Contents

1 Configuring AAA

1.1 Introduction

1.1.1 Overview

Authentication, authorization and accounting (AAA) is a network security management mechanism, which provides basic authentication, authorization, and accounting (billing) services for users who access networks. The content of AAA is described as follows:

- Authentication service: Identifies users before they access networks to check whether the users have access permissions.
- Authorization service: Classifies user permissions to grants different access permissions to users.
- Accounting service: Records users' usage of network resources. The statistical data can be used for analysis and billing.

AAA boasts strong flexibility and controllability, scalability, standardized authentication, and supports multiple backup systems. Compared with simple access control functions provided by devices such as local username authentication and line password-based authentication, AAA provides a higher level of security protection and therefore becomes the overriding access control method.

1.1.2 Principles

1. Basic Concepts

- Security method

  A security method refers to the method used to implement authentication, authorization, and accounting services. Security methods can be classified into AAA authentication methods, AAA authorization methods, and AAA accounting methods by service type.

  Based on the service provider, service methods can be further classified into service methods providing no security management, service methods providing security management through a local device, and service methods providing security management through a remote server. For details, see 1 3. AAA Authentication, 1 4. AAA Authorization, and 1 5. AAA Accounting.

- Method list

  Method lists are classified into authentication method lists, authorization method lists, and accounting method lists based on the AAA service type. Each method list provides multiple security methods for this type of AAA service, to ensure that alternative methods are available if one method is unavailable.

  A method list contains one or more security methods. The sequence for the methods to take effect is subject to the sequence of security methods defined in the list, that is, a method defined earlier takes effect earlier. If a method fails to respond during AAA service provision, a device switches to the next method until all methods in the method list are tried. If a method returns a failure or all methods fail to respond, the process stops and the device cannot provide the security service for users.

Notice

A device tries the next method only when no response is received from the previous method. For example, if a method denies user access during identity authentication, the identity authentication process ends and the device does not switch to other identity authentication methods.

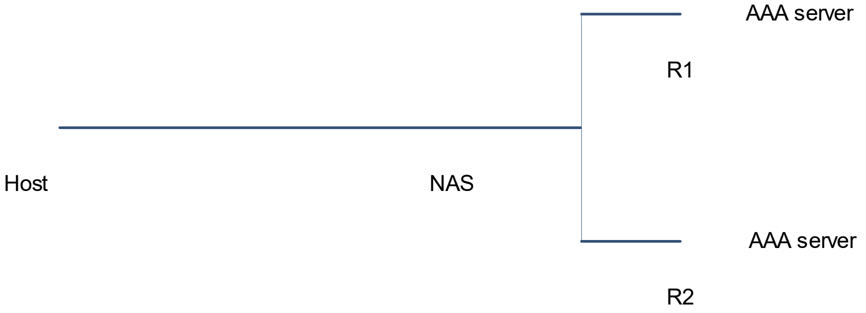
- AAA server group

  An AAA server is a device that provides remote AAA security services for users.

  An AAA server group is a collection of one or more AAA servers of the same type and provides security services for users as a security method.

2. AAA Basic Architecture

Figure 1-1 **Topology of a Typical AAA Network**



As shown in Figure 1-1, a typical AAA network consists of hosts (users), a network access server (NAS), and an AAA server (remote server). AAA uses the client/server (C/S) structure. A host sends an AAA request to the NAS as a client. After receiving the request, the NAS requests the AAA security services from the AAA server as a client and provides network access permissions for the host based on the returned result.

- Main roles

  Host: A host is a device that requests network access permissions and usually refers to a user.

  NAS: A NAS responds to hosts' network access requests and manages the hosts by using security methods provided by an AAA server.

  AAA server: An AAA server provides security methods for the NAS.

- Brief process of typical AAA services

  a Configure a method list and enable the AAA security services on the NAS. The method list provides three security methods: R1 server, R2 server, and local username database (with the effective sequence from left to right). Host-related identity information has been configured in the three methods.

  b After a host connects to the NAS through a network, the NAS provides the AAA security services for the host by using a method in the method list. According to the sequence that the methods take effect, the NAS requests the security services from R1 first.

  c If R1 responds to the NAS successfully, the NAS provides network access permissions for the host based on security information provided by R1. If R1 does not respond, the NAS switches the security method and requests the security services from R2, and so on until all methods in the method list are used up.

Instruction

An AAA server can use a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) server. Unless otherwise specified in this document, the RADIUS server is used as the AAA server. For details about TACACS+, see "Configuring TACACS" in the *Security Configuration Guide*.

3. AAA Authentication

AAA authentication checks information (username and password) about a user who requests the access service, to determine whether the user has the network access permission.

- AAA authentication methods

  AAA authentication methods are classified into authentication exemption, local authentication, and remote server group authentication based on the method provider.

  - Authentication exemption

    User legitimacy is not checked. This method is used only when users are very trustworthy. You are not advised to use this method.

  - Local authentication

    Local authentication uses the database on the NAS to manage user information (such as usernames, passwords, and attributes) and identify user identities.

  - Remote server group authentication

    This authentication method uses the user database on the remote server to manage user data and identify user identities. It can achieve multi-device centralized authentication with large capacity and high reliability. A remote server group supports RADIUS servers and TACACS+ servers.

