



Quidway S5300 Series Ethernet Switches
V100R002C02

Configuration Guide - Security

Issue	02
Date	2009-02-16
Part Number	

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://www.huawei.com>

Email: support@huawei.com

Copyright © Huawei Technologies Co., Ltd. 2009. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but the statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

About This Document.....	1
1 Security Protection on Interfaces.....	1-1
1.1 Overview of Security Protection on Interfaces.....	1-2
1.1.1 Introduction to Security Protection on Interfaces.....	1-2
1.1.2 Security Protection on Interfaces Supported by the S-switch.....	1-2
1.1.3 Logical Relationships Between Configuration Tasks.....	1-2
1.2 Configuring Security Protection on an Interface.....	1-2
1.2.1 Establishing the Configuration Task.....	1-3
1.2.2 Configuring the Limit on the Number of MAC Addresses Learnt by an Interface.....	1-3
1.2.3 Enabling Security Protection on an Interface.....	1-4
1.2.4 (Optional) Configuring the Security Protection Action for an Interface.....	1-4
1.2.5 (Optional) Configuring an Interface to Convert Secure Dynamic MAC Addresses into Static MAC Addresses.....	1-5
1.2.6 Checking the Configuration.....	1-5
1.3 Configuration Examples.....	1-6
1.3.1 Example for Configuring Security Protection on an Interface.....	1-6
2 MFF Configuration.....	2-1
2.1 Introduction to MFF.....	2-2
2.1.1 MFF Overview.....	2-2
2.1.2 MFF Functions Supported by the S-switch.....	2-3
2.1.3 Update History.....	2-4
2.2 Configuring MFF.....	2-4
2.2.1 Establishing the Configuration Task.....	2-4
2.2.2 Enabling MFF Globally.....	2-5
2.2.3 Configuring an MFF Network Interface.....	2-5
2.2.4 Enabling MFF in a VLAN.....	2-6
2.2.5 (Optional) Assigning an IP Address to the Static Gateway.....	2-6
2.2.6 (Optional) Enabling Timing Detection of the MAC Address of the Gateway.....	2-6
2.2.7 (Optional) Assigning an IP Address to the Server.....	2-7
2.2.8 Checking the Configuration.....	2-7
2.3 Configuration Examples.....	2-8
2.3.1 Example for Configuring MFF.....	2-8

3 Attack Defense Configuration.....	3-1
3.1 Overview of Attack Defense.....	3-2
3.1.1 Introduction to Attack Defense.....	3-2
3.1.2 Attack Defense Supported by the S-switch.....	3-2
3.1.3 Logical Relationships Between Configuration Tasks.....	3-2
3.2 Configuring the Defense Against IP Spoofing Attacks.....	3-2
3.2.1 Establishing the Configuration Task.....	3-3
3.2.2 Configuring the Defense Against IP Spoofing Attacks.....	3-3
3.2.3 Checking the Configuration.....	3-4
3.3 Configuring the Defense Against Land Attacks.....	3-4
3.3.1 Establishing the Configuration Task.....	3-5
3.3.2 Configuring the Defense Against Land Attacks.....	3-5
3.3.3 Checking the Configuration.....	3-6
3.4 Configuring the Defense Against Smurf Attacks.....	3-6
3.4.1 Establishing the Configuration Task.....	3-6
3.4.2 Configuring the Defense Against Smurf Attacks.....	3-7
3.4.3 Checking the Configuration.....	3-8
3.5 Configuring the Defense Against SYN Flood Attacks.....	3-8
3.5.1 Establishing the Configuration Task.....	3-8
3.5.2 Example for Configuring the Defense Against SYN Flood Attacks.....	3-9
3.5.3 Checking the Configuration.....	3-9
3.6 Configuring the Defense Against ICMP Flood Attacks.....	3-10
3.6.1 Establishing the Configuration Task.....	3-10
3.6.2 Configuring the Defense Against ICMP Flood Attacks.....	3-10
3.6.3 Checking the Configuration.....	3-11
3.7 Configuring the Defense Against Ping of Death Attacks.....	3-12
3.7.1 Establishing the Configuration Task.....	3-12
3.7.2 Configuring the Defense Against Ping of Death Attacks.....	3-12
3.7.3 Checking the Configuration.....	3-13
3.8 Configuring the Defense Against Teardrop Attacks.....	3-13
3.8.1 Establishing the Configuration Task.....	3-14
3.8.2 Configuring the Defense Against Teardrop Attacks.....	3-14
3.8.3 Checking the Configuration.....	3-15
3.9 Debugging Attack Defense.....	3-15
3.10 Configuration Examples.....	3-16
3.10.1 Example for Configuring the Defense Against Land Attacks.....	3-16
3.10.2 Example for Configuring the Defense Against SYN Flood Attacks.....	3-17
4 DHCP Snooping Configuration.....	4-1
4.1 Overview of DHCP snooping.....	4-2
4.1.1 Introduction to DHCP Snooping.....	4-2
4.1.2 DHCP Snooping Supported by the S-switch.....	4-2
4.1.3 Logical Relationships Between Configuration Tasks.....	4-4

4.2 Preventing the Bogus DHCP Server Attack.....	4-4
4.2.1 Establishing the Configuration Task.....	4-4
4.2.2 Enabling Global DHCP Snooping.....	4-5
4.2.3 Enabling Local DHCP Snooping.....	4-6
4.2.4 Configuring Trusted Interfaces.....	4-6
4.2.5 Checking the Configuration.....	4-6
4.3 Preventing the Middleman Attack and IP/MAC Spoofing Attack.....	4-7
4.3.1 Establishing the Configuration Task.....	4-7
4.3.2 Enabling Global DHCP Snooping.....	4-9
4.3.3 Enabling Local DHCP Snooping.....	4-9
4.3.4 Enabling Packet Check.....	4-9
4.3.5 Configuring the DHCP Snooping Binding Table.....	4-10
4.3.6 Configuring Option 82.....	4-11
4.3.7 Configuring Security Protection on an Interface.....	4-12
4.3.8 Checking the Configuration.....	4-12
4.4 Preventing the DoS Attack by Changing the CHADDR Field.....	4-13
4.4.1 Establishing the Configuration Task.....	4-13
4.4.2 Enabling Global DHCP Snooping.....	4-15
4.4.3 Enabling Local DHCP Snooping.....	4-15
4.4.4 Checking the CHADDR Field in DHCP Request Messages.....	4-15
4.4.5 Checking the Configuration.....	4-16
4.5 Preventing the Attacker from Sending Bogus Messages for Extending IP Address Leases.....	4-16
4.5.1 Establishing the Configuration Task.....	4-17
4.5.2 Enabling Global DHCP Snooping.....	4-18
4.5.3 Enabling Local DHCP Snooping.....	4-18
4.5.4 Enabling the Checking of DHCP Request Messages.....	4-19
4.5.5 Configuring Option 82.....	4-19
4.5.6 Checking the Configuration.....	4-20
4.6 Configuring the DHCP Option 82 String.....	4-21
4.6.1 Configuring the Storage Format of the Option 82 Field.....	4-21
4.6.2 Configuring the Circuit ID in the Option 82 Field in the System View.....	4-21
4.6.3 Configuring the Remote ID in the Option 82 Field in the System View.....	4-22
4.6.4 Configuring the Remote ID of the Option 82 Field in the Interface View.....	4-22
4.6.5 Checking the Configuration.....	4-22
4.7 Configuring the Packet Discarding Alarm.....	4-23
4.7.1 Establishing the Configuration Task.....	4-23
4.7.2 Configuring the Packet Discarding Alarm.....	4-24
4.7.3 Checking the Configuration.....	4-25
4.8 Maintaining DHCP Snooping.....	4-25
4.8.1 Backing Up the DHCP Snooping Binding Table.....	4-26
4.8.2 Debugging DHCP Snooping.....	4-26
4.9 Configuration Examples.....	4-26

4.9.1 Example for Configuring DHCP Snooping to Prevent Attacks Against the Network.....	4-26
5 AAA Configuration.....	5-1
5.1 Overview of AAA.....	5-2
5.1.1 Introduction to AAA.....	5-2
5.1.2 RADIUS.....	5-3
5.1.3 HWTACACS.....	5-5
5.1.4 Domain-based User Management.....	5-6
5.1.5 Local User Management.....	5-6
5.1.6 References.....	5-6
5.1.7 Logical Relationships Between Configuration Tasks.....	5-7
5.2 Configuring AAA.....	5-7
5.2.1 Establishing the Configuration Task.....	5-7
5.2.2 Configuring the Authentication Scheme.....	5-8
5.2.3 (Optional) Configuring the Authorization Scheme.....	5-9
5.2.4 Configuring the Accounting Scheme.....	5-9
5.2.5 (Optional) Configuring the Recording Scheme.....	5-10
5.2.6 Checking the Configuration.....	5-11
5.3 Configuring the RADIUS Server.....	5-11
5.3.1 Establishing the Configuration Task.....	5-12
5.3.2 Creating a RADIUS Server Template.....	5-13
5.3.3 Configuring the RADIUS Authentication Server.....	5-13
5.3.4 Configuring the RADIUS Accounting Server.....	5-13
5.3.5 (Optional) Configuring the Protocol Version for the RADIUS Server.....	5-14
5.3.6 (Optional) Configuring the Shared Key for the RADIUS Server.....	5-15
5.3.7 (Optional) Configuring the User Name Format for the RADIUS Server.....	5-15
5.3.8 (Optional) Setting the Traffic Unit for the RADIUS Server.....	5-15
5.3.9 (Optional) Configuring the Retransmission Parameters for the RADIUS Server.....	5-16
5.3.10 (Optional) Configuring the NAS Interface for the RADIUS Server.....	5-17
5.3.11 Checking the Configuration.....	5-17
5.4 Configuring the HWTACACS Server.....	5-17
5.4.1 Establishing the Configuration Task.....	5-18
5.4.2 Creating a HWTACACS Server Template.....	5-19
5.4.3 Configuring the HWTACACS Authentication Server.....	5-19
5.4.4 Configuring the HWTACACS Authorization Server.....	5-20
5.4.5 Configuring the HWTACACS Accounting Server.....	5-20
5.4.6 (Optional) Configuring the Source IP Address of the HWTACACS Server.....	5-21
5.4.7 (Optional) Configuring the Shared Key for the HWTACACS Server.....	5-21
5.4.8 (Optional) Configuring the User Name Format for the HWTACACS Server.....	5-22
5.4.9 (Optional) Setting the Traffic Unit for the HWTACACS Server.....	5-22
5.4.10 (Optional) Setting the Timer of the HWTACACS Server.....	5-23
5.4.11 Checking the Configuration.....	5-23
5.5 Configuring a Domain.....	5-23

5.5.1 Establishing the Configuration Task.....	5-24
5.5.2 Creating a Domain.....	5-24
5.5.3 Configuring Authentication, Authorization, and Accounting Schemes for the Domain.....	5-25
5.5.4 (Optional) Configuring the RADIUS Server Template for the Domain.....	5-25
5.5.5 (Optional) Configuring the HWTACACS Server Template for the Domain.....	5-26
5.5.6 (Optional) Configuring the Status of the Domain.....	5-27
5.5.7 (Optional) Setting the Maximum Number of Access Users for the Domain.....	5-27
5.5.8 Checking the Configuration.....	5-28
5.6 Configuring Local User Management.....	5-28
5.6.1 Establishing the Configuration Task.....	5-28
5.6.2 Creating Local User Accounts.....	5-29
5.6.3 (Optional) Configuring the Service Type for Local Users.....	5-29
5.6.4 (Optional) Configuring the Authority of Accessing the FTP Directory for Local Users.....	5-30
5.6.5 (Optional) Configuring the Status of Local Users.....	5-30
5.6.6 (Optional) Setting the Priority of Local Users.....	5-31
5.6.7 (Optional) Setting the Access Limit for Local Users.....	5-31
5.6.8 Checking the Configuration.....	5-31
5.7 Maintaining AAA.....	5-32
5.7.1 Clearing HWTACACS Statistics.....	5-32
5.7.2 Debugging AAA.....	5-32
5.8 Configuration Examples.....	5-33
6 MAC Address Authentication.....	6-1
6.1 Overview of MAC Address Authentication.....	6-2
6.1.1 Introduction to MAC Address Authentication.....	6-2
6.1.2 MAC Address Authentication Features Supported by the S-switch.....	6-3
6.1.3 Update History.....	6-3
6.2 Configuring MAC Address Authentication.....	6-3
6.2.1 Establishing the Configuration Task.....	6-4
6.2.2 Configuring MAC Address Authentication on Global MAC Address Authentication.....	6-4
6.2.3 Configuring MAC Address Authentication on an Interface.....	6-5
6.2.4 Configuring a MAC Address as a Username for MAC Address Authentication.....	6-5
6.2.5 Configuring a Fixed Username for a MAC Address Authentication User.....	6-5
6.2.6 (Optional)Configuring a Domain Name for a MAC Address Authentication User.....	6-6
6.2.7 (Optional)Configuring Timers for MAC Address Authentication.....	6-6
6.2.8 Checking the Configuration.....	6-7
6.3 Configuring Enhanced MAC Address Authentication.....	6-7
6.3.1 Establishing the Configuration Task.....	6-7
6.3.2 Configuring a Guest VLAN.....	6-8
6.3.3 Configuring the Maximum Number of MAC Address Authentication Users on an Interface.....	6-9
6.3.4 Checking the Configuration.....	6-9
6.4 Maintaining MAC Address Authentication.....	6-10
6.4.1 Resetting Statistics of MAC Address Authentication.....	6-10

6.5 Configuration Examples.....	6-10
6.5.1 Example for Configuring MAC Address Authentication.....	6-10
7 802.1X Configuration.....	7-1
7.1 Overview of 802.1X.....	7-2
7.1.1 Introduction to 802.1X.....	7-2
7.1.2 802.1X Authentication System.....	7-2
7.1.3 802.1X Authentication Process.....	7-3
7.1.4 Implementation of 802.1X on the S-switch.....	7-6
7.1.5 Logical Relationships Between Configuration Tasks.....	7-7
7.1.6 Update History.....	7-7
7.2 Configuring 802.1X.....	7-7
7.2.1 Establishing the Configuration Task.....	7-7
7.2.2 Enabling 802.1X Globally and on the Interface.....	7-8
7.2.3 (Optional) Setting the Port Access Control Mode.....	7-8
7.2.4 (Optional) Setting the Port Access Control Method.....	7-9
7.2.5 (Optional) Setting the Maximum Number of Concurrent Access Users.....	7-9
7.2.6 (Optional) Enabling DHCP Trigger.....	7-9
7.2.7 (Optional) Setting the Authentication Method for the 802.1X User.....	7-10
7.2.8 (Optional) Configuring the Guest VLAN.....	7-10
7.2.9 (Optional) Setting the Maximum Number of Times for Sending an Authentication Request.....	7-11
7.2.10 (Optional) Setting the Timer Parameters.....	7-11
7.2.11 (Optional) Enabling the Quiet-Period Timer.....	7-11
7.2.12 (Optional) Enabling the Handshake-Period Timer.....	7-12
7.2.13 Checking the Configuration.....	7-12
7.3 Configuration Examples.....	7-13
7.3.1 Example for Configuring 802.1X.....	7-13

Figures

Figure 1-1 Networking diagram of configuring security protection on an interface.....	1-6
Figure 2-1 Networking diagram of configuring dynamic MFF.....	2-8
Figure 3-1 Networking for configuring the defense against Land attacks.....	3-16
Figure 3-2 Networking for configuring the defense against SYN flood attacks.....	3-18
Figure 4-1 Networking for the DHCP snooping application on the S-switch.....	4-3
Figure 4-2 Diagram of preventing the bogus DHCP server attack.....	4-4
Figure 4-3 Diagram of preventing the middleman attack and IP/MAC spoofing attack.....	4-8
Figure 4-4 Networking diagram of preventing the DoS attack by changing the CHADDR field.....	4-14
Figure 4-5 Networking diagram of preventing the attacker from sending bogus messages for extending IP address leases.....	4-17
Figure 4-6 Networking for configuring DHCP snooping to prevent attacks against the network.....	4-27
Figure 5-1 Message exchange between the RADIUS client and the RADIUS server.....	5-4
Figure 5-2 Message structure defined by RADIUS.....	5-4
Figure 5-3 Networking diagram of AAA.....	5-33
Figure 6-1 Networking diagram for configuring local authentication with a fixed username.....	6-10
Figure 7-1 802.1X authentication system.....	7-3
Figure 7-2 802.1X authentication process in EAP-MD5 relay mode.....	7-4
Figure 7-3 802.1X authentication process in EAP termination mode.....	7-6
Figure 7-4 Authentication through 802.1X and RADIUS.....	7-13

Tables

Table 4-1 Attack types and DHCP snooping working modes.....4-3

Table 4-2 Relationship between the type of attacks and the type of discarded packets.....4-23

Table 5-1 Comparisons between HWTACACS and RADIUS.....5-5

About This Document

Purpose

This document describes procedures and provides examples for configuring the security features of the S-switch.

This document covers the following topics:

- Feature description
- Data preparation
- Pre-configuration tasks
- Configuration procedures
- Checking the configuration
- Configuration examples

This document guides you through the configuration and applicable environment of the security features of the S-switch.

Related Versions

The following table lists the product versions related to this document.

Product Name	Version
S5300	V100R002C02

Intended Audience

This document is intended for:

- Commissioning engineers
- Data configuration engineers
- Network monitoring engineers
- System maintenance engineers

Organization



This document is organized as follows.




Chapter	Description
1 Security Protection on Interfaces	This chapter describes the basics and configuration of security protection on interfaces.
2 MFF Configuration	This chapter describes the basics of MAC Forced Forwarding (MFF) and the procedures and examples for configuring MFF.
3 Attack Defense Configuration	This chapter describes how to implement and configure attack defense on the S-switch.
4 DHCP Snooping Configuration	This chapter describes the implementation and configuration procedures of DHCP snooping on the S-switch.
5 AAA Configuration	This chapter describes the basic concepts and configuration procedures of Authentication, Authorization, and Accounting (AAA), Remote Authentication Dial in User Service (RADIUS), Huawei Terminal Access Controller Access Control System (HWTACACS), domains, and local users.
6 MAC Address Authentication Configuration	This chapter describes the basic concepts of MAC address authentication and the procedure for configuring MAC address authentication, and provides examples for configuring MAC address authentication.
7 802.1X Configuration	This chapter describes the basics, methods, and configuration example of 802.1X.

Conventions

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injuries.

Symbol	Description
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 TIP	Indicates a tip that may help you address a problem or save your time.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

General Conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in boldface . For example, log in as user root .
<i>Italic</i>	Book titles are in italics.
Courier New	Terminal display is in Courier New. The messages input on terminals by users that are displayed are in boldface.

Command Conventions

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in boldface . For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

Keyboard Operations

Format	Description
Key	Press the key. For example, press Enter and press Tab .
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+Alt+A means the three keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, A means the two keys should be pressed in turn.

Mouse Operation

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Update History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Updates in Issue 02 (2009-02-16)

Second commercial release. The document is updated as follows:

- Fixing bug
- Rewriting copyright statement
- Updating manual version

Updates in Issue 01 (2008-12-26)

This is the first release.

1 Security Protection on Interfaces

About This Chapter

This chapter describes the basics and configuration of security protection on interfaces.

[1.1 Overview of Security Protection on Interfaces](#)

This section describes security protection on interfaces.

[1.2 Configuring Security Protection on an Interface](#)

This section describes how to configure security protection on an interface.

[1.3 Configuration Examples](#)

This section provides examples of security protection on interfaces.

1.1 Overview of Security Protection on Interfaces

This section describes security protection on interfaces.

[1.1.1 Introduction to Security Protection on Interfaces](#)

[1.1.2 Security Protection on Interfaces Supported by the S-switch](#)

[1.1.3 Logical Relationships Between Configuration Tasks](#)

1.1.1 Introduction to Security Protection on Interfaces

As a security mechanism to control network access, security protection on interfaces ensures the security of interfaces. It detects invalid packets and takes corresponding protection actions by checking whether the source MAC addresses of received data frames are valid.

1.1.2 Security Protection on Interfaces Supported by the S-switch

Ethernet interfaces on the S-switch support security protection on interfaces. After security protection is enabled on Ethernet interfaces, the S-switch considers the following types of MAC addresses as valid:

- Static MAC addresses that are manually configured
- Dynamic or static MAC addresses in a Dynamic Host Configuration Protocol (DHCP) snooping binding table
- Dynamic MAC addresses learnt before the number of MAC addresses reaches the upper limit

Source MAC addresses that do not fall into the preceding types are considered invalid. When an interface receives packets with invalid source MAC addresses, security protection takes effect on the interface. At present, the S-switch supports the following security protection actions on an interface:

- restrict: The interface neither learns the source MAC addresses of received packets with invalid source MAC addresses nor forwards the packets, but directly discards them and sends a trap message to the Network Management System (NMS).
- shutdown: The interface is automatically shut down when receiving packets with invalid source MAC addresses. You have to manually restore the interface if required.
- protect: The interface neither learns the source MAC addresses of received packets with invalid source MAC addresses nor forwards the packets, but directly discards them.

1.1.3 Logical Relationships Between Configuration Tasks

In the chapter, all configuration tasks are optional and not listed in sequence. You can configure them as required.

1.2 Configuring Security Protection on an Interface

This section describes how to configure security protection on an interface.

[1.2.3 Enabling Security Protection on an Interface](#) is the prerequisite for [1.2.4 \(Optional\) Configuring the Security Protection Action for an Interface](#) and [1.2.5 \(Optional\)](#)

Configuring an Interface to Convert Secure Dynamic MAC Addresses into Static MAC Addresses. That is, you can perform **1.2.4 (Optional) Configuring the Security Protection Action for an Interface** and **1.2.5 (Optional) Configuring an Interface to Convert Secure Dynamic MAC Addresses into Static MAC Addresses** only after performing **1.2.3 Enabling Security Protection on an Interface**.

[1.2.1 Establishing the Configuration Task](#)

[1.2.2 Configuring the Limit on the Number of MAC Addresses Learnt by an Interface](#)

[1.2.3 Enabling Security Protection on an Interface](#)

[1.2.4 \(Optional\) Configuring the Security Protection Action for an Interface](#)

[1.2.5 \(Optional\) Configuring an Interface to Convert Secure Dynamic MAC Addresses into Static MAC Addresses](#)

[1.2.6 Checking the Configuration](#)

1.2.1 Establishing the Configuration Task

Applicable Environment

After enabling security protection on an interface, the device can protect the interface by controlling packets with invalid source MAC addresses.

Pre-configuration Tasks

None.

Data Preparation

Before configuring security protection on an interface, you need the following data.

No.	Data
1	Number of the interface
2	Maximum number of MAC addresses that can be learnt and that of static MAC addresses on the interface

1.2.2 Configuring the Limit on the Number of MAC Addresses Learnt by an Interface

Context

Do as follows on devices on which the limit on the number of MAC addresses learnt by an interface should be configured.

Procedure

Step 1 Run:
`system-view`

The system view is displayed.

Step 2 Run:

```
mac-address restrict
```

MAC address learning restriction and forwarding restriction are enabled on interfaces of the device.

Step 3 Run:

```
mac-table limit interface-type interface-number limit-number
```

The limit on the number of MAC addresses that can be learnt is configured for an interface.

By default, the MAC address learning restriction and forwarding restriction on interfaces are disabled on the device. That is, there is no limit on the number of MAC addresses learnt and static MAC addresses on an interface.

----End

1.2.3 Enabling Security Protection on an Interface

Context

Do as follows on devices on which security protection on interfaces should be enabled.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
port-security enable
```

Security protection is enabled on the interface.

By default, security protection is disabled on interfaces of the device.

----End

1.2.4 (Optional) Configuring the Security Protection Action for an Interface

Context

Do as follows on devices on which the security protection actions on interfaces should be configured.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
port-security protect-action { protect | restrict | shutdown }
```

A security protection action is configured for the interface.

By default, the security protection action on an interface is restrict.

----End

1.2.5 (Optional) Configuring an Interface to Convert Secure Dynamic MAC Addresses into Static MAC Addresses

Context

Do as follows on devices on which security protection on interfaces should be configured.

