasks: 6 (limit: 1113)
     Memory: 77.5M
     CGroup: /system.slice/freeradius.service
             mq895 /usr/bin/radiusd -d /etc/raddb

Feb 14 22:14:07 Workstation systemd[1]: Starting FreeRADIUS high performance RADIUS
server....
Feb 14 22:14:07 Workstation systemd[1]: Started FreeRADIUS high performance RADIUS
server..
```

Step 2: Test your configuration.

You can test and verify your RADIUS server configurations on your router before exiting the router by using the **test aaa** command. The output message indicates that there is no authoritative response from the RADIUS sever.

```
R1# test aaa group radius RadUser RadUserpass legacy
Attempting authentication test to server-group radius using radius
No authoritative response from any server
```

You may also see messages similar to the following may display after the attempted tests indicating that the RADIUS server at 192.168.1.11 is not communicating with the router.

```
*Feb 15 02:30:26.504: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.11:1645,1646 is
not responding.
*Feb 15 02:30:26.504: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.11:1645,1646 is
being marked alive.
```

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

The **show radius server-group radius** command indicates that the router is using UDP ports 1645 and 1646 for communications.

```
R1# show radius server-group radius
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(192.168.1.11:1645,1646) Transactions:
    Authen: 32  Author: 0       Acct: 0
```

```
        Server_auto_test_enabled: FALSE
         Keywrap enabled: FALSE
```

RFC 2865 officially assigned port numbers 1812 and 1813 for RADIUS. This indicates that the router and RADIUS server are not communicating on the same ports.

Step 4: Change the RADIUS port numbers on R1 to match the RADIUS server.

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

a. Re-issue the address sub-mode command again. This time specify port numbers **1812** and **1813**, along with the IPv4 address**.**

```
R1(config)# radius server NetSec
R1(config-radius-server)# address ipv4 192.168.1.11 auth-port 1812 acct-port
1813
```

b. Test the router to RADIUS server communications again by using the **test aaa** command.

```
R1# test aaa group radius RadUser RadUserpass legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

Step 5: 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. 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?

d. Log in again using the local user credentials, **admin** / **cisco12345** or **user01** / **user01pass**.

Were you able to log in? Explain.

Step 6: Create an authentication method list for SSH and test it.

a. Log back into R1 as necessary.

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

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

c. 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 SSH_LINES
```

d. Establish an SSH session from PC-C to R1 (10.1.1.1) and log in with the username **RadUser** and the password of **RadUserpass**. Were you able to gain access to log in? Explain.

e. Establish an SSH session from PC-C to R1 again. Log in with the username **user01** and the password of **user01pass**. Were you able to log in? Explain.

Reflection

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

2. Contrast local authentication and local authentication with AAA.

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.