- AAA authentication types

  AAA authentication is classified into login authentication, enable authentication, IEEE 802.1X authentication, 2nd-generation Web authentication, and File Transfer Protocol (FTP) authentication based on the user access mode.

  - Login authentication

    This authentication verifies user identities when the users log in to the command line interface (CLI) of the NAS through Secure Shell (SSH), telnet, or FTP.

  - Enable authentication

    After users log in to the NAS CLI, this authentication verifies the users' identity information before their CLI execution permissions are elevated, that is, users are authenticated before they enter the privileged EXEC mode.

  - IEEE 802.1X authentication

    This authentication is used to verify identities of IEEE 802.1X access users.

  - 2nd-generation Web authentication

This authentication uses a 2nd-generation portal server to verify the identities of users who access networks.

- FTP authentication

  FTP authentication is especially used for FTP users. If no FTP authentication method is configured, login authentication is used to authenticate FTP users.

- General authentication method

  You can specify a general authentication method for IEEE 802.1X authentication and 2nd-generation Web authentication. If no authentication method is configured for 2nd-generation Web authentication and IEEE 802.1X authentication or the configured methods fail to respond, the configured general authentication method takes effect as an alternative method.

4. AAA Authorization

AAA authorization is used to manage services available to users and control network access permissions of access users. After the AAA authorization service is enabled, users can use only permitted services and are granted permissions in their permitted scopes.

- AAA authorization methods

  AAA authorization methods are classified into direct authorization, local authentication, and remote server group authentication based on the method provider.

  - Direct authorization

    Direct authorization provides default permissions that the access device allows users to use. It is used only when users are very trustworthy.

  - Local authorization

    Configure attribute authorization for local users on the NAS, which completes the authorization.

  - Remote server group authorization

    Configure user attribute authorization on the remote server. The NAS completes authorization by means of a remote server group. When all servers in a remote server group fail, you can configure local authorization or direct authorization as an alternative method.

- AAA authorization types

  AAA authorization is classified into EXEC authorization, command authorization, config-commands authorization, console authorization, and network authorization based on the permission type.

  - EXEC authorization

    EXEC authorization grants different privilege levels (0–15) to users when the users log in to the NAS CLI.

    EXEC authorization is usually used in conjunction with login authentication. After login authentication and EXEC authorization are configured on the same line, if a user passes login authentication but fails in EXEC authorization, the user cannot open the CLI.

  - Command authorization

    Command authorization grants authorization to commands after users log in to the NAS CLI.

When a user enters a command and attempts to run it, AAA sends the command to the security server. If the security server allows this command, the command is executed. Otherwise, the command is not executed and a command execution denial message is displayed.

- Config-commands authorization

  This authorization grants authorization to commands in configuration modes (including the global configuration mode and sub-modes).

- Console authorization

  This authorization grants authorization to commands to be executed by users who log in through the console.

  The system can differentiate users who log in through the console from those who log in through other terminals. You can enable or disable command authorization for users who log in through the console. If command authorization is disabled for users who log in through the console, the command authorization method list that has been applied to the console line no longer takes effect.

- Network authorization

  Network authorization grants available network services to users, such as traffic, bandwidth, and timeout services.

  Network authorization is based on authentication. Network authorization is available only for authenticated users. The RADIUS or TACACS+ server grants permissions to authenticated users by returning a series of attributes.

5. AAA Accounting

AAA accounting is used to record users' usage of network resources to implement billing, auditing, and tracking functions.

The accounting service starts accounting after a user passes authentication and records the user's network access activities. It stops accounting when the user logs out, and generates a network resource access report for the user.

- AAA accounting methods

  AAA accounting methods are classified into no accounting, local accounting, and remote server group accounting based on the method provider.

  - No accounting

    Accounting is not performed on users.

  - Local accounting

    Local accounting is completed by the NAS, which collects statistics on and limits the number of local user connections. The fee calculation function is unavailable.

  - Remote server group accounting

    Accounting is performed by a remote server. You can configure local accounting as an alternative method to avoid an accounting failure occurring when all servers in a remote server group fail.

- AAA accounting types

  AAA accounting can be classified into EXEC accounting, command accounting, and network accounting based on the accounting content.

  - EXEC accounting

    Accounting is both performed when users log in to and log out of the NAS CLI.

  - Command accounting

    Command accounting is used to record commands run by a user after the user logs in to the NAS CLI from a terminal.

  - Network accounting

    Network accounting is used to record information about sessions of users who access the network (such as IEEE 802.1X users and 2nd-generation Web-authenticated users).

6. Multi-Domain AAA

In multi-domain AAA, users are assigned to different domains and independent security methods are defined for each domain so that users in different domains use different security methods.

In a multi-domain environment, you can configure a separate AAA method list for each domain on the NAS. Therefore, users with the same attribute can be assigned to the same domain for the ease of management.

- Basic principles of AAA service based on domain names

  a A user submits identity authentication information to the NAS.

  b The NAS resolves the domain name in the identity authentication information.

  c The NAS checks whether the domain name is defined. If no, the NAS refuses to provide security services. If yes, the NAS makes further judgment.

  d If no method list is defined for the domain name, the NAS refuses to provide security services. If a method list is defined, the NAS provides security services.

