Security Configuration

S5900-24S4T2Q Ethernet Switch

Contents

Chapter 1 AAA Configuration

1.1 AAA Overview

Access control is the way to control access to the network and services. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your OLT or access server.

1.1.1 AAA Security Service

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- Authentication: It is a method of identifying users, including username/password inquiry and encryption according to the chosen security protocol.

  Authentication is a method to distinguish the user's identity before users access the network and enjoy network services. AAA authentication can be configured through the definition of an authentication method list and then application of this method list on all interfaces. This method list defines the authentication type and the execution order; any defined authentication method list must be applied on a specific interface before it is executed. The only exception is the default authentication method list (which is named default). If there are no other authentication method lists, the default one will be applied on all interfaces automatically. If any one is defined, it will replace the default one. For how to configure all authentications, see "Authentication Configuration".

- Authorization: it is a remote access control method to limit user's permissions.

  AAA authorization takes effect through a group of features in which a user is authorized with some permissions. Firstly, the features in this group will be compared with the information about a specific user in the database, then the comparison result will be returned to AAA to confirm the actual permissions of this user. This database can be at the accessed local server or switch, or remote Radius/TACACS+ server. The Radius or TACACS+ server conducts user authorization through a user-related attribute-value peer. The attribute value (AV) defines the allowably authorized permissions. All authorization methods are defined through AAA. Like authentication, an authorization method list will be first defined and then this list will be applied on all kinds of interfaces. For how to carry on the authorization configuration, see "Authorization Configuration".

- Accounting: it is a method to collect user's information and send the information to the security server. The collected information can be used to open an account sheet, make auditing and form report lists, such as the user ID, start/end time, execution commands, and the number of packets or bytes.

The accounting function can track the services that users access, and at the same time track the service-consumed network resource number. When AAA accounting is activated, the access server can report user's activities to the TACACS+ or Radius server in way of accounting. Each account contains an AV peer, which is stored on the security server. The data can be used for network management, client's accounting analysis or audit. Like authentication and authorization, an accounting method list must be first defined and then applied on different interfaces. For how to carry on the accounting configuration, see "Accounting Configuration".

1.1.2 Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS, TACACS+, and Kerberos
- Multiple backup systems

1.1.3 AAA Principles

AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

1.1.4 AAA Method List

To configure AAA, define a named method list first and then apply it to the concrete service or interface. This method list defines the running AAA type and their running sequence. Any defined method list must be applied to a concrete interface or service before running. The only exception is the default method list. The default method list is automatically applied to all interfaces or services. Unless the interface applies other method list explicitly, the method list will replace the default method list.

A method list is a sequential list that defines the authentication methods used to authenticate a user. In AAA method list you can specify one or more security protocols. Thus, it provides with a backup authentication system, in case the initial method is failed. Our software uses the first method listed to authenticate users; if that method does not respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

It is important to notice that the software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local user name database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

The following figures shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. Take the authentication as an example to demonstrate the relation between AAA service and AAA method list.

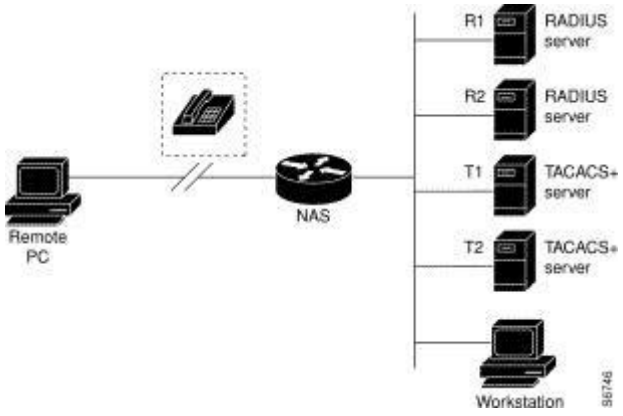

Figure 1- 1 Typical AAA Network Configuration

In this example, default is the name of the method list, including the protocol in the method list and the request sequence of the method list follows the name. The default method list is automatically applied to all interfaces.

When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated.

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Suppose the system administrator wants to apply the method list to a certain or a specific port. In such case, the system administrator should create a non-default method list and then apply the list of this name to an appropriate port.

