Security Configuration

1 Configuring AAA

1.1 Overview

Authentication, authorization, and accounting (AAA) provides a unified framework authorization, and accounting services. Orion 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 se classified into local authentication and authentication through Remote Authentication Dial In User Service (RAI Terminal Access Controller Access Control System+ (TACACS+).

Authorization: Refers to the granting of specific network services to users according to a series of defined attribut (AV) pairs. The pairs describe what operations users are authorized to perform. AV pairs are stored on netw 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 Networks also provides other simple access control functions, such as local username authentication and online password authentication. Compared to them, AAA offers higher level c network security.

AAA has the following advantages:

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

1.2 Applications

Application	Description
Configuring AAA in a Single-Domain Environment	AAA is performed for all the users in one domain.
Configuring AAA in a Multi-Domain Environment	AAA is performed for the users in different domains by using different methods.

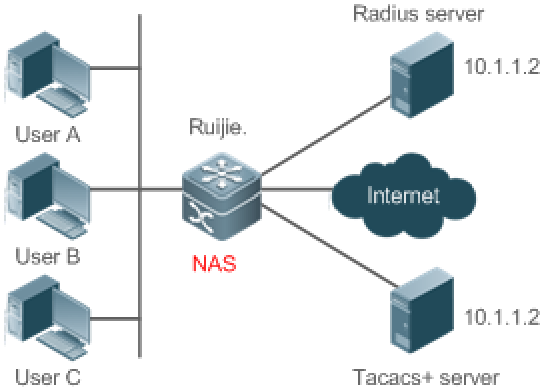
1.2.1 **Configuring AAA in a Single-Domain Environment**

Scenario

In the network scenario shown in Figure 1-1, the following application requirements must be satisfied to improve 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 centra 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 ar
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



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

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.

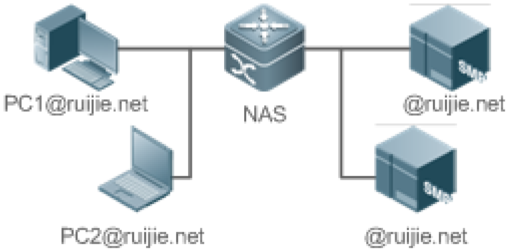
1.2.2 Configuring AAA in a Multi-Domain Environment

Scenario

Configure the domain-based AAA service on the NAS.

- A user can log in by entering the username PC1@Orion_B54Q.net or PC2@Orion_B54Q.com.cn and correct password on an 802.1X client.
- Permission management: Users managed are classified into Super User and Common User. Super users hav 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



Remarks	The clients with the usernames **PC1@Orion_B54Q.net** and **PC2@Orion_B54Q.com.** are connected to the NAS in wired or wireless way. The NAS is an access or convergence switch. The Security Accounts Manager (SAM) server is a universal RADIUS server provided by Orion_B54Q Networks.

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_B54Q 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 sec 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_B54Q 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_B54Q devices only when the current method does not respo When a method denies user access, the authentication process ends without trying other methods.

Figure 1-3

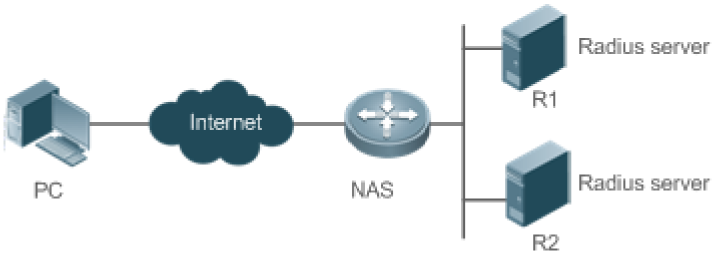


Figure 1 -3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

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 use initiates dial-up access, the NAS first queries the user's identity on R1. When the authentication on R1 is comple 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 try remaining authentication methods, until t

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 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 configur 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.

VRF-Enabled AAA Group

Virtual private networks (VPNs) enable users to share bandwidths securely on the backbone networks of Internet se providers (ISPs). A VPN is a site set consisting of shared routes. An STA site connects to the network of an ISP through one or multiple interfaces. AAA supports assigning a VPN routing forwarding (VRF) table to each user-defined server group.

When AAA is implemented by the server in a group assigned with a VRF table, the NAS sends request packets to the remote servers in the server group. The source IP address of request packets is an address selected from the VRF table according to the IP addresses of the remote servers.

If you run the**ip radius/tacacs+ source-interface**command to specify the source interface for the request packets, the IP address obtained from the source interface takes precedence over the source IP address selected from the VRF table.

Overview

Feature	Description
AAA Authentication	Verifies whether users can access the Internet.
AAA Authorization	Determines what services or permissions users can enjoy.
AAA Accounting	Records the network resource usage of users.
Multi-Domain AAA	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 verifie users can access the Internet. During authentication, the username, password, and other user information are exchange 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 l authentication according to the method list. The method list defines the types of authentication and the sequen 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** 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 grou 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_B54Q 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 proc 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 authentic authentication. If the latter is to be implemented, config 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 acces 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 s 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-g authorization. If remote server-group authorization needs to be implemented, configure a RADIUS or TACACS+ serv 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 a 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 accountin 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 accounting. If remote server-group accounting needs to be implemented, configure a RADIUS or 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 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 conf 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.

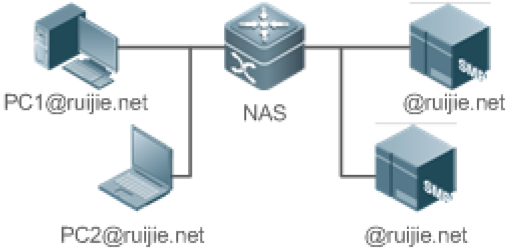
The NAS provides the domain-based AAA service based on the following principles:

- 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 user
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.

ℹ The system supports a maximum of 32 domains.

1.4 Configuration

Configuration	Description and Command	
Configuring Authentication	⚠ Mandatory if user identities need to be verified.	
	aaa new-model	Enables AAA.
	aaa authentication login	Defines a method list of login authentication.
	aaa authentication enable	Defines a method authentication.
	aaa authentication dot1x	Defines a method authentication.
	login authentication	Applies login authentication to terminated line.
	dot1x authentication	Indicates 802.1x authentication.
	aaa local authentication attempts	Sets the maximum number of login attempts.
	aaa local authentication lockout-time	Sets the lockout time for a login user.
Configuring Authorization	⚠ Mandatory if different permissions and services need to be assigned to users.	
	aaa new-model	Enables AAA.
	aaa authorization exec	Defines a method list of EXEC authorization.
	aaa authorization commands	Defines a method li authorization.
	aaa authorization network	Configures a method l authorization.
	authorization exec	Applies EXEC authorization methods specified VTY line.
	authorization commands	Applies command authorization methods to a specified VTY line.
Configuring AAA Accounting	⚠ Mandatory if accounting, statistics, and tracking need to be performed on the netwo resource usage of users.	
	aaa new-model	Enables AAA.
	aaa accounting exec	Defines a method list of EXEC accounting.
	aaa accounting commands	Defines a method l accounting.

Configuration	Description and Command	
	aaa accounting network	Defines a method list of network accounting.
	accounting exec	Applies EXEC accounting me specified VTY line.
	accounting commands	Applies command accounting methods to a specified VTY line.
	aaa accounting update	Enables accounting update.
	aaa accounting update periodic	Configures the accounting update i
Configuring an AAA Server Group	⚠ Recommended if a server group needs to be configured to handle AAA through different servers in the group.	
	aaa group server	Creates a user-defined AAA server g
	server	Adds an AAA server group member.
	ip vrf forwarding	Configures the VRF attribute o server group.
Configuring the Domain-Based AAA Service	⚠ Mandatory if AAA management of 802.1X access STAs nee according to domains.	
	aaa new-model	Enables AAA.
	aaa domain enable	Enables the domain-based AAA service.
	aaa domain	Creates a domain and e configuration mode.
	authentication dot1x	Associates the domain wi authentication method list.
	accounting network	Associates the domain w accounting method list.
	authorization network	Associates the domain w authorization method list.
	state	Configures the domain status.
	username-format	Configures whether to contain the d name in usernames.
	access-limit	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 t configured sequence.
- The next authentication method is executed only when the current method does not respond. If the current r 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 because the username that the user entered during login authentication is automatically filled in. However, th must enter the password previously used for login authentication.
- The username is not recorded if the user does not perform login authentication when **none** method is used during login authentication. Then, a user is required to enter the username each 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.

Defining a Method List of 802.1X Authentication

- Run the **aaa authentication dot1x** command to configure a method list of 802.1X authentication.
- This configuration is mandatory if you need to configure an 802.1X authenti
configuration of the default method list).
- By default, no method list of 802.1X authentication is configured.

Applying Login Authentication to a Specific Terminated Line

- In the Line mode, run the **login authentication** command to apply login authentication to a specific terminated line.
- This configuration is mandatory, if you need to apply login authentication to a specific terminated line.
- By default, the default method list is applied to all terminated lines.

802.1x Authentication

- Run the **dot1x authentication** command to configure 802.1x Authentication.
- This configuration is mandatory, if you need to specify 802.1x Authentication.
- By default, 802.1x Authentication is not applied.

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 attempt
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

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

Defining a Method List of Login Authentication

Command	**aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default:** With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a login authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, and **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS a server groups are supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform login au negotiation through AAA. Run the **aaa authentication login** command to configure the default or optional method lists for login authentication. 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 authentication; otherwise, the methods will not take effect.

Defining a Method List of Enable Authentication

Command	**aaa authentication enable default** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an Enable authentication method list in characters. *method*: Indicates authentication methods from **enable**, **local**, **none**, and **group**. A method list contains up to four methods. **enable**: Indicates that the password that is configured using the **enable** command is used for the authentication. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS a server groups are supported.

Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform Enable authenticat negotiation through AAA. Run the **aaa authentication enable** command to configure the default or optional method lists for Enable authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of 802.1X Authentication

Command	**aaa authentication dot1x** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an 802.1X authentication method list in characters. *method* Indicates authentication methods from **local**, **none**, and **group** A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group** Indicates that a server group is used for authentication. Currently, the RADIUS se supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA 802.1X authentication service is enabled on the NAS, users must perform 802.1X authentication negotiation through AAA. Run the **aaa authentication dot1x** command to configure the default or optional method lists for 802.1X authentication. In a method list, the next method is executed only when the current method does not receive response.

Setting the Maximum Number of Login Attempts

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

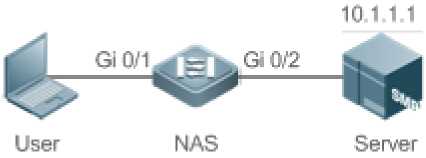
Setting the Maximum Lockout Time After a Login Failure

Command	**aaa local authentication lockout-time** *lockout-time*
Parameter Description	*lockout-time* Indicates the time during which a user is locked after entering wrong passwords u specified times. The value ranges from 1 to 2,147,483,647, in the unit of minutes.
Command Mode	Global configuration mode
Usage Guide	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.

Scenario **Figure 1-5**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication need 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.) Step 3: Configure an AAA authentication method list for login authentication users. (This ex **group** *radius* and **local** in order.) Step 4: Apply the configured method list to an interface or line. Skip this step if the default authenticati method is used.

NAS	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#username user password  pass`
	`Orion_B54Q(config)#aaa new-model`
	`Orion_B54Q(config)#radius-server host 10.1.1.1`
	`Orion_B54Q(config)#radius-server key Orion_B54Q`
	`Orion_B54Q(config)#aaa authentication login list1 group radius local`
	`Orion_B54Q(config)#line vty 0 20`
	`Orion_B54Q(config-line)#login authentication list1`
	`Orion_B54Q(config-line)#exit`

Verification	Run the **show aaa method-list** command on the NAS to display the configuration.

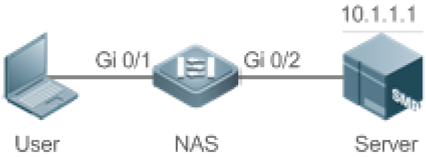
NAS	`Orion_B54Q#show aaa method-list`
	
	`Authentication method-list:`
	`aaa authentication login list1 group radius local`
	
	`Accounting method-list:`

	`Authorization method-list:`
	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. The user must enter the correct username and password to access the NAS.

User	`User Access Verification`
	
	`Username:user`
	`Password:pass`

Configuring AAA Enable Authentication

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

Scenario **Figure 1-6**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication need implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. Configure Enable authentication passwords on the NAS i authentication. Step 3: Configure an AAA authentication method list for Enable authentication users. ⓘ 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.

NAS	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#username user privilege 15 password  pass`
	`Orion_B54Q(config)#enable secret w`
	`Orion_B54Q(config)#aaa new-model`
	`Orion_B54Q(config)#radius-server host 10.1.1.1`
	`Orion_B54Q(config)#radius-server key Orion_B54Q`
	`Orion_B54Q(config)#aaa authentication enable default group radius local enable`

Verification	Run the **show aaa method-list** command on the NAS to display the configuration.

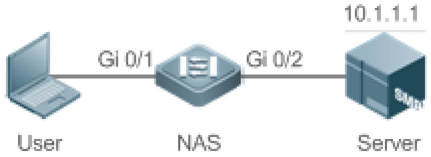
NAS	`Orion_B54Q#show aaa method-list`
	
	`Authentication method-list:`
	`aaa authentication enable default group radius local enable`
	
	`Accounting method-list:`
	
	`Authorization method-list:`

	The CLI displays an authentication prompt when The user must enter the correct username and password to access the NAS.

NAS	`Orion_B54Q>enable`
	`Username:user`
	`Password:pass`
	`Orion_B54Q#`

Configuring AAA 802.1X Authentication

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

Scenario **Figure 1-7**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if group-server authentication needs to be implem 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.) Cu 802.1X authentication does not support TACACS+. Step 3: Configure an AAA authentication method list for 802.1X authentication users. (This example use **group** *radius* and **local** in order.) Step 4: Apply the AAA authentication method list. Skip this step if the default authentication method is used. Step 5: Enable 802.1X authentication on an interface.

NAS	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#username user1 password  pass1`

	`Orion_B54Q(config)#username user2 password  pass2`
	`Orion_B54Q(config)#aaa new-model`
	`Orion_B54Q(config)#radius-server host 10.1.1.1`
	`Orion_B54Q(config)#radius-server key Orion_B54Q`
	`Orion_B54Q(config)#aaa authentication dot1x default group radius local`
	`Orion_B54Q(config)#interface gigabitEthernet 0/1`
	`Orion_B54Q(config-if-gigabitEthernet 0/1)#dot1 port-control auto`
	`Orion_B54Q(config-if-gigabitEthernet 0/1)#exit`

Verification	Run the **show aaa method-list** command on the NAS to display the configuration.

NAS	`Orion_B54Q#show aaa method-list`
	
	`Authentication method-list:`
	`aaa authentication dot1x default group radius local`
	
	`Accounting method-list:`
	
	`Authorization method-list:`

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 meth sequence. The next authorization method is executed only when the current method does not receive re authorization fails using a method, the next method will be not tried.
- Command authorization is supported only by TACACS+.
- Console authorization: The NOS 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 authoriza 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 conf 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

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

↘ Defining a Method List of EXEC Authorization

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

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

Defining a Method List of Command Authorization

Command	**aaa authorization commands** *level* { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command authorization is not performed. **group** Indicates that a server group is used for command authorization. Currently, the TACACS+ serv group is supported.
Command Mode	Global configuration mode
Usage Guide	The NOS 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. 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.) After you configure command authorization methods, apply the methods to the VTY command authorization; otherwise, the methods will not take effect.

Configuring a Method List of Network Authorization

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

Command Mode	Global configuration mode
Usage Guide	The NOS supports authorization of network-related service requests such as PPP an 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. RADIUS or TACACS+ servers return a series of AV pai Network authorization is based on authentication. Only authe authorization.

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

Command	**aaa authorization config-commands**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	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 no 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

Command	**aaa authorization console**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The NOS 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 auth method list applied to the Console line no longer takes effect.

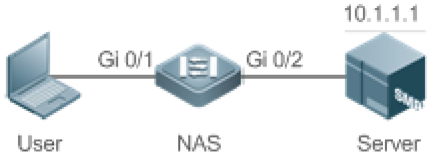
Configuration Example

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.

Scenario

Figure 1-8



Configuration Steps

Step 1: Enable AAA.

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, configu information on the NAS.

Step 3: Configure an AAA authorization method list according to different access modes and service types.

Step 4: Apply the configured method list to an interface or line. Skip this step if the default autho method is used.

EXEC authorization is often used with login authentication, which can be implemented on the same line.

NAS

```
Orion_B54Q#configure terminal

Orion_B54Q(config)#username user password  pass

Orion_B54Q(config)#username user privilege 6

Orion_B54Q(config)#aaa new-model

Orion_B54Q(config)#radius-server host 10.1.1.1

Orion_B54Q(config)#radius-server key  test

Orion_B54Q(config)#aaa authentication login list1 group local

Orion_B54Q(config)#aaa authorization exec list2 group radius local

Orion_B54Q(config)#line vty 0 4

Orion_B54Q(config-line)#login authentication list1

Orion_B54Q(config-line)# authorization exec list2

Orion_B54Q(config-line)#exit
```

Verification

Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.

NAS

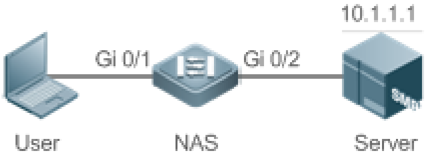
```
Orion_B54Q#show aaa method-list


Authentication method-list:

aaa authentication login list1 group local


Accounting method-list:
```

```
Authorization method-list:
aaa authorization exec list2 group radius local
```

```
Orion_B54Q# show running-config
aaa new-model
!
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

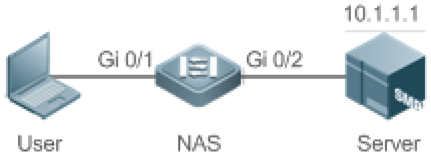
Provide command authorization for login users according to the following default authorization method: Authorize leve commands first by using a TACACS+ server. If the TACACS+ server does not respond, local authorization is perfo Authorization is applied to the users who log in through the Console and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

Scenario **Figure 1-9**	
Configuration Steps	Step 1: Enable AAA. 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, configu

	information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default autho method is used.
NAS	Orion_B54Q#configure terminal Orion_B54Q(config)#username user1 password pass1 Orion_B54Q(config)#username user1 privilege 15 Orion_B54Q(config)#aaa new-model Orion_B54Q(config)#tacacs-server host 192.168.217.10 Orion_B54Q(config)#tacacs-server key aaa Orion_B54Q(config)#aaa authentication login default local Orion_B54Q(config)#aaa authorization commands 15 default group tacacs+ local Orion_B54Q(config)#aaa authorization console
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	Orion_B54Q#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
	Orion_B54Q#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 ! tacacs-server host 192.168.217.10 tacacs-server key aaa ! line con 0 line vty 0 4 ! ! end

↘ Configuring AAA Network Authorization

Scenario **Figure 1-10**	
Configuration Steps	Step 1: Enable AAA. 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, configu information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default autho method is used.
NAS	Orion_B54Q#configure terminal Orion_B54Q(config)#aaa new-model Orion_B54Q(config)#radius-server host 10.1.1.1

	`Orion_B54Q(config)#radius-server key  test`
	`Orion_B54Q(config)#aaa authorization network default group radius none`
	`Orion_B54Q(config)# end`

Verification	Run the **show aaa method-list** command on the NAS to display the configuration.

NAS	`Orion_B54Q#show aaa method-list`
	
	`Authentication method-list:`
	
	`Accounting method-list:`
	
	`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 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 automatica 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 ac 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 is configured. Only the TACACS+ protocol supports comm 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 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

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands canbe effective if AAA is not enabled.

Defining a Method List of EXEC Accounting

Command	**aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that EXEC accounting is not performed. **group** Indicates that a server group is used for EXEC accounting. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The NOS enables EXEC accounting only when login authentication is completed. EXEC accounting is not performed if login authentication is not performed or the **none** authentication method is used. 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. After you configure EXEC accounting methods, apply the methods to the VTY lines that r accounting; otherwise, the methods will not take effect.

Defining a Method List of Command Accounting

Command	**aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*level*: Indicates the command level for which accounting will be performed. The value ranges from 0 to 15. After a command of the configured level is executed, the accounting server records relate based on the received accounting packet. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command accounting is not performed. **group**Indicates that a server group is used for command accounting. Currently, the TACAC group is supported.
Command Mode	Global configuration mode
Usage Guide	The NOS enables command accounting only when login authentication is completed. Command accounting is not performed if login authentication is not performed or the **none** 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. After you configure command accounting methods, apply the methods to the

	command accounting; otherwise, the methods will not take effect.

Defining a Method List of Network Accounting

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

Enabling Accounting Update

Command	**aaa accounting update**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	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.

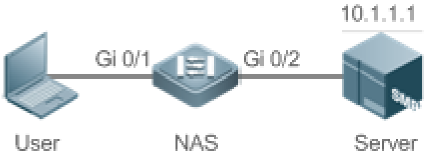
Configuring the Accounting Update Interval

Command	**aaa accounting update periodic** *interval*
Parameter Description	*Interval*: Indicates the accounting update interval, in the unit of minutes. The shortest is 1 minute.
Command Mode	Global configuration mode
Usage Guide	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.

Scenario **Figure 1-11**	
Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the defaul method is used.

NAS	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#username user password  pass`
	`Orion_B54Q(config)#aaa new-model`
	`Orion_B54Q(config)#radius-server host 10.1.1.1`
	`Orion_B54Q(config)#radius-server key  test`
	`Orion_B54Q(config)#aaa authentication login list1 group local`
	`Orion_B54Q(config)#aaa accounting exec list3 start-stop group radius`
	`Orion_B54Q(config)#line vty 0 4`
	`Orion_B54Q(config-line)#login authentication list1`
	`Orion_B54Q(config-line)# accounting  exec list3`
	`Orion_B54Q(config-line)#exit`

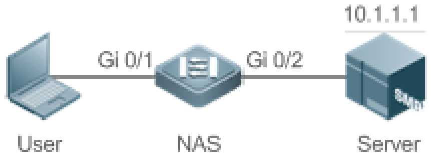
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.

NAS	`Orion_B54Q#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:`

```
Orion_B54Q# 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
```

Configuring AAA Command Accounting

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

Scenario **Figure 1-12**	
Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the defaul method is used.
NAS	`Orion_B54Q#configure terminal`

	`Orion_B54Q(config)#username user1 password pass1`
	`Orion_B54Q(config)#username user1 privilege 15`
	`Orion_B54Q(config)#aaa new-model`
	`Orion_B54Q(config)#tacacs-server host 192.168.217.10`
	`Orion_B54Q(config)#tacacs-server key aaa`
	`Orion_B54Q(config)#aaa authentication login default local`
	`Orion_B54Q(config)#aaa accounting commands 15 default start-stop group tacacs+`

Verification	Run the **show aaa method-list** command on the NAS to display the configuration.

NAS	`Orion_B54Q#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:`

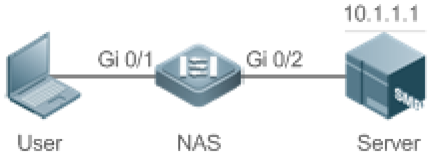
	`Orion_B54Q#show run`
	`!`
	`aaa new-model`
	`!`
	`aaa authorization config-commands`
	`aaa accounting commands 15 default start-stop group tacacs+`
	`aaa authentication login default local`
	`!`
	`!`
	`nfpp`
	`!`
	`vlan 1`
	`!`

```
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.

Scenario
Figure 1-13



Configuration Steps

Step 1: Enable AAA.

Step 2: If remote server-group accounting needs to be implemented, configu
advance.

Step 3: Configure an AAA accounting method list according to different access modes and service types.

Step 4: Apply the configured AAA accounting method list. Skip this step if the default accounting method is used.

Accounting is performed only when 802.1X authentication is completed.

NAS

```
Orion_B54Q#configure terminal

Orion_B54Q(config)#username user password  pass

Orion_B54Q(config)#aaa new-model

Orion_B54Q(config)#radius-server host 10.1.1.1

Orion_B54Q(config)#radius-server key test
```

	Orion_B54Q(config)#aaa authentication dot1x aut1x group radius local Orion_B54Q(config)#aaa accounting network acc1x start-stop group radius Orion_B54Q(config)#dot1x authentication aut1x Orion_B54Q(config)#dot1x accounting acc1x Orion_B54Q(config)#interface gigabitEthernet 0/1 Orion_B54Q(config-if-GigabitEthernet 0/1)#dot1 port-control auto Orion_B54Q(config-if-GigabitEthernet 0/1)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Orion_B54Q#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:

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 afte 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.

Configuring the VRF Attribute of an AAA Server Group

- Optional.
- Run the **ip vrf forwarding** command to configure the VRF attribute of an AAA server group.
- By default, the AAA server group belongs to the global VRF table.

Verification

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

Related Commands

Creating a User-Defined AAA Server Group

Command	**aaa group server** {**radius** | **tacacs+**} *name*
Parameter Description	*name*: Indicates the name of the server group to be created. The **radius** and **tacacs+** keywords because they are the names of the default RADIUS and TACACS+ server groups.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure an AAA server group. Currently, the RADIUS and TACACS+ server groups are supported.

Adding an AAA Server Group Member

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

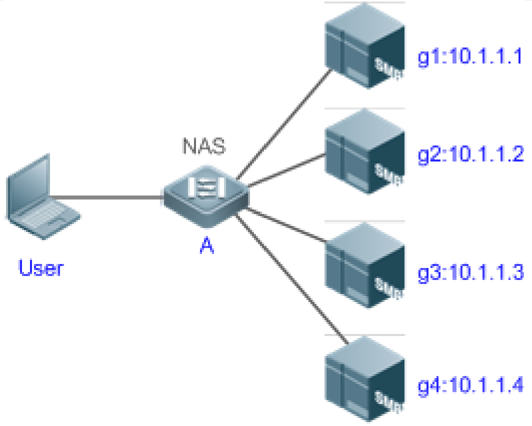
Configuring the VRF Attribute of an AAA Server Group

Command	**ip vrf forwarding** *vrf_name*
Parameter Description	*vrf_name*: Indicates the name of a VRF table.
Command Mode	Server group configuration mode
Usage Guide	Use this command to assign a VRF table to the specified server group.

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.

Scenario **Figure 1-14**	 g1:10.1.1.1 NAS g2:10.1.1.2 User A g3:10.1.1.3 g4:10.1.1.4
Prerequisites	1. The required interfaces, IP addresses, and VLANs have been configured on th network connections have been set up, and the routes from the N reachable. 2. Enable AAA.
Configuration Steps	Step 1: Configure a server (which belongs to the default server group). Step 2: Create user-defined AAA server groups. Step 3: Add servers to the AAA server groups.

NAS	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#radius-server host 10.1.1.1`
	`Orion_B54Q(config)#radius-server host 10.1.1.2`
	`Orion_B54Q(config)#radius-server host 10.1.1.3`
	`Orion_B54Q(config)#radius-server host 10.1.1.4`
	`Orion_B54Q(config)#radius-server key secret`

```
Orion_B54Q(config)#aaa group server radius g1
Orion_B54Q(config-gs-radius)#server 10.1.1.1
Orion_B54Q(config-gs-radius)#server 10.1.1.2
Orion_B54Q(config-gs-radius)#exit
Orion_B54Q(config)#aaa group server radius g2
Orion_B54Q(config-gs-radius)#server 10.1.1.3
Orion_B54Q(config-gs-radius)#server 10.1.1.4
Orion_B54Q(config-gs-radius)#exit
```

Verification Run the **show aaa group** and **show run** commands on the NAS to display the configuration.

NAS

```
Orion_B54Q#show aaa group
Type       Reference  Name
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          g1
radius     1          g2
```

```
Orion_B54Q#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 ! !

Common Errors

- For RADIUS servers that use non-default authenti
server command to add servers, specify the authentication or accounting port.
- Only the RADIUS server group can be configured with the VRF attribute.

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 sy
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 ne
created manually. The default domain name is **default**. It is used to provide the AAA service to the users whos
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 longes
principle. For example, if two domains, **domain.com** and **domain.com.** 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**

- 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 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

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

↘ Enabling the Domain-Based AAA Service

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

↘ Creating a Domain and Entering Domain Configuration Mode

Command	**aaa domain** { **default** | *domain-name* }
Parameter Description	**default**: Uses this parameter to configure the default domain. *domain-name*: Indicates the name of the domain to be created.

Command Mode	Global configuration mode
Usage Guide	Use this command to configure a domain to provide **default** 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 t The *domain-name* 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 assoc 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

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

↘ Associating the Domain with a Network Accounting Method List

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

↘ Associating the Domain with a Network Authorization Method List

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

↘ Configuring the Domain Status

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

Configuring Whether to Contain the Domain Name in Usernames

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

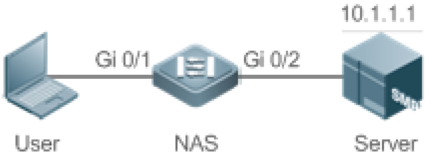
Configuring the Maximum Number of Domain Users

Command	**access-limit** *num*
Parameter Description	*num*: Indicates the maximum number of access users allowed in a domain. This limit is applicable only to 802.1X STAs.
Command Mode	Domain configuration mode
Usage Guide	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 (user@domain.com) that access the NAS. The usernames that the NAS sends to the RADIUS server do not carry domain inform number of access users is not limited.

Scenario **Figure 1-15**	
Configuration Steps	The following example shows how to configure RADIUS authentication and accounting, which requires the configuration of a RADIUS server in advance. Step 1: Enable AAA. Step 2: Define an AAA method list. Step 3: Enable the domain-based AAA service. Step 4: Create a domain. Step 5: Associate the domain with the AAA method list. Step 6: Configure the domain attribute.

NAS	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#aaa new-model`

	Orion_B54Q(config)#radius-server host 10.1.1.1 Orion_B54Q(config)#radius-server key test Orion_B54Q(config)#aaa authentication dot1x default group radius Orion_B54Q(config)#aaa accounting network list3 start-stop group radius Orion_B54Q(config)# aaa domain enable Orion_B54Q(config)# aaa domain domain.com Orion_B54Q(config-aaa-domain)# authentication dot1x default Orion_B54Q(config-aaa-domain)# accounting network list3 Orion_B54Q(config-aaa-domain)# username-format without-domain
Verification	Run the **show run** and **show aaa domain** command on the NAS to display the configuration.
NAS	Orion_B54Q#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
	Orion_B54Q#show run Building configuration... Current configuration : 1449 bytes version NOS 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
!
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.	**clear aaa local user lockout** {**all** | **user-name** *username* }

Displaying

Description	Command
Displays the accounting update information.	**show aaa accounting update**
Displays the current domain configuration.	**show aaa domain**

Displays the current lockout configuration.	**show aaa lockout**
Displays the AAA server groups.	**show aaa group**
Displays the AAA method lists.	**show aaa method-list**
Displays the AAA users.	**show aaa user**

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 NOS implementation, a RADIUS client runs on a device or Network Access Server (NAS) and transmits identity authentication requests to the central RADIOUS 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 acce users. RADIUS is a completely open protocol and the RADIUS server is installed on many c component, for example, on UNIX, Windows 2000, and Windows 2008. Therefore, RADIUS is the most 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 d 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 locate according to the user session information, user name, and other information carried in the request and b offline. Then, the device returns a response packet that carries the processing result to the R 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
P r o	Authentication, authorization, and accounting are conducted on access users

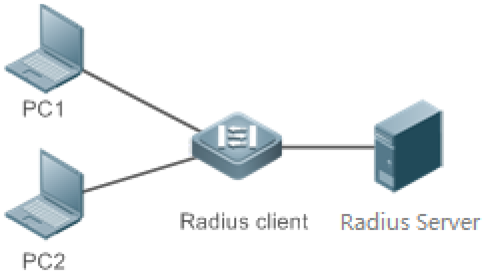
Application	Description
Authorization, and Accounting Services for Access Users	network, to prevent unauthorized access or operations.
Forcing Users to Go Offline	The server forces an authenticated user to go offline.

2.2.1 Providing Authentication, Authorization, and Accounting Service 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, th returns the authentication acceptance/authentication rejection/accounting respons The RADIUS client performs processing on the access user according to the response from the RADIUS server.

Figure 2-16 Typical RADIUS Networking Topology



Remarks	PC 1 and PC 2 are connected to the RADIUS client as access users in wired or wireless mode, an authentication and accounting requests. The RADIUS client is usually an access switch or aggregate switch. 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.

Deployment

- Configure access device information on the RADIUS server, including the IP address and shared key of the acc 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.

2.2.2 Forcing Users to Go Offline

Scenario

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

See Figure 2 -16 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

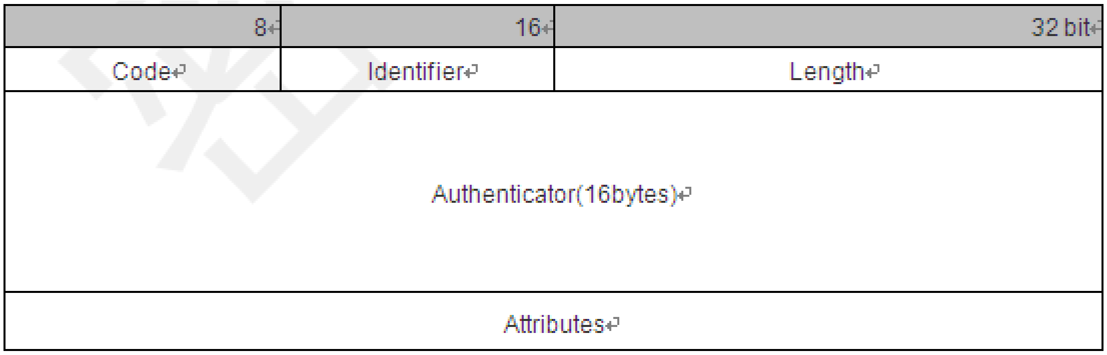
Basic Concepts

↘ 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 serv The processing includes accepting user access, rejecting user access, or collecting more user inf RADIUS server.
- Server: Multiple RADIUS clients map to one RADIUS server. The RADIUS server maintains the IP addr 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	32 bit
Code	Identifier	Length
Authenticator(16bytes)		
Attributes		

- Code: Identifies the type of RADIUS packets, which occupies one byte. The following table 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 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 acco **Attributes** field usually contains multiple attributes. Each attribute is represented in the Type, Length, Va 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
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access

Attribute No.	Attribute Name	Attribute No.	Attribute Name
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 Each RADIUS method corresponds to one RADIUS server group and one or more RADIUS severs can be added to o 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 R 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 n uniquely identify a user. Therefore, it is often set to the MAC address of a user. For exa 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: 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: 00d0.f833.22ac
Unformatted	Indicates the format without separators. This format is used by default. Example: 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 RADIUS protocol. Table 1-3 lists private attributes supported by Orion_B54Q products. The **TYPE** column indicates the default configuration of private attributes of Orion_B54Q products and the **Extended TYPE** column indicates the default configuration of private attributes of other non-Orion_B54Q 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-supplicant-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-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20

ID	Function	TYPE	Extended TYPE
21	dailup-avoid	21	21
22	ip-privilege	22	22
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

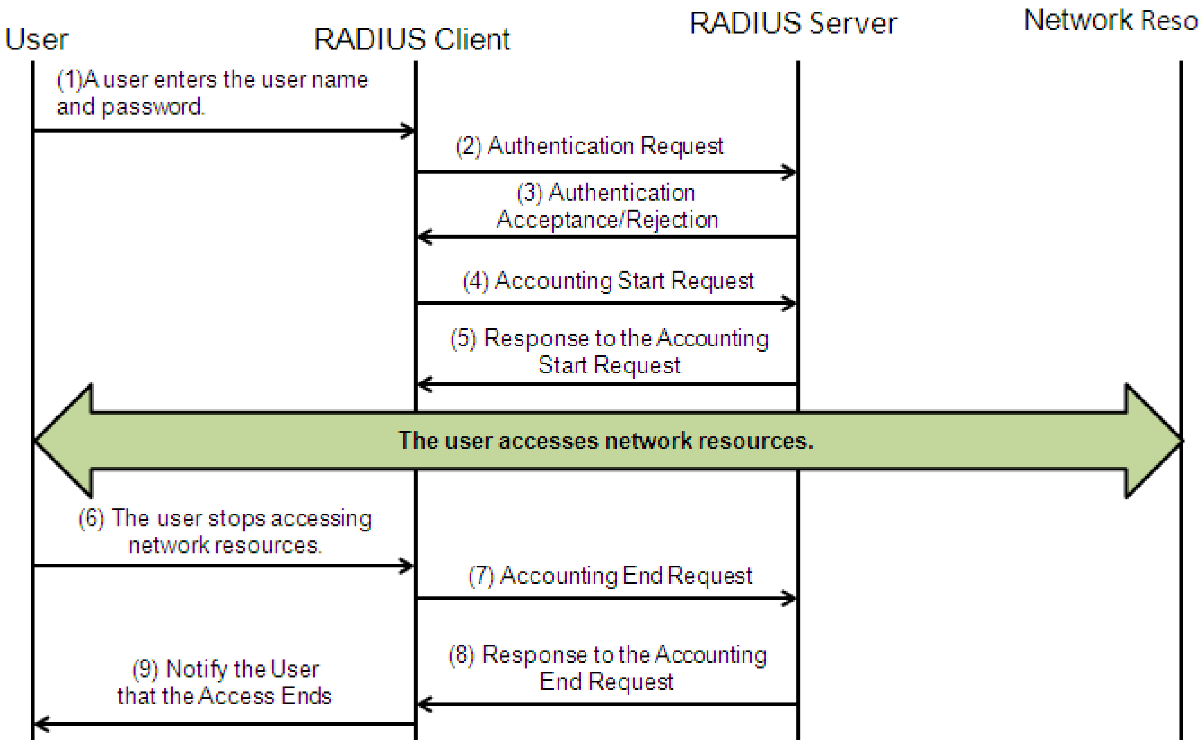
Feature	Description
RADIUS Authentication, Authorization, and Accounting	Conducts identity authentication and accounting on access users, safegu security, and facilitates management for network administrators.
Source Address of RADIUS Packets	Specifies the source IP address used by a RADIUS client to transmit packets to a RADIUS server.
RADIUS Timeout Retransmission	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.
RADIUS Server Accessibility Detection	Enables a RADIUS client to actively detect whether a RADIUS server is reachable maintain the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.
RADIUS Forced Offline	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 2-17


User
RADIUS Client
RADIUS Server
Network Resources
(1)A user enters the user name and password.
(2) Authentication Request
(3) Authentication Acceptance/Rejection
(4) Accounting Start Request
(5) Response to the Accounting Start Request
The user accesses network resources.
(6) The user stops accessing network resources.
(7) Accounting End Request
(8) Response to the Accounting End Request
(9) Notify the User that the Access Ends

The RADIUS authentication and authorization process is described as follows:

1. A user enters the user name and password and transmits them to the RADIUS client.
2. After receiving the user name and password, the RADIUS client transmits an authentication request RADIUS server. The password is encrypted for transmission. For the encryption method, see RFC2865.
3. The RADIUS server accepts or rejects the authentication request according to the user name and password. W accepting the authentication request, the RADIUS server also issues authori authentication acceptance information. The authorization information varies with the type of access users.

The RADIUS accounting process is described as follows:

1. 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.
2. The RADIUS server returns the accounting start response packet, indicating accounting start.
3. The user stops accessing network resources and requests the RADIUS client to disconnect the network connection.
4. The RADIUS client transmits the accounting end request packet to the RADIUS server.
5. The RADIUS server returns the accounting end response packet, indicating accounting end.
6. 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
group radius when setting the authentication method.

The RADIUS authentication can be conducted only after the AAA authentication method list of re
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 lis
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 a
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 th 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 a 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 RAD 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.xtestusername xxx** command to configure the test user name.

2.3.5 RADIUS Forced Offline

Working Principle

Figure 2-18 DM Message Exchange of the RADIUS Dynamic Authorization Extension Protocol

```
+----------+    Disconnect-Request     +----------+
|          |    <--------------------  |          |
|    NAS   |                           |  RADIUS  |
|          |    Disconnect-Response    |  Server  |
|          |    --------------------->  |          |
+----------+                           +----------+
```

The preceding figure shows the exchange of DM messages between the RADIUS server and the device. Th 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	
RADIUS Basic Configuration	⚠ (Mandatory) It is used to configure RADIUS auth accounting.	
	radius-serverhost	Configures the IP address of the remote RAD security server.
	radius-serverkey	Configures the shared key f between the device and the RADIUS server.
	radius-serverretransmit	Configures the request transmissio which the device confirms that a RADIUS server is unreachable.
	radius-servertimeout	Configures the waiting time, after which the device retransmits a request.

Configuration	Description and Command	
	radius-server account update retransmit	Configures retransmission of accounting update packets for authenticated users.
	ip radius source-interface	Configures the source address of RADIUS packets.
Configuring the RADIUS Attribute Type	⚠ (Optional) It is used to define attribute processing adopted when the device encapsulates and parses RADIUS packets.	
	radius-serverattribute31	Configures the MAC address format of attribute No. 31 (Calling-Station-ID).
	radius attribute	Configures the RADIUS private attribute type.
	radius set qoscos	Sets the private attribute port-priority issued by the server to the COS value. For COS-relevant concepts, see *Configuring QoS*.
	radius support cui	Configures the device to support the CUI attribute.
	radius vendor-specific	Configures the mode of parsing private attributes by the device.
Configuring the RADIUS Accessibility Detection	⚠ (Optional) It is used to detect whether a RADIUS server is reachable and maintain the accessibility of the RADIUS server.	
	radius-server dead-criteria	Configures the global criteria for judging whether a RADIUS security server is unreachable.
	radius-server deadtime	Configures the duration for the device to stop transmitting request packets to an unreachable RADIUS server.
	radius-server host	Configures the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.

2.4.1 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 R Unreachable

- Optional.
- Configure the request transmission count, after which the device confirms that a RADIUS ser 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 802.1X authenticator and Orion_B54Q SU is used as the 802.1X clien **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

Command	**radius-server host** [**oob** [**via** *mgmt_name*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]
Parameter Description	**oob** Indicates oob authentication, that is, the source interface for transmitting packet server is an mgmt port. **via** *mgmt_name*: Specifies a specific mgmt port when oob supports multiple mgmt ports. *ipv4-address*: Indicates the IPv4 address of the RADIUS security server. *Ipv6-address*: Indicates the IPv6 address of the RADIUS security server. **auth-port** *port-number*: Indicates the UDP port for RADIUS identity authentication. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct identity authentication. **acct-port** *port-number*: Indicates the UDP port for RADIUS accounting. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct accounting. **test username** *name*: Enables the function of actively detecting the RADIUS security server and specifies the user name used for active detection. **idle-time** *time*: 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). **ignore-auth-port**: Disables the function of detecting the authentication port of the RADIUS security server. It is enabled by default. **ignore-acct-port**: Disables the function of detecting the accounting port of the RADIUS security server. It is enabled by default. **key** [**0** | **7**] *text-string*: Configures the shared key of the server. The global shared key is used if it is not configured.
Command Mode	Global configuration mode
Usage Guide	A RADIUS security server must be defined to implement the AAA security service by using RADIUS. You can run the **radius-server host** command to define one or more RADIUS security servers. If a RADIUS security server is not added to a RADIUS server group, the device uses the global routin transmitting RADIUS packets to the RADIUS server. Otherwise, the device uses the VRF routing table of the RADIUS server group.

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

Command	**radius-server key** [**0** | **7**] *text-string*
Parameter Description	*text-string*: Indicates the text of the shared key. **0** | **7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7** indicates simple encryption. The default value is **0**.

Command Mode	Global configuration mode
Usage Guide	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 tha communicate with each other successfully.

Configuring the Request Transmission Count, After Which the Device Confirms That a R Unreachable

Command	**radius-server retransmit**_retries_
Parameter Description	*retries*: Indicates the RADIUS retransmission count. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	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 serv 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

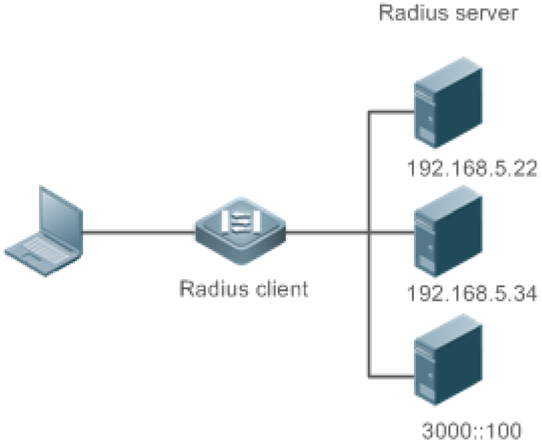
Command	**radius-server timeout**_seconds_
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to seconds.
Command Mode	Global configuration mode
Usage Guide	Use this command to adjust the packet retransmission timeout time.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

Command	**radius-server account update retransmit**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	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

Scenario **Figure 2-19**	 Radius server 192.168.5.22 Radius client 192.168.5.34 3000::100
Configuration Steps	● Enable AAA. ● Configure the RADIUS server information. ● Configure to use the RADIUS authentication, authorization, and accounting methods. ● Apply the configured authentication method on the interface.

RADIUS Client	`Orion_B54Q#configure terminal`
	`Orion_B54Q (config)#aaa new-model`
	`Orion_B54Q (config)# radius-server host 192.168.5.22`
	`Orion_B54Q (config)#radius-server host 3000::100`
	`Orion_B54Q (config)# radius-server key aaa`
	`Orion_B54Q (config)#aaa authentication login test group radius`
	`Orion_B54Q (config)#aaa authorizationexectest group radius`
	`Orion_B54Q (config)#aaa accountingexectest start-stop group radius`
	`Orion_B54Q (config)# line vty 0 4`
	`Orion_B54Q (config-line)#login authentication test`
	`Orion_B54Q (config-line)# authorization exec test`
	`Orion_B54Q (config-line)# accounting exec test`

Verification	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 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.
	`Orion_B54Q#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
!
```

Common Errors

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

2.4.2 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_B54Q 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 RADIUS Private Attribute Type

- Optional.
- If the server is a Orion_B54Q 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_B54Q private attribute parsed by the device as required.

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 dev Orion_B54Q 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 t CUI attribute is correctly parsed by the device.

Related Commands

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

Command	**radius-server attribute 31 mac format** {**ietf** | **normal** | **unformatted** }
Parameter Description	**ietf** Indicates the standard format specified in the IETF standard (RFC3580), which is separated separator (-). Example: 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: 00d0.f833.22ac.

	unformatted: Indicates the format without separators. This format 00d0f83322ac.
Command Mode	Global configuration mode
Usage Guide	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 RADIUS Private Attribute Type

Command	**radius attribute**{*id* | **down-rate-limit** | **dscp** | **mac-limit** | **up-rate-limit**} **vendor-type** *type*
Parameter Description	*id*: Indicates the function ID. The value ranges from 1 to 255. *type*: Indicates the type of private attributes. **down-rate-limit**: Indicates the downstream rate limit attribute. **dscp**: Indicates the DSCP attribute. **mac-limit**: Indicates the MAC-limit attribute. **up-rate-limit**: Indicates the upstream rate limit attribute.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the type of private attributes.

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

Command	**radius set qoscos**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to use the issued QoS value as the CoS value. The QoS value is used DSCP value by default.

Configures the Device to Support the CUI Attribute

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

Configuring the Mode of Parsing Private Attributes by the Device

Command	**Radius vendor-specific extend**
Parameter Description	N/A

Command Mode	Global configuration mode
Usage Guide	Use this command to identify attributes of all vendor IDs by type.

Configuration Example

↘ Configuring the RADIUS Attribute Type

Scenario	One authentication device
Configuration Steps	● Configure the MAC address format of RADIUS Calling-Station-Id. ● Configure the RADIUS private attribute type. ● Set the QoS value issued by the RADIUS server as the COS value of the interface. ● Configure the RADIUS function to support the CUI attribute. ● Configure the device to support private attributes of other vendors.

	`Orion_B54Q(config)#radius-server attribute 31 mac format ietf`
	`Orion_B54Q(config)#radius attribute 16 vendor-type 211`
	`Orion_B54Q(config)#radiussetqoscos`
	`Orion_B54Q(config)#radiussupport cui`
	`Orion_B54Q(config)#radiusvendor-specific extend`

Verification	Conduct packet capture or display debug information of the device to check whether the RADIUS standard attributes and private attributes are encapsulated/parsed correctly.

2.4.3 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 th detection function is enabled for a specified RADIUS server, the device will, according to the configurat transmits detection requests (authentication The transmission interval is as follows:

- For a reachable RADIUS server, the interval is the active detection interval of the reachable RAD 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 retransmis
  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
  function.

↘ Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreacha
Server

- Optional.
- The configured duration for the device to stop transmitting request packets to an unreachable RADIUS server t
  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

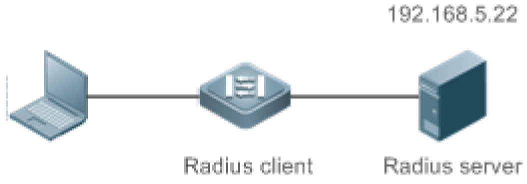
Command	**radius-server dead-criteria** { **time***seconds* [**tries***number*] | **tries***number* }
Parameter Description	**time***seconds*: Indicates the time condition parameter. If the device fails to receive a correct response packet from a RADIUS security server within the specified time, it is deemed that the RADIUS security server meets the inaccessibility duration condition. The value ranges from 1 second to 120 seconds. **tries***number*Indicates the consecutive request timeout count. If the timeout count of 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 inaccessibili ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	If a RADIUS security server meets both the duration condition and the consecutive request timeout cour 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 Unreacha Server

Command	**Radius-server deadtime***minutes*
Parameter Description	*minutes*Indicates the duration for the device to stop transmitting requests to an unreacha security server, with the unit of minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).
Command Mode	Global configuration mode
Usage Guide	If the active detection function is enabled for a RADIUS security server on the device, the time parameter in **radius-server deadtime** does not take effect on the RADIUS server. If the active detection fun 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 **radius-server deadtime**.

Configuration Example

↘ Configuring Accessibility Detection on the RADIUS Server

Scenario **Figure 2-20**	
Configuration Steps	● Configure the global criteria for judging that a RADIUS security server is unreachable. ● Configure the IP address of the remote RADIUS security server, authentication port, accounting port,

	and active detection parameters.

