

## AAA Concepts:

- o AAA is a term which stands for Authentication, Authorization and Accounting.
- o AAA is a centralized management of users to access the network devices etc.
- o AAA services allow setting up access control on Cisco Routers & Cisco Switches.
- o Whenever user's attempts to login these network devices verifies by AAA database.
- o User management done on AAA database without need to reconfigure each device.
- o AAA also control connections passing through router for access network resources.
- o AAA provides flexibility and scalability, using privilege levels allows the flexibility.
- o AAA server can be RADIUS protocol or TACACS+ protocol where database located.
- o Use the local database fallback if the TACACS+/RADIUS server becomes unavailable.
- o Fallback method only occurs and work if the AAA server is unavailable or down.
- o There are two uses of AAA one is device administration and second network access.

**Authentication**  
Who are you?

**Authorization**  
How much can you spend?

**Accounting**  
What did you spend it on?

**Statement of Personal Credit Card Account**

Account Number: 1234-567-890 | Statement Closing Date: 01-31-01 | Current Amount Due: \$278.50

JOE EMPLOYEE  
456 SKYVIEW DRIVE  
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO:  
THE BANK  
132 VINE STREET  
ANYTOWN, USA 67500-0010

872919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

**Statement of Personal Credit Card Account**  
Retain this portion for your files.

Cardmember Name: JOE EMPLOYEE | Account Number: 1234-567-890 | Statement Closing Date: 01-31-01

Statement Date: 02-01-01 | Payment Due Date: 03-01-01

Closing Date: 01-31-01

Credit Limit: \$1,500.00 | Credit Available: \$1221.50

New Balance: \$278.50 | Minimum Payment Due: \$20.00

**Account Summary**

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	<b>NEW BALANCE:</b>	<b>\$278.50</b>

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
78543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

PAGE 1 OF 1

### Authentication:

- o Check the user's credentials to verify their identity.
- o Authentication is the process of proving identity to the system.
- o Authentication is the validation of an identity or a credential.
- o The user or computer has to prove its identity to the server or client.
- o Log on to a PC with a user name and password you are authenticating.
- o Authentication does not determine what tasks the individual can do.
- o Authentication merely identifies and verifies who the person or system is.
- o In short or summary basically, Authentication is about who somebody is.

### Authorization:

- o Authorization determines what the user is allowed to do in network.
- o Authorization restrict the access to the user when login to device.
- o Server determines client has permission to use a resource or access file.
- o Authorization is the process of verifying access to something.
- o In short or summary Authorization is about what they are allowed to do.
- o Authorization is the function of specifying access rights to resources.
- o Authorization is process to confirm what you are authorized to perform.

### Accounting:

- o In AAA model, accounting features is also very much important in security.
  - o Accounting command tracking commands, services and resources used by user.
  - o Accounting is the measure of resources consumed by a user during access.
  - o Accounting, includes amount of time, amount of data user has send or received.
  - o Accounting is carried in the form of logs of session statistics and usage information.
  - o Accounting data is used for authorization control, resources utilization, billing & planning.
  - o Accounting is also very much helpful to troubleshoot if network devices are not working.
  - o Accounting is disabled by default in Authentication, Authorization and Accounting model.
  - o AAA Accounting Types Network, Exec, Commands, Connection and Resource.
  - o Accounting collects and stores information regarding and about logins and activity.
  - o Accounting recorded while accessing the specific device during specific time.
-

### AAA Options:

- o Cisco provides a number of ways to implement AAA.
- o Two main protocols are TACACS Server and Radius Server.

### AAA with TACACS+:

- o TACACS+ stands for Terminal Access Controller Access Control System Plus.
- o TACACS+ is a Cisco proprietary protocol that is use to deliver AAA security services.
- o TACACS+ is an application, which is implement through AAA.
- o TACACS+ provides centralized acceptance of user to take the access control of routers.
- o TACACS+ provides other access servers in the network as well.
- o TACACS+ provides to control the authorization of router commands per-user or group.
- o TACACS+ offers multiprotocol support.
- o TACACS+ encrypts entire body of the packet but leaves a standard TACACS+ header.
- o TACACS+ uses the AAA architecture, which separates AAA.

### AAA with RADIUS:

- o RADIUS stand for Remote Authentication Dial in User Service.
- o RADIUS is a security protocol that secures the network against unauthorized access.
- o RADIUS clients run on routers & send authentication request to a centralized server.
- o RADIUS Server contains network service access information and user authentication.
- o RADIUS does not allow users to control which commands can be executed or not.
- o RADIUS is not as useful for router or switch management.
- o RADIUS does not support multiprotocol.
- o RADIUS encrypts password of the access-request packet only from Client to server.
- o RADIUS uses UDP as a transport protocol while TACACS+ uses TCP.
- o RADIUS combines authentication and authorization processes.

<b>RADIUS</b>	<b>TACACS+</b>
RADIUS uses UDP	TACACS+ uses TCP
Uses ports 1812/1645 for authentication Uses ports 1813/1646 for accounting	TACACS+ uses TCP port 49
RADIUS encrypts passwords only	TACACS+ encrypts the entire communication
RADIUS combines authentication and Authorization	TACACS+ treats Authentication, Authorization, and Accountability differently
RADIUS is an open protocol	TACACS+ is Cisco proprietary protocol
RADIUS is a light-weight protocol consuming less resources	TACACS+ is a heavy-weight protocol consuming more resources
RADIUS is limited to privilege mode	TACACS+ supports 15 privilege levels
Mainly used for Network Access	Mainly used for Device Administration