- Username forms

  A username can be expressed in four forms. In the usernames below, "domain-name" indicates a domain name.

  - userid@domain-name
  - domain-name\userid
  - userid.domain-name
  - userid

  In the preceding username forms, the username form (userid) with no domain name uses the default domain name (**default**).

- Domain name matching

  If the username of an authenticated user carries domain information but the domain is not configured on the NAS, the NAS cannot provide AAA services for the user.

  Exact match is adopted to match domain names carried in usernames with those configured on the NAS. For example, if domain.com and domain.com.cn are configured on the NAS and a username is expressed in the form of aaa@domain.com, the NAS determines that the user belongs to domain.com rather than domain.com.cn.

1.2 Restrictions and Guidelines

- Before configuring any AAA function, run the **aaa new-model** command to enable the AAA security services.

Otherwise, no command can be configured.

- AAA authentication, authorization, and accounting are three independent processes. You can use only the authentication service without authorization or accounting.
- The basic methodology and process of configuring the AAA authentication, authorization, or accounting services are as follows:

  a Enable AAA security services.

  b Determine the required AAA security service type based on the scenario.

  c Configure an AAA method list for the security service type.

  d In a corresponding mode, apply an AAA method list to make it take effect (methods do not need to be applied for some security services. For details, see specific configuration tasks).

  If this step is not configured, methods configured in step C do not take effect but the default method is used.
- Configure user information before configuring security methods.
  - To use the remote server group method, configure user data on remote servers. For details about how to configure user data, see the operation instructions of the remote servers.
  - To use the local method, configure local user data on the local device. For details about local users, see "Configuring Basic Management" in the *Basic Configuration Manual*.

1.3 Configuration Task Summary

AAA configuration includes the following tasks:

(1) (Optional) Configuring an AAA Server Group

(2) Configuring AAA Authentication

- Configuring Basic Features of AAA Authentication
- (Optional) Configuring a General Authentication Method
- (Optional) Configuring AAA Authentication Logging

(3) (Optional) Configuring AAA Authorization

- Configuring Basic Features of AAA Authorization
- (Optional) Configuring the Function of Caching Command Authorization Results
- (Optional) Configuring the Default Role for AAA Users
- (Optional) Configuring AAA Accounting
- Configuring Basic Features of AAA Accounting
- (Optional) Configuring a Policy for User Accounting Start Failures

(4) (Optional) Configuring Domain-Based AAA Services

1.4 Configuring an AAA Server Group

1.4.1 Overview

AAA usually uses the remote server group method to provide AAA services for users. This method provides more flexible and rich security services than the local method.

1.4.2 Restrictions and Guidelines

- One or more servers can be added to each server group.
- Both RADIUS and TACACS+ support server group configuration. The configuration procedure below uses RADIUS as an example. For details about a TACACS+ server group, see "Configuring TACACS" in the *Security Configuration Guide*.
- When configuring the authentication, authorization, and accounting method lists, you can specify different server groups for them.
- In a custom server group, only servers in the default server group can be specified and applied.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an AAA custom server group.

aaa group server radius *group-name*

No server group is configured by default.

The name of a server group cannot be set to a predefined keyword "radius" or "tacacs+".

(4) Add an AAA server group member.

server { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port* | **acct-port** *acct-port*] *

No AAA server group member is added to a server group by default.

(5) (Optional) Specify a VRF instance for the AAA server group.

ip vrf forwarding *vrf-name*

No VRF instance is specified for an AAA server group by default.

When a server group in a specified VRF instance is used, the source IP address used by the device to communicate with a remote server needs to be acquired from the VRF instance. If you run the **ip radius source-interface** command to specify the source interface of request packets, the IP address obtained from this source interface is prior to that acquired from the VRF instance.

(6) Configure the MGMT interface for the AAA server group.

ip oob [**via mgmt** *mgmt-number*]

An AAA server group uses MGMT 0 by default.

1.5 Configuring Basic Features of AAA Authentication

1.5.1 Overview

AAA authentication is used to verify user identities. After AAA authentication is configured, users can access network resources only after passing the authentication specified in security methods in the method list.

1.5.2 Restrictions and Guidelines

- After AAA authentication is configured, if no authentication method is configured and the default authentication method does not exist, users can log in through the console without authentication but other types of access users need to pass local authentication.
- If multiple methods are defined in the method list, when a method fails to respond, the device switches to the next method. The execution sequence of methods is the sequence of methods configured in the method list. If a method responds and returns a failure, the device does not switch to the next method.
- If you have passed login authentication (except the authentication exemption method) when logging in to the CLI, the device records the username, and then uses the username for authentication when Enable authentication is performed. You do not need to enter the username again but the entered password must match the username. If login authentication fails or the authentication exemption method is used when you log in to the CLI, the username will not be recorded, and you need to enter the username for authentication in the further Enable authentication.
- The authentication exemption method allows any user to access network resources without authentication. You are not advised to use this method. Only in some special cases (all access users are trustworthy and no network failure caused by authentication system problems is allowed), this method can be used as an alternative method when the device receives no response in the remote server group authentication and local authentication.

