

# Security Configuration

---

1. Configuring AAA
  2. Configuring RADIUS
  3. Configuring TACACS+
  4. Configuring Global IP-MAC Binding
  5. Configuring Password Policy
  6. Configuring Port Security
  7. Configuring Storm Control
  8. Configuring SSH
  9. Configuring CPU Protection
  10. Configuring DHCP Snooping
  11. Configuring DHCPv6 Snooping
  12. Configuring ARP Check
  13. Configuring Dynamic ARP Inspection
  14. Configuring IP Source Guard
  15. Configuring DoS Protection
  16. Configuring PPPoE Intermediate Agent
-

# 1 Configuring AAA

## 1.1 Overview

Authentication, authorization, and accounting (AAA) provides a unified framework for configuring the authentication, authorization, and accounting services. Orion Alpha A28X Networks devices support the AAA application.

AAA provides the following services in a modular way:

**Authentication:** Refers to the verification of user identities for network access and network services. Authentication is classified into local authentication and authentication through Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access Control System+ (TACACS+).

**Authorization:** Refers to the granting of specific network services to users according to a series of defined attribute-value (AV) pairs. The pairs describe what operations users are authorized to perform. AV pairs are stored on network access servers (NASs) or remote authentication servers.

**Accounting:** Refers to the tracking of the resource consumption of users. When accounting is enabled, NASs collect statistics on the network resource usage of users and send them in AV pairs to authentication servers. The records will be stored on authentication servers, and can be read and analyzed by dedicated software to realize the accounting, statistics, and tracking of network resource usage.

AAA is the most fundamental method of access control. Orion Alpha A28X Networks also provides other simple access control functions, such as local username authentication and online password authentication. Compared to them, AAA offers higher level of network security.

AAA has the following advantages:

- Robust flexibility and controllability
- Scalability
- Standards-compliant authentication
- Multiple standby systems

## 1.2 Applications

| Application  | Description   |
|--|---|
| <a href="#">Configuring AAA in a Single-Domain Environment</a> | AAA is performed for all the users in one domain.                               |
| <a href="#">Configuring AAA in a Multi-Domain Environment</a>  | AAA is performed for the users in different domains by using different methods. |

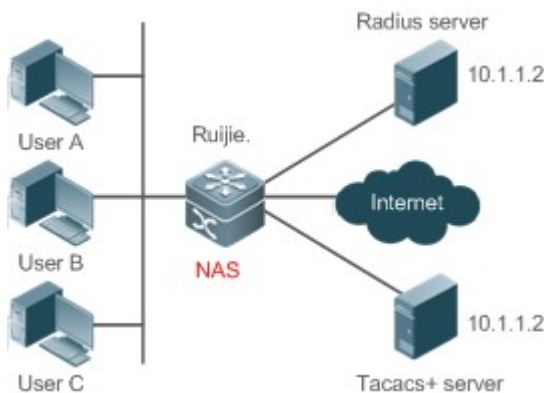
## 1.2.1 Configuring AAA in a Single-Domain Environment

### Scenario

In the network scenario shown in Figure 1-1, the following application requirements must be satisfied to improve the security management on the NAS:

1. To facilitate account management and avoid information disclosure, each administrator has an individual account with different username and password.
2. Users must pass identity authentication before accessing the NAS. The authentication can be in local or centralized mode. It is recommended to combine the two modes, with centralized mode as active and local mode as standby. As a result, users must undergo authentication by the RADIUS server first. If the RADIUS server does not respond, it turns to local authentication.
3. During the authentication process, users can be classified and limited to access different NASs.
4. Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
5. The AAA records of users are stored on servers and can be viewed and referenced for auditing. (The TACACS+ server in this example performs the accounting.)

Figure 1-1



|                |   |
|----------------|---|
| <b>Remarks</b> | <p>User A, User B, and User C are connected to the NAS in wired or wireless way.</p> <p>The NAS is an access or convergence switch.</p> <p>The RADIUS server can be the Windows 2000/2003 Server (IAS), UNIX system component, and dedicated server software provided by a vendor.</p> <p>The TACACS+ server can be the dedicated server software provided by a vendor.</p> |
|----------------|---|

### Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Configure the authentication service on the NAS.
- Configure the authorization service on the NAS.

- Configure the accounting service on the NAS.

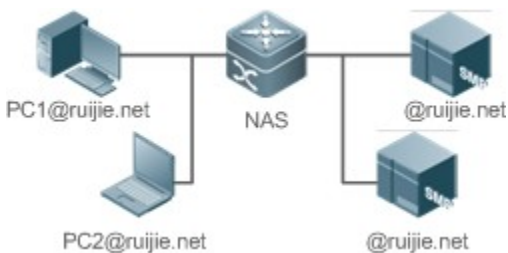
## 1.2.2 Configuring AAA in a Multi-Domain Environment

### Scenario

Configure the domain-based AAA service on the NAS.

- A user can log in by entering the username PC1@Orion Alpha A28X.net or PC2@Orion Alpha A28X.com.cn and correct password on an 802.1X client.
- Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
- The AAA records of users are stored on servers and can be viewed and referenced for auditing.

Figure 1-2



|                |  |
|----------------|--|
| <b>Remarks</b> | <p>The clients with the usernames <b>PC1@Orion Alpha A28X.net</b> and <b>PC2@Orion Alpha A28X.com.cn</b> are connected to the NAS in wired or wireless way.</p> <p>The NAS is an access or convergence switch.</p> <p>The Security Accounts Manager (SAM) server is a universal RADIUS server provided by Orion Alpha A28X Networks.</p> |
|----------------|--|

### Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Define an AAA method list on the NAS.
- Enable domain-based AAA on the NAS.
- Create domains and AV sets on the NAS.

## 1.3 Features

### Basic Concepts

#### Local Authentication and Remote Server Authentication

Local authentication is the process where the entered passwords are verified by the database on the NAS.

Remote server authentication is the process where the entered passwords are checked by the database on a remote server. It is mainly implemented by the RADIUS server and TACACS+ server.

#### Method List

AAA is implemented using different security methods. A method list defines a method implementation sequence. The method list can contain one or more security protocols so that a standby method can take over the AAA service when the first method fails. On Orion Alpha A28X devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection process continues until a security method responds or all the security methods in the list are tried out. Authentication fails if no method in the list responds.

A method list contains a series of security methods that will be queried in sequence to verify user identities. It allows you to define one or more security protocols used for authentication, so that the standby authentication method takes over services when the active security method fails. On Orion Alpha A28X devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection process continues until a method responds or all the methods in the method list are tried out. Authentication fails if no method in the list responds.

- The next authentication method proceeds on Orion Alpha A28X devices only when the current method does not respond. When a method denies user access, the authentication process ends without trying other methods.

Figure 1-3

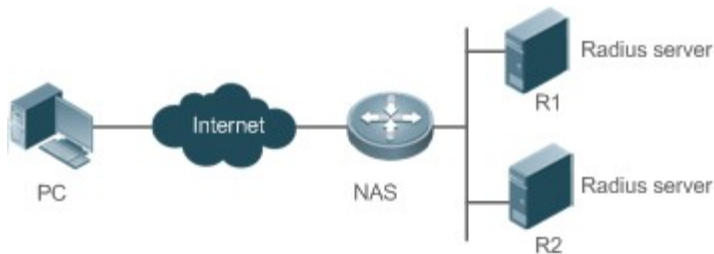


Figure 1-3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

Assume that the system administrator defines a method list, where the NAS selects R1 and R2 in sequence to obtain user identity information and then accesses the local username database on the server. For example, when a remote PC user initiates dial-up access, the NAS first queries the user's identity on R1. When the authentication on R1 is completed, R1 returns an Accept response to the NAS. Then the user is permitted to access the Internet. If R1 returns a Reject response, the user is denied Internet access and the connection is terminated. If R1 does not respond, the NAS considers that the R1 method times out and continues to query the user's identity on R2. This process continues as the NAS keeps trying the remaining authentication methods, until the user request is authenticated, rejected, or terminated. If all the authentication methods are responded with Timeout, authentication fails and the connection will be terminated.

- The Reject response is different from the Timeout response. The Reject response indicates that the user does not meet the criteria of the available authentication database and therefore fails in authentication, and the Internet access request is denied. The Timeout response indicates that the authentication server fails to respond to the identity query. When detecting a timeout event, the AAA service proceeds to the next method in the list to continue the authentication process.

- 
- This document describes how to configure AAA on the RADIUS server. For details about the configuration on the TACACS+ server, see the *Configuring TACACS+*.
- 

## ↳ AAA Server Group

You can define an AAA server group to include one or more servers of the same type. If the server group is referenced by a method list, the NAS preferentially sends requests to the servers in the referenced server group when the method list is used to implement AAA.

## Overview

---

| Feature                            | Description  |
|------------------------------------|--|
| <a href="#">AAA Authentication</a> | Verifies whether users can access the Internet.                                      |
| <a href="#">AAA Authorization</a>  | Determines what services or permissions users can enjoy.                             |
| <a href="#">AAA Accounting</a>     | Records the network resource usage of users.   |
| <a href="#">Multi-Domain AAA</a>   | Creates domain-specific AAA schemes for 802.1X stations (STAs) in different domains. |

### 1.3.1 AAA Authentication

Authentication, authorization, and accounting are three independent services. The authentication service verifies whether users can access the Internet. During authentication, the username, password, and other user information are exchanged between devices to complete users' access or service requests. You can use only the authentication service of AAA.

- 
- To configure AAA authentication, you need to first configure an authentication method list. Applications perform authentication according to the method list. The method list defines the types of authentication and the sequence in which they are performed. Authentication methods are implemented by specified applications. The only exception is the default method list. All applications use the default method list if no method list is configured.
- 

#### ↳ AAA Authentication Scheme

- No authentication (**none**)

The identity of trusted users is not checked. Normally, the no-authentication (None) method is not used.

- Local authentication (**local**)

Authentication is performed on the NAS, which is configured with user information (including usernames, passwords, and AV pairs). Before local authentication is enabled, run the **username password/secret** command to create a local user database.

- Remote server group authentication (**group**)

Authentication is performed jointly by the NAS and a remote server group through RADIUS or TACACS+. A server group consists of one or more servers of the same type. User information is managed centrally on a remote server, thus realizing multi-device centralized and unified authentication with high capacity and reliability. You can configure local authentication as standby to avoid authentication failures when all the servers in the server group fail.

#### ↳ AAA Authentication Types

Orion Alpha A28X products support the following authentication types:

---

- Login authentication

Users log in to the command line interface (CLI) of the NAS for authentication through Secure Shell (SSH), Telnet, and File Transfer Protocol (FTP).

- Enable authentication

After users log in to the CLI of the NAS, the users must be authenticated before CLI permission update. This process is called Enable authentication (in Privileged EXEC mode).

- Dot1X (IEEE802.1X) authentication

Dot1X (IEEE802.1X) authentication is performed for users that initiate dial-up access through IEEE802.1X.

- Web (second generation portal) authentication

Web authentication is performed by the second generation portal server.

## Related Configuration

### ↳ Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

### ↳ Configuring an AAA Authentication Scheme

By default, no AAA authentication scheme is configured.

Before you configure an AAA authentication scheme, determine whether to use local authentication or remote server authentication. If the latter is to be implemented, configure a RADIUS or TACACS+ server in advance. If local authentication is selected, configure the local user database information on the NAS.

### ↳ Configuring an AAA Authentication Method List

By default, no AAA authentication method list is configured.

Determine the access mode to be configured in advance. Then configure authentication methods according to the access mode.

## 1.3.2 AAA Authorization

AAA authorization allows administrators to control the services or permissions of users. After AAA authorization is enabled, the NAS configures the sessions of users according to the user configuration files stored on the NAS or servers. After authorization, users can use only the services or have only the permissions permitted by the configuration files.

### ↳ AAA Authorization Scheme

- Direct authorization (**none**)

Direct authorization is intended for highly trusted users, who are assigned with the default permissions specified by the NAS.

- Local authorization (**local**)

Local authorization is performed on the NAS, which authorizes users according to the AV pairs configured for local users.

---

- Remote server-group authorization (**group**)

Authorization is performed jointly by the NAS and a remote server group. You can configure local or direct authorization as standby to avoid authorization failures when all the servers in the server group fail.

### ↳ AAA Authorization Types

- EXEC authorization

After users log in to the CLI of the NAS, the users are assigned with permission levels (0 to 15).

- Config-commands authorization

Users are assigned with the permissions to run specific commands in configuration modes (including the global configuration mode and sub-modes).

- Console authorization

After users log in through consoles, the users are authorized to run commands.

- Command authorization

Authorize users with commands after login to the CLI of the NAS.

- Network authorization

After users access the Internet, the users are authorized to use the specific session services. For example, after users access the Internet through PPP and Serial Line Internet Protocol (SLIP), the users are authorized to use the data service, bandwidth, and timeout service.

## Related Configuration

### ↳ Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

### ↳ Configuring an AAA Authorization Scheme

By default, no AAA authorization scheme is configured.

Before you configure an AAA authorization scheme, determine whether to use local authorization or remote server-group authorization. If remote server-group authorization needs to be implemented, configure a RADIUS or TACACS+ server in advance. If local authorization needs to be implemented, configure the local user database information on the NAS.

### ↳ Configuring an AAA Authorization Method List

By default, no AAA authorization method list is configured.

Determine the access mode to be configured in advance. Then configure authorization methods according to the access mode.

---



### 1.3.3 AAA Accounting

In AAA, accounting is an independent process of the same level as authentication and authorization. During the accounting process, start-accounting, update-accounting, and end-accounting requests are sent to the configured accounting server, which records the network resource usage of users and performs accounting, audit, and tracking of users' activities.

In AAA configuration, accounting scheme configuration is optional.

#### ↳ AAA Accounting Schemes

- No accounting (**none**)

Accounting is not performed on users.

- Local accounting (**local**)

Accounting is completed on the NAS, which collects statistics on and limits the number of local user connections. Billing is not performed.

- Remote server-group accounting (**group**)

Accounting is performed jointly by the NAS and a remote server group. You can configure local accounting as standby to avoid accounting failures when all the servers in the server group fail.

#### ↳ AAA Accounting Types

- EXEC accounting

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

- Command accounting

Records are kept on the commands that users run on the CLI of the NAS.

- Network accounting

Records are kept on the sessions that users set up after completing 802.1X and Web authentication to access the Internet.

### Related Configuration

#### ↳ Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

#### ↳ Configuring an AAA Accounting Scheme

By default, no AAA accounting method is configured.

Before you configure an AAA accounting scheme, determine whether to use local accounting or remote server-group accounting. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. If local accounting needs to be implemented, configure the local user database information on the NAS.

#### ↳ Configuring an AAA Accounting Method List

By default, no AAA accounting method list is configured.

Determine the access mode to be configured in advance. Then configure accounting methods according to the access mode.

### 1.3.4 Multi-Domain AAA

In a multi-domain environment, the NAS can provide the AAA services to users in different domains. The user AVs (such as usernames and passwords, service types, and permissions) may vary with different domains. It is necessary to configure domains to differentiate the user AVs in different domains and configure an AV set (including an AAA service method list, for example, RADIUS) for each domain.

Our products support the following username formats:

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

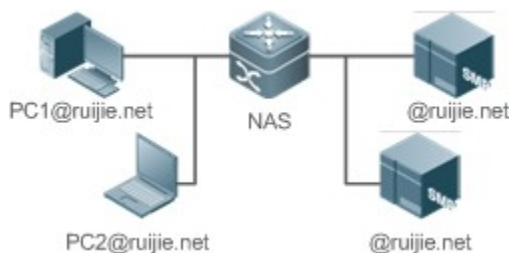
The fourth format (userid) does not contain a domain name, and it is considered to use the **default** domain name.

The NAS provides the domain-based AAA service based on the following principles:

- Resolves the domain name carried by a user.
  - Searches for the user domain according to the domain name.
  - Searches for the corresponding AAA method list name according to the domain configuration information on the NAS.
  - Searches for the corresponding method list according to the method list name.
  - Provides the AAA services based on the method list.
- 
- If any of the preceding procedures fails, the AAA services cannot be provided.

Figure 1-4 shows the typical multi-domain topology.

Figure 1-4



#### Related Configuration

##### ↳ Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

### ↘ [Configuring an AAA Method List](#)

By default, no AAA method list is configured.

For details, see section 5.2.1, section 5.2.2, and section 5.2.3.

### ↘ [Enabling the Domain-Based AAA Service](#)

By default, the domain-based AAA service is disabled.

To enable the domain-based AAA service, run the **aaa domain enable** command.

### ↘ [Creating a Domain](#)

By default, no domain is configured.

To configure a domain, run the **aaa domain domain-name** command.

### ↘ [Configuring an AV Set for a Domain](#)

By default, no domain AV set is configured.

A domain AV set contains the following elements: AAA method lists, the maximum number of online users, whether to remove the domain name from the username, and whether the domain name takes effect.

### ↘ [Displaying Domain Configuration](#)

To display domain configuration, run the **show aaa domain** command.

- The system supports a maximum of 32 domains.

## 1.4 Configuration

| Configuration                                  | Description and Command   |  |
|--|---|--|
| <a href="#">Configuring AAA Authentication</a> | • Mandatory if user identities need to be verified.                             |  |
|  | <b>aaa new-model</b>  | Enables AAA.   |
|  | <b>aaa authentication login</b>   | Defines a method list of login authentication.       |
|  | <b>aaa authentication enable</b>  | Defines a method list of Enable authentication.      |
|  |   |  |
|  | <b>aaa local authentication attempts</b>  | Sets the maximum number of login attempts.           |
|  | <b>aaa local authentication lockout-time</b>                                    | Sets the maximum lockout time after a login failure. |
| <a href="#">Configuring AAA Authorization</a>  | • Mandatory if different permissions and services need to be assigned to users. |  |
|  | <b>aaa new-model</b>  | Enables AAA.   |
|  | <b>aaa authorization exec</b>   | Defines a method list of EXEC authorization.         |

| Configuration  | Description and Command  |  |
|--|--|--|
|  | <b>aaa authorization commands</b>  | Defines a method list of command authorization.                  |
|  | <b>aaa authorization network</b>   | Configures a method list of network authorization.               |
|  | <b>authorization exec</b>  | Applies EXEC authorization methods to a specified VTY line.      |
|  | <b>authorization commands</b>  | Applies command authorization methods to a specified VTY line.   |
| <a href="#">Configuring AAA Accounting</a>               | <ul style="list-style-type: none"> <li>Mandatory if accounting, statistics, and tracking need to be performed on the network resource usage of users.</li> </ul> |  |
|  | <b>aaa new-model</b>   | Enables AAA.   |
|  | <b>aaa accounting exec</b>   | Defines a method list of EXEC accounting.                        |
|  | <b>aaa accounting commands</b>   | Defines a method list of command accounting.                     |
|  | <b>aaa accounting network</b>  | Defines a method list of network accounting.                     |
|  | <b>accounting exec</b>   | Applies EXEC accounting methods to a specified VTY line.         |
|  | <b>accounting commands</b>   | Applies command accounting methods to a specified VTY line.      |
|  | <b>aaa accounting update</b>   | Enables accounting update.                                       |
| <b>aaa accounting update periodic</b>                    | Configures the accounting update interval.   |  |
| <a href="#">Configuring an AAA Server Group</a>          | <ul style="list-style-type: none"> <li>Recommended if a server group needs to be configured to handle AAA through different servers in the group.</li> </ul>     |  |
|  | <b>aaa group server</b>  | Creates a user-defined AAA server group.                         |
|  | <b>server</b>  | Adds an AAA server group member.                                 |
| <a href="#">Configuring the Domain-Based AAA Service</a> | <ul style="list-style-type: none"> <li>Mandatory if AAA management of 802.1X access STAs needs to be performed according to domains.</li> </ul>                  |  |
|  | <b>aaa new-model</b>   | Enables AAA.   |
|  | <b>aaa domain enable</b>   | Enables the domain-based AAA service.                            |
|  | <b>aaa domain</b>  | Creates a domain and enters domain configuration mode.           |
|  | <b>authentication dot1x</b>  | Associates the domain with an 802.1X authentication method list. |
| <b>accounting network</b>                                | Associates the domain with a network accounting method list.   |  |

| Configuration | Description and Command      |   |
|---------------|------------------------------|---|
|               | <b>authorization network</b> | Associates the domain with a network authorization method list. |
|               | <b>state</b>                 | Configures the domain status.                                   |
|               | <b>username-format</b>       | Configures whether to contain the domain name in usernames.     |
|               | <b>access-limit</b>          | Configures the maximum number of domain users.                  |

## 1.4.1 Configuring AAA Authentication

### Configuration Effect

Verify whether users are able to obtain access permission.

### Notes

- If an authentication scheme contains multiple authentication methods, these methods are executed according to the configured sequence.
- The next authentication method is executed only when the current method does not respond. If the current method fails, the next method will be not tried.
- When the **none** method is used, users can get access even when no authentication method gets response. Therefore, the **none** method is used only as standby.
- Normally, do not use None authentication. You can use the **none** method as the last optional authentication method in special cases. For example, all the users who may request access are trusted users and the users' work must not be delayed by system faults. Then you can use the **none** method to assign access permissions to these users when the authentication server does not respond. It is recommended that the local authentication method be added before the **none** method.
- If AAA authentication is enabled but no authentication method is configured and the default authentication method does not exist, users can directly log in to the Console without being authenticated. If users log in by other means, the users must pass local authentication.
- When a user enters the CLI after passing login authentication (the **none** method is not used), the username is recorded. When the user performs Enable authentication, the user is not prompted to enter the username again, because the username that the user entered during login authentication is automatically filled in. However, the user must enter the password previously used for login authentication.
- The username is not recorded if the user does not perform login authentication when entering the CLI or the **none** method is used during login authentication. Then, a user is required to enter the username each time when performing Enable authentication.

### Configuration Steps

#### ↳ Enabling AAA

- Mandatory.

- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

#### ↘ Defining a Method List of Login Authentication

- Run the **aaa authentication login** command to configure a method list of login authentication.
- This configuration is mandatory if you need to configure a login authentication method list (including the configuration of the default method list).
- By default, no method list of login authentication is configured.

#### ↘ Defining a Method List of Enable Authentication

- Run the **aaa authentication enable** command to configure a method list of Enable authentication.
- This configuration is mandatory if you need to configure an Enable authentication method list. (You can configure only the default method list.)
- By default, no method list of Enable authentication is configured.
- 

#### ↘ Setting the Maximum Number of Login Attempts

- Optional.
- By default, a user is allowed to enter passwords up to three times during login.

#### ↘ Setting the Maximum Lockout Time After a Login Failure

- Optional.
- By default, a user is locked for 15 minutes after entering wrong passwords three times.

### Verification

- Run the **show aaa method-list** command to display the configured method lists.
- Run the **show aaa lockout** command to display the settings of the maximum number of login attempts and the maximum lockout time after a login failure.
- Run the **show running-config** command to display the authentication method lists associated with login authentication and 802.1X authentication.

### Related Commands

#### ↘ Enabling AAA

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa new-model</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA |

|  |                 |
|--|-----------------|
|  | is not enabled. |
|--|-----------------|

### ↘ Defining a Method List of Login Authentication

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>aaa authentication login</b> { <b>default</b>   <i>list-name</i> } <i>method1</i> [ <i>method2...</i> ]  |
| <b>Parameter Description</b> | <p><b>default:</b> With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of a login authentication method list in characters.</p> <p><i>method:</i> Indicates authentication methods from <b>local</b>, <b>none</b>, <b>group</b>, and <b>subs</b>. A method list contains up to four methods.</p> <p><b>local:</b> Indicates that the local user database is used for authentication.</p> <p><b>none:</b> Indicates that authentication is not performed.</p> <p><b>group:</b> Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported.</p> <p><b>subs:</b> Indicates that the subs database is used for authentication.</p> |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | <p>If the AAA login authentication service is enabled on the NAS, users must perform login authentication negotiation through AAA. Run the <b>aaa authentication login</b> command to configure the default or optional method lists for login authentication.</p> <p>In a method list, the next method is executed only when the current method does not receive response. After you configure login authentication methods, apply the methods to the VTY lines that require login authentication; otherwise, the methods will not take effect.</p>  |

### ↘ Defining a Method List of Enable Authentication

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>aaa authentication enable default</b> <i>method1</i> [ <i>method2...</i> ]   |
| <b>Parameter Description</b> | <p><b>default:</b> With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of an Enable authentication method list in characters.</p> <p><i>method:</i> Indicates authentication methods from <b>enable</b>, <b>local</b>, <b>none</b>, and <b>group</b>. A method list contains up to four methods.</p> <p><b>enable:</b> Indicates that the password that is configured using the <b>enable</b> command is used for authentication.</p> <p><b>local:</b> Indicates that the local user database is used for authentication.</p> <p><b>none:</b> Indicates that authentication is not performed.</p> <p><b>group:</b> Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported.</p> |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | <p>If the AAA login authentication service is enabled on the NAS, users must perform Enable authentication negotiation through AAA. Run the <b>aaa authentication enable</b> command to configure the default or optional method lists for Enable authentication.</p> <p>In a method list, the next method is executed only when the current method does not receive response.</p>  |

### ↘ Setting the Maximum Number of Login Attempts

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>aaa local authentication attempts</b> <i>max-attempts</i>  |
| <b>Parameter Description</b> | <i>max-attempts</i> : Indicates the maximum number of login attempts. The value ranges from 1 to 2,147,483,647. |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Use this command to set the maximum number of times a user can attempt to login.                                |

### ↳ Setting the Maximum Lockout Time After a Login Failure

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa local authentication lockout-time</b> <i>lockout-time</i>   |
| <b>Parameter Description</b> | <i>lockout-time</i> : Indicates the time during which a user is locked after entering wrong passwords up to the specified times. The value ranges from 1 to 2,147,483,647, in the unit of minutes. |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Use this command to set the maximum time during which a user is locked after entering wrong passwords up to the specified times.   |

## Configuration Example

### ↳ Configuring AAA Login Authentication

Configure a login authentication method list on the NAS containing **group** *radius* and **local** methods in order.


|                               |   |
|-------------------------------|---|
| <b>Scenario</b><br>Figure 1-5 | <pre> graph LR     User[User] --- Gi01[Gi 0/1] --- NAS[NAS]     NAS --- Gi02[Gi 0/2] --- Server[Server 10.1.1.1] </pre>   |
| <b>Configuration Steps</b>    | <p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.)</p> <p>Step 3: Configure an AAA authentication method list for login authentication users. (This example uses <b>group</b> <i>radius</i> and <b>local</b> in order.)</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authentication method is used.</p> |
| <b>NAS</b>                    | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#username user password pass Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server key Orion Alpha A28X Orion Alpha A28X(config)#aaa authentication login list1 group radius local Orion Alpha A28X(config)#line vty 0 20 </pre>   |



|                     |   |
|---------------------|---|
|                     | <pre>Orion Alpha A28X(config-line)#login authentication list1 Orion Alpha A28X(config-line)#exit</pre>  |
| <b>Verification</b> | Run the <b>show aaa method-list</b> command on the NAS to display the configuration.  |
| <b>NAS</b>          | <pre>Orion Alpha A28X#show aaa method-list  Authentication method-list: aaa authentication login list1 group radius local  Accounting method-list:  Authorization method-list:</pre>                                      |
|                     | <p>Assume that a user remotely logs in to the NAS through Telnet. The user is prompted to enter the username and password on the CLI.</p> <p>The user must enter the correct username and password to access the NAS.</p> |
| <b>User</b>         | <pre>User Access Verification  Username:user  Password:pass</pre>   |

### ↘ Configuring AAA Enable Authentication


Configure an Enable authentication method list on the NAS containing **group radius**, **local**, and then **enable** methods in order.

|                                      |  |
|--------------------------------------|--|
| <b>Scenario</b><br><b>Figure 1-6</b> |  <pre> graph LR     User[User] --- Gi01[Gi 0/1] --- NAS[NAS]     NAS --- Gi02[Gi 0/2] --- Server[Server]     Server --- IP[10.1.1.1]   </pre>   |
| <b>Configuration Steps</b>           | <p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. Configure Enable authentication passwords on the NAS if you use Enable password authentication.</p> <p>Step 3: Configure an AAA authentication method list for Enable authentication users.</p> <ul style="list-style-type: none"> <li>You can define only one Enable authentication method list globally. You do not need to define the list name but just default it. After that, it will be applied automatically.</li> </ul> |

|                     |  |
|---------------------|--|
| <b>NAS</b>          | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#username user privilege 15 password pass Orion Alpha A28X(config)#enable secret w Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server key Orion Alpha A28X Orion Alpha A28X(config)#aaa authentication enable default group radius local enable </pre> |
| <b>Verification</b> | Run the <b>show aaa method-list</b> command on the NAS to display the configuration.   |
| <b>NAS</b>          | <pre> Orion Alpha A28X#show aaa method-list  Authentication method-list: aaa authentication enable default group radius local enable  Accounting method-list:  Authorization method-list: </pre>   |
|                     | The CLI displays an authentication prompt when the user level is updated to level 15. The user must enter the correct username and password to access the NAS.   |
| <b>NAS</b>          | <pre> Orion Alpha A28X&gt;enable Username:user Password:pass Orion Alpha A28X# </pre>  |

### ↳ Configuring AAA 802.1X Authentication

Configure an 802.1X authentication method list on the NAS containing **group radius**, and then **local** methods in order.

|                                      |   |
|--------------------------------------|---|
| <b>Scenario</b><br><b>Figure 1-7</b> |  <pre> graph LR     User[Laptop] --- Gi01[Gi 0/1] --- NAS[Switch]     NAS --- Gi02[Gi 0/2] --- Server[Server]     Server --- IP[10.1.1.1] </pre>                     |
| <b>Configuration Steps</b>           | <p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS server in advance if group-server authentication needs to be implemented.</p> <p>Configure the local user database information on the NAS if local authentication needs to be implemented.</p> |

|                     |   |
|---------------------|---|
|                     | <p>(This example requires the configuration of a RADIUS server and local database information.) Currently, 802.1X authentication does not support TACACS+.</p> <p>Step 3: Configure an AAA authentication method list for 802.1X authentication users. (This example uses <b>group radius</b> and <b>local</b> in order.)</p> <p>Step 4: Apply the AAA authentication method list. Skip this step if the default authentication method is used.</p> <p>Step 5: Enable 802.1X authentication on an interface.</p>  |
| <b>NAS</b>          | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#username user1 password pass1 Orion Alpha A28X(config)#username user2 password pass2 Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server key Orion Alpha A28X Orion Alpha A28X(config)#aaa authentication dot1x default group radius local Orion Alpha A28X(config)#interface gigabitEthernet 0/1 Orion Alpha A28X(config-if-gigabitEthernet 0/1)#dot1x port-control auto Orion Alpha A28X(config-if-gigabitEthernet 0/1)#exit </pre> |
| <b>Verification</b> | Run the <b>show aaa method-list</b> command on the NAS to display the configuration.  |
| <b>NAS</b>          | <pre> Orion Alpha A28X#show aaa method-list  Authentication method-list:  aaa authentication dot1x default group radius local  Accounting method-list:  Authorization method-list: </pre>   |

### Common Errors

- No RADIUS server or TACACS+ server is configured.
- Usernames and passwords are not configured in the local database.

## 1.4.2 Configuring AAA Authorization

### Configuration Effect

- Determine what services or permissions authenticated users can enjoy.

## Notes

---

- EXEC authorization is often used with login authentication, which can be implemented on the same line. Authorization and authentication can be performed using different methods and servers. Therefore, the results of the same user may be different. If a user passes login authentication but fails in EXEC authorization, the user cannot enter the CLI.
- The authorization methods in an authorization scheme are executed in accordance with the method configuration sequence. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried.
- Command authorization is supported only by TACACS+.
- Console authorization: The switch can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

## Configuration Steps

---

### ↳ Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

### ↳ Defining a Method List of EXEC Authorization

- Run the **aaa authorization exec** command to configure a method list of EXEC authorization.
  - This configuration is mandatory if you need to configure an EXEC authorization method list (including the configuration of the default method list).
  - By default, no EXEC authorization method list is configured.
- 
- The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)
- 

### ↳ Defining a Method List of Command Authorization

- Run the **aaa authorization commands** command to configure a method list of command authorization.
- This configuration is mandatory if you need to configure a command authorization method list (including the configuration of the default method list).
- By default, no command authorization method list is configured.

### ↳ Configuring a Method List of Network Authorization

- Run the **aaa authorization network** command to configure a method list of network authorization.
  - This configuration is mandatory if you need to configure a network authorization method list (including the configuration of the default method list).
  - By default, no authorization method is configured.
-

### ↘ Applying EXEC Authorization Methods to a Specified VTY Line

- Run the **authorization exec** command in line configuration mode to apply EXEC authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

### ↘ Applying Command Authorization Methods to a Specified VTY Line

- Run the **authorization commands** command in line configuration mode to apply command authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

### ↘ Enabling Authorization for Commands in Configuration Modes

- Run the **aaa authorization config-commands** command to enable authorization for commands in configuration modes.
- By default, authorization is disabled for commands in configuration modes.

### ↘ Enabling Authorization for the Console to Run Commands

- Run the **aaa authorization console** command to enable authorization for console users to run commands.
- By default, authorization is disabled for the Console to run commands.

## Verification

Run the **show running-config** command to verify the configuration.

## Related Commands

### ↘ Enabling AAA

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa new-model</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled. |

### ↘ Defining a Method List of EXEC Authorization

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>aaa authorization exec { default   list-name } method1 [ method2...]</b>   |
| <b>Parameter Description</b> | <b>default:</b> With this parameter used, the configured method list will be defaulted.<br><b>list-name:</b> Indicates the name of an EXEC authorization method list in characters.<br><b>method:</b> Specifies authentication methods from <b>local</b> , <b>none</b> , and <b>group</b> . A method list contains up to four |

|                     |  |
|---------------------|--|
|                     | <p>methods.</p> <p><b>local:</b> Indicates that the local user database is used for EXEC authorization.</p> <p><b>none:</b> Indicates that EXEC authorization is not performed.</p> <p><b>group:</b> Indicates that a server group is used for EXEC authorization. Currently, the RADIUS and TACACS+ server groups are supported.</p>  |
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | <p>The switch supports authorization of the users who log in to the CLI of the NAS to assign the users CLI operation permission levels (0 to 15). Currently, EXEC authorization is performed only on the users who have passed login authentication. If a user fails in EXEC authorization, the user cannot enter the CLI.</p> <p>After you configure EXEC authorization methods, apply the methods to the VTY lines that require EXEC authorization; otherwise, the methods will not take effect.</p> |

### ↘ Defining a Method List of Command Authorization

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>aaa authorization commands</b> <i>level</i> { <b>default</b>   <i>list-name</i> } <i>method1</i> [ <i>method2...</i> ]   |
| <b>Parameter Description</b> | <p><b>default:</b> With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of a command authorization method list in characters.</p> <p><i>method:</i> Indicates authentication methods from <b>none</b> and <b>group</b>. A method list contains up to four methods.</p> <p><b>none:</b> Indicates that command authorization is not performed.</p> <p><b>group:</b> Indicates that a server group is used for command authorization. Currently, the TACACS+ server group is supported.</p>  |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | <p>The switch supports authorization of the commands executable by users. When a user enters a command, AAA sends the command to the authentication server. If the authentication server permits the execution, the command is executed. If the authentication server forbids the execution, the command is not executed and a message is displayed showing that the execution is rejected.</p> <p>When you configure command authorization, specify the command level, which is used as the default level. (For example, if a command above Level 14 is visible to users, the default level of the command is 14.)</p> <p>After you configure command authorization methods, apply the methods to the VTY lines that require command authorization; otherwise, the methods will not take effect.</p> |

### ↘ Configuring a Method List of Network Authorization

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa authorization network</b> { <b>default</b>   <i>list-name</i> } <i>method1</i> [ <i>method2...</i> ]  |
| <b>Parameter Description</b> | <p><b>default:</b> With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of a network authorization method list in characters.</p> <p><i>method:</i> Indicates authentication methods from <b>none</b> and <b>group</b>. A method list contains up to four methods.</p> <p><b>none:</b> Indicates that authentication is not performed.</p> <p><b>group:</b> Indicates that a server group is used for network authorization. Currently, the RADIUS and TACACS+ server groups are supported.</p> |
| <b>Command</b>               | Global configuration mode  |

|                    |  |
|--------------------|--|
| <b>Mode</b>        |  |
| <b>Usage Guide</b> | <p>The switch supports authorization of network-related service requests such as PPP and SLIP requests. After authorization is configured, all authenticated users or interfaces are authorized automatically. You can configure three different authorization methods. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried.</p> <p>RADIUS or TACACS+ servers return a series of AV pairs to authorize authenticated users. Network authorization is based on authentication. Only authenticated users can perform network authorization.</p> |

### ↘ Enabling Authorization for Commands in Configuration Modes (Including the Global Configuration Mode and Sub-Modes)

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa authorization config-commands</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | If you need to enable authorization for commands only in non-configuration modes (for example, privileged EXEC mode), disable authorization in configuration modes by using the <b>no</b> form of this command. Then users can run commands in configuration mode and sub-modes without authorization. |

### ↘ Enabling Authorization for the Console to Run Commands

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa authorization console</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | The switch can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect. |

## Configuration Example

### ↘ Configuring AAA EXEC Authorization

Configure login authentication and EXEC authorization for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC authorization is performed on a RADIUS server. If the RADIUS server does not respond, users are redirected to the local authorization.

|                                      |  |
|--------------------------------------|--|
| <b>Scenario</b><br><b>Figure 1-8</b> | <pre> graph LR     User[Laptop] --- Gi01[Gi 0/1] --- NAS[NAS]     NAS --- Gi02[Gi 0/2] --- Server[Server]     Server --- IP[10.1.1.1]   </pre> |
|--------------------------------------|--|

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.</p> <p>EXEC authorization is often used with login authentication, which can be implemented on the same line.</p>       |
| <b>NAS</b>                 | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#username user password pass Orion Alpha A28X(config)#username user privilege 6 Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server key test Orion Alpha A28X(config)#aaa authentication login list1 group local Orion Alpha A28X(config)#aaa authorization exec list2 group radius local Orion Alpha A28X(config)#line vty 0 4 Orion Alpha A28X(config-line)#login authentication list1 Orion Alpha A28X(config-line)# authorization exec list2 Orion Alpha A28X(config-line)#exit </pre> |
| <b>Verification</b>        | <p>Run the <b>show run</b> and <b>show aaa method-list</b> commands on the NAS to display the configuration.</p>  |
| <b>NAS</b>                 | <pre> Orion Alpha A28X#show aaa method-list  Authentication method-list: aaa authentication login list1 group local  Accounting method-list:  Authorization method-list: aaa authorization exec list2 group radius local </pre>   |
|                            | <pre> Orion Alpha A28X# show running-config  aaa new-model  !</pre>   |




```

aaa authorization exec list2 group local
aaa authentication login list1 group radius local
!
username user password pass
username user privilege 6
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
  authorization exec list2
  login authentication list1
!
End

```

### ↘ Configuring AAA Command Authorization

Provide command authorization for login users according to the following default authorization method:  
 Authorize level-15 commands first by using a TACACS+ server. If the TACACS+ server does not respond, local authorization is performed. Authorization is applied to the users who log in through the Console and the users who log in through other types of clients.

|                                      |   |
|--------------------------------------|---|
| <b>Scenario</b><br><b>Figure 1-9</b> |    |
| <b>Configuration Steps</b>           | <p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.</p> |
| <b>NAS</b>                           | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#username user1 password pass1 Orion Alpha A28X(config)#username user1 privilege 15 </pre>  |


|                     |   |
|---------------------|---|
|                     | <pre> Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#tacacs-server host 192.168.217.10 Orion Alpha A28X(config)#tacacs-server key aaa Orion Alpha A28X(config)#aaa authentication login default local Orion Alpha A28X(config)#aaa authorization commands 15 default group tacacs+ local Orion Alpha A28X(config)#aaa authorization console </pre> |
| <b>Verification</b> | Run the <b>show run</b> and <b>show aaa method-list</b> commands on the NAS to display the configuration.   |
| <b>NAS</b>          | <pre> Orion Alpha A28X#show aaa method-list  Authentication method-list: aaa authentication login default local  Accounting method-list:  Authorization method-list: aaa authorization commands 15 default group tacacs+ local </pre>   |
|                     | <pre> Orion Alpha A28X#show run ! aaa new-model ! aaa authorization console aaa authorization commands 15 default group tacacs+ local aaa authentication login default local ! ! nfpp ! vlan 1 ! username user1 password 0 pass1 username user1 privilege 15 no service password-encryption </pre>  |

```

!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end

```

### ↘ Configuring AAA Network Authorization

|                                       |   |
|---------------------------------------|---|
| <b>Scenario</b><br><b>Figure 1-10</b> |  <pre> graph LR     User[Laptop] --- Gi01[Gi 0/1] --- NAS[NAS]     NAS --- Gi02[Gi 0/2] --- Server[Server]     Server --- IP[10.1.1.1] </pre>  |
| <b>Configuration Steps</b>            | <p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.</p> |
| <b>NAS</b>                            | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server key test Orion Alpha A28X(config)#aaa authorization network default group radius none Orion Alpha A28X(config)# end </pre>   |
| <b>Verification</b>                   | <p>Run the <b>show aaa method-list</b> command on the NAS to display the configuration.</p>   |
| <b>NAS</b>                            | <pre> Orion Alpha A28X#show aaa method-list  Authentication method-list:  Accounting method-list: </pre>  |

```
Authorization method-list:
```

```
aaa authorization network default group radius none
```

## Common Errors

---

N/A

## 1.4.3 Configuring AAA Accounting

### Configuration Effect

---

- Record the network resource usage of users.
- Record the user login and logout processes and the commands executed by users during device management.

### Notes

---

About accounting methods:

- If an accounting scheme contains multiple accounting methods, these methods are executed according to the method configuration sequence. The next accounting method is executed only when the current method does not receive response. If accounting fails using a method, the next method will be not tried.
- After the default accounting method list is configured, it is applied to all VTY lines automatically. If a non-default accounting method list is applied to a line, it will replace the default one. If you apply an undefined method list to a line, the system will display a message indicating that accounting on this line is ineffective. Accounting will take effect only when a defined method list is applied.

EXEC accounting:

- EXEC accounting is performed only when login authentication on the NAS is completed. EXEC accounting is not performed if login authentication is not configured or the **none** method is used for authentication. If Start accounting is not performed for a user upon login, Stop accounting will not be performed when the user logs out.

Command accounting

- Only the TACACS+ protocol supports command accounting.

### Configuration Steps

---

#### ↳ Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

#### ↳ Defining a Method List of EXEC Accounting

- Run the **aaa accounting exec** command to configure a method list of EXEC accounting.
-

- This configuration is mandatory if you need to configure an EXEC accounting method list (including the configuration of the default method list).
- The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)
- By default, no EXEC accounting method list is configured.

#### ↘ Defining a Method List of Command Accounting

- Run the **aaa accounting commands** command to configure a method list of command accounting.
- This configuration is mandatory if you need to configure a command accounting method list (including the configuration of the default method list).
- By default, no command accounting method list is configured. Only the TACACS+ protocol supports command accounting.

#### ↘ Defining a Method List of Network Accounting

- Run the **aaa accounting network** command to configure a method list of network accounting.
- This configuration is mandatory if you need to configure a network accounting method list (including the configuration of the default method list).
- By default, no network accounting method list is configured.

#### ↘ Applying EXEC Accounting Methods to a Specified VTY Line

- Run the **accounting exec** command in line configuration mode to apply EXEC accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

#### ↘ Applying Command Accounting Methods to a Specified VTY Line

- Run the **accounting commands** command in line configuration mode to apply command accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

#### ↘ Applying 802.1X Network Accounting Methods

- Run the **dot1x accounting network** command to configure 802.1X network accounting methods.
  - This configuration is mandatory if you need to specify 802.1X network accounting methods.
  - You do not need to run this command if you apply the default method list.
  - By default, all VTY lines are associated with the default accounting method list.
-

## ↳ Enabling Accounting Update

- Optional.
- It is recommended that accounting update be configured for improved accounting accuracy.
- By default, accounting update is disabled.

## ↳ Configuring the Accounting Update Interval

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

## Verification

Run the **show running-config** command to verify the configuration.

## Related Commands

### ↳ Enabling AAA

|                     |  |
|---------------------|--|
| <b>Command</b>      | <b>aaa new-model</b>   |
| <b>Parameter</b>    | N/A  |
| <b>Description</b>  |  |
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled. |

### ↳ Defining a Method List of EXEC Accounting

|                     |  |
|---------------------|--|
| <b>Command</b>      | <b>aaa accounting exec { default   list-name } start-stop method1 [ method2...]</b>  |
| <b>Parameter</b>    | <b>default:</b> With this parameter used, the configured method list will be defaulted.  |
| <b>Description</b>  | <i>list-name:</i> Indicates the name of an EXEC accounting method list in characters.<br><i>method:</i> Indicates authentication methods from <b>none</b> and <b>group</b> . A method list contains up to four methods.<br><b>none:</b> Indicates that EXEC accounting is not performed.<br><b>group:</b> Indicates that a server group is used for EXEC accounting. Currently, the RADIUS and TACACS+ server groups are supported.  |
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | The switch enables EXEC accounting only when login authentication is completed. EXEC accounting is not performed if login authentication is not performed or the <b>none</b> authentication method is used.<br>After accounting is enabled, when a user logs in to the CLI of the NAS, the NAS sends a start-accounting message to the authentication server. When the user logs out, the NAS sends a stop-accounting message to the authentication server. If the NAS does not send a start-accounting message when the user logs in, the NAS will not send a stop-accounting message when the user logs out.<br>After you configure EXEC accounting methods, apply the methods to the VTY lines that require EXEC accounting; otherwise, the methods will not take effect. |

## ↳ Defining a Method List of Command Accounting

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa accounting commands</b> <i>level</i> { <b>default</b>   <i>list-name</i> } <b>start-stop</b> <i>method1</i> [ <i>method2...</i> ]   |
| <b>Parameter Description</b> | <p><i>level</i>: Indicates the command level for which accounting will be performed. The value ranges from 0 to 15.</p> <p>After a command of the configured level is executed, the accounting server records related information based on the received accounting packet.</p> <p><b>default</b>: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name</i>: Indicates the name of a command accounting method list in characters.</p> <p><i>method</i>: Indicates authentication methods from <b>none</b> and <b>group</b>. A method list contains up to four methods.</p> <p><b>none</b>: Indicates that command accounting is not performed.</p> <p><b>group</b>: Indicates that a server group is used for command accounting. Currently, the TACACS+ server group is supported.</p> |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | <p>The switch enables command accounting only when login authentication is completed. Command accounting is not performed if login authentication is not performed or the <b>none</b> authentication method is used. After accounting is enabled, the NAS records information about the commands of the configured level that users run and sends the information to the authentication server.</p> <p>After you configure command accounting methods, apply the methods to the VTY lines that require command accounting; otherwise, the methods will not take effect.</p>  |

## ↳ Defining a Method List of Network Accounting

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa accounting network</b> { <b>default</b>   <i>list-name</i> } <b>start-stop</b> <i>method1</i> [ <i>method2...</i> ]   |
| <b>Parameter Description</b> | <p><b>default</b>: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name</i>: Indicates the name of a network accounting method list in characters.</p> <p><b>start-stop</b>: Indicates that a start-accounting message and a stop-accounting message are sent when a user accesses a network and when the user disconnects from the network respectively. The start-accounting message indicates that the user is allowed to access the network, regardless of whether accounting is successfully enabled.</p> <p><i>method</i>: Indicates authentication methods from <b>none</b> and <b>group</b>. A method list contains up to four methods.</p> <p><b>none</b>: Indicates that network accounting is not performed.</p> <p><b>group</b>: Indicates that a server group is used for network accounting. Currently, the RADIUS and TACACS+ server groups are supported.</p> |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | <p>The switch sends record attributes to the authentication server to perform accounting of user activities. The <b>start-stop</b> keyword is used to configure user accounting options.</p>   |

## ↳ Enabling Accounting Update

|                              |                              |
|------------------------------|------------------------------|
| <b>Command</b>               | <b>aaa accounting update</b> |
| <b>Parameter Description</b> | N/A                          |
| <b>Command</b>               | Global configuration mode    |

---

|                    |   |
|--------------------|---|
| <b>Mode</b>        |   |
| <b>Usage Guide</b> | Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to enable accounting update. |


### ↘ [Configuring the Accounting Update Interval](#)

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>aaa accounting update periodic <i>interval</i></b>   |
| <b>Parameter Description</b> | <i>Interval</i> : Indicates the accounting update interval, in the unit of minutes. The shortest is 1 minute.   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to configure the accounting update interval. |

## [Configuration Example](#)

### ↘ [Configuring AAA EXEC Accounting](#)

Configure login authentication and EXEC accounting for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC accounting is performed on a RADIUS server.

|                                       |  |
|---------------------------------------|--|
| <b>Scenario</b><br><b>Figure 1-11</b> |  <p>The diagram illustrates a network topology for AAA EXEC accounting. A User (represented by a laptop) is connected to a Network Access Server (NAS) via interface Gi 0/1. The NAS is then connected to a Server (represented by a server rack) via interface Gi 0/2. The Server's IP address is 10.1.1.1.</p>   |
| <b>Configuration Steps</b>            | <p>Step 1: Enable AAA.</p> <p>If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance.</p> <p>Step 2: Configure an AAA accounting method list according to different access modes and service types.</p> <p>Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.</p>  |
| <b>NAS</b>                            | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#username user password pass Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server key test Orion Alpha A28X(config)#aaa authentication login list1 group local Orion Alpha A28X(config)#aaa accounting exec list3 start-stop group radius Orion Alpha A28X(config)#line vty 0 4 Orion Alpha A28X(config-line)#login authentication list1 Orion Alpha A28X(config-line)# accounting exec list3 </pre> |



|                     |   |
|---------------------|---|
|                     | Orion Alpha A28X(config-line)#exit  |
| <b>Verification</b> | Run the <b>show run</b> and <b>show aaa method-list</b> commands on the NAS to display the configuration.   |
| <b>NAS</b>          | <pre> Orion Alpha A28X#show aaa method-list  Authentication method-list: aaa authentication login list1 group local  Accounting method-list: aaa accounting exec list3 start-stop group radius  Authorization method-list: </pre>   |
|                     | <pre> Orion Alpha A28X# show running-config aaa new-model ! aaa accounting exec list3 start-stop group radius aaa authentication login list1 group local ! username user password pass ! radius-server host 10.1.1.1 radius-server key 7 093b100133 ! line con 0 line vty 0 4   accounting exec list3   login authentication list1 ! End </pre> |

### ↘ **Configuring AAA Command Accounting**

Configure command accounting for login users according to the default accounting method. Login authentication is performed in local mode, and command accounting is performed on a TACACS+ server.

|                                       |  |
|---------------------------------------|--|
| <b>Scenario</b><br><b>Figure 1-12</b> |   |
| <b>Configuration Steps</b>            | <p>Step 1: Enable AAA.</p> <p>If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance.</p> <p>Step 2: Configure an AAA accounting method list according to different access modes and service types.</p> <p>Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.</p>  |
| <b>NAS</b>                            | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#username user1 password pass1 Orion Alpha A28X(config)#username user1 privilege 15 Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#tacacs-server host 192.168.217.10 Orion Alpha A28X(config)#tacacs-server key aaa Orion Alpha A28X(config)#aaa authentication login default local Orion Alpha A28X(config)#aaa accounting commands 15 default start-stop group tacacs+ </pre> |
| <b>Verification</b>                   | <p>Run the <b>show aaa method-list</b> command on the NAS to display the configuration.</p>  |
| <b>NAS</b>                            | <pre> Orion Alpha A28X#show aaa method-list  Authentication method-list: aaa authentication login default local  Accounting method-list: aaa accounting commands 15 default start-stop group tacacs+  Authorization method-list: </pre>  |
|                                       | <pre> Orion Alpha A28X#show run  ! aaa new-model ! aaa authorization config-commands </pre>  |


```

aaa accounting commands 15 default start-stop group tacacs+
aaa authentication login default local
!
!
nfp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end

```

### ↘ Configuring AAA Network Accounting

Configure a network accounting method list for 802.1X STAs, and configure a RADIUS remote server for authentication and accounting.

|   |   |
|---|---|
| <p><b>Scenario</b><br/><b>Figure 1-13</b></p> |    |
| <p><b>Configuration Steps</b></p>             | <p>Step 1: Enable AAA.</p> <p>Step 2: If remote server-group accounting needs to be implemented, configure a RADIUS server in advance.</p> <p>Step 3: Configure an AAA accounting method list according to different access modes and service types.</p> <p>Step 4: Apply the configured AAA accounting method list. Skip this step if the default accounting method is used.</p> |

|                     |   |
|---------------------|---|
|                     | <ul style="list-style-type: none"> <li>Accounting is performed only when 802.1X authentication is completed.</li> </ul>   |
| <b>NAS</b>          | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#username user password pass Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server key test Orion Alpha A28X(config)#aaa authentication dot1x aut1x group radius local Orion Alpha A28X(config)#aaa accounting network acc1x start-stop group radius Orion Alpha A28X(config)#dot1x authentication aut1x Orion Alpha A28X(config)#dot1x accounting acc1x Orion Alpha A28X(config)#interface gigabitEthernet 0/1 Orion Alpha A28X(config-if-GigabitEthernet 0/1)#dot1 port-control auto Orion Alpha A28X(config-if-GigabitEthernet 0/1)#exit </pre> |
| <b>Verification</b> | Run the <b>show aaa method-list</b> command on the NAS to display the configuration.  |
| <b>NAS</b>          | <pre> Orion Alpha A28X#show aaa method-list  Authentication method-list: aaa authentication dot1x aut1x group radius local  Accounting method-list: aaa accounting network acc1x start-stop group radius  Authorization method-list: </pre>   |

## Common Errors

N/A

## 1.4.4 Configuring an AAA Server Group

### Configuration Effect

- Create a user-defined server group and add one or more servers to the group.
- When you configure authentication, authorization, and accounting method lists, name the methods after the server group name so that the servers in the group are used to handle authentication, authorization, and accounting requests.
- Use self-defined server groups to separate authentication, authorization, and accounting.

## Notes

---

In a user-defined server group, you can specify and apply only the servers in the default server group.

## Configuration Steps

---

### ↳ Creating a User-Defined AAA Server Group

- Mandatory.
- Assign a meaningful name to the user-defined server group. Do not use the predefined **radius** and **tacacs+** keywords in naming.

### ↳ Adding an AAA Server Group Member

- Mandatory.
- Run the **server** command to add AAA server group members.
- By default, a user-defined server group does not have servers.

## Verification

---

Run the **show aaa group** command to verify the configuration.

