QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Security Configuration

Оглавление

1.1. Overview

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

AAA provides the following services in a modular way:

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

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

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

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

AAA has the following advantages:

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

1.2. Applications

Application	Description
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.

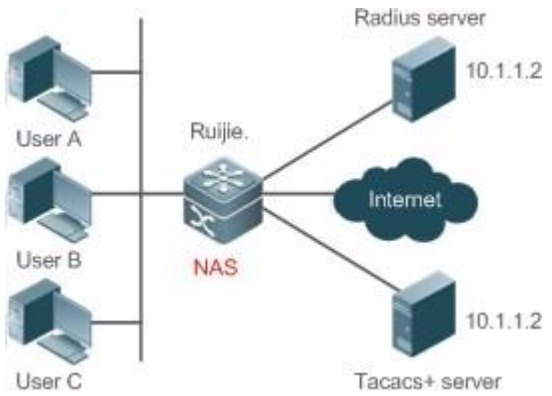
1.2.1. Configuring AAA in a Single-Domain Environment

Scenario

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

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

Figure 1-1



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, and dedicated server software provided by a vendor.** **The TACACS+ server can be the dedicated server software**

	provided by a vendor.

Deployment

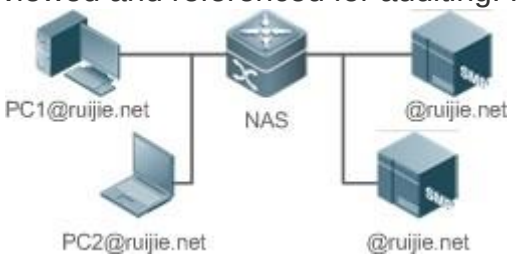
- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Configure the authentication service on the NAS.
- Configure the authorization service on the NAS.
- Configure the accounting service on the NAS.

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@QTECH.net or PC2@QTECH.com.cn and correct password on an 802.1X client.
- Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
- The AAA records of users are stored on servers and can be viewed and referenced for auditing. Figure 1-2



Remarks	**The clients with the usernames PC1@QTECH.net and PC2@QTECH.com.cn 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 QTECH 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 QTECH devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection process continues until a security method responds or all the security methods in the list are tried out. Authentication fails if no method in the list responds.

A method list contains a series of security methods that will be queried in sequence to verify user identities. It allows you to define one or more security protocols used for authentication, so that the standby authentication method takes over services when the active security method fails. On QTECH 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 QTECH devices only when the current method does not respond. When a method denies user access, the authentication process ends without trying other methods.

Figure 1-3

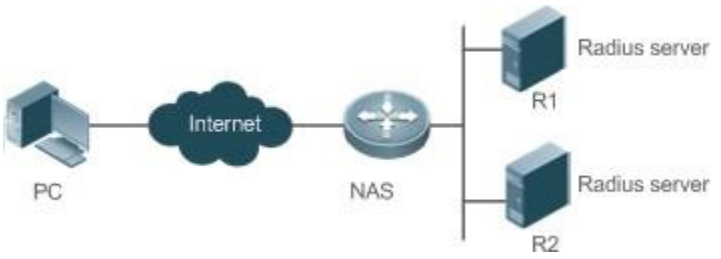


Figure 1-3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

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

The Reject response is different from the Timeout response. The Reject response indicates that the user does not meet the criteria of the available authentication database and therefore fails in authentication, and the Internet access request is denied. The Timeout response indicates that the authentication server fails to respond to the identity query.

When detecting a timeout event, the AAA service proceeds to the next method in the list to continue the authentication process.

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

- **AAA Server Group**

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

- **VRF-Enabled AAA Group**

Virtual private networks (VPNs) enable users to share bandwidths securely on

the backbone networks of Internet service 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 verifies whether users can access the Internet. During authentication, the username, password, and other user information are exchanged between devices to complete users' access or service requests. You can use only the authentication service of AAA.

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

❖ **AAA Authentication Scheme**

- No authentication (**none**)

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

- Local authentication (**local**)

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

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

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

❖ **AAA Authentication Types**

QTECH products support the following authentication types:

- Login authentication

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

- Enable authentication

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

- Point-to-Point Protocol (PPP) authentication

PPP authentication is performed for users that initiate dial-up access through PPP.

- Dot1X (IEEE802.1X) authentication

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

- iPortal (built-in portal) authentication

iPortal authentication is performed by the first generation portal server.

- Web (second generation portal) authentication

Web authentication is performed by the second generation portal server.

- Common authentication

The specified authentication of Dot1X/ iPortal/Web authentication.

Related Configuration

❖ **Enabling AAA**

By default, AAA is disabled.

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

❖ **Configuring an AAA Authentication Scheme**

By default, no AAA authentication scheme is configured.

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

❖ **Configuring an AAA Authentication Method List**

By default, no AAA authentication method list is configured.

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

1.3.2. AAA Authorization

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

❖ **AAA Authorization Scheme**

- Direct authorization (**none**)

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

- Local authorization (**local**)

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

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

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

❖ **AAA Authorization Types**

- EXEC authorization

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

- Config-commands authorization

Users are assigned with the permissions to run specific commands in configuration

modes (including the global configuration mode and sub-modes).

- Console authorization

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

- Command authorization

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

- Network authorization

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

Related Configuration

❖ **Enabling AAA**

By default, AAA is disabled.

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

❖ **Configuring an AAA Authorization Scheme**

By default, no AAA authorization scheme is configured.

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

❖ **Configuring an AAA Authorization Method List**

By default, no AAA authorization method list is configured.

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

1.3.3. AAA Accounting

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

In AAA configuration, accounting scheme configuration is optional.

❖ **AAA Accounting Schemes**

- No accounting (**none**) Accou nting is not performed on users.
- Local accounting (**local**)

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

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

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

❖ **AAA Accounting Types**

- EXEC accounting

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

- Command accounting

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

- Network accounting

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

Related Configuration

❖ **Enabling AAA**

By default, AAA is disabled.

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

❖ **Configuring an AAA Accounting Scheme**

By default, no AAA accounting method is configured.

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

❖ **Configuring an AAA Accounting Method List**

By default, no AAA accounting method list is configured.

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

1.3.4. Multi-Domain AAA

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

Our products support the following username formats:

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

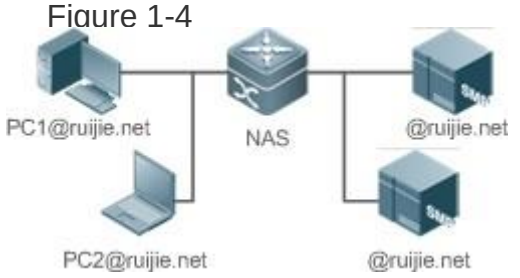
The fourth format (userid) does not contain a domain name, and it is considered to use the **default** domain name. The NAS provides the domain-based AAA service based on the following principles:

- Resolves the domain name carried by a user.
- Searches for the user domain according to the domain name.
- Searches for the corresponding AAA method list name according to the domain configuration information on the NAS.
- Searches for the corresponding method list according to the method list name.
- Provides the AAA services based on the method list.

If any of the preceding procedures fails, the AAA services cannot be provided.

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

Figure 1-4



Related Configuration

❖ **Enabling AAA**

By default, AAA is disabled.

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

- **Configuring an AAA Method List**

By default, no AAA method list is configured.

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

- **Enabling the Domain-Based AAA Service**

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

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

- **Creating a Domain**

By default, no domain is configured.

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

- **Configuring an AV Set for a Domain**

By default, no domain AV set is configured.

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

- **Displaying Domain Configuration**

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

The system supports a maximum of 32 domains.

1.4. Configuration

Configuration	Description and Command	
	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 ist of Enable authentication.

Configuring AAA Authentication	**aaa authentication dot1x**	Defines a method list of 802.1X authentication.
	aaa authentication ppp	Defines a method list of PPP authentication.
	aaa authentication sslvpn	Defines a method list of SSL VPN authentication.
	aaa authentication web-auth	Configures a method list of Web authentication.
	aaa authentication iportal	Configures a method list of iPortal Web authentication.
	aaa local authentication attempts	Sets the maximum number of login attempts.
	aaa local authentication lockout-time	Sets the maximum lockout time after a login failure.
Configuring AAA 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	Definesa methodlist of command authorization.
	aaa authorization network	Configures a method list of network authorization.
	authorization exec	Applies EXEC authorization methods to a 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 network 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 list of command accounting.
	aaa accounting network	Defines a method list of network accounting.
	accounting exec	Applies EXEC accounting methods to a 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 interval.
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 group.
	server	Adds an AAA server group member.
	ip vrf forwarding	Configures the VRF attribute of an AAA server group.

Configuring the Domain-Based AAA Service	Mandatory if AAA management of 802.1X access STAs needs to be performed according to domains.	
	aaa new-model	Enables AAA.
	aaa domain enable	Enables the domain-based AAA service.
	aaa domain	Creates a domain and enters domain configuration mode.
	authentication dot1x	Associates the domain with an 802.1X authentication method list.
	accounting network	Associates the domain with a network accounting method list.
	authorization network	Associates the domain with a network authorization method list.
	state	Configures the domain status.
	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 to the configured sequence.
- When the **none** method is used, users can get access even when no authentication method gets response. Therefore, the **none** method is used only as standby.

Normally, do not use None authentication. You can use the **none** method as the last optional authentication method in special cases. For example, all the users who may request access are trusted users and the users' work must not be

delayed by system faults. Then you can use the **none** method to assign access permissions to these users when the authentication server does not respond. It is recommended that the local authentication method be added before the **none** method.

- If AAA authentication is enabled but no authentication method is configured and the default authentication method does not exist, users can directly log in to the Console without being authenticated. If users log in by other means, the users must pass local authentication.
- When a user enters the CLI after passing login authentication (the **none** method is not used), the username is recorded. When the user performs Enable authentication, the user is not prompted to enter the username again, because the username that the user entered during login authentication is automatically filled in. However, the user must enter the password previously used for login authentication.
- The username is not recorded if the user does not perform login authentication when entering the CLI or the **none** method is used during login authentication. Then, a user is required to enter the username each time when performing Enable authentication.

Configuration Steps

❖ **Enabling AAA**

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

❖ **Defining a Method List of Login Authentication**

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

❖ **Defining a Method List of Enable Authentication**

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

❖ **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 authentication method list (including the configuration of the default method list).
- By default, no method list of 802.1X authentication is configured.

❖ **Defining a Method List of PPP Authentication**

- Run the **aaa authentication ppp** command to configure a method list of PPP authentication.
- This configuration is mandatory if you need to configure an authentication method list for PPP dial-up access.
- By default, no method list of PPP authentication is configured.

❖ **Defining a Method List of Web Authentication**

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

❖ **Defining a Method List of iPortal Web Authentication**

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

❖ **Defining a Method List of SSL VPN Authentication**

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

❖ **Setting the Maximum Number of Login Attempts**

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

❖ **Setting the Maximum Lockout Time After a Login Failure**

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

Verification

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

Related Commands

❖ **Enabling AAA**

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 can be 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**, **group**, and **subs**. 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 and TACACS+ server groups are supported. **subs**: Indicates that the subs database is used for authentication.

Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform login authentication 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 require login 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 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 and TACACS+ 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 authentication 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 server group is 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.

❖ Defining a Method List of PPP, Web, iPortal or SSL VPN Authentication

Command	**aaa authentication { ppp | web-auth | iportal | sslvpn} { default | *list-name* } *method1* [*method2*...]**
Parameter Description	**ppp:** Configures a method list of PPP authentication. **web-auth**: Configures a method list of Web authentication. **iportal**: Configures a method list of iportal authentication. **sslvpn**: Configures a method list of SSL VPN authentication. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a PPP authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. 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 server group is supported. subs: Specifies the SUBS authentication method using the SUBS

	database.
Command Mode	Global configuration mode
Usage Guide	If the AAA PPP authentication service is enabled on the NAS, users must perform PPP authentication negotiation through AAA. Run the **aaa authentication ppp** command to configure the default or optional method lists for PPP 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 up to the specified times. The value ranges from 1 to 43200, 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 needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be
	implemented. (This example requires the configuration of a RADIUS server and local database information.) Step 3: Configure an AAA authentication method list for login authentication users. (This example uses group *radius* and local in order.) Step 4: Apply the configured method list to an interface or line. Skip this step if the default authentication method is used.

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

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

NAS	`QTECH#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 needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. Configure Enable authentication passwords on the NAS if you use Enable password authentication. 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	QTECH#configure terminal QTECH(config)#username user privilege 15 password pass QTECH(config)#enable secret w QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key QTECH QTECH(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	QTECH#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 level is updated to level 15. The user must enter
	the correct username and password to access the NAS.
NAS	`QTECH>enable Username:user Password:pass` `QTECH#`

❖ 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 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.) Currently, 802.1X authentication does not support TACACS+. Step 3: Configure an AAA authentication method list for 802.1X authentication users. (This example uses **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	`QTECH#configure terminal QTECH(config)#username user1 password pass1 QTECH(config)#username user2 password pass2 QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key QTECH`
	`QTECH(config)#aaa authentication dot1x default group radius local QTECH(config)#interface gigabitEthernet 0/1`
	`QTECH(config-if-gigabitEthernet 0/1)#dot1 port-control auto`
	`QTECH(config-if-gigabitEthernet 0/1)#exit`

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

	Authentication method-list: aaa authentication dot1x default group radius local Accounting method-list: Authorization method-list:

Commonrrors

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

1.4.2. Configuring AAA Authorization

Configuration Effect

- Determine what services or permissions authenticated users can enjoy.

Notes

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

Configuration Steps

❖ **Enabling AAA**

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

❖ **Defining a Method List of EXEC Authorization**

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

authorization.

- This configuration is mandatory if you need to configure an EXEC authorization method list (including the configuration of the default method list).
- By default, no EXEC authorization method list is configured.

The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)

❖ **Defining a Method List of Command Authorization**

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

❖ **Configuring a Method List of Network Authorization**

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

❖ **Applying EXEC Authorization Methods to a Specified VTY Line**

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

❖ **Applying Command Authorization Methods to a Specified VTY Line**

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

❖ **Enabling Authorization for Commands in Configuration Modes**

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

❖ **Enabling Authorization for the Console to Run Commands**

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

Verification

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

Related Commands

❖ **Enabling AAA**

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 can be 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 OS supports authorization of the users who log in to the CLI of the NAS to assign the users CLI operation permission levels (0 to 15). Currently, EXEC authorization is performed only on the users who have passed login authentication. If a user fails in EXEC authorization, the user cannot enter the CLI. After you configure EXEC authorization methods, apply the methods to the VTY lines that require EXEC 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+ server group is supported.
Command Mode	Global configuration mode
Usage Guide	The OS 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 lines that require 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. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The OS supports authorization of network-related service requests such as PPP and SLIP requests. After authorization is configured, all authenticated users or interfaces are authorized automatically. You can configure three different authorization methods. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried. RADIUS or TACACS+ servers return a series of AV pairs to authorize authenticated users. Network authorization is based on authentication. Only authenticated users can perform network authorization.

❖ 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 OS can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Example

❖ Configuring AAA EXEC Authorization

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

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, configure the local user database 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 authorization method is used. EXEC authorization is often used with login authentication, which can be implemented on the same line.

NAS	QTECH#configure terminal QTECH(config)#username user password pass QTECH(config)#username user privilege 6 QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key test QTECH(config)#aaa authentication login list1 group local QTECH(config)#aaa authorization exec list2 group radius local
	QTECH(config)#line vty 0 4 QTECH(config-line)#login authentication list1 QTECH(config- line)# authorization exec list2 QTECH(config-line)#exit
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.

NAS	QTECH#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 QTECH# 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 level-15 commands first by using a TACACS+ server. If the TACACS+ server does not respond, local authorization is performed. Authorization is applied to the users who log in through the Console and the users who log in through other types of clients.

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, configure the local user database 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 authorization method is used.
NAS	QTECH#configure terminal QTECH(config)#username user1 password pass1 QTECH(config)#username user1 privilege 15 QTECH(config)#aaa new-model QTECH(config)#tacacs-server host 192.168.217.10 QTECH(config)#tacacs-server key aaa QTECH(config)#aaa authentication login default local QTECH(config)#aaa authorization commands 15 default group tacacs+ local QTECH(config)#aaa authorization console
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	QTECH#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

❖ 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, configure the local user database 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

	authorization method is used.
NAS	QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key test QTECH(config)#aaa authorization network default group radius none QTECH(config)# end
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	QTECH#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 receive response. If accounting fails using a method, the next method will be

not tried.

- After the default accounting method list is configured, it is applied to all VTY lines automatically. If a non-default accounting method list is applied to a line, it will replace the default one. If you apply an undefined method list to a line, the system will display a message indicating that accounting on this line is ineffective. Accounting will take effect only when a defined method list is applied.

EXEC accounting:

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

Command accounting

- Only the TACACS+ protocol supports command accounting.

Configuration Steps

❖ **Enabling AAA**

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

❖ **Defining a Method List of EXEC Accounting**

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

❖ **Defining a Method List of Command Accounting**

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

- **Defining a Method List of Network Accounting**
  - Run the **aaa accounting network** command to configure a method list of network accounting.
  - This configuration is mandatory if you need to configure a network accounting method list (including the configuration of the default method list).
  - By default, no network accounting method list is configured.
- **Applying EXEC Accounting Methods to a Specified VTY Line**
  - Run the **accounting exec** command in line configuration mode to apply EXEC accounting methods to a specified VTY line.
  - This configuration is mandatory if you need to apply an EXEC accounting method list to a specified VTY line.
  - You do not need to run this command if you apply the default method list.
  - By default, all VTY lines are associated with the default accounting method list.
- **Applying Command Accounting Methods to a Specified VTY Line**
  - Run the **accounting commands** command in line configuration mode to apply command accounting methods to a specified VTY line.
  - This configuration is mandatory if you need to apply a command accounting method list to a specified VTY line.
  - You do not need to run this command if you apply the default method list.
  - By default, all VTY lines are associated with the default accounting method list.
- **Applying 802.1X Network Accounting Methods**
  - Run the **dot1x accounting network** command to configure 802.1X network accounting methods.
  - This configuration is mandatory if you need to specify 802.1X network accounting methods.
  - You do not need to run this command if you apply the default method list.
  - By default, all VTY lines are associated with the default accounting method list.
- **Enabling Accounting Update**
  - Optional.
  - It is recommended that accounting update be configured for improved accounting accuracy.
  - By default, accounting update is disabled.
- **Configuring the Accounting Update Interval**

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

Verification

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

Related Commands

❖ **Enabling AAA**

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 can be 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 OS 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 require EXEC 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 related information 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 TACACS+ server group is supported.
Command Mode	Global configuration mode
Usage Guide	The OS 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 VTY lines that require 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-accounting message indicates that the user is allowed to access the network, regardless of whether accounting is 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 OS sends record attributes to the authentication server to perform accounting of user activities. 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 in 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 default accounting method is used.

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

Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	`QTECH#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:
	QTECH# 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 method. Login authentication is performed in local mode, and command accounting is performed on a TACACS+ server.

Scenario Figure 1-12	
Configuration	Step 1: Enable AAA.
Steps	If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in 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 default accounting method is used.

NAS	QTECH#configure terminal QTECH(config)#username user1 password pass1 QTECH(config)#username user1 privilege 15 QTECH(config)#aaa new-model QTECH(config)#tacacs-server host 192.168.217.10 QTECH(config)#tacacs-server key aaa QTECH(config)#aaa authentication login default local QTECH(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	QTECH#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: QTECH#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, configure a RADIUS server in 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	QTECH#configure terminal QTECH(config)#username user password pass QTECH(config)#aaa new-model QTECH(config)#radius- server host 10.1.1.1 QTECH(config)#radius-server key test QTECH(config)#aaa authentication dot1x aut1x group radius local QTECH(config)#aaa accounting network acc1x start- stop group radius QTECH(config)#dot1x authentication aut1x QTECH(config)#dot1x accounting acc1x QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#dot1 port-control auto QTECH(config-if-GigabitEthernet 0/1)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	QTECH#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 after the server group name so that the servers in the group are used to handle authentication, authorization, and accounting requests.
- Use self-defined server groups to separate authentication, authorization, and accounting.

Notes

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

Configuration Steps

❖ **Creating a User-Defined AAA Server Group**

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

❖ **Adding an AAA Server Group Member**

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

❖ **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 name must not contain 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 server 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

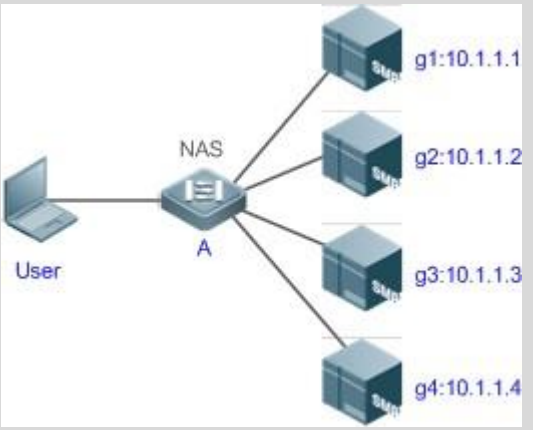
Command	**ip vrf forwarding *vrf_name***
Parameter Description	*vrf_name*: Indicates the name of a VRF table.
Command Mode	Server group configuration mode
Usage Guide	Use this command to assign a VRF table to the specified server group.

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	
Prerequisites	1. The required interfaces, IP addresses, and VLANs have been configured on the network, network connections have been set up, and the routes from the NAS to servers are reachable. 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	`QTECH#configure terminal` `QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server host 10.1.1.2`

	`QTECH(config)#radius-server host 10.1.1.3 QTECH(config)#radius-server host 10.1.1.4`
	`QTECH(config)#radius-server key secret QTECH(config)#aaa group server radius g1 QTECH(config-gs-radius)#server 10.1.1.1`
	`QTECH(config-gs-radius)#server 10.1.1.2 QTECH(config-gs-radius)#exit QTECH(config)#aaa group server radius g2`
	`QTECH(config-gs-radius)#server 10.1.1.3 QTECH(config-gs-radius)#server 10.1.1.4`
	`QTECH(config-gs-radius)#exit`

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

NAS	QTECH#show aaa group Type Reference Name radius 1 radius tacacs+ 1 tacacs+ radius 1 g1 radius 1 g2
	QTECH#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 authentication and accounting ports, when you run the **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 system prompts that the configurations do not exist.
- The names of the AAA method lists selected in domain configuration mode must be consistent with those of the method lists defined for the AAA service. If they are inconsistent, the AAA service cannot be properly provided to the users in the domain.

About the default domain:

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

About domain names:

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

Configuration Steps

❖ **Enabling AAA**

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

❖ **Enabling the Domain-Based AAA Service**

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

❖ **Creating a Domain and Entering Domain Configuration Mode**

- Mandatory.
- Run the **aaa domain** command to create a domain or enter the configured domain.

- By default, no domain is configured.

❖ **Associating the Domain with an 802.1X Authentication Method List**

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

❖ **Associating the Domain with a Network Accounting Method List**

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

❖ **Associating the Domain with a Network Authorization Method List**

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

❖ **Configuring the Domain Status**

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

❖ **Configuring Whether to Contain the Domain Name in Usernames**

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

❖ **Configuring the Maximum Number of Domain Users**

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

Verification

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

Related Commands

❖ **Enabling AAA**

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 can be 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 the domain-based AAA service. The **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 the AAA service to the

	user. 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 associated with this domain to provide the AAA service to the user. The system supports a maximum of 32 domains.

❖ Associating the Domain with an 802.1X Authentication Method List

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 Web Authentication Method List

Command	**authentication web-auth { 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 Web 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 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 (username: *user*@domain.com) that access the NAS. The usernames that the NAS sends to the RADIUS server do not carry domain information, and the number of access users is not limited.

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	QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#radius-server host 10.1.1.1 QTECH(config)#radius-server key test QTECH(config)#aaa authentication dot1x default group radius QTECH(config)#aaa accounting network list3 start-stop group radius QTECH(config)# aaa domain enable QTECH(config)# aaa domain domain.com QTECH(config-aaa-domain)# authentication dot1x default QTECH(config-aaa-domain)# accounting network list3
Verification	Run the **show run** and **show aaa domain** command on the NAS to display the configuration.
NAS	QTECH#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

	QTECH#show run Building configuration... Current configuration : 1449 bytes version OS 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 qtech.ru
	authentication dot1x default accounting network list3 ! aaa accounting network list3 start-stop group radius aaa authentication dot1x default group radius ! n f p p ! no service password-encryption ! radius-server host 10.1.1.1 radius- server key test ! lin e con 0 lin e 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

2.1. 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 OS 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 access of remote users. RADIUS is a completely open protocol and the RADIUS server is installed on many operating systems as a component, for example, on UNIX, Windows 2000, and Windows 2008. Therefore, RADIUS is the most widely applied security server currently.

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

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

Protocols and Standards

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

2.2. Applications

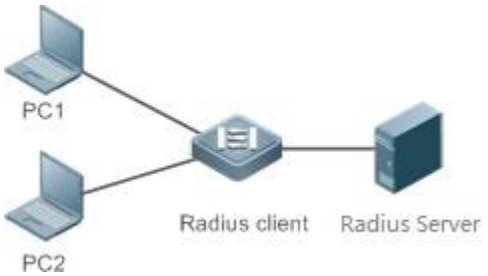
Application	Description
Providing Authentication, Authorization, and Accounting	Authentication, authorization, and accounting are conducted on access users on a network, to prevent unauthorized access or operations.
Services for Access Users	
Forcing Users to Go Offline	The server forces an authenticated user to go offline.

2.2.1. Providing Authentication, Authorization, and Accounting Services for Access Users

Scenario

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

Figure 2-1 Typical RADIUS Networking Topology



Remarks	**PC 1 and PC 2 are connected to the RADIUS client as access users in wired or wireless mode, and initiate authentication and accounting requests.** **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 access devices.

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

2.2.2. Forcing Users to Go Offline

Scenario

The RADIUS server forces authenticated online users to go offline for the sake of management. See Figure 2-1 for the networking topology.

Deployment

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

2.3. Features

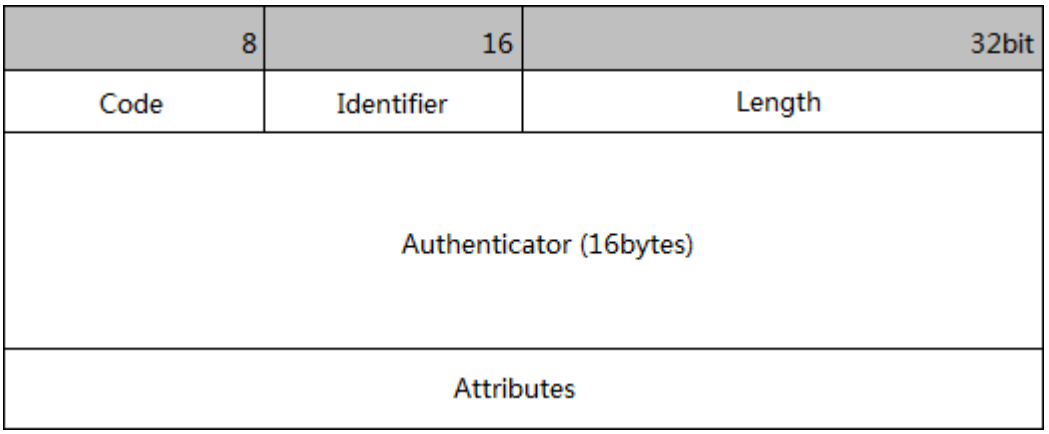
Basic Concepts

❖ **Client/Server Mode**

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

❖ **Structure of RADIUS Packets**

The following figure shows the structure of RADIUS packets.



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

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

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

Attribute No.	Attribute Name	Attribute No.	Attribute Name

1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-	68	Acct-Tunnel-

	Network		Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

- **Shared Key**

A RADIUS client and a RADIUS server mutually confirm their identities by using a

shared key during communication. The shared key cannot be transmitted over a network. In addition, user passwords are encrypted for transmission for the sake of security.

- **RADIUS Server Group**

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

- **RADIUS Attribute Type**

  - Standard attributes

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

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

Format	Description
Ietf	Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 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 the standard RADIUS protocol. Table 1-3 lists private attributes supported by QTECH products. The **TYPE** column indicates the default configuration of private attributes of QTECH products and the **Extended TYPE** column indicates the default configuration of private attributes of other non-QTECH 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

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

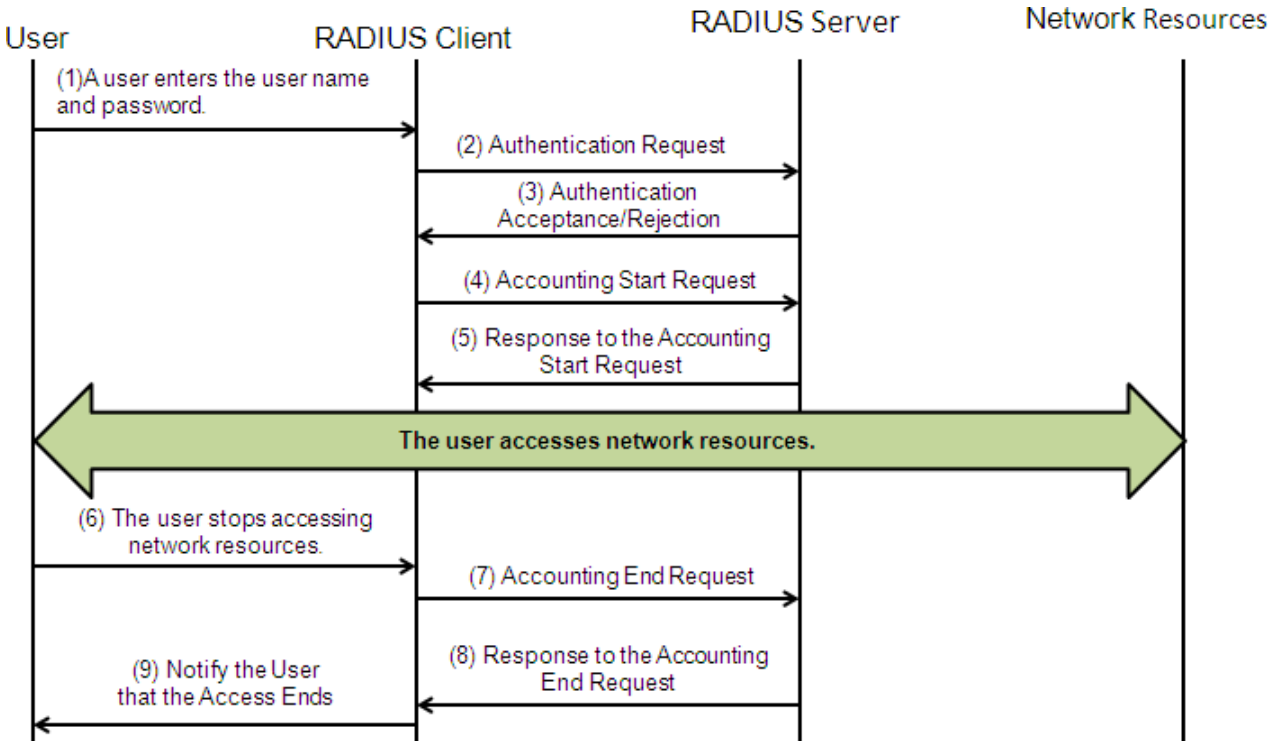
Feature	Description
RADIUS Authentication, Authorization, and Accounting	Conducts identity authentication and accounting on access users, safeguards network security, and facilitates management for network administrators.
Source Address of RADIUS Packets	Specifies the source IP address used by a RADIUS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



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 packet to the 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. When accepting the authentication request, the RADIUS server also issues authorization information apart from the authentication acceptance information. The authorization information varies with the type of access users.

The RADIUS accounting process is described as follows:

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 user types and select **group radius**

when setting the authentication method.

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

- **Configuring the AAA Authorization Method List**

No AAA authorization method list is configured by default.

You can run the **aaa authorization** command to configure an authorization method list for different user types and select

group radius when setting the authorization method.

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

- **Configuring the AAA Accounting Method List**

No AAA accounting method list is configured by default.

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

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

2.3.2. Source Address of RADIUS Packets

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

Working Principle

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

Related Configuration

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

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

2.3.3. RADIUS Timeout Retransmission

Working Principle

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

Related Configuration

- **Configuring the RADIUS Server Timeout Time**

The default timeout time is 5 seconds.

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

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

- **Configuring the Retransmission Count**

The default retransmission count is 3.

You can run the **radius-server retransmit** command to configure the retransmission count. The value ranges from 0 to 100.

- **Configuring Whether to Retransmit Accounting Update Packets**

Accounting update packets are not retransmitted by default.

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

2.3.4. RADIUS Server Accessibility Detection

Working Principle

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

Related Configuration

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

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

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

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

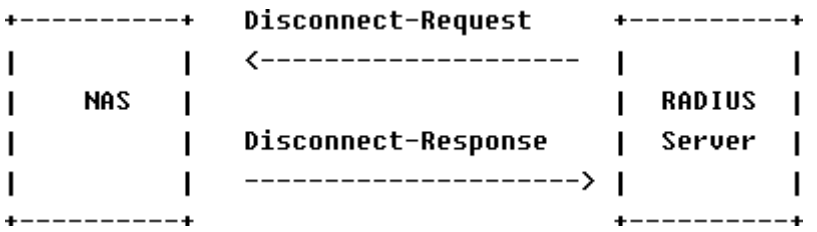
No test user name is specified for actively detecting the RADIUS security server by default.

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

2.3.5. RADIUS Forced Offline

Working Principle

Figure 2-3 DM Message Exchange of the RADIUS Dynamic Authorization Extension Protocol



The preceding figure shows the exchange of DM messages between the RADIUS server and the device. The RADIUS server transmits the Disconnect-Request

message to UDP Port 3799 of the device. After processing, the device returns the Disconnect-Response message that carries the processing result to the RADIUS server.

Related Configuration

N/A

2.4. Configuration

Configuration	Description and Command	
RADIUS Basic Configuration	(Mandatory) It is used to configure RADIUS authentication, authorization, and accounting.	
	radius-server host	Configures the IP address of the remote RADIUS security server.
	radius-server key	Configures the shared key for communication between the device and the RADIUS server.
	radius-server retransmit	Configures the request transmission count, after which the device confirms that a RADIUS server is unreachable.
	radius-server timeout	Configures the waiting time, after which the device retransmits a request.
	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 Attribute Type the RADIUS	(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 RADIUS attribute No. 31 (Calling-Station-ID).
	radius-server attribute class	Configures the parsing mode of the RADIUS Class attribute.
	radius set qos cos	Sets the private attribute port-priority issued by the server to the COS value of an interface. For COS-relevant concepts, see the *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.
	radius-server attribute authentication	Configures whether RADIUS authentication request packets carry a specified attribute.
	radius-server account attribute	Configures whether RADIUS accounting request packets carry a specified attribute.
	radius-server vendor authentication	Configures whether RADIUS authentication request packets carry the private attributes of other vendors.
	radius-server account vendor	Configures whether RADIUS accounting request packets carry the private attributes of other vendors.
Configuring 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 that a RADIUS security server is unreachable.

	radius-server deadtime	Configures the duration for the transmitting request packets to RADIUS server.	device to stop an unreachable
	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 RADIUS Server Is Unreachable

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

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

- Optional.
- Configure the waiting time, after which the device retransmits a request, according to the actual network environment.

  In an 802.1X authentication environment that uses the RADIUS security protocol, if a network device serves as the 802.1X authenticator and QTECH SU is used as the 802.1X client software, it is recommended that **radius-server timeout** be set to 3 seconds (the default value is 5 seconds) and **radius-server retransmit** be set to 2 (the default value is 3) on the network device.

