Practical 2 - Configure AAA Authentication on Cisco Routers

Lesson Outcomes

- Configure a local user account on R1 and authentication on the console using local AAA
- Verify local AAA authentication from the R1 console and the PC-A client
- Configure server-based AAA authentication using TACACS+
- Verify server-based AAA authentication from the PC-B client
- Configure server-based AAA authentication using RADIUS
- Verify server-based AAA authentication from the PC-C client

Addressing table

| Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252		N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252		N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252		N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252		N/A
TACACS+ Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S2 F0/18

Background / Scenario

The network topology shows routers R1, R2 and R3. Currently, all administrative security is based on knowledge of the enable secret password. Your task is to configure and test local and server-based AAA solutions. You will create a local user account and configure local AAA on router R1 to test the console and vty logins. You will then configure router R2 to support server-based authentication using the TACACS+ protocol. Finally, you will configure router R3 to support server-based authentication using the RADIUS protocol.

The devices in the topology are initially configured with the following passwords:

- o Console password: **ciscoconpa55**
- o Enable secret password: **ciscoenpa55**

Note: IOS version 15.3 uses SCRYPT as a secure encryption hashing algorithm; however, the IOS version that is currently supported in Packet Tracer uses MD5. Always use the most secure option available on your equipment.

Network Diagram
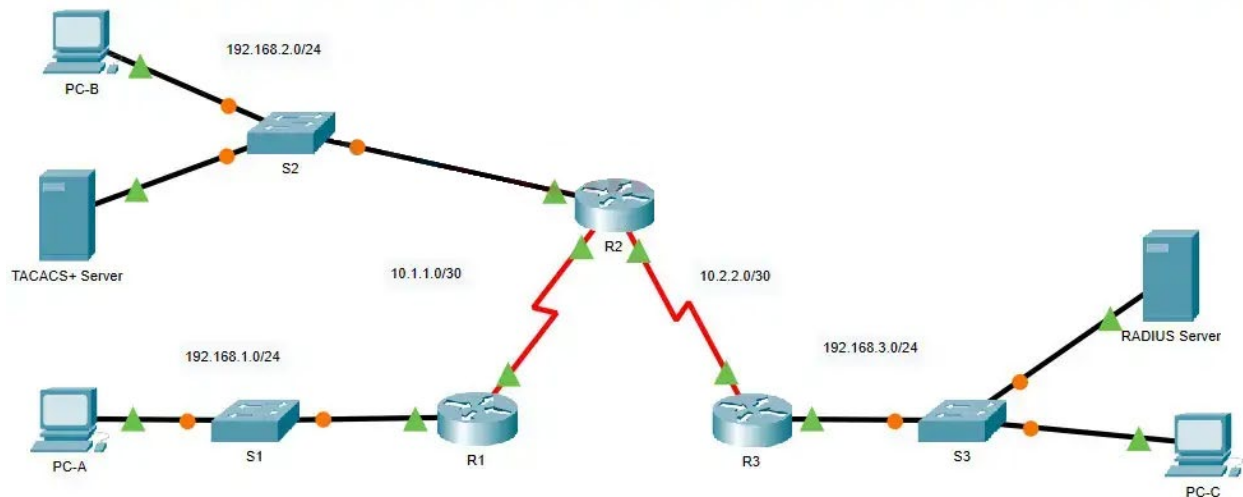
Part 1. Configure Local AAA Authentication for Console Access on R1

1. Test connectivity between the three PCs:
      - Ping from PC-A to PC-B
      - Ping from PC-A to PC-C
      - Ping from PC-B to PC-C

There should be response back and forth from each PC.

2. Configure a local username on R1 with a secret password.
   ```
   R1(config)# username Admin1 secret admin1pa55
   ```

3. Configure local AAA authentication for console access on R1. Enable AAA on R1 for the console login to use the local database.

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

   R1(config)# aaa authentication login default local
   ```

4. Configure the line console to use the defined AAA authentication method. Enable AAA on **R1** and configure for the console login to use the default method list.

```
R1(config)# line console 0

R1(config-line)# login authentication default
```

5. Verify the user EXEC login using the local database.

```
R1(config-line)# end

%SYS-5-CONFIG_I: Configured from console by console

R1# exit


R1 con0 is now available

Press RETURN to get started.

************ AUTHORIZED ACCESS ONLY ************

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Username: Admin1

Password: admin1pa55

R1>
```

Part 2. Configure Local AAA Authentication for vty lines on R1

6. Configure domain name and crypto key for use with SSH. Use **ccnasecurity.com** as the domain name on **R1**.

```
R1(config)# ip domain-name ccnasecurity.com
```

7. Create a RSA crypto key using 1024 bits.

