Lab Report Reflection Sheet

Name of Activity: AAA Authentication Project

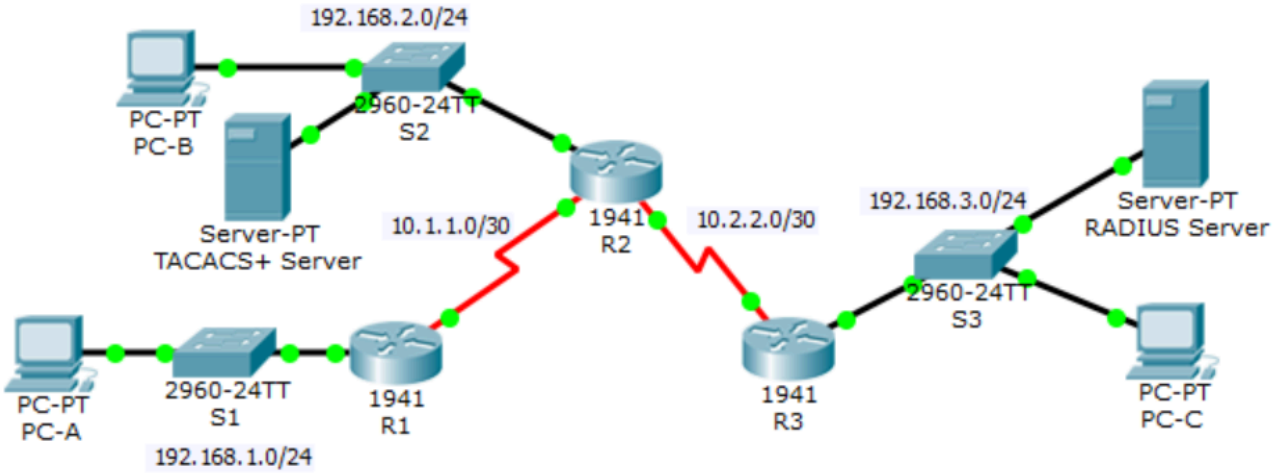
Description of this activity: The purpose of this project is to explain and demonstrate the use of AAA authentication protocols as well as explain the differences between local AAA authentication and server-based AAA authentication (for both RADIUS and TACACS+).

Research Narrative: AAA is a security framework commonly used on Cisco devices to provide security and accountability. AAA stands for: authentication, authorization, and accounting. The first step in the AAA process is authentication. AAA authentication works by storing usernames and passwords in a local database or a server. Users must authenticate against this database with a correct password to enter the device. With local authentication, the passwords are stored in a database on the device that is used for authentication, while in server based authentication the usernames and passwords are stored in an AAA server that the device must communicate with to perform authentication. After authentication AAA moves on to authorization. AAA authorization happens automatically. To authorize users, AAA uses a set of attributes assigned to each user to decide what they can and can't access. The final part of AAA is accounting. AAA keeps logs of everything an authenticated user does on a device. When a user types in a command, it is put in the log. The log also contains all usernames and passwords entered which can help identify malicious individuals. AAA uses a few protocols to perform its actions; these include: TACACS+, RADIUS and 802.1x. TACACS and RADIUS are protocols that both facilitate authentication through a server. 802.1x is a protocol that restricts unauthorized access to the network. 802.1x requires three devices: a server that runs the protocol, an intermediary device, and a user. When a device running the protocol tries to join the network, the intermediary device sends a request to the client asking for authentication info. Once the client provides this information the intermediary device sends it to the server, which then validates the client's identity and sends a response to the intermediary device. If the device has a valid identity it is allowed to access the LAN and any services that it provides.

The two main network access control protocols are RADIUS and TACACS+. They both are used to control what users can access on a network but they function differently. RADIUS is an open source protocol that can be used on any network and uses the UDP protocol to communicate with the server. TACACS+ is a Cisco proprietary protocol that can only be used on Cisco devices and it uses the more secure TCP protocol. The main function of RADIUS is to control network access as its protocols are more suited to authenticating users that are trying to access the network and securing it from attacks.it uses 802.1x port control to transport the AAA info to the server which determines if a device can access the network. TACACS+ is a protocol mostly used for network device administration. It allows administrators to determine network privileges on a user by user basis, it also allows accounting for commands and uses multiple privilege levels to prevent unauthorized access to network resources. They also perform AAA differently, RADIUS bundles authentication and authorization making it impossible to use them separately while accounting is separate.

TACACS+ deals with each separately allowing the administrator to manage each device separately. While both encrypt packets, TACACS+ encrypts all packets on the network ensuring maximus security, while RADIUS only encrypts passwords making it less secure. While they both perform overlapping functions, they each have ideal use cases. RADIUS will be used on a network where you only need to control who can access parts of the network, such as a more public facing network with large numbers of users. TACACS+ on the other hand is better suited for devices where users are entering commands or making modifications as TACACS+ has to authorize every command or action a user performs on a device and record it, it is better used in internal networks where employees will be directly modifying information or configurations on network devices. In conclusion, if I was given the choice over TACACS+ or RADIUS I would choose TACACS+ because it is more secure and allows for more flexibility for implementations.

Lab Summary: Wanting to configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA. Below are the commands we verified local AAA authentication from the R1 console and the PC-A client, configured server-based AAA authentication using TACACS+, Verified server-based AAA authentication from the PC-B client, configured server-based AAA authentication using RADIUS, verified server-based AAA authentication from the PC-C client, configured Local AAA Authentication for vty Lines on R1, and configured Local AAA Authentication for Console Access on R1.