❖ **Configuring Retransmission of Accounting Update Packets for Authenticated Users**

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

❖ **Configuring the Source Address of RADIUS Packets**

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

Verification

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

Related Commands

❖ **Configuring the Remote RADIUS Security Server**

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 packets to the RADIUS 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 routing table when 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 that they can communicate with each other successfully.

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

Command	**radius-server retransmit *retries***
Parameter Description	*retries*: Indicates the RADIUS retransmission count. The value ranges from 0 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 server does not respond are that the security server does not respond within the RADIUS packet retransmission duration of the specified retransmission count. There is an interval between consecutive two retransmissions.

❖ Configuring the Waiting Time, After which the Device Retransmits a Request

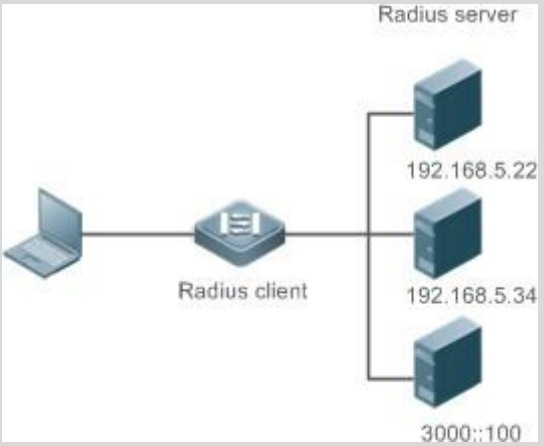
Command	**radius-server timeout *seconds***
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.
Command Mode	Global configuration mode
Usage Guide	Use this command to adjust the packet retransmission timeout time.

❖ 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 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 2-4	
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	`QTECH#configure terminal` `QTECH (config)#aaa new-model`
	`QTECH (config)# radius-server host 192.168.5.22`
	`QTECH (config)#radius-server host 3000::100`

	QTECH (config)# radius-server key aaa
	QTECH (config)#aaa authentication login test group radius
	QTECH (config)#aaa authorizationexectest group radius
	QTECH (config)#aaa accountingexectest start-stop group radius
	QTECH (config)# line vty 0 4
	QTECH (config-line)#login authentication test
	QTECH (config-line)# authorization exec test
	QTECH (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 of the user on the RADIUS server. Perform management operations on the device as the user and then log out. Display the accounting information on the user on the RADIUS server.
	QTECH#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 QTECH private attributes.

Configuration Steps

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

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

❖ **Configuring the Parsing Mode of the RADIUS Class Attribute**

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

❖ **Configuring the RADIUS Private Attribute Type**

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

- **Configuring Whether RADIUS Authentication Request Packets Carry a Specified Attribute**
  - Optional.
  - Configure whether to specify the attribute type for RADIUS authentication request packets as required.
- **Configuring Whether RADIUS Accounting Request Packets Carry a Specified Attribute**
  - Optional.
  - Configure whether to specify the attribute type for RADIUS accounting request packets as required.
- **Configuring Whether RADIUS Authentication Request Packets Carry the Private Attribute of a Specified Vendor**
  - Optional.
  - Configure whether RADIUS authentication request packets carry the private attribute of a specified vendor as required.
- **Configuring Whether RADIUS Accounting Request Packets Carry the Private Attribute of a Specified Vendor**
  - Optional.
  - Configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.
- **Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft**
  - Optional.
  - Configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.
- **Configuring the Nas-Port-Id Encapsulation Format for RADIUS Packets**
  - Optional.
  - In either QINQ or non-QINQ scenarios, configure the nas-nort-id encapsulation format for RADIUS packets. By default, the packets are encapsulated in the normal format.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to display the MAC address format of Calling-Station-Id.

- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that QTECH private attributes are correctly parsed by the device.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that the CUI attribute is correctly parsed by the device.

Related Commands

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

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 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.
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 Parsing Mode of the RADIUS Class Attribute

Command	**radius-server attribute class user-flow-control { format-16bytes | format-32bytes }**
Parameter Description	**user-flow-control:** Parses the rate limit configuration from the class attribute. **format-16bytes:** Sets the format of the rate limit value to 16 bytes in the **class** attribute. **format-32bytes:** Sets the format of the rate limit value to 32 bytes in the **class** attribute.
Command Mode	Global configuration mode

Usage Guide	Configure this command if the server needs to issue the rate limit value by using the Class attribute.

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

Command	**radius set qos cos**
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 as the 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.

❖ Configuring Whether RADIUS Authentication Request Packets Carry a Specified Attribute

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

❖ Configuring Whether RADIUS Accounting Request Packets Carry a Specified Attribute

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

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

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

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

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

❖ Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft

Command	**radius vendor-specific attribute support *vendor_name***
Parameter Description	*vendor_name*: Indicates the vendor name. It can be set to cisco, huawei or ms.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

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. ▪ Configure authentication requests not to carry the NAS-PORT-ID attribute. ▪ Configure accounting requests to carry the CMCC private attribute.

	▪ Configure the RAIUDS server not to parse Cisoc's private attributes contained in packets. ▪ Configure application of the nas-port-id encapsulation format in a QINQ scenario.
	QTECH(config)#radius-server attribute 31 mac format ietf QTECH(config)#radius set qos cos QTECH(config)#radiussupport cui QTECH(config)# radius vendor-specific extend QTECH(config)# radius-server authentication attribute 87 unpackage QTECH(config)# radius-server account vendor cmcc package QTECH(config)# no radius vendor-specific attribute support cisco
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 the active detection function is enabled for a specified RADIUS server, the device will, according to the configuration, periodically transmits detection requests (authentication requests or accounting requests) to the RADIUS server. The transmission interval is as follows:

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

Notes

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

- The test user name of the RADIUS server is configured on the device.
- At least one tested port (authentication port or accounting port) of the RADIUS server is configured on the device. If the following two conditions are all met, it is deemed that a reachable RADIUS server becomes unreachable:
- After the previous correct response is received from the RADIUS server, the time set in **radius-server dead-criteria time** *seconds* has elapsed.

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

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

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

Configuration Steps

❖ **Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable**

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

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

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

❖ **Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server**

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

Verification

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

Related Commands

❖ **Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable**

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 request packets transmitted by the device to the same RADIUS security server reaches the preset count, it is deemed that the RADIUS security server meets the consecutive timeout count condition of inaccessibility. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	If a RADIUS security server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS security server is unreachable. Users can use this command to adjust parameter values in the duration condition and consecutive request timeout count condition.

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

Command	**Radius-server deadtime *minutes***
Parameter Description	*minutes*: Indicates the duration for the device to stop transmitting requests to an unreachable RADIUS security server, with the unit of minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).
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 function is disabled for a RADIUS security server, the device automatically restores the RADIUS security server to the reachable state when the duration that the RADIUS security server is in the unreachable state exceeds the time specified in **radius-server deadtime**.

Configuration Example

❖ Configuring Accessibility Detection on the RADIUS Server

Scenario Figure 2-5	
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	`QTECH(config)#radius-server dead-criteria time120 tries 5`
	
	`QTECH(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90`

Verification	Disconnect the network communication between the device and the server with the IP address of 192.168.5.22.Conduct RADIUS authentication through the device. After 120 seconds, run the **show radius server** command to check that the server state is **dead**.

	`QTECH#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 relevant to the RADIUS dynamic authorization extension function.	**show radius dynamic-authorization-extension statistics**
Displays statistics relevant to RADIUS authentication.	**show radius auth statistics**
Displays statistics relevant to RADIUS accounting.	**show radius acct statistics**
Displays configuration of RADIUS server groups.	**show radius group**
Displays RADIUS standard attributes.	**show radius attribute**

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 radiusextension event**

Debugs the RADIUS dynamic authorization extension packet printing.	**debug radius extension detail**

3.1. Overview

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

Protocols and Standards

- RFC 1492 Terminal Access Controller Access Control System

3.1.1. Applications

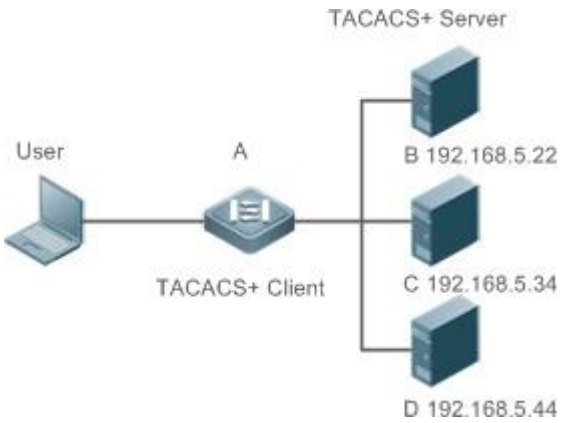
Application	Description
Managing and Controlling Login of End Users	Password verification and authorization need to be conducted on end users.

3.1.2. Managing and Controlling Login of End Users

Scenario

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

Figure 3-1



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

3.2. Features

Basic Concepts

❖ **Format of TACACS+ Packets**

Figure 3-2

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

- Major Version: Indicates the major TACACS+ version number.
- Minor Version: Indicates the minor TACACS+ version number.
- Packet Type: Indicates the type of packets, with the options including: TAC_PLUS_AUTHEN: = 0x01 (authentication); TAC_PLUS_AUTHOR: = 0x02 (authorization); TAC_PLUS_ACCT: = 0x03 (accounting)
- Sequence Number: Indicates the sequence number of a data packet in the current session. The sequence number of the first TACACS+ data packet in a session must be 1 and the sequence number of subsequent each data packet increases by one. Therefore, the client sends data packets only with an odd sequence number and TACACS+ Daemon sends packets only with an even sequence number.
- Flags: Contains various bitmap format flags. One of the bits in the value

specifies whether data packets need to be encrypted.

- Session ID: Indicates the ID of a TACACS+ session.
- Length: Indicates the body length of a TACACS+ data packet (excluding the header). Packets are encrypted for transmission on a network.

Overview

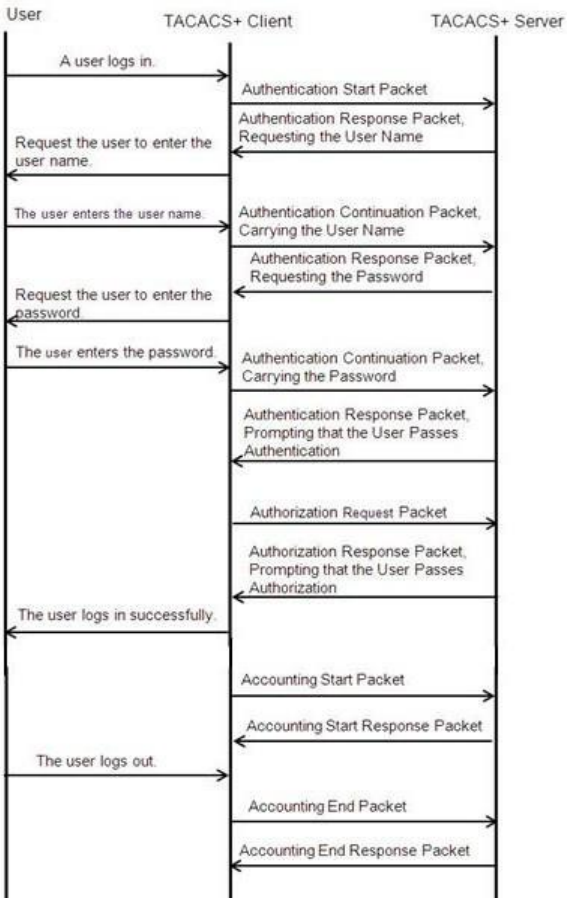
Feature	Description
TACACS+ Authentication, Authorization, and Accounting	Conducts authentication, authorization, and accounting on end users.

3.2.1. TACACS+ Authentication, Authorization, and Accounting

Working Principle

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

Figure 3-3



The entire basic message interaction process includes three sections:

1. The authentication process is described as follows:

1) A user requests to log in to a network device.

2) After receiving the request, the TACACS+ client sends an authentication start packet to the TACACS+ server.

3) The TACACS+ server returns an authentication response packet, requesting the user name.

4) The TACACS+ client requests the user to enter the user name.

5) The user enters the login user name.

6) After receiving the user name, the TACACS+ client sends an authentication continuation packet that carries the user name to the TACACS+ server.

7) The TACACS+ server returns an authentication response packet, requesting the login password.

8) The TACACS+ client requests the user to enter the login password.

9) The user enters the login password.

10) After receiving the login password, the TACACS+ client sends an authentication continuation packet that carries the login password to the TACACS+ server.

11) The TACACS+ server returns an authentication response packet, prompting that the user passes authentication.

2. The user authorization starts after successful authentication:

1) The TACACS+ client sends an authorization request packet to the TACACS+ server.

2) The TACACS+ server returns an authorization response packet, prompting that the user passes authorization.

3) After receiving the authorization success packet, the TACACS+ client outputs the network device configuration screen for the user.

3. Accounting and audit need to be conducted on the login user after successful authorization:

1) The TACACS+ client sends an accounting start packet to the TACACS+ server.

2) The TACACS+ server returns an accounting response packet, prompting that the accounting start packet has been received.

3) The user logs out.

4) The TACACS+ client sends an accounting end packet to the TACACS+ server.

5) The TACACS+ server returns an accounting response packet, prompting that the accounting end packet has been received.

3.3. 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.
	tacacs-server timeout	Configures the global waiting timeout time of the TACACS+ server for communication between a network device and the TACACS+ server.
Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+	(Optional) It is used to separately process authentication, authorization, and accounting requests.	
		Configures TACACS+ server groups and
	aaa group server tacacs+	divides TACACS+ servers into different groups.
	server	Adds servers to TACACS+ server groups.

3.3.1. Configuring TACACS+ Basic Functions

Configuration Effect

- The TACACS+ basic functions are available after the configuration is complete. When configuring the AAA method list, specify the method of using TACACS+ to implement TACACS+ authentication, authorization, and

accounting.

- When authentication, authorization, and accounting operations are performed, TACACS+ initiates the authentication, authorization, and accounting requests to configured TACACS+ servers according to the configured sequence. If response timeout occurs on a TACACS+ server, TACACS+ traverses the TACACS+ server list in sequence.

Notes

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

Configuration Steps

❖ **Enabling AAA**

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

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* | *ipv6-address*} [port *integer*] [timeout *integer*] [key [0 | 7] *text-string*]**

Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. *ipv6-address*: Indicates the IPv6 address of the TACACS+ server. **oob**: Uses an MGMT port as the source interface for communicating with the TACACS+ server. A non-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 global 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 server. If no 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 Mode	Global configuration mode
Usage Guide	This command is used to configure a global shared key for servers. To specify a different key for each 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 1,000 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 users by using TACACS+.

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

Configuration Example

❖ **Using TACACS+ for Login Authentication**

Scenario Figure 3-4	
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	`QTECH# configure terminal QTECH(config)# aaa new-model`
	`QTECH(config)# tacacs-server host 192.168.5.22 QTECH(config)# tacacs-server key aaa`
	`QTECH(config)# aaa authentication login test group tacacs+ QTECH(config)# line vty 0 4`
	`QTECH(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 user on the 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.

3.3.2. Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+

Configuration Effect

- The authentication, authorization, and accounting in the security service are

processed by different TACACS+ servers, which improves security and achieves load balancing to a certain extent.

Notes

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

Configuration Steps

❖ **Configuring TACACS+ Server Groups**

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

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 are the 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 different server groups.

❖ **Adding Servers to TACACS+ Server Groups**

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

Command	**server {*ipv4-address* | *ipv6-address*}**
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. *ipv6-address*: Indicates the IPv6 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 through a 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 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 VRF configured in a TACACS+ server group, a valid name must be configured for VRF by using the **vrf** definition command in global configuration mode.

❖ **Configuring oob of a TACACS+ Server Group**

- Optional. Configure oob if a device needs to send TACACS+ packets through a specified MGMT port.
- In server group configuration mode, specify routing for the communication of servers in the group.

Command	**ip oob** **ip oob via *mgmt.-name*** **ip vrf forwarding *vrf-name***
Parameter Description	**ip oob**: Indicates the MGMT0 port. *mgmt.-name*: Name of management port. vrf-name: Indicates the VRF name.
Defaults	No oob is specified by default.
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. If no MGMT port is specified, the MGMT0 port is used by default.

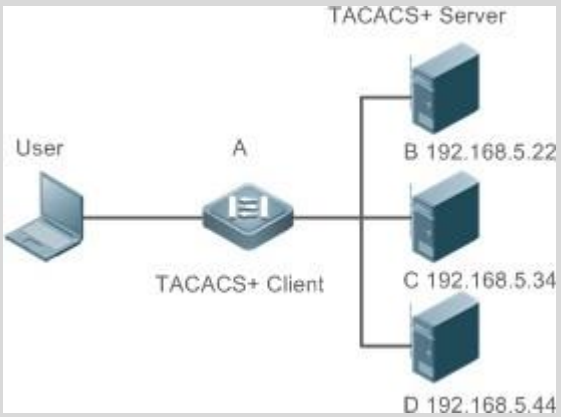
Verification

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

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

Configuration Example

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

Scenario **Figure 3-5**	
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.
	QTECH# configure terminal QTECH(QTECH(config)# aaa new-model QTECH(config)# tacacs-server host 192.168.5.22 QTECH(config)# tacacs-server host 192.168.5.34 QTECH(config)# tacacs-server host 192.168.5.44 QTECH(config)# tacacs-server key aaa QTECH(config)# aaa group server tacacs+ tacgrp1 QTECH(config-gs-tacacs)# server 192.168.5.22 QTECH(config-gs-tacacs)# exit QTECH(config)# aaa group server tacacs+ tacgrp2 QTECH(config-gs-tacacs)# server 192.168.5.34 QTECH(config-gs-tacacs)# exit QTECH(config)# aaa group server tacacs+ tacgrp3 QTECH(config-gs-tacacs)# server 192.168.5.44 QTECH(config-gs-tacacs)# exit QTECH(config)# aaa authentication login test1 group tacacs+ QTECH(config)# aaa authentication enable default group tacgrp1 QTECH(config)# aaa authorization exec test2 group tacgrp2 QTECH(config)# aaa accounting commands 15 test3 start-stop group tacgrp3 QTECH(config)# line vty 0 4 QTECH(config-line)# login authentication test1 QTECH(config-line)#authorization exec test2 QTECH(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 passing the 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.

3.4. 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+**

4.1. 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.

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.

802.1X can be deployed in a network to realize user authentication, authorization and other functions.

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, 802.1X authentication is deployed on access switches.

4.2.1 Wired 802.1X Authentication

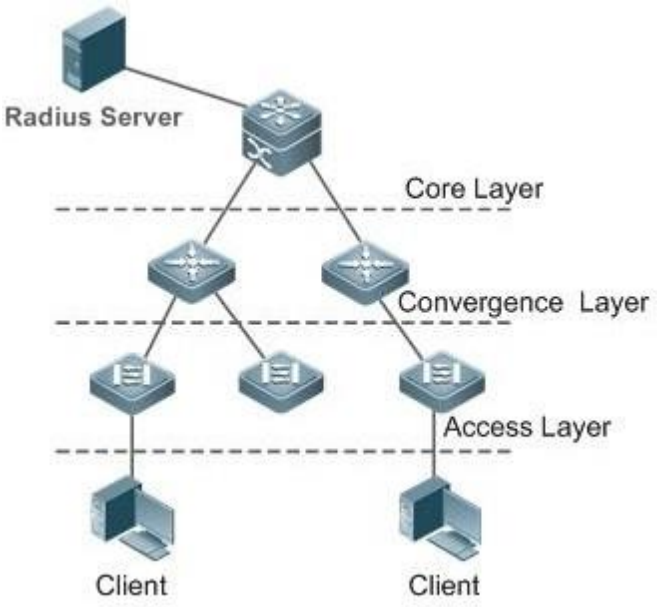
Scenario

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

accessing the campus network.

As shown in Figure 4-1:

- User ends must be installed with 802.1X clients (which can come with the operating system, or others like QTECH Supplicant).
- Access switches support 802.1X.
- One or multiple Remote Authentication Dial-In User Service (RADIUS) servers perform authentication. Figure 4-1



Remarks	**The supplicant software installed on the user ends (or software coming with the operating system) performs 802.1X authentication. 802.1X authentication is deployed on access switches, convergence switches, or core 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. Only authenticated users on one port can access the network.
- Configure an AAA authentication method list so that 802.1X can adopt the appropriate method and authentication server.
- Configure RADIUS parameters to ensure proper communication between a switch and the RADIUS server. For details, see the *Configuring RDS*.
- If a QTECH RADIUS server is used, configure SNMP parameters to allow the

RADIUS server to manage devices, such as querying and setting.

- Configure the port between the access switch and the RADIUS server as an uncontrolled port to ensure proper communication between them.
- Create an account on the RADIUS server, register the IP address of an access switch, and configure RADIUS-related parameters. Only in this case, can the RADIUS server respond to the requests of the switch.

4.2.2 MAB Auto Authentication

Scenario

MAC address bypass (MAB) auto authentication indicates that MAB authentication is performed together with Web authentication. In the original wireless Web authentication scenario, it is complained that the ease-to-use performance of Web authentication is poor. During each Web authentication, a user needs to associate the STA with an SSID, open the browser, and enter the user name and password. In addition, if the STA drops out of the network, the STA cannot automatically access the network again. To ensure that all Web authenticated STAs are always online and access the network imperceptibly, MAB auto authentication is proposed. After a STA passes Web authentication, the STA can access the network again imperceptibly without Web authentication.

As shown in Figure 4-1:

- Only the browser is mandatory on the client.
- The AC supports Web authentication and MAB authentication.
- One or multiple RADIUS servers provide authentication. In addition, the authentication server supports the authentication mode of using the MAC address as the user name and password.

Remarks	**Wireless MAB authentication is triggered by a STA advertisement. When a STA is already online, MAB authentication will not be triggered again. If MAB authentication fails, it can be triggered again only after the STA goes offline and reconnects to the network.**

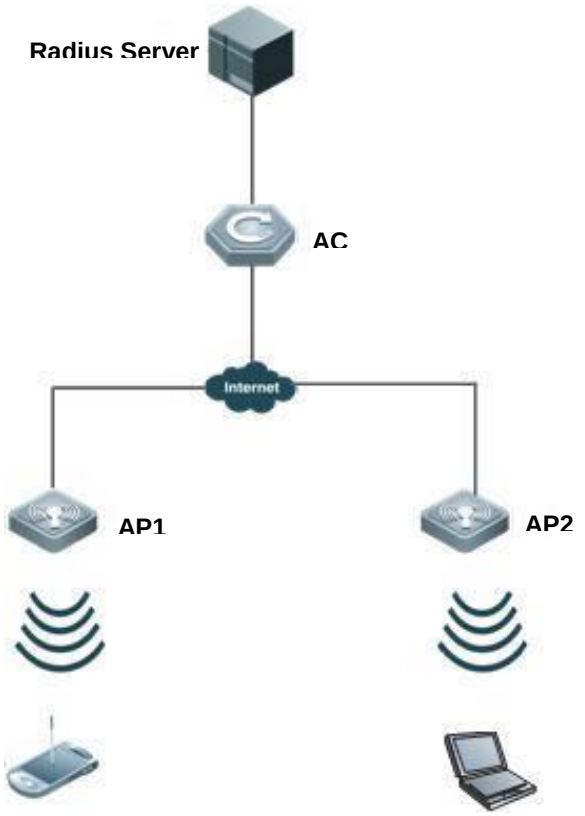


Figure 4-2

Deployment

- Enable Web authentication, DOT1X authentication, and MAB authentication on the interface of the AC. MAB authentication can be performed only after DOT1X authentication is enabled. (For details about MAB authentication, see section 0 "Common Errors
- The MAC account format is incorrect on the authentication server.
- Configuring MAB Auto Authentication". For details about Web authentication, see the WEB-AUTH-SCG document.)
- Configure an AAA authentication method list, so that a correct method and authentication server can be used for MAB/Web authentication. (For details about the AAA authentication method list configuration, see the AAA-SCG document.)
- Configure RADIUS parameters to ensure proper communication between the AC and the RADIUS server. In addition, configure the RADIUS server to support the authentication mode of using the MAC address as the user name and password. For details about the RADIUS configuration, see the corresponding configuration guide.
- If a QTECH RADIUS server is used, configure SNMP parameters to allow the RADIUS server to perform operations such as querying and setting on the

AP.

- Create an account on the RADIUS server, register the IP address of the AC, and configure RADIUS-related parameters. The RADIUS server can respond to the requests of the AP and AC only after the foregoing settings are completed.

4.3 Features

Basic Concepts

❖ User

In wired environment, 802.1X is a LAN-based protocol. It identifies users based on physical information but not accounts. In a LAN, a user is 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 practice. Using this protocol, the 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 the time specified by 802.1X, authentication will fail. 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 password for authentication. Since QTECH 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. Defined in RFC3748, EAP provides a universal authentication framework, in which multiple authentication modes are embedded, including Message Digest Algorithm 5 (MD5), Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), and Transport Layer Security (TLS). QTECH 802.1X authentication supports various modes including MD5, CHAP, PAP, PEAP-MSCHAP, and TLS.

❖ **Authorization**

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

- **Accounting**

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

Some RADIUS servers such as RG-SAM\RG-SMP 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 network. Users must pass authentication to obtain the network access permission. They can access the network only after the authentication server verifies the account. Before user authentication succeeds, only EAPOL packets (Extensible Authentication Protocol over LAN, 802.1X packets) can be transmitted over the network for authentication.

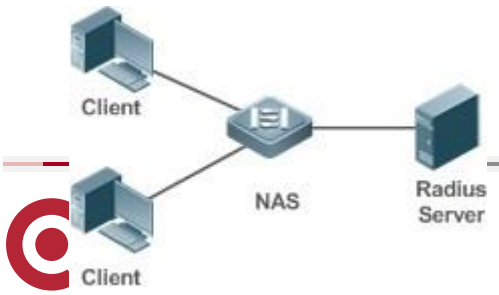
Working Principle

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 4-3



- Supplicant

The supplicant is the role of end users, usually a PC. It requests to access network services and replies to the request 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, QTECH has launched a QTECH 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 connection of a client based on the client's authentication status. As a proxy between the client and the authentication server, the 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 RADIUS Client. It 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 controlled ports can access network resources only when authenticated. Users connected to uncontrolled ports can directly access network 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

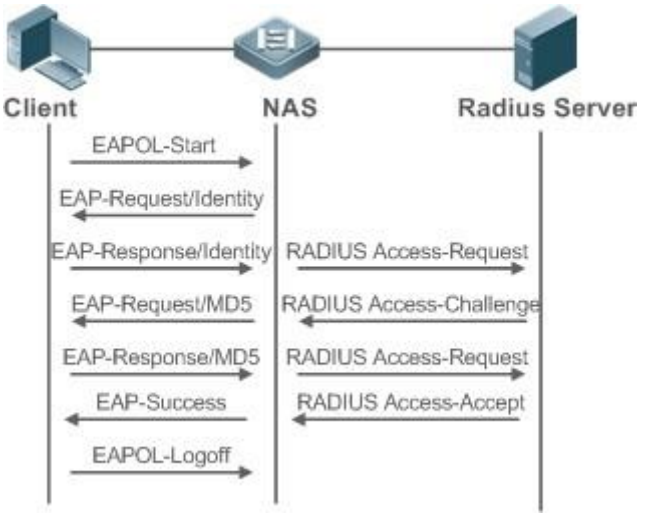
The authenticator server is usually an RADIUS server. It cooperates with the authenticator to provide authentication service for users. The authentication server saves the user names, passwords, and related authorization information. One server can provides authentication service for multiple authenticators to achieve centralized user management. The authentication server also manages accounting data received from authenticators. QTECH 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 while exchanges information with the 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. QTECH Supplicant may also use 01-D0-F8-00-00-03 to for initial authentication packets.

Figure 4-4 shows the typical

authentication process of a wired user.
Figure 4-4



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 authentication status of the port. QTECH products extend the 802.1X and realizes access control based on users ((identify a wired user by the MAC address and VLAN ID while an STA by the MAC address) by default. QTECH 802.1X can also be enabled in interface configuration mode. For details, see the chapter "Configuration."

All users on an uncontrolled port can access network resources, while users on a controlled port can access network resources only after authorized. When a user initiates authentication, its status remains Unauthorized and cannot access the network yet. After it passes authentication, its status changes to Authorized and can access network 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 Unauthorized 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 and directly accesses network 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 authorized.

If a user passes authentication (that is, the NAS receives a success packet from the RADIUS server), the user becomes Authorized and can freely access network resources. If the user fails in authentication, it remains Unauthorized and re-initiates authentication. If the communication between the NAS and the RADIUS

server fails, the user remains Unauthorized and cannot access network resources.

When a user sends an EAPOL-LOGOFF packet, the user's status changes from Authorized to Unauthorized. When a port of the NAS goes down, all users on this port will become Unauthorized.
When the NAS restarts, all users on it become Unauthorized.

- **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 RG-SAM/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 method 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 QTECH 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 Graphical User Interfaces (GUIs). It is recommended to use QTECH Supplicant as the authentication client. If other software is used, see related software description.

- Offline

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

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. QTECH 802.1X authentication extends 802.1X to support IP-MAC binding, which is called IP authorization. IP authorization supports four modes:

Supplicant authorization: The IP address is provided by QTECH 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 QTECH Supplicant preferred, then the IP address provided by the RADIUS server, and finally the IP address provided by DHCP.

- **ACL Authorization**

After user authentication is complete, the authentication server delivers the ACL or ACE to users. The ACL must be configured on the authentication server before delivery while no extra configuration is required for ACE delivery. ACL authorization delivers the ACL based on RADIUS attributes such as standard attributes, QTECH-proprietary attributes, and Cisco-proprietary attributes. For details, see the software description related to the RADIUS server.

- Kickoff

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

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 start packet carrying user accounting attributes such as user name and accounting ID. After receiving the packet, the RADIUS server starts accounting.

- **Accounting Update**

The NAS periodically sends Accounting Update packets to the RADIUS server, making the accounting more real-time. 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.

4.4 Configuration

Configuration	Description and Command	
Configuring Functions 802.1X Basic	(Mandatory) It is used to configure basic authentication and accounting.	
	aaa new-model	Enables AAA.
	aaa authentication dot1x	Configures an AAA authentication method list.
	aaa accounting network	Configures an AAA accounting method list.
	radius-server host	Configures the RADIUS server parameters.
	radius-server key	Configures the preshared key for communication between the NAS and the RADIUS server.
	dot1x port-control auto	Enables 802.1X authentication on a port.
	(Optional) It is used to configure 802.1X parameters. Ensure that the 802.1X server timeout is longer than the RADIUS server timeout.	

Configuring Parameters802.1	Online QTECH client detection applies only to QTECH Supplicant.	
	dot1x re-authentication	Enables re-authentication.
	dot1x timeout re-authperiod	Configures the re-authentication interval.
	dot1x timeout tx-period	Configures the interval o retransmission.
	dot1x reauth-max	Configures the maximum times of EAP-Request/Identity pac ket retransmission.
	dot1x timeout supp-timeout	Configures the interval of EAP-Request/Challenge packet retransmission.
	dot1x max-req	Configures the maximum times of EAP-equest/Challenge packet retransmission.
	dot1x timeout server-timeout	Configures the authentication server timeout.
	dot1x timeout quiet-period	Configuresthe quiet period after authentication fails.
	dot1x auth-mode	Specifies the authentication mode (EAP/CHAP/PAP).
	dot1x client-probe enable	Enables online QTECH client detection.
	dot1x probe-timer interval	Configures the interval of online QTECH client detection.
	dot1x probe-timer alive	Configures the duration of online QTECH client detection.
	(Optional) It is used to configure authorization. QTECH Supplicant should be used to perform supplicant authorization in IP authorization mode.	

Configuring Authorization	**aaa authorization ip-auth-mode**	Specifies the IP authorization mode.
	dot1x private-supplicant-only	Filters non-QTECH clients.
	dot1x redirect	Enables Web Redirection for 2G QTECH Supplicant Deployment.
	snmp	Configures SNMP parameters. RG-SAM/SMP can implement functions for 802.1X online users through SNMP. 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.
	dot1x mab-username upper	Enables uppercase letters in MAB user names.
	(Optional) It is used to configure Inaccessible Authentication Bypass (IAB).	

Configuring IAB	**dot1x critical**	Enables IAB.
	dot1x critical recovery action reinitialize	Enables IAB recovery.
	dot1x critical vlan	Configures the IAB VLAN.
Configuring Port Control	**dot1x port-control-mode mac-based**	Enables the MAC-based control mode.
	dot1x port-control-mode port-based	Enables the port-based control mode.
	dot1x port-control-mode port-based single-host	Enables the single-user port-based control mode.
	dot1x stationarity enable	Disables migration of dynamic users.
Configuring Dynamic VLAN Assignment	(Optional) It is used to configure dynamic VLAN assignment on a port. VLAN authorization can be performed based on a port or MAC address.	
	dot1x dynamic-vlan enable	Enables dynamic VLAN assignment on a port.
Configuring the Guest VLAN	(Optional) It is used to configure the guest VLAN. Port-based dynamic VLAN assignment should be enabled.	
	dot1x guest-vlan	Configures the guest VLAN.
Configuring the Failed VLAN	(Optional) It is used to configure the failed VLAN.	
	dot1x auth-fail vlan	Configures the failed VLAN.
	dot1x auth-fail max-attempt	Configures the maximum number of failed VLAN attempts.

Configuring Extended Functions	(Optional) It is used to configure active authentication requests on a port. (Optional) It is used to configure the authenticated client list. (Optional) It is used to enable 802.1X packet sending with the pseudo source MAC address. (Optional) It is used to configure multiple accounts for the same MAC address.	
	dot1x auto-req	Enables active authentication.
	dot1x auto-req packet-num	Configuresthe number of active authentication requests.
	dot1x auto-req user-detect	Enables user detection for active authentication.
	dot1x auto-req req-interval	Configuresthe interval of active authentication request.
	dot1x auth-address-table address	Configures the authenticatable client list.
	dot1x pseudo source-mac	Enables 802.1X packets sending with the pseudo source MAC address.
	dot1x multi-account enable	Enables multi-account authentication with one MAC address.
	dot1x valid-ip-acct enable	Enables IP-triggered accounting.
	dot1x valid-ip-acct timeout	Configures the timeout of obtaining IP addresses after users get authenticated. If timeout is reached, they will be kicked off.

4.4.1 Configuring 802.1X Basic Functions

Configuration Effect

- Enable basic authentication and accounting services.
- On a wired network, run the **dot1x port-control auto** command in interface configuration mode to enable 802.1X authentication on a port.
- Run the **radius-server host** *ip-address* 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.

- Run the **aaa accounting update** command in global configuration mode to enable accounting update and the **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.

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, 802.1X users must re-initiate authentication requests to continue the communication.
- Users with IP addresses statically configured or compliant with IP-MAC binding can access the network without authentication.
- 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 the it.
- When RG-SAM/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.

Configuration Steps

❖ **Enabling AAA**

- (Mandatory) 802.1X authentication and accounting take effect only after AAA is enabled.
- Enable AAA on the NAS that needs to control user access by 802.1X.

Command	aaa new-model

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

❖ **Enabling an AAA Authentication Method List**

- Mandatory.
- The AAA authentication method list must be consistent with the 802.1X authentication method list.
- Enable an AAA authentication method list after 802.1X authentication is enabled on the NAS.

Command	**aaa authentication dot1x *list-name* group radius**
Parameter Description	*list-name*: Indicates the 802.1X authentication method list of AAA.
Defaults	No AAA authentication method list is configured by default.
Command Mode	Global configuration mode
Usage Guide	AAA authentication modes are disabled by default. The AAA authentication mode must be consistent with the 802.1X authentication mode.

