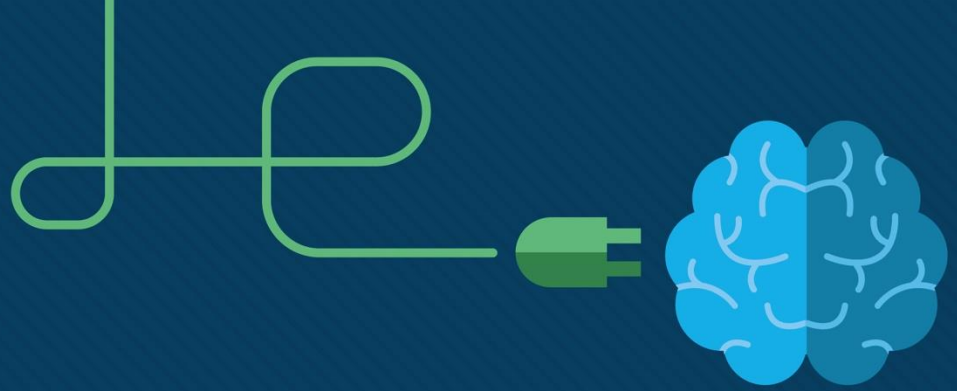


Module 19: Access Control

CyberOps Associate v1.0

Module Objectives

Module Title: Access Control

Module Objective: Explain access control as a method of protecting a network.

Topic Title	Topic Objective
Access Control Concepts	Explain how access control protocols network data.
AAA Usage and Operation	Explain how AAA is used to control network access.

19.1 Access Control Concepts

Communications Security: CIA

Information security deals with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

CIA Triad

The CIA triad consists of three components of information security:

- **Confidentiality -** Only authorized individuals, entities, or processes can access sensitive information.
- **Integrity -** This refers to the protection of data from unauthorized alteration.
- **Availability -** Authorized users must have uninterrupted access to the network resources and data that they require.

Zero Trust Security

- Zero trust is a comprehensive approach to securing all access across networks, applications, and environments.
- This approach helps secure access from users, end-user devices, APIs, IoT, microservices, containers, and more.
- The principle of a zero trust approach is "never trust always verify".
- A zero trust security framework helps to prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through a network.
- In a Zero trust approach, any place at which an access control decision is required should be considered a perimeter.

Zero Trust Security (Contd.)

The three pillars of zero trust are workforce, workloads, and workplace.

- **Zero Trust for the Workforce -** This pillar consists of people who access work applications by using their personal or corporate-managed devices. It ensures only the right users and secure devices can access applications, regardless of location.
- **Zero Trust for Workloads -** This pillar is concerned with applications that are running in the cloud, in data centers, and other virtualized environments that interact with one another. It focuses on secure access when an API, a microservice, or a container is accessing a database within an application.
- **Zero Trust for the Workplace -** This pillar focuses on secure access for all devices, including on the internet of things (IoT), that connect to enterprise networks, such as user endpoints, physical and virtual servers, printers, cameras and more.

Access Control Models

- An organization must implement proper access controls to protect its network resources, information system resources, and information.
- A security analyst should understand the different basic access control models to have a better understanding of how attackers can break the access controls.
- The following table lists various types of access control models:

Access Control Models	Description
Discretionary access control (DAC)	• This is the least restrictive model and allows users to control access to their data as owners of that data. • It may use ACLs or other methods to specify which users or groups of users have access to the information.
Mandatory access control (MAC)	• This applies the strictest access control and is used in military or mission critical applications. • It assigns security level labels to information and enables users with access based on their security level clearance.

Access Control Models (Contd.)

Access Control Models	Description
Role-based access control (RBAC)	• Access decisions are based on an individual's roles and responsibilities within the organization. • Different roles are assigned security privileges, and individuals are assigned to the RBAC profile for the role. • Also known as a type of non-discretionary access control.
Attribute-based access control (ABAC)	It allows access based on attributes of the object to be accessed, the subject accessing the resource, and environmental factors regarding how the object is to be accessed.
Rule-based access control (RBAC)	• Network security staff specify sets of rules or conditions that are associated with access to data or systems. • These rules may specify permitted or denied IP addresses, or certain protocols and other conditions. • Also known as Rule Based RBAC.
Time-based access control (TAC)	It allows access to network resources based on time and day.

19.2 AAA Usage and Operation

AAA Operation

- A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected. These design requirements are identified in the network security policy.
- The policy specifies how network administrators, corporate users, remote users, business partners, and clients access network resources.
- The network security policy can also mandate the implementation of an accounting system that tracks who logged in and when and what they did while logged in.
- The Authentication, Authorization, and Accounting (AAA) protocol provides the necessary framework to enable scalable access security.