1.1.5 AAA Configuration Process

You must first decide what kind of security solution you want to implement. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack. Before you configure AAA, you need know the basic configuration procedure. To do AAA security configuration on switches or access servers, perform the following steps:

- If you decide to use a security server, configure security protocol parameters first, such as RADIUS, TACACS+, or Kerberos.
- Define the method lists for authentication by using an AAA authentication command.
- Apply the method lists to a particular interface or line, if required.

- (Optional) Configure authorization using the aaaauthorization command.
- (Optional) Configure accounting using the aaa accountingcommand.

1.2 Authentication Configuration

1.2.1 AAA Authentication Configuration Task List

- Configuring Login Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Configuring Message Banners for AAA Authentication
- Modifying the Notification Character String for Username Input
- Modifying AAA authentication password-prompt
- Creating the Authentication Database with the Local Priviledge

1.2.1 AAA Authentication Configuration Task

General configuration process of AAA authentication

To configure AAA authentication, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(2) Configuring Authentication Method List Using aaa authentication

(3) If necessary, apply the accounting method list to a specific interface or line.

1.2.2.1 Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the aaa authentication login command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the aaa authentication login command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command. After the authentication method lists are configured, you can apply these lists by running login authentication. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa authentication login {**default** | *list-name*}*method1* [*method2...*]	Enables AAA globally.
line [**console** | **vty**] *line-number* [*ending-line-number*]	Enter the configuration mode of a line.
login authentication {**default** | *list-name*}	Applies the authentication list to a line or set of lines. (In the line configuration mode)

The list-name is a character string used to name the list you are creating. The key word method specifies the actual method of the authentication method. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

aaa authentication login default group radius

Note:
Because the none keyword enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.
If you cannot find the authentication method list, you can only login through the console port. Any other way of login is in accessible.

The following table lists the supported login authentication methods:

Keyword	Notes
enable	Uses the enable password for authentication.
group *name*	Uses named server group for authentication.
group radius	Uses RADIUS for authentication.
group tacacs+	Uses group tacacs+ for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
localgroup	Uses the local strategy group username database for authentication.
local-case	Uses case-sensitive local user name authentication.
none	Passes the authentication unconditionally.

(1) Using the enable password to carry on the login authentication:

To specify the enable password as the user authentication method, run the following command:

aaa authentication login default enable

(2) Using the line password to login

Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default line

Before you can use a line password as the login authentication method, you need to define a line password.

(3) Using the local password to carry on the login authentication:

When you run aaa authentication login, you can use the keyword “local” to designate the local database as the login authentication method. For example, if you want to specify the local username database as the user authentication method and not define any other method, run the following command:

aaa authentication login default local

For information about adding users into the local username database, refer to the section "Establishing Username Authentication" in this chapter.

(4) Login Authentication Using RADIUS

Use the aaa authentication login command with the group radius method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default group radius

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter "Configuring RADIUS."

1.2.2.2 Enabling Password Protection at the Privileged Level

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line. Use the following command in global configuration mode:

Command	Purpose
aaa authentication enable default *method1* [*method2...*]	Enables user ID and password checking for users requesting privileged EXEC level.

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered.

The following table lists the supported enable authentication methods:

Keyword	Notes
enable	Uses the enable password for authentication.
group *group-name*	Uses named server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses tacacs+ for authentication.
line	Uses the line password for authentication.
none	Passes the authentication unconditionally.

When configuring enable authentication method as the remote authentication, use RADIUS for authentication. Do as follows:

(1) Uses RADIUS for enable authentication:

The user name for authentication is $ENABLE*level*$; level is the privileged level the user enters, that is, the number of the privileged level after enable command. For instance, if the user wants to enter the privileged level 7, enter command enable 7; if configuring RADIUS for authentication, the user name presenting to Radius-server host is $ENABLE7$; the privileged level of enable is 15 by default, that is, the user name presenting to Radius-server host in using RADIUS for authentication is $ENABLE15$. The user name and the password need to configured on Radius-server host in advance. The point is that in user database of Radius-server host, the Service-Type of the user specifying the privileged authentication is 6, that is, Admin-User.