By configuring an interface to convert secure dynamic MAC addresses into static MAC addresses, you can prevent secure dynamic MAC addresses from being lost after the device is rebooted.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
port-security dynamic-to-static mac-address { all | mac-address vlan vlan-id }
```

The interface is configured to convert secure dynamic MAC addresses into static MAC addresses.

----End

1.2.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the secure MAC address table.	display port-security mac-address <i>interface-type interface-number</i> [dynamic static]
Check the configurations on interfaces.	display current-configuration [configuration [<i>configuration-type</i>] controller interface <i>interface-type</i> [<i>interface-number</i>]] [{ begin exclude include } <i>regular-expression</i>]

1.3 Configuration Examples

This section provides examples of security protection on interfaces.

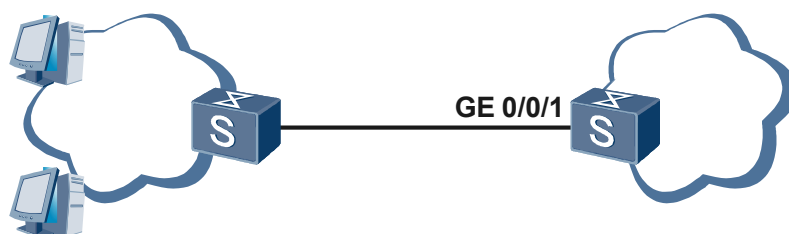
1.3.1 Example for Configuring Security Protection on an Interface

1.3.1 Example for Configuring Security Protection on an Interface

Networking Requirements

In the network shown in [Figure 1-1](#), you need to enable security protection on GigabitEthernet 0/0/1 of the S-switch to protect the interface. You are also required to configure the security protection action on the interface as shutdown and configure the interface to convert secure dynamic MAC addresses into static MAC addresses.

Figure 1-1 Networking diagram of configuring security protection on an interface



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the limit on the number of MAC addresses learnt by the interface.
2. Enable security protection on the interface.
3. Configure the security protection action for the interface.
4. Configure the interface to convert secure dynamic MAC addresses into static MAC addresses.

Data Preparation

To complete the configuration, you need the following data:

- Number of the interface
- Maximum number of MAC addresses learnt by the interface, which is set to 100

Configuration Procedure

1. Configure the limit on the number of MAC addresses learnt by the interface.

```
<Quidway> system-view
[Quidway] mac-address restrict
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] mac-table limit 100
```

2. Enable security protection on the interface.

```
[Quidway-GigabitEthernet0/0/1] port-security enable
```

3. Set the security protection action on the interface as shutdown.

```
[Quidway-GigabitEthernet0/0/1] port-security protect-action shutdown
```

4. Configure the interface to convert secure dynamic MAC addresses into static MAC addresses.

```
[Quidway-GigabitEthernet0/0/1] port-security dynamic-to-static mac-address all
```

5. Verify the configuration.

Run the **display current-configuration** command to check the configuration of security protection on the interface.

```
[S-switch-A-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 mac-table limit 100
 port-security enable
 port-security protect-action shutdown
#
return
```

Configuration Files

Configuration file of the S-switch

```
#
 sysname Quidway
#
mac-address restrict
#
interface GigabitEthernet0/0/1
mac-table limit 100
 port-security enable
 port-security protect-action shutdown
```


2 MFF Configuration

About This Chapter

This chapter describes the basics of MAC Forced Forwarding (MFF) and the procedures and examples for configuring MFF.

[2.1 Introduction to MFF](#)

This section describes the definition, principle, and specification of MFF.

[2.2 Configuring MFF](#)

In an access network, configuring MFF implements Layer 2 isolation between user hosts and enables the traffic between user hosts to be forwarded through ARs.

[2.3 Configuration Examples](#)

This section provides several configuration examples of MFF.

2.1 Introduction to MFF

This section describes the definition, principle, and specification of MFF.

2.1.1 MFF Overview

2.1.2 MFF Functions Supported by the S-switch

2.1.3 Update History

2.1.1 MFF Overview

In traditional Ethernet networking schemes, to implement Layer 2 isolation and Layer 3 interconnection between different clients, Virtual Local Area Networks (VLANs) are often used on the switch. If a large number of users need to be isolated at Layer 2, a large number of VLANs are occupied. To implement Layer 3 interconnection between clients, you need to plan different IP network segments for VLANs and assign IP addresses to VLANIF interfaces. Thus, dividing too many VLANs reduces the efficiency in allocating IP addresses.

MFF provides a solution to the preceding issues, implementing Layer 2 isolation and Layer 3 interconnection between clients in the same broadcast domain. MFF captures Address Resolution Protocol (ARP) request packets and sends ARP response packets with the MAC address of the gateway through proxy ARP. In this manner, all traffic including the traffic in the same subnet can be forcibly sent to the gateway so that the gateway can monitor data traffic. This prevents malicious attacks between user hosts and improves the security of network deployment.

MFF involves two types of interface roles: user interface and network interface.

1. User interface

The MFF user interface refers to the interface connected to the network terminal users.

The user interface processes different packets as follows:

- Permits protocol packets to pass through.
- Sends ARP packets and Dynamic Host Configuration Protocol (DHCP) packets to the CPU for processing.
- Permits only the unicast packets with the destination address as the MAC address of the gateway to pass through if the MAC address of the gateway is learnt, and discards other packets. Discards the unicast packets with the destination address as the MAC address of the gateway if the MAC address of the gateway is not learnt.
- Denies multicast and broadcast packets to pass through.

2. Network interface

The MFF network interface refers to the interface that is connected to another network device such as the access switch, the convergence switch, or the gateway.

The network interface processes different packets as follows:

- Permits multicast packets and DHCP packets to pass through.
- Sends ARP packets to the CPU for processing.
- Denies other broadcast packets to pass through.

 **NOTE**

The interfaces that connect upstream devices and the gateway, the interfaces that are connected to other downstream MFF devices in a cascading network where multiple MFF devices are connected, or the interfaces connecting devices in a ring network should be configured as network interfaces.

The network interface is just a type of interface roles, and is irrelevant to the position of the interface in the network.

In a VLAN where MFF is enabled, there are only network interfaces and user interfaces.

2.1.2 MFF Functions Supported by the S-switch

Static Gateway

The static gateway is applied in a scenario where the IP address is configured statically because the information about the gateway cannot be obtained through DHCP packets. When configuring the IP address statically, you need to maintain an IP address of the static gateway in a VLAN. If the IP address of the static gateway is not configured, user hosts except for valid user hosts dynamically allocated by DHCP cannot communicate normally.

Detection and Maintenance of the MAC Address of the Gateway

If timing detection of the gateway is configured, the gateway is detected periodically. The bogus ARP packets are used during detection. Their IP address and source MAC address are originated from the user list recorded by MFF. Generally, the IP address and MAC address of the first user recorded by MFF are selected. If the entry of this user is deleted, you need to re-select user information of bogus ARP packets. If no user host corresponds to the gateway after the user entry is deleted, information about detection of the gateway is cleared.

Proxy ARP

Proxy ARP ensures Layer 3 interconnection between user hosts. In addition, proxy ARP reduces the number of broadcast packets at the network side and at the user side.

MFF processes ARP packets as follows:

- Responds to ARP requests. Replaces the gateway to respond to ARP packets to the user host so that packets between users are forwarded at Layer 3 through the gateway. Here, ARP requests of user hosts include ARP requests on the gateway and ARP requests on IP information of other users.
- Replaces the gateway to respond to ARP requests. Replaces the user host to respond to ARP packets to the gateway. If the entry requested by the gateway exists on the MFF, the response is replied according to the entry. If the entry is not created, the request is forwarded. In this manner, broadcast packets are reduced.
- Forwards ARP responses sent by the user host and the gateway.
- Monitors ARP packets in the network, and updates the mapping table between IP addresses and MAC addresses of the gateway.

Deploying the Server in a Network

The IP address of the server can be the IP address of the DHCP server, the IP address of the server bearing other services, or the virtual IP address of the Virtual Router Redundancy Protocol (VRRP). If ARP requests with the source IP address as the IP address of the server are received at the network side, MFF responds to these ARP requests of the server as follows:

- MFF forwards the packets sent from the user host to the server through the gateway.
- MFF forwards the packets sent from the server to the user host without using the gateway.

2.1.3 Update History

Version	Revision
V200R002C01B010	This is the first release.

2.2 Configuring MFF

In an access network, configuring MFF implements Layer 2 isolation between user hosts and enables the traffic between user hosts to be forwarded through ARs.

[2.2.1 Establishing the Configuration Task](#)

[2.2.2 Enabling MFF Globally](#)

[2.2.3 Configuring an MFF Network Interface](#)

[2.2.4 Enabling MFF in a VLAN](#)

[2.2.5 \(Optional\) Assigning an IP Address to the Static Gateway](#)

[2.2.6 \(Optional\) Enabling Timing Detection of the MAC Address of the Gateway](#)

[2.2.7 \(Optional\) Assigning an IP Address to the Server](#)

[2.2.8 Checking the Configuration](#)

2.2.1 Establishing the Configuration Task

Applicable Environment

In the Metro Ethernet network at the access layer, you can configure MFF to implement the following functions:

- Isolate multiple access users at Layer 2.
- The traffic between user hosts is forwarded through ARs at Layer 3 so that user traffic can be filtered, scheduled, and charged.

Pre-configuration Tasks

Before configuring basic MFF functions, complete the following tasks:

If there are user hosts whose IP addresses are allocated dynamically, you need to:

- Enable DHCP snooping.
- Set the trusted interface of DHCP snooping.

Data Preparation

To configure basic MFF functions, you need the following data.

No.	Data
1	ID of the VLAN where MFF needs to be configured
2	Number of the network interface
3	IP address of the static gateway
4	IP address of the server

2.2.2 Enabling MFF Globally

Context

Do as follows on the AN.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mac-forced-forwarding enable
```

MFF is enabled globally.

----End

2.2.3 Configuring an MFF Network Interface

Context

Do as follows on the AN.

Procedure

Step 1 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 2 Run:

```
mac-forced-forwarding network-port
```

The interface is configured as the MFF network interface.

 **NOTE**

This configuration can be performed before MFF is enabled, but takes effect only after MFF is enabled.

----End

2.2.4 Enabling MFF in a VLAN

Context

Do as follows on the AN.

Procedure

Step 1 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

Step 2 Run:

```
mac-forced-forwarding enable
```

MFF is enabled in the VLAN.

 **NOTE**

If entries on the device are insufficient, MFF fails to be configured.

----End

2.2.5 (Optional) Assigning an IP Address to the Static Gateway

Context

Do as follows on the AN.

Procedure

Step 1 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

Step 2 Run:

```
mac-forced-forwarding static-gateway ip-address
```

An IP address is assigned to the static gateway.

----End

2.2.6 (Optional) Enabling Timing Detection of the MAC Address of the Gateway

Context

Do as follows on the AN.

Procedure

Step 1 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

Step 2 Run:

```
mac-forced-forwarding gateway-detect
```

Detection of the MAC address of the gateway is enabled in the VLAN.

----End

2.2.7 (Optional) Assigning an IP Address to the Server

Context

Do as follows on the AN.

Procedure

Step 1 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

Step 2 Run:

```
mac-forced-forwarding server ip-address <1-10>
```

An IP address is assigned to the server deployed in a network.

----End

2.2.8 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the MFF network interface.	display mac-forced-forwarding network-port
Check information about the MFF user and gateway in a VLAN.	display mac-forced-forwarding vlan <i>vlan-id</i>

Run the **display mac-forced-forwarding network-port** command, and you can view information about the network interface in a VLAN where MFF is enabled. For example:

```
[Quidway] display mac-forced-forwarding network-port
```

```
-----
VLAN ID          Network-ports
-----
VLAN 111         Ethernet0/0/4
```

Run the **display mac-forced-forwarding vlan *vlan-id*** command, and you can view information about the MFF user and gateway in a specified VLAN. For example:

```
[Quidway] display mac-forced-forwarding vlan 111
```

```
Servers
```

User IP	User MAC	Gateway IP	Gateway MAC
10.1.1.1	a-1-1-1	10.1.1.100	a-1-1-64

2.3 Configuration Examples

This section provides several configuration examples of MFF.

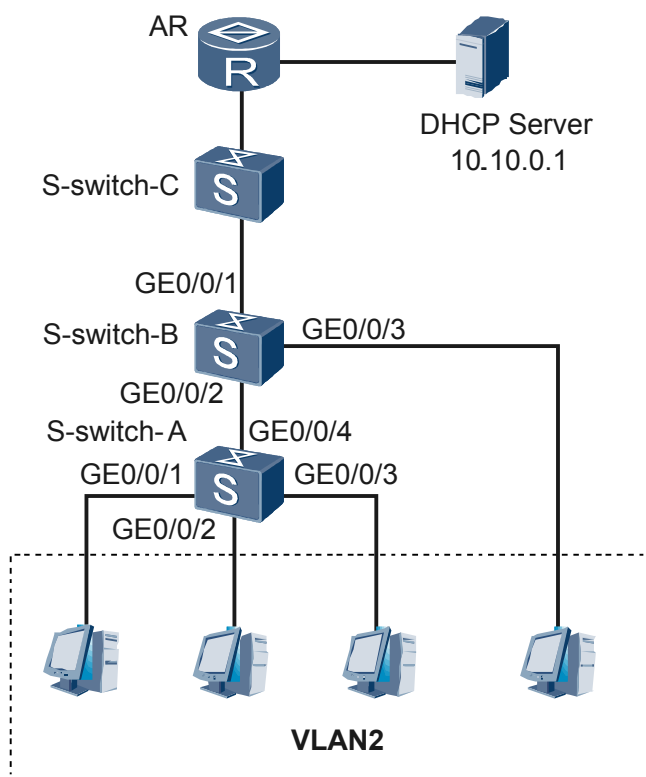
2.3.1 Example for Configuring MFF

2.3.1 Example for Configuring MFF

Networking Requirements

As shown in [Figure 2-1](#), all user hosts obtain IP addresses dynamically through the DHCP server. It is required that all user hosts should be interconnected through the AR.

Figure 2-1 Networking diagram of configuring dynamic MFF



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure DHCP snooping.
2. Enable MFF globally.
3. Configure MFF network interfaces.
4. Enable MFF in a VLAN.
5. (Optional) Configure timing detection of the gateway.
6. (Optional) Configure the server.

Data Preparation

To complete the configuration, you need the following data:

- ID of the VLAN where MFF needs to be configured
- Number of the network interface
- IP address of the static gateway
- (Optional) IP address of the server

Configuration Procedure

1. Configure DHCP snooping.
Configure DHCP snooping globally on S-switch-A.
`[S-switch-A] dhcp snooping enable`
Configure DHCP snooping in a VLAN on S-switch-A.
`[S-switch-A] vlan 2`
`[S-switch-A-Vlan2] dhcp snooping enable`
Configure GigabitEthernet 0/0/4 as the trusted interface on S-switch-A.
`[S-switch-A-vlan2] dhcp snooping trusted interface GigabitEthernet0/0/4`
`[S-switch-A-vlan2] quit`
Configure DHCP snooping globally on S-switch-B.
`[S-switch-B] dhcp snooping enable`
Configure DHCP snooping in a VLAN on S-switch-B.
`[S-switch-B] vlan 2`
`[S-switch-B-vlan2] dhcp snooping enable`
Configure Ethernet 0/0/1 as the trusted interface on S-switch-B.
`[S-switch-B-vlan2] dhcp snooping trusted interface GigabitEthernet0/0/1`
`[S-switch-B-vlan2] quit`
2. Enable MFF globally.
Enable MFF globally on S-switch-A.
`[S-switch-A] mac-forced-forwarding enable`
Enable MFF globally on S-switch-B.
`[S-switch-B] mac-forced-forwarding enable`
3. Configure MFF network interfaces.
Configure Ethernet 0/0/4 as the MFF network interface on S-switch-A.
`[S-switch-A] interface GigabitEthernet0/0/4`
`[S-switch-A-GigabitEthernet0/0/4] mac-forced-forwarding network-port`

```
[S-switch-A-GigabitEthernet0/0/4] quit
```

Configure GigabitEthernet 0/0/1 and GigabitEthernet0/0/2 as MFF network interfaces on S-switch-B.

```
[S-switch-B] interface GigabitEthernet0/0/1
[S-switch-B-GigabitEthernet0/0/1] mac-forced-forwarding network-port
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface GigabitEthernet0/0/2
[S-switch-B-GigabitEthernet0/0/2] mac-forced-forwarding network-port
[S-switch-B-GigabitEthernet0/0/2] quit
```

4. Enable MFF in a VLAN.

Enable MFF in VLAN 2 on S-switch-A.

```
[S-switch-A] vlan 2
[S-switch-A-vlan2] mac-forced-forwarding enable
```

Enable MFF in VLAN 2 on S-switch-B.

```
[S-switch-B] vlan 2
[S-switch-B-vlan2] mac-forced-forwarding enable
```

5. (Optional) Configure timing detection of the gateway.

Configure timing detection of the gateway on S-switch-A.

```
[S-switch-A-vlan2] mac-forced-forwarding gateway-detect
```

Configure timing detection of the gateway on S-switch-B.

```
[S-switch-B-vlan2] mac-forced-forwarding gateway-detect
```

6. (Optional) Configure the server.

Configure the server on S-switch-A.

```
[S-switch-A-vlan2] mac-forced-forwarding server 10.10.0.1
```

Configure the server on S-switch-B.

```
[S-switch-B-vlan2] mac-forced-forwarding server 10.10.0.1
```

Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
 vlan batch 2
#
 dhcp snooping enable
 mac-forced-forwarding enable
#
 vlan 2
 dhcp snooping enable
 dhcp snooping trusted interface GigabitEthernet0/0/4
 mac-forced-forwarding enable
 mac-forced-forwarding gateway-detect
 mac-forced-forwarding server 10.10.0.1
#
 interface GigabitEthernet0/0/1
 port default vlan 2
#
 interface GigabitEthernet0/0/2
 port default vlan 2
#
 interface GigabitEthernet0/0/3
 port default vlan 2
#
 interface GigabitEthernet0/0/4
 port trunk allow-pass vlan 2
 mac-forced-forwarding network-port
```

```
#
return
● Configuration file of S-switch-B
#
sysname S-switch-B
#
vlan batch 2
#
dhcp snooping enable
mac-forced-forwarding enable
#
vlan 2
dhcp snooping enable
  dhcp snooping trusted interface GigabitEthernet0/0/1
  mac-forced-forwarding enable
  mac-forced-forwarding gateway-detect
  mac-forced-forwarding server 10.10.0.1
#
interface GigabitEthernet0/0/1
  port trunk allow-pass vlan 2
  mac-forced-forwarding network-port
#
interface GigabitEthernet0/0/2
  port trunk allow-pass vlan 2
  mac-forced-forwarding network-port
#
interface GigabitEthernet0/0/3
  port default vlan 2
#
return
```


3 Attack Defense Configuration

About This Chapter

This chapter describes how to implement and configure attack defense on the S-switch.

[3.1 Overview of Attack Defense](#)

This section describes the concepts and types of attack defense.

[3.2 Configuring the Defense Against IP Spoofing Attacks](#)

This section describes how to configure the defense against IP spoofing attacks.

[3.3 Configuring the Defense Against Land Attacks](#)

This section describes how to configure the defense against Land attacks.

[3.4 Configuring the Defense Against Smurf Attacks](#)

This section describes how to configure the defense against Smurf attacks.

[3.5 Configuring the Defense Against SYN Flood Attacks](#)

This section describes how to configure the defense against SYN flood attacks.

[3.6 Configuring the Defense Against ICMP Flood Attacks](#)

This section describes how to configure the defense against ICMP flood attacks.

[3.7 Configuring the Defense Against Ping of Death Attacks](#)

This section describes how to configure the defense against Ping of Death attacks.

[3.8 Configuring the Defense Against Teardrop Attacks](#)

This section describes how to configure the defense against Teardrop attacks.

[3.9 Debugging Attack Defense](#)

This section describes how to debug attack defense.

[3.10 Configuration Examples](#)

This section provides several configuration examples of attack defense.

3.1 Overview of Attack Defense

This section describes the concepts and types of attack defense.

[3.1.1 Introduction to Attack Defense](#)

[3.1.2 Attack Defense Supported by the S-switch](#)

[3.1.3 Logical Relationships Between Configuration Tasks](#)

3.1.1 Introduction to Attack Defense

Network attacks are generally launched in the following ways: The network attack intrudes or destroys a network server (a host) to steal sensitive data or to interrupt the server's service. The network attacker directly destroys network devices, which results in abnormality of network services or even service interruption.

With the attack defense function, the S-switch can locate types of network attacks and protect the Intranet against malicious attacks to ensure normal running of the system.

3.1.2 Attack Defense Supported by the S-switch

The S-switch defends the system against the following attacks:

- Denial of Service (DoS) attack: The attacker consumes a large quantity of system resources by sending numerous unsolicited packets or forged connection packets to the S-switch. As a result, the S-switch reboots or crashes, interrupting normal services.
- Malformed packet attack: The attacker sends a defective IP packet to the S-switch, causing the system to crash during the processing of such an IP packet.

3.1.3 Logical Relationships Between Configuration Tasks

To protect the S-switch against attacks, you can configure the following attack defense functions. All configuration tasks are not listed in sequence. You can configure them as required.

- [3.2 Configuring the Defense Against IP Spoofing Attacks](#)
- [3.3 Configuring the Defense Against Land Attacks](#)
- [3.7 Configuring the Defense Against Ping of Death Attacks](#)
- [3.8 Configuring the Defense Against Teardrop Attacks](#)
- [3.6 Configuring the Defense Against ICMP Flood Attacks](#)

To protect an Intranet connected to the S-switch against attacks, you can configure the following attack defense functions. All configuration tasks are not listed in sequence. You can configure them as required.

- [3.4 Configuring the Defense Against Smurf Attacks](#)
- [3.5 Configuring the Defense Against SYN Flood Attacks](#)

3.2 Configuring the Defense Against IP Spoofing Attacks

This section describes how to configure the defense against IP spoofing attacks.

[3.2.1 Establishing the Configuration Task](#)

[3.2.2 Configuring the Defense Against IP Spoofing Attacks](#)

[3.2.3 Checking the Configuration](#)

3.2.1 Establishing the Configuration Task

Applicable Environment

In the IP spoofing attack, an attacker forges a packet carrying a valid source IP address to access a targeted system, or even control it. To defend the S-switch against IP spoofing attacks, you need to configure the defense against IP spoofing attacks on the S-switch.

Pre-configuration Tasks

Before configuring the defense against IP spoofing attacks, complete the following task:

- Create a VLAN and the corresponding VLANIF interface
- Adding the interface connecting the Extranet to a VLAN and assigning an IP address to the VLANIF interface

Data Preparation

To configure the defense against IP spoofing attacks, you need the following data.

No.	Data
1	ID of the VLAN that the interface joins

3.2.2 Configuring the Defense Against IP Spoofing Attacks

Context

Do as follows on the S-switch to be configured with the defense against IP spoofing attacks.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

A VLAN is created and the view of the VLAN is displayed.

Step 3 Run:

```
quit
```

The system view is returned to.

Step 4 Run:

```
firewall enable
```

The firewall is enabled.

Step 5 Run:

```
interface vlanif vlan-id
```

The VLANIF interface view is displayed.

Step 6 Run:

```
firewall defend enable
```

Attack defense is enabled.

Step 7 Run:

```
quit
```

The system view is returned to.

Step 8 Run:

```
firewall defend ip-spoofing enable
```

The defense against IP spoofing attacks is enabled.

By default, the defense against IP spoofing attacks is disabled.

After the S-switch is enabled with the defense against IP spoofing attacks, the attack information is recorded when the S-switch suffers IP spoofing attacks and a log is output. The log displays the records maintained by the system within the last 30 seconds. The records include the source IP addresses of the attack packets, the start time of the attacks, the end time of the attacks, and the total number of the attack packets. In addition, a maximum of 12 different IP addresses can be displayed. When the attack sources are more than 12, "..." is displayed.

----End

3.2.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of attack defense on the S-switch.	display firewall defend flag

Run the **display firewall defend flag** command on the S-switch. If **ip-spoofing** is displayed, it means that the defense against IP spoofing attacks is enabled.

```
<Quidway> display firewall defend flag
The attack defend flag is:
    ip-spoofing
```

3.3 Configuring the Defense Against Land Attacks

This section describes how to configure the defense against Land attacks.

3.3.1 Establishing the Configuration Task

[3.3.2 Configuring the Defense Against Land Attacks](#)

[3.3.3 Checking the Configuration](#)

3.3.1 Establishing the Configuration Task

Applicable Environment

To protect the S-switch against Land attacks, you need to configure the defense against Land attacks on the S-switch.

Pre-configuration Tasks

Before configuring the defense against Land attacks, complete the following task:

- Create a VLAN and the corresponding VLANIF interface.
- Adding the interface to a VLAN and assigning an IP address to the VLANIF interface

Data Preparation

To configure the defense against Land attacks, you need the following data.

No.	Data
1	ID of the VLAN to which the interface belongs

3.3.2 Configuring the Defense Against Land Attacks

Context

Do as follows on the S-switch to be configured with the defense against Land attacks.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

A VLAN is created and the view of the VLAN is displayed.

Step 3 Run:

```
quit
```

The system view is returned to.

Step 4 Run:

```
firewall enable
```

The firewall is enabled.

Step 5 Run:

```
interface vlanif vlan-id
```

The VLANIF interface view is displayed.

Step 6 Run:

```
firewall defend enable
```

Attack defense is enabled.

Step 7 Run:

```
quit
```

The system view is returned to.

Step 8 Run:

```
firewall defend land enable
```

The defense against Land attacks is enabled.

By default, the defense against Land attacks is disabled.

----End

3.3.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of attack defense on the S-switch.	display firewall defend flag

Run the **display firewall defend flag** command on the S-switch. If **land** is displayed, it means that the defense against Land attacks is enabled.