RADIUS Client	`Orion_B54Q(config)#radius-server dead-criteria time120 tries 5`
	`Orion_B54Q(config)# radius-server host 192.168.5.22 test username test ignore-acct-por`
	`time 90`

Verification	Disconnect the network communication between the device and the ser 192.168.5.22. Conduct RADIUS authentication through the d **show radius server** command to check that the server state is **dead**.

	`Orion_B54Q#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`
	`…`

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.	**clear radius dynamic-authorization-extension statistics**

Displaying

Description	Command
Displays global parameters of the RADIUS server.	**show radius parameter**
Displays the configuration of the RADIUS server.	**show radius server**
Displays the configuration of the RADIUS private attribute type.	**show radius vendor-specific**
Displays statistics of the RADIUS dynamic authorization extension function.	**show radius dynamic-authorization-extension statistics**
Displays statistics relevant to RADIUS authentication.	**show radius auth statistics**

Description	Command
Displays statistics relevant to RADIUS accounting.	**show radius acct statistics**
Displays configuration of RADIUS server groups.	**show radius group**

Debugging

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

Description	Command
Debugs the RADIUS event.	**debugradiusevent**
Debugs RADIUS packet printing.	**debugradiusdetail**
Debugs the RADIUS dynamic authorization extension function.	**debug radius extension event**
Debugs the RADIUS dynamic authorization extension packet printing.	**debug radius extension detail**

3 Configuring TACACS+

3.1 Overview

TACACS+ is a security protocol enhanced in functions based on the Terminal Access Controller Access Control (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

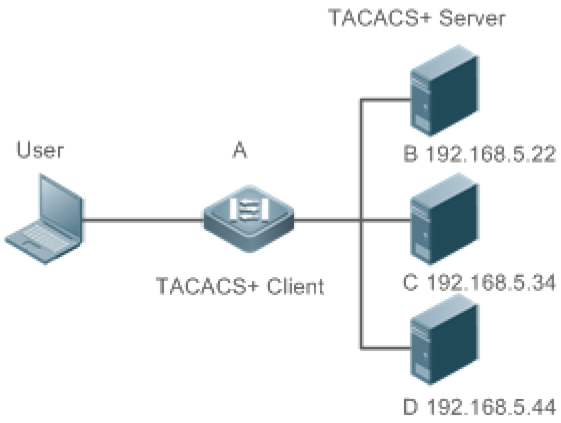
Application	Description
Managing and Controlling End Users	Password verification and authorization need to be conducted on end users.

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 t network device and perform operations a See the following figure.

Figure 3-1



Remarks	● A is a client that initiates TACACS+ requests.

	● B, C, and D are servers that process TACACS+ requests.

Deployment

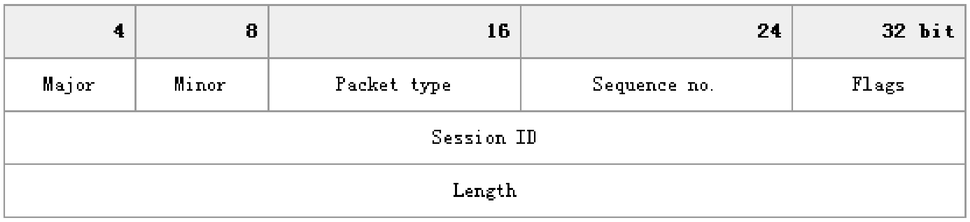
- Start the TACACS+ server on Server B, Server C, and Server D, and configure information on the ac (Device A) so that the servers provide TACACS+-based AAA function for the access device. Enable the AAA function on Device A to start authentication for the user login.
- Enable the TACACS+ client function 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 TA 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 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 t encrypted.
- Session ID: Indicates the ID of a TACACS+ session.
- Length: Indicates the body length of a TACACS+ data packet (excluding the header). Packets transmission on a network.

Overview

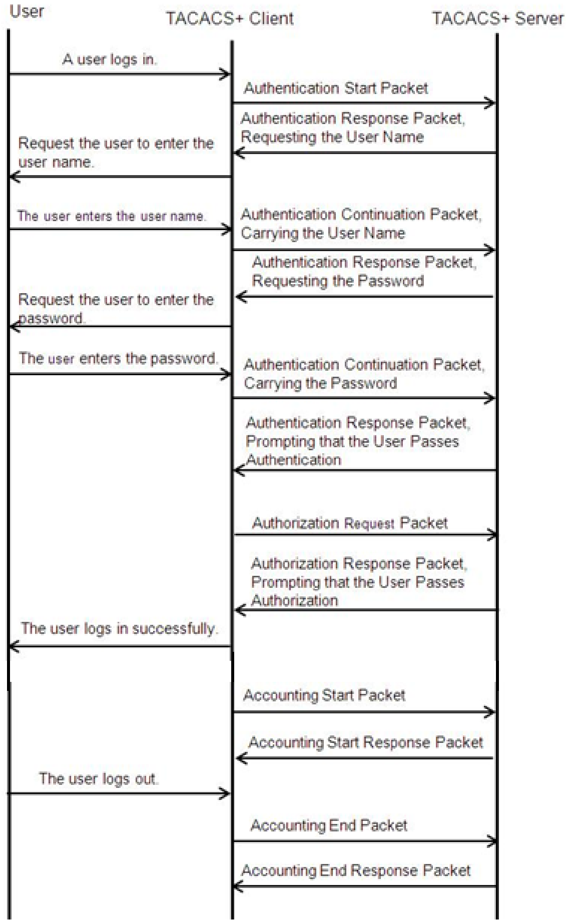
Feature	Description
TACACS+ Authorization, and Accounting	Conducts authentication, authorization, and accounting on end users.

3.3.1 TACACS+ Authentication, Authorization, and Accounting

Working Principle

The following figure uses basic authentication, authorization, and accounting of user l
TACACS+ data packets.

Figure 3-3


User
TACACS+ Client
TACACS+ Server
A user logs in.
Authentication Start Packet
Authentication Response Packet, Requesting the User Name
Request the user to enter the user name.
The user enters the user name.
Authentication Continuation Packet, Carrying the User Name
Authentication Response Packet, Requesting the Password
Request the user to enter the password.
The user enters the password.
Authentication Continuation Packet, Carrying the Password
Authentication Response Packet, Prompting that the User Passes Authentication
Authorization Request Packet
Authorization Response Packet, Prompting that the User Passes Authorization
The user logs in successfully.
Accounting Start Packet
Accounting Start Response Packet
The user logs out.
Accounting End Packet
Accounting End Response Packet

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.

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 configu 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

Configuration	Description and Command	
Configuring TACACS+ Basic Functions	⚠ (Mandatory) It is used to enable the TACACS+ security service.	
	tacacs-server host	Configures the TACACS+ server.
	tacacs-server key	Specifies the key shared by the server and network device.

Configuration	Description and Command	
	tacacs-server timeout	Configures the global waiting timeout time of the TACACS+ server for comm between a network device and the TACACS+ server.
Configuring Sepa Processing of Authentication, Authorization, and Accounting of TACACS+	⚠ (Optional) It is used to separately process authentication, authorization, and accounting requests.	
	aaa group server tacacs+	Configures TACACS+ server gro divides TACACS+ servers i groups.
	server	Adds servers to TACACS+ server groups.

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 authenticat authorization, and accounting requests to configured TACACS+ servers according to the con 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.

Command	**aaa new-model**
Parameter Description	N/A
Defaults	The AAA function is disabled.
Command Mode	Global configuration mode
Usage Guide	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.

Command	**tacacs-server host** [**oob**] [**via** *mgmt_name*] *ipv4-address* [**port** *integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. **oob**: Uses an MGMT port as the source interface for communicating with the TACACS+ server. MGMT port is used for communication by default. **via** *mgmt_name*: Specifies a specific MGMT port when oob supports multiple MGMT ports. **port** *integer*: Indicates the TCP port used for TACACS+ communication. The default TCP port is 49. **timeout** *integer*: Indicates the timeout time of the communication with the TACACS+ server. The timeout time is used by default. **key** [**0** | **7**] *text-string* 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 **0** indicates no encryption and **7** indicates simple encryption. The default value is **0**.
Defaults	No TACACS+ server is configured.
Command Mode	Global configuration mode
Usage Guide	1. You can specify the shared key of the server when configuring the IP address of the serv shared key is specified, the global key configured using the **tacacs-server key** command is used as the shared key of the server. The shared key must be completely the same as that configured on the server. 2. You can specify the communication port of the server when configuring the IP address. 3. You can specify the communication timeout time of the server when configuring the IP address.

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.

Command	**tacacs-server** [**key** [**0** | **7**] *text-string*]
Parameter Description	*text-string*: Indicates the text of the shared key. **0** | **7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7** indicates simple encryption.
Defaults	No shared key is configured for any TACACS+ server.
Command	Global configuration mode

Mode	
Usage Guide	This command is used to configure a global shared key for servers. To specify a different key server, set **key** when running the **tacacs-server host** 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.

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

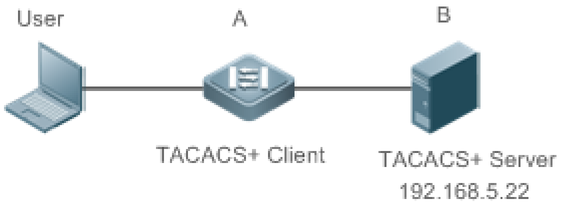
Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on us 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

Scenario **Figure 3-4**	 User A B TACACS+ Client TACACS+ Server 192.168.5.22
Remarks	● A is a client that initiates TACACS+ requests. ● B is a server that processes TACACS+ requests.
Configuration Steps	● Enable AAA. ● Configure the TACACS+ server information.

	● Configure the method of using TACACS+ for authentication. ● Apply the configured authentication method on an interface.
A	Orion_B54Q# configure terminal Orion_B54Q(config)# aaa new-model Orion_B54Q(config)# tacacs-server host 192.168.5.22 Orion_B54Q(config)# tacacs-server key aaa Orion_B54Q(config)# aaa authentication login test group tacacs+ Orion_B54Q(config)# line vty 0 4 Orion_B54Q(config-line)# login authentication test
Verification	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 us TACACS+ server.

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
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 pro
authentication, authorization, and accounting.

- Three TACACS+ server groups need to be configured for separately processing authentication, aut accounting.

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

Command	**server** *ipv4-address*
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server.
Defaults	No server is configured.
Command Mode	TACACS+ server group configuration mode
Usage Guide	Before configuring this command, you must run the **aaa group server tacacs+** command to enter the TACACS+ server group configuration mode. For the address of a server configured in a TACACS+ server group, the server must be configured using the **tacacs-server host** command in global configuration mode. 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.

Configuring VRF of a TACACS+ Server Group

- Optional. Configure Virtual Routing and Forwarding (VRF) if a device needs to send TACACS+ packets t specified address.
- In server group configuration mode, use a configured VRF name to specify the routing for the communication of servers in this group.

Command	**ip vrf forwarding** *vrf-name*
Parameter Description	*vrf-name*: Indicates the VRF name.
Defaults	No VRF is specified by default.
Command	TACACS+ server group configuration mode

Mode	
Usage Guide	Before configuring this command, you must run the **aaa group server tacacs+** command to enter the TACACS+ server group configuration mode. For VRF configured in a TACACS+ server group, a valid name must be configured for VRF by using t **vrf definition** command in global configuration mode.

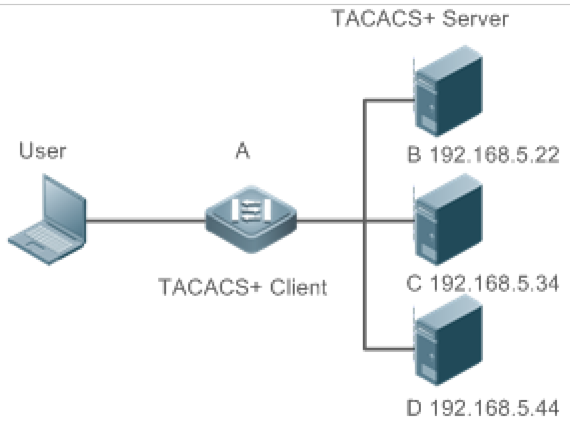
Verification

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

- Enable a device to interact with TACACS+ servers. Conduct packet captu 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, Accounting

Scenario **Figure 3-5**	 TACACS+ Server User A TACACS+ Client B 192.168.5.22 C 192.168.5.34 D 192.168.5.44
Remarks	● A is a client that initiates TACACS+ requests. ● B is a server that processes TACACS+ authentication requests. ● C is a server that processes TACACS+ authorization requests. ● D is a server that processes TACACS+ accounting requests.
Configuration Steps	● Enable AAA. ● Configure the TACACS+ server information. ● Configure TACACS+ server groups. ● Add servers to TACACS+ server groups. ● Configure the method of using TACACS+ for authentication. ● Configure the method of using TACACS+ for authorization. ● Configure the method of using TACACS+ for accounting.

	● Apply the configured authentication method on an interface. ● Apply the configured authorization method on an interface. ● Apply the configured accounting method on an interface.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(Orion_B54Q(config)# aaa new-model`
	`Orion_B54Q(config)# tacacs-server host 192.168.5.22`
	`Orion_B54Q(config)# tacacs-server host 192.168.5.34`
	`Orion_B54Q(config)# tacacs-server host 192.168.5.44`
	`Orion_B54Q(config)# tacacs-server key aaa`
	`Orion_B54Q(config)# aaa group server tacacs+ tacgrp1`
	`Orion_B54Q(config-gs-tacacs)# server 192.168.5.22`
	`Orion_B54Q(config-gs-tacacs)# exit`
	`Orion_B54Q(config)# aaa group server tacacs+ tacgrp2`
	`Orion_B54Q(config-gs-tacacs)# server 192.168.5.34`
	`Orion_B54Q(config-gs-tacacs)# exit`
	`Orion_B54Q(config)# aaa group server tacacs+ tacgrp3`
	`Orion_B54Q(config-gs-tacacs)# server 192.168.5.44`
	`Orion_B54Q(config-gs-tacacs)# exit`
	`Orion_B54Q(config)# aaa authentication login test1 group tacacs+`
	`Orion_B54Q(config)# aaa authentication enable default group tacgrp1`
	`Orion_B54Q(config)# aaa authorization exec test2 group tacgrp2`
	`Orion_B54Q(config)# aaa accounting commands 15 test3 start-stop group tacgrp3`
	`Orion_B54Q(config)# line vty 0 4`
	`Orion_B54Q(config-line)# login authentication test1`
	`Orion_B54Q(config-line)#authorization exec test2`
	`Orion_B54Q(config-line)# accounting commands 15 test3`

Verification	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 **enable** command and enter the correct **enable** password to initiate **enable** authentication. Enter the privilege EXEC mode after authentication. Perform operations on the device and then exit the device. View the authentication log of the user on the server with the IP address of 192.168.5.22. View the **enable** authentication log of the user on the server with the IP address of 192.168.5.22.

	View the **exec** authorization log of the user on the server with the IP address of 192.168.5.34. View the command accounting log of the user on the server with the IP address of 192.168.5.44.

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.	**show tacacs**

Debugging

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

Description	Command
Debugs TACACS+.	**debug tacacs+**

4 Configuring 802.1X

4.1 Overview

IEEE 802.1X is a standard for port-based network access control that provides secure access service for local area networks (LANs).

In IEEE 802-compliant LANs, users connecting to the network access devices (NASs) can access network resources without authentication and authorization, bringing security risks to the network. IEEE 802.1X was proposed to resolve security problems of such LANs.

Before user authentication succeeds, only EAPOL pa
802.1X packets) can be transmitted over the network for authentication.

802.1X supports three security applications: authentication, authorization, and accounting, which are called AAA.

- Authentication: Checks whether to allow user access and restricts unauthorized users.
- Authorization: Grants specified services to users and controls permissions of authorized users.
- Accounting: Records network resource status of users to provide statistics for charges.

Protocols and Standards

- IEEE 802.1X: Port-Based Network Access Control

4.2 Applications

Application	Description
Wired 802.1X Authentication	To ensure secure admission on the campus network, 802.1 deployed on access switches.

4.2.1 Wired 802.1X Authentication

Scenario

The campus network is deployed at the access, convergence, and core layers. 802.1X is deployed on acce connected to dormitories to perform secure admission. Dormitory users must pass 802.1X authentication before accessing the campus network.

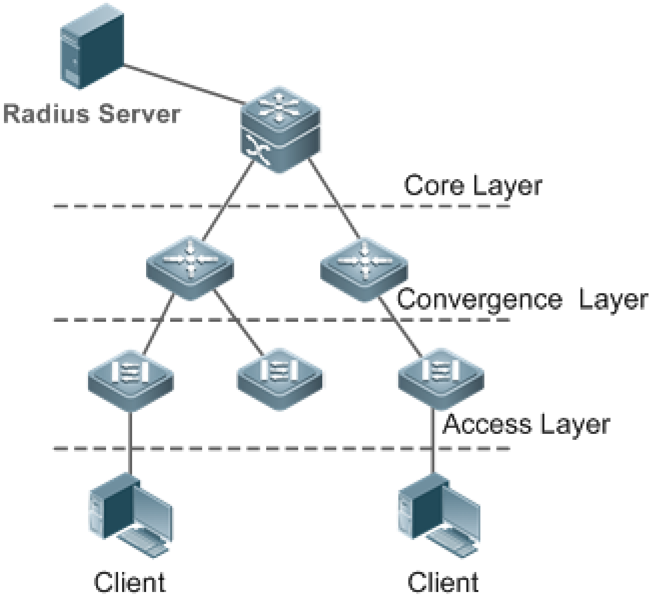
As shown in Figure 4 -21:

- User ends must be installed with 802.1X clients (which can come with the operating system, or others like Orion_B54Q Supplicant).

- Access switches support 802.1X.

- One or multiple Remote Authentication Dial-In User Service (RADIUS) servers perform authentication.

Figure 4-21



Remarks	The supplicant software installed on the user ends (or software coming with the operating sys 802.1X authentication. 802.1X authentication is deployed on access switches, convergence switc switches. The RADIUS server runs the RADIUS server software to perform identity verification.

Deployment

- Enable 802.1X authentication on ports between access switches and users to make ports controllable.

- Configure an AAA authentication method list.

- Configure RADIUS parameters. For details, see the *Configuring RDS*.

- If a Orion_B54Q RADIUS server is used, configure SNMP parameters.

- Configure the port between the access switch and the RADIUS server as an uncontrolled por communication between them.

- Create an account on the RADIUS server, register the IP address of an access switch, and configure RADIUS-related parameters.

4.3 Features

Basic Concepts

↘ User

802.1X is a LAN-based protocol. It identifies users based on physical information but not accounts. In a LAN
identified by the MAC address and VLAN ID (VID). Except them, all other information such as the account ID and IP address can be changed.

↘ RADIUS

RADIUS is a remote authentication protocol defined in RFC2865, which get wide prac
authentication server can remotely deploy and perform authentication. During 802.1X deployment, the authentication server is remotely deployed, and 802.1X authentication information between the NAS and the authentication server is transmitted through RADIUS.

↘ Timeout

During authentication, an NAS needs to communicate with the authentication client and server. If the authentication client or server times out, not responding within
During deployment, ensure that the timeout specified by 802.1X is longer than that specified by RADIUS.

↘ MAB

MAC address bypass (MAB) authentication means that the MAC address is used as the user name and
authentication. Since Orion_B54Q Supplicant cannot be installed on some dumb ends such as network printers, use MAB to perform security control.

↘ EAP

802.1X uses Extensible Authentication Protocol (EAP) to carry authentication information
provides a universal authentication framework, in which multiple authentication modes are embedded, including Me
Digest Algorithm 5 (MD5), Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP),
and Transport Layer Security (TLS). Orion_B54Q 802.1X authentication supports variou
CHAP, PAP, PEAP-MSCHAP, and TLS.

↘ Authorization

Authorization means to bind specified services to authenticated users, such as IP address, VLAN, Ac
(ACL), and Quality of Service (QoS).

↘ Accounting

Accounting performs network audit on network usage duration and traffic for users, which facilitates ne
maintenance, and management.

Some RADIUS servers such as ORIONSAM\ORIONSMP servers need to check the online

/offline status based on accounting packets. Therefore, accounting must be enabled on these RADIUS servers.

Overview

Feature	Description
Authentication	Provides secure admission for users. Only authenticated users can access the network.
Authorization	Grants network access rights to authenticated users, such as IP address binding and ACL binding
Accounting	Provides online record audit, such as online duration and traffic.

4.3.1 Authentication

Authentication aims to check whether users are authorized and prevent unauthorized users from accessing the Users must pass authentication to obtain the network access permission. They can access the netv authentication server verifies the account.

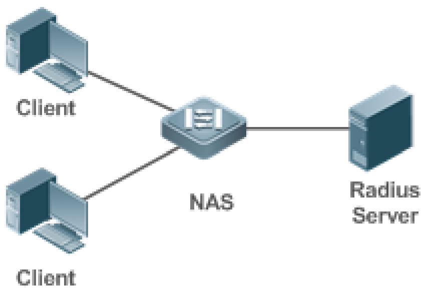
Working Principle

802.1X authentication is very simple. After a user submits its account information, the NAS sends the account information to the remote RADIUS server for identity authentication. If the authentication succeeds, the user can access the network.

Roles in Authentication

802.1X authentication involves three roles: supplicant, authenticator, and server. In real applications, their respective roles are client, network access server (NAS), and authentication server (mostly RADIUS server).

Figure 4-22



- Supplicant

The supplicant is the role of end users, usually a PC. It requests to access network services and replies to t packets of the authenticator. The supplicant must run software compliant with the 802.1X standard. Except the typical 802.1X client support embedded in the operating system, Orion_B54Q has launched a Orion_B54Q Supplicant compliant with the 802.1X standard.

- Authenticator

The authenticator is usually an NAS such as a switch or wireless access hotspot. It controls the network connectio client based on the client's authentication status. As a proxy between the client and authenticator requests the user name from the client, verifies the authentication information from the authentication server, and forwards it to the client. Except as the 802.1X authenticator, the so-called NAS also acts as a RADIU encapsulates the replies of the client into the RADIUS-format packets and forwards the packets to the RADIUS server. After receiving the information from the RADIUS server, it interprets the information and forwards it to the client.

The authenticator has two types of ports: controlled port and uncontrolled port. Users connected to controll access network resources only when authenticated. Users connected to uncontrolled ports can directly resources without authentication. We can connect users to controlled ports to control users. Uncontrolled ports are mainly used to connect the authentication server to ensure proper communication between the authentication server and the NAS.

- Authentication server

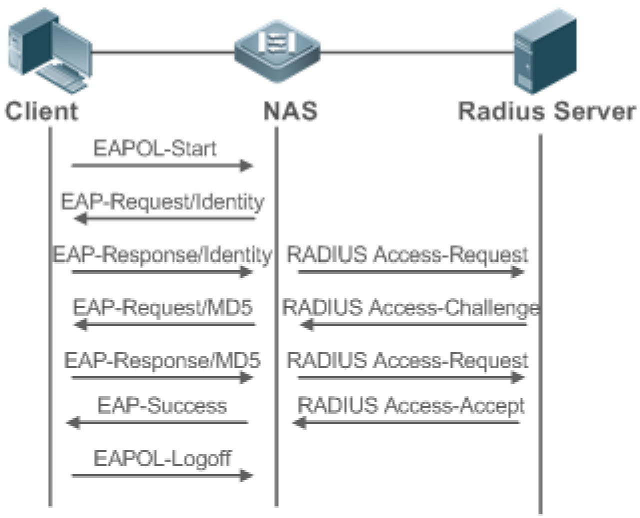
The authenticator server is usually an RADIUS server. It cooperates with the authenticator to provide authentication service for users. The authentication server saves the user names, passwords, and related authorization information. One server can provides authentication service for multiple authenticators to achieve centralized user managemen server also manages accounting data received from authenticators. Omicron_B54Q RADIUS servers compliant with 802.1X standard include Microsoft IAS/NPS, Free RADIUS Server, and Cisco ACS.

↘ Authentication Process and Packet Exchange

The supplicant exchanges information with the authenticator through EAPOL whil authentication server through RADIUS. EAPOL is encapsulated on the MAC layer, with the type number of 0x888E. IEEE assigned a multicast MAC address 01-80-C2-00-00-03 for EAPOL to exchange packets during initial authentication.

Figure 4 -23 shows the typical authentication process of a wired user.

Figure 4-23



This is a typical authentication process initiated by a user. In special cases, the NAS, may take place of the user to initiate an authentication request.

↘ Authenticating User Status

802.1X determines whether a user on a port can access the network based on the authenticatio Orion_B54Q products extend the 802.1X and realizes access control based on users (identify a user by the MAC address and VLAN ID) by default. Orion_B54Q 802.1X can also be enabled in interface configuration mode. For details, se chapter "Configuration."

All users on an uncontrolled port can access network resources, while users on a controlled port ca resources only after authenticated. When a user initiates authentication, its status remains Unauthenticated and access the network yet. After it passes authentication, its status changes to Authenticat resources.

If the user connected to a controlled port does not support 802.1X, it will not respond to the NAS requesting the user name of the user. That means, the user remains Unauthenticated and cannot access network resources.

In the case of 802.1X-enabled user and 802.1X-disabled NAS, if the user does not receive any responses after sending a specified number of EAPOL-Start packets, it regards the connected port uncontrolled an resources.

On 802.1X-enabled devices, all ports are uncontrolled by default. We can configure a port as controlled so that all users on this port have to be authenticated.

If a user passes authentication (that is, the NAS receives a success packet from the RADIUS server), the user becc Authenticated and can freely access network resources. If the user fails in authentication, it remains Unauthenticated and re-initiates authentication. If the communication between the NAS and the RADIUS serv Unauthenticated and cannot access network resources.

When a user sends an EAPOL-LOGOFF packet, the user's status changes from Authenticated to Unauthenticated.

When a port of the NAS goes down, all users on this port will become Unauthenticated.

When the NAS restarts, all users on it become Unauthenticated.

If you want to forcibly make a client free from authentication, it is recommended to add a static MAC address or enable the IP-MAC binding.

↘ Deploying the Authentication Server

802.1X authentication uses the RADIUS server as the authentication server. Therefore, when 802.1X secure admission is deployed, the RADIUS server also needs to be deployed. Common RADIUS servers include Microsoft IAS/NPS, Cisco ACS, and ORIONSAM/SMP. For details about the deployment procedure, see related software description.

↘ Configuring Authentication Parameters

To use 802.1X authentication, enable 802.1X authentication on the access port and configure AAA authentication metho list and RADIUS server parameters. To ensure the accessibility between the NAS and RADIUS server, the 802.1X server timeout should be longer than the RADIUS server timeout.

Supplicant

A user should start Orion_B54Q Supplicant to enter the user name and initiate authentication. If the operating system brings an own authentication client and the network is available, a dialog box will be displayed, asking the user to enter the user name. Different clients may have different implementation processes and Gra recommended to use Orion_B54Q Supplicant as the authentication client. If other software is used, see related description.

Offline

If a user does not want to access the network, it can ch such as powering off the device, connecting the port to the network, and offline function provided by some supplicants.

Configuration Steps

Enabling 802.1X

- By default, 802.1x is disabled.
- In the interface configuration mode, run the **dot1x port-control auto** command to enable or disable 80 authentication on a port.

Configuring a Method List

- By default, there is not a method list configured for AAA.
- In the global configuration mode, run the **aaa new-model** command to enable AAA. Then, run the **aaa authentication dot1x** *list-name* **group radius** command to configure an authentication method list. It is recommended to use “default” as the list name. If the list name is not “default”, run the **dot1x authentication** *list-name* to ensure the same list name. For the usage guide of method lists, please refer to *AAA-SCG*.

Configuring RADIUS

- By default, there is not RADIUS information.
- Run the **radius-server host** command to configure the IP address and port information of the RADIUS server and the **radius-server key** command to configure the RADIUS communication key between the NAS and the RADIUS server to ensure secure communication.

Configuring Timeout

- 802.1X and RADIUS have separate server timeouts. By default, the authentication server time seconds while that of RADIUS is 15 seconds. In actual situations, ensure that the former is greater than the latter. You can run the **dot1x timeout server-timeout** command to adjust the authentication server timeout of 802.1X.

4.3.2 Authorization

After a user passes authentication, the NAS restricts the accessible network resources of the user in multiple approaches, such as binding the IP address and the MAC address, and specifying the maximum online time or period, accessible VLANs, and bandwidth limit.

Working Principle

Authorization means to bind the permissions with the users. A user is identified based on the MAC address and VLAN ID, as mentioned before. Besides MAC-VID binding, some other information such as the IP address and VLAN ID are bound with a user to implement authorization.

↘ IP Authorization

802.1X does not support IP address identification. Orion_B54Q 802.1X authentication extends 802.1X to support IP-M binding, which is called IP authorization. IP authorization supports four modes:

Supplicant authorization: The IP address is provided by Orion_B54Q Supplicant.

RADIUS authorization: After successful authentication, the RADIUS server delivers the IP address to the NAS.

DHCP authorization: In such case, an authenticated user will initiate a DHCP request to obtain an IP address, and then bind the IP address with the MAC address of the client.

Mixed authorization: IP-MAC binding is configured for users in the following sequence: Supplicant authorization -> RADIUS authorization -> DHCP authorization. That is, the IP address provided by Orion_B54Q Supplicant preferred, then th address provided by the RADIUS server, and finally the IP address provided by DHCP.

↘ Kickoff

Used with ORIONSAM/SMP, Orion_B54Q 802.1X server can kick off online users who will be d network. This function applies to the environment where the maximum online period and real-time accounting check function are configured.

Related Configuration

↘ Configuring IP Authorization

- By default, 802.1x ip authorization is disabled.
- In the global configuration mode, run the **aaa authorization ip-auth-mode** command to configure ip authentication.

↘ Enabling Dynamic VLAN Assignment on a Port.

- By default, vlan jumping is disabled.
- In the interface configuration mode, run the **dot1x dynamic-vlan** command to enable. Enables dynamic VLAN assignment on a port.

↘ Kickoff

- This function of Orion_B54Q's SAM/SMP is based on the snmp protocol. Therefore, snmp parameters configured. For more details, please refer to *SNMP-SCG*.

4.3.3 Accounting

Accounting allows the network operators to audit the network access or fees of accessed users, including the online time and traffic.

Working Principle

Accounting is enabled on the NAS. The RADIUS server supports RFC2869-based accounting. When a user goes online, the NAS sends an accounting start packet to the RADIUS server which then starts accounting. When the user goes offline, the NAS sends an accounting end packet to the RADIUS server which then completes the accounting and generates a network fee accounting list. Different servers may perform accounting in different ways. Moreover, not all servers support accounting. Therefore, refer to the usage guide of the authentication server during actual deployment and accounting.

↘ Accounting Start

After a user passes authentication, the accounting-enabled switch sends the RADIUS server an accounting carrying user accounting attributes such as user name and accounting ID. After receiving the packet, the RADIUS se starts accounting.

↘ Accounting Update

The NAS periodically sends Accounting Update packets to the RADIUS server, making the accounting The accounting update interval can be provided by the RADIUS server or configured on the NAS.

↘ Accounting End

After a user goes offline, the NAS sends the RADIUS server an accounting end packet carrying the online period and traffic of the user. The RADIUS server generates online records based on the information carried in this packet.

Configuration Steps

↘ Configuring an AAA Authentication Method List

- By default, there is no aaa authentication method list.
- In the global configuration mode, run the **aaa accounting network** command to configure an aaa anthentication method list. It is recommended to use the default method name. If not, run the **dot1x accounting** command to ensure an accurate accounting list.

↘ Configuring RADIUS

- By default, there is not RADIUS information.
- Run the **radius-server host** command to configure the IP address and port information of the RADIUS server and the **radius-server key** command to configure the RADIUS communication key between the NAS and the RADIUS server to ensure secure communication.

↘ Configuring Accounting Update

- By default, this function is disabled.
- Run the **aaa accounting update** command in global configuration mode to enable accounting u **aaa accounting update interval** command on the NAS to configure the accounting update interval. If the RADIUS server supports accounting update, you can also configure it on the RADIUS server. Prefer to use the parameters assigned by the authentication server than the parameters configured on the NAS.

4.4 Configuration

Configuration	Description and Command	
Configuring 802.1X Basic Functions	⚠ (Mandatory) It is used to configure basic authentication and accounting. ⚠ 802.1X uses the default method list by default. If the default method list is not configured for AAA, run the **dot1x authentication** and **dot1x accounting** commands to reconfigure it. ⚠ When ORIONSAM/SMP is used, accounting must be enabled. Otherwise, the RADIUS server will fail to detect users going offline, causing offline users remaining in the online user table.	
	aaa new-model	Enables AAA.
	aaa authentication dot1x	Configures an AAA authentication me list.
	aaa accounting networks	Configures an AAA accounting method list.
	radius-server host	Configures the RADIUS server parameters.
	radius-server key	Configures the communication between the NAS and t RADIUS server.
	dot1x port-control auto	Enables 802.1X authentication on a port.
Configuring 8 Parameters	⚠ (Optional) It is used to configure 802.1X parameters. ⚠ Ensure that the 802.1X server timeout is longer than the RADIUS server timeout. ⚠ Online Orion_B54Q client detection applies only to Orion_B54Q Supplicant.	
	dot1x re-authentication	Enables re-authentication.
	dot1x timeout re-authperiod	Configures the re-authentication interval.
	dot1x timeout tx-period	Configur EAP-Request/Identity packet retransmission.
	dot1x reauth-max	Configures the maximum times Request/Identity packet retransmission.

	dot1x timeout supp-timeout	Configur EAP-R retransmission.
	dot1x max-req	Configures the maximum times Request/Challenge packet retransmission.
	dot1x timeout server-timeout	Configures the authentication server timeout.
	dot1x timeout quiet-period	Configures the authentication fails.
	dot1x auth-mode	Specifies the (EAP/CHAP/PAP).
	dot1x client-probe enable	Enables online Orion_B54Q client detection.
	dot1x probe-timer interval	Configures the interval of online Orion_B54Q client detection.
	dot1x probe-timer alive	Configures the duration of online Orion_B54Q client detection.
Configuring Authorization	⚠ (Optional) It is used to configure authorization. ⚠ Orion_B54Q Supplicant should be used to perform supplica authorization mode.	
	aaa authorization ip-auth-mode	Specifies the IP authorization mode.
	dot1x private-supplicant-only	Filters non-Orion_B54Q clients.
	dot1x redirect	Enables Web Redirection for 2G Orion_B54Q Supplicant Deployment.
	snmp	Configur ORIONSAM/SMP can implement functio for 802.1X online users throu SNMP parameters should be configured to implement such functions.
Configuring MAB	⚠ (Optional) It is used to configure MAC Authentication Bypass (MAB). ⚠ 802.1X authentication takes priority over MAB. ⚠ MAB does not support IP authorization. ⚠ Single-user MAB and multi-user MAB cannot be enabled at the same time. ⚠ MAB adopts the PAP authentication mode. Ensure correct server configurations during deployment.	
	dot1x mac-auth-bypass	Enables single-user MAB.
	dot1x mac-auth-bypass multi-user	Enables multi-user MAB.
	dot1x multi-mab quiet-period	Configures the quiet period after multi-user MAB fails.

	dot1x mac-auth-bypass timeout-activity	Configures the timeout of MAB users.
	dot1x mac-auth-bypass violation	Enables MAB violation mode.
	dot1x mac-auth-bypass vlan	Configures VLAN-based MAB.
Configuring IAB	**dot1x critical**	Enables IAB.
	dot1x critical recovery action reinitialize	Enables IAB recovery.
Configuring Extended Functions	**dot1x auto-req**	Enables active authentication.
	dot1x auto-req packet-num	Configures the authentication requests.
	dot1x auto-req user-detect	Enables user de authentication.
	dot1x auto-req req-interval	Configures the authentication request.
	dot1x auth-address-table address	Configures the authenticatable client list.
	dot1x pseudo source-mac	Enables 802.1X packets sending with pseudo source MAC address.
	dot1x multi-account enable	Enables multi-account authenti one MAC address.
	dot1x valid-ip-acct enable	Enables IP-triggered accounting.
	dot1x valid-ip-acct timeout	Configures the timeout of addresses after users get authenticated. timeout is reached, they will be kicked off.

4.4.1 Configuring 802.1X Basic Functions

Configuration Effect

- Enable basic authentication and accounting services.

Notes

- Configure accurate RADIUS parameters so that the basic RADIUS communication is proper.
- The 802.1X authentication method list and accounting method list must be configured in AAA. Otherwise, errors may occur during authentication and accounting.
- Due to chipset restriction on switches, if 802.1X is enabled on one port, all ports will send 802.1X packets to the CPU.
- If 802.1X is enabled on a port but the number of authenticated users exceeds the maximum number of users configured for port security, port security cannot be enabled.
- If port security and 802.1X are both enabled but the security address has aged, 802. authentication requests to continue the communication.
- Users with IP addresses statically configured or compliant with IP-MAC binding can acce authentication.

Configuration Steps

Enabling AAA

- Mandatory.

Configuring the RADIUS Server Parameters

- Mandatory.
- The IP address of the NAS must be the same as that registered on the RADIUS server.
- The preshared key on the NAS must be the same as that on the RADIUS server.
- If the default RADIUS communication ports are changed on the RADIUS communication ports on the NAS correspondingly.

Configuring 802.1x

- Mandatory.
- The default method list is used by default. If the 802.1X authentication method list in AAA is not the default one, the configured 802.1X authentication method list should match.

Verification

Start Orion_B54Q Supplicant, enter the correct account information, and initiate authentication. Then chec 802.1X and RADIUS configurations are correct.

- Run the **show dot1x summary** command to check for 802.1X authentication entries.
- Run the **show aaa user all** command to check for aaa user entries.
- Check whether the RADIUS server responds to authentication based on the RADIUS packets between the NAS and the RADIUS server. If no, it means that the network is disconnected or parameter configurations ar RADIUS server directly returns a rejection reply, check the log file on the RADIUS server to identify the cause, e.g., of the authentication mode of the authentication server is incorrectly configured.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	AAA is disabled by default. This command is mandatory for the deployment of 802.1X authentication.

Configuring the RADIUS Server Parameters

Command	**radius-server host** *ip-address* [**auth-port** *port1*] [**acct-port** *port2*]
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server. *port1*: Indicates the authentication port. *port2*: Indicates the accounting port.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the Preshared Key for Communication between the NAS and RADIUS Server

Command	**radius-server key** *string*
Parameter Description	*string*: Indicates the preshared key.
Command Mode	Global configuration mode
Usage Guide	N/A

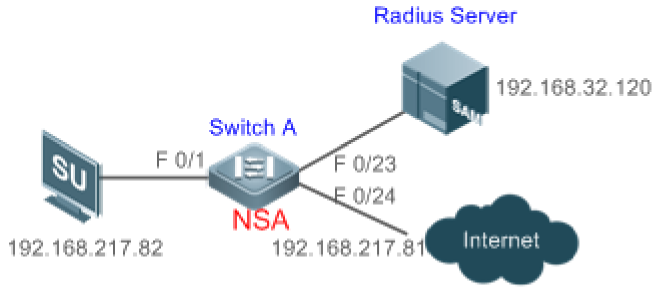
↘ Enabling 802.1X

Command	**dot1x port-control auto**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	802.1X is disabled on a port by default. This command is mandatory for the deployme authentication.

Configuration Example

In this example, ORIONSAM acts as the authentication server.

↘ Configuring 802.1X Authentication

Scenario **Figure 4-24**	 Radius Server 192.168.32.120 SAM Switch A SU F 0/1 F 0/23 F 0/24 NSA 192.168.217.82 192.168.217.81 Internet
Configuration Steps	● Register the IP address of the switch on the RADIUS server and configure the communication key between the switch and the RADIUS server.

	● Create an account on the RADIUS server. ● Enable AAA on the switch. ● Configure RADIUS parameters on the switch. ● Enable 802.1X authentication on ports of the switch. Switch configurations are as follows. For detailed configuration on the RADIUS *Configuring RADIUS*.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q (config)# aaa new-model`
	`Orion_B54Q (config)# radius-server host 192.168.32.120`
	`Orion_B54Q (config)# radius-server key Orion_B54Q`
	`Orion_B54Q (config)# interface FastEthernet 0/1`
	`Orion_B54Q (config-if)# dot1x port-control auto`

Verification	Check whether authentication is proper and network access behaviors change after authentication. ● The account is successfully created, such as **username:test,password:test**. ● The user fails to ping 192.168.32.120 before authentication. ● After the user enters account information and click **Authenticate** on Orion_B54Q Supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120.

Common Errors

- RADIUS parameters are incorrectly configured.
- The RADIUS server has a special access policy, for example, the RADIUS packets must carry certain attributes.
- The AAA authentication mode list is different from the 802.1X authentication mode list, causing authentication failure.

4.4.2 Configuring 802.1X Parameters

Configuration Effect

- Adjust 802.1X parameter configurations based on the actual network situation. For example, if the authentication server has poor performance, you can raise the authentication server timeout.

Notes

- Ensure that the authentication server timeout is greater than the timeout of RADIUS. For detailed configuration about the RADIUS server timeout, see the *Configuring RADIUS*.

- Online client detection applies only to Orion_B54Q Supplicant.

Configuration Steps

↘ Configuring 802.1X Parameters

- Enable re-authentication to lauch mandatory authentication to authenticated users over a certain period of time.
- When using Orion_B54Q Supplicant, you are recommended to enable client detection to ensure the accurancy of online statistics.

Verification

Run the **show dot1x** command to check whether parameter configurations take effect.

Related Commands

↘ Enabling Re-authentication

Command	**dot1x re-authentication**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Re-authentication is disabled by default.

↘ Configuring the Re-authentication Interval

Command	**dot1x timeout re-authperiod** *period*
Parameter Description	*period*: Indicates the re-authentication interval in the unit of seconds. *port1*: authentication port *port2*: accounting port
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the Interval of EAP-Request/Identity Packet Retransmission

Command	**dot1x timeout tx-period** *period*
Parameter Description	*period*: Indicates the interval of EAP-Request/Identity packet retransmission in the unit of seconds.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the Maximum Times of EAP-Request/Identity Packet Retransmission

Command	**dot1x reauth-max** *num*
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Identity packet retransmission.
Command Mode	Global configuration mode

Usage Guide	N/A

Configuring the Interval of EAP-Request/Challenge Packet Retransmission

Command	**dot1x timeout supp-timeout** *time*
Parameter Description	*time*: Indicates the interval of EAP-Request/Challenge packet transmission in the unit default value is 3 seconds.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Maximum Times of EAP-Request/Challenge Packet Retransmission

- (Optional) A larger value indicates more frequent retransmissions.
- Configure the maximum times of EAP-Request/Challenge packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x max-req** *num*
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Challenge packet retransmission in the unit of seconds.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Authentication Server Timeout

Command	**dot1x timeout server-timeout** *time*
Parameter Description	*time*: Indicates the authentication server timeout in the unit of seconds. The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Quiet Period after Authentication Fails

Command	**dot1x timeout quiet-period** *time*
Parameter Description	*time*: Indicates the quiet period after authentication fails. The unit is second. The seconds.
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Authentication Mode

Command	**dot1x auth-mode** {**eap** | **chap** | **pap**}

Parameter Description	**eap**: Indicates EAP authentication. **chap**: Indicates CHAP authentication. **pap**: Indicates PAP authentication.
Command Mode	Global configuration mode
Usage Guide	Select the authentication mode supported by Orion_B54Q Supplicant and authentication server. The default value is **eap**.

Enabling Online Orion_B54Q Client Detection

Command	**dot1x client-probe enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	It is recommended to enable this function when Orion_B54Q Supplicant is used.

Configuring the Interval of Online Orion_B54Q Client Detection

Command	**dot1x probe-timer interval** *time*
Parameter Description	*time* Indicates the time interval after failed authentication. The unit is second. The def seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value.

Configuring the Duration of Online Orion_B54Q Client Detection

Command	**dot1x probe-timer alive** *time*
Parameter Description	*time*: Indicates the duration of online Orion_B54Q client detection in the unit of seconds. The default value is 60 seconds.
Command Mode	Global configuration mode
Usage Guide	If the NAS does not receive any detection packets from an online client within the detection regards the client offline. It is recommended to use the default value.

Configuration Example

- It is recommended to apply default configuration.

Common Errors

- The server timeout is shorter than the RADIUS timeout.
- Online client detection is enabled but the authentication program is not Orion_B54Q Supplicant.

4.4.3 Configuring Authorization

Configuration Effect

- In IP authorization, authenticated users have to use the specified IP addresses to access the network, preventing IP address fake.
- Enable non-Orion_B54Q client filtering. If this function is enabled, users must u authentication so that they will enjoy services provided by Orion_B54Q Supplicant, such as anti-proxy or SMS.
- Enable Web redirection to support 2G Orion_B54Q Supplicant deployment. 2G Orion_B54Q Supplicant dep means that a user needs to download Orion_B54Q Supplicant through the browser and then initiate auth through Orion_B54Q Supplicant. 2G Orion_B54Q Supplicant deployment facilitates quick deployment of Orion_B54Q Supplicant in the case of massive users.

Notes

- If the real-time kickoff function of ORIONSAM/SMP is used, you need to configure correct SNMP para details, see the *Configuring SNMP*.
- If multiple authentication supplicants are used, disable this function.
- If the IP authorization mode is changed, all authenticated users will go offline and have to get re-authenticated before online again.
- In mixed authorization mode, IP authorization with a higher priority is used during user authentication. For example, if Orion_B54Q Supplicant provides an IP address for this RADIUS-authentication user during its re-authentication, this IP address will be used for authorization.
- 2G Orion_B54Q Supplicant deployment and Web authentication cannot be used at the same time.
- 2G Orion_B54Q Supplicant deployment requires the setting of the**redirect** parameter. For details, see the *Configuring Web Authentication*.

Configuration Steps

Specifying the IP Authorization Mode

- The **supplicant** mode only applies to Orion_B54Q Supplicant.
- In **radius-server** mode, the authentication server needs to assign IP addresses based on the **framed-ip** parameters.
- In **dhcp-server** mode, DHCP snooping or dhcp relay must be enabled on the NAS.

Enabling Web Redirection for 2G Orion_B54Q Supplicant Deployment

- The **redirect** parameter must be configured. For details, see the *Configuring Web Authentication*.

Verification

- After IP authorization is enabled, use the client to initiate authentication and go online, and then change the IP address. As a result, the client cannot access the network.
- Enable Web redirection for 2G Orion_B54Q Supplicant deployment. When you start the browser to visit a website, the system automatically redirects to the download Web page and downloads the authentication client. You can access the network only when authenticated by the client.
- After a user is authenticated and goes online, enable the kickoff function on ORIONSAM/SMP. The NAS will force the user offline and the user will fail to access the network.

Related Commands

↘ Specifying the IP Authorization Mode

Command	**aaa authorization ip-auth-mode** { **disable** | **supplicant** | **radius** **mixed** }
Parameter Description	**disable**: Disables IP authorization. **supplicant**: Indicates IP authorization by the supplicant. **radius-server**: Indicates IP authorization by the RADIUS server. **dhcp-server**: Indicates IP authorization by the DHCP server. **mixed**: Indicates IP authorization in a mixed manner.
Command Mode	Global configuration mode
Usage Guide	Select the IP authorization mode based on actual deployment.

↘ Enabling Non-Orion_B54Q Client Filtering

Command	**dot1x private-supplicant-only**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This function can be enabled only when Orion_B54Q Supplicant is used.

↘ Configuring Redirection for 2G Orion_B54Q Supplicant Downloading

Command	**dot1x redirect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The **redirect** parameter must be configured. For details, see the *Configuring Web Authentication*.

Configuration Example

- It is recommended to use the default parameters.

Common Errors

- There are multiple authentication clients on the network but non-Orion_B54Q client filtering is enabled, causing some users to fail authentication.
- ORIONSAM/SMP is used but SNMP parameters are not configured on the switch, causing kickoff failure.
- The **redirect** parameter is incorrectly configured, causing abnormalities in redirection for 2G Orion_B54Q Supplica downloading.

4.4.4 Configuring MAB

Configuration Effect

- If the MAC address of an access user is used as the authentication account, the user does not need to ins supplicants. This applies to some dumb users such as networking printers.
- Single-user MAB applies to two scenarios:
  - There is only one dumb user connected to a port.
  - Only one user needs to be authenticated. After this, all other users can access the network. For example, if a port is connected with a wireless router, you can enable real-time MAB on the wireless router. If authentication succeeds, all users connected to the wireless router can access the network.
- Multi-user MAB applies to the scenario where multiple dumb users connected to a port. For example, multiple devices are deployed in the network call center.
- Multi-user MAB can be used with 802.1X authentication. It applies to mixed access scenarios such as the PC daisy-chain topology.

Notes

- A MAB-enabled port sends an authentication request packet as specified by **tx-period**. If the number of the sent packets exceeds the number specified by **reauth-max** but still no client responds, this port enters the MAB mode. Ports in MAB mode can learn the MAC addresses and use them as the account information for authentication.
- When using the MAC address as the user name and password on the authentication server, delete all delimiters. For example, if the MAC address of a user is 00-d0-f8-00-01-02, the user name and p 00d0f8000102 on the authentication server.
- 802.1X takes priority over MAB. Therefore, if a user having passed MBA authentication uses a client to initiate 802.1X authentication, MAB entries will be removed.
- MAB supports only PAP authentication. PAP authentication should be enabled also on the authentication server.

- Only when active authentication is enabled, can MAB detect whether the user can perform 802.1X a Therefore, automatic authentication must be enabled for MAB deployment.

Configuration Steps

Enabling Single-User MAB

- Single-user MAB applies when only one user connected to a port needs to be authenticated.

Configuring the Timeout of MAB Users

- Optional. The MAB timeout applies to both single-user MAB and multi-user MAB.
- After a MAC address in MAB mode is authenticated and goes online, the NAS regards the MAC address online unless re-authentication fails, the port goes down, or the MAC address goes offline due to management poli kickoff. You can configure the timeout of authenticated MAC addresses. The default value is 0, ind online.

Enabling the MAB Violation Mode

- Optional. The MAB violation mode only applies to single-user MAB.
- By default, after one MAC address passes MAB authentication, data of all switches connected to the forwarded. However, for security purposes, the administrator may request one MAB port to support onl address. In this case, you can enable MAB violation on the port. If more than one MAC address is found connected to a MAB violation-enabled port after the port enters MAB mode, the port will become a violation.

Enabling Multi-user MAB

- Multi-user MAB applies when multiple users connected to a port needs to be authenticated.