1.2.2.3 Configuring Message Banners for AAA Authentication

The banner of configurable, personal logon or failed logon is supported. When AAA authentication fails during system login, the configured message banner will be displayed no matter what the reason of the failed authentication is.

Configuring the registration banner

Run the following command in global configuration mode.

Command	Purpose
aaa authentication banner *delimiter text-string delimiter*	Configures a personal logon registration banner.

Configuring the banner of failed logon

Run the following command in global configuration mode.

Command	Purpose
aaa authentication fail-message *delimiter text-string delimiter*	Configures a personal banner about failed logon.

Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the text character string, indicating that the banner is ended.

1.2.2.4 Modifying the Notification Character String for Username Input

To modify the default text of the username input prompt, run aaa authentication username-prompt. You can run no aaa authentication username-prompt to resume the password input prompt.

username：

The aaa authentication username-prompt command does not change any prompt information provided by the remote TACACS+ server or the RADIUS server. Run the following command in global configuration mode:

Command	Purpose
aaa authentication username-prompt *text-string*	Modifies the default text of the username input prompt.

1.2.2.5 Modifying AAA authentication password-prompt

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt command. To return to the default password prompt text, use the no form of this command. You can run no aaa authentication username-prompt to resume the password input prompt.

password：

The aaa authentication password-prompt command does not change any prompt information provided by the remote TACACS+ server or the RADIUS server. Run the following command in global configuration mode:

Command	Purpose
aaa authentication password-prompt *text-string*	String of text that will be displayed when the user is prompted to enter a password.

1.2.2.6 Creating the Authentication Database with the Local Priviledge

To create the enable password database with the local priviledge level, run enable password { [encryption-type] encrypted-password} [level level] in global configuration mode. To cancel the enable password database, run no enable password [level level].

enable password { [***encryption-type***] *encrypted-password*} [**level** *level*]

no enable password [**level** *level*]

1.2.3 AAA Authentication Configuration Example

1.2.3.1 RADIUS Authentication Example

The following example shows how to configure the switch to authenticate and authorize using RADIUS:

```
aaa authentication login radius-login group radius local aaa
authorization network radius-network group radius line vty 3
login authentication radius-login
```

The meaning of each command line is shown below:

- The aaa authentication login radius-login group radius local command configures the switch to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated usingthe local database.

The aaa authorization network radius-network group radius command queries RADIUS for network authorization, address assignment, and other access lists.

- The login authentication radius-login command enables the radius-login method list for line 3.

1.3 Authorization Configuration

1.3.1 AAA Authorization Configuration Task List

- Configuring EXEC authorization through AAA

1.3.2 AAA Authorization Configuration Task

General configuration process of AAA authorization

To configure AAA authorization, perform the following configuration processes：

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(2) Run aaa authorization to define the authorization method list. The authorization service is not provided by default.

(3) If necessary, apply the accounting method list to a specific interface or line.

1.3.2.1 Configuring EXEC authorization through AAA

To enable AAA authorization, run aaa authorization. The aaa authorization exec command can create one or several authorization method lists and enable the EXEC authorization to decide whether the EXEC hull program is run by the users or not, or decide whether the users are authorized with the priviledge when entering the EXEC hull program. After the authorization method lists are configured, you can apply these lists by running login authorization. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	Creates the global authorization list.
line [**console** | **vty**] *line-number* [*ending-line-number*]	Enter the configuration mode of a line.
login authorization {**default** | *list-name*}	Applies the authorization list to a line or set of lines. (In the line configuration mode)

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the authorization process. Only when the previously-used method returns the authorization error can other authorization methods be used. If the authorization fails because of the previous method, other authorization methods will not be used. If you requires the EXEC shell to be entered even when all authorization methods returns the authorization errors, designate none as the last authorization method in

the command line.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. For example, you can run the following command to designate RADIUS as the default authorization method of EXEC:

aaa authorization exec default group radius

Note:

If the authorization method list cannot be found during authorization, the authorization will be directly passed without the authorization service conducted.

