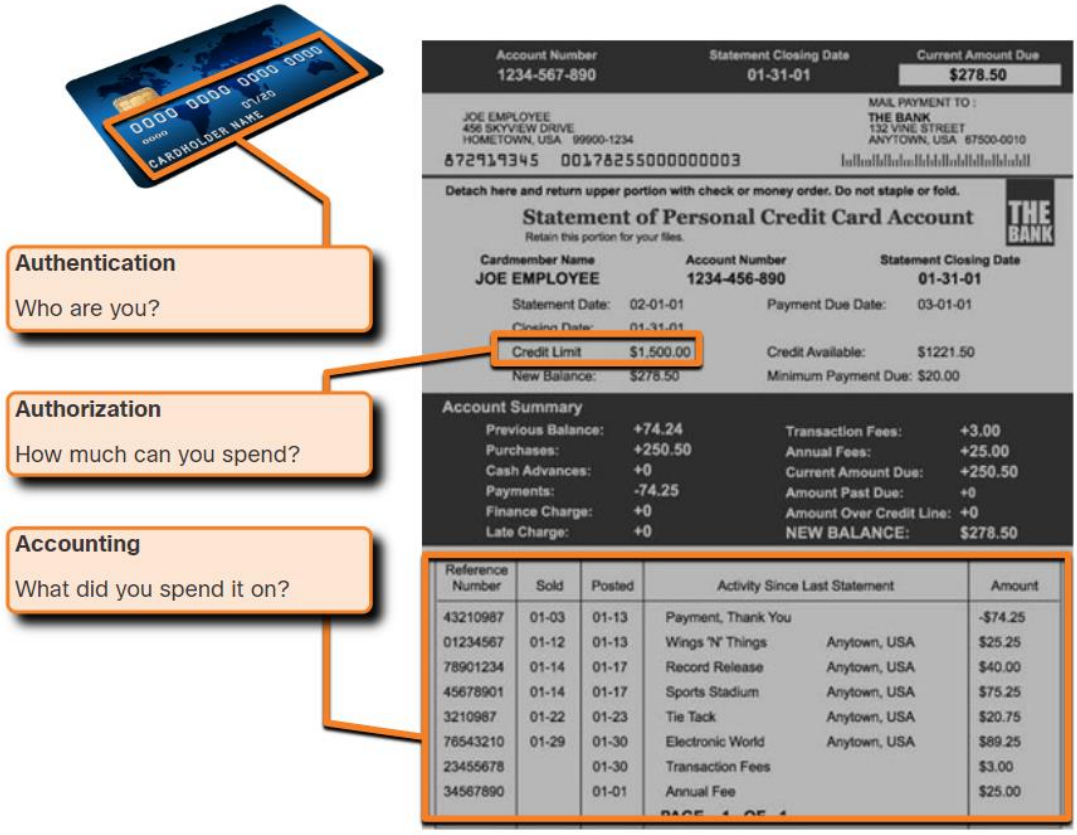
10.2.2

AAA Components

AAA stands for Authentication, Authorization, and Accounting. The AAA concept is similar to using a credit card, as shown in the figure. The credit card identifies who can use it, how much that user can spend, and keeps an account of what items or services the user purchased.

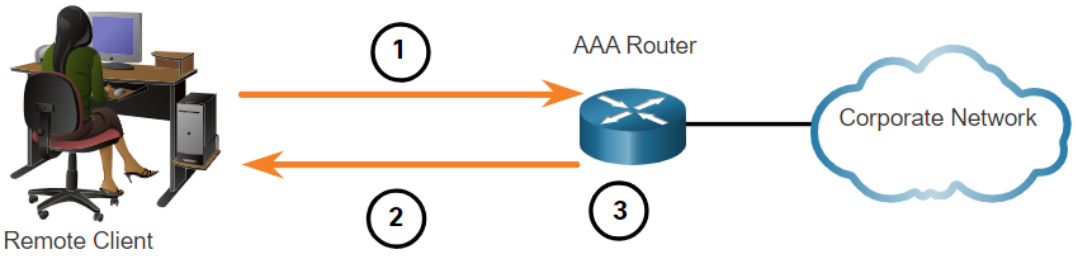
AAA provides the primary framework to set up access control on a network device. AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).



Local and server-based are two common methods of implementing AAA authentication.

Local AAA Authentication

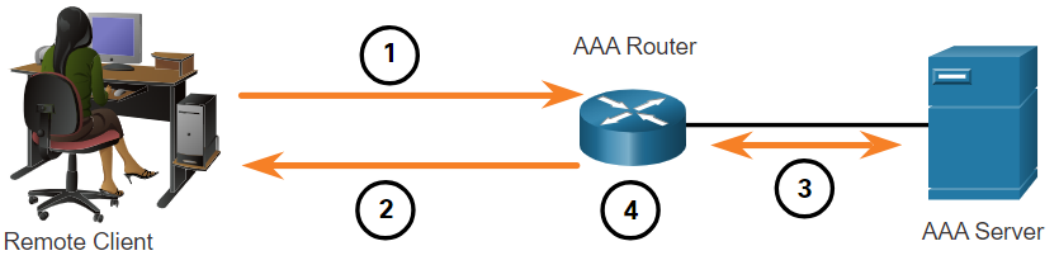
Local AAA stores usernames and passwords locally in a network device such as the Cisco router. Users authenticate against the local database, as shown in figure. Local AAA is ideal for small networks.