Configuring the Quiet Period after Multi-user MAB Fails

- If multi-user MAB is enabled, you should prohibit unauthorized users from frequently initiating authentication to protect the NAS from attacks of these users and thereby re Configure the quite period of the multi-user MAB failure in global configuration mode. That is, if a MAC address fails authentication, it needs to re-initiate authentication after the quiet period. Configure this quiet perio actual situation. The default value is 0, indicating that a user can re-initia authentication fails.

Configuring VLAN-based MAB

- If you configure VLANs as MAB VLANs, only users in these VLANs can perform MAB.

Verification

Check whether the dumb user can access the network. If yes, MAB takes effect. If no, MAB does not take effect.

- Check whether MAB functions are configured on the authentication server and NAS.
- Check whether dumb users with illegitimate MAC addresses cannot access the network.

- Check whether dumb users with illegitimate MAC addresses can access the network.

Related Commands

↘ Enabling Single-User MAB

Command	**dot1x mac-auth-bypass**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Single-user MAB applies when only one dumb user connected to a port needs to be authenticated. If you want to restrict the number of users, enable the violation mode.

↘ Configuring the Timeout of MAB Users

Command	**dot1x mac-auth-bypass timeout-activity** *value*
Parameter Description	*value*: Indicates the maximum online time of MAB users in the unit of seconds.
Command Mode	Interface configuration mode
Usage Guide	N/A

↘ Enabling the MAB Violation Mode

Command	**dot1x mac-auth-bypass violation**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Configure this command only when only one dumb user is connected to the port.

↘ Enabling Multi-user MAB

Command	**dot1x mac-auth-bypass multi-user**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Configure this command when multiple dumb users connected to the port need to be authenticated.

↘ Configuring the Quiet Period after Multi-user MAB Fails

Command	**dot1x multi-mab quiet-period** *value*
Parameter	*value*: Indicates the quiet period after authentication fails.

Description	
Command Mode	Global configuration mode
Usage Guide	If too many dumb users connected to a port are authenticated, run this command to limit the authentication rate.

Configuring VLAN-based MAB

- Optional.
- Enable VLAN-based MAB after multi-user MAB is enabled on the NAS.
- If you configure VLANs as MAB VLANs, only users in these VLANs can perform MAB.

Command	**dot1x mac-auth-bypass vlan** *vlan-list*
Parameter Description	*vlan-list*: Indicates the VLANs supporting MAB.
Command Mode	Interface configuration mode
Usage Guide	Run this command when a port allows only users in specified VLANs to perform MAB.

Configuration Example

Please refer to the configuration example of 802.1x. But it is MAB authentication that is enabled on the interface in this case. And the account format should conform to the rules described in this chapter.

Common Errors

- The MAC account format is incorrect on the authentication server.

4.4.5 Configuring IAB

Configuration Effect

- Enable IAB. After IAB is enabled, newly authenticated users can access the network even when all RADIUS servers configured on the NAS are inaccessible.
- Enable IAB recovery. When RADIUS servers recover to their reachable status, re-verify the users authorized du inaccessibility.

Notes

- Configure an account and standards for testing RA *Configuring RADIUS*.
- IAB takes effect only when only RADIUS authentication exists in the globally configured 802.1X authentication mode list and all RADIUS servers in the list are inaccessible. If other authentication modes (for example, local and none) exist in the list, IAB does not take effect.

- After multi-domain AAA is enabled, 802.1X authentication does not need the globally configured authentication mode list any more.If IAB detects that all RADIUS servers configured in the globally configured 802.1X authentication mode list are inaccessible, it directly returns an authentication success reply to users, with no need to enter the user name. Therefore, multi-domain AAA does not take effect on this port.
- Users authenticated in IAB mode do not need to initiate accounting requests to the accounting server.
- Authenticated users can properly access the network, not affected by server inaccessibility.
- If 802.1X-based IP authorization is enabled globally, users on this port, except those having I cannot be authenticated.

Configuration Steps

Enabling IAB

- This function is port-based.

Enabling IAB Recovery

- Optional.
- If IAB recovery is enabled on a port, properly authenticated users on the port can access the netwo authentication after the authentication server is recovered. After the authentication serve initiates authentication only to users authenticated in IAB mode during server inaccessibility.

Verification

- When the authentication server is accessible, check whether users can go online only by using the correct user name and password.
- When the authentication server is inaccessible, check whether new users can be authorized to access the immediately after connecting to the NAS.

Related Commands

Enabling IAB

Command	**dot1x critical**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	This command applies to ports on which newly authenticated users need to be au authentication server is inaccessible.

Enabling IAB Recovery

Command	**dot1x critical recovery action reinitialize**

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

4.4.6 Configuring Extended Functions

Configuration Effect

- Some users use authentication clients embedded in the operating system. These clients may not initiate authentication immediately after the users access the network, affecting user experience or authentication to so that such users can initiate authentication immediately after accessing the network.
- Active authentication means that the NAS sends a request/id packet to trigger Orion_B54Q Supplicant to perform 802.1 authentication. Therefore, you can use this function to detect whether Orion_B54Q Supplicant is used. For exampl this function is required for MAB deployment.
- Configure the authenticable host list to specify users that can be authenticated on the port, which restricts access points of users to enhance network security
- The multi-account function allows a user to switch its account upon re-authentication. In special scenari Windows domain authentication, multiple authentications are required to access the domain and th changes during authentication. This function applies to these scenarios.
- By default, the NAS uses its own MAC address as the source MAC address of EAI authentication. Some versions of Orion_B54Q supplicants check whether the access switch is a Orion_B54Q switcl based on the MAC address of EAP packets and implement some private feature authentication with these supplicants, you can enable the virtual source MAC address to use related private features.
- 802.1X allows users to obtain IP addresses before accounting. In this manner, the IP address is carried during us accounting, meeting service requirements. And when this function is enabled, dhcp snooping should also be enabled. After a user is authenticated and goes online, the NAS can obtain the IP address of the user, and then 802.1X server initiates an accounting request. To avoid the case in which the NAS does not initiate accounting for a long time due to the user’s failure to send dhcp requests, conf If the NAS does not obtain the IP address of the user within the configured time (5 minutes by default), it forces t user offline.

Notes

- The multi-account function must be disabled if accounting is enabled. Otherwise, accounting may be inaccurate.
- MAB requires active authentication. Therefore, active authentication must be enabled if MAB is enabled.
- IP-based accounting is not required in two situations:
  - IPv4 addresses and Orion_B54Q Supplicant are deployed. This function is not require

Supplicant can upload the IPv4 addresses of users.

- Static IP addresses are deployed.

Configuration Steps

- You can choose whether to configure these optional functions according to your actual needs.

Verification

- N/A

Related Commands

Enabling Active Authentication

Command	**dot1x auto-req**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The destination addresses of active authentication packets are the multicast function is recommended to be enabled when there is only one user.

Configuring the Number of Active Authentication Requests

Command	**dot1x auto-req packet-num** *num*
Parameter Description	*num*: Indicates the number of active authentication requests.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling User Detection for Active Authentication

Command	**dot1x auto-req user-detect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Interval of Active Authentication Request

Command	**dot1x auto-req req-interval** *time*
Parameter Description	*Time*: Indicates the interval of active authentication request.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Authenticatable Client List

Command	**dot1x auth-address-table address** *mac-addr* **interface** *interface*
Parameter Description	*mac-addr*: Indicates the MAC address of the access user. *interface*: Indicates the port of the access user.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling 802.1X Packets Sending with the Pseudo Source MAC Address

Command	**dot1x pseudo source-mac**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Multi-account Authentication with One MAC Address

Command	**dot1x multi-account enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command when multi-account authentication is required, e.g. in the case of Windows domain authentication. Multi-account authentication is disabled by default.

Configuring the Maximum Number of Authenticated Users on a Port

Command	**dot1x default-user-limit** *num*
Parameter Description	*num*: Indicates the maximum number of online users.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when there is a need to restrict the number of authenticated users on a port.

↘ Enabling IP-triggered Accounting

Command	**dot1x valid-ip-acct enable**
Parameter Description	N/A
Defaults	IP-triggered accounting is disabled by default.
Command Mode	Global configuration mode
Usage Guide	When accounting is supposed to initiate after the user’s IP is obtained, configure this command.

↘ Configuring the Timeout of Obtaining IP Addresses After Authentication

Command	**dot1x valid-ip-acct timeout** *time*
Parameter Description	*time:* Indicates the timeout in the unit of minutes.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Configure this command when there is a need to change the IP address obtaining timeout after users pass authentication.

4.5 Monitoring

Clearing

⚠ Authentication user information can be cleared after 802.1X is disabled.

Description	Command
Clears 802.1X user information.	**no do1x port-control auto**
Clears 802.1X user information.	**clear dot1x user**

Displaying

Description	Command
Displays the parameters and status of the RADIUS server.	**show radius server**
Displays 802.1X status and parameters.	**show dot1x**
Displays the authenticable host list.	**show dot1x auth-address-table**
Displays the active authentication status.	**show dot1x auto-req**
Displays the port control status.	**show dot1x port-control**
Displays the status and parameters of host probe.	**show dot1x probe-timer**

Displays of the information of authenticated users.	**show dot1x summary**
Displays the maximum times of EAP-Request/Chal retransmission.	**show dot1x max-req**
Displays the information of controlled ports.	**show dot1x port-control**
Displays the non-Orion_B54Q client filtering information.	**show dot1x private-supplicant-only**
Displays the re-authentication status.	**show dot1x re-authentication**
Displays the maximum times of EAP-Request/Id retransmission.	**show dot1x reauth-max**
Displays the quiet period after authentication fails.	**show dot1x timeout quiet-period**
Displays the re-authentication interval.	**show dot1x timeout re-authperiod**
Displays the authentication server timeout.	**show dot1x timeout server-timeout**
Displays the supplicant timeout.	**show dot1x timeout supptimeout**
Displays the interval of EAP-Request/Id retransmission.	**show dot1x timeout tx-period**
Displays user information based on the user ID.	**show dot1x user id**
Displays user information based on the MAC address.	**show dot1x user mac**
Displays user information based on the user name.	**show dot1x user name**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disab immediately after use.

Description	Command
Debugs AAA.	**debug aaa**
Debugs RADIUS.	**debug radius**
Debugs 802.1X information.	**debug dot1x**

5 Configuring SCC

5.1 Overview

The Security Control Center (SCC) provides common configuration methods and policy integrati control and network security services, so that these access control and network security services can coexist on one device to meet diversified access and security control requirements in various scenarios.

Typical access control services are dot1x, Web authentication, Address Resolution Protocol (ARP) check, and IP S Guard. The network security services include Access Control List (ACL), Network Foundation Protection Policy (NFPP), and anti-ARP gateway spoofing. When two or more access control or network security services are simultaneously enabled on the device, or when both access control and network security services are simultaneously enabled on the device, the SCC coordinates the coexistence of these services according to relevant policies.

For details about the access control and network security services, see the related configuration guide. This document describes the SCC only.

Protocol and Standards

N/A

5.2 Application

Typical Application	Scenario
Access Control of Extended Layer 2 Campus Networks	Students on a campus network can access the Internet based on dot1x authentication or Web authentication. ARP spoofing between the students should be prevented. In addition, terminal devices in some departments (su headmaster's office) can access

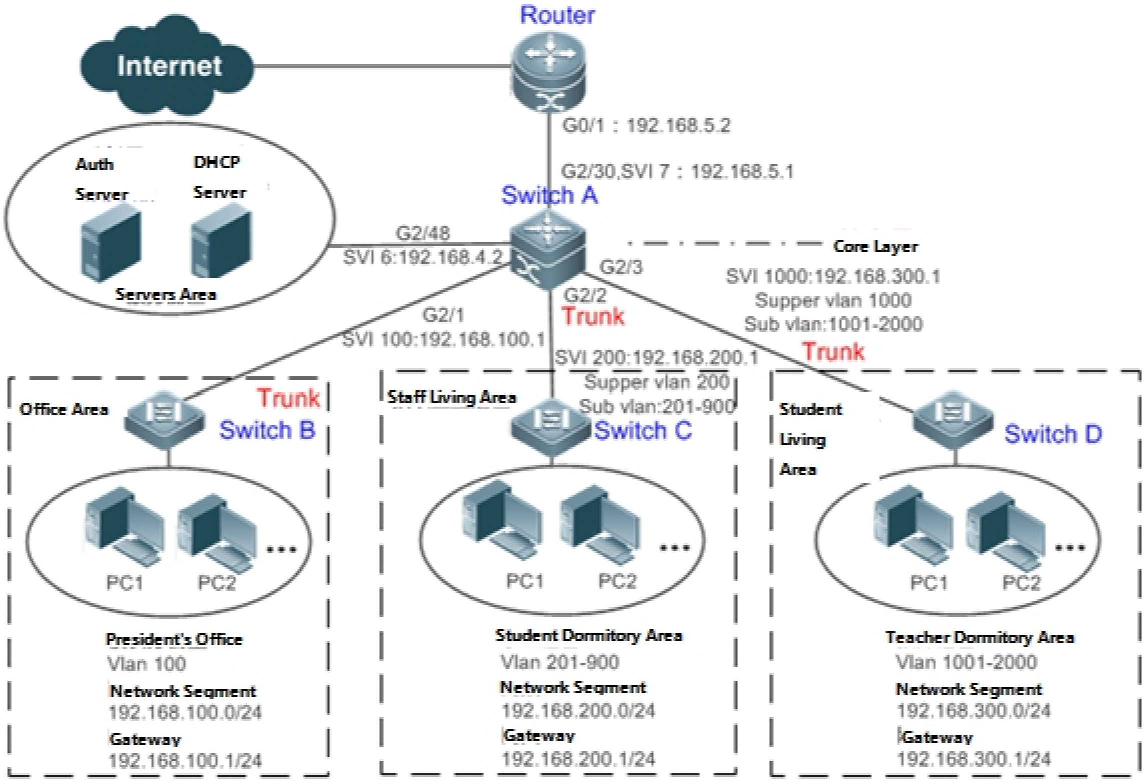
5.2.1 Access Control of Extended Layer 2 Campus Networks

Scenario

Students on a campus network of a university usually need to be authenticated through the dot1x client or accessing the Internet, so as to facilitate accounting and guarantee the benefits of the university.

- The students can access the Internet through dot1x client authentication or Web authentication.
- ARP spoofing between the students is prevented, so as to guarantee the stability of the network.
- Terminal devices in some departments (such as the headmaster's of authentication.

Figure 5-6



Remarks	A traditional campus network is hierarchically designed, which consists of an access layer, a converger layer and a core layer, where the access layer performs user access control. On an extended Layer 2 campus network, however, user access control is performed by a core switch, below which access switche without involving any convergence device in between. The ports between the core switch and the a switches (such as switches B, C, and D in Figure 1-1) are all trunk ports. The user access switches B, C, and D connect to PCs in various departments via access ports, and VLANs correspond to sub VLANs configured on the downlink ports of the core switch, so that access users are ir different VLANs to prevent ARP spoofing. The core switch A connects to various servers, such as the authentication server and the DHC Super VLANs and sub VLANs are configured on the downlink ports. One super VLAN correspond to multiple sub VLANs, and each sub VLAN represents an access user.

Deployment

On the core switch, different access users are identified by VLAN and port numbers. Each access user (or a group of access users) corresponds to one VLAN. The ports on each access switch that connect to downstream users are configu access ports, and one user VLAN is assigned to each access user according to VLAN planning. The core switch does not forward ARP requests. The core switch replies to the ARP requests from authenticated users only, so as to prevent AI spoofing. On the core switch A, user VLANs are regarded as sub VLANs, super VLANs corresponding to the super VLANs are configured as user gateways.

- On the downlink ports of the core switch (switch A in this example) that connect to the teachers' living area and students' living area, both dot1x authentication and Web authentication are enabled, so that users can freel either authentication mode for Internet access.
- Any special department (such as the headmaster's office in this example) can be allocated to a particular VLAN, and this VLAN can be configured as an authentication-exemption VLAN so that users in this department can access t Internet without authentication.

5.3 Basic Concepts

Authentication Mode

There are two authentication modes: access authentication and gateway authentication. network, access authentication is usually performed by access switches. On a extended Layer 2 network, the access function moves forward to a core switch while the access devices need only to support basic VLAN and Layer 2 forwarding functions. As the access authentication is performed by access switches on a traditional hierarchical network while performed by a core switch on a de-layered extended Layer 2 network, some extrinsic functions and behaviors will differ accordingly with the two different authentication modes. Therefore, the authentication mode fa authentication. If the access authentication moves to the core switch, the core switch needs to be enabled with the gateway authentication mode to support a large number of user entries, typically including a large-capacity MAC address table, ARP table and routing table. Otherwise, the supported user capacity is subject to hardware ACL entry restrictions. In general, the capacity of hardware ACL entries is limited and cannot support a large user capacity. The access authentication mod generally applicable only in scenarios where the access authentication is deployed on access switches.

Authentication-Exemption VLAN

Some special departments may be allocated to authentication-exemption VLANs to simplify network management, so tha users in these departments can access network resources without authentication. For example, the headmaster's office can be divided into the authentication-exemption VLANs on the campus network, so that users in the headmaster's office c access the Internet without authentication.

IPv4 User Capacity

The number of IPv4 access users can be restricted to protect the access stability of online users on the Internet and improve the operational stability of the device.

⚠ The number of IPv4 access users is not restricted by default; that is, a large number of users can get online after being authenticated, till reaching the maximum hardware capacity of the device.

ℹ IPv4 access users include IP users (such as IP authenticated users) based on dot1x authentication, users based o Web authentication, and IP users manually bound (using IP source guard, ARP check, or other means).

Authenticated-User Migration

Online-user migration means that an online user can get authenticated again from different physical locations to access the network. On the campus network, however, for ease of management, students are usually requested to get authenticated from a specified location before accessing the Internet, but cannot get authenticated on other access ports. This means that the users cannot migrate. In another case, some users have the mobile office requirement and can get authenticated from different access locations. Then the users can migrate.

User Online-Status Detection

For a chargeable user, accounting starts immediately after the user passes the authenti accounting process does not end until the user actively gets offline. Some users, however, forget to get offline when leaving their PCs, or cannot get offline because of terminal problems. Then the users suffer certain econom accounting process continues. To more precisely determine whether a user is really online, we can preset a traffic value, so that the user is considered as not accessing the Internet and therefore directly brought offline when the user's traffic is lower than the preset value in a period of time or there is not traffic of the user at all in a period of time.

Features

Feature	Function
Authentication Mode	This feature determines whether access control is deployed on access switches or core switches depending on network deployment needs.
Authentication-Exemption VLAN	Users in a specified VLAN can be configured as authentication-exemption users.
IPv4 User Capacity	The IPv4 user capacity of a specified interface can be restricted to guarantee the access stability of users on the Internet.
Authenticated-User Migration	You can specify whether the authenticated can migrate.
User Online-Status Detection	You can specify whether to detect the traffic of online users, so that a user is forced offline when the traffic of the user is lower than a preset value in a period of time.

5.3.1 Authentication Mode

There are two authentication modes: access authentication and gateway authentication. In access authen access control such as dot1x or Web authentication is enabled on access switches. In gateway authentication mode, access control is enabled on core switches. On a large-scale network such as a campus network, there are hundreds of access switches. Compared with the access authentication mode, the gateway authen maintenance and management on the access switches, because the access switches need only to support basic VLAN and Layer 2 forwarding functions. Therefore, the gateway authentication mode is recommended.

Working Principle

The authentication mode on a device depends on the network layer where the access control device works. If access control is deployed on core switches (for example, on an extended Layer 2 network), gateway authentication mode on core switches is required. If access control is deployed on access switches, the authentication mode should be set to access authentication on the access switches.

ℹ The access authentication mode applies by default. In addition, only the N18000 switches support authentication mode switching.

⚠ Restart the device after the authentication mode is changed, so that the new authentication mode takes effect. Save the current configuration before restarting the device.

5.3.2 Authentication-Exemption VLAN

Authentication-exemption VLANs are used to accommodate departments with special access requirements, so that users in these departments can access the Internet without authentication such as dot1x or Web authentication.

Working Principle

Suppose the authentication-exemption VLAN feature is enabled on a device. When the device detects that a packet comes from an authentication-exemption VLAN, access control is not performed. In this way, users in the authentication-exemption VLAN can access the Internet without authentication. The authentication-exemption VLAN feature can be regarded as a kind of applications of secure channels.

ℹ Only the switches support the authentication-exemption VLAN feature.

ℹ A maximum of 100 authentication-exemption VLANs can be configured.

ℹ The authentication-exemption VLANs occupy hardware entries. When access con
disabled, configuring authentication-exemption VLANs has the same effect as the case whe
exemption VLANs are configured. Therefore, it is recommended that authentication-exemption VLANs be configu
for users who need to access the Internet without authentication, only when the access control funct
enabled.

⚠ Although packets from authentication-exemption VLANs are exempt from access control, they still need to be checked by a security ACL. If the packets of the users in an authentication-exemption VLAN are denied according to the security ACL, the users still cannot access the Internet.

⚠ In gateway authentication mode, the device does not initiate any ARP request to a user in an authentication-exemption VLAN, and the ARP proxy will not work. Therefore, in gateway authentication mode, users in different authentication-exemption VLANs cannot access each other unless the users have been authenticated.

5.3.3 IPv4 User Capacity

To improve the operational stability of the device and guard against brutal force impacts from unauthorized users, you can restrict the total number of IPv4 access users on a certain port of the device.

Working Principle

If the total number of IPv4 access users is restricted, new users going beyond the total number cannot access the Internet.

ℹ Only the switches support the restriction on the number of IPv4 access users.

ℹ The number of IPv4 access users is not restricted on the device by default, but depends on the hardware capacity of the device.

⚠ The number of IPv4 access users includes the IPv4 authenticated users based on dot1x authentication, IP based on Web authentication, and IPv4 users based on various binding functions. Because the number of IPv4 access users is configured in interface configuration mode, the restriction includes both the number of IPv4 users generated on the port and IPv4 users globally generated. For example, you can set the maximum number of IPv4 access users on the Gi 0/1 port to 2, run commands to bind an IPv4 user to the port, and then run commands to bind a global IPv4 user to the port. Actually there are already two access users on the port. If you attempt to bind another IPv4 user or another global IPv4 user to the port, the binding operation fails.

5.3.4 Authenticated-User Migration

On an actual network, users do not necessarily access the Internet from a fixed place. Instead, users may be transferred to another department or office after getting authenticated at one place. They do not actively get offline but remove netw cables and carry their mobile terminals to the new office to access the network. Then this brings about an authenticated-user migration. If authenticated-user migration is not configured, a user who gets online at one place cannot get online at another place without getting offline first.

Working Principle

When authenticated-user migration is enabled, the dot1x or Web authentication module of the device detects that the port number or VLAN corresponding to a user's MAC address has changed. Then the user is forced offline and need authenticated again before getting online.

ℹ Only the switches or wireless devices support authenticated-user migration. In addition, cross-switch migration is no supported. For example, authentication and migration are enabled on two N18000, and a user gets online after being authenticated on one of the two N18000. If the user attempts to migrate to the other N18000, the migration fails.

⚠ The authenticated-user migration function requires a check of users' MAC addresses, and is invalid for users who have IP addresses only.

⚠ The authenticated-user migration function enables a user who gets online at one place to get online at another place without getting offline first. If the user gets online at one place and then gets offline at that place, or if the user does not get online before moving to another place, the situation is beyond the control range of authenticated-user migration.

⚠ During migration, the system checks whether the VLAN ID or port number that corresponds to a user's MAC address has changed, so as to determine whether the user has migrated. If the VLAN ID or port number is the same, it indicates that the user does not migrate; otherwise, it indicates that the user has migrated. According to the preceding principle, if another user on the network uses the MAC address of an online user, the system will wrongly disconnect the online user unless extra judgment is made. To prevent such a problem, the dot1x or Web authentication will check whether a user has actually migrated. For a user who gets online through Web authentication or dot1x authenticat authorization, the dot1x or Web authentication sends an ARP request to the original place of the user if detecting that the same MAC address is online in another VLAN or on another port. If no response is received within the specifie time, it indicates that the user's location has indeed changed and then the migration is allowed. If a response is received within the specified time, it indicates that the user actually does not migrate and a fraudulent user may exist o network. In the latter case, the migration is not performed. The ARP request is sent once every second by default, and sent for a total of five times. This means that the migration cannot be confirmed until five seconds later. Timeout-related parameters, including the probe interval and probe times, can be changed using the **arp retry** times *times* and **arp retry** interval *interval* commands. For details about the specific configuration, see *ARP-SCG.doc*. It should be noted that the migration check requires the configuration of IP authorization for users based on dot1x authentication. In addition, the ARP probe is triggered only for user migration in gateway authentication mode but not triggered for user migration in access authentication mode.

5.3.5 User Online-Status Detection

After a user accesses the Internet, the user may forget to get offline or cannot actively get offline due to terminal faults. In this case, the user will keep being charged and therefore will suffer a certain economical loss. To protect the benefits of users on the Internet, the device provides a function to detect whether the users are really online. If the device considers that a user is not online, the device actively disconnects the user.

Working Principle

A specific detection interval is preset on the device. If a user's traffic is lower than a certain value in this interval, the device considers that the user is not using the network and therefore directly disconnects the user.

ⓘ Only the switches and wireless devices support the user online-status detection function.

ⓘ The user online-status detection function applies to only users who get online through dot1x or Web authentication.

ⓘ Currently, the N18000 supports zero-traffic detection only.

⚠ Currently, due to hardware chip restrictions of the N18000, the time to disconnect a user without any traffic relates to the configured MAC address aging time. If the traffic detection interval is set to m minutes and the MAC address aging time is set to n minutes, the interval from the moment when an authenticated user leaves the network without actively getting offline to the moment when the user is disconnected upon detection of zero traffic is about [m, m+n] minutes. In other words, if an online user does not incur any Internet access traffic, the user is disconnected about [m, m+n] min later.

5.4 Configuration

Configuration Item	Suggestions and Related Commands	
Configuring Authentication Mode	⚠ Optional configuration, which is used to configure the authentication mode device.	
	[no] auth-mode gateway	Configures the authentication mode.
Configuring Authentication-Exemption VLANs	⚠ Optional configuration, which is used to specify the users of which VLANs can access the Internet without authentication.	
	[no] direct-vlan	Configure VLANs.
Configuring the IPv4 User Capacity	⚠ Optional configuration, which is used to specify the maximum number of users who are allowed to access a certain interface.	
	[no] nac-author-user maximum	Configures the number of IPv4 users who are allowed to access a certain interface.
Configuring Authenticated-User Migration	⚠ Optional configuration, which is used to specify whether online users with static MAC addresses can migrate.	
	[no] station-move permit	Configures whether authenticat can migrate.
Configuring User Online-Status Detection	⚠ Optional configuration, which is used to specify whether to enable the user onl status detection function.	
	offline-detect interval threshold	Configures the parameters of th online-status detection function.
	no offline-detect	Disables the user online-status detectio function.
	default offline-detect	Restores the default user onli detection mode.

5.4.1 Configuring the Authentication Mode

Configuration Effect

Perform this configuration or not perform this configuration, which shall depend on actual ne hierarchical network, access switches perform access control and you do not need to specify the authentication mode bu can simply keep the default configuration. On a de-layered extended Layer 2 network, the gateway device performs access control and then you need to set the authentication mode to gateway authentication, so that users can be authenticated and get online after the access control service such as dot1x or Web authentication is enabled on the gateway device.

Precautions

- If access control is deployed on the core switch, you need to change the authentication mode on the core switch gateway authentication. If access control is not deployed on the core switch, you do not authentication mode.
- You need to restart the device after the authentication mode is changed, so that the new authentication mode tak effect. Save the current configuration before restarting the device.

Configuration Method

Configuring the Authentication Mode

- Optional configuration. It determines the access position of the device on the actual network.
- Perform the configuration according to actual network deployment. If the core switch performs access control, set the authentication mode to gateway authentication on the core switch; otherwise, simply keep the default configuration.

Command	**[no] auth-mode gateway**
Parameter Description	no: If the command carries this parameter, it indicates that the authentication mode is restored to access authentication; that is, the local device is only an access device and not a gateway device any longer. **auth-mode gateway:** If the command carries this parameter, it indicates that the authentication mode is set to gateway authentication; that is, the local device is both a gateway device and an access device.
Defaults	Access authentication mode
Command Mode	Global configuration mode
Usage Guide	Use this command to determine the access position of the device on the ne configuration or not perform this configuration, which depends on whether the access control function is deployed on access switches on the network or deployed on the gateway device. Use this command to change the authentication mode configured authentication to gateway authentication. Use the **no auth-mode gateway** command to change the authentication mode configured on the device from gate authentication.

Verification

Check the configuration using the following method:

- Enable dot1x or Web authentication on one port of the device, and perform corresponding authentication on the client. After getting online, check whether you can access network resources. Then get offline, and check whether you cannot access specified network resources.

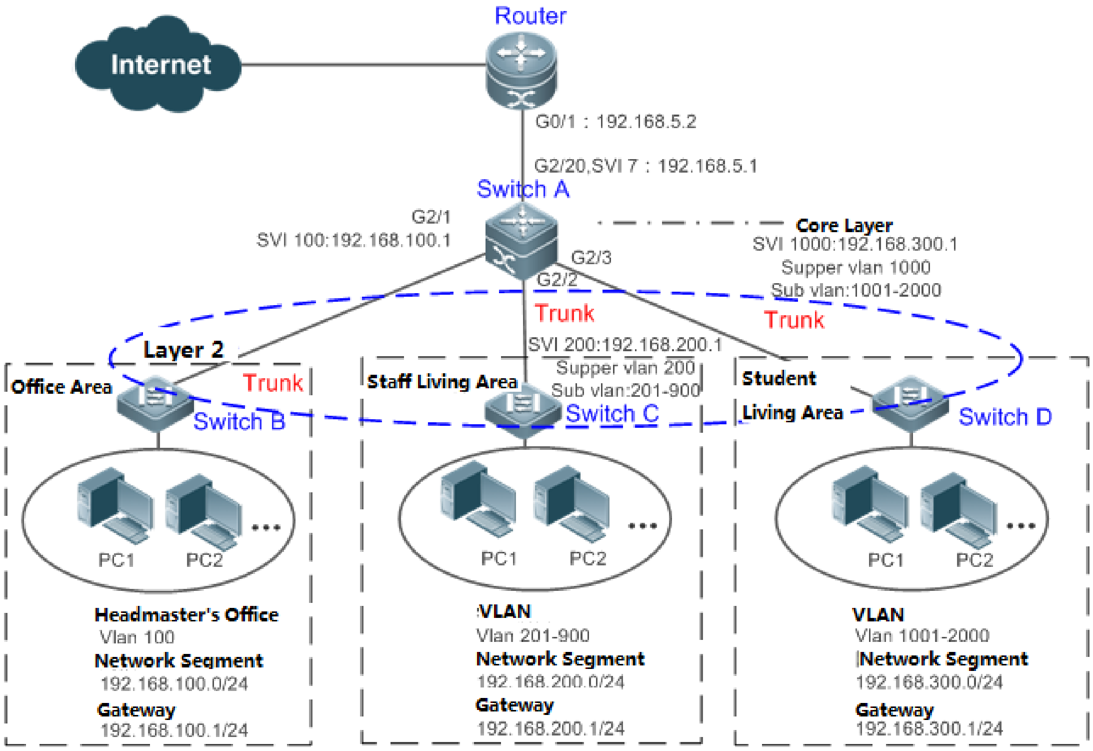
Configuration Examples

- The following configuration example describes SCC-related configuration only.

Setting the Authentication Mode to Gateway Authentication so that the Access Control Function Moves Up to the Core Gateway Device on a De-layered extended Layer 2 Network

Scenario

Figure 5-7



Configuration Steps

- On switch A (which is a core gateway device), set the authenti authentication.

Switch A

```
SwitchA(config)#auth-mode gateway

Please save config and reload system.

SwitchA(config)#exit

*Nov  7 10:13:27: %SYS-5-CONFIG_I: Configured from console by console

SwitchA#reload

Reload system?(Y/N)y

SwitchA#
```

Verification

- Use the **show running** command to check whether the configuration has taken effect.

Switch A

```
SwitchA(config)#show running-config | include auth-mode

auth-mode gateway

SwitchA(config)#
```

5.4.2 Configuring Authentication-Exemption VLANs

Configuration Effect

Configure authentication-exemption VLANs, so that users in these VLANs can access the Internet witho dot1x or Web authentication.

Notices

Authentication-exemption VLANs only mean that users in these VLANs do not need to experience a check related to access authentication, but still need to experience a check based on a security ACL. If specified users or according to the security ACL, corresponding users still cannot access the Internet. Therefore, during ACL configuration, you need to ensure that specified VLANs or specified users in the authentication-exemption VLANs are not blocked if you hope that users in the authentication-exemption VLANs can access the Internet without being authenticated.

Configuration Steps

Configuring Authentication-Exemption VLANs

- Optional configuration. To spare all users in certain VLANs from dot1x or Web authentication, configure these VLANS as authentication-exemption VLANs.
- Perform this configuration on access, convergence, or core switches depending on user distribution.

Command	**[no] direct-vlan** *vlanlist*
Parameter Description	**no** If the command carries this parameter, it indicates that the authe configuration will be deleted. *vlanlist*: This parameter indicates the list of authentication-exemption VLANs to be configured or deleted.
Defaults	No authentication-exemption VLAN has been configured.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure or delete authentication-exemption VLANs.

Verification

Check the authentication-exemption VLAN configuration using the following method:

- Enable dot1x authentication on downlink ports that connect to user terminals, add the downlink ports that connect to the user terminals to a specific VLAN, and configure the VLAN as an authentication-exemption VLAN. Tl Internet Explorer, and enter a valid extranet address (such as www.baidu.com). If the users can open the corresponding webpage on the Internet, it indicates that the authentication-exemption VLAN is valid; otherwise, the authent exemption VLAN does not take effect.
- Use the **show direct-vlan** command to check the authentication-exemption VLAN configuration on the device.

Command	**show direct-vlan**
Parameter Description	-

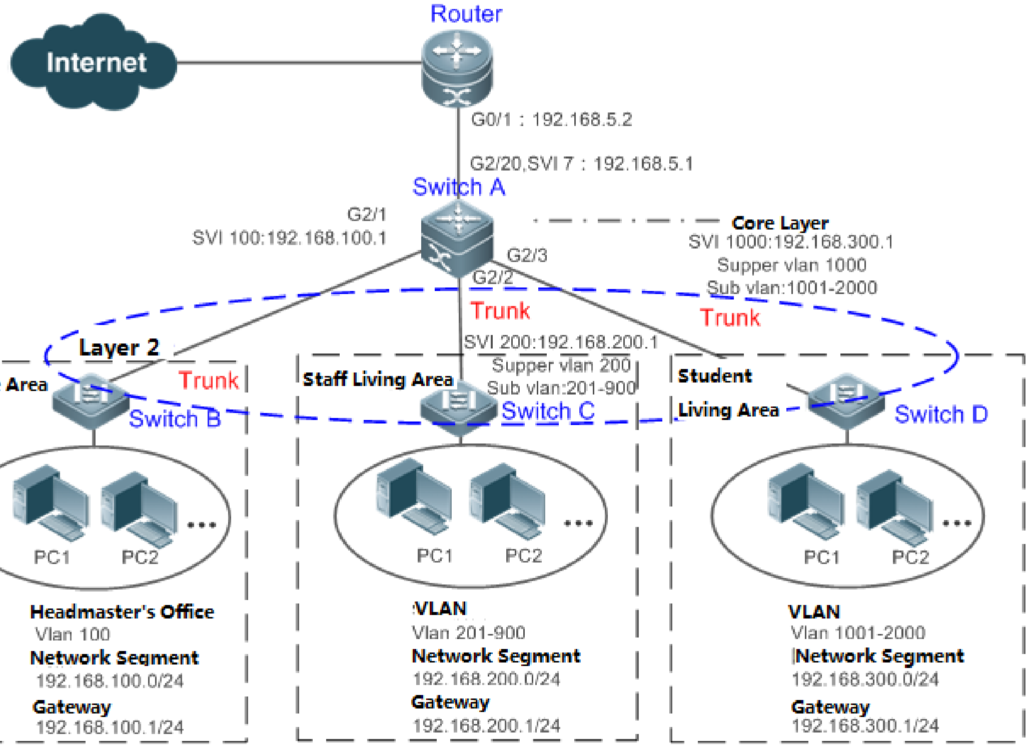
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Global configuration mode

Usage Example	`Orion_B54Q#show direct-vlan`
	`direct-vlan 100`

Configuration Examples

The following configuration example describes SCC-related configuration only.

Configuring Authentication-exemption VLANs so that Specific Users Can Access the Internet Without Being Authenticated

<table>
<tr><td><b>Scenario</b>
<b>Figure 5-8</b></td><td>


</td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Configuration Steps</b></td><td>● On switch A (which is the core gateway device), set the GI 2/1 port as a trunk port, and enable dot1x authentication on this port.
● On switch A (which is the core gateway device), configure VLAN 100 to which the headmaster's office belongs as an authentication-exemption VLAN.</td></tr>
<tr><td><b>Switch A</b></td><td><code>SwitchA(config)#vlan 100</code>
<code>SwitchA(config-vlan)#exit</code></td></tr>
</table>

	SwitchA(config)#direct-vlan 100 SwitchA(config)#int GigabitEthernet 0/1 SwitchA(config-if-GigabitEthernet 0/1)#switchport mode trunk SwitchA(config-if-GigabitEthernet 0/1)#dot1x port-control auto *Oct 17 16:06:45: %DOT1X-6-ENABLE_DOT1X: Able t authentication enabled.
Verification	● Open the Internet Explorer from any PC in the headmaster's office, enter a valid extranet address, and confirm that the corresponding webpage can be opened. ● Use the **show direct-vlan** command to check whether the authentication-exemption VLAN is valid.
Switch A	SwitchA(config)#show direct-vlan direct-vlan 100

5.4.3 Configuring the IPv4 User Capacity

Configuration Effect

Configure the IPv4 user capacity, so as to restrict the number of users who are allowed to access an access port.

Precautions

N/A

Configuration Method

Configuring the IPv4 User Capacity

- Optional configuration. To limit the maximum of users who are allowed to access an access port, configure the IPv user capacity. The access user capacity is not limited on an access port by default. Suppose the user capacity limit is configured on a specific interface. When the number of authenticated users on the interface reaches the maximum, new users cannot be authenticated on this interface and cannot get online, until existing authenticated users get offline on the interface.
- Perform this configuration on access switches, which may be access switches on the network edge or core gateway devices.

Command	**nac-author-user maximum** *max-user-num* **no nac-author-user maximum**
Parameter Description	**no**: If the command carries this parameter, it indicates that the limit on the IPv4 access user capacity will be removed from the port. *max-user-num*: This parameter indicates the maximum number of IPv4 users who allowed to access the port. The value range is from 1 to 1024.

Defaults	The number of IPv4 access users is not limited.
Command Mode	Interface configuration mode
Usage Guide	Use this command to limit the number of IPv4 access users on a specific access port.

Verification

Check the IPv4 user capacity configuration on a port using the following method:

- dot1x authentication: When the number of users who get online based on 1x client authentication on the port reaches the specified user capacity, no any new user can get online from this port.
- Web authentication: When the number of users who get online based on Web authentication on the port reaches the specified user capacity, no any new user can get online from this port.
- Use the **show nac-author-user** [**interface** *interface-name*] command to check the IPv4 user capacity configured on the device.

Command	**show nac-author-user** [**interface** *interface-name*]
Parameter Description	***interface-name***: This parameter indicates the interface name.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Global configuration mode

Usage Example	`Orion_B54Q#show nac-author-user interface GigabitEthernet 0/1`
	`Port      Cur_num  Max_num`
	`--------  -------  -------`
	`Gi0/1     0         4`

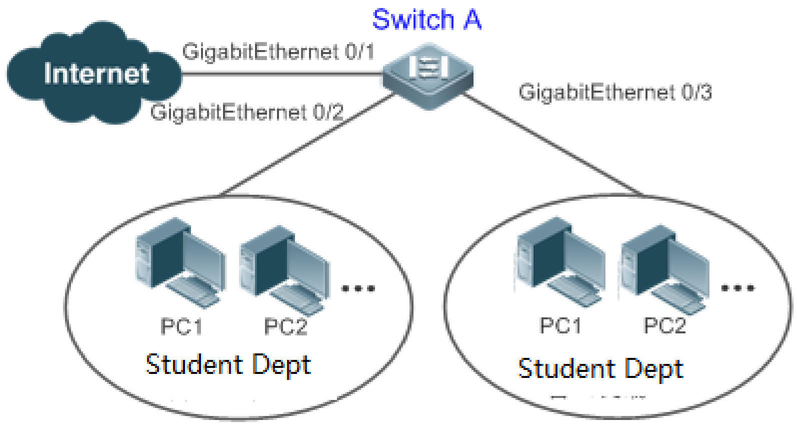
Configuration Examples

The following configuration example describes SCC-related configuration only.

Restricting the Number of IP4 Users on a Port to Prevent Excessive Access Terminals from Impacting the Network

Scenario

Figure 5-9



Configuration Steps

- Assume that the dot1x authentication environment has been well configured on the access switch A, and dot1x authentication is enabled on the Gi 0/2 port.
- Set the maximum number of IPv4 access users on the Gi 0/2 port to 4.

Switch A

```
SwitchA(config)#int GigabitEthernet 0/2

SwitchA(config-if-GigabitEthernet 0/2)#nac-author-user maximum 4
```

Verification

- Perform dot1x authentication for all the four PCs in the dormitory, so that the PCs get online. Then take an additional terminal to access the network, and attempt to perform dot1x authentication for this terminal. Verify that the terminal cannot be successfully authenticated to get online.
- Use the **show nac-author-user** command to check whether the configuration has taken effect.

Switch A

```
SwitchA(config)#show nac-author-user

 Port       Cur_num  Max_num

 --------   -------  -------

 Gi0/1      0         4
```

5.4.4 Configuring Authenticated-User Migration

Configuration Effect

By default, when a user gets online after passing dot1x or Web authentication at a physical location (which is represented by a specific access port plus the VLAN number) and quickly moves to another physical location without getting offline, the user cannot get online through dot1x or Web authentication from the new physical location, unles migration feature has been configured in advance.

Precautions

- If the authenticated-user migration feature is not yet configured, an online user cannot get online from the new physical location after quickly moving from one physical location to another physical location w However, if the user gets offline before changing the physical location or gets offline during the location change example, the user online-status detection function disconnects the user), the user can still normally get o being authenticated at the new physical location, even if the authenticated-user migration feature is not configured.
- After moving to the new physical location, the online user needs to perform dot1x or Web authentication so as to get online.

Configuration Method

Configuring Authenticated-User Migration

- Optional configuration. To allow users to be authenticated and get online from different physical locations, enable the authenticated-user migration function.
- Perform this configuration on access, convergence, or core switches depending on user distribution.

Command	**[no] station-move permit**
Parameter Description	**no station-move permit**: Indicates that aut permitted. **station-move permit**: Indicates that authenticated-user migration is permitted.
Defaults	Authenticated-user migration is not permitted; that is, when a user getting online from c location on the network moves to another physical location and attempts to get online from th physical location without getting offline first, the authentication fails and the user cannot get online from the new physical location.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure authenticated-user migration.

Verification

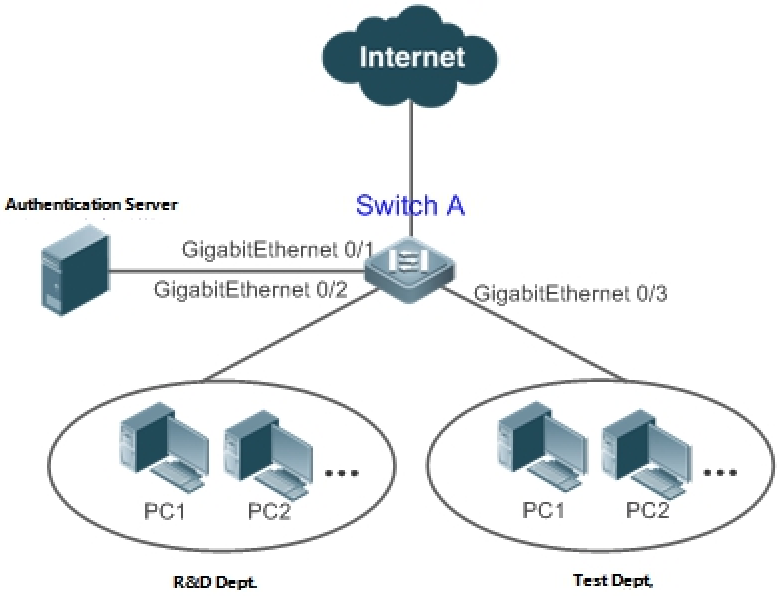
Check the authenticated-user migration configuration using the following method:

- A PC is authenticated and gets online from a dot1x-based port of the device using dot1x SU client, an actively get offline. Move the PC to another port of the device on which dot1x authentication is enabled, and perform dot1x authentication again. Check whether the PC can successfully get online.

Configuration Examples

The following configuration example describes SCC-related configuration only.

Configuring Online-User Migration so that an Online User Can Perform Authentication and Get Online from Different Ports Without Getting Offline First

Scenario **Figure 5-10**	 Internet Switch A Authentication Server GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 PC1 PC2 PC1 PC2 R&D Dept. Test Dept.
Configuration Steps	● Enable dot1x authentication on access ports Gi 0/2 and Gi 0/3, and configure parameters. The authentication is MAC-based. ● Configure online-user migration.
Switch A	`sw1(config)#station-move permit`
Verification	● A lap-top PC in the R&D department performs authentication using dot1x SU client online. Remove the network cable from the PC, connect the PC to the LAN w department resides, and perform dot1x authentication for the PC again using dot1x Confirm that the PC can successfully get online.

Switch A	`sw1(config)#show running-config | include station`
	`station-move permit`

5.4.5 Configuring User Online-Status Detection

Configuration Effect

After the user online-status detection function is enabled, if a user's traffic is lower than a certain specified period of time, the device automatically disconnects the user, so as to avoid the economical l constant charging to the user.

Precautions

It should be noted that if disconnecting zero-traffic users is configured, generally software such as 360 Security Guard will run on a user terminal by default. Then such software will send packets time and again, and the device will disconnect the user only when the user's terminal is powered off.

Configuration Method

Configuring User Online-Status Detection

- Optional configuration. A user is disconnected if the user does not involve any traffic within eight hours by default.
- Perform this configuration on access, convergence, or core switches depending on user distribution. The configuration acts on only the configured device instead of other devices on the network.
- If the traffic threshold parameter threshold is set to 0, it indicates that zero-traffic detection will be performed.

Command	**offline-detect interval** *interval* **threshold** *threshold* **no offline-detect** **default offline-detect**
Parameter Description	*interval*This parameter indicates the offline-detection interval. The value range is from 6 to 65535 i minutes on a switch or from 1 to 65535 in minutes on a non-switch device. The default value is 8 hours, that is, 480 minutes. *threshold*This parameter indicates the traffic threshold. The value range is from 0 to 4294967294 i bytes. The default value is 0, indicating that the user is disconnected when no traffic of th detected. **no offline-detect**: Disables the user online-status detection function. **default offline-detect**Restores the default value. In other words, an online user will be disconnected when the device detects that the user does not have any traffic within eight hours.
Defaults	8 hours
Command Mode	Global configuration mode
Usage Guide	Use this command to configure user online-status detection, so that a user is disconnected whe traffic is lower than a specific threshold wi **no offline-detect** command to disable the user online-status detec **default offline-detect** command to restore the default detection mode.

Verification

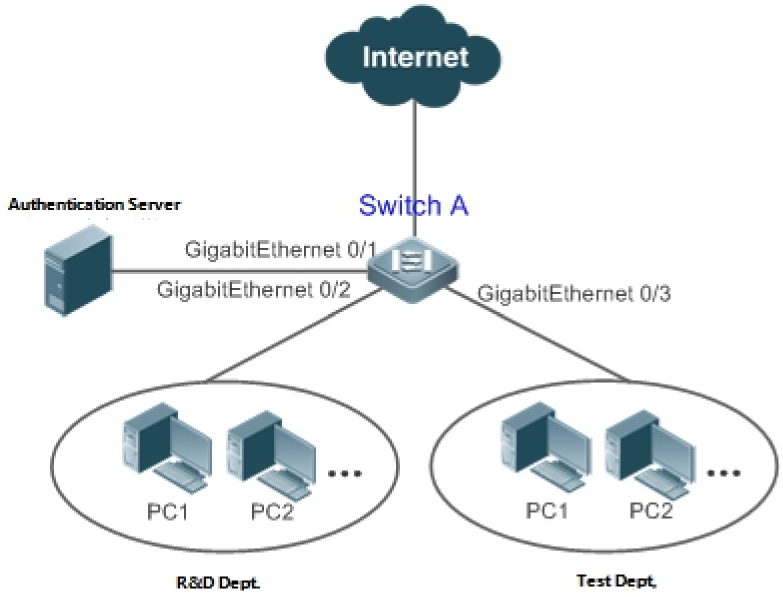
Check the user online-status detection configuration using the following method:

- After the user online-status detection function is enabled, power off the specified authenticat corresponding user gets online. Then wait for the specified period of time, and run the online user query co associated with dot1x or Web authentication on the device to confirm that the user is already offline.

Configuration Examples

The following configuration example describes SCC-related configuration only.

Configuring User Online-Status Detection so that a User Is Disconnected if the User Does Not Have Traffic Within Five Minutes

Scenario **Figure 5-11**	 Internet Authentication Server Switch A GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 PC1 PC2 PC1 PC2 R&D Dept. Test Dept.
Configuration Steps	● Enable dot1x authentication on the access port Gi 0/2, and configure authentication parameters. The authentication is MAC-based. ● Configure user online-status detection so that a user is disconnected if the user does not traffic within five minutes.
Switch A	`sw1(config)# offline-detect interval 5 threshold 0`
Verification	● Perform dot1x authentication using dot1x SU client for a PC in the R&D department, so that the PC gets online. Then power off the PC, wait for 6 minutes, and run the online user query command available with dot1x authentication on switch 1 to confirm that the user of the PC is already offline.

Switch A	`sw1(config)#show running-config | include offline-detect`
	`offline-detect interval 5`

5.5 Monitoring

Displaying

Command	Function
show direct-vlan	Displays the authentication-exemption VLAN configuration.
show nac-author-user [**interface** *interface-name*]	Displays information about IPv4 user entries on a specific interface.

Debugging

⚠ System resources are occupied when debugging information is output. Theref
immediately after use.

