

Security Configuration

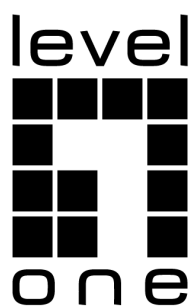


Table of Contents

Security Configuration	I
Table of Contents	II
Chapter 1 AAA Configuration	1
1. 1 AAA Overview	1
1. 1. 1 AAA Security Service	1
1. 1. 2 Benefits of Using AAA	2
1. 1. 3 AAA Principles	2
1. 1. 4 AAA Configuration Process	2
1. 2 Authentication Configuration	2
1. 2. 1 AAA Authentication Configuration Task List	2
1. 2. 2 AAA Authentication Configuration Task	3
1. 2. 3 AAA Authentication Configuration Example	4
Chapter 2 Configuring RADIUS	5
2. 1 Overview	5
2. 1. 1 RADIUS Overview	5
2. 1. 2 RADIUS Operation	6
2. 2 RADIUS Configuration Steps	6
2. 3 RADIUS Configuration Task List	6
2. 4 RADIUS Configuration Task	7
2. 4. 1 Configuring Switch to RADIUS Server Communication	7
2. 4. 2 Specifying RADIUS Authentication	7
2. 5 RADIUS Configuration Examples	7
2. 5. 1 RADIUS Authentication Example	7
2. 5. 2 RADIUS Application in AAA	7

Chapter 1 AAA Configuration

1.1 AAA Overview

Access control is used to control the users to access switch or NAS and to limit their service types. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your switch 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 anyone 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 server. The Radius 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
- 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 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 LEVELONE switch or access servers, perform the following steps:

- If you decide to use a security server, configure security protocol parameters first, such as RADIUS.
- Define the method lists for authentication by using an AAA authentication command.

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 local user name authentication database
- Creating the Privileged Level authentication database

1. 2. 2 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. Refer to the relevant section for the concrete configuration methods.
- (2) Configuring Authentication Method List Using aaa authentication

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.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. For example, to specify RADIUS as the default authentication method for user login, use the following command:

```
aaa authentication login default radius
```

The following table lists the supported login authentication methods:

Keyword	Notes:
group radius	Uses RADIUS for authentication.
local	Uses the local username database for authentication.

(1) Login Authentication Using Local Password

Use the `aaa authentication login` command with the `local` method keyword to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter 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.

(2) Login Authentication Using Group 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 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 Create a local username authentication database

Create users and passwords based on local authentication, mainly used to provide authentication methods for users when AAA servers (such as RADIUS) are not supported, and to provide registration under special circumstances: for example, access list authentication, no password authentication, automatic registration execution and the "no escape code" case.

To establish local username authentication, you can use the following command in global configuration mode to configure, and use the no form of the command to delete the username:

username *name* **password** [**encryption-type**] *encrypted-password*

no username *name*

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 default radius

The meaning of each command line is shown below:

- The aaa authentication login default radius command configures the switch to use RADIUS for authentication at the login prompt.

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

- Conditions of switch to other switching devices. 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.
- (3) The username and encrypted password are sent over the network to the RADIUS server.
- (4) 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:

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

2.3 RADIUS Configuration Task List

- Configuring switch to RADIUS Server Communication
- Configuring switch to Use Vendor-Specific RADIUS Attributes
- Specifying RADIUS Authentication

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. Use the **radius-server host** command to specify RADIUS server, Use the **radius-server key** command to specify a shared secret text (key) string.

To configure per-server RADIUS server communication, use the following command in global configuration mode:

command	purpose
radius-server host <i>ip-address</i> key <i>key</i> [auth-port <i>port-number</i>] [timeout <i>time</i>]	Specifies the IP address of the remote RADIUS server, specifies the shared key used between the switch and the RADIUS server, specifies the authentication destination port number, and the timeout period.

2.4.2 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, refer to the chapter "Configuring Authentication."

2.5 RADIUS Configuration Examples

2.5.1 RADIUS Authentication Example

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

```
aaa authentication login default radius
```

The meaning of each command line is shown below:

The switch uses RADIUS for authentication during login

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 key myRaDiUSpassWoRd
```

The meaning of each command line is shown below:

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

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