❖ **Configuring the RADIUS Server Parameters**

- (Mandatory) The RADIUS server parameters must be configured to ensure proper communication between the NAS and the RADIUS server.
- Configure RADIUS server parameters after 802.1X authentication is enabled on the NAS.

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.

Defaults	No RADIUS server parameters are configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ **Configuring the Preshared Key for Communication between the NAS and RADIUS Server**

- (Mandatory) The preshared key for communication between the NAS and RADIUS server must be configured to ensure proper communication between the NAS and the RADIUS server.
- Configure the preshared key of the RADIUS server after 802.1X authentication is enabled on the NAS.

Command	**radius-server key *string***
Parameter Description	*string*: Indicates the preshared key.
Defaults	No preshared key is configured for communication between the NAS and RADIUS server by default.
Command Mode	Global configuration mode
Usage Guide	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 server, you need to change the communication ports on the NAS correspondingly.

❖ **Enabling 802.1X on a Port**

- This command is mandatory for a wired network.
- Enable 802.1X on switches.

Command	**dot1x port-control auto**
Parameter Description	N/A
Defaults	802.1X is disabled on a port by default.

Command Mode	Interface configuration mode/VXLAN mode
Usage Guide	802.1X is disabled on a port by default. This command is mandatory for the deployment of 802.1X authentication. 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 QTECH Supplicant, enter the correct account information, and initiate authentication. Then check whether the 802.1X and RADIUS configurations are correct.

❖ **Checking for 802.1X Authentication Entries**

Command	**show dot1x summary**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Display entries of authenticated users to check the authentication status of users, for example, authenticating, authenticated, or quiet.
Command Display	`QTECH#show dot1x summary` `ID Username MAC Interface VLAN Auth-State Backend-state Port-Status User-Type Time`
	`16777302 ts-user b048.7a7f.f9f3 wlan 1 1 Authenticated Idle Authed static 0days 0h 0m12s`

❖ Checking for AAA User Entries

Command	**show aaa user all**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Display information of AAA users.

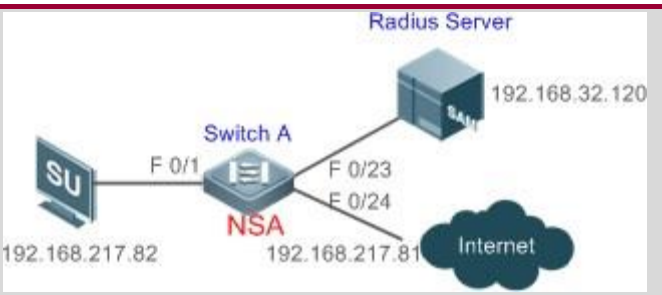
Command Display	QTECH#show aaa user all Id--Name 2345687901 wwxy

- 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 are incorrect. If the 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.

Configuration Example

In this example, RG-SAM acts as the authentication server.

❖ **Configuring 802.1X Authentication on a Switch**

Scenario Figure 4-5	

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 server, see the Configuring RADIUS.
	`QTECH# configure terminal QTECH (config)# aaa new-model`
	`QTECH (config)# radius-server host 192.168.32.120 QTECH (config)# radius-server key QTECH`
	`QTECH (config)# interface FastEthernet 0/1 QTECH (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:tests-user,password:test**.
	▪ The user fails to ping 192.168.32.120 before authentication.
	▪ After the user enters account information and click **Authenticate** on QTECH Supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120.
	▪ Information of the authenticated user is displayed.
	`QTECH# show dot1x summary`
	`ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time`
	`16778217 ts-user 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed`
	`static 0days 0h 0m 7s`

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

- 802.1X and RADIUS have separate server timeouts. By default, the authentication server timeout of 802.1X is 5 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. For detailed configuration about the RADIUS server timeout, see the *Configuring RADIUS*.
- Online client detection applies only to QTECH Supplicant.

Configuration Steps

❖ **Enabling Re-authentication**

- (Optional) After re-authentication is enabled, the NAS can periodically re-authenticate online users.
- Enable re-authentication after 802.1X authentication is enabled on the NAS.

Command	dot1x re-authentication

Parameter Description	N/A
Defaults	Re-authentication is disabled by default.
Command Mode	Global configuration mode
Usage Guide	You can run this command to periodically re-authenticate users.

❖ **Configuring the Re-authentication Interval**

- (Optional) You can configure the re-authentication interval for users.
- Configure the re-authentication interval after 802.1X authentication is enabled on the NAS. The re-authentication interval takes effect only after re-authentication is enabled.

Command	**dot1x timeout re-authperiod *period***
Parameter Description	*period*: Indicates the re-authentication interval in the unit of seconds.
Defaults	The default value is 3,600 seconds.
Command Mode	Global configuration mode
Usage Guide	Adjust the re-authentication interval as required.

❖ **Configuring the Interval of EAP-Request/Identity Packet Retransmission**

- (Optional) A larger value indicates a longer interval of packet retransmission.
- Configure the interval of EAP-Request/Identity packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout tx-period *period***
Parameter Description	*period*: Indicates the interval of EAP-Request/Identity packet retransmission in the unit of seconds.
Defaults	The default value is 3 seconds.
Command Mode	Global configuration mode

Usage Guide	It is recommended to use the default value. Adjust the value based on how long the authentication client responds to the NAS's requests.

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

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

Command	**dot1x reauth-max *num***
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Identity packet retransmission.
Defaults	The default value is 3 for switches and 6 for wireless devices
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. In the case of high-rate packet loss, increase this value so that the clients can easily receive packets from the NAS.

❖ **Configuring the Interval of EAP-Request/Challenge Packet Retransmission**

- (Optional) A larger value indicates a longer retransmission interval.
- Configure the interval of EAP-Request/Challenge packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout supp-timeout *time***
Parameter Description	*time*: Indicates the interval of EAP-Request/Challenge packet transmission in the unit of seconds.
Defaults	The default value is 3 seconds for switches and 6 seconds for wireless devices
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value in the case of high-rate packet loss.

❖ **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.
Defaults	The default value is 3.
Command Mode	Global configuration mode
Usage Guide	Optional. It is recommended to use the default value. Increase this value in the case of high-rate packet loss.

❖ **Configuring the Authentication Server Timeout**

- (Optional) A larger value indicates a longer authentication server timeout.
- Configure the authentication server timeout after 802.1X authentication is enabled on the NAS.
- The server timeout of RADIUS must be greater than that of 802.1X.

Command	dot1x timeout server-timeout *time*
Parameter Description	*time*: Indicates the authentication server timeout in the unit of seconds.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value if the communication between the NAS and RADIUS server is unstable.

❖ **Configuring the Quiet Period after Authentication Fails**

- (Optional) A larger value indicates a longer quiet period.
- Configure the quiet period after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout quiet-period *time***
Parameter Description	*time*: Indicates the quiet period after authentication fails. The unit is second.
Defaults	The default value is 10 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value to prevent users from frequently initiating authentication to the RADIUS server, thereby reducing the load of the authentication server.

❖ **Specifying the Authentication Mode**

- (Optional) Configure the mode for 802.1X authentication.
- Configure the authentication mode after 802.1X authentication is enabled on the NAS.

Command	**dot1x auth-mode** {eap | chap | pap}
Parameter Description	**eap**: Indicates EAP authentication. **chap**: Indicates CHAP authentication. **pap**: Indicates PAP authentication.
Defaults	The default value is **eap**.
Command Mode	Global configuration mode
Usage Guide	Select the authentication mode supported by QTECH Supplicant and authentication server.

❖ **Enabling Online QTECH Client Detection**

- (Optional) If online QTECH client detection is enabled, the NAS can find clients going offline in a timely manner to prevent incorrect accounting.
- This function applies only to QTECH 802.1X authentication clients.
- Enable online QTECH client detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x client-probe enable**

Parameter Description	N/A
Defaults	Online QTECH client detection is disabled by default.
Command Mode	Global configuration mode
Usage Guide	It is recommended to enable this function when QTECH Supplicant is used.

❖ **Configuring the Interval of Online QTECH Client Detection**

- (Optional) A larger value indicates a longer time interval at which QTECH clients send detection packets.
- Configure the interval of online QTECH client detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x probe-timer interval *time***
Parameter Description	*time*: Indicates the time interval at which QTECH Supplicant sends a heartbeat packet to the NAS. The unit is second.
Defaults	The default value is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value.

❖ **Configuring the Duration of Online QTECH Client Detection**

- (Optional) A larger value indicates a longer interval at which the NAS finds clients going offline.
- Configure the duration of online QTECH client detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x probe-timer alive *time***
Parameter Description	*time*: Indicates the duration of online QTECH client detection in the unit of seconds.
Defaults	The default value is 250 seconds.

Command Mode	Global configuration mode
Usage Guide	Optional. If the NAS does not receive any detection packets from an online client within the detection duration, it regards the client offline. It is recommended to use the default value.

Verification

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

Configuration Example

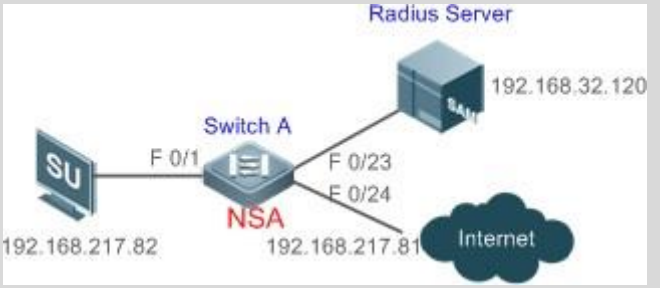
- **Specifying the Authentication Mode**

Scenario	**The NAS is deployed in standalone mode.**
Configuration Steps	Set the authentication mode to **chap**.
	`QTECH(config)#dot1x auth-mode chap`
Verification	Display the configurations.

```
QTECH(config)#show dot1x

802.1X basic information:
  802.1X Status      enable
  Authentication Mode      chap
  Authorization mode disable
  Total User Number  0  (exclude dynamic user)
  Authenticated User Number       0  (exclude dynamic user)
  Dynamic User Number      0
  Re-authentication disable
  Re-authentication Period 3600 seconds
  Re-authentication max    3 times
  Quiet Period       10 seconds
  Tx Period   30 seconds
  Supplicant Timeout 3 seconds
  Server Timeout     5 seconds
  Maximum Request    3 times
  Client Online Probe      disable
  Eapol Tag   disable
  802.1x redirect    disable
Private supplicant only disable
```

❖ Enabling Online Client Detection

Scenario **Figure 4-6**	
Configuration Steps	Enable online client detection.
	`QTECH(config)#dot1x client-probe enable`
Verification	▪ Users can remain online only when their QTECH Supplicant sends online detection packets as scheduled. ▪ Display the configurations.

	`QTECH(config)#show dot1x`
	`802.1X basic information:`
	`802.1X Status ..... enable`
	`Authentication Mode ..... chap`
	`Authorization mode ..... disable`
	`Total User Number ..... 0 (exclude dynamic user)`
	`Authenticated User Number ..... 0 (exclude dynamic user)`
	`Dynamic User Number ..... 0`
	`Re-authentication disable`
	`Re-authentication Period ..... 3600 seconds`
	`Re-authentication max ..... 3 times`
	`Quiet Period ..... 10 seconds`
	`Tx Period ..... 30 seconds`
	`Supplicant Timeout ..... 3 seconds`
	`Server Timeout ..... 5 seconds`
	`Maximum Request ..... 3 times`
	`Client Online Probe..... enable`
	`Eapol Tag ..... disable`
	`802.1x redirect ..... disable`

Common Errors

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

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. IP authorization can be enabled in global configuration mode or interface configuration mode. IP authorization enabled in interface configuration mode takes priority over that configured in global configuration mode.
- Enable non-QTECH client filtering. If this function is enabled, users must use QTECH Supplicant for authentication so that they will enjoy services provided by QTECH Supplicant, such as anti-proxy or SMS.
- Enable Web redirection to support 2G QTECH Supplicant deployment. 2G QTECH Supplicant deployment means that a user needs to download QTECH Supplicant through the browser and then initiate authentication through QTECH Supplicant. 2G QTECH Supplicant deployment facilitates quick deployment of QTECH Supplicant in the case of massive users.

Notes

- If the real-time kickoff function of RG-SAM/SMP is used, you need to configure correct SNMP parameters. For 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 QTECH Supplicant provides an IP address for this RADIUS-authentication user during its re-authentication, this IP address will be used for authorization.
- For 802.1X authentication, when a user attempts to obtain an IP address through DHCP in gateway authentication mode and IP authorization mode, you can enable IP DHCP snooping and IP source guard to prevent the user from stealing an IP address.
- In gateway authentication mode and DHCP or mixed authorization mode, the NAS automatically grants the latest IP address obtained though DHCP to a user so that the user can properly communicate after being migrated to the same Super VLAN.
- 2G QTECH Supplicant deployment and Web authentication cannot be used at the same time.
- 2G QTECH Supplicant deployment requires the setting of the **redirect** parameter. For details, see the *Configuring Web Authentication*.
- The kickoff function of RG-SAM/SMP is implemented through SNMP.

Therefore, you need to configure SNMP parameters. For details, see the *Configuring SNMP*.

Configuration Steps

❖ **Specifying the Global IP Authorization Mode**

- The **supplicant** mode only applies to QTECH 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 must be enabled on the NAS.
- (Optional) Configure an IP-MAC binding.
- Configure the IP authorization mode after 802.1X authentication is enabled on the NAS.

Command	**aaa authorization ip-auth-mode { disable | supplicant | radius-server | dhcp-server | 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.
Defaults	IP authorization is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Select the IP authorization mode based on actual deployment.

❖ **Enabling Web Redirection for 2G QTECH Supplicant Deployment**

- (Optional) If the redirection for 2G QTECH Supplicant deployment is enabled, users not having any 802.1X authentication clients on a controlled port can download and install an 802.1X authentication client through Web pages.
- Enable Web redirection for 2G QTECH Supplicant deployment after 802.1X authentication is enabled on the NAS.
- The **redirect** parameter must be configured. For details, see the *Configuring Web Authentication*.

Command	**dot1x redirect**

Parameter Description	N/A
Defaults	The redirection for 2G QTECH Supplicant deployment is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The **redirect** parameter must be configured. For details, see the *Configuring Web Authentication*.

❖ **Enabling Non-QTECH Client Filtering**

- (Optional) If this function is enabled, non-QTECH clients cannot perform authentication.
- Enable non-QTECH client filtering after 802.1X authentication is enabled on the NAS.

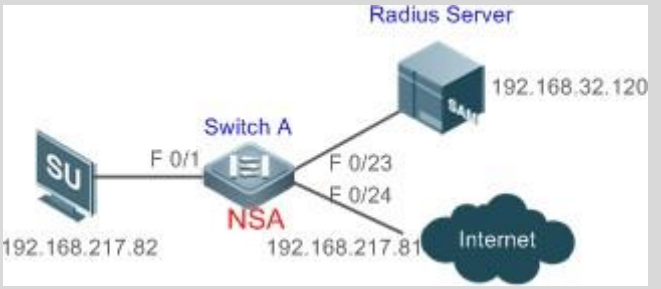
Command	**dot1x private-supplicant-only**
Parameter Description	N/A
Defaults	Non-QTECH client filtering is disabled by default.
Command Mode	Global configuration mode
Usage Guide	This function can be enabled only when QTECH Supplicant is used.

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 QTECH 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 RG-SAM/SMP. The NAS will force the user offline and the user will fail to access the network.

Configuration Example

❖ **Configuring the IP Authorization Mode**

Scenario **Figure 4-7**	
Configuration Steps	Enable AAA. Configure RADIUS. Enable 802.1X on a controlled port. Globally enable IP authorization in **supplicant** mode.
	`QTECH(config)#aaa authorization ip-auth-mode supplicant`
	QTECH Supplicant initiates authentication and the authentication succeeds. QTECH Supplicant only uses 192.168.217.82 for communication.
Verification	Display the configurations.

	`QTECH(config)#show dot1x user name ts-user Supplicant information:`
	`MAC address.....b048.7a7f.f9f3`
	`Username ts-user`
	`User ID.....16777303`
	`Type static`
	`VLAN.....1`
	Port.....wlan 1
	Online duration 0days 0h 0m21s
	Up average bandwidth.....0 kBps
	Down average bandwidth .....0 kBps
	Authorized VLAN 1
	Authorized session time.....20736000 seconds
	Authorized flux.....unlimited
	Accounting.....No
	Proxy user .....Permit
	Dial user .....Permit
	IP privilege.....0
	Private supplicant .....no
	Max user number on this port 0

Common Errors

- There are multiple authentication clients on the network but non-QTECH client filtering is enabled, causing some users to fail authentication.
- RG-SAM/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 QTECH Supplicant 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 install any 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 VoIP 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-VoIP daisy-chain topology.

Notes

- A MAB-enabled port sends an authentication request packet as scheduled 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 password should be set to 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 authentication. Therefore, automatic authentication must be enabled for MAB deployment.

Configuration Steps

❖ **Enabling Single-User MAB**

- Optional.
- Single-user MAB applies when only one user connected to a port needs to be authenticated.
- Enable single-user MAB on the 802.1X controlled port of the NAS.

Command	**dot1x mac-auth-bypass**
Parameter Description	N/A
Defaults	Single-user MAB is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	This command applies only to switches. 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**

- Optional.
- 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 policies such as kickoff. You can configure the timeout of authenticated MAC addresses. The default value is 0, indicating always online.
- Configure the timeout of MAB users on the 802.1X controlled port of the NAS.

Command	**dot1x mac-auth-bypass timeout-activity *value***
Parameter Description	*value*: Indicates the maximum online time of MAB users in the unit of seconds.
Defaults	The default value is 0, indicating no time restriction.
Command Mode	Interface configuration mode/VXLAN mode
Usage Guide	The MAB timeout applies to both single-user MAB and multi-user MAB.

❖ Enabling the MAB Violation Mode

- Optional.
- Enable MAB violation on the 802.1X controlled port of the NAS.
- By default, after one MAC address passes MAB authentication, data of all switches connected to the port can be forwarded. However, for security purposes, the administrator may request one MAB port to support only one MAC 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.

Command	dot1x mac-auth-bypass violation
Parameter Description	N/A
Defaults	MAB violation is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	This command applies only to switches. Configure this command only when only one dumb user is connected to the port. MAB violation applies only to single-user MAB.

❖ Enabling Multi-user MAB

- Optional.
- Enable multi-user MAB on the 802.1X controlled port of the NAS.

Command	dot1x mac-auth-bypass multi-user
Parameter Description	N/A
Defaults	Multi-user MAB is disabled by default.
Command Mode	Interface configuration mode/VXLAN mode
Usage Guide	This command applies only to switches. Configure this command when multiple dumb users connected to the port need to be authenticated.

❖ Configuring the Quiet Period after Multi-user MAB Fails

- Optional.
- Configure the quite period of the multi-user MAB failure after multi-user MAB is enabled on the NAS.
- 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 reduce the load of the authentication server. 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 period based on the actual situation. The default value is 0, indicating that a user can re-initiate authentication immediately after authentication fails.

Command	**dot1x multi-mab quiet-period *value***
Parameter Description	*value*: Indicates the quiet period after authentication fails.
Defaults	The default value is 0s.
Command Mode	Global configuration mode
Usage Guide	This command applies only to switches. 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.
Defaults	VLAN-based MAB is disabled by default.
Command	Interface configuration mode

Mode	
Usage Guide	This command applies only to switches. Run this command when a port allows only users in specified VLANs to perform MAB.

❖ **Enabling Uppercase Letters in MAB User Names**

- Optional.
- Enable this function in global configuration mode.

Command	**dot1x mab-username upper**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	By default, lowercase letters are used in the user name of MAB. After this function is enabled, uppercase letters are used in new user names of MAB to meet server requirements.

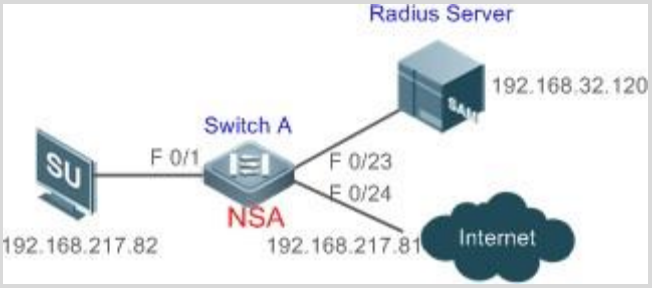
Verification

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.

Configuration Example

❖ **Enabling Multi-user MAB on a Switch**

Scenario **Figure 4-8**	
Configuration Steps	▪ Register the IP address of the Switch A on the RADIUS server and configure the communication key between Switch A and the RADIUS server. ▪ Create an account on the RADIUS server. ▪ Enable AAA on Switch A. ▪ Configure RADIUS parameters on Switch A. ▪ Enable 802.1X and multi-user MAB on a port of Switch A. Switch configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.

	`QTECH# configure terminal QTECH (config)# aaa new-model`
	`QTECH (config)# radius-server host 192.168.32.120 QTECH (config)# radius-server key QTECH`
	`QTECH (config)# interface FastEthernet 0/1 QTECH (config-if)# dot1x port-control auto`
	`QTECH (config-if)# dot1x mac-auth-bypass multi-user`

Verification	Check whether authentication is proper and network access behaviors change after authentication.
	▪ The account is successfully created, such as **username: 0023aeaa4286,password: 0023aeaa4286**.
	▪ The user fails to ping 192.168.32.120 before authentication.
	▪ The user connects to the switch, the authentication succeeds, and the user can successfully ping 192.168.32.120.
	▪ Information of the authenticated user is displayed.
	`QTECH# show dot1x summary`
	`ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time`
	`16778217 0023aea. ... 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 0h 5m 8s`

Common Errors

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

4.4.5 Configuring MAB Auto Authentication

Configuration Effect

- When a STA accesses the network for the first time, Web authentication is performed. When the STA is disconnected from and then reconnects to the network, authentication is not required.

Notes

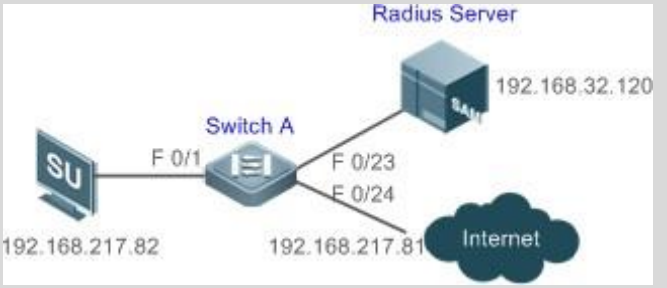
- Wireless MAB authentication is triggered by a STA advertisement. If a STA is already online, MAB authentication will not be triggered again. MAB authentication is triggered only after the STA is disconnected from and then reconnects to the network.
- When a STA accesses the network for the second time, a dialog box may be displayed for MAB authentication. When the STA accesses the network for the third time, the dialog box will not be displayed.
- If MAB authentication fails, a dialog box is displayed for Web authentication when the STA accesses the network next time.

Configuration Steps

For details about Web authentication configuration, see the Web authentication configuration document. For details about MAB authentication configuration, see section “Configuring MAB”.

Configuration Example

❖ **Configuring MAB Auto Authentication**

Scenario **Figure 4-9**	

Configuration Steps	▪ Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ▪ Create an account on the RADIUS server and bind it with a MAC address for imperceptible authentication. ▪ Enable AAA on the NAS. ▪ Configure RADIUS parameters on the NAS. ▪ Enable 802.1X authentication and MAB authentication on an interface of the NAS. ▪ Enable second-generation (or first-generation/embedded) Web authentication on an interface of the NAS and configure the Web authentication template globally. The following describes the NAS configurations. For detailed configuration on the RADIUS server, see the related configuration guide (The following describes configuration on the switch, which is similar to that on the AC/AP, except that the configuration on the switch is performed in interface configuration mode instead of WLAN RSNA configuration mode.)

	`QTECH#configure`
	`terminal QTECH`
	`(config)#aaa new-`
	`model`
	`QTECH (config)#aaa authentication web-auth default group`
	`radius QTECH (config)#aaa authentication dot1x default`
	`group radius`
	`QTECH (config)aaa accounting net-work default start-stop group`
	`radius QTECH (config)#radius-server host 192.168.32.120`
	`QTECH (config)#radius-server key`
	`QTECH QTECH (config)#web-auth`
	`template eportalv2 QTECH (config-`
	`tmplt-v2)#ip 192.158.32.9`
	`QTECH (config-tmplt-v2)#url`
	`http://192.168.32.9:8080/eportal/index.jsp QTECH (config-tmplt-`
	`v2)#exit`
	`QTECH (config)#interface`
	`FastEthernet 0/1 QTECH (config-`
	`if)#dot1x port-control auto`
	`QTECH (config-if)#dot1x mac-auth-bypass multi-user`
	`QTECH (config-if)#web-auth enable eportalv2`

Verification	Check whether authentication is normal and network access behaviors change after authentication. ▪ The account is successfully created, for example, the username is 0023aeaa4286 and the password is 0023aeaa4286. ▪ The STA fails to ping 192.168.32.120 before authentication. ▪ The STA connects to the NAS, a page indicating the authentication succeeds is displayed, and the STA can successfully ping 192.168.32.120. ▪ The STA is disconnected from and then reconnects to the network and can successfully ping 192.168.32.120.

```
QTECH#show dot1x summary
ID     Username      MAC    Interface  VLAN  Auth-State  Backend-State
Port-Status User-Type Time
16778217     0023aea...          0023.aeaa.4286      Fa0/1  2
       AuthenticatedIdle Authed          static 0days 0h 5m 8s
```

Common Errors

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

4.4.6 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 during inaccessibility.
- Configure IAB VLANs. When RADIUS servers are inaccessible and cannot authenticate users temporarily, you can add the ports connected with users to specified VLANs so that users can access only network resources of specified VLANs.

Notes

- Configure an account and standards for testing RADIUS server accessibility. For details, see the *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.
- In access authentication configuration mode, when 802.1X-based IP authotication is enabled globally, users on this port, except those habing been authenticated, cannot be authenticated in IAB mode. In gateway authentication mode, users are IP authorized if their IP addresses are

obtained.

- Complete 802.1X authentication is required on such 802.1X authentication clients as those of Windows. It is possible that though these clients already pass the IAB authentication, there are prompts on the clients suggesting failed authentication.
- If the failed VLAN configured does not exist, a failed VLAN will be dynamically created when a port enters the failed VLAN and automatically removed when the port exits the failed VLAN.
- Failed VLANs cannot be private VLANs, remote VLANs, and super VLANs (including sub VLANs).

Configuration Steps

❖ **Enabling IAB**

- (Optional) After IAB is enabled, the NAS authorizes newly authenticated users if the authentication server is faulty.
- Enable IAB after 802.1X authentication is enabled on the NAS.

Command	dot1x critical
Parameter Description	N/A
Defaults	IAB is disabled by default.
Command Mode	Interface configuration mode/VXLAN mode
Usage Guide	This command applies to ports on which newly authenticated users need to be authorized when the authentication server is inaccessible.

❖ **Enabling IAB Recovery**

- (Optional) After the authentication server is recovered, the NAS re-authenticates users that are authorized when the authentication server is inaccessible.
- Enable IAB recovery actions after 802.1X authentication is enabled on the NAS.

Command	dot1x critical recovery action reinitialize
Parameter Description	N/A
Defaults	IAB recovery is disabled by default.

Command Mode	Interface configuration mode/VXLAN mode
Usage Guide	If IAB recovery is enabled on a port, properly authenticated users on the port can access the network without re-authentication after the authentication server is recovered. After the authentication server is recovered, the NAS initiates authentication only to users authenticated in IAB mode during server inaccessibility.

❖ **Configuring the IAB VLAN**

- (Optional) Configure the VLAN on which newly authenticated users are authorized when the authentication server becomes inaccessible.
- Enable VLAN-based IAB after 802.1X authentication is enabled on the NAS.

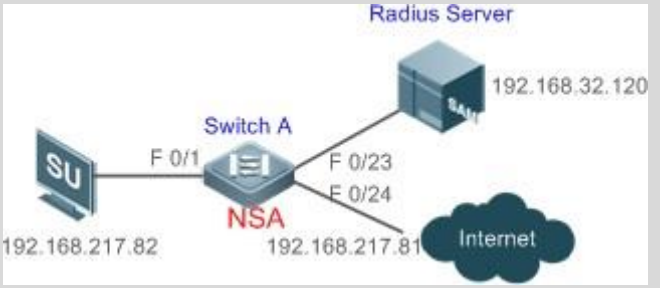
Command	**dot1x critical vlan *vlan-id***
Parameter Description	*vlan-id*: Indicates the VLAN to redirect when the authentication server becomes inaccessible.
Defaults	The IAB VLAN is not configured by default.
Command Mode	Interface configuration mode/VXLAN mode
Usage Guide	Configure the IAB VLAN so that temporary network resources can be provided for users when servers are inaccessible.

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 network immediately after connecting to the NAS.

Configuration Example

❖ **Enabling IAB**

Scenario **Figure 4-10**	
Configuration Steps	▪ Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ▪ Create an account on the RADIUS server. ▪ Enable AAA on the NAS. ▪ Configure RADIUS parameters and enable server accessibility probe on the NAS. ▪ Enable 802.1X and multi-user MAB on a port of the NAS. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.

	`QTECH# configure terminal QTECH (config)# aaa new-model`
	`QTECH (config)# radius-server host 192.168.32.120 QTECH (config)# radius-server key QTECH`
	`QTECH (config)# interface FastEthernet 0/1`
	`QTECH (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**.
	▪ When the authentication server is accessible, the user fails to ping 192.168.32.120 before authentication.
	▪ When the authentication server becomes inaccessible, the user connects to the NAS, authentication succeeds, and the user can successfully ping 192.168.32.120.
	▪ Information of the authenticated user is displayed.
	`QTECH# show dot1x summary`
	`ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time`
	`16778217 test ... 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 0h10m20s`

4.4.7 Configuring Port Control

Configuration Effect

- By default, the 802.1X controlled port is controlled based on the MAC address. That is, users using this MAC address can access the network only after authenticated.
- Configure the port-based control mode. As long as a user on a controlled port passes authentication, this port becomes authenticated and all users connected to this port can properly access the network.
- Configure the single-user control mode on a port. This port allows only a single user to pass authentication. If this port becomes authenticated, this user can properly access the network. At this time, if the NAS detects other users connected to this port, it will clear all users connected to this port and the user needs to re-initiate authentication.
- The port-based control mode allows or prohibits dynamic users migrating among different ports. By default, dynamic users can migrate among different ports.

Notes

- In port-based authentication mode, a controlled port supports only one authenticated user while all others are dynamic users.
- In single-user port-based authentication mode, only one user on a controlled port can pass authentication and access the network. This restriction remains even when a specified number of users is configured on this port.

Configuration Steps

❖ **Enabling the MAC-based Control Mode**

- (Optional) After the MAC-based control mode is enabled, each user on an 802.1X controlled port must pass MAC-based authentication to access the network.
- Enable the MAC-based control mode after 802.1X authentication is enabled on the NAS.

Command	dot1x port-control-mode mac-based
Parameter Description	N/A
Defaults	The default port control mode is MAC-based control.
Command Mode	Interface configuration mode

Usage Guide	Configure the MAC-based control mode if all the users on a controlled port have to pass authentication to access the network.

❖ **Enabling the Port-based Control Mode**

- (Optional) After a user on an 802.1X controlled port passes authentication, all other users on this port can access the network.
- Enable the port-based control mode after 802.1X authentication is enabled on the NAS.

Command	**dot1x port-control-mode port-based**
Parameter Description	N/A
Defaults	The default port control mode is MAC-based control.
Command Mode	Interface configuration mode
Usage Guide	You can configure the port-based control mode if the remaining users can access the network after a user on a controlled port passes authentication.

❖ **Enabling the Single-User Port-based Control Mode**

- (Optional) Configure only one dynamic user to access the network in port-based authentication mode.
- Enable the single-user port-based control mode after 802.1X authentication is enabled on the NAS.

Command	**dot1x port-control-mode port-based single-host**
Parameter Description	N/A
Defaults	The single-user port-based control mode is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when only the authenticated user can act as a dynamic user in port-based control mode.

❖ **Disabling Migration of Dynamic Users**

- (Optional) If this function is disabled, dynamic users on a controlled port cannot migrate to other ports until the port has aged.
- Disable this function after 802.1X authentication is enabled on the NAS.

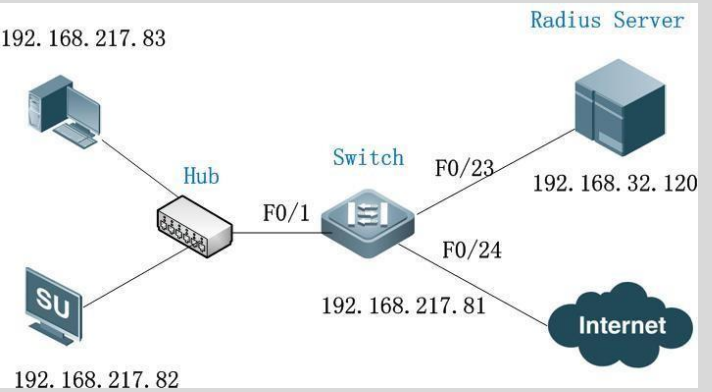
Command	dot1x stationarity enable
Parameter Description	N/A
Defaults	Dynamic users can migrate to other ports by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command to prohibit dynamic users on a controlled port from migrating to other ports.

Verification

- In MAC-based control mode, each user on a controlled port can access the network only after authenticated.
- In port-based control mode, as long as a user on a controlled port passes authentication, other users can access the network without authentication.

Configuration Example

❖ **Enabling the Port-based Control Mode**

Scenario Figure 4-11	

Configuration Steps	▪ Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ▪ Create an account on the RADIUS server. ▪ Enable AAA on the NAS. ▪ Configure RADIUS parameters on the NAS. ▪ Enable 802.1X authentication on ports of the NAS. ▪ Enable port-based authentication on a controlled port. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	QTECH# configure terminal QTECH (config)# aaa new-model QTECH (config)# radius-server host 192.168.32.120 QTECH (config)# radius-server key QTECH QTECH (config)# interface FastEthernet 0/1 QTECH (config-if)# dot1x port-control auto QTECH (config-if)# dot1x port-control-mode port-based
Verification	Check whether authentication is proper, network access behaviors change after authentication, and dynamic users can access the network. ▪ The account is successfully created, such as **username:tests-user,password:test**. ▪ The user fails to ping 192.168.32.120 before authentication. ▪ After the user enters account information and click **Authenticate** on QTECH Supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120. ▪ After passing authentication, dynamic users can successfully ping 192.168.32.120. ▪ Information of the authenticated user is displayed. QTECH# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time 16778217 ts-user 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 2h17m29s none N/A .... 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed Dynamic N/A

4.4.8 Configuring Dynamic VLAN Assignment

Configuration Effect

- Enable 802.1X-based dynamic VLAN assignment for a port. If the authentication server assigns a VLAN to redirect after a user passes authentication, the NAS can add this user to the assigned VLAN to perform authorization on this user.
- Controlled ports on the VLAN to redirect fall in three types: Access, Trunk, and Hybrid (MAC VLAN is disabled). You can change native VLANs of these ports to realize 802.1X-based dynamic VLAN assignment.
- If controlled ports on the VLAN to redirect are Hybrid ports (and MAC VLAN is enabled), dynamically create MAC VLAN entries to add users to the assigned VLAN.

Notes

- The NAS can extend RADIUS attributes to assign VLANs. When assigning VLANs to the access switch based on extended attributes, the RADIUS server encapsulates these attributes in RADIUS Attribute 26, with the vendor ID of 0x00001311. The default type No. of the extended attribute is 4. You can run the **radius attribute 4 vendor-type type** command on the NAS to receive the VLAN of which the extended attribute type No. is set to **type**. For details about the
command, see the *Configuring RADIUS*.

