**Authentication, Authorization, and Accounting (AAA)**is an architectural framework to gain access to computer resources, enforcing policies, auditing usage, to provide essential information required for billing of services and other processes essential for network management and security.

**Authentication**

[Authentication](https://www.strongdm.com/authentication)is the process of identifying a user and granting them access to the network. Most of the time, this is done through traditional username and password credentials. However, users could also use [passwordless authentication](https://www.strongdm.com/blog/passwordless-authentication) methods, including biometrics like eye scans or fingerprints, and hardware such as hardware tokens or smart cards.

The server evaluates the credential data submitted by the user compared to the ones stored in the network's database.

**Authorization**

After authentication, the authorization process enforces the network policies, granular access control, and user privileges. The cybersecurity AAA protocol determines which specific network resources the user has permission to access, such as a particular application, database, or online service. It also establishes the tasks and activities that users can perform within those authorized resources.

**Accounting**

Accounting, the final process in the framework, is all about measuring what's happening within the network. As part of the protocol, it will collect and log data on user sessions, such as length of time, type of session, and resource usage. The value here is that it offers a clear audit trail for compliance and business purposes.

Accounting helps in both security and operational evaluations. For instance, network administrators can look at user access privileges to specific resources to see about any changes. They could also adjust capacity based on the resources most frequently used and common activity trends.

**The Pros**

1. AAA framework increases the scalability of a network: Scalability is the property of a system to handle a growing amount of work by adding resources to the system.
2. It causes increased flexibility and better control of the network.
3. It helps maintain standard protocols in the network.
4. RADIUS allows for unique credentials for each user.
5. IT Admins will have a central point for the user and system authentication.

**The Cons**

1. On RADIUS Servers, Configuration and Initial setup can be complicated and time-consuming.
2. It is a very hard choice to determine which is the best RADIUS server software and implementation model for your organization.
3. Maintenance can be difficult and time-consuming for on-prem hardware.

Windows NT LAN Manager (NTLM) is a challenge-response authentication protocol used to authenticate a client to a resource on an Active Directory domain. When the client requests access to a service associated with the domain, the service sends a challenge to the client, requiring that the client perform a mathematical operation using its authentication token, and then return the result of this operation to the service. The service may validate the result or send it to the Domain Controller (DC) for validation. If the service or DC confirm that the client’s response is correct, the service allows access to the client.

NTLM is generally considered insecure because it uses outdated cryptography that is vulnerable to several modes of attacks. NTLM is also vulnerable to the pass-the-hash attack and brute-force attacks.

NTLM is used is places where backwards compatibility is required. Microsoft does not recommend NTLM for new implementations.

Role-Based Access Control (RBAC):

* This method grants access based on a user's assigned role within an organization.
* For example, an "administrator" role might have full access, while a "viewer" role has limited permissions.
* RBAC is a widely used and relatively straightforward approach

Attribute-Based Access Control (ABAC):

* ABAC grants access based on a combination of user attributes, resource attributes, and environmental conditions.
* This offers more granular control than RBAC and allows for dynamic authorization decisions.
* For instance, access to a file might depend on the user's security clearance, the file's sensitivity level, and the time of day

KDC: Key Distribution Center

TGS: Ticket Granting Server

Ticket Granting Ticket

SAR SAML Authentication request