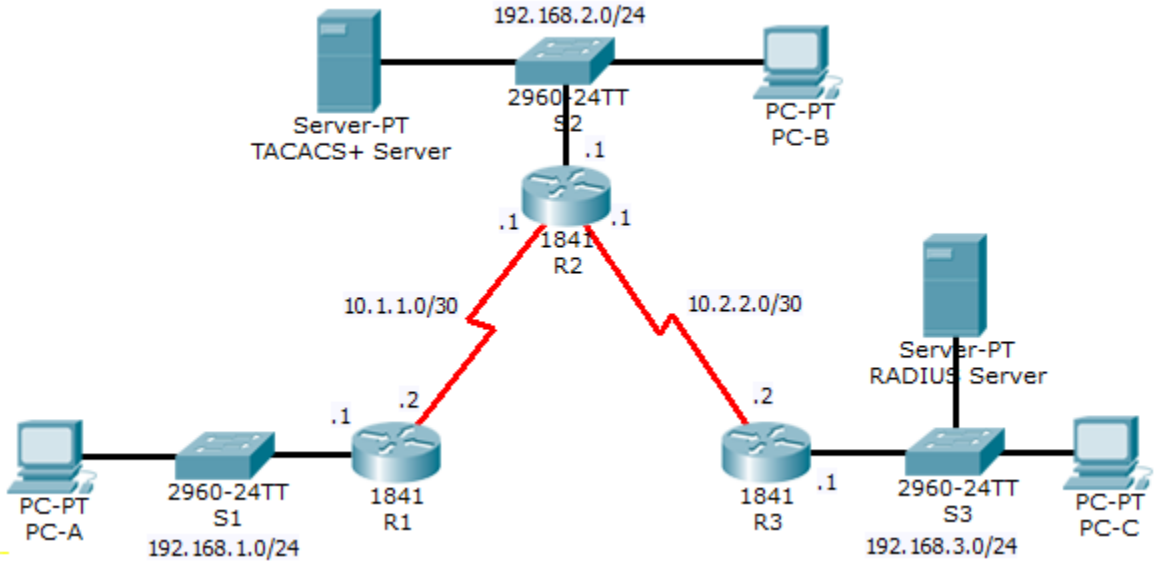
Packet Tracer - Configure AAA Authentication on Cisco Routers

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A	S1 Fa0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	Fa0/0	192.168.2.1	255.255.255.0	N/A	S2 Fa0/2
	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	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
TACACS+ Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 Fa0/6
RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 Fa0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 Fa0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Objectives

- Configure a local user account on R1 and authenticate on the console and VTY lines using local AAA.
- Verify local AAA authentication from the R1 console and the PC-A client.
- Configure a server-based AAA authentication using TACACS+.

- Verify server-based AAA authentication from PC-B client.
- Configure a server-based AAA authentication using RADIUS.
- Verify server-based AAA authentication from PC-C 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**

You will then configure router R2 to support server-based authentication using the TACACS+ protocol. The TACACS+ server has been pre-configured with the following:

- Client: **R2** using the keyword **tacacspa55**
- User account: **Admin2** and password **admin2pa55**

Finally, you will configure router R3 to support server-based authentication using the RADIUS protocol. The RADIUS server has been pre-configured with the following:

- Client: **R3** using the keyword **radiuspa55**
- User account: **Admin3** and password **admin3pa55**

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

- Enable secret password: **ciscoenpa55**
- RIP version 2

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

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

Step 1: Test connectivity.

- Ping from **PC-A** to **PC-B**.
- Ping from **PC-A** to **PC-C**.
- Ping from **PC-B** to **PC-C**.

Step 2: Configure a local username on R1.

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

Step 3: Configure local AAA authentication for console access on R1.

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

Step 4: Configure the line console to use the defined AAA authentication method.

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

Step 5: 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 a named list AAA authentication method for VTY lines on R1.

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

Step 2: Configure the VTY lines to use the defined AAA authentication method.

Configure the VTY lines to use the named AAA method.

Step 3: Verify the AAA authentication method.

Verify the Telnet configuration. From the command prompt of **PC-A**, Telnet to **R1**.

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

Step 1: Configure a backup local database entry called Admin.

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

Step 2: Verify the TACACS+ Server configuration.

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

Step 3: Configure the TACACS+ server specifics on R2.

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

Step 4: Configure AAA login authentication for console access on R2.

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

Step 5: Configure the line console to use the defined AAA authentication method.

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

Step 6: Verify the AAA authentication method.

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

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

Step 1: Configure a backup local database entry called Admin.

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

Step 2: Verify the RADIUS Server configuration.

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

Step 3: Configure the RADIUS server specifics on R3.

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

Step 4: Configure AAA login authentication for console access on R3.

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

Step 5: Configure the line console to use the defined AAA authentication method.

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

Step 6: Verify the AAA authentication method.

Verify the user EXEC login using the AAA RADIUS server.

Step 7: Check results.

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