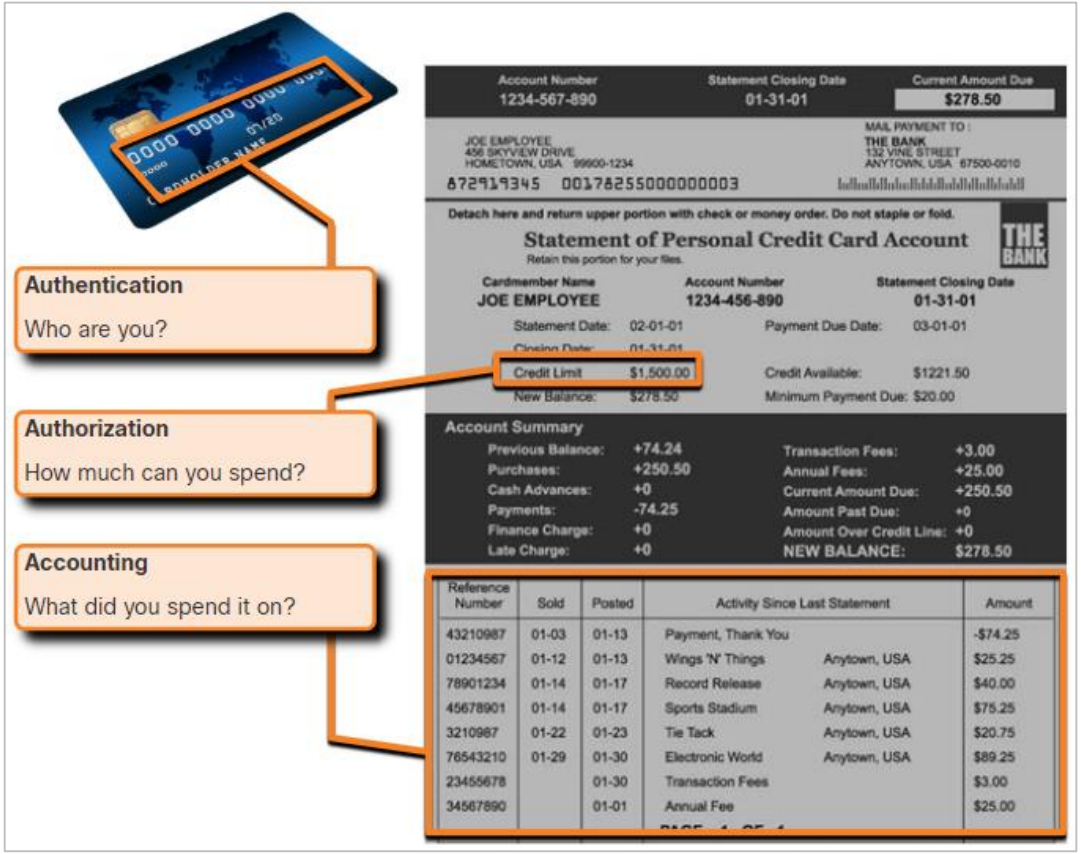
AAA Operation (Contd.)

The following table lists the three independent security functions provided by the AAA architectural framework:

AAA Component	Description
Authentication	• Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods. • AAA authentication provides a centralized way to control access to the network.
Authorization	• After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform. • An example is "User can access host server XYZ using SSH only."
Accounting	• Accounting records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made. • Accounting keeps track of how network resources are used. • An example is "User accessed host server XYZ using SSH for 15 minutes."

AAA Operation (Contd.)

This concept is similar to the use of a credit card, as indicated by the figure. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.