Command	Function
debug scc event	Debugs the SCC running process.
debug scc user [mac | author | mac]	Debugs SCC user entries.
debug scc acl-show summary	Debugs ACLs stored in the current SCC and delivered by various services.
debug scc acl-show all	Debugs all ALCs stored in the current SCC.

6 Configuring Global IP-MAC Binding

6.1 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).

6.2 Applications

Application	Description
Global IP-MAC Binding	Only hosts with the specified IP addresses can access the network, and the hosts connected to a device can move freely.

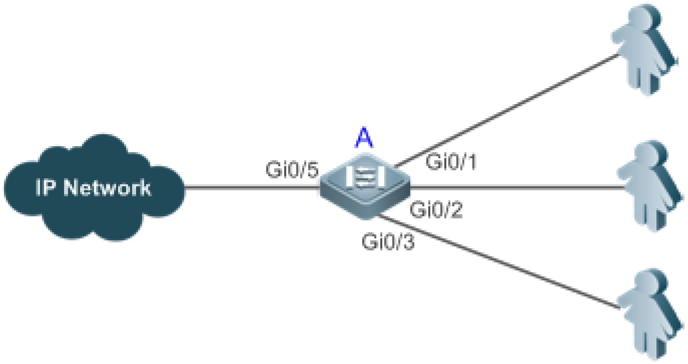
6.2.1 Global IP-MAC Binding

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 6-12



Remarks	A is an access device. A user is a host configured with a static IP address.

	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.

6.3 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 no 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 IP 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 I 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. generated by other access security functions, such as port security and IPv6 Source Guard.) If IPv6-MAC binding does not exist, all IPv6 pack 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 pa forwarded. 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
Configuring Global IP-MAC Binding	Control forwarding of IPv4 or IPv6 packets.
Configuring the IPv6 Address Binding Mode	Change the IPv6 packet forwarding rules.
Configuring the Exclude Port	Disable the global address binding function on the specified port.

6.3.1 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.

6.3.2 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.

6.3.3 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 p

6.4 Configuration

Configuration	Description and Command	
Configuring Global IP-MAC Binding	⚠ (Mandatory) It is used to configure and enable address binding.	
	address-bind	Configures a global IPv4-MAC binding.
	address-bind install	Enables the address binding function.
Configuring IPv6 Address Binding Mode	⚠ (Optional) It is used to configure the IPv6 address binding mode.	
	address-bind ipv6-mode	Configures the IPv6 address binding mode.
Configuring the Exclude Port	⚠ (Optional) It is used to disable the address binding function on a specified port.	
	address-bind uplink	Configures an exclude port.

6.4.1 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.

Verification

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

Related Commands

↘ Configuring Global IP-MAC Binding

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

↘ Enabling the Address Binding Function

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

Configuration Example

↘ Configuring Global IP-MAC Binding and Enabling Address Binding

Configuration Steps	● Configure a global IPv4-MAC binding. ● Enable the address binding function.

	`Orion_B54Q# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Orion_B54Q(config)# address-bind 192.168.5.1 00d0.f800.0001`
	`Orion_B54Q(config)# address-bind install`

Verification	Display the global IP-MAC binding on the device.
	`Orion_B54Q#show address-bind`

```
Total Bind Addresses in System : 1

IP Address          Binding MAC Addr

----------------    ----------------

192.168.5.1         00d0.f800.0001
```

6.4.2 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

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

Configuration Example

Configuring the IPv6 Address Binding Mode

Configuration Steps	● Configure a global IP-MAC binding. ● Enable the address binding function. ● Set the IPv6 address binding mode to Compatible.

```
Orion_B54Q# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Orion_B54Q(config)# address-bind 192.168.5.1 00d0.f800.0001
```

	`Orion_B54Q(config)# address-bind install`
	`Orion_B54Q(config)# address-bind ipv6-mode compatible`

Verification	Run the **show run** command to display the configuration on the device.

6.4.3 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 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

Command Syntax	**address-bind uplink** *interface-id*
Parameter Description	*interface-id*: Indicates the ID of a switching port or an L2 aggregate port.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

↘ Configuring the Exclude Port

Configuration Steps	● Create a global IPv4-MAC binding. ● Enable the address binding function. ● Configure an exclude port.

```
Orion_B54Q# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Orion_B54Q(config)# address-bind 192.168.5.1 00d0.f800.0001
Orion_B54Q(config)# address-bind install
Orion_B54Q(config)# address-bind uplink GigabitEthernet 0/1
```

Verification	Display the global IP-MAC binding on the device.

```
Orion_B54Q#show address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
---------------     ----------------
192.168.5.1         00d0.f800.0001
Orion_B54Q#show address-bind uplink
Port        State
---------- ---------
Gi0/1       Enabled
Default     Disabled
```

6.5 Monitoring

Displaying

Description	Command
Displays the IP-MAC binding on the device.	**show address-bind**
Displays the exclude port.	**show address-bind uplink**

7 Configuring Password Policy

7.1 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.

ℹ The following sections introduce password policy only.

7.1.1 Protocols and Standards

N/A

7.2 Features

7.2.1 Basic Concepts

Minimum Password Length

Administrators can set a minimum length for user passwords according to system security requirements. If the pa 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 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;

2. 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, 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 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 pas records of a user is greater than the maximum number configured for this user, the new password overwrite the user's oldest password history record.

Storage of Encrypted Passwords

Administrators can enable the storage of encrypted passwords for security consideration. When adr **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 passw time, the passwords already in cipher text format will not be restored to plaintext passwords.

7.3 Configuration

Configuration	Description and Command	
Configuring the Password Security Policy	Optional configuration, which is used to configure a combination of parameters related to the password security policy.	
	password policy life-cycle	Configures the password life cycle.
	password policy min-size	Configures the minimum length of passwords.
	password policy no-repeat-times	Sets the no-repeat times of latest password configuration, so that t specified in these times of latest password configuration can no longer be use future password configuration.
	password policy strong	Enables the strong password de function.
	service password-encryption	Sets the storage of encrypted passwords.

7.3.1 Configuring the Password Security Policy

7.3.1.1 Networking Requirements

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

7.3.1.2 Notes

- The configured password security policy is valid for global p **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.

7.3.1.3 Configuration Steps

Configuring the Password Life Cycle

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

7.3.1.4 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.

7.3.1.5 Corresponding

Configuring the Password Life Cycle

Command Syntax	**password policy life-cycle** *days*
Parameter Description	**life-cycle** *days*: Indicates the password life cycle in the unit of days. The value range is from 1 to 65535.
Command Mode	Global configuration mode
Usage Guide	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 change the password.

Configuring the Minimum Length of User Passwords

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

Setting the No-Repeat Times of Latest Password Configuration

Command Syntax	**password policy no-repeat-times** *times*
Parameter Description	**no-repeat-times***times*: Indicates the no-repeat times of latest password configuration. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	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. You can configure the maximum number of password history records per user. When the numbe

	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

Command Syntax	**password policy strong**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	After the strong password detection function is enabled, a prompt is displayed for the following types of passwords: 4. Passwords that are the same as corresponding accounts; 5. Simple passwords that contain characters or digits only.

Setting the Storage of Encrypted Passwords

Command Syntax	**service password-encryption**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	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 consi **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 you disable the storage encrypted passwords next time, the passwords already in cipher text format will not be plaintext passwords.

Checking User-Configured Password Security Policy Information

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

7.3.1.6 Configuration Examples

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

Configuring Password Security Check on the Device

Typical Application	Assume that the following password security requirements arise in a network environment: 1. The minimum length of passwords is 8 characters; 2. The password life cycle is 90 days; 3. Passwords are stored and transmitted in cipher text format; 4. The number of no-repeat times of password history records is 3; 5. Passwords shall not be the same as user names, and shall not contain simple characters or digits only.
Configuration Steps	● Set the minimum length of passwords to 8. ● Set the password life cycle to 90 days. ● Enable the storage of encrypted passwords. ● Set the no-repeat times of password history records to 3. ● Enable the strong password detection function.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# password policy min-size 8`
	`Orion_B54Q(config)# password policy life-cycle 90`
	`Orion_B54Q(config)# service password-encryption`
	`Orion_B54Q(config)# password policy no-repeat-times 3`
	`Orion_B54Q(config)# password policy strong`

Verification	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. ● Run the **show password policy** command to display user-configured password security policy information.
	`Orion_B54Q# show password policy`

```
Global password policy configurations:
 Password encryption:                Enabled
 Password strong-check:              Enabled
 Password min-size:                  Enabled (8 characters)
 Password life-cycle:                Enabled (90 days)
 Password no-repeat-times:           Enabled (max history record: 3)
```

7.3.1.7 Common Errors

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

7.4 Monitoring

7.4.1 Displaying the Running Status

Command	Function
show password policy	Displays user-configured password security policy information.

8 Configuring Port Security

8.1 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 tha dynamically learned to restrict the packets that can enter the port. Ports enabled with port security are called secure ports.

8.2 Applications

Application	Description
Allowing Only Specified Hosts to Use Ports	For network security, certain ports of a device can be used only by specified hosts.

8.2.1 Allowing Only Specified Hosts to Use Ports

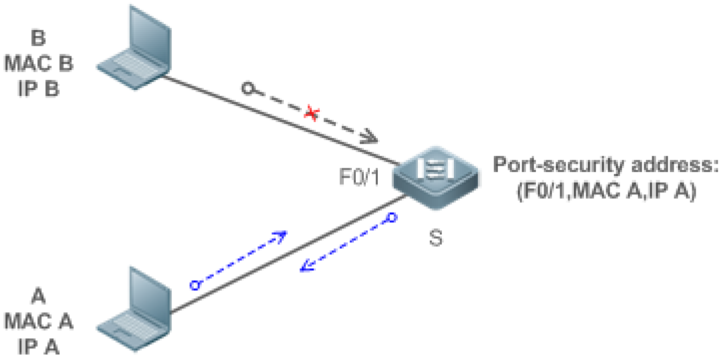
Scenario

In a scenario that has requirements for the network security, devices car

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 8-25



Remarks	S is the access device. A is a PC that can use the port F0/1. 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.

8.3 Features

Basic Concepts

↘ Secure Port

Ports configured with port security are called secure ports. At present, Orion_B54Q 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 address bound to IP+MAC; otherwise, communication may fail due to inconsistency with the binding. Similarly, i binding is set, only packets whose secure MAC addresses are statically configured or learned 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 speci 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 handing 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 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 st 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 nur 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
Enabling Port Security	Creates a secure address list for a port.
Filtering Layer-2 Users	Processes the packets received by a port from non-secure addresses.
Filtering Layer-3 Users	Checks the layer-2 and layer-3 addresses of packets passing a port.
Aging of Secure Addresses	Regularly deletes secure addresses.

8.3.1 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 modu 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 or 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.

8.3.2 Filtering Layer-2 Users

Set the secure addresses on a port to ensure that only devices whose MAC addresses are the s
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
maximum number, the secure port can dynamically learn new dynamic secure addresses. When the num
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.

8.3.3 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 bind 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 dis 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.

8.3.4 Aging of Secure Addresses

Regularly delete secure addresses. When this function is enabled, you need to set the maximum numb 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.

8.4 Configuration

Configuration	Description and Command

Configuring Secure ports and Violation Handling Modes	⚠ (Mandatory) It is used to enable the port security service.	
	switchport port-security	Enables port security.
	switchport port-security maximum	Sets the maximum number of addresses for a port.
	switchport port-security violation	Configures the violation handling mode for port security.
	switchport port-security mac-address sticky	Configures automatic saving of dynamic addresses.
Configuring Secure Addresses on Secure Ports	⚠ (Optional) It is used to configure security filtering items.	
	switchport port-security mac-address	Configures the static secure addresses in the interface configuration mode.
	switchport port-security interface mac-address	Configures the static secure addresses in the global configuration mode.
	switchport port-security binding	Configures binding of secure addresses in the interface configuration mode.
	switchport port-security interface binding	Configures binding of secure addresses in the global configuration mode.
	switchport port-security aging	Configures aging time for addresses on a port.

8.4.1 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 bindin source guard. When these functions are used together, packets can enter a switch only when passing 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

- OptionalIf 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 config effect.

Related Commands

Setting Port Security

Command	**switchport port-security**
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	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

Command	**switchport port-security maximum** *value*
Parameter Description	*value*: Indicates the number of secure addresses, ranging from 1 to 128.
Command	Interface configuration mode

Mode	
Usage Guide	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. The limitation only works for secure addresses. It does not restrict the number of binding.

↘ Configuring the Violation Handling Mode for Port Security

Command	**switchport port-security violation** { **protect** | **restrict** | **shutdown** }
Parameter Description	**protect**: Discards violated packets. **restrict**: Discards violated packets and send trap notifications. **shutdown**: Discards packets and disables the port.
Command Mode	Interface configuration mode
Usage Guide	-

↘ Saving Dynamic Secure Addresses to a Configuration File

Command	**switchport port-security mac-address sticky** *mac-address* [**vlan** *vlan-id*]
Parameter Description	*mac-address*: Indicates a static secure address. *vlan-id*: Indicates the VID of a MAC address.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration Example

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

Configuration Steps	● Enable port security. ● Set the maximum number of secure addresses. ● Modify the violation handling mode.

```
Orion_B54Q# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(config)# interface gigabitethernet 0/3
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport mode access
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security maximum 8
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security violation protect
```

	`Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security mac-address sticky`
	`Orion_B54Q(config-if-GigabitEthernet 0/3)# end`

Verification	Check the port security configuration on the device.

	`Orion_B54Q# show port-security interface gigabitethernet 0/3`
	`Interface : Gi0/3`
	`Port Security: Enabled`
	`Port status : down`
	`Violation mode: Protect`
	`Maximum MAC Addresses:8`
	`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.

8.4.2 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.

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

Command	**switchport port-security interface** *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]
Parameter Description	*interface-id*: Indicates the interface ID. *mac-address*: Indicates a static secure address. *vlan-id*: Indicates the VID of a MAC address.
Command Mode	Global configuration mode
Usage Guide	-

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

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

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

Command	**switchport port-security interface** *interface-id* **binding** [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }
Parameter Description	*interface-id*: Indicates the interface ID. *mac-address*: Indicates a bound source MAC address. *vlan_id*: Indicates the VID of a bound source MAC address. *ipv4-address*: Indicates a bound IPv4 address.

	ipv6-address: Indicates a bound IPv6 address.
Command Mode	Global configuration mode
Usage Guide	-

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

Command	**switchport port-security binding** [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }
Parameter Description	*mac-address*: Indicates a bound source MAC address. *vlan_id*: Indicates the VID of a bound source MAC address. *ipv4-address*: Indicates a bound IPv4 address. *ipv6-address*: Indicates a bound IPv6 address.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring Aging Time for All Secure Addresses on a Port

Command	**switchport port-security aging** { **static** | **time** *time* }
Parameter Description	**static**Indicates that the aging time will be applied to manually configured secure automatically learned addresses; otherwise, the aging time will be applied to only automatically learned addresses. **time** *time*: 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.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration Example

Configuring a Secure MAC Address 00d0.f800.073c for the Port gigabitethernet 0/3

<table>
<tr><td><b>Configuration Steps</b></td><td>● Enable port security.
● Add a secure address.</td></tr>
<tr><td></td><td>

```
Orion_B54Q# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(config)# interface gigabitethernet 0/3
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport mode access
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security
Orion_B54Q(config-if-Gigab
00d0.f800.073c  vlan 1
```

</td></tr>
</table>

	`Orion_B54Q(config-if-GigabitEthernet 0/3)# end`
Verification	Check the port security configuration on the device.

	`Orion_B54Q# 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`

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

Configuration Steps	● Enable port security. ● Add a binding of the secure address.

	`Orion_B54Q# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Orion_B54Q(config)# interface gigabitethernet 0/3`
	`Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport mode access`
	`Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security`
	`Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security binding 192.168.12.202`
	`Orion_B54Q(config-if-GigabitEthernet 0/3)# end`

Verification	Check the port security configuration on the device.

	`Orion_B54Q# 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`

Configuring a Secure MAC Address 00d0.f800.073c an
0000::313b:2413:955a:38f4 for the Port gigabitethernet 0/3

Configuration Steps	● Enable port security. ● Add a binding of the secure address.
	`Orion_B54Q# configure terminal`

```
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(config)# interface gigabitethernet 0/3
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport mode access
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security binding 00
vlan 1 0000::313b:2413:955a:38f4
Orion_B54Q(config-if)# end
```

Verification	Check the port security configuration on the device.

```
Orion_B54Q# 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
```

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

Configuration Steps	● Enable port security. ● Configure aging time.

```
Orion_B54Q# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(config)# interface gigabitthernet 0/3
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security aging time 8
Orion_B54Q(config-if-GigabitEthernet 0/3)# switchport port-security aging static
Orion_B54Q(config-if-GigabitEthernet 0/3)# end
```

Verification	Check the port security configuration on the device.

8.5 Monitoring

Displaying

Description	Command

Displays all secure addresses or all secure addresses of a specified port.	**show port-security address** [**interface** *interface-id*]
Displays all bindings or all bindings of a specified port.	**show port-security binding** [**interface** *interface-id*]
Displays all valid secure addresses of ports and the security binding records of the ports.	**show port-security all**
Displays port security configurations of an interface.	**show port-security interface** *interface-id*
Displays the statistics about port security.	**show port-security**

9 Configuring Storm Control

9.1 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 unknow If the rate of data flows received by a device port is within the configured bandwidth thre 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 t causing a storm.

9.2 Applications

Application	Description
Network Attack Prevention	Enable storm control to prevent flooding.

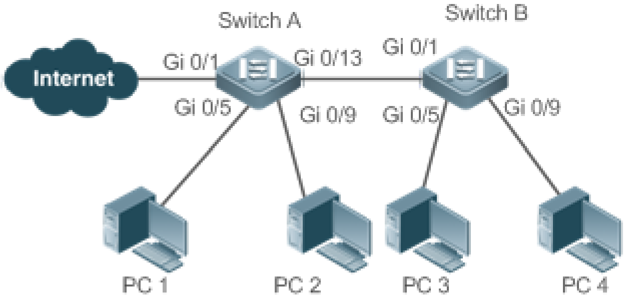
9.2.1 Network Attack Prevention

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 9-13



Remarks	Switch A and Switch B are access devices. 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).

9.3 Features

Basic Concepts

Storm Control

If the rate of data flows (broadcast packets, multicast packets, or unknown unicast packets) received by a devic 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 th 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 th threshold.

Overview

Feature	Description
Unicast Packet Storm Control	Limits unknown unicast packets to prevent flooding.
Multicast Packet Storm Control	Limits multicast packets to prevent flooding.
Broadcast Packet Storm Control	Limits broadcast packets to prevent flooding.

9.3.1 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 e 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.

9.3.2 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.

9.3.3 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.

The default command parameters are determined by related products.

9.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of Storm Control	⚠ (Mandatory) It is used to enable storm control.	
	storm-control { **broadcast** | **multicast** | **unicast** } [{ **level** *percent* | **pps** *packets* | *rate-bps* }]	Enables storm control.

9.4.1 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 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

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

↘ Enabling Multicast Packet Storm Control

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

↘ Enabling Broadcast Packet Storm Control

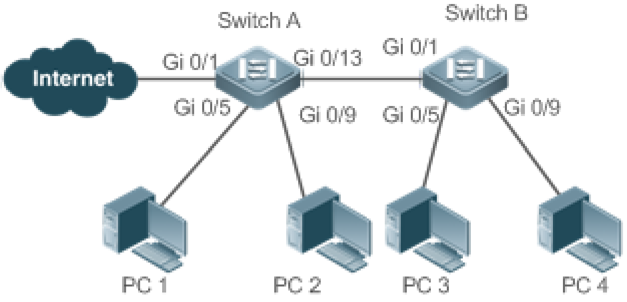
Command	**storm-control broadcast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }]
Parameter Description	**level** *percent*: Indicates the bandwidth percentage. **pps** *packets*: Indicates the number of packets per second. *rate-bps*: Indicates the packet rate.
Command Mode	Interface configuration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

Configuration Example

↘ Enabling Storm Control on Devices

Scenario

Figure 9-14



Configuration Step

- Enable storm control on Switch A and Switch B.

Switch A

```
Orion_B54Q(config)#interface range gigabitEthernet 0/5,0/9,0/13

Orion_B54Q(config-if-range)#storm-control broadcast

Orion_B54Q(config-if-range)#storm-control multicast

Orion_B54Q(config-if-range)#storm-control unicast
```

Switch B

```
Orion_B54Q(config)#interface range gigabitEthernet 0/1,0/5,0/9

Orion_B54Q(config-if-range)#storm-control broadcast

Orion_B54Q(config-if-range)#storm-control multicast

Orion_B54Q(config-if-range)#storm-control unicast
```

Verification

Check whether storm control is enabled on Switch A and Switch B.

Switch A

```
Orion_B54Q# 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
```

Switch B

```
Orion_B54Q#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
```

9.5 Monitoring

Displaying

Description	Command
Displays storm control information.	**show storm-control** [*interface-type interface-number*]

10 Configuring SSH

10.1 Overview

Secure Shell (SSH) connection is similar to a Telnet connection except that all data transmitted over SSH is
When a user in an insecure network environment logs into a device remotely, SSH helps ensure information security ar
powerful authentication, protecting the device against attacks such as IP address sp
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, supportingSSHv1 and
  Orion_B54Q 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
  server functions, but not the SSH client functions.

10.2 Applications

Application	Description
SSH Device Management	Use SSH to manage devices.
SSH Local Line Authentication	Use the local line password authentication for SSH user authentication.
SSH AAA Authentication	Use the authentication, authorization and accounting (AAA) mode for SSH us authentication.
SSH Public Key Authentication	Use the public key authentication for SSH user authentication.
SSH File Transfer	Use the Secure Copy (SCP) commands on the client to exchange data with the SSH server.

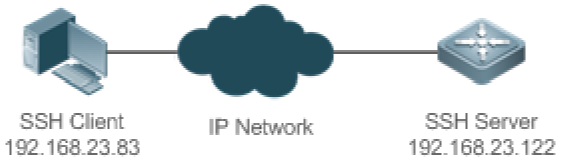
10.2.1 SSH Device Management

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-compa

The following takes the PuTTY as an example to introduce the configurations of the SSH client. Figure 10 -26 shows the network topology.

Figure 10-26 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 **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.

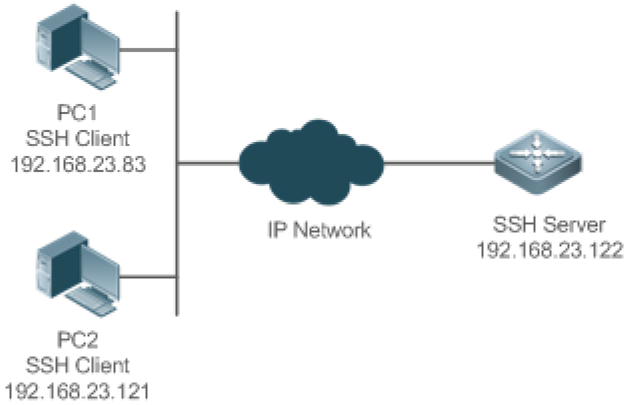
10.2.2 **SSH Local Line Authentication**

Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 10-27. 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 10-27 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.
2. Configure the key. With this key, the SSH server decrypts the encrypted password received from the S compares the decrypted plain text with the password stored on the server, and returns a messag successful or unsuccessful authentication. SSHv1 uses an RSA key, whereas SSHv2 adopts an RSA or DSA key.
3. 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 take example to explain the method for configuring the SSH clients.

1. Open the PuTTY connection tab, and select SSHv1 for authenticated login. (The method selected.)
2. 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

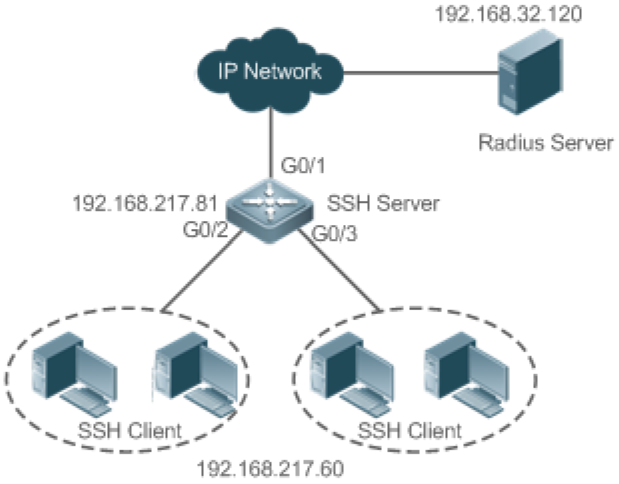
does not require a user name, you can type in any user name, but cannot be null. (In this example, the user name is "anyname".)

10.2.3 **SSH AAA Authentication**

Scenario

SSH users can use the AAA authentication mode for user authentication, as shown in Figure 10 -28. 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 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 10-28 Networking Topology of SSH AAA Authentication



Deployment

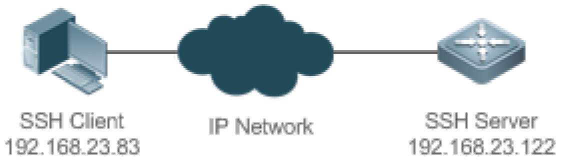
- The routes from the SSH clients to the SSH server are reachable, and the route from the SSH server to the Radiu server is also reachable.
- Configure the SSH server on the network device that functions as an SSH client.
- Configure the AAA parameters on the network device. When the AAA authentication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

10.2.4 **SSH Public Key Authentication**

Scenario

SSH clients can use the public keys for authentication, and the public key algorithm can be RSA or DSA, Figure 10 -29SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 10-29 Network Topology for Public Key Authentication of SSH Users



Deployment

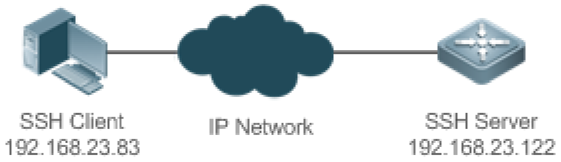
- To implement public key authentication for the client, generate a key pair (RSA or DSA) on the client, configure public key on the SSH server, and select the public key authentication mode.
- After the key is generated on the client, the SSH server will copy the file of the public key from the client 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.

10.2.5 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 serv shown in Figure 10 -30.

Figure 10-30 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.

10.3 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 thos 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 incl 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, 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 followi 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 exchange the algorithm negotiation packet with each other, and determine the final algorithm basec In addition, the server and the client work together to generate a session key and a session ID ac exchange algorithm and host key, which will be applied to subsequent user authentication, data decryption.

- User authentication

After the encrypted channel is set up, the client sends an authentication request to the server. Th 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 processe 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. Enc 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. decrypts the execution result.

- Session ending

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

Overview

Feature	Description
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.
SCP Service	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.
SSH Client	You can use the SSH client on the device to set up a secure connection with the SSH server on a network device.

10.3.1 **SSH Server**

Enable the SSH server function on a network device, and you can set up a secure connection with the netw 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 C 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 orSSHv2 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 rea 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 p 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 re
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
If authentication still does not succeed when the maximum number of user authenti
authentication fails.

↘ 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. Whe
authenticated upon login, a public key file is specified based on the user name.

10.3.2 **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 fil
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.

10.4 Configuration

Configuration	Description and Command	
Configuring the SSH Server	⚠ It is mandatory to enable the SSH server.	
	enable service ssh-server	Enables the SSH server.
	disconnect ssh[**vty**] *session-id*	Disconnects an established SSH session.
	crypto key generate {**rsa**|**dsa**}	Generates an SSH key.
	ip ssh version {**1**|**2**}	Specifies the SSH version.
	ip ssh time-out *time*	Configures the SS timeout.
	ip ssh authentication-retries *retry times*	Configures the maximum number of SSH authentication retries.
	ip ssh peer *test* **public-key rsa flash** *:rsa.pub*	Associates an RSA public key file with a user.
	ip ssh peer *test* **public-key dsa flash***:dsa.pub*	Associates a DSA public key file with a user.
Configuring the SCP Service	⚠ Mandatory.	
	ip scp server enable	Enables the SCP server.

10.4.1 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, f security.
- You can use diversified SSH user a 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.

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 supervi modules, if no SSH key file exist on the new activ **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, If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to th 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. ranges from 0 to 5.

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 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

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

Disconnecting an Established SSH Session

Command	**disconnect ssh**[**vty**] *session-id*
Parameter Description	**vty:** Indicates an established virtual teletype terminal (VTY) session. session-id: Indicates the ID of the established SSH session. The value ranges from 0 to 35.
Command Mode	Privileged EXEC mode
Usage Guide	Specify an SSH session ID to disconnect the established SSH session. Alternatively, specif session ID to disconnect a specified SSH session. Only an SSH session can be disconnected.

Generating an SSH Key

Command	**crypto key generate** {**rsa**|**dsa**}
Parameter Description	**rsa:** Generates an RSA key. **dsa:** Generates a DSA key.
Command Mode	Global configuration mode
Usage Guide	The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key. SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key. 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

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

Configuring the SSH Authentication Timeout

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

Configuring the Maximum Number of SSH Authentication Retries

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

Configuring RSA Public Key Authentication

Command	**ip ssh peer** *test* **public-key rsaflash**:*rsa.pub*
Parameter Description	*test***:** Indicates the user name. **rsa:** Indicates that the public key type is RSA. *rsa.pub***:** Indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the RSA public key file associated with user *test*. 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 fi specified based on the user name.

↘ Configuring DSA Public Key Authentication

Command	**ip ssh peer** *test* **public-key dsaflash**:*dsa.pub*
Parameter Description	*test*: Indicates the user name. **dsa:** Indicates that the public key type is DSA. *dsa.pub*: Indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the DSA key file associated with user **test**. 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 fi 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

Configuration Steps	● Run the **crypto key generate { rsa | dsa }** command to generate a RSA public key for the server.

SSH Server	`Orion_B54Q#configure terminal`
	`Orion_B54Q(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]:`
	● If the generation of the RSA key is successful, the following information is displayed:
	`% Generating 512 bit RSA1 keys ...[ok]`
	`% Generating 512 bit RSA keys ...[ok]`
	● If the generation of the RSA key fails, the following information is displayed:
	`% Generating 512 bit RSA1 keys ...[fail]`
	`% Generating 512 bit RSA keys ...[fail]`

Verification	● Run the **show crypto key mypubkey rsa** command to display the public information about the RSA key. If the public information about the RSA key exists, the RSA key has been generated.

<table>
<tr>
<td><b>SSH Server</b></td>
<td>

```
Orion_B54Q(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
         OdKBcCfN tr0r/CT+ cs5tlGKV SOICGifz 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 F3RlKhTN /7PmQYoE v0a2VXTX 8ZCa7Sll EghLDLJc
         w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISgIfZ9 8o5No3Zz MPMOLnQR
         G4c7/28+ GOHzYkTk 4IiQuTIL HRgtbyEYXCFaaxU=
```

</td>
</tr>
</table>

Specifying the SSH Version

<table>
<tr>
<td><b>Configuration Steps</b></td>
<td>● Run the <b>ip ssh version</b> {<b>1</b> | <b>2</b>} command to set the version supported by the SSH server to SSHv2.</td>
</tr>
<tr>
<td><b>SSH Server</b></td>
<td>

```
Orion_B54Q#configure terminal
Orion_B54Q(config)#ip ssh version 2
```

</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><b>Verification</b></td>
<td>● Run the <b>show ip ssh</b> command to display the SSH version currently supported by the SSH server.</td>
</tr>
<tr>
<td><b>SSH Server</b></td>
<td>

```
Orion_B54Q(config)#show ip ssh
SSH Enable - version 2.0
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled
```

</td>
</tr>
</table>

Configuring the SSH Authentication Timeout

Configuration Steps	● Run the **ip ssh time-out** *time* command to set the SSH authentication timeout to 100s.

SSH Server	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#ip sshtime-out100`

Verification	● Run the **show ip ssh** command to display the configured SSH authentication timeout.

SSH Server	`Orion_B54Q(config)#show ip ssh`
	`SSH Enable - version 2.0`
	`Authentication timeout: 100 secs`
	`Authentication retries: 3`
	`SSH SCP Server: disabled`

Configuring the Maximum Number of SSH Authentication Retries

Configuration Steps	● Run the **ip ssh authentication-retries** *retry times* command to set the maximum number of user authentication retries on the SSH server to 2.

SSH Server	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#ip ssh authentication-retries 2`

Verification	● Run the **show ip ssh** command to display the configured maximum number of authentica retries.

SSH Server	`Orion_B54Q(config)#show ip ssh`
	`SSH Enable - version 2.0`
	`Authentication timeout: 100 secs`
	`Authentication retries: 3`
	`SSH SCP Server: disabled`

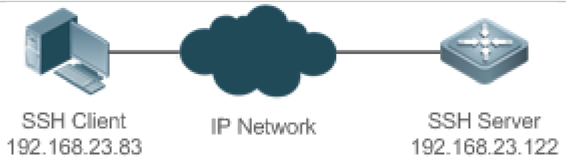
Configuring the Public Key Authentication

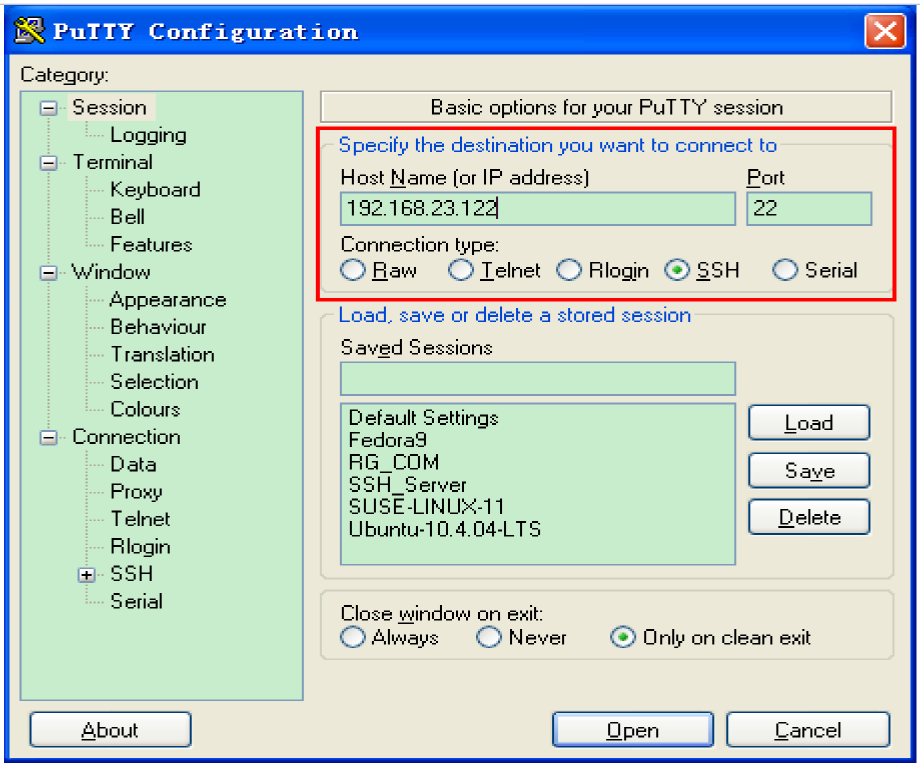
Configuration Steps	● Run the **ip ssh peer** *username* **public-key** { **rsa** | **dsa**}*filename* command to associate a public key file of the client with a user name. When the client is authenticated upon login, a public key file (for example, RSA)is specified based on the user name.

SSH Server	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)# ip ssh peer test public-key rsaflash:rsa.pub`

Verification	● 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 serv If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

Configuring SSH Device Management

Scenario **Figure 10-31**	 SSH Client 192.168.23.83 IP Network SSH Server 192.168.23.122 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 soft includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client.
Configuration Steps	● Start the PuTTY software. ● On the **Session** option tab of PuTTY, type in the host IP address **192.168.23.122** 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** tab of PuTTY, select the au **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.
SSH Client	Figure 10-32



Host Name (or IP address): 192.168.23.122

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

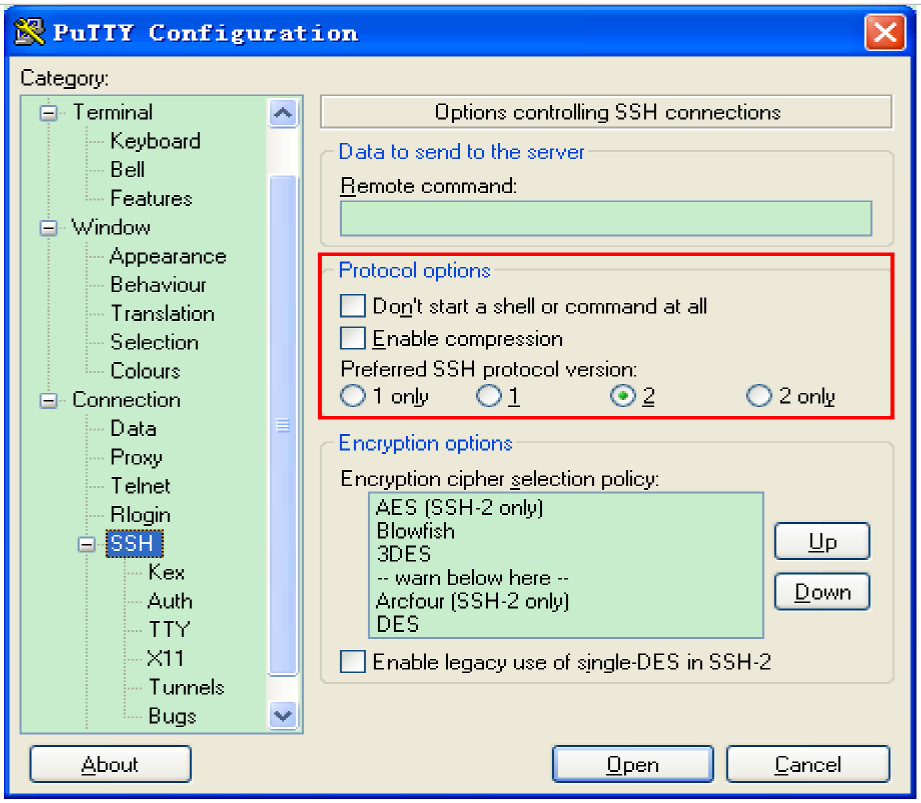
Saved Sessions

Default Settings
Fedora9
RG_COM
SSH_Server
SUSE-LINUX-11
Ubuntu-10.4.04-LTS

Close window on exit: ○ Always ○ Never ● Only on clean exit

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 10-33



Data to send to the server

Remote command:

Protocol options

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version:

○ 1 only ○ 1 ● 2 ○ 2 only

Encryption options

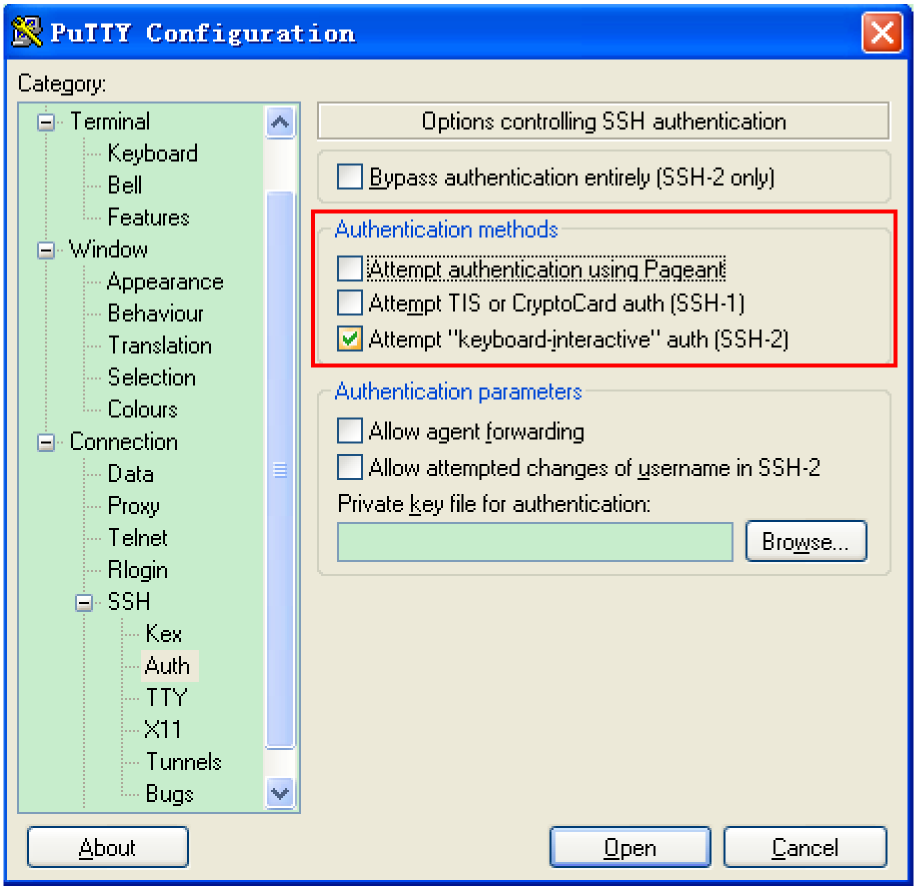
Encryption cipher selection policy:

AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
Arcfour (SSH-2 only)
DES

□ Enable legacy use of single-DES in SSH-2

As shown in Figure 10 -33, select **2** as the preferred SSH protocol version in the **Protocol options** pane because SSHv2 is used for login.

Figure 10-34



Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)

Authentication methods

□ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

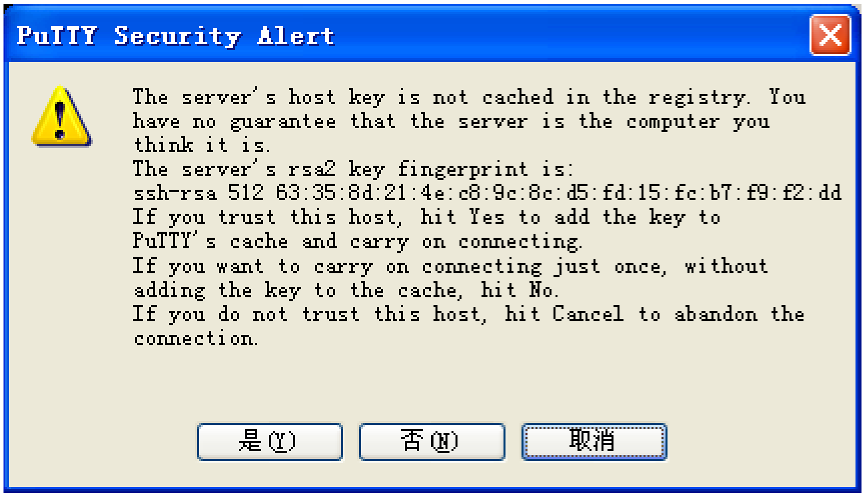
□ Allow attempted changes of username in SSH-2

Private key file for authentication:

As shown in Figure 10 -34, 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 10 -35.

Figure 10-35

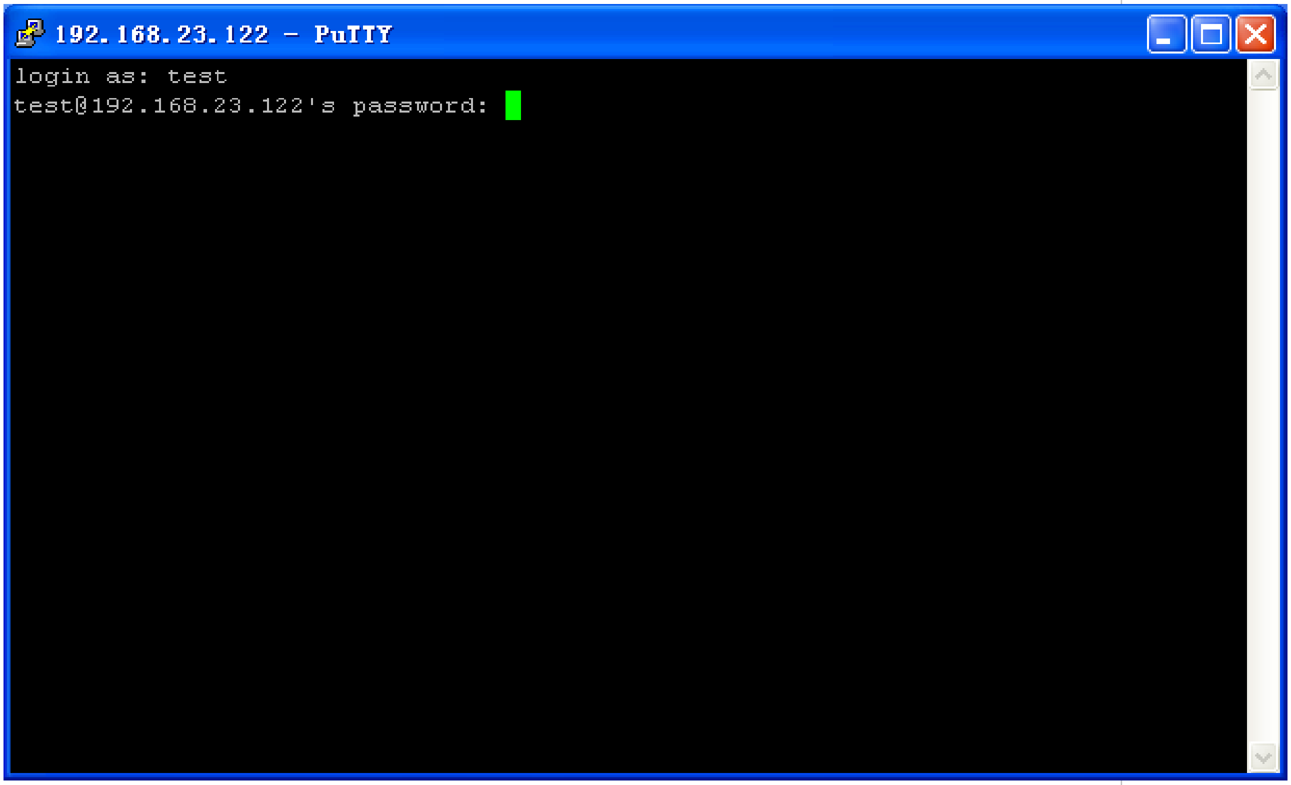


```
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 512 63:35:8d:21:4e:c8:9c:8c:d5:fd:15:fc:b7:f9:f2:dd
If you trust this host, hit Yes to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the
connection.
```

The **PuTTY Security Alert** indicates that you are logging in to the clie
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 10 -36.

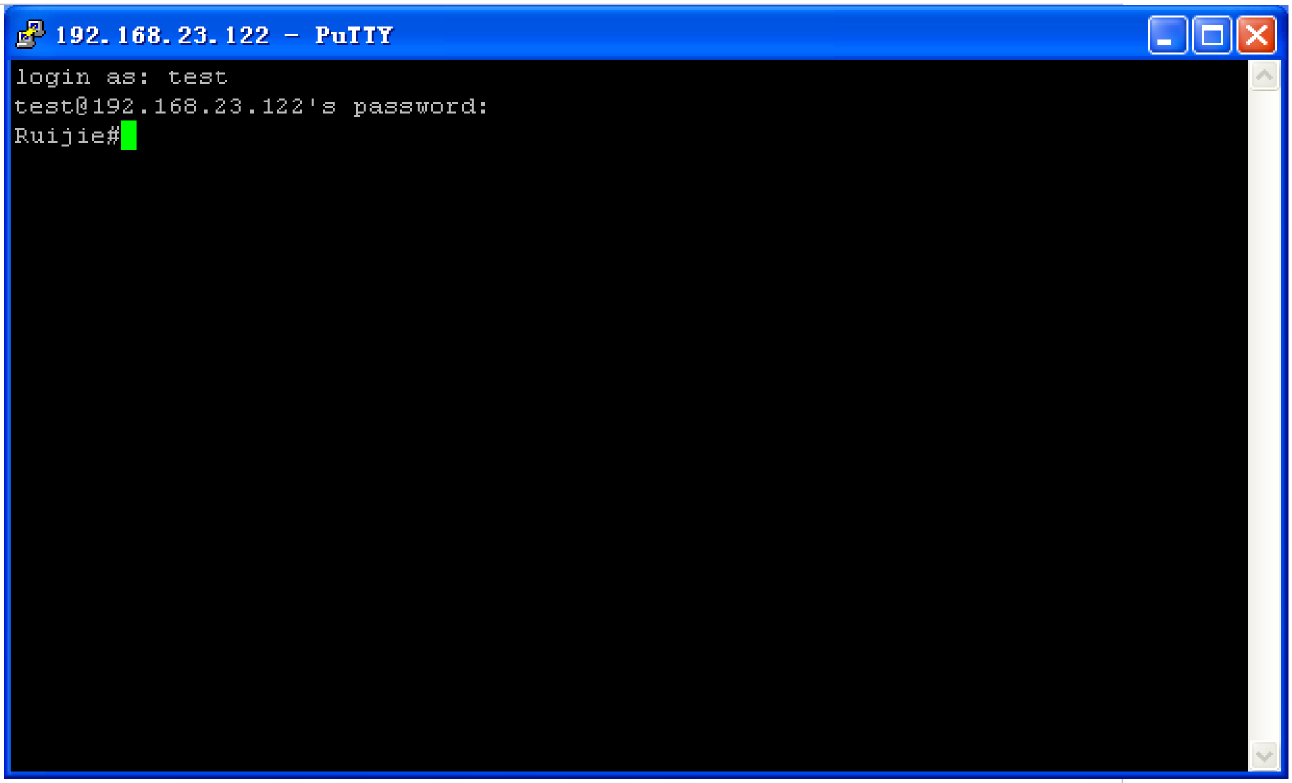
Figure 10-36



```
login as: test
test@192.168.23.122's password:
```

Type in the correct user name and password, and you can log in to the SSH terminal interface, as shown in Figure 10 -37.