```
<Quidway> display firewall defend flag
The attack defend flag is:
land
```

3.4 Configuring the Defense Against Smurf Attacks

This section describes how to configure the defense against Smurf attacks.

[3.4.1 Establishing the Configuration Task](#)

[3.4.2 Configuring the Defense Against Smurf Attacks](#)

[3.4.3 Checking the Configuration](#)

3.4.1 Establishing the Configuration Task

Applicable Environment

To protect the S-switch against Smurf attacks, you need to configure the defense against Smurf attacks on the S-switch.

Pre-configuration Tasks

Before configuring the defense against Smurf attacks, complete the following task:

- Create a VLAN and the corresponding VLANIF interface
- Adding the interface to a VLAN and assigning an IP address to the VLANIF interface

Data Preparation

To configure the defense against Smurf attacks, you need the following data.

No.	Data
1	ID of the VLAN to which the interface belongs

3.4.2 Configuring the Defense Against Smurf Attacks

Context

Do as follows on the S-switch to be configured with the defense against Smurf attacks.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

A VLAN is created and the view of the VLAN is displayed.

Step 3 Run:

```
quit
```

The system view is returned to.

Step 4 Run:

```
firewall enable
```

The firewall is enabled.

Step 5 Run:

```
interface vlanif vlan-id
```

The VLANIF interface view is displayed.

Step 6 Run:

```
firewall defend enable
```

Attack defense is enabled.

Step 7 Run:

```
quit
```

The system view is returned to.

Step 8 Run:

```
firewall defend smurf enable
```

The defense against Smurf attacks is enabled.

By default, the defense against Smurf attacks is disabled.

----End

3.4.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of attack defense on a S-switch.	display firewall defend flag

Run the **display firewall defend flag** command on the S-switch. If **smurf** is displayed, it means that the defense against Smurf attacks is enabled.

```
<Quidway> display firewall defend flag
The attack defend flag is:
    smurf
```

3.5 Configuring the Defense Against SYN Flood Attacks

This section describes how to configure the defense against SYN flood attacks.

[3.5.1 Establishing the Configuration Task](#)

[3.5.2 Example for Configuring the Defense Against SYN Flood Attacks](#)

[3.5.3 Checking the Configuration](#)

3.5.1 Establishing the Configuration Task

Applicable Environment

To protect the S-switch against SYN flood attacks, you need to configure the defense against SYN flood attacks on the S-switch.

Pre-configuration Tasks

Before configuring the defense against SYN flood attacks, complete the following task:

- Create a VLAN and the corresponding VLANIF interface.
- Adding the interface to a VLAN and assigning an IP address to the VLANIF interface

Data Preparation

To configure the defense against SYN flood attacks, you need the following data.

No.	Data
1	ID of the VLAN to which the interface belongs
2	IP address of a device to be protected
3	(Optional) Maximum rate of SYN packets
4	(Optional) Maximum number of half-open connections

3.5.2 Example for Configuring the Defense Against SYN Flood Attacks

Context

Do as follows on the S-switch to be configured with the defense against SYN flood attacks.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan** *vlan-id* command to create a VLAN and enter the view of the VLAN.
- Step 3** Run the **quit** command to return to the system view.
- Step 4** Run the **firewall enable** command to enable the firewall.
- Step 5** Run the **firewall defend syn-flood enable** command to enable the defense against SYN flood attacks.

By default, the defense against SYN flood attacks is disabled.

- Step 6** Run the **interface** **vlanif** *vlan-id* command to enter the VLANIF interface view.
- Step 7** Run the **firewall defend enable** command to enable attack defense.
- Step 8** Run the **quit** command to return to the system view.
- Step 9** (Optional) Run the **firewall defend syn-flood ip** *ip-address* [**max-rate** *rate-number*] [**max-number** *max-number*] command to specify the IP address of a device to be protected from SYN flood attacks and specify relevant parameters.

By default, the maximum rate of SYN packets is 1000 packets per second; the maximum number of half-open connections is 1000.

----End

3.5.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of attack defense on a S-switch.	display firewall defend flag

Run the **display firewall defend flag** command on the S-switch. If **syn-flood** is displayed, it means that the defense against SYN flood attacks is enabled.

```
<Quidway> display firewall defend flag
The attack defend flag is:
    syn-flood
```

3.6 Configuring the Defense Against ICMP Flood Attacks

This section describes how to configure the defense against ICMP flood attacks.

3.6.1 Establishing the Configuration Task

3.6.2 Configuring the Defense Against ICMP Flood Attacks

3.6.3 Checking the Configuration

3.6.1 Establishing the Configuration Task

Applicable Environment

To protect the S-switch against ICMP flood attacks, you need to configure the defense against ICMP flood attacks on the S-switch.

Pre-configuration Tasks

Before configuring the defense against ICMP flood attacks, complete the following task:

- Create a VLAN and the corresponding VLANIF interface.
- Adding the interface to a VLAN and assigning an IP address to the VLANIF interface

Data Preparation

To configure the defense against ICMP flood attacks, you need the following data.

No.	Data
1	ID of the VLAN to which the interface belongs
2	IP address of a device to be protected
3	(Optional) Maximum rate of ICMP packets

3.6.2 Configuring the Defense Against ICMP Flood Attacks

Context

Do as follows on the S-switch to be configured with the defense against ICMP flood attacks.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

vlan *vlan-id*

A VLAN is created and the view of the VLAN is displayed.

Step 3 Run:

quit

The system view is returned to.

Step 4 Run:

firewall enable

The firewall is enabled.

Step 5 Run:

interface **vlanif** *vlan-id*

The VLANIF interface view is displayed.

Step 6 Run:

firewall defend enable

Attack defense is enabled.

Step 7 Run:

quit

The system view is returned to.

Step 8 Run:

firewall defend icmp-flood enable

The global defense against ICMP flood attacks is enabled.

By default, the defense against ICMP flood attacks is disabled.

Step 9 (Optional) Run:

firewall defend icmp-flood ip *ip-address* [**max-rate** *rate-number*]

The relevant parameters are specified for the device with a specified IP address to be protected from ICMP flood attacks.

By default, the maximum rate of ICMP packets is 1000 packets per second.

----End

3.6.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of attack defense on the S-switch.	display firewall defend flag

Run the **display firewall defend flag** command on the S-switch. If **icmp-flood** is displayed, it means that the defense against ICMP flood attacks is enabled.

```
<Quidway> display firewall defend flag
The attack defend flag is:
    icmp-flood
```

3.7 Configuring the Defense Against Ping of Death Attacks

This section describes how to configure the defense against Ping of Death attacks.

3.7.1 Establishing the Configuration Task

3.7.2 Configuring the Defense Against Ping of Death Attacks

3.7.3 Checking the Configuration

3.7.1 Establishing the Configuration Task

Applicable Environment

To protect the S-switch against attacks of oversized ICMP packets, you need to configure the defense against Ping of Death attacks on the S-switch.

Pre-configuration Tasks

Before configuring the defense against Ping of Death attacks, complete the following task:

- Create a VLAN and the corresponding VLANIF interface.
- Adding the interface to a VLAN and assigning an IP address to the VLANIF interface

Data Preparation

To configure the defense against Ping of Death attacks, you need the following data.

No.	Data
1	ID of the VLAN to which the interface belongs

3.7.2 Configuring the Defense Against Ping of Death Attacks

Context

Do as follows on the S-switch to be configured with the defense against Ping of Death attacks.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

A VLAN is created and the view of the VLAN is displayed.

Step 3 Run:

```
quit
```

The system view is returned to.

Step 4 Run:

```
firewall enable
```

The firewall is enabled.

Step 5 Run:

```
interface vlanif vlan-id
```

The VLANIF interface view is displayed.

Step 6 Run:

```
firewall defend enable
```

Attack defense is enabled.

Step 7 Run:

```
quit
```

The system view is returned to.

Step 8 Run:

```
firewall defend ping-of-death enable
```

The defense against Ping of Death attacks is enabled.

By default, the defense against Ping of Death attacks is disabled.

----End

3.7.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of attack defense on the S-switch.	display firewall defend flag

Run the **display firewall defend flag** command on the S-switch. If **ping-of-death** is displayed, it means that the defense against Ping of Death attacks is enabled.

```
<Quidway> display firewall defend flag
The attack defend flag is:
    ping-of-death
```

3.8 Configuring the Defense Against Teardrop Attacks

This section describes how to configure the defense against Teardrop attacks.

[3.8.1 Establishing the Configuration Task](#)[3.8.2 Configuring the Defense Against Teardrop Attacks](#)[3.8.3 Checking the Configuration](#)

3.8.1 Establishing the Configuration Task

Applicable Environment

To protect the S-switch against attacks of forged fragmented IP packets, you need to configure the defense against Teardrop attacks on the S-switch.

Pre-configuration Tasks

Before configuring the defense against Teardrop attacks, complete the following task:

- Create a VLAN and the corresponding VLANIF interface.
- Adding the interface to a VLAN and assigning an IP address to the VLANIF interface

Data Preparation

To configure the defense against Teardrop attacks, you need the following data.

No.	Data
1	ID of the VLAN to which the interface belongs

3.8.2 Configuring the Defense Against Teardrop Attacks

Context

Do as follows on the S-switch to be configured with the defense against Teardrop attacks.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

A VLAN is created and the view of the VLAN is displayed.

Step 3 Run:

```
quit
```

The system view is returned to.

Step 4 Run:

```
firewall enable
```

The firewall is enabled.

Step 5 Run:

```
interface vlanif vlan-id
```

The VLANIF interface view is displayed.

Step 6 Run:

```
firewall defend enable
```

Attack defense is enabled.

Step 7 Run:

```
quit
```

The system view is returned to.

Step 8 Run:

```
firewall defend teardrop enable
```

The defense against Teardrop attacks is enabled.

By default, the defense against Teardrop attacks is disabled.

----End

3.8.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of attack defense on a S-switch.	display firewall defend flag

Run the **display firewall defend flag** command on the S-switch. If **teardrop** is displayed, it means that the defense against Teardrop attacks is enabled.

```
<Quidway> display firewall defend flag
The attack defend flag is:
teardrop
```

3.9 Debugging Attack Defense

This section describes how to debug attack defense.



CAUTION

Enabling the debugging affects the system performance. So, after debugging, run the **undo debugging all** command to disable it at once.

When a fault occurs, run the following **debugging** command in the user view to locate the fault.

Action	Command
Enable the debugging of attack defense.	debugging firewall defend { all ip-spoofing land smurf syn-flood icmp-flood ping-of-death tear-drop }

3.10 Configuration Examples

This section provides several configuration examples of attack defense.

3.10.1 Example for Configuring the Defense Against Land Attacks

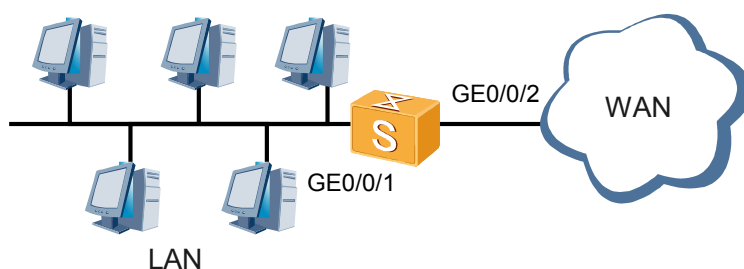
3.10.2 Example for Configuring the Defense Against SYN Flood Attacks

3.10.1 Example for Configuring the Defense Against Land Attacks

Networking Requirements

As shown in [Figure 3-1](#), on the S-switch, GE 0/0/1 is connected to an Intranet and GE 0/0/2 is connected to the Internet. It is required that GE 0/0/2 be enabled with the defense against Land attacks.

Figure 3-1 Networking for configuring the defense against Land attacks



Configuration Roadmap

The configuration roadmap is as follows:

1. Add GE 0/0/2 to a VLAN and assign an IP address to the VLANIF interface.
2. Enable the defense against Land attacks on the S-switch.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of the interfaces on the S-switch
- ID of the VLAN to which GE 0/0/2 is added and the IP address of the VLANIF interface

Configuration Procedure

1. Enable the global attack defense on the S-switch.

```
<Qidway> system-view
[Qidway] firewall enable
[Qidway] vlan 2
[Qidway -vlan2] port gigabitethernet 0/0/2
[Qidway -vlan2] quit
[Qidway] interface vlanif 2
[Qidway -Vlanif2] ip address 192.168.0.1 24
[Qidway -Vlanif2] firewall defend enable
[Qidway -Vlanif2] quit
```

2. Enable the defense against Land attacks on the S-switch.

```
[Qidway] firewall defend land enable
```

3. Verify the configuration.

Run the **display firewall defend flag** command on the S-switch, and you can view that the defense against Land attacks is enabled.

```
[Qidway] display firewall defend flag
The attack defend flag is:
land
```

Configuration Files

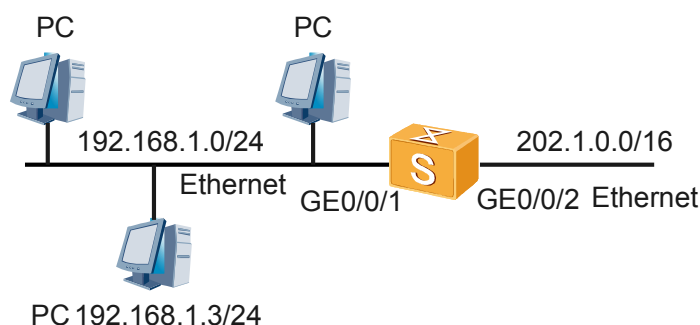
- The following lists the configuration file of the S-switch.

```
sysname Qidway
#
firewall enable
#
vlan batch 1 2
#
firewall defend land enable
#
interface Vlanif2
ip address 192.168.0.1 255.255.255.255
firewall defend enable
#
interface GigabitEthernet0/0/2
port default vlan 2
.....
#
return
```

3.10.2 Example for Configuring the Defense Against SYN Flood Attacks

Networking Requirements

As shown in [Figure 3-2](#), on the S-switch, GE 0/0/1 is connected to an Intranet and GE 0/0/2 is connected to the Internet. It is required that the defense against SYN flood attacks be enabled on the [Figure 3-2](#) to protect the device at 192.168.1.3.

Figure 3-2 Networking for configuring the defense against SYN flood attacks

Configuration Roadmap

The configuration roadmap is as follows:

1. Add GE 0/0/1 and GE 0/0/2 to VLANs respectively and assign an IP address to each VLANIF interface.
2. Configure the defense function on the VLANIF interfaces corresponding to GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 respectively
3. Configure the defense against SYN flood attacks on the S-switch to protect the device at 192.168.1.3.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of the interfaces on the S-switch
- IDs of the VLANs to which GE 0/0/1 and GE 0/0/2 are respectively added and the IP addresses of the VLANIF interfaces
- IP address of the device to be protected
- Maximum rate of SYN packets
- Maximum number of half-open connections

Configuration Procedure

1. Add GE 0/0/1 to VLAN 30 and assign an IP address to VLANIF 30.

```
<Quidway> system-view
[Quidway] firewall enable
[Quidway] vlan 30
[Quidway-vlan30] port gigabitethernet 0/0/1
[Quidway-vlan30] quit
[Quidway] interface vlanif 30
[Quidway-Vlanif30] ip address 192.168.1.0 24
[Quidway-Vlanif30] firewall defend enable
[Quidway-Vlanif30] quit
```

2. Add GE 0/0/2 to VLAN 40 and assign an IP address to VLANIF 40.

```
[Quidway] vlan 40
[Quidway-vlan40] port gigabitethernet 0/0/2
[Quidway-vlan40] quit
[Quidway] interface vlanif 40
[Quidway-Vlanif40] ip address 202.1.0.0 16
```

- ```
[Quidway-Vlanif40] firewall defend enable
[Quidway-Vlanif40] quit
```
3. Enable the global defense against SYN flood attacks.  

```
[Quidway] firewall defend syn-flood enable
```
  4. Configure the defense against SYN flood attacks. Set the maximum rate of SYN packets to 500 packets per second and the maximum number of half-open connections to 2000.  

```
[Quidway] firewall defend syn-flood ip 192.168.1.3 max-rate 500 max-number 2000
```
  5. Verify the configuration.  
Run the **display firewall defend flag** command on the S-switch, and you can view that the defense against SYN flood attacks is enabled.  

```
<Quidway> display firewall defend flag
The attack defend flag is:
syn-flood
```

## Configuration Files

- The following lists the configuration file of the S-switch.

```
sysname Quidway
#
firewall enable
#
vlan batch 1 30 40
#
firewall defend syn-flood enable
firewall defend syn-flood ip 192.168.1.3 max-rate 500 max-number 2000
#
interface Vlanif30
ip address 192.168.1.0 255.255.255.0
firewall defend enable
#
interface Vlanif40
ip address 202.1.0.0 255.255.0.0
firewall defend enable
#
interface GigabitEthernet0/0/1
port default vlan 30
#
interface GigabitEthernet0/0/2
port default vlan 40
.....
#
return
```



# 4 DHCP Snooping Configuration

---

## About This Chapter

This chapter describes the implementation and configuration procedures of DHCP snooping on the S-switch.

### [4.1 Overview of DHCP snooping](#)

This section describes the concept and types of DHCP snooping.

### [4.2 Preventing the Bogus DHCP Server Attack](#)

This section describes how to prevent the bogus DHCP server attack through the S-switch.

### [4.3 Preventing the Middleman Attack and IP/MAC Spoofing Attack](#)

### [4.4 Preventing the DoS Attack by Changing the CHADDR Field](#)

This section describes how to prevent the DoS attack by changing the CHADDR field.

### [4.5 Preventing the Attacker from Sending Bogus Messages for Extending IP Address Leases](#)

This section describes how to prevent the attacker from sending bogus messages for extending IP address leases.

### [4.6 Configuring the DHCP Option 82 String](#)

This section describes how to configure the DHCP Option 82 string.

### [4.7 Configuring the Packet Discarding Alarm](#)

This section describes how to configure the packet discarding alarm.

### [4.8 Maintaining DHCP Snooping](#)

This section describes how to maintain DHCP snooping.

### [4.9 Configuration Examples](#)

This section provides several examples for configuring DHCP snooping.

## 4.1 Overview of DHCP snooping

This section describes the concept and types of DHCP snooping.

### 4.1.1 Introduction to DHCP Snooping

#### 4.1.2 DHCP Snooping Supported by the S-switch

#### 4.1.3 Logical Relationships Between Configuration Tasks

### 4.1.1 Introduction to DHCP Snooping

Dynamic Host Configuration Protocol (DHCP) snooping intercepts and analyzes DHCP messages transmitted between the DHCP client and the DHCP server agent. In this manner, DHCP snooping creates and maintains a DHCP snooping binding table, and filters untrusted DHCP messages according to the table. The binding table contains the MAC address, IP address, lease, binding type, VLAN ID, and interface information. DHCP snooping acts as a firewall between DHCP clients and a DHCP server.

DHCP snooping prevents DHCP Denial of Service (DoS) attacks, bogus DHCP server attacks, and middleman and IP/MAC spoofing attacks when DHCP is enabled on the device.

The S-switch supports security features such as the MAC address limit, DHCP snooping binding table, binding of the IP address and MAC address, and Option 82. In this manner, security of the device enabled with DHCP is ensured.

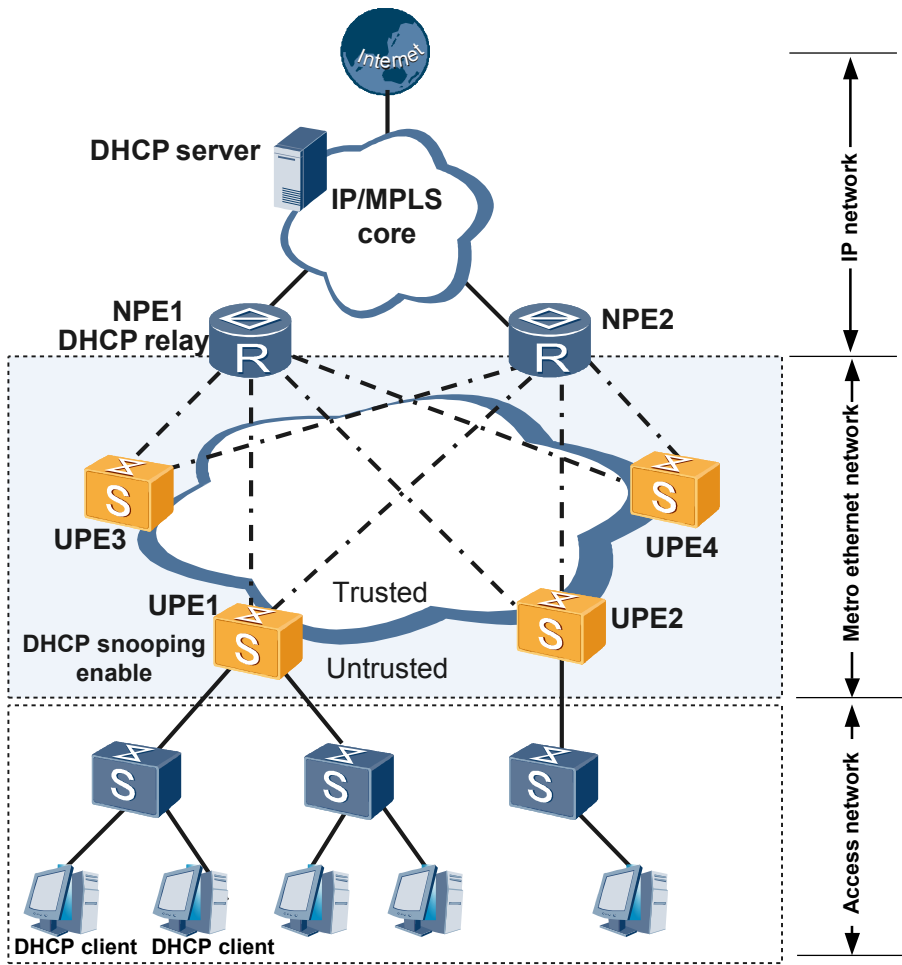
### 4.1.2 DHCP Snooping Supported by the S-switch

The S-switch supports the following DHCP snooping features:

- MAC address limit
- Configuring the trusted/untrusted interfaces
- Checking the CHADDR field in DHCP messages
- DHCP snooping binding table

**Figure 4-1** shows the DHCP snooping application on the S-switch where DHCP snooping is enabled.

Figure 4-1 Networking for the DHCP snooping application on the S-switch



As shown in [Figure 4-1](#), the S-switch enabled with DHCP snooping is deployed between the DHCP client and the DHCP relay agent. The S-switch forwards DHCP reply messages received from a trusted interface but discards DHCP reply messages received from an untrusted interface. The DHCP snooping binding table is then generated on the basis of the DHCP reply messages received from the trusted interface. IP packets and ARP packets received from the untrusted interface are forwarded only when there are matching entries in the binding table; otherwise, they are discarded.

When DHCP snooping is configured for a VLAN of the S-switch, the S-switch checks packets coming from the VLAN.

The working mode of DHCP snooping varies according to the type of attacks, as shown in [Table 4-1](#).

Table 4-1 Attack types and DHCP snooping working modes

| Type of Attacks        | DHCP Snooping Working Mode |
|------------------------|----------------------------|
| DHCP exhaustion attack | MAC Address limit          |

| Type of Attacks                                              | DHCP Snooping Working Mode                                                                              |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Bogus DHCP server attack                                     | Configuring an interface as trusted or untrusted                                                        |
| Middleman attack and IP/MAC spoofing attack                  | Checking whether the IP packets or ARP packets have matching entries in the DHCP snooping binding table |
| DoS attack by changing the value of the CHADDR field         | Checking the CHADDR field in DHCP messages                                                              |
| Attack of sending bogus messages to extend IP address leases | Checking whether the DHCP request messages have matching entries in the DHCP snooping binding table     |

### 4.1.3 Logical Relationships Between Configuration Tasks

All configuration tasks in this chapter are not listed in sequence. You can configure them as required.

## 4.2 Preventing the Bogus DHCP Server Attack

This section describes how to prevent the bogus DHCP server attack through the S-switch.

[4.2.1 Establishing the Configuration Task](#)

[4.2.2 Enabling Global DHCP Snooping](#)

[4.2.3 Enabling Local DHCP Snooping](#)

[4.2.4 Configuring Trusted Interfaces](#)

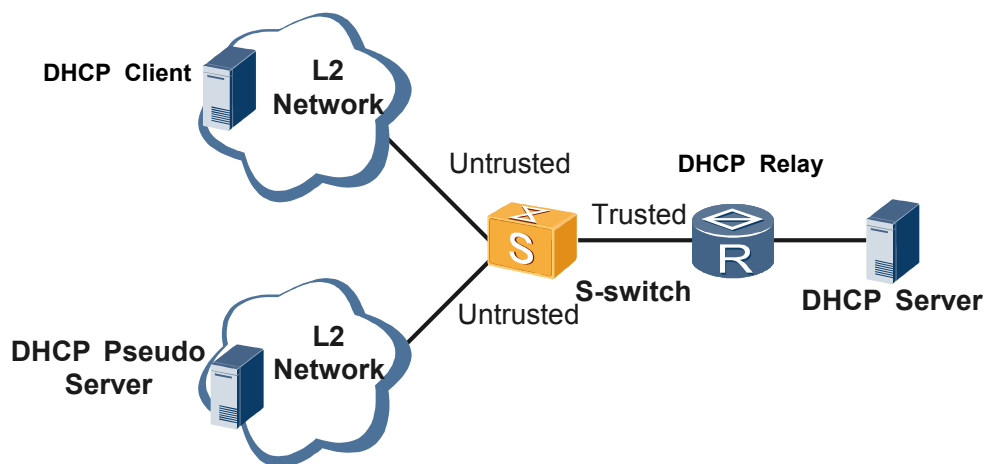
[4.2.5 Checking the Configuration](#)

### 4.2.1 Establishing the Configuration Task

#### Applicable Environment

As shown in [Figure 4-2](#), a bogus DHCP server on the user network replies incorrect messages such as the incorrect IP address of the gateway, incorrect DNS server, and incorrect IP address to the DHCP client, so that the DHCP client cannot access the network.

**Figure 4-2** Diagram of preventing the bogus DHCP server attack



To prevent the bogus DHCP server attack, you can configure DHCP snooping on the S-switch, and set the interface at the user side to be untrusted and the interface at the network side to be trusted. In this manner, DHCP reply messages received from the untrusted interface are discarded. Only DHCP reply messages received from the trusted interface are forwarded.

## Pre-configuration Tasks

Before preventing the bogus DHCP server attack through the S-switch, complete the following tasks:

- Configuring the DHCP server
- Configuring the DHCP relay agent



### NOTE

The DHCP server and the DHCP relay agent are configured on the upstream router or server of the S-switch.

## Data Preparation

To prevent the bogus DHCP server attack through the S-switch, you need the following data.

| No. | Data                                              |
|-----|---------------------------------------------------|
| 1   | Name of the interface to be added to a VLAN       |
| 2   | ID of the VLAN to which the interfaces belong     |
| 3   | Name of the interface to be configured as trusted |

## 4.2.2 Enabling Global DHCP Snooping

### Context

Do as follows on the S-switch.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
dhcp snooping enable
```

Global DHCP snooping is enabled.