AAA Authentication

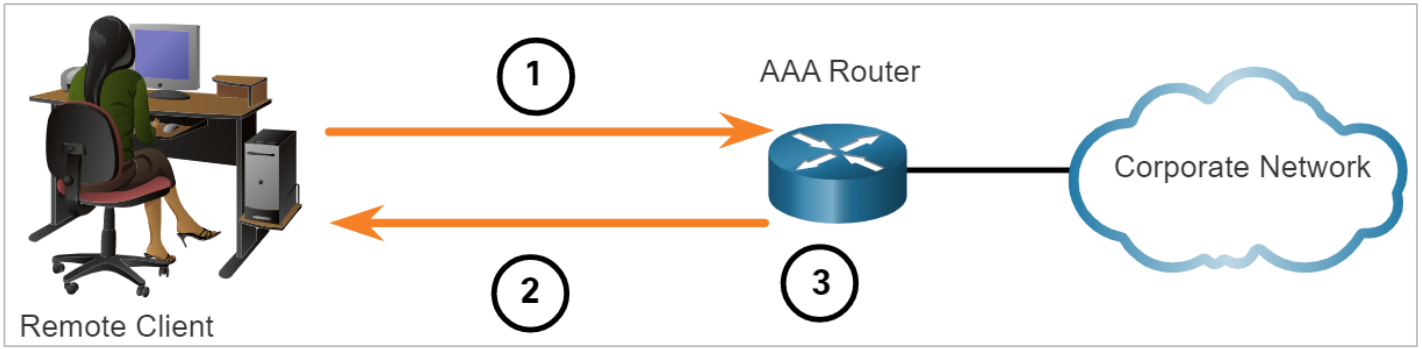
- AAA Authentication can be used to authenticate users for administrative access or it can be used to authenticate users for remote network access.
- Cisco provides two common methods for implementing AAA Services:

Local AAA Authentication

- This method is known as self-contained authentication because it authenticates users against locally stored usernames and passwords.
- Local AAA is ideal for small networks.

AAA Authentication (Contd.)

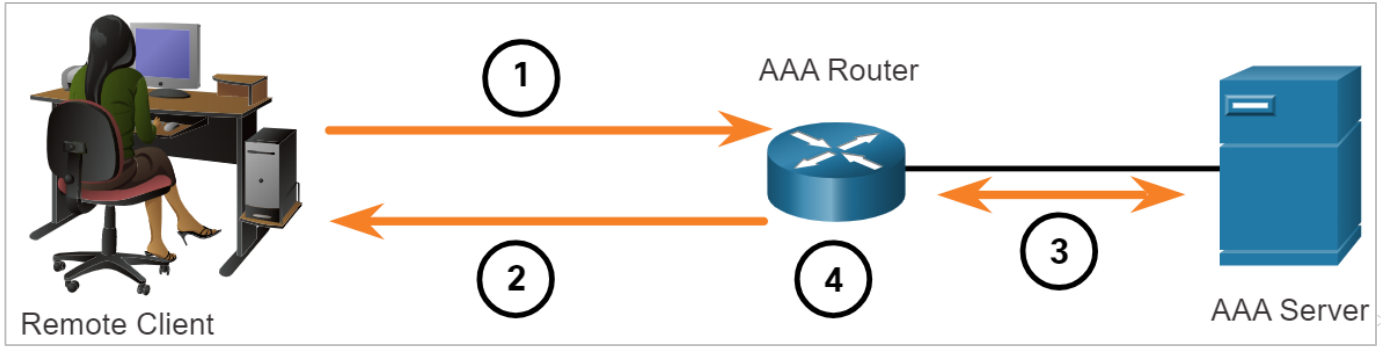
- The client establishes a connection with the router.
- The AAA router prompts the user for a username and password.
- The router authenticated the username and password using the local database and the user is provided access to the network based on information in the local database.



AAA Authentication (Contd.)

Server-based AAA Authentication

- This method authenticates against a central AAA server that contains the usernames and passwords for all users. This is ideal for medium-to-large networks.
- The client establishes a connection with the router.
- The AAA router prompts the user for a username and password.
- The router authenticates the username and password using a AAA server.
- The user is provided access to the network based on information in the remote AAA server.



AAA Authentication (Contd.)

Centralized AAA

- Centralized AAA is more scalable and manageable than local AAA authentication, and therefore, it is the preferred AAA implementation.
- A centralized AAA system may independently maintain databases for authentication, authorization, and accounting.
- It can leverage Active Directory or Lightweight Directory Access Protocol (LDAP) for user authentication and group membership, while maintaining its own authorization and accounting databases.
- Devices communicate with the centralized AAA server using either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocols.

AAA Authentication (Contd.)

The following table lists the differences between the two protocols:

Functions	TACACS+	RADIUS
Functionality	It separates authentication, authorization, and accounting functions according to the AAA architecture. This allows modularity of the security server implementation.	It combines authentication and authorization but separates accounting, which allows less flexibility in implementation than TACACS+.
Standard	Mostly Cisco supported	Open/RFC standard
Transport	TCP port 49	UDP ports 1812 and 1813, or 1645 and 1646
Protocol CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client

AAA Authentication (Contd.)