1.5.3 Configuration Tasks

Configure basic features of AAA authentication. Select at least one of the following tasks to configure.

- Configuring Login Authentication
- Configuring Enable Authentication
- Configuring IEEE 802.1X Authentication
- Configuring 2nd-Generation Web Authentication
- Configuring FTP Authentication

1.5.4 Configuring Login Authentication

1. Overview

After login authentication is configured, access users who log in through SSH, telnet, or FTP need to be authenticated before accessing network resources.

2. Restrictions and Guidelines

A configured login authentication method must be applied to a line that needs login authentication. Otherwise, the method does not take effect.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure a login authentication method list.

aaa authentication login { **default** | *list-name* } *method*&<1-4>

No login authentication method list is configured by default.

(5) (Optional) Configure the maximum number of consecutive failed login attempts.

aaa local authentication attempts *max-attempts*

The default maximum number of consecutive failed login attempts is **3**.

(6) (Optional) Configure the user lockout duration.

aaa local authentication lockout-time *lockout-time*

After the number of login attempts of a user exceeds the configured number of consecutive failed login attempts, the user is locked out for 15 minutes by default.

(7) Enter the configuration mode of a specified line.

line { **console** | **vty** } *first-line* [*last*‑*line*]

(8) Apply the login authentication method list to the line.

login authentication { **default** | *list-name* }

The default login authentication method list applied to a line is the default method list.

1.5.5 Configuring Enable Authentication

1. Overview

After Enable authentication is configured and a user logs in to the NAS CLI through a terminal, the user must be authenticated before running the **enable** command to enter the privileged EXEC mode.

1. Restrictions and Guidelines

After an Enable authentication method list is configured, the Enable authentication function takes effect automatically.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure an Enable authentication method list.

aaa authentication enable default *method*&<1-4>

No Enable authentication method list is configured by default.

1.5.6 Configuring IEEE 802.1X Authentication

1. Overview

After IEEE 802.1X authentication is configured on an interface, users connected to the interface must be authenticated before accessing network resources.

2. Restrictions and Guidelines

For details about IEEE 802.1X configuration, see "Configuring IEEE 802.1X" in the *Security Configuration Guide*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure the address and key of a RADIUS server.

radius-server host { *ipv4-address* | *ipv6-address* } [**key** [**0** | **7**] *text-string*]

The address and key of a RADIUS server are not configured by default.

(5) Configure an IEEE 802.1X authentication method list.

aaa authentication dot1x { **default** | *list-name* } *method*&<1-4>

No IEEE 802.1X authentication method list is configured by default.

(6) Apply the IEEE 802.1X authentication method list.

dot1x authentication { **default** | *list-name* }

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable IEEE 802.1X authentication on the interface.

dot1x port-control auto

IEEE 802.1X authentication is disabled on a port by default.

1.5.7 Configuring 2nd-Generation Web Authentication

1. Overview

After 2nd-generation Web authentication is configured, identity authentication needs to be performed by a 2nd-generation portal server.

2. Restrictions and Guidelines

- If a local account is used for authentication, you can run the **aaa local user allow public account** command to enable the function of allowing multiple clients to share one account.

- For details about Web authentication configuration, see "Configuring Web Authentication" in the *Security Configuration Guide*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure the address and key of a RADIUS server.

radius-server host { *ipv4-address* | *ipv6-address* } [**key** [**0** | **7**] *text-string*]

The address and key of a RADIUS server are not configured by default.

(5) Configure the communication key between the NAS and the portal server.

web-auth portal key *key-string*

No key is configured for the communication between the device and the authentication server by default.

(6) Configure a 2nd-generation Web authentication method list.

aaa authentication web-auth { **default** | *list-name* } *method*&<1-4>

(7) Enter the 2nd-generation Web authentication template configuration mode.

web-auth template eportalv2

(8) Configure parameters for the 2nd-generation Web authentication template.

a Configure an authentication method list for the template.

authentication *method-list*

The default authentication method list is used by a template by default.

b Configure an IP address for the portal server used for Web authentication.

ip [*ip-address* | **oob** | **vrf** *name*]

No IP address and VRF instance are specified for the Web authentication server by default.

c Configure the authentication page of the portal server used for Web authentication.

url *url-string*

No page address of the authentication server is configured by default.

(9) Return to the global configuration mode.

exit

(10) Enter the interface configuration mode.

interface *interface-type interface-number*

(11) Enable 2nd-generation Web authentication on the interface.

web-auth enable eportalv2

2nd-generation Web authentication is disabled on a port by default.

1.5.8 Configuring FTP Authentication

1. Overview

After FTP authentication is configured, FTP users need to pass FTP authentication upon login.

2. Restrictions and Guidelines

If the AAA FTP security service is enabled on a device, users must perform FTP authentication through AAA.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Enable the FTP server function.

ftp-server enable

The FTP server function is disabled by default.

(5) Configure an FTP authentication method list.

aaa authentication ftp { **default** | *list-name* } *method*&<1-4>

No FTP authentication method list is configured by default.