By default, DHCP snooping is disabled.

----End

## 4.2.3 Enabling Local DHCP Snooping

### Context

Do as follows on the S-switch.

### Procedure

- Step 1** Run:
- ```
system-view
```
- The system view is displayed.
- Step 2** Run:
- ```
vlan vlan-id
```
- The VLAN view is displayed.
- Step 3** Run:
- ```
dhcp snooping enable
```
- DHCP snooping is enabled in the VLAN.
- By default, DHCP snooping is disabled.
- End

4.2.4 Configuring Trusted Interfaces

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
- ```
system-view
```
- The system view is displayed.
- Step 2** Run:
- ```
vlan vlan-id
```
- The VLAN view is displayed.
- The VLAN should be the one to which the interface connected to the DHCP server belongs.
- Step 3** Run:
- ```
dhcp snooping trusted interface interface-type interface-number
```
- A specified interface is configured in the VLAN as trusted.
- End

## 4.2.5 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                        | Command                             |
|-----------------------------------------------|-------------------------------------|
| Check information about global DHCP snooping. | <b>display dhcp snooping global</b> |

Run the **display dhcp snooping global** command. You can view that global DHCP snooping is enabled.

```
<Quidway> display dhcp snooping global
dhcp snooping enable
```

## 4.3 Preventing the Middleman Attack and IP/MAC Spoofing Attack

### [4.3.1 Establishing the Configuration Task](#)

### [4.3.2 Enabling Global DHCP Snooping](#)

### [4.3.3 Enabling Local DHCP Snooping](#)

### [4.3.4 Enabling Packet Check](#)

### [4.3.5 Configuring the DHCP Snooping Binding Table](#)

### [4.3.6 Configuring Option 82](#)

### [4.3.7 Configuring Security Protection on an Interface](#)

This section describes how to configure security protection on an interface.

### [4.3.8 Checking the Configuration](#)

## 4.3.1 Establishing the Configuration Task

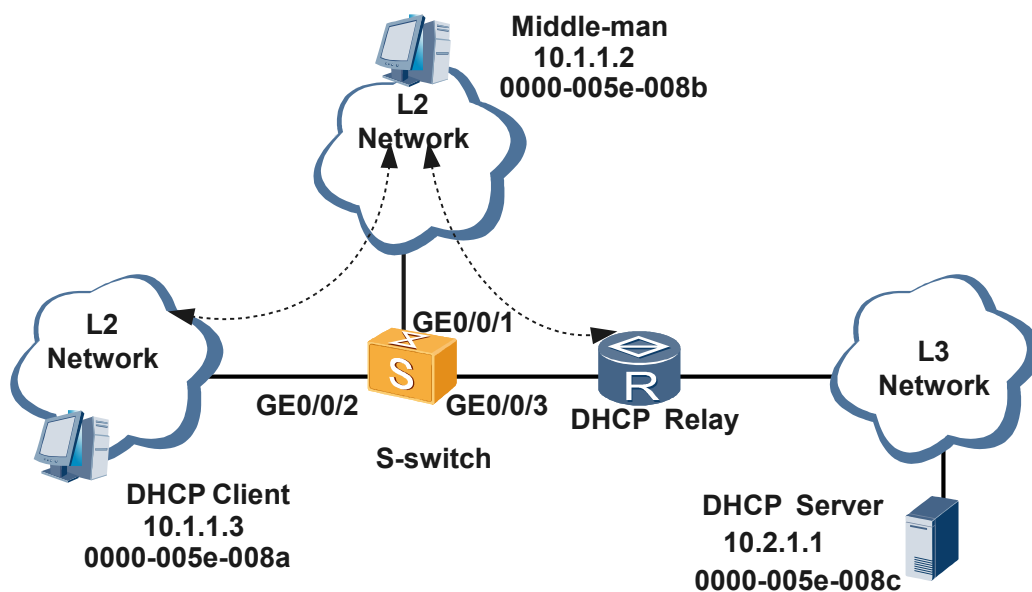
### Applicable Environment

When a middleman attack exists or an IP/MAC spoofing attack occurs, the attacker pretends to be the DHCP server or DHCP client to exchange data with the actual DHCP server and DHCP client.

As shown in **Figure 4-3**, the middleman sends IP or ARP packets to the DHCP server. Thus, the DHCP server learns the IP address 10.1.1.3 of the DHCP client and the MAC address 0000-005e-008b of the middleman. The DHCP server considers that all the packets are coming from or sending to the DHCP client. In fact, all the packets are processed by the middleman.

The middleman then sends IP or ARP packets to the DHCP client. Thus, the DHCP client learns the IP address 10.2.1.1 of the DHCP server and the MAC address 0000-005e-008b of itself. In the same manner, the DHCP client considers that all the packets are coming from or sending to the DHCP server. In fact, all the packets are processed by the middleman.

As a result, the middleman can pretend to be the DHCP server or the DHCP client and obtain data exchanged between the DHCP server and the DHCP client.

**Figure 4-3** Diagram of preventing the middleman attack and IP/MAC spoofing attack

To prevent the middleman attack and the IP/MAC spoofing attack, configure DHCP snooping on the S-switch and use the DHCP snooping binding table. The received packets can be forwarded only when they match with entries in the binding table; otherwise, packets are discarded.

## Pre-configuration Tasks

Before preventing the middleman attack and the IP/MAC spoofing attack through the S-switch, complete the following tasks:

- Configuring the DHCP server
- Configuring the DHCP relay agent

### NOTE

The DHCP server and the DHCP relay agent are configured on the upstream router or server of the S-switch.

## Data Preparation

To prevent the middleman attack and the IP/MAC spoofing attack through the S-switch, you need the following data.

| No. | Data                                                 |
|-----|------------------------------------------------------|
| 1   | Name of the interface to be added to a VLAN          |
| 2   | ID of the VLAN to which the interfaces belong        |
| 3   | Static IP addresses from which packets are forwarded |

## 4.3.2 Enabling Global DHCP Snooping

### Context

Do as follows on the S-switch.

### Procedure

- Step 1** Run:
- ```
system-view
```
- The system view is displayed.
- Step 2** Run:
- ```
dhcp snooping enable
```
- Global DHCP snooping is enabled.
- By default, DHCP snooping is disabled.
- End

## 4.3.3 Enabling Local DHCP Snooping

### Context

Do as follows on the S-switch.

### Procedure

- Step 1** Run:
- ```
system-view
```
- The system view is displayed.
- Step 2** Run:
- ```
vlan vlan-id
```
- The VLAN view is displayed.
- Step 3** Run:
- ```
dhcp snooping enable
```
- DHCP snooping is enabled in the VLAN.
- By default, DHCP snooping is disabled.
- End

4.3.4 Enabling Packet Check

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The Ethernet interface view, GigabitEthernet interface view, or Eth-Trunk interface view is displayed.

The interface should be at the user side.

Step 3 Run:

```
dhcp snooping check { arp | ip | dhcp-chaddr | dhcp-request } enable
```

Packet check is enabled on the interface and whether packets received on the interface match entries in the binding table is checked.

By default, packet check is disabled.

Step 4 Run:

```
dhcp snooping check dhcp-rate enable
```

The rate of sending DHCP messages to the protocol stack is checked.

By default, the S-switch is disabled from checking the rate of sending DHCP messages to the protocol stack.

Step 5 Run:

```
dhcp snooping check dhcp-rate rate-value
```

The rate of sending DHCP messages to the protocol stack is set.

By default, the rate of sending DHCP messages to the protocol stack is 100 per second.

----End

4.3.5 Configuring the DHCP Snooping Binding Table

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

The VLAN should be the one to which the interface at the user side belongs.

Step 3 Run:

```
dhcp snooping bind-table static ip-address ip-address mac-address mac-address  
interface interface-type interface-number
```

A static entry binding the IP address and MAC address is configured in the DHCP snooping table.

The static binding table contains the MAC address, IP address, VLAN ID, and interface information. If users access the network through static IP addresses, user packets can be forwarded by the S-switch only after the MAC address, IP address, VLAN ID, and inbound interface of the packets match entries in the static binding table. Otherwise, user packets are discarded.

If users are assigned static IP addresses, you can configure static binding entries for these static IP addresses. If static entries are not configured in the DHCP snooping binding table, packets from all users with static IP addresses are discarded. All static users thus cannot access the DHCP server.

The dynamic entries in the DHCP snooping binding table require no configuration. They are automatically generated when DHCP snooping is enabled. The static entries, however, need to be configured through commands.

----End

4.3.6 Configuring Option 82

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

The VLAN should be the one to which the interface at the user side belongs.

Step 3 Run:

```
dhcp option82 rebuild enable interface interface-type interface-number
```

The Option 82 field is forcibly appended to the DHCP messages on a specified interface in the VLAN.

By default, the Option 82 field cannot be forcibly appended.

The DHCP reply messages are broadcast packets. Thus, the S-switch cannot determine to which interface the packets are sent. As a result, dynamic binding entries do not include interfaces.

To protect the S-switch against attacks with the forged Option 82 field, you can enable the S-switch to forcibly append the Option 82 field to DHCP messages. The Option 82 field is appended to DHCP discovery messages if original DHCP discovery messages are not appended

with the Option 82 field. If the original DHCP discovery messages are appended with the Option 82 field, the original Option 82 field is removed and a new one is appended.

----End

4.3.7 Configuring Security Protection on an Interface

This section describes how to configure security protection on an interface.

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mac-address restrict
```

The S-switch is enabled to restrict MAC address learning and packet forwarding.

Step 3 Run:

```
mac-table limit interface-type interface-number limit-number
```

The limit on the number of MAC addresses that can be learnt by an interface is configured.

Step 4 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 5 Run:

```
port-security enable
```

Security protection is enabled on the interface.

By default, the S-switch is disabled from restricting MAC address learning and packet forwarding. If the S-switch is not enabled to restrict MAC address learning and packet forwarding, you cannot enable security protection on interfaces.

----End

4.3.8 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about global DHCP snooping.	display dhcp snooping global

Action	Command
Check information about the DHCP snooping binding table.	display dhcp snooping bind-table { all dynamic ip-address <i>ip-address</i> mac-address <i>mac-address</i> static vlan <i>vlan-id</i> } interface <i>interface-type interface-number</i> }
Check the Option 82 status.	display dhcp option82 vlan <i>vlan-id</i> [interface <i>interface-type interface-number</i>]

Run the **display dhcp snooping global** command. You can view that global DHCP snooping is enabled.

```
<Quidway> display dhcp snooping global
dhcp snooping enable
```

Run the **display dhcp snooping bind-table** command. You can view the static entries generated in the DHCP snooping binding table.

```
<Quidway> display dhcp snooping bind-table ip-address 10.1.1.1
bind-table:
ifname    vrf    vsi    p/cvlan    mac-address    ip-address    tp lease
-----
Eth0/0/1          0000-0020/0000 003e-0001-0001 010.001.001.001 S    0
-----
binditem count: 1    binditem total count: 1
```

Run the **display dhcp option82** command. You can view the Option 82 status.

```
<Quidway> display dhcp option82 vlan 20 interface Ethernet 0/0/1
dhcp option82 rebuild enable interface Ethernet0/0/1
```

4.4 Preventing the DoS Attack by Changing the CHADDR Field

This section describes how to prevent the DoS attack by changing the CHADDR field.

4.4.1 Establishing the Configuration Task

4.4.2 Enabling Global DHCP Snooping

4.4.3 Enabling Local DHCP Snooping

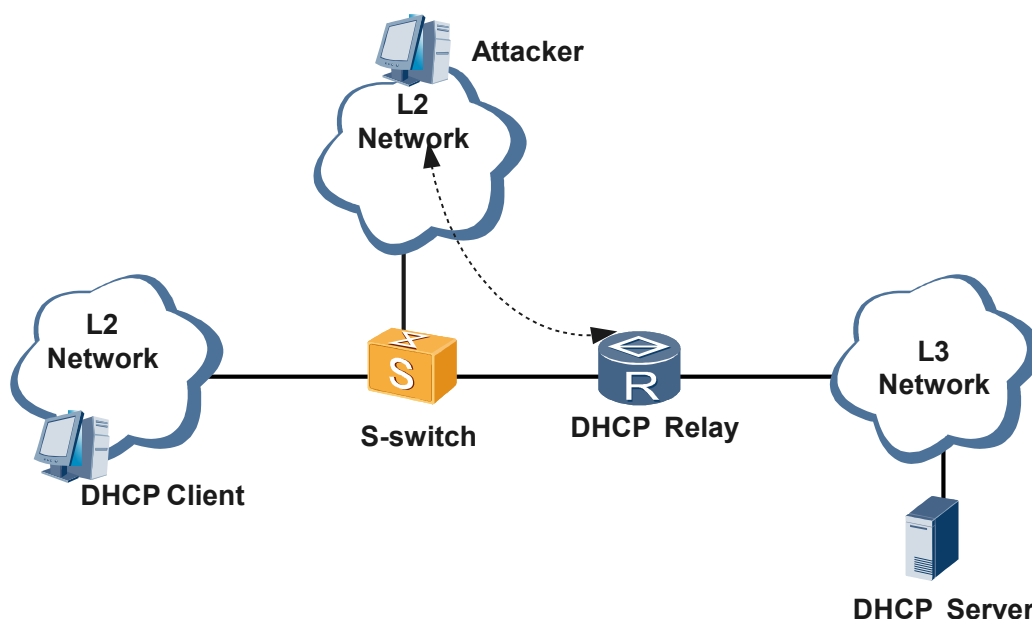
4.4.4 Checking the CHADDR Field in DHCP Request Messages

4.4.5 Checking the Configuration

4.4.1 Establishing the Configuration Task

Applicable Environment

As shown in **Figure 4-4**, the attacker continuously applies for IP addresses in a DHCP domain through various MAC addresses until all IP addresses are exhausted. Thus, legal users cannot obtain IP addresses. To prevent the DHCP exhaustion attack, you can apply the MAC address limit, that is, limit to the number of MAC addresses learned on interfaces. This protects the S-switch against attacks of sending a large number of DHCP request messages through various MAC addresses.

Figure 4-4 Networking diagram of preventing the DoS attack by changing the CHADDR field

The attacker may change the CHADDR field carried in a DHCP message instead of the source MAC address in the frame header to apply for IP addresses continuously. If the S-switch checks the validity of packets based on the source MAC address in the frame header, attack packets can still be forwarded normally. The MAC address limit cannot take effect in this manner.

To prevent the attacker from changing the CHADDR field, you can configure DHCP snooping on the S-switch to check the CHADDR field carried in DHCP request messages. If the CHADDR field matches the source MAC address in the frame header, the messages are forwarded. Otherwise, the messages are discarded.

Pre-configuration Tasks

Before preventing the DoS attack by changing the CHADDR field, complete the following tasks:

- Configuring the DHCP server
- Configuring the DHCP relay agent

NOTE

The DHCP server and the DHCP relay agent are configured on the upstream router or server of the S-switch.

Data Preparation

To prevent the DoS attack by changing the CHADDR field, you need the following data.

No.	Data
1	Name of the interface to be added to a VLAN
2	ID of the VLAN to which the interfaces belong

4.4.2 Enabling Global DHCP Snooping

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp snooping enable
```

Global DHCP snooping is enabled.

By default, DHCP snooping is disabled.

All the other DHCP snooping configurations can be performed only after global DHCP snooping is enabled.

----End

4.4.3 Enabling Local DHCP Snooping

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

Step 3 Run:

```
dhcp snooping enable
```

DHCP snooping is enabled in the VLAN.

By default, DHCP snooping is disabled.

----End

4.4.4 Checking the CHADDR Field in DHCP Request Messages

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **dhcp snooping check dhcp-chaddr enable** command to enable the interface to check the CHADDR field in DHCP request messages.

By default, checking the CHADDR field is disabled.

----End

4.4.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about global DHCP snooping.	display dhcp snooping global
Check information about DHCP snooping on an interface.	display dhcp snooping interface <i>interface-type</i> <i>interface-number</i>

Run the **display dhcp snooping global** command. You can view that global DHCP snooping is enabled.

```
<Quidway> display dhcp snooping global
dhcp snooping enable
```

Run the **display dhcp snooping interface** command. You can view the DHCP snooping configuration on the interface.

```
<Quidway> display dhcp snooping interface ethernet 0/0/1
dhcp snooping check dhcp-chaddr enable
arp total                0
ip total                  0
dhcp-request total       0
chaddr&src mac total      0
dhcp-reply total         0
```

4.5 Preventing the Attacker from Sending Bogus Messages for Extending IP Address Leases

This section describes how to prevent the attacker from sending bogus messages for extending IP address leases.

[4.5.1 Establishing the Configuration Task](#)

[4.5.2 Enabling Global DHCP Snooping](#)

[4.5.3 Enabling Local DHCP Snooping](#)

[4.5.4 Enabling the Checking of DHCP Request Messages](#)

[4.5.5 Configuring Option 82](#)

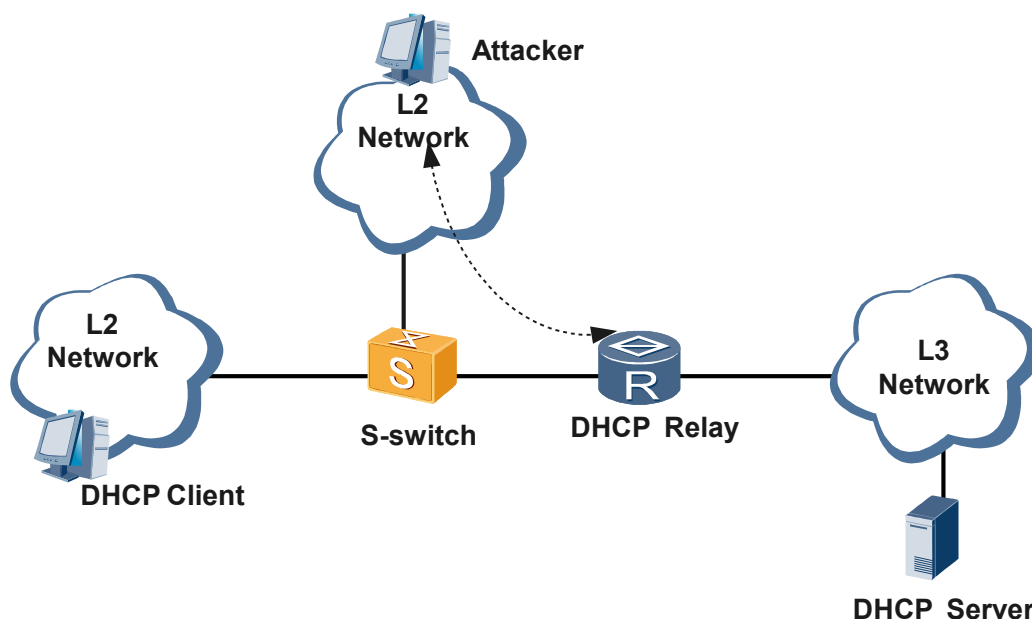
[4.5.6 Checking the Configuration](#)

4.5.1 Establishing the Configuration Task

Applicable Environment

As shown in [Figure 4-5](#), the attacker pretends to be a legal user and continuously sends DHCP request messages intending to extend the IP address lease. This prevents certain expired IP addresses from being reused, which is not the purpose of a legal user.

Figure 4-5 Networking diagram of preventing the attacker from sending bogus messages for extending IP address leases



To prevent the attacker from sending bogus messages to extend IP address leases, you can configure DHCP snooping on the S-switch to check the source IP address and source MAC address of DHCP request messages.

- If there are no entries that match the source IP address in the DHCP snooping binding table, the DHCP request messages are forwarded.
- If there are entries that match the source IP address but do not match the source MAC address, the DHCP request messages are discarded.

Pre-configuration Tasks

Before preventing the attacker from sending bogus messages for extending IP address leases through the S-switch, complete the following tasks:

- Configuring the DHCP server
- Configuring the DHCP relay agent



NOTE

The DHCP server and the DHCP relay agent are configured on the upstream router or server of the S-switch.

Data Preparation

To prevent the attacker from sending bogus messages for extending IP address leases through the S-switch, you need the following data.

No.	Data
1	Name of the interface to be added to a VLAN
2	ID of the VLAN to which the interfaces belong
3	Static IP addresses from which packets are forwarded

4.5.2 Enabling Global DHCP Snooping

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp snooping enable
```

Global DHCP snooping is enabled.

By default, DHCP snooping is disabled.

All the other DHCP snooping configurations can be performed only after global DHCP snooping is enabled.

----End

4.5.3 Enabling Local DHCP Snooping

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

Step 3 Run:
`dhcp snooping enable`
DHCP snooping is enabled in the VLAN.
By default, DHCP snooping is disabled.
----End

4.5.4 Enabling the Checking of DHCP Request Messages

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:
`system-view`
The system view is displayed.

Step 2 Run:
`interface interface-type interface-number`
The Ethernet interface view or Eth-Trunk interface view is displayed.
The interface should be at the user side.

Step 3 Run:
`dhcp snooping check dhcp-request enable`
The checking of DHCP request messages is enabled on the interface.
By default, checking DHCP request messages is disabled.
----End

4.5.5 Configuring Option 82

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:
`system-view`
The system view is displayed.

Step 2 Run:
`vlan vlan-id`
The VLAN view is displayed.
The VLAN should be the one to which the interface at the user side belongs.

Step 3 Run:

```
dhcp option82 rebuild enable interface interface-type interface-number
```

The Option 82 field is forcibly appended to the DHCP messages on a specified interface in the VLAN.

By default, the Option 82 field cannot be forcibly appended.

The DHCP reply messages are broadcast packets. Thus, the S-switch cannot determine to which interface the packets are sent. As a result, the related dynamic binding entries cannot be generated.

To protect the S-switch against attacks with the forged Option 82 field, you can enable the S-switch to forcibly append the Option 82 field to DHCP messages. The Option 82 field is appended to DHCP discovery messages if original DHCP discovery messages are not appended with the Option 82 field. If the original DHCP discovery messages are appended with the Option 82 field, the original Option 82 field is removed and a new one is appended.

----End

4.5.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about global DHCP snooping.	display dhcp snooping global
Check information about DHCP snooping on an interface.	display dhcp snooping interface <i>interface-type interface-number</i>
Check the Option 82 status.	display dhcp option82 vlan <i>vlan-id</i> [interface <i>interface-type interface-number</i>]

Run the **display dhcp snooping global** command. You can view that global DHCP snooping is enabled.