- The RADIUS server can assign VLANs based on the following RADIUS attributes: Attribute 64: Tunnel-Type, with the value being VLAN (13).
Attribute 65: Tunnel-Medium-Type, with the value being 802 (6).

  Attribute 81: Tunnel-Private-Group-ID, which can be the VLAN ID or VLAN name.

- The NAS can perform 802.1X authentication on Access, Trunk, and Hybrid ports. If 802.1X-based dynamic VLAN assignment is enabled on other ports, authentication will fail.
- If the assigned VLAN is the VLAN name, the system checks whether the VLAN name exists on the access switch. If yes, the port of the user redirects to this VLAN. If no, the NAS identifies the assigned VLAN as the VLAN ID. If the VLAN ID is valid (in the VLAN ID range supported by the system), the port of the user redirects to this VLAN. If the VLAN ID is 0, no VLAN information is assigned. In other cases, users fail authentication.
- Private VLANs, remote VLANs, or super VLANs (including sub VLANs) cannot be assigned for redirection.
- In dynamic VLAN assignment on an Access port, check whether any assigned VLAN is configured on the switch:

  - Yes: If the Access port can redirect to the assigned VLAN, the port will leave the configured VLAN and migrate to the assigned VLAN, and user authentication will succeed. Otherwise (see the related description below), user authentication will fail.
  - No: If the NAS identifies the assigned VLAN attribute as the VLAN ID, it will

create a VLAN and enable the port to redirect to the new VLAN, and user authentication will succeed. If the NAS identifies the assigned VLAN attribute as the VLAN name, it will fail to find the corresponding VLAN ID, causing authentication failure.

- In dynamic VLAN assignment on a Trunk port, check whether any assigned VLAN is configured on the switch:

  - Yes: If the Trunk port can redirect to the assigned VLAN, the NAS will use the native VLAN of the port as the assigned VLAN, and user authentication will succeed. Otherwise (see the related description below), user authentication will fail.
  - No: If the NAS identifies the assigned VLAN attribute as the VLAN ID, it will use the native VLAN of the port, and user authentication will succeed. If the NAS identifies the assigned VLAN attribute as the VLAN name, it will fail to find the corresponding VLAN ID, causing authentication failure.

- If MAC VLAN is disabled on a Hybrid port, check whether any assigned VLAN is configured on the switch:

  - Yes: If the Hybrid port can redirect to the assigned VLAN or the assigned VLAN does not exist in the tagged VLAN list of the Hybrid port, the NAS will allow the assigned VLAN to pass through the Hybrid port without carrying any tags and uses the native VLAN as the assigned VLAN, and user authentication will succeed. Otherwise (see the related description below), user authentication will fail.
  - No: If the NAS identifies the assigned VLAN attribute as the VLAN ID, it will create a VLAN, allow the VLAN to pass through the Hybrid port without carrying any tags, and use the native VLAN as the assigned VLAN, and user authentication will succeed. If the NAS identifies the assigned VLAN attribute as the VLAN name, it will fail to find the corresponding VLAN ID, causing authentication failure.

- If MAC VLAN is enabled on a Hybrid port, VLAN assignment is as follows:

  If the VLAN assigned by the authentication server does not exist on the NAS (MAC VLAN requires VLANs to have static configurations), or has been added to the Hybrid port with tags, or is not supported by MAC VLAN (see the *Configuring MAC VLAN*), user authentication will fail. Otherwise, the NAS will dynamically create MAC VLAN entries based on the assigned VLAN and the MAC addresses of users, and user authentication will succeed. When users go offline, MAC VLAN entries will be dynamically removed.

- If MAC VLAN is disabled on a port, VLAN assignment changes only the native VLAN but not the **native vlan** command configurations of the port. The assigned VLAN takes priority over the VLAN configured in related commands. That is, the native VLAN effective after authentication acts as the assigned VLAN while the native VLAN configured in related commands takes effect only when users go offline.
- If MAC VLAN is enabled on a port and user authentication is based on the MAC address, VLAN assignment dynamically creates MAC VLAN entries without changing the native VLAN of the port.

- No matter MAC VLAN is enabled or not on a Hybrid port, if the assigned VLAN is added to the port with tags, VLAN assignment fails.
- If MAC VLAN is enabled on a port (see the *Configuring MAC VLAN*), VLAN assignment creates an MAC VLAN entry with an all-F mask. If the MAC address of an 802.1X user is overwritten by the MAC address specified by the new MAC VLAN entry, the assigned VLAN must be the same as the VLAN specified by the new MAC VLAN entry. Otherwise, errors will occur to 802.1X users in VLAN assignment. Errors are as follows (including but not limited to): User authentication succeeds but subsequent valid data packets are discarded, causing network access failure.
  When a user goes offline by sending an EAPOL-LOGOFF packet, the 802.1X authentication entry remains on the NAS and the user status on the authentication server is still online.

Configuration Steps

❖ **Enabling Dynamic VLAN Assignment on a Port**

- (Optional) After dynamic VLAN assignment is enabled on a port, authenticated users on this port will enter the assigned VLAN.
- Enable dynamic VLAN assignment after 802.1X authentication is enabled on the NAS.

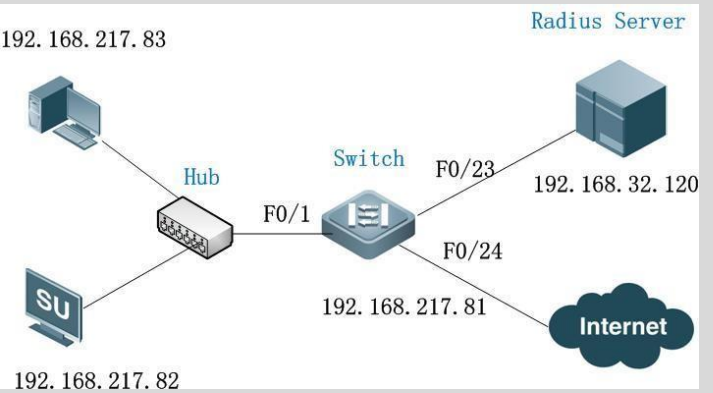
Command	dot1x dynamic-vlan enable
Parameter Description	N/A
Defaults	Dynamic VLAN assignment is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when authenticated users should be added to the VLAN assigned by the authentication server.

Verification

- Run the **show dot1x summary** command to display the VLAN of a user.
- Users with VLANs assigned can access the network in the assigned VLANs.

Configuration Example

❖ **Enabling Dynamic VLAN Assignment on a Port**

Scenario Figure 4-12	
Configuration Steps	▪ Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ▪ Create an account on the RADIUS server. ▪ Enable AAA on the NAS. ▪ Configure RADIUS parameters and enable VLAN delivery on the NAS. ▪ Enable 802.1X authentication on ports of the NAS. ▪ Enable dynamic VLAN assignment on a controlled port. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.

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

Verification	Check whether authentication is proper, network access behaviors change after authentication, and dynamic users can access the network.
	▪ The account is successfully created, such as **username:tests-user,password:test**.
	▪ The user fails to ping 192.168.32.120 before authentication.
	▪ After the user enters account information and click **Authenticate** on QTECH Supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120.
	▪ After passing authentication, dynamic users can successfully ping 192.168.32.120.
	▪ Information of the authenticated user is displayed, showing that the user jumps from VLAN 2 to VLAN 3.
	`QTECH# show dot1x summary`
	`ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time`
	`16778217 ts-user 0023.aeaa.4286 Fa0/1 3 Authenticated Idle Authed static 0days 2h17m29s`

Common Errors

- RADIUS attributes for VLAN assignment are incorrectly configured on the authentication server.
- RADIUS attribute support for VLAN assignment is disabled on the NAS.
- When MAC VLAN is enabled on a Hybrid port for dynamic VLAN assignment, the assigned VLAN has tags.

4.4.9 Configuring the Guest VLAN

Configuration Effect

- If no 802.1X authentication client is available on a controlled port, add the port to the guest VLAN so that users without any authentication clients can temporarily access the network in the guest VLAN.
- If the NAS receives an EAPOL packet after adding a port to a guest VLAN, it regards that this port has an 802.1X authentication client. Then this port is forced out of the guest VLAN to perform 802.1X authentication.

Notes

- A controlled port has no 802.1X authentication client if any one of the following conditions is met:

  1. The port sends three consecutive active authentication packets but does not receive any EAPOL replies within the specified period (**auto-req req-interval** x 3).

2. The port does not receive any EAPOL replies within 90 seconds.
3. MAB fails.

- 802.1X-based dynamic VLAN assignment must be enabled for a port.
- When the port status switches from up to down, the port exits from the guest VLAN. When the port status switches from down to up, the NAS re-checks whether to add this port to the guest VLAN.
- If failing to receive eapol packets after 90s, an interface enters the guest VLAN. Because of the increment mechanism of sending shcp discover packets, it may take a long time for a downlink terminal to initiate a dhcp request again. Therefore, the interface cannot obtain the ip address promptly.

Configuration Steps

❖ **Configuring the Guest VLAN**

- (Optional) After the guest VLAN is configured on a port, check whether the port has 802.1X authentication clients. If no, add the port to the guest VLAN.
- Configure the guest VLAN after 802.1X authentication is enabled on the NAS.

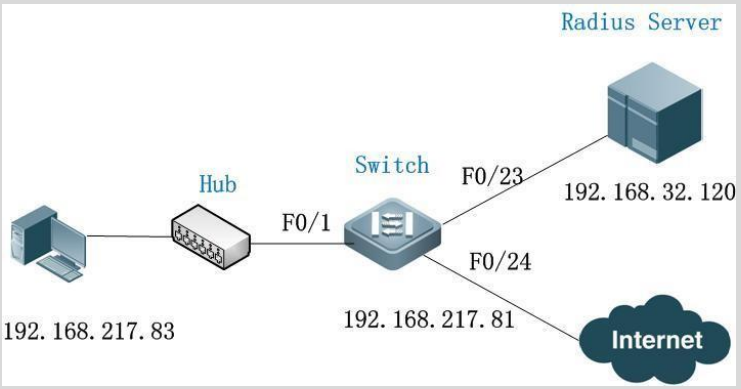
Command	**dot1x guest-vlan *vid***
Parameter Description	*vid*: Indicates the guest VLAN to join.
Defaults	The guest VLAN is not configured by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when a user connects to an 802.1X controlled port but has no authentication client. When guest VLAN is enabled on a port, do not configure Layer-2 attributes, and specially do not manually set the VLAN of the port.

Verification

- After a port switches to the guest VLAN, users connected to the port can communicate only in the guest VLAN.
- If a user connected to a port in the guest VLAN installs an 802.1X authentication client and initiates authentication, the port will exit the guest VLAN.

Configuration Example

❖ **Configuring Dynamic VLAN Assignment and Guest VLAN**

Scenario Figure 4-13	
Configuration Steps	▪ Enable 802.1X authentication on ports of the NAS. ▪ Enable dynamic VLAN assignment on a controlled port. ▪ Configure the guest VLAN on a controlled port. NAS configurations are as follows:
	`QTECH (config)# interface FastEthernet 0/1 QTECH (config-if)# dot1x port-control auto QTECH (config-if)# dot1x dynamic-vlan enable` `QTECH (config-if)# dot1x guest-vlan 3`
Verification	Check whether network access behaviors change after a port joins a guest VLAN. Users cannot communicate before the port joins the guest VLAN while can communicate after that. The NAS prints the log as follows:
	`%DOT1X-5-TRANS_DEFAULT_TO_GUEST: Transformed interface Fa0/1 from default-vlan 1 to` `guest-vlan 3 OK.`

Common Errors

- A port receives an EAPOL packet, causing its failure to join the guest VLAN.

4.4.10 Configuring the Failed VLAN

Configuration Effect

- Configure the failed VLAN on an 802.1X controlled port. If a user fails authentication after failed VLAN is enabled, the port can be added to a failed VLAN so that the user can still access the network.
- Configure the maximum number of consecutive authentication failures. If this number is exceeded, the NAS adds the port to a failed VLAN.

Notes

- If the failed VLAN configured does not exist, a failed VLAN will be dynamically created when a port enters the failed VLAN and automatically removed when the port exits the failed VLAN.
- 802.1X-based dynamic VLAN assignment must be enabled for a port.
- If a port goes down, the port will automatically exit the failed VLAN.
- The failed VLAN and guest VLAN can be configured to the same VLAN.
- In port-based control mode, after a controlled port enters a failed VLAN, only users failing authentication can re-initiate authentication and other users' authentication requests will be discarded. This restriction does not exist in MAC-based control mode.
- Failed VLAN does not support private VLANs. That is, private VLANs cannot be configured as 802.1X failed VLANs.
- If GSN address binding is enabled on a port, users in a failed VLAN cannot access the network.

Configuration Steps

❖ **Configuring the Failed VLAN**

- (Optional) If the failed VLAN is configured, the NAS adds users rejected by the authentication server to a failed VLAN.
- Configure the failed VLAN after 802.1X authentication is enabled on the NAS.

Command	**dot1x auth-fail vlan *vid***
Parameter Description	*vid*: Indicates the failed VLAN to join.
Defaults	Failed VLAN is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command if users need to access the network even after authentication fails.

❖ **Configuring the Maximum Number of Failed VLAN Attempts**

- (Optional) Configure the maximum number of times when a user is rejected by the authentication server. If this number is exceeded, the port can be added to a failed VLAN.
- Configure the maximum number of failed VLAN attempts after 802.1X authentication is enabled on the NAS.

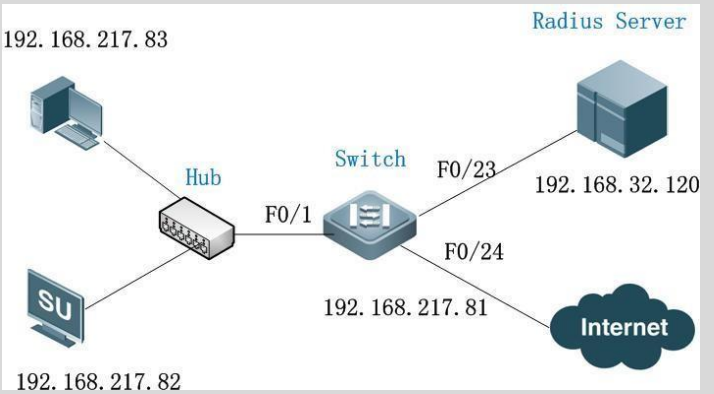
Command	dot1x auth-fail max-attempt *value*
Parameter Description	*value*: Indicates the maximum number of times when a user fails authentication.
Defaults	The default value is 3.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when the maximum number of failed VLAN attempts needs to be adjusted.

Verification

- When a port switches to a failed VLAN, users connected to the port can communicate only in the failed VLAN.

Configuration Example

❖ **Configuring the Failed VLAN**

Scenario **Figure 4-14**	
Configuration Steps	▪ Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ▪ Create an account on the RADIUS server. ▪ Enable AAA on the NAS. ▪ Configure RADIUS parameters on the NAS. ▪ Enable 802.1X authentication on ports of the NAS. ▪ Enable port-based authentication on a controlled port. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.

	QTECH# configure terminal QTECH (config)# aaa new-model QTECH (config)# radius-server host 192.168.32.120 QTECH (config)# radius-server key QTECH QTECH (config)# interface FastEthernet 0/1 QTECH (config-if)# dot1x port-control auto QTECH (config-if)# dot1x auth-fail vlan 3
Verification	Check whether authentication is proper, network access behaviors change after authentication, and dynamic users can access the network. ▪ The account is successfully created, such as **username:tests-user,password:test**. ▪ The user fails to ping 192.168.32.120 before authentication. ▪ Start QTECH Supplicant, enter incorrect account information, and click **Authenticate**. The authentication fails, the user can successfully ping the IP address of a failed VLAN. ▪ Information of the authenticated user is displayed.
	QTECH(config)#show dot1x user name ts-user Supplicant information: MAC address.....b048.7a7f.f9f3 Username ts-user User ID.....16777303 Type static VLAN.....1 Port.....wlan 1 Online duration.....0days 0h 0m21s Up average bandwidth.....0 kBps Down average bandwidth.....0 kBps Authorized VLAN.....1 Authorized session time.....20736000 seconds Authorized flux.....unlimited Accounting.....No Proxy user.....Permit Dial user.....Permit IP privilege.....0 Private supplicant.....no Authorized by Auth-Fail-Vlan.....3 Max user number on this port 0

Common Errors

- If a user fails authentication not due to rejection of the authentication server, for example, due to installation failure as a result of hardware resource insufficiency, it cannot enter the failed VLAN.

4.4.11 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 on network access. Enable active 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 QTECH Supplicant to perform 802.1 authentication. Therefore, you can use this function to detect whether QTECH Supplicant is used. For example, this function is required for MAB deployment.
- Configure the authenticable host list to specify users that can be authenticated on the port, which restricts physical access points of users to enhance network security
- The multi-account function allows a user to switch its account upon re-authentication. In special scenarios such as Windows domain authentication, multiple authentications are required to access the domain and the user account changes during authentication. This function applies to these scenarios.
- By default, the NAS uses its own MAC address as the source MAC address of EAP packets during 802.1X authentication. Some versions of QTECH supplicants check whether the access switch is a QTECH switch based on the MAC address of EAP packets and implement some private features. When performing 802.1X 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 user accounting, meeting service requirements. After a user is authenticated and goes online, the NAS can obtain the IP address of the user from the supplicant or through DHCP snooping, 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 failure to obtain the IP
  address of the authentication client, configure the IP detection timeout for this function. If the NAS does not obtain the IP address of the user within the configured time (5 minutes by default), it forces the user offline.
- The global 802.1X control switch is supported. If global 802.1X control is disabled, users can access the network without authentication and authenticated users are not affected. If global 802.1X control is enabled, users can access the network only after authentication.
- After 802.1X authentication is prevented from preempting MAB authentication resources, MAC authentication users will not be forced to get offline by eapol packets.
- Configure the rate for initiating authentication for to-be-authenticated users in a link table in a case of ARP-triggered MAB authentication.

- Configure the maximum number to-be-authenticated of users in a link table.

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 QTECH Supplicant are deployed. This function is not required because QTECH Supplicant can upload the IPv4 addresses of users.
  - Static IP addresses are deployed.

- After global 802.1X control is disabled, client authentication packets are discarded. A message is displayed on the client indicating that authentication cannot be performed. However, the network is available and users can access the network.
- After 802.1X authentication is prevented from preempting MAB authentication resources, 802.1X authentication can be performed only after the MAB authentication user gets offline.

Configuration Steps

❖ **Enabling Active Authentication**

- (Optional) If active authentication is enabled, the controlled port sends an authentication request actively after configuration. After receiving this request, the authentication client initiates 802.1X authentication.
- Enable active authentication after 802.1X authentication is enabled on the NAS.

Command	dot1x auto-req
Parameter Description	N/A
Defaults	Apart from on N1800K switches, active authentication is enabled by default.
Command Mode	Global configuration mode
Usage Guide	The destination addresses of active authentication packets are the multicast address. If the connected clients may not initiate authentication automatically, configure this command to make the NAS actively initiate authentication. When controlled ports are Trunk ports, enable active authentication so that authentication requests can be sent based on each VLAN of trunk ports.

❖ Configuring the Number of Active Authentication Requests

- (Optional) Configure the number of active authentication requests sent by the NAS.
- Configure the number of active authentication requests after 802.1X authentication is enabled on the NAS.

Command	dot1x auto-req packet-num*num*
Parameter Description	*num*: Indicates the number of active authentication requests.
Defaults	The number of active authentication request is not configured by default.
Command Mode	Global configuration mode
Usage Guide	If active authentication is enabled, configure this command to restrict the number of active authentication packets sent by a port and thereby avoid sending excessive packets.

❖ Enabling User Detection for Active Authentication

- (Optional) Configure the NAS not to send authentication requests actively if there are authenticated users on a controlled port.
- Enable user detection for active authentication after 802.1X authentication is enabled on the NAS.

Command	dot1x auto-req user-detect
Parameter Description	N/A
Defaults	User detection for active authentication is enabled by default.
Command Mode	Global configuration mode
Usage Guide	After this command is configured, the NAS does not send authentication packets actively if there are authenticated users on controlled Access ports. On Trunk ports, the NAS checks for authenticated users based each VLAN. If there are authenticated users on a VLAN, the NAS does not send authentication packets automatically.

❖ Configuring the Interval of Active Authentication Request

- (Optional) Configure the interval at which the NAS sends an authentication request

actively.

- Enable the interval of active authentication request after 802.1X authentication is enabled on the NAS.

Command	**dot1x auto-req req-interval *time***
Parameter Description	*Time*: Indicates the interval of active authentication request.
Defaults	The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ **Configuring the Authenticatable Client List**

- (Optional) Configure the authenticable client list on a controlled port. Only clients on the list can perform 802.1X authentication.
- Configure the authenticable client list after 802.1X authentication is enabled on the NAS.

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.
Defaults	All users can perform authentication.
Command Mode	Global configuration mode
Usage Guide	Configure this command when specified users should be able to perform authentication on a controlled port.

❖ **Enabling 802.1X Packets Sending with the Pseudo Source MAC Address**

- (Optional) Configure the **dot1x pseudo source-mac** command when QTECH Supplicant fails to identify the NAS as a QTECH device based on the MAC address of the NAS.
- Configure the pseudo MAC address as the source MAC address for 802.1X authentication after 802.1X authentication is enabled on the NAS.

Command	**dot1x pseudo source-mac**

Parameter Description	N/A
Defaults	User detection for active authentication is enabled by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command when QTECH Supplicants cannot identify the NAS as a QTECH device based on the source MAC address in the EAPOL packet sent by the NAS or implement private attributes during authentication. If this command is configured, the EAPOL packet sent by the NAS uses 00-1A-A9-17-FF-FF as the source MAC address so that these QTECH Supplicants can identify the NAS as a QTECH device.

❖ **Enabling Multi-account Authentication with One MAC Address**

- (Optional) Run the **dot1x multi-account enable** command to allow the same MAC address to be used by multiple accounts.
- Enable multi-account authentication with one MAC address after 802.1X authentication is enabled on the NAS.

Command	**dot1x multi-account enable**
Parameter Description	N/A
Defaults	Multi-account authentication is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command when multi-account authentication is required in 802.1X authentication, e.g. in the case of Windows domain authentication. In this case, the authentication client can directly use a new account to initiate authentication while the previous account is still online. Multi-account authentication is disabled by default.

❖ **Configuring the Maximum Number of Authenticated Users on a Port**

- (Optional) You can restrict the number of online users on a controlled port, including static users and dynamic users.
- Configure the maximum number of authenticated users on a port after 802.1X authentication is enabled on the NAS.

Command	dot1x default-user-limit *num*
Parameter Description	*num*: Indicates the maximum number of online users.
Defaults	There is no restriction on the number of users on a port by default.
Command Mode	Interface configuration mode/VXLAN 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**

- (Optional) If IP-triggered accounting is enabled, the NAS sends an accounting request to the authentication server after obtaining the IP address of the user.
- Enable IP-triggered accounting after 802.1X authentication is enabled on the NAS.

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	If both accounting and IP-triggered accounting are enabled, the NAS initiates accounting only after obtaining the IP address of the authentication client, and forces the user offline if it fails to obtain the IP address. If accounting is disabled but IP-triggered accounting is enabled, the NAS does not initiate accounting after obtaining the IP address of the authentication client, and forces the user offline if it fails to obtain the IP address within the timeout.

❖ **Configuring the Timeout of Obtaining IP Addresses After Authentication**

- (Optional) Configure the timeout of obtaining IP addresses if IP-triggered accounting is enabled.
- Configure the IP address obtaining timeout after 802.1X authentication is enabled on the NAS.

Command	dot1x valid-ip-acct timeout *time*

Parameter Description	*time:* Indicates the timeout in the unit of minutes.
Defaults	The default value is 5 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.

❖ **Using the Accounting Update Interval Delivered by the Server Upon the First Authentication**

- (Optional) If this function is enabled, online users always use the accounting update interval assigned by the authentication server upon the first authentication, instead of the accounting update interval configured on the NAS.

Command	**dot1x acct-update base-on first-time server**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command when the authentication server does not deliver the accounting update interval upon user re-authentication but the NAS must send accounting update packets according to the accounting update interval assigned by the authentication server upon the first authentication.

❖ **Disabling Global 802.1X**

- (Optional) This function is effective to both 802.1x and MAB-authenticated users.

Command	**dot1x system disable**
Parameter Description	-
Defaults	By default, global 802.1x is enabled.

Command Mode	Global configuration mode
Usage Guide	When the server is unreachable, disable global 802.1x, so users can access the Internet without authentication. After the server resumes reachability, enable global 802.1x, and users have to pass authentication before accessing the Internet.

❖ **Configuring the Rate for Initiating Authentication for To-be-authenticated Users in a Link Table in a Case of ARP-triggered MAB Authentication**

- (Optional) Configure the rate for initiating authentication for to-be-authenticated users in a link table in a case of ARP-triggered MAB authentication.
- 802.1X authentication and MAB authentication need to be enabled on the port.

Command	**dot1x pending-user authen-num *num***
Parameter Description	*num*: Indicates the number of authentications initiated every second for to-be-authenticated users in a link table.
Defaults	24
Command Mode	Global configuration mode
Usage Guide	Configure the rate for initiating authentication for to-be-authenticated users in a link table in a case of ARP-triggered MAB authentication.

❖ **Configuring the Maximum Number of To-be-authenticated Users in a Link Table in a Case of ARP-triggered MAB Authentication**

- (Optional) Configure the maximum number of to-be-authenticated users in a link table in a case of ARP-triggered MAB authentication.
- 802.1X authentication and MAB authentication need to be enabled on the port.

Command	**dot1x pending-user max-num *num***
Parameter Description	*num*: Indicates the maximum number of to-be-authenticated users in a link table.
Defaults	10000

Command Mode	Global configuration mode
Usage Guide	Configure the maximum number of to-be-authenticated users in a link table in a case of ARP-triggered MAB authentication.

❖ **Preventing 802.1X Authentication from Preempting MAB Authentication Resources**

- Optional. This function is configured to prevent 802.1X authentication packets from forcing MAB authentication users to get offline.
- 802.1X authentication and MAB authentication are enabled on the port.

Command	**dot1x mac-auth-bypass precedence**
Parameter Description	N/A
Defaults	By default, 802.1X authentication is prevented from preempting MAB authentication resources.
Command Mode	Interface configuration mode
Usage Guide	Enable this function to ensure that MAB authentication users will not be forced to get offline by 802.1X packets.

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**
Restores the default 802.1X	**dot1x default**

configuration.	

Notes

- The **dot1x default** command is used to restore global configurations.

Description	Command
Restore the default value of status machine timeout duration.	dot1x timeout quiet-period dot1x timeout server-timeout dot1x timeout supp-timeout dot1x timeout tx-period
Restore default values of configurations related to re-authentication.	dot1x re-authentication dot1x timeout re-authperiod dot1x reauth-max
Restore default values of configurations related to proactive requests.	dot1x auto-req dot1x auto-req user-detect dot1x auto-req req-interval dot1x auto-req packet-num
Restores the default value of the number of retransmission times.	dot1x mac-req
Restores the default value of the authentication mode.	dot1x auth-mode
Restore the default values of configurations related to client probing.	dot1x client-probe enable dot1x probe-timer alive dot1x probe-timer interval
Restores the default value of the function of supporting only the private client.	dot1x private-supplicant-only
Restores the default value of the pseudo source MAC address function.	dot1x pseudo source-mac
Restores the default value of the number of VLAN redirection times upon	dot1x auth-fail max-attempt

authentication failures.	
Restores the default value of the function of one MAC address for multiple accounts.	dot1x multiaccount enable
Restores the default value of the dot1x redirection function.	dot1x redirect
Restores the default value of the silent timeout duration.	dot1x multi-mab quiet-period
Restorethe default values of functions related to accounting after obtaining the IP address.	dot1x valid-ip-acct enable dot1x valid-ip-acct timeout

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/Challenge packet retransmission.	show dot1x max-req
Displays the information of controlled ports.	show dot1x port-control
Displays the non-QTECH client filtering information.	show dot1x private-supplicant-only
Displays the re-authentication status.	show dot1x re-authentication
Displays the maximum times of EAP-Request/Identity packet 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/Identity packet 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, disable the debugging switch immediately after use.

Description	Command
Debugs AAA. (For details, see the *Configuring AAA*.)	debug aaa
Debugs RADIUS. (For details, see the *Configuring RADIUS*.)	debug radius
Debugs 802.1X events.	debug dot1x event
Debugs 802.1X packets.	debug dot1x packet
Debugs 802.1X state machine (STM).	debug dot1x stm
Debugs 802.1X internal communication.	debug dot1x com
Debugs 802.1X errors.	debug dot1x error

5.1. Overview

5.1.1. Web Authentication

Web authentication controls user access to networks. It requires no authentication software on clients. Instead, users can perform authentication on common browsers.

When unauthenticated clients attempt to access the Internet using browsers, the network access server (NAS) forcibly redirects the browsers to a specified site pointing to a Web authentication server, also called a portal server. Users can access the services on the portal server before being authenticated, such as downloading security patches and reading notices. If a user wants to access network resources beyond the portal server, the user must get authenticated by the portal server through a browser.

Besides providing convenient authentication, the portal server performs Webpage interaction with browsers, providing personalized services, such as advertisements, notices, and business links on the authentication page.

QTECH Web Authentication Versions

There are three versions of QTECH Web authentication, including QTECH First-Generation Web Authentication, QTECH Second-Generation Web Authentication, and QTECH Internal Portal (iPortal) Web Authentication. The Web authentication process varies with authentication versions. For details, see Section 5.3 "Features".

The three versions of Web authentication are highly divergent in features and configurations. It is recommended to read through the relevant chapters carefully before configuration.

Both QTECH Second-Generation Web Authentication and QTECH iPortal Web Authentication support local account authentication on the NAS. Because Remote Authentication Dial In User Service (RADIUS) authentication is more

commonly used in reality, it is used as an example in the chapter "Applications".

The concept of "interface" varies with product types. For example, the interfaces on a layer-2 switch are physical ports. This document uses the unified term "interface" to include them. In application, recognize the real meaning based on

specific products and functions.

Web authentication supports user online traffic detection. For details, see the Configuring SCC.

Web authentication supports the authentication of domain names. That is, accounts can be authenticated in the format of user name@domain name. This requires enabling the domain-name-based authentication, authorization and accounting (AAA) service. For details, see the Configuring AAA.

Protocols and Standards

- HTTP: RFC1945 and RFC2068
- HTTPS: RFC2818
- SNMP: RFC1157 and RFC 2578
- RADIUS: RFC2865, RFC2866, and RFC3576

5.2. Applications

Application	Description
Basic Scenario of Web Authentication	Basic layer-2 authentication scenario, where a NAS, portal server, and RADIUS server constitute an authentication system which connects a client with the NAS through the layer-2 network.

5.2.1. Basic Scenario of Web Authentication

Scenario

See Figure 5-1.

- Deploy a Web authentication scheme on the NAS.
- The client connected to the NAS needs to pass Web authentication before accessing the Internet. Figure 5-1 Networking Topology of Web Authentication

Remarks	**Web authentication is applicable to both layer-2 and layer-3**

	networks. At layer 3, the source MAC address and VID of a packet are changed after it is routed, but the source IP address remains the same as the only identifier of a client. Therefore, the binding policy of Web authentication on layer-3 devices must adopt the IP-only binding mode. Here, layer-2 NAS is used as an example. **RG-SAM program is installed on the RADIUS server. RG-ePortal program is installed on the portal server.**

Deployment

- Enable Web authentication on the client-accessed interface or globally on the NAS (globally on on EG).
- Configure the ePortal server and the communication key on the NAS (for only QTECH First-Generation and Second-Generation Web Authentication).
- Configure the Simple Network Management Protocol (SNMP) communication parameters of the ePortal server on the NAS (for only QTECH First-Generation and Second-Generation Web Authentication).
- Configure the consistent communication parameters on the ePortal server and SAM server (for only QTECH First-Generation Web Authentication).
- Create user accounts on the SAM server.
- Configure AAA and method lists on the NAS (for only QTECH Second-Generation and iPortal Web Authentication).
- Configure the IP address of the SAM server on the NAS (for only QTECH Second-Generation and iPortal Web Authentication).
- Configure the names of the Web authentication method lists on the NAS (for only QTECH Second-Generation and iPortal Web Authentication).

5.3. Features

Basic Concepts

❖ QTECH First-Generation Web Authentication

QTECH First-Generation Web Authentication should cooperate with the RG-ePortal software. The server installed with RG-ePortal provides a login page to submit user authentication information, and initiates an authentication request to the RADIUS server directly. After authentication succeeds, the NAS gets user information delivered through the SNMP protocol, and thereby controls user

access permissions. Communication during Web authentication of this version depends on private SNMP nodes. Moreover, the ePortal server takes the place of the NAS in authentication and accounting, which relieves the NAS from service burden.

❖ **QTECH Second-Generation Web Authentication**

QTECH Second-Generation Web Authentication complies with the *CMCC WLAN Service Portal Specification*. The portal server is responsible only for Webpage interaction with users. The NAS interacts with the RADIUS server to implement authentication. The interaction between the portal server and the NAS complies with the *CMCC WLAN Service Portal Specification*. The portal server provides a login page for users to submit their information, and informs the NAS of user information through the portal protocols. The NAS completes authentication by interacting with the RADIUS server based on the user information, assigns access permissions to authenticated clients, and returns authentication results to the portal server.

The implementation process of QTECH Second-Generation Web Authentication is mainly completed on the NAS. This raises a higher demand on the NAS's capability to handle heavy tasks. Meanwhile, the portal server is simplified. The standard *CMCC WLAN Service Portal Specification*, which gains highly industry support, enables various vendors to develop compatible products.

❖ **Version Comparison**

Authentication roles:

- Client: Its functions are the same among the three types of Web authentication.
- NAS: In QTECH First-Generation Web Authentication, the NAS implements only URL redirection and exchanges user login/logout notifications with the portal server. In QTECH Second-Generation Web Authentication, the NAS is responsible for redirecting and authenticating users as well as notifying the portal server of authentication results.
- Portal server: In QTECH First-Generation Web Authentication, the portal server is responsible for interaction with clients through Webpages, authenticating users, and notifying the NAS of authentication results. In QTECH Second-Generation Web Authentication, the portal server is responsible for interacting with clients through Webpages, notifying the NAS of users' authentication information, and receiving authentication results from the NAS.
- RADIUS server: Its functions are the same among the three types of Web authentication. Authentication process:
- In QTECH Second-Generation Web Authentication, the authentication and accounting functions are transferred from the portal server to the NAS.
- Because authentication proceeds on the NAS, the second-generation NAS does not need to wait for the authentication results notified by the portal server as the first generation.

Logout process:

- In QTECH First-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, or traffic detection or port status detection performed by the NAS. In QTECH Second-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, a kickout notification from the RADIUS server, or traffic detection or port status detection performed by the NAS.
- In QTECH First-Generation Web Authentication, Accounting Stop packets are sent by the portal server. In QTECH Second-Generation Web Authentication, Accounting Stop packets are sent by the NAS.

The selection of the Web authentication versions depends on the type of the portal server in use.

Command parameters in this document may be shared by the three Web authentication versions or not. Read through this document carefully to avoid parameter misconfiguration that will affect Web authentication.

Overview

Feature	Description
QTECH First-Generation Web Authentication	The portal server is deployed and supports only QTECH First-Generation Web Authentication.
QTECH Second-Generation Web Authentication	The portal server is deployed and complies with the *CMCC WLAN Service Portal Specification*.