## Related Commands

---

### ↳ Creating a User-Defined AAA Server Group

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>aaa group server {radius   tacacs+} name</b>   |
| <b>Parameter Description</b> | <i>name</i> : Indicates the name of the server group to be created. The name must not contain the <b>radius</b> and <b>tacacs+</b> keywords because they are the names of the default RADIUS and TACACS+ server groups. |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Use this command to configure an AAA server group. Currently, the RADIUS and TACACS+ server groups are supported.   |

### ↳ Adding an AAA Server Group Member

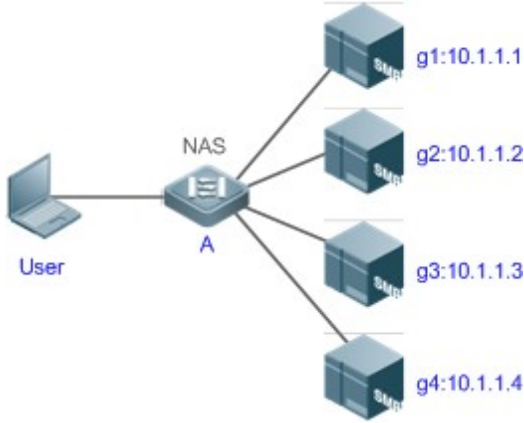
|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>server ip-addr [auth-port port1] [acct-port port2]</b>  |
| <b>Parameter Description</b> | <i>ip-addr</i> : Indicates the IP address of a server.<br><i>port1</i> : Indicates the authentication port of a server. (This parameter is supported only by the RADIUS server group.)<br><i>port2</i> : Indicates the accounting port of a server. (This parameter is supported only by the RADIUS server group.) |
| <b>Command Mode</b>          | Server group configuration mode  |
| <b>Usage Guide</b>           | When you add servers to a server group, the default ports are used if you do not specify ports.  |

---

## Configuration Example

### Creating an AAA Server Group

Create RADIUS server groups named g1 and g2. The IP addresses of the servers in g1 are 10.1.1.1 and 10.1.1.2, and the IP addresses of the servers in g2 are 10.1.1.3 and 10.1.1.4.

|                                       |  |
|---------------------------------------|--|
| <b>Scenario</b><br><b>Figure 1-14</b> |  <p>The diagram illustrates a network setup where a User (represented by a laptop) is connected to a Network Access Server (NAS) labeled 'A'. The NAS is connected to four RADIUS servers. The servers are labeled as follows: g1:10.1.1.1, g2:10.1.1.2, g3:10.1.1.3, and g4:10.1.1.4.</p>  |
| <b>Prerequisites</b>                  | <ol style="list-style-type: none"><li>1. The required interfaces, IP addresses, and VLANs have been configured on the network, network connections have been set up, and the routes from the NAS to servers are reachable.</li><li>2. Enable AAA.</li></ol>  |
| <b>Configuration Steps</b>            | <p>Step 1: Configure a server (which belongs to the default server group).</p> <p>Step 2: Create user-defined AAA server groups.</p> <p>Step 3: Add servers to the AAA server groups.</p>  |
| <b>NAS</b>                            | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server host 10.1.1.2 Orion Alpha A28X(config)#radius-server host 10.1.1.3 Orion Alpha A28X(config)#radius-server host 10.1.1.4 Orion Alpha A28X(config)#radius-server key secret Orion Alpha A28X(config)#aaa group server radius g1 Orion Alpha A28X(config-gs-radius)#server 10.1.1.1 Orion Alpha A28X(config-gs-radius)#server 10.1.1.2 Orion Alpha A28X(config-gs-radius)#exit Orion Alpha A28X(config)#aaa group server radius g2 Orion Alpha A28X(config-gs-radius)#server 10.1.1.3 Orion Alpha A28X(config-gs-radius)#server 10.1.1.4</pre> |

|                     |  |
|---------------------|--|
|                     | Orion Alpha A28X(config-gs-radius)#exit  |
| <b>Verification</b> | Run the <b>show aaa group</b> and <b>show run</b> commands on the NAS to display the configuration.  |
| <b>NAS</b>          | <pre> Orion Alpha A28X#show aaa group  Type      Reference Name ----- radius    1      radius tacacs+   1      tacacs+ radius    1      g1 radius    1      g2 </pre>  |
|                     | <pre> Orion Alpha A28X#show run  ! radius-server host 10.1.1.1 radius-server host 10.1.1.2 radius-server host 10.1.1.3 radius-server host 10.1.1.4 radius-server key secret ! aaa group server radius g1 server 10.1.1.1 server 10.1.1.2 ! aaa group server radius g2 server 10.1.1.3 server 10.1.1.4 ! ! </pre> |

### Common Errors

- For RADIUS servers that use non-default authentication and accounting ports, when you run the **server** command to add servers, specify the authentication or accounting port.

## 1.4.5 Configuring the Domain-Based AAA Service

### Configuration Effect

---

Create AAA schemes for 802.1X users in different domains.

### Notes

---

About referencing method lists in domains:

- The AAA method lists that you select in domain configuration mode should be defined in advance. If the method lists are not defined in advance, when you select them in domain configuration mode, the system prompts that the configurations do not exist.
- The names of the AAA method lists selected in domain configuration mode must be consistent with those of the method lists defined for the AAA service. If they are inconsistent, the AAA service cannot be properly provided to the users in the domain.

About the default domain:

- Default domain: After the domain-based AAA service is enabled, if a username does not carry domain information, the AAA service is provided to the user based on the default domain. If the domain information carried by the username is not configured in the system, the system determines that the user is unauthorized and will not provide the AAA service to the user. If the default domain is not configured initially, it must be created manually.
- When the domain-based AAA service is enabled, the default domain is not configured by default and needs to be created manually. The default domain name is **default**. It is used to provide the AAA service to the users whose usernames do not carry domain information. If the default domain is not configured, the AAA service is not available for the users whose usernames do not carry domain information.

About domain names:

- The domain names carried by usernames and those configured on the NAS are matched in the longest matching principle. For example, if two domains, **domain.com** and **domain.com.cn** are configured on a NAS and a user sends a request carrying **aaa@domain.com**, the NAS determines that the user belongs to **domain.com**, instead of **domain.com.cn**.
- If the username of an authenticated user carries domain information but the domain is not configured on the NAS, the AAA service is not provided to the user.

### Configuration Steps

---

#### ↳ Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

#### ↳ Enabling the Domain-Based AAA Service

- Mandatory.
-



- Run the **aaa domain enable** command to enable the domain-based AAA service.
- By default, the domain-based AAA service is disabled.

#### ↳ **Creating a Domain and Entering Domain Configuration Mode**

- Mandatory.
- Run the **aaa domain** command to create a domain or enter the configured domain.
- By default, no domain is configured.

#### ↳ **Associating the Domain with an 802.1X Authentication Method List**

- Run the **authentication dot1x** command to associate the domain with an 802.1X authentication method list.
- This configuration is mandatory if you need to apply a specified 802.1X authentication method list to the domain.
- Currently, the domain-based AAA service is applicable only to 802.1X access.

#### ↳ **Associating the Domain with a Network Accounting Method List**

- Run the **accounting network** command to associate the domain with a network accounting method.
- This configuration is mandatory if you need to apply a specified network accounting method list to the domain.
- If a domain is not associated with a network accounting method list, by default, the global default method list is used for accounting.

#### ↳ **Associating the Domain with a Network Authorization Method List**

- Run the **authorization network** command to associate the domain with a network authorization method list.
- This configuration is mandatory if you need to apply a specified network authorization method list to the domain.
- If a domain is not associated with a network authorization method list, by default, the global default method list is used for authorization.

#### ↳ **Configuring the Domain Status**

- Optional.
- When a domain is in Block state, the users in the domain cannot log in.
- By default, after a domain is created, its state is Active, indicating that all the users in the domain are allowed to request network services.

#### ↳ **Configuring Whether to Contain the Domain Name in Usernames**

- Optional.
- By default, the usernames exchanged between the NAS and an authentication server carry domain information.

#### ↳ **Configuring the Maximum Number of Domain Users**

- Optional.
  - By default, the maximum number of access users allowed in a domain is not limited.
-

## Verification

Run the **show aaa domain** command to verify the configuration.

## Related Commands

### ↳ Enabling AAA

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa new-model</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled. |

### ↳ Enabling the Domain-Based AAA Service

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa domain enable</b>                                 |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode                                |
| <b>Usage Guide</b>           | Use this command to enable the domain-based AAA service. |

### ↳ Creating a Domain and Entering Domain Configuration Mode

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>aaa domain { default   domain-name }</b>   |
| <b>Parameter Description</b> | <b>default:</b> Uses this parameter to configure the default domain.<br><b>domain-name:</b> Indicates the name of the domain to be created.   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Use this command to configure a domain to provide the domain-based AAA service. The <b>default</b> parameter specifies the default domain. If a username does not carry domain information, the NAS uses the method list associated with the default domain to provide the AAA service to the user. The <b>domain-name</b> parameter specifies the name of the domain to be created. If the domain name carried by a username matches the configured domain name, the NAS uses the method list associated with this domain to provide the AAA service to the user. The system supports a maximum of 32 domains. |

### ↳ Associating the Domain with an 802.1X Authentication Method List

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>authentication dot1x { default   list-name }</b>  |
| <b>Parameter Description</b> | <b>default:</b> Indicates that the default method list is used.<br><b>list-name:</b> Indicates the name of the method list to be associated. |
| <b>Command Mode</b>          | Domain configuration mode  |
| <b>Usage Guide</b>           | Use this command to associate the domain with a 802.1X authentication method list.   |

---

### ↘ Associating the Domain with a Web Authentication Method List

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>authentication web-auth</b> { <b>default</b>   <i>list-name</i> }   |
| <b>Parameter Description</b> | <b>default:</b> Indicates that the default method list is used.<br><i>list-name:</i> Indicates the name of the method list to be associated. |
| <b>Command Mode</b>          | Domain configuration mode  |
| <b>Usage Guide</b>           | Use this command to associate the domain with a Web authentication method list.  |

### ↘ Associating the Domain with a Network Accounting Method List

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>accounting network</b> { <b>default</b>   <i>list-name</i> }  |
| <b>Parameter Description</b> | <b>default:</b> Indicates that the default method list is used.<br><i>list-name:</i> Indicates the name of the method list to be associated. |
| <b>Command Mode</b>          | Domain configuration mode  |
| <b>Usage Guide</b>           | Use this command to associate the domain with a network accounting method list.  |

### ↘ Associating the Domain with a Network Authorization Method List

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>authorization network</b> { <b>default</b>   <i>list-name</i> }   |
| <b>Parameter Description</b> | <b>default:</b> Indicates that the default method list is used.<br><i>list-name:</i> Indicates the name of the method list to be associated. |
| <b>Command Mode</b>          | Domain configuration mode  |
| <b>Usage Guide</b>           |  |

### ↘ Configuring the Domain Status

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>state</b> { <b>block</b>   <b>active</b> }   |
| <b>Parameter Description</b> | <b>block:</b> Indicates that the configured domain is invalid.<br><b>active:</b> Indicates that the configured domain is valid. |
| <b>Command Mode</b>          | Domain configuration mode   |
| <b>Usage Guide</b>           | Use this command to make the configured domain valid or invalid.  |

### ↘ Configuring Whether to Contain the Domain Name in Usernames

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>username-format</b> { <b>without-domain</b>   <b>with-domain</b> }   |
| <b>Parameter Description</b> | <b>without-domain:</b> Indicates to remove domain information from usernames.<br><b>with-domain:</b> Indicates to keep domain information in usernames.                                 |
| <b>Command Mode</b>          | Domain configuration mode   |
| <b>Usage Guide</b>           | Use this command in domain configuration mode to determine whether to include domain information in usernames when the NAS interacts with authentication servers in a specified domain. |

---


## ↘ Configuring the Maximum Number of Domain Users

|                     |  |
|---------------------|--|
| <b>Command</b>      | <code>access-limit num</code>  |
| <b>Parameter</b>    | <i>num</i> : Indicates the maximum number of access users allowed in a domain. This limit is applicable only to 802.1X STAs. |
| <b>Description</b>  | 802.1X STAs.   |
| <b>Command Mode</b> | Domain configuration mode  |
| <b>Usage Guide</b>  | Use this command to limit the number of access users in a domain.  |

## Configuration Example

### ↘ Configuring the Domain-Based AAA Services

Configure authentication and accounting through a RADIUS server to 802.1X users (username: *user@domain.com*) that access the NAS. The usernames that the NAS sends to the RADIUS server do not carry domain information, and the number of access users is not limited.

|                                |   |
|--------------------------------|---|
| <b>Scenario</b><br>Figure 1-15 |  <pre> graph LR     User[User] --- Gi01[Gi 0/1] --- NAS[NAS]     NAS --- Gi02[Gi 0/2] --- Server[Server]     Server --- IP[10.1.1.1] </pre>  |
| <b>Configuration Steps</b>     | <p>The following example shows how to configure RADIUS authentication and accounting, which requires the configuration of a RADIUS server in advance.</p> <p>Step 1: Enable AAA.</p> <p>Step 2: Define an AAA method list.</p> <p>Step 3: Enable the domain-based AAA service.</p> <p>Step 4: Create a domain.</p> <p>Step 5: Associate the domain with the AAA method list.</p> <p>Step 6: Configure the domain attribute.</p>   |
| <b>NAS</b>                     | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#aaa new-model Orion Alpha A28X(config)#radius-server host 10.1.1.1 Orion Alpha A28X(config)#radius-server key test Orion Alpha A28X(config)#aaa authentication dot1x default group radius Orion Alpha A28X(config)#aaa accounting network list3 start-stop group radius Orion Alpha A28X(config)# aaa domain enable Orion Alpha A28X(config)# aaa domain domain.com Orion Alpha A28X(config-aaa-domain)# authentication dot1x default Orion Alpha A28X(config-aaa-domain)# accounting network list3 Orion Alpha A28X(config-aaa-domain)# username-format without-domain </pre> |

|                     |   |
|---------------------|---|
| <b>Verification</b> | Run the <b>show run</b> and <b>show aaa domain</b> command on the NAS to display the configuration.   |
| <b>NAS</b>          | <pre> Orion Alpha A28X#show aaa domain domain.com  =====Domain domain.com=====  State: Active  Username format: With-domain  Access limit: No limit  802.1X Access statistic: 0  Selected method list:  authentication dot1x default  accounting network list3 </pre>   |
|                     | <pre> Orion Alpha A28X#show run  Building configuration...  Current configuration : 1449 bytes  version switch 10.4(3) Release(101069)(Wed Oct 20 09:12:40 CST 2010 -ngcf67)  co-operate enable  !  aaa new-model  aaa domain enable  !  aaa domain domain.com  authentication dot1x default  accounting network list3  !  aaa accounting network list3 start-stop group radius  aaa authentication dot1x default group radius  !  nfpp  !  no service password-encryption </pre> |

```
!  
radius-server host 10.1.1.1  
radius-server key test  
!  
line con 0  
line vty 0 4  
!  
end
```

## Common Errors

---

N/A

## 1.5 Monitoring

### Clearing

---

| Description              | Command  |
|--------------------------|--|
| Clears the locked users. | <b>clear aaa local user lockout {all   user-name <i>username</i> }</b> |

### Displaying

---

| Description                                 | Command                           |
|---|-----------------------------------|
| Displays the accounting update information. | <b>show aaa accounting update</b> |
| Displays the current domain configuration.  | <b>show aaa domain</b>            |
| Displays the current lockout configuration. | <b>show aaa lockout</b>           |
| Displays the AAA server groups.             | <b>show aaa group</b>             |
| Displays the AAA method lists.              | <b>show aaa method-list</b>       |
| Displays the AAA users.                     | <b>show aaa user</b>              |

## 2 Configuring RADIUS

### 2.1 Overview

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system.

RADIUS works with the Authentication, Authorization, and Accounting (AAA) to conduct identity authentication on users who attempt to access a network, to prevent unauthorized access. In switch implementation, a RADIUS client runs on a device or Network Access Server (NAS) and transmits identity authentication requests to the central RADIUS server, where all user identity authentication information and network service information are stored. In addition to the authentication service, the RADIUS server provides authorization and accounting services for access users.

RADIUS is often applied in network environments that have high security requirements and allow the access of remote users. RADIUS is a completely open protocol and the RADIUS server is installed on many operating systems as a component, for example, on UNIX, Windows 2000, and Windows 2008. Therefore, RADIUS is the most widely applied security server currently.

The Dynamic Authorization Extensions to Remote Authentication Dial In User Service is defined in the IETF RFC3576. This protocol defines a user offline management method. Devices communicate with the RADIUS server through the Disconnect Messages (DMs) to bring authenticated users offline. This protocol implements compatibility between devices of different vendors and the RADIUS server in terms of user offline processing.

In the DM mechanism, the RADIUS server actively initiates a user offline request to a device, the device locates a user according to the user session information, user name, and other information carried in the request and brings the user offline. Then, the device returns a response packet that carries the processing result to the RADIUS server, thereby implementing user offline management of the RADIUS server.

#### Protocols and Standards

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

### 2.2 Applications

| Application   | Description   |
|---|---|
| <a href="#">Providing Authentication, Authorization, and Accounting Services for Access Users</a> | Authentication, authorization, and accounting are conducted on access users on a network, to prevent unauthorized access or operations. |

---

| Application                                 | Description  |
|---|--|
| <a href="#">Forcing Users to Go Offline</a> | The server forces an authenticated user to go offline. |

## 2.2.1 Forcing Users to Go Offline

### Scenario

The RADIUS server forces authenticated online users to go offline for the sake of management.

See Figure 2-18 for the networking topology.

### Deployment

- Add the following deployment on the basis of 1.2.1 "Deployment".
- Enable the RADIUS dynamic authorization extension function on the RADIUS client.

## 2.3 Features

### Basic Concepts

#### ↳ Client/Server Mode

- Client: A RADIUS client initiates RADIUS requests and usually runs on a device or NAS. It transmits user information to the RADIUS server, receives responses from the RADIUS server, and performs processing accordingly. The processing includes accepting user access, rejecting user access, or collecting more user information for the RADIUS server.
- Server: Multiple RADIUS clients map to one RADIUS server. The RADIUS server maintains the IP addresses and shared keys of all RADIUS clients as well as information on all authenticated users. It receives requests from a RADIUS client, conducts authentication, authorization, and accounting, and returns processing information to the RADIUS client.

#### ↳ Structure of RADIUS Packets

The following figure shows the structure of RADIUS packets.

| 8                       | 16         | 32bit  |
|-------------------------|------------|--------|
| Code                    | Identifier | Length |
| Authenticator (16bytes) |            |        |
| Attributes              |            |        |



- **Code:** Identifies the type of RADIUS packets, which occupies one byte. The following table lists the values and meanings.

| Code | Packet Type    | Code | Packet Type         |
|------|----------------|------|---------------------|
| 1    | Access-Request | 4    | Accounting-Request  |
| 2    | Access-Accept  | 5    | Accounting-Response |
| 3    | Access-Reject  | 11   | Access-Challenge    |

- **Identifier:** Indicates the identifier for matching request packets and response packets, which occupies one byte. The identifier values of request packets and response packets of the same type are the same.
- **Length:** Identifies the length of a whole RADIUS packet, which includes **Code**, **Identifier**, **Length**, **Authenticator**, and **Attributes**. It occupies two bytes. Bytes that are beyond the **Length** field will be truncated. If the length of a received packet is smaller than the value of **Length**, the packet is discarded.
- **Authenticator:** Verifies response packets of the RADIUS server by a RADIUS client, which occupies 16 bytes. This field is also used for encryption/decryption of user passwords.
- **Attributes:** Carries authentication, authorization, and accounting information, with the length unfixed. The **Attributes** field usually contains multiple attributes. Each attribute is represented in the Type, Length, Value (TLV) format. Type occupies one byte and indicates the attribute type. The following table lists common attributes of RADIUS authentication, authorization, and accounting. Length occupies one byte and indicates the attribute length, with the unit of bytes. Value indicates the attribute information.

| Attribute No. | Attribute Name     | Attribute No. | Attribute Name         |
|---------------|--------------------|---------------|------------------------|
| 1             | User-Name          | 43            | Acct-Output-Octets     |
| 2             | User-Password      | 44            | Acct-Session-Id        |
| 3             | CHAP-Password      | 45            | Acct-Authentic         |
| 4             | NAS-IP-Address     | 46            | Acct-Session-Time      |
| 5             | NAS-Port           | 47            | Acct-Input-Packets     |
| 6             | Service-Type       | 48            | Acct-Output-Packets    |
| 7             | Framed-Protocol    | 49            | Acct-Terminate-Cause   |
| 8             | Framed-IP-Address  | 50            | Acct-Multi-Session-Id  |
| 9             | Framed-IP-Netmask  | 51            | Acct-Link-Count        |
| 10            | Framed-Routing     | 52            | Acct-Input-Gigawords   |
| 11            | Filter-ID          | 53            | Acct-Output-Gigawords  |
| 12            | Framed-MTU         | 55            | Event-Timestamp        |
| 13            | Framed-Compression | 60            | CHAP-Challenge         |
| 14            | Login-IP-Host      | 61            | NAS-Port-Type          |
| 15            | Login-Service      | 62            | Port-Limit             |
| 16            | Login-TCP-Port     | 63            | Login-LAT-Port         |
| 18            | Reply-Message      | 64            | Tunnel-Type            |
| 19            | Callback-Number    | 65            | Tunnel-Medium-Type     |
| 20            | Callback-ID        | 66            | Tunnel-Client-Endpoint |
| 22            | Framed-Route       | 67            | Tunnel-Server-Endpoint |
| 23            | Framed-IPX-Network | 68            | Acct-Tunnel-Connection |

| Attribute No. | Attribute Name           | Attribute No. | Attribute Name           |
|---------------|--------------------------|---------------|--------------------------|
| 24            | State                    | 69            | Tunnel-Password          |
| 25            | Class                    | 70            | ARAP-Password            |
| 26            | Vendor-Specific          | 71            | ARAP-Features            |
| 27            | Session-Timeout          | 72            | ARAP-Zone-Access         |
| 28            | Idle-Timeout             | 73            | ARAP-Security            |
| 29            | Termination-Action       | 74            | ARAP-Security-Data       |
| 30            | Called-Station-Id        | 75            | Password-Retry           |
| 31            | Calling-Station-Id       | 76            | Prompt                   |
| 32            | NAS-Identifier           | 77            | Connect-Info             |
| 33            | Proxy-State              | 78            | Configuration-Token      |
| 34            | Login-LAT-Service        | 79            | EAP-Message              |
| 35            | Login-LAT-Node           | 80            | Message-Authenticator    |
| 36            | Login-LAT-Group          | 81            | Tunnel-Private-Group-id  |
| 37            | Framed-AppleTalk-Link    | 82            | Tunnel-Assignment-id     |
| 38            | Framed-AppleTalk-Network | 83            | Tunnel-Preference        |
| 39            | Framed-AppleTalk-Zone    | 84            | ARAP-Challenge-Response  |
| 40            | Acct-Status-Type         | 85            | Acct-Interim-Interval    |
| 41            | Acct-Delay-Time          | 86            | Acct-Tunnel-Packets-Lost |
| 42            | Acct-Input-Octets        | 87            | NAS-Port-Id              |

### ↳ Shared Key

A RADIUS client and a RADIUS server mutually confirm their identities by using a shared key during communication. The shared key cannot be transmitted over a network. In addition, user passwords are encrypted for transmission for the sake of security.

### ↳ RADIUS Server Group

The RADIUS security protocol, also called RADIUS method, is configured in the form of a RADIUS server group. Each RADIUS method corresponds to one RADIUS server group and one or more RADIUS servers can be added to one RADIUS server group. For details about the RADIUS method, see the *Configuring AAA*. If you add multiple RADIUS servers to one RADIUS server group, when the communication between a device and the first RADIUS server in this group fails or the first RADIUS server becomes unreachable, the device automatically attempts to communicate with the next RADIUS server till the communication is successful or the communication with all the RADIUS servers fails.

### ↳ RADIUS Attribute Type

- Standard attributes

The RFC standards specify the RADIUS attribute numbers and attribute content but do not specify the format of some attribute types. Therefore, the format of attribute contents needs to be configured to adapt to different RADIUS server requirements. Currently, the format of the RADIUS Calling-Station-ID attribute (attribute No.: 31) can be configured.

The RADIUS Calling-Station-ID attribute is used to identify user identities when a network device transmits request packets to the RADIUS server. The RADIUS Calling-Station-ID attribute is a string, which can adopt multiple formats. It needs to uniquely identify a user. Therefore, it is often set to the MAC address of a user. For example, when IEEE 802.1X

authentication is used, the Calling-Station-ID attribute is set to the MAC address of the device where the IEEE 802.1X client is installed. The following table describes the format of MAC addresses.

| Format      | Description  |
|-------------|--|
| ietf        | Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example:<br>00-D0-F8-33-22-AC             |
| Normal      | Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example:<br>00d0.f833.22ac |
| Unformatted | Indicates the format without separators. This format is used by default. Example:<br>00d0f83322ac  |

- Private attributes

RADIUS is an extensible protocol. According to RFC2865, the Vendor-Specific attribute (attribute No.: 26) is used by device vendors to extend the RADIUS protocol to implement private functions or functions that are not defined in the standard RADIUS protocol. Table 1-3 lists private attributes supported by Orion Alpha A28X products. The **TYPE** column indicates the default configuration of private attributes of Orion Alpha A28X products and the **Extended TYPE** column indicates the default configuration of private attributes of other non-Orion Alpha A28X products.

| ID | Function                   | TYPE | Extended TYPE |
|----|----------------------------|------|---------------|
| 1  | max-down-rate              | 1    | 76            |
| 2  | port-priority              | 2    | 77            |
| 3  | user-ip                    | 3    | 3             |
| 4  | vlan-id                    | 4    | 4             |
| 5  | last-supplciant-version    | 5    | 5             |
| 6  | net-ip                     | 6    | 6             |
| 7  | user-name                  | 7    | 7             |
| 8  | password                   | 8    | 8             |
| 9  | file-directory             | 9    | 9             |
| 10 | file-count                 | 10   | 10            |
| 11 | file-name-0                | 11   | 11            |
| 12 | file-name-1                | 12   | 12            |
| 13 | file-name-2                | 13   | 13            |
| 14 | file-name-3                | 14   | 14            |
| 15 | file-name-4                | 15   | 15            |
| 16 | max-up-rate                | 16   | 16            |
| 17 | current-supplciant-version | 17   | 17            |
| 18 | flux-max-high32            | 18   | 18            |
| 19 | flux-max-low32             | 19   | 19            |
| 20 | proxy-avoid                | 20   | 20            |
| 21 | dailup-avoid               | 21   | 21            |
| 22 | ip-privilege               | 22   | 22            |

| ID  | Function               | TYPE | Extended TYPE |
|-----|------------------------|------|---------------|
| 23  | login-privilege        | 42   | 42            |
| 26  | ipv6-multicast-address | 79   | 79            |
| 27  | ipv4-multicast-address | 87   | 87            |
| 62  | sdg-type               | 62   | 62            |
| 85  | sdg-zone-name          | 85   | 85            |
| 103 | sdg-group-name         | 103  | 103           |

## Overview

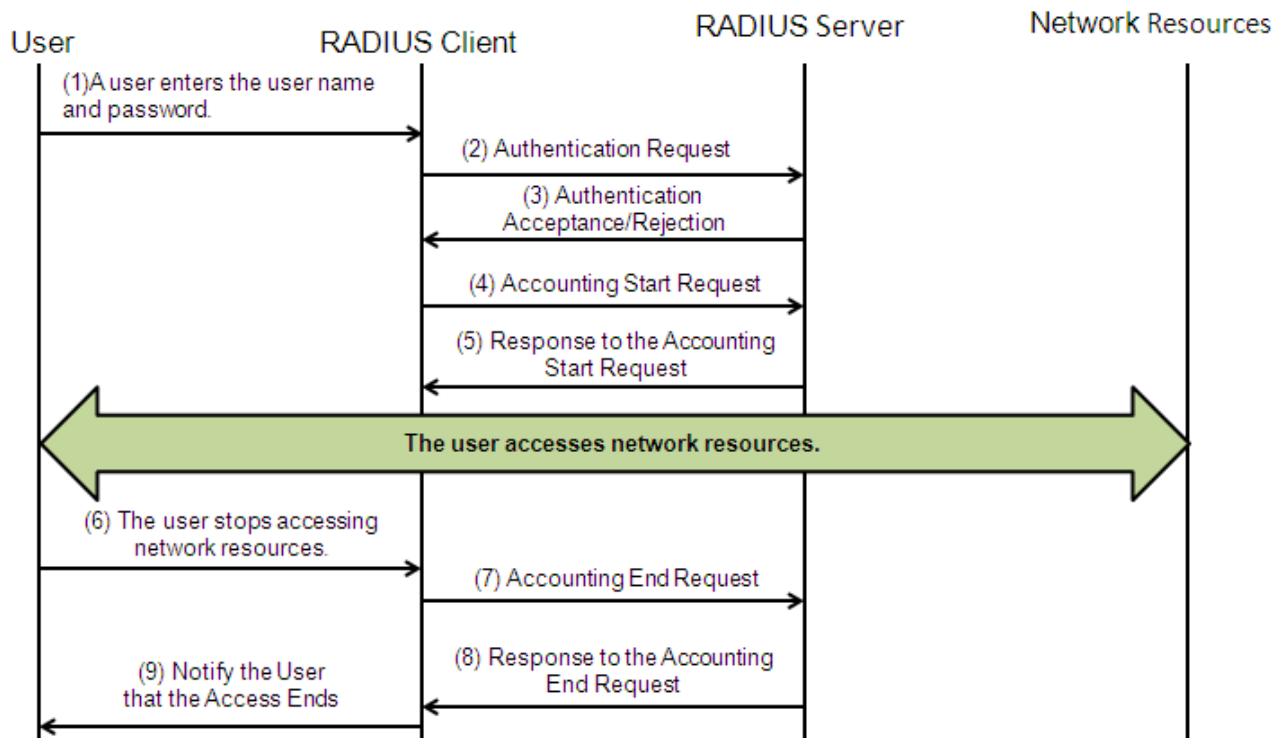
| Feature  | Description  |
|--|--|
| <a href="#">RADIUS Authentication, Authorization, and Accounting</a> | Conducts identity authentication and accounting on access users, safeguards network security, and facilitates management for network administrators.   |
| <a href="#">Source Address of RADIUS Packets</a>                     | Specifies the source IP address used by a RADIUS client to transmit packets to a RADIUS server.  |
| <a href="#">RADIUS Timeout Retransmission</a>                        | Specifies the packet retransmission parameter for a RADIUS client when a RADIUS server does not respond to packets transmitted from the RADIUS client within a period of time.   |
| <a href="#">RADIUS Server Accessibility Detection</a>                | Enables a RADIUS client to actively detect whether a RADIUS server is reachable and maintain the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services. |
| <a href="#">RADIUS Forced Offline</a>                                | Enables a RADIUS server to actively force authenticated users to go offline.   |

### 2.3.1 RADIUS Authentication, Authorization, and Accounting

Conduct identity authentication and accounting on access users, safeguard network security, and facilitate management for network administrators.

## Working Principle

Figure 2-16



The RADIUS authentication and authorization process is described as follows:

6. A user enters the user name and password and transmits them to the RADIUS client.
7. After receiving the user name and password, the RADIUS client transmits an authentication request packet to the RADIUS server. The password is encrypted for transmission. For the encryption method, see RFC2865.
8. The RADIUS server accepts or rejects the authentication request according to the user name and password. When accepting the authentication request, the RADIUS server also issues authorization information apart from the authentication acceptance information. The authorization information varies with the type of access users.

The RADIUS accounting process is described as follows:

9. If the RADIUS server returns authentication acceptance information in Step (3), the RADIUS client sends an accounting start request packet to the RADIUS server immediately.
10. The RADIUS server returns the accounting start response packet, indicating accounting start.
11. The user stops accessing network resources and requests the RADIUS client to disconnect the network connection.
12. The RADIUS client transmits the accounting end request packet to the RADIUS server.
13. The RADIUS server returns the accounting end response packet, indicating accounting end.
14. The user is disconnected and cannot access network resources.

## Related Configuration

### ↳ [Configuring RADIUS Server Parameters](#)

No RADIUS server is configured by default.

You can run the **radius-server host** command to configure a RADIUS server.

At least one RADIUS server must be configured so that RADIUS services run normally.

### ↳ [Configuring the AAA Authentication Method List](#)

No AAA authentication method list is configured by default.

You can run the **aaa authentication** command to configure a method list for different user types and select **group radius** when setting the authentication method.

The RADIUS authentication can be conducted only after the AAA authentication method list of relevant user types is configured.

### ↳ [Configuring the AAA Authorization Method List](#)

No AAA authorization method list is configured by default.

You can run the **aaa authorization** command to configure an authorization method list for different user types and select **group radius** when setting the authorization method.

The RADIUS authorization can be conducted only after the AAA authorization method list of relevant user types is configured.

### ↳ [Configuring the AAA Accounting Method List](#)

No AAA accounting method list is configured by default.

You can run the **aaa accounting** command to configure an accounting method list for different user types and select **group radius** when setting the accounting method.

The RADIUS accounting can be conducted only after the AAA accounting method list of relevant user types is configured.

## 2.3.2 Source Address of RADIUS Packets

Specify the source IP address used by a RADIUS client to transmit packets to a RADIUS server.

### Working Principle

When configuring RADIUS, specify the source IP address to be used by a RADIUS client to transmit RADIUS packets to a RADIUS server, in an effort to reduce the workload of maintaining a large amount of NAS information on the RADIUS server.

### Related Configuration

The global routing is used to determine the source address for transmitting RADIUS packets by default.

Run the **ip radius source-interface** command to specify the source interface for transmitting RADIUS packets. The device uses the first IP address of the specified interface as the source address of RADIUS packets.

---

## 2.3.3 RADIUS Timeout Retransmission

### Working Principle

After a RADIUS client transmits a packet to a RADIUS server, a timer is started to detect the response of the RADIUS server. If the RADIUS server does not respond within a certain period of time, the RADIUS client retransmits the packet.

### Related Configuration

#### ↳ **Configuring the RADIUS Server Timeout Time**

The default timeout time is 5 seconds.

You can run the **radius-server timeout** command to configure the timeout time. The value ranges from 1 second to 1,000 seconds.

The response time of a RADIUS server is relevant to its performance and the network environment. Set an appropriate timeout time according to actual conditions.

#### ↳ **Configuring the Retransmission Count**

The default retransmission count is 3.

You can run the **radius-server retransmit** command to configure the retransmission count. The value ranges from 1 to 100.

#### ↳ **Configuring Whether to Retransmit Accounting Update Packets**

Accounting update packets are not retransmitted by default.

You can run the **radius-server account update retransmit** command to configure retransmission of accounting update packets for authenticated users.

## 2.3.4 RADIUS Server Accessibility Detection

### Working Principle

A RADIUS client actively detects whether a RADIUS server is reachable and maintains the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.

### Related Configuration

#### ↳ **Configuring the Criteria for the Device to Judge That a RADIUS Server Is Unreachable**

The default criteria configured for judging that a RADIUS server is unreachable meet the two conditions simultaneously: 1. The device does not receive a correct response packet from the RADIUS security server within 60 seconds. 2. The device transmits the request packet to the same RADIUS security server for consecutive 10 times.

You can run the **radius-server dead-criteria** command to configure the criteria for the device to judge that the RADIUS security server is unreachable.

#### ↳ **Configuring the Test User Name for Actively Detecting the RADIUS Security Server**

No test user name is specified for actively detecting the RADIUS security server by default.

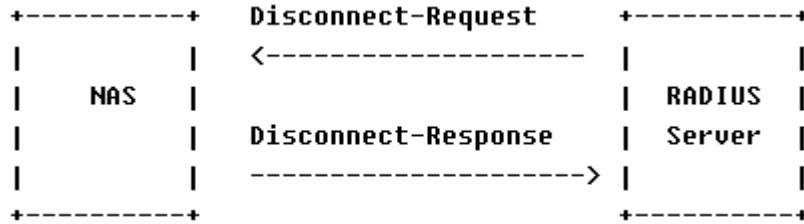
---

You can run the `radius-server host x.x.x.testusername xxx` command to configure the test user name.

## 2.3.5 RADIUS Forced Offline

### Working Principle

Figure 2-17 DM Message Exchange of the RADIUS Dynamic Authorization Extension Protocol



The preceding figure shows the exchange of DM messages between the RADIUS server and the device. The RADIUS server transmits the Disconnect-Request message to UDP Port 3799 of the device. After processing, the device returns the Disconnect-Response message that carries the processing result to the RADIUS server.

### Related Configuration

N/A

## 2.4 Configuration

| Configuration   | Description and Command  |   |
|---|--|---|
| <a href="#">RADIUS Basic Configuration</a>            | <ul style="list-style-type: none"> <li>(Mandatory) It is used to configure RADIUS authentication, authorization, and accounting.</li> </ul>                            |   |
|   | <code>radius-serverhost</code>   | Configures the IP address of the remote RADIUS security server.   |
|   | <code>radius-serverkey</code>  | Configures the shared key for communication between the device and the RADIUS server.                           |
|   | <code>radius-serverretransmit</code>   | Configures the request transmission count, after which the device confirms that a RADIUS server is unreachable. |
|   | <code>radius-servertimeout</code>  | Configures the waiting time, after which the device retransmits a request.                                      |
|   | <code>radius-server account update retransmit</code>   | Configures retransmission of accounting update packets for authenticated users.                                 |
|   | <code>ip radius source-interface</code>  | Configures the source address of RADIUS packets.  |
| <a href="#">Configuring the RADIUS Attribute Type</a> | <ul style="list-style-type: none"> <li>(Optional) It is used to define attribute processing adopted when the device encapsulates and parses RADIUS packets.</li> </ul> |   |
|   | <code>radius-serverattribute31</code>  | Configures the MAC address format of RADIUS attribute No. 31 (Calling-Station-ID).                              |



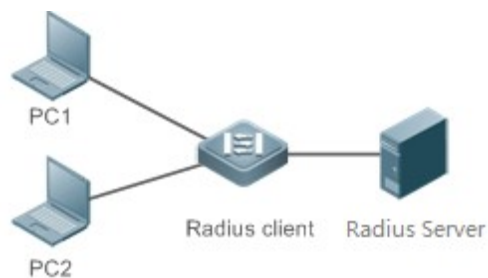
| Configuration  | Description and Command   |   |
|--|---|---|
|  | <b>radius-server attribute class</b>  | Configures the parsing mode of the RADIUS Class attribute.  |
|  | <b>radius attribute</b>   | Configures the RADIUS private attribute type.   |
|  | <b>radius set qoscos</b>  | Sets the private attribute port-priority issued by the server to the COS value of an interface. For COS-relevant concepts, see the <i>Configuring QoS</i> . |
|  | <b>radius support cui</b>   | Configures the device to support the CUI attribute.   |
|  | <b>radius-server authentication attribute</b>   | Configures whether RADIUS authentication request packets carry a specified attribute.   |
|  | <b>radius-server account attribute</b>  | Configures whether RADIUS accounting request packets carry a specified attribute.   |
|  | <b>radius-server authentication vendor</b>  | Configures whether RADIUS authentication request packets carry the private attributes of other vendors.   |
|  | <b>radius-server account vendor</b>   | Configures whether RADIUS accounting request packets carry the private attributes of other vendors.   |
| <a href="#">Configuring RADIUS Accessibility Detection</a> | <ul style="list-style-type: none"> <li>• (Optional) It is used to detect whether a RADIUS server is reachable and maintain the accessibility of the RADIUS server.</li> </ul> |   |
|  | <b>radius-server dead-criteria</b>  | Configures the global criteria for judging that a RADIUS security server is unreachable.  |
|  | <b>radius-server deadtime</b>   | Configures the duration for the device to stop transmitting request packets to an unreachable RADIUS server.  |
|  | <b>radius-server host</b>   | Configures the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.                      |

## 2.4.1 Providing Authentication, Authorization, and Accounting Services for Access Users

### Scenario

RADIUS is typically applied in the authentication, authorization, and accounting of access users. A network device serves as a RADIUS client and transmits user information to a RADIUS server. After completing processing, the RADIUS server returns the authentication acceptance/authentication rejection/accounting response information to the RADIUS client. The RADIUS client performs processing on the access user according to the response from the RADIUS server.

Figure 2-18 Typical RADIUS Networking Topology



|                |  |
|----------------|--|
| <b>Remarks</b> | <p>PC 1 and PC 2 are connected to the RADIUS client as access users in wired or wireless mode, and initiate authentication and accounting requests.</p> <p>The RADIUS client is usually an access switch or aggregate switch.</p> <p>The RADIUS server can be a component built in the Windows 2000/2003, Server (IAS), or UNIX operating system or dedicated server software provided by vendors.</p> |
|----------------|--|

## Deployment

- Configure access device information on the RADIUS server, including the IP address and shared key of the access devices.
- Configure the AAA method list on the RADIUS client.
- Configure the RADIUS server information on the RADIUS client, including the IP address and shared key.
- Enable access control on the access port of the RADIUS client.
- Configure the network so that the RADIUS client communicates with the RADIUS server successfully.

## 2.4.2 RADIUS Basic Configuration

### Configuration Effect

- RADIUS authentication, authorization, and accounting can be conducted after RADIUS basic configuration is complete.

### Notes

- Before configuring RADIUS on the device, ensure that the network communication of the RADIUS server is in good condition.
- When running the **ip radius source-interface** command to configure the source address of RADIUS packets, ensure that the device of the source IP address communicates with the RADIUS server successfully.
- When conducting RADIUS IPv6 authentication, ensure that the RADIUS server supports RADIUS IPv6 authentication.

### Configuration Steps

#### ↘ Configuring the Remote RADIUS Security Server

- Mandatory.
- Configure the IP address, authentication port, accounting port, and shard key of the RADIUS security server.

#### ↘ Configuring the Shared Key for Communication Between the Device and the RADIUS Server

- Optional.
- Configure a shared key in global configuration mode for servers without a shared key.
- The shared key on the device must be consistent with that on the RADIUS server.

#### ↘ **Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable**

- Optional.
- Configure the request transmission count, after which the device confirms that a RADIUS server is unreachable, according to the actual network environment.

#### ↘ **Configuring the Waiting Time, After which the Device Retransmits a Request**

- Optional.
- Configure the waiting time, after which the device retransmits a request, according to the actual network environment.
- In an 802.1X authentication environment that uses the RADIUS security protocol, if a network device serves as the 802.1X authenticator and Orion Alpha A28X SU is used as the 802.1X client software, it is recommended that **radius-server timeout** be set to 3 seconds (the default value is 5 seconds) and **radius-server retransmit** be set to 2 (the default value is 3) on the network device.

#### ↘ **Configuring Retransmission of Accounting Update Packets for Authenticated Users**

- Optional.
- Determine whether to enable the function of retransmitting accounting update packets of authenticated users according to actual requirements.

#### ↘ **Configuring the Source Address of RADIUS Packets**

- Optional.
- Configure the source address of RADIUS packets according to the actual network environment.

### Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to confirm that the device communicates with the RADIUS server over the RADIUS protocol.

### Related Commands

#### ↘ **Configuring the Remote RADIUS Security Server**

|                    |   |
|--------------------|---|
| <b>Command</b>     | <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i> } [ <b>auth-port</b> <i>port-number</i> ] [ <b>acct-port</b> <i>port-number</i> ][ <b>test</b> <i>username</i> <i>name</i> [ <b>idle-time</b> <i>time</i> ] [ <b>ignore-auth-port</b> ] [ <b>ignore-acct-port</b> ] ] [ <b>key</b> [ <b>0</b>   <b>7</b> ] <i>text-string</i> ] |
| <b>Parameter</b>   | <i>ipv4-address</i> : Indicates the IPv4 address of the RADIUS security server.   |
| <b>Description</b> | <i>ipv6-address</i> : Indicates the IPv6 address of the RADIUS security server.   |

|                     |  |
|---------------------|--|
|                     | <p><b>auth-port</b> <i>port-number</i>: Indicates the UDP port for RADIUS identity authentication. The value ranges from 0 to 65,535. If it is set to <b>0</b>, the host does not conduct identity authentication.</p> <p><b>acct-port</b> <i>port-number</i>: Indicates the UDP port for RADIUS accounting. The value ranges from 0 to 65,535. If it is set to <b>0</b>, the host does not conduct accounting.</p> <p><b>test username</b> <i>name</i>: Enables the function of actively detecting the RADIUS security server and specifies the user name used for active detection.</p> <p><b>idle-time</b> <i>time</i>: Indicates the interval for the device to transmit test packets to a reachable RADIUS security server. The default value is 60 minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).</p> <p><b>ignore-auth-port</b>: Disables the function of detecting the authentication port of the RADIUS security server. It is enabled by default.</p> <p><b>ignore-acct-port</b>: Disables the function of detecting the accounting port of the RADIUS security server. It is enabled by default.</p> <p><b>key</b> [ <b>0</b>   <b>7</b> ] <i>text-string</i> : Configures the shared key of the server. The global shared key is used if it is not configured.</p> |
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | A RADIUS security server must be defined to implement the AAA security service by using RADIUS. You can run the <b>radius-server host</b> command to define one or more RADIUS security servers.   |

#### ↘ Configuring the Shared Key for Communication Between the Device and the RADIUS Server

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server key</b> [ <b>0</b>   <b>7</b> ] <i>text-string</i>  |
| <b>Parameter Description</b> | <p><i>text-string</i>: Indicates the text of the shared key.</p> <p><b>0</b>   <b>7</b>: Indicates the encryption type of the key. The value <b>0</b> indicates no encryption and <b>7</b> indicates simple encryption. The default value is <b>0</b>.</p> |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | A shared key is the basis for correct communication between the device and the RADIUS security server. The same shared key must be configured on the device and RADIUS security server so that they can communicate with each other successfully.          |

#### ↘ Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server retransmit</b> <i>retries</i>   |
| <b>Parameter Description</b> | <i>retries</i> : Indicates the RADIUS retransmission count. The value ranges from 1 to 100.  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | The prerequisite for AAA to use the next user authentication method is that the current security server used for authentication does not respond. The criteria for the device to judge that a security server does not respond are that the security server does not respond within the RADIUS packet retransmission duration of the specified retransmission count. There is an interval between consecutive two retransmissions. |

#### ↘ Configuring the Waiting Time, After which the Device Retransmits a Request

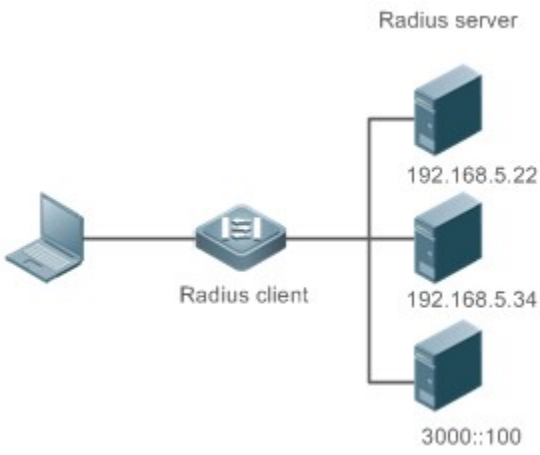
|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>radius-server timeoutseconds</b>   |
| <b>Parameter Description</b> | <i>seconds</i> : Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds. |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Use this command to adjust the packet retransmission timeout time.  |

### ↳ Configuring Retransmission of Accounting Update Packets for Authenticated Users

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server account update retransmit</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Configure retransmission of accounting update packets for authenticated users. Accounting update packets are not retransmitted by default. The configuration does not affect users of other types. |

## Configuration Example

### ↳ Using RADIUS Authentication, Authorization, and Accounting for Login Users

|                                |  |
|--------------------------------|--|
| <b>Scenario</b><br>Figure 2-19 |  <p>The diagram illustrates a network setup for RADIUS authentication. On the left, a laptop is connected to a central device labeled 'Radius client'. This client is connected to three separate servers under the heading 'Radius server'. The servers are labeled with their IP addresses: 192.168.5.22, 192.168.5.34, and 3000::100.</p> |
| <b>Configuration Steps</b>     | <ul style="list-style-type: none"> <li>● Enable AAA.</li> <li>● Configure the RADIUS server information.</li> <li>● Configure to use the RADIUS authentication, authorization, and accounting methods.</li> <li>● Apply the configured authentication method on the interface.</li> </ul>  |
| <b>RADIUS Client</b>           | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X (config)#aaa new-model Orion Alpha A28X (config)# radius-server host 192.168.5.22 Orion Alpha A28X (config)#radius-server host 3000::100 Orion Alpha A28X (config)# radius-server key aaa </pre>  |

|                     |  |
|---------------------|--|
|                     | <pre> Orion Alpha A28X (config)#aaa authentication login test group radius Orion Alpha A28X (config)#aaa authorizationexecetest group radius Orion Alpha A28X (config)#aaa accountingexecetest start-stop group radius Orion Alpha A28X (config)# line vty 0 4 Orion Alpha A28X (config-line)#login authentication test Orion Alpha A28X (config-line)# authorization exec test Orion Alpha A28X (config-line)# accounting exec test </pre>  |
| <b>Verification</b> | <p>Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. After obtaining a certain access level granted by the server, only run commands under this access level. Display the authentication log of the user on the RADIUS server. Perform management operations on the device as the user and then log out. Display the accounting information on the user on the RADIUS server.</p> |
|                     | <pre> Orion Alpha A28X#show running-config ! radius-server host 192.168.5.22 radius-server host 3000::100 radius-server key aaa aaa new-model aaa accounting exec test start-stop group radius aaa authorization exec test group radius aaa authentication login test group radius no service password-encryption iptcp not-send-rst ! vlan 1 ! line con 0 line vty 0 4 accounting exec test authorization exec test login authentication test ! </pre>  |

## Common Errors

---

- The key configured on the device is inconsistent with that configured on the server.
- No method list is configured.

### 2.4.3 Configuring the RADIUS Attribute Type

#### Configuration Effect

---

- Define the attribute processing adopted when the device encapsulates and parses RADIUS packets.

#### Notes

---

- Private attributes involved in "Configuring the RADIUS Attribute Type" refer to Orion Alpha A28X private attributes.

#### Configuration Steps

---

##### ↘ Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

- Optional.
- Set the MAC address format of **Calling-Station-Id** to a type supported by the server.

##### ↘ Configuring the Parsing Mode of the RADIUS Class Attribute

- Optional.
- Configure the parsing mode of the Class attribute according to the server type.

##### ↘ Configuring the RADIUS Private Attribute Type

- Optional.
- If the server is a Orion Alpha A28X application server, the RADIUS private attribute type needs to be configured.

##### ↘ Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

- Optional.
- Set the private attribute **port-priority** issued by the server to the COS value of an interface as required.

##### ↘ Configures the Device to Support the CUI Attribute

- Optional.
- Configure whether the device supports the RADIUS CUI attribute as required.

##### ↘ Configuring the Mode of Parsing Private Attributes by the Device

- Optional.
- Configure the index of a Orion Alpha A28X private attribute parsed by the device as required.

##### ↘ Configuring Whether RADIUS Authentication Request Packets Carry a Specified Attribute

- Optional.
-

- Configure whether to specify the attribute type for RADIUS authentication request packets as required.

#### ↘ **Configuring Whether RADIUS Accounting Request Packets Carry a Specified Attribute**

- Optional.
- Configure whether to specify the attribute type for RADIUS accounting request packets as required.

#### ↘ **Configuring Whether RADIUS Authentication Request Packets Carry the Private Attribute of a Specified Vendor**

- Optional.
- Configure whether RADIUS authentication request packets carry the private attribute of a specified vendor as required.

#### ↘ **Configuring Whether RADIUS Accounting Request Packets Carry the Private Attribute of a Specified Vendor**

- Optional.
- Configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.

#### ↘ **Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft**

- Optional.
- Configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

#### ↘ **Configuring the Nas-Port-Id Encapsulation Format for RADIUS Packets**

- Optional.
- In either QINQ or non-QINQ scenarios, configure the nas-port-id encapsulation format for RADIUS packets. By default, the packets are encapsulated in the normal format.

### **Verification**

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to display the MAC address format of Calling-Station-Id.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that Orion Alpha A28X private attributes are correctly parsed by the device.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that the CUI attribute is correctly parsed by the device.

### **Related Commands**

#### ↘ **Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)**

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>radius-server attribute 31 mac format {ietf   normal   unformatted }</b>   |
| <b>Parameter Description</b> | <b>ietf:</b> Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC.<br><b>normal:</b> Indicates the common format that represents a MAC address (dotted hexadecimal format), which is |



|                     |  |
|---------------------|--|
|                     | separated by the separator (.). Example: 00d0.f833.22ac.<br><b>unformatted:</b> Indicates the format without separators. This format is used by default. Example: 00d0f83322ac.                  |
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | Some RADIUS security servers (mainly used for 802.1X authentication) can identify only MAC addresses in the IETF format. In this case, set the MAC address format of Calling-Station-ID to IETF. |

#### ↘ Configuring the Parsing Mode of the RADIUS Class Attribute

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server attribute class user-flow-control</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Configure this command if the server needs to issue the rate limit value by using the Class attribute. |

#### ↘ Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius set qos cos</b>  |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Configure this command to use the issued QoS value as the CoS value. The QoS value is used as the DSCP value by default. |

#### ↘ Configures the Device to Support the CUI Attribute

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius support cui</b>  |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Configure this command to enable the RADIUS-compliant device to support the CUI attribute. |

#### ↘ Configuring Whether RADIUS Authentication Request Packets Carry a Specified Attribute

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server authentication attribute <i>type</i> package</b><br><b>radius-server authentication attribute <i>type</i> unpackage</b> |
| <b>Parameter Description</b> | <b><i>type</i>:</b> Indicates the RADIUS attribute type. The value ranges from 1 to 255.   |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Use this command to specify the attribute to be carried in authentication request packets.   |

---

## ↘ Configuring Whether RADIUS Accounting Request Packets Carry a Specified Attribute

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server account attribute <i>type</i> package</b><br><b>radius-server account attribute <i>type</i> unpackage</b> |
| <b>Parameter Description</b> | <b><i>type</i></b> : Indicates the RADIUS attribute type. The value ranges from 1 to 255.                                  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Use this command to specify the attribute to be carried in accounting request packets.                                     |

## ↘ Configuring Whether RADIUS Authentication Request Packets Carry the Private Attribute of a Specified Vendor

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server authentication vendor <i>vendor_name</i> package</b>  |
| <b>Parameter Description</b> | <b><i>vendor_name</i></b> : Indicates the vendor name. It can be set to <b>cmcc</b> , <b>Microsoft</b> , or <b>cisco</b> . |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Use this command to configure whether authentication request packets carry the private attribute of a specified vendor.    |

## ↘ Configuring Whether RADIUS Accounting Request Packets Carry the Private Attribute of a Specified Vendor

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server account vendor <i>vendor_name</i> package</b>   |
| <b>Parameter Description</b> | <b><i>vendor_name</i></b> : Indicates the vendor name. It can be set to <b>cmcc</b> , <b>Microsoft</b> , or <b>cisco</b> . |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Use this command to configure whether accounting request packets carry the private attribute of a specified vendor.        |

## Configuration Example

### ↘ Configuring the RADIUS Attribute Type

|                            |  |
|----------------------------|--|
| <b>Scenario</b>            | One authentication device  |
| <b>Configuration Steps</b> | <ul style="list-style-type: none"><li>● Configure the MAC address format of RADIUS Calling-Station-Id.</li><li>● Configure the RADIUS private attribute type.</li><li>● Set the QoS value issued by the RADIUS server as the COS value of the interface.</li><li>● Configure the RADIUS function to support the CUI attribute.</li><li>● Configure the device to support private attributes of other vendors.</li><li>● Configure authentication requests not to carry the NAS-PORT-ID attribute.</li><li>● Configure accounting requests to carry the CMCC private attribute.</li><li>● Configure the RADIUS server not to parse Cisco's private attributes contained in packets.</li></ul> |

|                     |   |
|---------------------|---|
|                     | <ul style="list-style-type: none"> <li>● Configure application of the nas-port-id encapsulation format in a QINQ scenario.</li> </ul>   |
|                     | <pre>Orion Alpha A28X(config)#radius-server attribute 31 mac format ietf Orion Alpha A28X(config)#radius attribute 16 vendor-type 211 Orion Alpha A28X(config)#radiussetqoscos Orion Alpha A28X(config)#radiussupport cui Orion Alpha A28X(config)#radius-server authentication attribute 87 unpackage Orion Alpha A28X(config)#radius-server account vendor cmcc package</pre> |
| <b>Verification</b> | Conduct packet capture or display debug information of the device to check whether the RADIUS standard attributes and private attributes are encapsulated/parsed correctly.   |

## 2.4.4 Configuring RADIUS Accessibility Detection

### Configuration Effect

The device maintains the accessibility status of each configured RADIUS server: reachable or unreachable. The device will not transmit authentication, authorization, and accounting requests of access users to an unreachable RADIUS server unless all the other servers in the same RADIUS server group as the unreachable server are all unreachable.