```
<Quidway> display dhcp snooping global
dhcp snooping enable
```

Run the **display dhcp snooping interface** command. You can view the DHCP snooping configuration on the interface.

```
<Quidway> display dhcp snooping interface ethernet 0/0/1
dhcp snooping check dhcp-request enable
arp total                0
ip total                  0
dhcp-request total       0
chaddr&src mac total     0
dhcp-reply total         0
```

Run the **display dhcp option82** command. You can view the Option 82 status.

```
<Quidway> display dhcp option82 vlan 20 interface ethernet 0/0/1
dhcp option82 rebuild enable interface Ethernet0/0/1
```

4.6 Configuring the DHCP Option 82 String

This section describes how to configure the DHCP Option 82 string.

[4.6.1 Configuring the Storage Format of the Option 82 Field](#)

[4.6.2 Configuring the Circuit ID in the Option 82 Field in the System View](#)

[4.6.3 Configuring the Remote ID in the Option 82 Field in the System View](#)

[4.6.4 Configuring the Remote ID of the Option 82 Field in the Interface View](#)

[4.6.5 Checking the Configuration](#)

4.6.1 Configuring the Storage Format of the Option 82 Field

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **dhcp snooping enable** command to enable DHCP snooping on the S-switch. By default, DHCP snooping is disabled.
- Step 3** Run the **dhcp snooping information format { hex | ascii }** command to configure the storage format of the Option 82 field.

By default, the storage format for the Option 82 field is **hex**.

----End

4.6.2 Configuring the Circuit ID in the Option 82 Field in the System View

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **dhcp snooping information circuit-id string *string*** command to configure the circuit ID in the Option 82 field.

By default, the circuit ID in the Option 82 field is the ID of the VLAN to which the interface receiving the DHCP client's request belongs.

----End

4.6.3 Configuring the Remote ID in the Option 82 Field in the System View

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dhcp snooping information remote-id { sysname | string string }** command to configure the remote ID in the Option 82 field.

By default, the remote ID in the Option 82 field is the bridge MAC address of the DHCP snooping device that receives the DHCP client's request.



NOTE

If you have configured the remote ID both in the interface view and in the system view, the remote ID configured in the interface view is applied. If no remote ID is configured in the interface view, the remote ID configured in the system view is applied.

----End

4.6.4 Configuring the Remote ID of the Option 82 Field in the Interface View

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface interface-type interface-number** to enter the Ethernet interface view.

Step 3 Run the **dhcp snooping information [vlan vlan-id] remote-id string string** command to configure the remote ID in the Option 82 field.

By default, the remote ID in the Option 82 field is the bridge MAC address of the DHCP snooping device that receives the DHCP client's request.



NOTE

With **vlan vlan-id** specified, the customized remote ID applies only to the DHCP packets from the specified VLAN. With no **vlan vlan-id** specified, the customized remote ID applies to all DHCP packets that pass through the current interface.

----End

4.6.5 Checking the Configuration

Run the following commands in the user view to check the previous configuration.

Action	Command
Check information about global DHCP snooping.	display dhcp snooping global
Check information about DHCP snooping on an interface.	display dhcp snooping interface

4.7 Configuring the Packet Discarding Alarm

This section describes how to configure the packet discarding alarm.

4.7.1 Establishing the Configuration Task

4.7.2 Configuring the Packet Discarding Alarm

4.7.3 Checking the Configuration

4.7.1 Establishing the Configuration Task

Applicable Environment

With DHCP snooping configured, the S-switch can discard packets sent from the attacker. [Table 4-2](#) shows the relationship between the type of attacks and the type of discarded packets.

Table 4-2 Relationship between the type of attacks and the type of discarded packets

Type of Attacks	Type of Discarded Packets
Bogus attack	DHCP reply messages received from untrusted interfaces
Middleman and IP/MAC spoofing attack	IP packets or ARP packets that do not match entries in the DHCP snooping binding table
DoS attack by changing the CHADDR field	DHCP request messages whose CHADDR field does not match the source MAC address in the frame header
Attack of sending bogus messages to extend IP address leases	DHCP request messages that do not match entries in the DHCP snooping binding table
Attack of sending DHCP request messages	Messages exceeding the rate limit

After the packet discarding alarm is enabled, an alarm is generated when the number of discarded packets on the S-switch reaches the threshold.

Pre-configuration Tasks

Before configuring the packet discarding alarm, complete the following tasks:

- Configuring the DHCP server
- Configuring the DHCP relay agent

- Configuring the discarding of DHCP reply messages from the untrusted interface at the user side
- Configuring the checking of ARP packets, IP packets, and DHCP request messages
- Configuring the checking of the CHADDR field in DHCP request messages
- Configuring the checking of the rate of sending DHCP messages

**NOTE**

The DHCP server and the DHCP relay agent are configured on the upstream router or server of the S-switch.

Data Preparation

To configure the packet discarding alarm, you need the following data.

No.	Data
1	Alarm threshold for the number of discarded ARP packets
2	Alarm threshold for the number of discarded IP packets
3	Alarm threshold for the number of discarded DHCP CHADDR packets
4	Alarm threshold for the number of discarded DHCP reply messages
5	Alarm threshold for the number of discarded DHCP request messages

4.7.2 Configuring the Packet Discarding Alarm

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
dhcp snooping alarm { arp | dhcp-chaddr | dhcp-reply | dhcp-request | ip } enable
```

The packet discarding alarm is enabled on the interface.

By default, the packet discarding alarm is disabled.

Step 4 Run:

```
dhcp snooping alarm { arp | dhcp-chaddr | dhcp-reply | dhcp-request | ip }  
threshold threshold
```

The threshold that triggers the alarm is set for the discarded packets on the interface.

By default, the threshold that triggers the alarm for discarded packets is 100.

Step 5 Run:

```
dhcp snooping alarm dhcp-rate enable
```

The alarm is enabled for the rate of sending DHCP messages to the protocol stack.

By default, the alarm for the rate of sending DHCP messages to the protocol stack is disabled.

Step 6 Run:

```
dhcp snooping alarm dhcp-rate threshold threshold-value
```

The threshold that triggers the alarm is set for the rate of sending DHCP messages to the protocol stack.

By default, the threshold that triggers the alarm for the rate of sending DHCP messages to the protocol stack is 100.

----End

4.7.3 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about global DHCP snooping.	display dhcp snooping global
Check information about DHCP snooping on an interface.	display dhcp snooping interface <i>interface-type</i> <i>interface-number</i>

Run the **display dhcp snooping global** command. You can view that global DHCP snooping is enabled.

```
<Quidway> display dhcp snooping global
dhcp snooping enable
```

Run the **display dhcp snooping interface** command. You can view the DHCP snooping configuration on the interface.

```
<Quidway> display dhcp snooping interface ethernet 0/0/1
dhcp snooping check arp enable
dhcp snooping alarm arp enable
dhcp snooping alarm arp threshold 50
arp total                0
ip total                  0
dhcp-request total       0
chaddr&src mac total     0
dhcp-reply total         0
```

4.8 Maintaining DHCP Snooping

This section describes how to maintain DHCP snooping.

[4.8.1 Backing Up the DHCP Snooping Binding Table](#)

[4.8.2 Debugging DHCP Snooping](#)

4.8.1 Backing Up the DHCP Snooping Binding Table

To back up the DHCP snooping binding table, run the following command in the system view.

Action	Command
Back up the DHCP snooping binding table.	dhcp snooping bind-table autosave <i>file-name</i>

If the backup of the binding table is configured, the system automatically backs up the binding table to a specified path every 24 hours.

If no backup binding table exists, the DHCP snooping dynamic binding table is lost after the S-switch reboots. As a result, users cannot obtain IP addresses dynamically from the DHCP server so that they cannot communicate normally.

4.8.2 Debugging DHCP Snooping



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When an operation fault occurs, run the following **debugging** command in the user view to display the debugging information and locate the fault.

Action	Command
Enable DHCP snooping debugging.	debugging dhcp snooping

4.9 Configuration Examples

This section provides several examples for configuring DHCP snooping.

4.9.1 Example for Configuring DHCP Snooping to Prevent Attacks Against the Network

4.9.1 Example for Configuring DHCP Snooping to Prevent Attacks Against the Network

Networking Requirements

You can configure DHCP snooping to prevent the following network attacks:

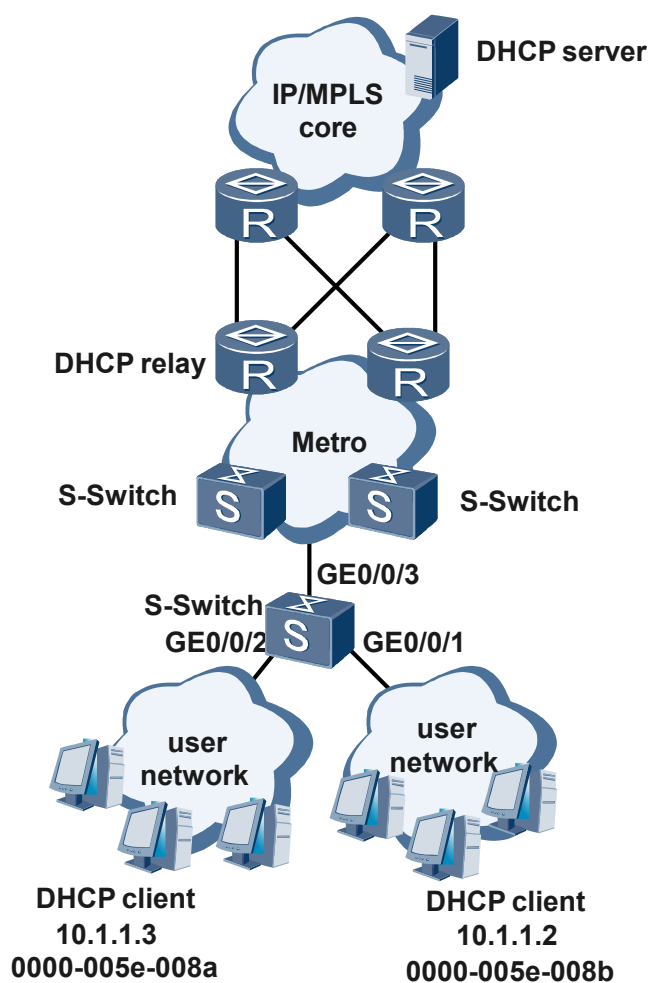
- Bogus DHCP server attack
- Middleman and IP/MAC spoofing attack
- DoS attack by changing the value of the CHADDR field

- Attack of sending bogus messages to extend IP address leases

As shown in [Figure 4-6](#), to prevent attacks against the network, you need to configure trusted/untrusted interfaces, enable packet check, set up a static binding table, and enable the sending of alarms to the NMS on the S-switch.

Two DHCP clients access the network through the static IP addresses 10.1.1.2 and 10.1.1.3 respectively. It is required that a static DHCP snooping binding table be configured to ensure the forwarding of packets from the DHCP clients.

Figure 4-6 Networking for configuring DHCP snooping to prevent attacks against the network



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP snooping globally and in the VLAN view.
2. Set the interface at the network side to be trusted.
3. Enable packet check.

4. Configure a static binding table.
5. Configure Option 82 and create a binding table covering accurate interface information.
6. Configure the sending of alarms to the NMS.

Data Preparation

To complete the configuration, you need the following data:

- IDs of VLANs to which the interfaces belong
- Static IP addresses and MAC addresses assigned to users
- Threshold for sending alarms to the NMS

Configuration Procedure

The following describes how to configure the S-switch. For the configuration procedures for the other devices shown in [Figure 4-6](#), refer to the related configuration guides.

1. Configure DHCP snooping on the S-switch.

Enable global DHCP snooping.

```
[Quidway] dhcp snooping enable
```

Configure the VLAN to which the interfaces at the user side belong.

```
[Quidway] vlan 100
```

```
[Quidway-vlan100] quit
```

```
[Quidway] interface GigabitEthernet 0/0/1
```

```
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
```

```
[Quidway-GigabitEthernet0/0/1] quit
```

```
[Quidway] interface GigabitEthernet 0/0/2
```

```
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
```

```
[Quidway-GigabitEthernet0/0/2] quit
```

Configure the VLAN to which the interface at the network side belong.

```
[Quidway] interface GigabitEthernet 0/0/3
```

```
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 100
```

```
[Quidway-GigabitEthernet0/0/3] quit
```

Enable DHCP snooping for VLAN 100.

```
[Quidway]vlan 100
```

```
[Quidway-vlan100] dhcp snooping enable
```

2. Configure the interface at the network side as trusted.

```
[Quidway-vlan100] dhcp snooping trusted interface GigabitEthernet 0/0/3
```

```
[Quidway-vlan100] quit
```

3. Enable packet check on the interfaces at the user side.

```
[Quidway]interface GigabitEthernet 0/0/1
```

```
[Quidway-GigabitEthernet0/0/1]dhcp snooping check arp enable
```

```
[Quidway-GigabitEthernet0/0/1]dhcp snooping check ip enable
```

```
[Quidway-GigabitEthernet0/0/1]dhcp snooping check dhcp-chaddr enable
```

```
[Quidway-GigabitEthernet0/0/1]dhcp snooping check dhcp-request enable
```

```
[Quidway-GigabitEthernet0/0/1]quit
```

```
[Quidway]interface GigabitEthernet 0/0/2
```

```
[Quidway-GigabitEthernet0/0/2]dhcp snooping check arp enable
```

```
[Quidway-GigabitEthernet0/0/2]dhcp snooping check ip enable
```

```
[Quidway-GigabitEthernet0/0/2]dhcp snooping check dhcp-chaddr enable
```

```
[Quidway-GigabitEthernet0/0/2]dhcp snooping check dhcp-request enable
```

```
[Quidway-GigabitEthernet0/0/2]quit
```

4. Configure static binding entries.

```
[Quidway]vlan 100
```

```
[Quidway-vlan100]dhcp snooping bind-table static ip-address 10.1.1.3 mac-  
address 0000-005e-008a interface GigabitEthernet 0/0/2
```

```
[Quidway-vlan100]dhcp snooping bind-table static ip-address 10.1.1.2 mac-  
address 0000-005e-008b interface GigabitEthernet 0/0/1
```

5. Forcibly append the Option 82 field to DHCP messages.

```
[Quidway-vlan100] dhcp option82 rebuild enable interface GigabitEthernet 0/0/1  
[Quidway-vlan100]dhcp option82 rebuild enable interface GigabitEthernet 0/0/2  
[Quidway-vlan100]quit
```

6. Configure the sending of alarms to the NMS.

Enable the sending of alarms to the NMS.

```
[Quidway]interface GigabitEthernet 0/0/1  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm arp enable  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm ip enable  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm dhcp-chaddr enable  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm dhcp-request enable  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm dhcp-reply enable  
[Quidway-GigabitEthernet0/0/1]quit  
[Quidway]interface GigabitEthernet 0/0/2  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm arp enable  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm ip enable  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm dhcp-chaddr enable  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm dhcp-request enable  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm dhcp-reply enable  
[Quidway-GigabitEthernet0/0/2]quit
```

Set the threshold for sending alarms.

```
[Quidway]interface GigabitEthernet 0/0/1  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm arp threshold 10  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm ip threshold 10  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm dhcp-chaddr threshold 10  
[Quidway-GigabitEthernet0/0/1]dhcp snooping alarm dhcp-request threshold 10  
[Quidway-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-reply threshold 10  
[Quidway-GigabitEthernet0/0/1]quit  
[Quidway]interface GigabitEthernet 0/0/2  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm arp threshold 10  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm ip threshold 10  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm dhcp-chaddr threshold 10  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm dhcp-request threshold 10  
[Quidway-GigabitEthernet0/0/2]dhcp snooping alarm dhcp-reply threshold 10  
[Quidway-GigabitEthernet0/0/2]quit
```

7. Verify the configuration.

Run the **display dhcp snooping bind-table** command and the **display dhcp option82** command. You can view that DHCP snooping is enabled in the system view. You can also view the configurations of sending alarms to the NMS and the statistics on the discarded packets.

Check DHCP snooping configurations in the system view.

```
[Quidway]display dhcp snooping global  
dhcp snooping enable
```

Check static entries in the DHCP snooping binding table.

```
[Quidway]display dhcp snooping bind-table static  
bind-table:  
ifname          vrf   vsi   p/cvlan   mac-address      ip-address      tp lease  
-----  
-  
GE0/0/1         0000  -    0100/0000 0000-005e-008b 010.001.001.002 S  0  
GE0/0/2         0000  -    0100/0000 0000-005e-008a 010.001.001.003 S  0  
-----  
-  
binditem count:      1                      binditem total count: 1
```

Check whether Option 82 is enabled on GigabitEthernet 0/0/1.

```
[Quidway]display dhcp option82 vlan 100 interface GigabitEthernet 0/0/1  
dhcp option82 rebuilt enable interface GigabitEthernet 0/0/1
```

Configuration Files

The following lists configuration files of the S-switch.

```
#
sysname Quidway
#
vlan batch 100
#
dhcp snooping enable
#
vlan 100
dhcp snooping trusted interface GigabitEthernet0/0/3
  dhcp option82 rebuild enable interface GigabitEthernet0/0/1
dhcp option82 rebuild enable interface GigabitEthernet0/0/2
  dhcp snooping bind-table static ip-address 10.1.1.3 mac-address 0000-005e-008a
interface GigabitEthernet0/0/2
dhcp snooping bind-table static ip-address 10.1.1.2 mac-address 0000-005e-008b
interface GigabitEthernet 0/0/1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 100
  dhcp snooping check arp enable
  dhcp snooping alarm arp enable
  dhcp snooping alarm arp threshold 10
  dhcp snooping check ip enable
  dhcp snooping alarm ip enable
  dhcp snooping alarm ip threshold 10
  dhcp snooping check dhcp-chaddr enable
  dhcp snooping alarm dhcp-chaddr enable
  dhcp snooping alarm dhcp-chaddr threshold 10
  dhcp snooping alarm dhcp-reply enable
  dhcp snooping alarm dhcp-reply threshold 10
  dhcp snooping check dhcp-request enable
  dhcp snooping alarm dhcp-request enable
  dhcp snooping alarm dhcp-request threshold 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 100
  dhcp snooping check arp enable
  dhcp snooping alarm arp enable
  dhcp snooping alarm arp threshold 10
  dhcp snooping check ip enable
  dhcp snooping alarm ip enable
  dhcp snooping alarm ip threshold 10
  dhcp snooping check dhcp-chaddr enable
  dhcp snooping alarm dhcp-chaddr enable
  dhcp snooping alarm dhcp-chaddr threshold 10
  dhcp snooping alarm dhcp-reply enable
  dhcp snooping alarm dhcp-reply threshold 10
  dhcp snooping check dhcp-request enable
  dhcp snooping alarm dhcp-request enable
  dhcp snooping alarm dhcp-request threshold 10
#
interface GigabitEthernet0/0/3
  port trunk allow-pass vlan 100
#
return
#
```

5 AAA Configuration

About This Chapter

This chapter describes the basic concepts and configuration procedures of Authentication, Authorization, and Accounting (AAA), Remote Authentication Dial in User Service (RADIUS), Huawei Terminal Access Controller Access Control System (HWTACACS), domains, and local users.

[5.1 Overview of AAA](#)

This section describes the basic principle and concepts of AAA and user management.

[5.2 Configuring AAA](#)

This section describes how to configure AAA.

[5.3 Configuring the RADIUS Server](#)

This section describes how to configure the RADIUS server.

[5.4 Configuring the HWTACACS Server](#)

This section describes how to configure the HWTACACS server.

[5.5 Configuring a Domain](#)

This section describes how to configure a domain.

[5.6 Configuring Local User Management](#)

This section describes how to configure local user management.

[5.7 Maintaining AAA](#)

This section describes how to clear or debug AAA.

[5.8 Configuration Examples](#)

This section provides an example for configuring AAA.

5.1 Overview of AAA

This section describes the basic principle and concepts of AAA and user management.

[5.1.1 Introduction to AAA](#)

[5.1.2 RADIUS](#)

[5.1.3 HWTACACS](#)

[5.1.4 Domain-based User Management](#)

[5.1.5 Local User Management](#)

[5.1.6 References](#)

[5.1.7 Logical Relationships Between Configuration Tasks](#)

5.1.1 Introduction to AAA

AAA provides the following security functions for users:

- Authentication
It determines the users that can access the network.
- Authorization
It authorizes users to use certain services.
- Accounting
It records the network resource usage of users.

Generally, AAA adopts the client/server model. In this model, the client runs at the resource side that is managed through AAA, whereas the server collects and keeps all user information. This model features good extensibility and facilitates concentrated management over user information.

Authentication

AAA, implemented on the S-switch, provides the following authentication modes:

- Non-authentication
Users are completely trusted and there is no check on their validity. This authentication mode is not recommended.
- Local authentication
For local authentication, user information, including the user name, password, and attributes, is configured on the S-switch. This authentication mode features high processing speed and low operation cost; however, the capacity of information storage is restricted by the hardware of the device.
- Remote authentication
Users are remotely authenticated through the RADIUS protocol or the HWTACACS protocol. In this process, the S-switch serves as the client to communicate with the RADIUS or HWTACACS authentication server. The RADIUS protocol can be either a standard RADIUS protocol or an extended RADIUS protocol of Huawei, which is used on the

iTELLIN or the Comprehensive Access Management Server (CAMS) to complete the authentication.

Authorization

AAA, implemented on the S-switch, provides the following authorization modes:

- Non-authorization
Users are completely trusted and directly authorized.
- Local authorization
Local users are authorized based on their attributes configured on the S-switch.
- HWTACACS authorization
Users are authorized by the HWTACACS server.
- If-authenticated authorization
Users are authorized if they pass the authentication and the authentication mode is not non-authentication.
- RADIUS authorization
RADIUS authentication and RADIUS authorization are bound together. Therefore, RADIUS authorization cannot be performed separately. The RADIUS server authorizes users immediately after they pass the RADIUS authentication.

Accounting

AAA, implemented on the S-switch, provides the following accounting modes:

- Non-accounting
Free services are provided.
- Remote accounting
It supports remote accounting through the RADIUS server or the HWTACACS server.

5.1.2 RADIUS

AAA can be implemented through many protocols, of which the RADIUS protocol is the most commonly used. The RADIUS protocol was initially used for managing a large number of scattered users who accessed the network through serial interfaces and modems. Later, this protocol is widely applied to the network access server (NAS) system.

RADIUS prescribes how to transmit user information and accounting information between the NAS and the RADIUS server. The authentication information between the NAS and the RADIUS server is transmitted with a key. This can protect the user password from theft on an insecure network.

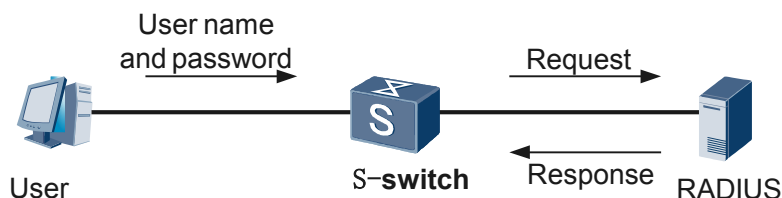
To obtain the right to access certain networks or to use some network resources, a user needs to set up a connection with the NAS through a network. In this case, the NAS is in charge of authenticating the user or the connection. After this authentication, the NAS sends the AAA information about the user to the RADIUS server.

The RADIUS server receives connection requests from users, authenticates users, and then sends the required configuration information back to the NAS.

Message Exchange Defined by RADIUS

The RADIUS protocol prescribes the message exchange between the client and the server, and the structure of the exchanged messages. The server where the RADIUS protocol is applied is called a RADIUS server. **Figure 5-1** shows the simple message exchange defined by RADIUS.

Figure 5-1 Message exchange between the RADIUS client and the RADIUS server

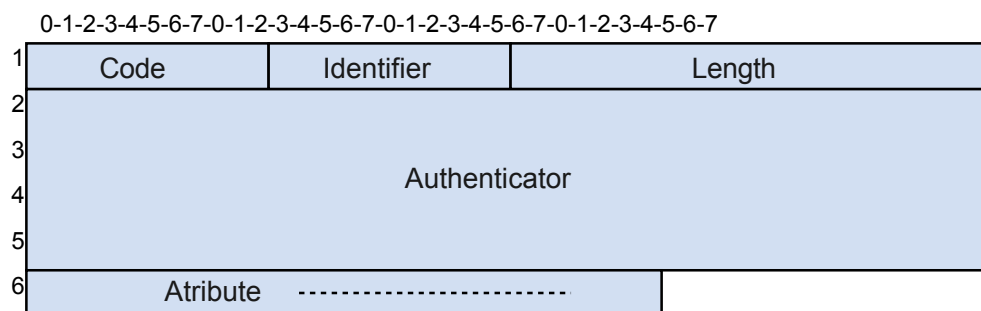


To log in to the S-switch, a user first sends its user name and password to the S-switch. On receiving the user name and password, the RADIUS client on the S-switch sends a request to the RADIUS server for authentication. If the request is legal, the RADIUS server completes the authentication and returns required user authentication information to the S-switch. Authentication information is transmitted between the S-switch and the RADIUS server with a key, that is, authentication information is transmitted on the network only after being encrypted. This can protect user information against theft on an insecure network. The exchange of accounting information is the same as that of authentication and authorization information.

