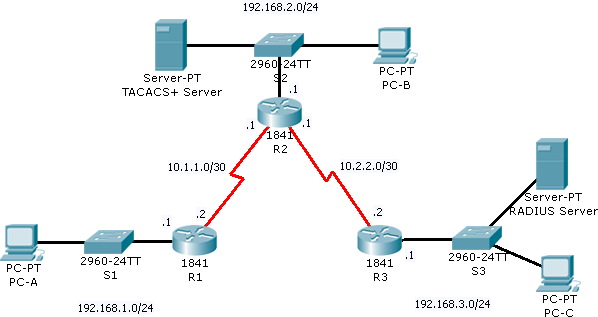
**Assignment AAA - Network Security**

Configure AAA Authentication on Cisco Routers

**Topology Diagram**



**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| R1 | Fa0/0 | 192.168.1.1 | 255.255.255.0 |
| S0/0/0 | 10.1.1.2 | 255.255.255.252 |
| R2 | S0/0/0 | 10.1.1.1 | 255.255.255.252 |
| Fa0/0 | 192.168.2.1 | 255.255.255.0 |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 |
| R3 | S0/0/1 | 10.2.2.2 | 255.255.255.252 |
| Fa0/0 | 192.168.3.1 | 255.255.255.0 |
| TACACS+ Server | NIC | 192.168.2.2 | 255.255.255.0 |
| RADIUS Server | NIC | 192.168.3.2 | 255.255.255.0 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 |
| PC-B | NIC | 192.168.2.3 | 255.255.255.0 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 |

**Learning 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.

# Initial Configuration

The given topology is intended to simulate a network that stretches over three sites with high-speed serial lines connecting the sites. We can use the names of the switches at each site when referring to the sites. Thus “site 1” is the site using switch S1, etc. In real life there would, of course, be multiple PCs and other end systems at each site.

When setting up the topology, you will need to add an HWIC-2T interface card to the routers. Do this by going into the router’s physical view, powering down the router (click on the power switch), and dragging an HWIC-2T interface card from the left side of the window to slot #0 on the router (slot #0 is on the right side as seen from the back of the device). Don’t forget to power the router back on.

After doing this, you will see that the router now has two additional interfaces, Serial0/0/0 and Serial0/0/1. Use the “Serial DTE” line (red lightning bolt *without* a little clock icon) to connect the serial interfaces. You will not see any green connection indicators until IP addresses have been assigned and the interfaces are brought up on *both* sides of the connection.

Set the enable secret to “class” (as usual) on all three routers.

It is probably a good idea to set up each site independently and check local access as you go by pinging the router interface from the end systems. Pings between sites will not work until routing is configured.

To configure routing, use RIP version 2 on each router. For example, on R1 do:

R1# configure terminal  
R1(config)# router rip  
R1(config-router)# version 2  
R1(config-router)# network 192.168.1.0  
R1(config-router)# network 10.0.0.0  
R1(config-router)# exit

Notice that RIP uses classful network address (hence 10.0.0.0). After setting up the routing, it should be possible to ping across the network.

Next, set up the two AAA servers. On the “Services” tab of the configuration dialog for the TACACS+ server, add R2 as a client with secret tacacspa42 (be sure the server type is set to “Tacacs”). Add the user AdminT with password cisco to the user database. Set up the RADIUS server similarly (use secret radiusps42) with R3 as a client and user AdminR with password cisco.

Don’t forget to turn on the AAA services.

# Task 1: Configure Local AAA Authentication for Console Access on R1

## Step 1. Configure a local username on R1.

Configure a username of **Admin** and secret password of **cisco**

## Step 2. Configure AAA method lists.

Enable AAA on R1 and define a default method list that uses the local user database. Also define a separate TELNET-LOGIN method list that also uses the local user database.

## Step 3. Apply the TELNET-LOGIN method list.

Next, configure the vty lines to use the TELNET-LOGIN authentication method list.

## Step 4. Verify the AAA authentication method.

Log out from the console and verify that you can log back in using the Admin user account. Telnet to the router from the end system and verify that you also login using the Admin user account.

# Task 2: 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 **Admin** and secret password of **cisco**

## Step 2. Verify the TACACS+ Server configuration.

Select the TACACS+ Server. From the Config tab, click on **AAA** and check that there is a network configuration entry for R2 and a User Setup entry for AdminT. Also verify that the AAA service is “on”.

## 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 default login authentication methods 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. Verify the AAA authentication method.

Verify the console login using the AAA TACACS+ server. Verify the telnet login using the TACACS+ server.

# Task 3: 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 **Admin** and secret password of **cisco**

## Step 2. Verify the RADIUS Server configuration.

Select the RADIUS Server. From the Config tab, click on **AAA** and check that there is a network configuration entry for R3 and a User Setup entry for AdminR. Make sure you use the correct port for RADIUS. Also verify that the AAA service is “on”.

## Step 3. Configure the RADIUS server specifics on R3.

Repeat the steps as for R2 except using RADIUS.

**Task 4: (OPTIONAL) Backup Configuration Challenge**

**Step 1:** Create a backup Radius Server for Site 2 (192.168.2.0 network). If the TACACS+ server goes down does the Radius server authenticate users? (Note- you should configure the same user ids in the Radius Server as are in the TACACS+ server.

**Step 2:** If the Radius Server crashes on site 3—would site 2 be able to function as a backup site? Try to configure this and list the steps you did to attempt this configuration.