The device actively detects a specified RADIUS server. The active detection function is disabled by default. If the active detection function is enabled for a specified RADIUS server, the device will, according to the configuration, periodically transmits detection requests (authentication requests or accounting requests) to the RADIUS server.

The transmission interval is as follows:

- For a reachable RADIUS server, the interval is the active detection interval of the reachable RADIUS server (the default value is 60 minutes).
- For an unreachable RADIUS server, the interval is always 1 minute.

### Notes

All the following conditions need to be met before the active detection function is enabled for a specified RADIUS server:

- The test user name of the RADIUS server is configured on the device.
- At least one tested port (authentication port or accounting port) of the RADIUS server is configured on the device.

If the following two conditions are all met, it is deemed that a reachable RADIUS server becomes unreachable:

- After the previous correct response is received from the RADIUS server, the time set in **radius-server dead-criteria time seconds** has elapsed.
- After the previous correct response is received from the RADIUS server, the count that the device transmits requests to the RADIUS server but fails to receive correct responses (including retransmission) reaches the value set in **radius-server dead-criteria tries number**.

If any of the following conditions is met, it is deemed that an unreachable RADIUS server becomes reachable:

- The device receives correct responses from the RADIUS server.

- The duration that the RADIUS server is in the unreachable state exceeds the time set in **radius-server deadtime** and the active detection function is disabled for the RADIUS server.
- The authentication port or accounting port of the RADIUS server is updated on the device.

## Configuration Steps

### ↳ Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable

- Mandatory.
- Configuring the global criteria for judging that a RADIUS security server is unreachable is a prerequisite for enabling the active detection function.

### ↳ Configuring the IP Address of the Remote RADIUS Security Server, Authentication Port, Accounting Port, and Active Detection Parameters

- Mandatory.
- Configuring active detection parameters of the RADIUS server is a prerequisite for enabling the active detection function.

### ↳ Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

- Optional.
- The configured duration for the device to stop transmitting request packets to an unreachable RADIUS server takes effect only when the active detection function is disabled for the RADIUS server.

## Verification

- Run the **show radius server** command to display the accessibility information of each RADIUS server.

## Related Commands

### ↳ Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable


|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>radius-server dead-criteria { timeseconds [ triesnumber ]   triesnumber }</b>   |
| <b>Parameter Description</b> | <p><b>timeseconds</b>: Indicates the time condition parameter. If the device fails to receive a correct response packet from a RADIUS security server within the specified time, it is deemed that the RADIUS security server meets the inaccessibility duration condition. The value ranges from 1 second to 120 seconds.</p> <p><b>triesnumber</b>: Indicates the consecutive request timeout count. If the timeout count of request packets transmitted by the device to the same RADIUS security server reaches the preset count, it is deemed that the RADIUS security server meets the consecutive timeout count condition of inaccessibility. The value ranges from 1 to 100.</p> |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | If a RADIUS security server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS security server is unreachable. Users can use this command to adjust parameter values in the duration condition and consecutive request timeout count condition.   |

## ↘ Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>radius-server deadtime</b> <i>minutes</i>  |
| <b>Parameter Description</b> | <i>minutes</i> : Indicates the duration for the device to stop transmitting requests to an unreachable RADIUS security server, with the unit of minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).  |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | If the active detection function is enabled for a RADIUS security server on the device, the time parameter in <b>radius-server deadtime</b> does not take effect on the RADIUS server. If the active detection function is disabled for a RADIUS security server, the device automatically restores the RADIUS security server to the reachable state when the duration that the RADIUS security server is in the unreachable state exceeds the time specified in <b>radius-server deadtime</b> . |

## Configuration Example

### ↘ Configuring Accessibility Detection on the RADIUS Server

|                                |  |
|--------------------------------|--|
| <b>Scenario</b><br>Figure 2-20 |  <p style="text-align: center;">192.168.5.22</p> <p style="text-align: center;">Radius client      Radius server</p>  |
| <b>Configuration Steps</b>     | <ul style="list-style-type: none"> <li>● Configure the global criteria for judging that a RADIUS security server is unreachable.</li> <li>● Configure the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.</li> </ul> |
| <b>RADIUS Client</b>           | <pre>Orion Alpha A28X(config)#radius-server dead-criteria time120 tries 5 Orion Alpha A28X(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90</pre>   |
| <b>Verification</b>            | <p>Disconnect the network communication between the device and the server with the IP address of 192.168.5.22. Conduct RADIUS authentication through the device. After 120 seconds, run the <b>show radius server</b> command to check that the server state is <b>dead</b>.</p>             |
|                                | <pre>Orion Alpha A28X#show running-config ... radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90 radius-server dead-criteria time 120 tries 5 ...</pre>  |

## 2.5 Monitoring

### Clearing

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

| Description   | Command  |
|---|--|
| Clears statistics of the RADIUS dynamic authorization extension function and restarts statistics. | <b>clear radius dynamic-authorization-extension statistics</b> |

### Displaying

| Description  | Command   |
|--|---|
| Displays global parameters of the RADIUS server.                                     | <b>show radius parameter</b>                                  |
| Displays the configuration of the RADIUS server.                                     | <b>show radius server</b>                                     |
| Displays statistics relevant to the RADIUS dynamic authorization extension function. | <b>show radius dynamic-authorization-extension statistics</b> |
| Displays statistics relevant to RADIUS authentication.                               | <b>show radius auth statistics</b>                            |
| Displays statistics relevant to RADIUS accounting.                                   | <b>show radius acct statistics</b>                            |
| Displays configuration of RADIUS server groups.                                      | <b>show radius group</b>                                      |
| Displays RADIUS standard attributes.   | <b>Show radius attribute</b>                                  |

### Debugging

- System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

| Description  | Command                              |
|--|--------------------------------------|
| Debugs the RADIUS event.   | <b>debugradiusevent</b>              |
| Debugs RADIUS packet printing.                                     | <b>debugradiusdetail</b>             |
| Debugs the RADIUS dynamic authorization extension function.        | <b>debug radiusextension event</b>   |
| Debugs the RADIUS dynamic authorization extension packet printing. | <b>debug radius extension detail</b> |

# 3 Configuring TACACS+

## 3.1 Overview

TACACS+ is a security protocol enhanced in functions based on the Terminal Access Controller Access Control System (TACACS) protocol. It is used to implement the authentication, authorization, and accounting (AAA) of multiple users.

### Protocols and Standards

- RFC 1492 Terminal Access Controller Access Control System

## 3.2 Applications

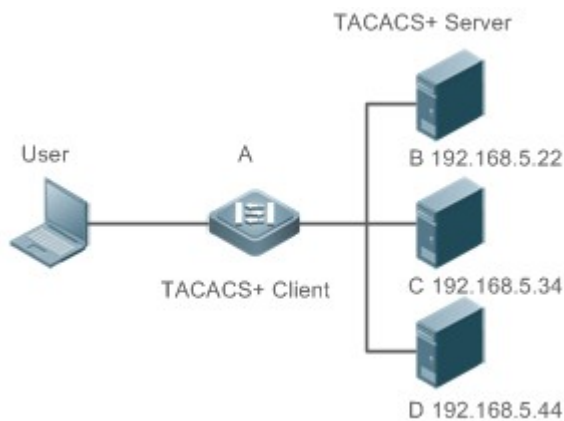
| Application   | Description  |
|---|--|
| <a href="#">Managing and Controlling Login of End Users</a> | Password verification and authorization need to be conducted on end users. |

### 3.2.1 Managing and Controlling Login of End Users

#### Scenario

TACACS+ is typically applied in the login management and control of end users. A network device serves as the TACACS+ client and sends a user name and password to the TACACS+ server for verification. The user is allowed to log in to the network device and perform operations after passing the verification and obtaining authorization. See the following figure.

Figure 3-1



| Remarks |   |
|---------|---|
|         | <ul style="list-style-type: none"><li>● A is a client that initiates TACACS+ requests.</li><li>● B, C, and D are servers that process TACACS+ requests.</li></ul> |

## Deployment

- Start the TACACS+ server on Server B, Server C, and Server D, and configure information on the access device (Device A) so that the servers provide TACACS+-based AAA function for the access device. Enable the AAA function on Device A to start authentication for the user login.
- Enable the TACACS+ client function on Device A, add the IP addresses of the TACACS+ servers (Server B, Server C, and Server D) and the shared key so that Device A communicates with the TACACS+ servers over TACACS+ to implement the AAA function.

## 3.3 Features

### Basic Concepts

#### Format of TACACS+ Packets

Figure 3-2

| 4          | 8     | 16          | 24           | 32 bit |
|------------|-------|-------------|--------------|--------|
| Major      | Minor | Packet type | Sequence no. | Flags  |
| Session ID |       |             |              |        |
| Length     |       |             |              |        |

- Major Version: Indicates the major TACACS+ version number.
- Minor Version: Indicates the minor TACACS+ version number.
- Packet Type: Indicates the type of packets, with the options including:  
TAC\_PLUS\_AUTHEN: = 0x01 (authentication);  
TAC\_PLUS\_AUTHOR: = 0x02 (authorization);  
TAC\_PLUS\_ACCT: = 0x03 (accounting)
- Sequence Number: Indicates the sequence number of a data packet in the current session. The sequence number of the first TACACS+ data packet in a session must be 1 and the sequence number of subsequent each data packet increases by one. Therefore, the client sends data packets only with an odd sequence number and TACACS+ Daemon sends packets only with an even sequence number.
- Flags: Contains various bitmap format flags. One of the bits in the value specifies whether data packets need to be encrypted.
- Session ID: Indicates the ID of a TACACS+ session.
- Length: Indicates the body length of a TACACS+ data packet (excluding the header). Packets are encrypted for transmission on a network.

### Overview

| Feature | Description |
|---------|-------------|
|---------|-------------|

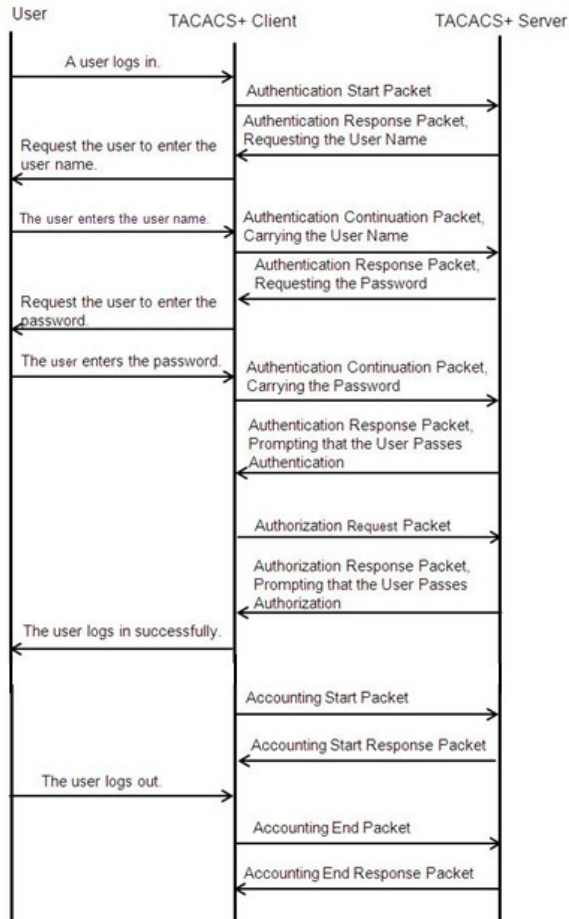


### 3.3.1 TACACS+ Authentication, Authorization, and Accounting

#### Working Principle

The following figure uses basic authentication, authorization, and accounting of user login to describe interaction of TACACS+ data packets.

Figure 3-3



The entire basic message interaction process includes three sections:

1. The authentication process is described as follows:
  - 1) A user requests to log in to a network device.
  - 2) After receiving the request, the TACACS+ client sends an authentication start packet to the TACACS+ server.
  - 3) The TACACS+ server returns an authentication response packet, requesting the user name.
  - 4) The TACACS+ client requests the user to enter the user name.
  - 5) The user enters the login user name.

- 6) After receiving the user name, the TACACS+ client sends an authentication continuation packet that carries the user name to the TACACS+ server.
- 7) The TACACS+ server returns an authentication response packet, requesting the login password.
- 8) The TACACS+ client requests the user to enter the login password.
- 9) The user enters the login password.
- 10) After receiving the login password, the TACACS+ client sends an authentication continuation packet that carries the login password to the TACACS+ server.
- 11) The TACACS+ server returns an authentication response packet, prompting that the user passes authentication.

| Configuration   | Description and Command   |   |
|---|---|---|
| <a href="#">Configuring TACACS+ Basic Functions</a>   | <ul style="list-style-type: none"> <li>● (Mandatory) It is used to enable the TACACS+ security service.</li> </ul>                                      |   |
|   | <b>tacacs-server host</b>   | Configures the TACACS+ server.  |
|   | <b>tacacs-server key</b>  | Specifies the key shared by the server and network device.  |
|   | <b>tacacs-server timeout</b>  | Configures the global waiting timeout time of the TACACS+ server for communication between a network device and the TACACS+ server. |
| <a href="#">Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+</a> | <ul style="list-style-type: none"> <li>● (Optional) It is used to separately process authentication, authorization, and accounting requests.</li> </ul> |   |
|   | <b>aaa group server tacacs+</b>   | Configures TACACS+ server groups and divides TACACS+ servers into different groups.   |
|   | <b>server</b>   | Adds servers to TACACS+ server groups.  |

2. The user authorization starts after successful authentication:
    - 1) The TACACS+ client sends an authorization request packet to the TACACS+ server.
    - 2) The TACACS+ server returns an authorization response packet, prompting that the user passes authorization.
    - 3) After receiving the authorization success packet, the TACACS+ client outputs the network device configuration screen for the user.
  3. Accounting and audit need to be conducted on the login user after successful authorization:
    - 1) The TACACS+ client sends an accounting start packet to the TACACS+ server.
    - 2) The TACACS+ server returns an accounting response packet, prompting that the accounting start packet has been received.
    - 3) The user logs out.
    - 4) The TACACS+ client sends an accounting end packet to the TACACS+ server.
    - 5) The TACACS+ server returns an accounting response packet, prompting that the accounting end packet has been received.
-

## 3.4 Configuration

### 3.4.1 Configuring TACACS+ Basic Functions

#### Configuration Effect

- The TACACS+ basic functions are available after the configuration is complete. When configuring the AAA method list, specify the method of using TACACS+ to implement TACACS+ authentication, authorization, and accounting.
- When authentication, authorization, and accounting operations are performed, TACACS+ initiates the authentication, authorization, and accounting requests to configured TACACS+ servers according to the configured sequence. If response timeout occurs on a TACACS+ server, TACACS+ traverses the TACACS+ server list in sequence.

#### Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

#### Configuration Steps

##### ↳ Enabling AAA

- Mandatory. The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

|                     |  |
|---------------------|--|
| <b>Command</b>      | <b>aaa new-model</b>   |
| <b>Parameter</b>    | N/A  |
| <b>Description</b>  |  |
| <b>Defaults</b>     | The AAA function is disabled.  |
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list. |

##### ↳ Configuring the IP Address of the TACACS+ Server

- Mandatory. Otherwise, a device cannot communicate with the TACACS+ server to implement the AAA function.

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i> } [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> [ <b>0</b>   <b>7</b> ] <i>text-string</i> ]  |
| <b>Parameter Description</b> | <i>ipv4-address</i> : Indicates the IPv4 address of the TACACS+ server.<br><i>ipv6-address</i> : Indicates the IPv6 address of the TACACS+ server.<br><b>port</b> <i>integer</i> : Indicates the TCP port used for TACACS+ communication. The default TCP port is 49.<br><b>timeout</b> <i>integer</i> : Indicates the timeout time of the communication with the TACACS+ server. The global timeout time is used by default. |

|                     |  |
|---------------------|--|
|                     | <b>key [ 0   7 ] text-string:</b> Indicates the shared key of the server. The global key is used if it is not configured. An encryption type can be specified for the configured key. The value <b>0</b> indicates no encryption and <b>7</b> indicates simple encryption. The default value is <b>0</b> .   |
| <b>Defaults</b>     | No TACACS+ server is configured.   |
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | <ol style="list-style-type: none"> <li>1. You can specify the shared key of the server when configuring the IP address of the server. If no shared key is specified, the global key configured using the <b>tacacs-server key</b> command is used as the shared key of the server. The shared key must be completely the same as that configured on the server.</li> <li>2. You can specify the communication port of the server when configuring the IP address.</li> <li>3. You can specify the communication timeout time of the server when configuring the IP address.</li> </ol> |

### ↘ Configuring the Shared Key of the TACACS+ Server

- Optional.
- If no global communication protocol is configured using this command, set **key** to specify the shared key of the server when running the **tacacs-server host** command to add server information. Otherwise, a device cannot communicate with the TACACS+ server.
- If no shared key is specified by using **key** when you run the **tacacs-server host** command to add server information, the global key is used.

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>tacacs-server [ key [ 0   7 ] text-string ]</b>  |
| <b>Parameter Description</b> | <i>text-string:</i> Indicates the text of the shared key.<br><b>0   7:</b> Indicates the encryption type of the key. The value <b>0</b> indicates no encryption and <b>7</b> indicates simple encryption. |
| <b>Defaults</b>              | No shared key is configured for any TACACS+ server.   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | This command is used to configure a global shared key for servers. To specify a different key for each server, set <b>key</b> when running the <b>tacacs-server host</b> command.                         |

### ↘ Configuring the Timeout Time of the TACACS+ Server

- Optional.
- You can set the timeout time to a large value when the link between the device and the server is unstable.

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>tacacs-server timeoutseconds</b>  |
| <b>Parameter Description</b> | <i>seconds:</i> Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.   |
| <b>Defaults</b>              | The default value is 5 seconds.  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | This command is used to configure the global server response timeout time. To set different timeout time for each server, set <b>timeout</b> when running the <b>tacacs-server host</b> command. |


## Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- Enable the device to interact with the TACACS+ server and conduct packet capture to check the TACACS+ interaction process between the device and the TACACS+ server.
- View server logs to check whether the authentication, authorization, and accounting are normal.

## Configuration Example

### ↳ Using TACACS+ for Login Authentication

|                               |  |
|-------------------------------|--|
| <b>Scenario</b><br>Figure 3-4 |  <p>The diagram illustrates the TACACS+ architecture. On the left, a laptop icon represents the 'User'. A horizontal line connects the laptop to a central device labeled 'A', which is identified as the 'TACACS+ Client'. Another horizontal line connects device 'A' to a server rack icon labeled 'B', identified as the 'TACACS+ Server' with the IP address '192.168.5.22'.</p> |
| <b>Remarks</b>                | <ul style="list-style-type: none"><li>● A is a client that initiates TACACS+ requests.</li><li>● B is a server that processes TACACS+ requests.</li></ul>  |
| <b>Configuration Steps</b>    | <ul style="list-style-type: none"><li>● Enable AAA.</li><li>● Configure the TACACS+ server information.</li><li>● Configure the method of using TACACS+ for authentication.</li><li>● Apply the configured authentication method on an interface.</li></ul>  |
| <b>A</b>                      | <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# aaa new-model Orion Alpha A28X(config)# tacacs-server host 192.168.5.22 Orion Alpha A28X(config)# tacacs-server key aaa Orion Alpha A28X(config)# aaa authentication login test group tacacs+ Orion Alpha A28X(config)# line vty 0 4 Orion Alpha A28X(config-line)# login authentication test</pre>  |
| <b>Verification</b>           | <p>Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. View the authentication log of the user on the TACACS+ server.</p>   |

## Common Errors

- The AAA security service is disabled.

- The key configured on the device is inconsistent with the key configured on the server.
- No method list is configured.

### 3.4.2 Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+

#### Configuration Effect

- The authentication, authorization, and accounting in the security service are processed by different TACACS+ servers, which improves security and achieves load balancing to a certain extent.

#### Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

#### Configuration Steps

##### ↳ Configuring TACACS+ Server Groups

- Mandatory. There is only one TACACS+ server group by default, which cannot implement separate processing of authentication, authorization, and accounting.
- Three TACACS+ server groups need to be configured for separately processing authentication, authorization, and accounting.

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>aaa group server tacacs+group-name</b>  |
| <b>Parameter Description</b> | <i>group-name</i> : Indicates the name of a group. A group name cannot be radius or tacacs+, which are the names of embedded groups. |
| <b>Defaults</b>              | No TACACS+ server group is configured.   |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Group TACACS+ servers so that authentication, authorization, and accounting are completed by different server groups.                |

##### ↳ Adding Servers to TACACS+ Server Groups

- Mandatory. If no server is added to a server group, a device cannot communicate with TACACS+ servers.
- In server group configuration mode, add the servers that are configured using the **tacacs-server host** command.

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>server {ipv4-address   ipv6-address}</b>  |
| <b>Parameter Description</b> | <i>ipv4-address</i> : Indicates the IPv4 address of the TACACS+ server.<br><i>ipv6-address</i> : Indicates the IPv6 address of the TACACS+ server. |
| <b>Defaults</b>              | No server is configured.   |
| <b>Command Mode</b>          | TACACS+ server group configuration mode  |

|                    |   |
|--------------------|---|
| <b>Usage Guide</b> | <p>Before configuring this command, you must run the <b>aaa group server tacacs+</b> command to enter the TACACS+ server group configuration mode.</p> <p>For the address of a server configured in a TACACS+ server group, the server must be configured using the <b>tacacs-server host</b> command in global configuration mode.</p> <p>If multiple servers are added to one server group, when one server does not respond, the device continues to send a TACACS+ request to another server in the server group.</p> |
|--------------------|---|

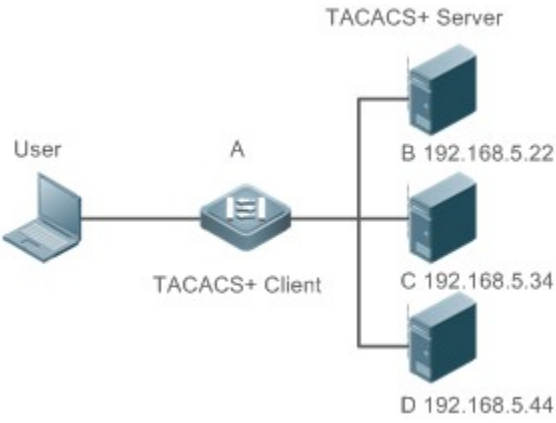
## Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- Enable a device to interact with TACACS+ servers. Conduct packet capture, check that the authentication, authorization, and accounting packets are interacted with different servers, and check the source addresses in packets.

## Configuration Example

### Configuring Different TACACS+ Server Groups for Separately Processing Authentication, Authorization, and Accounting

|                               |   |
|-------------------------------|---|
| <b>Scenario</b><br>Figure 3-5 |  <p>The diagram illustrates a network setup for TACACS+ services. On the left, a 'User' (represented by a laptop icon) is connected to a 'TACACS+ Client' (represented by a switch icon labeled 'A'). This client is then connected to a group of three 'TACACS+ Servers' (represented by server rack icons). The servers are labeled as follows: 'B 192.168.5.22', 'C 192.168.5.34', and 'D 192.168.5.44'. The connections show that the client 'A' is the central point for all TACACS+ requests, which are then distributed to the respective servers B, C, and D.</p> |
| <b>Remarks</b>                | <ul style="list-style-type: none"> <li>● A is a client that initiates TACACS+ requests.</li> <li>● B is a server that processes TACACS+ authentication requests.</li> <li>● C is a server that processes TACACS+ authorization requests.</li> <li>● D is a server that processes TACACS+ accounting requests.</li> </ul>  |
| <b>Configuration Steps</b>    | <ul style="list-style-type: none"> <li>● Enable AAA.</li> <li>● Configure the TACACS+ server information.</li> <li>● Configure TACACS+ server groups.</li> <li>● Add servers to TACACS+ server groups.</li> <li>● Configure the method of using TACACS+ for authentication.</li> <li>● Configure the method of using TACACS+ for authorization.</li> <li>● Configure the method of using TACACS+ for accounting.</li> <li>● Apply the configured authentication method on an interface.</li> </ul>  |

|                            |  |
|----------------------------|--|
|                            | <ul style="list-style-type: none"> <li>● Apply the configured authorization method on an interface.</li> <li>● Apply the configured accounting method on an interface.</li> </ul>  |
|                            | <pre> Orion Alpha A28X# configure terminal Orion Alpha A28X(Orion Alpha A28X(config)# aaa new-model Orion Alpha A28X(config)# tacacs-server host 192.168.5.22 Orion Alpha A28X(config)# tacacs-server host 192.168.5.34 Orion Alpha A28X(config)# tacacs-server host 192.168.5.44 Orion Alpha A28X(config)# tacacs-server key aaa Orion Alpha A28X(config)# aaa group server tacacs+ tacgrp1 Orion Alpha A28X(config-gs-tacacs)# server 192.168.5.22 Orion Alpha A28X(config-gs-tacacs)# exit Orion Alpha A28X(config)# aaa group server tacacs+ tacgrp2 Orion Alpha A28X(config-gs-tacacs)# server 192.168.5.34 Orion Alpha A28X(config-gs-tacacs)# exit Orion Alpha A28X(config)# aaa group server tacacs+ tacgrp3 Orion Alpha A28X(config-gs-tacacs)# server 192.168.5.44 Orion Alpha A28X(config-gs-tacacs)# exit Orion Alpha A28X(config)# aaa authentication login test1 group tacacs+ Orion Alpha A28X(config)# aaa authentication enable default group tacgrp1 Orion Alpha A28X(config)# aaa authorization exec test2 group tacgrp2 Orion Alpha A28X(config)# aaa accounting commands 15 test3 start-stop group tacgrp3 Orion Alpha A28X(config)# line vty 0 4 Orion Alpha A28X(config-line)# login authentication test1 Orion Alpha A28X(config-line)#authorization exec test2 Orion Alpha A28X(config-line)# accounting commands 15 test3 </pre> |
| <p><b>Verification</b></p> | <p>Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. Enter the <b>enable</b> command and enter the correct <b>enable</b> password to initiate <b>enable</b> authentication. Enter the privilege EXEC mode after passing the authentication. Perform operations on the device and then exit the device.</p> <p>View the authentication log of the user on the server with the IP address of 192.168.5.22.</p> <p>View the <b>enable</b> authentication log of the user on the server with the IP address of 192.168.5.22.</p> <p>View the <b>exec</b> authorization log of the user on the server with the IP address of 192.168.5.34.</p> <p>View the command accounting log of the user on the server with the IP address of 192.168.5.44.</p>   |



## Common Errors

---

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- Undefined servers are added to a server group.
- No method list is configured.

## 3.5 Monitoring

### Displaying

---

| Description                                    | Command            |
|--|--------------------|
| Displays interaction with each TACACS+ server. | <b>show tacacs</b> |

### Debugging

---

- System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

| Description     | Command              |
|-----------------|----------------------|
| Debugs TACACS+. | <b>debug tacacs+</b> |

---

## 4 Configuring Global IP-MAC Binding

### 4.1 Overview

Enable the global IP-MAC binding function manually to verify the input packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing matched IP address and MAC address. The other packets are discarded.

The address bounding feature is used to verify the input packets. Note that the address binding feature takes precedence over the 802.1X authentication, port security, and access control list (ACL).

### 4.2 Applications

| Application                           | Description   |
|---------------------------------------|---|
| <a href="#">Global IP-MAC Binding</a> | Only hosts with the specified IP addresses can access the network, and the hosts connected to a device can move freely. |

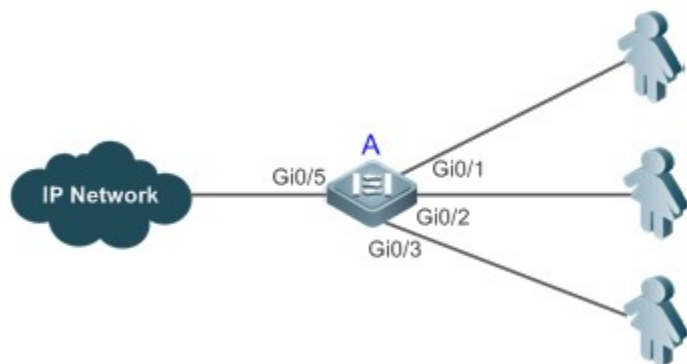
#### 4.2.1 Global IP-MAC Binding

##### Scenario

The administrator assigns a fixed IP address for each host to facilitate management.

- Only hosts with the specified IP addresses can access the external network, which prevents IP address embezzlement by unauthorized hosts.
- Hosts can move freely under the same device.

Figure 7-6



|                |  |
|----------------|--|
| <b>Remarks</b> | A is an access device.<br>A user is a host configured with a static IP address.<br>IP Network is an external IP network. |
|----------------|--|

## Deployment

- Manually configure the global IP-MAC binding. (Take three users as an example.)

| User   | MAC Address    | IP Address   |
|--------|----------------|--------------|
| User 1 | 00d0.3232.0001 | 192.168.1.10 |
| User 2 | 00d0.3232.0002 | 192.168.1.20 |
| User 3 | 00d0.3232.0003 | 192.168.1.30 |

- Enable the IP-MAC binding function globally.
- Configure the uplink port (Gi0/5 port in this example) of the device as the exclude port.

## 4.3 Features

### Basic Concepts

#### IPv6 Address Binding Mode

IPv6 address binding modes include Compatible, Loose, and Strict. The default mode is Strict. If IPv4-MAC binding is not configured, the IPv6 address binding mode does not take effect, and all IPv4 and IPv6 packets are allowed to pass through. If IPv4-MAC binding is configured, the IPv6 address binding mode takes effect, and the device forwards IPv4 and IPv6 packets based on the forwarding rules described in the following table:

| Mode       | IPv4 Packet Forwarding Rule                                 | IPv6 Packet Forwarding Rule   |
|------------|---|---|
| Strict     | Packets matching the global IPv4-MAC binding are forwarded. | Packets matching the global IPv6-MAC binding are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.)   |
| Loose      | Packets matching the global IPv4-MAC binding are forwarded. | If IPv6+MAC address binding is configured, packets matching the IPv6-MAC binding are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.)<br>If IPv6-MAC binding does not exist, all IPv6 packets are forwarded.                                |
| Compatible | Packets matching the global IPv4-MAC binding are forwarded. | If the IPv6 packets contain a MAC address matching the MAC address in the IPv4-MAC binding, the IPv6 packets are forwarded.<br>Packets matching the global IPv6-MAC binding conditions are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.) |

#### Exclude Port

By default, the IP-MAC binding function takes effect on all ports of the device. You can configure exclude ports so that the address binding function does not take effect on these ports. In practice, the IP-MAC bindings of the input packets on the

uplink port are not fixed. Generally, the uplink port of the device is configured as the exclude port so that the packets on the uplink port are not checked for IP-MAC binding.

## Overview

---

| Feature   | Description  |
|---|--|
| <a href="#">Configuring Global IP-MAC Binding</a>         | Control forwarding of IPv4 or IPv6 packets.                        |
| <a href="#">Configuring the IPv6 Address Binding Mode</a> | Change the IPv6 packet forwarding rules.                           |
| <a href="#">Configuring the Exclude Port</a>              | Disable the global address binding function on the specified port. |

### 4.3.1 Configuring Global IP-MAC Binding

#### Working Principle

---

Enable the global IP-MAC binding function manually to verify the input packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing matched IP address and MAC address. The other packets are discarded.

#### Related Configuration

---

##### ↳ [Configuring IP-MAC Binding](#)

Run the **address-bind** command in global configuration mode to add or delete an IPv4-MAC binding.

##### ↳ [Enabling the IP-MAC Binding Function](#)

Run the **address-bind install** command in global configuration mode to enable the IP-MAC binding function. By default, this function is disabled.

### 4.3.2 Configuring the IPv6 Address Binding Mode

#### Working Principle

---

After the global IPv4-MAC binding is configured and enabled, IPv6 packets are forwarded based on the IPv6 address binding mode. IPv6 binding modes include Compatible, Loose, and Strict.

#### Related Configuration

---

##### ↳ [Configuring the IPv6 Address Binding Mode](#)

By default, the IPv6 address binding mode is Strict.

Run the **address-bind ipv6-mode** command to specify an IPv6 address binding mode.

---

### 4.3.3 Configuring the Exclude Port

#### Working Principle

Configure an exclude port so that the address binding function does not take effect on this port.

#### Related Configuration

##### ↘ [Configuring the Exclude Port](#)

Run the **address-bind uplink** command to configure an exclude port. By default, no port is the exclude port.

## 4.4 Configuration

| Configuration   | Description and Command  |   |
|---|--|---|
| <a href="#">Configuring Global IP-MAC Binding</a>         | ● (Mandatory) It is used to configure and enable address binding.                    |   |
|   | <b>address-bind</b>  | Configures a global IPv4-MAC binding.                   |
|   | <b>address-bind install</b>  | Enables the address binding function.                   |
|   | <b>address-bind binding-filter logging</b>   | Configures a logging filter of global IPv4-MAC binding. |
| <a href="#">Configuring the IPv6 Address Binding Mode</a> | ● (Optional) It is used to configure the IPv6 address binding mode.                  |   |
|   | <b>address-bind ipv6-mode</b>  | Configures the IPv6 address binding mode.               |
| <a href="#">Configuring the Exclude Port</a>              | ● (Optional) It is used to disable the address binding function on a specified port. |   |
|   | <b>address-bind uplink</b>   | Configures an exclude port.                             |

### 4.4.1 Configuring Global IP-MAC Binding

#### Configuration Effect

- Configure a global IPv4-MAC binding.
- Enable the address binding function to control forwarding of the IPv4 or IPv6 packets.

#### Notes

- If you run the **address-bind install** command without IP-MAC binding configured, IP-MAC binding does not take effect and all packets are allowed to pass through.

#### Configuration Steps

##### ↘ [Configuring Global IP-MAC Binding](#)

- (Mandatory) Perform this configuration in global configuration mode.

##### ↘ [Enabling the Address Binding Function](#)

- (Mandatory) Perform this configuration in global configuration mode.

### ↳ Configuring a Logging Filter of Global IP-MAC Binding

- (Optional) Perform this configuration in global configuration mode.

### Verification

Run the **show run** or **show address-bind** command to check whether the configuration takes effect.

### Related Commands

#### ↳ Configuring Global IP-MAC Binding

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>address-bind { ip-address   ipv6-address } mac-address</b>   |
| <b>Parameter Description</b> | <i>ip-address</i> : Indicates the bound IPv4 address.<br><i>ipv6-address</i> : Indicates the bound IPv6 address.<br><i>mac-address</i> : Indicates the bound MAC address. |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Configuration Usage</b>   | Run this command to configure the binding relationship between an IPv4/IPv6 address and a MAC address.  |

#### ↳ Enabling the Address Binding Function

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>address-bind install</b>   |
| <b>Parameter Description</b> | N/A   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Configuration Usage</b>   | Run this command to enable the global IP-MAC binding function. This function is used to control forwarding of IPv4 or IPv6 packets. |

#### ↳ Configuring a Logging Filter of Global IP-MAC Binding

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>address-bind binding-filter logging [ rate-limit rate ]</b>  |
| <b>Parameter Description</b> | <b>rate-limit rate</b> : Indicates the printing rate of logging filter of global IPv4-MAC binding.  |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Configuration Usage</b>   | By default, the rate is 10 logs per minute.<br>When a logging filter is configured, alert logs are printed if IP packets not containing matched IP address and MAC address are detected.<br>When a logging filter is configured, the number of non-printed logs is prompted if the actual printing rate exceeds the set rate. |

## Configuration Example

### ↳ Configuring Global IP-MAC Binding and Enabling Address Binding

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"><li>● Configure a global IPv4-MAC binding.</li><li>● Enable the address binding function.</li></ul>   |
|                            | <pre>Orion Alpha A28X# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)# address-bind 192.168.5.1 00d0.f800.0001 Orion Alpha A28X(config)# address-bind install</pre> |
| <b>Verification</b>        | Display the global IP-MAC binding on the device.  |
|                            | <pre>Orion Alpha A28X#show address-bind Total Bind Addresses in System : 1 IP Address      Binding MAC Addr ----- 192.168.5.1    00d0.f800.0001</pre>   |

## 4.4.2 Configuring the IPv6 Address Binding Mode

### Configuration Effect

- Change the IPv6 address binding mode so as to change the forwarding rules for IPv6 packets.

### Configuration Steps

#### ↳ Configuring the IPv6 Address Binding Mode

- (Optional) Perform this configuration when you want to change the forwarding rules for IPv6 packets.

### Verification

- Run the **show run** command to check whether the configuration takes effect.

### Related Commands

#### ↳ Configuring the IPv6 Address Binding Mode

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>address-bind ipv6-mode { compatible   loose   strict }</b>   |
| <b>Parameter Description</b> | <b>compatible:</b> Indicates the Compatible mode.<br><b>loose:</b> Indicates the Loose mode.<br><b>strict:</b> Indicates the strict mode. |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Configuration</b>         | N/A   |

|              |  |
|--------------|--|
| <b>Usage</b> |  |
|--------------|--|

## Configuration Example

### ↳ Configuring the IPv6 Address Binding Mode

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Configure a global IP-MAC binding.</li> <li>● Enable the address binding function.</li> <li>● Set the IPv6 address binding mode to Compatible.</li> </ul>  |
|                            | <pre>Orion Alpha A28X# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)# address-bind 192.168.5.1 00d0.f800.0001 Orion Alpha A28X(config)# address-bind install Orion Alpha A28X(config)# address-bind ipv6-mode compatible</pre> |
| <b>Verification</b>        | Run the <b>show run</b> command to display the configuration on the device.   |

## 4.4.3 Configuring the Exclude Port

### Configuration Effect

- The address binding function is disabled on the exclude port, and all IP packets can be forwarded.

### Notes

- The configuration can be performed only on a switching port or an L2 aggregate port.

### Configuration Steps

#### ↳ Configuring the Exclude Port

- (Optional) Perform this configuration in global configuration mode when you want to disable the address binding function on a specified port.

### Verification

Run the **show run** or **show address-bind uplink** command to check whether the configuration takes effect.

### Related Commands

#### ↳ Configuring the Exclude Port

|                              |   |
|------------------------------|---|
| <b>Command Syntax</b>        | <b>address-bind uplink</b> <i>interface-id</i>                                      |
| <b>Parameter Description</b> | <i>interface-id</i> : Indicates the ID of a switching port or an L2 aggregate port. |
| <b>Command Mode</b>          | Global configuration mode   |



|                            |     |
|----------------------------|-----|
| <b>Configuration Usage</b> | N/A |
|----------------------------|-----|

## Configuration Example

### ↘ Configuring the Exclude Port

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Create a global IPv4-MAC binding.</li> <li>● Enable the address binding function.</li> <li>● Configure an exclude port.</li> </ul>   |
|                            | <pre> Orion Alpha A28X# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)# address-bind 192.168.5.1 00d0.f800.0001 Orion Alpha A28X(config)# address-bind install Orion Alpha A28X(config)# address-bind uplink GigabitEthernet 0/1 </pre> |
| <b>Verification</b>        | Display the global IP-MAC binding on the device.  |
|                            | <pre> Orion Alpha A28X#show address-bind  Total Bind Addresses in System : 1  IP Address      Binding MAC Addr ----- 192.168.5.1    00d0.f800.0001  Orion Alpha A28X#show address-bind uplink  Port    State ----- Gi0/1   Enabled Default Disabled </pre>  |

## 4.5 Monitoring

### Displaying

| Description                                | Command                         |
|--|---------------------------------|
| Displays the IP-MAC binding on the device. | <b>show address-bind</b>        |
| Displays the exclude port.                 | <b>show address-bind uplink</b> |

# 5 Configuring Password Policy

## 5.1 Overview

The Password Policy is a password security function provided for local authentication of the device. It is configured to control users' login passwords and login states.

- The following sections introduce password policy only.

### Protocols and Standards

N/A

## 5.2 Features

### Basic Concepts

#### ↳ **Minimum Password Length**

Administrators can set a minimum length for user passwords according to system security requirements. If the password input by a user is shorter than the minimum password length, the system does not allow the user to set this password but displays a prompt, asking the user to specify another password of an appropriate length.

#### ↳ **Strong Password Detection**

The less complex a password is, the more likely it is to crack the password. For example, a password that is the same as the corresponding account or a simple password that contains only characters or digits may be easily cracked. For the sake of security, administrators can enable the strong password detection function to ensure that the passwords set by users are highly complex. After the strong password detection function is enabled, a prompt will be displayed for the following types of passwords:

1. Passwords that are the same as corresponding accounts;
4. Simple passwords that contain characters or digits only.

#### ↳ **Password Life Cycle**

The password life cycle defines the validity time of a user password. When the service time of a password exceeds the life cycle, the user needs to change the password.

If the user inputs a password that has already expired during login, the system will give a prompt, indicating that the password has expired and the user needs to reset the password. If the new password input during password resetting does not meet system requirements or the new passwords consecutively input twice are not the same, the system will ask the user to input the new password once again.

## ↳ Guard Against Repeated Use of Passwords

When changing the password, the user will set a new password while the old password will be recorded as the user's history records. If the new password input by the user has been used previously, the system gives an error prompt and asks the user to specify another password.

The maximum number of password history records per user can be configured. When the number of password history records of a user is greater than the maximum number configured for this user, the new password history record will overwrite the user's oldest password history record.

## ↳ Storage of Encrypted Passwords

Administrators can enable the storage of encrypted passwords for security consideration. When administrators run the **show running-config** command to display configuration or run the **write** command to save configuration files, various user-set passwords are displayed in the cipher text format. If administrators disable the storage of encrypted passwords next time, the passwords already in cipher text format will not be restored to plaintext passwords.

## 5.3 Configuration

| Configuration  | Description and Command   |  |
|--|---|--|
| <a href="#">Configuring the Password Security Policy</a> | <ul style="list-style-type: none"><li>Optional configuration, which is used to configure a combination of parameters related to the password security policy.</li></ul> |  |
|  | <b>password policy life-cycle</b>   | Configures the password life cycle.  |
|  | <b>password policy min-size</b>   | Configures the minimum length of user passwords.   |
|  | <b>password policy no-repeat-times</b>  | Sets the no-repeat times of latest password configuration, so that the passwords specified in these times of latest password configuration can no longer be used in future password configuration. |
|  | <b>password policy strong</b>   | Enables the strong password detection function.  |
|  | <b>service password-encryption</b>  | Sets the storage of encrypted passwords.   |

### Networking Requirements

- Provide a password security policy for local authentication of the device. Users can configure different password security policies to implement password security management.

### Notes

- The configured password security policy is valid for global passwords (configured using the commands **enable password** and **enable secret**) and local user passwords (configured using the **username name password password** command). It is invalid for passwords in Line mode.

## Configuration Steps

### ↳ Configuring the Password Life Cycle

- Optional
- Perform this configuration on each device that requires the configuration of a password life cycle unless otherwise stated.

### ↳ Configuring the Minimum Length of User Passwords

- Optional
- Perform this configuration on each device that requires a limit on the minimum length of user passwords unless otherwise stated.

### ↳ Setting the No-Repeat Times of Latest Password Configuration

- Optional
- Perform this configuration on each device that requires a limit on the no-repeat times of latest password configuration unless otherwise stated.

### ↳ Enabling the Strong Password Detection Function

- Optional
- Perform this configuration on each device that requires strong password detection unless otherwise stated.

### ↳ Setting the Storage of Encrypted Passwords

- Optional
- Perform this configuration on each device that requires the storage of passwords in encrypted format unless otherwise stated.

## Verification

Configure a local user on the device, and configure a valid password and an invalid password for the user.

- When you configure the valid password, the device correctly adds the password.
- When you configure the invalid password, the device displays a corresponding error log.

## Related Commands

### ↳ Configuring the Password Life Cycle

|                              |  |
|------------------------------|--|
| <b>Command Syntax</b>        | <b>password policy life-cycle days</b>   |
| <b>Parameter Description</b> | <b>life-cycle days:</b> Indicates the password life cycle in the unit of days. The value range is from 1 to 65535. |
| <b>Command Mode</b>          | Global configuration mode  |

|                    |  |
|--------------------|--|
| <b>Usage Guide</b> | The password life cycle is used to define the validity period of user passwords. If the user logs in with a password whose service time already exceeds the life cycle, a prompt is given, asking the user to change the password. |
|--------------------|--|

#### ↘ **Configuring the Minimum Length of User Passwords**

|                              |  |
|------------------------------|--|
| <b>Command Syntax</b>        | <b>password policy min-size</b> <i>length</i>  |
| <b>Parameter Description</b> | <b>min-size</b> <i>length</i> : Indicates the minimum length of passwords. The value range is from 1 to 31.  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | This command is used to configure the minimum length of passwords. If the minimum length of passwords is not configured, users can input a password of any length. |

#### ↘ **Setting the No-Repeat Times of Latest Password Configuration**

|                              |   |
|------------------------------|---|
| <b>Command Syntax</b>        | <b>password policy no-repeat-times</b> <i>times</i>   |
| <b>Parameter Description</b> | <b>no-repeat-times</b> <i>times</i> : Indicates the no-repeat times of latest password configuration. The value range is from 1 to 31.  |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | After this function is enabled, all old passwords used in the several times of latest password configuration will be recorded as the user's password history records. If the new password input by the user has been used previously, the system gives an error prompt and the password modification fails.<br>You can configure the maximum number of password history records per user. When the number of password history records of a user is greater than the maximum number configured for the user, the new password history record will overwrite the user's oldest password history record. |

#### ↘ **Enabling the Strong Password Detection Function**

|                              |  |
|------------------------------|--|
| <b>Command Syntax</b>        | <b>password policy strong</b>  |
| <b>Parameter Description</b> | -  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | After the strong password detection function is enabled, a prompt is displayed for the following types of passwords:<br><br><ol style="list-style-type: none"> <li>5. Passwords that are the same as corresponding accounts;</li> <li>6. Simple passwords that contain characters or digits only.</li> </ol> |

#### ↘ **Setting the Storage of Encrypted Passwords**

|                              |  |
|------------------------------|--|
| <b>Command Syntax</b>        | <b>service password-encryption</b>   |
| <b>Parameter Description</b> | -  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Before the storage of encrypted passwords is set, all passwords used in the configuration process will be displayed and stored in plaintext format, unless the passwords are configured in cipher text format. You can enable the storage of encrypted passwords for security consideration. When you run the <b>show running-config</b> command to display configuration or run the <b>write</b> command to save configuration files, various user-set passwords are displayed in the cipher text format. If you disable the storage of encrypted passwords next time, the passwords already in cipher text format will not be restored to plaintext passwords. |

#### ↘ [Checking User-Configured Password Security Policy Information](#)

|                              |  |
|------------------------------|--|
| <b>Command Syntax</b>        | <b>show password policy</b>  |
| <b>Parameter Description</b> | -  |
| <b>Command Mode</b>          | Privileged EXEC mode/ Global configuration mode/ Interface configuration mode      |
| <b>Usage Guide</b>           | Use this command to display the password security policy configured on the device. |

#### ↘ [Checking Information Such as the Default Password Dictionary and Weak Passwords Manually Set](#)

|                              |  |
|------------------------------|--|
| <b>Command Syntax</b>        | <b>show password policy</b>  |
| <b>Parameter Description</b> | -  |
| <b>Command Mode</b>          | Privileged EXEC mode   |
| <b>Usage Guide</b>           | Use this command to display information such as the default password dictionary and weak passwords manually set on the device. |

### Configuration Examples

- The following configuration example describes configuration related to a password security policy.

#### ↘ [Configuring Password Security Check on the Device](#)

|                            |  |
|----------------------------|--|
| <b>Typical Application</b> | Assume that the following password security requirements arise in a network environment: <ol style="list-style-type: none"> <li>1. The minimum length of passwords is 8 characters;</li> <li>2. The password life cycle is 90 days;</li> <li>3. Passwords are stored and transmitted in cipher text format;</li> <li>4. The number of no-repeat times of password history records is 3;</li> </ol> |
|----------------------------|--|

|                            |  |
|----------------------------|--|
|                            | 5. Passwords shall not be the same as user names, and shall not contain simple characters or digits only.  |
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Set the minimum length of passwords to 8.</li> <li>● Set the password life cycle to 90 days.</li> <li>● Enable the storage of encrypted passwords.</li> <li>● Set the no-repeat times of password history records to 3.</li> <li>● Enable the strong password detection function.</li> <li>● Enable the password dictionary detection function.</li> </ul> <pre> Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# password policy min-size 8 Orion Alpha A28X(config)# password policy life-cycle 90 Orion Alpha A28X(config)# service password-encryption Orion Alpha A28X(config)# password policy no-repeat-times 3 Orion Alpha A28X(config)# password policy strong </pre>                        |
| <b>Verification</b>        | <p>When you create a user and the corresponding password after configuring the password security policy, the system will perform relevant detection according to the password security policy.</p> <ul style="list-style-type: none"> <li>● Run the <b>show password policy</b> command to display user-configured password security policy information.</li> </ul> <pre> Orion Alpha A28X# show password policy Global password policy configurations: Password encryption:           Enabled Password strong-check:         Enabled Password secret-dictionary-check: Enabled Password min-size:             Enabled (8 characters) Password life-cycle:           Enabled (90 days) Password no-repeat-times:      Enabled (max history record: 3) </pre> |

### Common Errors

- The time configured for giving a pre-warning notice about password expiry to the user is greater than the password life cycle.

## 5.4 Monitoring

### Displaying

| Command | Function |
|---------|----------|
|---------|----------|

**show password policy**

Displays user-configured password security policy information.

---



# 6 Configuring Port Security

## 6.1 Overview

Port security is used to restrict access to a port. Source MAC addresses of packets can be used to restrict the packets that enter the ports of a switch. You can set the number of static MAC addresses or the number of MAC addresses that are dynamically learned to restrict the packets that can enter the port. Ports enabled with port security are called secure ports.

## 6.2 Applications

| Application  | Description  |
|--|--|
| <a href="#">Allowing Only Specified Hosts to Use Ports</a> | For network security, certain ports of a device can be used only by specified hosts. |

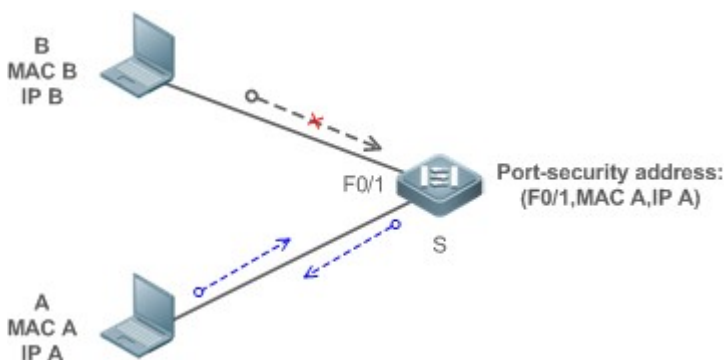
### 6.2.1 Allowing Only Specified Hosts to Use Ports

#### Scenario

In a scenario that has requirements for the network security, devices cannot be completely isolated physically. In this case, the devices need to be configured to restrict the PCs that connected to the ports of the devices.

- Only specified PCs can connect to the ports and normally use the network.
- Other PCs cannot use the network even if connected to the ports.
- After the configuration is complete, the administrator does not need to perform regular maintenance.

Figure 9-21



|                |   |
|----------------|---|
| <b>Remarks</b> | S is the access device.<br>A is a PC that can use the port F0/1.<br>B is an unknown PC. |
|----------------|---|

## Deployment

---

- Enable ARP Check for port F0/1 (omitted).
- Enable port security on access device S and set the violation handling mode to protect.
- Set the maximum number of secure addresses allowed by port F0/1 to 1.
- Configure a static port security address on the port F0/1.

## 6.3 Features

### Basic Concepts

---

#### ↳ Secure Port

Ports configured with port security are called secure ports. At present, Orion Alpha A28X devices require that secure ports cannot be destination ports of mirroring.

#### ↳ Secure Addresses

Addresses bound to secure ports are called secure addresses. Secure addresses can be layer-2 addresses, namely MAC addresses, and can also be layer-3 addresses, namely, IP or IP+MAC addresses. When a secure address is bound to IP+MAC and a static secure MAC address is configured, the static secure MAC address must be the same as the MAC address bound to IP+MAC; otherwise, communication may fail due to inconsistency with the binding. Similarly, if only IP binding is set, only packets whose secure MAC addresses are statically configured or learned and whose source IP addresses are the bound IP address can enter the device.

#### ↳ Dynamic Binding

A method for a device to automatically learn addresses and convert learned addresses into secure addresses.

#### ↳ Static Binding

A command for manually binding secure addresses.

#### ↳ Aging of Secure Addresses

Regularly delete secure address records. Secure addresses for port security support aging configuration. You can specify only dynamically learned addresses for aging or specify both statically configured and dynamically learned secure addresses for aging.

#### ↳ Sticky MAC Address

Convert dynamically learned secure addresses into statically configured addresses. Addresses will not age. After the configurations are saved, dynamic secure addresses will not be learned again upon restart. If this function is not enabled, the secure MAC addresses dynamically learned must be learned again after device restart.

#### ↳ Security Violation Events

When the number of learned MAC addresses learned by a port exceeds the maximum number of secure addresses, security violation events will be triggered. You can configure the following modes for handling security violation events:

- protect: When security violation occurs, a corresponding secure port will stop learning MAC addresses and discard all packets of newly accessed users. This is the default mode for handling violation.
- restrict: When violation occurs, a port violation trap notification will be sent in addition to the behavior in the protect mode.
- shutdown: When violation occurs, the port will be disabled in addition to the behaviors in the preceding two modes.

#### ↘ **Maximum Number of Secure Addresses**

The maximum number of secure addresses indicates the total number of secure addresses statically configured and dynamically learned. When the number of secure addresses under a secure port does not reach the maximum number of secure addresses, the secure port can dynamically learn new dynamic secure addresses. When the number of secure addresses reaches the maximum number, the secure port will not learn dynamic secure addresses any longer. If new users access the secure port in this case, security violation events will occur.

### Overview

| Feature                                   | Description   |
|---|---|
| <a href="#">Enabling Port Security</a>    | Creates a secure address list for a port.                           |
| <a href="#">Filtering Layer-2 Users</a>   | Processes the packets received by a port from non-secure addresses. |
| <a href="#">Filtering Layer-3 Users</a>   | Checks the layer-2 and layer-3 addresses of packets passing a port. |
| <a href="#">Aging of Secure Addresses</a> | Regularly deletes secure addresses.                                 |

## 6.3.1 Enabling Port Security

Enable port security for a port to restrict packets that access the network through the port.

### Working Principle

When port security is enabled, the device security module will check the sources of received packets.

Only packets from addresses in the secure address list can be normally forwarded; otherwise, the packets will be discarded or the port performs other violation handling behaviors.

When the port security and 802.1x are configured at the same time, packets can enter a switch only when the MAC addresses of the packets meet the static MAC address configurations of 802.1x or port security. If a port is configured with a secure channel or is bound to global IP+MAC, packets in compliance with the secure channel or bound to global IP+MAC can avoid checking of port security.

### Related Configuration

#### ↘ **Enabling Port Security for a Port**

By default, port security is disabled.