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
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	S3 F0/18

In part one we configured local AAA authentication for console access on R1. We did this by adding username and passwords for R1 and configuring the line console on R1 using these commands.

```
R1(config)# username Admin1 secret admin1pa55
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
R1(config)# line console 0
R1(config-line)# login authentication default
```

In part two we configured domain name and crypto key for use with SSH, we Configure a named list AAA authentication method for the vty lines on R1, and Configure the vty lines to use the defined AAA authentication method using these commands.

```
R1(config)# ip domain-name ccnasecurity.com
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]
R1(config)# aaa authentication login SSH-LOGIN local
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
R1(config-line)# transport input ssh
R1(config-line)# end
```

In part 3 we configured a backup local database entry called Admin. Next we configured the TACACS+ server specifics on R2. After that we configured AAA login authentication for console access on R2. lastly configured the line console to use the defined AAA authentication method.

```
R2(config)# username Admin2 secret admin2pa55
R2(config)# tacacs-server host 192.168.2.2
R2(config)# tacacs-server key tacacspa55
R2(config)# aaa new-model
R2(config)# aaa authentication login default group tacacs+ local
R2(config-line)# login authentication default
```

In part 4 we started by configuring a backup local database entry called Admin on R3. Then we configured the RADIUS server specifics on R3. Next we configured AAA login authentication for console access on R3. Finally configuring the line console to use the defined AAA authentication method.

```
R3(config)# username Admin3 secret admin3pa55
R3(config)# radius-server host 192.168.3.2
R3(config)# radius-server key radiuspa55
R3(config)# aaa new-model
R3(config)# aaa authentication login default group radius local
R3(config-line)# login authentication default
```

Device configurations:

R1	R2	R3
hostname R1 ! enable secret 5 1mERr$TfFTxE.mmb5O5 BVC56ndL0 ! aaa new-model ! aaa authentication login SSH-LOGIN local aaa authentication login default local ! username Admin1 secret 5 1mERr$yqLDyfDDWkZGJ 9y568Vjq0 ! line con 0 password ciscoconpa55 login authentication default ! line vty 0 4 password ciscovtypa55 login authentication SSH-LOGIN transport input ssh ! end	hostname R2 ! enable secret 5 1mERr$TfFTxE.mmb5O5 BVC56ndL0 ! aaa new-model ! aaa authentication login default group tacacs+ local ! username Admin2 secret 5 1mERr$lfxtLKoTWhTjn9w Jx3u4s. ! tacacs-server host 192.168.2.2 tacacs-server key tacacspa55 ! line con 0 password ciscoconpa55 login authentication default ! line vty 0 4 password ciscovtypa55 ! end	Hostname R3 ! Enable secret 5 1mERr$TfFTxE.mmb5O5 BVC56ndL0 ! aaa new-model ! aaa authentication login default group radius local ! Username Admin3 secret 5 1mERr$lfxtLKoTWhTjn9w Jx3u4s. ! Radius server 192.168.3.2 Address ipv4 192.168.3.2 auth-port 1645 ! Line con0 Password ciscoenpa55 Login authentication default ! Line vty 0 4 Password ciscovtypa55 ! end

What I learned:

In this activity I learned to configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA. Configure server-based AAA authentication using TACACS+. Configure server-based AAA authentication using RADIUS. We did this by first starting with configuring local AAA Authentication for Console Access on R1. To start we tested the connectivity between PC-A to PC-B, PC-A to PC-C, and PC-B to PC-C to confirm connection. Next was adding a username and password onto R1 setting the username to Admin1 and password(secret) to admin1pa55. Then we enabled AAA and configured AAA authentication for the console to allow use on the local database. Next we set a defined AAA authentication method for the line console on R1. Once all of the commands were imputed correctly we verified the AA authentication by exiting the router and going back in making sure the username and passwords put into the line console work and the proper information is displayed. Next was the Configuration of local AAA authentication for the vty Lines. In this

part we set the domain name to ccnasecurity.com and generated the crypto keys setting the amount of bits to 1024. These steps were to get ready for the use of SSH. Next we configured a named list called SSH-LOGIN to authenticate logins using local AAA. After that we configured the vty lines to use only the called AAA method and only allow for SSH to be used. From there we verified that the SSH worked, logging in from PC-A and confirming the connection. After that we moved to R2 giving it a local username and password. To confirm TACACS+ configuration we entered the server and clicked on the AAA option in the services tab. Making sure that there was entry for R2 and a User Setup entry for Admin2. Next was to configure the TACACS+ server specifics giving it a server host and server key. After that we turned on AAA on R2 and then configured all of the logins to authenticate using the TACACS+ server and set it to know if the TACACS+ server is not available then use the local server. Next was the configuration of the line console 0 to use the default authentication method. The final step is to configure R3 with AAA authentication using RADIUS. I started by configuring the local username and secret password. Next we entered the RADIUS server and saw that the network configuration entry was for R3 and a User Setup entry for Admin3. After that we configured RADIUS server specifics on R3, configuring the server host IP and the secret key. Then we turned on AAA on the R3 router and configured all of the logins to be authenticated by the RADIUS server and set it so that if the RADIUS server is not available then use the local server. Lastly we configured the AAA authentication for the line console to the default authentication method. Finally verifying all AAA authentication methods.