(6) Configure FTP to use AAA accounts for login authentication.

ftp-server authentication { **default** | *list-name* }

FTP does not support login authentication on AAA accounts by default.

1.6 Configuring a General Authentication Method

1.6.1 Overview

A general authentication method can be used as an alternative method of 2nd-generation Web authentication and IEEE 802.1X authentication. If no authentication method is configured for 2nd-generation Web authentication or IEEE 802.1X authentication or the configured method fails to respond, the general authentication method takes effect as an alternative method.

1.6.2 Restrictions and Guidelines

If both IEEE 802.1X authentication and 2nd-generation Web authentication are configured on the device, you can configure a general method for them together.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4) Configure a general authentication method list.

aaa authentication general { **default** | *list-name* } *method*&<1-4>

No general authentication method is configured by default.

1.7 Configuring AAA Authentication Logging

1.7.1 Overview

The device generates logs when an AAA user passes authentication. If a large number of users go online concurrently, the device generates considerable logs, which may degrade the device performance or cause frequent screen refreshing. In this case, you can disable the logging function or restrict the logging rate.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure AAA authentication logging. Please configure only one task.

- Disable AAA authentication logging.

  no aaa log enable

  AAA authentication logging is enabled by default.

- Configure the rate of AAA authentication logging.

  aaa log rate-limit *rate-limit*

  Five AAA authentication logs are printed per second by default.

1.8 Configuring Basic Features of AAA Authorization

1.8.1 Overview

AAA authorization is used to manage services available to users and control network use permissions of access users. After the basic features of AAA authorization are enabled, users can use only the permitted services and are granted permissions in their permitted scopes.

1.8.2 Restrictions and Guidelines

- EXEC authorization is usually used together with login authentication. Authentication and authorization can use different methods and different servers, and the authentication and authorization results of the same user may be different. If a user passes login authentication but fails in EXEC authorization, the user cannot open the CLI.

- When configuring command authorization, specify the command level, which is used as the default level of commands. For example, if a command is visible to users above level 14, the default level of the command is 14.
- EXEC authorization and command authorization need to be applied to a line so that they take effect.
- Command authorization is unavailable when role-based access control (RBAC) is enabled. For details about RBAC, see "Configuring RBAC" in the *Basic Configuration Guide*.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an AAA authorization method. Configure at least one of the tasks.

- Configure an EXEC authorization method list to authorize permitted users to open the CLI.

  aaa authorization exec { **default** | *list-name* } *method*&<1-4>

  No EXEC authorization method list is configured by default.

- Configure a network authorization method list to authorize permitted users to access network services.

  aaa authorization network { **default** | *list-name* } *method*&<1-4>

  No network authorization method list is configured by default.

- Grant authorization to all commands in configuration modes.

  aaa authorization config-commands

  The authorization for commands in configuration modes is disabled by default.

- Enable command authorization for users who log in through the console. You can enable command authorization for users who log in through the console and users who log in through other terminals separately.

  aaa authorization console

  Command authorization is disabled for users who log in through the console by default.

(4) (Optional) Enter the configuration mode of a specified line.

line { **console** | **vty** } *first-line* [*last−line*]

(5) (Optional) Apply the authorization method to the specific line. Please configure only one task.

- Apply the EXEC authorization method to the specific line.

  authorization exec { **default** | *list-name* }

  EXEC authorization is disabled by default.

- Apply the command authorization method to the specific line.

  authorization commands *level* { **default** | *list-name* }

  The command authorization function is disabled by default.

1.9 Configuring the Function of Caching Command Authorization Results

1.9.1 Overview

After this function is configured, the device locally caches command authorization results returned by the AAA server. For subsequent commands with the level same as the cached authorized commands, command authorization can be performed based on the locally cached results.

1.9.2 Restrictions and Guidelines

Authorization results in the local cache apply only to the current session and commands of the current level. The authorization of other sessions or commands of other levels are performed by the remote server and local authorization can be performed only after their results are cached locally.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the function of caching command authorization results.

aaa command-author cache

The function of caching command authorization results is disabled by default.

1.10 Configuring the Default Role for AAA Users

1.10.1 Overview

This function is used to configure the global user role. If no role is configured for an authorized user, the role is used by default. Different roles have different levels of command execution permissions on the device. The global user role **network-operator** is used by default. This role has the permission to run commands of the lowest level on the device.

1.10.2 Restrictions and Guidelines

- Run the **aaa new-model** and **role enable** commands before configuring this function.
- For details about user roles, see "Configuring RBAC" in the *Basic Configuration Guide*.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the default role for AAA authorized users.

aaa user-role default { *priv-level* | *role-name* | **network-admin** | **network-operator** }

The default role of AAA authorized users is **network-operator**.

1.11 Configuring Basic Features of AAA Accounting

1.11.1 Overview

AAA accounting is used to record users' usage of network resources, login and logout processes, and command execution information.

1.11.2 Restrictions and Guidelines

- EXEC accounting is performed only on users who pass login authentication and log in to the NAS. When login authentication is not configured or the authentication exemption method is adopted, EXEC accounting is not performed.
- If accounting start is not performed on a user upon login, accounting stop will not be performed when the user logs out.
- The remote server group method used in the command accounting function supports only the TACACS+ protocol.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an AAA accounting method. Configure at least one of the tasks.