You can run the **switchport port-security** command to enable or disable the port security function for a port.

You cannot enable this function for a destination port of SPAN.

#### ↳ [Setting the Maximum Number of Secure Addresses for a Port](#)

By default, the maximum number of secure addresses for a port is 128.

You can run the **switchport port-security maximum** command to adjust the maximum number of secure addresses for the port.

A smaller number of secure addresses mean fewer users that access the network through this port.

#### ↳ [Setting the Mode for Handling Violation](#)

By default, when the number of secure addresses reaches the maximum number, the secure port will discard packets from unknown addresses (none of the secure addresses of the port).

You can run the **switchport port-security violation** command to modify the violation handling mode.

#### ↳ [Setting Secure Addresses That Can Be Dynamically Saved](#)

By default, no secure address dynamically learned will be saved.

You can run the **switchport port-security mac-address sticky** command to save dynamically learned addresses to the configuration file. As long as the configuration file is saved, the device does not need to re-learn the secure addresses after the device is restarted.

## 6.3.2 Filtering Layer-2 Users

Set the secure addresses on a port to ensure that only devices whose MAC addresses are the same as the secure addresses can access the network through this port.

### Working Principle

Add secure addresses for a secure port. When the number of secure addresses for a secure port does not reach the maximum number, the secure port can dynamically learn new dynamic secure addresses. When the number of secure addresses for the secure port reaches the maximum number, the secure port will not learn dynamic secure addresses any longer. The MAC addresses of users connecting to this port must be in the secure address list; otherwise, violation events will be triggered.

### Related Configuration

#### ↳ [Adding Secure Addresses for a Secure port](#)

By default, a port dynamically learns secure addresses. If an administrator has special requirements, the administrator can manually configure secure addresses.

You can run the **switch portport-security interface** command to add or delete secure addresses for a device.

---

### 6.3.3 Filtering Layer-3 Users

Add binding of secure addresses and check layer-2 and layer-3 addresses of packets passing a port.

#### Working Principle

Layer-3 secure addresses support only IP binding and IP+MAC binding, and supports only static binding (not dynamic binding).

When a layer-3 secure port receives packets, layer-2 and layer-3 addresses need to be parsed. Only packets whose addresses are bound are valid packets. Other packets are considered as invalid packets and will be discarded, but no violation event will be triggered.

#### Related Configuration

##### ↳ [Configuring Binding of Secure Addresses on Secure Ports](#)

Binding of layer-3 secure addresses must be added manually.

You can run the **switchport port-security binding** command to add binding of secure addresses.

If only IP addresses are input, only IP addresses are bound. If IP addresses and MAC addresses are input, IP+MAC will be bound.

### 6.3.4 Aging of Secure Addresses

Regularly delete secure addresses. When this function is enabled, you need to set the maximum number of secure addresses. In this way, the device can automatically add and delete secure addresses on this port.

#### Working Principle

Enable the aging timer to regularly query and delete secure addresses whose aging time expires.

#### Related Configuration

##### ↳ [Configuring Aging Time of Secure Addresses](#)

By default, no secure address of a port will be aged.

You can run the **switchport port-security aging** command to enable aging time.

The **static** parameter can be used to age static addresses.

## 6.4 Configuration

| Configuration   | Description and Command   |
|---|---|
| <a href="#">Configuring Secure ports and Violation Handling Modes</a> | ● (Mandatory) It is used to enable the port security service.                                   |
|   | <b>switchport port-security</b> Enables port security.  |
|   | <b>switchport port-security maximum</b> Sets the maximum number of secure addresses for a port. |

|  |  |   |
|--|--|---|
|  | <b>switchport port-security violation</b>                      | Configures the violation handling mode for port security.                   |
|  | <b>switchport port-security mac-address sticky</b>             | Configures automatic saving of dynamic addresses.                           |
| <a href="#">Configuring Secure Addresses on Secure Ports</a> | ● (Optional) It is used to configure security filtering items. |   |
|  | <b>switchport port-security mac-address</b>                    | Configures the static secure addresses in the interface configuration mode. |
|  | <b>switchport port-security interface mac-address</b>          | Configures the static secure addresses in the global configuration mode.    |
|  | <b>switchport port-security binding</b>                        | Configures binding of secure addresses in the interface configuration mode. |
|  | <b>switchport port-security interface binding</b>              | Configures binding of secure addresses in the global configuration mode.    |
|  | <b>switchport port-security aging</b>                          | Configures aging time for all secure addresses on a port.                   |
|  | <b>switchport port-security binding-filter logging</b>         | Enables binding filter logging in the global configuration mode.            |

## 6.4.1 Configuring Secure ports and Violation Handling Modes

### Configuration Effect

- Restrict the number of MAC addresses that can be learned from a port.
- Filter invalid packets based on MAC addresses, IP addresses or IP+MAC.

### Notes

- A secure port cannot be the destination port of SPAN.
- The port security function cannot be configured for a DHCP Snooping trusted port.
- The port security function cannot be configured for excluded ports of global IP+MAC.
- The security function can be enabled only for wired switching ports and layer-2 AP ports in the interface configuration mode.
- The port security can work with other access control functions such as the 802.1x, global IP+MAC binding, and IP source guard. When these functions are used together, packets can enter a switch only when passing all security checks. If a security channel is configured for a port, packets in compliance with the security channel will avoid checking of the port security.

### Configuration Steps

#### ↳ Enabling the Port Security Service

- Mandatory.
- If there is no special requirement, enable the port security service for a port on the access device.

### ↘ [Configuring the Maximum Number of Secure Addresses for a Port](#)

- Optional. To adjust the maximum number of secure addresses running on a secure port, you can configure this item.
- Configure this item on a port enabled with port security.

### ↘ [Configuring Violation Handling Modes](#)

- Optional. If you hope that other handling modes except discarding packets are implemented in case of violation, you can configure other handling modes.
- Configure this item on a port enabled with port security.

### ↘ [Saving Dynamically Learned Addresses](#)

- Optional. If you hope that secure addresses are not re-learned after the device is restarted, you can configure this item.
- Configure this item on a port enabled with port security.

## Verification

Run the command of the device for displaying the port security configurations to check whether the configurations take effect.

## Related Commands

### ↘ [Setting Port Security](#)

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>switchport port-security</b>   |
| <b>Parameter Description</b> | -   |
| <b>Command Mode</b>          | Interface configuration mode  |
| <b>Usage Guide</b>           | By using the port security feature, you can strictly control the input of a port of a device by restricting the MAC addresses and IP addresses (optional) that access the port. |

### ↘ [Setting the Maximum Number of Secure Addresses for a Port](#)

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>switchport port-security maximum <i>value</i></b>   |
| <b>Parameter Description</b> | <i>value</i> : Indicates the number of secure addresses, ranging from 1 to 128.  |
| <b>Command Mode</b>          | Interface configuration mode   |
| <b>Usage Guide</b>           | If you set the maximum number to 1 and configure a secure address for this port, the workstation (whose address is the configured secure address) connected to this port will exclusively use all bandwidth of the port. |

### ↘ [Configuring the Violation Handling Mode for Port Security](#)

|                  |   |
|------------------|---|
| <b>Command</b>   | <b>switchport port-security violation { protect   restrict   shutdown }</b> |
| <b>Parameter</b> | <b>protect</b> : Discards violated packets.                                 |

---

|                     |   |
|---------------------|---|
| <b>Description</b>  | <b>restrict:</b> Discards violated packets and send trap notifications.<br><b>shutdown:</b> Discards packets and disables the port. |
| <b>Command Mode</b> | Interface configuration mode  |
| <b>Usage Guide</b>  | -   |

### ↳ Saving Dynamic Secure Addresses to a Configuration File

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>switchport port-security mac-address sticky</b> <i>mac-address</i> [ <b>vlan</b> <i>vlan-id</i> ]            |
| <b>Parameter Description</b> | <i>mac-address</i> : Indicates a static secure address.<br><i>vlan-id</i> : Indicates the VID of a MAC address. |
| <b>Command Mode</b>          | Interface configuration mode  |
| <b>Usage Guide</b>           | -   |

### Configuration Example

#### ↳ Enabling Port Security for the Port gigabitethernet 0/3, Setting the Maximum Number of Addresses to 8, and Setting the Violation Handling Mode to protect

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable port security.</li> <li>● Set the maximum number of secure addresses.</li> <li>● Modify the violation handling mode.</li> </ul>  |
|                            | <pre> Orion Alpha A28X# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)# interface gigabitethernet 0/3 Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport mode access Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security maximum 8 Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security violation protect Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security mac-address sticky Orion Alpha A28X(config-if-GigabitEthernet 0/3)# end </pre> |
| <b>Verification</b>        | Check the port security configuration on the device.   |
|                            | <pre> Orion Alpha A28X# show port-security interface gigabitethernet 0/3 Interface : Gi0/3 Port Security: Enabled Port status : down Violation mode: Protect Maximum MAC Addresses:8 </pre>  |



|                                       |
|---------------------------------------|
| Total MAC Addresses:0                 |
| Configured MAC Addresses:0            |
| Aging time : 0 mins                   |
| SecureStatic address aging : Disabled |

### Common Errors

- Port security is enabled on a SPAN port.
- Port security is enabled on a DHCP trusted port.
- The configured maximum number of secure addresses is smaller than the number of existing secure addresses.

## 6.4.2 Configuring Secure Addresses on Secure Ports

### Configuration Effect

- Allow specified users to use ports.
- Regularly update secure addresses of users.

### Notes

- Sticky MAC addresses are special MAC addresses not affected by the aging mechanism. No matter dynamic or static aging is configured, sticky MAC addresses will not be aged.

### Configuration Steps

#### ↳ **Configuring Secure Addresses**

- Optional. You need to manually add secure addresses for configuration.
- Configure this item on a port enabled with port security.

#### ↳ **Configuring Binding of Secure Addresses**

- Optional. You need to add layer-3 secure addresses for configuration.
- Configure this item on a port enabled with port security.

#### ↳ **Configuring Aging Time**

- Optional.
- Configure this item on a port enabled with port security.

#### ↳ **Enabling Binding Filter Logging**

- Optional.
  - Enable binding filter logging in the global configuration mode.
-

## Verification

- Run the command of the device for displaying the port security configurations to check whether the configurations take effect.

## Related Commands

### Adding Secure Addresses for Secure Ports in the Global Configuration Mode

|                     |  |
|---------------------|--|
| <b>Command</b>      | <b>switchport port-security interface</b> <i>interface-id</i> <b>mac-address</b> <i>mac-address</i> [ <b>vlan</b> <i>vlan-id</i> ] |
| <b>Parameter</b>    | <i>interface-id</i> : Indicates the interface ID.  |
| <b>Description</b>  | <i>mac-address</i> : Indicates a static secure address.<br><i>vlan-id</i> : Indicates the VID of a MAC address.                    |
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | -  |

### Adding Secure Addresses for Secure Ports in the Interface Configuration Mode

|                     |  |
|---------------------|--|
| <b>Command</b>      | <b>switchportport-security mac-address</b> <i>mac-address</i> [ <b>vlan</b> <i>vlan_id</i> ] |
| <b>Parameter</b>    | <i>mac-address</i> : Indicates a static secure address.                                      |
| <b>Description</b>  | <i>vlan-id</i> : Indicates the VID of a MAC address.   |
| <b>Command Mode</b> | Interface configuration mode   |
| <b>Usage Guide</b>  | -  |

### Adding Binding of Secure Addresses for Secure Ports in the Global Configuration Mode

|                     |   |
|---------------------|---|
| <b>Command</b>      | <b>switchport port-security interface</b> <i>interface-id</i> <b>binding</b> [ <i>mac-address</i> <b>vlan</b> <i>vlan_id</i> ] { <i>ipv4-address</i>   <i>ipv6-address</i> }  |
| <b>Parameter</b>    | <i>interface-id</i> : Indicates the interface ID.   |
| <b>Description</b>  | <i>mac-address</i> : Indicates a bound source MAC address.<br><i>vlan_id</i> : Indicates the VID of a bound source MAC address.<br><i>ipv4-address</i> : Indicates a bound IPv4 address.<br><i>ipv6-address</i> : Indicates a bound IPv6 address. |
| <b>Command Mode</b> | Global configuration mode   |
| <b>Usage Guide</b>  | -   |

### Adding Binding of Secure Addresses for Secure Ports in the Interface Configuration Mode

|                    |   |
|--------------------|---|
| <b>Command</b>     | <b>switchport port-security binding</b> [ <i>mac-address</i> <b>vlan</b> <i>vlan_id</i> ] { <i>ipv4-address</i>   <i>ipv6-address</i> }   |
| <b>Parameter</b>   | <i>mac-address</i> : Indicates a bound source MAC address.  |
| <b>Description</b> | <i>vlan_id</i> : Indicates the VID of a bound source MAC address.<br><i>ipv4-address</i> : Indicates a bound IPv4 address.<br><i>ipv6-address</i> : Indicates a bound IPv6 address. |
| <b>Command</b>     | Interface configuration mode  |

|                    |   |
|--------------------|---|
| <b>Mode</b>        |   |
| <b>Usage Guide</b> | - |

### ↘ [Configuring Aging Time for All Secure Addresses on a Port](#)

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>switchport port-security aging { static   time <i>time</i> }</b>  |
| <b>Parameter Description</b> | <p><b>static:</b> Indicates that the aging time will be applied to manually configured secure addresses and automatically learned addresses; otherwise, the aging time will be applied to only automatically learned addresses.</p> <p><b>time <i>time</i>:</b> Indicates the aging time of the secure addresses on this port, ranging from 0 to 1440 minutes. If it is set to 0, it indicates that the aging function is disabled actually.</p> |
| <b>Command Mode</b>          | Interface configuration mode   |
| <b>Usage Guide</b>           | -  |

### ↘ [Enabling Binding Filter Logging](#)

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>switchport port-security binding-filter logging [ rate-limit <i>rate</i> ]</b>   |
| <b>Parameter Description</b> | <b>rate-limit <i>rate</i>:</b> Indicates the printing rate of binding filter logging.   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | <ol style="list-style-type: none"> <li>1. If you run the <b>switchport port-security binding-filter logging</b> command without configuring the <i>rate</i> parameter, binding filter logging is enabled and the default printing rate, 10logs/minute, is adopted.</li> <li>2. After binding filter logging is enabled, for packets that do not comply with IP/IP-MAC binding, warnings are printed.</li> <li>3. After binding filter logging is enabled, if the printing rate exceeds the configured rate, the number of suppressed packets is displayed.</li> </ol> |

## Configuration Example

### ↘ [Configuring a Secure MAC Address 00d0.f800.073c for the Port gigabitethernet 0/3](#)

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable port security.</li> <li>● Add a secure address.</li> </ul>   |
|                            | <pre> Orion Alpha A28X# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)# interface gigabitethernet 0/3 Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport mode access Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security mac-address 00d0.f800.073c vlan 1 </pre> |

|                     |   |
|---------------------|---|
|                     | Orion Alpha A28X(config-if-GigabitEthernet 0/3)# end  |
| <b>Verification</b> | Check the port security configuration on the device.  |
|                     | <pre> Orion Alpha A28X# show port-security address Vlan Mac Address IP Address Type Port Remaining Age(mins) ----- 1 00d0.f800.073c 192.168.12.202 Configured Gi0/3 8 1 00d0.f800.3cc9 192.168.12.5 Configured Gi0/1 7 </pre> |

#### ↘ Configuring a Security Binding of the IP Address 192.168.12.202 for the Port gigabitethernet 0/3

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable port security.</li> <li>● Add a binding of the secure address.</li> </ul>  |
|                            | <pre> Orion Alpha A28X# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)# interface gigabitethernet 0/3 Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport mode access Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security binding 192.168.12.202 Orion Alpha A28X(config-if-GigabitEthernet 0/3)# end </pre> |
| <b>Verification</b>        | Check the port security configuration on the device.   |
|                            | <pre> Orion Alpha A28X# show port-security address Vlan Mac Address IP Address Type Port Remaining Age(mins) ----- 1 00d0.f800.073c 192.168.12.202 Configured Gi0/3 8 1 00d0.f800.3cc9 192.168.12.5 Configured Gi0/1 7 </pre>  |

#### ↘ Configuring a Secure MAC Address 00d0.f800.073c and a Security Binding of the IP Address 0000::313b:2413:955a:38f4 for the Port gigabitethernet 0/3

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable port security.</li> <li>● Add a binding of the secure address.</li> </ul>  |
|                            | <pre> Orion Alpha A28X# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)# interface gigabitethernet 0/3 Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport mode access </pre> |

|                     |   |
|---------------------|---|
|                     | <pre> Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security binding 00d0.f800.073c vlan 1 0000::313b:2413:955a:38f4 Orion Alpha A28X(config-if)# end </pre> |
| <b>Verification</b> | Check the port security configuration on the device.  |
|                     | <pre> Orion Alpha A28X# show port-security address Vlan Mac Address IP Address Type Port Remaining Age(mins) ----- 1 00d0.f800.073c 192.168.12.202 Configured Gi0/3 8 1 00d0.f800.3cc9 192.168.12.5 Configured Gi0/1 7 </pre>                             |

↘ **Configuring the Aging Time of the Port gigabitethernet 0/3 to 8 Minutes, Which Is Also Applied to Statically Configured Secure Addresses**

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable port security.</li> <li>● Configure aging time.</li> </ul>  |
|                            | <pre> Orion Alpha A28X# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion Alpha A28X(config)# interface gigabitethernet 0/3 Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security aging time 8 Orion Alpha A28X(config-if-GigabitEthernet 0/3)# switchport port-security aging static Orion Alpha A28X(config-if-GigabitEthernet 0/3)# end </pre> |
| <b>Verification</b>        | Check the port security configuration on the device.  |
|                            | <pre> Orion Alpha A28X# show port-security gigabitethernet 0/3 Interface : Gi0/3 Port Security: Enabled Port status : down Violation mode:Shutdown Maximum MAC Addresses:8 Total MAC Addresses:0 Configured MAC Addresses:0 Aging time : 8 mins SecureStatic address aging : Enabled </pre>   |

## 6.5 Monitoring

### Displaying

---

| Description   | Command   |
|---|---|
| Displays all secure addresses or all secure addresses of a specified port.                  | <b>show port-security address [ interface <i>interface-id</i> ]</b> |
| Displays all bindings or all bindings of a specified port.                                  | <b>show port-security binding [ interface <i>interface-id</i> ]</b> |
| Displays all valid secure addresses of ports and the security binding records of the ports. | <b>show port-security all</b>                                       |
| Displays the port security configurations of an interface.                                  | <b>show port-security interface <i>interface-id</i></b>             |
| Displays the statistics about port security.  | <b>show port-security</b>   |

# 7 Configuring Storm Control

## 7.1 Overview

When a local area network (LAN) has excess broadcast data flows, multicast data flows, or unknown unicast data flows, the network speed will slow down and packet transmission will have an increased timeout probability. This situation is called a LAN storm. A storm may occur when topology protocol execution or network configuration is incorrect.

Storm control can be implemented to limit broadcast data flows, multicast data flows, or unknown unicast data flows.

If the rate of data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds. This prevents flood data from entering the LAN causing a storm.

## 7.2 Applications

| Application                               | Description                               |
|---|---|
| <a href="#">Network Attack Prevention</a> | Enable storm control to prevent flooding. |

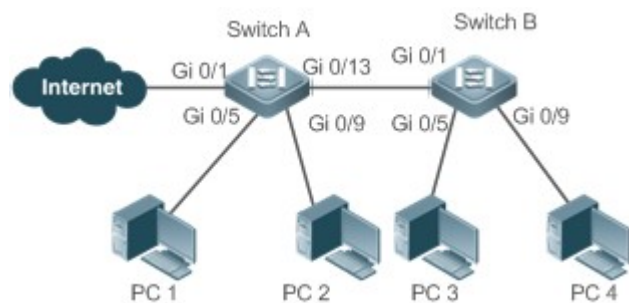
### 7.2.1 Network Attack Prevention

#### Scenario

The application requirements of network attack prevention are described as follows:

- Protect devices from flooding of broadcast packets, multicast packets, or unknown unicast packets.

Figure 10-7



|                |  |
|----------------|--|
| <b>Remarks</b> | Switch A and Switch B are access devices.<br>PC 1, PC 2, PC 3, and PC 4 are desktop computers. |
|----------------|--|

#### Deployment

- Enable storm control on the ports of all access devices (Switch A and Switch B).

## 7.3 Features

### Basic Concepts

---

#### ↳ Storm Control

If the rate of data flows (broadcast packets, multicast packets, or unknown unicast packets) received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds.

#### ↳ Storm Control Based on the Bandwidth Threshold

If the rate of data flows received by a device port is within the configured bandwidth threshold, the data flows are permitted to pass through. If the rate exceeds the threshold, excess data flows are discarded until the rate falls within the threshold.

#### ↳ Storm Control Based on the Packets-per-Second Threshold

If the rate of data flows received by a device port is within the configured packets-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the threshold, excess data flows are discarded until the rate falls within the threshold.

#### ↳ Storm Control Based on the Kilobits-per-Second Threshold

If the rate of data flows received by a device port is within the configured kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the threshold, excess data flows are discarded until the rate falls within the threshold.

### Overview

---

| Feature  | Description   |
|--|---|
| <a href="#">Unicast Packet Storm Control</a>   | Limits unknown unicast packets to prevent flooding. |
| <a href="#">Multicast Packet Storm Control</a> | Limits multicast packets to prevent flooding.       |
| <a href="#">Broadcast Packet Storm Control</a> | Limits broadcast packets to prevent flooding.       |

### 7.3.1 Unicast Packet Storm Control

The unicast packet storm control feature monitors the rate of unknown unicast data flows received by a device port to limit LAN traffic and prevent flooding caused by excess data flows.

#### Working Principle

---

If the rate of unknown unicast data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds.

---



## Related Configuration

### ↳ Enabling Unicast Packet Storm Control on Ports

By default, unicast packet storm control is disabled on ports.

Run the **storm-control unicast** [ { *level percent* | **pps packets** | *rate-bps* } ] command to enable unicast packet storm control on ports.

Run the **no storm-control unicast** or **default storm-control unicast** command to disable unicast packet storm control on ports.

The default command parameters are determined by related products.

## 7.3.2 Multicast Packet Storm Control

The multicast packet storm control feature monitors the rate of multicast data flows received by a device port to limit LAN traffic and prevent flooding caused by excess data flows.

### Working Principle

If the rate of multicast data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds.

## Related Configuration

### ↳ Enabling Multicast Packet Storm Control on Ports

By default, multicast packet storm control is disabled on ports.

Run the **storm-control multicast** [ { *level percent* | **pps packets** | *rate-bps* } ] command to enable multicast packet storm control on ports.

Run the **no storm-control multicast** or **default storm-control multicast** command to disable multicast packet storm control on ports.

The default command parameters are determined by related products.

## 7.3.3 Broadcast Packet Storm Control

The broadcast packet storm control feature monitors the rate of broadcast data flows received by a device port to limit LAN traffic and prevent flooding caused by excess data flows.

### Working Principle

If the rate of broadcast data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds.

## Related Configuration

### ↳ Enabling Broadcast Packet Storm Control on Ports

---

By default, broadcast packet storm control is disabled on ports.

Run the **storm-control broadcast** [ { *level percent* | *pps packets* | *rate-bps* } ] command to enable broadcast packet storm control on ports.

Run the **no storm-control broadcast** or **default storm-control broadcast** command to disable broadcast packet storm control on ports.

## 7.4 Configuration

| Configuration  | Description and Command   |
|--|---|
| <a href="#">Configuring Basic Functions of Storm Control</a> | <ul style="list-style-type: none"><li>● (Mandatory) It is used to enable storm control.</li></ul>   |
|  | <b>storm-control</b> { <b>broadcast</b>   <b>multicast</b>   <b>unicast</b> } [ { <i>level percent</i>   <i>pps packets</i>   <i>rate-bps</i> } ]<br>Enables storm control. |

### 7.4.1 Configuring Basic Functions of Storm Control

#### Configuration Effect

- Prevent flooding caused by excess broadcast packets, multicast packets, and unknown unicast packets.

#### Notes

- When you run a command (for example, **storm-control unicast**) to enable storm control, if you do not set the parameters, the default values are used.

#### Configuration Steps

##### ↘ Enabling Unicast Packet Storm Control

- Mandatory.
- Enable unicast packet storm control on every device unless otherwise specified.

##### ↘ Enabling Multicast Packet Storm Control

- Mandatory.
- Enable multicast packet storm control on every device unless otherwise specified.

##### ↘ Enabling Broadcast Packet Storm Control

- Mandatory.
- Enable broadcast packet storm control on every device unless otherwise specified.

#### Verification

- Run the **show storm-control** command to check whether the configuration is successful.
-

## Related Commands

### ↳ Enabling Unicast Packet Storm Control

|                     |  |
|---------------------|--|
| <b>Command</b>      | <b>storm-control unicast</b> [ { <i>level percent</i>   <b>pps packets</b>   <i>rate-bps</i> } ]                 |
| <b>Parameter</b>    | <i>level percent</i> : Indicates the bandwidth percentage.   |
| <b>Description</b>  | <b>pps packets</b> : Indicates the number of packets per second.<br><i>rate-bps</i> : Indicates the packet rate. |
| <b>Command Mode</b> | Interface configuration mode   |
| <b>Usage Guide</b>  | Storm control can be enabled only on switch ports.   |

### ↳ Enabling Multicast Packet Storm Control

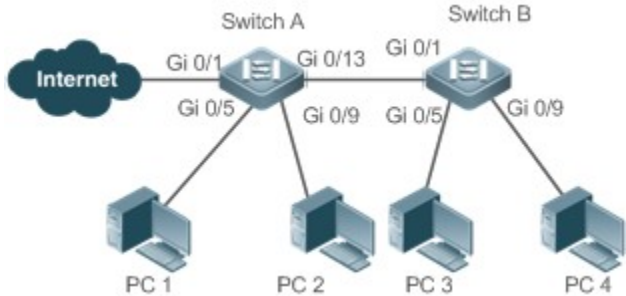
|                     |  |
|---------------------|--|
| <b>Command</b>      | <b>storm-control multicast</b> [ { <i>level percent</i>   <b>pps packets</b>   <i>rate-bps</i> } ]               |
| <b>Parameter</b>    | <i>level percent</i> : Indicates the bandwidth percentage.   |
| <b>Description</b>  | <b>pps packets</b> : Indicates the number of packets per second.<br><i>rate-bps</i> : Indicates the packet rate. |
| <b>Command Mode</b> | Interface configuration mode   |
| <b>Usage Guide</b>  | Storm control can be enabled only on switch ports.   |

### ↳ Enabling Broadcast Packet Storm Control

|                     |  |
|---------------------|--|
| <b>Command</b>      | <b>storm-control broadcast</b> [ { <i>level percent</i>   <b>pps packets</b>   <i>rate-bps</i> } ]               |
| <b>Parameter</b>    | <i>level percent</i> : Indicates the bandwidth percentage.   |
| <b>Description</b>  | <b>pps packets</b> : Indicates the number of packets per second.<br><i>rate-bps</i> : Indicates the packet rate. |
| <b>Command Mode</b> | Interface configuration mode   |
| <b>Usage Guide</b>  | Storm control can be enabled only on switch ports.   |

## Configuration Example

### ↳ Enabling Storm Control on Devices

|                    |   |
|--------------------|---|
| <b>Scenario</b>    |   |
| <b>Figure 10-8</b> |  |
|                    |   |

|                           |   |
|---------------------------|---|
| <b>Configuration Step</b> | <ul style="list-style-type: none"> <li>Enable storm control on Switch A and Switch B.</li> </ul>  |
| <b>Switch A</b>           | <pre>Orion Alpha A28X(config)#interface range gigabitEthernet 0/5,0/9,0/13 Orion Alpha A28X(config-if-range)#storm-control broadcast Orion Alpha A28X(config-if-range)#storm-control multicast Orion Alpha A28X(config-if-range)#storm-control unicast</pre>  |
| <b>Switch B</b>           | <pre>Orion Alpha A28X(config)#interface range gigabitEthernet 0/1,0/5,0/9 Orion Alpha A28X(config-if-range)#storm-control broadcast Orion Alpha A28X(config-if-range)#storm-control multicast Orion Alpha A28X(config-if-range)#storm-control unicast</pre>   |
| <b>Verification</b>       | Check whether storm control is enabled on Switch A and Switch B.  |
| <b>Switch A</b>           | <pre>Orion Alpha A28X# sho storm-control Interface          Broadcast Control Multicast Control Unicast Control Action ----- GigabitEthernet 0/1    Disabled      Disabled      Disabled      none GigabitEthernet 0/5    default       default       default       none GigabitEthernet 0/9    default       default       default       none GigabitEthernet 0/13  default       default       default       none</pre> |
| <b>Switch B</b>           | <pre>Orion Alpha A28X#sho storm-control Interface          Broadcast Control Multicast Control Unicast Control Action ----- GigabitEthernet 0/1    default       default       default       none GigabitEthernet 0/5    default       default       default       none GigabitEthernet 0/9    default       default       default       none</pre>   |

## 7.5 Monitoring

### Displaying

| Description                         | Command  |
|-------------------------------------|--|
| Displays storm control information. | <b>show storm-control</b> [ <i>interface-type interface-number</i> ] |

## 8 Configuring SSH

### 8.1 Overview

Secure Shell (SSH) connection is similar to a Telnet connection except that all data transmitted over SSH is encrypted. When a user in an insecure network environment logs into a device remotely, SSH helps ensure information security and powerful authentication, protecting the device against attacks such as IP address spoofing and plain-text password interception.

An SSH-capable device can be connected to multiple SSH clients. In addition, the device can also function as an SSH client, and allows users to set up an SSH connection with a SSH-server device. In this way, the local device can safely log in to a remote device through SSH to implement management.

- Currently, a device can work as either the SSH server or an SSH client, supporting SSHv1 and SSHv2 versions. Orion Alpha A28X SSH service supports both IPv4 and IPv6.
- Unless otherwise specified, SSH in this document refers to SSHv2.

#### Protocols and Standards

- RFC 4251: The Secure Shell (SSH) Protocol Architecture
- RFC 4252: The Secure Shell (SSH) Authentication Protocol
- RFC 4253: The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254: The Secure Shell (SSH) Connection Protocol
- RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4716: The Secure Shell (SSH) Public Key File Format
- RFC 4819: Secure Shell Public Key Subsystem
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 1950: ZLIB Compressed Data Format Specification version 3.3
- draft-ietf-secsh-filexfer-05: SSH File Transfer Protocol
- draft-ylonen-ssh-protocol-00: The version of the SSH Remote Login Protocol is 1.5. Comware implements the SSH server functions, but not the SSH client functions.

### 8.2 Applications

| Application                                   | Description   |
|---|---|
| <a href="#">SSH Device Management</a>         | Use SSH to manage devices.  |
| <a href="#">SSH Local Line Authentication</a> | Use the local line password authentication for SSH user authentication. |

| Application                                   | Description  |
|---|--|
| <a href="#">SSH AAA Authentication</a>        | Use the authentication, authorization and accounting (AAA) mode for SSH user authentication. |
| <a href="#">SSH Public Key Authentication</a> | Use the public key authentication for SSH user authentication.                               |
| <a href="#">SSH File Transfer</a>             | Use the Secure Copy (SCP) commands on the client to exchange data with the SSH server.       |

## 8.2.1 SSH Device Management

### Scenario

You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows system does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client. Figure 11-22 shows the network topology.

Figure 11-22 Networking Topology of SSH Device Management



### Deployment

Configure the SSH client as follows:

- Start the PuTTY software.
- On the **Session** option tab of PuTTY, type in the host IP address of the SSH server and SSH port number **22**, and select the connection type **SSH**.
- On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**.
- On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**.
- Click **Open** to connect to the SSH server.
- Type in the correct user name and password to enter the terminal login interface.

## 8.2.2 SSH Local Line Authentication

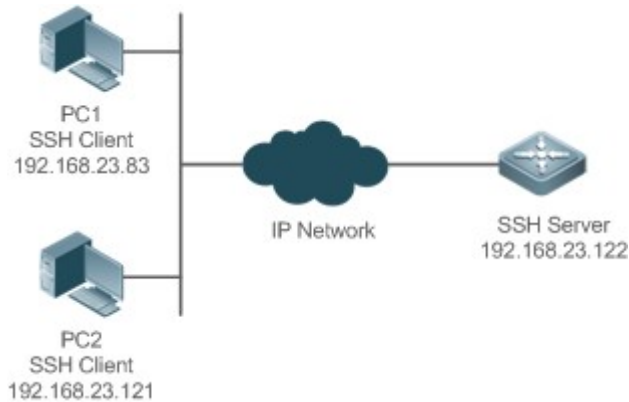
### Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 11-23. To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server function is enabled. The requirements are as follows:

- SSH users use the local line password authentication mode.

- Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.

Figure 11-23 Networking Topology of SSH Local Line Password Authentication



## Deployment

- Configure the SSH server as follows:
  1. Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2.
  7. Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH clients, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses an RSA key, whereas SSHv2 adopts an RSA or DSA key.
  8. Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server using this IP address. The routes from the SSH clients to the SSH server are reachable.
- Configure the SSH client as follows:

Diversified SSH client software is available, including PuTTY, Linux, and OpenSSH. This document takes PuTTY as an example to explain the method for configuring the SSH clients.

15. Open the PuTTY connection tab, and select SSHv1 for authenticated login. (The method is similar if SSHv2 is selected.)
16. Set the IP address and connected port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22. Click **Open** to start the connection. As the current authentication mode does not require a user name, you can type in any user name, but cannot be null. (In this example, the user name is "anyname".)

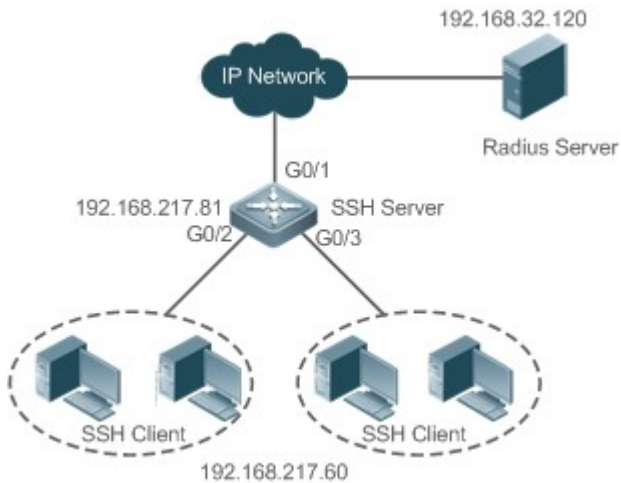
## 8.2.3 SSH AAA Authentication

### Scenario

SSH users can use the AAA authentication mode for user authentication, as shown in Figure 11-24. To ensure security of data exchange, the PCs function as the SSH clients, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used for user login on the SSH clients. Two authentication methods, including Radius server authentication and local

authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, it turns to the local authentication.

Figure 11-24 Networking Topology of SSH AAA Authentication



## Deployment

- The routes from the SSH clients to the SSH server are reachable, and the route from the SSH server to the Radius server is also reachable.
- Configure the SSH server on the network device that functions as an SSH client.
- Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.

## 8.2.4 SSH Public Key Authentication

### Scenario

SSH clients can use the public keys for authentication, and the public key algorithm can be RSA or DSA, as shown in Figure 11-25. SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 11-25 Network Topology for Public Key Authentication of SSH Users



## Deployment

- To implement public key authentication for the client, generate a key pair (RSA or DSA) on the client, configure the public key on the SSH server, and select the public key authentication mode.



- After the key is generated on the client, the SSH server will copy the file of the public key from the client to the flash and associates the file with the SSH user name. Each user can be associated with one RSA public key and one DSA public key.

## 8.2.5 SSH File Transfer

### Scenario

The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server, as shown in Figure 11-26.

Figure 11-26 Networking Topology of SSH File Transfer



### Deployment

- Enable the SCP service on the server.
- On the client, use SCP commands to upload files to the server, or download files from the server.

## 8.3 Features

### Basic Concepts

#### ↳ User Authentication Mechanism

- Password authentication

During the password authentication, a client sends a user authentication request and encrypted user name and password to the server. The server decrypts the received information, compares the decrypted information with those stored on the server, and then returns a message indicating the successful or unsuccessful authentication.

- Public key authentication

During the public key authentication, digital signature algorithms, such as RSA and DSA, are used to authenticate a client. The client sends a public key authentication request to the server. This request contains information including the user name, public key, and public key algorithm. On receiving the request, the server checks whether the public key is correct. If wrong, the server directly sends an authentication failure message. If right, the server performs digital signature authentication on the client, and returns a message indicating the successful or unsuccessful authentication.

- Public key authentication is applicable only to the SSHv2 clients.

#### ↳ SSH Communication

To ensure secure communication, interaction between an SSH server and an SSH client undergoes the following seven stages:

- Connection setup

The server listens on Port 22 to the connection request from the client. After originating a socket initial connection request, the client sets up a TCP socket connection with the server.

- Version negotiation

If the connection is set up successfully, the server sends a version negotiation packet to the client. On receiving the packet, the client analyzes the packet and returns a selected protocol version to the server. The server analyzes the received information to determine whether version negotiation is successful.

- Key exchange and algorithm negotiation

If version negotiation is successful, key exchange and the algorithm negotiation are performed. The server and the client exchange the algorithm negotiation packet with each other, and determine the final algorithm based on their capacity. In addition, the server and the client work together to generate a session key and a session ID according to the key exchange algorithm and host key, which will be applied to subsequent user authentication, data encryption, and data decryption.

- User authentication

After the encrypted channel is set up, the client sends an authentication request to the server. The server repeatedly conducts authentication for the client until the authentication succeeds or the server shuts down the connection because the maximum number of authentication attempts is reached.

- Session request

After the successful authentication, the client sends a session request to the server. The server waits and processes the client request. After the session request is successfully processed, SSH enters the session interaction stage.

- Session interaction

After the session request is successfully processed, SSH enters the session interaction stage. Encrypted data can be transmitted and processed in both directions. The client sends a command to be executed to the client. The server decrypts, analyzes, and processes the received command, and then sends the encrypted execution result to the client. The client decrypts the execution result.

- Session ending

When the interaction between the server and the client is terminated, the socket connection disconnects, and the session ends.

## Overview

---

| Feature                     | Description  |
|-----------------------------|--|
| <a href="#">SSH Server</a>  | Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client.   |
| <a href="#">SCP Service</a> | After the SCP service is enabled, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security. |

### 8.3.1 SSH Server

Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client. You can also shut down the SSH server function to disconnect from all SSH clients.

#### Working Principle

For details about the working principle of the SSH server, see the "SSH Communication" in "Basic Concepts."

In practice, after enabling the SSH server function, you can configure the following parameters according to the application requirements:

- Version: Configure the SSH version as SSHv1 or SSHv2 to connect SSH clients.
- Authentication timeout: The SSH server starts the timer after receiving a user connection request. The SSH server is disconnected from the client either when the authentication succeeds or when the authentication timeout is reached.
- Maximum number of authentication retries: The SSH server starts authenticating the client after receiving its connection request. If authentication does not succeed when the maximum number of user authentication retries is reached, a message is sent, indicating the authentication failure.
- Public key authentication: The public key algorithm can be RSA or DSA. It provides a secure connection between the client and the server. The public key file on the client is associated with the user name. In addition, the public key authentication mode is configured on the client, and the corresponding private key file is specified. In this way, when the client attempts to log in to the server, public key authentication can be implemented to set up a secure connection.

#### Related Configuration

##### ↳ Enabling the SSH Server

By default, the SSH server is disabled.

In global configuration mode, run the `[no] enable service ssh-server` command to enable or disable the SSH server.

To generate the SSH key, you also need to enable the SSH server.

##### ↳ Specifying the SSH Version

By default, the SSH server supports both SSHv1 and SSHv2, connecting either SSHv1 clients or SSHv2 clients.

Run the `ip ssh version` command to configure the SSH version supported by the SSH server.

If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

##### ↳ Configuring the SSH Authentication Timeout

By default, the user authentication timeout is 120s.

Run the `ip ssh time-out` command to configure the user authentication timeout of the SSH server. Use the `no` form of the command to restore the default timeout. The SSH server starts the timer after receiving a user connection request. If authentication does not succeed before the timeout is reached, authentication times out and fails.

##### ↳ Configuring the Maximum Number of SSH Authentication Retries

By default, the maximum number of user authentication retries is 3.

---

Run the **ip ssh authentication-retries** command to configure the maximum number of user authentication retries on the SSH server. Use the **no** form of the command to restore the default number of user authentication retries.

If authentication still does not succeed when the maximum number of user authentication retries is reached, user authentication fails.

#### ↳ Specifying the SSH Encryption Mode

By default, the encryption mode supported by the SSH server is Compatible, that is, supporting cipher block chaining (CBC), counter (CTR) and other encryption modes.

Run the **ip ssh cipher-mode** command to configure the encryption mode supported by the SSH server. Use the **no** form of the command to restore the default encryption mode supported by the SSH server.

#### ↳ Specifying the SSH Message Authentication Algorithm

By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5,SHA1,SHA1-96, and MD5-96, are supported.

Run the **ip ssh hmac-algorithm** command to configure the message authentication algorithm supported by the SSH server. Use the **no** form of the command to restore the default message authentication algorithm supported by the SSH server.

#### ↳ Enabling the Public Key Authentication on the SSH Server

Run the **ip ssh peer** command to associate the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

## 8.3.2 SCP Service

The SSH server provides the SCP service to implement secure file transfer between the server and the client.

### Working Principle

- SCP is a protocol that supports online file transfer. It runs on Port 22 based on the BSC RCP protocol, whereas RCP provides the encryption and authentication functions based on the SSH protocol. RCP implements file transfer, and SSH implements authentication and encryption.
- Assume that the SCP service is enabled on the server. When you use an SCP client to upload or download files, the SCP client first analyzes the command parameters, sets up a connection with a remote server, and starts another SCP process based on this connection. This process may run in source or sink mode. (The process running in source mode is the data provider. The process running in sink mode is the destination of data.) The process running in source mode reads and sends files to the peer end through the SSH connection. The process running in sink mode receives files through the SSH connection.

### Related Configuration

#### ↳ Enabling the SCP Server

By default, the SCP server function is disabled.

Run the **ip scp server enable** command to enable SCP server function on a network device.

---

## 8.4 Configuration

| Configuration   | Description and Command   |  |
|---|---|--|
| <a href="#">Configuring the SSH Server</a>                                | <ul style="list-style-type: none"> <li>It is mandatory to enable the SSH server.</li> </ul> |  |
|   | <b>enable service ssh-server</b>  | Enables the SSH server.                                      |
|   | <b>disconnect ssh[<i>vty</i>] <i>session-id</i></b>   | Disconnects an established SSH session.                      |
|   | <b>crypto key generate {<i>rsa dsa</i>}</b>   | Generates an SSH key.  |
|   | <b>ip ssh version {<i>1 2</i>}</b>  | Specifies the SSH version.                                   |
|   | <b>ip ssh time-out <i>time</i></b>  | Configures the SSH authentication timeout.                   |
|   | <b>ip ssh authentication-retries <i>retry times</i></b>                                     | Configures the maximum number of SSH authentication retries. |
|   | <b>ip ssh cipher-mode{<i>cbc   ctr   others</i> }</b>                                       | Specifies the SSH encryption mode.                           |
|   | <b>ip ssh hmac-algorithm{<i>md5   md5-96   sha1   sha1-96</i>}</b>                          | Specifies the SSH message authentication algorithm.          |
|   | <b>ip ssh peer <i>test</i> public-key <i>rsa</i> flash :<i>rsa.pub</i></b>                  | Associates an RSA public key file with a user.               |
| <b>ip ssh peer <i>test</i> public-key <i>dsa</i> flash:<i>dsa.pub</i></b> | Associates a DSA public key file with a user.   |  |
| <a href="#">Configuring the SCP Service</a>                               | <ul style="list-style-type: none"> <li>Mandatory.</li> </ul>                                |  |
|   | <b>ip scp server enable</b>   | Enables the SCP server.                                      |

### 8.4.1 Configuring the SSH Server

#### Configuration Effect

- Enable the SSH server function on a network device so that you can set up a secure connection with a remote network device through the SSH client. All interactive data is encrypted before transmitted, featuring authentication and security.
- You can use diversified SSH user authentications modes, including local line password authentication, AAA authentication, and public key authentication.
- You can generate or delete an SSH key.
- You can specify the SSH version.
- You can configure the SSH authentication timeout.
- You can configure the maximum number of SSH authentication retries.
- You can specify the SSH encryption mode.
- You can specify the SSH message authentication algorithm.

- You can specify ACL filtering of the SSH server.

## Notes

---

- The precondition of configuring a device as the SSH server is that communication is smooth on the network that the device resides, and the administrator can access the device management interface to configure related parameters.
- The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key.
- The SSH module does not support hot standby. Therefore, for products that supports hot standby on the supervisor modules, if no SSH key file exist on the new active module after failover, you must run the **crypto key generate** command to re-generate a key before using SSH.

## Configuration Steps

---

### ↳ Enabling the SSH Server

- Mandatory.
- By default, the SSH server is disabled. In global configuration mode, enable the SSH server and generate an SSH key so that the SSH server state changes to ENABLE.

### ↳ Specifying the SSH Version

- Optional.
- By default, the SSH server supports SSHv1 and SSHv2, connecting either SSHv1 or SSHv2clients. If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

### ↳ Configuring the SSH Authentication Timeout

- Optional.
- By default, the SSH authentication timeout is 120s. You can configure the user authentication timeout as required. The value ranges from 1 to 120. The unit is second.

### ↳ Configuring the Maximum Number of SSH Authentication Retries

- Optional.
- Configure the maximum number of SSH authentication retries to prevent illegal behaviors such as malicious guessing. By default, the maximum number of SSH authentication retries is 3, that is, a user is allowed to enter the user name and password three times for authentication. You can configure the maximum number of retries as required. The value ranges from 0 to 5.

### ↳ Specifying the SSH Encryption Mode

- Optional.
- Specify the encryption mode supported by the SSH server. By default, the encryption mode supported by the SSH server is Compatible, that is, supporting CBC, CTR and other encryption modes.

### ↳ Specifying the SSH Message Authentication Algorithm

- Optional.
- Specify the message authentication algorithm supported by the SSH server. By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5, SHA1, SHA1-96, and MD5-96, are supported.

#### ↘ Setting ACL Filtering of the SSH Server

- Optional.
- Set ACL filtering of the SSH server. By default, ACL filtering is not performed for all connections to the SSH server. According to needs, set ACL filtering to perform for all connections to the SSH server.

#### ↘ Enabling the Public Key Authentication for SSH Users

- Optional.
- Only SSHv2 supports authentication based on the public key. This configuration associates a public key file on the client with a user name. When a client is authenticated upon login, a public key file is specified based on the user name.

### Verification

- Run the **show ip ssh** command to display the current SSH version, authentication timeout, and maximum number of authentication retries of the SSH server.
- Run the **show crypto key mypubkey** command to display the public information of the public key to verify whether the key has been generated.
- Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

### Related Commands

#### ↘ Enabling the SSH Server

|                     |   |
|---------------------|---|
| <b>Command</b>      | <b>enable service ssh-server</b>  |
| <b>Parameter</b>    | N/A   |
| <b>Description</b>  |   |
| <b>Command Mode</b> | Global configuration mode   |
| <b>Usage Guide</b>  | To disable the SSH server, run the <b>no enable service ssh-server</b> command in global configuration mode. After this command is executed, the SSH server state changes to DISABLE. |

#### ↘ Disconnecting an Established SSH Session

|                    |  |
|--------------------|--|
| <b>Command</b>     | <b>disconnect ssh[vty] session-id</b>  |
| <b>Parameter</b>   | <b>vty:</b> Indicates an established virtual teletype terminal (VTY) session.                      |
| <b>Description</b> | <b>session-id:</b> Indicates the ID of the established SSH session. The value ranges from 0 to 35. |
| <b>Command</b>     | Privileged EXEC mode   |

|                    |  |
|--------------------|--|
| <b>Mode</b>        |  |
| <b>Usage Guide</b> | Specify an SSH session ID to disconnect the established SSH session. Alternatively, specify a VTY session ID to disconnect a specified SSH session. Only an SSH session can be disconnected. |

### ↘ Generating an SSH Key

|                     |   |
|---------------------|---|
| <b>Command</b>      | <b>crypto key generate {rsa dsa}</b>  |
| <b>Parameter</b>    | <b>rsa:</b> Generates an RSA key.   |
| <b>Description</b>  | <b>dsa:</b> Generates a DSA key.  |
| <b>Command Mode</b> | Global configuration mode   |
| <b>Usage Guide</b>  | The <b>no crypto key generate</b> command does not exist. You need to run the <b>crypto key zeroize</b> command to delete a key.<br>SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key.<br>If an RSA key is generated, both SSHv1 and SSHv2 are supported. If only a DSA key is generated, only SSHv2 can use the key. |

### ↘ Specifying the SSH Version

|                     |   |
|---------------------|---|
| <b>Command</b>      | <b>ip ssh version {1 2}</b>   |
| <b>Parameter</b>    | <b>1:</b> Indicates that the SSH server only receives the connection requests sent by SSHv1 clients.                                |
| <b>Description</b>  | <b>2:</b> Indicates that the SSH server only receives the connection requests sent by SSHv2 clients.                                |
| <b>Command Mode</b> | Global configuration mode   |
| <b>Usage Guide</b>  | Run the <b>no ip ssh version</b> command to restore the default settings. By default, the SSH server supports both SSHv1 and SSHv2. |

### ↘ Configuring the SSH Authentication Timeout

|                     |   |
|---------------------|---|
| <b>Command</b>      | <b>ip ssh time-out <i>time</i></b>  |
| <b>Parameter</b>    | <b><i>time</i>:</b> Indicates the SSH authentication timeout. The value ranges from 1 to 120. The unit is second. |
| <b>Description</b>  |   |
| <b>Command Mode</b> | Global configuration mode   |
| <b>Usage Guide</b>  | Run the <b>no ip ssh time-out</b> command to restore the default SSH authentication timeout, which is 120s.       |

### ↘ Configuring the Maximum Number of SSH Authentication Retries

|                     |   |
|---------------------|---|
| <b>Command</b>      | <b>ip ssh authentication-retries <i>retry times</i></b>   |
| <b>Parameter</b>    | <b><i>retry times</i>:</b> Indicates the maximum number of user authentication retries. The value ranges from 0 to 5.             |
| <b>Description</b>  |   |
| <b>Command Mode</b> | Global configuration mode   |
| <b>Usage Guide</b>  | Run the <b>no ip ssh authentication-retries</b> command to restore the default number of user authentication retries, which is 3. |



## ↳ Specifying the SSH Encryption Mode

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <code>ip ssh cipher-mode{cbc   ctr   others }</code>   |
| <b>Parameter Description</b> | <p><b>cbc:</b> Sets the encryption mode supported by the SSH server to the CBC mode. Corresponding algorithms include DES-CBC,3DES-CBC,AES-128-CBC,AES-192-CBC,AES-256-CBC, and Blowfish-CBC.</p> <p><b>ctr:</b> Sets the encryption mode supported by the SSH server to the CTR mode. Corresponding algorithms include AES128-CTR, AES192-CTR, and AES256-CTR.</p> <p><b>others:</b> Sets the encryption mode supported by the SSH server to others. The corresponding algorithm is RC4.</p>  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | <p>This command is used to configure the encryption mode supported by the SSH server.</p> <p>On Orion Alpha A28X devices, the SSHv1 server supports the DES-CBC, 3DES-CBC, and Blowfish-CBC encryption algorithms; the SSHv2 server supports the AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4 encryption algorithms. These algorithms can be grouped into three encryption modes: CBC, CTR, and others.</p> <p>As the cryptography continuously develops, it is approved that encryption algorithms in the CBC and others modes can be decrypted in a limited period of time. Therefore, organizations or companies that have high security requirements can set the encryption mode supported by the SSH server to CTR to increase the security level of the SSH server.</p> |

## ↳ Specifying the SSH Message Authentication Algorithm

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <code>ip ssh hmac-algorithm{md5   md5-96   sha1   sha1-96}</code>   |
| <b>Parameter Description</b> | <p><b>md5:</b> Indicates that the message authentication algorithm supported by the SSH server is MD5.</p> <p><b>md5-96:</b> Indicates that the message authentication algorithm supported by the SSH server is MD5-96.</p> <p><b>sha1:</b> Indicates that the message authentication algorithm supported by the SSH server is SHA1.</p> <p><b>sha1-96:</b> Indicates that the message authentication algorithm supported by the SSH server is SHA1-96.</p> |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | <p>This command is used to configure the message authentication algorithm supported by the SSH server.</p> <p>On Orion Alpha A28X devices, the SSHv1 server does support any message authentication algorithm; the SSHv2 server supports the MD5, SHA1, SHA1-96, <b>and</b> MD5-96 message authentication algorithms. You can select message authentication algorithms supported by the SSH server as required.</p>   |

## ↳ Configuring RSA Public Key Authentication

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <code>ip ssh peer test public-key rsaflash:rsa.pub</code>  |
| <b>Parameter Description</b> | <p><b>test:</b> Indicates the user name.</p> <p><b>rsa:</b> Indicates that the public key type is RSA.</p> <p><b>rsa.pub:</b> Indicates the name of a public key file.</p> |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | This command is used to configure the RSA public key file associated with user <i>test</i> .   |

---

|  |   |
|--|---|
|  | Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name. |
|--|---|

### ↘ **Configuring DSA Public Key Authentication**

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>ip ssh peer test public-key dsaflash:dsa.pub</b>  |
| <b>Parameter Description</b> | <i>test</i> : Indicates the user name.<br><b>dsa</b> : Indicates that the public key type is DSA.<br><i>dsa.pub</i> : Indicates the name of a public key file.   |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | This command is used to configure the DSA key file associated with user <b>test</b> .<br>Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name. |

### Configuration Example

- The following configuration examples describe only configurations related to SSH.