The following table lists currently-supported EXEC authorization methods:

Keyword	Notes
group *WORD*	Uses the named server group to conduct authorization.
group radius	Uses RADIUS authorization.
group tacacs+	Uses tacacs+ authorization.
local	Uses the local database to perform authorization.
if-authenticated	Automatically authorizes the authencated user with all required functions.
none	Passes the authorization unconditionally.

1.3.3 AAA Authorization Examples

1.3.3.1 Example of Local EXECAuthorization

The following example shows how to perform the local authorization and local authorization by configuring the switch:

aaa authentication login default local aaa
authorization exec default local
!

localauthor a1

exec privilege default 15

!

local author-group a1

username exec1 password 0 abc

username exec2 password 0 abc author-group a1 username
exec3 password 0 abc maxlinks 10
username exec4 password 0 abc autocommand telnet 172.16.20.1

!

The following shows the meaning of each command line:

- The aaa authentication login default local command is used to define the default login-authentication method list, which will be automatically applied to all login authentication services.

- The command is used to define the default EXEC authorization method list, which will be automatically applied to all users requiring to enter the EXEC shell.
- Command localauthor al defines a local authority policy named al. Command exec privilege default 15 means the privileged level of exec login user is 15 by default.
- Command local author-group a1 means apply the local authorization policy a1 to global configuration (the default local policy group).
- Command username exec1 password 0 abc defines an account exec1 with password abc in the global configuration mode.
- Command username exec2 password 0 abc author-group a1 defines an account exec 2 with password abc in the global configuration mode. The account is applied to the local authorization policy a1.
- Command username exec3 password 0 abc maxlinks 10 defines an account exec 3 with password abc in the global configuration mode. The account makes 10 users available simultaneously.
- Command username exec4 password 0 abc autocommand telnet 172.16.20.1 defines an account exec4 with password abc. telnet 172.16.20.1 is automatically run when the user login the account.

1.4 AAA Accounting Configuration

1.4.1 AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA
- Configuring Network Accounting using AAA
- Configuring Accounting Update Through AAA
- Limiting User Accounting Without Username

1.4.2 AAA Accounting Configuration Task

General configuration process of AAA accounting

To configure AAA accounting, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(2) Apply the method lists to a particular interface or line, if required. The accounting service is not provided by default.

(3) If necessary, apply the accounting method list to a specific interface or line.

1.4.2.1 Configuring Connection Accounting using AAA

To enable AAA acounting, run command aaa accounting. To create a or multiple method list(s) to provide accounting information about all outbound connections made from the switch, use the aaa accounting connection command. The outbound connections include Telnet, PAD, H323 and rlogin. Only H323 is supported currently. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting connection {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	Establishes the global accounting list.

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the accounting process.

The following table lists currently-supported connection accounting methods:

Keyword	Notes
group *WORD*	Uses the named server group to conduct accounting.
group radius	Uses the RADIUS for accounting.
group tacacs+	Uses the TACACS+ for accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

1.4.2.2 Configuring Network Accounting usingAAA

To enable AAA acounting, run command aaa accounting. The aaa accounting network command can be used to establish one or multiple accounting method lists. The network accounting is enabled to provide information to all PPP/SLIP sessions, these information including packets, bytes and time accounting. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting network {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	Establishes the global accounting list.

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the accounting process.

The following table lists currently-supported network accounting methods:

Keyword	Notes
group *WORD*	Uses the named server group to conduct accounting.
group radius	Uses the RADIUS for accounting.
group tacacs+	Uses the TACACS+ for accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

1.4.2.3 Configuring Accounting Update Through AAA

To activate the AAA accounting update function forAAA to send the temporary accounting record to all users in the system, run the following command: You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting update [**newinfo**] [**periodic** *number*]	Enables AAA accounting update.

If the newinfo keyword is used, the temporary accounting record will be sent to the accounting server when there is new accounting information to be reported. For example, after IPCP negotiates with the IP address of the remote terminal, the temporary accounting record, including the IP address of the remote terminal, will be sent to the accounting server.

When the periodic keyword is used, the temporary accounting record will be sent periodically. The period is defined by the number parameter. The temporary accounting record includes all accounting information occurred before the accounting record is sent.

