Packet Tracer - Configure Local AAA for Console and VTY Access

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	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	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	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	N/A
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	S3 F0/18

Objectives

- Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.
- Verify local AAA authentication from the R1 console and the PC-A client.

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.

- User account: **Admin1** and password **admin1pa55**

The routers have also been pre-configured with the following:

- Enable secret password: **ciscoenpa55**
- OSPF routing protocol with MD5 authentication using password: **MD5pa55**

Note: The console and vty lines have not been pre-configured.

Note: Newer IOS images use more secure encryption hashing algorithm; however, the IOS version currently supported in Packet Tracer uses MD5. Always use the most secure option available on your physical equipment.

Part 1: Configure Local AAA Authentication for Console Access on R1

Step 1: Configure a local username on R1.

Configure a username of **Admin1** with a secret password of **admin1pa55**.

Step 2: Configure local AAA authentication for console access on R1.

Enable AAA on R1 and configure AAA authentication for the console login to use the local database.

Step 3: Configure the line console to use the defined AAA authentication method.

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

Step 4: Verify the AAA authentication method.

Verify the user EXEC login using the local database.

Part 2: Configure Local AAA Authentication for vty Lines on R1

Step 1: Configure domain name and crypto key for use with SSH.

a. Use **netsec.com** as the domain name on R1.

b. Create an RSA crypto key using 1024 bits.

Step 2: Configure a named list AAA authentication method for the vty lines on R1.

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

Step 3: Configure the vty lines to use the defined AAA authentication method.

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

Step 4: Verify the AAA authentication method.

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
```