### ↘ **Generating a Public Key on the SSH Server**

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Run the <b>crypto key generate { rsa   dsa }</b> command to generate a RSA public key for the server.</li> </ul>  |
| <b>SSH Server</b>          | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)# crypto key generate rsa Choose the size of the rsa key modulus in the range of 512 to 2048 and the size of the dsa key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes.  How many bits in the modulus [512]:</pre> <ul style="list-style-type: none"> <li>● If the generation of the RSA key is successful, the following information is displayed: <pre>% Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok]</pre> </li> <li>● If the generation of the RSA key fails, the following information is displayed: <pre>% Generating 512 bit RSA1 keys ...[fail] % Generating 512 bit RSA keys ...[fail]</pre> </li> </ul> |
| <b>Verification</b>        | <ul style="list-style-type: none"> <li>● Run the <b>show crypto key mypubkey rsa</b> command to display the public information about the</li> </ul>  |

|                   |  |
|-------------------|--|
|                   | RSA key. If the public information about the RSA key exists, the RSA key has been generated.   |
| <b>SSH Server</b> | <pre> Orion Alpha A28X(config)#show crypto key mypubkey rsa  % Key pair was generated at: 1:49:47 UTC Jan 4 2013  Key name: RSA1 private Usage: SSH Purpose Key Key is not exportable.  Key Data: AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU       8O3LojHL ayJ8G4pG 7j4T4ZSf FKg09kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t qFIKDj1j       0dKBcCfN tr0r/CT+ cs5tlGKV S0ICGifz oB+pYaE=  % Key pair was generated at: 1:49:47 UTC Jan 4 2013  Key name: RSA private Usage: SSH Purpose Key Key is not exportable.  Key Data: AAAAAwEAAQAAAHJfLwKnzOgO F3RIKhTN /7PmQYoE v0a2VXTX 8ZCa7SII EghLDLJc       w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISglfZ9 8o5No3Zz MPM0LnQR       G4c7/28+ GOHzYkTk 4liQuTIL HRgtbyEYXCFaaxU= </pre> |

### ↳ Specifying the SSH Version

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>Run the <b>ip ssh version { 1   2 }</b> command to set the version supported by the SSH server to SSHv2.</li> </ul>        |
| <b>SSH Server</b>          | <pre> Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#ip ssh version 2 </pre>  |
| <b>Verification</b>        | <ul style="list-style-type: none"> <li>Run the <b>show ip ssh</b> command to display the SSH version currently supported by the SSH server.</li> </ul>            |
| <b>SSH Server</b>          | <pre> Orion Alpha A28X(config)#show ip ssh  SSH Enable - version 2.0  Authentication timeout: 120 secs Authentication retries: 3  SSH SCP Server: disabled </pre> |

### ↳ Configuring the SSH Authentication Timeout

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>Run the <b>ip ssh time-out <i>time</i></b> command to set the SSH authentication timeout to 100s.</li> </ul>          |
| <b>SSH Server</b>          | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#ip ssh time-out 100</pre>  |
| <b>Verification</b>        | <ul style="list-style-type: none"> <li>Run the <b>show ip ssh</b> command to display the configured SSH authentication timeout.</li> </ul>                   |
| <b>SSH Server</b>          | <pre>Orion Alpha A28X(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled</pre> |

### ↘ Configuring the Maximum Number of SSH Authentication Retries

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>Run the <b>ip ssh authentication-retries <i>retry times</i></b> command to set the maximum number of user authentication retries on the SSH server to 2.</li> </ul> |
| <b>SSH Server</b>          | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#ip ssh authentication-retries 2</pre>  |
| <b>Verification</b>        | <ul style="list-style-type: none"> <li>Run the <b>show ip ssh</b> command to display the configured maximum number of authentication retries.</li> </ul>   |
| <b>SSH Server</b>          | <pre>Orion Alpha A28X(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled</pre>   |

### ↘ Specifying the SSH Encryption Mode

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>Run the <b>ip ssh cipher-mode {cbc   ctr   others }</b> command to set the encryption mode supported by the SSH server to CTR.</li> </ul>          |
| <b>SSH Server</b>          | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)# ip ssh cipher-mode ctr</pre>   |
| <b>Verification</b>        | <ul style="list-style-type: none"> <li>Select the CTR encryption mode on the SSH client, and verify whether you can successfully log in to the SSH server from the SSH client.</li> </ul> |

### ↘ Specifying the SSH Message Authentication Algorithm


|                      |  |
|----------------------|--|
| <b>Configuration</b> | <ul style="list-style-type: none"> <li>Run the <b>ip ssh hmac-algorithm {md5   md5-96   sha1   sha1-96 }</b> command to set the message</li> </ul> |
|----------------------|--|

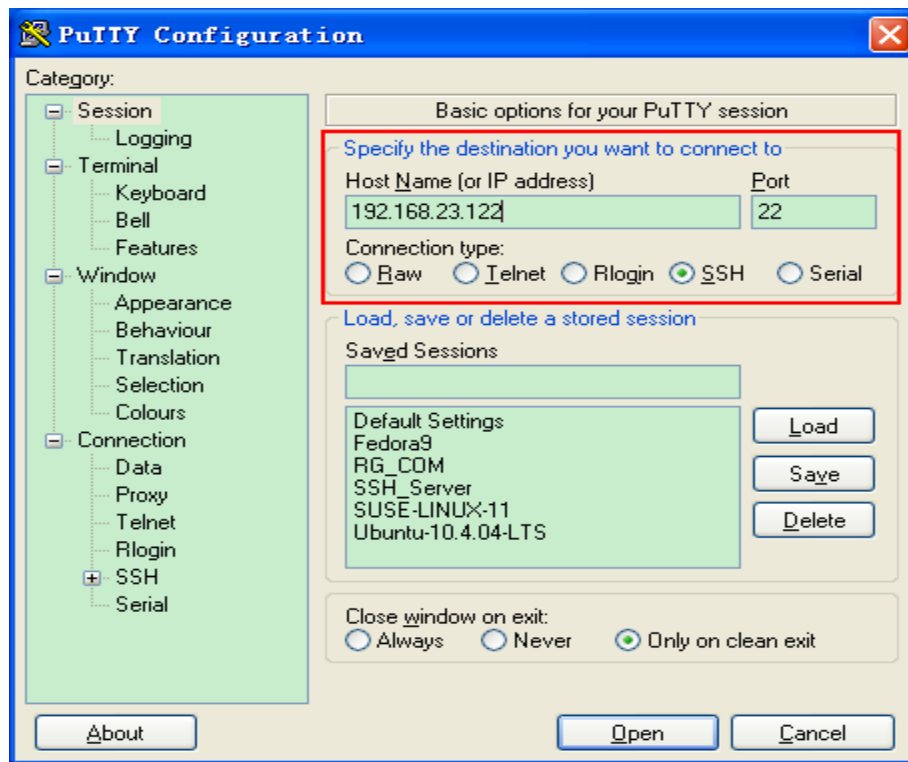
|                     |   |
|---------------------|---|
| <b>Steps</b>        | authentication algorithm supported by the SSH server to SHA1.   |
| <b>SSH Server</b>   | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)# ip ssh hmac-algorithmsha1</pre>  |
| <b>Verification</b> | <ul style="list-style-type: none"> <li>Select the SHA1 message authentication algorithm on the SSH client, and verify whether you can successfully log in to the SSH server from the SSH client.</li> </ul> |

### ↳ Configuring the Public Key Authentication

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>Run the <code>ip ssh peer <i>username</i> public-key { <i>rsa</i>   <i>dsa</i> } <i>filename</i></code> command to associate a public key file of the client with a user name. When the client is authenticated upon login, a public key file (for example, RSA) is specified based on the user name.</li> </ul>                    |
| <b>SSH Server</b>          | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)# ip ssh peer test public-key rsaflash:rsa.pub</pre>  |
| <b>Verification</b>        | <ul style="list-style-type: none"> <li>Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.</li> </ul> |

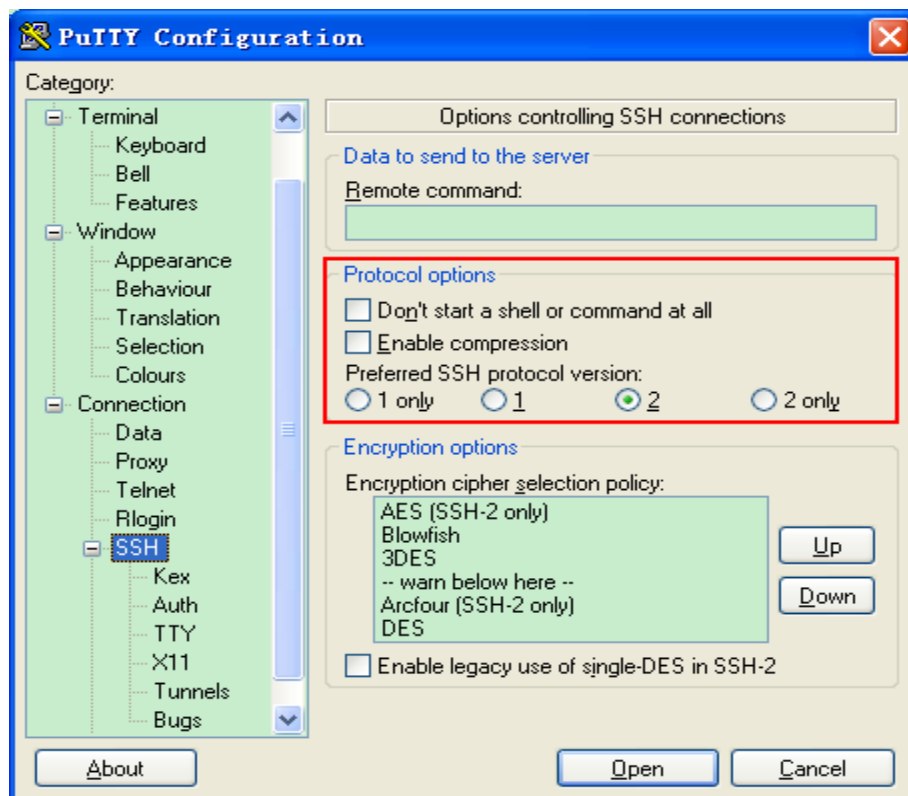
### ↳ Configuring SSH Device Management

|                                 |  |
|---------------------------------|--|
| <b>Scenario</b><br>Figure 11-27 |  <p>The diagram illustrates the SSH device management setup. On the left is the SSH Client with IP address 192.168.23.83. In the center is the IP Network. On the right is the SSH Server with IP address 192.168.23.122. Lines connect the client to the network and the network to the server.</p> <p>You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible client software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client.</p> |
| <b>Configuration Steps</b>      | <ul style="list-style-type: none"> <li>Start the PuTTY software.</li> <li>On the <b>Session</b> option tab of PuTTY, type in the host IP address <b>192.168.23.122</b> and SSH port number <b>22</b>, and select the connection type <b>SSH</b>.</li> <li>On the <b>SSH</b> option tab of PuTTY, select the preferred SSH protocol version <b>2</b>.</li> <li>On the <b>SSH authentication</b> option tab of PuTTY, select the authentication method <b>Attempt "keyboard-interactive" auth</b>.</li> <li>Click <b>Open</b> to connect to the SSH server.</li> <li>Type in the correct user name and password to enter the terminal login interface.</li> </ul>  |
| <b>SSH Client</b>               | Figure 11-28   |



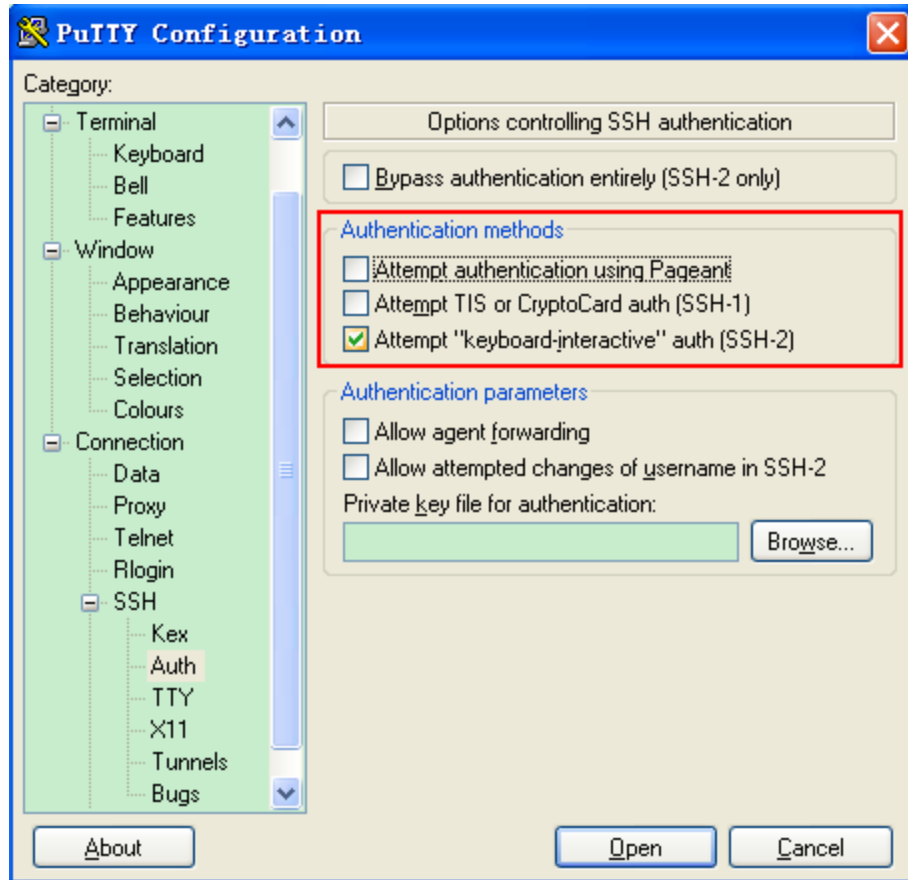
Host Name (or IP address) indicates the IP address of the host to be logged in. In this example, the IP address is 192.168.23.122. Port indicates the port ID 22, that is, the default ID of the port listened by SSH. Connection type is SSH.

Figure 11-29



As shown in Figure 11-29, select 2 as the preferred SSH protocol version in the Protocol options pane because SSHv2 is used for login.

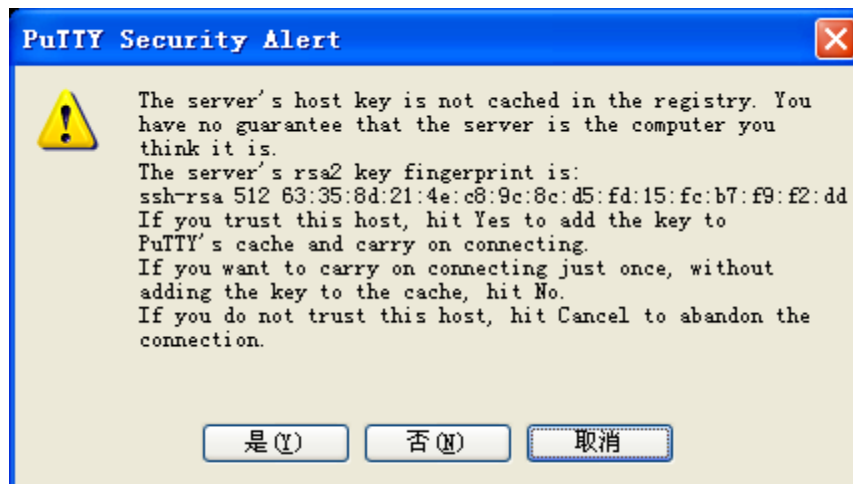
Figure 11-30



As shown in Figure 11-30, select Attempt "keyboard-interactive" auth as the authentication method to support authentication based on the user name and password.

Then, click Open to connect to the configured server host, as shown in Figure 11-30.

Figure 11-31

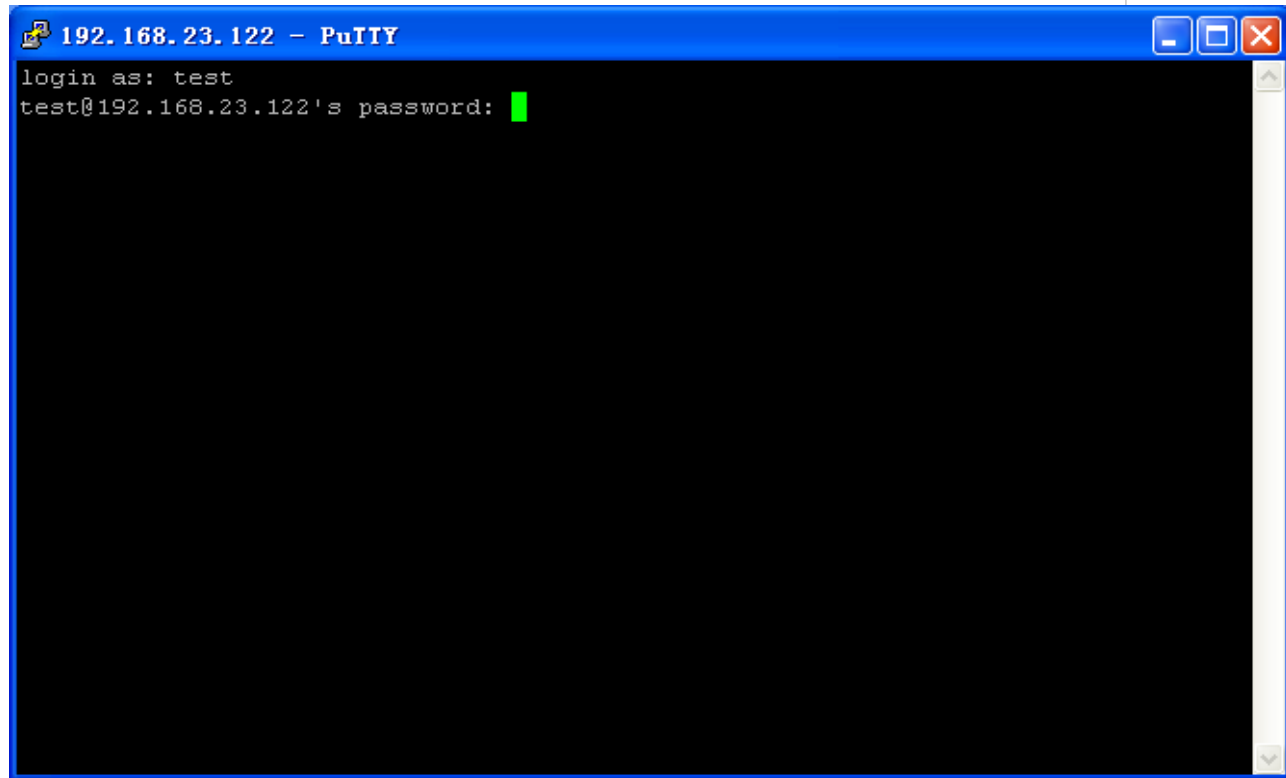


The PuTTY Security Alert box indicates that you are logging in to the client of the server 192.168.23.122, and asks you whether to receive the key sent from the server.

If you select Yes, a login dialog box is displayed, as shown in Figure 11-31.



Figure 11-32



Type in the correct user name and password, and you can log in to the SSH terminal interface, as shown in Figure 11-32.

Figure 11-33

```
192.168.23.122 - PuTTY
login as: test
test@192.168.23.122's password:
Ruijie#
```

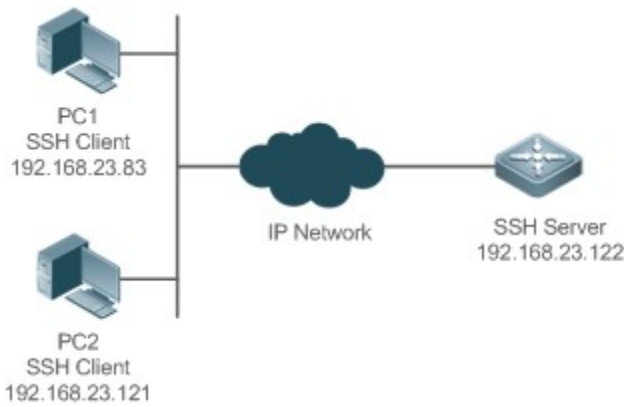
**Verification**

- Run the **show ip ssh** command to display the configurations that are currently effective on the SSH server.
- Run the **show ssh** command to display information about every SSH connection that has been established.

```
Orion Alpha A28X#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
Orion Alpha A28X#show ssh
Connection Version Encryption   Hmac   State   Username
-----
0    2.0 aes256-cbc   hmac-sha1  Session started test
```

↳ [Configuring SSH Local Line Authentication](#)

**Scenario**  
**Figure 11-34**



SSH users can use the local line password for user authentication, as shown in Figure 11-34. To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server is enabled. The requirements are as follows:

- SSH users use the local line password authentication mode.
- Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.

**Configuration**  
**Steps**

Configure the SSH server as follows:

- Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2.
- Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses the RSA key, whereas SSHv2 uses the RSA or DSA key.
- Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server based on this IP address. The route from the SSH client to the SSH server is reachable.

Configure the SSH client as follows:

- Diversified SSH client software is available, including PuTTY, Linux, and SecureCRT. This document takes PuTTY as an example to explain the method for configuring the SSH client. For details about the configuration method, see "Configuration Steps."

**SSH Server**

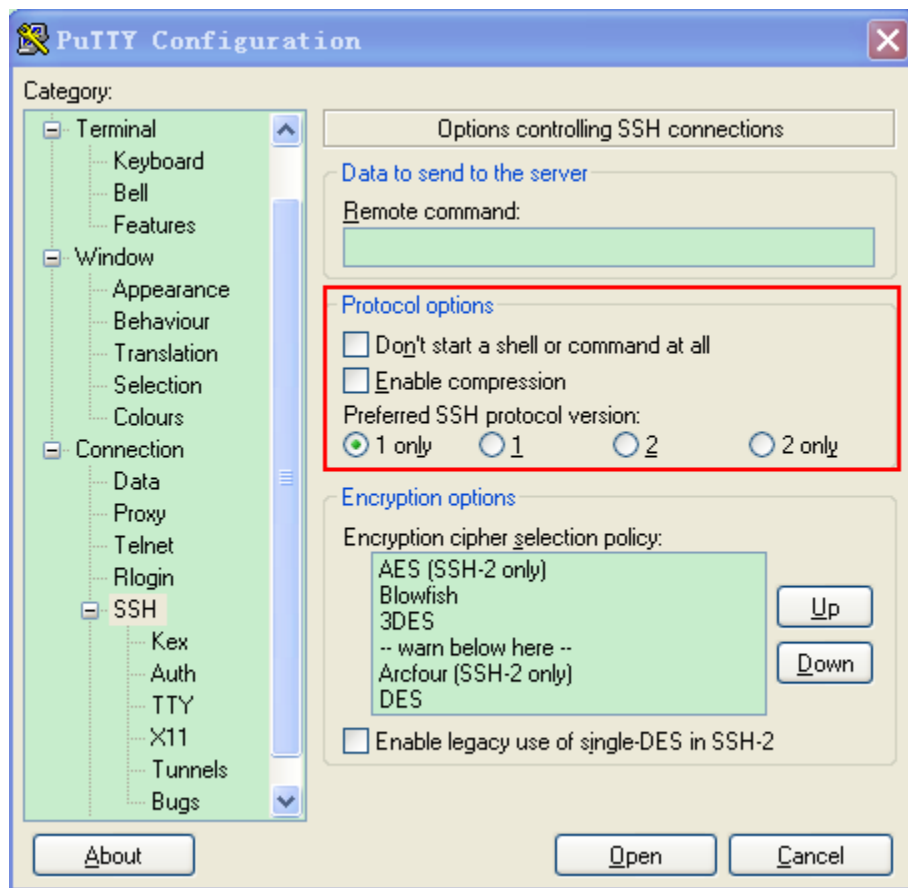
Before configuring SSH-related function, ensure that the route from the SSH user to the network segment of the SSH server is reachable. The interface IP address configurations are shown in Figure -6. The detailed procedures for configuring IP addresses and routes are omitted.

```
Orion Alpha A28X(config)# enable service ssh-server
Orion Alpha A28X(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
```

```
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
Orion Alpha A28X(config)#interface fastEthernet0/1
Orion Alpha A28X(config-if-fastEthernet0/1)#ip address 192.168.23.122 255.255.255.0
Orion Alpha A28X(config-if-fastEthernet0/1)#exit
Orion Alpha A28X(config)#line vty 0
Orion Alpha A28X(config-line)#password passzero
Orion Alpha A28X(config-line)#privilege level 15
Orion Alpha A28X(config-line)#login
Orion Alpha A28X(config-line)#exit
Orion Alpha A28X(config)#line vty1 4
Orion Alpha A28X(config-line)#password pass
Orion Alpha A28X(config-line)#privilege level 15
Orion Alpha A28X(config-line)#login
Orion Alpha A28X(config-line)#exit
```

**SSH**  
**Client(PC1/**  
**PC2)**

Figure 11-35



Set the IP address and port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22 (For details about the configuration method, see "Configuring SSH Device Management."). Click **Open** to start the SSH server. As the current authentication mode does not require a user name, you can type in any user name, but cannot leave the user name unspecified. (In this example, the user name is "anyname".)

#### Verification

- Run the **show running-config** command to display the current configurations.
- Verify that the SSH client configurations are correct.

#### SSH Server

```
Orion Alpha A28X#show running-config
Building configuration...

!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server

!

interface fastEthernet0/1
ip address 192.168.23.122 255.255.255.0

!
```

```
line vty 0
privilege level 15
login
password passzero
line vty 1 4
privilege level 15
login
password pass
!
end
```

### SSH Client

Set up a connection, and enter the correct password. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Then, the SSH server operation interface is displayed, as shown in Figure 11-36.

Figure 11-36

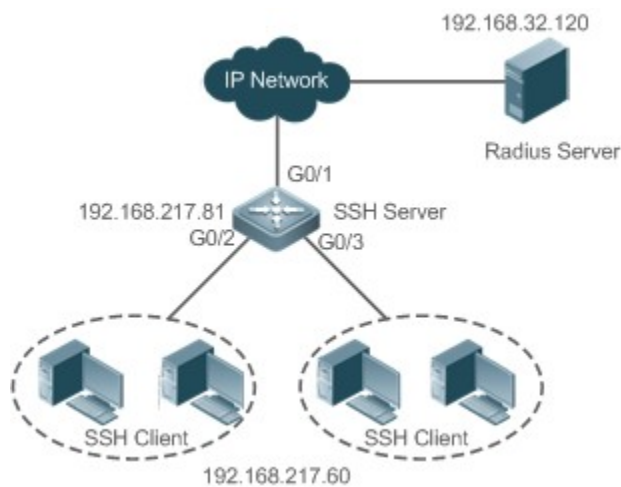


```
Orion Alpha A28X#show users
```

| Line      | User | Host(s) | Idle     | Location      |
|-----------|------|---------|----------|---------------|
| * 0 con 0 | ---  | idle    | 00:00:00 | ---           |
| 1 vty 0   | ---  | idle    | 00:08:02 | 192.168.23.83 |

## Configuring AAA Authentication of SSH Users

### Scenario Figure 11-37



SSH users can use the AAA authentication mode for user authentication, as shown in Figure 11-37. To ensure security of data exchange, the PC functions as the SSH client, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used on the user login interface of the SSH client. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, select the local authentication method.

### Configuration Steps

- The route from the SSH client to the SSH server is reachable, and the route from the SSH server to the Radius server is also reachable.
- Configure the SSH server on the network device. The configuration method is already described in the previous example, and therefore omitted here.
- Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.

### SSH Server

```
Orion Alpha A28X(config)# enable service ssh-server
Orion Alpha A28X(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```

How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
Orion Alpha A28X(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
Orion Alpha A28X(config)#interface gigabitEthernet1/1
Orion Alpha A28X(config-if-gigabitEthernet1/1)#ip address 192.168.217.81 255.255.255.0
Orion Alpha A28X(config-if-gigabitEthernet1/1)#exit
Orion Alpha A28X#configure terminal
Orion Alpha A28X(config)#aaa new-model
Orion Alpha A28X(config)#radius-server host 192.168.32.120
Orion Alpha A28X(config)#radius-server key aaradius
Orion Alpha A28X(config)#aaa authentication login methodgroup radius local
Orion Alpha A28X(config)#line vty 0 4
Orion Alpha A28X(config-line)#login authentication method
Orion Alpha A28X(config-line)#exit
Orion Alpha A28X(config)#username user1 privilege 1 password 111
Orion Alpha A28X(config)#username user2 privilege 10 password 222
Orion Alpha A28X(config)#username user3 privilege 15 password 333
Orion Alpha A28X(config)#enable secret w

```

**Verification**

- Run the **show running-config** command to display the current configurations.
- This example assumes that the SAM server is used.
- Set up a remote SSH connection on the PC.
- Check the login user.

```

Orion Alpha A28X#show run
aaa new-model
!
aaa authentication login method group radius local

```



```
!  
username user1 password 111  
username user2 password 222  
username user2 privilege 10  
username user3 password 333  
username user3 privilege 15  
no service password-encryption  
!  
radius-server host 192.168.32.120  
radius-server key aaaradius  
enable secret 5 $1$hbz$ArCsyqy6yyzpz03  
enable service ssh-server  
!  
interface gigabitEthernet1/1  
no ip proxy-arp  
ip address 192.168.217.81 255.255.255.0  
!  
ip route 0.0.0.0 0.0.0.0 192.168.217.1  
!  
line con 0  
line vty 0 4  
login authentication method  
!  
End
```

On the SSH client, choose **System Management>Device Management**, and add the device IP address **192.168.217.81** and the device key **aaaradius**.

Choose **Security Management>Device Management Rights**, and set the rights of the login user.

Choose **Security Management>Device Administrator**, and add the user name **user** and password **pass**.


Configure the SSH client and set up a connection to the SSH server. For details, see the previous example.

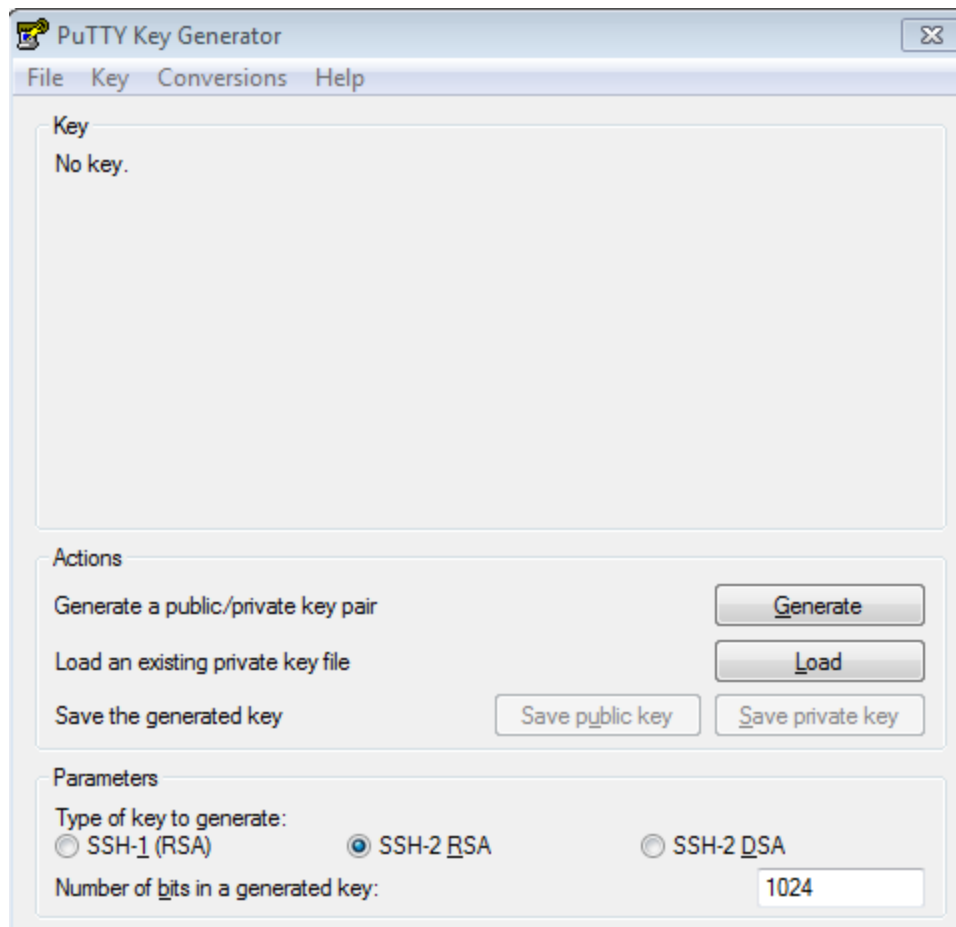
Type in the user name **user** and password **pass**. Verify that you can log in to the SSH server successfully.

```
Orion Alpha A28X#show users
```

| Line      | User | Host(s) | Idle     | Location       |
|-----------|------|---------|----------|----------------|
| 0 con 0   |      | idle    | 00:00:31 |                |
| * 1 vty 0 | user | idle    | 00:00:33 | 192.168.217.60 |

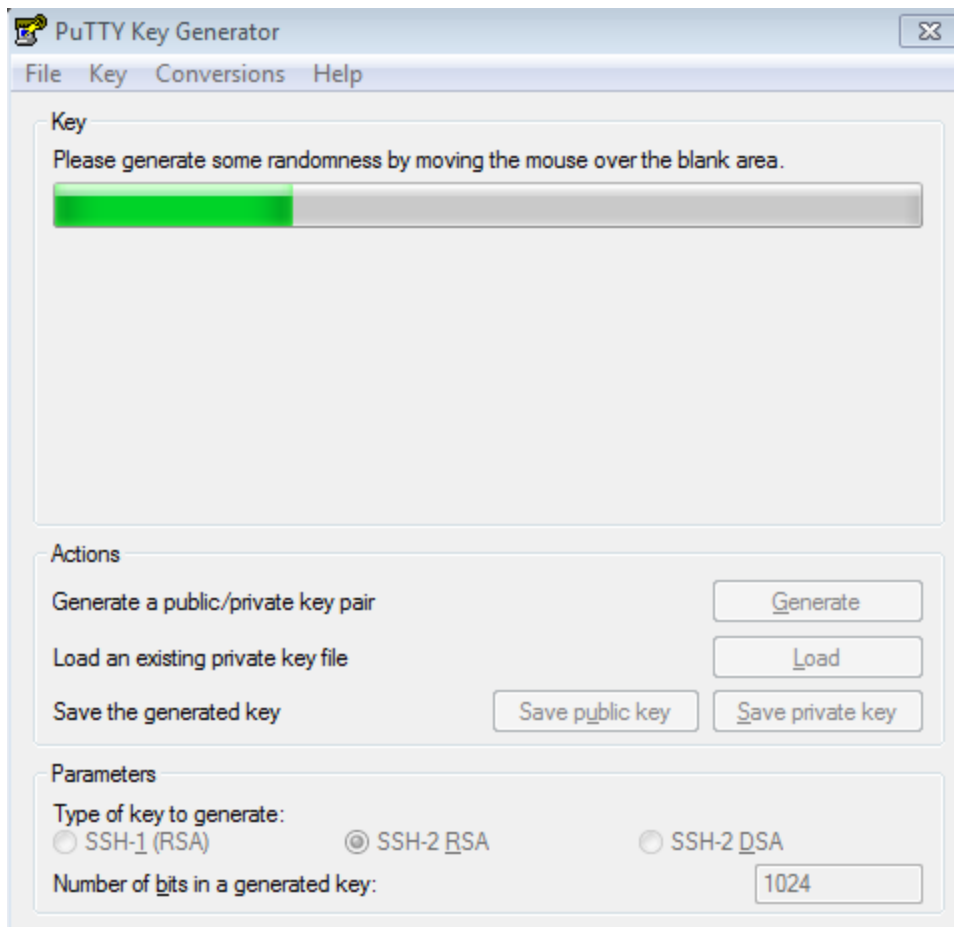
## ↘ Configuring Public Key Authentication of SSH Users

|   |   |
|---|---|
| <p><b>Scenario</b><br/>Figure 11-38</p> |  <p>SSH Client<br/>192.168.23.83</p> <p>IP Network</p> <p>SSH Server<br/>192.168.23.122</p> <p>SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in Figure -17. SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.</p>  |
| <p><b>Configuration Steps</b></p>       | <ul style="list-style-type: none"> <li>● To implement public key authentication on the client, generate a key pair (for example, RSA key) on the client, place the public key on the SSH server, and select the public key authentication mode.</li> <li>● After the key pair is generated on the client, you must save and upload the public key file to the server and complete the server-related settings before you can continue to configure the client and connect the client with the server.</li> <li>● After the key is generated on the client, copy the public key file from the client to the flash of the SSH server, and associate the file with an SSH user name. A user can be associated with one RSA public key and one DSA public key.</li> </ul> |
| <p><b>SSH Client</b></p>                | <p>Run the <b>puttygen.exe</b> software on the client. Select <b>SSH-2 RSA</b> in the <b>Parameters</b> pane, and click <b>Generate</b> to generate a key, as shown in Figure 11-39.</p> <p>Figure 11-39</p>  |



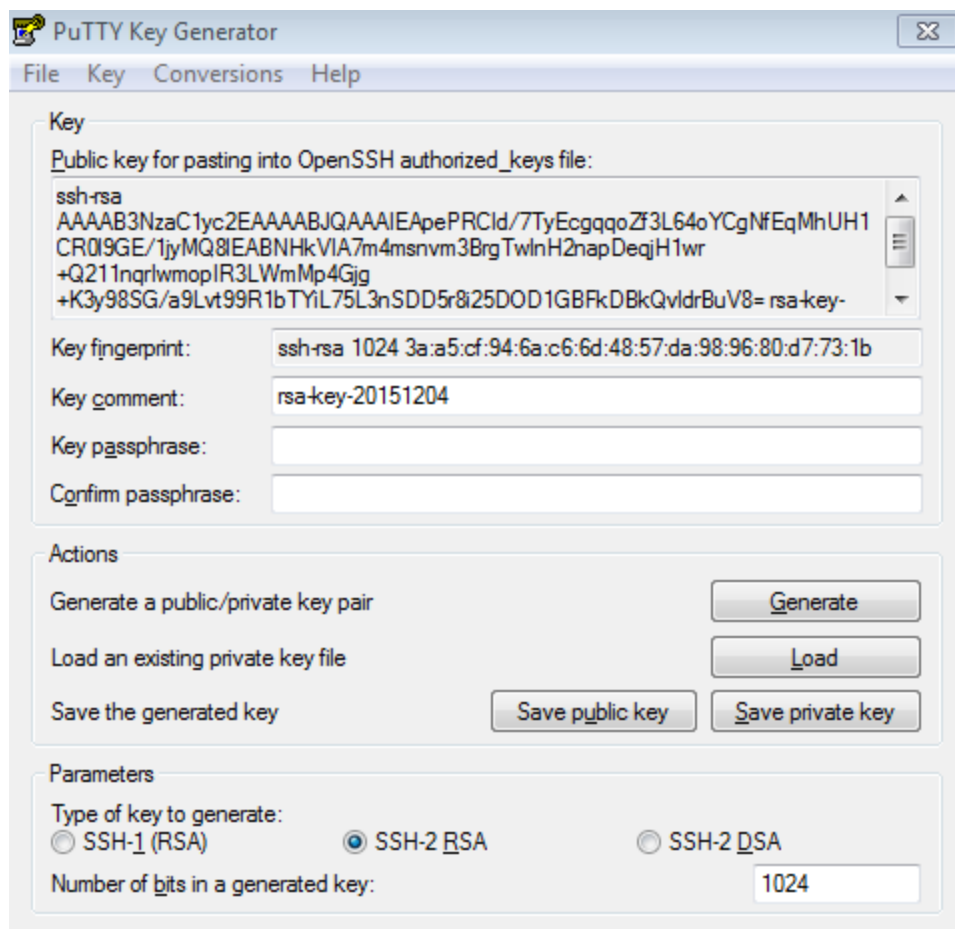
When a key is being generated, you need to constantly move the mouse over a blank area outside the green progress bar; otherwise, the progress bar does not move and key generation stops, as shown in Figure 11-40.

Figure 11-40



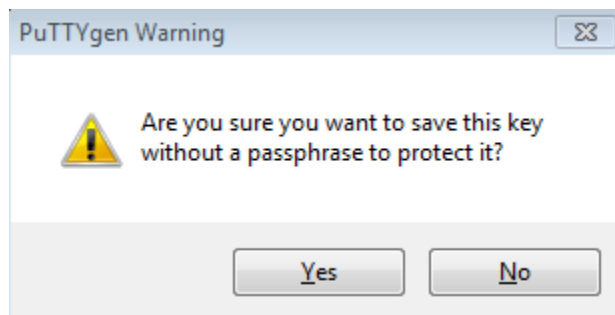
To ensure security of the RSA public key authentication, the length of the generated RSA key pair must be equal to or larger than 768 bits. In this example, the length is set to 1024 bits.

Figure 11-41



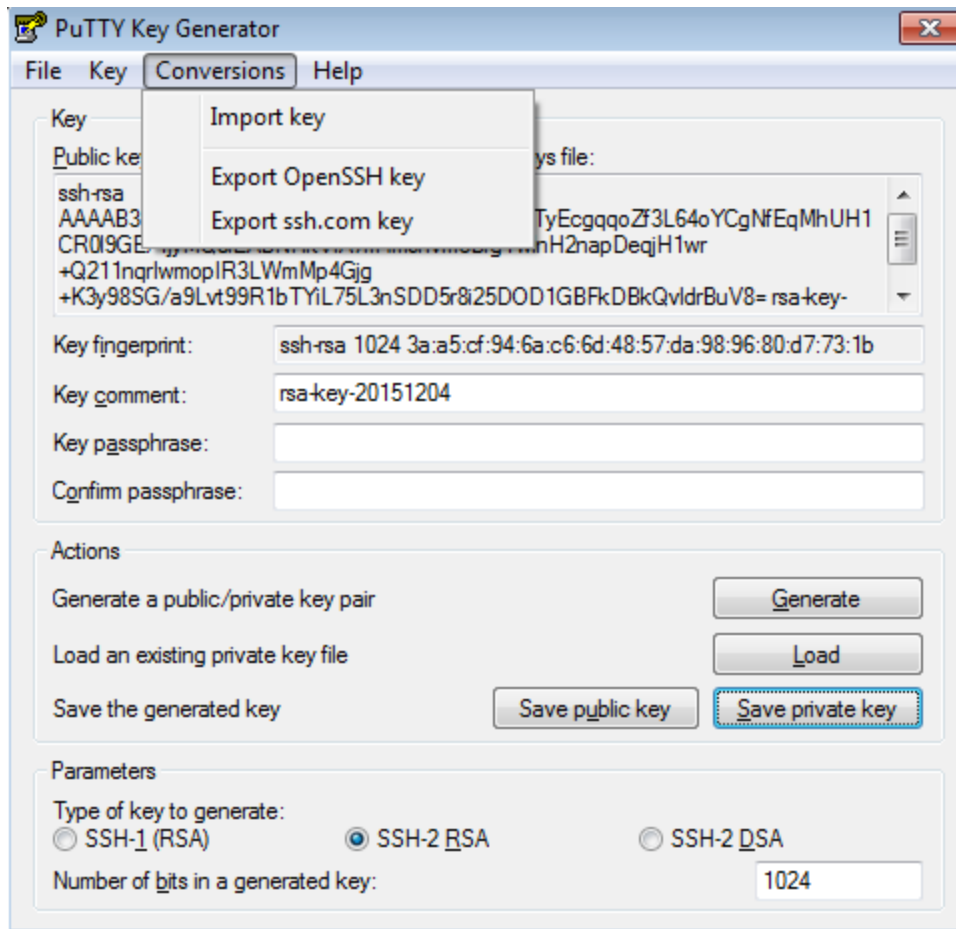
After the key pair is generated, click **Save public key**, type in the public key name **test\_key.pub**, select the storage path, and click **Save**. Then click **Save private key**. The following prompt box is displayed. Select **Yes**, type in the public key name **test\_private**, and click **Save**.

Figure 11-42

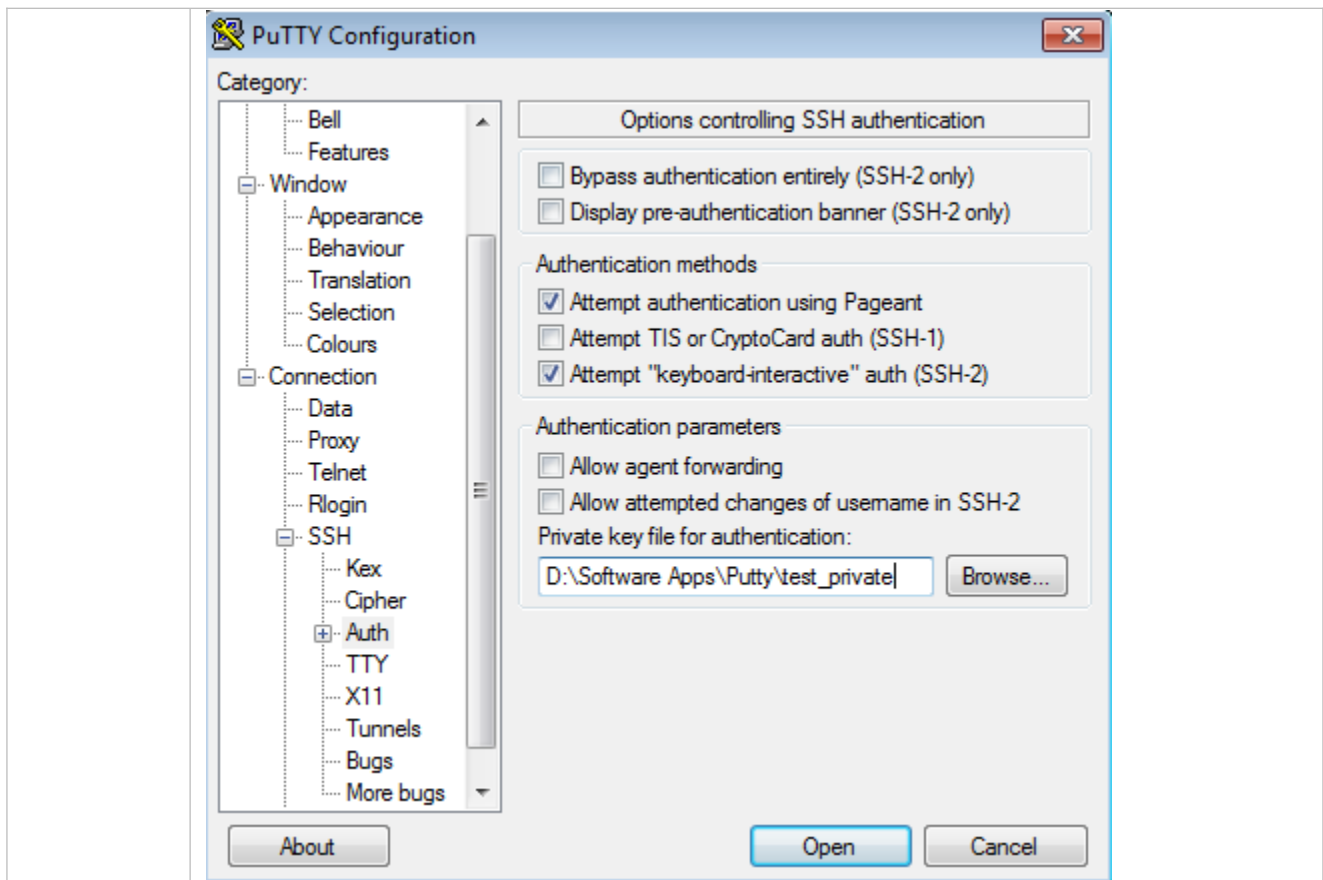


You must select the OpenSSH key file; otherwise, the key file cannot be used. The **puttygen.exe** software can be used to generate a key file in OpenSSH format, but this file cannot be directly used by the PuTTY client. You must use **puttygen.exe** to convert the private key to the PuTTY format. Format conversion is not required for the public key file stored on the server, and the format of this file is still OpenSSH, as shown in Figure 11-43.

Figure 11-43



|                     |   |
|---------------------|---|
| <b>SSH Server</b>   | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)# ip ssh peer test public-key rsaflash:test_key.pub</pre>  |
| <b>Verification</b> | <ul style="list-style-type: none"> <li>After completing the basic configurations of the client and the server, specify the private key file <b>test_private</b> on the PuTTY client, and set the host IP address to <b>192.168.23.122</b> and port ID to <b>22</b> to set up a connection between the client and the server. In this way, the client can use the public key authentication mode to log in to the network device.</li> </ul> |
|                     | Figure 11-44  |



## Common Errors

- The **no crypto key generate** command is used to delete a key.

## 8.4.2 Configuring the SCP Service

### Configuration Effect

After the SCP function is enabled on a network device, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

### Notes

- The SSH server must be enabled in advance.

### Configuration Steps

#### ↳ Enabling the SCP Server

- Mandatory.
- By default, the SCP server function is disabled. Run the **ip scp server enable** command to enable the SCP server function in global configuration mode.

## Verification

Run the **show ip ssh** command to check whether the SCP server function is enabled.

## Related Commands

### ↳ Enabling the SCP Server


|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>ip scp server enable</b>   |
| <b>Parameter Description</b> | N/A   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | This command is used to enable the SCP server.<br>Run the <b>no ip scp server enable</b> command to disable the SCP server. |

## Configuration Example

### ↳ Enabling the SCP Server

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"><li>Run the <b>ip scp server enable</b> command to enable the SCP server.</li></ul> <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)#ip scp server enable</pre>  |
| <b>Verification</b>        | <ul style="list-style-type: none"><li>Run the <b>show ip ssh</b> command to check whether the SCP server function is enabled.</li></ul> <pre>Orion Alpha A28X(config)#show ipssh SSH Enable - version 1.99 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: enabled</pre> |

### ↳ Configuring SSH File Transfer

|                                 |  |
|---------------------------------|--|
| <b>Scenario</b><br>Figure 11-45 |  <p>The diagram illustrates a network setup for SSH file transfer. On the left, an 'SSH Client' with IP address 192.168.23.83 is shown. A line connects it to a central 'IP Network' represented by a cloud. Another line connects the 'IP Network' to an 'SSH Server' with IP address 192.168.23.122 on the right.</p> |
|                                 | The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server.  |
| <b>Configuration Steps</b>      | <ul style="list-style-type: none"><li>Enable the SCP service on the server.</li><li>The SCP server uses SSH threading. When connecting to a network device for SCP transmission, the client occupies a VTY session (You can find out that the user type is SSH by running the show</li></ul>   |



|                     |  |
|---------------------|--|
|                     | <p>user command).</p> <ul style="list-style-type: none"> <li>On the client, use SCP commands to upload files to the server, or download files from the server.</li> </ul> <p>Syntax of the SCP command:</p> <pre>scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-iidentity_file]     [-l limit] [-o ssh_option] [-P port] [-S program]     [[user@]host1:]file1 [...] [[user@]host2:]file2</pre> <p>Descriptions of some options:</p> <ul style="list-style-type: none"> <li>-1: Uses SSHv1 (If not specified, SSHv2 is used by default);</li> <li>-2: Uses SSHv2 (by default);</li> <li>-C: Uses compressed transmission.</li> <li>-c: Specifies the encryption algorithm to be used.</li> <li>-r: Transmits the whole directory;</li> <li>-i: Specifies the key file to be used.</li> <li>-l: Limits the transmission speed (unit: Kbit/s).</li> </ul> <p>For other parameters, see the file scp.0.</p> <p>Most options are related to terminals. Few options are supported on both terminals and servers. Orion Alpha A28X's SCP servers do not support d-p-q-r options. When these options are applied, there are prompts.</p> |
| <b>SSH Server</b>   | <pre>Orion Alpha A28X#configure terminal Orion Alpha A28X(config)# ip scp server enable</pre>  |
| <b>Verification</b> | <ul style="list-style-type: none"> <li>File transmission example on the Ubuntu 7.10 system:</li> </ul> <p>Set the username of a client to <b>test</b> and copy the <b>config.text</b> file from the network device with the IP address of 192.168.195.188 to the <b>/root</b> directory on the local device.</p>   |
|                     | <pre>root@dhcpd:~#scp test@192.168.23.122:/config.text /root/config.text test@192.168.195.188's password: config.text          100% 1506   1.5KB/s  00:00 Read from remote host 192.168.195.188: Connection reset by peer</pre>  |

## 9 Configuring CPP

### 9.1 Overview

The CPU Protect Policy (CPP) provides policies for protecting the CPU of a switch.

In network environments, various attack packets spread, which may cause high CPU usages of the switches, affect protocol running and even difficulty in switch management. To this end, switch CPUs must be protected, that is, traffic control and priority-based processing must be performed for various incoming packets to ensure the processing capabilities of the switch CPUs.

CPP can effectively prevent malicious attacks in the network and provide a clean environment for legitimate protocol packets.

CPP is enabled by default. It provides protection during the entire operation of switches.

## 9.2 Monitoring

### Displaying

| Description  | Command                         |
|--|---------------------------------|
| Displays the effective SSH server configurations.      | <b>show ipssh</b>               |
| Displays the established SSH connection.               | <b>show ssh</b>                 |
| Displays the public information of the SSH public key. | <b>show crypto key mypubkey</b> |

### Debugging

- System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

| Description          | Command                          |
|----------------------|----------------------------------|
| Debugs SSH sessions. | <a href="#"><b>debug ssh</b></a> |

## 9.3 Applications

| Application   | Description  |
|---|--|
| <a href="#">Preventing Malicious Attacks</a>          | When various malicious attacks such as ARP attacks intrude in a network, CPP divides attack packets into queues of different priorities so that the attack packets will not affect other packets.    |
| <a href="#">Preventing CPU Processing Bottlenecks</a> | Even when no attacks exist, it would become a bottleneck for CPU to handle excessive normal traffic. CPP can limit the rate of packets being sent to the CPU to ensure normal operation of switches. |

### 9.3.1 Preventing Malicious Attacks

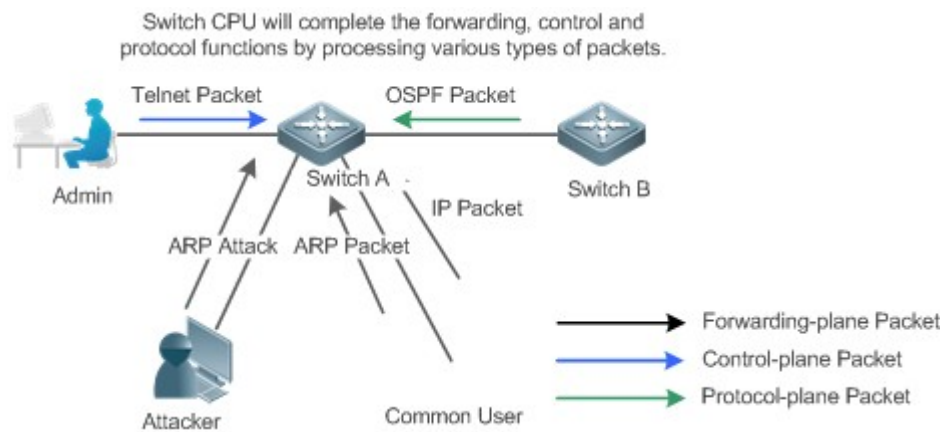
#### Scenario

Network switches at all levels may be attacked by malicious packets, typically ARP attacks.

As shown in Figure 13-46, switch CPUs process three types of packets: forwarding-plane, control-plane and protocol-plane. Forwarding-plane packets are used for routing, including ARP packets and IP route disconnection packets. Control-plane packets are used to manage services on switches, including Telnet packets and HTTP packets. Protocol-plane packets serve for running protocols, including BPDUs and OSPF packets.

When an attacker initiates attacks by using ARP packets, the ARP packets will be sent to the CPU for processing. Since the CPU has limited processing capabilities, the ARP packets may force out other packets (which may be discarded) and consume many CPU resources (for processing ARP attack packets). Consequently, the CPU fails to work normally. In the scenario as shown in Figure 13-46, possible consequences include: common users fail to access the network; administrators fail to manage switches; the OSPF link between switch A and the neighbor B is disconnected and route learning fails.

Figure 13-46 Networking Topology of Switch Services and Attacks



#### Deployment

- By default, CPP classifies ARP packets, Telnet packets, IP route disconnection packets, and OSPF packets into queues of different priorities. In this way, ARP packets will not affect other packets.

- By default, CPP limits the rates of ARP packets and the rates of the priority queue where the ARP packets reside to ensure that the attack packets do not occupy too many CPU resources.
  - Packets in the same priority queue with ARP packets may be affected by ARP attack packets. You can divide the packets and the ARP packets into different priority queues by means of configuration.
  - When ARP attack packets exist, CPP cannot prevent normal ARP packets from being affected. CPP can only differentiate the packet type but cannot distinguish attack packets from normal packets of the same type. In this case, the Network Foundation Protection Policy (NFPP) function can be used to provide higher-granularity attack prevention.
- 
- For description of NFPP configurations, see the *Configuring NFPP*.
- 

## 9.3.2 Preventing CPU Processing Bottlenecks

### Scenario

---

Even though no attacks exist, many packets may need to be sent to the CPU for processing at an instant.