Message Structure Defined by RADIUS

Figure 5-2 shows the message structure defined by RADIUS.

Figure 5-2 Message structure defined by RADIUS



Code: indicates the message type, such as the access request, access permission, and accounting request.

Identifier: is a string of ascending numbers for matching the request and response packets.

Length: indicates the total length of all fields.

Authenticator: is a value for checking the validity of a RADIUS message.

Attribute: is the main body of a message, providing the attributes of the user.

Features of RADIUS

Using the User Datagram Protocol (UDP) as the transmission protocol, RADIUS features good and real-time performance. In addition, RADIUS features high reliability by providing retransmission and standby server mechanisms.

RADIUS is easy to implement and is applicable to the multithreading structure of the server for a large number of users. Owing to these features, RADIUS is widely applied.

As the RADIUS client, the S-switch provides the following functions:

- Functions defined in the standard and extended RADIUS protocols including RFC 2865 and RFC 2866
- Functions defined in Huawei extended RADIUS+v1.1
- Active detection of the RADIUS server: After receiving an AAA authentication or accounting message, the RADIUS client enables the server detection if the status of the current server is Down. The RADIUS client then transforms the message into a packet that functions as the server-probe packet, and sends the packet to the server. If the client receives a response packet from the RADIUS server, the client considers the server as available.
- Caching Accounting Stop packets locally and retransmitting them: If the number of retransmission failures exceeds the set value, the Accounting Stop packets are stored into the buffer queue. The system periodically scans the queue, extracts the packets, and then sends them to the specified server. After the sending, the system enables a timer. If the transmission fails or no response packet comes from the server within the timeout period, the packets are replaced into the buffer queue.
- Automatic switchover of the RADIUS server: When the timer expires, you can send packets to another server in the configured server group if the current server does not work or the number of transmissions exceeds the maximum number.

5.1.3 HWTACACS

HWTACACS is an access control protocol based on TACACS (RFC1492).

Like RADIUS, HWTACACS carries out several AAA services in server/client mode.

Compared with RADIUS, HWTACACS is more reliable in transmission by encrypting the packets. **Table 5-1** shows the comparisons between HWTACACS and RADIUS.

Table 5-1 Comparisons between HWTACACS and RADIUS

HWTACACS	RADIUS
Uses the Transmission Control Protocol (TCP) to provide reliable transmission.	Uses UDP.
Encrypts the main structure of the authentication packet except the standard HWTACACS header.	Encrypts only the password field in the authentication packet.
Separates authentication from authorization.	Performs authentication together with authorization.
Is suitable for security control.	Is suitable for accounting.

HWTACACS	RADIUS
Authorizes users to use the commands for configuring the device.	None.

5.1.4 Domain-based User Management

The NAS manages users in the following ways: One is based on the domain in which you can configure default authorization, RADIUS or HWTACACS server template, and authentication and accounting schemes in the domain; the other is based on the user account. In current AAA implementation, users are categorized into different domains. The domain to which a user belongs depends on the character string that follows the "@" in the user name. For example, the user "user@huawei" belongs to the domain "huawei". If there is no "@" in the user name, the user belongs to the domain "default".

To perform AAA for access users, you need to configure authentication, authorization, and accounting modes respectively in the AAA view, and then apply the authentication, authorization, and accounting schemes in the domain view. AAA, by default, adopts local authentication, local authorization, and non-accounting schemes respectively. If a domain is created but no scheme is applied in it, AAA adopts the default schemes for this domain. In addition, to use the RADIUS or HWTACACS schemes for a user, the RADIUS or HWTACACS server template must be pre-configured in the system view and then applied in the view of the domain to which the user belongs. For details about the configuration procedures, see examples in the following sections.

When a domain and users in the domain are configured with the same attribute at the same time, the user-based configuration takes precedence over the domain-based configuration.

The authorization precedence configured within a domain is lower than that configured on an AAA server. In other words, the authorization attribute of the AAA server is used preferentially. The domain authorization attribute is valid only when the AAA server lacks this authorization or does not support this authorization. In this way, you can add services flexibly when using domains regardless of the attribute limitations of the AAA server.

On the S-switch, you can configure multiple domains. Packets are transmitted according to their domain names. Functioning as an NAS, the S-switch determines the Internet service provider (ISP) to which a user belongs according to the domain name of the user, and then transmits packets of the user to this ISP network.

5.1.5 Local User Management

To perform local user management, you need to set up the local user database, maintain user information, and manage users on the local S-switch. In addition to creating local user accounts, you can also implement functions such as local authentication and authorization.

5.1.6 References

For more information about AAA and RADIUS, refer to the following documents:

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support

- RFC2869: RADIUS Extensions
- RFC2903: Generic AAA Architecture
- RFC2904: AAA Authorization Framework
- RFC2906: AAA Authorization Requirements

5.1.7 Logical Relationships Between Configuration Tasks

1. Categorize users as required.
2. Create authentication, authorization, and accounting schemes.
3. Configure the RADIUS or HWTACACS server to implement RADIUS or HWTACACS authentication, authorization, or accounting.
4. Create a domain.
5. Apply the authentication, authorization, and accounting schemes configured in Step 2 in the domain.
6. Apply the RADIUS or HWTACACS server configured in Step 5 in the domain.
7. Configure local users.

5.2 Configuring AAA

This section describes how to configure AAA.

[5.2.1 Establishing the Configuration Task](#)

[5.2.2 Configuring the Authentication Scheme](#)

[5.2.3 \(Optional\) Configuring the Authorization Scheme](#)

[5.2.4 Configuring the Accounting Scheme](#)

[5.2.5 \(Optional\) Configuring the Recording Scheme](#)

[5.2.6 Checking the Configuration](#)

5.2.1 Establishing the Configuration Task

Applicable Environment

You can configure AAA to provide network access services for legal users in the following scenarios:

- The network devices need to be protected.
- Illegal access needs to be denied.
- The credibility of legal users is low.



NOTE

AAA is always enabled on the S-switch.

Pre-configuration Tasks

None.

Data Preparation

To configure AAA, you need the following data.

No.	Data
1	Name of the authentication scheme and authentication mode
2	(Optional) Name of the authorization scheme and authorization mode
3	Name of the accounting scheme, accounting mode, and interval for real-time accounting
4	(Optional) Policy for accounting start failures, policy for real-time accounting failures, and maximum number of real-time accounting failures
5	(Optional) Name of the recording scheme, name of the HWTACACS server template related to the recording mode, and events to be recorded
6	Types and numbers of the interfaces at the server side and the client side

5.2.2 Configuring the Authentication Scheme

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
authentication-scheme authentication-scheme-name
```

An authentication scheme is created and the authentication scheme view is displayed.

Step 4 Run:

```
authentication-mode { hwtacacs | radius | local }*[ none ]  
or  
authentication-mode none
```

The authentication mode is set.

In this step, more than one authentication mode can be chosen, with the **none** mode as the last choice. During the actual authentication, the order for the modes to take effect is determined by the order of input commands. The next mode takes effect only after the preceding one becomes invalid.

----End

5.2.3 (Optional) Configuring the Authorization Scheme

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
authorization-scheme authorization-scheme-name
```

An authorization scheme is created and the authorization scheme view is displayed.

Step 4 Run:

```
authorization-mode { hwtacacs | if-authenticated | local }*[ none ]  
or  
authorization-mode none
```

The authorization mode is set.

In this step, more than one authorization mode can be chosen, with the **none** mode as the last choice. During the actual authorization, the order for the modes to take effect is determined by the order of input commands. The next mode takes effect only after the preceding one becomes invalid.

----End

5.2.4 Configuring the Accounting Scheme

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
accounting-scheme accounting-scheme-name
```

An accounting scheme is created and the accounting scheme view is displayed.

Step 4 Run:

```
accounting-mode { hwtacacs | none | radius }
```

The accounting mode is set.

Step 5 (Optional) Run:

```
accounting realtime interval
```

Real-time accounting is enabled and the accounting interval is set.

By default, the value of *interval* is 5, in minutes.

Step 6 (Optional) Run:

```
accounting interim-fail [ max-times times ] [ offline | online ]
```

The policy for real-time accounting failures is configured.

By default, the value of *times* is 3.

Step 7 (Optional) Run:

```
accounting start-fail [ offline | online ]
```

The policy for accounting start failures is configured.

By default, the policy for accounting start failures is **offline**.

----End

5.2.5 (Optional) Configuring the Recording Scheme

Context

**NOTE**

You can configure the recording scheme only when HWTACACS has been enabled and the HWTACACS server template has been set.

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
recording-scheme recording-scheme-name
```

A recording scheme is created and the recording scheme view is displayed.

Step 4 Run:

```
recording-mode hwtacacs template-name
```

The recording mode is set.

Step 5 Run:

```
quit
```

The recording scheme view is quit and the AAA view is displayed.

Step 6 Run:

```
cmd recording-scheme recording-scheme-name
```

The commands that are used by the user are recorded on the device.

Step 7 Run:

```
outbound recording-scheme recording-scheme-name
```

The operations that are implemented on the device are recorded for the client.

Step 8 Run:

```
system recording-scheme recording-scheme-name
```

The system-level events are recorded.

[Step 6](#) and [Step 8](#) are not listed in sequence.

----End

5.2.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the summary of AAA.	display aaa configuration
Check the accounting scheme.	display accounting-scheme [<i>accounting-scheme-name</i>]
Check the authentication scheme.	display authentication-scheme [<i>authentication-scheme-name</i>]
Check the authorization scheme.	display authorization-scheme [<i>authorization-scheme-name</i>]
Check the recording scheme.	display recording-scheme [<i>recording-scheme-name</i>]

5.3 Configuring the RADIUS Server

This section describes how to configure the RADIUS server.

[5.3.1 Establishing the Configuration Task](#)

[5.3.2 Creating a RADIUS Server Template](#)

[5.3.3 Configuring the RADIUS Authentication Server](#)

[5.3.4 Configuring the RADIUS Accounting Server](#)

[5.3.5 \(Optional\) Configuring the Protocol Version for the RADIUS Server](#)

[5.3.6 \(Optional\) Configuring the Shared Key for the RADIUS Server](#)[5.3.7 \(Optional\) Configuring the User Name Format for the RADIUS Server](#)[5.3.8 \(Optional\) Setting the Traffic Unit for the RADIUS Server](#)[5.3.9 \(Optional\) Configuring the Retransmission Parameters for the RADIUS Server](#)[5.3.10 \(Optional\) Configuring the NAS Interface for the RADIUS Server](#)[5.3.11 Checking the Configuration](#)

5.3.1 Establishing the Configuration Task

Applicable Environment

When the RADIUS protocol is adopted for AAA, you need to configure the RADIUS server.

 **NOTE**

Although most RADIUS configurations have default ones, you can modify them as required.

The configurations, however, can be modified only when the RADIUS server template is not in use.

Pre-configuration Tasks

None.

Data Preparation

To configure the RADIUS server, you need the following data.

No.	Data
1	Name of the RADIUS server template
2	IP address, interface number, and source interface number of the primary RADIUS server for authentication and accounting
3	(Optional) IP address, interface number, and source interface number of the secondary RADIUS server for authentication and accounting
4	(Optional) Retransmission times or prohibited retransmission of Accounting Stop packets
5	(Optional) Protocol version of the RADIUS server
6	(Optional) Shared key of the RADIUS server
7	(Optional) User name format (with or without the domain name) of the RADIUS server
8	(Optional) Traffic unit of the RADIUS server
9	(Optional) Response timeout period and retransmission times of the RADIUS server
10	(Optional) NAS interface format and its ID format of the RADIUS server

5.3.2 Creating a RADIUS Server Template

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
radius-server template template-name
```

A RADIUS server template is created and the RADIUS view is displayed.

----End

5.3.3 Configuring the RADIUS Authentication Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
radius-server template template-name
```

The RADIUS view is displayed.

Step 3 Run:

```
radius-server authentication ip-address port [ source loopback interface-number ]
```

The primary RADIUS authentication server is configured.

Step 4 Run:

```
radius-server authentication ip-address port [ source loopback interface-number ]  
secondary
```

The secondary RADIUS authentication server is configured.

----End

5.3.4 Configuring the RADIUS Accounting Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
radius-server template template-name
```

The RADIUS view is displayed.

Step 3 Run:

```
radius-server accounting ip-address port [ source loopback interface-number ]
```

The primary RADIUS accounting server is configured.

Step 4 Run:

```
radius-server accounting ip-address port [ source loopback interface-number ]  
secondary
```

The secondary RADIUS accounting server is configured.

----End

5.3.5 (Optional) Configuring the Protocol Version for the RADIUS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
radius-server template template-name
```

The RADIUS view is displayed.

Step 3 Run:

```
radius-server type { portal | standard }
```

The protocol version is configured for the RADIUS server.

----End

5.3.6 (Optional) Configuring the Shared Key for the RADIUS Server

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`radius-server template template-name`
The RADIUS view is displayed.
- Step 3** Run:
`radius-server shared-key key-string`
The shared key is configured for the RADIUS server.
- End

5.3.7 (Optional) Configuring the User Name Format for the RADIUS Server

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`radius-server template template-name`
The RADIUS view is displayed.
- Step 3** Run:
`radius-server user-name domain-included`
The user name format is configured for the RADIUS server.
- End

5.3.8 (Optional) Setting the Traffic Unit for the RADIUS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
radius-server template template-name
```

The RADIUS view is displayed.

Step 3 Run:

```
radius-server traffic-unit { byte | kbyte | mbyte | gbyte }
```

The traffic unit is set for the RADIUS server.

----End

5.3.9 (Optional) Configuring the Retransmission Parameters for the RADIUS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
radius-server template template-name
```

The RADIUS view is displayed.

Step 3 Run:

```
radius-server timeout seconds
```

The response timeout period is set for the RADIUS server.

Step 4 Run:

```
radius-server retransmit retry-times
```

The retransmission times are set for the RADIUS server.

Step 3 and **Step 4** are not listed in sequence.

----End

5.3.10 (Optional) Configuring the NAS Interface for the RADIUS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
radius-server template template-name
```

The RADIUS view is displayed.

Step 3 Run:

```
radius-server nas-port-format { new | old }
```

The NAS interface format is configured for the RADIUS server.

Step 4 Run:

```
radius-server nas-port-id-format { new | old }
```

The ID format of the NAS interface is configured for the RADIUS server.

[Step 3](#) and [Step 4](#) are not listed in sequence.

----End

5.3.11 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of the RADIUS server.	display radius-server configuration [template <i>template-name</i>]

5.4 Configuring the HWTACACS Server

This section describes how to configure the HWTACACS server.

[5.4.1 Establishing the Configuration Task](#)

[5.4.2 Creating a HWTACACS Server Template](#)

[5.4.3 Configuring the HWTACACS Authentication Server](#)

[5.4.4 Configuring the HWTACACS Authorization Server](#)

[5.4.5 Configuring the HWTACACS Accounting Server](#)

[5.4.6 \(Optional\) Configuring the Source IP Address of the HWTACACS Server](#)[5.4.7 \(Optional\) Configuring the Shared Key for the HWTACACS Server](#)[5.4.8 \(Optional\) Configuring the User Name Format for the HWTACACS Server](#)[5.4.9 \(Optional\) Setting the Traffic Unit for the HWTACACS Server](#)[5.4.10 \(Optional\) Setting the Timer of the HWTACACS Server](#)[5.4.11 Checking the Configuration](#)

5.4.1 Establishing the Configuration Task

Applicable Environment

When the HWTACACS protocol is adopted for AAA, you need configure the HWTACACS server.

 **NOTE**

The configuration of the HWTACACS server differs from that of the RADIUS server as follows:

The S-switch does not check whether the HWTACACS template is in use when you modify attributes of the HWTACACS server except for deleting the configuration of the server.

By default, no authentication key is configured for the HWTACACS server.

HWTACACS can process Accounting Stop packets on both integrated devices and distributed devices.

Pre-configuration Tasks

None.

Data Preparation

To configure AAA, you need the following data.

No.	Data
1	Name of the HWTACACS server template
2	IP address and interface number of the primary HWTACACS server for authentication, authorization, and accounting
3	(Optional) IP address and interface number of the secondary HWTACACS server for authentication, authorization, and accounting
4	(Optional) Retransmission times or prohibited retransmission of Accounting Stop packets
5	(Optional) Source IP address of the HWTACACS server
6	(Optional) Shared key of the HWTACACS server
7	(Optional) User name format (with or without the domain name) of the HWTACACS server
8	(Optional) Traffic unit of the HWTACACS server

No.	Data
9	(Optional) Response timeout period of the HWTACACS server and the time for restoring the primary HWTACACS server to be active

5.4.2 Creating a HWTACACS Server Template

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`hwtacacs-server template template-name`
A HWTACACS server template is created and the HWTACACS view is displayed.
- End

5.4.3 Configuring the HWTACACS Authentication Server

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`hwtacacs-server template template-name`
The HWTACACS view is displayed.
- Step 3** Run:
`hwtacacs-server authentication ip-address [port]`
The primary HWTACACS authentication server is configured.
- Step 4** Run:
`hwtacacs-server authentication ip-address [port]`
The secondary HWTACACS authentication server is configured.
- End

5.4.4 Configuring the HWTACACS Authorization Server

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`hwtacacs-server template template-name`
The HWTACACS view is displayed.
- Step 3** Run:
`hwtacacs-server authorization ip-address [port]`
The primary HWTACACS authorization server is configured.
- Step 4** Run:
`hwtacacs-server authorization ip-address [port] secondary`
The secondary HWTACACS authorization server is configured.
- End

5.4.5 Configuring the HWTACACS Accounting Server

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`hwtacacs-server template template-name`
The HWTACACS view is displayed.
- Step 3** Run:
`hwtacacs-server accounting ip-address [port]`
The primary HWTACACS accounting server is configured.
- Step 4** Run:
`hwtacacs-server accounting ip-address [port] secondary`

The secondary HWTACACS accounting server is configured.

Step 5 Run:

```
quit
```

The HWTACACS view is quit.

Step 6 Run:

```
hwtacacs-server accounting-stop-packet resend { disable | enable number }
```

The retransmission of Accounting Stop packets is configured.

----End

5.4.6 (Optional) Configuring the Source IP Address of the HWTACACS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
hwtacacs-server template template-name
```

The HWTACACS view is displayed.

Step 3 Run:

```
hwtacacs-server source-ip ip-address
```

The source IP address of the HWTACACS server is configured.

----End

5.4.7 (Optional) Configuring the Shared Key for the HWTACACS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
hwtaacs-server template template-name
```

The HWTACACS view is displayed.

Step 3 Run:

```
hwtaacs-server shared-key key-string
```

The shared key is configured for the HWTACACS server.

----End

5.4.8 (Optional) Configuring the User Name Format for the HWTACACS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
hwtaacs-server template template-name
```

The HWTACACS view is displayed.

Step 3 Run:

```
hwtaacs-server user-name domain-included
```

The user name format is configured for the HWTACACS server.

----End

5.4.9 (Optional) Setting the Traffic Unit for the HWTACACS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
hwtaacs-server template template-name
```

The HWTACACS view is displayed.

Step 3 Run:

```
hwtaacs-server traffic-unit { byte | kbyte | mbyte | gbyte }
```

The traffic unit is set for the HWTACACS server.

----End

5.4.10 (Optional) Setting the Timer of the HWTACACS Server

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
hwtaacs-server template template-name
```

The HWTACACS view is displayed.

Step 3 Run:

```
hwtaacs-server timer response-timeout timeout
```

The response timeout period is set for the HWTACACS server.

Step 4 Run:

```
hwtaacs-server timer quiet time
```

The restoration period is set for the HWTACACS server.

----End

5.4.11 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the HWTACACS server.	display hwtaacs-server template [<i>template-name</i>] [<i>verbose</i>]]
Check Accounting Stop packets on the HWTACACS server.	display hwtaacs-server accounting-stop-packet { <i>all</i> <i>number</i> <i>ip ip-address</i> }

5.5 Configuring a Domain

This section describes how to configure a domain.

[5.5.1 Establishing the Configuration Task](#)

[5.5.2 Creating a Domain](#)

[5.5.3 Configuring Authentication, Authorization, and Accounting Schemes for the Domain](#)[5.5.4 \(Optional\) Configuring the RADIUS Server Template for the Domain](#)[5.5.5 \(Optional\) Configuring the HWTACACS Server Template for the Domain](#)[5.5.6 \(Optional\) Configuring the Status of the Domain](#)[5.5.7 \(Optional\) Setting the Maximum Number of Access Users for the Domain](#)[5.5.8 Checking the Configuration](#)

5.5.1 Establishing the Configuration Task

Applicable Environment

You can configure a domain to implement AAA management on users who access the S-switch through the domain.

Pre-configuration Tasks

Configure the RADIUS or HWTACACS server template if the remote authentication, authorization, and accounting schemes are adopted.

Data Preparation

To configure a domain, you need the following data.

No.	Data
1	Domain name
2	Names of the authentication, authorization and accounting schemes to be used for the domain
3	(Optional) Name of the RADIUS or HWTACACS template to be used for the domain
4	(Optional) Maximum number of access users allowed in the domain

5.5.2 Creating a Domain

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

aaa

The AAA view is displayed.

Step 3 Run:

domain *domain-name*

A domain is created and the domain view is displayed.

----End

5.5.3 Configuring Authentication, Authorization, and Accounting Schemes for the Domain

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

aaa

The AAA view is displayed.

Step 3 Run:

domain *domain-name*

The domain view is displayed.

Step 4 Run:

authentication-scheme *authentication-scheme-name*

The authentication scheme is configured for the domain.

Step 5 Run:

authorization-scheme *authorization-scheme-name*

The authorization scheme is configured for the domain.

Step 6 Run:

accounting-scheme *accounting-scheme-name*

The accounting scheme is configured for the domain.

----End

5.5.4 (Optional) Configuring the RADIUS Server Template for the Domain

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`aaa`
The AAA view is displayed.
- Step 3** Run:
`domain domain-name`
The domain view is displayed.
- Step 4** Run:
`radius-server template-name`
The RADIUS server template is configured for the domain.
- End

5.5.5 (Optional) Configuring the HWTACACS Server Template for the Domain

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`aaa`
The AAA view is displayed.
- Step 3** Run:
`domain domain-name`
The domain view is displayed.
- Step 4** Run:
`hwtacacs-server template-name`
The HWTACACS server template is configured for the domain.
- End

5.5.6 (Optional) Configuring the Status of the Domain

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`aaa`
The AAA view is displayed.
- Step 3** Run:
`domain domain-name`
The domain view is displayed.
- Step 4** Run:
`state { active | block }`
The status of the domain is configured.
----End

5.5.7 (Optional) Setting the Maximum Number of Access Users for the Domain

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`aaa`
The AAA view is displayed.
- Step 3** Run:
`domain domain-name`
The domain view is displayed.
- Step 4** Run:

```
access-limit max-number
```

The maximum number of access users is set for the domain.

----End

5.5.8 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the domain.	display domain [<i>domain-name</i>]

5.6 Configuring Local User Management

This section describes how to configure local user management.

[5.6.1 Establishing the Configuration Task](#)

[5.6.2 Creating Local User Accounts](#)

[5.6.3 \(Optional\) Configuring the Service Type for Local Users](#)

[5.6.4 \(Optional\) Configuring the Authority of Accessing the FTP Directory for Local Users](#)

[5.6.5 \(Optional\) Configuring the Status of Local Users](#)

[5.6.6 \(Optional\) Setting the Priority of Local Users](#)

[5.6.7 \(Optional\) Setting the Access Limit for Local Users](#)

[5.6.8 Checking the Configuration](#)

5.6.1 Establishing the Configuration Task

Applicable Environment

You can create local users and manage them on the S-switch.

Pre-configuration Tasks

None.

Data Preparation

To configure AAA, you need the following data.

No.	Data
1	User names and passwords
2	(Optional) Service type of local users
3	(Optional) Name of the FTP directory for local users

No.	Data
4	(Optional) Status of local users
5	(Optional) Priority of local users
6	(Optional) Maximum number of local access users

5.6.2 Creating Local User Accounts

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`aaa`
The AAA view is displayed.
- Step 3** Run:
`local-user user-name password { simple | cipher } password`
Local user accounts are created.
- End

5.6.3 (Optional) Configuring the Service Type for Local Users

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`aaa`
The AAA view is displayed.
- Step 3** Run:
`local-user user-name service-type { ftp | ppp | ssh | telnet | terminal } *`
The service type is configured for local users.