The two keywords are contradictable, that is, the previously-configured parameter will replace the latter-configured one. For example,if aaa accounting update periodic and then aaa accounting update newinfo are configured, all currently-registered users will generate temporary accounting records periodically. All new users have accounting records generated according to the newinfo algorithm.

1.4.2.4 Limiting User Accounting WithoutUsername

To prevent the AAA system from sending the accounting record to the users whose username character string is null, run the following command in global configuration mode:

- **aaa accounting suppress null-username**

1.5 Local Account Policy Configuration

1.5.1 Local Account Policy Configuration Task List

- Local authentication policy configuration
- Local authorization policy configuration
- Local password policy configuration
- Local policy group configuration

1.5.2 Local Account Policy Configuration Task

1.5.2.1 Local authentication policy configuration

To enter local authentication configuration, run command localauthen WORD in global configuration mode.

(1) The max login tries within a certain time

login max-tries *<1-9>* **try-duration** *1d2h3m4s*

The configured local authentication policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

1.5.2.2 Local authorization policy configuration

To enter local authorization configuration, run command localauthor *WORD* in global configuration mode.

(1) To authorize priority for login users.

exec privilege {**default | console | ssh | telnet**} *<1-15>*

The configured local authorization policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

1.5.2.3 Local password policy configuration

To enter local authorization configuration, run command localpass *WORD* in global configuration mode.

(1) The password cannot be the same with the user name

non-user

(2) The history password check (The new password cannot be the same with the history password. The history password record is 20.)

non-history

(3) Specify the components of the password (complicate the password)

element *[number] [lower-letter] [upper-letter] [special-character]*

(4) Specify the components of the password (complicate the password)

min-length *<1-127>*

(5) password validity period (the validity of the password)

validity 1d2h3m4s

The configured local authorization policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

1.5.2.4 Local policy group configuration

To configure local policy group, run localgroup *WORD* in global configuration mode:

(1) local authentication configuration: apply the configured local authentication policy to the policy group

local authen-group *WORD*

(2) local authorization configuration: apply the configured local authorization policy to the policy group

local author-group *WORD*

(3) local password configuration: apply the configured local password policy to the policy group

local pass-group *WORD*

(4) local account configuration: set the maxlinks and freeze for the policy group

local user {{maxlinks *<1-255>***} | { freeze** *WORD* **}}**

(5) account configuration: set the account for the policy group and establish the local database

username *username* [**password** *password* | {**encryption-type** *encrypted-password*}] [**maxlinks** *number*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*] [**autocommand** *command*]

The configured local policy group can be used in local authentication and authorization.
Local method is applicable to the default policy group and local group word is to a local policy group.

1.5.3 Local Account Policy Example

This section provides one sample configuration using local account policy. The following example shows how to configure the local authentication and local authorization.

aaa authentication login default local aaa
authorization exec default local
!

```
localpass a3 non-user
non-history
element number lower-letter upper-letter special-character min-length 10
validity 2d
!
localauthen a1
login max-tries 4 try-duration 2m
!
localauthor a2
exec privilege default 15
!
local pass-group a3 local authen-
group a1 local author-group a2
!
```

The meaning of each command line is shown below:

- The aaa authentication login default local command is used to define the default login-authentication method list, which will be automatically applied to all login authentication services.
- The command is used to define the default EXEC authorization method list, which will be automatically applied to all users requiring to enter the EXEC shell.
- The command localpass a3 defines the password policy named a3.
- The command localauthen a1 defines the authentication policy named a1.
- The command localauthor a2 defines the authorization policy named a2.
- The command local pass-group a3 applies the password policy named a3 to the default policy group.
- The command localauthen a1 applies the authentication policy named a1 to the default policy group.
- The command localauthor a2 applies the authorization policy named a2 to the default policy group.

Chapter 2 Configuring RADIUS

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology. The "RADIUS Configuration Task List" section describes how to configure RADIUS with the authentication, authorization, and accounting (AAA) command set. The last section in this chapter-RADIUS Configuration Examples- provides with two examples. Refer to RADIUS Configuration Commands for more details of RADIUS command.

2.1 Overview

2.1.1 RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server.

- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.

- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.