For example, the accesses to the core device of a campus network are counted in ten thousands. The traffic of normal ARP packets may reach dozens of thousands packets per second (PPS). If all packets are sent to the CPU for processing, the CPU resources cannot support the processing, which may cause protocol flapping and abnormal CPU running.

### Deployment

---

- By default, the CPP function limits the rates of ARP packets and the rates of the priority queue where the APR packets reside to control the rate of ARP packets sent to the CPU and ensure that the CPU resource consumption is within a specified range and that the CPU can normally process other protocols.
- By default, the CPP function also limits the rates of other packets at the user level, such as Web authentication and 802.1X authentication packets.

## 9.4 Features

### Basic Concepts

---

#### ↳ QoS, DiffServ

Quality of Service (QoS) is a network security mechanism, a technology used to solve the problems of network delay and congestion.

DiffServ refers to the differentiated service model, which is a typical model implemented by QoS for classifying service streams to provide differentiated services.

#### ↳ Bandwidth, Rate

Bandwidth refers to the maximum allowable data rate, which refers to the rate threshold in this document. Packets whose rates exceed the threshold will be discarded.

The rate indicates an actual data rate. When the rate of packets exceeds the bandwidth, packets out of the limit will be discarded. The rate must be equal to or smaller than the bandwidth.

---

The bandwidth and rate units in this document are packets per second (pps).

## ↳ L2, L3, L4

The structure of packets is hierarchical based on the TCP/IP model.

L2 refers to layer-2 headers, namely, the Ethernet encapsulation part; L3 refers to layer-3 headers, namely, the IP encapsulation part; L4 refers to layer-4 headers, usually, the TCP/UDP encapsulation part.

## ↳ Priority Queue, SP

Packets are cached inside a switch and packets in the output direction are cached in queues. Priority queues are mapped to Strict Priorities (SPs). Queues are not equal but have different priorities.

The SP is a kind of QoS scheduling algorithm. When a higher priority queue has packets, the packets in this queue are scheduled first. Scheduling refers to selecting packets from queues for output and refers to selecting and sending the packets to the CPU in this document.

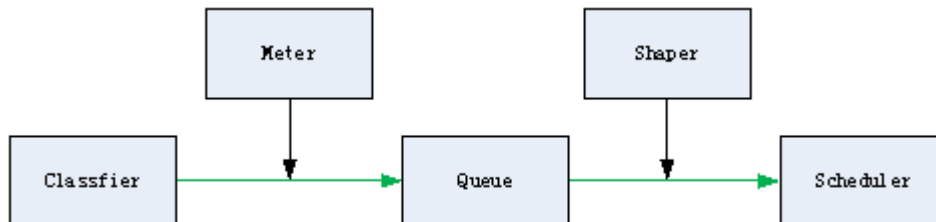
## ↳ CPU interface

Before sending packets to the CPU, a switch will cache the packets. The process of sending packets to the CPU is similar to the process of packet output. The CPU interface is a virtual interface. When packets are sent to the CPU, the packets will be output from this virtual interface. The priority queue and SP mentioned above are based on the CPU interface.

## Overview

CPP protects the CPU by using the standard QoS DiffServ model.

Figure 13-47 CPP Implementation Model



| Feature                    | Description   |
|----------------------------|---|
| <a href="#">Classifier</a> | Classifies packet types and provides assurance for the subsequent implementation of QoS policies. |
| <a href="#">Meter</a>      | Limits rates based on packet types and controls the bandwidth for a specific packet type.         |
| <a href="#">Queue</a>      | Queue packets to be sent to the CPU and select different queues based on packet types.            |
| <a href="#">Scheduler</a>  | Selects and schedules queues to be sent to the CPU.   |
| <a href="#">Shaper</a>     | Performs rate limit and bandwidth control on priority queues and the CPU interface.               |

## 9.4.1 Classifier

### Working Principle

The Classifier classifies all packets to be sent to the CPU based on the L2, L3 and L4 information of the packets. Classifying packets is the basis for implementing QoS policies. In subsequent actions, different policies are implemented based on the classification to provide differentiated services. A switch provides fixed classification. The management function classifies packet types based on the protocols supported by the switch, for example, STP BPDU packets and ICMP packets. Packet types cannot be customized.

## 9.4.2 Meter

### Working Principle

The Meter limits the rates of different packets based on the preset rate thresholds. You can set different rate thresholds for different packet types. When the rate of a packet type exceeds the corresponding threshold, the packets out of the limit will be discarded.

By using the Meter, you can control the rate of a packet type sent to the CPU within a threshold to prevent specific attack packets from exerting large impacts on the CPU resources. This is the level-1 protection of the CPP.

### Related Configuration

- By default, each packet type corresponds to a rate threshold (bandwidth) and Meter policies are implemented based on the rate threshold.
- In application, you can run the **cpu-protect type packet-type bandwidth bandwidth-value** command to set Meter policies for specified packet types.

## 9.4.3 Queue

### Working Principle

Queues are used to classify packets at level 2. You can select the same queue for different packet types; meanwhile, queues cache packets inside switches and provide services for the Scheduler and Shaper.

CPP queues are SP queues. The SPs of the packets are determined based on the time when they are added to a queue. Packets with a larger queue number have a higher priority.

### Related Configuration

- By default, each packet type is mapped to an SP queue.
  - In application, you can run the **cpu-protect type packet-type traffic-class traffic-class-num** command to select SP queues for specific packet types.
-

## 9.4.4 Scheduler

### Working Principle

The Scheduler schedules packets based on SPs of queues. That is, packets in a queue with a higher priority are scheduled first.

Before being scheduled, packets to be sent to the CPU are cached in queues. When being scheduled, the packets are sent to the CPU for processing.

- Only the SP scheduling policy is supported and cannot be modified.

## 9.4.5 Shaper

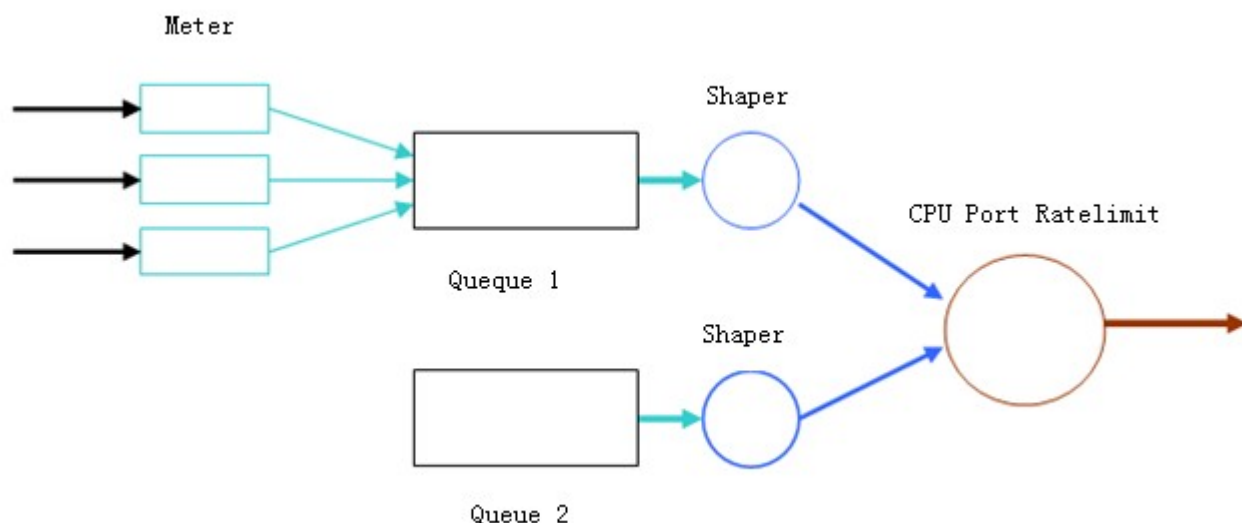
### Working Principle

The Shaper is used to shape packets to be sent to the CPU, that is, when the actual rate of packets is greater than the shaping threshold, the packets must stay in the queue and cannot be scheduled. When packet rates fluctuate, the Shaper ensures that the rates of packets sent to the CPU are smooth (no more than the shaping threshold).

When the Shaper is available, packets in a queue with a lower priority may be scheduled before all packets in a queue with a higher priority are scheduled. If the rate of packets in a queue with certain priority exceeds the shaping threshold, scheduling of the packets in this queue may be stopped temporarily. Therefore, the Shaper can prevent packets in queues with lower priorities from starvation (which means that only packets in queues with higher priorities are scheduled and packets in queues with higher priorities are not scheduled).

Since the Shaper limits the scheduling rates of packets, it actually plays the rate limit function. The Shaper provides level-2 rate limit for priority queues and all packets sent to the CPU (CPU interface). The Shaper and Meter functions provide 3-level rate limit together and provide level-3 protection for the CPU.

Figure 13-48 3-Level Rate Limit of the CPP



### Related Configuration

- ↳ [Configuring the Shaper for priority queues](#)

- By default, each priority queue determines a shaping threshold (bandwidth).
- In application, you can run the **cpu-protect traffic-class** *traffic-class-num* **bandwidth** *bandwidth\_value* command to perform Shaper configuration for a specific priority queue.

#### ↘ **Configuring the Shaper for the CPU Interface**

- By default, the CPU interface determines a shaping threshold (bandwidth).
- Run the **cpu-protect cpu** **bandwidth** *bandwidth\_value* command to perform Shaper configuration for the CPU interface.

## 9.5 Configuration

| Configuration                   | Description and Command  |   |
|---------------------------------|--|---|
| <a href="#">Configuring CPP</a> | <ul style="list-style-type: none"> <li>● (Optional and configured by default) It is used to adjust the configuration parameters of CPP.</li> </ul> |   |
|                                 | <b>cpu-protect type</b> <i>packet-type</i> <b>bandwidth</b>  | Configures the Meter for a packet type. |
|                                 |  |   |
|                                 |  |   |

### 9.5.1 Configuring CPP

#### Configuration Effect

- By configuring the Meter function, you can set the bandwidth and rate limit for a packet type. Packets out of the limit will be directly discarded.
- By configuring the Queue function, you can select a priority queue for a packet type. Packets in a queue with a higher priority will be scheduled first.
- By configuring the Shaper function, you can set the bandwidth and rate limit for a CPU interface and a priority queue. Packets out of the limit will be directly discarded.

#### Notes

- Pay special attention when the bandwidth of a packet type is set to a smaller value, which may affect the normal traffic of the same type. To provide per-user CPP, combine the NFPP function.
- When the Meter and Shaper functions are combined, 3-level protection will be provided. Any level protection fights alone may bring negative effects. For example, if you want to increase the Meter of a packet type, you also need to adjust the Shaper of the corresponding priority queue. Otherwise, the packets of this type may affect other types of packets in the same priority queue.

#### Configuration Steps

##### ↘ **Configuring the Meter for a packet type**

- You can use or modify the default value but cannot disable it.



- You need to modify the configuration in the following cases: when packets of a type are not attackers but are discarded, you need to increase the Meter of this packet type. If attacks of a packet type cause abnormal CPU running, you need to decrease the Meter of this packet type.
- This configuration is available on all switches in a network environment.

#### ↘ **Configuring the priority queue for a packet type**

- You can use or modify the default value but cannot disable it.
- You need to modify the configuration in the following cases: When attacks of a packet type cause abnormality of other packets in the same queue, you can put the packet type in an unused queue. If a packet type cannot be discarded but the packet type is in the same queue with other packet types in use, you can put this packet type in a queue with a higher priority.
- This configuration is available on all switches in a network environment.

#### ↘ **Configuring the Shaper for a priority queue**

- You can use or modify the default value and cannot disable it.
- You need to modify the configuration in the following cases: If the Meter value of a packet type is greater which causes that other packets in the corresponding priority queue do not have sufficient bandwidth, you need to increase the Shaper for this priority queue. If attack packets are put in a priority queue and no other packets are in use, you need to increase the Shaper of this priority queue.
- This configuration is available on all switches in a network environment.

#### ↘ **Configuring the Shaper for the CPU interface**

- You can use or modify the default value and cannot disable it.
- You are not advised to change the Shaper of the CPU interface.
- This configuration is available on all switches in a network environment.

### Verification

- Modify the configurations when the system runs abnormally, and view the system running after the modification to check whether the configurations take effect.
- Check whether the configurations take effect by viewing corresponding configurations and statistic values. For details, see the following commands.

### Related Commands

#### ↘ **Configuring the Meter for a packet type**

|                     |   |
|---------------------|---|
| <b>Command</b>      | <b>cpu-protect type</b> <i>packet-type</i> <b>bandwidth</b> <i>bandwidth_value</i>    |
| <b>Parameter</b>    | <i>packet-type</i> : Specifies a packet type. Packet types are defined.               |
| <b>Description</b>  | <i>bandwidth_value</i> : Sets the bandwidth, in the unit of packets per second (pps). |
| <b>Command Mode</b> | Global configuration mode   |

|             |     |
|-------------|-----|
| Usage Guide | N/A |
|-------------|-----|

## Configuration Example

### ↳ Preventing packet attacks and network flapping by using CPP

|                            |   |
|----------------------------|---|
| <b>Scenario</b>            | <ul style="list-style-type: none"> <li>ARP, IP, OSPF, dot1x, VRRP, Telnet and ICMP streams are available in the system. In the current configurations, ARP and 802.1X are in priority queue 2; IP, ICMP and Telnet streams are in priority queue 4; OSPF streams are in priority queue 3; VRRP streams are in priority queue 6. The Meter for each packet type is 10,000 pps; the shaper for each priority queue is 20,000 pps; the Shaper for the CPU interface is 100,000 pps.</li> <li>ARP attacks and IP scanning attacks exist in the system, which causes abnormal running of the system, authentication failure, Ping failure, management failure, and OSPF flapping.</li> </ul> |
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>limit the bandwidth for ARP packets</li> <li></li> </ul>   |
|                            | <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# cpu-protect type arp bandwidth 5000 Orion Alpha A28X(config)# end</pre>   |
| <b>Verification</b>        | Run the <b>show cpu-protect</b> command to view the configuration and statistics.   |

## 9.6 Monitoring

### Clearing

| Description                | Command   |
|----------------------------|---|
| Clears the CPP statistics. | <b>clear cpu-protect counters</b> [ <b>device</b> <i>device_num</i> ] [ <b>slot</b> <i>slot_num</i> ] |
|                            |   |

### Displaying

| Description  | Command                 |
|--|-------------------------|
|  |                         |
| Displays all configurations and statistics on the master device. | <b>show cpu-protect</b> |
|  |                         |

### Debugging

N/A

- The preceding monitoring commands are available on both chassis and cassette devices in either the standalone mode or the VSU mode.
- If the **device** and **slot** values are not specified, the **clear** command is used to clear the statistics of all nodes in the system and the **show** command is used to display the configurations on the master device.

- 
- In the standalone mode, the parameter **device** is unavailable. For chassis devices, the parameter **slot** is used to specify a line card; for cassette devices, **slot** is unavailable.
  - In the VSU mode, the parameter **device** indicates a chassis or cassette device. If the **device** value is not specified, it indicates the master chassis or the master device. For chassis devices, if the **device** value is specified the **slot** value must also be specified to identify a line card in a chassis; for cassette devices, **slot** is unavailable.
-

# 10 Configuring DHCP Snooping

## 10.1 Overview

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record and monitor users' IP addresses and filter out illegal DHCP packets, including client request packets and server response packets. The legal user database generated from DHCP Snooping records may serve security applications like IP Source Guard.

### Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

## 10.2 Applications

| Application  | Description  |
|--|--|
| <a href="#">Guarding against DHCP service spoofing</a> | In a network with multiple DHCP servers, DHCP clients are allowed to obtain network configurations only from legal DHCP servers. |
| <a href="#">Guarding against DHCP packet flooding</a>  | Malicious network users may frequently send DHCP request packets.  |
| <a href="#">Guarding against forged DHCP packets</a>   | Malicious network users may send forged DHCP request packets, for example, DHCP-RELEASE packets.                                 |
| <a href="#">Guarding against IP/MAC spoofing</a>       | Malicious network users may send forged IP packets, for example, tampered source address fields of packets.                      |
| <a href="#">Preventing Lease of IP Addresses</a>       | Network users may lease IP addresses rather than obtaining them from a DHCP server.  |
| <a href="#">Detecting ARP attack</a>                   | Malicious users forge ARP response packets to intercept packets during normal users' communication.                              |

### 10.2.1 Guarding Against DHCP Service Spoofing

#### Scenario

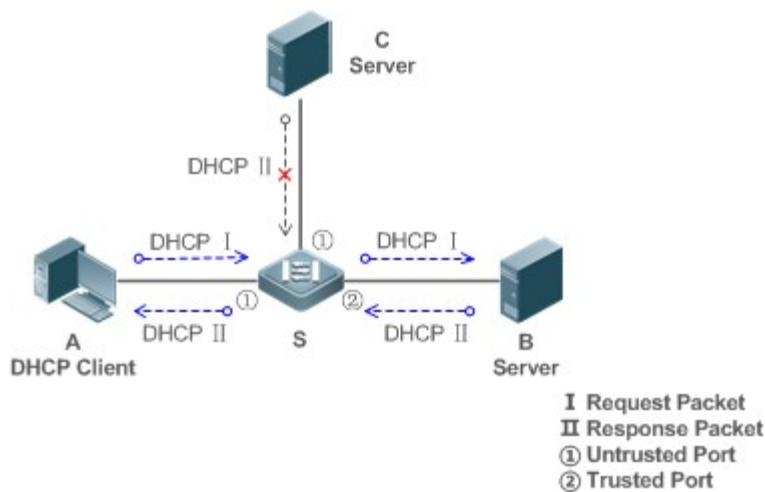
Multiple DHCP servers may exist in a network. It is essential to ensure that user PCs obtain network configurations only from the DHCP servers within a controlled area.

Take the following figure as an example. The DHCP client can only communicate with trusted DHCP servers.

- Request packets from the DHCP client can be transmitted only to trusted DHCP servers.
- Only the response packets from trusted DHCP servers can be transmitted to the client.

Figure 14-9

---



|                 |  |
|-----------------|--|
| <b>Remarks:</b> | <p>S is an access device.</p> <p>A is a user PC.</p> <p>B is a DHCP server within the controlled area.</p> <p>C is a DHCP server out of the controlled area.</p> |
|-----------------|--|

## Deployment

- Enable DHCP Snooping on S to realize DHCP packet monitoring.
- Set the port on S connecting to B as trusted to transfer response packets.
- Set the rest of ports on S as untrusted to filter response packets.

## 10.2.2 Guarding Against DHCP Packet Flooding

### Scenario

Potential malicious DHCP clients in a network may send high-rate DHCP packets. As a result, legitimate users cannot obtain IP addresses, and access devices are highly loaded or even break down. It is necessary to take actions to ensure network stability.

With the DHCP Snooping rate limit function for DHCP packets, a DHCP client can only send DHCP request packets at a rate below the limit.

- The request packets from a DHCP client are sent at a rate below the limit.
- Packets sent at rates beyond the limit will be discarded.
- Enable DHCP Snooping correlation with ARP, and delete the non-existing entries.

### Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Limit the rates of DHCP packets from the untrusted ports.
- Enable DHCP Snooping correlation with ARP, and detect whether the user is online.

## 10.2.3 Guarding Against Forged DHCP Packets

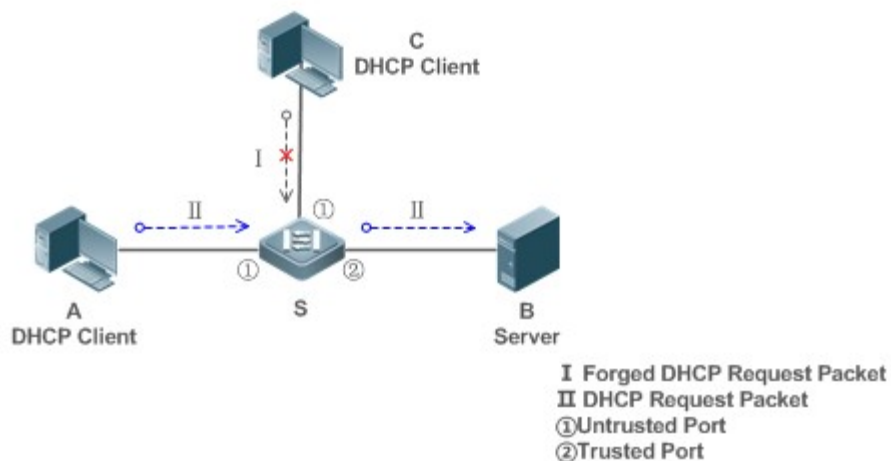
### Scenario

Potential malicious clients in a network may forge DHCP request packets, consuming applicable IP addresses from the servers and probably preempting legal users' IP addresses. Therefore, it is necessary to filter out illegal DHCP packets.

For example, as shown in the figure below, the DHCP request packets sent from DHCP clients will be checked.

- The source MAC address fields of the request packets from DHCP clients must match the **chaddr** fields of DHCP packets.
- The Release packets and Decline packets from clients must match the entries in the DHCP Snooping binding database.

Figure 14-10



|                 |   |
|-----------------|---|
| <b>Remarks:</b> | S is an access device.<br>A and C are user PCs.<br>B is a DHCP server within the controlled area. |
|-----------------|---|

### Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set the port on S connecting to B as trusted to transfer response packets.
- Set the rest of ports on S as untrusted to filter response packets.
- Enable DHCP Snooping Source MAC Verification on untrusted ports of S to filter out illegal packets.

## 10.2.4 Guarding Against IP/MAC Spoofing

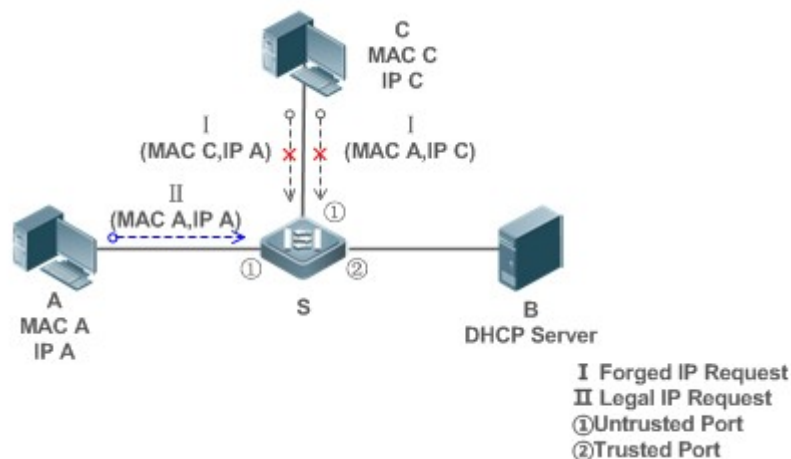
### Scenario

Check IP packets from untrusted ports to filter out forged IP packets based on IP or IP-MAC fields.

For example, in the following figure, the IP packets sent by DHCP clients are validated.

- The source IP address fields of IP packets must match the IP addresses assigned by DHCP.
- The source MAC address fields of layer-2 packets must match the **chaddr** fields in DHCP request packets from clients.

Figure 14-11



|                 |   |
|-----------------|---|
| <b>Remarks:</b> | S is an access device.<br>A and C are user PCs.<br>B is a DHCP server within the controlled area. |
|-----------------|---|

### Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on the S as DHCP Snooping untrusted.
- Enable IP Source Guard on S to filter IP packets.
- Enable IP Source Guard in IP-MAC based mode to check the source MAC and IP address fields of IP packets.

## 10.2.5 Preventing Lease of IP Addresses

### Scenario

Validate the source addresses of IP packets from untrusted ports compared with DHCP-assigned addresses.

If the source addresses, connected ports, and layer-2 source MAC addresses of ports in IP packets do not match the assignments of the DHCP server, such packets will be discarded.

The networking topology scenario is the same as that shown in the previous figure.

## Deployment

- The same as that in the section "Guarding Against IP/MAC Spoofing".

## 10.2.6 Detecting ARP Attacks

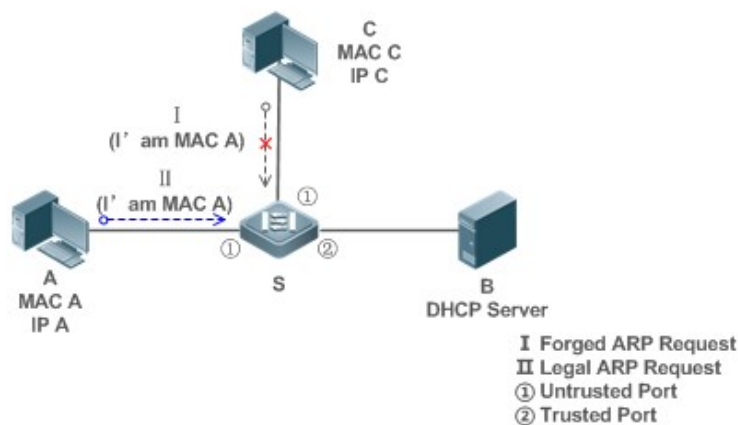
### Scenario

Check the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

For example, in the following figure, the ARP packets sent from DHCP clients will be checked.

- The ports receiving ARP packets, the layer-2 MAC addresses, and the source MAC addresses of ARP packets senders shall be consistent with the DHCP Snooping histories.

Figure 14-12



|                 |   |
|-----------------|---|
| <b>Remarks:</b> | S is an access device.<br>A and C are user PCs.<br>B is a DHCP server within the controlled area. |
|-----------------|---|

## Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on the S as untrusted.
- Enable IP Source Guard and ARP Check on all the untrusted ports on S to realize ARP packet filtering.
- All the above security control functions are only effective to DHCP Snooping untrusted ports.



## 10.3 Features

### Basic Concepts

---

#### ↳ DHCP Request Packets

Request packets are sent from a DHCP client to a DHCP server, including DHCP-DISCOVER packets, DHCP-REQUEST packets, DHCP-DECLINE packets, DHCP-RELEASE packets and DHCP-INFORM packets.

#### ↳ DHCP Response Packets

Response packets are sent from a DHCP server to a DHCP client, including DHCP-OFFER packets, DHCP-ACK packets and DHCP-NAK packets.

#### ↳ DHCP Snooping Trusted Ports

IP address request interaction is complete via broadcast. Therefore, illegal DHCP services will influence normal clients' acquisition of IP addresses and lead to service spoofing and stealing. To prevent illegal DHCP services, DHCP Snooping ports are divided into two types: trusted ports and untrusted ports. The access devices only transmit DHCP response packets received on trusted ports, while such packets from untrusted ports are discarded. In this way, we may configure the ports connected to a legal DHCP Server as trusted and the other ports as untrusted to shield illegal DHCP Servers.

On switches, all switching ports or layer-2 aggregate ports are defaulted as untrusted, while trusted ports can be specified.

#### ↳ DHCP Snooping Packet Suppression

To shield all the DHCP packets on a specific client, we can enable DHCP Snooping packet suppression on its untrusted ports.

#### ↳ VLAN-based DHCP Snooping

DHCP Snooping can work on a VLAN basis. By default, when DHCP Snooping is enabled, it is effective to all the VLANs of the current client. Specify VLANs help control the effective range of DHCP Snooping flexibly.

#### ↳ DHCP Snooping Binding Database

In a DHCP network, clients may set static IP addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legal clients with IP addresses assigned by the DHCP server may fail to use the network normally due to address conflict. Through snooping packets between clients and servers, DHCP Snooping summarizes the user entries including IP addresses, MAC address, VLAN ID (VID), ports and lease time to build the DHCP Snooping binding database. Combined with ARP detection and ARP check, DHCP Snooping controls the reliable assignment of IP addresses for legal clients.

#### ↳ DHCP Snooping Rate Limit

DHCP Snooping rate limit function can be configured through the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see the *Configuring NFPP*.

#### ↳ DHCP Option82

DHCP Option82, an option for DHCP packets, is also called DHCP Relay Agent Information Option. As the option number is 82, it is known as Option82. Option82 is developed to enhance the security of DHCP servers and improve the strategies of IP address assignment. The option is often configured for the DHCP relay services of a network access device like DHCP Relay and DHCP Snooping. This option is transparent to DHCP clients, and DHCP relay components realize the addition and deduction of the option.

### ↘ Illegal DHCP Packets

Through DHCP Snooping, validation is performed on the DHCP packets passing through a client. Illegal DHCP packets are discarded, user information is recorded into the DHCP Snooping binding database for further applications (for example, ARP detection). The following types of packets are considered illegal DHCP packets.

- The DHCP response packets received on untrusted ports, including DHCP-ACK, DHCP-NACK and DHCP-OFFER packets
- The DHCP request packets carrying gateway information **giaddr**, which are received on untrusted ports
- When MAC verification is enabled, packets with source MAC addresses different with the value of the **chaddr** field in DHCP packets
- DHCP-RELEASE packets with the entry in the DHCP Snooping binding database Snooping while with untrusted ports inconsistent with settings in this binding database
- DHCP packets in wrong formats, or incomplete

### Overview

| Feature   | Description  |
|---|--|
| <a href="#">Filtering DHCP packets</a>                      | Perform legality check on DHCP packets and discard illegal packets (see the previous section for the introduction of illegal packets). Transfer requests packets received on trusted ports only. |
| <a href="#">Building the DHCP Snooping binding database</a> | Snoop the interaction between DHCP clients and the server, and generate the DHCP Snooping binding database to provide basis for other filtering modules.   |

## 10.3.1 Filtering DHCP Packets

Perform validation on DHCP packets from untrusted ports. Filter out the illegal packets as introduced in the previous section "Basic Concepts".

### Working Principle

During snooping, check the receiving ports and the packet fields of packets to realize packet filtering, and modify the destination ports of packets to realize control of transmit range of the packets.

### ↘ Checking Ports

In receipt of DHCP packets, a client first judges whether the packet receiving ports are DHCP Snooping trusted ports. If yes, legality check and binding entry addition are skipped, and packets are transferred directly. For not, both the check and addition are needed.

### ↘ Checking Packet Encapsulation and Length

A client checks whether packets are UDP packets and whether the destination port is 67 or 68. Check whether the packet length match the length field defined in protocols.

### ↘ Checking Packet Fields and Types

According to the types of illegal packet introduced in the section "Basic Concepts", check the fields **giaddr** and **chaddr** in packets and then check whether the restrictive conditions for the type of the packet are met.

## Related Configuration

### ↘ Enabling Global DHCP Snooping

By default, DHCP Snooping is disabled.

It can be enabled on a device using the **ip dhcp snooping** command.

Global DHCP Snooping must be enabled before VLAN-based DHCP Snooping is applied.

### ↘ Configuring VLAN-based DHCP Snooping

By default, when global DHCP Snooping is effective, DHCP Snooping is effective to all VLANs.

Use the [ **no** ] **ip dhcp snooping vlan** command to enable DHCP Snooping on specified VLANs or delete VLANs from the specified VLANs. The value range of the command parameter is the actual range of VLAN numbers.

### ↘ Configuring DHCP Snooping Source MAC Verification

By default, the layer-2 MAC addresses of packets and the **chaddr** fields of DHCP packets are not verified.

When the **ip dhcp snooping verify mac-address** command is used, the source MAC addresses and the **chaddr** fields of the DHCP request packets sent from untrusted ports are verified. The DHCP request packets with different MAC addresses will be discarded.

## 10.3.2 Building the Binding Database

DHCP Snooping detects the interactive packets between DHCP clients and the DHCP server, and generate entries of the DHCP Snooping binding database according to the information of legal DHCP packets. All these legal entries are provided to other security modules of a client as the basis of filtering packets from network.

## Working Principle

During snooping, the binding database is updated timely based on the types of DHCP packets.

### ↘ Generating Binding Entries

When a DHCP-ACK packet on a trusted port is snooped, the client's IP address, MAC address, and lease time field are extracted together with the port ID (a wired interface index) and VLAN ID. Then, a binding entry of it is generated.

### ↘ Deleting Binding Entries

When the recorded lease time of a binding entry is due, it will be deleted if a legal DHCP-RELEASE/DHCP-DECLINE packet sent by the client or a DHCP-NCK packet received on a trusted port is snooped, or the **clear** command is used.

---

## Related Configuration

No configuration is needed except enabling DHCP Snooping.

## 10.4 Configuration

| Configuration  | Description and Command   |   |
|--|---|---|
| <a href="#">Configuring basic functions of DHCP Snooping</a> | <ul style="list-style-type: none"> <li>(Mandatory) It is used to enable DHCP Snooping.</li> </ul>                           |   |
|  | <b>ip dhcp snooping</b>   | Enables DHCP Snooping.  |
|  | <b>ip dhcp snooping suppression</b>   | Enables DHCP Snooping packet suppression.   |
|  | <b>ip dhcp snooping vlan</b>  | Enables VLAN-based DHCP Snooping.   |
|  | <b>ip dhcp snooping verify mac-address</b>  | Configures DHCP Snooping source MAC verification.   |
|  | <b>ip dhcp snooping database write-delay</b>  | Writes the DHCP Snooping binding database to Flash periodically.                            |
|  | <b>ip dhcp snooping database write-to-flash</b>   | Writes the DHCP Snooping binding database to Flash manually.                                |
|  | <b>renew ip dhcp snooping database</b>  | Imports Flash storage to the DHCP Snooping Binding database.                                |
|  | <b>ip dhcp snooping trust</b>   | Configures DHCP Snooping trusted ports.   |
|  | <b>ip dhcp snooping bootp</b>   | Enables BOOTP support.  |
|  | <b>ip dhcp snooping check-giaddr</b>  | Enables DHCP Snooping to support the function of processing Relay requests.                 |
| <b>ip dhcp snooping loose-forward</b>                        | Enables loose forwarding.   |   |
| <a href="#">Configuring Option82</a>                         | <ul style="list-style-type: none"> <li>(Optional) It is used to optimize the address assignment by DHCP servers.</li> </ul> |   |
|  | <b>ip dhcp snooping Information option</b>  | Adds Option82 functions to DHCP request packets.  |
|  | <b>ip dhcp snooping information option format remote-id</b>   | Configures the sub-option <b>remote-id</b> of Option82 as a user-defined character string.  |
|  | <b>ip dhcp snooping vlan information option format-type circuit-id string</b>   | Configures the sub-option <b>circuit-id</b> of Option82 as a user-defined character string. |
| <b>ip dhcp snooping information option strategy</b>          | Configures the strategy of Option82.  |   |

## 10.4.1 Configuring Basic Features

### Configuration Effect

---

- Enable DHCP Snooping.
- Generate the DHCP Snooping binding database.
- Control the transmit range of DHCP packets.
- Filter out illegal DHCP packets.

### Notes

---

- The ports on clients connecting a trusted DHCP server must be configured as trusted.
- DHCP Snooping is effective on the wired switching ports, layer-2 aggregate ports, and layer-2 encapsulation sub-interfaces. The configuration can be implemented in interface configuration mode.
- DHCP Snooping and DHCP Relay are mutually exclusive in VRF scenarios.

### Configuration Steps

---

#### ↳ Enabling Global DHCP Snooping

- Mandatory.
- Unless otherwise noted, the feature should be configured on access devices.

#### ↳ Enabling or Disabling VLAN-based DHCP Snooping

- DHCP Snooping can be disabled if not necessary for some VLANs.
- Unless otherwise noted, the feature should be configured on access devices.

#### ↳ Configuring DHCP Snooping Trusted Ports

- Mandatory.
- Configure the ports connecting a trusted DHCP server as trusted.

#### ↳ Enabling DHCP Snooping Source MAC Validation

- This configuration is required if the **chaddr** fields of DHCP request packets match the layer-2 source MAC addresses of data packets.
- Unless otherwise noted, the feature should be enabled on all the untrusted ports of access devices.

#### ↳ Writing the DHCP Snooping Binding Database to Flash Periodically

- Enable this feature to timely save the DHCP Snooping binding database information in case that client reboot.
- Unless otherwise noted, the feature should be configured on access devices.

#### ↳ Enabling BOOTP Support

- Optional
-

- Unless otherwise noted, the feature should be configured on access devices.

#### ↳ Enabling DHCP Snooping to Process Relay Requests

- Optional.
- Unless otherwise noted, the feature should be enabled on access devices.

#### ↳ Enabling Loose Forwarding

- Optional.
- Unless otherwise noted, the feature is disabled.

### Verification

Configure a client to obtain network configurations through the DHCP protocol.

- Check whether the DHCP Snooping Binding database is generated with entries on the client.

### Related Commands

#### ↳ Enabling or Disabling DHCP Snooping

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <code>[ no ] ip dhcp snooping</code>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | After global DHCP Snooping is enabled, you can check DHCP Snooping using the <b>show ip dhcp snooping</b> command. |

#### ↳ Configuring VLAN-based DHCP Snooping

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <code>[ no ] ip dhcp snooping vlan { <i>vlan-rng</i>   { <i>vlan-min</i> [ <i>vlan-max</i> ] } }</code>                                       |
| <b>Parameter Description</b> | <i>vlan-rng</i> : Indicates the range of VLANs<br><i>vlan-min</i> : The minimum VLAN ID<br><i>vlan-max</i> : The maximum VLAN ID              |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Use this command to enable or disable DHCP Snooping on specified VLANs. This feature is available only after global DHCP Snooping is enabled. |

#### ↳ Configuring DHCP Snooping Packet Suppression

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <code>[ no ] ip dhcp snooping suppression</code> |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Interface configuration mode                     |

|                    |   |
|--------------------|---|
| <b>Usage Guide</b> | Use this command to reject all DHCP request packets at the port, that is, to forbid all users under the port to apply for addresses via DHCP. |
|--------------------|---|

### ↳ Configuring DHCP Snooping Source MAC Verification

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>[ no ] ip dhcp snooping verify mac-address</b>   |
| <b>Parameter Description</b> | N/A   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Through the source MAC address verification, the MAC addresses in link headers and the CLIENT MAC fields in the request packets sent by a DHCP CLIENT are checked for consistence. When the source MAC address verification fails, packets will be discarded. |

### ↳ Writing DHCP Snooping Database to Flash Periodically

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>[ no ] ip dhcp snooping database write-delay [ time ]</b>  |
| <b>Parameter Description</b> | <i>time</i> : Indicates the interval between two times of writing the DHCP Snooping database to the Flash.  |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Use this command to write the DHCP Snooping database to FLASH document. This can avoid binding information loss which requires re-obtaining IP addresses to resume communication after the device restarts. |

### ↳ Writing the DHCP Snooping Database to Flash Manually

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>ip dhcp snooping database write-to-flash</b>   |
| <b>Parameter Description</b> | N/A   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | Use this command to write the dynamic user information in the DHCP Snooping database in FLASH documents in real time.<br><br>If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored from FLASH documents because of version differences between FLASH documents. |

### ↳ Importing Backup File Storage to the DHCP Snooping Binding Database

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>renew ip dhcp snooping database</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Privileged configuration mode  |
| <b>Usage Guide</b>           | Use this command to import the information from backup file to the DHCP Snooping binding database. |

---

### ↘ Configuring DHCP Snooping Trusted Ports

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>[ no ] ip dhcp snooping trust</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Interface configuration mode   |
| <b>Usage Guide</b>           | Use this command to configure a port connected to a legal DHCP server as a trusted port. The DHCP response packets received by trusted ports are transferred, while those received by untrusted ports are discarded. |

### ↘ Enabling or Disabling BOOTP Support

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>[ no ] ip dhcp snooping bootp</b>            |
| <b>Parameter Description</b> | N/A   |
| <b>Command Mode</b>          | Global configuration mode                       |
| <b>Usage Guide</b>           | Use this command to support the BOOTP protocol. |

### ↘ Enabling DHCP Snooping to Process Relay Requests

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>[ no ] ip dhcp snooping check-giaddr</b>  |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet.<br>After the feature is enabled, the <b>ip dhcp snooping verify mac-address</b> command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses. |

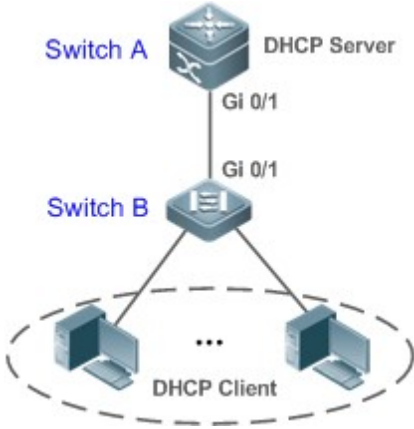
### ↘ Enabling DHCP Snooping Loose Forwarding

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>ip dhcp snooping loose-forward</b>   |
| <b>Parameter Description</b> | N/A   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | After this feature is enabled, when the capacity of DHCP Snooping binding entries is reached, DHCP packets of new users are forwarded and obtain addresses, but DHCP Snooping does not record binding entries of new users. |



## Configuration Example

### DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

|                                 |   |
|---------------------------------|---|
| <b>Scenario</b><br>Figure 14-13 |    |
| <b>Configuration Steps</b>      | <ul style="list-style-type: none"><li>● Enable DHCP Snooping on an access device (Switch B in this case).</li><li>● Configure the uplink port (port Gi 0/1 in this case) as a trusted port.</li></ul>   |
| <b>B</b>                        | <pre>B#configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)#ip dhcp snooping B(config)#interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust B(config-if-GigabitEthernet 0/1)#end</pre>  |
| <b>Verification</b>             | <p>Check the configuration on Switch B.</p> <ul style="list-style-type: none"><li>● Check whether DHCP Snooping is enabled, and whether the configured DHCP Snooping trusted port is uplink.</li><li>● Check the DHCP Snooping configuration on Switch B, and especially whether the trusted port is correct.</li></ul> |
| <b>B</b>                        | <pre>B#show running-config ! ip dhcp snooping ! interface GigabitEthernet 0/1 B#show ip dhcp snooping Switch DHCP Snooping status           : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds</pre>  |

```

DHCP Snooping option 82 status      : DISABLE
DHCP Snooping Support BOOTP bind status  : DISABLE
Interface      Trusted      Rate limit (pps)
-----
GigabitEthernet 0/1      YES      unlimited
B#show ip dhcp snooping binding
Total number of bindings: 1
MacAddress      IpAddress      Lease(sec)  Type      VLAN  Interface
-----
0013.2049.9014  172.16.1.2  86207      DHCP-Snooping 1  GigabitEthernet 0/11

```

### Common Errors

- The uplink port is not configured as a DHCP trusted port.
- Another access security option is already configured for the uplink port, so that a DHCP trusted port cannot be configured.

## 10.4.2 Configuring Option82

### Configuration Effect

- Enable a DHCP server to obtain more information and assign addresses better.
- The Option82 function is client-oblivious.

### Notes

- The Option82 functions for DHCP Snooping and DHCP Relay are mutually exclusive.

### Configuration Steps

- To realize optimization of address allocation, implement the configuration.
- Unless otherwise noted, enable this function on access devices with DHCP Snooping enabled.

### Verification

Check whether the DHCP Snooping configuration options are configured successfully.

### Related Commands

#### Adding Option82 to DHCP Request Packets

|                    |   |
|--------------------|---|
| <b>Command</b>     | [ no ] ip dhcp snooping information option [ standard-format   dot1x-format ] |
| <b>Parameter</b>   | <b>standard-format:</b> Indicates a standard format of the Option82 options   |
| <b>Description</b> | <b>dot1x-format:</b> Indicates a dot1x format of the Option82 options         |

|                     |  |
|---------------------|--|
| <b>Command Mode</b> | Global configuration mode  |
| <b>Usage Guide</b>  | Use this command to add Option82 to DHCP request packets so that a DHCP server assigns addresses according to such information.<br><br>When dot1x-format is used, if DHCP Relay is configured on the local device and the uplink port connected to the DHCP Server is an SVI port, DHCP Snooping needs to be disabled in the VLAN to which the SVI port belongs. |

#### ↘ Configuring Sub-option remote-id of Option82 as User-defined Character String

|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] ip dhcp snooping information option format remote-id { string ASCII-string   hostname }  |
| <b>Parameter Description</b> | <b>string ASCII-string:</b> Indicates the content of the extensible format, the Option82 option<br><b>remote-id,</b> is a user-defined character string<br><b>hostname:</b> Indicates the content of the extensible format, the Option82 option <b>remote-id,</b> is a host name. |
| <b>Configuration mode</b>    | Global configuration mode   |
| <b>Usage Guide</b>           | Use this command to configure the sub-option <b>remote-id</b> of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.   |

#### ↘ Configuring Sub-Option circuit-id of Option82 as User-defined Character String

|                              |  |
|------------------------------|--|
| <b>Command</b>               | [ no ] ip dhcp snooping vlan <i>vlan-id</i> information option format-type circuit-id string <i>ascii-string</i>   |
| <b>Parameter Description</b> | <b>vlan-id:</b> Indicates the VLAN where a DHCP request packet is<br><b>ascii-string:</b> Indicates the user-defined string  |
| <b>Configuration mode</b>    | Interface configuration mode   |
| <b>Usage Guide</b>           | Use this command to configure the sub-option <b>circuit-id</b> of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information. |

#### ↘ Configuring the Strategy of Option82

|                              |   |
|------------------------------|---|
| <b>Command</b>               | ip dhcp snooping information option strategy {keep   drop   replace}  |
| <b>Parameter Description</b> | <b>keep:</b> Indicates reception of request packets with Option82. Option82 is kept and the packets are forwarded.<br><b>drop:</b> Indicates reception of request packets with Option82. The packets are dropped.<br><b>replace:</b> Indicates reception of request packets with Option82. Option82 of the packets are replaced with Option82 configured latest. The packets are forwarded. |
| <b>Configuration mode</b>    | Global configuration mode   |
| <b>Usage Guide</b>           | This command only works for request packets with Option82.<br>If the strategy is keep or drop, there is no need to configure sub-option <b>circuit-id</b> of the Option82.<br>If the strategy is replace, sub-option <b>circuit-id</b> of the Option82 needs configuring.   |

In terms of request packets without Option82, configured sub-option **circuit-id** of the Option82 is added.

## Configuration Example

### ↳ Configuring Option82 to DHCP Request Packets

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"><li>● Configuring basic functions of DHCP Snooping.</li><li>● Configuring Option82.</li></ul>  |
| <b>B</b>                   | <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ip dhcp snooping information option Orion Alpha A28X(config)# end</pre>  |
| <b>Verification</b>        | Check the DHCP Snooping configuration.   |
| <b>B</b>                   | <pre>B#show ip dhcp snooping Switch DHCP Snooping status           : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time  : 0 seconds DHCP Snooping option 82 status         : ENABLE DHCP Snooping Support bootp bind status  : DISABLE Interface      Trusted      Rate limit (pps) ----- GigabitEthernet 0/1      YES      unlimited</pre> |

## Common Errors

- N/A

## 10.5 Monitoring

### Clearing

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

| Description  | Command  |
|--|--|
| Clears dynamic user information of DHCP Snooping database. | <b>clear ip dhcp snooping binding [ ip ] [ mac ] [ vlan vlan-id ] [ interface interface-id ]</b> |

### Displaying

| Description                           | Command                      |
|---------------------------------------|------------------------------|
| Displays DHCP Snooping configuration. | <b>show ip dhcp snooping</b> |

|  |                                      |
|--|--------------------------------------|
| Displays the DHCP Snooping binding database. | <b>show ip dhcp snooping binding</b> |
|--|--------------------------------------|

## Debugging

- System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

| Description                                 | Command  |
|---|--|
| Debugs DHCP Snooping events.                | <b>debug snooping ipv4 event</b>                       |
| Disables debugging DHCP Snooping events.    | <b>no debug snooping ipv4 event</b>                    |
| Debugs DHCP Snooping packets.               | <b>debug snooping ipv4 packet</b>                      |
| Disables debugging DHCP Snooping packets.   | <b>no debug snooping ipv4 packet</b>                   |
| Enables debugging MAC-based DHCP Snooping.  | <b>debug snooping ipv4 mac-address <i>H.H.H</i></b>    |
| Disables debugging MAC-based DHCP Snooping. | <b>no debug snooping ipv4 mac-address <i>H.H.H</i></b> |
| Enables debugging all DHCP Snooping         | <b>debug snooping ipv4 all</b>                         |
| Disables debugging all DHCP Snooping        | <b>no debug snooping ipv4 all</b>                      |

# 11 Configuring DHCPv6 Snooping

## 11.1 Overview

DHCPv6 Snooping: Dynamic Host Configuration Protocol version 6 (DHCPv6) snooping enables recording and monitoring of IPv6 address usage by snooping DHCPv6 packets exchanged between the client and the server, and filters illegal DHCPv6 packets, including request packets from the client and response packets from the server. The user data entries generated by DHCPv6 snooping recording can serve security applications such as IPv6 Source Guard.

### Protocols and Standards

- RFC3315 Dynamic Host Configuration Protocol For IPv6
- RFC5007 DHCPv6 Leasequery
- RFC5460 DHCPv6 Bulk Leasequery

## 11.2 Applications

| Application   | Description   |
|---|---|
| <a href="#">Prevention of DHCPv6 Spoofing</a>                 | There is more than one DHCPv6 server on the network, and DHCPv6 clients can obtain network configuration parameters only from legal DHCPv6 servers. |
| <a href="#">Prevention of Forged DHCPv6 Packet Attacks</a>    | Malicious users on the network frequently send DHCPv6 request packets.  |
| <a href="#">Prevention of Forged DHCPv6 Packet Attacks</a>    | Malicious users on the network send forged DHCPv6 request packets such as DHCPv6 release packets.   |
| <a href="#">Prevention of IPv6/MAC Spoofing</a>               | Malicious users on the network send forged IPv6 request packets that temper the source address fields.  |
| <a href="#">Prevention of Unauthorized IPv6 Configuration</a> | Users do not obtain IPv6 addresses from the DHCPv6 server as required and configure IPv6 addresses without authorization.                           |

### 11.2.1 Prevention of DHCPv6 Spoofing

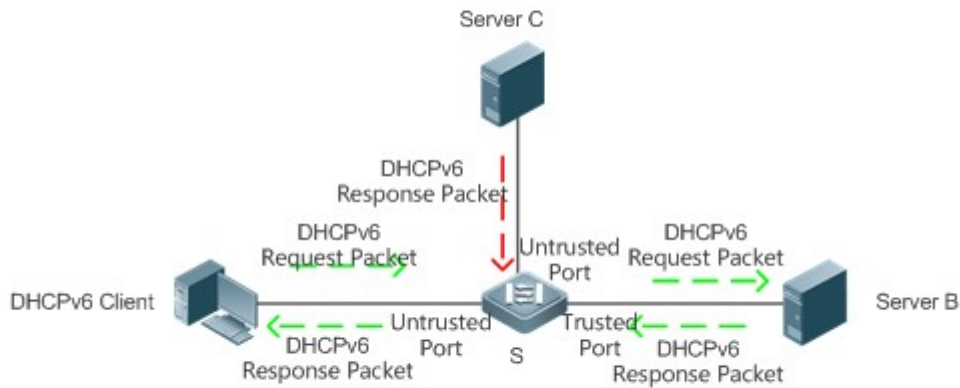
#### Scenario

There may exist more than one DHCPv6 server on the network, and it is necessary to ensure that user PCs obtain network configuration parameters only from the controlled DHCPv6 servers.

As shown in the following figure, the DHCPv6 client only communicates with trusted DHCPv6 servers.

- The request packets from the DHCPv6 client are transmitted only to a trusted DHCPv6 server.
  - Only the response packets from the trusted DHCPv6 server can be transmitted to the client.
-

Figure 15-49



|                |  |
|----------------|--|
| <b>Remarks</b> | S is an access device.<br>A is a user PC.<br>B is a controlled DHCPv6 server.<br>C is an uncontrolled DHCPv6 server. |
|----------------|--|

### Deployment

- Enable DHCPv6 snooping on the access device S for DHCPv6 packet monitoring.
- Set the port connecting the access device S to the DHCPv6 server B as a DHCPv6 trusted port to forward response packets.
- Set the other ports of the access device S as DHCPv6 untrusted ports to filter response packets.

## 11.2.2 Prevention of Forged DHCPv6 Packet Attacks

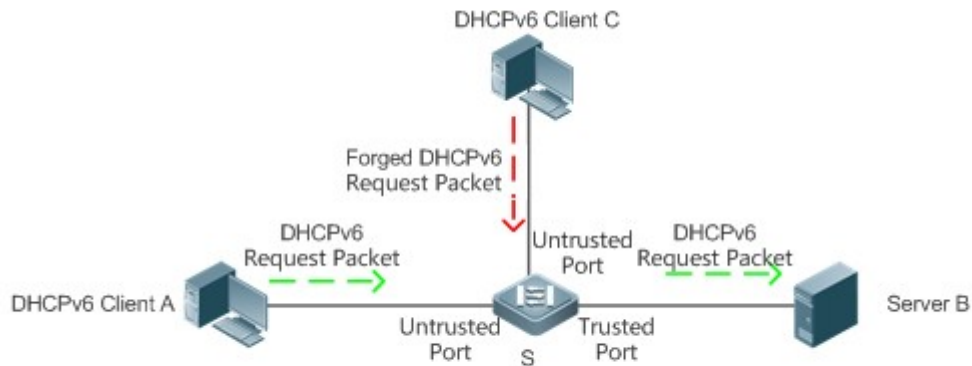
### Scenario

There may exist malicious users on the network who forge DHCPv6 request packets. The packets not only consume available IPv6 addresses of the server but may also snatch IPv6 addresses from legal users. Therefore, such packets on the network must be filtered.

As shown in the following figure, the DHCPv6 request packets sent by the DHCPv6 client will be checked.

- Release packets and decline packets from the client must match those recorded in the internal snooping database.

Figure 15-50



|                |   |
|----------------|---|
| <b>Remarks</b> | S is an access device.<br>A and C are user PCs.<br>B is a controlled DHCPv6 server. |
|----------------|---|

### Deployment

- Enable DHCPv6 snooping on the access device S for DHCPv6 monitoring.
- Set the port connecting the access device S to the DHCPv6 server as a DHCPv6 trusted port to forward response packets.
- Set the other ports of the access device S as DHCPv6 untrusted ports to filter DHCPv6 packets.

## 11.2.3 Prevention of IPv6/MAC Spoofing

### Scenario

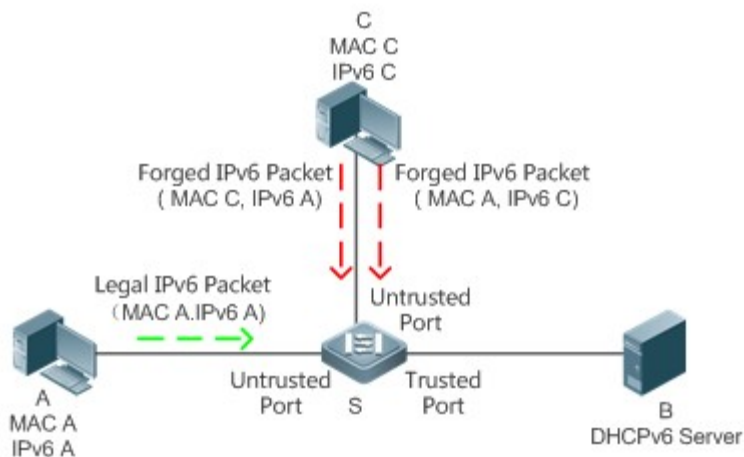
When checking IPv6 packets from the untrusted port, you may check IP address fields only or IP+MAC fields to filter forged IPv6 packets.

As shown in the following figure, IPv6 packets sent from the DHCPv6 client will be checked.