 **NOTE**

Through this configuration procedure, user management based on the service type is implemented.

----End

5.6.4 (Optional) Configuring the Authority of Accessing the FTP Directory for Local Users

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
local-user user-name ftp-directory directory
```

The authority of accessing the FTP directory is configured for local users.

----End

5.6.5 (Optional) Configuring the Status of Local Users

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
local-user user-name state { active | block }
```

The status of local users is configured.

----End

5.6.6 (Optional) Setting the Priority of Local Users

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`aaa`
The AAA view is displayed.
- Step 3** Run:
`local-user user-name level level`
The priority of local users is set.
- End

5.6.7 (Optional) Setting the Access Limit for Local Users

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`aaa`
The AAA view is displayed.
- Step 3** Run:
`local-user user-name access-limit access-limit`
The access limit is set for local users.
- End

5.6.8 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the attributes of local users.	display local-user [domain <i>domain-name</i> user-name <i>user-name</i>]

5.7 Maintaining AAA

This section describes how to clear or debug AAA.

5.7.1 Clearing HWTACACS Statistics

5.7.2 Debugging AAA

5.7.1 Clearing HWTACACS Statistics



CAUTION

HWTACACS statistics cannot be restored after you clear it. So, confirm the action before you use the commands.

Action	Command
Clear statistics about the HWTACACS server.	reset hwtacacs-server statistics { all accounting authentication authorization }
Clear statistics about Accounting Stop packets on the HWTACACS server.	reset hwtacacs-server accounting-stop-packet { all ip <i>ip-address</i> }

5.7.2 Debugging AAA



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it at once.

When an AAA fault occurs, run the following **debugging** commands in the user view to locate the fault. For details about debugging, see Chapter 6 "Debugging and Diagnosis."

Action	Command
Debug RADIUS packets.	debugging radius packet
Debug the HWTACACS server.	debugging hwtacacs { all error event message receive-packet send-packet }

5.8 Configuration Examples

This section provides an example for configuring AAA.

Networking Requirements

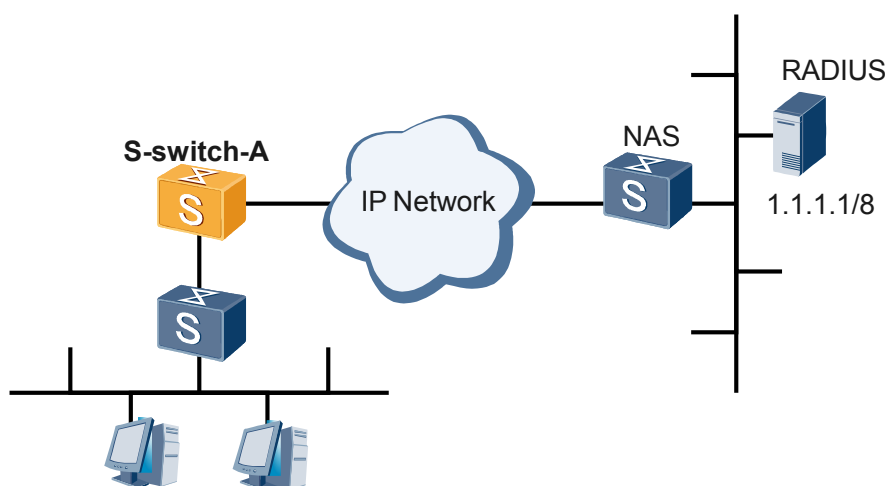
It is required that Telnet users be authenticated through the RADIUS protocol.

A maximum of five Telnet users can log in to the S-switch. Telnet users are first authenticated by the RADIUS authentication server. If the RADIUS authentication server does not respond, the non-authentication mode is adopted. The IP address of the RADIUS authentication server is 1.1.1.1. There is no secondary authentication server. By default, the interface number is 1812.

Networking diagram

See .

Figure 5-3 Networking diagram of AAA



Configuration Procedure

Configure the mode in which users access the S-switch to only Telnet and set the AAA authentication for users.

```
[S-switch-A] user-interface vty 0 4
[S-switch-A-ui-vty0-4] protocol inbound telnet
[S-switch-A-ui-vty0-4] authentication-mode aaa
[S-switch-A-ui-vty0-4] quit
```

Configure the RADIUS server template.

```
[S-switch-A] radius-server template shiva
```

Configure the IP address and interface of the RADIUS authentication server.

```
[S-switch-A-radius-shiva] radius-server authentication 1.1.1.1 1812

# Set the shared key and retransmission times for the RADIUS server.

[S-switch-A-radius-shiva] radius-server shared-key it-is-my-secret
[S-switch-A-radius-shiva] radius-server retransmit 2
[S-switch-A-radius-shiva] quit

# Enter the AAA view.

[S-switch-A] aaa

# Configure the authentication scheme r-n and set the authentication mode to radius and none in sequence, that is, if the RADIUS authentication server does not respond, the non-authentication is adopted.

[S-switch-A-aaa] authentication-scheme r-n
[S-switch-A-aaa-authen-r-n] authentication-mode radius none
[S-switch-A-aaa-authen-r-n] quit

# Configure the default domain. Adopt the authentication scheme r-n, default accounting scheme (non-accounting scheme), and the RADIUS template shiva in the domain view.

[S-switch-A-aaa] domain default
[S-switch-A-aaa-domain-default] authentication-scheme r-n
[S-switch-A-aaa-domain-default] radius-server shiva
```

Configuration Files

```
#
sysname S-switch-A
#
radius-server template shiva
radius-server shared-key it-is-my-secret
radius-server authentication 1.1.1.1 1812
radius-server retransmit 2
#
aaa
authentication-scheme default
authentication-scheme r-n
authentication-mode radius none
#
authorization-scheme default
#
accounting-scheme default
#
domain default
authentication-scheme r-n
radius-server shiva
#
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
authentication-mode aaa
#
```

6 MAC Address Authentication Configuration

About This Chapter

This chapter describes the basic concepts of MAC address authentication and the procedure for configuring MAC address authentication, and provides examples for configuring MAC address authentication.

[6.1 Overview of MAC Address Authentication](#)

This section describes the basic principle and concepts of MAC address authentication.

[6.2 Configuring MAC Address Authentication](#)

This section describes how to configure MAC address authentication.

[6.3 Configuring Enhanced MAC Address Authentication](#)

This section describes how to configure a guest VLAN and the maximum number of MAC address authentication users attached to an interface of an S-switch.

[6.4 Maintaining MAC Address Authentication](#)

Run the **reset** command in the user view to reset the statistics of MAC address authentication.

[6.5 Configuration Examples](#)

This section provides a configuration example for MAC address authentication.

6.1 Overview of MAC Address Authentication

This section describes the basic principle and concepts of MAC address authentication.

6.1.1 Introduction to MAC Address Authentication

6.1.2 MAC Address Authentication Features Supported by the S-switch

6.1.3 Update History

6.1.1 Introduction to MAC Address Authentication

The switch adopt MAC address authentication in the following modes:

- Remote Authentication Dial-In User Service (RADIUS) server authentication
- Local authentication

After confirming the authentication mode, you can select one of the following types of authentication usernames:

- MAC-address usernames: The MAC address of a user is used as a username for authentication.
- Fixed username: All users that use the same MAC address use the username and password pre-configured on an S-switch; therefore, whether users can pass the authentication depends on the correctness of the username and password, and the maximum number of users allowed to use the username.

MAC Address Authentication in RADIUS Server Authentication Mode

When MAC address authentication adopts the RADIUS server authentication mode, an S-switch functioning as a RADIUS client cooperates with the RADIUS server to implement MAC address authentication.

- When the MAC-address username type is adopted, the S-switch takes the MAC address of a detected user as the username and password of the user, and sends it to the RADIUS server.
- When the fixed username type is adopted, the S-switch takes the locally configured username and password as the username and password of a user to be authenticated, and sends them to the RADIUS server.

Users that pass the authentication on the RADIUS server can access the network.

MAC Address Authentication in Local Authentication Mode

When MAC address authentication adopts the local authentication mode, users are authenticated on the local S-switch. You need to configure the local username and password on the S-switch.

- When the MAC-address username type is adopted, the MAC address of an access user is configured as the local username and the password for the authentication. Whether the local username contains delimiter - should be consistent with the format of a username configured on a device; otherwise, MAC address authentication fails.

- When the fixed username type is adopted, the MAC addresses of all the users match the configured local username and password automatically.

6.1.2 MAC Address Authentication Features Supported by the S-switch

Timers for MAC Address Authentication

MAC address authentication is controlled by the following timers:

- Offline-detect timer: specifies the interval for an S-switch to check whether a user goes offline. When a user goes offline, the S-switch immediately notifies the RADIUS server to stop charging the user.
- Quiet timer: specifies the period for a switch to wait to re-authenticate a user that fails in the authentication. During this period, the S-switch does not process the authentication requests of the user.
- Server-timeout timer: specifies the timeout period of the connection between an S-switch and the RADIUS server. During the authentication process, if the connection between an S-switch and a RADIUS server times out, the authentication fails.

Silent MAC Address

After the authentication of a MAC address fails, the MAC address becomes a silent MAC address. During the timeout period of the quiet timer, the S-switch directly discards data packets received from users of this MAC address. The silent MAC address is configured to prevent invalid MAC addresses from being authenticated repeatedly in a short time.

Guest VLAN

When the authentication of a user connected to an interface fails, the interface is added to a guest VLAN if the conditions for validating a guest VLAN are met. The user connected to the interface can access network resources of the guest VLAN. This is an authorization method of enabling users that fail in the authentication to access limited resource of specific VLANs.

6.1.3 Update History

Version	Revision
V200R002C02	This is the first release.

6.2 Configuring MAC Address Authentication

This section describes how to configure MAC address authentication.

[6.2.1 Establishing the Configuration Task](#)

[6.2.2 Configuring MAC Address Authentication on Global MAC Address Authentication](#)

[6.2.3 Configuring MAC Address Authentication on an Interface](#)

[6.2.4 Configuring a MAC Address as a Username for MAC Address Authentication](#)

[6.2.5 Configuring a Fixed Username for a MAC Address Authentication User](#)[6.2.6 \(Optional\)Configuring a Domain Name for a MAC Address Authentication User](#)[6.2.7 \(Optional\)Configuring Timers for MAC Address Authentication](#)[6.2.8 Checking the Configuration](#)

6.2.1 Establishing the Configuration Task

Applicable Environment

MAC address authentication can be configured on an interface before global MAC address authentication is enabled, but MAC address authentication does not take effect on the interface. After global MAC address authentication is enabled, MAC address authentication enabled on the interface takes effect immediately.

NOTE

- If MAC address authentication is enabled on an interface, 802.1x cannot be enabled on the interface; if 802.1x is enabled on an interface, MAC address authentication cannot be enabled on the interface.
- If MAC address authentication is enabled on an interface, VLAN mapping cannot be enabled on the interface; if VLAN mapping is enabled on an interface, MAC address authentication cannot be enabled on the interface.

Pre-configuration Tasks

Before configuring MAC address authentication, complete the following tasks:

- Connecting interfaces and configuring physical parameters for the interfaces to ensure that the physical layer status of the interfaces is Up
- Configuring parameters of the link layer protocol for interfaces and ensuring that the status of the link layer protocol on the interfaces is Up

Data Preparation

To configure MAC address authentication, you need the following data.

No.	Data
1	Number of an interface to be authenticated

6.2.2 Configuring MAC Address Authentication on Global MAC Address Authentication

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **mac-authen** command to enable global MAC address authentication.

----End

6.2.3 Configuring MAC Address Authentication on an Interface

Context

Do as follows on the S-switch in the system view and in the interface view respectively.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **mac-authen interface** { *interface-type interface-number1* [**to** *interface-number2*] } command to enable MAC address authentication on a specified interface.

NOTE

In addition, you can run the **mac-authen** command in the interface view to enable MAC address authentication on the interface.

----End

6.2.4 Configuring a MAC Address as a Username for MAC Address Authentication

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **mac-authen username macaddress** command to configure a MAC address as a username for MAC address authentication.

By default, a MAC address without delimiter - is used as a username for MAC address authentication.

Step 3 (Optional)Run the **mac-authen username macaddress format with-hyphen** command to configure a MAC address with delimiter - as a username for MAC address authentication.

----End

6.2.5 Configuring a Fixed Username for a MAC Address Authentication User

Context

To configure a fixed username for a MAC address authentication user, do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **mac-authen username fixed** command to configure a fixed username for a MAC address authentication user.
- Step 3** Run the **mac-authen username** *username* command to configure a username for MAC address authentication.
- Step 4** Run the **mac-authen password** *password* command to configure a password for MAC address authentication.

----End

6.2.6 (Optional)Configuring a Domain Name for a MAC Address Authentication User

Context

When a user adopts MAC address authentication, you must configure an authentication domain for the user. To configure a domain name for a MAC address authentication user, do as follows on the S-switch.

The configuration is invalid for a user with a fixed username. By default, MAC address authentication without a domain is used, and a username does not contains a domain name.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **mac-authen domain** *isp-name* command to configure a domain name for a MAC address authentication user.

NOTE

Configure an authentication domain for a MAC address authentication user. Check whether there is an available domain before configuring the domain; otherwise, the system prompts that an error occurs.

----End

6.2.7 (Optional)Configuring Timers for MAC Address Authentication

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **mac-authen timer offline-detect** *offline-detect-value* command to configure the value of the offline-detect timer.
- The default value is 300 seconds.

Step 3 Run the **mac-authen timer quiet-period** *quiet-value* command to configure the value of the quiet timer.

The default value is 300 seconds.

The default value is 60 seconds.

Step 4 Run the **mac-authen timer server-timeout** *server-timeout-value* command to configure the value of the server timeout timer.

The default value is 30 seconds.

----End

6.2.8 Checking the Configuration

Prerequisite

All configurations of MAC address authentication are complete.

Procedure

Run the **display mac-authen** command to view the status of MAC address authentication.

----End

Example

Run the **display mac-authen** command to check the configuration results of MAC address authentication. For example:

```
<Quidway> display mac-authen
Mac address authentication is Enabled.
Fixed username: test
Fixed Password: test123
  Offline detect period is 60s
  Quiet period is 65s
  Server response timeout value is 66s
  Guest VLAN reauthenticate period is 30s
  Max online user is 1024
  Current online user is 0
  Current domain: not configured
```

6.3 Configuring Enhanced MAC Address Authentication

This section describes how to configure a guest VLAN and the maximum number of MAC address authentication users attached to an interface of an S-switch.

[6.3.1 Establishing the Configuration Task](#)

[6.3.2 Configuring a Guest VLAN](#)

[6.3.3 Configuring the Maximum Number of MAC Address Authentication Users on an Interface](#)

[6.3.4 Checking the Configuration](#)

6.3.1 Establishing the Configuration Task

Applicable Environment

After the authentication of a user connected to an interface fails, the interface is added to a guest VLAN. The MAC address of the user is added to the MAC address table of the guest VLAN. Thus, the user can access network resources of the guest VLAN.

By configuring the maximum number of MAC address authentication users, you can control users accessing an interface. The number of users accessing an interface of an S-switch reaches a limit value, the S-switch does not trigger MAC address authentication for subsequent users accessing the interface. Therefore, these users cannot access the network normally.

Pre-configuration Tasks

Before configuring enhanced MAC address authentication, complete the following tasks:

- Enabling MAC address authentication
- Creating a VLAN to be configured as a guest VLAN
- Configuring the maximum number of MAC address authentication users to one.

Data Preparation

To configure enhanced MAC address authentication, you need the following data.

No.	Data
1	Number of an interface on a S-switch that performs MAC address authentication
2	ID of a guest VLAN

6.3.2 Configuring a Guest VLAN

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* to enter the Ethernet interface view.
- Step 3** Run the **mac-authen guest-vlan** *vlan-id* [**interface** { *interface-type interface-number1* [**to** *interface-number2*] }] command to configure a guest VLAN on the interface.
- Step 4** (Optional) Run the **mac-authen timer guest-vlan reauthenticate-period** *interval* command to configure the interval for the **S-switch** to re-authenticate users of the guest VLAN.
- Step 5** Run the **quit** command to return to the system view.

----End

6.3.3 Configuring the Maximum Number of MAC Address Authentication Users on an Interface

Context

To set the maximum number of online users on an interface of a S-switch, do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* to enter the Ethernet interface view.
- Step 3** Run the **mac-authen max-user** *user-number* [**interface** { *interface-type interface-number1* [*to interface-number2*] }] command to set the maximum number of MAC address authentication users on the interface.
- Step 4** Run the **quit** command to return to the system view.
- End

6.3.4 Checking the Configuration

Prerequisite

All configurations of enhanced MAC address authentication are complete.

Procedure

Run the **display mac-authen** command to check the configuration of enhanced MAC address authentication.

----End

Example

Run the **display mac-authen** command to check the configuration results of enhanced MAC address authentication.

For example:

```
<Quidway> display mac-authen
Mac address authentication is Enabled.
Fixed username:
Fixed Password: test123
Offline detect period is 60s
Quiet period is 65s
Server response timeout value is 66s
Guest VLAN reauthenticate period is 30s
Max online user is 1024
Current online user is 0
Current domain: not configured
```

6.4 Maintaining MAC Address Authentication

Run the **reset** command in the user view to reset the statistics of MAC address authentication.

6.4.1 Resetting Statistics of MAC Address Authentication

Context



CAUTION

Statistics of MAC address authentication cannot be restored after you clear them. So, confirm the action before you use the command.

Procedure

After confirming the action of resetting the statistics of MAC address authentication, run the **reset mac-authentication statistics** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] }] command in the user view to clear them.

----End

6.5 Configuration Examples

This section provides a configuration example for MAC address authentication.

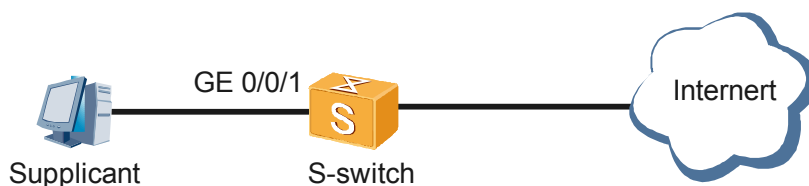
6.5.1 Example for Configuring MAC Address Authentication

6.5.1 Example for Configuring MAC Address Authentication

Networking Requirements

- The administrator of the S-switch wants to perform MAC address authentication on users accessing Ethernet 0/0/1 to control users' access to the Internet.
- Local authentication with a fixed username is adopted; the fixed username is set to huawei; the fixed password is set to huawei. Only users that pass the authentication can access the Internet.

Figure 6-1 Networking diagram for configuring local authentication with a fixed username



Configuration Roadmap

The configuration roadmap is as follows:

- Add a local access user and configure the username and password for the user.
- Configure MAC address authentication on Ethernet 0/0/1.
- Adopt a fixed username for MAC address authentication.
- Enable global MAC address authentication.

NOTE

Configure global MAC address authentication after setting all related parameters. Otherwise, authorized users may fail to access the Internet.

Data Preparation

To complete this configuration, you need the following data:

- Interface for authentication
- Username for authentication
- Password for authentication
- Authentication type

Procedure

Step 1 Add a local access user to an S-switch, and configure the username and password for the user.

```
<Quidway> system-view
[Quidway] aaa
[Quidway-aaa] local-user huawei password simple huawei
[Quidway-aaa] local-user huawei service-type ppp
[Quidway-aaa] quit
```

Step 2 Configure MAC address authentication on Ethernet 0/0/1.

```
[Quidway-aaa] interface Ethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] mac-authen
[Quidway-GigabitEthernet0/0/1] quit
```

Step 3 Adopt a fixed username for MAC address authentication.

```
[Quidway] mac-authen username fixed
[Quidway] mac-authen username huawei
[Quidway] mac-authen password huawei
```

Step 4 Enable global MAC address authentication.

```
[Quidway]] mac-authen
[Quidway] quit
```

----End

Configuration Files

Configuration file of the **S-switch**

```
#
sysname Quidway
#
```

6 MAC Address Authentication Configuration

```
in: not configured
#
interface GigabitEthernet0/0/1
 mac-authen
#
aaa
 local-user huawei password simple huawei
  local-user huawei service-type ppp
 authentication-scheme default
#
  authorization-scheme default
#
 accounting-scheme default
#
  domain default
#
return
```

7 802.1X Configuration

About This Chapter

This chapter describes the basics, methods, and configuration example of 802.1X.

[7.1 Overview of 802.1X](#)

This section describes the basic concepts of 802.1X and the 802.1X functions supported by the S-switch.

[7.2 Configuring 802.1X](#)

This section describes the scenario, procedures, and precautions for configuring 802.1X.

[7.3 Configuration Examples](#)

This section describes a configuration example of 802.1X.

7.1 Overview of 802.1X

This section describes the basic concepts of 802.1X and the 802.1X functions supported by the S-switch.

[7.1.1 Introduction to 802.1X](#)

[7.1.2 802.1X Authentication System](#)

[7.1.3 802.1X Authentication Process](#)

[7.1.4 Implementation of 802.1X on the S-switch](#)

[7.1.5 Logical Relationships Between Configuration Tasks](#)

[7.1.6 Update History](#)

7.1.1 Introduction to 802.1X

The IEEE 802.1X standard, 802.1X in brief, is a port-based network access control protocol. It is put forward based on the IEEE 802.11 standard for wireless local area network (WLAN) access to solve the authentication problem. Later, the 802.1X protocol is applied on the Ethernet as a common access control mechanism on the local area network (LAN) interface to solve problems in terms of authentication and security on the Ethernet.

"Port-based network access control" indicates the authentication and control implemented for access devices on an interface of a LAN access control device. A user device can access LAN resources only after it passes the authentication.

7.1.2 802.1X Authentication System

As shown in [Figure 7-1](#), 802.1X authentication adopts the typical client/server model and involves three entities, that is, the supplicant, authenticator, and the authentication server.

- The supplicant is usually a user terminal installed with the 802.1X client software provided by Huawei or the Windows XP operating system. The supplicant initiates the 802.1X authentication by running the 802.1X client software. The supplicant must support the Extensible Authentication Protocol over LAN (EAPoL).
- The authenticator is usually a network device supporting the 802.1X protocol. The authenticator provides the interface, either physical or logical, for LAN access of the supplicant.
- The authentication server is usually a Remote Authentication Dial-In User Service (RADIUS) server for implementing authentication, authorization, and accounting (AAA). The authentication server stores information such as the user name, password, user VLAN, committed access rate (CAR) parameters, priority, and user access control list (ACL).

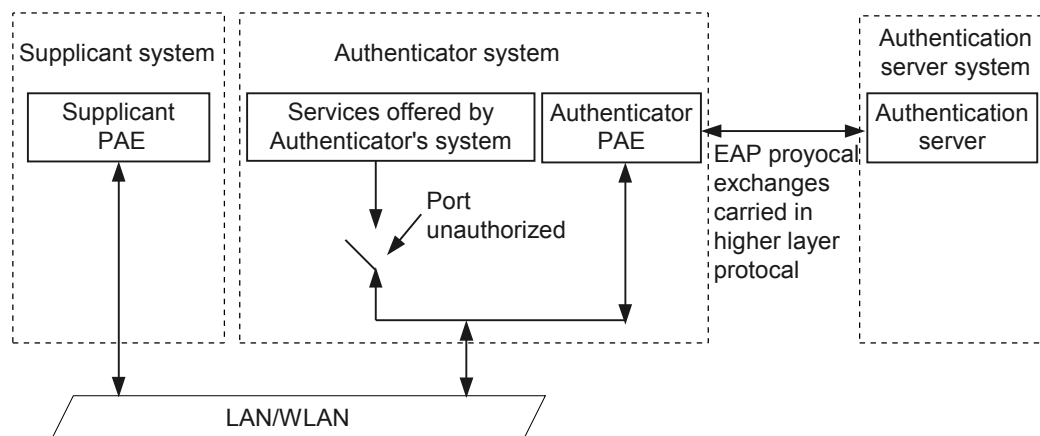
The information exchange between the three entities is as follows:

- The authenticator and the authentication server exchange information through the Extensible Authentication Protocol (EAP).
- The supplicant and the authenticator exchange information through EAPoL defined in the IEEE 802.1X standard.

The authenticator encapsulates authentication data in an EAP packet and then encapsulates the EAP packet in an upper-layer AAA protocol packet such as the RADIUS protocol packet. In

this manner, the authentication data can travel through the complex network to reach the authentication server.

Figure 7-1 802.1X authentication system



The three authentication entities involve the following basic concepts:

1. **PAE**

The Port Access Entity (PAE) performs the algorithm and implements the protocol.

2. **Controlled or uncontrolled interface**

- In authorized mode, a controlled interface can transmit packets in both directions; in unauthorized mode, a controlled interface cannot receive packets from the supplicant.
- An uncontrolled interface can bidirectionally transmit EAPoL protocol packets in either mode to ensure that the supplicant sends and receives packets at any time.