5.3.1. QTECH First-Generation Web Authentication

HTTP Interception

HTTP interception means the NAS intercepts to-be-forwarded HTTP packets. Such HTTP packets are initiated by the browsers of the clients connected to the NAS, but they are not destined for the NAS. For example, when a client attempts to visit the website www.google.com using the Internet Explorer, the NAS is expected to forward the HTTP request packets to the gateway. If HTTP interception is enabled, these packets will not be forwarded.

After HTTP interception is successful, the NAS redirects the HTTP requests from the client to itself to establish a session between them. Then, the NAS pushes a Webpage to the client through HTTP redirection, which can be used for authentication, software downloading or other purposes.

You can specify the clients and destination interfaces to enable or disable HTTP interception for Web authentication. In general, HTTP requests from unauthenticated clients will be intercepted, and those from authenticated clients will not. HTTP interception is the foundation of Web authentication. Web

authentication is automatically triggered once HTTP interception succeeds.

HTTP Redirection

According to HTTP protocols, after the NAS receives a HTTP GET or HEAD request packet from a client, a packet with 200 (Ok) status code is replied if it is able to provide the required resources, or a packet with 302 (Moved Temporarily) status code is returned if unable. Another URL is provided in the 302 packet. After receiving the packet, the client may resend a HTTP GET or HEAD request packet to the new URL for requesting resources. This process is called redirection.

HTTP redirection is an important procedure following HTTP interception in Web authentication. It takes the advantage of 302 status code defined in HTTP protocols. HTTP interception creates a session between the NAS and a client. The client sends HTTP GET or HEAD request packets (which should have been sent to another site) to the NAS. The NAS responds with a 302 packet with a specific redirection page. Thereby, the client resends the requests to the redirection page.

Because more and more application programs run HTTP protocols, the use of the 302 redirection packet may divert a large amount of HTTP traffic (not sent by browsers) to the portal server, which will affect network authentication. To address this problem, HTTP redirection technology on the NAS adopts noise reduction to replace the 302 packets with the **js** script.

Working Principle

Figure 5-1 shows the networking topology of Web authentication. First-generation Webauth roles:

- Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
- NAS: Is an access-layer device in a network. The NAS is directly connected to clients and must be enabled with Web authentication.
- Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, sends the information to the RADIUS server for authentication, and notifies the client and NAS of the authentication result. Figure 5-1 shows QTECH ePortal server.
- RADIUS server: Provides the RADIUS-based authentication service to remote clients. The portal server extracts users' authentication account information from HTTP packets and initiates authentication requests to the RADIUS server through the RADIUS protocol. The RADIUS server returns the authentication result to the portal server through the RADIUS protocol. Figure 5-1 shows the RADIUS server installed with the RG-SAM program.

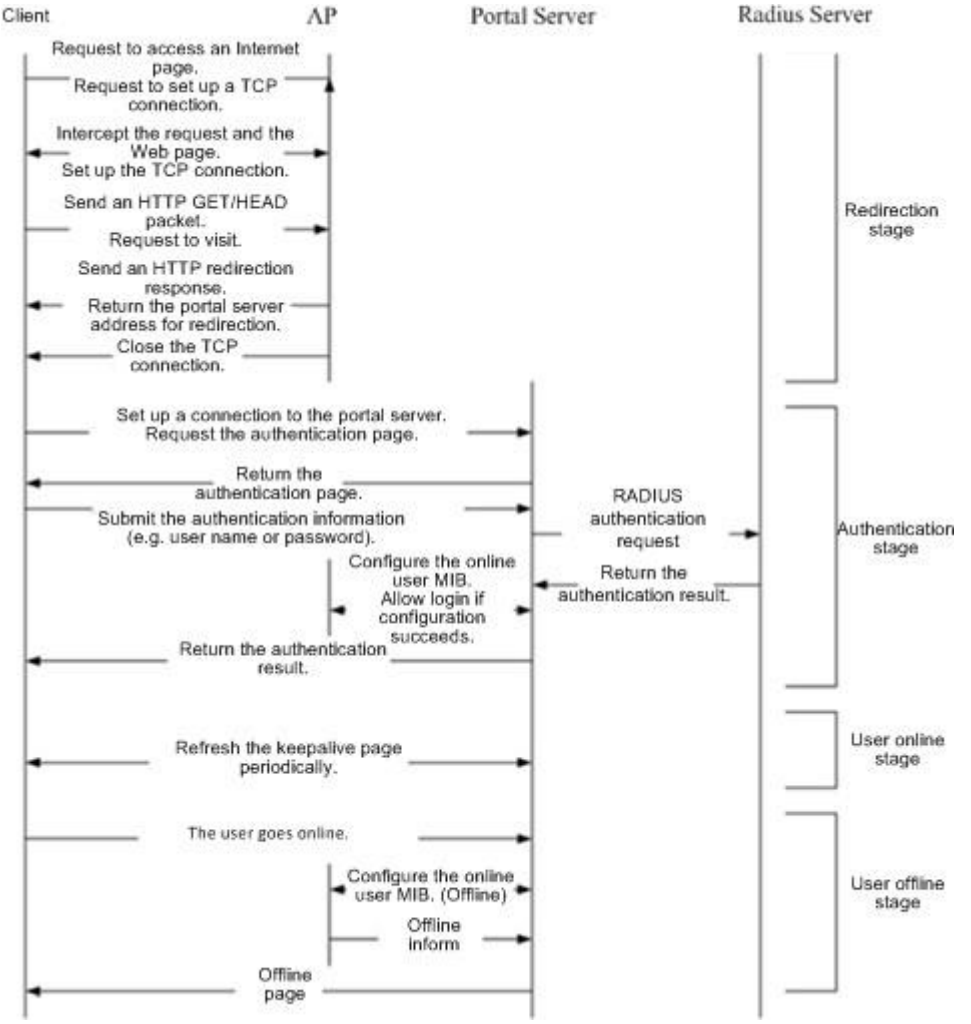
First-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication

page is displayed on the browser.

2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server and complete authentication.
3. After the user is authenticated, the portal server notifies the NAS that the client has passed authentication, and the NAS allows the client to access resources on the Internet.

Figure 5-2 shows the flowchart of QTECH First-Generation Web Authentication by using an AP as the NAS. Figure 5-2 Flowchart of QTECH First-Generation Web Authentication



First-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. Scenario 1: The NAS detects a client to logout and informs the portal server. Then the portal server deletes the user information on the NAS through SNMP and displays a logout page to the client.
2. Scenario 2: The portal server detects a client to logout and informs the NAS through SNMP and displays a logout page to the client.
3. In the two scenarios, the portal server sends an Accounting Stop request to the RADIUS server and notifies the RADIUS server that the client has logged out.

Related Configuration

- **Configuring the First-Generation Webauth Template**

By default, the first-generation Webauth template is not configured.

Run the **web-auth template eportalv1** command in global configuration mode to create the first-generation Webauth template.

The template is used to implement Web authentication.

- **Configuring the IP Address of the Portal Server**

By default, the IP address of the portal server is not configured.

Run the **ip** {*ip-address* } command in template configuration mode to configure the IP address of the portal server. Any request packets to access the portal server will be filtered and rate-limited by the NAS.

- **Configuring the Webauth URL of the Portal Server**

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server. The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

- **Specifying the Webauth Binding Mode**

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

- **Configuring the Webauth Communication Key**

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** {*string* } command in global configuration mode to configure the Webauth communication key. The communication key is used to encrypt URL parameters to avoid information disclosure.

- **Enabling QTECH First-Generation Web Authentication**

By default, QTECH First-Generation Web Authentication is disabled.

Run the **web-auth enable** command in interface configuration mode to enable QTECH First-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

- **Configuring the SNMP-Server Host**

By default, the SNMP-server host and community string are not configured.

Run the **snmp-server host** {*ip-address* }**version 2c** {*community-string* }**web-auth** command in global configuration mode to configure the SNMP-server host and community string for Web authentication.

The SNMP-server host is configured to receive Inform/Trap packets of user logout.

- **Configuring the SNMP-Server Community String**

By default, the SNMP-server community string is not configured.

Run the **snmp-server community** {*community-string*} **rw** command in global configuration mode to configure the SNMP-server community string.

The SNMP-server community string is configured to read/write user information from/to the NAS.

- **Enabling the SNMP Trap/Inform Function**

By default, the SNMP Trap/Inform function is disabled.

Run the **snmp-server enable traps web-auth** command in global configuration mode to enable the SNMP Trap/Inform function.

The SNMP Trap/Inform function is configured to enable the NAS to inform the portal server of user logout.

5.3.2. QTECH Second-Generation Web Authentication

HTTP Interception

Same as the HTTP interception technology of QTECH First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of QTECH First-Generation Web Authentication.

Working Principle

Figure 5-1 shows the networking topology of Web authentication.

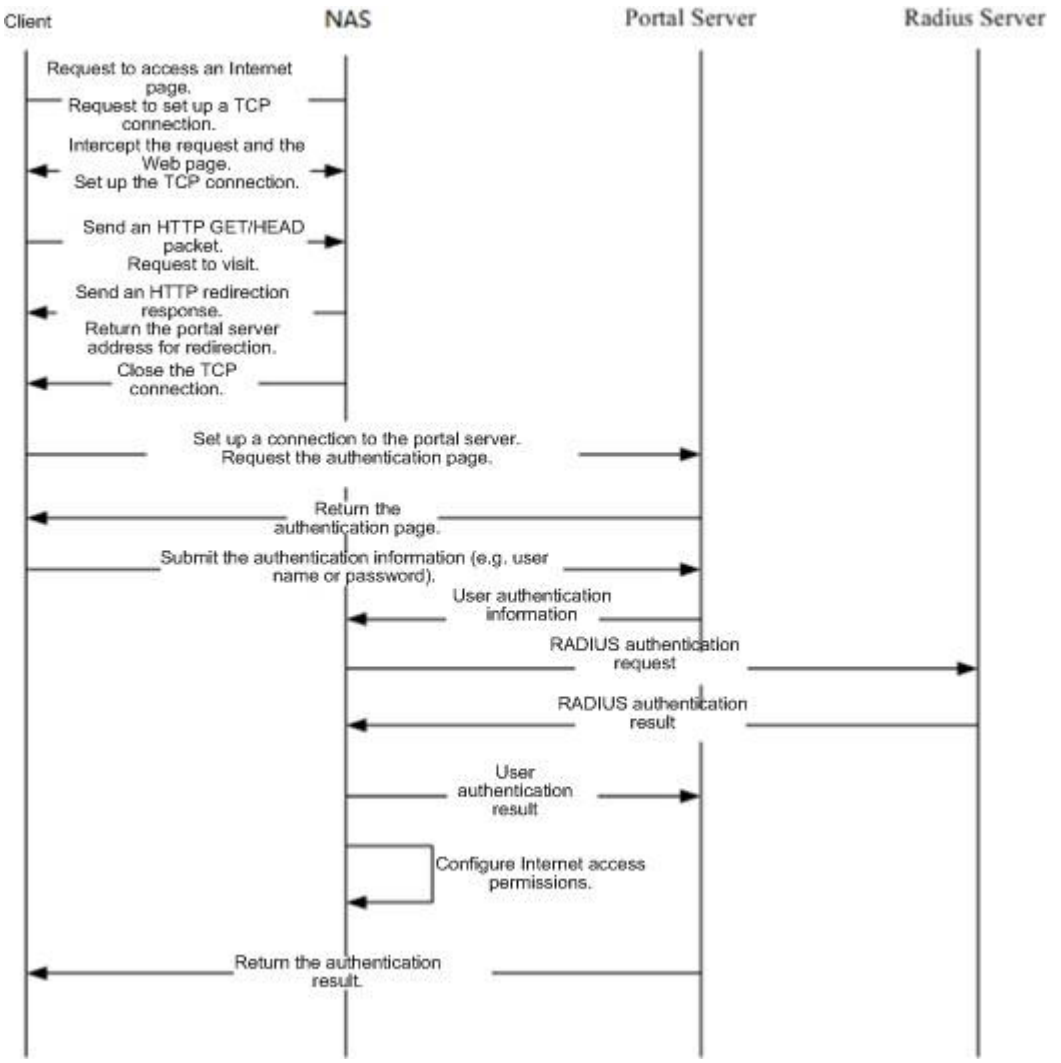
Second-generation Webauth roles:

1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network. The NAS is directly connected to clients and must be enabled with Web authentication. The NAS receives user authentication information from the portal server, sends authentication requests to the RADIUS server, determines whether users can access the Internet according to authentication results, and returns the authentication results to the portal server.
3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, transfers the information to the NAS, and displays the authentication result returned by the NAS to the user on a page. Figure 5-1 shows QTECH ePortal server.
4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. Figure 5-1 shows the RADIUS server installed with the RG-SAM program.

Second-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server.
3. The portal server sends the user authentication information to the NAS.
4. The NAS initiates authentication to the RADIUS server and returns the authentication result to the portal server.
5. The portal server displays the authentication result (success or failure) to the user on a page.

Figure 5-3 Flowchart of QTECH Second-Generation Web Authentication



Second-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. When a user clicks the **Logout** button on the online page, the portal server notifies the NAS to get the user offline.
2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.
3. When the RADIUS server plans to force a client offline based on a certain policy, the NAS notifies the portal server to push a logout page to the client.

Related Configuration

- **Configuring the Second-Generation Webauth Template**

By default, the second-generation Webauth template is not configured.

Run the **web-auth template{eportalv2 |** *template-name* **v2}** command in global configuration mode to create a second-generation Webauth template.

The template is used to implement Web authentication.

- **Configuring the IP Address of the Portal Server**

By default, the IP address of the portal server is not configured.

Run the **ip** { *ip-address* } command in template configuration mode to configure the IP address of the portal server. Any request packets to access the portal server will be filtered and rate-limited by the NAS.

- **Configuring the Webauth URL of the Portal Server**

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server. The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

- **Specifying the Webauth Binding Mode**

The default Webauth binding mode is IP binding mode on EG and NBR.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

- **Configuring the Webauth Communication Key**

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** { *string* } command in global configuration mode to configure the Webauth communication key. The communication key is used to encrypt URL parameters to avoid information disclosure.

- **Enabling QTECH Second-Generation Web Authentication**

By default, QTECH Second-Generation Web Authentication is disabled.

Run the **web-auth enable {eportalv2 |** *template-name* **v2}** command in interface configuration mode to enable QTECH Second-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

- **Enabling AAA**

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

QTECH Second-Generation Web Authentication relies on AAA. Enable AAA before you implement the former.

- **Configuring the RADIUS-Server Host and Communication Key**

By default, the RADIUS-server host and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS-server host and communication key.

The RADIUS-server host is responsible for authenticating users.

- **Configuring an AAA Method List for QTECH Second-Generation Web Authentication**

By default, no AAA method list is configured for QTECH Second-Generation Web Authentication.

Run the **aaa authentication web-auth** command in global configuration mode to configure an AAA method list for QTECH Second-Generation Web Authentication.

The AAA authentication method list is used for interaction during the Webauth process.

- **Configuring an AAA Method List for QTECH Second-Generation Web Accounting**

By default, no AAA method list is configured for QTECH Second-Generation Web Accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for QTECH Second-Generation Web Accounting.

The AAA method list for Web accounting is used for accounting interaction during the Webauth process.

- **Specifying an AAA Method List**

The default AAA method list is used if no list is specified.

Run the **authentication** command in template configuration mode to specify an AAA method list. The AAA method list is specified to send authentication requests to AAA.

- **Specifying an AAA Accounting Method List**

The default AAA accounting method list is used if no list is specified.

Run the **accounting** command in template configuration mode to specify an AAA accounting method list.

The AAA accounting method list is specified to send accounting requests to AAA.

❖ **Specifying the UDP Port of the Portal Server**

By default, UDP Port 50100 is used.

Run the **port** command in template configuration mode to specify the UDP port of the portal server. The UDP port is specified for the portal server to communicate with the NAS.

5.4. Configuration

Configuration	Description and Command	
Configuring First-Generation Authentication QTECH Web	(Mandatory) It is used to set the basic parameters of QTECH First-Generation Web Authentication.	
	web-auth template eportalv1	Configures the first-generation Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.
	web-auth portal key { *key-string* }	Configures the Webauth communication key.
	snmp-server community { *community-string* } **rw**	Configures the SNMP-server community string.
	snmp-server host { *ip-address* } **inform version** 2c { *community-string* } **web-auth**	Configures the SNMP-server host.
	snmp-server enable traps web-auth	Enables the SNMP-server Trap/Inform function.
	web-auth enable	Enables QTECH First-Generation Web Authentication on an interface.

Configuring Second-Generation Authentication QTECH Web	(Mandatory) It is used to set the basic parameters of QTECH Second-Generation Web Authentication.	
	aaa new-model	Enables AAA.
	radius-server host {*ip-address*}[**auth-port** *port-number*] [**acct-port** *port-number*] **key** {*string*}	Configures the RADIUS-server host and communication key.
	aaa authentication web-auth { **default** |*list-name* } *method1* [*method2*...]	Configures an AAA method list for Web authentication. (RADIUS authentication is implemented.)
Configuration	Description and Command	
	aaa accounting network {**default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for Web Accounting. (RADIUS accounting is implemented.)
	web-auth template{**eportalv2 |***portal-name***v2**}	Configures a second-generation Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.
	web-auth portal key { *key-string* }	Configures the Webauth communication key.
	web-auth enable	Enables QTECH Second-Generation Web Authentication on an interface.
Specifying an Authentication Method List	(Optional) It is used to specify an AAA authentication method list in template configuration mode. The name of the method list must be correctly specified.	
	authentication { *mlist-name* }	Specifies an AAA authentication method list(only for QTECH Second-Generation Web Authentication and QTECH iPortal Web Authentication.)

Specifying an Accounting Method List	(Optional) It is used to specify an AAA accounting method in template configuration mode. The name of the method list must be correctly specified.	
	accounting { *mlist-name* }	Specifies an AAA accounting method list(only for QTECH Second-Generation Web Authentication and QTECH iPortal Web Authentication.)
Configuring the Communication Port of the Portal Server	(Optional) It is used to specify the UDP port of the portal server in template configuration mode. The configured port number must be consistent with that on the RADIUS server.	
	port { *port-num* }	Configures the communication port of the portal server.
Specifying the Webauth Binding Mode	(Optional) It is used to specify the entry binding mode in template configuration mode.	
	bindmode {ip-mac-mode | ip-only-mode}	Specifies the template binding mode.
Configuring the Redirection HTTP Port	(Optional) It is used to configure the TCP interception port for redirection, so that the packets on the specified port can be redirected when interception is enabled.	
	http redirect port { *port-num* }	Configures the redirection TCP port.
Configuring Rate Limit	(Optional) It is used to configure the syslog function in Web authentication.	
Configuration	Description and Command	
Webauth Logging	**web-auth logging enable** {*num* }	Configures the rate limit Webauth logging.
Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients	(Optional) It is used to adjust the HTTP session limit. The limit value needs to be increased when there are many sessions in the background.	
	http redirect session-limit { *session-num* } [**port** { *port-session-num* }]	Configures the maximum number of HTTP sessions for unauthenticated clients.

Configuring the HTTP Redirection Timeout	(Optional) It is used to modify the timeout period for redirection connections. The timeout needs to be increased to complete redirection when the network condition is bad.	
	http redirect timeout{ *seconds* }	Configures the HTTP redirection timeout.
Configuri the Straight-Through ARP Resource Range	(Optional) It is used to permit the ARP of the specified addresses to pass. The gateway ARP must be permitted to pass when ARP check is enabled.	
	http redirectdirect-arp {*ip-address* [*ip-mask*] }	Configures the straight-through ARP resource.
Configuring an	(Optional) It is used to exempt clients from authentication when accessing the Internet.	
	web-auth direct-host { *ip-address* [ip-*mask*] [**arp**] } [**port** *interface-name* | *mac-address* }	Configures the range of the IP or MAC addresses of clients free from authentication.
Configuring the Interval for Updating Online User Information	(Optional) It is used to configure the interval for updating online user information.	
	web-auth update-interval *{ seconds }*	Configures the interval for updating online user information.
Configuring Portal Detection	(Optional) It is used to detect the availability of the portal server. If it is not available, the services are switched to the standby portal server. This function must be used together with portal standby function.	
	web-auth portal-check [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries**]**	Configures the portal server detection interval, timeout period, and timeout retransmission times.
Configuring Portal Escape	(Optional) It is used to allow new clients to access the Internet without authentication when the portal server is not available.	
	web-auth portal-escape	Configures portal escape.

Enabling DHCP Address Check	(Optional) It is used to check whether the IP address of a client is allocated by the DHCP server. If not, the client's authentication request is denied.	
	web-auth dhcp-check	Checks whether the IP address of a client is assigned by the DHCP server.
Disabling Portal Extension	(Optional) It is used to disable portal extension in order to interwork with CMCC standard portal server. Portal extension must be enabled for interworking with QTECH portal server software.	
	no web-auth portal extension	Disables portal extension.
Configuring a Whitelist	(Optional) It is used to configure a whitelist to allow unauthenticated clients to access some network resources.	
	web-auth acl white-url *name*	Configures a whitelist.
Configuring the Portal Communication Port	(Optional) It is used to configure the port (source port) used for the communication between the NAS and portal server.	
	ip portal source-interface *interface-type interface-num*	Specifies the port used for the communication between the NAS and portal server.
Configuring VLAN-Based Authentication on a Port	(Optional) It is used to configure the VLAN in which only the STAs inside the configured VLAN cannot initiate Web authentication.	
	web-auth vlan-control *vlan-list*	Configures the VLAN-based authentication on a port.
Disabling DHCP Server Detection	(Optional) It is used to disable DHCP server detection.	
	no web-auth dhcp-server check	Disables the DHCP server detection.

5.4.1. Configuring QTECH First-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication.

Notes

N/A

Configuration Steps

- **Configuring the Portal Server**
  - (Mandatory)To enable Web authentication successfully, you must configure and apply the portal server.
  - When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.
- **Configuring the Communication Key Between the NAS and Portal Server**
  - (Mandatory) To enable Web authentication successfully, you must configure the key used for the communication between the NAS or convergence device and portal server.
  - When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.
- **Setting the SNMP Parameters Between the NAS and Portal Server**
  - (Mandatory) To enable Web authentication successfully, you must set the SNMP network management parameters used for the communication between the NAS and portal server.
  - The NAS or convergence device and portal server jointly manage authenticated clients through SNMP/MIB. A table of authenticated clients is managed by MIB on the NAS. The portal server is able to access the MIB to obtain client statistics so as to control client login and logout. When a client logs out, the NAS or convergence device will inform the portal server by Webauth Inform packets.
- **Enabling QTECH First-Generation Web Authentication on an Interface**
  - Mandatory.
  - When QTECH First-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.

- Check whether authenticated clients can access the Internet normally.

Related Commands

❖ **Configuring the First-Generation Webauth Template**

Command	**web-auth template eportalv1**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	**eportalv1** is the default template of QTECH First-Generation Web Authentication.

❖ Configuring the IP Address of the Portal Server

Command	**ip {*ip-address*}**
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

❖ Configuring the Webauth URL of the Portal Server

Command	**url {*url-string*}**
Parameter Description	*url-string*: Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

❖ Configuring the Format of the Webauth URL

Command	▪ **fmt { ace | QTECH }**

Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	ACE association is supported when **fmt** is set to **ace**.

❖ Specifying the Webauth Binding Mode

Command	▪ **bindmode { ip-mac-mode | ip-only-mode }**
Parameter Description	Indicates the Webauth binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

❖ Specifying the Redirection Method

Command	▪ **redirect { http | js }**
Parameter Description	Indicates the encapsulation format of redirected packets.
Command Mode	Webauth template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

❖ Configuring the Webauth Communication Key

Command	**web-auth portal key {*key-string*}**
Parameter Description	*key-string:* Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring the SNMP-Server Community String

Command	**snmp-server community {*community-string*}rw**
Parameter Description	*community-string*: Indicates the community string. **rw**: Must be set to **rw** to support the read and write operations as the Set operation on MIB is required.
Command Mode	Global configuration mode
Usage Guide	The SNMP-server community string is used by the portal server to manage the online clients on the NAS or convergence device.

❖ Configuring the SNMP-Server Host

Command	**snmp-server host {*ip-address*} inform version 2c {*community-string*} web-auth**
Parameter Description	*ip-address*: Indicates the IP address of the SNMP-server host, that is, the portal server. *community-string*: Configures the community string used to send an SNMP Inform message.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP-server host to receive Webauth messages, including the type, version, community string, and other parameters. **inform:** Enables the SNMP Inform function. The NAS or convergence device will send a message to the portal server when a client logs out. The message type is set to Inform instead of Trap to avoid message loss. **version 2c**: Indicates SNMPv2 for SNMP Inform is not supported in all SNMP versions excluding SNMPv1. **web-auth**: Indicates the preceding parameters to be used for Web authentication. For details regarding SNMP configuration and others, see the *Configuring SNMP*. The SNMP parameter **version 2c**listed here is aimed at SNMPv2. SNMPv3 is recommended if higher security is required for the SNMP communication between the NAS and portal server. To use SNMPv3, change **SNMP Community** to **SNMP User**, **version 2c** to **SNMPv3**, and set SNMPv3-related security parameters. For details, see the *Configuring SNMP*.

❖ Enabling the Webauth Trap/Inform Function

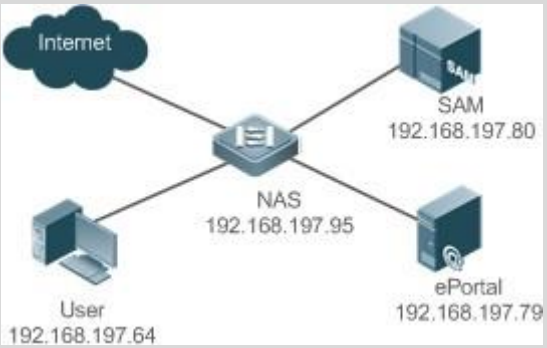
Command	▪ snmp-server enable traps web-auth
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the NAS or convergence device to send Webauth Trap and Inform messages externally. web-auth: Indicates Web authentication messages.

❖ Enabling QTECH First-Generation Web Authentication on an Interface

Command	web-auth enable
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring QTECH First-Generation Web Authentication

Scenario Figure 5-4	

Configuration Steps	▪ On the NAS, configure the IP address of the ePortal server and the key (QTECH) used for communicating with the ePortal server. ▪ Configure the Webauth URL on the NAS. ▪ Set the SNMP network management parameters (community string: public) used for the communication between the NAS and ePortal server. ▪ Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.

	`QTECH# config`
	
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`QTECH(config)#web-auth template eportalv1 QTECH(config.tmplt.eportalv1)#ip 192.168.197.79 QTECH(config.tmplt.eportalv1)#exit`
	`QTECH(config)# web-auth portal key QTECH`
	`QTECH(config)# web-auth template eportalv1`
	`QTECH(config.tmplt.eportalv1)#url http://192.168.197.79:8080/eportal/index.jsp`
	`QTECH(config.tmplt.eportalv1)#exit`
	`QTECH(config)# snmp-server community public rw`
	`QTECH(config)# snmp-server enable traps web-auth`
	`QTECH(config)# snmp-server host 192.168.197.79 inform version 2c public web-auth`
	`QTECH(config)# exit`
	`QTECH(config)# interface range GigabitEthernet 0/2-3`
	`QTECH(config-if-range)# web-auth enable QTECH(config-if-range)# exit`

Verification	Check whether Web authentication is configured successfully.

	QTECH(config)#show running-config … snmp-server host 192.168.197.79 inform version 2c public web-auth snmp-server enable traps web-auth snmp-server community public rw … web-auth template eportalv1 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp ! web-auth portal key QTECH … interface GigabitEthernet 0/2 web-auth enable ! interface GigabitEthernet 0/3 web-auth enable
	QTECH#show web-auth control Port Control Server Name Online User Count … GigabitEthernet 0/2On eportalv1 0 GigabitEthernet 0/3On eportalv1 0
	QTECH#show web-auth template Webauth Template Settings: Name: eportalv1 Url: http://17.17.1.21:8080/eportal/index.jsp Ip..... 17.17.1.21 BindMode: ip-mac-mode Type: v1 ……

Common Errors

- The SNMP parameters used for the communication between the portal server and NAS are configured incorrectly, causing authentication failures.
- Specify the IP-MAC binding mode to deploy Web authentication on layer-3 networks, causing authentication failures.

5.4.2. Configuring QTECH Second-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication. IPv6 is supported.

Notes

- QTECH Second-Generation Web Authentication complies with the CMCC WLAN Service Portal Specification. Furthermore, it is extended to support QTECH portal server. Perform compatible configuration based on the server performance in actual deployment. For details, see the subsequent chapter.
- The cmcc-normal and cmcc-ext1 parameters in the fmt command support only IPv4. If IPv6 is used, the configuration of the portal server is invalid.

Configuration Steps

❖ **Enabling AAA**

- (Mandatory) To enable QTECH Second-Generation Web Authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in QTECH Second-Generation Web Authentication.

❖ **Configuring the RADIUS-Server Host and Communication Key**

- (Mandatory) To enable QTECH Second-Generation Web Authentication, you must configure the RADIUS server.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

❖ **Configuring an AAA Method List for Web Authentication**

- (Mandatory) To enable QTECH Second-Generation Web Authentication, you must configure an AAA authentication method list.
- An AAA authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the method list.

❖ **Configuring an AAA Method List for Web Accounting**

- (Mandatory) To enable QTECH Second-Generation Web Authentication, you must configure an AAA method list for Web accounting.

- An accounting method list is used to associate an accounting method and server. In Web authentication, accounting is implemented to record client fees.

❖ **Configuring the Portal Server**

- (Mandatory) To enable QTECH Second-Generation Web Authentication, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

❖ **Configuring the Communication Key Between the NAS and Portal Server**

- (Mandatory) To enable QTECH Second-Generation Web Authentication, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

❖ **Configuring the Portal Server in Global or Interface Configuration Mode**

- (Mandatory) To enable QTECH Second-Generation Web Authentication, you must specify the use of the second generation portal server in global or interface configuration mode.
- The NAS first selects the portal server in interface configuration mode. If such a portal server does not exist, the NAS selects the portal server in global configuration mode. If such a portal server does not exist, eportalv1 is used by default. The NAS redirects users to the selected portal server.

❖ **Enabling QTECH Second-Generation Web Authentication on an Interface**

- Mandatory.
- When QTECH Second-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

❖ **Enabling AAA**

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

❖ Configuring the RADIUS-Server Host and Communication Key

Command	**radius-server host {*ip-address*} [auth-port*port-number1*] [acct-port *port-number 2*] key {*string*}**
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

❖ Configuring an AAA Method List for Web Authentication

Command	**aaa authentication web-auth { default | *list-name* } *method1* [*method2*...]**
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	QTECH Second-Generation Web Authentication adopts the RADIUS authentication method.

❖ Configuring an AAA Method List for Web Accounting

Command	**aaa accounting network { default | *list-name* } start-stop *method1* [*method2*...]**
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	QTECH Second-Generation Web Authentication adopts the RADIUS accounting method.

❖ Configuring the Second-Generation Webauth Template

Command	**web-auth template{eportalv2 | *portal-name* v2}**
Parameter Description	*portal-name*: Indicates the customized portal server name.
Command Mode	Global configuration mode
Usage Guide	**eportalv2** indicates the default template of QTECH Second-Generation Web Authentication.

❖ Configuring the IP Address of the Portal Server

Command	**ip { *ip-address* | *ipv6-address* }**
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

❖ Configuring the Webauth URL of the Portal Server

Command	**url { *url-string* }**

Parameter Description	Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

❖ Configuring the Format of the Webauth URL

Command	**fmt { cmcc-ext1 | cmcc-ext2 | cmcc-mtx | cmcc-normal | ct-jc }**
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	The **cmcc-normal** and **cmcc-ext1** parameters in the **fmt** command support only IPv4. The **cmcc-ext2** is supported for Liaoning CMCC. When **fmt** is set to **cmcc-mtx**, the URL format of mobile AC vendors is supported. The **ct-jc** format is supported for Chine Telecom. The **custom** format is defined by users.

❖ Specifying the Encapsulation Format of Redirected Packets

Command	**redirect { http | js }**
Parameter Description	Indicates the encapsulation format of redirected packets.
Command Mode	Webauth template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

❖ Specifing the Template Binding Mode

Command	**bindmode {ip-mac-mode | ip-only-mode}**
Parameter Description	Indicates the template binding mode.

Command Mode	Webauth template configuration mode
Usage Guide	N/A

❖ Configuring the Webauth Communication Key

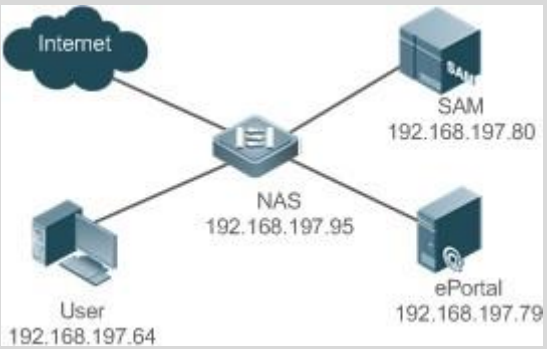
Command	**web-auth portal key { *key-string* }**
Parameter Description	*key-string*: Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Enabling QTECH Second-Generation Web Authentication on an Interface

Command	**web-auth enable {eportalv2 | *template-name*}**
Parameter Description	Indicates a Webauth template.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring QTECH Second-Generation Web Authentication

Scenario Figure 5-5	

Configuration Steps	▪ Enable AAA on the NAS. ▪ Configure the RADIUS-server host and communication key on the NAS. ▪ Configure the default AAA method lists for Web authentication and accounting on the NAS. ▪ Configure the IP address of the portal server and the Webauth communication key (QTECH) used for communicating with the portal server on the NAS. ▪ Configure the Webauth URL on the NAS. ▪ Configure QTECH Second-Generation Web Authentication in global configuration mode on the NAS. ▪ Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	QTECH#configure Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#aaa new-model QTECH(config)#radius-server host 192.168.197.79 key QTECH QTECH(config)#aaa authentication web-auth default group radius QTECH(config)#aaa accounting network default start-stop group radius QTECH(config)#web-auth template eportalv2 QTECH(config.tmplt.eportalv2)#ip 192.168.197.79 QTECH(config.tmplt.eportalv2)#exit QTECH(config)#web-auth portal key QTECH QTECH(config)# web-auth template eportalv2 QTECH(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp QTECH(config.tmplt.eportalv2)#exit QTECH(config)# interface range GigabitEthernet 0/2-3 QTECH(config-if-range)# web-auth enable eportalv2 QTECH(config-if-range)# exit BindMode: ip-mac-mode Type: v2 Port: 50100 State: Active Acctmlist: default Authmlist: default …

Common Errors

- The communication key between the portal server and NAS is configured incorrectly or only on the portal server or NAS, causing authentication errors.
- The communication parameters of the RADIUS server and NAS are set incorrectly, causing authentication errors.
- The portal server does not support the *CMCC WLAN Service Portal Specification*,

causing compatibility failure.

5.4.3. Specifying an Authentication Method List

Configuration Effect

- The portal server sends an authentication request to the NAS when a user submits authentication information. The NAS resolves the authentication server information and other information based on the configured authentication method list name before initiating authentication.
- The NAS selects the authentication server based on the specified authentication method list.

Notes

- Before you configure an authentication method list name, ensure that the authentication methods in the list have been configured on the AAA module. The command used to configure authentication methods on the AAA module is **aaa authentication web-auth** { **default** | *list-name* }*method1* [*method2*...].
- Different authentication methods for IPv4 authentication and IPv6 authentication are not supported.

Configuration Steps

- Optional.
- The default authentication method is used if no authentication method list is configured. Run the **authentication**

  { *mlist-name* } command to configure an authentication method list name when the authentication method list name on the AAA module needs to be modified or multiple method lists exist.