- The source address fields of IPv6 packets must match IPv6 addresses assigned by the DHCPv6 client.
- The source Media Access Control (MAC) addresses of Layer-2 packets must match the client MAC addresses in DHCPv6 request packets of the client.



Figure 15-51



|                |   |
|----------------|---|
| <b>Remarks</b> | S is an access device.<br>A and C are user PCs.<br>B is a controlled DHCPv6 server. |
|----------------|---|

## Deployment

- Enable DHCPv6 snooping on the access device S for DHCPv6 monitoring.
- Set all downstream ports on the access device S as DHCPv6 untrusted ports.
- Enable IPv6 Source Guard on the access device S to filter IPv6 packets.
- On the access device S, set the match mode of IPv6 Source Guard as IPv6+MAC to check both MAC fields and IPv6 fields of IPv6 packets.

## 11.2.4 Prevention of Unauthorized IPv6 Configuration

### Scenario

When checking IPv6 packets from untrusted ports, you need to check whether source IPv6 addresses of the packets are consistent with the IPv6 addresses assigned by the DHCPv6.

If the source IPv6 addresses, connection ports, or Layer-2 MAC addresses of IPv6 packets fail to match the assignment records of the DHCPv6 server snooped by the device, the packets should be discarded.

The operating process of the device in the scenario is the same as that in the preceding figure.

### Deployment

- See section 11.2.3 "Prevention of IPv6/MAC Spoofing".

## 11.3 Features

### Basic Concepts

---

#### ↳ DHCPv6 Request Packet

A DHCPv6 request packet is the packet sent from the DHCPv6 client to the DHCPv6 server. It includes DHCPv6 solicit packet, DHCPv6 request packet, DHCPv6 confirm packet, DHCPv6 rebind packet, DHCPv6 release packet, DHCPv6 decline packet, DHCPv6 renew packet, DHCPv6 inform-req packet, and DHCPv6 leasequery packet.

#### ↳ DHCPv6 Response Packet

A DHCPv6 response packet is the packet sent from the DHCPv6 server to the DHCPv6 client. It includes DHCPv6 advertise packet, DHCPv6 reply packet, DHCPv6 reconfigure packet, DHCPv6 relay-reply packet, DHCPv6 leasequery-reply packet, DHCPv6 leasequery-done packet, and DHCPv6 leasequery-data packet.

#### ↳ DHCPv6 Snooping Trusted Port

As the interactive packets used by DHCPv6 to obtain IPv6 addresses or prefixes are multicast packets, there may exist illegal DHCPv6 services affecting IPv6 acquisition, and user information may even be stolen by such illegal services. To prevent such issues, DHCPv6 snooping classifies ports into trusted and untrusted ports, and the devices forwards only the DHCPv6 response packets received by the trusted port and discards all DHCPv6 response packets from the untrusted port. By setting the ports connected to a legal DHCPv6 server as trusted ports and the others as untrusted ports, illegal DHCPv6 servers will be shielded.

On a switch, all switch ports or Layer-2 aggregate ports (APs) are untrusted ports by default, which can be configured as trusted ports.

#### ↳ Filtering DHCPv6 Snooping Request Packets

When DHCPv6 packets are disabled for an individual user, any DHCPv6 packets sent from the user's device shall be shielded. DHCPv6 request packet filtering can be configured on an untrusted port to filter all DHCPv6 request packets received by the port.

#### ↳ VLAN-based DHCPv6 Snooping

DHCPv6 snooping takes effect in the unit of VLAN. If DHCPv6 snooping is enabled by default, the function is enabled on all VLANs of the device. The VLAN on which DHCPv6 snooping takes effect can be flexibly controlled through configuration.

#### ↳ DHCPv6 Snooping User Database

On a DHCPv6 network, a frequently encountered problem is that users may arbitrarily set static IPv6 addresses. Such addresses are difficult to maintain and may conflict with legal user addresses, making the users unable to access the Internet. By snooping the packets exchanged between the client and the server, DHCPv6 snooping forms IPv6 information obtained by users, user MAC, VID, PORT, and lease time into a user record, thus making a DHCPv6 snooping user database to control legal use of IPv6 addresses.

#### ↳ DHCPv6 Option 18 and Option 37

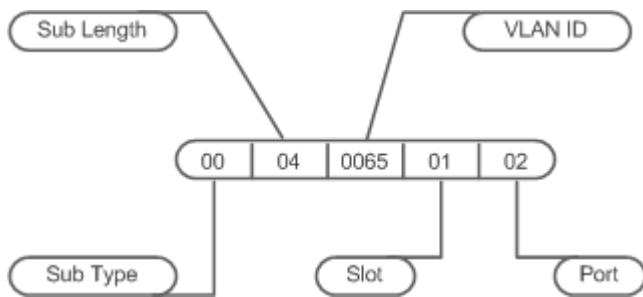
When managing user IP addresses, some network administrators expect to determine the IP addresses to be assigned according to the user locations; that is, they expect to assign IP addresses to users according to the information on the connected network devices, thereby adding user-related device information to DHCP request packets through DHCPv6 option while performing DHCPv6 snooping. The option number for RFC3315 is 18; the option number for RFC4649, the option number used is 37. After the content of Option 18 and Option 37 is parsed on the DHCPv6 server, the server can obtain information of more users according to the content uploaded by Option 18 and option 37 so as to assign IP addresses more accurately.

- Option 18: Interface ID

The default content of Interface ID include the number of the VLAN to which the port receiving request packets from the DHCPv6 client belongs, and the port index (the values of the port index are the slot number and port number); the extension content is a customized character string. Default and extension fillings take effect only for wired interfaces, including switch ports, Layer-2 APs, or Layer-2 encapsulation sub-interfaces.

The Interface ID filling format can be classified into standard and extension formats, only one of which can be used on the same network. When the standard filling format is used, only default content can be filled in for sub-options of Interface ID, as shown in the following figure:

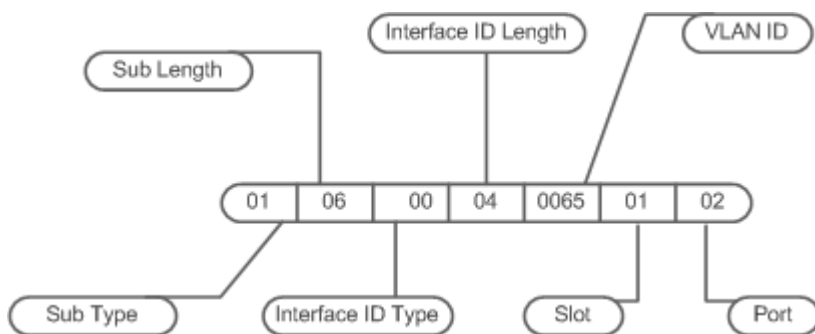
Figure 15-52



To use customized content, the extension filling format can be used. The content filled in by extension can be default or extension content. To distinguish between the content, add a content type field and a content length field of one byte respectively following the sub-option length. For default content, set the content type as 0; for extension content, set the content type as 1.

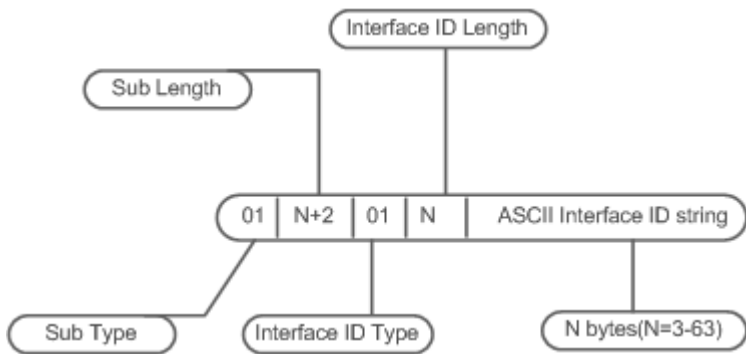
The format of default content is as follows:

Figure 15-53



The format of extension content is as follows:

Figure 15-54

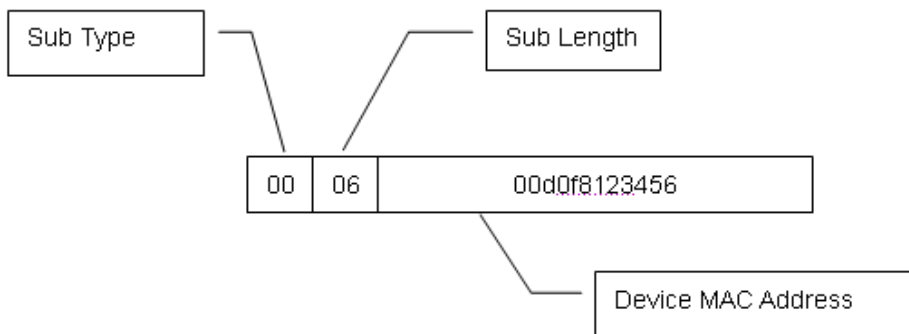


- Option 37: Remote ID

The default content of Remote ID is the bridge MAC address of the DHCPv6 relay that receives request packets from the DHCPv6 client, and the extension content is a customized character string.

The Remote ID filling format can be classified into standard and extension formats, only one of which can be used on the same network. When the standard filling format is used, only default content are filled in for sub-options of Remote ID, as shown in the following figure:

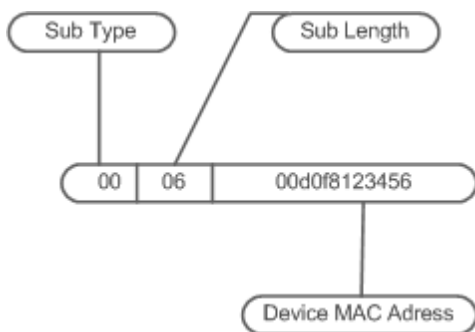
Figure 15-55



To use customized content, the extension filling format can be used. The content filled in by extension can be default or extension content. To distinguish between the content, add a content type field and a content length field of one byte respectively following the sub-option length. For default content, set the content type as 0; for extension content, set the content type as 1.

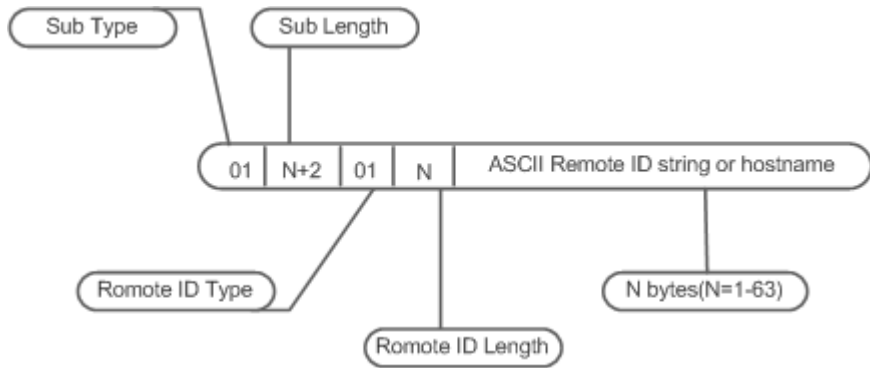
The format of default content is as follows:

Figure 15-56



The format of extension content is as follows:

Figure 15-57



● Note

Option 18: The values of port index for Interface ID are the slot number and port number. The port can be a wired switch port, Layer-2 AP, or Layer-2 encapsulation sub-interface. The port number refers to the sequence number of the port in the slot. The port number of a Layer-2 AP is an AP number. For example, the port number of Fa0/10 is 10, the port number of AP 11 is 11;

Slot numbers are the sequence numbers of all slots on a device (one device in stack mode). The slot number of an AP is the last one. The sequence numbers of slots start from 0. Run the **show slots** command to display the numbers. For example:

Example 1:

```
Orion Alpha A28X#show slots (only Dev and slot displayed)
```

```
Dev Slot
```

```
-----
```

```
1 0 -----> The slot number is 0.
```

```
1 1 -----> The slot number is 1.
```

```
1 2 -----> The slot number is 2.
```

In this case, the slot number of an AP is 3.

Example 2:

```
Orion Alpha A28X#show slots (only Dev and slot displayed)
```

```
Dev Slot
```

```
-----
```

```
1 0 -----> The slot number is 0.
```

```
1 1 -----> The slot number is 1.
```

```
1 2 -----> The slot number is 2.
```

```
2 0 -----> The slot number is 3.
```

```
2 1 -----> The slot number is 4.
```

2 2 -----> The slot number is 5.

In this case, the slot number of an AP is 6.

## Illegal DHCPv6 Packet

DHCPv6 snooping checks the validity of DHCPv6 packets passing through the device, discards illegal DHCPv6 packets, records user information, and generates a DHCPv6 snooping binding database for query of other functions.

The following packets are considered as illegal DHCPv6 packets.

- DHCPv6 response packets received by untrusted ports. For details, see the section DHCPv6 Response Packet.
- Relayed DHCPv6 packets received by untrusted ports, namely DHCPv6 relay-forward packets and DHCPv6 relay-reply packets.
- DHCPv6 relay-reply packets received by trusted ports. The egress for these packets is an untrusted ports according to the entry.
- DHCPv6 release packets; no corresponding users are found in the DHCPv6 snooping user database according to the Layer-2 source MAC and VID of these packets.
- DHCPv6 release packets. The IPv6 addresses or prefixes of these packets do not exist in the DHCPv6 snooping user database.
- DHCPv6 release packets. The IPv6 addresses or prefixes of these packets all exist in the DHCPv6 snooping user database but the untrusted ports of DHCPv6 release packets are inconsistent with those untrusted ports in the DHCPv6 snooping user database.
- DHCPv6 packets in incorrect formats or incomplete packets.

## Overview

| Features   | Description  |
|--|--|
| <a href="#">Filtering Illegal DHCPv6 Packets</a> | Checks the validity of exchanged DHCPv6 packets, and discards illegal packets (see the preceding section for instructions for illegal packets). Forwards only legal response packets to trusted ports. |
| <a href="#">Establishing a User Database</a>     | Snoops interaction between the client and the server, and generates the DHCPv6 snooping user database to provide a basis for other security filtering modules.   |

### 11.3.1 Filtering Illegal DHCPv6 Packets

This function is to check the validity of DHCPv6 packets from untrusted ports, filter the packets according to the types of illegal packets described in Basic Concepts above, and control the transmission scope of packets to prevent malicious users from spoofing.

## Working Principle

During snooping, the receipt ports of packets and packet fields are checked to filter the packets; the destination ports of packets are modified to control the transmission scope of packets.

## Checking Ports

When receiving DHCPv6 packets, the device first determines whether the port receiving packets is a DHCPv6 trusted port. If the port is a trusted port, the packets will be forwarded without validity check, binding, or prefix record generation. If the port is an untrusted port, validity check is required.

#### ↘ Checking whether Packet Encapsulation and Length are Complete

Check whether the packets are User Datagram Protocol (UDP) packets and the destination port is 546 or 547. Check whether the actual length of a packet matches the length field described in the protocol.

#### ↘ Checking Whether DHCPv6 Packet Field and Packet Type are Correct

Check whether the packets are relayed according to the types of illegal packets described in the preceding section Basic Concepts, and then check whether the restrictions specific to a type of packets are met according to the actual type of packets.

### Related Configuration

#### ↘ Enabling Global DHCPv6 Snooping

By default, DHCPv6 snooping is disabled.

Run the [ **no** ] **ipv6 dhcp snooping** command to enable or disable DHCPv6 snooping.

To enable or disable DHCPv6 snooping on different VLANs, global DHCPv6 snooping must be enabled first.

#### ↘ Setting DHCPv6 Snooping on a VLAN

By default, when global DHCPv6 snooping is enabled, DHCPv6 snooping takes effect on all VLANs.

Run the [ **no** ] **ipv6 dhcp snooping vlan** command to enable or disable DHCPv6 snooping on a VLAN. The range of command parameter values is the actual range of VLAN numbers.

## 11.3.2 Establishing a User Database

The packets exchanged between the DHCPv6 client and the DHCPv6 server are snooped, and DHCPv6 snooping binding entries and prefix entries are generated according to the information on legal DHCPv6 packets. All the entries are provided for other security configuration modules as an information list of legal users and a basis for network packet filtering.

### Working Principle

During snooping, binding database and prefix database are continuously updated according to the types of DHCPv6 packets.

#### ↘ Generating Binding or Prefix Records

When DHCPv6 reply packets are snooped on a trusted port, client IPv6 addresses or prefixes, client MAC addresses, and lease time fields of the packets are extracted, and a binding or prefix record is generated according to the client port ID recorded by the device (wired interface index), and the client VLAN.

#### ↘ Deleting Binding or Prefix Records

When the recorded lease time is over, or the legal DHCPv6 release/DHCPv6 decline packets sent from the client are snooped, or users run the clear command to delete binding or prefix records, the corresponding binding or prefix records are deleted.

## Related Configuration

Enable DHCPv6 snooping without extra configuration.

## 11.4 Configuration

| Configuration   | Description and Command  |   |
|---|--|---|
| <a href="#">Configuring Basic DHCPv6 Snooping Functions</a> | <ul style="list-style-type: none"> <li>(Mandatory) It is used to establish DHCPv6 snooping.</li> </ul>                     |   |
|   | <b>ipv6 dhcp snooping</b>  | Enables DHCPv6 snooping.  |
|   | <b>ipv6 dhcp snooping binding-delay</b>  | Delays assignment of the DHCPv6 snooping binding entries to the hardware filtering entries.   |
|   | <b>ipv6 dhcp snooping filter-dhcp-pkt</b>  | Enables DHCPv6 request packet filtering.  |
|   | <b>ipv6 dhcp snooping vlan</b>   | Enables and disables DHCPv6 snooping for specified VLANs.   |
|   | <b>ipv6 dhcp snooping database write-delay</b>   | Enables the function for regularly saving DHCPv6 snooping binding and prefix records.   |
|   | <b>ipv6 dhcp snooping database write-to-flash</b>  | Manually saves DHCPv6 snooping binding and prefix records.  |
|   | <b>renew ipv6 dhcp snooping database</b>   | Manually imports the user records saved in flash to the DHCPv6 snooping user database.  |
|   | <b>ipv6 dhcp snooping trust</b>  | Configures DHCPv6 snooping trusted ports.   |
| <b>ipv6 dhcp snooping link-detection</b>                    | Clears dynamical biding entries on a port when the port is configured into Link Down state.                                |   |
| <a href="#">Configuring Option 18 and Option 37</a>         | <ul style="list-style-type: none"> <li>(Optional) It is used to optimize assignment of DHCPv6 server addresses.</li> </ul> |   |
|   | <b>ipv6 dhcp snooping Information option [standard-format]</b>   | Adds Option 18 or Option 37 to DHCPv6 request packets.<br><b>standard-format:</b> Fills in content in a standard format if such keyword exists; otherwise, fills in content in an extension format. |



| Configuration | Description and Command   |  |
|---------------|---|--|
|               | <b>ipv6 dhcp snooping information option format remote-id [ string ASCII-string   hostname ]</b>              | Configures Remote ID in an extension format.<br><b>string</b> : Indicates that the content filled in is a customized character string.<br><b>hostname</b> : Indicates that the content filled in is hostname.            |
|               | <b>ipv6 dhcp snooping vlan <i>vlan-id</i> information option format-type interface-id string ASCII-string</b> | Configures the customized character string of Interface ID in an extension format.   |
|               | <b>ipv6 dhcp snooping vlan <i>vlan-id</i> information option change-vlan-to vlan <i>vlan-id</i></b>           | Configures VLAN mapping for Interface ID in an extension format, which is exclusive from the [no] <b>ipv6 dhcp snooping vlan <i>vlan-id</i> information option format-type interface-id string ASCII-string</b> command. |

## 11.4.1 Configuring Basic DHCPv6 Snooping Functions

### Configuration Effect

- Enable DHCPv6 snooping.
- Generate DHCPv6 snooping binding and prefix databases.
- Control the transmission scope of DHCPv6 packets.
- Filter illegal DHCPv6 packets.

### Notes

- The port connecting the device to a trusted DHCPv6 server must be set as a trusted port.
- The port on which DHCPv6 snooping takes effect can be a wired switch port, Layer-2 AP or Layer-2 encapsulation sub-interface. Configuration on a port can be classified into configuration in interface mode.
- The Link Down entry clearing function applies only to wired ports.

### Configuration Steps

#### ▾ Enabling Global DHCPv6 Snooping

- Mandatory.
- If not specified, configure this function on an access device.

#### ▾ Delaying Assignment of DHCPv6 Snooping Binding Entries to Hardware Filtering Entries

- Configure the function if assignment needs to be delayed. Assignment is not delayed by default.
- If not specified, configure this function on an access device.

#### ▾ Enabling DHCPv6 Request Packet Filtering

- Enable the function if users' DHCPv6 requests need to be restricted on a port.
- If not specified, disable the function on the access device.

#### ↘ Enabling and Disabling VLAN-based DHCPv6 Snooping

- Disable DHCPv6 snooping if the function is not needed on a VLAN.
- If not specified, configure this function on an access device.

#### ↘ Enabling Regular Saving of DHCPv6 Snooping Binding Records

- This function should be enabled if DHCPv6 snooping binding records need to be maintained after the device is restarted.
- If not specified, enable the function on the access device.

#### ↘ Configuring DHCPv6 Trusted Ports

- Mandatory.
- Set the port connecting the device to a trusted DHCPv6 device as a DHCPv6 trusted port.

#### ↘ Enabling and Disabling Clearing of Dynamically Bound Entries When the Port is Configured into Link Down State

- On a stable network, enable the function to release spaces occupied by hardware entries and timely clear the entries on the Link Down port.
- If not specified, disable the function on the access device.

### Verification

Enable the device to use DHCPv6 to obtain network configuration parameters.

- Check whether user records are generated in the DHCPv6 snooping binding database.

### Related Commands

#### ↘ Enabling and Disabling DHCPv6 Snooping

|                              |  |
|------------------------------|--|
| <b>Command</b>               | [ no ] ipv6 dhcp snooping  |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | After global DHCPv6 snooping is enabled, run the <b>show ipv6 dhcp snooping</b> command to check whether DHCPv6 snooping is enabled. |

#### ↘ Delaying Assignment of the DHCPv6 Snooping Binding Entries to the Hardware Filtering Entries

|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] ipv6 dhcp snooping binding-delay   |
| <b>Parameter Description</b> | <i>seconds</i> : Indicates the time for delaying assignment of binding entries to hardware filtering entries, in the unit of seconds. |

|                     |   |
|---------------------|---|
|                     | The value is 0 by default.  |
| <b>Command Mode</b> | Global configuration mode   |
| <b>Usage Guide</b>  | By default, dynamically bound entries are added to hardware filtering entries in real time.<br>After the function is configured, the dynamically generated binding entries are bound to hardware filtering entries only when no IPv6 address conflicts are detected within a specified time period. |

#### ↘ Configuring a VLAN on Which DHCPv6 Snooping Takes Effect

|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] ipv6 dhcp snooping vlan { <i>vlan-rng</i>   { <i>vlan-min</i> [ <i>vlan-max</i> ] } }  |
| <b>Parameter Description</b> | <i>vlan-rng</i> : Indicates the VLAN scope in which DHCPv6 snooping takes effect.<br><i>vlan-min</i> : Indicates the lower VLAN limit where DHCPv6 snooping takes effect.<br><i>vlan-max</i> : Indicates the upper VLAN limit where DHCPv6 snooping takes effect. |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | DHCPv6 snooping is enabled or disabled on a specified VLAN by configuring the command.<br>This function takes effect only if global DHCPv6 snooping is enabled.   |

#### ↘ Filtering DHCPv6 Request Packets on a Port

|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] ipv6 dhcp snooping filter-dhcp-pkt   |
| <b>Parameter Description</b> | N/A   |
| <b>Command Mode</b>          | Interface configuration mode  |
| <b>Usage Guide</b>           | All DHCPv6 request packets can be prohibited on the port by configuring the command; that is, all users are prohibited from applying for addresses on the port. |

#### ↘ Regularly Writing DHCPv6 Snooping Database Information into Flash

|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] ipv6 dhcp snooping database write-delay [ <i>time</i> ]  |
| <b>Parameter Description</b> | <i>time</i> : Indicates the interval for regularly writing the DHCPv6 snooping database into flash.   |
| <b>Command Mode</b>          | Global configuration mode   |
| <b>Usage Guide</b>           | The DHCPv6 snooping database can be written into a flash file by configuring the command.<br>The function prevents user information loss after the device restarts. If user information is lost, users have to re-obtain IP addresses for normal communication. |

#### ↘ Manually Writing DHCPv6 Snooping Database Information into Flash

|                              |  |
|------------------------------|--|
| <b>Command</b>               | ipv6 dhcp snooping database write-to-flash |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode                  |

---

|                    |  |
|--------------------|--|
| <b>Usage Guide</b> | Dynamic user information in the DHCPv6 snooping database can be written into a flash file in real time by running the command. |
|--------------------|--|

### ↳ Manually Importing Information in Flash to the DHCPv6 Snooping Binding Database

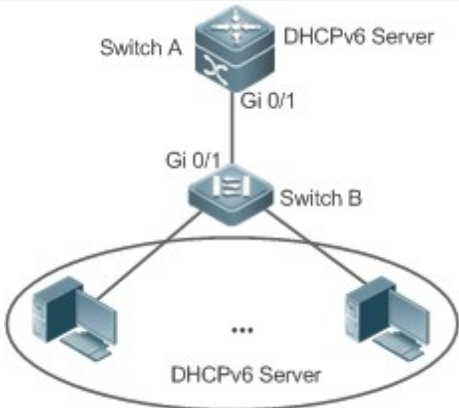
|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>renew ipv6 dhcp snooping database</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Privileged EXEC mode   |
| <b>Usage Guide</b>           | Flash file information can be written into the DHCPv6 snooping database in real time by running the command. |

### ↳ Configuring a Port as a Trusted Port

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>[ no ] ipv6 dhcp snooping trust</b>  |
| <b>Parameter Description</b> | N/A   |
| <b>Command Mode</b>          | Interface configuration mode  |
| <b>Usage Guide</b>           | The port connecting to a legal DHCPv6 server is configured as a trusted port by configuring the command. The DHCPv6 response packets received by a trusted port are forwarded, while the DHCPv6 response packets received by an untrusted port are discarded. |

## Configuration Example

### ↳ Dynamically obtaining IPv6 addresses through the legal DHCPv6 server on a DHCPv6 client

|                                 |   |
|---------------------------------|---|
| <b>Scenario</b><br>Figure 15-58 |  <p>The diagram illustrates a network topology for DHCPv6 snooping. At the top, Switch A is connected to a DHCPv6 Server. Switch A's Gi 0/1 port is connected to Switch B's Gi 0/1 port. Switch B is connected to a group of DHCPv6 Servers, represented by computer icons, via its other ports. The DHCPv6 Servers are enclosed in an oval.</p> |
| <b>Configuration Steps</b>      | <ul style="list-style-type: none"> <li>● Enable DHCPv6 snooping on the access device (Switch B).</li> <li>● Set the uplink port (Gi 0/1) as a trusted port.</li> </ul>  |
| <b>B</b>                        | <pre>B#configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)#ipv6 dhcp snooping</pre>   |

|                     |   |
|---------------------|---|
|                     | <pre>B(config)#interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ipv6 dhcp snooping trust B(config-if-GigabitEthernet 0/1)#end</pre>   |
| <b>Verification</b> | <p>Confirm configuration of Switch B.</p> <ul style="list-style-type: none"> <li>● Confirm whether DHCPv6 snooping is enabled and whether the DHCPv6 snooping trusted port configured is the uplink port.</li> <li>● On Switch B, check the configuration of DHCP snooping, especial whether the trusted port is correct.</li> </ul>  |
| <b>B</b>            | <pre>Orion Alpha A28X#show ipv6 dhcp snooping DHCPv6 snooping status : ENABLE DHCPv6 snooping database write-delay time : 0 seconds DHCPv6 snooping binding-delay time : 0 seconds DHCPv6 snooping option18/37 status : DISABLE DHCPv6 snooping link detection : DISABLE Interface          Trusted  Filter DHCPv6 ----- GigabitEthernet 0/1  YES     DISABLE Orion Alpha A28X#show ipv6 dhcp snooping binding Total number of bindings: 1 NO.  MacAddress      IPv6 Address                Lease(sec)  VLAN  Interface ----- 1    00d0.f801.0101   2001::10                    42368      2    GigabitEthernet 0/1</pre> |

### Common Errors

- The uplink port is not set as a DHCPv6 trusted port.
- Other access security options are configured on the uplink port, resulting in failure of DHCPv6 trusted port configuration.

## 11.4.2 Configuring Option 18 and Option 37

### Configuration Effect

- The DHCPv6 server can obtain more information during address assignment, thus improving address assignment.
- The option is transparent to the DHCPv6 client, and such function is perception-free to the client.

## Configuration Steps

- Run the configuration if the optimization is needed.
- If not specified, enable the function on the device where DHCPv6 snooping is enabled.

## Verification

Check the configuration of DHCPv6 snooping to ensure that such function is enabled.

## Related Commands

### Adding Option18 and Option 37 to DHCPv6 Request Packets

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <code>[no] ipv6 dhcp snooping information option [ standard-format ]</code>  |
| <b>Parameter Description</b> | <b>standard-format:</b> Fills in content in a standard format if such keyword exists; otherwise, fills in content in an extension format.  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Information on Option 18 and Option 37 is added to DHCPv6 request packets by configuring the command, and the DHCPv6 server assigns addresses according to information on Option 18 and Option 37. |

### Setting Option 37 (Remote ID) as a Customized Character String

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <code>[ no ] ipv6 dhcp snooping information option format remote-id { string ASCII-string   hostname }</code>  |
| <b>Parameter Description</b> | <b>string ASCII-string:</b> Indicates that the content of Remote ID in an extension format is a customized character string.<br><b>hostname:</b> Indicates that the content of Remote ID in an extension format is hostname. |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Remote ID is configured in an extension format by configuring the command. Remote ID is customized, and the DHCPv6 server assigns addresses according to information on Option 37.   |

### Setting Option 18 (Interface ID) as a Customized Character String

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <code>[ no ] ipv6 dhcp snooping vlan <i>vlan-id</i> information option format-type <i>interface-id</i> string ASCII-string</code>   |
| <b>Parameter Description</b> | <b>vlan-id:</b> Indicates the VLAN to which DHCPv6 request packets belong.<br><b>ASCII-string:</b> Indicates the user-customized content to be filled in for Interface-ID.                    |
| <b>Command Mode</b>          | Interface configuration mode  |
| <b>Usage Guide</b>           | Customized character strings of Interface ID are configured in an extension format by configuring the command, and the DHCPv6 server assigns addresses according to information on Option 18. |

### Setting Option 18 (Interface ID) as a Modified VLAN

|                |  |
|----------------|--|
| <b>Command</b> | <code>[ no ] ipv6 dhcp snooping vlan <i>vlan-id</i> information option change-vlan-to vlan <i>vlan-id</i></code> |
|----------------|--|

---

|                              |  |
|------------------------------|--|
| <b>Parameter Description</b> | <i>vlan-id</i> (the first one): Indicates the VLAN to which DHCPv6 request packets belong.<br><i>vlan-id</i> (the second one): Indicates the VLAN after modification.        |
| <b>Command Mode</b>          | Interface configuration mode   |
| <b>Usage Guide</b>           | Interface ID is configured as VLAN mapping in an extension format by configuring the command, and the DHCPv6 server assigns addresses according to information on Option 18. |

## Configuration Example

↳ The following example shows how to add Option 18 and Option 37 to DHCPv6 request packets.

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>Configure basic DHCPv6 snooping functions.(Omitted)</li> <li>Enable the function for adding Option 18 and Option 37.</li> </ul>   |
| <b>B</b>                   | <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ipv6 dhcp snooping information option Orion Alpha A28X(config)# end</pre>  |
| <b>Verification</b>        | Display the DHCPv6 snooping configuration.   |
| <b>B</b>                   | <pre>Orion Alpha A28X #show ipv6 dhcp snooping DHCPv6 snooping status : ENABLE DHCPv6 snooping database write-delay time : 0 seconds DHCPv6 snooping binding-delay time : 0 seconds DHCPv6 snooping option 18/37 status : ENABLE DHCPv6 snooping link detection : DISABLE Interface           Trusted   Filter DHCPv6 ----- FastEthernet0/10   YES     DISABLE</pre> |

## 11.5 Monitoring and Maintenance

### Clearing

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

| Description  | Command  |
|--|--|
| Clears dynamic user information in the DHCPv6 snooping database. | <b>clear ipv6 dhcp snooping binding</b> [ <i>vlan</i> <i>vlan-id</i>   <i>mac</i>   <i>ipv6</i>   <b>interface</b> <i>interface-id</i> ] |
| Clears all entries in the DHCPv6 snooping prefix database.       | <b>clear ipv6 dhcp snooping prefix</b>   |
| Clears statistics about DHCPv6 snooping handling DHCPv6 packets. | <b>clear ipv6 dhcp snooping statistics</b>   |

## Displaying

---

| Description   | Command                                   |
|---|---|
| Displays DHCPv6 snooping configuration.   | <b>show ipv6 dhcp snooping</b>            |
| Displays the VLANs on which DHCPv6 snooping fails to take effect.   | <b>show ipv6 dhcp snooping vlan</b>       |
| Displays all dynamically bound entries in the DHCPv6 snooping binding database.   | <b>show ipv6 dhcp snooping binding</b>    |
| Displays all entries in the DHCPv6 snooping prefix database.  | <b>show ipv6 dhcp snooping prefix</b>     |
| Displays the counters of DHCPv6 snooping handling packets.  | <b>show ipv6 dhcp snooping statistics</b> |
| Displays all statically bound entries added manually and all dynamically bound entries in the DHCPv6 snooping binding database. | <b>show ipv6 source binding</b>           |

## Debugging

---

- System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

| Description                                    | Command                              |
|--|--------------------------------------|
| Debugs DHCPv6 snooping events.                 | <b>debug snooping ipv6 event</b>     |
| Disables debugging of DHCPv6 snooping events.  | <b>no debug snooping ipv6 event</b>  |
| Debugs DHCPv6 snooping packets.                | <b>debug snooping ipv6 packet</b>    |
| Disables debugging of DHCPv6 snooping packets. | <b>no debug snooping ipv6 packet</b> |

---

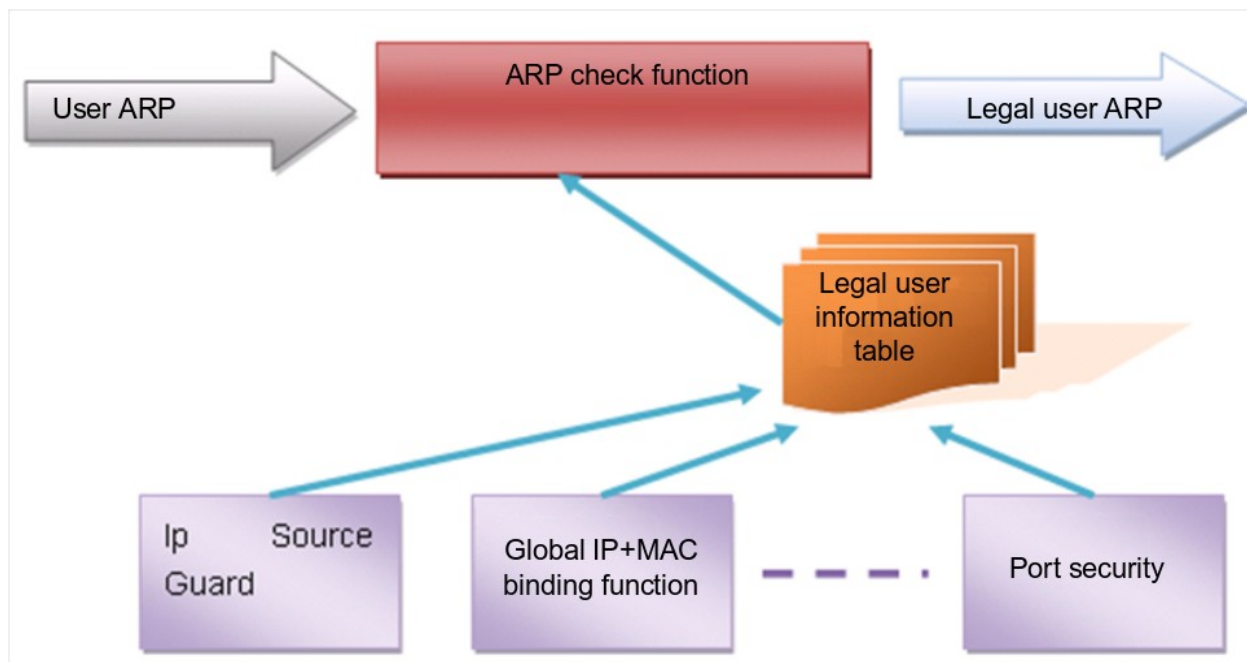


# 12 Configuring ARP Check

## 12.1 Overview

The Address Resolution Protocol (ARP) packet check filters all ARP packets under ports (including wired layer-2 switching ports, layer-2 aggregate ports (APs), and layer-2 encapsulation sub-interfaces) and discards illegal ARP packets, so as to effectively prevent ARP deception via networks and to promote network stability. On devices supporting ARP check, illegal ARP packets in networks will be ignored according to the legal user information (IP-based or IP-MAC based) generated by security application modules such as IP Source Guard, global IP+MAC binding, 802.1X authentication, GSN binding, Web authentication and port security.

Figure 16-14



The above figure shows that security modules generate legal user information (IP-based or IP-MAC based). ARP Check uses the information to detect whether the Sender IP fields or the <Sender IP, Sender MAC>fields in all ARP packets at ports matches those in the list of legal user information. If not, all unlisted ARP packets will be discarded.

### Protocols and Standards

- RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

## 12.2 Applications

| Application | Description |
|-------------|-------------|
|-------------|-------------|

## 12.2.1 Filtering ARP Packets in Networks

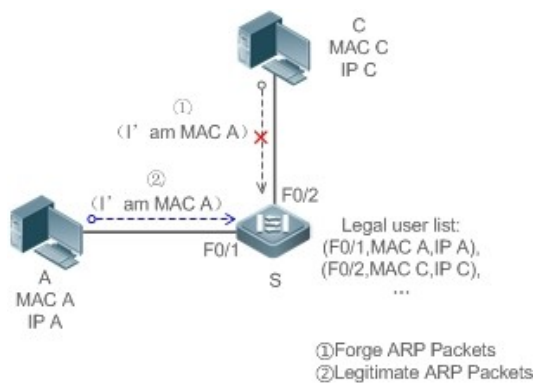
### Scenario

Check ARP packets from distrusted ports and filter out ARP packets with addresses not matching the results assigned by the DHCP server.

For example, in the following figure, the ARP packets sent by DHCP clients are checked.

- The ports receiving ARP packets, the source MAC addresses of ARP packets, and the source IP addresses of ARP packets shall be consistent with the snooped DHCP-assigned records.

Figure 16-15



**Remarks:** S is an access device.  
A and C are user PCs.

### Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all the downlink ports on S as DHCP distrusted ports.
- Enable IP Source Guard and ARP Check on all distrusted ports on S to realize ARP packet filtration.

## 12.3 Features

### Basic Concepts

#### Compatible Security Modules

Presently, the ARP Check supports the following security modules.

- IP-based: IP-based mode: port security, and static configuration of IP Source Guard.
- IP-MAC based: IP-MAC based mode: port security, global IP+MAC binding, 802.1X authorization, IP Source Guard, GSN binding, and Web authentication.

## ↘ Two Modes of APR Check

The ARP Check has two modes: Enabled and Disabled. The default is Enabled.

### 17. Enabled Mode

Through ARP Check, ARP packets are detected based on the IP/IP-MAC based binding information provided by the following modules.

- Global IP-MAC binding
  - 802.1X authorization
  - IP Source Guard
  - GSN binding
  - Port security
  - Web authentication
  - Port security IP+MAC binding or IP binding
- 
- When only ARP Check is enabled on a port but the above-mentioned modules are not enabled, legal user information cannot be generated, and thereby all ARP packets from this port will be discarded.
  - When the ARP Check and VRRP functions are enabled on an interface, if the physical IP address and virtual IP address of the interface can be used as the gateway address, the physical IP address and VRRP IP address need to be permitted to pass. Otherwise, ARP packets sent to the gateway will be filtered out.
- 

### 18. Disabled Mode

ARP packets on a port are not checked.

## Overview

| Feature                               | Description  |
|---------------------------------------|--|
| <a href="#">Filtering ARP Packets</a> | Check the source IP and source MAC addresses of ARP packets to filter out illegal ARP packets. |

### 12.3.1 Filtering ARP Packets

Enable ARP Check on specified ports to realize filtration of illegal ARP packets.

#### Working Principle

A device matches the source IP and source MAC addresses of the ARP packets received at its ports with the legal user information of the device. With successful matching, packets will be transferred, or otherwise they will be discarded.

#### Related Configuration

##### ↘ Enabling ARP Check on Ports

By default, the ARP Check is disabled on ports.

Use the **arp-check** command to enable ARP Check.

Unless otherwise noted, this function is usually configured on the ports of access devices.

---

## 12.4 Configuration

| Configuration                         | Description and Command   |
|---------------------------------------|---|
| <a href="#">Configuring ARP Check</a> | <ul style="list-style-type: none"><li>(Mandatory) It is used to enable APR Check.</li></ul> |
|                                       | <b>arp-check</b> Enables ARP Check.   |

### 12.4.1 Configuring ARP Check

#### Configuration Effect

- Illegal ARP packets are filtered out.

#### Notes

- When ARP Check is enabled, the number of policies or users of related security applications may decrease.
- ARP Check cannot be configured on mirrored destination ports.
- ARP Check cannot be configured on the trusted ports of DHCP Snooping.
- ARP Check cannot be configured on global IP+MAC exclude ports.
- ARP Check can be enabled only on wired switching ports, layer-2 APs, layer-2 encapsulation sub-interfaces.  
Enable ARP check for the wired in interface configuration mode.

#### Configuration Steps

##### ↳ Enabling ARP Check

- (Mandatory) The function is disabled by default. To use the ARP Check function, an administrator needs to run a command to enable it.

#### Verification

- Use the **show run** command to display the system configuration.
- Use the **show interface { interface-type interface-number } arp-check list** command to display filtering entries.

#### Related Commands

##### ↳ Enabling ARP Check

|                    |  |
|--------------------|--|
| <b>Command</b>     | <b>arp-check</b>   |
| <b>Parameter</b>   | N/A  |
| <b>Description</b> |  |
| <b>Command</b>     | Interface configuration mode   |
| <b>Usage Guide</b> | Generate ARP filtration information according to the legal user information of security application modules to filter out illegal ARP packets in networks. |

## Configuration Example

- The following configuration example introduces only ARP Check related configurations.

### ↳ Enabling ARP Check on ports

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"><li>Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard, port security, or global IP+MAC binding.</li></ul> <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)#address-bind 192.168.1.3 00D0.F800.0003 Orion Alpha A28X(config)#address-bind install Orion Alpha A28X(config)#ip source binding 00D0.F800.0002 vlan 1 192.168.1.4 interface gigabitEthernet 0/1 Orion Alpha A28X(config)# interface GigabitEthernet 0/1 Orion Alpha A28X(config-if-GigabitEthernet 0/1)#arp-check Orion Alpha A28X(config-if-GigabitEthernet 0/1)#ip verify source port-security Orion Alpha A28X(config-if-GigabitEthernet 0/1)#switchport port-security Orion Alpha A28X(config-if-GigabitEthernet 0/1)#switchport port-security binding 00D0.F800.0001 vlan 1 192.168.1.1 Orion Alpha A28X(config-if-GigabitEthernet 0/1)#exit Orion Alpha A28X(config)#interface gigabitEthernet 0/4 Orion Alpha A28X(config-if-GigabitEthernet 0/4)#switchport port-security Orion Alpha A28X(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5 Orion Alpha A28X(config-if-GigabitEthernet 0/4)#arp-check Orion Alpha A28X(config-if-GigabitEthernet 0/4)#exit Orion Alpha A28X(config)#interface gigabitEthernet 0/5 Orion Alpha A28X(config-if-GigabitEthernet 0/5)#arp-check Orion Alpha A28X(config-if-GigabitEthernet 0/5)#end</pre> |
| <b>Verification</b>        | Use the <b>show interface arp-check list</b> command to display the effective ARP Check list for interfaces.   |
|                            | <pre>Orion Alpha A28X# show interface arp-check list  INTERFACE          SENDER MAC          SENDER IP          POLICY SOURCE ----- -----</pre>  |

|                     |                |             |               |
|---------------------|----------------|-------------|---------------|
| GigabitEthernet 0/1 | 00d0.f800.0003 | 192.168.1.3 | address-bind  |
| GigabitEthernet 0/1 | 00d0.f800.0001 | 192.168.1.1 | port-security |
| GigabitEthernet 0/1 | 00d0.f800.0002 | 192.168.1.4 | DHCP snooping |
| GigabitEthernet 0/4 | 00d0.f800.0003 | 192.168.1.3 | address-bind  |
| GigabitEthernet 0/4 |                | 192.168.1.5 | port-security |
| GigabitEthernet 0/5 | 00d0.f800.0003 | 192.168.1.3 | address-bind  |

### Common Errors

- If ARP packets at a port need to be checked but APR-Check is disabled, then APR-Check will not be effective.

## 12.5 Monitoring

### Displaying

| Description   | Command   |
|---|---|
| Displays the effective ARP Check list based on ports. | <b>show interface</b> [ <i>interface-type interface-number</i> ] <b>arp-checklist</b> |

# 13 Configuring Dynamic ARP Inspection

## 13.1 Overview

Dynamic Address Resolution Protocol (ARP) inspection (DAI) checks the validity of received ARP packets. Invalid ARP packets will be discarded.

DAI ensures that only valid ARP packets can be forwarded by devices. DAI mainly performs the following steps:

- Intercepts all ARP request packets and ARP reply packets on untrusted ports in the virtual local area networks (VLANs) where the DAI function is enabled.
- Checks the validity of intercepted ARP packets according to user records stored in a security database.
- Discards the ARP packets that do not pass the validity check.
- Sends the ARP packets that pass the validity check to the destination.
- The DAI validity criteria are the same as those of ARP Check. For details, see the *Configuring ARP Check*.

DAI and ARP Check have same functions. The only difference is that DAI takes effect by VLAN whereas ARP Check takes effect by port.

### Protocols and Standards

- RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

## 13.2 Applications

| Application                             | Description  |
|---|--|
| <a href="#">ARP Spoofing Prevention</a> | Prevent ARP spoofing that is mounted by taking advantage of ARP defects. |

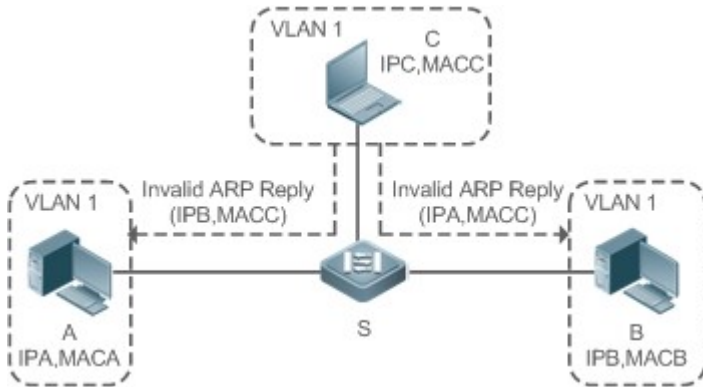
### 13.2.1 ARP Spoofing Prevention

#### Scenario

Due to inherent defects, ARP does not check the validity of received ARP packets. Attackers can take advantage of the defects to mount ARP spoofing. A typical example is man-in-the-middle (MITM) attack. See Figure 17-59.

---

Figure 17-59



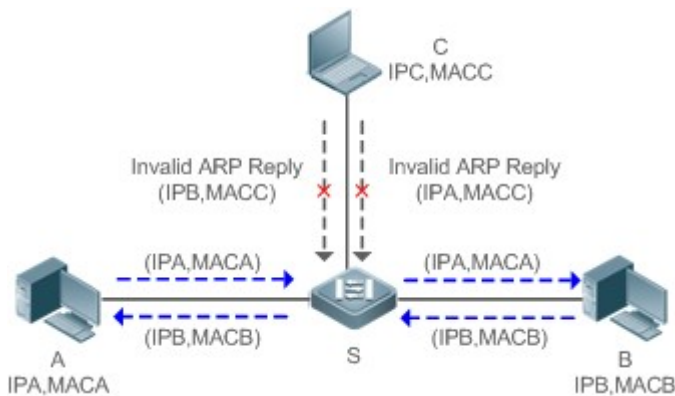
|                |   |
|----------------|---|
| <b>Remarks</b> | <p>Device S is a Orion Alpha A28X access switch enabled with DAI.</p> <p>User A and User B are connected to Device S, and they are in the same subnet.</p> <p>User C is a malicious user connected to Device S.</p> <p>IP A and MAC A are the IP address and MAC address of User A.</p> <p>IP B and MAC B are the IP address and MAC address of User B.</p> <p>IP C and MAC C are the IP address and MAC address of User C.</p> |
|----------------|---|

When User A needs to initiate network layer communication with User B, User A broadcasts an ARP request in the subnet to query the MAC address of User B. Upon receiving the ARP request packet, User B updates its ARP cache with IP A and MAC A, and sends an ARP reply. Upon receiving the ARP reply packet, User A updates its ARP cache with IP B and MAC B.

In this model, User C can make the ARP entry mapping between User A and User B incorrect by continuously broadcasting ARP reply packets to the network. The reply packets contain IP A, IP B, and MAC C. After receiving these reply packets, User A stores the ARP entry (IP B, MAC C), and User B stores the ARP entry (IP A, MAC C). As a result, the communication between User A and User B is directed to User C, without the knowledge of User A and User B. Here User C acts as the man in the middle by modifying received packets and forwarding them to User A or User B.

If Device S is enabled with DAI, it will filter out forged ARP packets to prevent ARP spoofing as long as the IP addresses of User A and User B meet the validity criteria described in section 13.1 Overview. Figure 17-60 shows the working process of DAI.

Figure 17-60





|                |   |
|----------------|---|
| <b>Remarks</b> | <p>Device S is a Orion Alpha A28X access switch enabled with DAI.</p> <p>User A and User B are connected to Device S, and they are in the same subnet.</p> <p>User C is a malicious user connected to Device S.</p> <p>IP A and MAC A are the IP address and MAC address of User A.</p> <p>IP B and MAC B are the IP address and MAC address of User B.</p> <p>IP C and MAC C are the IP address and MAC address of User C.</p> |
|----------------|---|

The ARP packets of User A and User B are forwarded normally by Device S. The forged ARP packets of User C are discarded because the packets do not match the records in the security database of Device S.

## Deployment

- Enable DHCP Snooping on Device S.
- Enable DAI and IP Source Guard on Device S.

## 13.3 Features

### Basic Concepts

#### Trust Status of Ports and Network Security

ARP packet check is performed according to the trust status of ports. DAI considers packets received from trusted ports as valid without checking their validity, but it checks the validity of packets received from untrusted ports.

For a typical network configuration, you should configure Layer-2 ports connected to network devices as trusted ports, and configure Layer-2 ports connected to hosts as untrusted ports.

- Network communication may be affected if a Layer-2 port connected to a network device is configured as an untrusted port.

### Overview

| Feature                                   | Description   |
|---|---|
| <a href="#">Invalid ARP Packet Filter</a> | Checks the source IP addresses and MAC addresses of ARP packets to filter out invalid packets.        |
| <a href="#">DAI Trusted Port</a>          | Permits the ARP packets received from specific ports to pass through without checking their validity. |

#### 13.3.1 Invalid ARP Packet Filter

Enable DAI in a specific VLAN to filter out invalid ARP packets. The DAI validity criteria are the same as those of ARP Check.

#### Working Principle

Upon receiving an ARP packet, the device matches the IP address and MAC address of the packet with the valid user records in its security database. If the packet matches a record, it will be forwarded normally. If it does not match any record, it will be discarded.

DAI and ARP Check use the same set of valid user records. For details, see the packet validity check description in the *Configuring ARP Check*.

## Related Configuration

### ↳ Enabling DAI in a VLAN

By default, DAI is disabled in VLANs.

Run the **ip arp inspection vlan** *vlan-id* command to enable DAI in a specific VLAN.

- After DAI is enabled in a VLAN, DAI may not take effect on all ports in the VLAN. A DHCP Snooping trusted port does not perform DAI check.

### ↳ Disabling DAI in a VLAN

By default, DAI is disabled in VLANs.

After DAI is enabled in a VLAN, you can run the **no ip arp inspection vlan** *vlan-id* command to disable DAI.

- Disabling DAI in a VLAN does not mean disabling packet validity check on all ports in the VLAN. The ports with ARP Check effective still check the validity of received ARP packets.

## 13.3.2 DAI Trusted Port

Configure specific device ports as DAI trusted ports.

### Working Principle

The validity of ARP packets received from trusted ports is not checked. The ARP packets received from untrusted ports are checked against the user records in a security database.

## Related Configuration

### ↳ Configuring DAI Trusted Ports

By default, all ports are untrusted ports.

Run the **ip arp inspection trust** command to set ports to trusted state.

- A port already enabled with access security control cannot be set to DAI trusted state. To set the port to DAI trusted state, first disable access security control.
- In normal cases, uplink ports (ports connected to network devices) can be configured as DAI trusted ports.

## 13.4 Configuration

| Configuration                   | Description and Command  |                               |
|---------------------------------|--|-------------------------------|
| <a href="#">Configuring DAI</a> | <ul style="list-style-type: none"><li>• (Optional) It is used to enable ARP packet validity check.</li></ul> |                               |
|                                 | <b>ip arp inspection vlan</b>  | Enables DAI.                  |
|                                 | <b>ip arp inspection trust</b>   | Configures DAI trusted ports. |

## 13.4.1 Configuring DAI

### Configuration Effect

- Check the validity of incoming ARP packets in a specific VLAN.

### Notes

- DAI cannot be enabled on DHCP Snooping trusted ports.

### Configuration Steps

#### ↳ Enabling ARP Packet Validity Check in a Specific VLAN

- Optional.
- Perform this configuration when you need to enable ARP packet validity check on all ports in a VLAN.
- Perform this configuration on Orion Alpha A28X access devices unless otherwise specified.

#### ↳ Configuring DAI Trusted Ports

- Optional.
- It is recommended to configure uplink ports as DAI trusted ports after DAI is enabled. Otherwise, the uplink ports enabled with other security features and set to trusted state accordingly may filter out valid ARP packets due to the absence of DAI user entries.
- Perform this configuration on Orion Alpha A28X access devices unless otherwise specified.

#### ↳ Configuring the ARP Packet Reception Rate

- For details, see the rate limit command description in the *Configuring the NFPP*.

### Verification

- Construct invalid ARP packets by using a packet transfer tool and check whether the packets are filtered out on DAI-enabled devices.
- Run the **show** command to check the device configuration.