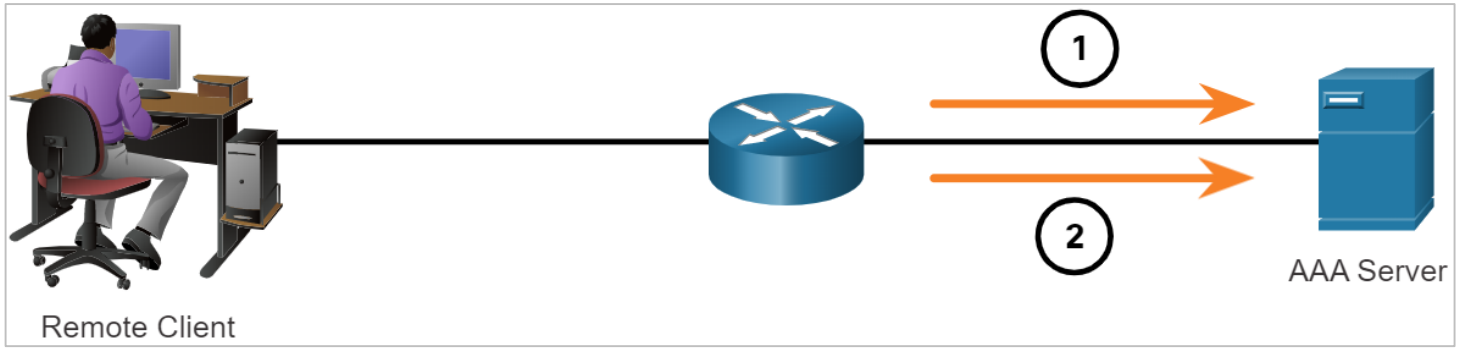
Functions	TACACS+	RADIUS
Confidentiality	Encrypts the entire body of the packet but leaves a standard TACACS+ header.	Encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is unencrypted, leaving the username, authorized services, and accounting unprotected.
Customization	Provides authorization of router commands on a per-user or per-group basis.	Has no option to authorize router commands on a per-user or per-group basis.
Accounting	Limited	Extensive

AAA Accounting Logs

- Centralized AAA also enables the use of the Accounting method.
- Accounting records from all devices are sent to centralized repositories, which simplifies auditing of user actions.
- AAA Accounting collects and reports usage data in AAA logs. These logs are useful for security auditing.
- The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.
- One widely deployed use of accounting is to combine it with AAA authentication. This helps with managing access to internetworking devices by network administrative staff.

AAA Accounting Logs (Contd.)

- Accounting provides more security than just authentication. The AAA servers keep a detailed log of exactly what the authenticated user does on the device.
- This includes all EXEC and configuration commands issued by the user.
- When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
- When the user finishes, a stop message is recorded and the accounting process ends.



AAA Accounting Logs (Contd.)

The following table describes the types of accounting information that can be collected:

Types of Accounting Information	Description
Network Accounting	It captures information for all Point-to-Point Protocol (PPP) sessions, including packet and byte counts.
Connection Accounting	It captures information about all outbound connections that are made from the AAA client, such as by SSH.
EXEC Accounting	It captures information about user EXEC terminal sessions on the network access server, including username, date, start and stop times, and the access server IP address.
System Accounting	It captures information about all system-level events.
Command Accounting	It captures information about the EXEC shell commands for a specified privilege level ,as well as the date and time each command was executed, and the user who executed it.
Resource Accounting	It captures 'start' and 'stop' record support for connections that have passed user authentication.

19.3 Access Control Summary

What Did I Learn in this Module?

- The CIA triad consists of the primary three components of information security: confidentiality, integrity, and availability.
- Zero trust is a comprehensive approach to securing all access across networks, applications, and environments.
- The principle of zero trust is "never trust, always verify". The pillars of trust are zero trust for workforce, zero trust for workloads, and zero trust for workplace.
- In a zero trust approach, any place at which an access control decision is required should be considered a perimeter.
- Access control methods include discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), attribute-based control (ABAC), rule-based access (RBAC), and time-based access control (TAC).
- A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected which is specified in the network security policy.

What Did I Learn in this Module? (Contd.)

- Authentication, Authorization, and Accounting (AAA) systems provide the necessary framework to enable scalable security.
- Cisco provides two common methods of implementing AAA services: Local AAA Authentication and Server-based AAA Authentication.
- Centralized AAA is more scalable and manageable than local AAA and is the preferred AAA implementation.
- Devices communicate with the centralized AAA server using with the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control Systems (TACACS+) protocols.
- Centralized AAA also enables the use of the accounting method. AAA accounting collects and reports usage data in AAA logs.
- Various types of accounting information that can be collected are network accounting, connection accounting, EXEC accounting, system accounting, command accounting, and resource accounting.


CISCO