RADIUS is not suitable in the following network security situations:

- RADIUS does not support the following protocols: AppleTalk Remote Access (ARA)

  NetBIOS Frame Control Protocol (NBFCP)

- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD connections

- Switch-to-switch situations. RADIUS does not provide two-way authentication. On the switch only incoming call authentication is available when running RADIUS. The outbound call is impossible.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

2.1.2 RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

(1) The user is prompted for and enters a username and password.
(2) The username and encrypted password are sent over the network to the RADIUS server.
(3) The user receives one of the following responses from the RADIUS server: ACCEPT—The user is authenticated.

REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.

CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

Services that the user can access, including Telnet or rlogin.

Connection parameters, including the host or client IP address, access list, and user timeouts.

2.2 RADIUS Configuration Steps

To configure RADIUS on your switch or access server, you must perform the following tasks:

- Use the aaa authentication global configuration command to define method lists for RADIUS authentication. For more information about using the aaa authentication command, refer to the "Configuring Authentication" chapter.

- Use line and interface commands to enable the defined method lists to be used. For more information, refer to the "Configuring Authentication" chapter.

The following configuration tasks are optional:

- If necessary, run aaa authorization in global configuration mode to authorize the user’s service request. For more information about using the aaa authorization command, refer to the "Configuring Autorization" chapter.

- If necessary, run aaa accounting in global configuration mode to record the whole service procedure. For more information about running aaa accounting, see Record Configuration.

2.3 RADIUS Configuration Task List

- Configuring Switch to RADIUS Server Communication
- Configuring Switch to Use Vendor-Specific RADIUS Attributes
- Specifying RADIUS Authentication
- Specifying RADIUS Authorization
- Specifying RADIUS Accounting

2.4 RADIUS Configuration Task

2.4.1 Configuring Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider. A RADIUS server and a switch use a shared secret text string to encrypt passwords and exchange responses. To set RADIUS server, run command radius-server host; to set the shared key, run command radius-server key. Use the following command in global configuration mode:

Command	Purpose
radius-server host *ip-address* [**auth-port** *port-number*][**acct-port** *portnumber*]	Specifies the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers.
radius-server key *string*	Specifies the shared secret text string used between the switch and a RADIUS server.

To configure global communication settings between the switch and a RADIUS server, use the following radius-server commands in global configuration mode:

Command	Purpose
radius-server retransmit *retries*	Specifies how many times the switch transmits each RADIUS request to the server before giving up (the default is 2).
radius-server timeout *seconds*	Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
radius-server deadtime *minutes*	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

2.4.2 Configuring Switch to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. For more information about vendor-IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS). To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

Command	Purpose
radius-server vsa send [authentication]	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.

2.4.3 Specifying RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the aaa authentication command, specifying RADIUS as the authentication method. For more information about the two commands, see Authentication Configuration.

2.4.4 Specifying RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service. Because RADIUS authorization is facilitated through AAA, you must issue the aaa authorization command, specifying RADIUS as the authorization method. For more information, refer to the chapter "Configuring Authorization."

2.4.5 Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the aaa accounting command, specifying RADIUS as the accounting method. For more information about the two commands, see Authentication Configuration.

2.5 RADIUS Configuration Examples

2.5.1 RADIUS Authentication Example

The following example shows how to configure the switch switch to authenticate and authorize using RADIUS:

aaa authentication login use-radius group radius local

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

aaa authentication login use-radius radius local configures the switch to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, use-radius is the name of the method list, which specifies RADIUS and then local authentication.

2.5.2 RADIUS Application in AAA

The following example shows a general configuration using RADIUS with the AAA command set:

```
radius-server host 1.2.3.4
radius-server key myRaDiUSpassWoRd username root
password AlongPassword
aaa authentication login admins group radius local line vty 1 16
login authentication admins
```

The meaning of each command line is shown below:

radius-server host is used to define the IP address of the RADIUS server.

radius-server key is used to define the shared key between network access server and RADIUS server.

aaa authentication login admins group radius local command defines the authentication method list "admins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.

login authentication admins is used to designate to apply the admins method list during login.