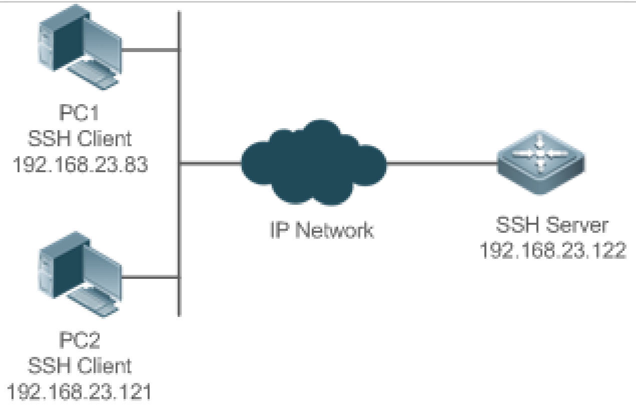
Figure 10-37

	 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_B54Q#show ip ssh SSH Enable - version 1.99 Authentication timeout: 120 secs Authentication retries: 3 Orion_B54Q#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 10-38



SSH users can use the local line password for user authentication as shown in Figure 10-38. 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, returns a message indicating t 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:

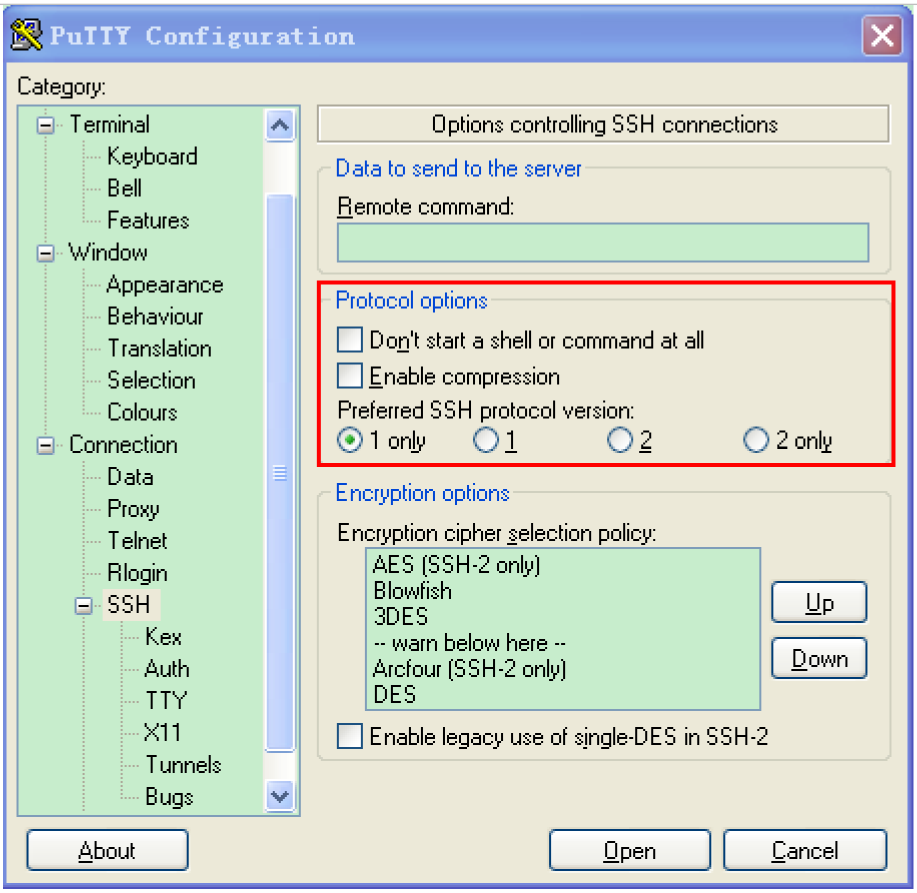
- Diversified SSH client software is available, including SecureCRT, Linux, and PuTTY. This document takes PuTTY as an example to explain the method for configuring the For details about the configuration method, see "Configuration Steps."

SSH Server

Before configuring SSH-related function, ensure that the route from the SSH us segment of the SSH server is reachable. The interface IP address config Figure 10 -39. The detailed procedures for configuring IP addresses and routes are omitted.

```
Orion_B54Q(config)# enable service ssh-server

Orion_B54Q(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_B54Q(config)#interface fastEthernet0/1 Orion_B54Q(config-if-fastEthernet0/1)#ip address 192.168.23.122 255.255.255.0 Orion_B54Q(config-if-fastEthernet0/1)#exit Orion_B54Q(config)#line vty 0 Orion_B54Q(config-line)#password passzero Orion_B54Q(config-line)#privilege level 15 Orion_B54Q(config-line)#login Orion_B54Q(config-line)#exit Orion_B54Q(config)#line vty1 4 Orion_B54Q(config-line)#password pass Orion_B54Q(config-line)#privilege level 15 Orion_B54Q(config-line)#login Orion_B54Q(config-line)#exit
SSH Client(PC1/ PC2)	Figure 10-39



Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version:

● 1 only ○ 1 ○ 2 ○ 2 only

Encryption options

Encryption cipher selection policy:

AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
Arcfour (SSH-2 only)
DES

□ Enable legacy use of single-DES in SSH-2

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 metho "Configuring SSH Device".) 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

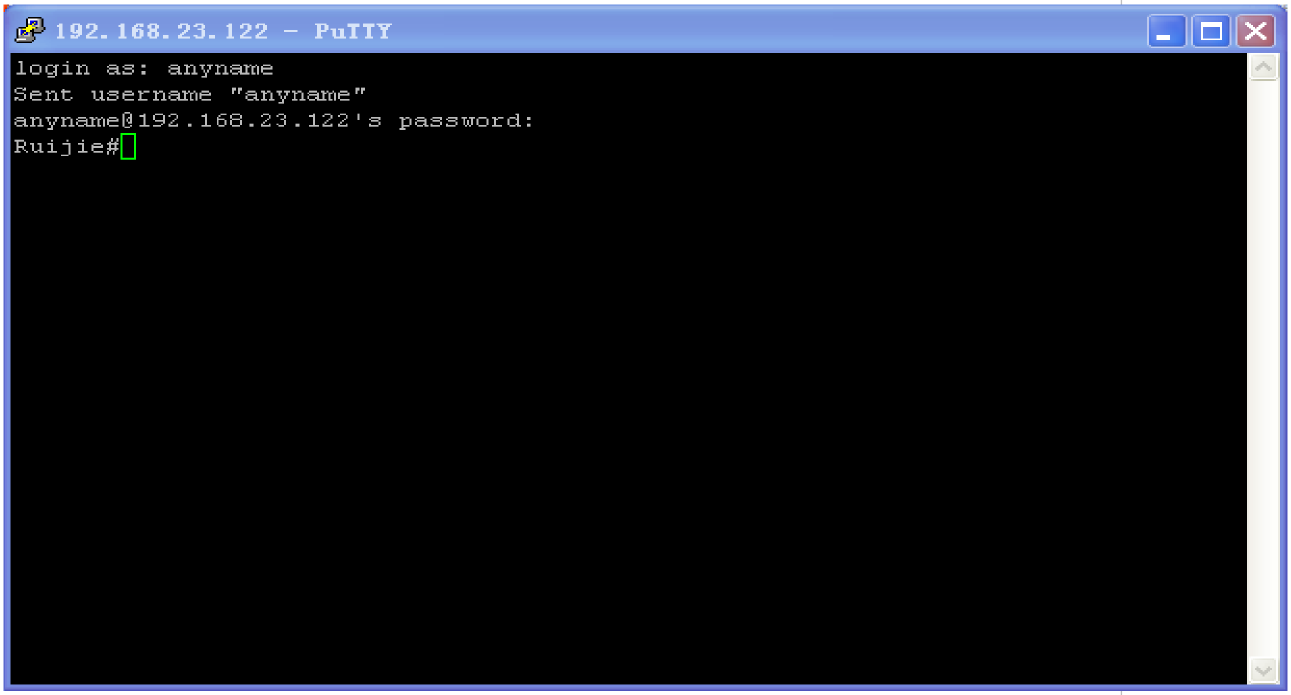
```
Orion_B54Q#show running-config

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, Figure 10 -40.

Figure 10-40

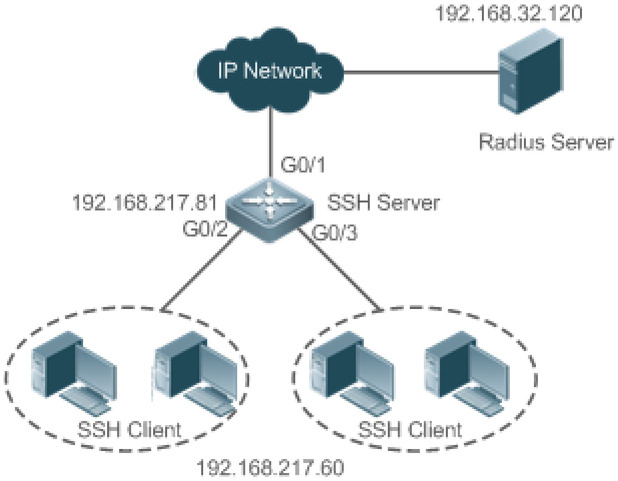


```
login as: anyname
Sent username "anyname"
anyname@192.168.23.122's password:
Ruijie#
```

```
Orion_B54Q#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`
	`2 vty 1 --- idle 00:00:58 192.168.23.121`

↘ Configuring AAA Authentication of SSH Users

Scenario **Figure 10-41**	 192.168.32.120 IP Network Radius Server G0/1 192.168.217.81 SSH Server G0/2 G0/3 SSH Client SSH Client 192.168.217.60 SSH users can use the AAA authentication mode for Figure 10 -41To 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 managemen,tthe AAA authentication mode is used on the user login interface of the SSH client. Two authentication methods auth,eanrteicpartoiwinded in the AAA aut 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_B54Q(config)# enable service ssh-server`
	`Orion_B54Q(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_B54Q(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_B54Q(config)#interface gigabitEthernet1/1
Orion_B54Q(config-if-gigabitEthernet1/1)#ip address 192.168.217.81 255.255.255.0
Orion_B54Q(config-if-gigabitEthernet1/1)#exit
Orion_B54Q#configure terminal
Orion_B54Q(config)#aaa new-model
Orion_B54Q(config)#radius-server host 192.168.32.120
Orion_B54Q(config)#radius-server key aaaradius
Orion_B54Q(config)#aaa authentication login methodgroup radius local
Orion_B54Q(config)#line vty 0 4
Orion_B54Q(config-line)#login authentication method
Orion_B54Q(config-line)#exit
Orion_B54Q(config)#username user1 privilege 1 password 111
Orion_B54Q(config)#username user2 privilege 10 password 222
Orion_B54Q(config)#username user3 privilege 15 password 333
Orion_B54Q(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_B54Q#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 $1$hbgz$ArCsyqty6yyzzp03
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**.

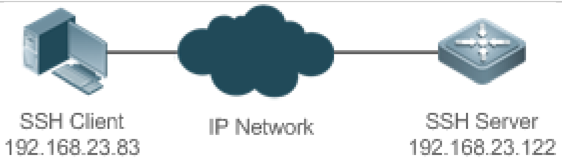
Choose **Security Management**>**Device Management Rights**, and set the rights of the login user.

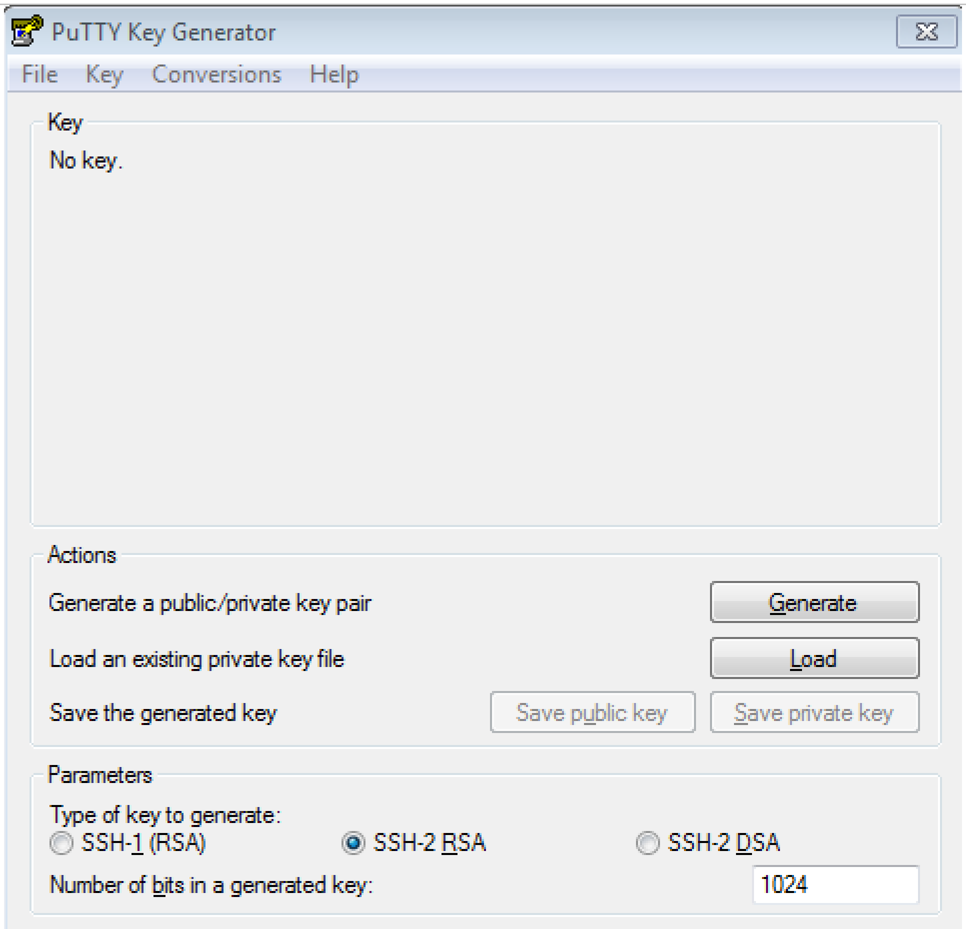
Choose **Security Management**>**Device Administrator**, and add the user name **user** and password

	pass. Configure the SSH client and set up a connection to the SSH server. For details, see the example. Type in the user name **user** and password **pass**. Verify that you can log in to the SSH serv successfully.

```
Orion_B54Q#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

Scenario **Figure 10-42**	 SSH Client 192.168.23.83 IP Network SSH Server 192.168.23.122 SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in Figure 10 -42. SSH is configured on the client so that a secure connection is set between the SSH client and the SSH server.
Configuration Steps	● 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. 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. ● 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.
SSH Client	Run the **puttygen.exe** software on the client. Select **SSH-2 RSA** in the **Parameters** pane, and click **Generate** to generate a key, as shown in Figure 10 -43. Figure 10-43



Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

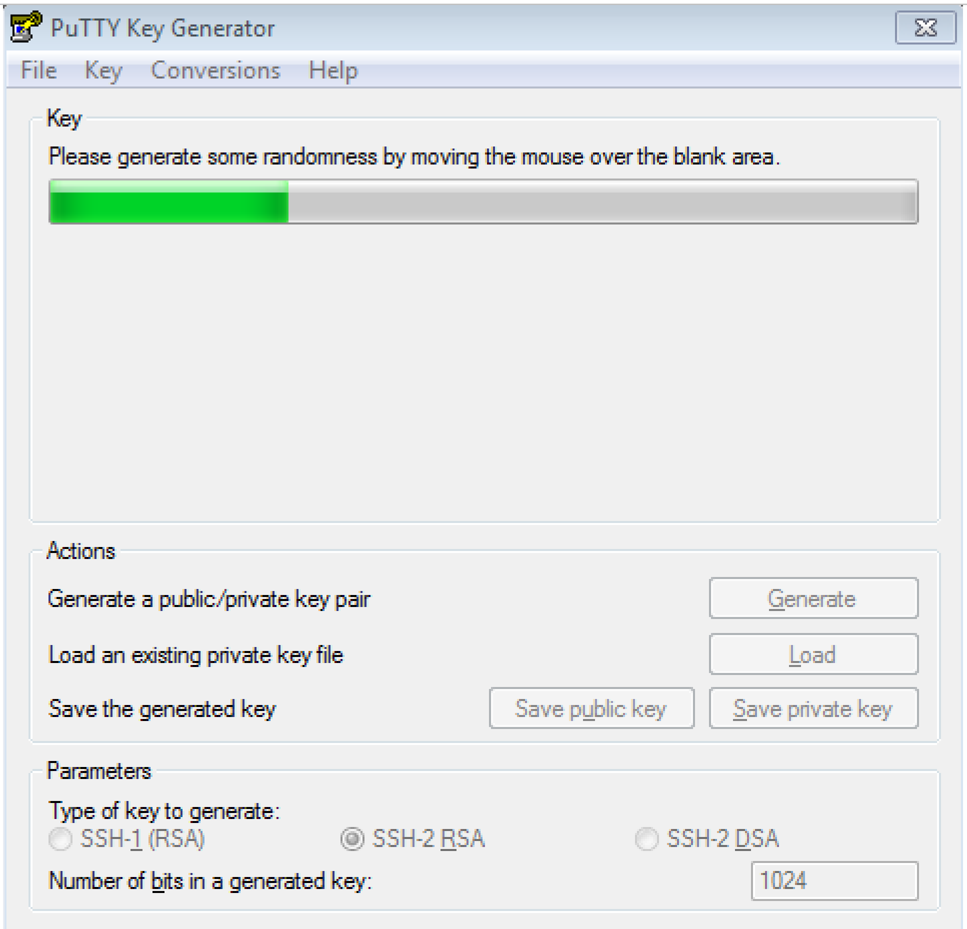
Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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 10 -44.

Figure 10-44



Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

Load an existing private key file

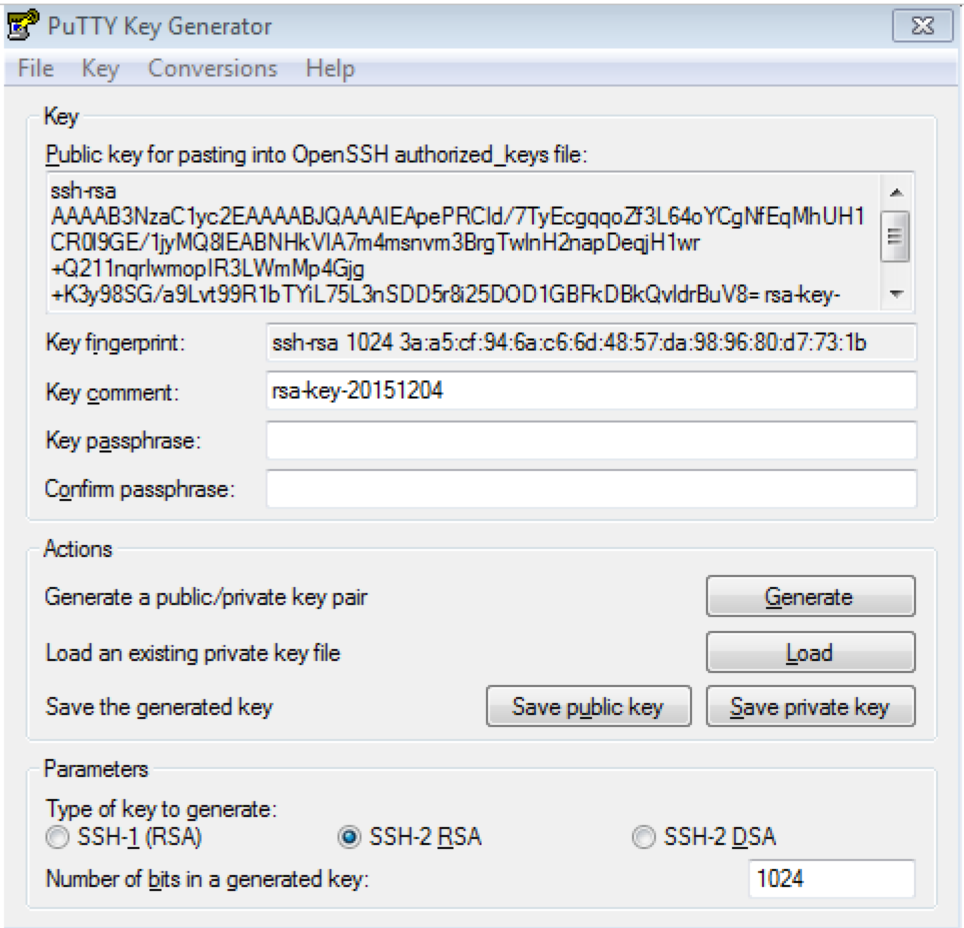
Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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 10-45



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEApePRCld/7TyEcgqqoZf3L64oYCgNfEqMhUH1
CR0I9GE/1jyMQ8lEABNHkVIA7m4msnvm3BrgTwlnH2napDeqjH1wr
+Q211nqrlwmopIR3LWmMp4Gjg
+K3y98SG/a9Lvt99R1bTYiL75L3nSDD5r8i25DOD1GBFkDBkQvldrBuV8= rsa-key-
```

Key fingerprint: ssh-rsa 1024 3a:a5:cf:94:6a:c6:6d:48:57:da:98:96:80:d7:73:1b

Key comment: rsa-key-20151204

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

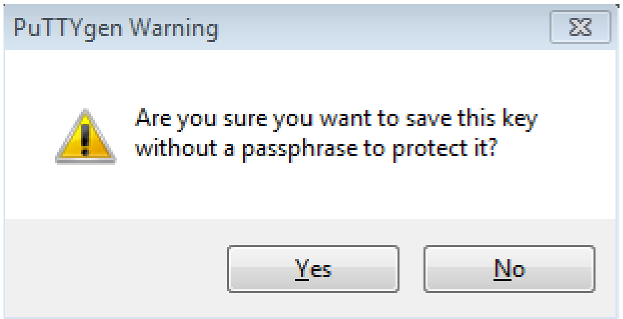
Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

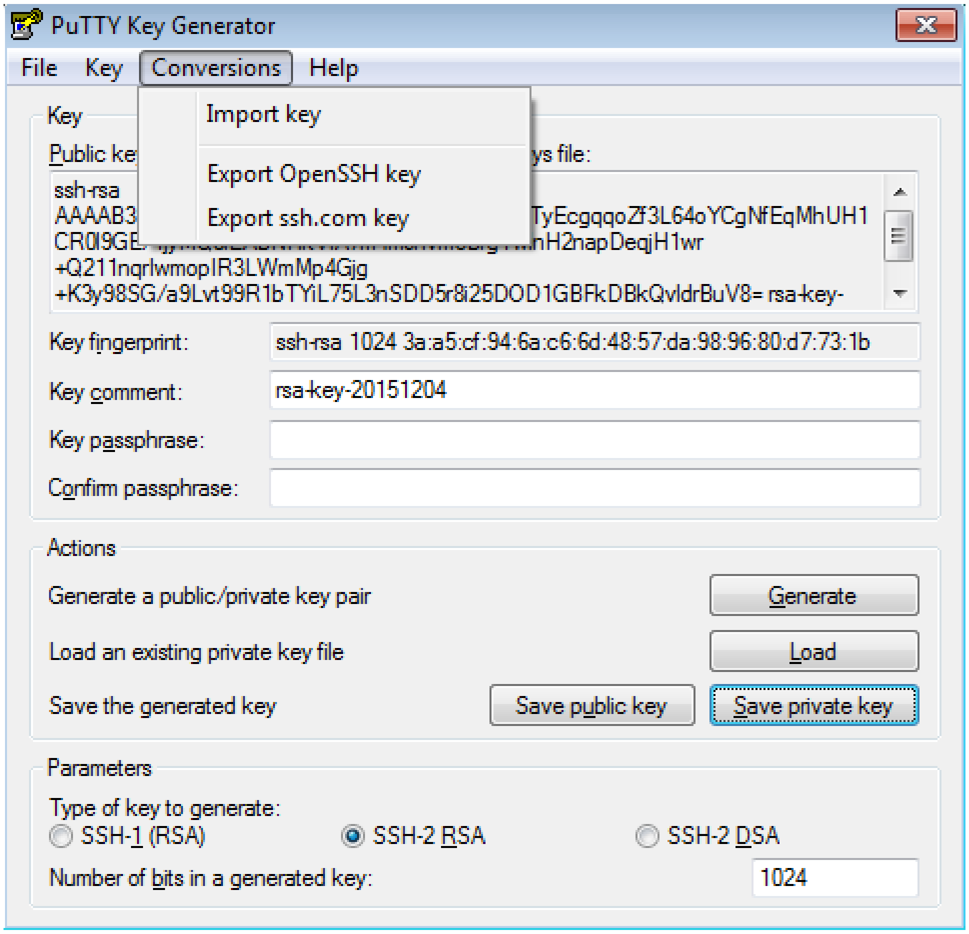
After the key pair is generated, click **Save public key**, type in the public key name **test_key.pub**, select the storage path, and click **Save**. Then click **Save private key**The following prompt box is displayed. Select **Yes**, type in the public key name **test_private**, and click **Save**.

Figure 10-46



Are you sure you want to save this key without a passphrase to protect it?

You must select the OpenSSH key file; otherwise, **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 10 -47.

<table>
<tr><td></td><td>Figure 10-47


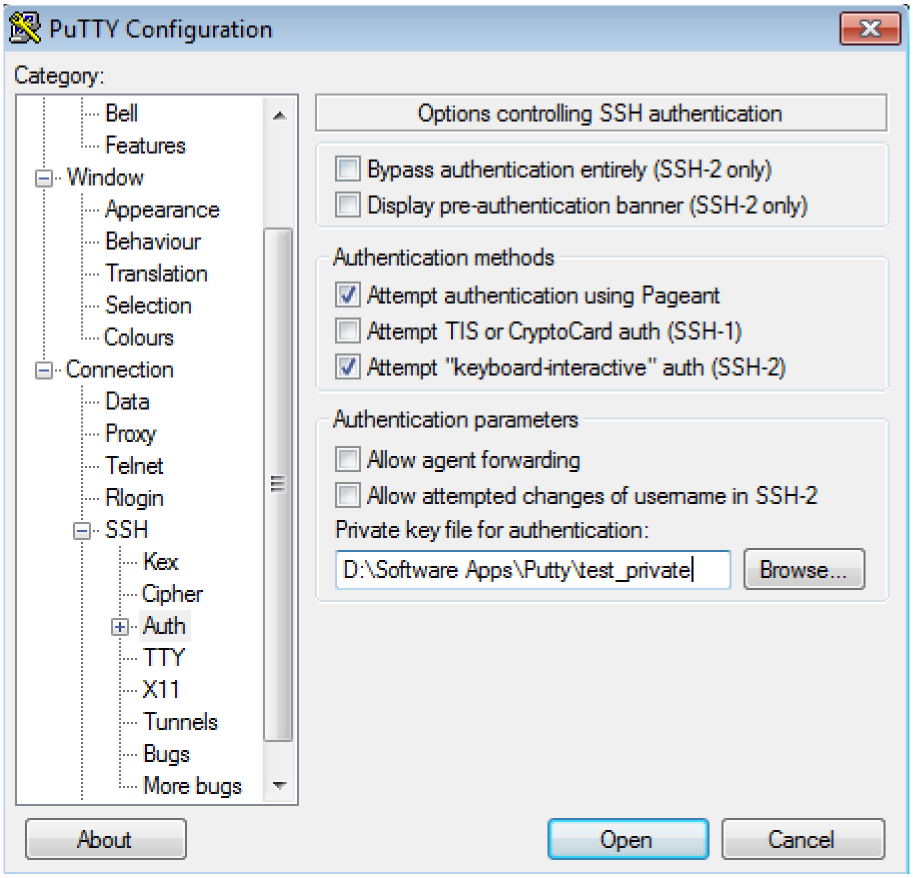
Public ke... ys file:
ssh-rsa
AAAAB3 ... TyEcgqqoZf3L64oYCgNfEqMhUH1
CR0l9GE ... nH2napDeqjH1wr
+Q211nqrlwmopIR3LWmMp4Gjg
+K3y98SG/a9Lvt99R1bTYiL75L3nSDD5r8i25DOD1GBFkDBkQvldrBuV8= rsa-key-
Key fingerprint: ssh-rsa 1024 3a:a5:cf:94:6a:c6:6d:48:57:da:98:96:80:d7:73:1b
Key comment: rsa-key-20151204
Key passphrase:
Confirm passphrase:
Generate a public/private key pair
Load an existing private key file
Save the generated key
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA
Number of bits in a generated key: 1024</td></tr>
<tr><td><b>SSH Server</b></td><td>

```
Orion_B54Q#configure terminal

Orion_B54Q(config)# ip ssh peer test public-key rsaflash:test_key.pub
```

</td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Verification</b></td><td>

- After completing the basic configurations of the client and the server, specify the private key fil **test_private** on the PuTTY client, and set the host IP address **192.168.23.122** and port ID to **22** 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.

</td></tr>
<tr><td></td><td>Figure 10-48</td></tr>
</table>



PuTTY Configuration

Category:

Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)

□ Display pre-authentication banner (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication:

D:\Software Apps\Putty\test_private

Common Errors

- The **no crypto key generate** command is used to delete a key.

10.4.2 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

Command	**ip scp server enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to enable the SCP server. Run the **no ip scp server enable** command to disable the SCP server.

Configuration Example

Enabling the SCP Server

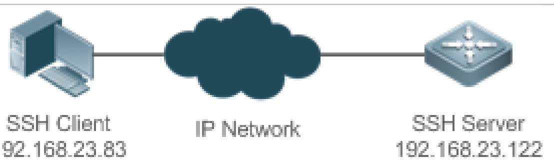
Configuration Steps	● Run the **ip scp server enable** command to enable the SCP server.

	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)#ip scp server enable`

Verification	● Run the **show ip ssh** command to check whether the SCP server function is enabled.

	`Orion_B54Q(config)#show ipssh`
	`SSH Enable - version 1.99`
	`Authentication timeout: 120 secs`
	`Authentication retries: 3`
	`SSH SCP Server: enabled`

Configuring SSH File Transfer

Scenario **Figure 10-49**	 SSH Client 192.168.23.83 IP Network SSH Server 192.168.23.122 The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server.
Configuration	● Enable the SCP service on the server.

Steps

ℹ The SCP server uses SSH threading. When connecting to a network device for SCP transmission, the client occupies a VTY session (You can finds out that the user type is SSH by running the show user command).

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

```
Syntax of the SCP command:
scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-iidentity_file]
         [-l limit] [-o ssh_option] [-P port] [-S program]
         [[user@]host1:]file1 [...] [[user@]host2:]file2
Descriptions of some options:
-1: Uses SSHv1 (If not specified, SSHv2 is used by default);
-2: Uses SSHv2 (by default);
-C: Uses compressed transmission.
-c: Specifies the encryption algorithm to be used.
-r:Transmits the whole directory;
-i: Specifies the key file to be used.
-l: Limits the transmission speed (unit: Kbit/s).
For other parameters, see the filescp.0.
```

SSH Server

```
Orion_B54Q#configure terminal
Orion_B54Q(config)# ip scp server enable
```

Verification

- File transmission example on the Ubuntu 7.10 system:

Set the username of a client **test** and copy the **config.text** file from the network device with the IP address of 192.168.195.188 to the **/root** directory on the local device.

```
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
```

10.5 Monitoring

Displaying

Description	Command
Displays the effective SSH server configurations.	**show ipssh**
Displays the established SSH connection.	**show ssh**
Displays the public information of the SSH public key.	**show crypto key mypubkey**
Displays the established SSH client session.	**show ssh-session**

Debugging

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

Description	Command
Debugs SSH sessions.	**debug ssh**
Debugs SSH client sessions.	**debug ssh client**

11 Configuring URPF

11.1 Overview

Unicast Reverse Path Forwarding (URPF) is a function that protects the network against source address spoofing.

URPF obtains the source address and inbound interface of a received packet, and searches a forwarc forwarding table based on the source address. If the entry does not exist, the packet is dropped. If the outbound interface of the forwarding entry does not match the inbound interfac Otherwise, the packet is forwarded.

URPF is implemented in two modes:

- Strict mode: It is often deployed on a point-to-point (P2P) interface, and inbound and outbound data streams must go through the network of the P2P interface.
- Loose mode: It is applicable to the asymmetric routes or multihomed network that have the problem of asy traffic.

Protocols a Standards

- RFC 2827: Network Ingress Filtering: DDOS Attacks which employ IP Source Address Spoofing
- RFC 3704: Ingress Filtering for Multi-homed Networks

11.2 Applications

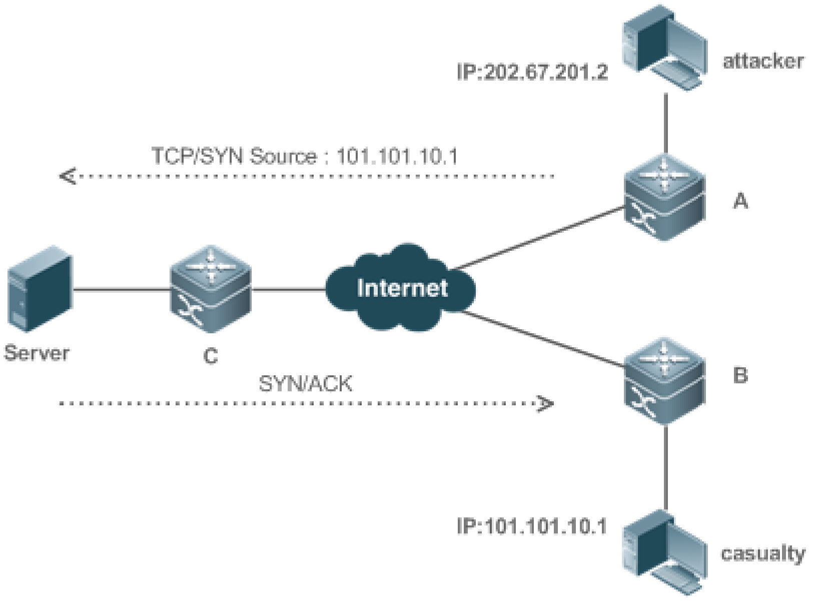
Application	Description
Strict Mode	Block the packets with spoofed sourced addresses at t aggregation layer to prevent sending these packets from PCs to the core network.
Loose Mode	On a multihomed network, the user network is connected to multi service providers (ISPs), and the inbound and outbound traffic is not symmetric. Deploy the URPF loose mode on the outbound interface connected to ISF prevent invalid packets from attacking the user network.

11.2.1 Strict Mode

Scenario

An attacker initiates an attack by sending packets with the spoofed source address 11.0.0.1. As a result, the server sends a lot of SYN or ACK packets to the hosts that do not initiate the attack, and the host with the real source address 11.0.0.1 is also affectedEven worse, if the network administrator determines that this address initiates an attack to the network, and therefore blocks all data streams coming from this source address, the denial of service (DoS) of this source address occurs.

Figure 11-50



Remarks	The attacker sends spoofing packets using a spoofed address of the casualty.

Deployment

- Deploy the URPF strict mode on device A to protect the device against source address spoofing.

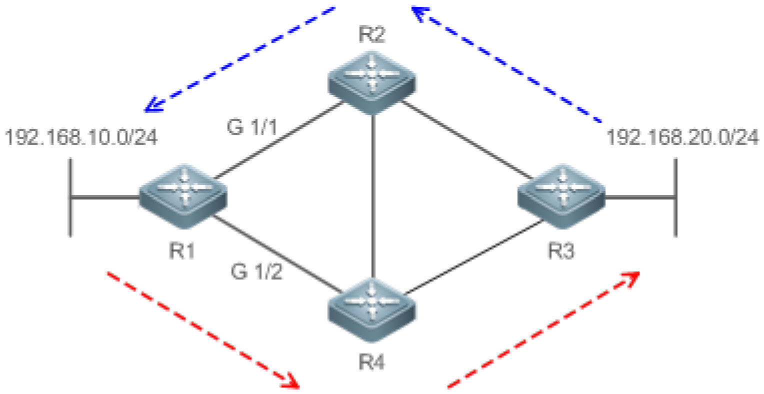
11.2.2 Loose Mode

Scenario

The asymmetric route is a common network application used to control the network traffic or to meet the ro requirements.

As shown in Figure 11 -51, if the URPF strict mode is enabled on the G1/1 interface of R 1, R1 receives a packet from the network segment 192.168.20.0/24 on the G1/1 interface, but the interface obtained through the Therefore, this packet fails in the URPF check and is dropped.

Figure 11-51



Deployment

- Reversely search a route based on the source IP address of a received packet. The purpose is to find a route, and it is not required that the outbound interface of the next hop on the route must be the inbound interface of the rec packet.
- The URPF loose mode can resolve the asymmetric traffic problem of the asymmetric route and prevents acc invalid data streams.

11.3 Features

Basic Concepts

↘ URPF Strict Mode

Obtain the source address and inbound interface of a received packet, and search a forwarding entry in the forwarding table based on the source address. If the entry does not exist, the packet is dropped. If the outbound interface of the forwarding entry does not match the inbound interface of the packet, the packet is also dropped. The strict mode requires that the inbound interface of a received packet must be the outbound interface of the route entry to the source address of the packet.

↘ URPF Loose Mode

Reversely search a route based on the source IP address of a received packet. The purpose is to find a route, and it is not required that the outbound interface of the next hop on the route must be the inbound interface of the recei However, the route cannot be a route of a host on the local network.

↘ URPF Packet Loss Rate

The URPF packet loss rate is equal to the number of packets dropped due The unit is packets/second, that is, pps.

↘ Calculation Interval of the URPF Packet Loss Rate

It is the interval from the previous time the packet loss rate is calculated to the current time the packet loss rate is calculated.

Sampling Interval of the URPF Packet Loss Rate

It the interval at which the number of lost packets is
This interval must be equal to or longer than the calculation interval of the packet loss rate.

Threshold of the URPF Packet Loss Rate

It refers to the maximum packet loss rate that is acceptable. When the packet loss rate exceeds the threshold, alarms can be sent to users through syslogs or trap messages. You can adjust the threshold of the packet loss rate based on the actua conditions of the network.

Alarm Interval of the URPF Packet Loss Rate

It is the interval at which alarms are sent to users. You can adjust the alarm based on the actual conditions of the network to prevent frequently output of logs or trap messages.

Calculation of the URPS Packet Loss Rate

Between the period of time from enabling of URPF to the time that the sampling interval arrives, the packet loss rate is equal to the number of lost packets measured within the sampling interval divided by the URPF enabling duration. After that, the packet loss rate is calculated as follows: Current packet loss rate = (Current number of lost packets measure calculation interval – Number of lost packets measured before the sampling interval)/Sampling interval

Overview

Feature	Description
Enabling URPF	Enable URPF to perform a URPF check,thus protecting the device against spoofing.
Notifying the URPF Packet Loss Rate	To facilitate monitoring of information about lost packets after URPF is enabled, O devices support the use of syslogs and trap messages to proactively notify users of the packet loss information detected in the URPF check.

11.3.1 Enabling URPF

Enable URPF to perform a URPF check on IPv4 packets, thus protecting the device against source address spoofing.

Working Principle

URPF can be applied to IPv4 packets based on configurations, but the following packets are not checked by URPF:

1. After URPF is enabled, the source address of a packet is checked only if the destination address of the packet is an IPv4/IPv6 unicast address, and is not checked if the packet is a multicast packet or an IPv4 broadcast packet.
2. If the source IP address of a DHCP/BOOTP packet is 0.0.0.0 and the destination IP address is 255.255.255.255, the packet is not checked by URPF.
3. A loopback packet sent by the local device to itself is not checked by URPF.

URPF Configured in Interface configuration mode

URPF, including IPv4 URPF, is performed on packets received on the configured interface.

- By default, the default route is not used for the URPF check. You can configure data to use the default route for the URPF check if necessary.
- By default, packets that fail in the URPF check will be dropped. If the ACL (*acl-name*) is configured, the packet is matched against the ACL after it fails in the URPF check. If no ACL exists, or a packet matches a deny ACL entry (ACE), the packet will be dropped. If the packet matches a permit ACE, the packet will be forwarded.
- After the URPF IPv4 command is configured to enable URPF, a switch will perform a URPF check on IPv4 packets,

✓ A switch supports configuration of URPF on a routed port of L3 aggregate port (AP). The following constraints exists:

- URPF does not support association with the ACL option.
- URPF does not support the use of IPv6 routes with a 65-bit to 127-bit prefix for a URPF check.
- After URPF is enabled on interfaces, a URPF check is performed on all packets corresponding to these interfaces, which increase the scope of packets checked by URPF. If a packet received on a tunnel port is also received on the preceding physical ports, the packet is also checked by URPF. In such as scenario, be cautious in enabling URPF.
- After URPF is enabled, the route forwarding capacity of the device will be reduced by half.
- After the URPF strict mode is enabled, if a packet received on an interface matches an equal-cost route duri URPF check, the packet will be processed according to the URPF loose mode.

Related Configuration

↘ Enabling URPF for a Specified Interface

By default, URPF is disabled for a specified interface.

Run the **ip verify unicast source reachable-via**{**rx** | **any** }[**allow-default**][*acl-name*] command to enable or disable the IPv4 URPF function for a specified interface.

By default, the default route is not used for the URPF check. You can use the **allow-default** keyword to use the default route for the URPF check if necessary.

By default, packets that fail in the URPF check will be dropped. If the ACL (*acl-name*) is configured, the packet is matched against the ACL after it fails in the URPF check. If no ACL exists, or a packet matches a deny ACE, the packet will be dropped. If the packet matches a permit ACE, the packet will be forwarded.

11.3.2 Notifying the URPF Packet Loss Rate

To facilitate monitoring of information about lost packets after URPF is enabled, Orion_B54Q devices support th syslogs and trap messages to proactively notify users of the packet loss information detected in the URPF check.

Working Principle

Between the period of time from enabling of URPF to the time that the sampling interval arrives, the packet loss rate is equal to the number of lost packets measured within the sampling interval divided by the URPF enabling duration. After that, the packet loss rate is calculated as follows: Current packet loss rate = (Current number of lost packets measured calculation interval – Number of lost packets measured before the sampling interval)/Sampling interval

After the function of monitoring the URPF packet loss information is enabled, the device can proactively send syslogs or trap messages to notify users of the packet loss information detected in the URPF check so that users can monitor the network status conveniently.

Related Configuration

Configuring the Calculation Interval of the URPF Packet Loss Rate

By default, the calculation interval of the URPF packet loss rate is 30s. If the calculation interval is found too short, run the **ip verify urpf drop-rate compute interval** *seconds* command to modify the calculation interval.

The calculation interval of the URPF packet loss rate ranges from 30 to 300.

Configuring the Alarm Interval of the URPF Packet Loss Rate

By default, the alarm interval of the URPF packet loss rate is 300s. If the alarm interval is found inappropriate, run the **ip verify urpf drop-rate notify hold-down** *seconds* command to modify the alarm interval of the URPF packet loss rate.

The unit of the alarm interval is second. The value ranges from 30 to 300.

Configuring the Function of Monitoring the URPF Packet Loss Information

By default, the function of monitoringthe URPF packet loss information is disabled.

Run the **ip** [**ipv6**] **verify urpf drop-rate notify** command to enable or disable the function of monitoringthe URPF packet loss information.

Configuring the Threshold of the URPF Packet Loss Rate

By default, the threshold of the URPF packet loss rate is 1000 pps. If the threshold is found inappropriate, ru **ip [ipv6] verify urpf notification threshold** *rate-value* command to modify the threshold of the URPF packet loss rate.

The unit of the threshold is pps. The value ranges from 0 to 4,294,967,295.

11.4 Configuration

Configuration Item	Description and Command	
Enabling URPF	⚠ (Mandatory) It is used to enable URPF.	
	ip verify unicast source reachable-via { rx | any } [allow-default] [*acl-name* **] (Interface configuration mode)**	Enables URPF for a specified interface.
Configuring the Function of Monitoring the URPF Packet	⚠ (Optional) It is used to enable the function of monitoring the URPF pac information.	

Loss Information	**ip verify urpf drop-rate compute interval** *seconds*	Configures the calculation interval of th URPF packet loss rate.
	ip verify urpf drop-rate notify	Configures thefunction of monitoring URPF packet loss information.
	ip verify urpf drop-rate notify hold-down *seconds*	Configures the alarm interval of the URPF packet loss rate.
	Ip verify urpf notification threshold *rate-value*	Configures the threshold of th packet loss rate.

11.4.1 **Enabling URPF**

Configuration Effect

- Enable URPF to perform a URPF check on IPv4 packets, thus protecting the device against source address spoofing.
- URPF can be enabled in interface configuration mode.
- URPF enabled in global configuration mode supports only the strict mode, whereas URP configuration mode supports both the strict and loose modes.

Notes

- URPF is implemented with the help of the existing unicast routes on the network. Therefore, IPv4 unicast routes must be configured on the network.
- URPF configured in global configuration mode is mutually exclusive with URPF configured in interface configu mode.

Configuration Steps

↘ Enabling IPv4 URPF for a Specified Interface

- Mandatory.

Verification

Enable URPF and check the source address as follows:

- If the strict mode is used, check whether a packet is forwarded only when the forwarding table contains the s address of the received IPv4 or IPv6 packet and the outbound interface of the searched forwarding entry matches the inbound interface of the packet; otherwise, the packet is dropped.
- If the loose mode is used, check whether a packet is forwarded when a forwarding entry can be found in the forwarding table for the source address of the received IPv4 or IPv6 packet; otherwise, the packet is dropped.

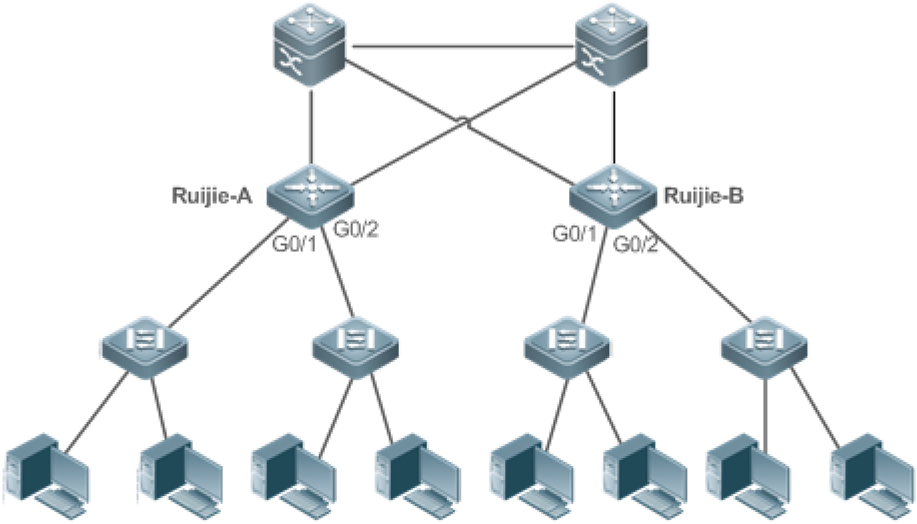
Related Commands

↘ Enabling IPv4 URPF for a Specified Interface

Command	**ip verify unicast source reachable-via { rx | any } [allow-default] [** *acl-id* **]**
Parameter Description	**rx**: Indicates that the URPF check is implemented in strict mode.The strict mode requires that the outbound interface of the forwarding entry found in the forwarding table based on the source address of a received IP packet must match the inbound interface of the packet. **any**: Indicates that the URPF check is implemented in loose mode.The loose mode only requires that a forwarding entry can be found in the forwarding table based on the source address of a receiv packet. **allow-default**: (Optional) Indicates that the default route can be used for the URPF check. ***acl-id***: (Optional) Indicates the ID of the ACL. Values include 1 t list), 100 to 199 (IP extended access list), 1300 to 1999 (IP standard access lis range), and 2000 to 2699 (IP extended access list, expanded range).
Command Mode	Interface configuration mode
Usage Guide	Based on the source address of a received IP packet, URPF checks whether any route to the source address exists in the forwarding table and accordingly determines whether the packet is v forwarding entry is matched, the packet is determined as invalid. You can enable URPF in interface configuration mode to perform a URPF check on packets received on the interface. By default, the default route is not used for the URPF check. You can use the **allow-default** keyword to use the default route for the URPF check if necessary. By default, packets that fail in the URPF check will be dropped. If the ACL (*acl-name*) is configured, the packet is matched against the ACL after it fails in the URPF check. If no ACL exists, or a packet matches a deny ACE, the packet will be dropped. If the packet matches a permit ACE, the forwarded. A switch supports configuration of URPF on a routed port or L3 AP port. In addition, the following constraints exists: 1. URPF does not support association with the ACL option. 2. URPF does not support the use of IPv6 routes with a 65-bit to 127-bit prefix for a URPF check. 3. After URPF is enabled on interfaces, a URPF check is performed on all packets r physical ports corresponding to these interfaces, which increase the scope of packets checked by URPF.If a packet received on a tunnel port is also received on the preceding physical ports, the packet is also checked by URPF. In such as scenario, be cautious in enabling URPF. 4. After URPF is enabled, the route forwarding capacity of the device will be reduced by half. 5. After the URPF strict mode is enabled, if a packet received on an interface matches an equal-cost route during the URPF check, the packet will be processed according to the URPF loose mode. URPF configured in global configuration mode is mutually exclusive with URP interface configuration mode.

Configuration Example

Configuring the Strict Mode

	Block the packets with spoofed sourced addresses at the access layer or aggregation layer to prevent sending these packets from PCs to the core network. To meet the preceding requirement, enable URPF in strict mode on the i aggregation device and the access device.
Scenario **Figure 11-52**	
Verification	As shown in Figure 11-52, enable URPF in strict mode on the aggregation devices, in Orion_B54Q A and Orion_B54Q B. The configurations are as follows:

Orion_B54Q-A	`Orion_B54Q-A# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Orion_B54Q-A (config)# interface gigabitEthernet0/1`
	`Orion_B54Q-A (config-if-GigabitEthernet 0/1)#ip address 195.52.1.1 255.255.255.0`
	`Orion_B54Q-A (config-if-GigabitEthernet 0/1)#ip verify unicast source reachable-via rx`
	`Orion_B54Q-A (config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify`
	`Orion_B54Q-A (config-if-GigabitEthernet 0/1)#exit`
	`Orion_B54Q-A (config)# interface gigabitEthernet0/2`
	`Orion_B54Q-A (config-if-GigabitEthernet 0/2)#ip address 195.52.2.1 255.255.255.0`
	`Orion_B54Q-A (config-if-GigabitEthernet 0/2)#ip verify unicast source reachable-via rx`
	`Orion_B54Q-A (config-if-GigabitEthernet 0/2)# ip verify urpf drop-rate notify`
	`Orion_B54Q-A (config-if-GigabitEthernet 0/2)#exit`

Orion_B54Q-B	`Orion_B54Q-B# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`

	`Orion_B54Q-B (config)# interface gigabitEthernet0/1`
	`Orion_B54Q-B (config-if-GigabitEthernet 0/1)#ip address 195.52.3.1 255.255.255.0`
	`Orion_B54Q-B (config-if-GigabitEthernet 0/1)#ip verify unicast source reachable-via rx`
	`Orion_B54Q-B (config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify`
	`Orion_B54Q-B (config-if-GigabitEthernet 0/1)#exit`
	`Orion_B54Q-B (config)# interface gigabitEthernet0/2`
	`Orion_B54Q-B (config-if-GigabitEthernet 0/2)#ip address 195.52.4.1 255.255.255.0`
	`Orion_B54Q-B (config-if-GigabitEthernet 0/2)#ip verify unicast source reachable-via rx`
	`Orion_B54Q-B (config-if-GigabitEthernet 0/2)# ip verify urpf drop-rate notify`
	`Orion_B54Q-B (config-if-GigabitEthernet 0/2)#exit`

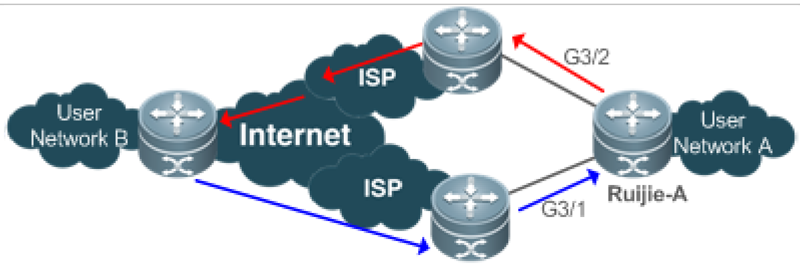
Verification	If source address spoofing exists on the network, run the **show ip urpf** command to display the number of spoofing packets dropped by URPF.

A	`Orion_B54Q-A#show ip urpf interface gigabitEthernet 0/1`
	`IP verify source reachable-via RX`
	`IP verify URPF drop-rate notify enabled`
	`IP verify URPF notification threshold is 1000pps`
	`Number of drop packets in this interface is 124`
	`Number of drop-rate notification counts in this interface is 0`
	
	`Orion_B54Q-A#show ip urpf interface gigabitEthernet 0/2`
	`IP verify source reachable-via RX`
	`IP verify URPF drop-rate notify enabled`
	`IP verify URPF notification threshold is 1000pps`
	`Number of drop packets in this interface is 133`
	`Number of drop-rate notification counts in this interface is 0`

B	`Orion_B54Q-B#show ip urpf interface gigabitEthernet 0/1`
	`IP verify source reachable-via RX`
	`IP verify URPF drop-rate notify enabled`
	`IP verify URPF notification threshold is 1000pps`
	`Number of drop packets in this interface is 124`

	Number of drop-rate notification counts in this interface is 0 Orion_B54Q-B#show ip urpf interface gigabitEthernet 0/2 IP verify source reachable-via RX IP verify URPF drop-rate notify enabled IP verify URPF notification threshold is 1000pps Number of drop packets in this interface is 250 Number of drop-rate notification counts in this interface is 0

Configuring the Loose Mode

	On the egress device Orion_B54Q A of user network A, to prevent invalid packets from attacking the user network, enable URPF in loose mode on the outbound interfaces G3/1 and G3/2 that connect to two ISPs.
Scenario **Figure 11-53**	 User Network B Internet ISP ISP G3/2 G3/1 User Network A Ruijie-A
Orion_B54Q-A	Orion_B54Q-A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Orion_B54Q-A (config)# interface gigabitEthernet3/1 Orion_B54Q-A (config-if-GigabitEthernet 3/1)# ip address 195.52.1.2 255.255.255.252 Orion_B54Q-A (config-if-GigabitEthernet 3/1)# ip verify unicast source reachable-via any Orion_B54Q-A (config-if-GigabitEthernet 3/1)# ip verify urpf drop-rate notify Orion_B54Q-A (config-if-GigabitEthernet 3/1)# exit Orion_B54Q-A (config)# interface gigabitEthernet3/2 Orion_B54Q-A (config-if-GigabitEthernet 3/2)# ip address 152.95.1.2 255.255.255.252 Orion_B54Q-A (config-if-GigabitEthernet 3/2)# ip verify unicast source reachable-via any Orion_B54Q-A (config-if-GigabitEthernet 3/2)# ip verify urpf drop-rate notify Orion_B54Q-A (config-if-GigabitEthernet 3/2)# end
Verification	If source address spoofing exists on the network, run the**show ip urpf** command to display the number

	of spoofing packets dropped by URPF.
A	Orion_B54Q #show ip urpf IP verify URPF drop-rate compute interval is 300s IP verify URPF drop-rate notify hold-down is 300s Interface gigabitEthernet3/1 IP verify source reachable-via ANY IP verify URPF drop-rate notify enabled IP verify URPF notification threshold is 1000pps Number of drop packets in this interface is 4121 Number of drop-rate notification counts in this interface is 2 Interface gigabitEthernet3/2 IP verify source reachable-via ANY IP verify URPF drop-rate notify enabled IP verify URPF notification threshold is 1000pps Number of drop packets in this interface is 352 Number of drop-rate notification counts in this interface is 0

11.4.2 Configuring the Function of Monitoring the URPF Packet Loss Information

Configuration Effect

- After the function of monitoring the URPF packet loss information is enabled, the device can proactively send syslogs or trap messages to notify users of the packet loss information detected in the URPF check so that users can monitor the network status conveniently.

Notes

- URPF must be enabled.

Configuration Steps

↘ Configuring the Calculation Interval of the URPF Packet Loss Rate

- Optional.
- The configuration takes effect on IPv4 URPF.
- Global configuration mode

↘ Configuring the Alarm Interval of the URPF Packet Loss Rate

- Optional.
- The configuration takes effect on IPv4 URPF .
- Global configuration mode

↘ Configuring the Function of Monitoring the URPF Packet Loss Information

- Optional.
- Interface configuration mode

↘ Configuring the Threshold of the URPF Packet Loss Rate

- Optional.
- Interface configuration mode

Verification

Simulate a source address spoofing attack, enable URPF, and check as follows:

- Enable the alarm function. After the packet loss rate exceeds the threshold, check whether an alarm can be generated normally.

Related Commands

↘ Configuring the Calculation Interval of the URPF Packet Loss Rate

Command	**ip verify urpf drop-rate compute interval** *seconds*
Parameter Description	**interval *seconds***: Indicates the calculation interva The unit is second. The value ranges from 30 to 300. The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	The calculation interval of the URPF packet loss rate is configured in global configuration mode. T configuration is applied to the global and interface-based calculation of the URPF packet loss rate, and takes effect on both IPv4 URPF and IPv6 URPF.

↘ Configuring the Alarm Interval of the URPF Packet Loss Rate

Command	**ip verify urpf drop-rate notify hold-down** *seconds*
Parameter Description	**hold-down *seconds***: Indicates the alarm interval of the URPF packet loss rate.The unit is second. The value ranges from 30 to 300. The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	The alarm interval of the URPF packet loss rate is configured in global config configuration is applied to the global and interface-based alarms of the URPF packet loss rate, and takes effect on both IPv4 URPF and IPv6 URPF.

Configuring the Function of Monitoring the IPv4 URPF Packet Loss Information

Command	**ip verify urpf drop-rate notify**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	After the function of monitoring the URPF packet loss information is enabled, the device can proactively send syslogs or trap messages to notify users of the packet loss information detected in the URPF check so that users can monitor the network status conveniently.

Configuring the Threshold of the IPv4 URPF Packet Loss Rate

Command	**ip verify urpf notification threshold** *rate-value*
Parameter Description	**threshold*rate-value*** Indicates the threshold of the URPF packet loss rate. The unit is pps. The value ranges from 0 to 4,294,967,295. The default value is 1,000 pps.
Command Mode	Interface configuration mode
Usage Guide	If the threshold is 0, a notification is sent for every packet that is dropped because it fails in the URPF check. You can adjust the threshold based on the actual situation of the network.

Configuration Example

Setting the Calculation Interval of the URPF Packet Loss Rate to 120s

Configuration Steps	Set the calculation interval of the URPF packet loss rate to 120s in global configuration m configuration takes effect on both IPv4 URPF and IPv6 URPF.

	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)# ip verify urpf drop-rate compute interval 120`
	`Orion_B54Q(config)# end`

Verification	Run the **show ip urpf** command to check whether the configuration takes effect.

	`Orion_B54Q# show ip urpf`
	`IP verify URPF drop-rate compute interval is 120s`

Setting the Alarm Interval of the URPF Packet Loss Rate to 120s

Configuration Steps	Set the alarm interval of the URPF packet loss rate to 120s in global con configuration takes effect on both IPv4 URPF and IPv6 URPF.

	`Orion_B54Q#configure terminal`
	`Orion_B54Q(config)# ip verify urpf drop-rate notify hold-down 120`
	`Orion_B54Q(config)# end`

Verification	Run the **show ip urpf** command to check whether the configuration takes effect.
	`Orion_B54Q# show ip urpfIP verify URPF drop-rate notify hold-down is 120s`

11.5 Monitoring

Clearing

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

Description	Command
Clears statistics of the number of packets dropped during the IPv4 URPF check.	**clear ip urpf** [**interface** *interface-name*]

Displaying

Description	Command
Displays the IPv4 URPF configuration and statistics.	**show ip urpf** [**interface** *interface-name*]

12 Configuring CPP

12.1 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 a 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 packets.

CPP is enabled by default. It provides protection during the entire operation of switches.

12.2 Applications

Application	Description
Preventing Malicious Attacks	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.
Preventing CPU Bottlenecks	Even when no attacks exist, it would become a bottleneck for CPU to excessive normal traffic. CPP can limit the rate of packets being sent to the CPU to ensure normal operation of switches.

12.2.1 Preventing Malicious Attacks

Scenario

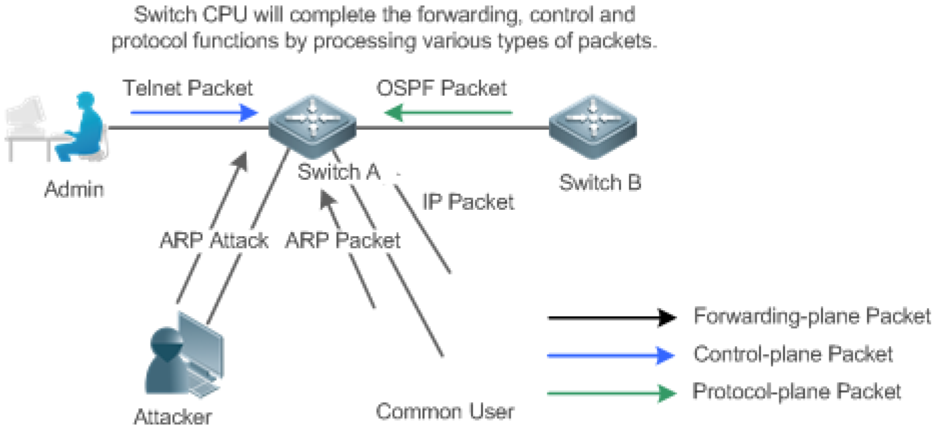
Network switches at all levels may be attacked by malicious packets, typically ARP attacks.

As shown in Figure 12-54, switch CPUs process three types of packets: forwarding-plane, control-plane and prot 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 pa packets serve for running protocols, including BPDU packets 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 b consume many CPU resources (for processing ARP attack packets). Consequently, the CPU fails to work normally. In the scenario as shown in Figure 12-54, possible consequences include: common users fail to acc

administrators fail to manage switches; the OSPF link between switch A and the neighbor B is disconnecte
learning fails.

Figure 12-54 Networking Topology of Switch Services and Attacks



Deployment

- By default, CPP classifies ARP packets, Telnet packets, IP route disconnection packets, and
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 di
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
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*.

12.2.2 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 an 802.1X authentication packets.

12.3 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 cla 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 li 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 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 que scheduled first. Scheduling refers to selecting packets from queues for output and refers to selecti packets to the CPU in this document.

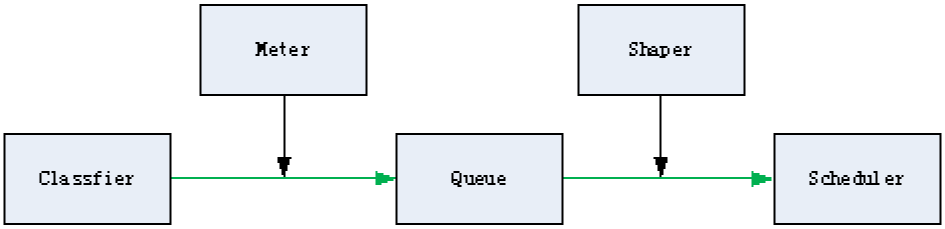
CPU interface

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 12-55 CPP Implementation Model



Feature	Description
Classfier	Classifies packet types and provides assurance for the subsequent impl policies.
Meter	Limits rates based on packet types and controls the bandwidth for a specific packet type.
Queue	Queue packets to be sent to the CPU and select different queues based on packet types.
Scheduler	Selects and schedules queues to be sent to the CPU.
Shaper	Performs rate limit and bandwidth control on priority queues and the CPU interface.

12.3.1 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 c packet types based on the protocols supported by the switch, for example, STP BPDU packets and ICMP packets. Packet types cannot be customized.

12.3.2 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.

12.3.3 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.

12.3.4 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.

12.3.5 Shaper

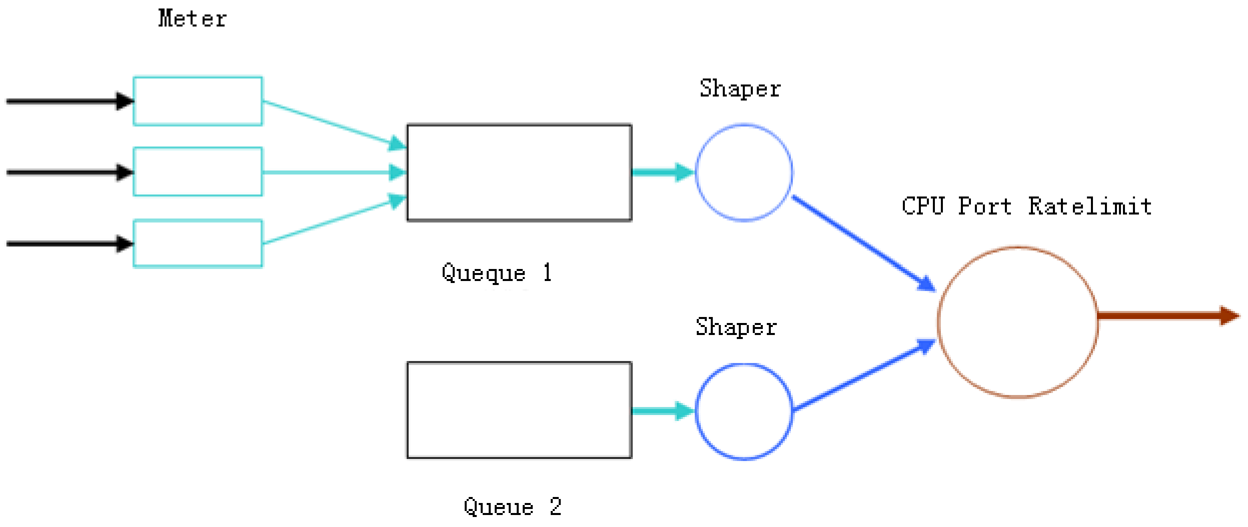
Working Principle

The Shaper is used to shape packets to be sent to the CPU, that is, when the actual rate of packets is greater tha 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 schedule 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 12-56 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 t interface.

12.4 Configuration

Configuration	Description and Command	
Configuring CPP	⚠ (Optional and configured by default) It is used to adjust the configuration parameters of CPP.	
	cpu-protect type *packet-type* **bandwidth**	Configures the Meter for a packet type.

Configuration	Description and Command	
	cpu-protect type *packet-type* **traffic-class**	Configures the priority queue for a packet type.
	cpu-protect traffic-class *traffic-class-num* **bandwidth**	Configures the Shaper for a priority queue.
	cpu-protect cpu bandwidth	Configures the Shaper fo interface.

12.4.1 Configuring CPP

Configuration Effect

- By configuring the Meter function, you can set the 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 protect 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 typ 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 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 t 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 moc 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

Command	**cpu-protect type** *packet-type* **bandwidth** *bandwidth_value*
Parameter Description	*packet-type*: Specifies a packet type. Packet types are defined. *bandwidth_value***:** Sets the bandwidth, in the unit of packets per second (pps).
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the priority queue for a packet type

Command	**cpu-protect type** *packet-type* **traffic-class** *traffic-class-num*
Parameter Description	*packet-type*: Specifies a packet type. Packet types are defined. *traffic-class-num***:** Specifies a priority queue.
Command Mode	Global configuration mode

Usage Guide	N/A

↘ Configuring the Shaper for a priority queue

Command	**cpu-protect traffic-class** *traffic-class-num* **bandwidth** *bandwidth_value*
Parameter Description	*traffic-class-num***:** Specifies a priority queue. *bandwidth_value***:** Sets the bandwidth, in the unit of pps.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the Shaper for a CPU interface

Command	**cpu-protect cpu bandwidth** *bandwidth_value*
Parameter Description	*bandwidth_value***:** Sets the bandwidth, in the unit of pps.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Preventing packet attacks and network flapping by using CPP

Scenario	● 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. ● 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.
Configuration Steps	● Put ARP attack packets in priority queue 1 and limit the bandwidth for ARP corresponding priority queue. ● Put OSPF packets in priority queue 5. ● Put IP Ping failure attack packets in priority queue 3 and limit the bandwidth for IP packets or the corresponding priority queue.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# cpu-protect type arp traffic-class 1`
	`Orion_B54Q(config)# cpu-protect type arp bandwidth 5000`
	`Orion_B54Q(config)# cpu-protect type ospf traffic-class 5`
	`Orion_B54Q(config)# cpu-protect type v4uc-route traffic-class 3`