- Configure an EXEC accounting method list.

  aaa accounting exec { **default** | *list-name* } **start-stop** *method*&<1-4>

  NO EXEC accounting method list is configured by default.

  A configured EXEC accounting method list must be applied to a line so that it takes effect.

- Configure a command accounting method list.

  aaa accounting commands *level* { **default** | *list-name* } **start-stop** *method*&<1-4>

  No command accounting method list is configured by default.

  A configured command accounting method list must be applied to a line so that it takes effect.

- Configure a network accounting method list.

  aaa accounting network { **default** | *list-name* } **start-stop** *method*&<1-4>

  No network accounting method list is configured by default.

(4) (Optional) Enable the accounting update function.

aaa accounting update

Accounting update is disabled by default.

After this function is configured, the device updates accounting information periodically. This function helps improve the accounting accuracy. You are advised to configure it.

(5) (Optional) Configure the accounting update interval.

aaa accounting update periodic *interval*

The default accounting update interval is **5** minutes.

It is recommended that the accounting update interval not be configured unless otherwise specified.

(6) Apply the accounting method. Please configure only one task.

- Enter the line configuration mode and apply the EXEC accounting method. Run the following commands in sequence:

  line { **console** | **vty** } *first-line* [*last*－*line*]

  accounting exec { **default** | *list-name* }

  A line is associated with the default method list by default.

- Enter the line configuration mode and apply the command accounting method. Run the following commands in sequence:

  line { **console** | **vty** } *first-line* [*last*－*line*]

  accounting commands [*accounting-commands-level*] { **default** | *list-name* }

  A line is associated with the default method list by default.

- Apply the network accounting method to IEEE 802.1X accounting.

  dot1x accounting { **default** | *list-name* }

  IEEE 802.1X accounting is associated with the default method by default.

1.12 Configuring a Policy for User Accounting Start Failures

1.12.1 Overview

After this function is configured, the user status is online or offline if the accounting start fails.

1.12.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the user online/offline status after the accounting start fails.

aaa accounting start-fail { **offline** | **online** }

The user online/offline status after an accounting start failure is not configured by default.

1.13 Configuring Domain-Based AAA Services

1.13.1 Overview

The domain-based AAA services classify users into different domains and the domains use different security methods to provide AAA services.

1.13.2 Restrictions and Guidelines

- The device supports a maximum of 32 domains.
- After the domain-based AAA services are enabled, if information of a user does not carry domain information, the user is assigned to the default domain **default**. A method list for the **default** domain must be configured on the device. Otherwise, users without domain information cannot use AAA services.

1.13.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable domain-based AAA services.

aaa domain enable

The domain-based AAA services are disabled by default.

(4) Create a domain and enter the domain configuration mode.

aaa domain { **default** | *domain-name* }

No domain is configured by default.

(5) Configure an authentication method list for the AAA domain.

authentication { **dot1x** | **enable** | **login** } { **default** | *list-name* }

The default authentication method list used in an AAA domain is the default method list.

(6) Configure an accounting method list for the AAA domain.

accounting { **commands** | **exec** | **network** } { **default** | *list-name* }

The default accounting method list used in an AAA domain is the default method list.

(7) Configure an authorization method list for the AAA domain.

authorization { **commands** | **exec** | **network** } { **default** | *list-name* }

The default authorization method list used in an AAA domain is the default method list.

(8) (Optional) Set the domain status.

state { **active** | **block** }

A configured domain is active by default.

(9) (Optional) Configure whether usernames carry domain name information.

username-format { **with-domain** | **without-domain** }

Usernames carry domain name information during interaction between the NAS and the server by default.

(10) (Optional) Configure a limit on the number of users supported in the domain.

access-limit *access-limit-number*

No limit on the number of users supported in a domain is configured by default.

1.14 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

⚠ **Notice**

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1 AAA Monitoring

Command	Purpose
show aaa accounting update	Displays accounting update information.
show aaa domain [**default** | *domain-name*]	Displays information about a configured domain.
show aaa lockout	Displays lockout parameter configuration in the current login authentication.
show aaa group	Displays all AAA server groups.
show aaa method-list	Displays all AAA method lists.
show aaa user { **all** | **by-id** *session-id* | **by-name** *user-name* | **lockout** }	Displays AAA user information.
clear aaa local user lockout { **all** | **user-name** *user-name-id* }	Clears the list of locked users.

1.15 Configuration Examples

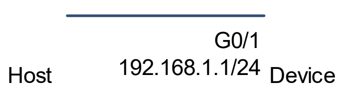
1.15.1 Configuring Local Login Authentication and Local EXEC Authorization

1. Requirements

You can use local login authentication and local EXEC authorization together to control the permissions of users who log in to the device. In this method, you need to configure accounts and their permissions only in the local user database of the device, to control user permissions with no need to use an authentication server.

2. Topology

Figure 1-1 **Topology of Local Login Authentication and Local EXEC Authorization**



3. Notes

- Enable AAA security services on the device.
- Add accounts to the local user database of the device.
- Create an authentication method list and an authorization method list.
- Apply the authentication method and authorization method to a specific line.