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is provided access to the network based on information in the local database.

Server-Based AAA Authentication

With the server-based method, the router accesses a central AAA server, as shown in figure. The AAA server contains the usernames and passwords for all users. The router uses either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocols to communicate with the AAA server. When there are multiple routers and switches, server-based AAA is more appropriate.



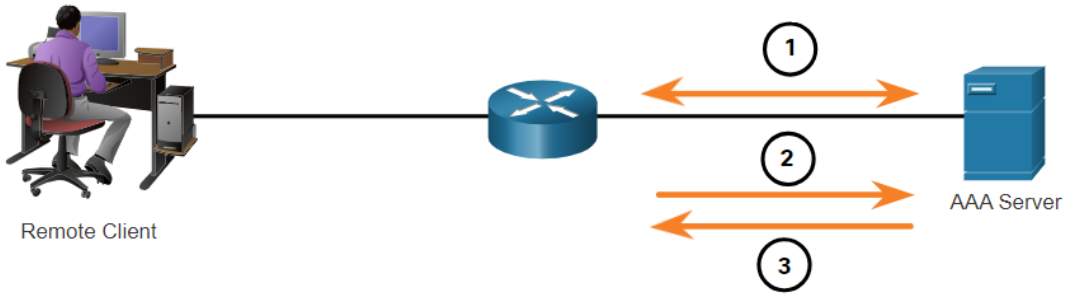
1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a AAA server.
4. The user is provided access to the network based on information in the remote AAA server.

10.2.4

Authorization

AAA authorization is automatic and does not require users to perform additional steps after authentication. Authorization governs what users can and cannot do on the network after they are authenticated.

Authorization uses a set of attributes that describes the user's access to the network. These attributes are used by the AAA server to determine privileges and restrictions for that user, as shown in the figure.



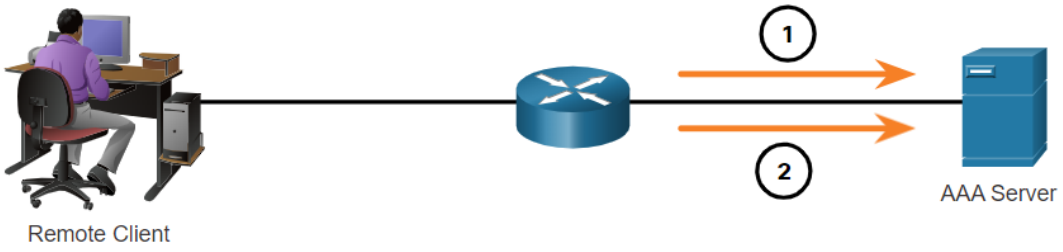
1. When a user has been authenticated, a session is established between the router and the AAA server.
2. The router requests authorization from the AAA server for the client's requested service.
3. The AAA server returns a PASS/FAIL response for authorization.

10.2.5

Accounting

AAA accounting collects and reports usage data. This data can be used for such purposes as auditing or billing. The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.

A primary use of accounting is to combine it with AAA authentication. The AAA server keeps a detailed log of exactly what the authenticated user does on the device, as shown in the figure. This includes all EXEC and configuration commands issued by the user. The log contains numerous data fields, including the username, the date and time, and the actual command that was entered by the user. This information is useful when troubleshooting devices. It also provides evidence for when individuals perform malicious acts.



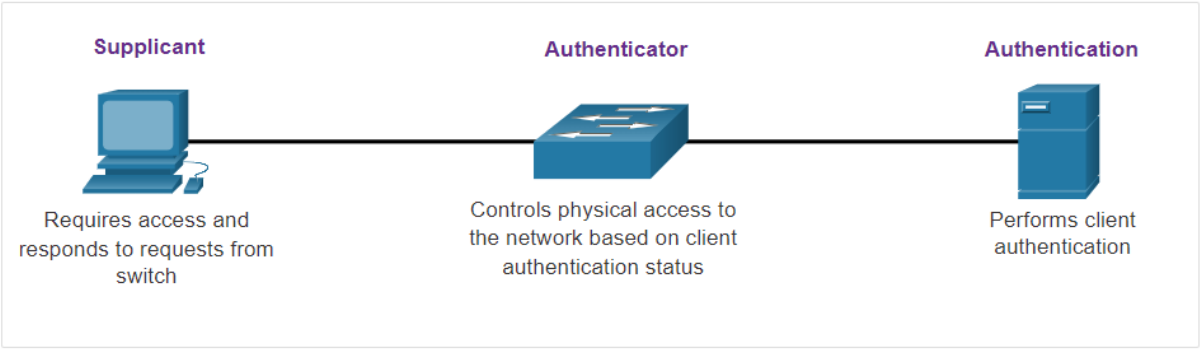
1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

10.2.6

802.1X

The IEEE 802.1X standard is a port-based access control and authentication protocol. This protocol restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.

With 802.1X port-based authentication, the devices in the network have specific roles, as shown in the figure.



- **Client (Supplicant)** - This is a device running 802.1X-compliant client software, which is available for wired or wireless devices.
- **Switch (Authenticator)** –The switch acts as an intermediary between the client and the authentication server. It requests identifying information from the client, verifies that information with the authentication server, and relays a response to the client. Another device that could act as authenticator is a wireless access point.
- **Authentication server** –The server validates the identity of the client and notifies the switch or wireless access point that the client is or is not authorized to access the LAN and switch services.