```
Orion_B54Q(config)# cpu-protect type traffic-class 3 bandwidth 5000

Orion_B54Q(config)# end
```

Verification	Run the **show cpu-protect** command to view the configuration and statistics.

```
Orion_B54Q# show cpu-protect

%cpu port bandwidth: 80000(pps)

Traffic-class   Bandwidth(pps)  Rate(pps)       Drop(pps)

-------------   --------------  ---------       ---------

 0              8000            0               0

 1              8000            0               0

 2              8000            0               0

 3              8000            0               0

 4              8000            0               0

 5              8000            0               0

 6              8000            0               0

 7              8000            0               0

Packet Type          Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total     Total
Drop

- - - - - - - - - - - - - - - - - - -    - - - - - - - - - - - - - -    - - - - - - - - - - - - - - -    -
----------

bpdu                    6              128            0          0          0          0

arp                     3              10000          0          0          0          0

arp-dai                 3              10000          0          0          0          0

arp-proxy               3              10000          0          0          0          0

tpp                     7              128            0          0          0          0

dot1x                   4              128            0          0          0          0

gvrp                    5              128            0          0          0          0

rldp                    6              128            0          0          0          0

lacp                    6              128            0          0          0          0

rerp                    6              128            0          0          0          0

reup                    6              128            0          0          0          0

lldp                    5              128            0          0          0          0
```

```
cdp                  5               128            0          0          0         0
dhcps                4               128            0          0          0         0
dhcps6               4               128            0          0          0         0
dhcp6-client         4               128            0          0          0         0
dhcp6-server         4               128            0          0          0         0
dhcp-relay-c         4               128            0          0          0         0
dhcp-relay-s         4               128            0          0          0         0
option82             4               128            0          0          0         0
tunnel-bpdu          5               128            0          0          0         0
tunnel-gvrp          5               128            0          0          0         0
unknown-v6mc         3               128            0          0          0         0
known-v6mc           3               128            0          0          0         0
xgv6-ipmc            3               128            0          0          0         0
stargv6-ipmc         3               128            0          0          0         0
unknown-v4mc         3               128            0          0          0         0
known-v4mc           3               128            0          0          0         0
xgv-ipmc             3               128            0          0          0         0
sgv-ipmc             3               128            0          0          0         0
udp-helper           4               128            0          0          0         0
dvmrp                5               128            0          0          0         0
igmp                 4               128            0          0          0         0
icmp                 4               128            0          0          0         0
ospf                 5               128            0          0          0         0
ospf3                5               128            0          0          0         0
pim                  6               128            0          0          0         0
pimv6                6               128            0          0          0         0
rip                  6               128            0          0          0         0
ripng                6               128            0          0          0         0
vrrp                 6               128            0          0          0         0
vrrp6                6               128            0          0          0         0
ttl0                 6               128            0          0          0         0
```

```
ttl1               6        128      0     0     0     0
err_hop_limit      1        800      0     0     0     0
local-ipv4         6        128      0     0     0     0
local-ipv6         6        128      0     0     0     0
route-host-v4      0        4096     0     0     0     0
route-host-v6      0        4096     0     0     0     0
mld                0        1000     0     0     0     0
nd-snp-ns-na       6        128      0     0     0     0
nd-snp-rs          6        128      0     0     0     0
nd-snp-ra-redirect 6        128      0     0     0     0
nd-non-snp         6        128      0     0     0     0
erps               4        128      0     0     0     0
mpls-ttl0          6        128      0     0     0     0
mpls-ttl1          6        128      0     0     0     0
mpls-ctrl          6        128      0     0     0     0
isis               5        2000     0     0     0     0
bgp                1        128      0     0     0     0
cfm                0        128      0     0     0     0
fcoe-fip           6        128      0     0     0     0
fcoe-local         6        128      0     0     0     0
bfd-echo           6        5120     0     0     0     0
bfd-ctrl           6        5120     0     0     0     0
madp               7        1000     0     0     0     0
ip4-other          6        128      0     0     0     0
ip6-other          6        128      0     0     0     0
non-ip-other       6        20000    0     0     0     0
trill              2        1000     0     0     0     0
trill-oam          2        1000     0     0     0     0
efm                2        1000     0     0     0     0
```

12.5 Monitoring

Clearing

Description	Command
Clears the CPP statistics.	**clear cpu-protect counters** [**device** *device_num*]
Clears the CPP statistics on the master device.	**clear cpu-protect counters mboard**

Displaying

Description	Command
Displays the configuration and statistics of a packet type.	**show cpu-protect type** *packet-type* [**device** *device_num*]
Displays the configuration and statistics of a priority queue.	**show cpu-protect traffic-class** *traffic-class-num* [**device** *device_num*]
Displays the configuration on a CPU interface.	**show cpu-protect cpu**
Displays all configurations and statistics on the master device.	**show cpu-protect** {**mboard** | **summary**}
Displays all configurations and statistics of CPP.	**show cpu-protect** [**device** *device_num*]

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** value is 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.
- 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.

13 Configuring DHCP Snooping

13.1 Overview

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record an 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

13.2 Applications

Application	Description
Guarding against DHCP service spoofing	In a network with multiple DHCP servers, DHCP clients are allowed t network configurations only from legal DHCP servers.
Guarding against DHCP packet flooding	Malicious network users may frequently send DHCP request packets.
Guarding against forged DHCP packets	Malicious network users may send forged DHCP request packets, for examp DHCP-RELEASE packets.
Guarding against IP/MAC spoofing	Malicious network users may send forged IP packets, for exampl source address fields of packets.
Preventing Lease of IP Addresses	Network users may lease IP addresses rather than obtaining them from a DHCP server.
Detecting ARP attack	Malicious users forge ARP response packets to intercept packets during norma users' communication.

13.2.1 Guarding Against DHCP Service Spoofing

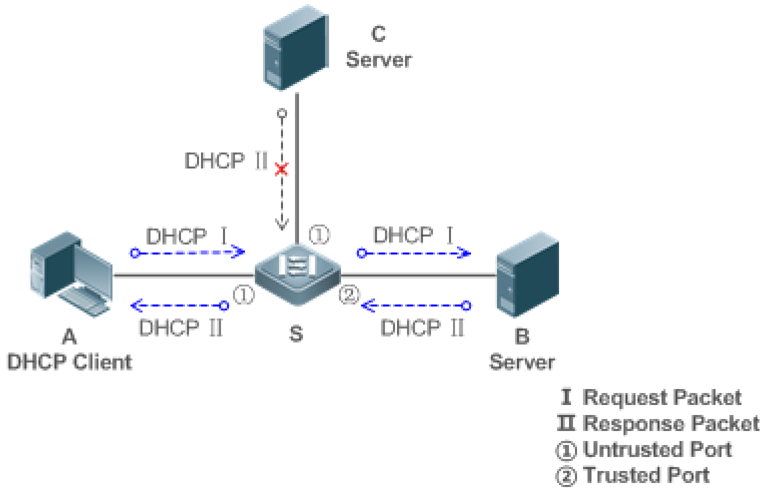
Scenario

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 13-15



Remarks:	S is an access device. A is a user PC. B is a DHCP server within the controlled area. C is a DHCP server out of the controlled area.

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.

13.2.2 **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.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Limit the rates of DHCP packets from the untrusted ports.

13.2.3 **Guarding Against Forged DHCP Packets**

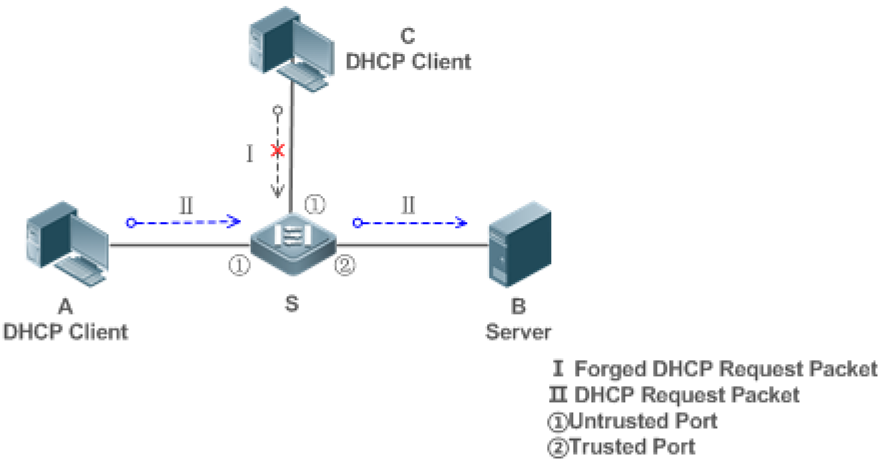
Scenario

Potential malicious clients in a network may forge DHCP request packets, consuming applicable IP addres servers and probably preempting legal users' IP addresses. Therefore, it is 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 database.

Figure 13-16



Remarks:	S is an access device. A and C are user PCs. 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.

13.2.4 Guarding Against IP/MAC Spoofing

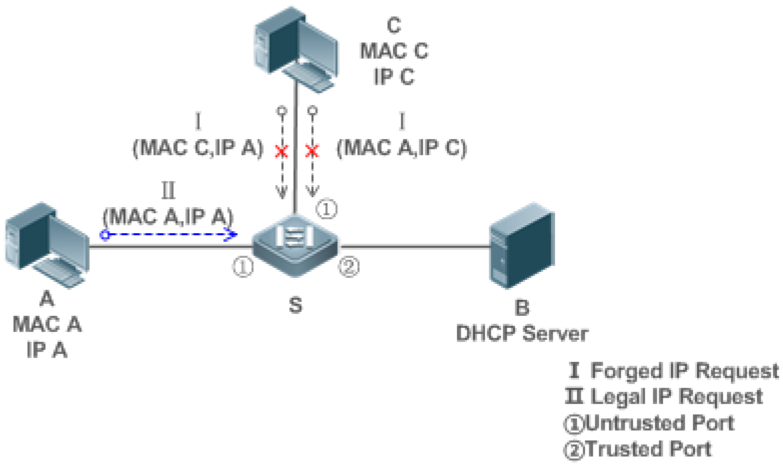
Scenario

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 13-17



Remarks:	S is an access device. A and C are user PCs. 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.

13.2.5 Preventing Lease of IP Addresses

Scenario

Validate the source addresses of IP packets addresses.

If the source addresses, connected ports, and layer-2 source MAC addresses of ports in IP packets do 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".

13.2.6 **Detecting ARP Attacks**

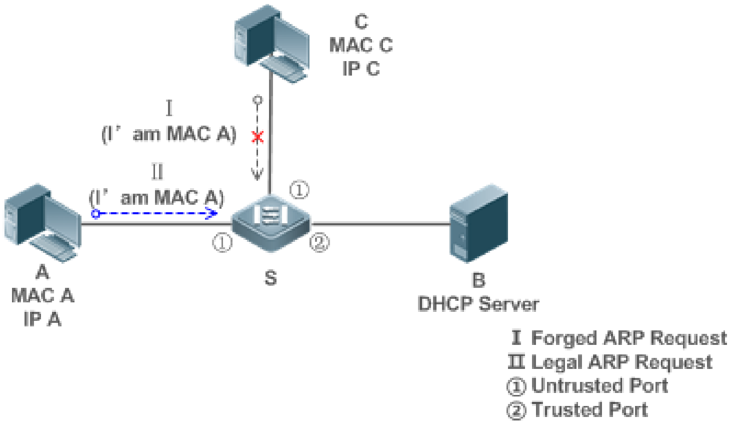
Scenario

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 13-18



Remarks:	S is an access device. A and C are user PCs. 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.

13.3 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 Snoopi 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 wa 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 onl maintenance but also the possibility that legal clients with IP addresses assigned by the DHCP server may fail to use t network normally due to address conflict. Through snooping packets between clients 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 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 Foundatio 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 addi 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 Sno (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 add **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
Filtering DHCP packets	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.
Building the DHCP Snooping database	Snoop the interaction between DHCP clients and the server, and generate the DHCP Snooping binding database to provide basis for other filtering modules.

13.3.1 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 filter 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 t 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 i **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.

13.3.2 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 a 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.

13. 4 Configuration

Configuration	Description and Command	
Configuring basic functions of DHCP Snooping	⚠ (Mandatory) It is used to enable DHCP Snooping.	
	ip dhcp snooping	Enables DHCP Snooping.
	ip dhcp snooping suppression	Enables DHCP suppression.
	ip dhcp snooping vlan	Enables VLAN-based DHCP Snooping.
	ip dhcp snooping verify mac-address	Configures DHCP Snooping source MAC verification.
	ip dhcp snooping database write-delay	Writes the DHCP Snoo database to Flash periodically.
	ip dhcp snooping database write-to-flash	Writes the DHCP Snoo database to Flash manually.
	renew ip dhcp snooping database	Imports Flash storage to Snooping Binding database.
	ip dhcp snooping trust	Configures DHCP S ports.
	ip dhcp snooping bootp	Enables BOOTP support.
Configuring Option82	⚠ (Optional)It is used to optimize the address assignment by DHCP servers.	
	ip dhcp snooping Information option	Adds Option82 functions to DHCP request packets.
	ip dhcp snooping information option format remote-id	Configures the **remote-id** Option82 as a user-define string.
	ip dhcp snooping vlan information option format-type circuit-id string	Configures the **circuit-id** Option82 as a user-define string.

13.4.1 **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 enca 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 b 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.

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

Command	[**no**] **ip dhcp snooping**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After global DHCP Snooping is enabled, you can check DHCP Snooping using the **show ip dhcp snooping** command.

Configuring VLAN-based DHCP Snooping

Command	[**no**] **ip dhcp snooping vlan** { *vlan-rng* | {*vlan-min* [*vlan-max*] } }
Parameter Description	*vlan-rng*: Indicates the range of VLANs *vlan-min*: The minimum VLAN ID *vlan-max*: The maximum VLAN ID
Command Mode	Global configuration mode
Usage Guide	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

Command	[**no**] **ip dhcp snooping suppression**
Parameter Description	**N/A**
Command Mode	Interface configuration mode
Usage Guide	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

Command	[**no**] **ip dhcp snooping verify mac-address**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	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

Command	[**no**] **ip dhcp snooping database write-delay** [*time*]
Parameter Description	*time*Indicates the interval between two times of writing the DHCP Sn Flash.
Command Mode	Global configuration mode
Usage Guide	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 restarts.

Writing the DHCP Snooping Database to Flash Manually

Command	**ip dhcp snooping database write-to-flash**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	Use this command to write the dynamic user information in the DHCP Snooping database in FLA documents in real time. If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), bindi cannot be restored from FLASH documents because of version differences between FLASH documents.

Importing Flash Storage to the DHCP Snooping Binding Database

Command	**renew ip dhcp snooping database**
Parameter Description	**N/A**
Command Mode	Privileged configuration mode
Usage Guide	Use this command to import the information from Flash documents to the DHCP Snoopi database.

Configuring DHCP Snooping Trusted Ports

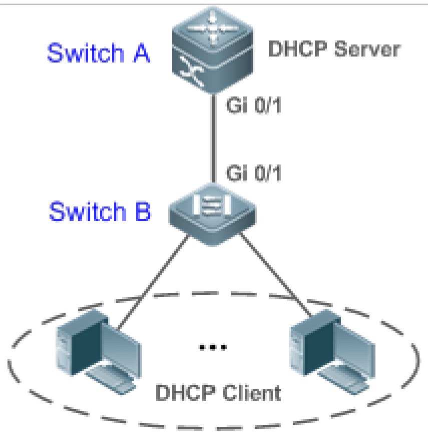
Command	**[no] ip dhcp snooping trust**
Parameter Description	**N/A**
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure a port connected to a legal DHCP server as a trusted port. The DHCP response packets received by trusted ports are transferred, while those received by untrusted ports are discarded.

↘ Enabling or Disabling BOOTP Support

Command	**[no] ip dhcp snooping bootp**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	Use this command to support the BOOPT protocol.

Configuration Example

↘ DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

Scenario Figure 13-19	 Switch A DHCP Server Gi 0/1 Gi 0/1 Switch B ... DHCP Client
Configuration Steps	● Enable DHCP Snooping on an access device (Switch B in this case). ● Configure the uplink port (port Gi 0/1 in this case) as a trusted port.

B	`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
Verification	Check the configuration on Switch B. ● Check whether DHCP Snooping is enabled, and whether the configured DHCP Snooping trusted port is uplink. ● Check the DHCP Snooping configuration on Switch B, and especially whether the trusted port is correct.
B	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 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 tru configured.

13.4.2 **Configuring Option82**

Configuration Effect

- Enable a DHCP server to obtain more information and assign addresses better.
- The Option82 function is client-oblivious.

Notes

- The Opion82 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

Command	[**no**] **ip dhcp snooping information option** [**standard-format**]
Parameter Description	**standard-format**: Indicates a standard format of the Option82 options
Command Mode	Global configuration mode
Usage Guide	Use this command to add Option82 to DHCP request packets so that a DHCP server assigns addresses according to such information.

↘ Configuring Sub-option remote-id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping information option format remote-id** { **string** *ASCII-string* | **hostname** }
Parameter Description	**string** *ASCII-string*: indicates the content of the extensibl **remote-id**, is a user-defined character string **hostname**: indicates the content of the extensible format, the **Option82** **remote-id** is a host name.
Configuration mode	Global configuration mode
Usage Guide	Use this command to configure the sub-option **remote-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses information.

↘ Configuring Sub-Option circuit -id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*
Parameter Description	*vlan-id*: Indicates the VLAN where a DHCP request packet is *ascii-string*: Indicates the user-defined string
Configuration mode	Interface configuration mode
Usage Guide	Use this command to configure the sub-option**circuit-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses information.

Configuration Example

↘ Configuring Option82 to DHCP Request Packets

<table>
<tr><td><b>Configuration Steps</b></td><td>● Configuring basic functions of DHCP Snooping.
● Configuring Option82.</td></tr>
<tr><td><b>B</b></td><td><pre>
Orion_B54Q# configure terminal

Orion_B54Q(config)# ip dhcp snooping information option

Orion_B54Q(config)# end
</pre></td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Verification</b></td><td>Check the DHCP Snooping configuration.</td></tr>
<tr><td><b>B</b></td><td><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></td></tr>
</table>

Common Errors

- N/A

13.5 Monitoring

Clearing

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

Description	Command
Clears the DHCP Snooping binding database.	**clear ip dhcp snooping binding** [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id*]

Displaying

Description	Command
Displays DHCP Snooping configuration.	**show ip dhcp snooping**
Displays the DHCP Snooping binding database.	**show ip dhcp snooping binding**

Debugging

⚠ System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

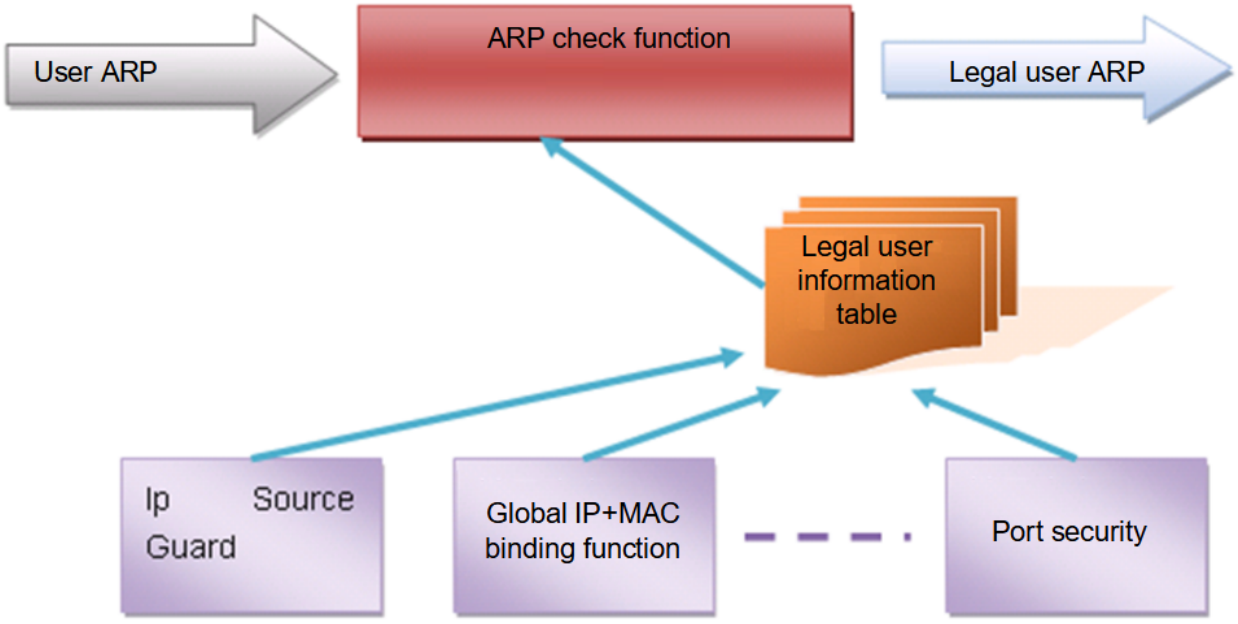
Description	Command
Debugs DHCP Snooping events.	**debug snooping ipv4 event**
Disables debugging DHCP Snooping events.	**no debug snooping ipv4 event**
Debugs DHCP Snooping packets.	**debug snooping ipv4 packet**
Disables debugging DHCP Snooping packets.	**no debug snooping ipv4 packet**

14 Configuring ARP Check

14.1 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, as well as WLAN interfaces) and disc 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+M authentication, GSN binding, Web authentication and port security.

Figure 14-20



The above figure shows that security modules generate legal user information (IP-based or IP-MAC based). ARF 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

14.2 Applications

Application	Description
Filtering ARP packets in Networks	Illegal users in networks launch attacks using forged ARP packets.

14.2.1 Filtering ARP Packets in Networks

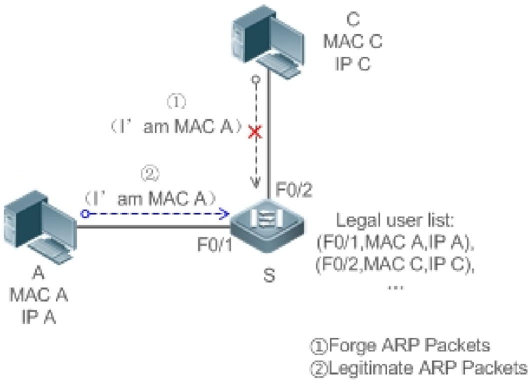
Scenario

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 14-21



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.

14.3 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 basedP-MAC based mode: port security, global IP+MAC binding, 802.1X authorization, IP Source Guar GSN binding, and Web authentication.

↘ Two Modes of APR Check

The ARP Check has two modes: Enabled and Disabled. The default is Enabled.

1. Enabled Mode

Through ARP Check, ARP packets are detected based on the IP/IP-MAC based binding informa 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 a 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.

2. Disabled Mode

ARP packets on a port are not checked.

Overview

Feature	Description
Filtering ARP Packets	Check the source IP and source MAC addresses of ARP packets to filter out illegal ARP packets.

14.3.1 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 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.

14.4 Configuration

Configuration	Description and Command	
Configuring ARP Check	⚠ (Mandatory) It is used to enable APR Check.	
	arp-check	Enables ARP Check.

14.4.1 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, as well as WLAN interfaces. Enable ARP check for the wired in interface configuration mode, while for the wireles security configuration mode.

Configuration Steps

Enabling ARP Check

- (Mandatory) The function is disabled by default. To use the ARP Check function, an administrator ne 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

Command	**arp-check**
Parameter Description	N/A
Command	Interface configuration mode, or WLAN security configuration mode
Usage Guide	Generate ARP filtration information according to the legal user information 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

Configuration Steps	● Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003`
	`Orion_B54Q(config)#address-bind install`
	`Orion_B54Q(config)#ip source binding 00D`
	`gigabitEthernet 0/1`
	`Orion_B54Q(config)# interface GigabitEthernet 0/1`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur`
	`vlan 1 192.168.1.1`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#exit`
	`Orion_B54Q(config)#interface gigabitEthernet 0/4`
	`Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security`
	`Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5`
	`Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check`
	`Orion_B54Q(config-if-GigabitEthernet 0/4)#exit`
	`Orion_B54Q(config)#interface gigabitEthernet 0/5`
	`Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check`
	`Orion_B54Q(config-if-GigabitEthernet 0/5)#end`
	`Orion_B54Q# configure terminal`
	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)#wlansec 1`
	`Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1`
	`Orion_B54Q(config-wlansec)#arp-check`
	`Orion_B54Q(config-wlansec)#end`

Verification	Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.
	`Orion_B54Q# show interface arp-check list`

Configuration Steps	● Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

```
Orion_B54Q# configure terminal

Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003

Orion_B54Q(config)#address-bind install

Orion_B54Q(config)#ip source binding 00D
gigabitEthernet 0/1

Orion_B54Q(config)# interface GigabitEthernet 0/1

Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check

Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security

Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security

Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur
vlan 1 192.168.1.1

Orion_B54Q(config-if-GigabitEthernet 0/1)#exit

Orion_B54Q(config)#interface gigabitEthernet 0/4

Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security

Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5

Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check

Orion_B54Q(config-if-GigabitEthernet 0/4)#exit

Orion_B54Q(config)#interface gigabitEthernet 0/5

Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check

Orion_B54Q(config-if-GigabitEthernet 0/5)#end

Orion_B54Q# configure terminal

Orion_B54Q# configure terminal

Orion_B54Q(config)#wlansec 1

Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1

Orion_B54Q(config-wlansec)#arp-check

Orion_B54Q(config-wlansec)#end
```

Verification	Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.

```
INTERFACE                SENDER MAC          SENDER IP           POLICY SOURCE

------------------------ -------------------- -------------------- --------------------
```

Configuration Steps	● Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003
Orion_B54Q(config)#address-bind install
Orion_B54Q(config)#ip source binding 00D
gigabitEthernet 0/1
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur
vlan 1 192.168.1.1
Orion_B54Q(config-if-GigabitEthernet 0/1)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/4
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5
Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/4)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/5
Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/5)#end
Orion_B54Q# configure terminal
Orion_B54Q# configure terminal
Orion_B54Q(config)#wlansec 1
Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1
Orion_B54Q(config-wlansec)#arp-check
Orion_B54Q(config-wlansec)#end
```

Verification	Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.

```
GigabitEthernet 0/1       00d0.f800.0003        192.168.1.3           address-bind
GigabitEthernet 0/1       00d0.f800.0001        192.168.1.1           port-security
```

Configuration Steps

- Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003
Orion_B54Q(config)#address-bind install
Orion_B54Q(config)#ip source binding 00D
gigabitEthernet 0/1
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur
vlan 1 192.168.1.1
Orion_B54Q(config-if-GigabitEthernet 0/1)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/4
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5
Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/4)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/5
Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/5)#end
Orion_B54Q# configure terminal
Orion_B54Q# configure terminal
Orion_B54Q(config)#wlansec 1
Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1
Orion_B54Q(config-wlansec)#arp-check
Orion_B54Q(config-wlansec)#end
```

Verification

Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.

```
GigabitEthernet 0/1     00d0.f800.0002      192.168.1.4         DHCP snooping
GigabitEthernet 0/4     00d0.f800.0003      192.168.1.3         address-bind
```

Configuration Steps

- Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003
Orion_B54Q(config)#address-bind install
Orion_B54Q(config)# ip source binding 00D
gigabitEthernet 0/1
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur
vlan 1 192.168.1.1
Orion_B54Q(config-if-GigabitEthernet 0/1)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/4
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5
Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/4)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/5
Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/5)#end
Orion_B54Q# configure terminal
Orion_B54Q# configure terminal
Orion_B54Q(config)#wlansec 1
Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1
Orion_B54Q(config-wlansec)#arp-check
Orion_B54Q(config-wlansec)#end
```

Verification

Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.

```
GigabitEthernet 0/4                          192.168.1.5          port-security
GigabitEthernet 0/5      00d0.f800.0003      192.168.1.3          address-bind
```

Configuration Steps

- Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003
Orion_B54Q(config)#address-bind install
Orion_B54Q(config)#ip source binding 00D
gigabitEthernet 0/1
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur
vlan 1 192.168.1.1
Orion_B54Q(config-if-GigabitEthernet 0/1)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/4
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5
Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/4)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/5
Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/5)#end
Orion_B54Q# configure terminal
Orion_B54Q# configure terminal
Orion_B54Q(config)#wlansec 1
Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1
Orion_B54Q(config-wlansec)#arp-check
Orion_B54Q(config-wlansec)#end
```

Verification

Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.