Verification

- Configure two authentication method lists on the AAA module. Apply list 1 to server 1 and list 2 to server 2.
- Create user a and configured a password for the user on server 1. Create user b on server 2.
- Configure the use of list 1.
- Perform authentication as user b and check that authentication fails.
- Perform authentication as user a and check that authentication is successful.

Related Commands

❖ **Specifying an Authentication Method List**

Command	**authentication {*mlist-name*}**

Parameter Description	Indicates a method list name.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured authentication method list name is consistent with that on the AAA module.

Configuration Example

- Specifying an Authentication Method List

Configuration Steps	**Specify the authentication method list mlist1.**
	`QTECH(config.tmplt.iportal)#authentication mlist1`
Verification	Check whether the configuration is successful.

	`QTECH#show web-auth template Webauth`
	`Template Settings:`
	
	`Name: eportalv2`
	
	`Url: http://17.17.1.21:8080/eportal/index.jsp Ip:17.17.1.21`
	`BindMode: ip-only-mode`
	`Type: v2`
	`Port: 50100`
	
	`State: Active`
	`Acctmlist:`
	`default`
	`Authmlist:`
	`mlist1`

5.4.4. Specifying an Accounting Method List

Configuration Effect

- The NAS sends an accounting request when a user passes authentication. The recipient of the request depends on the configuration of the accounting method list and is usually the portal server.
- Specify an accounting method list for the NAS to perform accounting.

Notes

- Ensure that the accounting method list has been configured on the AAA module. The command used to configure accounting methods on the AAA module is **aaa accounting network** {**default** | *list-name* }start-stop method1 [method2...].
- Different accounting methods for IPv4 authentication and IPv6 authentication are not supported.

Configuration Steps

- Optional.
- The default accounting method is used if no accounting method list is configured. Run the **accounting** {*mlist-name* } command to configure an accounting method list name when the accounting method list name on the AAA module needs to be modified or multiple method list names exist.

Verification

- Configure two accounting method lists on the AAA module. Apply list 1 to server 1 and list 2 to server 2.
- Configure the use of list 1.
- Use a valid account to perform authentication to access the Internet.
- View user accounting information on server1 and server2. Check that the user accounting information exists only on server1.

Related Commands

❖ **Specifying an Accounting Method List**

Command	**accounting{*mlist-name*}**
Parameter Description	Indicates a method list name.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured accounting method list name is consistent with that on the AAA module.

Configuration Example

❖ Specifying an Accounting Method List

Configuration Steps	**Specify the accounting method list mlist1.**

	QTECH(config.tmplt.eportalv2)#accounting mlist1
Verification	Check whether the configuration is successful.
	QTECH#show web-auth template Webauth Template Settings: Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip 17.17.1.21 BindMode: ip-mac-mode Type: v2 Port: 50100 State: Active Acctmlist: mlist1 Authmlist: mlist1

5.4.5. Configuring the Communication Port of the Portal Server

Configuration Effect

- When the NAS detects that a user logs out, it notifies the portal server. The NAS interacts with the portal server through the portal specification, which specifies the port number used to listen to and send/receive packets.
- When the listening port of the portal server is changed, the communication port of the portal server must be modified on the NAS to enable the NAS to interact with the portal server.
- In QTECH iPortal Web Authentication, this function is used to configure the HTTP listening port of the NAS. The default port number is 8081.

Notes

- The configured port number must be consistent with the port actually used by the portal server.
- This function is applicable to QTECH Second-Generation Web Authentication and iPortal Web Authentication. The two authentication schemes use different default port numbers. In QTECH Second-Generation Web Authentication, the configured port number is used for the interaction between the NAS and portal server through the portal specification. In QTECH iPortal Web Authentication, the configured port number is used for packet listening on the NAS.

Configuration Steps

- Optional.
- Run the **port** *port-num* command to maintain port configuration consistency

when the portal server does not use the default port number or the listening port of the NAS conflicts with other port and needs to be adjusted.

Verification

- Configure QTECH Second-Generation Web Authentication.
- Change the listening port of the server to 10000.
- Run the **port** *port-num* command to configure the port number 10000.
- Simulate the scenario where a user performs authentication to access the Internet.
- Force the user offline on the NAS, refresh the online page, and check that a user logout notification is displayed.

Related Commands

❖ **Configuring the Communication Port of the Portal Server**

Command	**port *port-num***
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring the Communication Port of the Portal Server

Configuration Steps	**Configure the communication port of the portal server as port 10000.**
	QTECH(config.tmplt.eportalv2)#port 10000
Verification	Check whether the configuration is successful.
	QTECH#show web-auth template Webauth Template Settings: Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip 17.17.1.21 BindMode: ip-only-mode Type: v2

Configuration Steps	Configure the communication port of the portal server as port 10000.
	QTECH(config.tmplt.eportalv2)#port 10000
Verification	Check whether the configuration is successful.
	Port: 10000 Acctmlist: Authmlist:

5.4.6. Specifying the Webauth Binding Mode

Configuration Effect

- When a user goes online, the user's entry needs to be written to a forwarding rule. The forwarding rule mapping method can be modified by specifying different binding modes, which further affects the Internet access rules applied to users. In IP-only mode, all the packets carrying the specified IP address are permitted to pass, and the STAs who send the packets can access the Internet. In IP+MAC mode, only the packets carrying both the specified IP address and MAC
address are permitted to pass, and the STAs who send the packets can access the Internet.

Notes

- In Layer-3 authentication, the MAC addresses visible to the NAS are the gateway addresses of STAs. Because these MAC addresses are not accurate, the IP-only mode should be used.

Configuration Steps

- (Optional) The default Webauth binding mode is IP+MAC.
- Determine a binding mode based on the accuracy of user information obtained by the NAS. When the IP and MAC addresses of STAs are accurate (in L2 authentication, for example), IP+MAC is recommended. When the IP and MAC addresses are not accurate, select IP-only.

Verification

- Change the binding mode to IP-only.
- Simulate the scenario where a user performs authentication to access the Internet.
- Modify the MAC address of the user, or use a client with the same IP address but a different MAC address to access the Internet.

- Check that the user accesses the Internet normally.

Related Commands

❖ **Specifying the Webauth Binding Mode**

Command	bindmode {ip-mac-mode | ip-only-mode}
Parameter Description	**ip-mac-mode**: Indicates IP-MAC binding mode. **ip-only-mode**: Indicates IP-only binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

❖ Specifying the Webauth Binding Mode

Configuration Steps	Set the binding mode to IP-only.
	QTECH(config.tmplt.eportalv2)#bindmode ip-only-mode
Verification	Check whether the configuration is successful.
	QTECH#show web-auth template Webauth Template Settings: Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip 17.17.1.21 BindMode: ip-only-mode Type: v2 Port: 10000 Acctmlist: Authmlist:

5.4.7. Configuring the Redirection HTTP Port

Configuration Effect

- When an STA accesses network resources (for example, the user accesses

the Internet using a browser), the STA sends HTTP packets. The NAS or convergence device intercepts these HTTP packets to determine whether the STA is accessing network resources. If the NAS or convergence device detects that the STA is not authenticated, it prevents the STA from accessing network resources and displays an authentication page to the STA. By default, the NAS
intercepts the HTTP packets that STAs send to port 80 to determine whether STAs are accessing network resources.

- After a redirection HTTP port is configured, the HTTP requests that STAs send to the specified destination port can be redirected.

Notes

- The commonly used management ports on the NAS or convergence device, such as ports 22, 23 and 53, and ports reserved by the system are not allowed to be configured as the redirection port. All ports except port 80 with numbers smaller than 1000 are seldom used by the HTTP protocol. To avoid a conflict with the well-known TCP port, do not configure a port with a small number as the redirection port unless necessary.

Configuration Steps

- Optional.
- When you configure automatic client acquisition, if you need to enable the NAS to intercept the HTTP packets that STAs send to the specified destination port, configure a redirection HTTP port.

Verification

- Configure an interception port.
- Open the browser of a PC and access the Internet through the port without performing authentication.
- Check whether the access requests are redirected to an authentication page.

Related Commands

❖ **Configuring the Redirection HTTP Port**

Command	**http redirect port *port-num***
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Global configuration mode
Usage Guide	A maximum of 10 different destination port numbers can be configured, not including default ports 80 and

	443.

Configuration Example

❖ Configuring the Redirection HTTP Port

Configuration Steps	Configure port 8080 as the redirection HTTP port.
	QTECH(config)#http redirect port 8080
Verification	Check whether the configuration is successful.
	QTECH(config)#show web-auth rdport Rd-Port: 80 443 8080

5.4.8. Configuring Rate Limit Webauth Logging

Configuration Effect

- The Web authentication module sends syslog messages to the administrator to display the information and relevant events of users who perform login/logout. By default, syslog messages are shielded.
- After syslog output rate limiting is configured, syslog messages are sent at a certain rate.

Notes

- When the login/logout rate is high, syslog messages are output frequently, which affects device performance and results in spamming.

Configuration Steps

- Optional.
- Configure syslog output rate limiting when you need to view the syslog messages about user login/logout.

Verification

- Configure logging rate limiting.
- Check whether users log in and out at a certain rate.
- Check that syslog messages are printed out at the limit rate.

Related Commands

❖ **Configuring Rate Limit Webauth Logging**

Command	web-auth logging enable *num*
Parameter Description	*num*: Indicates the syslog output rate (entry/second).
Command Mode	Global configuration mode
Usage Guide	When the syslog output rate is set to **0**, syslog messages are output without limit. The output of syslog messages of the critical level and syslog messages indicating errors is not limited.

Configuration Example

❖ Configuring Rate Limit Webauth Logging

Configuration Steps	▪ **Disable rate limit Webauth Logging.**
	`QTECH(config)#web-auth logging enable 0`
Verification	Check whether the configuration is successful.
Configuration Steps	Disable rate limit Webauth Logging.
	`QTECH(config)#web-auth logging enable 0`
Verification	Check whether the configuration is successful.

	`QTECH(config)#show running-config`
	`...`
	`web-auth logging enable 0`
	`...`

5.4.9. Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Effect

- When an unauthenticated user accesses network resources, the user's PC sends requests for HTTP session connection. The NAS or convergence device intercepts the HTTP packets and redirects the user to a Web authentication page. To prevent an unauthenticated user from initiating too

many HTTP connection requests and save resources on the NAS, it is necessary to limit the maximum number of HTTP sessions that the unauthenticated user
can initiate on the NAS.

- A user occupies an HTTP session when performing authentication, and the other application programs of the user may also occupy HTTP sessions. For this reason, it is recommended that the maximum number of HTTP sessions for an unauthenticated user be not set to 1. By default, each unauthenticated user can initiate 255 HTTP sessions globally, and each port supports up to 300 HTTP sessions initiated by unauthenticated clients.

Notes

- If the authentication page fails to be displayed during Web authentication, the maximum number of HTTP sessions may be reached. When this happens, the user can close the application programs that may occupy HTTP sessions and then perform Web authentication again.

Configuration Steps

- Optional.
- Perform this configuration when you need to change the maximum number of HTTP sessions that each unauthenticated user can initiate and the maximum number of HTTP sessions that unauthenticated clients can initiate on each port.
- Perform this configuration when you configure automatic SU client acquisition.

Verification

- Modify the maximum number of HTTP sessions that an unauthenticated user can initiate.
- Simulate the scenario where an unauthenticated user constructs identical sessions to connect to the NAS continuously.
- Simulate the scenario where the unauthenticated user accesses the Internet using a browser. Check whether the access requests are redirected and the NAS notifies the user that the maximum number of sessions is reached.

Related Commands

❖ **Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients**

Command	**http redirect session-limit { *session-num* }[port { *port-session-num* }]**
Parameter Description	*session-num*: Indicates the maximum number of HTTP sessions for unauthenticated clients. The value range is 1 to 255. The default value is 255. *port-session-num*: Indicates the maximum number of HTTP sessions on

	each port for authenticated clients. The value range is 1 to 65,535. The default value is 300.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Steps	▪ **Set the maximum number of HTTP sessions for unauthenticated clients to 3.**
	`QTECH(config)#http redirect session-limit 3`
Verification	Check whether the configuration is successful.

	`QTECH(config)#show web-auth parameter HTTP redirection setting:`
	`session-limit: 3`
	`timeout: 3 QTECH(config)#`

5.4.10. Configuring the HTTP Redirection Timeout

Configuration Effect

- Configure the HTTP redirection timeout to maintain redirection connections. When an unauthenticated user tries to access network resources through HTTP, the TCP connection requests sent by the user will be intercepted and re-established with the NAS or convergence device. Then, the NAS or convergence device waits for the HTTP GET/HEAD packets from the user and responds with HTTP redirection packets to close the connection. The redirection
  timeout is intended to prevent the user from occupying the TCP connection for a long time without sending GET/HEAD packets. By default, the timeout for maintaining a redirection connection is 3s.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to change the timeout for maintaining redirection

connections.

Verification

- Change the timeout period.
- Use a network packet delivery tool to set up a TCP connection.
- View the status of the TCP connection on the NAS. Check whether the TCP connection is closed when the timeout is reached.

Related Commands

❖ **Configuring the HTTP Redirection Timeout**

Command	**http redirect timeout { *seconds* }**
Parameter Description	*Seconds*: Indicates the timeout for maintaining redirection connections, in the unit of seconds. The value ranges from 1 to 10. The default value is 3s.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring the HTTP Redirection Timeout

Configuration Steps	**Set the HTTP redirection timeout to 5s.**
	`QTECH(config)#http redirect timeout 5`
Verification	Check whether the configuration is successful.

	`QTECH(config)#show web-auth parameter HTTP redirection setting:`
	`session-limit: 255`
	`timeout: 5`

5.4.11. Configuring the Straight-Through Network Resources

Configuration Effect

- After Web authentication or 802.1Xauthentication is enabled on a port, the users connecting to the port need to pass Web authentication or 802.1Xauthentication before accessing network resources.
- Perform this configuration to exempt users from authentication when accessing

some network resources.

- If a website is configured as a network resource of authentication exemption, all users, including unauthenticated clients, can access the website. By default, authentication exemption is not configured, and unauthenticated clients are not allowed to access network resources.
- IPv6 is supported.

Notes

- The maximum number of free resources and the maximum number of unauthenticated clients cannot exceed 1000 respectively. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be set.
- **http redirect direct-site** is used to configure the straight-through URL address for users, and **http redirect** is used to configure the straight-through IP address of the Web authentication server. The addresses configured using the two commands can be accessed without authentication, but they have different usages. It is recommended not to configure the IP address of the Web authentication server by using **http redirect direct-site**.
- When IPv6 addresses are used, you need to allow local link address learning. If this function is not configured, the NAS cannot learn the MAC addresses of clients.

Configuration Steps

- Optional.
- Run the **http redirect direct-site** command to enable unauthenticated clients to access network resources.

Verification

- Configure the straight-through network resources.
- Check whether unauthenticated clients can access the configured network resources using PCs.

Related Commands

❖ **Configuring the Straight-Through Network Resources**

Command	http redirect direct-site { *ipv6-address* | *ipv4-address* [*ip-mask*] [arp] }
Parameter Description	*Ipv6-address*: Indicates the IPv6 address of the network exempt from authenticati *ipv4-address*: Indicates the IPv4 address of the network exempt from authentication. *ip-mask*: Indicates the mask of the IPv4 address of the network exempt

	from authentication.
Command Mode	Global configuration mode
Usage Guide	To set authentication-exempted ARP resource, use the http redirect direct-arp command preferentially.

Configuration Example

❖ Configuring the Straight-Through Network Resources

Configuration Steps	▪ **Configure the straight-through network resources as 192.168.0.0/16.**
	QTECH(config)#http redirect direct-site 192.168.0.0 255.255.0.0
Verification	Check whether the configuration is successful.
	QTECH#show web-auth direct-site Direct sites: 0

5.4.12. Configuring the Straight-Through ARP Resource Range

Configuration Effect

- When ARP check or similar functions are enabled, the ARP learning performed by clients is controlled. As a result, clients cannot learn the ARPs of the gateway and other devices, which affects user experience. You can configure the straight-through ARP resource range to permit the ARP learning packets destined for the specified address to pass.

Notes

- When ARP check is enabled, you need to configure the gateway of the PCs connecting to the Layer-2 access device as a straight-through ARP resource. Note the following point when you perform the configuration:
- When ARP check is enabled, if the outbound addresses of the PCs connecting to the Layer-2 access device are not the gateway address, configure the outbound addresses as straight-through ARP resources. If multiple outbound addresses exist, configure these addresses as straight-through ARP resources.

Configuration Steps

- Optional.

- If ARP check is enabled on the NAS, you must configure the free resources and gateway address as straight-through ARP resources.

Verification

- Configure straight-through ARP resources.
- Clear the ARP cache of the PC of an unauthenticated user. (Run the **arp -d** command in the Windows operating system.)
- Run the **ping** command on the PC to access the straight-through ARP resources.
- View the ARP cache on the PC (run the **arp -a** command in the Windows operating system) and check whether the PC learns the ARP address of the straight-through ARP resources.

Related Commands

❖ **Configuring the Straight-Through ARP Resource Range**

Command	**http redirect direct-arp {*ip-address* [*ip-mask*] }**
Parameter Description	*ip-address*: Indicates the IP address of free resources. *ip-mask*: Indicates the mask of free resources.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring the Straight-Through ARP Resource

Configuration Steps	**Configure the straight-through ARP resource as 192.168.0.0/16.**
	`QTECH(config)#http redirect direct-arp 192.168.0.0 255.255.0.0`
Verification	Check whether the configuration is successful.

	`QTECH(config)#show web-auth direct-arp Direct arps:`
	`Address Mask`
	`192.168.0.0 255.255.0.0 QTECH(config)#`

5.4.13. Configuring an Authentication-Exempted Address Range

Configuration Effect

- Exempt users from Web authentication when accessing reachable network resources. By default, no authentication-exempted address range is configured. All users must pass Web authentication before accessing network resources.
- The authentication-exempted address range can be configured as an IP address range or MAC address range.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure an authentication-exempted user.
- Check whether the user can access the Internet without authentication.

Related Commands

❖ **Configuring an Authentication-Exempted Address Range**

Command	**web-auth direct-host { *ipv4-address* [*ipv4-mask*] [arp] [port *interface-name*] | *ipv6-address* }**
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the user exempt from authentication. *Ipv6-address*: Indicates the IPv6 address of the user exempt from authentication. *ip-mask*: Indicates the mask of the IPv4 address of the user exempt from authentication. *interface-name*: Indicates the name of the interface on which authentication exemption is enabled.
Command Mode	Global configuration mode
Usage Guide	The **arp** field is used to assign pass permissions to ARP packets. This field must be set when ARP check is enabled. After the **port** field is set, authentication exemption takes effect only on the configured interface.

Configuration Example

❖ Configuring an Authentication-Exempted Address Range

Configuration Steps	▪ **Configure an authentication-exempted address range.**
	QTECH (config)# web-auth direct-host 192.168.197.64
	Set the range of consecutive users exempt from authentication to 10.0.0.1-12.0.0.1. QTECH(config)# web-auth direct-host range 10.0.0.1 12.0.0.1
Verification	Check whether the configuration is successful.
	QTECH(config)#show web-auth direct-host Direct hosts: 0 Address Mask Port Binding ARP Binding Access Port List

5.4.14. Configuring the Interval for Updating Online User Information

Configuration Effect

- The NAS or convergence device maintains and periodically updates the information of online users, including users' online duration, to monitor the usage of network resources. When the online duration threshold is reached, users will be prevented from using network resources.

Notes

- The user information updating interval must be configured as 60 or multiple of 60; otherwise, the system will select the minimum multiple of 60 above and closest to the actual configuration as the interval.

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure the interval for updating online user information.
- View the information of online users after the update interval has elapsed.

Related Commands

❖ **Configuring the Interval for Updating Online User Information**

Command	**web-auth update-interval** ***{ seconds }***

Parameter Description	*seconds*: Indicates the interval for updating online user information, in the unit of seconds. The value ranges from 30 to 3,600. The default value is 180s.
Command Mode	Global configuration mode
Usage Guide	To restore the default updating interval, run the **no web-auth update-interval** command in global configuration mode.

Configuration Example

❖ Configuring the Interval for Updating Online User Information

Configuration Steps	▪ **Set the interval for updating online user information to 60s.**
	`QTECH (config)# web-auth update-interval 60`
Verification	Check whether the configuration is successful.
	`QTECH(config)#show run | include web-auth update-interval` `web-auth update-interval 60`

5.4.15. Configuring Portal Detection

Configuration Effect

- Detect the availability of the active portal server periodically. When the active portal server is unavailable, the standby portal server takes over the services.
- QTECH Second-Generation Web Authentication provides two detection methods. One is that the NAS constructs and sends portal packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available. Another is the NAS sends ping packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available. Because some servers or intermediate
  network segments filter ping packets, the first method is commonly used. The ping detection method is only used based on special requirements. In QTECH First-Generation Web Authentication, the NAS connects to a port of the portal server and checks whether the port is reachable. If the portal is reachable, the NAS determines that the portal server is available.
- For the first method in the second-generation authentication, the interval of

server availability detection is specified by the **interval** parameter, and the maximum number of packets that can be sent during each time of detection is specified by the **retransmit** parameter. If the portal server does not respond, the NAS determines that the portal server is unavailable. The timeout period for each packet is specified by the **timeout** parameter. The parameter settings are also supported by QTECH First-Generation Web Authentication.

- Portal server detection takes effect for QTECH First- and Second-Generation Web Authentication.
- If multiple portal servers are configured, these servers are working in active/standby mode.

Notes

- Multiple portal servers must be configured to realize failover when an error is detected on one server.
- Only one of the two detection methods can be used at a time in case of collision. If both detection methods are configured, a detection algorithm conflict will occur or the detection results will be inaccurate.
- The system will automatically select a detection method based on whether QTECH First- or Second-Generation Web Authentication is used.

Configuration Steps

- Optional.
- Configure multiple portal server templates applicable to QTECH First- or Second-Generation Web Authentication.

Verification

- Configure two portal server templates for QTECH First- or Second-Generation Web Authentication. Make the first template point to an unavailable server and the second template point to an available server.
- When the Console displays a log indicating that the portal server is not available, simulate the scenario where a user opens a browser to perform login authentication. Check whether the user is redirected to the second portal server.

Related Commands

❖ **Configuring Portal Detection**

Command	**web-auth portal-check [interval *intsec* [timeout *tosec]* [retransmit retries]**
Parameter Description	*intsec*: Indicates the detection interval. The default value is 10s. *tosec:* Indicates the packet timeout period. The default value is 5s.

	intsec: Indicates the timeout retransmission times. The default value is 3 (times).
Command Mode	Global configuration mode
Usage Guide	In many network environments, only one portal server is deployed, and portal server detection does not need to be configured. If multiple portal servers exist, it is recommended that the parameters of portal server detection be not set to small values; otherwise, the NAS will send many packets within a short time, affecting performance.

Configuration Example

❖ Configuring Portal Detection

Configuration Steps	▪ **Configure portal detection.**
	`QTECH(config)#web-auth portal-check interval 20 timeout 2 retransmit 2`
Verification	Check whether the configuration is successful.

	`QTECH(config)#show running-config`
	…
	`web-auth portal-check interval 20 timeout 2 retransmit 2`
	…

5.4.16. Configuring Portal Escape

Configuration Effect

- Allow new users to access the Internet without authentication when the portal server is not available.

Notes

- To use the portal escape function, you must configure portal detection.
- If multiple portal servers are configured, the escape function takes effect only when all the portal servers are not available.

- The escape function is intended only for the portal server, instead of the RADIUS server.

Configuration Steps

- Optional.
- Configure portal detection.
- Configure portal escape.
- (Optional) Configure the nokick attribute.

Verification

- Configure a portal server and disable the server.
- Configure the portal detection and escape functions.
- When the NAS detects that the portal server is not available, check whether a client accesses the Internet without authentication.

Related Commands

❖ **Configuring Portal Escape**

Command	web-auth portal-escape [nokick]
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure portal escape if the continuity of some critical services on the network needs to be maintained when the portal server is faulty. You must configure portal detection when you use this function. If the nokick attribute is configured, the system does not force users offline when the escape function takes effect. If the nokick attribute is deleted, the system forces users offline.

Configuration Example

❖ Configuring Portal Escape

Configuration Steps	▪ **Configure portal escape.**
	QTECH(config)#web-auth portal-escape

Verification	Check whether the configuration is successful.
Configuration Steps	Configure portal escape.
	QTECH(config)#web-auth portal-escape
Verification	Check whether the configuration is successful.
	QTECH(config)#show running-config ... web-auth portal-escape ...

5.4.17. Enabling DHCP Address Check

Configuration Effect

- Allow only the clients that are allocated with IP addresses through DHCP to perform authentication.

Notes

- To use the DHCP address check function, you must configure DHCP snooping.
- DHCP address check is supported only for IPv4.
- DHCP address check is applicable only to QTECH Second-Generation Web Authentication and iPortal Web Authentication.
- The requirement that users obtain IP addresses through DHCP must be specified during network deployment. Those users cannot also use static IP addresses; otherwise, the existing users that use static IP addresses will be affected.
- If a few users need to use static IP addresses, configure these IP addresses as straight-through addresses, and these users are exempt from authentication.
- If DHCP address check needs to be enabled only on some interfaces or some VLANs of interfaces, disable the global DHCP address check and configure the VLAN range in which DHCP address check needs to be enabled in each interface.

Configuration Steps

- Optional.
- Enable DHCP snooping.

- Enable DHCP address check.

Verification

- Enable DHCP address check.
- Configure a static IP address that is not allocated by the DHCP server on a client.
- Connect the client to the Internet and check whether the STA cannot perform authentication.

Related Commands

❖ **Enabling Global DHCP Address Check**

Command	**web-auth dhcp-check**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure DHCP address check to allow only the users who obtain IP addresses through DHCP to access the Internet. This function helps prevent the users who configure IP addresses without authorization from performing authentication to access the Internet.

❖ Enabling Interface-based DHCP Address Check

Command	▪ **web-auth dhcp-check {vlan [vlan-list]}**
Parameter Description	vlan-list: Indicates the VLAN range in which DHCP address check needs to be enabled in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	If DHCP address check needs to be enabled only on some interfaces or some VLANs of interfaces, disable the global DHCP address check and configure the VLAN range in which DHCP address check needs to be enabled in each interface.

Configuration Example

❖ Enabling DHCP Address Check

Configuration Steps	▪ **Enable global DHCP address check.**
	QTECH(config)#web-auth dhcp-check
Configuration Steps	Enable interface-based DHCP address check.
	QTECH(config-if-TenGigabitEthernet 3/1)# web-auth dhcp-check vlan 1,3-4
Verification	Check whether the configuration is successful. QTECH(config)#show running-config web-auth dhcp-check … interface TenGigabitEthernet 3/1 web-auth dhcp-check vlan 1,3-4

5.4.18. Disabling Portal Extension

Configuration Effect

- Enable portal extension to support QTECH portal server and portal servers that comply with the CMCC WLAN Service Portal Specification.
- You can select multiple redirection URL formats when interworking with the servers comply with the CMCC WLAN Service Portal Specification to achieve compatibility with different servers.

Notes

- Only QTECH Second-Generation Web Authentication supports portal extension.
- QTECH Second-Generation Web Authentication extends the CMCC WLAN Service Portal Specification. You need to determine whether to use the extension mode based on the server performance.
- If the portal server is a product of QTECH, use the default mode, that is, extension mode. If the portal server complies with the CMCC WLAN Service Portal Specification, disable portal extension.
- The CMCC WLAN Service Portal Specification supports multiple redirection

URL formats. If the portal server complies with the CMCC WLAN Service Portal Specification, select a redirection URL format supported by the server.

Configuration Steps

- Optional.
- Determine whether to disable portal extension based on the server type.
- Select a redirection URL format supported by the server if portal extension is disabled.

Verification

- Select QTECH portal server and a portal server compliant with the CMCC WLAN Service Portal Specification to be used in QTECH Second-Generation Web Authentication.
- Connect a client to the Internet. Check whether the client performs authentication normally on the two servers and can access the Internet.

Related Commands

❖ **Disabling Portal Extension**

Command	**no web-auth portal extension**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The portal servers that comply with the *CMCC WLAN Service Portal Specification* are deployed. If QTECH portal server is used, enable portal extension.

Configuration Example

❖ Disabling Portal Extension

Configuration Steps	▪ **Disable portal extension.**
	`QTECH(config)#no web-auth web-auth portal extension` `QTECH(config)# http redirect url-fmt ext1`
Verification	Check whether the configuration is successful.

	QTECH(config)#show running-config … no web-auth web-auth portal extension http redirect url- fmt ext1 …

5.4.19. Configuring the Whitelist

Configuration Effect

- The whitelist users can access some network resources before authentication.
- Support filtering by port, URL, IP, etc.

Notes

- At most 1000 whitelist items can be configured.
- When configure by domain, the DNS should be enabled on device to parse IP address.
- Multiple IP addresses may exist in some domain names. At most 8 IP addresses are supported.

Configuration Steps

- Optional.
- Configure DNS.
- Configure whitelist.

Verification

- Configure a whitelist item.
- The user can access the whitelist addresses before authentication.

Related Commands

❖ **Configure Whitelist**

Command	web-auth acl { white-url *name*}
Parameter Description	Name: whitelist URL

Command Mode	Global configuration mode
Usage Guide	The whitelist users can access some network resources before authentication.

Configuration Example

❖ Configure whitelist

Configuration Steps	▪ **Configure whitelist**
	QTECH(config)# web-auth acl white-url www.QTECH.com.cn
Verification	Check whether the configuration is successful.
	QTECH(config)#show running-config … web-auth acl white-url www.QTECH.com.cn

5.4.20. Configuring the Portal Communication Port

Configuration Effect

- Configure the port (source port) used for the communication between the NAS and portal server.

Notes

- Only one port can be configured for the communication between the NAS and portal server.

Configuration Steps

- Configure a port as the portal communication port.

Verification

- After Web authentication is enabled, capture a packet on the portal server during the authentication process and check whether the source IP address of the packet is the IP address of the specified port.

Related Commands

❖ **Configuring the Portal Communication Port**

Command	ip portal source-interface *interface-type interface-num*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring the Portal Communication Port

Configuration Steps	▪ **Configure an aggregate port as the portal communication port.**
	`QTECH(config)#ip portal source-interface Aggregateport 1`
Verification	Check whether the configuration is successful.

	`QTECH(config)#show running-config`
	
	`ip portal source-interface Aggregateport 1`

5.4.21. Configuring VLAN-Based Authentication on a Port

Configuration Effect

- With this function enabled, clients in a VLAN configured on a port of the NAS can initiate authentication. Otherwise, the authentication will not start.

Notes

- This function supports configuration of multiple VLANs. If no VLAN is specified, Web authentication is implemented based on ports.

Configuration Steps

- Configure port-based Web authentication.
- Configure the VLAN for Web authentication.

Verification

- After Web authentication is enabled, specify the VLAN in which clients can

initiate authentication. The HTTP packets sent outside the specified VLAN cannot be redirected.

Related Commands

❖ **Configuring VLAN-Based Authentication on a Port**

Command	web-auth vlan-control *vlan-list*
Parameter Description	*vlan-list* : Indicats the VLAN list to be authenticated.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring VLAN-Based Authentication on a Port

Configuration Steps	▪ **Specify VLAN1 as the VLAN in which users can initiate authentication.**
	`QTECH(config-if-GigabitEthernet 0/14)#web-auth vlan-control 1`
Verification	Check whether the configuration is successful.

	`QTECH(config)#show running-config`
	`...`
	`web-auth vlan-control 1`

5.4.22. Configuring the Authenticated User Logout Delay on a Port

Configuration Effect

▪ Configure the delay after which the authenticated clients connected to a port go offline when the port fails.

Configuration Steps

❖ **Configuring the Authenticated User Logout Delay on a Port**

▪ Configure the authenticated user logout delay on a port in global configuration mode.

Command	web-auth linkdown-timeout
Parameter Description	**timeout**: Indicates the logout delay. The default value is 60s.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check that the authenticated clients connected to the faulty port go offline after the configured time has elapsed.

Configuration Example

❖ **Configuring the Authenticated User Logout Delay on a Port**

Configuration Steps	▪ **Configure the logout delay.** `QTECH(config)#web-auth linkdown-timeout {timeout}`
Verification	Check whether the configuration is successful. `QTECH(config)#show running-config`

5.4.23. Disabling DHCP Server Detection

Configuration Effect

- Disable DHCP server detection. If DHCP server detection is enabled, when an online client that passes Web authentication sends the DHCP release packet, it goes offline. If DHCP server detection is disabled, the client will not go offline.

Notes

- This function is disabled by default. The DHCP server and Web authentication need to be configured on the same device.

Configuration Steps

- Optional.
- Disable this function when DHCP server detection is not required.

Related Commands

❖ **Disabling DHCP Server Detection in Global Configuration Mode**

Command	no web-auth dhcp-server check
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- After DHCP server detection is disabled, when online clients that pass Web authentication send DHCP release packets, check that the clients do not go offline. If DHCP server detection is enabled, check that the clients go offline.

Configuration Example

❖ **Disabling DHCP Server Detection**

Configuration Steps	▪ **Disable DHCP server detection.** `QTECH(config)#no web-auth dhcp-server check`
Verification	Check whether the configuration is successful. `QTECH(config)#show running-config`

5.5. Monitoring

Clearing

Description	Command
Forces users offline.	**clear web-auth user** { **all | ip** *ip-address* | **mac** *mac-address* **| name** *name-string* }
Clears all the straight-through	**clear web-auth direct-site**

network resources.	
Clears all the authentication-exempted users.	**clear web-auth direct-host**
Deletes all ARP resources exempt from authentication.	**clear web-auth direct-arp**

Displaying

Description	Command
Displays the basic parameters of Web authentication.	**show web-auth parameter**
Displays the whitelist	**show web-auth acl**
Displays the Webauth template configuration.	**show web-auth template**
Displays the authentication-exempted host range.	**show web-auth direct-host**
Displays the straight-through address range.	**show web-auth direct-site**
Displays the straight-through ARP range.	**show web-auth direct-arp**
Displays the TCP interception port.	**show web-auth rdport**
Displays the Webauth configuration on a port.	**show web-auth control**
Displays the online information of all users or specified users.	**show web-auth user**{ **all | ip** *ip-address* | **mac** *mac-address* **| name** *name-string* }

Displays the Webauth portal check information.	**show web-auth portal-check**
Displays online and offline records about users.	**show web-auth syslog ip** *ip-address*
Displays authentication experience data.	Show web-auth authmng [statistic | abnormal]

Debugging

System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs Web authentication.	**debug web-auth all**

6.1. Overview

The Security Control Center (SCC) provides common configuration methods and policy integration for various access 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 Source 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

6.2. Application

Typical Application	Scenario
Access Control of Extended Layer 2 Campus Networks	Students on a campus network can access the Internet based on dot1x client authentication or Web authentication. ARP spoofing between the students should be prevented. In addition, terminal devices in some departments (such as the headmaster's office) can access the Internet without authentication.

