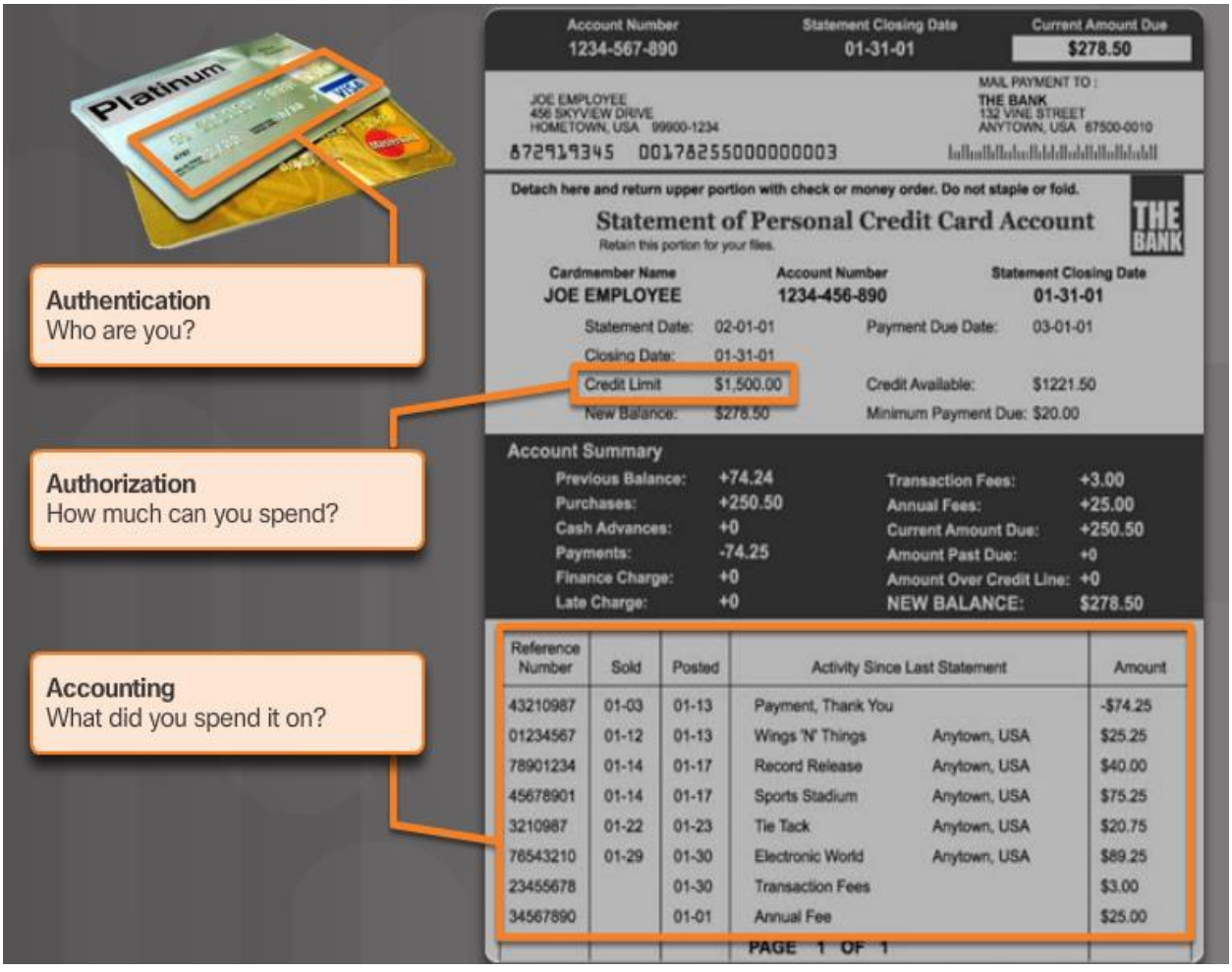
AAA Concepts:

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



Authentication:

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

Authorization:

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

Accounting:

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

AAA Options:

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

AAA with TACACS+:

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

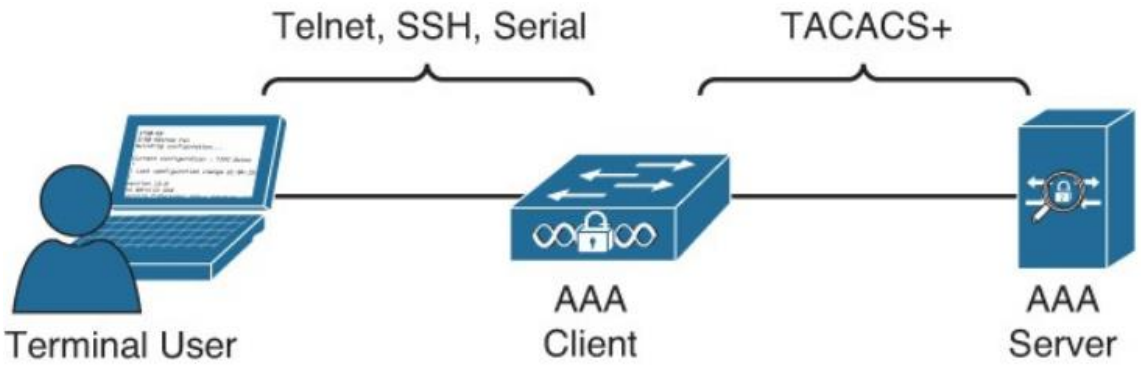
AAA with RADIUS:

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

RADIUS	TACACS+
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

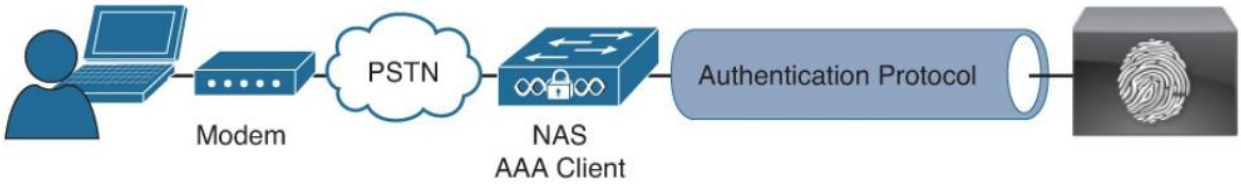
Device Administration:

- Controlling access to who can log in to a network device console, telnet, SSH session.
- Controlling access to who can log in to a network device via other methods.
- Device administration is a process of AAA for controlling the access to network device.
- Which can by any methods via Telnet session, VTY, TTY, SSH session or via Console.
- Device Administrator is user logs into the network devices such as switches routers etc.
- In order to perform the configuration and maintenance of the administered devices.
- There are two uses of AAA, Device Administration and Network Access.



Network Access:

- Securing network access can provide the identity of the device or user.
- Secure network access is necessary in order to identify the user or endpoint.
- Before permitting the entity to communicate or access the network.
- AAA has important role in Network Access authentication and authorization.
- To filter legitimate user AAA Network access authentication is required.
- AAA authenticates these devices & control what these users are authorized for.
- There are two uses of AAA, Device Administration and Network Access.



Local Privilege Authorization Fallback:

- For several functions local database act as fallback method.
- It is design to help the user to prevent accidental lockout from security devices.
- Use local database fallback if the TACACS+/RADIUS server becomes unavailable.
- Fallback only occurs if the AAA Server in unavailable or down.