```
Orion_B54Q# show wlan arp-check list
```

Configuration Steps	● Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003`
	`Orion_B54Q(config)#address-bind install`
	`Orion_B54Q(config)#ip source binding 00D`
	`gigabitEthernet 0/1`
	`Orion_B54Q(config)# interface GigabitEthernet 0/1`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur`
	`vlan 1 192.168.1.1`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)#exit`
	`Orion_B54Q(config)#interface gigabitEthernet 0/4`
	`Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security`
	`Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5`
	`Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check`
	`Orion_B54Q(config-if-GigabitEthernet 0/4)#exit`
	`Orion_B54Q(config)#interface gigabitEthernet 0/5`
	`Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check`
	`Orion_B54Q(config-if-GigabitEthernet 0/5)#end`
	`Orion_B54Q# configure terminal`
	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)#wlansec 1`
	`Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1`
	`Orion_B54Q(config-wlansec)#arp-check`
	`Orion_B54Q(config-wlansec)#end`

Verification	Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.
	`INTERFACE                 SENDER MAC          SENDER IP           POLICY SOURCE`

Configuration Steps

- Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003
Orion_B54Q(config)#address-bind install
Orion_B54Q(config)#ip source binding 00D
gigabitEthernet 0/1
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur
vlan 1 192.168.1.1
Orion_B54Q(config-if-GigabitEthernet 0/1)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/4
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5
Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/4)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/5
Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/5)#end
Orion_B54Q# configure terminal
Orion_B54Q# configure terminal
Orion_B54Q(config)#wlansec 1
Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1
Orion_B54Q(config-wlansec)#arp-check
Orion_B54Q(config-wlansec)#end
```

Verification

Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.

```
------------------------ -------------------- -------------------- --------------------

WLAN 1                   0026.c79f.6e4c       172.168.131.1        DHCP snooping
```

Configuration Steps

- Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard security, or global IP+MAC binding.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)#address-bind 192.168.1.3 00D0.F800.0003
Orion_B54Q(config)#address-bind install
Orion_B54Q(config)#ip source binding 00D
gigabitEthernet 0/1
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/1)#ip verify source port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/1)#switchport port-secur
vlan 1 192.168.1.1
Orion_B54Q(config-if-GigabitEthernet 0/1)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/4
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security
Orion_B54Q(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5
Orion_B54Q(config-if-GigabitEthernet 0/4)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/4)#exit
Orion_B54Q(config)#interface gigabitEthernet 0/5
Orion_B54Q(config-if-GigabitEthernet 0/5)#arp-check
Orion_B54Q(config-if-GigabitEthernet 0/5)#end
Orion_B54Q# configure terminal
Orion_B54Q# configure terminal
Orion_B54Q(config)#wlansec 1
Orion_B54Q(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 interface wlan 1
Orion_B54Q(config-wlansec)#arp-check
Orion_B54Q(config-wlansec)#end
```

Verification

Use the **show interface arp-check list** command to display the effective ARP Check list for interfaces.

Common Errors

- If ARP packets at a port need to be checked but APR-Check is disabled, then APR-Check will not be effective.

14.5 Monitoring

Displaying

Description	Command
Displays the effective ARP Check list based on ports.	**show interface** [*interface-type interface-number*] **arp-checklist**
Displays the effective ARP Check list based on WLAN.	**show wlan** [*wlan-id*] **arp-checklist**

15 Configuring Dynamic ARP Inspection

15.1 Overview

Dynamic Address Resolution Protocol (ARP) inspection (DAI)
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 a Standards

- RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

15.2 Applications

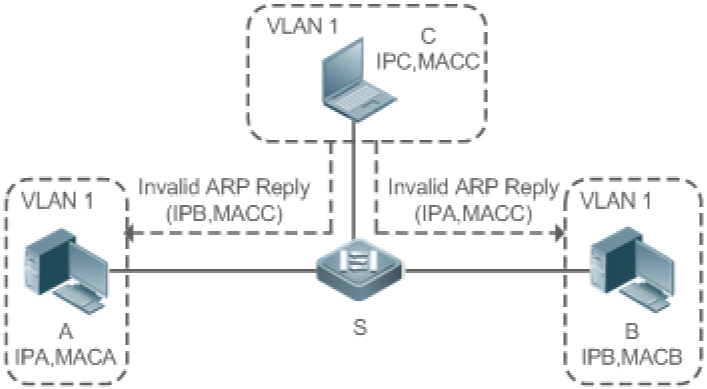
Application	Description
ARP Spoofing Prevention	Prevent ARP spoofing that is mounted by taking advantage of ARP defects.

15.2.1 ARP Spoofing Prevention

Scenario

Due to inherent defects, ARP does not check the validity of received ARP packets. Attackers can take advantag
defects to mount ARP spoofing. A typical example is man-in-the-middle (MITM) attack. See Figure 15 -57.

Figure 15-57



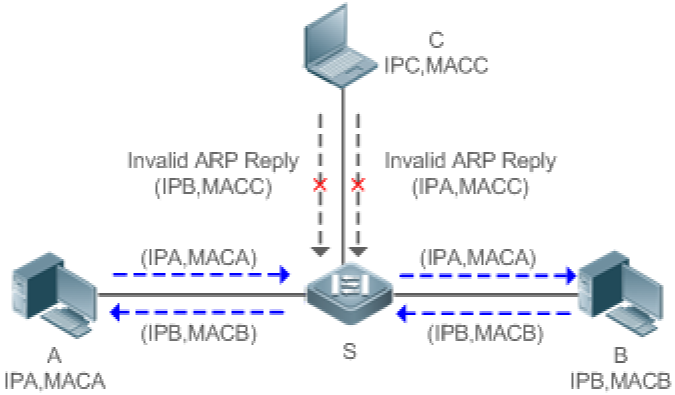
Remarks	Device S is a Orion_B54Q access switch enabled with DAI. User A and User B are connected to Device S, and they are in the same subnet. User C is a malicious user connected to Device S. IP A and MAC A are the IP address and MAC address of User A. IP B and MAC B are the IP address and MAC address of User B. IP C and MAC C are the IP address and MAC address of User C.

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 replyUpon 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 packet 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 15.1 Overview. Figure 15 -58 shows the working process of DAI.

Figure 15-58



Remarks	Device S is a Orion_B54Q access switch enabled with DAI. User A and User B are connected to Device S, and they are in the same subnet. User C is a malicious user connected to Device S. IP A and MAC A are the IP address and MAC address of User A. IP B and MAC B are the IP address and MAC address of User B. IP C and MAC C are the IP address and MAC address of User C.

The ARP packets of User A and User B are forwarded normally by Device S. The forged ARP packets of 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.

15.3 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

Invalid ARP Packet Filter	Checks the source IP addresses and MAC addresses of ARP packets to filter out invalid packets.
DAI Trusted Port	Permits the ARP packets received from specific ports to pass throug checking their validity.

15.3.1 **Invalid ARP Packet Filter**

Enable DAI in a specific VLAN to filter out invalid ARP packets. The DAI validity criteria are the same as thos Check.

Working Principle

Upon receiving an ARP packet, the device matches the IP address and MAC address of the packet with the 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 *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 va The ports with ARP Check effective still check the validity of received ARP packets.

15.3.2 **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.

15.4 Configuration

Configuration	Description and Command	
Configuring DAI	⚠ (Optional) It is used to enable ARP packet validity check.	
	ip arp inspection vlan	Enables DAI.
	ip arp inspection trust	Configures DAI trusted ports.

15.4.1 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_B54Q 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, th enabled with other security features and set to trusted state accordingly may filter out valid ARP packets due t absence of DAI user entries.
- Perform this configuration on Orion_B54Q 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

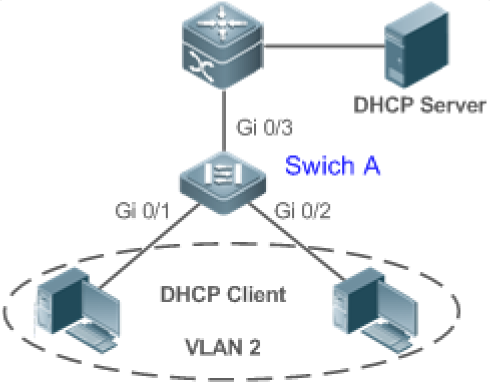
Command	**ip arp inspection vlan** { *vlan-id* | *word* }
Parameter Description	*vlan-id*: Indicates a VLAN ID. *word*: Indicates the VLAN range string, such as 1, 3–5, 7, and 9–11.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring DAI Trusted Ports

Command	**ip arp inspection trust**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	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

Scenario **Figure 15-59**	 DHCP Server Gi 0/3 Swich A Gi 0/1 Gi 0/2 DHCP Client VLAN 2

Configuration Steps	⚠ Enable DHCP Snooping on the access switch (Switch A) an (GigabitEthernet 0/3) connected to the valid DHCP server as a trusted port. ⚠ Enable IP Source Guard on Switch A. ⚠ Enable DAI.

Switch A	`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`
	`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`

Verification	● Check whether DHCP Snooping, IP Source Guard, and DAI are enabled and whether trusted ports are configured correctly. ● Check whether the uplink port on Switch A is a DHCP Snooping trusted port. ● Check whether DAI is enabled successfully in the VLAN and the uplink ports are DAI trusted ports.

Switch A	`A#show running-config`
	`A#show ip dhcp snooping`
	`A#show ip arp inspection vlan`

Common Errors

- A port with security control enabled is configured as a DAI trusted port.

15.5 Monitoring

Displaying

Description	Command
Displays the DAI state of a specific VLAN.	**show ip arp inspection vlan** [*vlan-id* | *word*]
Displays the DAI configuration state of each Layer-2 port.	**show ip arp inspection interface**

16 Configuring IP Source Guard

16.1 Overview

The IP Source Guard function realizes hardware-based IP packet filtering to ensure that only the users having information in the binding database can access networks normally, preventing users from forging IP packets.

16.2 Applications

Application	Description
Guarding Against IP/MAC Spoofing Attack	In network environments, users are not allowed to launch attacks by setting IP addresses or forging IP packets.

16.2.1 Guarding Against IP/MAC Spoofing Attack

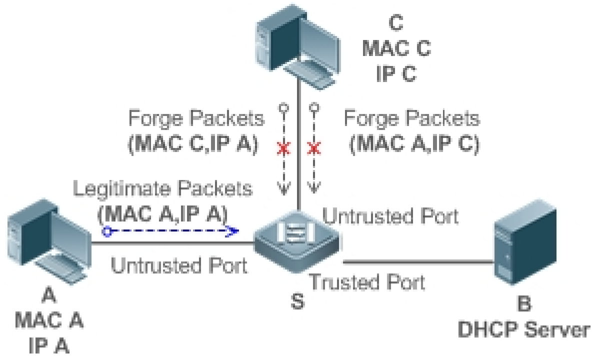
Scenario

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 16-22



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.

16.3 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 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 speci excluded VLANs, within which IP packets are not checked and filtered, which means that suchIP packets are not controlled by IP Source Guard. At most 32 excluded VLANs can be specified for a port.

Overview

Feature	Description
Checking Source Address Fields of Packets	Filter the IP packets passing through ports by IP-based or IP-MAC based filtering.

16.3.1 **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 enab DHCP Snooping can be enabled at any time on Orion_B54Q devices, either before or after IP 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.

16.4 Configuration

Configuration	Description and Command	
Configuring IP Source Guard	(Mandatory) It is used to enable IP Source Guard.	
	ip verify source	Enables IP Source Guard on a port.
	ip source binding	Configures a static binding.
	Ip verify source exclude-vlan	Specifies an excluded VLAN for IP Source Guard.

16.4.1 Configuring IP Source Guard

Configuration Effect

- Check input IP packets to filter out invalid IP packets.

Notes

- The enabling of IP Source Guard may affect forwarding of IP packets. In general, this function needs to be us combination with DHCP Snooping.
- IP Source Guard cannot be configured on DHCP Snooping trusted ports.
- IP Source Guard cannot be configured on global IP+MAC exclude ports.
- IP Source Guard can be configured only on wired exchange ports, Layer-2 AP ports, and Laye subinterfaces. The function is configured in interface configuration mode in the case of wired access.

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

Command	**ip verify source** [**port-security**]
Parameter Description	**port-security**: Enable IP-MAC based filtering.

Command	Interface configuration mode
Usage Guide	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

Command	**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **{ interface** *interface-id* **| ip-mac | ip-only }**
Parameter Description	**mac-address:** The MAC address of a static binding **Vlan-id:** The VLAN ID of a static binding. **ip-address:** The IP address of a static binding *interface-id*: The Port ID (PID) of a static binding **ip-mac:** IP-MAC based mode **ip-only:** IP-based mode
Configuration Mode	Global configuration mode
Usage Guide	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

Command	**ip verify source exclude-vlan** *vlan-id*
Parameter Description	**vlan-id:** A VLAN ID exempted from IP Source Guard on a port
Command	Interface configuration mode
Usage Guide	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

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.

	`Orion_B54Q(config)# interface GigabitEthernet 0/1`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)# ip verify source`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)# end`

Verification	Displays the address filtering table of IP Source Guard.
	`Orion_B54Q# show ip verify source`

Configuring a Static Binding

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard. ● Configure a static binding.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# ip source binding 00d0.f801.010`
	`GigabitEthernet 0/3`
	`Orion_B54Q(config)# end`

Verification	Display the address filtering table of IP Source Guard.

	`Orion_B54Q# show ip verify source`
	`NO.   INTERFACE              FilterType FilterStatus          IPADDRESS       MACADDRESS`
	`VLAN TYPE`
	`----- ------------------------------ --`
	`-------------- ---- -------------`
	`1     GigabitEthernet 0/3     UNSET     Inactive-restrict-off   1`
	`00d0.f801.0101 1    Static`
	`2     GigabitEthernet 0/1      IP-ONLY    Active                Deny-All`

Specifying an Excluded VLAN

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.

	`Orion_B54Q(config)# interface GigabitEthernet 0/1`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)# ip verify source`
	`Orion_B54Q(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1`
	`Orion_B54Q(config-if)# end`

Verification	Display the configuration of excluded VLANs specified on a port.
	`Orion_B54Q# show run`

Common Errors

- Enable IP Source Guard on a trusted port under DHCP Snooping.
- Specify an excluded VLAN before IP Source Guard is enabled.

16.5 Monitoring

Displaying

Description	Command
Displays the address filtering table of IP Source Guard.	**show ip verify source** [**interface** *interface-id*]
Displays the address binding database of IP Source Guard.	**show ip source binding**

17 Configuring Gateway-targeted ARP Spoofing Prevention

17.1 Overview

Gateway-targeted Address Resolution Protocol (ARP) spoofing prevention effectively p spoofing by checking on the logical port whether the source IP addresses of ARP packets (Sender IP fields of ARP packets) are the self-configured gateway IP addresses.

Protocols and Standards

RFC 826: Ethernet Address Resolution Protocol

17.2 Applications

Application	Description
Typical Application of Gateway-targeted ARP Spoofing Prevention	Blocks ARP spoofing packets with forged gateway address and intranet server IP addresses to ensure that users can access the Internet.

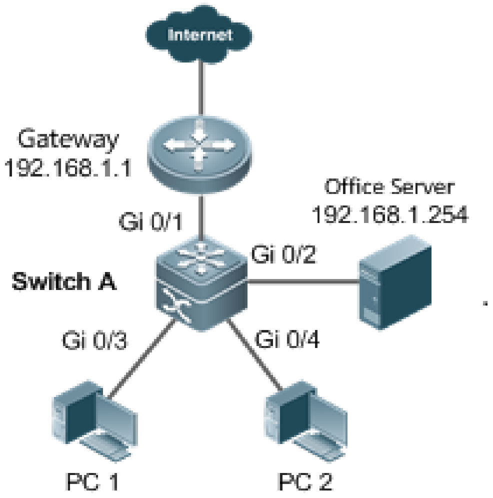
17.2.1 Typical Application of Gateway-targeted ARP Spoofing Prevention

Scenario

PC users access the office server through the access device Switch A, and connect to external netw gateway.

- If any users legally use forged gateway IP addresses or server IP addresses to perform ARP spoofing, the other users cannot access the Internet and the server.
- The ARP spoofing packets with forged gateway address and intranet server IP addresses must be blocked to ensure that users can access the Internet.

Figure 17-60 Typical Topology of Gateway-targeted ARP Spoofing Prevention



eployment

- On the access switch (Switch A), enable gateway-targeted spoofing prevention on the ports (Gi 0/3 and Gi 0/4 in this case) directly connected to the PC. The gateway addresses include intranet gateway address and address.

17.3 Features

Basic Concepts

ARP

ARP is a TCP/IP protocol that obtains physical addresses according to IP add The host broadcasts ARP requests to all hosts on the network and receives the returned packets to determin addresses of the target IP addresses, and saves the IP addresses and hardware addresses in the local ARP cache, which can be directly queried in response to future requestsOn the same network, all the hosts using the ARP are considered as mutually trustful to each other. Each host on the network can independently send ARP response packets; the other hos receive the response packets and record them in the local ARP cache without detecting their authenti attackers can send forged ARP response packets to target hosts so that the messages sent from these hosts cannot reach the proper host or reach a wrong host, thereby causing ARP spoofing.

Gateway-targeted ARP Spoofing

When User A sends an ARP packet requesting the media access control (MAC) address of a gateway, User B on the same VLAN also receives this packet, and User B can send an ARP response packet, passing off the gateway IP address as the source IP address of the packet, and User B's MAC address as the source MAC address. This is called gateway-targeted

ARP spoofing. After receiving the ARP response, User A regards User B's machine as the gateway, so all the packets sent from User A to the gateway during communication will be sent to User B. In this way, User A's c intercepted, thereby causing ARP spoofing.

Overview

Feature	Description
Gateway-targeted ARP Spoofing Prevention	Blocks ARP spoofing packets with forged gateway address and intranet server IP addresses to ensure that users can access the Internet

17.3.1 Gateway-targeted ARP Spoofing Prevention

Working Principle

↘ Gateway-targeted Spoofing Prevention

Gateway-targeted ARP spoofing prevention effectively prevents ARP spoofing aimed at gateways by checking on the logical port whether the source IP addresses of ARP packets are the self-configured gateway IP addresses. If an ARP packet uses the gateway address as the source IP address, the packet will be discarded to prevent users from receiving wro response packets. If not, the packet will not be handled. In this way, only the devices connected to the switch can send ARP packets, and the ARP response packets sent from the other PCs which pass for the gateway are filtered by the switch.

Related Configuration

↘ Configuring Gateway-targeted Spoofing Prevention Addresses

- By default, no gateway-targeted ARP spoofing prevention address is configured.
- Run the **anti-arp-spoofing ip** command to configure the gateway-targeted ARP spoofing prevention addresses.

17.4 Configuration

Configuration	Description and Command	
Configuring Gateway-targeted Spoofing Prevention	⚠ Optional.	
	anti-arp-spoofing ip	Configures gateway-targeted ARP spoofing prevention on the logical port and specifies the gateway IP address.

17.4.1 Configuring Gateway-targeted Spoofing Prevention

Configuration Effect

Enable gateway-targeted ARP spoofing prevention.

Configuration Steps

Configuring Gateway-targeted Spoofing Prevention

- Gateway-targeted ARP spoofing prevention is mandatory. It must be enabled.

Verification

- Run the **show run** command to check configuration.
- Run the **show anti-arp-spoofing** command to display all data on gateway-targeted ARP spoo

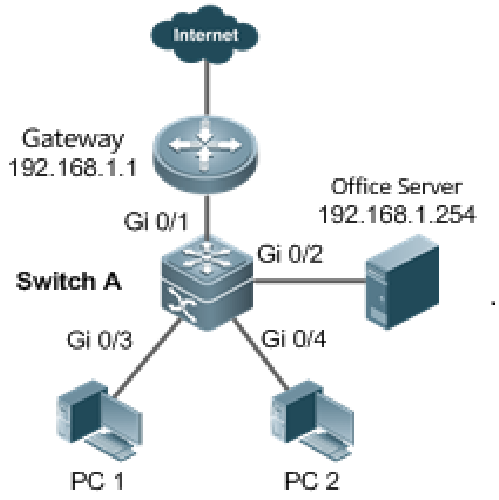
Related Commands

Configuring Gateway-targeted Spoofing Prevention

Command	**anti-arp-spoofing ip** *ip-address*
Parameter Description	*ip-address*: Indicates the IP address of the gateway.
Command Mode	Interface configuration mode or wireless security configuration mode
Usage Guide	Gateway-targeted ARP Spoofing prevention is supported only on Layer-2 ports. For an access controller (AC) or access point (AP), such function is supported only in wireless security configuration mode.

Configuration Example

Configuring Gateway-targeted Spoofing Prevention

Scenario **Figure 17-61**	 Internet Gateway 192.168.1.1 Office Server 192.168.1.254 Gi 0/1 Gi 0/2 Switch A Gi 0/3 Gi 0/4 PC 1 PC 2
	PC users access the office server through the access device Switch A, and connect external networks

	through the gateway. If any users legally use forged gateway IP addresses or server IP addresses to perform ARP spoofing, the other users cannot access the Internet or the server. The ARP spoofing packets with forged gateway address and intranet server IP addresses must be blocked to ensure that users can access the Internet.
Configuration Steps	Enable gateway-targeted spoofing prevention on the port directly connected to the PC.

```
SwitchA# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

SwitchA(config)#interface range gigabitEthernet 0/2-4

SwitchA(config-if-range)# anti-arp-spoofing ip 192.168.1.1

SwitchA(config-if-range)# anti-arp-spoofing ip 192.168.1.254
```

Verification	Run the **show anti-arp-spoofing** command to check for data on gateway-targeted ARP sp prevention.

```
SwitchA#show anti-arp-spoofing

NO    PORT       IP                STATUS

----- ---------- ----------------- ----------

1     Gi0/2      192.168.1.1       active

2     Gi0/2      192.168.1.254     active

3     Gi0/3      192.168.1.1       active

4     Gi0/3      192.168.1.254     active

5     Gi0/4      192.168.1.1       active

6     Gi0/4      192.168.1.254     active
```

17.5 Monitoring

Displaying

Description	Command
Displays all data on gateway-targeted ARP spoofing prevention.	**show anti-arp-spoofing**

18 Configuring NFPP

18.1 Overview

Network Foundation Protection Policy (NFPP) provides guards for switches.

Malicious attacks are always found in the network environment. These attacks bring heavy burdens to switches, resulting in high CPU usage and operational troubles. These attacks are as follows:

Denial of Service (DoS) attacks may consume lots of memory, entries, or other resources of a switch, which will cause system service termination.

Massive attack traffic is directed to the CPU, occupying the entire bandwidth of the CPU. In this case, normal protocol traffic and management traffic cannot be processed by the CPU, causing protocol flapping or management failure. The forwarding in the data plane will also be affected and the entire network will become abnormal.

A great number of attack packets directed to the CPU consume massive CPU resources, making the CPU highly loaded and thereby influencing device management and performance.

NFPP can effectively protect the system from these attacks.Facing attacks, NFPP maintains the proper running of various system services with a low CPU load, thereby ensuring the stability of the entire network.

18.2 Applications

Application	Description
Attack Rate Limiting	Due to various malicious attacks such as ARP attacks and IP scanning attacks in the network, the CPU cannot process normal protocol and management traffics, causing protocol flapping or management failure.The NFPP attack rate limiting function is used to limit the rate of attack traffic or isolate attack traffic to recover the network.
CentralizedBandwidth Allocation	If normal service traffics are too large, you need to classify and pr traffics. When a large number o CPU, the CPU will be highly loaded, thereby causing device management or device running failure The centralized bandwidth distribution function is used to increase the priority of such traffics so that switches can run stably.

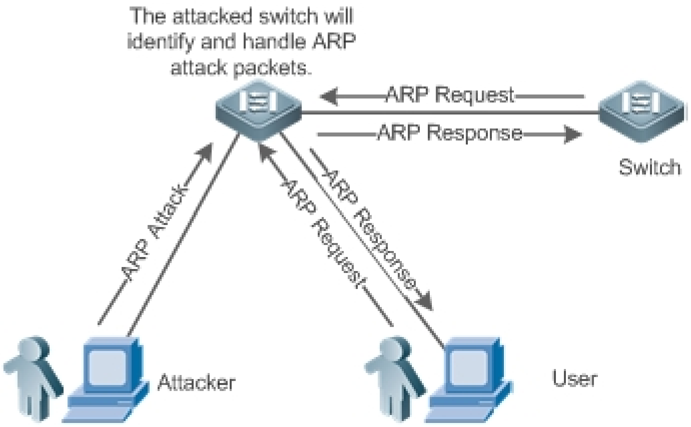
18.2.1 Attack Rate Limiting

Scenario

NFPP supports attack detection and rate limiting for various types of packets, including Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Dynamic Host Configuration Protocol (DHCP) packets. It also allows users to define packet matching characteristics and corresponding attack detection and rate limiting policies. The attack rate limiting function takes effect based on types of packets. This section uses ARP packets as an example scenario to descr application.

If an attacker floods ARP attack packets while CPU capability is insufficient, most of the CPU resources will be consumed for processing these ARP packets. If the rate of attacker's ARP packet rates exceeds the maximum ARP bandwidth specified in the CPU Protect Policy (CPP) of the switch, normal ARP packets may be dropped. As shown in Figure 18 -62, normal hosts will fail to access the network, and the switch will fail to send ARP replies to other devices.

Figure 18-62



Deployment

- By default, the ARP attack detection and rate limiting function is enabled with corresponding policies configured. If the rate of an attacker's ARP packets exceeds the rate limit, the packets are discarded. If it exceeds the attack threshold, a monitoring user is generated and prompt information is exported.
- If the rate of an attacker's ARP packets exceeds the rate limit defined in CPP and affects normal ARP replies, you can enable attack isolation to discard ARP attack packets based on the hardware and recover the network.

For details about CPP-related configurations, see the *Configuring CPU Protection*.

To maximize the use of NFPP guard functions, modify the rate limits of various services i application environment or use the configurations **show cpu-protect summary** command to display the configurations.

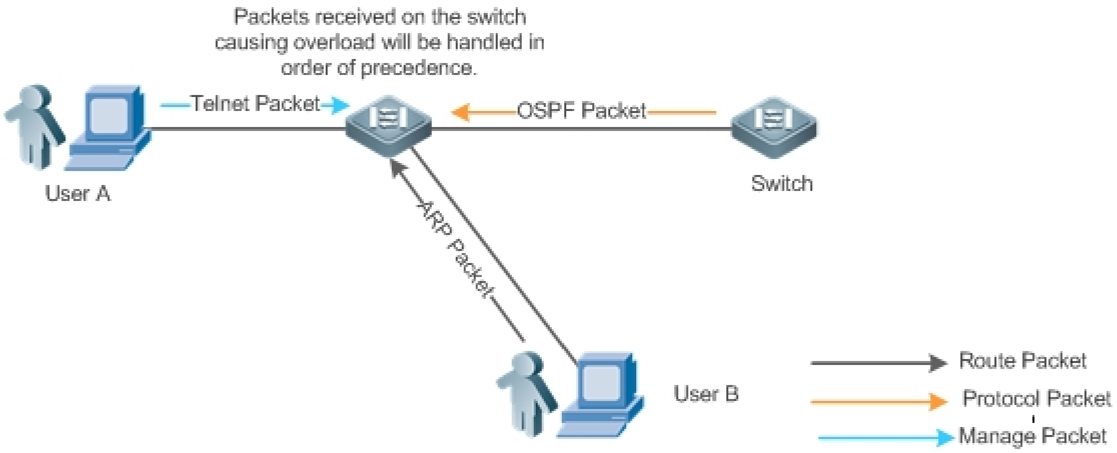
18.2.2 **Centralized Bandwidth Allocation**

Scenario

A switch classifies services defined in CPP into three types: Manage, Route, and Protocol. Each type of services ha independent bandwidth. Different types of services cannot share their bandwidths. Traffics with bandwidths exceeding th thresholds will be discarded. By such service classification, service packets are processed by orders of precedence.

As shown in Figure 18 -63, the switch receives a large number of Telnet packets, OSPF packets, and ARP packets, causing CPU overload. In this case, the CPU cannot process all packets, and a large quantity of packets are backlog queue, causing various problems such as frequent Telnet disconnection, OSPF protocol flapping, and ARP access failure on hosts.

Figure 18-63



Deployment

- By default, CPU centralized bandwidth allocation is enabled to assign an independent bandwidth and bandwidth ratio to each type of services. At the time, the CPU first processes Telnet packets to ensure uninterrupted connection of Telnet service, and then processes OSPF packets to maintain OSPF protocol stability, and finally processes ARP packets.
- If the preceding problems still occur in default configurations, you can accordingly adjust the bandwidths and bandwidth ratios of various types of services.

18.3 Features

Basic Concepts

↘ ARP Guard

In local area networks (LANs), IP addresses are mapped to MAC addresses through ARP, which has a significant role safeguarding network security. ARP-based DoS attacks mean that a large number of unauthorized ARP packets are sent to the gateway through the network, causing the failure of the gateway to provide services for normal hosts. To prevent such attacks, limit the rate of ARP packets and identify and isolate the attack source.

↘ IP Guard

Many hacker attacks and network virus intrusions Therefore, many scanning packets rapidly occupy the network bandwidth, causing network communication failure.

To solve this problem, Orion_B54Q Layer-3 switches provide IP guard function to prevent hacker scanning and Blaster Worm viruses and reduce the CPU load. Currently, there are mainly two types of IP attacks:

Scanning destination IP address changes: As the greatest threat to the network, this type of attacks not only consume network bandwidth and increases device load but also is a prelude of most hacker attacks.

Sending IP packets to non-existing destination IP addresses at high rates: This type of attacks is m consuming the CPU load. For a Layer-3 device, if the destination IP address exists, packets are directly forwarded by th switching chip without occupying CPU resources. If the destination IP address does not exist, IP packets are sen CPU, which then sends ARP requests to query the MAC address corresponding to the destination IP address. If too many packets are sent to the CPU, CPU resources will be consumed. This type of attack is less destructive than the former one.

To prevent the latter type of attack, limit the rate of IP packets and find and isolate the attack source.

↘ ICMP Guard

ICMP is a common approach to diagnose network failures. After receiving an ICMP echo request from a host, the router or switch returns an ICMP echo reply. The preceding process requires the CPU to process the packets, there consuming part of CPU resources. If an attacker sends a large number of ICMP echo requests to the destination dev massive CPU resources on the device will be consumed heavily, and the device may even fail to work properly. This type of attacks is called ICMP flood. To prevent this type of attacks, limit the rate of ICMP packets and find and isolate the attack source.

↘ DHCP Guard

DHCP is widely used in LANs to dynamically assign IP addresses. It is significant to network security. Currently, the most common DHCP attack, also called DHCP exhaustion attack, uses faked MAC addresses to broadcast DH Various attack tools on the Internet can easily complete this type of attack. A network attacker can send sufficient D requests to use up the address space provided by the DHCP server within a period. In this case, authorized hosts will fail to request DHCP IP addresses and thereby fail to access the network. To prevent this type of attacks, limit the rate of DHCP packets and find and isolate the attack source.

↘ DHCPv6 Guard

DHCP version 6 (DHCPv6) is widely used in LANs to dynamically assign IPv6 addresses. Both DHCP version 4 (DHCPv4) and DHCPv6 have security problems. Attacks to DHCPv4 apply also to DHCPv6. A network attacker can s number of DHCPv6 requests to use up the address space provided by the DHCPv6 server within a period. In this authorized hosts will fail to request IPv6 addresses and thereby fail to access the network. To prevent this type of attacks, limit the rate of DHCPv6 packets and find the attack source.

↘ ND Guard

Neighbor Discovery (ND) is mainly used in IPv6 networks to perform address resolution, router discovery, prefix discovery, and redirection. ND uses five types of packets: Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation (RS), Router Advertisement (RA), and Redirect. These packets are called ND packets.

ND snooping listens to ND packets in the network to filter unauthorized ND packets. It also monitors IPv network and bind monitored ones to ports to prevent IPv6 address stealing. ND snooping requires ND packets to be sent to the CPU. If ND packets are sent at a very high rate, the CPU will be attacked. Therefore, ND guard must be provided to limit the rate of ND packets.

↘ Self-Defined Guard

There are various types of network protocols, including routing protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Routing Information Protocol (RIP). Various devices need to excha different protocols. These packets must be sent to the CPU and processed by appropriate protocols. Once device runs a protocol, it is like opening a window for attackers. If an attacker sends a large number of protocol packets to a network device, massive CPU resources will be consumed on the device, and what's worse, the device may fail properly.

Since various protocols are being continuously developed, protocols in use vary w Orion_B54Q devices hereby provide self-defined guard. Users can customize and flexibly configure guard type guard requirements in different user environments.

Overview

Feature	Description
Host-based Rate Limiting and Attack Identification	Limits the rate according to the host-based rate limit and identify host attacks in the network.
Port-based Rate Limiting and Attack Identification	Limits the rate according to the port-based rate limit and identify port attacks.
Monitoring Period	Monitors host attackers in a specified period.
Isolation Period	Uses hardware to isolate host attackers or port attackers in a specified period.
Trusted Hosts	Trusts a host by not monitoring it.
Centralized BandwidthAllocation	Classifies and prioritizes packets.

18.3.1 **Host-based Rate Limiting and Attack Identification**

Limit the rate of attack packets of hosts and identify the attacks.

Identify ARP scanning.

Identify IP scanning.

Working Principle

Hosts can be identified in two ways: based on the source IP address, VLAN ID, and port and based on the link-layer source MAC address, VLAN ID, and port. Each host has a rate limit and an attack threshold (also called alarm threshold). The rate limit must be lower than the attack threshold. If the attack packet rate exceeds the rate limit of a host, the host discards the packets beyond the rate limit. If the attack packet rate exceeds the attack threshold of a host, the host identifies and logs the host attacks, and sends traps.

ARP scanning attack may have occurred if ARP packets beyond the scanning threshold received in the configured perio meet either of the following conditions:

- The link-layer source MAC address is fixed but the source IP address changes.
- The link-layer source MAC address and source IP address are fixed but the destination IP add changes.

Among IP packets beyond the scanning threshold received in the configured period, if the source IP address remains th same while the destination IP address continuously changes, IP scanning attack may have occurred.

- When NFPP detects a specific type of attack packets under a service, it sends a trap to the administrator. If the attack traffic persists, NFPP will not resend the alarm until 60 seconds later.
- To prevent CPU resource consumption caused by frequent log printing, NFPP writes attack detection logs to the buffer, obtains them from the buffer at a specified rate, and prints them. NFPP does not limit the rate of traps.

Related Configuration

Use ARP guard as an example:

↘ Configuring the Global Host-based Rate Limit, Attack Threshold, and Scanning Threshold

In NFPP configuration mode:

Run the **arp-guard rate-limit** {**per-src-ip** | **per-src-mac**} *pps* command to configure rate limits of hosts identified based on the source IP address, VLAN ID, and port and hosts identified based on the link-layer source MAC address, VLAN ID, and port.

Run the **arp-guard attack-threshold** {**per-src-ip** | **per-src-mac**} *pps* command to configure attack thresholds of host identified based on the source IP address, VLAN ID, and port and hosts identified based on the link-layer s address, VLAN ID, and port.

Run the **arp-guard scan-threshold** *pkt-cnt* command to configure the ARP scanning threshold.

↘ Configuring Host-based Rate Limit and Attack Threshold, and Scanning Threshold on an Interface

In interface configuration mode:

Run the **nfpp arp-guard policy** {**per-src-ip** | **per-src-mac**} *rate-limit-pps attack-threshold-pps* command to configure rate limits and attack thresholds of hosts identified based on the source IP address, VLAN ID, and port and hosts identified based on the link-layer source MAC address, VLAN ID, and port on an interface.

Run the **nfpp arp-guard scan-threshold** *pkt-cnt* command to configure the scanning threshold on an interface.

- Only ARP guard and IP guard support anti-scanning at present.

18.3.2 **Port-based Rate Limiting and Attack Identification**

Working Principle

Each port has a rate limit and an attack threshold. The rate limit must be lower than the attack threshold. If the packet rate exceeds the rate limit on a port, the port discards the packets. If the packet rate exceeds the attack threshold on a port, the port logs the attacks and sends traps.

Related Configuration

Use ARP guard as an example:

↘ Configuring the Global Port-based Rate Limit and Attack Threshold

In NFPP configuration mode:

Run the **arp-guard rate-limit per-port** *pps* command to configure the rate limit of a port.

Run the **arp-guard attack-threshold per-port** *pps* command to configure the attack threshold of a port.

↘ Configuring Port-based Rate Limit and Attack Threshold on an Interface

In interface configuration mode:

Run the **nfpp arp-guard policy per-port** *rate-limit-pps attack-threshold-pps* command to configure the rate limit and attack threshold of a port.

18.3.3 **Monitoring Period**

Working Principle

The monitoring user provides information about attackers in the current system. If the isolation period isolated), the guard module automatically performs software monitoring on attackers in the configured monitoring period. If the isolation period is set to a non-zero value, the guard module automatically isolates the hosts monitored by software and sets the timeout period as the isolation period. The monitoring period is valid only when the isolation period is 0.

Related Configuration

Use ARP guard as an example:

↘ Configuring the Global Monitoring Period

In NFPP configuration mode:

Run the **arp-guard monitor-period** *seconds* command to configure the monitoring period.

18.3.4 **Isolation Period**

Working Principle

Isolation is performed by the guard policies after attacks are detected. Isolation is implemented using the filter of t hardware to ensure that these attacks will not be sent to the CPU, thereby ensuring proper running of the device.

Hardware isolation supports two modes: host-based and port-based isolation. At present, only ARP or ND guard support port-based hardware isolation.

A policy is configured in the hardware to isolate attackers. However, hardware resources are limi resources are used up, the system prints logs to notify the administrator.

Related Configuration

Use ARP guard as an example:

↘ Configuring the Global Isolation Period

In NFPP configuration mode:

Run the **arp-guard isolate-period** [*seconds* | **permanent**] command to configure the isolation period. If the isolation period is set to 0, isolation is disabled. If it is set to a non-zero value, the value indicates the isolation p **permanent**, ARP attacks are permanently isolated.

↘ Configuring the Isolation Period on an Interface

In interface configuration mode:

Run the **nfpp arp-guard isolate-period** [*seconds* | **permanent**] command to configure the isolation period. If the isolation period is set to 0, isolation is disabled. If it is set to a non-zero value, the value indicates the isolation period. If it is set to **permanent**, ARP attacks are permanently isolated.

↘ Enabling Isolate Forwarding

In NFPP configuration mode:

Run the **arp-guard isolate-forwarding enable** command to enable isolate forwarding.

↘ Enabling Port-based Ratelimit Forwarding

In NFPP configuration mode:

Run the **arp-guard ratelimit-forwarding enable** command to enable port-based ratelimit forwarding.

At present, only ARP guard supports the configuration of isolate forwarding and ratelimit forwarding.

18.3.5 Trusted Hosts

Working Principle

If you do not want to monitor a host, you can run related commands to trust the host. This trusted host will be allowed to send packets to the CPU.

Related Configuration

Use IP anti-scanning as an example:

↘ Configuring Trusted Hosts

In NFPP configuration mode:

Run the **ip-guard trusted-host** *ip mask* command to trust a host.

Run the **trusted-host** {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*} command to trust a host for a self-defined guard.

18.3.6 Centralized Bandwidth Allocation

Working Principle

Services defined in CPP are classified into three types: Manage, Route, and Protocol. (For details, see the following table.) Each type of service has an independent bandwidth. Different types of services cannot share their bandw exceeding the bandwidth thresholds are discarded. By such service classification, service packets are processed by orders of precedence.

NFPP allows the administrator to flexibly assign bandwidth for three types of packets b environment so that Protocol and Manage packets can be first processed. Prior processing of Protocol packe proper running of protocols, and prior processing of Manage packets ensures proper management for the adr thereby ensuring proper running of important device functions and improving the guard capability of the device.

After classified rate limiting, all types of packets are centralized in a queue. When one type inefficiently, packets of this service will be backlogged in the queue and may finally use up resources of the queue. NFPP allows the administrator to configure the percentages of these three types of packets in the queue. When the queue length occupied by one type of packets exceeds the value of the total queue length multiplied by the percentage of this packet type, the excessive packets will be discarded. This efficiently prevents one type of packets from exclusively occu resources.

Packet Type	Service Type Defined in CPP
Protocol	tp-guard, dot1x, rldp, rerp, slow-packet, bpdu, isis dhcps, gvrp, ripng, dvmrp, igmp, mpls, ospf, pim, pimv6, rip, vrrp, ospf3, dhcp-relay-s, dhcp-relay-c, option82, tunnel-bpdu, tunnel-gvrp
Route	unknown-ipmc, unknown-ipmcv6, ttl1, ttl0, udp-helper, ip4-packet-other, ip6-packet-other, no ip-packet-other, arp
Manage	ip4-packet-local, ip6-packet-local

For the definitions of service types, see the Configuring CPU Protection.

Related Configuration

↘ Configuring the Maximum Bandwidth of Specified Packets

In global configuration mode:

Run the **cpu-protect sub-interface** {**manage** | **protocol** | **route**} **pps** *pps_value* command to configure the maximum bandwidth of specified packets.

↘ Configuring the Maximum Percentage of Specified Packets in the Queue

In global configuration mode:

Run the **cpu-protect sub-interface** { **manage** | **protocol** | **route** } **percent** *percent_value* command to configure the maximum percentage of specified packets in the queue.

18.4 Configuration

Configuration	Description and Command	
Configuring ARP Guard	**arp-guard enable**	Enables ARP guard globally.
	arp-guard isolate-period	Configures the global ARP-g period.
	arp-guard isolate-forwarding enable	Enables ARP-guard isolate forwarding.
	arp-guard ratelimit-forwarding enable	Enables APR-guard ratelimit forwarding.
	arp-guard monitor-period	Configures the global ARP-guard mon period.
	arp-guard monitored-host-limit	Configures the maximum number of ARP-guard monitored hosts.
	arp-guard rate-limit	Configures the global ARP-guard rate limit.
	arp-guard attack-threshold	Configures the global A threshold.
	arp-guard scan-threshold	Configures the global ARP-gua threshold.
	nfpp arp-guard enable	Enables ARP guard on an interface.
	nfpp arp-guard policy	Configures the APR-guard rate limit and attack threshold on an interface.
	nfpp arp-guard scan-threshold	Configures the APR-guard scanning threshold on an interface.
	nfpp arp-guard isolate-period	Configures the APR-guard isolation period on an interface.
Configuring IP Guard	**ip-guard enable**	Enables IP guard globally.
	ip-guard isolate-period	Configures the global IP-guard isolation period.
	ip-guard monitor-period	Configures the global IP-gu period.
	ip-guard monitored-host-limit	Configures the maximum number of IP-guard monitored hosts.
	ip-guard rate-limit	Configures the global IP-guard rate limit.
	ip-guard attack-threshold	Configures the global IP-guard attack threshold.
	ip-guard scan-threshold	Configures the global IP threshold.
	ip-guard trusted-host	Configures IP-guard trusted hosts.
	nfpp ip-guard enable	Enables IP guard on an interface.

Configuration	Description and Command	
	nfpp ip-guard policy	Configures the IP-guard rate limit and atta threshold on an interface.
	nfpp ip-guard scan-threshold	Configures the IP-guard scanning threshold on an interface.
	nfpp ip-guard isolate-period	Configures the IP-guard isolation period on an interface.
Configuring ICMP Guard	**icmp-guard enable**	Enables ICMP guard globally.
	icmp-guard isolate-period	Configures the global ICMP-gua period.
	icmp-guard monitor-period	Configures the global ICMP-guard monitori period.
	icmp-guard monitored-host-limit	Configures the maximum number of ICMP-guard monitored hosts.
	icmp-guard rate-limit	Configures the global ICMP-guard rate limit.
	icmp-guard attack-threshold	Configures the global ICM threshold.
	icmp-guard trusted-host	Configures ICMP-guard trusted hosts.
	nfpp icmp-guard enable	Enables ICMP guard on an interface.
	nfpp icmp-guard policy	Configures the ICMP-guard rate limit and attack threshold on an interface.
	nfpp icmp-guard isolate-period	Configures the ICMP-guard isolation period on an interface.
Configuring DHCP Guard	**dhcp-guard enable**	Enables DHCP guard globally.
	dhcp-guard isolate-period	Configures the global DHCP-guard period.
	dhcp-guard monitor-period	Configures the global DHCP-guard monitoring period.
	dhcp-guard monitored-host-limit	Configures the maximum number of DH guard monitored hosts.
	dhcp-guard rate-limit	Configures the global DHCP-guard rate limit.
	dhcp-guard attack-threshold	Configures the global DHCP threshold.
	nfpp dhcp-guard enable	Enables DHCP guard on an interface.
	nfpp dhcp-guard policy	Configures the DHCP-guard rate limit and attack threshold on an interface.
	nfpp dhcp-guard isolate-period	Configures the DHCP-guard isolation period on an interface.
Configuring DHCPv6 Guard	**dhcpv6-guard enable**	Enables DHCPv6 guard globally.

Configuration	Description and Command	
	dhcpv6-guard monitor-period	Configures the global DHCPv6-guard monitoring period.
	dhcpv6-guard monitored-host-limit	Configures the maximum number of DHCPv6-guard monitored hosts.
	dhcpv6-guard rate-limit	Configures the global DHCPv6-guard rate limit.
	dhcpv6-guard attack-threshold { **per-src-mac | per-port**} *pps*	Configures the global DHCPv6-guar threshold.
	nfpp dhcpv6-guard enable	EnablesDHCPv6 guard on an interface.
	nfpp dhcpv6-guard policy	Configures the DHCPv6-guard rate limit attack threshold on an interface.
Configuring ND Guard	**nd-guard enable**	Enables ND guard globally.
	nd-guard ratelimit-forwarding enable	Enables ND-guard ratelimit forwarding.
	nd-guard rate-limit per-port	Configures the global ND-guard rate limit.
	nd-guard attack-threshold per-port	Configures the globa threshold.
	nfpp nd-guard enable	Enables ND guard on an interface.
	nfpp nd-guard policy per-port	Configures the ND-guard rate limit and attack threshold on an interface.
Configuring a Self-Defined Guard	**define**	Configures the name of a self-defined guard.
	match	Configures **match** fields of a self-defined guard.
	global-policy	Configures the global rate limit a threshold of a self-defined guard.
	monitor-period	Configures the global monitoring period o self-defined guard.
	monitored-host-limit	Configures the maximum number of monitored hosts of a self-defined guard.
	trusted-host	Configures trusted hosts of a guard.
	define *name* **enable**	Enables a self-defined guard globally.
	nfpp define *name* **enable**	Enables a self-defined guard on an interface.
	nfpp define	Configures the rate limit and attack threshold of a self-defined guard on an interface.
Configuring NFPP Logging	**log-buffer entries**	Configures the log buffer size.
	log-buffer logs	Configures the log buffer rate.
	logging vlan	Configures VLAN-based logging filtering.
	logging interface	Configures interface-based logging filtering.
	logging enable	Enables log printing.

18.4.1 **Configuring ARP Guard**

Configuration Effect

- ARP attacks are identified based on hosts or ports. Host-based ARP attack identifica identification based on the source IP address, VLAN ID, and port and identification based on the link-layer source MAC address, VLAN ID, and port. Each type of attack identification has a rate limit and an attack threshold. packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ARP packet rate exceeds the attack threshold, the system prints alarm information and sends traps. In host-based attack identification, the syster also isolates the attack source.
- ARP guard can also detect ARP scanning attacks. ARP scanning attacks indicate that the link-lay address is fixed but the source IP address changes, or that the link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes. Due to the possibility of false positive, hosts poss performing ARP scanning are not isolated and are provided for the administrator's reference only.
- Configure ARP-guard isolation to assign hardware-isolated entries against host attacks so that att neither sent to the CPU nor forwarded.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.
- ARP guard prevents only ARP DoS attacks to the switch, but not ARP spoofing or ARP attacks in the network.
- For trusted ports configured for Dynamic ARP Inspection (DAI), ARP guard does not take effect, p positive of ARP traffic over the trusted ports. For details about DAI trusted ports, see the Configuring Dynamic A Inspection.

Configuration Steps

Enabling ARP Guard

- (Mandatory) ARP guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.
- If ARP guard is disabled, the system automatically clears monitored hosts, scanned hosts, and isolate ports.

Configuring the ARP-Guard Isolation Period

- (Optional) ARP-guard isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in NFPP configuration mode or interface configuration mode.

- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Enabling ARP-Guard Isolate Forwarding

- (Optional) ARP-guard isolate forwarding is enabled by default.
- To make isolation valid only at the management plane instead of the forwarding plane, you can enable this function.
- This function can be enabled in NFPP configuration mode.

Enabling ARP-Guard Ratelimit Forwarding

- (Optional) This function is enabled by default.
- If the port-based isolation entry takes effect, you can enable this function to pass some of the p discarding all of them.
- This function can be enabled in NFPP configuration mode.

Configuring the ARP-Guard Monitoring Period

- (Mandatory) The default ARP-guard monitoring period is 600 seconds.
- If the ARP-guard isolation period is configured, it is directly used as the monitoring p monitoring period will lose effect.
- The monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of ARP-Guard Monitored Hosts

- (Mandatory) The maximum number of ARP-guard monitored hosts is 20,000 by default.
- Set the maximum number of ARP-guard monitored hosts reasonably. As the number of monitored hosts incr more CPU resources are used.
- The maximum number of ARP-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This informa administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the ARP-Guard Attack Threshold

- Mandatory.
- To achieve the best ARP-guard effect, you are advised to configure the host-based rate limit and attack threshold based on the following order: Source IP address-based rate limit < Source IP address-based attack threshold <Source MAC address-based rate limit <Source MAC address-based attack threshold.
- The attack threshold can be configured in NFPP configuration mode or interface configuration mode.

- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack thresho smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the l NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over source IP address-based rate limiting while the latter takes priority over port-based rate limiting.

Configuring the ARP-Guard Scanning Threshold

- Mandatory.
- The scanning threshold can be configured in NFPP configuration mode or interface configuration mode.
- The ARP scanning table stores only the latest 256 records. When the ARP scanning table is full, the latest record will overwrite the earliest record.
- ARP scanning attack may have occurred if ARP packets received within 10 seconds meet either o conditions:

  - The link-layer source MAC address is fixed but the source IP address changes.

  - The link-layer source MAC address and source IP address are fixed but the destination IP address c changes, and the change times exceed the scanning threshold.

Verification

When a host in the network sends ARP attack packets to a switch configured with ARP guard, check whether these packets can be sent to the CPU.

- If the packets exceed the attack threshold or scanning threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling ARP Guard Globally

Command	**arp-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ARP-Guard Isolation Period

Command	**arp-guard isolate-period** [*seconds* | **permanent**]

Parameter Description	*seconds* Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. **permanent**: Indicates permanent isolation.
Command Mode	NFPP configuration mode
Usage Guide	N/A

↘ Enabling ARP-Guard Isolate Forwarding

Command	**arp-guard isolate-forwarding enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

↘ Enabling ARP-Guard Ratelimit Forwarding

Command	**arp-guard ratelimit-forwarding enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

↘ Configuring the Global ARP-Guard Monitoring Period

Command	**arp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	N/A

↘ Configuring the Maximum Number of ARP-Guard Monitored Hosts

Command	**arp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	N/A

↘ Configuring the Global ARP-Guard Rate Limit

Command	**arp-guard rate-limit** {**per-src-ip** |**per-src-mac** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Limits the rate of each source IP address. **per-src-mac**: Limits the rate of each source MAC address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ARP-Guard Attack Threshold

Command	**arp-guard attack-threshold** {**per-src-ip** | **per-src-mac** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Configures the attack threshold of each source IP address. **per-src-mac**: Configures the attack threshold of each source MAC address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is packets per second (pps).
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the Global ARP-Guard Scanning Threshold

Command	**arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling ARP Guard on an Interface

Command	**nfpp arp-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	ARP guard configured in interface configuration mode takes priority over that co configuration mode.

Configuring the ARP-Guard Isolation Period on an Interface

Command	**nfpp arp-guard isolate-period** [*seconds* | **permanent**]
Parameter	*seconds* Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to

Description	86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the ARP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp arp-guard policy** {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-src-ip**: Configures the rate limit and attack threshold of each source MAC address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the ARP-Guard Scanning Threshold on an Interface

Command	**nfpp arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

CPU Protection Based on ARP Guard

Scenario	● ARP host attacks exist in the system, and some hosts fail to properly establish ARP connection. ● ARP scanning exists in the system, causing a very high CPU utilization rate.
Configuration Steps	● Set the host-based attack threshold to 5 pps. ● Set the ARP scanning threshold to 10 pps. ● Set the isolation period to 180 pps.

```
Orion_B54Q# configure terminal

Orion_B54Q(config)# nfpp

Orion_B54Q (config-nfpp)#arp-guard rate-limit per-src-mac 5

Orion_B54Q (config-nfpp)#arp-guard attack-threshold per-src-mac 10

Orion_B54Q (config-nfpp)#arp-guard isolate-period 180
```

Verification	● Run the **show nfpp arp-guard summary** command to display the configuration.

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit      Attack-threshold Scan-threshold
Global    Disable 180            4/5/100         8/10/200         15


Maximum count of monitored hosts: 1000
Monitor period: 600s
```

- Run the **show nfpp arp-guard hosts** command to display the monitored hosts.

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface    IP address        MAC address     remain-time(s)
 ----    ---------    ----------        -----------     --------------
 1       Gi0/43       5.5.5.16          -               175
Total: 1 host
```

- Run the **show nfpp arp-guard scan** command to display the scanned hosts.