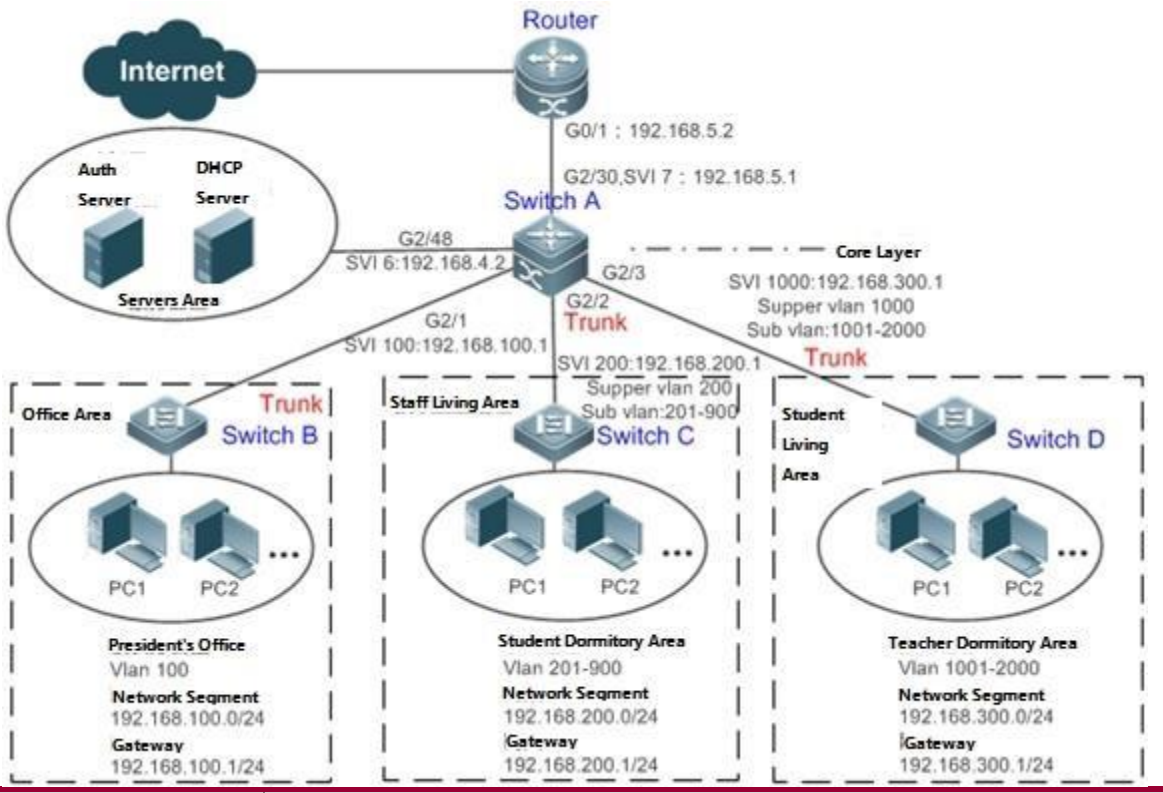
6.2.1. Access Control of Extended Layer 2 Campus Networks

Scenario

Students on a campus network of a university usually need to be authenticated through the dot1x client or Web before 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 office) can access the Internet without authentication.

Figure 6-1



Remarks	**A traditional campus network is hierarchically designed, which consists of an access layer, a convergence 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 switches exist without involving any convergence device in between. The ports between the core switch and the access switches (such as switches B, C, and D in Figure 6-1) 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 in different VLANs to prevent ARP spoofing.** **The core switch A connects to various servers, such as the**

	authentication server and the DHCP server. 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 configured as 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 ARP spoofing. On the core switch A, user VLANs are regarded as sub VLANs, super VLANs are configured, and SVIs 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 the students' living area, both dot1x authentication and Web authentication are enabled, so that users can freely select 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 the Internet without authentication.

6.3. Basic Concepts

Authentication-Exemptio n VLAN

Some special departments may be allocated to authentication-exemption VLANs to simplify network management, so that 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 can 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.

IPv4 access users include IP users (such as IP authenticated users) based on dot1x authentication, users based on 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 authentication and gets online. The 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 economical losses as the 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-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.

6.3.1. 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.

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

The authentication-exemption VLANs occupy hardware entries. When access control such as authentication is disabled, configuring authentication-exemption VLANs has the same effect as the case where no authentication-exemption

VLANs are configured. Therefore, it is recommended that authentication-exemption VLANs be configured for users who need to access the Internet without authentication, only when the access control function has been 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.

6.3.2. 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.

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

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, IPv4 users 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.

6.3.3. 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 network cables and carry their mobile terminals to the new office to access the network. Then this brings about an issue about 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 needs to be authenticated again before getting online.

Only the switches and wireless devices support authenticated-user migration. In addition, cross-switch migration is not 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 authentication with IP 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 specified 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 on the 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.

6.3.4. 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.

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] minutes later.

6.3.5. User Escape

After this function is enabled, if the system cannot finish user authentication timely, part or all users will be allowed to escape for a certain period of time, and the authentication will be resumed after the escape duration ends.

Working Principle

If authentication timeout users take a large proportion or the authentication duration deviates too much from the historical average, it is considered that the authentication system cannot finish the authentication timely, and part or all users will be allowed to escape for a certain period of time. The authentication will be resumed after the escape duration ends.

Enabling of this function has no impact on authenticated users.

You can configure to allow part or all users to escape upon failure of user authentication, but only for a certain period of time. The escape duration can be specified.

After the escape duration ends, the authentication needs to be resumed for the user.

Currently, this function is effective only to Web authentication.

6.4. Configuration

Configuration Item	Suggestions and Related Commands	
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	Configures authentication-exemption 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 authenticated users can migrate.

Configuring User Online-Status Detection	Optional configuration, which is used to specify whether to enable the user online-status detection function.	
	offline-detect interval threshold	Configures the parameters of the user online-status detection function.
	no offline-detect	Disables the user online-status detection function.
	default offline-detect	Restores the default user online-status detection mode.
Enabling User Escape	(Optional) It is used to specify user escape.	
	authmanage user-escape enable	Enables user escape.
	authmanage user-escape time *time-value authmanage user-escape life life-value*	Indicates the allowed escape duration. When the escape duration ends, user authentication needs to be resumed. Indicates the lifetime ofescape. After the lifetime ends, escape will not be allowed.
	authmanage user-escape when timeout-ratio *ratio-number* **authmanage user-escape when authentication-time** *time-value*	Indicates the conditions for user escape (namely under what conditions is the user allowed to escape).

6.4.1. Configuring Authentication-Exemption VLANs

Configuration Effect

Configure authentication-exemption VLANs, so that users in these VLANs can access the Internet without experiencing dot1x or Web authentication.

Configure authentication-exemption VLANs on a port, so that only users in specified VLANs on the port can access the Internet without experiencing authentication.

Precautions

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 VLANs are denied 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 Method

❖ **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.
- Authentication-exemption VLANs can be configured in interface configuration mode.

Command	[no] direct-vlan *vlanlist*
Parameter Description	**no**: If the command carries this parameter, it indicates that the authentication-exemption VLAN 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/interface 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. Then open the Internet Explorer, and enter a valid extranet address (such as www.google.com). If the users can open the corresponding webpage on the Internet, it indicates that the authentication-exemption VLAN is valid; otherwise, the authentication-exemption VLAN does not take effect.
- Use the **show direct-vlan** command to check the authentication-exemption VLAN configuration on the device.

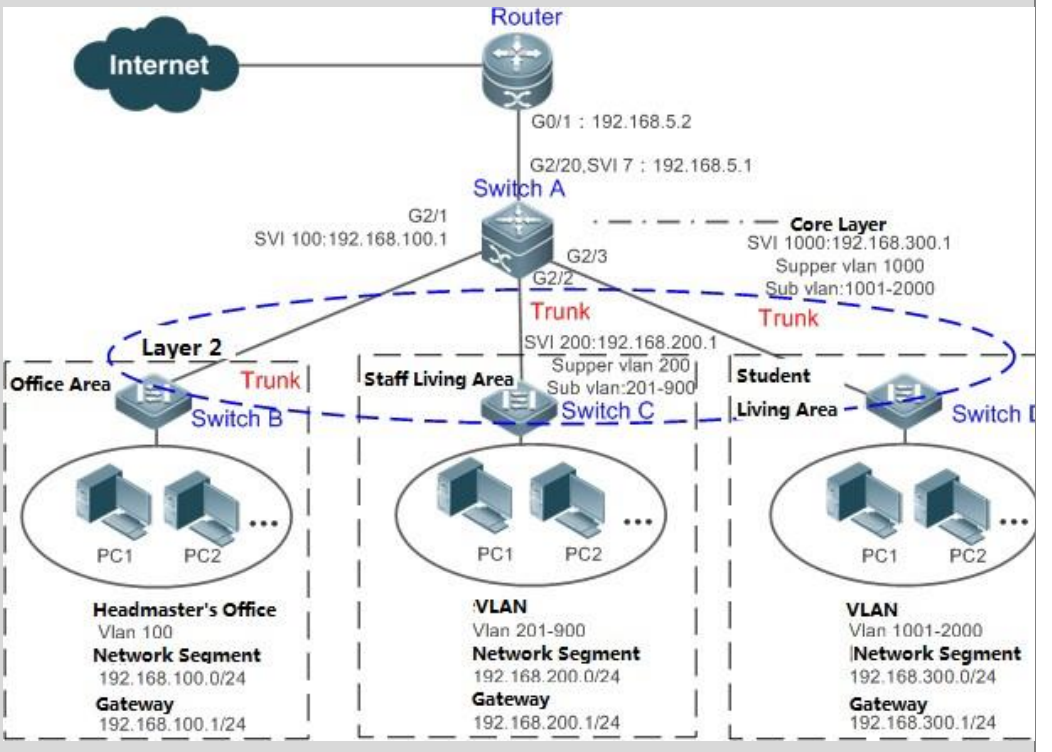
Command	show direct-vlan
Parameter Description	-
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Global configuration mode

Usage Example	`QTECH#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

Scenario Figure 6-2	

Configuration Steps	▪ 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.

Switch A	`SwitchA(config)#vlan 100 SwitchA(config-vlan)#exit`
	`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 to receive EAPOL packet and DOT1X 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`

6.4.2. 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 IPv4 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.

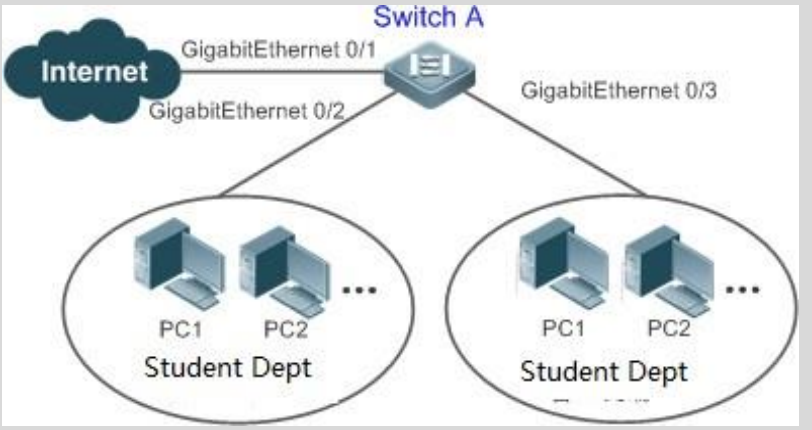
Command	**show nac-author-user [interface** ***interface-name*** **]**
Parameter Description	***interface-name***: This parameter indicates the interface name.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Global configuration mode

Usage Example	`QTECH#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 6-3**	
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`

6.4.3. 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, unless the authenticated-user 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 without getting offline first. However,

  if the user gets offline before changing the physical location or gets offline during the location change (for example, the user online-status detection function disconnects the user), the user can still normally get online after 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 authenticated-user migration is not 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 one physical location on the network moves to another physical location and attempts to get online from the new 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

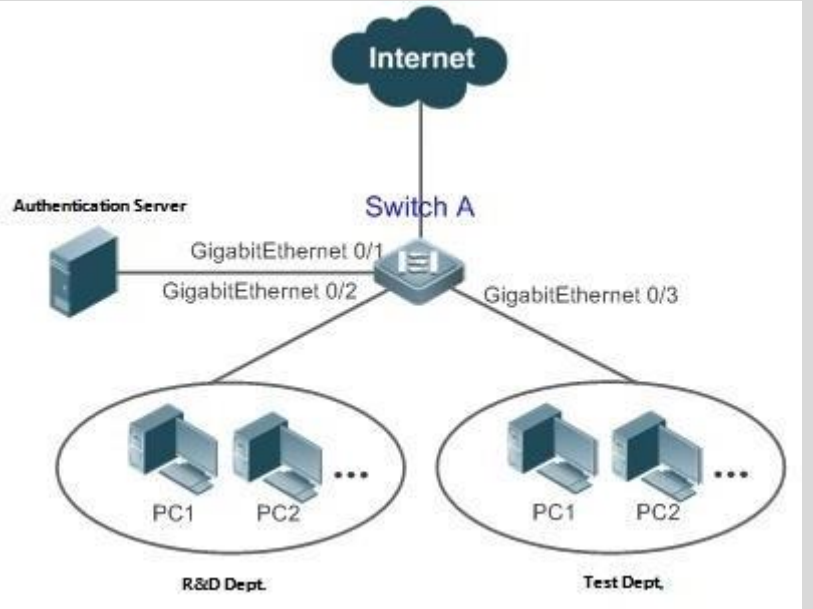
Check the authenticated-user migration configuration using the following method:

- A PC is authenticated and gets online from a dot1x-based port of the device using dot1x SU client, and does not 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 6-4	
Configuration Steps	▪ Enable dot1x authentication on access ports Gi 0/2 and Gi 0/3, and configure authentication 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, and gets online. Remove the network cable from the PC, connect the PC to the LAN where the test department resides, and perform dot1x authentication for the PC again using dot1x SU client. Confirm that the PC can successfully get online.

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

6.4.4. 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 threshold within the specified period of time, the device automatically disconnects the user, so as to avoid the economical loss incurred by 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 bydefault.
- 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 in 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 range is 0-4294967294 Bytes.The default value is 0, indicating that the user is disconnected when no traffic of the user is 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 when its traffic is lower than a specific threshold within a specific period of time. Use the **no offline-detect** command to disable the user online-status detection function, or use the **default offline-detect** command to restore the default detection mode.

Verification

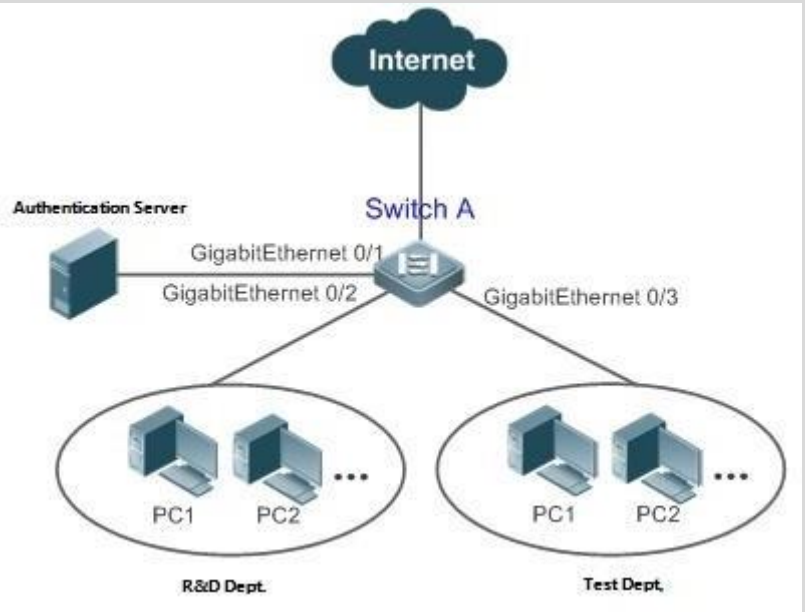
Check the user online-status detection configuration using the following method:

- After the user online-status detection function is enabled, power off the specified authenticated terminal after the corresponding user gets online. Then wait for the specified period of time, and run the online user query command 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 6-5	

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 have 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`

6.4.5. Enabling User Escape

Configuration Effect

After this function is enabled, if the system cannot finish user authentication timely, users will be allowed to escape for a certain period of time, and the authentication will be resumed after the escape duration ends.

Notes

- Enabling of this function will affect only new online users but not authenticated users.
- User escape needs to be enabled only when the system is detected to fail timely authentication.
- The escape duration can be configured. When the escape duration ends, user authentication needs to be resumed.
- Currently, this function is effective only to Web authentication.

Configuration Steps

❖ **Enabling User Escape**

- Optional.
- User escape needs to be enabled only when the system is detected to fail timely authentication.

Command	**authmanage user-escape { enable | time *time-value1* | when authentication-time *time-value2* | when timeout-ratio *ratio-number* | life *life-value* }**
Parameter Description	*time-value1*: Indicates the escape duration, in the unit of minutes. *time-value2*: Indicates the authentication duration, in the unit of ms. When the value exceeds that of *time-value2*, part of users is allowed to escape for *time-value1* minutes. *ratio-number*: When the ratio of authenticated users exceeds the value of *ratio-number*, part of users is allowed to escape for *time-value1* minutes. *life-value*: Indicates the escape lifetime, in the unit of minute.
Defaults	*time-value1*: The value is 30 minutes by default and can be set to 10 minutes to 240 minutes. *time-value2*: The default value is 5,000, which indicates that part of users are allowed to escape when the average handling duration exceeds 5s. The value ranges from 1,000 to 10,000. *ratio-number:* The default value is 10, which indicates that the part of users are allowed to escape when the ratio of timeout authentication users exceed 10%. The value ranges from 1 to 100. *life-value*: The value is 30 minutes by default and can be set to 10 minutes to 240 minutes.
Command Mode	Global configuration mode
Usage Guide	User escape needs to be enabled only when the system is detected to fail timely authentication.

Verification

- Run **show authmanage user-escape** to display user escape configuration.

Configuration Example

❖ **Enabling User Escape**

Configuration	▪ **Enable user escape in global configuration mode.**
Steps	
	`QTECH(config)# authmanage user-escape enable`

Verification	Run **show authmanage user-escape** to display user escape configuration.

6.5. 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.
show authmanage user-escape	Displays the configuration of user escape.

Debugging

System resources are occupied when debugging information is output. Therefore, close the debugging switch immediately after use.

Command	Function
debug scc event	Debugs the SCC running process.
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.
debug authmanage {event | error}	Displays the running process of user escape.

7.1. 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).

7.2. Applications

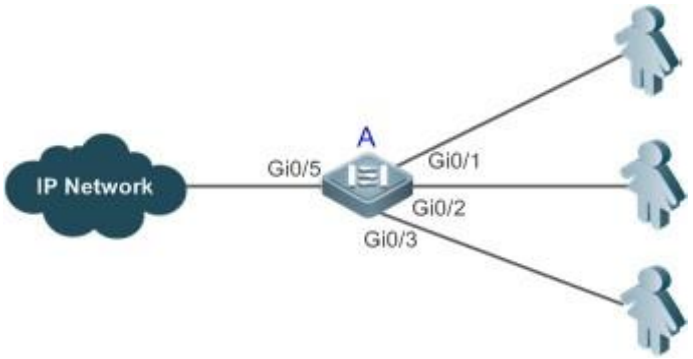
Application	Description
Global IP-MAC Binding	Only hosts with the specified IP addresses can access the network, and the hosts connected to a device can move freely.

7.2.1. Global IP-MAC Binding

Scenario

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

- Only hosts with the specified IP addresses can access the external network, which prevents IP address embezzlement by unauthorized hosts.



- Hosts can move freely under the same device.

Figure 7-1

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.

7.3. Features

Basic Concepts

❖ **IPv6 Address Binding Mode**

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

Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Strict	Packets matching the global IPv4-MAC binding are forwarded.	Packets matching the global IPv6-MAC binding are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.)

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

7.3.1. 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.

7.3.2. 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.

7.3.3. Configuring the Exclude Port

Working Principle

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

Related Configuration

- **Configuring the Exclude Port**

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

7.4. 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 the 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.

7.4.1. 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 and a MAC address. Not supported on AC.

❖ 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 used to control forwarding of IPv4 or IPv6 packets. Not supported on AC.

Configuration Example

❖ Configuring Global IP-MAC Binding and Enabling Address Binding

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

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

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

	QTECH#show address-bind Total Bind Addresses in System : 1 IP Address Binding MAC Addr 192.168.5.1 00d0.f800.0001

7.4.2 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.**
	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# address-bind 192.168.5.1 00d0.f800.0001 QTECH(config)# address-bind install
	QTECH(config)# address-bind ipv6-mode compatible
Verification	Run the **show run** command to display the configuration on the device.

7.4.3 Configuring the Exclude Port

Configuration Effect

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

Notes

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

Configuration Steps

❖ **Configuring the Exclude Port**

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

Verification

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

Related Commands

❖ **Configuring the Exclude Port**

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

Usage Guide	Not supported on AC.

Configuration Example

❖ Configuring the Exclude Port

Configuration Steps	▪ **Create a global IPv4-MAC binding.** ▪ **Enable the address binding function.** ▪ **Configure an exclude port.**
	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z.
	QTECH(config)# address-bind 192.168.5.1 00d0.f800.0001 QTECH(config)# address-bind install QTECH(config)# address-bind uplink GigabitEthernet 0/1
Verification	Display the global IP-MAC binding on the device. QTECH#show address-bind Total Bind Addresses in System : 1 IP Address Binding MAC Addr 192.168.5.1 00d0.f800.0001 QTECH#show address-bind uplink Port State Gi0/1 Enabled Default Disabled

7.5 Monitoring

Displaying

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

8.1. Overview

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

The following sections introduce password policy only.

Protocols and Standards

N/A

8.2 Features

Basic Concepts

- **Minimum Password Length**

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

- **Strong Password Detection**

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

1. Passwords that are the same as corresponding accounts;
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, indicating that the password has expired and the user needs to reset the password. If the new password input during password resetting does not meet system requirements or the new passwords consecutively input twice are not the same, the system will ask the user to input the new password once again.

- **Guard Against Repeated Use of Passwords**

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

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

- **Storage of Encrypted Passwords**

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

8.3 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 user passwords.
	password policy no-repeat-times	Sets the no-repeat times of latest password configuration, so that the passwords specified in these times of latest password configuration can no longer be used in future password configuration.

	password policy strong	Enables the strong password detection function.
	service password-encryption	Sets the storage of encrypted passwords.

8.3.1 Configuring Basic Function of Password Security Policy

Configuration Effect

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

Notes

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

Configuration Steps

❖ **Configuring the Password Life Cycle**

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

❖ **Configuring the Minimum Length of User Passwords**

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

❖ **Setting the No-Repeat Times of Latest Password Configuration**

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

❖ **Enabling the Strong Password Detection Function**

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

❖ **Setting the Storage of Encrypted Passwords**

- Optional

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

Verification

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

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

Related Commands

❖ **Configuring the Password Life Cycle**

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 the user to 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 minimum length of 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 number of password history records of a user is greater than the maximum number configured for the user, the new password history record will overwrite the user's oldest password history record.

❖ Enabling the Strong Password Detection Function

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

❖ Setting the Storage of Encrypted Passwords

Command	**service password-encryption**

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

❖ Checking User-Configured Password Security Policy Information

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.

❖ Checking Information Such as Weak Passwords Manually Set

Command Syntax	show password policy
Parameter Description	-
Command Mode	Privileged EXEC mode

Usage Guide	Use this command to display information such as the weak passwords manually set on the device.

Configuration Examples

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

❖ Configuring Password Security Check on the Device

Typical Application	**Assume that the following password security requirements arise in a network environment:** ▪ **The minimum length of passwords is 8 characters;** ▪ **The password life cycle is 90 days;** ▪ **Passwords are stored and transmitted in cipher text format;** ▪ **The number of no-repeat times of password history records is 3;** ▪ **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.
	`QTECH# configure terminal` `QTECH(config)# password policy min-size 8 QTECH(config)# password policy life-cycle 90 QTECH(config)# service password-encryption QTECH(config)# password policy no-repeat-times 3 QTECH(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.

```
QTECH# 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)
```

Common Errors

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

8.4 Monitoring

Displaying

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

9.1. Overview

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

9.2 Applications

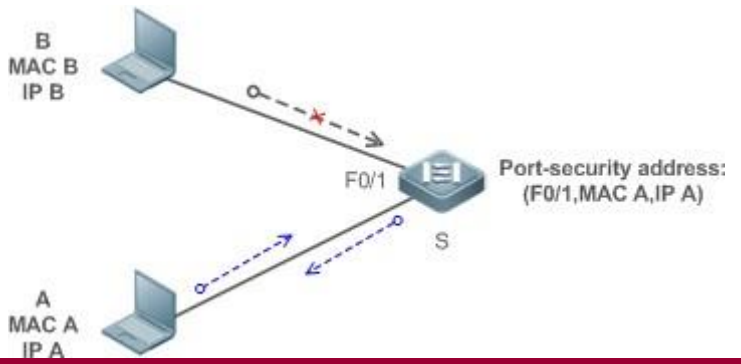
Application	Description
Allowing Only Specified Hosts to Use Ports	For network security, certain ports of a device can be used only by specified hosts.

9.2.1 Allowing Only Specified Hosts to Use Ports

Scenario

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

- Only specified PCs can connect to the ports and normally use the network.
- Other PCs cannot use the network even if connected to the ports.
- After the configuration is complete, the administrator does not need to perform regular maintenance. Figure 9-1



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.

9.3 Features

Basic Concepts

❖ **Secure Port**

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

❖ **Secure Addresses**

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

❖ **Dynamic Binding**

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

❖ **Static Binding**

A command for manually binding secure addresses.

❖ **Aging of Secure Addresses**

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

❖ **Sticky MAC Address**

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

❖ Security Violation Events

When the number of learned MAC addresses learned by a port exceeds the maximum number of secure addresses, security violation events will be triggered. You can configure the following modes for 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 protect mode.
- shutdown: When violation occurs, the port will be disabled in addition to the behaviors in the preceding two modes.

❖ Maximum Number of Secure Addresses

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

Overview

Feature	Description
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.

9.3.1 Enabling Port Security

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

Working Principle

When port security is enabled, the device security module will check the sources of received packets. Only packets from addresses in the secure address list can be normally forwarded; otherwise, the packets will be discarded or the port performs other violation handling behaviors.

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

Related Configuration

- **Enabling Port Security for a Port**

By default, port security is disabled.

You can run the **switchport port-security** command to enable or disable the port security function for a port. You cannot enable this function for a destination port of SPAN.

- **Setting the Maximum Number of Secure Addresses for a Port**

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

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

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

- **Setting the Mode for Handling Violation**

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

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

- **Setting Secure Addresses That Can Be Dynamically Saved**

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

You can run the **switchport port-security mac-address sticky** command to save dynamically learned addresses to the configuration file. As long as the

configuration file is saved, the device does not need to re-learn the secure addresses after the device is restarted.

9.3.2 Filtering Layer-2 Users

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

Working Principle

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

Related Configuration

- **Adding Secure Addresses for a Secure port**

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

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

9.3.3 Filtering Layer-3 Users

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

Working Principle

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

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

Related Configuration

- **Configuring Binding of Secure Addresses on Secure Ports**

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

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

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

9.3.4 Aging of Secure Addresses

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

Working Principle

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

Related Configuration

- **Configuring Aging Time of Secure Addresses**

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

You can run the **switchport port-security aging** command to enable aging time. The **static** parameter can be used to age static addresses.

9.4 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 secure 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.
	(Optional) It is used to configure security filtering items.	

Configuring Secure Addresses on Secure Ports	**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 all secure addresses on a port.
	switchport port-security binding-filter logging	Enables binding filter logging in the global configuration mode.

9.4.1 Configuring Secure ports and Violation Handling Modes

Configuration Effect

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

Notes

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

checks. If a security channel is configured for a port, packets in compliance with the security channel will avoid checking of the port security.

Configuration Steps

- **Enabling the Port Security Service**
  - Mandatory.
  - If there is no special requirement, enable the port security service for a port on the access device.
- **Configuring the Maximum Number of Secure Addresses for a Port**
  - Optional. To adjust the maximum number of secure addresses running on a secure port, you can configure this item.
  - Configure this item on a port enabled with port security.
- **Configuring Violation Handling Modes**
  - Optional. If you hope that other handling modes except discarding packets are implemented in case of violation, you can configure other handling modes.
  - Configure this item on a port enabled with port security.
- **Saving Dynamically Learned Addresses**
  - Optional. If you hope that secure addresses are not re-learned after the device is restarted, you can configure this item.
  - Configure this item on a port enabled with port security.

Verification

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

Related Commands

- **Setting Port Security**

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 Mode	Interface configuration 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.

❖ 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.**
	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# interface gigabitethernet 0/3 QTECH(config-if-GigabitEthernet 0/3)# switchport mode access QTECH(config-if-GigabitEthernet 0/3)# switchport port-security QTECH(config-if-GigabitEthernet 0/3)# switchport port-security maximum 8 QTECH(config-if-GigabitEthernet 0/3)# switchport port-security violation protect QTECH(config-if-GigabitEthernet 0/3)# switchport port-security mac-address sticky QTECH(config-if-GigabitEthernet 0/3)# end
Verification	Check the port security configuration on the device. QTECH# 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

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.

9.4.2 Configuring Secure Addresses on Secure Ports

Configuration Effect

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

Notes

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

Configuration Steps

❖ **Configuring Secure Addresses**

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

❖ **Configuring Binding of Secure Addresses**

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

❖ **Configuring Aging Time**

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

❖ **Enabling Binding Filter Logging**

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

Verification

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

Related Commands

❖ **Adding Secure Addresses for Secure Ports in the Global Configuration Mode**

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 addresses and 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	-

❖ Enabling Binding Filter Logging

Command	**switchport port-security binding-filter logging [rate-limit *rate*]**
Parameter Description	**rate-limit** *rate*: Indicates the printing rate of binding filter logging.
Command Mode	Global configuration mode
Usage Guide	1. If you run the **switchport port-security binding-filter logging** command without configuring the *rate* parameter, binding filter logging is enabled and the default printing rate, 10logs/minute, is adopted. 2. After binding filter logging is enabled, for packets that do not comply with IP/IP-MAC binding, warmings are printed. 3. After binding filter logging is enabled, if the printing rate exceeds the configured rate, the number of suppressed packets is displayed.

Configuration Example

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

Configuration	▪ **Enable port security.**
Steps	▪ Add a secure address.

	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# interface gigabitethernet 0/3 QTECH(config-if-GigabitEthernet 0/3)# switchport mode access QTECH(config-if-GigabitEthernet 0/3)# switchport port-security QTECH(config-if-GigabitEthernet 0/3)# switchport port-security mac-address 00d0.f800.073c vlan 1 QTECH(config-if-GigabitEthernet 0/3)# end
Verification	Check the port security configuration on the device.
	QTECH# show port-security address NO. VLAN MacAddress PORT TYPE RemainingAge(mins) STATUS 1 1 00d0.f800.073c GigabitEthernet 0/3 Configured -- active

❖ 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.**
	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# interface gigabitethernet 0/3 QTECH(config-if-GigabitEthernet 0/3)# switchport mode access QTECH(config-if-GigabitEthernet 0/3)# switchport port-security QTECH(config-if-GigabitEthernet 0/3)# switchport port-security binding 192.168.12.202 QTECH(config-if-GigabitEthernet 0/3)# end
Verification	Check the port security configuration on the device. NO. VLAN MacAddress PORT IpAddress FilterType FilterStatus 1 -- -- Gi0/3 192.168.12.202 ipv4-only active

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

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

	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# interface gigabitethernet 0/3 QTECH(config-if-GigabitEthernet 0/3)# switchport mode access QTECH(config-if-GigabitEthernet 0/3)# switchport port-security QTECH(config-if-GigabitEthernet 0/3)# switchport port-security binding 00d0.f800.073c vlan 1 0000::313b:2413:955a:38f4 QTECH(config-if)# end
Verification	Check the port security configuration on the device.
	QTECH#show port-security binding NO. VLAN MacAddress PORT IpAddress FilterType FilterStatus 1 -- -- Gi0/3 192.168.12.202 ipv4-only active 2 1 00d0.f800.073c Gi0/3 ::313b:2413:955a:38f4 ipv6-mac active

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

Configuration Steps	▪ **Enable port security.** ▪ **Configure aging time.**
	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# interface gigabitthernet 0/3
	QTECH(config-if-GigabitEthernet 0/3)# switchport port-security aging time 8 QTECH(config-if-GigabitEthernet 0/3)# switchport port-security aging static QTECH(config-if-GigabitEthernet 0/3)# end
Verification	Check the port security configuration on the device.

```
QTECH# show port-security gigabitethernet 0/3 Interface : Gi0/3
 Port
 Security:
 Enabled Port
 status :
 down
 Violation
 mode:Shutdow
 n Maximum
 MAC
 Addresses:8
 Total MAC
 Addresses:0
 Configured
 MAC
 Addresses:0
 Aging time :
 8 mins
SecureStatic address aging : Enabled
```

9.5 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 the port security configurations of an interface.	**show port-security interface** *interface-id*
Displays the statistics about port security.	**show port-security**

10.1. Overview

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

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

10.2. Applications

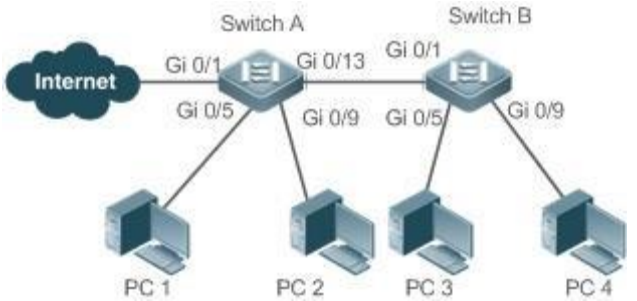
Application	Description
Network Attack Prevention	Enable storm control to prevent flooding.

10.2.1 Network Attack Prevention

Scenario

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

- Protect devices from flooding of broadcast packets, multicast packets, or unknown unicast packets. Figure 10-1



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).

10.3 Features

Basic Concepts

❖ **Storm Control**

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

❖ **Storm Control Based on the Bandwidth Threshold**

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

❖ **Storm Control Based on the Packets-per-Second Threshold**

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

❖ **Storm Control Based on the Kilobits-per-Second Threshold**

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

Overview

Feature	Description
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.

10.3.1 Unicast Packet Storm Control

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

Working Principle

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

Related Configuration

- **Enabling Unicast Packet Storm Control on Ports**

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

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

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

The default command parameters are determined by related products.

10.3.2 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.

10.3.3 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.

10.4 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.

10.4.1 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 unicas**t) to enable storm control, if you do not set the parameters, the default values are used.

Configuration Steps

❖ **Enabling Unicast Packet Storm Control**

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

❖ **Enabling Multicast Packet Storm Control**

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

❖ **Enabling Broadcast Packet Storm Control**

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

Verification

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

Related Commands

❖ **Enabling Unicast Packet Storm Control**

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.

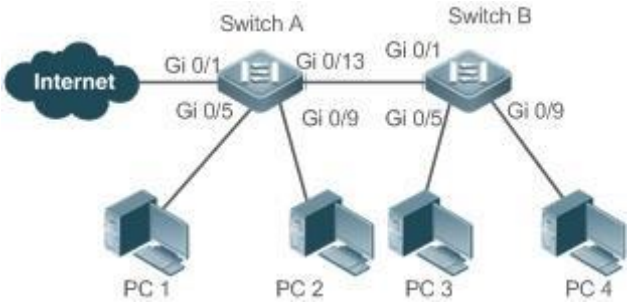
❖ Enabling Multicast Packet Storm Control

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.

Configuration Example

❖ Enabling Storm Control on Devices

Scenario	**GigabitEthernet 0/9 default default default none**
Figure 10-2	
Configuration Step	Enable storm control on Switch A and Switch B.
Switch A	QTECH(config)#interface range gigabitEthernet 0/5,0/9,0/13 QTECH(config-if-range)#storm-control broadcast QTECH(config-if-range)#storm-control multicast QTECH(config-if-range)#storm-control unicast
Switch B	QTECH(config)#interface range gigabitEthernet 0/1,0/5,0/9 QTECH(config-if-range)#storm-control broadcast QTECH(config-if-range)#storm-control multicast QTECH(config-if-range)#storm-control unicast
Verification	Check whether storm control is enabled on Switch A and Switch B.