Chapter 3 TACACS+ Configuration

3.1 TACACS+ Overview

As an access security control protocol, TACACS+ provides the centralized verification of acquiring the network access server's access right for users. . The communication's safety is guaranteed because the information exchange between network access server and TACACS+ service program is encrypted

Before using TACACS+ configured on network access server, TACACS+'s server has to be accessed and configured. TACACS+ provides independent modularized authentication, authorization and accounting.

Authentication—supporting multiple authentication ways (ASCII, PAP, CHAP and etc), provides the ability of processing any conversation with users (for example, bringing forward probing questions like family address, service type, ID number and etc. after providing login username and password). Moreover, TACACS+ authentication service supports sending information to user's screen, like sending information to notify user that their password has to be changed because of the company's password aging policy.

Authorization—detailed controlling of user's service limitation during service time, including setting up automatic commands, access control, dialog continuing time and etc. It can also limit the command enforcement which user might execute.

Accounting—collecting and sending the information of creating bills, auditing, or counting the usage status of network resources. Network manager can use accounting ability to track user's activities for security auditing or provide information for user's bills. The accounting function keeps track of user authentication, beginning and starting time, executed commands, packets' quantity and bytes' quantities, and etc.

3.1.1 The Operation of TACACS+ Protocol

3.1.1.1 Authentication in ASCII Form

When user logs in network access server which uses TACACS+, and asking for simple authentication in ASCII form, the following process might happen under typical circumstances:

When the connection is built up, network access server communicates with TACACS+ service program to acquire username prompt, and then gives it to user. User enters username, and network access server communicates with TACACS+ service program again to acquire password prompt. It shows password prompt to user. User enters password and then the password is sent to TACACS+ service program.

Note:

TACACS+ allows any dialogues between server's program and user until it collects enough information to identify user. Normally it is accomplished by the combination of prompting username and password, but it can also include other items, like ID number. All of these are under the control of TACACS+ server's program.

Network access server finally gets one of the following responses from TACACS+ server:

ACCEPT	User passes authentication, and service begins. If network access server is configured as requiring service authorization, authorization begins at this moment.
REJECT	User does not pass authentication. User might be rejected for further access or prompted to access again. It depends on the treatment of TACACS+ server.
ERROR	Error happens during authentication, and the cause might be at server. It also might happen at the network connection between server and network access server. If ERROR response is received, normally network access tries another way to identify user.
CONTINUE	It prompts user to enter additional authentication information.

3.1.1.2 Authentication in PAP and CHAP Ways

PAP login is similar with ASCII login, but the difference is that username and password of network access server is in PAP message not entered by user, thus it would not prompt user to enter relative information. CHAP login is similar in the main parts. After authentication, user need to enter authorization stage if network access server asks for the authorization for user. But before TACACS+ authorization is handled, TACACS+ authentication has to be finished.

If TACACS+ authorization needs to be processed, it needs to contact with TACACS+ server program again and go back to the authorization response of ACCEPT or REJECT. If back to ACCEPT, AV (attribute-value) for data, which is used for specifying the user's EXEC or NETWORK dialogue and confirming services which user can access, might be included.

3.2 TACACS+ Configuration Process

In order to configure as supporting TACACS+, the following tasks must be processed:

Using command tacacs-server to assign one or multiple IP addresses of TACACS+ server. Using command tacacs key to assign encrypted secret key for all the exchanged information between network access server and TACACS+ server. The same secret key has to be configured in TACACS+ server program.

Use the global configuration command aaa authentication to define the method table which uses TACACS+ for authentication. More information about command aaa authentication, please refer to "Authentication Configuration".

Use commands line and interface to apply the defined method table on interfaces or lines. More relative information, please refer to "Authentication Configuration".

3.3 TACACS+ Configuration Task List

- Assigning TACACS+ server
- Setting up TACACS+ encrypted secret key
- Assigning to use TACACS+ for authentication
- Assigning to use TACACS+ for authorization
- Assigning to use TACACS+ for accounting

3.4 TACACS+ Configuration Task

3.4.1 Assigning TACACS+ server

Command Tacacs-server could help to assign the IP address of TACACSC+ server. Because TACACS+ searching host in the configured order, this characteristic is useful for servers which configured with different priorities. In order to assign TACACS+ host, use the following commands under global configuration mode:

Command	Purpose
tacacs-server host *ip-address* [**single-connection**| **multi-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	To assign the IP address of TACACS+ server and relative features.