```
R1(config)# crypto key generate rsa
```

```
Choose the size of the key modulus in the range of 360 to
2048 for your

General Purpose Keys. Choosing a key modulus greater than
512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]
```

8. Configure a named list called SSH-LOGIN to authenticate logins using local AAA.

```
R1(config)# aaa authentication login SSH-LOGIN local
```

9. Configure the vty lines to use the named AAA method and only allow SSH for remote access.

```
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
R1(config-line)# transport input ssh
R1(config-line)# end
```

10. Verify the SSH configuration SSH to **R1** from the command prompt of **PC-A**.

```
PC> ssh -l Admin1 192.168.1.1

Open

Password: admin1pa55
```

Part 3. Configure Server-Based AAA Authentication Using TACACS+ on R2

11. Configure a backup local database entry called Admin.

12. For backup purposes, configure a local username of **Admin2** and a secret password of **admin2pa55**.

```
R2(config)# username Admin2 secret admin2pa55
```

13. Verify the TACACS+ Server configuration.

14. Click the TACACS+ Server. On the Services tab, click **AAA**. Notice that there is a Network configuration entry for **R2** and a User Setup entry for **Admin2**.

15. Configure the AAA TACACS server IP address and secret key on **R2**.

Note: The commands **tacacs-server host** and **tacacs-server key** are deprecated. Currently, Packet Tracer does not support the new command **tacacs server**.

```
R2(config)# tacacs-server host 192.168.2.2
R2(config)# tacacs-server key tacacspa55
```

16. Enable AAA on **R2** and configure all logins to authenticate using the AAA TACACS+ server. If it is not available, then use the local database.

```
R2(config)# aaa new-model
R2(config)# aaa authentication login default group
tacacs+ local
```

17. Configure AAA authentication for console login to use the default AAA authentication method.

```
R2(config)# line console 0
R2(config-line)# login authentication default
```

18. Verify the user EXEC login using the AAA TACACS+ server.

```
R2(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R2# exit

R2 con0 is now available
Press RETURN to get started.

*********** AUTHORIZED ACCESS ONLY ************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification

Username: Admin2
Password: admin2pa55
R2>
```

Part 4. Configure Server-Based AAA Authentication Using RADIUS on R3

19. Configure a backup local database entry called Admin3.

20. For backup purposes, configure a local username of **Admin3** and a secret password of **admin3pa55**.

    ```
    R3(config)# username Admin3 secret admin3pa55
    ```

21. Click the RADIUS Server. On the Services tab, click **AAA**. Notice that there is a Network configuration entry for **R3** and a User Setup entry for **Admin3**.

22. Configure the AAA RADIUS server IP address and secret key on **R3**.

Note: The commands **radius-server host** and **radius-server key** are deprecated. Currently Packet Tracer does not support the new command **radius server**.

    ```
    R3(config)# radius-server host 192.168.3.2
    R3(config)# radius-server key radiuspa55
    ```

23. Enable AAA on **R3** and configure all logins to authenticate using the AAA RADIUS server. If it is not available, then use the local database.

    ```
    R3(config)# aaa new-model
    R3(config)# aaa authentication login default group radius
    local
    ```

24. Configure AAA authentication for console login to use the default AAA authentication method.

    ```
    R3(config)# line console 0
    R3(config-line)# login authentication default
    ```

25. Verify the user EXEC login using the AAA RADIUS server.

    ```
    R3(config-line)# end
    %SYS-5-CONFIG_I: Configured from console by console
    R3# exit

    R3 con0 is now available
    Press RETURN to get started.

    ************ AUTHORIZED ACCESS ONLY ************
    UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

    User Access Verification

    Username: Admin3
    Password: admin3pa55
    ```

```
R3>
```

26. Check results.

27. Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

Scripts for R1

```
!!!Part 1
config t
username Admin1 secret admin1pa55
aaa new-model
aaa authentication login default local
line console 0
login authentication default
!!!Part 2
ip domain-name ccnasecurity.com
crypto key generate rsa
1024
aaa authentication login SSH-LOGIN local
line vty 0 4
login authentication SSH-LOGIN
transport input ssh
```

Scripts for R2

```
config t
username Admin2 secret admin2pa55
tacacs-server host 192.168.2.2
tacacs-server key tacacspa55
aaa new-model
aaa authentication login default group tacacs+ local
line console 0
login authentication default
```

Scripts for R3

```
config t
username Admin2 secret admin2pa55
tacacs-server host 192.168.2.2
tacacs-server key tacacspa55
aaa new-model
aaa authentication login default group tacacs+ local
line console 0
login authentication default
```

--- End ---