4. Procedure

Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

Add accounts **host1** and **host2** to the local user database of the device and configure account permissions.

```
Device(config)# username host1 privilege 15 password password1
Device(config)# username host2 privilege 4 password password2
```

Create a login authentication method list named **login-method**, in which the authentication method is local authentication, and create an EXEC authorization method list named **exec-method**, in which the authorization method is local authorization.

```
Device(config)# aaa authentication login login-method local
Device(config)# aaa authorization exec exec-method local
```

Apply the authentication method list and authorization method list to a line.

```
Device(config)# line vty 0 35
Device(config-line)# login authentication login-method
Device(config-line)# authorization exec exec-method
```

5. Verification

Run the **show aaa method-list** command on the device to display configured method lists.

```
Device# show aaa method-list

Authentication method-list:
aaa authentication login login-method local

Accounting method-list:
```

```
Authorization method-list:
aaa authorization exec exec-method local
```

Log in to the device through telnet by using client software (such as PuTTY or Xshell) and verify that different users have different account permissions.

- Log in to the device as user **host1** and check that the privilege level of the user is 15.

```
User Access Verification

Username:host1
Password:password1



Device# show privilege
Current privilege level is 15
```

- Log in to the device as user **host2** and check that the privilege level of the user is 4.

```
User Access Verification

Username:host2
Password:password2



Device# show privilege
Current privilege level is 4
```

6. Configuration Files

```
!
username host1 privilege 15 password password1
username host2 privilege 4 password password2
!
aaa new-model
!
aaa authorization exec exec-method local
aaa authentication login login-method local
!
line vty 0 35
 authorization exec exec-method
 login authentication login-method
!
end
```

7. Common Errors

- No authentication method list and authorization method list are applied to a specific line.
- No account is configured in the local user database.

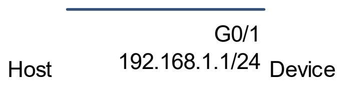
1.15.2 Configuring Enable Authentication

1. Requirements

Users can have execution permissions with a privilege level of 0 to 15. After Enable authentication is configured, users must be authenticated when running the **enable** command to switch the permission to a higher level. As shown in Figure 1-1, when both local authentication and Enable password authentication are configured on the device, local authentication is preferred. If local authentication is invalid, enable password authentication is used.

2. Topology

Figure 1-1 **Topology of Enable Authentication**



3. Notes

- Enable AAA security services on the device.
- Configure the local user database and Enable password.
- Configure an Enable authentication method list.

Instruction

Only one Enable authentication method list can be defined. Therefore, you do not need to define the name of the Enable authentication method list. After the default method list is configured, the Enable authentication function takes effect automatically.

4. Procedure

Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

Add account **host1** to the local user database and set the privilege level of the account to **15**.

```
Device(config)# username host1 privilege 15 password password1
```

Set the password to **enpassword1** for privilege level 15 in Enable authentication.

```
Device(config)# enable secret level 15 enpassword1
```

Configure an Enable authentication method list, in which local authentication is prior to Enable password authentication.

```
Device(config)# aaa authentication enable default local enable
```

5. Verification

Log in to the device as user **host1** and check that the privilege level of the user is 15.

```
User Access Verification

Username:host1
Password:password1



Device# show privilege
Current privilege level is 15
```

Switch the privilege level to 4 and verify that no password is required for authentication.

```
Device# enable 4
Device# show privilege
Current privilege level is 4
```

Switch the privilege level to 15 and verify that identity authentication is needed. Local authentication has a higher priority. Therefore, you can enter the password of **host1** (**password1**) for authentication to successfully switch the privilege level to 15.

```
Device# enable 15
Password:password1

Device# show privilege
Current privilege level is 15
```

6. Configuration Files

```
!
username host1 privilege 15 password password1
!
aaa new-model
!
aaa authentication enable default local enable
!
enable secret 5 $1$7b8Y$v6u11F23p9y3vwp6
!
end
```

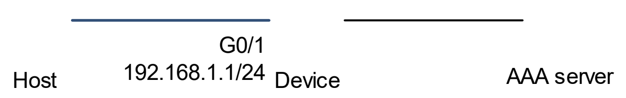
1.15.3 Configuring Network Authorization

1. Requirements

Network authorization needs to be configured to grant available network services to users, such as the traffic, bandwidth, and timeout services.

2. Topology

Figure 1-1 **Topology of Network Authorization**



3. Notes

- Enable AAA security services.
- Configure a network authorization method list.
- Apply the network authorization method list to a specific interface line (skip this step if you configure the default method).