Use command tacacs-server to configure the following as well:

- Use single-connection key word to assign the adoption of single connection. This would allow server program to deal with more TACACS+ operations and be more efficient. multi-connection means the adoption of multiple TCP connection.

- Use parameter port to assign TCP interface number which is used by TACACS+ server program. The default interface number is 49.

- Use parameter timeout to assign the time's upper limit (taken second as the unit) for OLT's waiting response from server.

- Use parameter key to assign the encrypted and decrypted secret keys for messages.

Note:

Connect host after using tacacs-server, and connect the timeout value defined by command timeout to cover the global timeout value configured by command tacacs-server timeout. Use the encrypted secret key assigned by tacacs-server to cover the default secret key configured by global configuration command tacacs-server key. Therefore, this command could be used to configure the unique TACACS+ connection to enhance the network security.

3.4.2 Setting up TACACS+ encrypted secret key

In order to set up the encrypted secret key of TACACS+ message, use the following command under the global configuration mode:

Command	Purpose
tacacs-server key *keystring*	To set up the encrypted secret key matched with the encrypted secret key used by TACACS+ server.

Note:

In order to encrypt successfully, the same secret key should also be configured for TACACS+ server program.

3.4.3 Assigning to use TACACS+ for authentication

After having marked the TACACS+ server and defined its related encrypted secret key, method table need to be defined for TACACS+ authentication. Because TACACS+ authentication is by AAA, command aaa authentication should be assigned as TACACS+'s authentication way. More information, please refer to "Authentication Configuration".

3.4.4 Assigning to use TACACS+ for authorization

AAA authorization could help to set up parameter to confine user's network access limitation. TACACS+ authorization could be applied to services like command, network connection, EXEC dialogue and etc. Because TACACS+ authorization is by AAA, command aaa authorization should be assigned as TACACS+'s authentication way. More information, please refer to "Authorization Configuration".

3.4.5 Assigning to use TACACS+ for accounting

AAA accounting is able to track user's current service and their consumed network resources' quantity. Because TACACS+ authorization is by AAA, command aaa accounting should be assigned as TACACS+'s accounting way. More information, please refer to "Accounting Configuration".

3.5 TACACS+ Configuration Example

This chapter includes the following TACACS+ configuration example.

3.5.1 TACACS+ authentication example

The following configuring login authentication is accomplished by TACACS+:

```
aaa authentication login test group tacacs+ local aaa
authorization exec test group tacacs+ tacacs -server host
1.2.3.4
tacacs-server key testkey
```

In this example:

Command aaa authentication defines the authentication method table test used on vty0. Key word tacacs+ means the authentication is processed by TACACS+, and if TACACS+ does not respond during authentication, key word local indicates to use the local database on the network access server to do authentication.

Command tacacs-server host marks TACACS+ server's IP address as 1.2.3.4. command tacacs-server key defines the shared encrypted secret key as testkey.

Command aaa authorization Ensure that you have permission to log in to the switch after successful authentication.

3.5.2 TACACS+ Authorization Examples

```
aaa authentication login default group tacacs+ local aaa
authorization exec default group tacacs+ tacacs-server host
10.1.2.3
tacacs-server key goaway
```

In this example:

Command aaa authentication defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command aaa authorization does network service authorization by TACACS+.

Command tacacs-server host marks TACACS+ server's IP as 10.1.2.3. Command tacacs-server key defines the shared encrypted secret key as goaway.

3.5.3 TACACS+ Accounting Example

The following configuration of login authentication's method table uses TACACS+ as one of the methods to configure the accounting by TACACS+:

```
aaa authentication login default group tacacs+ local
aaa accounting exec default start-stop group tacacs+ tacacs-server
host 10.1.2.3
tacacs-server key goaway
```

In this example:

Command aaa authentication defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command aaa accounting does accounting of network service by TACACS+. In this example, the relative information of starting and beginning time is accounted and sent to TACACS+ server.

Command tacacs-server host marks TACACS+ server's IP address as 10.1.2.3. command Command tacacs-server key defines the shared encrypted secret key as goaway.