```
VLAN  interface       IP address        MAC address     timestamp
----  ---------       ----------        -----------     ---------
1     Gi0/5           -                 001a.a9c2.4609  2013-4-30 23:50:32
1     Gi0/5           192.168.206.2     001a.a9c2.4609  2013-4-30 23:50:33
1     Gi0/5           -                 001a.a9c2.4609  2013-4-30 23:51:33
1     Gi0/5           192.168.206.2     001a.a9c2.4609  2013-4-30 23:51:34
Total: 4 record(s)
```

Common Errors

N/A

18.4.2 Configuring IP Guard

Configuration Effect

- IP attacks are identified based on hosts or physical interfaces. In host-based IP attack identification, IP a identified based on the source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an attack threshold. If the IP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the IP packet rate exceeds the attack threshold, the system prints alarm information and sends traps. In host-based at identification, the system also isolates the attack source.

- IP guard can also detect IP scanning attacks. IP anti-scanning applies to IP packet attacks as follows: the destination IP address continuously changes but the source IP address remains the same, and the destination IP address is not the IP address of the local device.
- Configure IP guard isolation to assign hardware-isolated entries against host attacks so that attack packets are neither sent to the CPU nor forwarded.
- IP anti-scanning applies to IP packet attacks where the destination IP address is not the local IP address. The C limits the rate of IP packets where the destination IP address is the local IP address.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.

Configuration Steps

Enabling IP Guard

- (Mandatory) IP guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.
- If IP guard is disabled, the system automatically clears monitored hosts.

Configuring the IP-Guard Isolation Period

- (Optional) IP-guard isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in NFPP configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the IP-Guard Monitoring Period

- (Mandatory) The default IP-guard monitoring period is 600 seconds.
- If the IP-guard isolation period is configured, it is directly used as the monitoring period, and the configured monitoring period will lose effect.
- The monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of IP-Guard Monitored Hosts

- (Mandatory) The maximum number of IP-guard monitored hosts is 20,000 by default.
- Set the maximum number of IP-guard monitored hosts reasonably. As the number of monitored hosts increases, more CPU resources are used.

- The maximum number of IP-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts." This informati administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the IP-Guard Attack Threshold

- Mandatory.
- The attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack thresho smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prin NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes priority over port-based rate limiting.

Configuring the IP-Guard Scanning Threshold

- Mandatory.
- The scanning threshold can be configured in NFPP configuration mode or interface configuration mode.
- ARP scanning attack may have occurred if ARP packets received wi conditions:

  - The source IP address remains the same.

  - The destination IP address continuously changes and is not the local IP address, and the change times exceed the scanning threshold.

Configuring IP-Guard Trusted Hosts

- (Optional) No IP-guard trusted host is configured by default.
- For IP guard, you can only configure a maximum of 500 IP addresses not to be monitored.
- Trusted hosts can be configured in NFPP configuration mode.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the sy automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.

- If a trusted host cannot be deleted, the system prints the log "%ERROR: Failed to del 255.255.255.0." to notify the administrator.
- If a host cannot be trusted, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the host to trust already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the host to delete from the trusted table does not exist, the system prints the log "%ERROR: Trusted host 1.1. 255.255.255.0 is not found." to notify the administrator.
- If the memory cannot be allocated to a trusted host, the system prints the log "%ERROR: Failed to alloc memory." to notify the administrator.

Verification

When a host in the network sends IP attack packets to a switch configured with IP guard, check whether these packets can be sent to the CPU.

- If the rate of packets from untrusted hosts exceeds the attack threshold or scanning thresh displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling IP Guard Globally

Command	**ip-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global IP-Guard Isolation Period

Command	**ip-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds* Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. **permanent**: Indicates permanent isolation.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global IP-Guard Monitoring Period

Command	**ip-guard monitor-period** *seconds*

Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of IP-Guard Monitored Hosts

Command	**ip-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global IP-Guard Rate Limit

Command	**ip-guard rate-limit** {**per-src-ip** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Limits the rate of each source IP address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global IP-Guard Attack Threshold

Command	**ip-guard attack-threshold** {**per-src-ip** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Configures the attack threshold of each source IP address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the Global IP-Guard Scanning Threshold

Command	**ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring IP-Guard Trusted Hosts

Command	**ip-guard trusted-host** *ip mask*
Parameter Description	*ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address. **all**: Used with **no** to delete all trusted hosts.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run t This trusted host can send IP packets to the CPU, without any rate limiting or alarm reporting.

Enabling IP Guard on an Interface

Command	**nfpp ip-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	IP guard configured in interface configuration mode takes priority over configuration mode.

Configuring the IP-Guard Isolation Period on an Interface

Command	**nfpp ip-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds* Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the IP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp ip-guard policy** {**per-src-ip** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the attack threshold of each source IP address. **per-port**: Configures the attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the IP-Guard Scanning Threshold on an Interface

Command	**nfpp ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

↘ CPU Protection Based on IP Guard

Scenario

- IP host attacks exist in the system, and packets of some hosts cannot be properly route forwarded.
- IP scanning exists in the system, causing a very high CPU utilization rate.
- Packet traffic of some hosts is very large in the system, and these packets need to pass through.

Configuration Steps

- Configure the host-based attack threshold.
- Configure the IP scanning threshold.
- Set the isolation period to a non-zero value.
- Configure trusted hosts.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# nfpp
Orion_B54Q (config-nfpp)#ip-guard rate-limit per-src-ip 20
Orion_B54Q (config-nfpp)#ip-guard attack-threshold per-src-ip 30
Orion_B54Q (config-nfpp)#ip-guard isolate-period 180
Orion_B54Q (config-nfpp)#ip-guard trusted-host 192.168.201.46 255.255.255.255
```

Verification

- Run the **show nfpp ip-guard summary** command to display the configuration.

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit      Attack-threshold Scan-threshold
Global    Disable 180            20/-/100        30/-/200         100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

- Run the **show nfpp ip-guard hosts** command to display the monitored hosts.

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface    IP address        Reason    remain-time(s)
 ----    ---------    ----------        ------    --------------
```

```
  1       Gi0/5        192.168.201.47     ATTACK     160
Total: 1 host
```

- Run the **show nfpp ip-guard trusted-host** command to display the trusted hosts.

```
IP address          mask
----------          ----

192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Common Errors

N/A

18.4.3 Configuring ICMP Guard

Configuration Effect

- ICMP attacks are identified based on hosts or ports. In host-based attack identification, ICMP attacks are i based on the source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an attac threshold. If the ICMP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ICMP packet rate exceeds the attack threshold, the system prints alarm information and sends traps. In host-based att identification, the system also isolates the attack source.
- Configure ICMP guard isolation to assign hardware-isolated entries against host attacks so that attack p neither sent to the CPU nor forwarded.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.

Configuration Steps

↘ Enabling ICMP Guard

- (Mandatory) ICMP guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.
- If ICMP guard is disabled, the system automatically clears monitored hosts.

↘ Configuring the ICMP-Guard Isolation Period

- (Optional) ICMP-guard isolation is disabled by default.

- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in NFPP configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the ICMP-Guard Monitoring Period

- (Mandatory) The default ICMP-guard monitoring period is 600 seconds.
- If the ICMP-guard isolation period is configured, it is directly used as the monitoring peri monitoring period will lose effect.
- The monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of ICMP-Guard Monitored Hosts

- (Mandatory) The maximum number of ICMP-guard monitored hosts is 20,000 by default.
- Set the maximum number of ICMP-guard monitored hosts reasonably. As the number of actually mo increases, more CPU resources are used.
- The maximum number of ICMP-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This informa administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the ICMP-Guard Attack Threshold

- Mandatory.
- The attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack thresho smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NF NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes priority over port-based rate limiting.

Configuring ICMP-Guard Trusted Hosts

- (Optional) No ICMP-guard trusted host is configured by default.

- For ICMP guard, you can only configure a maximum of 500 IP addresses not to be monitored.
- Trusted hosts can be configured in NFPP configuration mode.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the sy automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If a trusted host cannot be deleted, the system prints the log "%ERROR: Failed to del 255.255.255.0." to notify the administrator.
- If a host cannot be trusted, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the host to trust already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the host to delete from the trusted table does not exist, the system prints the log "%ERROR: Trusted host 1.1. 255.255.255.0 is not found." to notify the administrator.
- If the memory cannot be allocated to a trusted host, the system prints the log "%ERROR: Failed to alloc memory." to notify the administrator.

Verification

When a host in the network sends ICMP attack packets to a switch configured with ICMP guard, check w packets can be sent to the CPU.

- If the rate of packets from an untrusted host exceeds the attack threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling ICMP Guard Globally

Command	**icmp-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ICMP-Guard Isolation Period

Command	**icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds* Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.

Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Configuring the Global ICMP-Guard Monitoring Period

Command	**icmp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zer value, the system automatically performs hardware isolation against monitored attackers and sets th timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of ICMP-Guard Monitored Hosts

Command	**icmp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the lo SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the Global ICMP-Guard Rate Limit

Command	**icmp-guard rate-limit** {**per-src-ip** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Limits the rate of each source IP address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command	NFPP configuration mode

Mode	
Usage Guide	N/A

Configuring the Global ICMP-Guard Attack Threshold

Command	**icmp-guard attack-threshold** {**per-src-ip** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Configures the attack threshold of each source IP address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring ICMP-Guard Trusted Hosts

Command	**icmp-guard trusted-host** *ip mask*
Parameter Description	*ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address. **all**: Used with **no** to delete all trusted hosts.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run this command to trust the host. This trusted host can send ICMP packets to the CPU, without any rate limiting or alarm reporting. You can configure the mask so that no host in one network segment is monitored. You can configure a maximum of 500 trusted hosts.

Enabling ICMP Guard on an Interface

Command	**nfpp icmp-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	ICMP guard configured in interface configuration mode takes priority over that confi configuration mode.

Configuring the ICMP-Guard Isolation Period on an Interface

Command	**nfpp icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds* Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode

Usage Guide	N/A

Configuring the ICMP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp icmp-guard policy** {**per-src-ip** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

CPU Protection Based on ICMP Guard

Scenario	● ICMP host attacks exist in the system, and some hosts cannot successfully ping devices. ● Packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.

```
Orion_B54Q# configure terminal

Orion_B54Q(config)# nfpp

Orion_B54Q (config-nfpp)#icmp-guard rate-limit per-src-ip 20

Orion_B54Q (config-nfpp)#icmp-guard attack-threshold per-src-ip 30

Orion_B54Q (config-nfpp)#icmp-guard isolate-period 180

Orion_B54Q (config-nfpp)#icmp-guard trusted-host 192.168.201.46 255.255.255.255
```

Verification	● Run the **show nfpp icmp-guard summary** command to display the configuration.

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)

Interface Status  Isolate-period Rate-limit      Attack-threshold

Global    Disable 180            20/-/400        30/-/400



Maximum count of monitored hosts: 1000

Monitor period: 600s
```

● Run the **show nfpp icmp-guard hosts** command to display the monitored hosts.

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
```

```
 VLAN    interface   IP address        remain-time(s)
 ----    ---------   ----------        --------------
  1      Gi0/5       192.168.201.47    160
Total: 1 host
```

- Run the **show nfpp icmp-guard trusted-host** command to display the trusted hosts.

```
IP address          mask
----------          ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Common Errors

N/A

18.4.4 Configuring DHCP Guard

Configuration Effect

- DHCP attacks are identified based on hosts or ports. In host-based attack identification, DHCP attacks are identifi based on the link-layer source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an attack threshold. If the DHCP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the DHCP packet rate exceeds the attack threshold, the system prints alarm information and sends traps. In host-base attack identification, the system also isolates the attack source.
- Configure DHCP guard isolation to assign hardware-isolated entries against host attacks so that attack pac neither sent to the CPU nor forwarded.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.
- For trusted ports configured for DHCP snooping, DHCP guard does not take effect, preventing false positive of DHCP traffic on the trusted ports. For details about trusted ports of DHCP snooping, see "Configuring Basic I DHCP Snooping" in the Configuring DHCP Snooping.

Configuration Steps

↘ Enabling DHCP Guard

- (Mandatory) DHCP guard is enabled by default.

- This function can be enabled in NFPP configuration mode or interface configuration mode.
- If DHCP guard is disabled, the system automatically clears monitored hosts.

Configuring the DHCP-Guard Isolation Period

- (Optional) DHCP-guard isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in NFPP configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the DHCP-Guard Monitoring Period

- (Mandatory) DHCP-guard monitoring is enabled by default.
- If the DHCP-guard isolation period is configured, it is directly used as the monitoring perioc monitoring period will lose effect.
- The monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of DHCP-Guard Monitored Hosts

- (Mandatory) The maximum number of DHCP-guard monitored hosts is 20,000 by default.
- Set the maximum number of DHCP-guard monitored hosts reasonably. As the number of monitored hosts increases, more CPU resources are used.
- The maximum number of DHCP-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This informa administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the DHCP-Guard Attack Threshold

- Mandatory.
- The attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack thresho smaller than rate limit 300pps." to notify the administrator.

- If the memory cannot be allocated to detected attackers, the system prints the log "%N NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over port-based rate limiting.

Verification

When a host in the network sends DHCP attack packets to a switch configured with DHCP guard, check whethe packets can be sent to the CPU.

- If the parameter of the packets exceeds the attack threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling DHCP Guard Globally

Command	**dhcp-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global DHCP-Guard Isolation Period

Command	**dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds* Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Configuring the Global DHCP-Guard Monitoring Period

Command	**dhcp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zer

	value, the system automatically performs hardware isolation against monitored attackers and sets th timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of DHCP-Guard Monitored Hosts

Command	**dhcp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the Global DHCP-Guard Rate Limit

Command	**dhcp-guard rate-limit** {**per-src-mac** | **per-port**} *pps*
Parameter Description	**per-src-mac**: Limits the rate of each source MAC address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global DHCP-Guard Attack Threshold

Command	**dhcp-guard attack-threshold** {**per-src-mac** | **per-port**} *pps*
Parameter Description	**per-src-mac**: Configures the attack threshold of each source MAC address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling DHCP Guard on an Interface

Command	**nfpp dhcp-guard enable**

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	DHCP guard configured in interface configuration mode takes priority over that configu configuration mode.

Configuring the DHCP-Guard Isolation Period on an Interface

Command	**nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds* Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the DHCP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp dhcp-guard policy** {**per-src-mac | per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

CPU Protection Based on DHCP Guard

Scenario	● DHCP host attacks exist in the system, and some hosts fail to request IP addresses.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# nfpp`
	`Orion_B54Q (config-nfpp)#dhcp-guard rate-limit per-src-mac 8`
	`Orion_B54Q (config-nfpp)#dhcp-guard attack-threshold per-src-mac 16`
	`Orion_B54Q (config-nfpp)#dhcp-guard isolate-period 180`

Verification	● Run the **show nfpp dhcp-guard summary** command to display the configuration.

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit      Attack-threshold
Global    Disable 180            -/8/150         -/16/300


Maximum count of monitored hosts: 1000
Monitor period: 600s
```

- Run the **show nfpp dhcp-guard hosts** command to display the monitored hosts.

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   MAC address      remain-time(s)
 ----    ---------   -----------      --------------
 *1       Gi0/5      001a.a9c2.4609   160
Total: 1 host
```

Common Errors

N/A

18.4.5 **Configuring DHCPv6 Guard**

Configuration Effect

- DHCPv6 attacks are identified based on hosts or ports. In host-based attack identification identified based on the link-layer source IP address, VLAN ID, and port. Each type of attack identification has a ra limit and an attack threshold. If the DHCPv6 packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the DHCPv6 packet rate exceeds the attack threshold, the system prints alarm information a traps.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.
- For trusted ports configured for DHCPv6 snooping, DHCPv6 guard does not take effect, preventing false positiv DHCPv6 traffic on the trusted ports. For details about trusted ports of DHCPv6 snooping, see "C Functions of DHCPv6 Snooping" in the Configuring DHCPv6 Snooping.

Configuration Steps

↘ Enabling DHCPv6 Guard

- (Mandatory) DHCPv6 guard is enabled by default.
- DHCPv6 guard can be enabled in NFPP configuration mode or interface configuration mode.
- If DHCPv6 guard is disabled, the system automatically clears monitored hosts.

Configuring the DHCPv6-Guard Monitoring Period

- (Mandatory) The default DHCPv6-guard monitoring period is 600 seconds.
- If the DHCPv6-guard isolation period is configured, it is directly used as the monitoring period, and th monitoring period does not take effect.
- The DHCPv6-guard monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of DHCPv6-Guard Monitored Hosts

- (Mandatory) The maximum number of DHCPv6-guard monitored hosts is 20,000 by default.
- Set the maximum number of DHCPv6-guard monitored hosts reasonably. As the number of monitored hosts increases, more CPU resources are used.
- The maximum number of DHCPv6-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This informa administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DHCPV6_GUARD Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the DHCPv6-Guard Attack Threshold

- Mandatory.
- The DHCPv6-guard attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack thresho smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCPV NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over port-based rate limiting.

Verification

When a host in the network sends DHCPv6 attack packets to a switch configured with DHCPv6 guard, check whether these packets can be sent to the CPU.

- If the parameter of the packets exceeds the attack threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

↘ Enabling DHCPv6 Guard Globally

Command	**dhcpv6-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

↘ Configuring the Global DHCPv6-Guard Monitoring Period

Command	**dhcpv6-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zer value, the system automatically performs hardware isolation against monitored attackers and sets th timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

↘ Configuring the Maximum Number of DHCPv6-Guard Monitored Hosts

Command	**dhcpv6-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFP SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the Global DHCPv6-Guard Rate Limit

Command	**dhcpv6-guardrate-limit** { **per-src-mac** | **per-port**} *pps*
Parameter Description	**per-src-mac**: Limits the rate of each source MAC address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global DHCPv6-Guard Attack Threshold

Command	**dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port**} *pps*
Parameter Description	**per-src-mac**: Configures the attack threshold of each source MAC address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling DHCPv6 Guard on an Interface

Command	**nfpp dhcpv6-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	DHCPv6 guard configured in interface configuration mode takes priority over that configured in NFP configuration mode.

Configuring the DHCP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp dhcpv6-guard policy** {**per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

CPU Protection Based on DHCPv6 Guard

Scenario	● DHCPv6 host attacks exist in the system, and DHCPv6 neighbor discovery fails on some hosts.
Configuration Steps	● Configure the host-based attack threshold.

```
Orion_B54Q# configure terminal

Orion_B54Q(config)# nfpp

Orion_B54Q (config-nfpp)#dhcpv6-guard rate-limit per-src-mac 8

Orion_B54Q (config-nfpp)#dhcpv6-guard attack-threshold per-src-mac 16
```

Verification	● Run the **show nfpp dhcpv6-guard summary** command to display the configuration.

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)

Interface Status  Rate-limit      Attack-threshold

Global    Disable -/8/150         -/16/300


Maximum count of monitored hosts: 1000

Monitor period: 600s
```

	● Run the **show nfpp dhcpv6-guard hosts** command to display the monitored hosts.

```
If col_filter 1 shows '*', it means "hardware do not isolate host".

 VLAN    interface   MAC address     remain-time(s)

 ----    ---------   -----------     --------------

 *1       Gi0/5      001a.a9c2.4609  160

Total: 1 host
```

Common Errors

N/A

18.4.6 Configuring ND Guard

Configuration Effect

- AR ND guard classifies ND packets into three types based on their purposes: 1. NS and NA; 2. Redirect. Type 1 packets are used for address resolution. Type 2 packets are used by hosts to discover the gateway. Type 3 packets are related to routing: RAs are used to advertise the gateway and prefix while Redirect packets used to advertise a better next hop.

- At present, only port-based ND packet attack identification is supported. You can configure the rate limits and attac thresholds for these three types of packets respectively. If the ND packet rate exceeds the rate lim

beyond the rate limit are discarded. If the ND packet rate exceeds the attack threshold, the system prints l
sends traps.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.

Configuration Steps

Enabling ND Guard

- (Mandatory) ND guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.

Enabling ND-Guard Ratelimit Forwarding

- (Optional) This function is enabled by default.
- If the port-based isolation entry takes effect, you can enable this function to pass some of the p
discarding all of them.
- This function can be enabled in NFPP configuration mode.

Configuring the ND-Guard Attack Threshold

- Mandatory.
- The ND-guard attack threshold can be enabled in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack thresho
smaller than rate limit 300pps." to notify the administrator.
- If memories cannot assigned to detected attackers, the system prints the log "%NFPP_ND_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.

Verification

When a host in the network sends ND attack packets to a switch configured with ND guard, check whether these packets can be sent to the CPU.

- If the parameter of the packets exceeds the attack threshold, an attack log is displayed.

Related Commands

Enabling ND Guard Globally

Command	**nd-guard enable**
Parameter	N/A

Description	
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling ND-Guard Ratelimit Forwarding

Command	**nd-guard ratelimit-forwarding enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ND-Guard Rate Limit

Command	**nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*
Parameter Description	**ns-na**: Indicates NSs and NAs. **rs**: Indicates RSs. **ra-redirect**: Indicates RAs and Redirect packets. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ND-Guard Attack Threshold

Command	**nd-guard attack-threshold per-port**[**ns-na** | **rs** | **ra-redirect**] *pps*
Parameter Description	**ns-na**: Indicates NSs and NAs. **rs**: Indicates RSs. **ra-redirect**: Indicates RAs and Redirect packets. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Enabling ND Guard on an Interface

Command	**nfpp nd-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	ND guard configured in interface configuration mode takes priority over th

	configuration mode.

Configuring the ND-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps*
Parameter Description	**ns-na**: Indicates NSs and NAs. **rs**: Indicates RSs. **ra-redirect**: Indicates RAs and Redirect packets. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit. ND snooping classifies ports into two types: untrusted ports (connecting the host) and tru (connecting the gateway).As traffic on a trusted port is usually larger than that on an untrusted port, the rate limit for a trusted port should be higher than that for an untrusted port. If ND snooping is enabled on a trusted port, ND snooping sets the rate limit to 800 pps and the attack threshold to 900 pps for the three types of packets on the port. ND guard treats the rate limit configured for ND snooping and that configured by the a equally. The value configured overwrites the previously configured and is stored in the configuration file. The attack threshold configured for ND snooping is treated in a similar way.

Configuration Example

CPU Protection Based on ND Guard

Scenario	● ND host attacks exist in the system, and neighbor discovery fails on some hosts.
Configuration Steps	● Configure the host-based attack threshold.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# nfpp`
	`Orion_B54Q (config-nfpp)# nd-guard rate-limit per-port ns-na 30`
	`Orion_B54Q (config-nfpp)# nd-guard attack-threshold per-port ns-na 50`

Verification	● Run the **show nfpp nd-guard summary** command to display the configuration.

	`(Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT.)`
	`Interface Status  Rate-limit       Attack-threshold`
	`Global    Disable 30/15/15`

Common Errors

N/A

18.4.7 **Configuring a Self-Defined Guard**

Configuration Effect

- Configure a self-defined guard to resolve network attack problems in special scenarios.

Notes

- For a command that is configured both in self-defined guard configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in self-defined mode.
- A self-defined guard takes priority over basic guards. When configuring the match fields of self-defined guards, see the Configuration Guide.

Configuration Steps

↘ Configuring the Guard Name

- (Mandatory) Configure the name of a self-defined guard to create the self-defined guard.
- The guard name must be unique, and the match fields and values c must be different from those of ARP, ICMP, DHCP, IP, and DHCPv6 guards. If the parameters you want to configure already exist, a message is displayed to indicate the configuration failure.

↘ Configuring the Match Fields

- Mandatory.
- Self-defined packets are classified based on the following fields: etype (Ethernet link-layer type), smac (source MA address), dmac (destination MAC address), protocol (IPv4/IPv6 protocol number), sip (source IPv4/IPv6 address), dip (destination IPv4/IPv6 address), sport (source transport-layer port), and dport (destination transport-layer port).
- **protocol** is valid only when the value of **etype** is **ipv4** or **ipv6** **src-ip** and **dst-ip** are valid only when the value of **etype** is **ipv4**. **src-ipv6** and **dst-ipv6** are valid only when the value of **etype** is **ipv6**. **src-port** and **dst-port** are valid only when the value of **protocol** is **tcp** or **udp**.
- If the **match** fields and values of a self-defined guard are totally the same as those of an existing guard, the system prints the log "%ERROR: the match type and value are the same with define name (name of an existing guard)." t notify the administrator of the configuration failure.
- If **protocol** is configured but **etype** is IPv4 or IPv6 in the **match** policy, the system prints the log "%ERROR: protocol is valid only when etype is IPv4(0x0800) or IPv6(0x86dd)."
- If **src-ip** and **dst-ip** are configured but **etype** is not IPv4 in the **match** policy, the system prints the log "%ERROR: IP address is valid only when etype is IPv4(0x0800)."
- If **src-ipv6** and **dst-ipv6** are configured but **etype** is not IPv6 in the **match** policy, the system prints the log "%ERROR: IPv6 address is valid only when etype is IPv6(0x86dd)."

- If **src-port** and **dst-port** are configured but **protocol** is not TCP or UDP in the **match** policy, the system prints the log "%ERROR: Port is valid only when protocol is TCP(6) or UDP(17)."
- The following table lists guard policies corresponding to some common network protocols. The rate limits and attac thresholds listed below can meet the requirements in most network scenarios and are for reference onl configure valid rate limits and attack thresholds based on actual scenarios.

Protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
RIP	etype 0x0800 protocol 17 dst-port 520	rate-limit 100 attatch-threshold 150	Not applicable to this policy	rate-limit 300 attatch-threshold 500
RIPng	etype 0x86dd protocol 17 dst-port 521	rate-limit 100 attatch-threshold 150	Not applicable to this policy	rate-limit 300 attatch-threshold 500
BGP	etype 0x0800 protocol 6 dst-port 179	rate-limit 1000 attatch-threshold 1200	Not applicable to this policy	rate-limit 2000 attatch-threshold 3000
BPDU	dst-mac 0180.c200.0000	Not applicable to this policy	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
RERP	dst-mac 01d0.f800.0001	Not applicable to this policy	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
REUP	dst-mac 01d0.f800.0007	Not applicable to this policy	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
BGP	etype 0x0800 protocol 6 dst-port 179	Not applicable to this policy	Not applicable to this policy	Not applicable to this policy
OSPFv2	etype 0x0800 protocol 89	rate-limit 800 attatch-threshold 1200	Not applicable to this policy	rate-limit 2000 attatch-threshold 3000
OSPFv3	etype 0x86dd protocol 89	rate-limit 800 attatch-threshold 1200	Not applicable to this policy	rate-limit 2000 attatch-threshold 3000
VRRP	etype 0x0800 protocol 112	rate-limit 64 attatch-threshold 100	Not applicable to this policy	rate-limit 1024 attatch-threshold 1024
IPv6 VRRP	etype 0x86dd protocol 112	rate-limit 64 attatch-threshold 100	Not applicable to this policy	rate-limit 1024 attatch-threshold 1024
SNMP	etype 0x0800 protocol 17 dst-port 161	rate-limit 1000 attatch-threshold 1200	Not applicable to this policy	rate-limit 2000 attatch-threshold 3000
RSVP	etype 0x0800 protocol 46	rate-limit 800 attatch-threshold 1200	Not applicable to this policy	rate-limit 1200 attatch-threshold 1500

Protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
LDP (UDP hello)	etype 0x0800 protocol 17 dst-port 646	rate-limit 10 attatch-threshold 15	Not applicable to this policy	rate-limit 100 attatch-threshold 150

- To contain as many existing protocol types as possible and facilitate expansion of new protocol types, se guards allow hosts to freely combine type fields of packets. If the configuration is inappropriate, t become abnormal. Therefore, the network administrator needs to have a good knowledge of network protocols. As a reference, the following table lists valid configurations of currently known protocols for common se policies. For other protocols not listed in the table, configure them with caution.

↘ Configuring the Global Rate Limit and Attack Threshold

- (Mandatory) If these parameters are not configured, the self-defined guard cannot be enabled.
- You must configure one of the per-src-ip, per-src-mac, and per-port fields. Otherwise, the policy cannot take effect.
- per-src-ip is valid only when etype is IPv4 or IPv6.
- The rate limit configured based on the source MAC address, VLAN ID, and port takes priority over that c based on the source IP address, VLAN ID, and port.
- The port-based host identification policy of a self-defined guard must be consistent with the global port-l identification policy.
- If the **per-src-ip**policy is not configured globally but configured for a port, the system prints the log "%ERROR: name (name of a self-defined guard) has not per-src-ip policy." to notify the administrator of the configuration failure.
- If the **per-src-mac** policy is not configured globally but configured for a port, the system prints the log "%ERROR: name (name of a self-defined guard) has not per-src-mac policy." to notify the administrator of the configuration failure.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DE NO_MEMORY: Failed to allocate memory." to notify the administrator.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack thresho smaller than rate limit 300pps." to notify the administrator.

↘ Configuring the Global Monitoring Period

- (Mandatory) The default monitoring period is 600 seconds.
- If the isolation period is configured, it is directly used as the monitoring period, and the configured monitoring period will lose effect.
- The monitoring period can be configured in self-defined guard configuration mode.
- If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is tl monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically

performs hardware isolation against monitored attackers and sets the timeout period as the monitoring p monitoring period is valid only when the isolation period is 0.

- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of Monitored Hosts

- (Mandatory) The maximum number of monitored hosts is 20,000 by default.
- Set the maximum number of monitored hosts reasonably. As the number of monitored hosts increases, mo resources are used.
- The maximum number of monitored hosts can be configured in self-defined guard configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This informa administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DEFINE-4-SESSION_LI exceed limit of name's 20000 monitored hosts." to notify the administrator.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- You can configure a maximum of 500 trusted IP address or MAC address for a self-defined guard.
- Trusted hosts can be configured in self-defined guard configuration mode.
- If you do not want to monitor a host, you can run the following commands to trust the host. This trusted host can send ICMP packets to the CPU, without any rate limiting or alarm reporting.You can configure the mask so that no host in one network segment is monitored.
- You must configure the **match type** before configuring trusted hosts. If the pa **match** policy, you are not allowed to configure trusted IPv6 addresses. If the packet type is IPv6 in the match policy, you are not allowed to configure trusted IPv4 addresses.
- If the **match** type is not configured, the system prints the log "%ERROR: Please configure match rule first."
- If a trusted IPv4 host is added but **type** is not IPv4 in the **match** policy, the system prints the log "%ERROR: Match type can’t support IPv4 trusted host."
- If a trusted IPv6 host is added but **type** is not IPv6 in the **match** policy, the system prints the log "%ERROR: Match type can’t support IPv6 trusted host."
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the sy automatically deletes this entry.

- If a trusted host cannot be deleted, the system prints the log "%ERROR: Failed to del 255.255.255.0." to notify the administrator.
- If a host cannot be trusted, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the host to trust already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the host to delete from the trusted table does not exist, the system prints the log "%ERROR: Trusted host 1.1. 255.255.255.0 is not found." to notify the administrator.
- If the memory cannot be allocated to a trusted host, the system prints the log "%ERROR: Failed to allocate memory." to notify the administrator.

Enabling a Self-Defined Guard

- Mandatory.
- You have to configure at least one policy between host-based self-defined guard policy and port-based self-c guard policy. Otherwise, the self-defined guard cannot be enabled.
- If a self-defined guard is disabled, the system automatically clears monitored hosts.
- Self-defined guards can be configured in self-defined guard configuration mode or interface configuration mode.
- If a self-defined guard policy is not completely configured, the self-defined guard cannot be enabled and a prompt displayed to notify hosts of the missing policy configurations.
- If the name of a self-defined guard does not exist, the system prints the log "%ERROR: The name is not exist."
- If the match type is not configured for a self-defined guard, the system prints the log "%ERROR: name (name of the self-defined guard) doesn't match any type."
- If no policy is configured for a self-defined guard, the system prints the log "%ERROR: name (name of the self-defined guard) doesn't specify any policy."

Verification

When a host in the network sends packets to a switch configured with a self-defined NFPP guard, check wheth packets can be sent to the CPU.

- If the rate of packets from an untrusted host exceeds the attack threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Configuring the Name of a Self-defined Guard

Command	**define** *name*
Parameter Description	**name**: Indicates the name of a self-defined guard.

Command Mode	NFPP configuration mode
Usage Guide	N/A

↘ Configuring Match Fields of a Self-defined Guard

Command	**match** [**etype** *type*] [**src-mac** *smac* [**src-mac-mask** *smac_mask*]] [**dst-mac** *dmac* [**dst-mac-mask** *dst_mask*]] [**protocol** *protocol*] [**src-ip** *sip* [**src-ip-mask** *sip-mask*]] [**src-ipv6** *sipv6* [**src-ipv6-masklen** *sipv6-masklen*]] [**dst-ip** *dip* [**dst-ip-mask** *dip-mask*]] [**dst-ipv6** *dipv6* [**dst-ipv6-masklen** *dipv6-masklen*]][**src-port***sport*] [**dst-port** *dport*]
Parameter Description	*type*: Indicates the type of Ethernet link-layer packets. *smac*: Indicates the source MAC address. *smac_mask*: Indicates the mask of the source MAC address. *dmac*: Indicates the destination MAC address. *dst_mask*: Indicates the mask of the destination MAC address. *protocol*: Indicates the protocol number of IPv4/IPv6 packets. *sip*: Indicates the source IPv4 address. *sip-mask*: Indicates the mask of the source IPv4 address. *sipv6*: Indicates the source IPv6 address. *sipv6-masklen*: Indicates the mask length of the source IPv6 address. *dip*: Indicates the destination IPv4 address. *dip-mask*: Indicates the mask of the destination IPv4 address. *dipv6*: Indicates the destination IPv6 address. *dipv6-masklen*: Indicates the mask length of the destination IPv6 address. *sport*: Indicates the ID of the source transport-layer port. *dsport*: Indicates the ID of the destination transport-layer port.
Command Mode	Self-defined guard configuration mode
Usage Guide	Create a new self-defined guard and specify the packet fields matched by this guard.

↘ Configuring the Global Rate Limit and Attack Threshold of a Self-defined Guard

Command	**global-policy** {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip** Collects rate statistics for host identification based on the source IP address, VLAN ID, and port. **per-src-mac**: Collects rate statistics for host identification based on the source MAC address, VLAN ID, and port. **per-port**: Collects rate statistics based on each packet receiving port. *rate-limit-pps*: Indicates the rate limit. *attack-threshold-pps*: Indicates the attack threshold.
Command Mode	Self-defined guard configuration mode

Usage Guide	Before creating a self-defined guard type, you must specify rate statistic classification rules for this type, namely, source IP address-based host identification, source MAC address-based host i host-based self-defined packet rate statistics, or port-based rate statistics, and specify the rate limits and attack thresholds for the specified rules.

Configuring the Global Monitoring Period of a Self-defined Guard

Command	**monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	Self-defined guard configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Monitored Hosts of a Self-defined Guard

Command	**monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	Self-defined guard configuration mode
Usage Guide	N/A

Configuring Trusted Hosts of a Self-defined Guard

Command	**trusted-host** {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*}
Parameter Description	*mac*: Indicates the MAC address. *mac_mask*: Indicates the mask of an MAC address. *ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address. *IPv6/prefixlen*: Indicates the IPv6 address and its mask length. **all**: Used with **no** to delete all trusted hosts.
Command Mode	Self-defined guard configuration mode
Usage Guide	N/A

Enabling a Self-Defined Guard Globally

Command	**define** *name* **enable**
Parameter Description	*name*: Indicates the name of a self-defined guard.
Command Mode	NFPP configuration mode
Usage Guide	The configuration takes effect only after you have configured **match**, **rate-count**, **rate-limit**, and **attack-**

	threshold. Otherwise, the configuration fails.

Enabling a Self-defined Guard on an Interface

Command	**nfpp define** *name* **enable**
Parameter Description	*name*: Indicates the name of a self-defined guard.
Command Mode	Interface configuration mode
Usage Guide	The self-defined name must exist. The configuration takes effect only aft **match**, **rate-count**, **rate-limit**, and **attack-threshold**. Otherwise, the configuration fails.

Configuring the Rate Limit and Attack Threshold of a Self-defined Guard on an Interface

Command	**nfpp define** *name* **policy** {**per-src-ip** | **per-src-mac| per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	*name*: Indicates the name of a self-defined guard. **per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-src-mac**: Configures the rate limit and attack threshold of each source MAC address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

CPU Protection Based on a Self-Defined Guard

Scenario	● Basic guards cannot protect the system with RIP attacks.
Configuration Steps	● Configure a self-defined guard, with the key fields matching RIP packets. ● Configure the rate limit. ● Configure trusted hosts.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# nfpp`
	`Orion_B54Q (config-nfpp)#define rip`
	`Orion_B54Q (config-nfpp-define)#match etype 0x0800 protocol 17 dst-port 520`
	`Orion_B54Q (config-nfpp-define)#global-policy per-src-ip 100 150`
	`Orion_B54Q (config-nfpp-define)#trusted-host 192.168.201.46 255.255.255.255`
	`Orion_B54Q (config-nfpp-define)#exit`
	`Orion_B54Q (config-nfpp)#define rip enable`

Verification

- Run the **show nfpp define summary rip** command to display the configuration.

```
Define rip summary:
match etype 0x800 protocol 17 dst-port 520
Maximum count of monitored hosts: 1000
Monitor period:600s
(Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Rate-limit      Attack-threshold
Global    Enable  100/-/-         150/-/-
```

- Run the **show nfpp define trusted-host rip** command to display the trusted hosts.

```
Define rip:
IP trusted host number is 1:
IP address         IP mask
----------         -------
192.168.201.46     255.255.255.255


Total: 1 record(s)Global    Enable  180            100/-/-         150/-/-
```

- Run the **show nfpp define hosts rip** command to display the monitored hosts.

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address        remain-time(s)
 ----    ---------   ----------        --------------
  1      Gi0/5       192.168.201.47    160
Total: 1 host
```

Common Errors

N/A

18.4.8 **Configuring Centralized Bandwidth Allocation**

Configuration Effect

- Configure centralized bandwidth allocation so that Manage and Protocol packets are first processed when the network is busy.

Notes

- The following condition must be met: Valid percentage range of a type of packets ≤ 100% – Percentage of the sum of the other two types

Configuration Steps

Configuring the Maximum Bandwidth of Specified Packets

- (Mandatory) Manage, Route, and Protocol packets share the same default bandwidth.

Configuring the Maximum Percentage of Specified Packets in the Queue

- (Mandatory) By default, Manage packets occupy 30% of the bandwidth, Route packets occupy 25%, a packets occupy 45%.

Verification

Send a large number of protocol packets such as OSPF packets to a switch, causing high CPU utilization.

- When the host pings the switch, the pinging must be successful and no packet is lost.

Related Commands

Configuring the Maximum Bandwidth of Specified Packets

Command	**cpu-protect sub-interface** { **manage** | **protocol**|**route**} **pps** *pps_value*
Parameter Description	*pps_value*: Indicates the rate limit, ranging from 1 to 100,000.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Maximum Percentage of Specified Packets in the Queue

Command	**cpu-protect sub-interface** { **manage** | **protocol** | **route**} **percent** *percent_value*
Parameter Description	*percent_value*: Indicates the percentage of a type of packets in the queue, ranging from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	The following condition must be met: Valid percentage range of a type of packets ≤ 100% – Percentage of the sum of the other two types

Configuration Example

Prioritizing Packets Sent to the CPU Through Centralized Bandwidth Allocation

Scenario	● Various types of mass packets exist in the network and belong to different centralized types.
Configuration Steps	● Configure the maximum bandwidth of specified packets. ● Configure the maximum percentage of specified packets in the queue.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# cpu-protect sub-interface manage pps 5000`
	`Orion_B54Q(config)# cpu-protect sub-interface manage percent 25`

Verification	N/A

Common Errors

N/A

18.4.9 **Configuring NFPP Logging**

Configuration Effect

- NFPP obtains a log from the dedicated log buffer at a certain rate, generates a system message, and clears this log from the dedicated log buffer.

Notes

- Logs are continuously printed in the log buffer, even if attacks have stopped.

Configuration Steps

Configuring the Log Buffer Size

- Mandatory.
- If the log buffer is full, new logs replace the old ones.
- If the log buffer overflows, subsequent logs replace previous logs, and an entry with all attributes marked with a hyphen (-) is displayed in the log buffer. The administrator needs to increase the log buffer size or the generation rate.

Configuring the Log Buffer Rate

- Mandatory.
- The log buffer rate depends on two parameters: the time period and the number of system messages generated in the time period.
- If both of the preceding two parameters are set to 0, system messages are immediately generated for logs but are not stored in the log buffer.

Enabling Log Filtering

- (Optional) Log filtering is disabled by default.
- Logs can be filtered based on an interface or VLAN.
- If log filtering is enabled, logs not meeting the filtering rule are discarded.

Enabling Log Printing

- (Mandatory) Logs are stored in the buffer by default.
- If you want to monitor attacks in real time, you can configure logs to be printed on the screen t information in real time.

Verification

Check whether the configuration takes effect based on the log configuration and the number and interval of printed logs.

Related Commands

Configuring the Log Buffer Size

Command	**log-buffer entries** *number*
Parameter Description	*number*: Indicates the buffer size in the unit of the number of logs, ranging from 0 to 1,024.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Log Buffer Rate

Command	**log-buffer logs** *number_of_message* **interval** *length_in_seconds*
Parameter Description	*number_of_message*: Ranges from 0 to 1,024. The value 0 indicates that all logs are recorded in the log buffer and no system message is generated. *length_in_seconds*: Ranges from 0 to 86,400 (1 day). The value 0 indicates that logs are not recorded in the log buffer but system messages are i *number_of_message* and *length_in_seconds*. *number_of_message/length_in_second* indicates the system message generation rate.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring VLAN-based Log Filtering

Command	**logging vlan** *vlan-range*
Parameter Description	*vlan-range*: Records logs in a specified VLAN range. The value format is 1-3,5 for example.
Command Mode	NFPP configuration mode
Usage Guide	Run this command to filter logs so that only logs in the specified V Between interface-based log filtering and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Configuring Interface-based Log Filtering

Command	**logging interface** *interface-id*
Parameter Description	*interface-id*: Records logs of a specified interface.
Command Mode	NFPP configuration mode
Usage Guide	Run this command to filter logs so that only logs of the sp Between interface-based log filtering and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Enabling Log Printing

Command	**log-buffer enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuration Example

Configuring NFPP Logging

Scenario	● If attackers are too many, log printing will affect the usage of user interfaces, w restriction.
Configuration Steps	● Configure the log buffer size. ● Configure the log buffer rate. ● Configure VLAN-based log filtering.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# nfpp`
	`Orion_B54Q (config-nfpp)#log-buffer entries 1024`
	`Orion_B54Q (config-nfpp)#log-buffer logs 3 interval 5`
	`Orion_B54Q (config-nfpp)#logging interface vlan 1`

Verification	● Run the **show nfpp log summary** command to display the configuration.

	`Total log buffer size : 1024`
	`Syslog rate : 3 entry per 5 seconds`
	`Logging:`
	`    VLAN 1`

	● Run the **show nfpp log buffer** command to display logs in the log buffer.

	Protocol VLAN Interface IP address MAC address Reason Timestamp -------- ---- --------- ---------- ----------- ------ --------- ARP 1 Gi0/5 192.168.206.2 001a.a9c2.4609 SCAN 2013-5-1 5:4:24

18.5 Monitoring

Clearing

Description	Command
Clears the ARP-guard scanning table.	**clear nfpp arp-guard scan**
Clears ARP-guard monitored hosts.	**clear nfpp arp-guard hosts**
Clears IP-guard monitored hosts.	**clear nfpp ip-guard hosts**
Clears ND-guard monitored hosts.	**clear nfpp nd-guard hosts**
Clears ICMP-guard monitored hosts.	**clear nfpp icmp-guard hosts**
Clears DHCP-guard monitored hosts.	**clear nfpp dhcp-guard hosts**
Clears DHCPv6-guard monitored hosts.	**clear nfpp dhcpv6-guard hosts**
Clears self-defined guard monitored hosts.	**clear nfpp define** *name* **hosts**
Clears NFPP logs.	**clear nfpp log**

Displaying

Description	Command
Displays ARP-guard configuration.	**show nfpp arp-guard summary**
Displays ARP-guard monitored hosts.	**show nfpp arp-guard hosts**
Displays the ARP-guard scanning table.	**show nfpp arp-guard scan**
Displays IP-guard configuration.	**show nfpp ip-guard summary**
Displays IP-guard monitored hosts.	**show nfpp ip-guard hosts**
Displays the IP-guard scanning table.	**show nfpp ip-guard trusted-host**
Displays ICMP-guard configuration.	**show nfpp icmp-guard summary**
Displays ICMP-guard monitored hosts.	**show nfpp icmp-guard hosts**
Displays the ICMP-guard scanning table.	**show nfpp icmp-guard trusted-host**
Displays DHCP-guard configuration.	**show nfpp dhcp-guard summary**
Displays DHCP-guard monitored hosts.	**show nfpp dhcp-guard hosts**
Displays DHCPv6-guard configuration.	**show nfpp dhcpv6-guard summary**
Displays DHCPv6-guard monitored hosts.	**show nfpp dhcpv6-guard hosts**
Displays ND-guard configuration.	**show nfpp nd-guard summary**
Displays self-defined guard configuration.	**show nfpp define summary** [*name*]

Description	Command
Displays the monitored hosts.	**show nfpp define hosts** *name*
Displays the trusted hosts.	**show nfpp define trusted**-**host** *name*
Displays NFPP logs.	**show nfpp log summary**
Displays the NFPP log buffer.	**show nfpp log buffer** [**statistics**]

19 Configuring DoS Protection

19.1 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 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_B54Q products supports the following anti DoS attack functions:

- Denying land attacks
- Denying invalid TCP packets
- Denying invalid layer-4 (L4) ports

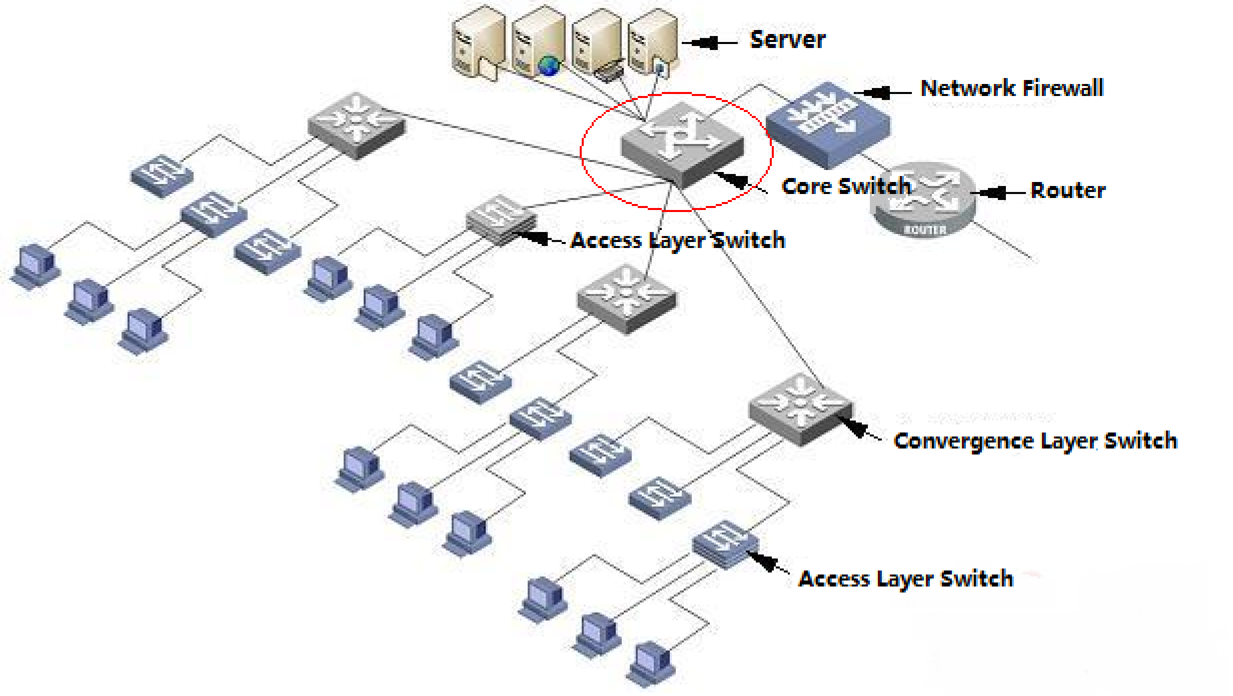
19.2 Applications

Application	Description
Protecting Servers Against DoS Attacks	On a campus network, configure the anti DoS attack function on th connected to servers to effectively reduce the negative impacts brought by DoS attacks to servers.

19.2.1 Protecting Servers Against DoS Attacks

As show in Figure 19-64, 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 19-64



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 ports.

19.3 Features

Overview

Feature	Description
Denying Land Attacks	Drop packets with the same source and destination IP addresses or the same L4 source destination port IDs on the device to prevent these packets from attacking OSs on the network.
Denying Invalid TCP Packets	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".
Denying Invalid L4 Ports	Drop packets with the same L4 source and destination port IDs on the device to prevent these packets from attacking OSs on the network.

19.3.1 **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 ev 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.

19.3.2 **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 pac 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 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 soo 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 flagsTherefore, 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 f packet (TCP SYN packet) must contain the SYN flag, and the subsequent packets contain the ACK flag. Based on 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 th ACK flagSome attackers may send TCP packets with the FIN flag but without the ACK flag to the target hosts, causin 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) proc 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.

19.3.3 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 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.

19.4 Configuration

Configuration Item	Description and Command	
Configuring the Function of Denying Land Attacks	⚠ Optional.	
	ip deny land	Enables the function of der attacks.
Configuring the Function of Denying Invalid TCP Packets	⚠ Optional.	
	Ip deny invalid-tcp	Enables the function of denying invalid TCP packets.
Configuring the Function of Denying Invalid L4 Ports	⚠ Optional.	
	ip deny invalid-l4port	Enables the function of denying invalid L4 ports.

19.4.1 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**

Command	**[no] ip deny land**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	N/A

Configuration Example

↘ Enabling the Function of Denying Land Attacks

Configuration Steps	● Enable the function of denying land attacks in global configuration mode.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# ip deny land`
	`Orion_B54Q(config)# end`

Verification	Run the **show ip deny land** command to display the status of the funct
	attacks.
	The following example shows how to display the status
	attacks:
	`Orion_B54Q#show ip deny land`
	`        DoS Protection Mode              State`
	`-------------------------------------     -----`
	`protect against land attack On`

19.4.2 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** to display the status of the function of de
  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

Command	**[no] ip deny invalid-tcp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Enabling the Function of Denying Invalid TCP Packets

Configuration Steps	● Enable the function of denying invalid TCP packets in global configuration mode.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# ip deny invalid-tcp`
	`Orion_B54Q(config)# end`

Verification	Run the **show ip deny invalid-tcp** command to display the status of the function of denying invalid TCP packets.

	The following example shows how to display the status of the function of denying invalid TCP packets:
	`Orion_B54Q#show ip deny invalid-tcp`
	`        DoS Protection Mode             State`
	`-------------------------------------     -----`
	`protect against invalid tcp attack   On`

19.4.3 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

Command	**[no] ip deny invalid-l4port**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Enabling the Function of Denying Invalid L4 Ports

Configuration Steps	● Enable the function of denying invalid L4 ports in global configuration mode.

	`Orion_B54Q# configure terminal`
	`Orion_B54Q(config)# ip deny invalid-l4port`
	`Orion_B54Q(config)# end`

Verification	Run the **show ip deny invalid-l4port** command to display the status of the function of denying invalid L4 ports.
	The following example shows how to display the status of the function of denying invalid L4 ports:
	`Orion_B54Q#show ip deny invalid-l4port`
	`        DoS Protection Mode             State`
	`-------------------------------------     -----`
	`protect against invalid l4port attack  On`

19.5 Monitoring

Displaying

Description	Command
Displays the status of the function of denying land attacks.	**showipdenyland**
Displays the status of the function of denying invalid TCP packets.	**show ip deny invalid-tcp**
Displays the status of the function of denying invalid L4 ports.	**show ip deny invalid-l4port**
Displays the status of all anti-DoS attack functions.	**show ip deny**