### Related Commands

#### ↳ Enabling DAI

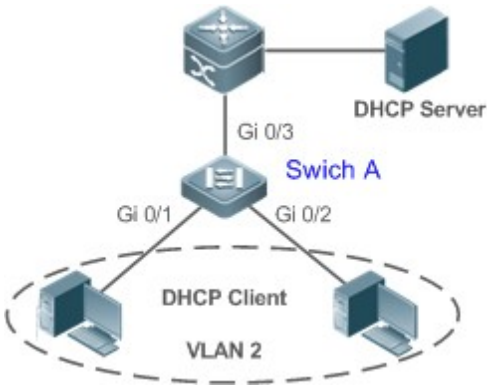
|                     |   |
|---------------------|---|
| <b>Command</b>      | <b>ip arp inspection vlan</b> { <i>vlan-id</i>   <i>word</i> }              |
| <b>Parameter</b>    | <i>vlan-id</i> : Indicates a VLAN ID.                                       |
| <b>Description</b>  | <i>word</i> : Indicates the VLAN range string, such as 1, 3–5, 7, and 9–11. |
| <b>Command Mode</b> | Global configuration mode   |
| <b>Usage Guide</b>  | N/A   |

#### ↳ Configuring DAI Trusted Ports

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>ip arp inspection trust</b>   |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Interface configuration mode   |
| <b>Usage Guide</b>           | Use this command to configure a DAI trusted port so that the ARP packets received by the port can pass through without validity check. |

## Configuration Example

### ↳ Allowing Users' PCs to Use only Addresses Allocated by a DHCP Server to Prevent ARP Spoofing

|   |   |
|---|---|
| <p><b>Scenario</b><br/>Figure 17-61</p> |    |
| <p><b>Configuration Steps</b></p>       | <ul style="list-style-type: none"> <li>● Enable DHCP Snooping on the access switch (Switch A) and configure its uplink port (GigabitEthernet 0/3) connected to the valid DHCP server as a trusted port.</li> <li>● Enable IP Source Guard on Switch A.</li> <li>● Enable DAI.</li> </ul>  |
| <p><b>Switch A</b></p>                  | <pre>A#configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)#vlan 2 A(config-vlan)#exit A(config)#interface range gigabitEthernet 0/1-2 A(config-if-range)#switchport access vlan 2 A(config-if-range)#ip verify source A(config-if-range)#exit A(config)#ip dhcp snooping A(config)#ip arp inspection vlan 2 A(config)#interface gigabitEthernet 0/3</pre> |

|                     |  |
|---------------------|--|
|                     | <pre>A(config-if-GigabitEthernet 0/3)#switchport access vlan 2 A(config-if-GigabitEthernet 0/3)#ip dhcp snooping trust A(config-if-GigabitEthernet 0/3)#ip arp inspection trust</pre>  |
| <b>Verification</b> | <ul style="list-style-type: none"> <li>● Check whether DHCP Snooping, IP Source Guard, and DAI are enabled and whether trusted ports are configured correctly.</li> <li>● Check whether the uplink port on Switch A is a DHCP Snooping trusted port.</li> <li>● Check whether DAI is enabled successfully in the VLAN and the uplink ports are DAI trusted ports.</li> </ul> |
| <b>Switch A</b>     | <pre>A#show running-config A#show ip dhcp snooping A#show ip arp inspection vlan</pre>   |

### Common Errors

- A port with security control enabled is configured as a DAI trusted port.

## 13.5 Monitoring

### Displaying

| Description  | Command   |
|--|---|
| Displays the DAI state of a specific VLAN.                 | <b>show ip arp inspection vlan</b> [ <i>vlan-id</i>   <i>word</i> ] |
| Displays the DAI configuration state of each Layer-2 port. | <b>show ip arp inspection interface</b>                             |

# 14 Configuring IP Source Guard

## 14.1 Overview

- The IP Source Guard function realizes hardware-based IP packet filtering to ensure that only the users having their information in the binding database can access networks normally, preventing users from forging IP packets.

## 14.2 Applications

| Application   | Description  |
|---|--|
| <a href="#">Guarding Against IP/MAC Spoofing Attack</a> | In network environments, users set illegal IP addresses and malicious users launch attacks through forging IP packets. |

### 14.2.1 Guarding Against IP/MAC Spoofing Attack

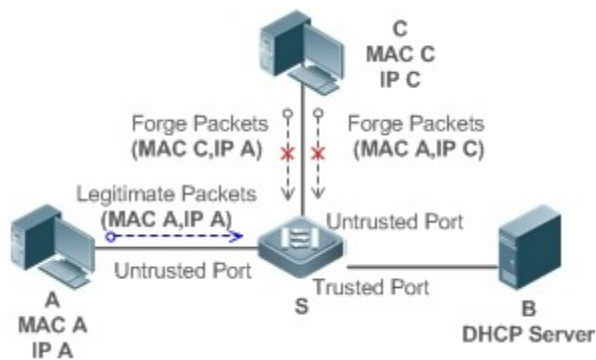
#### Scenario

Check the IP packets from DHCP untrusted ports. Forged IP packets will be filtered out based on the IP or IP-MAC field.

For example, in the following figure, the IP packets sent by DHCP clients are checked.

- The Source IP Address fields of IP packets should match DHCP-assigned IP addresses.
- The Source MAC Address fields of layer-2 packets should match the MAC addresses in DHCP request packets from clients.

Figure 18-16



**Remarks:** S is a network access server (NAS).  
A and C are user PCs.  
B is a DHCP server within the control area.

#### Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.

- Set all downlink ports on S as DHCP untrusted ports.
- Enable IP Source Guard on S to realize IP packet filtering.
- Enable IP-MAC match mode for IP Source Guard on S, filtering IP packets based on IP and MAC addresses.

## 14.3 Features

### Basic Concepts

#### ↳ Source IP Address

Indicate the source IP address field of an IP packet.

#### ↳ Source MAC Address

Indicate the source MAC address field of an IP packet.

#### ↳ IP-based Filtering

Indicate a policy of IP packet filtering, where only the source IP addresses of all IP packets (except DHCP packets) passing through a port are checked. It is the default filtering policy of IP Source Guard.

#### ↳ IP-MAC based Filtering

A policy of IP packet filtering, where both the source IP addresses and source MAC addresses of all IP packets are checked, and only those user packets with these IP addresses and MAC addresses existing in the binding database are permitted.

#### ↳ Address Binding Database

As the basis of security control of the IP Source Guard function, the data in the address binding database comes from two ways: the DHCP Snooping binding database and static configuration. When IP Source Guard is enabled, the data of the DHCP Snooping binding database is synchronized to the address binding database of IP Source Guard, so that IP packets can be filtered strictly through IP Source Guard on a device with DHCP Snooping enabled.

#### ↳ Excluded VLAN

By default, when IP Source Guard is enabled on a port, it is effective to all the VLANs under the port. Users may specify excluded VLANs, within which IP packets are not checked and filtered, which means that such IP packets are not controlled by IP Source Guard. At most 32 excluded VLANs can be specified for a port.

### Overview

| Feature   | Description  |
|---|--|
| <a href="#">Checking Source Address Fields of Packets</a> | Filter the IP packets passing through ports by IP-based or IP-MAC based filtering. |

## 14.3.1 Checking Source Address Fields of Packets

Filter the IP packets passing through ports based on source IP addresses or on both source IP addresses and source MAC addresses to prevent malicious attack by forging packets. When there is no need to check and filter IP packets within a VLAN, an excluded VLAN can be specified to release such packets.

### Working Principle

When IP Source Guard is enabled, the source addresses of packets passing through a port will be checked. The port can be a wired switching port, a layer-2 aggregate port (AP), or a layer-2 encapsulation sub-interface. Such packets will pass the port only when the source address fields of the packets match the set of the address binding records generated by DHCP Snooping, or the static configuration set by the administrator. There are two matching modes as below.

#### ↳ IP-based Filtering

Packets are allowed to pass a port only if the source IP address fields of them belong to the address binding database.

#### ↳ IP-MAC Based Filtering

Packets are allowed to pass a port only when both the layer-2 source MAC addresses and layer-3 source IP addresses of them match an entry in the address binding database.

#### ↳ Specifying Excluded VLAN

Packets within such a VLAN are allowed to pass a port without check or filtering.

### Related Configuration

#### ↳ Enabling IP Source Guard on a Port

By default, the IP Source Guard is disabled on ports.

It can be enabled using the **ip verify source** command.

- Usually IP Source Guard needs to work with DHCP Snooping. Therefore, DHCP Snooping should also be enabled. DHCP Snooping can be enabled at any time on Orion Alpha A28X devices, either before or after IP Source Guard is enabled.

#### ↳ Configuring a Static Binding

By default, legal users passing IP Source Guard check are all from the binding database of DHCP Snooping.

Bound users can be added using the **ip source binding** command.

#### ↳ Specifying an Excluded VLAN

By default, IP Source Guard is effective to all the VLANs under a port.

Excluded VLANs may be specified which are exempted from IP Source Guard using the **ip verify source exclude-vlan** command.

---



- Excluded VLANs can be specified only after IP Source Guard is enabled on a port. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on a port.
- The above-mentioned port can be a wired switching port, a layer-2 AP port or a layer-2 encapsulation sub-interface.

## 14.4 Configuration

| Configuration                               | Description and Command                             |   |
|---|---|---|
| <a href="#">Configuring IP Source Guard</a> | ● (Mandatory) It is used to enable IP Source Guard. |   |
|   | <b>ip verify source</b>                             | Enables IP Source Guard on a port.              |
|   | <b>ip source binding</b>                            | Configures a static binding.                    |
|   | <b>ip verify source exclude-vlan</b>                | Specifies an excluded VLAN for IP Source Guard. |

### 14.4.1 Configuring IP Source Guard

#### Configuration Effect

- Check the source IP addresses of input IP packets.

#### Notes

- When IP Source Guard is enabled, IP packets forwarding may be affected. In general case, IP Source Guard is enabled together with DHCP Snooping.
- IP Source Guard cannot be configured on the trusted ports controlled by DHCP Snooping.
- IP Source Guard cannot be configured on the global IP+MAC exclusive ports.
- IP Source Guard can be configured and enabled only on wired switch ports, Layer-2 AP ports and Layer-2 encapsulation sub-ports. In a wired access scenario, it is supposed to be configured in the interface configuration mode.

#### Configuration Steps

- Enable DHCP Snooping.
- Enable IP Source Guard.

#### Verification

Use the monitoring commands to display the address binding database of IP Source Guard.

#### Related Commands

##### ↳ Enabling IP Source Guard on a Port

|                  |   |
|------------------|---|
| <b>Command</b>   | <b>ip verify source [port-security]</b>               |
| <b>Parameter</b> | <b>port-security</b> : Enable IP-MAC based filtering. |

|                    |   |
|--------------------|---|
| <b>Description</b> |   |
| <b>Command</b>     | Interface configuration mode  |
| <b>Usage Guide</b> | Detection of users based on IP address or both IP and MAC addresses can be realized by enabling IP Source Guard for a port. |

### ↘ [Configuring a Static Binding](#)

|                              |  |
|------------------------------|--|
| <b>Command</b>               | <b>ip source binding</b> <i>mac-address</i> { <b>vlan</b> <i>vlan-id</i> } <i>ip-address</i> { <b>interface</b> <i>interface-id</i>   <b>ip-mac</b>   <b>ip-only</b> }   |
| <b>Parameter Description</b> | <i>mac-address</i> : The MAC address of a static binding<br><i>vlan-id</i> : The VLAN ID of a static binding. It indicates the outer VLAN ID of a QINQ-termination user.<br><b>ip-address</b> : The IP address of a static binding<br><i>interface-id</i> : The Port ID (PID) of a static binding<br><b>ip-mac</b> : IP-MAC based mode<br><b>ip-only</b> : IP-based mode |
| <b>Configuration Mode</b>    | Global configuration mode  |
| <b>Usage Guide</b>           | Through this command, legitimate users can pass IP Source Guard detection instead of being controlled by DHCP.   |

### ↘ [Specifying an Exception VLAN for IP Source Guard](#)

|                              |   |
|------------------------------|---|
| <b>Command</b>               | <b>ip verify source exclude-vlan</b> <i>vlan-id</i>   |
| <b>Parameter Description</b> | <b>vlan-id</b> : A VLAN ID exempted from IP Source Guard on a port  |
| <b>Command</b>               | Interface configuration mode  |
| <b>Usage Guide</b>           | By using this command, the specified VLANs under a port where IP Source Guard function is enabled can be exempted from check and filtering. |

## Configuration Example

### ↘ [Enabling IP Source Guard on Port 1](#)

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable DHCP Snooping.</li> <li>● Enable IP Source Guard.</li> </ul>  |
|                            | <pre>Orion Alpha A28X(config)# interface GigabitEthernet 0/1 Orion Alpha A28X(config-if-GigabitEthernet 0/1)# ip verify source Orion Alpha A28X(config-if-GigabitEthernet 0/1)# end</pre> |
| <b>Verification</b>        | Displays the address filtering table of IP Source Guard.  |
|                            | <pre>Orion Alpha A28X# show ip verify source</pre>  |

### ↘ [Configuring a Static Binding](#)

| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable DHCP Snooping.</li> <li>● Enable IP Source Guard.</li> <li>● Configure a static binding.</li> </ul>   |            |                       |               |                |           |            |      |      |   |                     |       |                       |               |                |   |        |   |                     |         |        |          |  |  |  |
|----------------------------|---|------------|-----------------------|---------------|----------------|-----------|------------|------|------|---|---------------------|-------|-----------------------|---------------|----------------|---|--------|---|---------------------|---------|--------|----------|--|--|--|
|                            | <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface GigabitEthernet 0/3 Orion Alpha A28X(config)# end</pre>   |            |                       |               |                |           |            |      |      |   |                     |       |                       |               |                |   |        |   |                     |         |        |          |  |  |  |
| <b>Verification</b>        | Displays the address filtering table of IP Source Guard.  |            |                       |               |                |           |            |      |      |   |                     |       |                       |               |                |   |        |   |                     |         |        |          |  |  |  |
|                            | <pre>Orion Alpha A28X# show ip verify source</pre> <table border="1"> <thead> <tr> <th>NO.</th> <th>INTERFACE</th> <th>FilterType</th> <th>FilterStatus</th> <th>IPADDRESS</th> <th>MACADDRESS</th> <th>VLAN</th> <th>TYPE</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>GigabitEthernet 0/3</td> <td>UNSET</td> <td>Inactive-restrict-off</td> <td>192.168.4.243</td> <td>00d0.f801.0101</td> <td>1</td> <td>Static</td> </tr> <tr> <td>2</td> <td>GigabitEthernet 0/1</td> <td>IP-ONLY</td> <td>Active</td> <td>Deny-All</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> | NO.        | INTERFACE             | FilterType    | FilterStatus   | IPADDRESS | MACADDRESS | VLAN | TYPE | 1 | GigabitEthernet 0/3 | UNSET | Inactive-restrict-off | 192.168.4.243 | 00d0.f801.0101 | 1 | Static | 2 | GigabitEthernet 0/1 | IP-ONLY | Active | Deny-All |  |  |  |
| NO.                        | INTERFACE   | FilterType | FilterStatus          | IPADDRESS     | MACADDRESS     | VLAN      | TYPE       |      |      |   |                     |       |                       |               |                |   |        |   |                     |         |        |          |  |  |  |
| 1                          | GigabitEthernet 0/3   | UNSET      | Inactive-restrict-off | 192.168.4.243 | 00d0.f801.0101 | 1         | Static     |      |      |   |                     |       |                       |               |                |   |        |   |                     |         |        |          |  |  |  |
| 2                          | GigabitEthernet 0/1   | IP-ONLY    | Active                | Deny-All      |                |           |            |      |      |   |                     |       |                       |               |                |   |        |   |                     |         |        |          |  |  |  |

### ↘ Specifying an Excluded VLAN

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable DHCP Snooping.</li> <li>● Enable IP Source Guard.</li> </ul>   |
|                            | <pre>Orion Alpha A28X(config)# interface GigabitEthernet 0/1 Orion Alpha A28X(config-if-GigabitEthernet 0/1)# ip verify source Orion Alpha A28X(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1 Orion Alpha A28X(config-if)# end</pre> |
| <b>Verification</b>        | Display the configuration of excluded VLANs specified on a port.   |
|                            | <pre>Orion Alpha A28X# show run</pre>  |

### Common Errors

- Enable IP Source Guard on a trusted port under DHCP Snooping.
- Specify an excluded VLAN before IP Source Guard is enabled.

## 14.5 Monitoring

### Displaying

| Description | Command |
|-------------|---------|
|-------------|---------|

|   |   |
|---|---|
| Displays the address filtering table of IP Source Guard.  | <b>show ip verify source</b> [ <b>interface</b> <i>interface-id</i> ] |
| Displays the address binding database of IP Source Guard. | <b>show ip source binding</b>   |

---

# 15 Configuring DoS Protection

## 15.1 Overview

Denial of Service (DoS) attacks refer to attacks that cause DoS and aim to put computers or networks out of service.

DoS attacks are diversified in types and can be implemented in many ways, but have one common purpose, that is, prevent victim hosts or networks cannot receive, respond, or process external requests in time. In particular, on a layer-2 (L-2) network, DoS attack packets can be spread in the entire broadcast domain. If hackers maliciously initiate DoS attacks, some operating systems (OSs) may collapse. Orion Alpha A28X products supports the following anti DoS attack functions:

- Denying land attacks
- Denying invalid TCP packets
- Denying invalid layer-4 (L4) ports

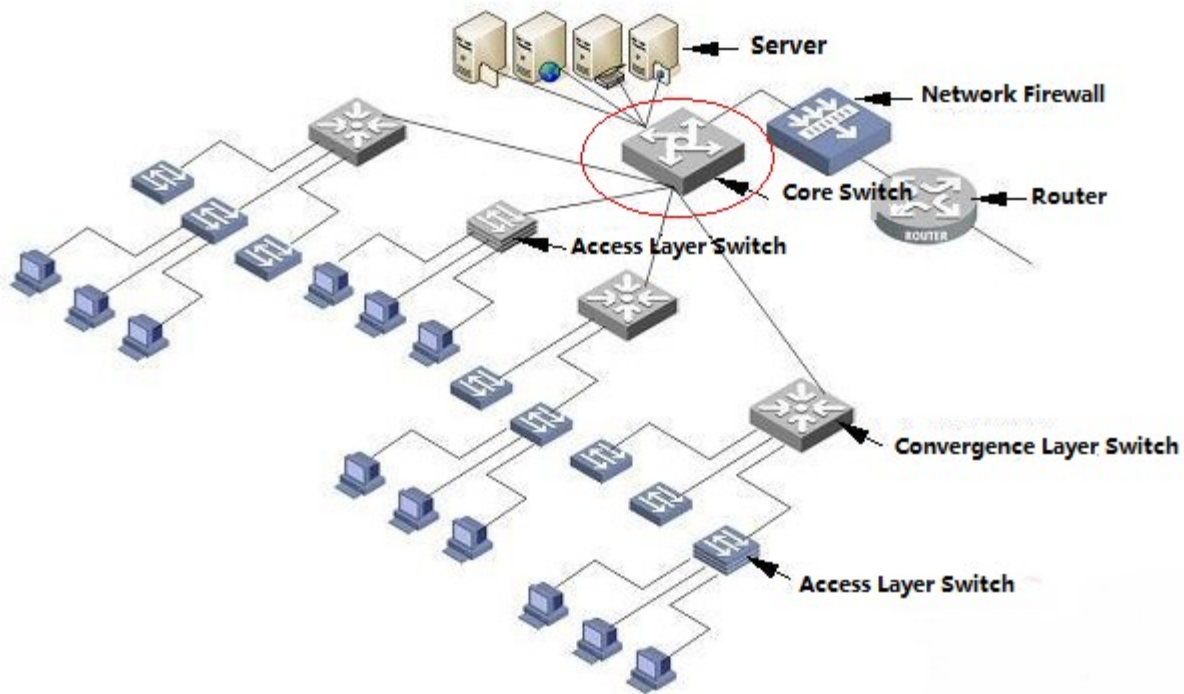
## 15.2 Applications

| Application  | Description   |
|--|---|
| <a href="#">Protecting Servers Against DoS Attacks</a> | On a campus network, configure the anti DoS attack function on the devices connected to servers to effectively reduce the negative impacts brought by DoS attacks to servers. |

### 15.2.1 Protecting Servers Against DoS Attacks

As show inFigure 22-62, servers are connected to the core switch. The anti DoS attack function is configured on the core switch to prevent malicious DoS attacks and ensure that servers can provide services normally.

Figure 22-62



## Deployment

Enable the function of denying land attacks on the core switch to protect servers against land attacks.

Enable the function of denying invalid TCP packets on the core switch to protect servers against invalid TCP packets.

Enable the function of denying invalid L4 ports on the core switch to protect servers against attacks caused by invalid L4 ports.

## 15.3 Features

### Overview

| Feature                                     | Description   |
|---|---|
| <a href="#">Denying Land Attacks</a>        | Drop packets with the same source and destination IP addresses or the same L4 source and destination port IDs on the device to prevent these packets from attacking OSs on the network.               |
| <a href="#">Denying Invalid TCP Packets</a> | Drop invalid TCP packets on the device to prevent invalid TCP packets from attacking OSs on the network. (For details about the definition of invalid TCP packets, see "Denying Invalid TCP Packets". |
| <a href="#">Denying Invalid L4 Ports</a>    | Drop packets with the same L4 source and destination port IDs on the device to prevent these packets from attacking OSs on the network.   |

### 15.3.1 Denying Land Attacks

This function protects servers against land attacks.

## Working Principle

In a land attack, the attacker sets the source and destination IP addresses or the L4 source and destination port IDs in a SYN packet to the same address of the target host. Consequently, the attacked host will be trapped in an infinite loop or even collapse when attempting to set up a TCP connection with itself.

If the function of denying land attacks is enabled, the device checks packets based on characteristics of land packets (that is, SYN packets with the same source and destination IP addresses), and drops invalid packets.

## Related Configuration

### ↳ Enabling the Function of Denying Land Attacks

By default, the function of denying land attacks is disabled.

Run the **ip deny land** command to enable or disable the function of denying land attacks.

## 15.3.2 Denying Invalid TCP Packets

This function protects servers against invalid TCP packets.

### Working Principle

There are several flag fields in the TCP packet header:

- SYN: Connection establishment flag. The TCP SYN packet is used to set this flag to 1 to request establishment of a connection.
- ACK: Acknowledgement flag. In a TCP connection, this field must be available in every flag (except the first packet, that is, the TCP SYN packet) as the acknowledgement of the previous packet.
- FIN: Finish flag. When a host receives the TCP packet with the FIN flag, the host disconnects the TCP connection.
- RST: Reset flag. When the IP protocol stack receives a TCP packet that contains a non-existent destination port, it responds with a packet with the RST flag.
- PSH: This flag notifies the protocol stack to submit TCP data to the upper-layer program for processing as soon as possible.

In invalid TCP packets, flag fields are set improperly so that the processing resources of hosts are exhausted or even the system collapses. The following lists several common methods for setting flag fields in invalid TCP packets:

- TCP packets with both the SYN and FIN flags

Normally, a TCP packet cannot contain both the SYN and FIN flags. In addition, RFC does not stipulate how the IP protocol stack should process such invalid packets containing both the SYN and FIN flags. Therefore, the protocol stack of each OS may process such packets in different ways when receiving these packets. Attackers can use this feature to send packets containing both the SYN and FIN flags to identify the OS type and initiate attacks on this OS.

- TCP packets without any flag

Normally, a TCP packet contains at least one of the five flags, including SYN, FIN, ACK, RST, and PSH. The first TCP packet (TCP SYN packet) must contain the SYN flag, and the subsequent packets contain the ACK flag. Based on such assumptions, some protocol stack does not specify the method for processing TCP packets without any flag,

---

and therefore may collapse if such protocol stack receives TCP packets without any flag. Attackers use this feature to initiate attacks on target hosts.

- TCP packets with the FIN flag but without the ACK flag

Normally, except the first packet (TCP SYN packet), all other packets, including the packets with the FIN flag, contain the ACK flag. Some attackers may send TCP packets with the FIN flag but without the ACK flag to the target hosts, causing breakdown of the target hosts.

- TCP packets with the SYN flag and the source port ID set to a value between 0 and 1,023

Port IDs 0 to 1,023 are known port IDs allocated by the Internet Assigned Numbers Authority (IANA). In most systems, these port IDs can be used only by the system (or root) processes or programs run by privileged users. These ports (0–1023) cannot be used as the source port IDs in the first TCP packets (with the SYN flag) sent by clients.

If the function of denying invalid TCP packets is enabled, the device checks packets based on characteristics of invalid TCP packets, and drops invalid TCP packets.

## Related Configuration

### ↳ Enabling the Function of Denying Invalid TCP Packets

By default, the function of denying invalid TCP packets is disabled.

Run the **ip deny invalid-tcp** command to enable or disable the function of denying invalid TCP packets.

## 15.3.3 Denying Invalid L4 Ports

This function protects servers against invalid L4 ports.

### Working Principle

Attackers sends packets in which the IP address of the target host is the same as the L4 port ID of the host to the host target. As a result, the target host sends TCP connection setup requests to itself. Under such attacks, resources of the target host will soon be exhausted and the system will collapse.

If the function of denying invalid L4 ports is enabled, the device checks the L4 source port ID and destination port ID in the packets. If they are the same, the device drops the packets.

## Related Configuration

### ↳ Enabling the Function of Denying Invalid L4 Ports

By default, the function of denying invalid L4 ports is disabled.

Run the **ip deny invalid-l4port** command to enable or disable the function of denying invalid L4 ports.

## 15.4 Configuration

| Configuration Item | Description and Command                                     |
|--------------------|---|
|                    | <ul style="list-style-type: none"><li>● Optional.</li></ul> |



|   |                               |  |
|---|-------------------------------|--|
| <a href="#">Configuring the Function of Denying Land Attacks</a>        | <b>ip deny land</b>           | Enables the function of denying land attacks.        |
| <a href="#">Configuring the Function of Denying Invalid TCP Packets</a> | ● Optional.                   |  |
|   | <b>ipdeny invalid-tcp</b>     | Enables the function of denying invalid TCP packets. |
| <a href="#">Configuring the Function of Denying Invalid L4 Ports</a>    | ● Optional.                   |  |
|   | <b>ip deny invalid-l4port</b> | Enables the function of denying invalid L4 ports.    |

## 15.4.1 Configuring the Function of Denying Land Attacks

### Configuration Effect

Enable the function of denying land attacks. Then, the device checks packets based on characteristics of land packets, and drops land packets.

### Configuration Steps

#### ↳ Enabling the Function of Denying Land Attacks

- Mandatory.
- Perform this configuration on a device connected to a server.

### Verification

- Run the **showipdenyland** command to display the status of the function of denying land attacks.
- After this function is enabled, construct a land attack packet and confirm that this packet cannot be forwarded.

### Related Commands

#### ↳ Configuring the Function of Denying Land Attacks

|                     |                           |
|---------------------|---------------------------|
| <b>Command</b>      | <b>[no] ip deny land</b>  |
| <b>Parameter</b>    | N/A                       |
| <b>Description</b>  |                           |
| <b>Command Mode</b> | Global configuration mode |
| <b>Usage Guide</b>  | N/A                       |

### Configuration Example

#### ↳ Enabling the Function of Denying Land Attacks

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>● Enable the function of denying land attacks in global configuration mode.</li> </ul> |
|                            | Orion Alpha A28X# configure terminal  |

|                     |   |
|---------------------|---|
|                     | <pre>Orion Alpha A28X(config)# ip deny land Orion Alpha A28X(config)# end</pre>   |
| <b>Verification</b> | <p>Run the <b>showipdenyland</b> command to display the status of the function of denying land attacks.</p> <p>The following example shows how to display the status of the function of denying land attacks:</p> <pre>Orion Alpha A28X#show ip deny land  DoS Protection Mode      State ----- protect against land attack  On</pre> |

## 15.4.2 Configuring the Function of Denying Invalid TCP Packets

### Configuration Effect

Enable the function of denying invalid TCP packets. Then, the device checks packets based on characteristics of invalid TCP packets, and drops invalid TCP packets.

### Configuration Steps

#### ↳ Enables the Function of Denying Invalid TCP Packets

- Mandatory.
- Perform this configuration on a device connected to a server.

### Verification

- Run the **show ip deny invalid-tcp** command to display the status of the function of denying invalid TCP packets.
- After this function is enabled, construct an invalid TCP packet and confirm that this packet cannot be forwarded.

### Related Commands

#### ↳ Configuring the Function of Denying Invalid TCP Packets

|                              |                                 |
|------------------------------|---------------------------------|
| <b>Command</b>               | <b>[no] ip deny invalid-tcp</b> |
| <b>Parameter Description</b> | N/A                             |
| <b>Command Mode</b>          | Global configuration mode       |
| <b>Usage Guide</b>           | N/A                             |

## Configuration Example

### ↳ Enabling the Function of Denying Invalid TCP Packets

|                            |  |
|----------------------------|--|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"><li>● Enable the function of denying invalid TCP packets in global configuration mode.</li></ul> <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ip deny invalid-tcp Orion Alpha A28X(config)# end</pre>   |
| <b>Verification</b>        | Run the <b>show ip deny invalid-tcp</b> command to display the status of the function of denying invalid TCP packets.<br><br>The following example shows how to display the status of the function of denying invalid TCP packets:<br><pre>Orion Alpha A28X#show ip deny invalid-tcp       DoS Protection Mode      State ----- protect against invalid tcp attack  On</pre> |

## 15.4.3 Configuring the Function of Denying Invalid L4 Ports

### Configuration Effect

Enable the function of denying invalid L4 ports. Then, the device checks the L4 source port ID and destination port ID in the packets. If they are the same, the device drops the packets.

### Configuration Steps

#### ↳ Enabling the Function of Denying Invalid L4 Ports

- Mandatory.
- Perform this configuration on a device connected to a server.

### Verification

- Run the **show ip deny invalid-l4port** command to display the status of the function of denying invalid L4 ports.
- After this function is enabled, construct a packet in which the L4 source port ID is the same as the destination port ID and confirm that this packet cannot be forwarded.

### Related Commands

#### ↳ Configuring the Function of Denying Invalid L4 Ports

|                    |                                    |
|--------------------|------------------------------------|
| <b>Command</b>     | <b>[no] ip deny invalid-l4port</b> |
| <b>Parameter</b>   | N/A                                |
| <b>Description</b> |                                    |

|                     |                           |
|---------------------|---------------------------|
| <b>Command Mode</b> | Global configuration mode |
| <b>Usage Guide</b>  | N/A                       |

## Configuration Example

### ↳ Enabling the Function of Denying Invalid L4 Ports

|                            |   |
|----------------------------|---|
| <b>Configuration Steps</b> | <ul style="list-style-type: none"> <li>Enable the function of denying invalid L4 ports in global configuration mode.</li> </ul>   |
|                            | <pre>Orion Alpha A28X# configure terminal Orion Alpha A28X(config)# ip deny invalid-l4port Orion Alpha A28X(config)# end</pre>  |
| <b>Verification</b>        | <p>Run the <b>show ip deny invalid-l4port</b> command to display the status of the function of denying invalid L4 ports.</p> <p>The following example shows how to display the status of the function of denying invalid L4 ports:</p> <pre>Orion Alpha A28X#show ip deny invalid-l4port  DoS Protection Mode      State ----- protect against invalid l4port attack On</pre> |

## 15.5 Monitoring

### Displaying

| Description   | Command                            |
|---|------------------------------------|
| Displays the status of the function of denying land attacks.        | <b>show ip deny land</b>           |
| Displays the status of the function of denying invalid TCP packets. | <b>show ip deny invalid-tcp</b>    |
| Displays the status of the function of denying invalid L4 ports.    | <b>show ip deny invalid-l4port</b> |
| Displays the status of all antiDoS attack functions.                | <b>show ip deny</b>                |

# 16 Configuring PPPoE Intermediate Agent

## 16.1 Overview

As the technology of broadband access becomes more mature, the broadband access network development. Under this background, security issues have been brought to the center of public attention, because users and devices accessing the network or the network itself are facing many threats, especially those from clients. In a traditional Ethernet, users can not be identified, traced and located, while the identification and location of users are the basic features and requirements in an open and manageable network for public use. PPPoE Intermediate Agent can offer these functions to prevent the use accounts from being stolen as an APP requires users to log in with accounts.

The working process of PPPoE protocol can be divided into two different stages: PPPoE discovery and PPPoE session. In the former stage, the protocol helps to get the MAC address of a remote server so as to build a point-to-point connection, and to establish a session ID used for communication in the session stage. In this chapter, we will briefly introduce the PPPoE discovery stage because PPPoE Intermediate Agent is only involved in this stage.

PPPoE protocol includes four steps:

1. A host sends a PPPoE Active Discovery Initiation (PADI) packet. The client regards the broadcast address as a destination address to broadcast PADI packet in order to discover the access concentrators in layer 2 network.

Please note that the packet might be sent to several access concentrators.

2. An access concentrator responses a PPPoE Active Discovery Offer (PADO) packet. According to the source MAC address received, the server will response the PADO packet that contains the names of the access concentrator and services.

3. The host sends a PPPoE Active Discovery Request (PADR) packet. With the PADO packet received, the client selects one access concentrator based on its requested services and the information contained in the PADO packet. As the access concentrator has been selected, the client can get the MAC address of the remote peer and send PADR packet for requesting a session with the access concentrator.

4. The selected access concentrator responses the PPPoE Active Discovery Session-confirmation (PADS) packet. With the PADR packet received, the client establishes a session ID and sent this ID to the client via packet

for session. As both the client and server get the session ID, the PPPoE discovery stage is over.

PPPoE Active Discovery Terminate (PADT) is a special packet of PPPoE protocol, which shares the same Ethernet protocol number 0x8863 with the above four packets, thus can be regarded as a packet in PPPoE discovery stage. However, the packet, mainly used to terminate a session, can be sent at any time after the PPPoE session stage starts. It can be sent by a host or an access concentrator.

PPPoE Intermediate Agent (PPPoE IA) provides a function of identifying and locating users. Its work principle is to tag the PADI and PADR packets sent by the host of a client with the access link of the device as the device accesses the network in the stage of PPPoE discovery so that the server (usually refers to BRAS) can accurately identify and locate users. If the access device is LAN Switch, the information added to the PPPoE packets includes the MAC address of the access switch, slot ID, port index and VLAN ID. The realization of PPPoE IA depends on the Migration to Ethernet-based DSL aggregation of DSL Forum Technical Report 101.

## 16.2 Applications

| Application              | Description   |
|--------------------------|---|
| <a href="#">PPPoE IA</a> | Both the host and server run PPPoE protocol and connect with each other through Layer 2 Ethernet. The PPPoE IA is enabled on the switch directly connected to the host. |

### 16.2.1 PPPoE IA Scenario

#### Scenario



The figure shown above is a typical PPPoE IA application topology: the switch processes the PADI and PADR packets sent by the PC and tags these packets with access link.

#### Deployment

- Enable the function of PPPoE IA on the switch globally.
- Enable the function of PPPoE IA on the Gi 0/1 port of the switch and configure the Gi 0/2 port connected to the server as a trusted port.
- Tag the Gi 0/1 port with customized access link.

## 16.3 Features

### Basic Concepts

Process PADI and PADR packets sent by users and add a circuit-id and a remote-id to the packets so as to identify and locate users.

#### PPPoE Packet Format

Ethernet II Frame Format

|                         |                    |            |            |     |
|-------------------------|--------------------|------------|------------|-----|
| Destination Mac Address | Source MAC address | Type Field | PPPoE data | CRC |
|-------------------------|--------------------|------------|------------|-----|

PPPoE Data

|         |      |      |            |              |       |     |       |
|---------|------|------|------------|--------------|-------|-----|-------|
| Version | Type | Code | Session ID | Length Field | TLV 1 | ... | TLV N |
|---------|------|------|------------|--------------|-------|-----|-------|

TLC Structure

|      |        |      |
|------|--------|------|
| Type | Length | Data |
|------|--------|------|

The meanings of above fields are as follows:

Type field of Ethernet frame (2 bytes): according to the Ethernet protocol, five packets involved in discovery stage share the same value of type field of 0x8863, while the value of packets in PPPoE session stage is 0x8864.

Version field of PPPoE (4 bits): indicates the current version of PPPoE protocol and configures 0x1 as its type field.

Code field of PPPoE (1 byte): indicates the types of PPPoE packets. 0x09 presents PADI packet; 0x07 presents PADO packet; 0x19 presents PADR packet; 0x65 presents PADS packet and 0xa7 presents PADT packet.

PPPoE session ID (2 bytes): indicates a session ID.

Length field of PPPoE (2 bytes): indicates all the length of TLV and the type field of TLV (2 bites). One TLV stands for one TAG and the type field presents TAG type. The length field of TLV in the following table indicates the length of the data field of TAG and the data field of TLV (varying in length) indicates the transmitted data of the TAG.

| Type   | Description   |
|--------|---|
| 0x0000 | Refers to the end of a series of tags in the data field of PPPoE packets. But some flags application in order to ensure version compatibility.  |
| 0x0101 | The name of a service. Indicates the service that can be offered by the network to users.   |
| 0x0102 | The name of an access concentrator. As the client receives the PADO packet responded by AC, it can gain the name of access concentrator from the tag contained in the packet. Based on the name, it can select the related access concentrator.   |
| 0x0103 | The only tag of the host. Being similar with the identify field in the data packets of PPP, it is mainly used to match the sending end and the receiving end, because several PPPoE data packets exist in the broadcast network at the same time. |
| 0x0104 | AC-Cookies. It is mainly used to prevent malicious DoS attack.  |
| 0x0105 | The identifier of vendor  |
| 0x0110 | Intermediate session ID. Like the data packets of DHCP, the data packets of PPPoE can also be intercepted and terminated in another AC. This field aims to maintain another connection.   |
| 0x0201 | The error name of a service. As the requested service name is rejected by the end, this tag will be contained in the response packet.   |
| 0x0202 | The error name of an access concentrator.   |
| 0x0203 | A common error.   |

Figure 16-1 The Type of TAG in PPPoE

### ↳ PPPoE Request Packets

The packets sent from a PPPoE client to a PPPoE server, including PADI and PADR packets.

### ↳ PPPoE Response Packets

The packets sent from a PPPoE server to a PPPoE client, including PADO and PADS packets.

### ↳ Trusted Ports of PPPoE Intermediate Agent

The port connected to a server is configured as a trusted port and the port connected to a client as a untrusted port so as to ensure the security and reduce the traffic generated in PPPoE IA. Trusted ports can receive the five packets mentioned above, while the untrusted ports only can receive the PADI, PADR and PADT packets sent from a server to client. For making the server run correctly, please configure the port connected to it as a trusted port and ensure that each access device has at least one trusted port.

### ↳ Strip Function

PPPoE IA vendor tag is not allowed to exist in the PPPoE packets sent from a server to a client. Therefore, if those packets contains it, you need to strip these vendor tags and then forward these packets. Strip function must be configured on trusted ports. If it is configured on untrusted ports, it would fail to take effect.

### ↳ Port-based PPPoE Intermediate Agent

The validity of PPPoE Intermediate Agent is based on ports. By default, this function is disabled. After being globally enabled, it can only become valid as it is enabled on ports.

### Overview

| Feature  | Description  |
|----------|--|
| PPPoE IA | Process the interactive PPPoE packets and forward legal request packets to trusted ports only. |

## 16.3.1 PPPoE IA

PPPoE IA provides a function of identifying and locating users.

### Working Principle

The following figure shows the structure of the designation of link added to PPPoE IA, which is the main function of PPPoE IA.

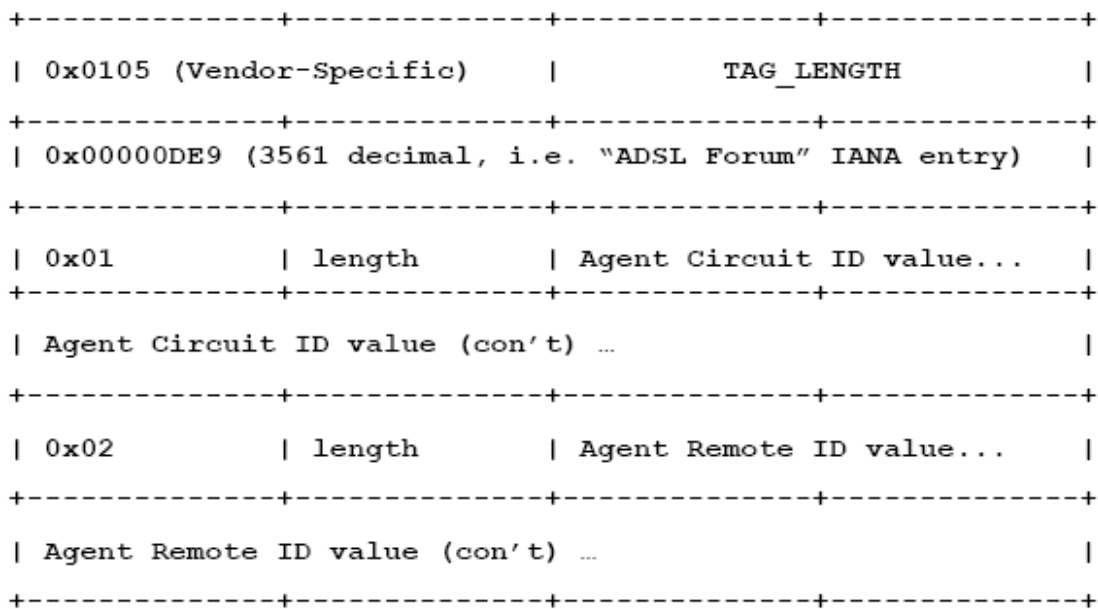


Figure 16-2 PPPoE IA Vendor-tag (four bits per line)

The type identifier of TLV added to PPPoE IA is 0x0105, and the TAG\_LENGTH refers to the length field of a vendor tag; 0x0000DE9 refers to "ADSL Forum" IANA entry fixed with 4 bytes; 0x01 refers to the type fields followed by its length and value; 0x02 refers to the type fields of Agent Remote ID followed by its length and value.



|                 |                   |                    |                   |                     |               |                           |   |          |                     |
|-----------------|-------------------|--------------------|-------------------|---------------------|---------------|---------------------------|---|----------|---------------------|
| ANI<br>(n byte) | Space<br>( 1byte) | eth<br>(3<br>byte) | Space<br>( 1byte) | Slot ID<br>( 2byte) | /<br>( 1byte) | Port<br>Index<br>( 3byte) | : | ( 1byte) | Vlan ID<br>( 4byte) |
|-----------------|-------------------|--------------------|-------------------|---------------------|---------------|---------------------------|---|----------|---------------------|

Figure 16-3 Agent Circuit ID Value

PPPoE IA provides a default circuit ID value shown as Figure 16-3. The circuit ID value consists of the Access Node Identifier (ANI), eth, slot ID, port index and VLAN ID. ANI with a length of less than 47 bits can be configured by users; if it is not configured, its value will be the MAC address (6 bytes) by default and separated with its following field by a space. The field "eth" with 3 bytes is also separated with its following field by a space. Slot ID with 2 bytes is separated with its following field by a "/" of 1 byte. Port index with 3 bytes is separated with others with a ":" of 1 byte. VLAN ID occupies 4 bytes. All the fields mentioned here are presented in ASCII code. In addition, you can also configure a circuit ID for each port based on your requirements. Orion Alpha A28X series switches do not support hexadecimal fields.

## Related Configuration

### Enabling PPPoE IA Globally

By default, this function is disabled.

Use **pppoe intermediate-agent** command to enable PPPoE IA on the device.

After being enabled globally, this function can be enabled on different ports.

The function must be enabled globally first, and then it can be allowed to be enabled on different ports.

### Enabling PPPoE IA on Ports

By default, after being enabled globally, this function becomes valid as it is enabled on ports.

Use **[ no ] pppoe intermediate-agent** command to enable or disable PPPoE IA on ports.

### Enabling PPPoE IA Trusted Ports

By default, PPPoE IA trusted ports is disabled on ports.

Use **pppoe intermediate-agent trust** command to enable PPPoE IA.

The PPPoE IA packets only can be forwarded as the PPPoE IA trusted ports are enabled on the ports connected to a server.

### Enabling the Strip Function of PPPoE IA Vendor Tag

By default, this function is disabled.

Use **pppoe intermediate-agent vendor-tag string** command to enable this function.

This function can be enabled on the port connected to a server.

## 16.4 Configuration

| Configuration                              | Description and Command   |  |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|--|---|--|--|--|---|--|---------------------------------------|--|--------------------------------------|---|---|--|---|--|-------------------------------------|---|------------------------------------|
| PPPoE IA                                   | <ul style="list-style-type: none"> <li>(Mandatory) It is used to establish PPPoE IA.</li> </ul>   |  |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <table border="1"> <tr> <td><b>pppoe intermediate-agent</b></td> <td>Enable PPPoE IA.</td> </tr> <tr> <td><b>pppoe intermediate-agent trust</b></td> <td>Configure a port as a trusted port.</td> </tr> </table>  | <b>pppoe intermediate-agent</b>  | Enable PPPoE IA.   | <b>pppoe intermediate-agent trust</b>                                    | Configure a port as a trusted port.               |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <b>pppoe intermediate-agent</b>   | Enable PPPoE IA.   |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <b>pppoe intermediate-agent trust</b>   | Configure a port as a trusted port.  |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <ul style="list-style-type: none"> <li>Optional.</li> </ul>   |  |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <table border="1"> <tr> <td><b>pppoe intermediate-agent type tr-101 circuit-id access-node-id</b></td> <td>Configure the value of access node id of circuit ID added to a vendor tag.</td> </tr> <tr> <td><b>pppoe intermediate-agent type tr-101 circuit-id identifier-string</b></td> <td>Configure the circuit-id of the added vendor tag.</td> </tr> <tr> <td><b>pppoe intermediate-agent type self-defined circuit-id</b></td> <td>Configure the format of a circuit-id.</td> </tr> <tr> <td><b>pppoe intermediate-agent type self-defined remoteid</b></td> <td>Configure the format of a remote-id.</td> </tr> <tr> <td><b>pppoe intermediate-agent delimiter</b></td> <td>Configure the separator among the fields of circuit-id and remote id.</td> </tr> <tr> <td><b>pppoe intermediate-agent vendor-tag strip</b></td> <td>Configure the vendor tag strip function of ports.</td> </tr> <tr> <td><b>pppoe intermediate-agent circuit-id</b></td> <td>Configure the circuit-id of a port.</td> </tr> <tr> <td><b>pppoe intermediate-agent remote-id</b></td> <td>Configure the remote-id of a port.</td> </tr> </table> | <b>pppoe intermediate-agent type tr-101 circuit-id access-node-id</b>      | Configure the value of access node id of circuit ID added to a vendor tag. | <b>pppoe intermediate-agent type tr-101 circuit-id identifier-string</b> | Configure the circuit-id of the added vendor tag. | <b>pppoe intermediate-agent type self-defined circuit-id</b> | Configure the format of a circuit-id. | <b>pppoe intermediate-agent type self-defined remoteid</b> | Configure the format of a remote-id. | <b>pppoe intermediate-agent delimiter</b> | Configure the separator among the fields of circuit-id and remote id. | <b>pppoe intermediate-agent vendor-tag strip</b> | Configure the vendor tag strip function of ports. | <b>pppoe intermediate-agent circuit-id</b> | Configure the circuit-id of a port. | <b>pppoe intermediate-agent remote-id</b> | Configure the remote-id of a port. |
|  | <b>pppoe intermediate-agent type tr-101 circuit-id access-node-id</b>   | Configure the value of access node id of circuit ID added to a vendor tag. |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <b>pppoe intermediate-agent type tr-101 circuit-id identifier-string</b>  | Configure the circuit-id of the added vendor tag.                          |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <b>pppoe intermediate-agent type self-defined circuit-id</b>  | Configure the format of a circuit-id.                                      |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <b>pppoe intermediate-agent type self-defined remoteid</b>  | Configure the format of a remote-id.                                       |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <b>pppoe intermediate-agent delimiter</b>   | Configure the separator among the fields of circuit-id and remote id.      |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
|  | <b>pppoe intermediate-agent vendor-tag strip</b>  | Configure the vendor tag strip function of ports.                          |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
| <b>pppoe intermediate-agent circuit-id</b> | Configure the circuit-id of a port.   |  |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |
| <b>pppoe intermediate-agent remote-id</b>  | Configure the remote-id of a port.  |  |  |  |   |  |                                       |  |                                      |   |   |  |   |  |                                     |   |                                    |

### 16.4.1 PPPoE IA

#### Configuration Effect

- Enable PPPoE IA.
- Add identifiers to the PPPoE packets of users.

#### Notes

- If you want to run pppoe intermediate-agent on the ports of switch, you must enable the function globally first, otherwise it is invalid to enable it on ports.
- Configure at least one trusted port to ensure it can be connected to the server.
- Vendor tag strip function must be configured on trusted ports.
- The priority order of the coverage of a circuit-id (1) pppoe intermediate-agent circuit-id (2) pppoe intermediate-agent identifier-string option delimiter; (3) pppoe intermediate-agent access-node-id.

#### Configuration Steps

##### ↳ Enabling PPPoE IA

- Mandatory
- Unless otherwise specified, this feature should be configured on an access device.

#### ↳ Enabling PPPoE IA Trusted Ports

- Mandatory
- Configure the port connected to a trusted PPPoE server as a trusted port.

#### ↳ Configuring the Format of Circuit-id

- Optional
- Unless otherwise specified, this feature should be enabled globally on access devices or ports.

#### ↳ Configuring the Format of Remote-id

- Optional
- Unless otherwise specified, this feature should be enable globally on an access device or a port.

#### ↳ Configuring Vendor Tag Strip Function on Ports

- Optional Unless otherwise specified, this feature should be enabled on a trusted port.

### Verification

- Access devices can process PPPoE packets normally.
- Clients and servers can interact with each other normally.

### Related Commands

#### ↳ Enabling or Disabling PPPoE IA

|                              |  |
|------------------------------|--|
| <b>Command</b>               | [ no ] pppoe intermediate-agent  |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode and port configuration mode  |
| <b>Usage Guide</b>           | If you want to run pppoe intermediate-agent on the ports of a switch, you must enable it globally first, otherwise it is invalid to enable this function on ports. |

#### ↳ Enabling PPPoE IA Trusted Ports

|                              |  |
|------------------------------|--|
| <b>Command</b>               | [ no ] pppoe intermediate-agent trust  |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Port configuration mode  |
| <b>Usage Guide</b>           | At least one port should be configured as a trusted port that can be connected to a server to copy and |

|  |                                       |
|--|---------------------------------------|
|  | forward the PPPoE packets of clients. |
|--|---------------------------------------|

#### ↘ Adding the Value of Access Node ID

|                              |  |
|------------------------------|--|
| <b>Command</b>               | [ no ] pppoe intermediate-agent type tr-101 circuit-id access-node-id <string> |
| <b>Parameter Description</b> | N/A  |
| <b>Command Mode</b>          | Global configuration mode  |
| <b>Usage Guide</b>           | Add the value of the access node id of the circuit ID in a vendor tag.         |

#### ↘ Configuring Circuit-id

|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> |
| <b>Parameter Description</b> | N/A   |
| <b>Configuration mode</b>    | Global configuration mode   |
| <b>Usage Guide</b>           | Add a circuit-id to a vendor tag.   |

#### ↘ Configuring a Customized Circuit-id

|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] pppoe intermediate-agent type self-defined circuit-id {vlan  port id (switch-id  remote-mac)  string WORD}   |
| <b>Parameter Description</b> | <i>vlan</i> : the VLAN where PPPoE request packets exist.<br><i>port</i> : the port used to receive PPPoE request packets.<br><i>id</i> : the MAC address and name of an access device. |
| <b>Configuration mode</b>    | Global configuration mode   |
| <b>Usage Guide</b>           | Configure a customized circuit-id.  |

#### ↘ Configuring a Customized Remote-id

|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] pppoe intermediate-agent type self-defined remoteid {mac  vlan-mac  hostname  string WORD}   |
| <b>Parameter Description</b> | <i>mac</i> : the MAC address of an access device.<br><i>vlan-mac</i> : the VLAN-MAC address of an access device.<br><i>hostname</i> : the name of an access device. |
| <b>Configuration mode</b>    | Global configuration mode   |
| <b>Usage Guide</b>           | Configure the format of a customized remote-id.   |

#### ↘ Configuring Separators between Fields

|                  |  |
|------------------|--|
| <b>Command</b>   | [ no ] pppoe intermediate-agent delimiter <WORD> |
| <b>Parameter</b> | N/A  |

---

|                           |  |
|---------------------------|--|
| <b>Description</b>        |  |
| <b>Configuration mode</b> | Global configuration mode  |
| <b>Usage Guide</b>        | Configure separators between the fields of circuit-id and remote-id. |

#### ↘ Configuring Vendor Tag Strip Function of Ports

|                              |  |
|------------------------------|--|
| <b>Command</b>               | [ no ] pppoe intermediate-agent vendor-tag strip   |
| <b>Parameter Description</b> | N/A  |
| <b>Configuration mode</b>    | Port configuration mode  |
| <b>Usage Guide</b>           | Strip function must be configured on trusted ports. If the function is configured on a untrusted port, it would fail to take effect. |

#### ↘ Configuring the Circuit-id of a Port


|                              |   |
|------------------------------|---|
| <b>Command</b>               | [ no ] pppoe intermediate-agent circuit-id <string> |
| <b>Parameter Description</b> | N/A   |
| <b>Configuration mode</b>    | Port configuration mode                             |
| <b>Usage Guide</b>           | Configure the circuit-id of a port.                 |

#### ↘ 配置端口的remote-id

|                              |  |
|------------------------------|--|
| <b>Command</b>               | [ no ] pppoe intermediate-agent remote-id <string> |
| <b>Parameter Description</b> | N/A  |
| <b>Configuration mode</b>    | Port configuration mode                            |
| <b>Usage Guide</b>           | Configure the remote-id of a port.                 |

### Configuration Example

#### ↘ The Scenarios of PPPoE IA

|                                |   |
|--------------------------------|---|
| <b>Scenario</b><br>Figure 16-1 |  <p>The diagram illustrates a network topology for PPPoE IA. On the left, a PC is connected to a Switch at port Gi 0/1. The Switch is connected to the Internet at port Gi 0/2. The Internet is represented by a cloud icon. On the right, the Internet is connected to a Server.</p> |
| <b>Configuration Steps</b>     | <ul style="list-style-type: none"> <li>● Enable PPPoE IA globally on the switch.</li> <li>● Configure the gi0/2 port connected to the server as a trust port, and vendor tag strip function.</li> <li>● Enable PPPoE IA on the gi0/1 port of VLAN 1.</li> </ul>   |

|                     |  |
|---------------------|--|
|                     | <ul style="list-style-type: none"> <li>● Configure pppoe intermediate-agent access-node-id as abcd.</li> <li>● Configure the remote-id as xyz on the gi0/1 port.</li> </ul>  |
| <b>Switch</b>       | <pre> Orion Alpha A28X(config)#pppoe intermediate-agent Orion Alpha A28X(config)#interface gigabitEthernet 0/2 Orion Alpha A28X(config-if-GigabitEthernet 0/2)#pppoe intermediate-agent trust Orion Alpha A28X(config-if-GigabitEthernet 0/2)#pppoe intermediate-agent vendor-tag strip Orion Alpha A28X(config-if-GigabitEthernet 0/2)#exit Orion Alpha A28X(config)#interface gigabitEthernet 0/1 Orion Alpha A28X(config-if-GigabitEthernet 0/1)#pppoe intermediate-agent Orion Alpha A28X(config-if-GigabitEthernet 0/1)#pppoe intermediate-agent remote-id xyz Orion Alpha A28X(config-if-GigabitEthernet 0/1)#exit Orion Alpha A28X(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd </pre> |
| <b>Verification</b> | <p>Check the configuration of the switch.</p> <ul style="list-style-type: none"> <li>● Check whether PPPoE IA is enabled and whether its trusted ports are uplink.</li> <li>● Check the configuration of PPPoE IA, especially to check whether trusted ports are correct.</li> </ul>   |