3. **Controlled direction**

In unauthorized mode, you can set an interface to be unidirectionally controlled or bidirectionally controlled.

If an interface is unidirectionally controlled, it can send packets to the supplicant but cannot receive packets from the supplicant.

NOTE

Currently, the S-switch supports only unidirectionally controlled interfaces.

7.1.3 802.1X Authentication Process

The 802.1X authentication can be initiated by either the authenticator or the supplicant.

• 802.1X authentication initiated by the supplicant

The supplicant sends an EAPoL-Start packet to the authenticator through the client software and initiates the authentication.

• 802.1X authentication initiated by the authenticator

On detecting an unauthenticated user accessing the network, the authenticator sends an EAP-Request/Identity packet to the user and initiates the authentication.

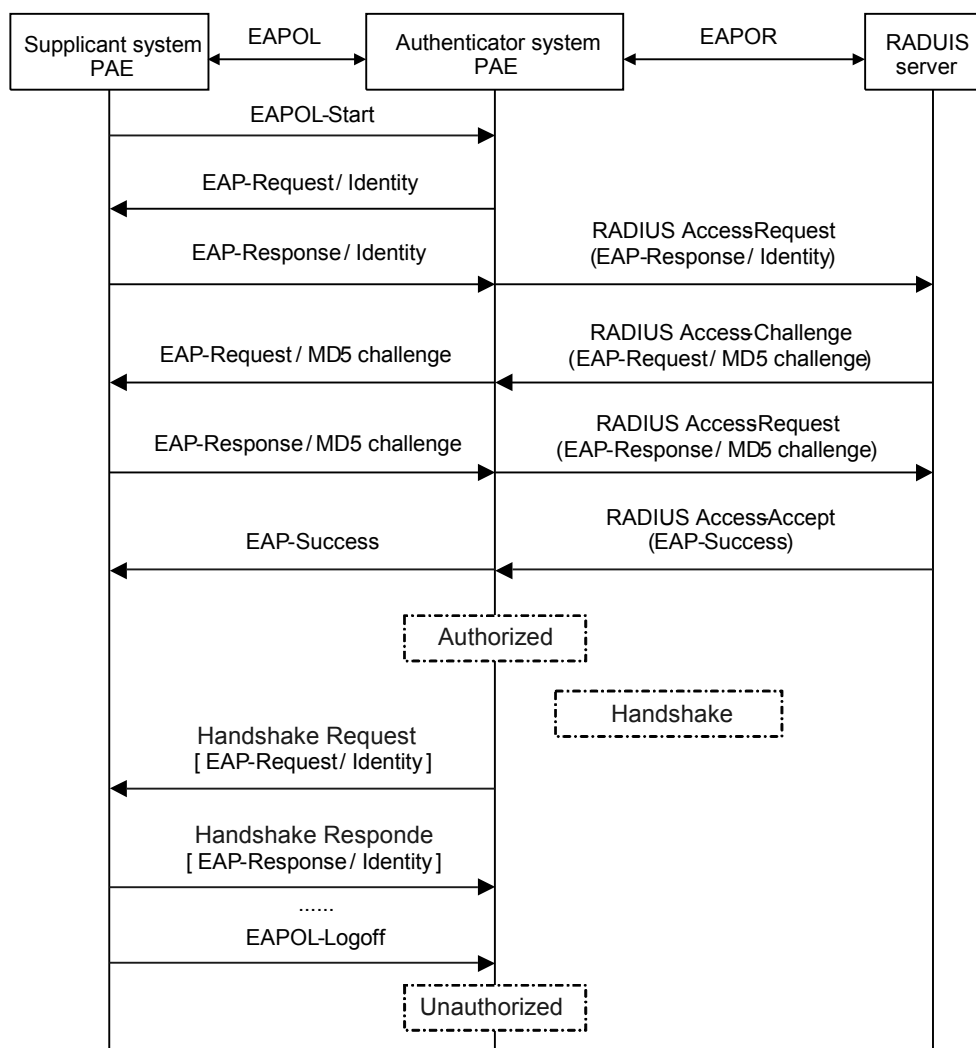
The 802.1X authentication system supports the EAP relay mode and the EAP termination mode to exchange information for user authentication. Take the 802.1X authentication initiated by the supplicant as an example. The authentication processes in preceding modes are as follows:

EAP Relay Mode

The EAP relay mode is defined in the IEEE 802.1X standard. The EAP protocol is borne by an upper-layer AAA protocol, for example EAP over RADIUS, to travel through the complex network and reach the authentication server. In EAP relay mode, the RADIUS server must support EAP attributes, EAP-Message and Message-Authenticator.

Currently, the S-switch supports the EAP-Message Digest 5 (MD5) relay mode. In EAP-MD5 relay mode, the RADIUS server sends an MD5 encryption word in an EAP-Request/MD5 Challenge packet to the supplicant. The supplicant encrypts the password with the MD5 encryption word. **Figure 7-2** shows the authentication process in EAP-MD5 relay mode.

Figure 7-2 802.1X authentication process in EAP-MD5 relay mode



The authentication process is as follows:

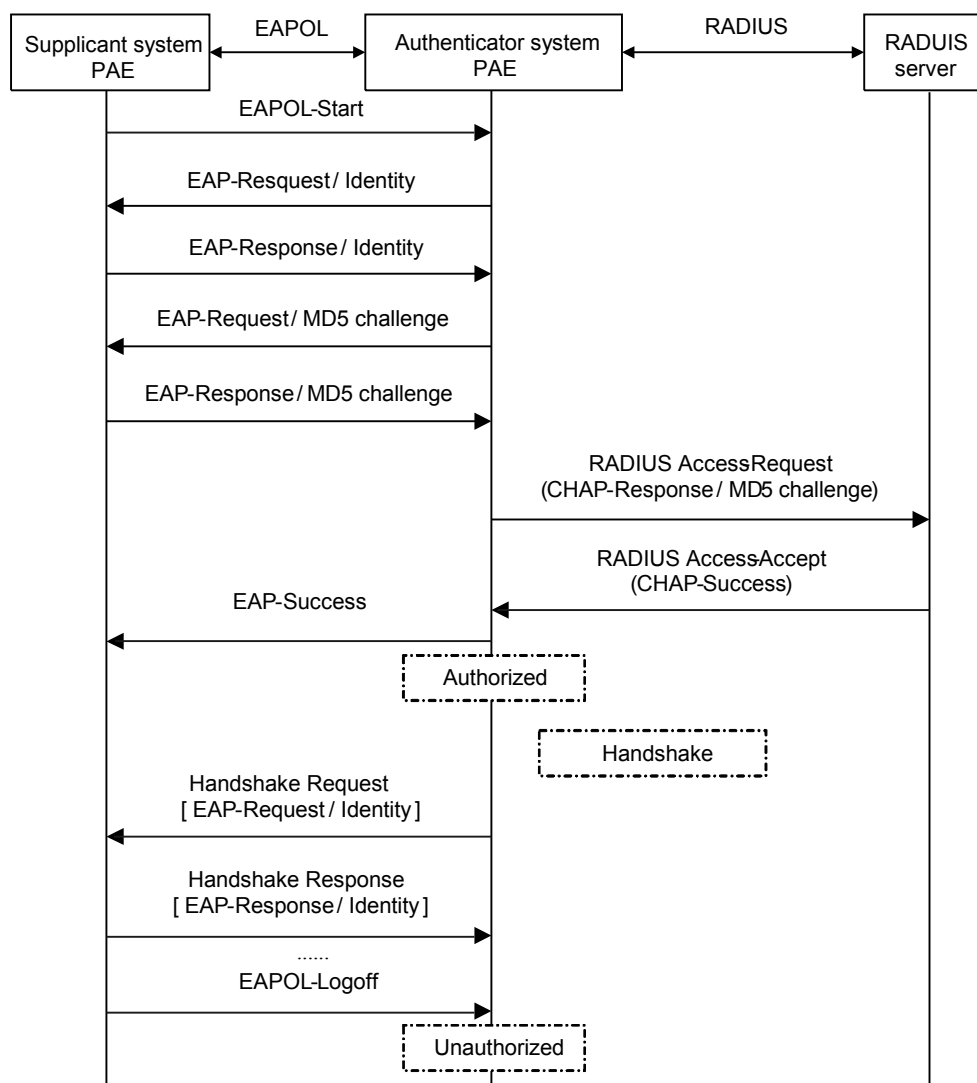
1. The user runs the 802.1X client program, enters the assigned and registered user name and password, and sends an EAPoL-Start packet to the authenticator.

2. After receiving the EAPoL-Start packet, the authenticator returns an EAP-Request/Identity packet, requiring the supplicant to send the entered user name.
3. The supplicant responds with an EAP-Response/Identity packet, carrying the user name to the authenticator. The authenticator receives the EAP-Response/Identity packet, encapsulates the packet into a RADIUS Access-Request packet, and sends it to the authentication server.
4. After receiving the user name from the authenticator, the authentication server searches for the password corresponding to the user name, encrypts the password through a randomly generated encryption word, and at the same time, sends the encryption word in a RADIUS Access-Challenge packet to the authenticator.
5. After receiving the encryption word in the EAP-Request/MD5 Challenge packet from the authenticator, the supplicant encrypts the password with the encryption word and then sends it in an EAP-Response/MD5 Challenge packet to the authentication server through the authenticator.
6. The authentication server compares the password in the RADIUS Access-Request packet from the authenticator with the local password generated through the MD5 algorithm. If the two passwords are the same, the authentication server responds with RADIUS Access-Accept and EAP-Success packets.
7. After the authenticator receives the packets, the interface becomes authorized and the user can access the network through this interface. After the interface becomes authorized, the authenticator periodically sends handshake packets to the supplicant to monitor the online user. By default, the authenticator disconnects a user after sending two handshake packets but receiving no response. In this manner, network resource waste caused by the authenticator's unawareness of abnormal user disconnection is prevented.

EAP Termination Mode

In EAP termination mode, EAP packets are terminated on the authenticator and mapped to RADIUS packets to complete the authentication, authorization, and accounting through the standard RADIUS protocol.

In EAP termination mode, the authenticator and the RADIUS server exchange information through the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). [Figure 7-3](#) takes authentication through CHAP as an example and shows the authentication process in EAP termination mode.

Figure 7-3 802.1X authentication process in EAP termination mode

The difference between the EAP termination mode and the EAP relay mode is: In EAP termination mode, the authenticator randomly generates an encryption word for user password encryption, and then sends the user name, random encryption word, and password encrypted on the supplicant to the RADIUS server for authentication.

7.1.4 Implementation of 802.1X on the S-switch

The S-switch supports port-based access authentication defined in the 802.1X protocol, and extends and optimizes this feature in the following ways to enhance the security and manageability of the system.

- Supporting a physical interface connected to multiple users
- Supporting MAC-based and port-based access control methods

7.1.5 Logical Relationships Between Configuration Tasks

Enabling 802.1X globally and on the interface is a required configuration task; other configuration tasks are optional. There is no strict logical relation between the configuration tasks. You can configure them as required.

7.1.6 Update History

Version	Revision
V100R002C02	This is the first release.

7.2 Configuring 802.1X

This section describes the scenario, procedures, and precautions for configuring 802.1X.

[7.2.1 Establishing the Configuration Task](#)

[7.2.2 Enabling 802.1X Globally and on the Interface](#)

[7.2.3 \(Optional\) Setting the Port Access Control Mode](#)

[7.2.4 \(Optional\) Setting the Port Access Control Method](#)

[7.2.5 \(Optional\) Setting the Maximum Number of Concurrent Access Users](#)

[7.2.6 \(Optional\) Enabling DHCP Trigger](#)

[7.2.7 \(Optional\) Setting the Authentication Method for the 802.1X User](#)

[7.2.8 \(Optional\) Configuring the Guest VLAN](#)

[7.2.9 \(Optional\) Setting the Maximum Number of Times for Sending an Authentication Request](#)

[7.2.10 \(Optional\) Setting the Timer Parameters](#)

[7.2.11 \(Optional\) Enabling the Quiet-Period Timer](#)

[7.2.12 \(Optional\) Enabling the Handshake-Period Timer](#)

[7.2.13 Checking the Configuration](#)

7.2.1 Establishing the Configuration Task

Applicable Environment

You can configure 802.1X to implement port-based network access control, that is, to authenticate and control access devices on an interface of a LAN access control device.

Pre-configuration Tasks

The 802.1X protocol provides only an implementation scheme for user identity authentication. To complete the user identity authentication, you need to select the RADIUS or local authentication method. Before configuring 802.1X, complete the following tasks:

- Configuring the Internet Service Provider (ISP) authentication domain and AAA scheme, that is, RADIUS or local authentication scheme, for the 802.1X user
- Configuring the user name and password on the RADIUS server if RADIUS authentication is selected.
- Adding the user name and password manually on the S-switch if local authentication is selected.

Data Preparation

None.

7.2.2 Enabling 802.1X Globally and on the Interface

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x** command to enable 802.1X globally.

By default, 802.1X is disabled globally and on an interface.



NOTE

To add the interface to the dynamic VLAN delivered by the server, you also need to run the **port hybrid untagged vlan** command in the interface view. In this manner, frames from the VLAN can pass through the interface in untagged mode.

Step 3 Run the **dot1x interface interface-type interface-number1 [to interface-number2]** command to enable 802.1X on the specified interface. Or run the **interface interface-type interface-number** command to enter the interface view and then run the **dot1x** command to enable 802.1X on the interface.

----End

7.2.3 (Optional) Setting the Port Access Control Mode

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x port-control { auto | authorized-force | unauthorized-force } [interface interface-type interface-number1 [to interface-number2]]** command to set the port access control mode.

By default, the port access control mode is **auto**.

----End

7.2.4 (Optional) Setting the Port Access Control Method

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x port-method { mac | port } [interface { interface-type interface-number1 [to interface-number2] }** command to set the port access control method.

By default, the port access control method is **mac**.

----End

7.2.5 (Optional) Setting the Maximum Number of Concurrent Access Users

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x max-user user-number [interface { interface-type interface-number1 [to interface-number2] }** command to set the maximum number of concurrent access users on the interface.

By default, an interface allows up to 256 concurrent access users.

----End

7.2.6 (Optional) Enabling DHCP Trigger

Context

Do as follows on the S-switch.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
dot1x dhcp-trigger

Dynamic Host Configuration Protocol (DHCP) trigger is enabled for user authentication.

By default, DHCP trigger is disabled.

----End

7.2.7 (Optional) Setting the Authentication Method for the 802.1X User

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x authentication-method { chap | eap | pap }** command to set the authentication method for the 802.1X user.

By default, the authentication method of an 802.1X user is **chap**.

----End

7.2.8 (Optional) Configuring the Guest VLAN

Context

Before configuring the guest VLAN, complete the following tasks:

- Enabling 802.1X
- Setting the maximum number of concurrent access users to 1 on the interface
- Setting the port access control mode to **auto** on the interface
- Creating a VLAN to be configured as the guest VLAN

After the preceding configurations, do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x guest-vlan vlan-id [interface { interface-type interface-number1 [to interface-number2] }** command to configure the guest VLAN on the interface. Or run the **interface interface-type interface-number1** command to enter the interface view and then run the **dot1x guest-vlan vlan-id** command to configure the guest VLAN on the interface.

By default, no guest VLAN is configured on an interface.

NOTE

The configured guest VLAN takes effect only when the maximum number of concurrent access users on the interface is 1. If the maximum number of concurrent access users on interface is not 1, you can configure the guest VLAN, whereas the configured guest VLAN does not take effect.

Assign different VLAN IDs to the voice VLAN, default VLAN, and 802.X guest VLAN on the interface to ensure normal services.

----End

7.2.9 (Optional) Setting the Maximum Number of Times for Sending an Authentication Request

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x retry max-retry-value** command to set the maximum number of times for sending an authentication request to the access user.

By default, the S-switch can send an authentication request to an access user twice.

----End

7.2.10 (Optional) Setting the Timer Parameters

Context

Do as follows on the S-switch

.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x timer { client-timeout client-timeout-value | handshake-period handshake-period-value | quiet-period quiet-period-value | reauthenticate-period reauthenticate-period-value | server-timeout server-timeout-value | tx-period tx-period-value }** command to set the timer parameters.

By default, the settings of the timers are as follows:

- The timeout period of the response from the client is 30s.
- The interval for sending handshake packets is 15s.
- The quiet period of a user failing the authentication is 60s.
- The authentication interval is 3600s.
- The timeout period of the response from the server is 30s.
- The interval for sending authentication requests is 30s.

----End

7.2.11 (Optional) Enabling the Quiet-Period Timer

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x quiet-period** command to enable the quiet-period timer.

By default, the quiet-period timer is disabled.

----End

7.2.12 (Optional) Enabling the Handshake-Period Timer

Context

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dot1x handshake** command to enable the handshake-period timer.

By default, the handshake-period timer is enabled.

----End

7.2.13 Checking the Configuration

Procedure

Using the **display dot1x** command, you can view information about the sessions and statistics about 802.1X.

----End

Example

Run the **display dot1x** command, you can view that the 802.1x is enabled globally and on interface.

```
[Quidway] display dot1x
Global 802.1x is Enabled
CHAP authentication is Enabled
DHCP-trigger is Disabled
Handshake is Enabled
Quiet function is disabled
Configuration:Handshake Period    15s    Reauthen Period    3600s
                  Client Timeout    30s    Server Timeout      30s
                  Quiet Period      60s
```

Total maximum 802.1x user resource number is 1024

Total current used 802.1x resource number is 3

```
Ethernet0/0/1 current state : UP
802.1x protocol is Enabled
Port control type is Auto
Authentication method is MAC-based
Reauthentication is enabled
Max online user is 256
Current online user is 1
```

Guest VLAN is disabled

Authentication Success:	0	Failure:	0
EAPOL Packets: TX	: 0	RX	: 0

7.3 Configuration Examples

This section describes a configuration example of 802.1X.

Context

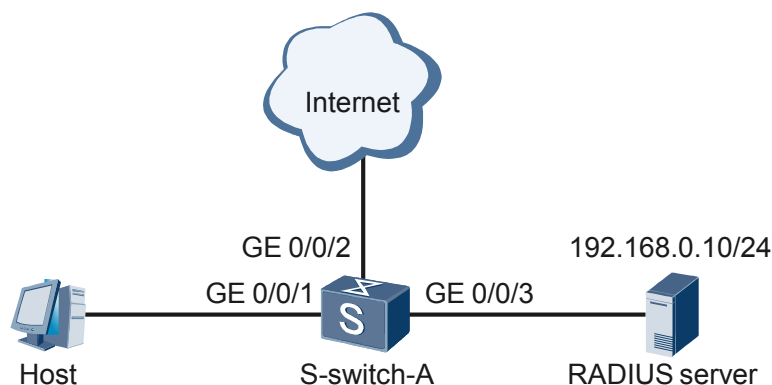
7.3.1 Example for Configuring 802.1X

7.3.1 Example for Configuring 802.1X

Networking Requirements

- The user must be authenticated on an interface of the S-switch before accessing the Internet; the MAC-based access control method is adopted.
- RADIUS authentication is performed for the user. If the RADIUS server does not respond, local authentication is performed for the user. The user name of the local 802.1X access user is **localuser** and the password is **localpass**.
- Configure the S-switch to remove the domain name from the user name before sending it to the RADIUS server.

Figure 7-4 Authentication through 802.1X and RADIUS



Configuration Roadmap

The configuration roadmap is as follows:

- Create a VLANIF interface and assign an IP address to it.
- Create a local access user and configure the user name and password for the user.
- Configure the domain for local authentication.
- Configure the domain for RADIUS authentication.

- Create a RADIUS scheme.
- Enable 802.1X authentication on the specified interface.
- Enable 802.1X authentication globally.

 **NOTE**

Perform this step after setting all related parameters. Otherwise, authorized users may fail to access the Internet.

Data Preparation

To configure 802.1X, you need the following data.

- IP address of the VLANIF interface
- IP address of the RADIUS server
- Interface for authentication
- User name for authentication
- Domain for authentication
- Password for authentication
- Service type

Procedure

Step 1 Create a VLANIF interface and assign an IP address to it on the S-switch.

```
<Quidway> system-view
[Quidway] vlan 10
[Quidway-vlan10] port GigabitEthernet 0/0/1
[Quidway-vlan10] quit
[Quidway] interface vlanif 10
[Quidway-Vlanif10] ip address 10.10.1.1 255.255.255.0
[Quidway-Vlanif10] quit
[Quidway] vlan 100
[Quidway-vlan100] port GigabitEthernet 0/0/2
[Quidway-vlan100] port GigabitEthernet 0/0/3
[Quidway-Vlan100] quit
[Quidway] interface vlanif 100
[Quidway-Vlanif100] ip address 192.168.0.1 255.255.255.0
[Quidway-Vlanif100] quit
```

Step 2 Create a local access user, and configure the user name and password for the user.

```
<Quidway> system-view
[Quidway] aaa
[Quidway-aaa] local-user localuser@test password simple localpass
[Quidway-aaa] local-user localuser@test service-type ppp
[Quidway-aaa] authentication-scheme test
[Quidway-aaa-authen-test] authentication-mode local
[Quidway-aaa-authen-test] quit
[Quidway-aaa] authorization-scheme test
[Quidway-aaa-author-test] authorization-mode none
[Quidway-aaa-author-test] quit
```

Step 3 Configure the domain for local authentication.

```
[Quidway-aaa] domain test
[Quidway-aaa-domain-test] authentication-scheme test
[Quidway-aaa-domain-test] authorization-scheme test
[Quidway-aaa-domain-test] quit
[Quidway-aaa] authentication-scheme server
[Quidway-aaa-authen-server] authentication-mode radius
[Quidway-aaa-authen-server] quit
[Quidway-aaa] accounting-scheme account
```

```
[Quidway-aaa-accounting-account] accounting-mode radius
[Quidway-aaa-accounting-account] quit
```

Step 4 Create a RADIUS template.

```
<Quidway> system-view
[Quidway] radius-server template account
[Quidway-radius-account] radius-server authentication 192.168.0.10 1000
[Quidway-radius-account] radius-server accounting 192.168.0.10 1001
[Quidway-radius-account] radius-server shared-key 3300
```

Step 5 Configure the domain for RADIUS authentication.

```
[Quidway-aaa] domain remote
[Quidway-aaa-domain-remote] authentication-scheme server
[Quidway-aaa-domain-remote] accounting-scheme account
[Quidway-aaa-domain-remote] radius-server account
```

Step 6 Enable 802.1X authentication on GigabitEthernet 0/0/1.

```
[Quidway] interface GigabitEthernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dot1x maxuser 1
[Quidway-GigabitEthernet0/0/1] dot1x
[Quidway-GigabitEthernet0/0/1] quit
```

Step 7 Enable 802.1X authentication globally.

```
[Quidway] dot1x
```

Step 8 Check the configuration.

```
[Quidway] display dot1x interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
  802.1x protocol is Enabled
  The port is an authenticator
  Port control type is Auto
  Authentication method is Port-based
  Reauthentication is disabled
  Max online user is 1
  Current online user is 1
  Guest VLAN is disabled
  Dynamic VLAN: 4000 Alias: VLAN 4000

Authentication Success: 2          Failure: 0
EAPOL Packets: TX      : 45        RX      : 26
Sent      EAPOL Request/Identity Packets : 21
          EAPOL Request/Challenge Packets : 2
          Multicast Trigger Packets       : 0
          DHCP Trigger Packets            : 0
          EAPOL Success Packets           : 21
          EAPOL Failure Packets           : 1
Received  EAPOL Start Packets            : 2
          EAPOL LogOff Packets            : 1
          EAPOL Response/Identity Packets : 21
          EAPOL Response/Challenge Packets: 2

Index  MAC/VLAN      UserOnlineTime  UserName
12     0001-0001-0002/4000 2008-01-01 08:20:35 localuser@test
Controlled User(s) amount to 1
```

----End

Configuration Files

Configuration files of the S-switch

```
#
sysname Quidway
#
dot1x
#
vlan 10
port GigabitEthernet0/0/1
```

```
#
interface vlanif 10
 ip address 10.10.1.1 255.255.255.0
#
vlan 100
 port GigabitEthernet 0/0/2
 port GigabitEthernet 0/0/3
#
interface vlanif 100
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 dot1x maxuser 1
 dot1x
#
aaa
 local-user localuser@test password simple localpass
 local-user localuser@test service-type ppp
 authentication-scheme default
 authentication-scheme server
   authentication-mode radius
 authentication-scheme test
#
 authorization-scheme default
   authorization-mode none
 authorization-scheme test
   authorization-mode none
#
 accounting-scheme default
 accounting-scheme account
   accounting-mode radius
#
 domain default
 domain remote
   authentication-scheme server
   accounting-scheme account
   radius-server account
 domain test
   authentication-scheme test
   authorization-scheme test
#
return
```