4. Procedure

Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

Configure the default network authorization method list.

```
Device(config)# aaa authorization network default group radius none
```

5. Verification

Run the **show aaa method-list** command on the device to display configuration results.

```
Device# show aaa method-list

Authentication method-list:

Accounting method-list:

Authorization method-list:
aaa authorization network default group radius none
```

6. Configuration Files

```
!
aaa new-model
!
aaa authorization network default group radius none
!
```

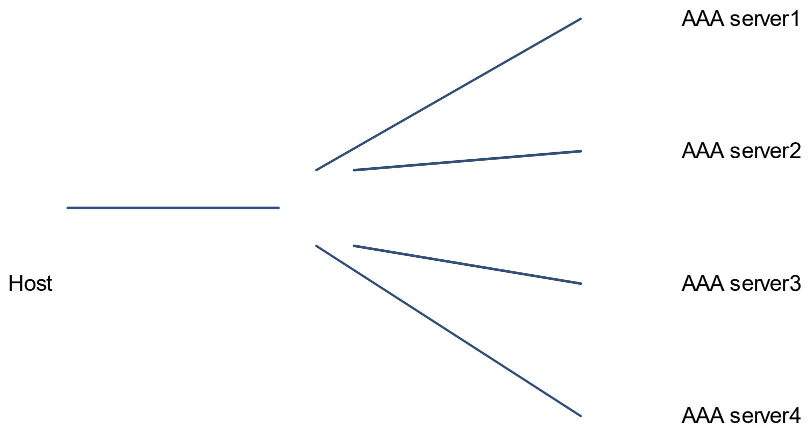
1.15.4 Configuring an AAA Server Group

1. Requirements

A custom AAA server group needs to be created to provide AAA services.

2. Topology

Figure 1-1 **Topology of an AAA Server Group**



3. Notes

- Configure AAA servers.
- Create an AAA custom server group.
- Add server group members to the custom server group.

4. Procedure

(1) Add AAA servers (the following uses RADIUS servers as an example).

```
Device> enable
Device# configure terminal
Device(config)# radius-server host 10.1.1.1
Device(config)# radius-server host 10.1.1.2
Device(config)# radius-server host 10.1.1.3
Device(config)# radius-server host 10.1.1.4
```

(2) Configure a global RADIUS server communication key.

```
Device(config)# radius-server key radiuskey
```

(3) Create a server group named **group1** and add members to the group.

```
Device(config)# aaa group server radius group1
Device(config-gs-radius)# server 10.1.1.1
Device(config-gs-radius)# server 10.1.1.2
Device(config-gs-radius)#exit
```

(4) Create a server group named **group2** and add members to the group.

```
Device(config)#aaa group server radius group2
Device(config-gs-radius)#server 10.1.1.3
Device(config-gs-radius)#server 10.1.1.4
Device (config-gs-radius)#exit
```

5. Verification

Run the **show aaa group** command on the device to display the configuration results.

```
Device# show aaa group
Type       Reference  Name
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          group1
radius     1          group2
```

6. Configuration Files

```
!
radius-server host 10.1.1.1
radius-server host 10.1.1.2
radius-server host 10.1.1.3
radius-server host 10.1.1.4
radius-server key radiuskey
!
aaa group server radius group1
 server 10.1.1.1
 server 10.1.1.2
!
aaa group server radius group2
 server 10.1.1.3
 server 10.1.1.4
!
```

7. Common Errors

For RADIUS servers that use non-default authentication ports and non-default accounting ports, the authentication port or accounting port is not specified when the **server** command is run to add servers.

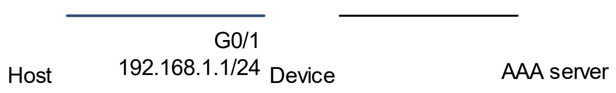
1.15.5 Configuring Domain-based AAA Services

1. Requirements

After a domain is created and a security method list is specified for the domain, users belonging to the domain use security methods of the domain for authentication, authorization, and accounting.

2. Topology

Figure 1-1 **Topology of Domain-Based AAA Services**



3. Notes

- Configure a RADIUS server in advance so that RADIUS server authentication and accounting can be performed.
- Enable AAA security services.
- Configure an AAA security method list.
- Enable domain-based AAA services.
- Create a domain.
- Associate the AAA security method list with the domain.
- Configure domain attributes.

4. Procedure

(1) Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(2) Configure an AAA server (the following uses the RADIUS server as an example).

```
Device(config)# radius-server host 192.168.1.2 key radiuskey
```

(3) Configure an AAA security method list.

```
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa accounting network list3 start-stop group radius
```

(4) Enable domain-based AAA services.

```
Hostname(config)# aaa domain enable
```

(5) Create a domain and configure domain attributes.

```
Device(config)# aaa domain domain.com
Device(config-aaa-domain)# authentication dot1x default
Device(config-aaa-domain)# accounting network list3
Device(config-aaa-domain)# username-format without-domain
```

5. Verification

Run the **show aaa domain** command on the device to display domain configuration.

```
Device# show aaa domain domain.com
```

```
=============Domain domain.com=============
State: Active
Username format: With-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
 accounting network list3
```

6. Configuration Files

```
!
aaa new-model
aaa domain enable
!
aaa domain domain.com
 authentication dot1x default
 accounting network list3
 username-format without-domain
!
aaa accounting network list3 start-stop group radius
aaa authentication dot1x default group radius
!
radius-server host 192.168.1.2 key radiuskey
!
```

1.16 Common Errors

- When a local method is configured to provide AAA security services, no user information is configured in the local database.
- When a remote server group method is configured to provide AAA security services, no RADIUS/TACACS+ server is configured and no user information is configured on the server.