Switch A	QTECH# 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	QTECH#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

10.5 Monitoring

Displaying

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

11.1. Overview

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

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

Currently, a device can work as either the SSH server or an SSH client, supporting SSHv1 and SSHv2 versions. QTECH SSH service supports both IPv4 and IPv6.

Unless otherwise specified, SSH in this document refers to SSHv2

Protocols and Standards

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

11.2 Applications

Application	Description
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 user 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.

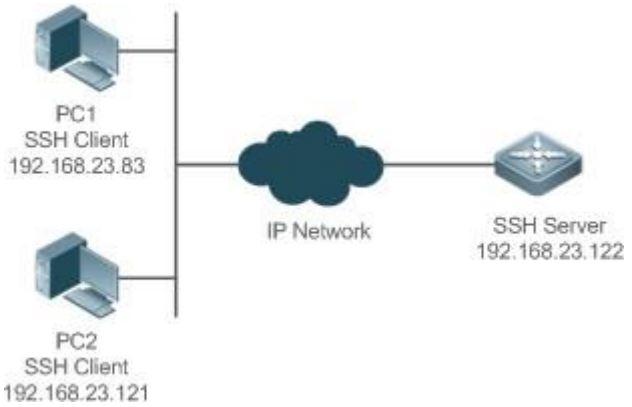
11.2.1 SSH Local Line Authentication

Scenario

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

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

Figure 11-1 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 SSH clients, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses an RSA key, whereas SSHv2 adopts an RSA or DSA key.
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:

1. Diversified SSH client software is available, including PuTTY,Linux, and OpenSSH. This document takes PuTTY as an example to explain the method for configuring the SSH clients.
2. Open the PuTTY connection tab, and select SSHv1 for authenticated login. (The method is similar if SSHv2 is selected.)
3. 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".)

11.2.2 SSH AAA Authentication

Scenario

SSH users can use the AAA authentication mode for user authentication, as shown in Figure 11-2.To ensure security of data exchange, the PCs function as the SSH clients, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used for user login on the SSH clients. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, it turns to the local authentication.

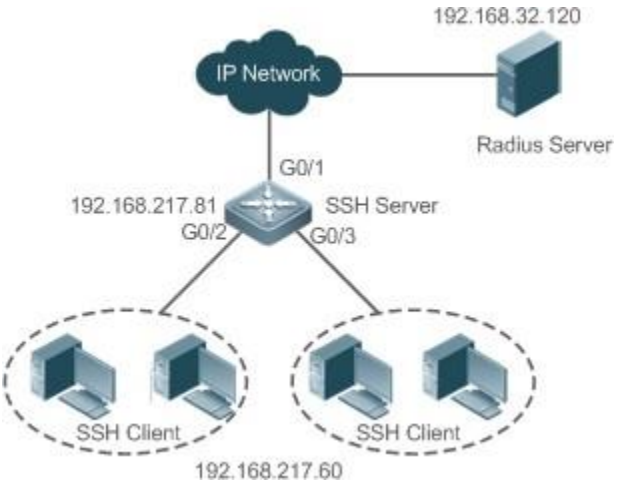


Figure 11-2 Networking Topology of SSH AAA Authentication

Deployment

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

11.2.3 SSH Public Key Authentication

Scenario

SSH clients can use the public keys for authentication, and the public key algorithm can be RSA or DSA, as shown in Figure 11-3.SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 11-3 Network Topology for Public Key Authentication of SSH Users

Deployment

- To implement public key authentication for the client, generate a key pair (RSA or DSA) on the client, configure the public key on the SSH server, and select the public key authentication mode.
- After the key is generated on the client, the SSH server will copy the file of the public key from the client to the flash and associates the file with the SSH user name. Each user can be associated with one RSA public key and one DSA

public key.

11.2.4 SSH File Transfer

Scenario

The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server, as shown in Figure 11-4.

Figure 11-4 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.

11.3 Features

Basic Concepts

❖ **User Authentication Mechanism**

- Password authentication

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

- Public key authentication

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

Public key authentication is applicable only to the SSHv2 clients.

❖ **SSH Communication**

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

- Connection setup

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

- Version negotiation

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

- Key exchange and algorithm negotiation

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

- User authentication

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

- Session request

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

- Session interaction

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

analyzes, and processes the received command, and then sends the encrypted execution result to the client. The client decrypts the execution result.

- Session ending

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

Overview

Feature	Description

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.

11.3.1 SSH Server

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

Working Principle

For details about the working principle of the SSH server, see the "SSH Communication" in "Basic Concepts." In practice, after enabling the SSH server function, you can configure the following parameters according to the application requirements:

- Version: Configure the SSH version as SSHv1 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 reached, a message is sent, indicating the authentication failure.
- Public key authentication: The public key algorithm can be RSA or DSA. It provides a secure connection between the client and the server. The public key file on the client is associated with the user name. In addition, the public key authentication mode is configured on the client, and the corresponding private key file is specified. In this way, when the client attempts to log in to the server, public key authentication can be implemented to set up a secure connection.

Related Configuration

❖ **Enabling the SSH Server**

By default, the SSH server is disabled.

In global configuration mode, run the [**no**] **enable service ssh-server** command to enable or disable the SSH server. To generate the SSH key, you also need to enable the SSH server.

❖ Specifying the SSH Version

By default, the SSH server supports both SSHv1 and SSHv2, connecting either SSHv1 clients or SSHv2 clients. Run the **ip ssh version** command to configure the SSH version supported by the SSH server.
If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

❖ Configuring the SSH Authentication Timeout

By default, the user authentication timeout is 120s.

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

❖ Configuring the Maximum Number of SSH Authentication Retries

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

Run the **ip ssh authentication-retries** command to configure the maximum number of user authentication retries on the SSH server. Use the **no** form of the command to restore the default number of user authentication retries. If authentication still does not succeed when the maximum number of user authentication retries is reached, user authentication fails.

❖ Specifying the SSH Encryption Mode

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

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

❖ Specifying the SSH Message Authentication Algorithm

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

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

❖ Setting A Monitoring Port ID for the SSH Server

The default port ID is 22.

Run the **ip ssh port** command to set a monitoring port ID for the SSH server. Use either the **no ip ssh port** command or the

ip ssh port 22 command to restore the default setting.

❖ **Enabling the Public Key Authentication on the SSH Server**

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

11.3.2 SCP Service

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

Working Principle

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

Related Configuration

❖ **Enabling the SCP Server**

By default, the SCP server function is disabled.

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

11.4 Configuration

Configuration	Description and Command	
	It is mandatory to enable the SSH server.	
	enable service ssh-server	Enables the SSH server.

Configuring 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 SSH authentication timeout.
	ip ssh authentication-retries *retry times*	Configures the maximum number of SSH authentication retries.
	Ip ssh cipher-mode{**cbc** | **ctr** | **others** }	Specifies the SSH encryption mode.
	Ip ssh hmac-algorithm{**md5** | **md5-96** | **sha1** | **sha1-96**}	Specifies the SSH message authentication algorithm.
	ip ssh key-exchange { dh_group_exchange_sha1 |dh_group14_sha1 | dh_group1_sha1 }	Configures support for Diffie-Hellman on the SSH server.
	ip ssh port *port*	Sets a monitoring port ID for the SSH server.
	{ip | ipv6} ssh access-class { *access-list-number* | *access-list-name* }	Enables ACL filtering of the SSH server.
	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	Mandatory.	
	ip scp server enable	Enables the SCP server.

Service	**ip scp server topdir {flash:**/*path*** | flash2:**/*path*** | usb0:**/*path*** | usb1:**/*path*** | sd0:**/*path*** | sata0:**/*path*** | tmp:**/*path*** }**	Configures the transmission path for files of the SCP server

11.4.1 Configuring the SSH Server

Configuration Effect

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

Notes

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

Configuration Steps

❖ **Enabling the SSH Server**

- Mandatory.
- By default, the SSH server is disabled. In global configuration mode, enable

the SSH server and generate an SSH key so that the SSH server state changes to ENABLE.

- **Specifying the SSH Version**
  - Optional.
  - By default, the SSH server supports SSHv1 and SSHv2, connecting either SSHv1 or SSHv2clients. If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.
- **Configuring the SSH Authentication Timeout**
  - Optional.
  - By default, the SSH authentication timeout is 120s. You can configure the user authentication timeout as required. The value ranges from 1 to 120. The unit is second.
- **Configuring the Maximum Number of SSH Authentication Retries**
  - Optional.
  - Configure the maximum number of SSH authentication retries to prevent illegal behaviors such as malicious guessing. By default, the maximum number of SSH authentication retries is 3, that is, a user is allowed to enter the user name and password three times for authentication. You can configure the maximum number of retries as required. The value ranges from 0 to 5.
- **Specifying the SSH Encryption Mode**
  - Optional.
  - Specify the encryption mode supported by the SSH server. By default, the encryption mode supported by the SSH server is Compatible, that is, supporting CBC, CTR and other encryption modes.
- **Specifying the SSH Message Authentication Algorithm**
  - Optional.
  - Specify the message authentication algorithm supported by the SSH server. By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5, SHA1, SHA1-96, and MD5-96, are supported.
- **Setting ACL Filtering of the SSH Server**
  - Optional.
  - Set ACL filtering of the SSH server. By default, ACL filtering is not performed for all connections to the SSH server. According to needs, set ACL filtering to perform for all connections to the SSH server.

❖ **Enabling the Public Key Authentication for SSH Users**

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

Verification

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

Related Commands

❖ **Enabling the SSH Server**

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, specify a VTY 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.

❖ Specifying the SSH Encryption Mode

Command	**ip ssh cipher-mode{cbc | ctr | others }**
Parameter Description	**cbc:** Sets the encryption mode supported by the SSH server to the CBC mode. Corresponding algorithms include DES-CBC,3DES-CBC,AES-128-CBC,AES-192-CBC,AES-256-CBC, and Blowfish-CBC. **ctr:** Sets the encryption mode supported by the SSH server to the CTR mode. Corresponding algorithms include AES128-CTR, AES192-CTR, and AES256-CTR. **others:** Sets the encryption mode supported by the SSH server to others. The corresponding algorithm is RC4.
Command Mode	Global configuration mode

Usage Guide	This command is used to configure the encryption mode supported by the SSH server. On QTECH devices, the SSHv1 server supports the DES-CBC, 3DES-CBC, and Blowfish-CBC encryption algorithms; the SSHv2 server supports the AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4 encryption algorithms. These algorithms can be grouped into three encryption modes: CBC, CTR, and others. As the cryptography continuously develops, it is approved that encryption algorithms in the CBC and others modes can be decrypted in a limited period of time. Therefore, organizations or companies that have high security requirements can set the encryption mode supported by the SSH server to CTR to increase the security level of the SSH server.

❖ Specifying the SSH Message Authentication Algorithm

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

❖ Configuring Support for DH Key Exchange Algorithm on the SSH Server

Command	**ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }**

Parameter Description	**dh_group_exchange_sha1**: Indicates configuration of diffie-hellman-group-exchange-sha1 for key exchange. **dh_group14_sha1**: Indicates configuration of diffie-hellman-group14-sha1 for key exchange. **dh_group1_sha1**: Indicates configuration of diffie-hellman-group1-sha1 for key exchange.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a DH key exchange method on the SSH. QTECH's SSHv1 server does not support DH key exchange method, while the SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 for key exchange.

❖ Setting A Monitoring Port ID for the SSH Server

Command	**ip ssh port *port***
Parameter Description	*port*: Indicates the monitoring port ID of the SSH server. The value ranges from 1025 to 65535.
Command Mode	Global configuration mode
Usage Guide	Use either the **no ip ssh port** or the **ip ssh port 22** to restore the monitoring port ID of the SSH server to the default value.

❖ Configuring ACL Filtering of the SSH Server

Command	**{ip | ipv6} ssh access-class { *access-list-number* | *access-list-name* }**
Parameter Description	*access-list-number*: Indicates the ACL number and the number range is configurable. The standard ACL number ranges are 1 to 99 and 1300 to 1999. The extended ACL number ranges are 100 to 199 and 2000 to 2699. Only IPv4 addresses are supported. *access-list-name*: Indicates an ACL name. Both IPv4 and IPv6 addresses are supported.
Command Mode	Global configuration mode

Usage Guide	Run this command to perform ACL filtering for all connections to the SSH server. In line mode, ACL filtering is performed only for specific lines. However, ACL filtering rules of the SSH are effective to all SSH connections.

❖ 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 file is 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 file is specified based on the user name.

Configuration Example

The following configuration examples describe only configurations related to SSH.

❖ Generating a Public Key on the SSH Server

Configuration Steps	▪ **Run the crypto key generate { rsa | dsa } command to generate a RSA public key for the server.**
SSH Server	QTECH#configure terminal QTECH(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.

SSH Server	QTECH(config)#show crypto key mypubkey rsa % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA1 private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU 8O3LojHL ayJ8G4pG 7j4T4ZSf FKg09kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t qFIKDj1j 0dKBcCfN tr0r/CT+ cs5tlGKV S0ICGifz oB+pYaE= % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEAAQAAAHJfLwKnzOgO F3RlKhTN /7PmQYoE v0a2VXTX 8ZCa7Sll EghLDLJc w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISgIfZ9 8o5No3Zz MPM0LnQR G4c7/28+ GOHzYkTk 4IiQuTIL HRgtbyEYXCFaaxU=

❖ Specifying the SSH Version

Configuration Steps	**Run the ip ssh version { 1 | 2 } command to set the version supported by the SSH server to SSHv2.**
SSH Server	QTECH#configure terminal QTECH(config)#ip ssh version 2
Verification	Run the **show ip ssh** command to display the SSH version currently supported by the SSH server.
SSH Server	QTECH(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled

❖ 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	QTECH#configure terminal QTECH(config)#ip sshtime-out100
Verification	Run the **show ip ssh** command to display the configured SSH authentication timeout.
SSH	QTECH(config)#show ip ssh SSH Enable - version 2.0 SSH Cipher Mode: cbc,ctr,others 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	QTECH#configure terminal QTECH(config)#ip ssh authentication-retries 2
Verification	Run the **show ip ssh** command to display the configured maximum number of authentication retries.
SSH Server	QTECH(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 2 SSH SCP Server: disabled

❖ Specifying the SSH Encryption Mode

Configuration Steps	**Run the ip ssh cipher-mode {cbc | ctr | others }command to set the encryption mode supported by the SSH server to CTR.**
SSH Server	QTECH#configure terminal QTECH(config)# ip ssh cipher-mode ctr

Verification	Select the CTR encryption mode on the SSH client, and verify whether you can successfully log in to the SSH server from the SSH client.

❖ Specifying the SSH Message Authentication Algorithm

Configuration Steps	**Run the ip ssh hmac-algorithm {md5 | md5-96 | sha1 | sha1-96 } command to set the message authentication algorithm supported by the SSH server to SHA1.**

SSH Server	`QTECH#configure terminal`
	
	`QTECH(config)# ip ssh hmac-algorithmsha1`

Verification	Select the SHA1 message authentication algorithm on the SSH client, and verify whether you can successfully log in to the SSH server from the SSH client.

❖ Configuring Support for DH Key Exchange Algorithm on the SSH Server

Command	**ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }**
Parameter Description	**dh_group_exchange_sha1**: Indicates configuration of diffie-hellman-group-exchange-sha1 for key exchange. **dh_group14_sha1**:Indicates configuration of diffie-hellman-group14-sha1 for key exchange. **dh_group1_sha1**: Indicates configuration of diffie-hellman-group1-sha1 for key exchange.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a DH key exchange method on the SSH. QTECH's SSHv1 server does not support DH key exchange method, while the SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 for key exchange.

❖ Setting A Monitoring Port ID for the SSH Server

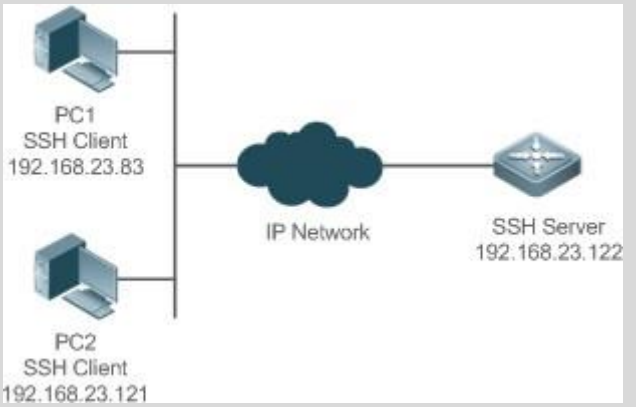
Configuration Steps	**Run the ip ssh port *port* command to set a monitoring port ID to 10000.**

SSH Server	QTECH# configure terminal QTECH(config)# ip ssh port 10000
Verification	Run the show ip ssh command to display information about a monitoring port ID for the SSH server.
	QTECH(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 10000 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 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	QTECH#configure terminal QTECH(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 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.

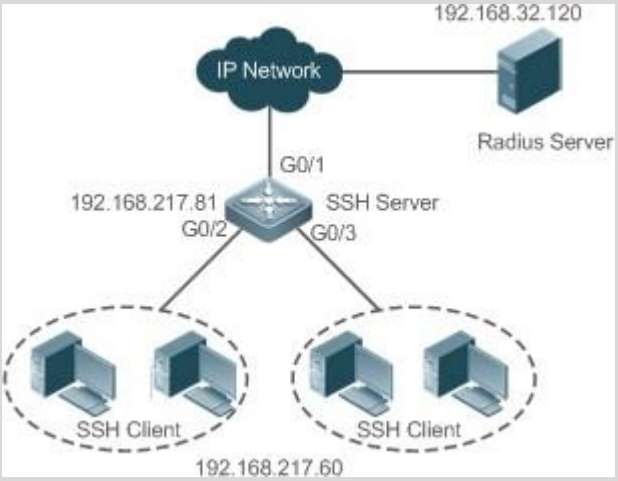
❖ Configuring SSH Local Line Authentication

Scenario **Figure 11-14**	 **SSH users can use the local line password for user authentication, as shown in Figure 11-14.To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server is enabled. The requirements are as follows:** ▪ **SSH users use the local line password authentication mode.** ▪ **Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.**
Configuration Steps	Configure the SSH server as follows: ▪ Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. ▪ Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses the RSA key, whereas SSHv2 uses the RSA or DSA key. ▪ Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server based on this IP address. The route from the SSH client to the SSH server is reachable.

SSH Server	Before configuring SSH-related function, ensure that the route from the SSH user to the network segment of the SSH server is reachable. The interface IP address configurations are shown in Figure 11-14. The detailed procedures for configuring IP addresses and routes are omitted. QTECH(config)# enable service ssh-server QTECH(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] QTECH(config)#interface fastEthernet0/1 QTECH(config-if-fastEthernet0/1)#ip address 192.168.23.122 255.255.255.0 QTECH(config-if-fastEthernet0/1)#exit QTECH(config)#line vty 0 QTECH(config-line)#password passzero QTECH(config-line)#privilege level 15 QTECH(config-line)#login QTECH(config-line)#exit QTECH(config)#line vty1 4 QTECH(config-line)#password pass QTECH(config-line)#privilege level 15 QTECH(config-line)#login QTECH(config-line)#exit
Verification	Run the **show running-config** command to display the current configurations.
SSH Server	QTECH#show running-config Building configuration... ! enable secret 5 1eyy2$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

❖ Configuring AAA Authentication of SSH Users

Scenario **Figure 11-17**	 **SSH users can use the AAA authentication mode for user authentication, as shown in Figure 11-17.To ensure security of data exchange, the PC functions as the SSH client, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used on the user login interface of the SSH client. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, select the local authentication method.**
Configuration Steps	▪ The route from the SSH client to the SSH server is reachable, and the route from the SSH server to the Radius server is also reachable.
	▪ Configure the SSH server on the network device. The configuration method is already described in the previous example, and therefore omitted here. ▪ Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types,

	and applied to a specified service or interface.
SSH Server	QTECH(config)# enable service ssh-server QTECH(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] QTECH(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] QTECH(config)#interface gigabitEthernet1/1 QTECH(config-if-gigabitEthernet1/1)#ip address 192.168.217.81 255.255.255.0 QTECH(config-if-gigabitEthernet1/1)#exit QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#radius-server host 192.168.32.120 QTECH(config)#radius-server key aaaradius QTECH(config)#aaa authentication login methodgroup radius local QTECH(config)#line vty 0 4 QTECH(config-line)#login authentication method QTECH(config-line)#exit QTECH(config)#username user1 privilege 1 password 111 QTECH(config)#username user2 privilege 10 password 222 QTECH(config)#username user3 privilege 15 password 333 QTECH(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.

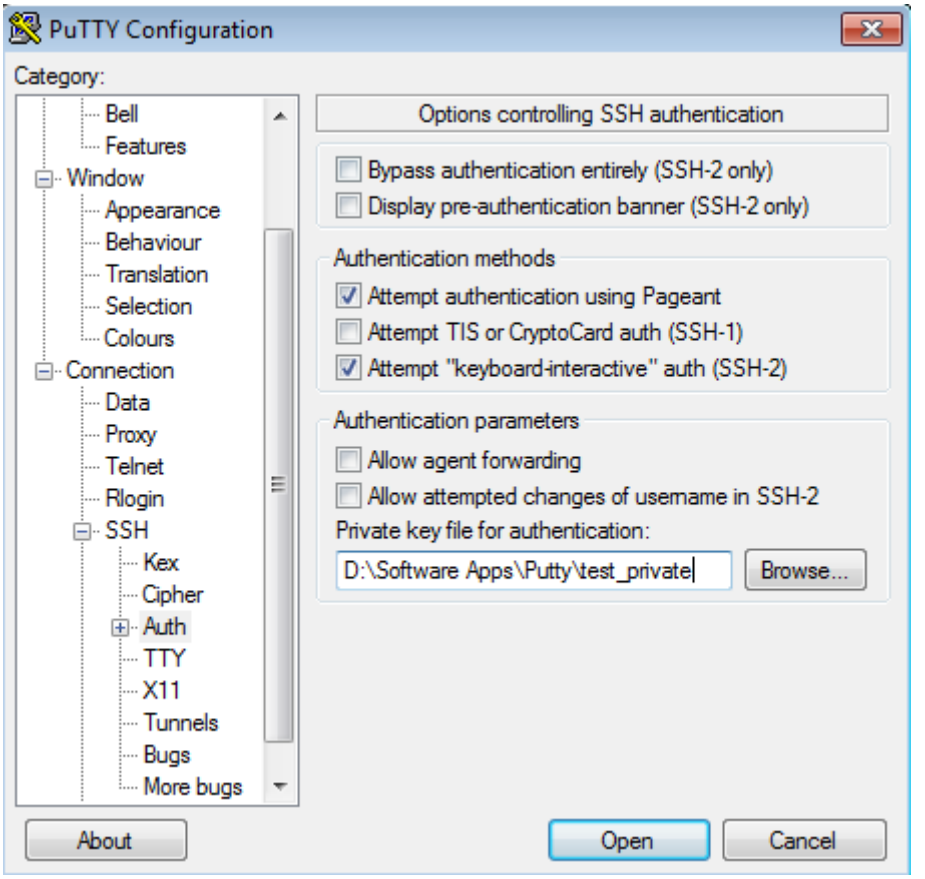
	▪ Check the login user.
	QTECH#show run aaa new-model ! aaa authentication login method group radius local ! username user1 password 111 username user2 password 222 username user2 privilege 10 username user3 password 333 username user3 privilege 15 no service password-encryption ! radius-server host 192.168.32.120 radius-server key aaaradius enable secret 5 1hbgz$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 ! On the SSH client, choose **System Management>Device Management**, and add the device IP address **192.168.217.81** and the device key **aaaradius**. Choose **Security Management>Device Management Rights**, and set the rights of the login user. Choose **Security Management>Device Administrator**, and add the user name **user** and password **pass**. Configure the SSH client and set up a connection to the SSH server. For details, see the previous example. Type in the user name **user** and password **pass**. Verify that you can log in to the SSH server

	successfully.

❖ Configuring Public Key Authentication of SSH Users

Scenario Figure 11-18	 **SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in Figure 11-18.SSH is configured on the client so that a secure connection is set up 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 Server	`QTECH#configure terminal` `QTECH(config)# ip ssh peer test public-key rsaflash:test_key.pub`
Verification	After completing the basic configurations of the client and the server, specify the private key file
	▪ test_private on the PuTTY client, and set the host IP address to 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.

Figure 11-24



Common Errors

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

11.4.2 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.

❖ **Configuring the Transmission Path for Files of the SCP Server**

- Optional.
- The default transmission path is **flash:/**. Run the **ip scp server topdir {flash:/*path* | flash2:/*path* | usb0:/*path* | usb1:/*path* | sd0:/*path* | sata0:/*path* | tmp:/*path* }** command to configure the transmission path to upload files to or download files from the SCP server.

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.

❖ Configuring the Transmission Path for Files of the SCP Server

Command	**ip scp server topdir {flash:/*path* | flash2:/*path* | usb0:/*path* | usb1:/*path* | sd0:/*path* | sata0:/*path* | tmp:/*path* }**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the transmission path to upload files to or download files from the SCP server. Run the **no ip scp server topdir** command to restore the default transmission path.

Configuration Example

❖ Enabling the SCP Server

Configuration Steps	**Run the ip scp server enable command to enable the SCP server.**
	QTECH#configure terminal QTECH(config)#ip scp server enable
Verification	Run the **show ip ssh** command to check whether the SCP server function is enabled.
	QTECH(config)#show ipssh QTECH(config)#show ip ssh SSH Enable - version 1.99 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: enabled

❖ Configuring SSH File Transfer

Scenario Figure 11-25	 **The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server.**
Configuration Steps	▪ Enable the SCP service on the server. 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. Most options are related to terminals. Few options are supported on both terminals and servers. QTECH's SCP servers do not support d-p-q-r options. When these options are applied, there are prompts.
SSH Server	QTECH#configure terminal QTECH(config)# ip scp server enable
Verification	File transmission example on the Ubuntu 7.10 system: Set the username of a client to **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

11.5 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**

Debugging

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

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

12.1. 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 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. 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 asymmetric traffic.

Protocols and Standards

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

12.2. Applications

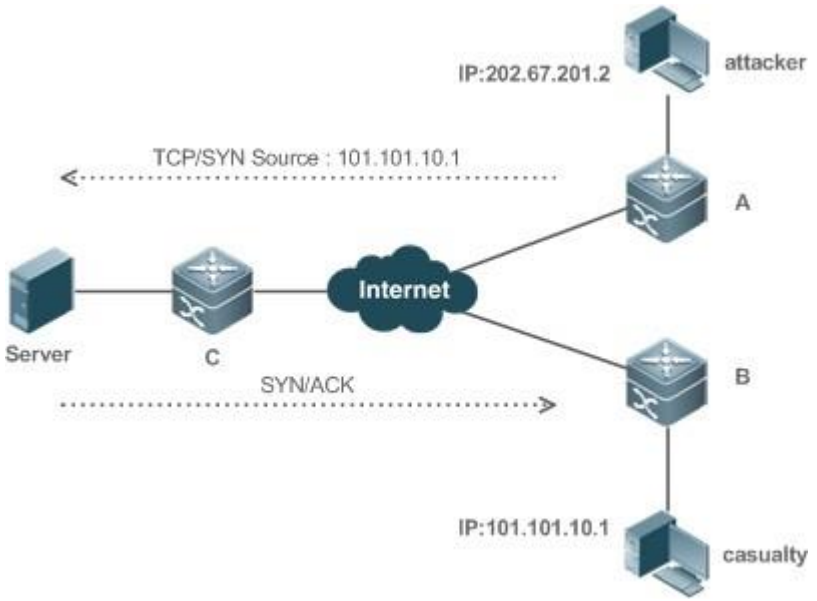
Application	Description
Strict Mode	Block the packets with spoofed sourced addresses at the access layer or aggregation layer to prevent sending these packets from PCs to the core network.
Loose Mode	On a multihomed network, the user network is connected to multiple Internet service providers (ISPs),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

12.2.1 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 affected. Even 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 12-1



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.

12.2.2 Loose Mode

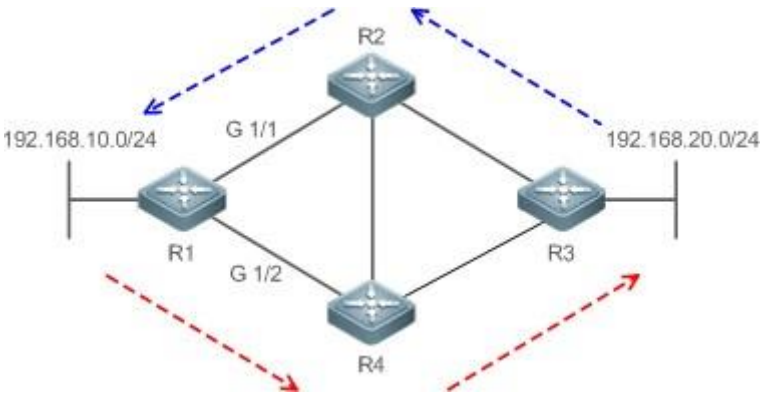
Scenario

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

As shown in Figure 12-2, 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 URPF check is G1/2.

Therefore, this packet fails in the URPF check and is dropped.

Figure 12-2



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 received packet.
- The URPF loose mode can resolve the asymmetric traffic problem of the asymmetric route and prevents access of invalid data streams.

12.3. 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 received packet. 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 to the URPF check per second. 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 collected for calculating the packet loss rate. 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 actual 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 measured at the 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 source address spoofing.
Notifying the URPF Packet Loss Rate	To facilitate monitoring of information about lost packets after URPF is enabled, QTECH devices support the use of syslogs and trap messages to proactively notify users of the packet loss information detected in the URPF check.

12.3.1. Enabling URPF

Enable URPF to perform a URPF check on IPv4 or IPv6 packets, thus protecting the device against source address spoofing.

Working Principle

URPF can be applied to IP 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 a 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 and IPv6 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.

A switch supports configuration of URPF on a routed port of L3 aggregate port (AP). Some switches also support configuration of URPF on a switch virtual interface (SVI). (For details about the switch products, contact QTECH technical support engineers.) The following constraints exists:

- After URPF is enabled on interfaces, a URPF check is performed on all packets received on 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 a 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 during the 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 or IPv6 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.

12.3.2. Notifying the URPF Packet Loss Rate

To facilitate monitoring of information about lost packets after URPF is enabled, QTECH devices support the use of 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 at the 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 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 fond inappropriate, run the **ip 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.

12.4. Configuration

Configuration Item	Description and Command	
Enabling URPF	(Mandatory) It is used to enable URPF.	
	ip unicast source reachable-via { rx | any } [allow-default] (Interface configuration mode)	Enables URPF for a specified interface.
Configuring the Function of Monitoring the URPF Packet Loss Information	(Optional) It is used to enable the function of monitoring the URPF packet loss information.	
	ip verify urpf drop-rate compute interval *seconds*	Configures the calculation interval of the URPF packet loss rate.
	ip verify urpf drop-rate notify	Configures the function 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 the URPF packet loss rate.

12.4.1 Enabling URPF

Configuration Effect

- Enable URPF to perform a URPF check on IP packets, thus protecting the device against source address spoofing.
- URPF can be enabled in interface configuration mode
- URPF enabled in interface 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, unicast routes must be configured on the network.

- URPF cannot be enabled on a range of interfaces.

Configuration Steps

❖ **Enabling IPv4 URPF for a Specified Interface**

- Mandatory.
- Switches supports configuration of IPv4 URPF on a routed port or L3 AP port, other products supports configuration of IPv4 URPF on a routed port.

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 source address of the received IPv4 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 packet; otherwise, the packet is dropped.

Related Commands

❖ **Enabling IPv4 URPF for a Specified Interface**

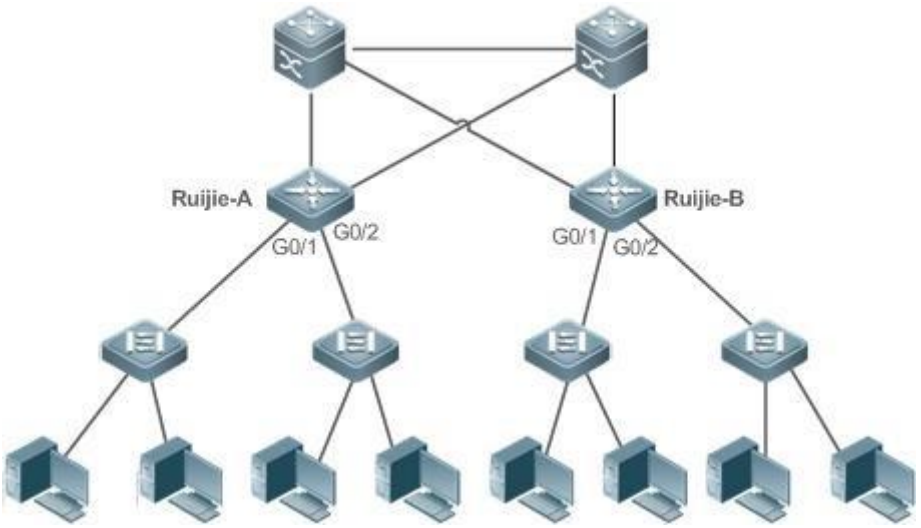
Command	**ip verify unicast source reachable-via { rx | any } [allow-default]**
Parameter Description	**rx**: Indicates that the URPF check is implemented in strict mode. The strict mode requires that the outbound interface of the forwarding entry found in the forwarding table based on the source address 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 received IP packet. **allow-default**: (Optional) Indicates that the default route can be used for the URPF check.
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 valid. If no 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. A switch will enable URPF check on IPv4 Packets. A switch supports configuration of URPF on a routed port or L3 AP port. In addition, the following constraints exists: 1. After URPF is enabled on interfaces, a URPF check is performed on all packets received on 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 a scenario, be cautious in enabling URPF. 2. 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 during the URPF check, the packet will be processed according to the URPF loose 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 interface between the aggregation** **device and the access device.**

Scenario Figure 12-3	
Verification	As shown in Figure 12-3, enable URPF in strict mode on the aggregation devices, including QTECH A and QTECH B. The configurations are as follows:
QTECH-A	QTECH-A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH-A (config)# interface gigabitEthernet0/1 QTECH-A (config-if-GigabitEthernet 0/1)#ip address 195.52.1.1 255.255.255.0 QTECH-A (config-if-GigabitEthernet 0/1)#ip verify unicast source reachable-via rx QTECH-A (config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify QTECH-A (config-if-GigabitEthernet 0/1)#exit QTECH-A (config)# interface gigabitEthernet0/2 QTECH-A (config-if-GigabitEthernet 0/2)#ip address 195.52.2.1 255.255.255.0 QTECH-A (config-if-GigabitEthernet 0/2)#ip verify unicast source reachable-via rx QTECH-A (config-if-GigabitEthernet 0/2)# ip verify urpf drop-rate notify QTECH-A (config-if-GigabitEthernet 0/2)#exit
QTECH-B	QTECH-B# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH-B (config)# interface gigabitEthernet0/1 QTECH-B (config-if-GigabitEthernet 0/1)#ip address 195.52.3.1 255.255.255.0 QTECH-B (config-if-GigabitEthernet 0/1)#ip verify unicast source reachable-via rx QTECH-B (config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify QTECH-B (config-if-GigabitEthernet 0/1)#exit QTECH-B (config)# interface gigabitEthernet0/2 QTECH-B (config-if-GigabitEthernet 0/2)#ip address 195.52.4.1 255.255.255.0 QTECH-B (config-if-GigabitEthernet 0/2)#ip verify unicast source reachable-via rx QTECH-B (config-if-GigabitEthernet 0/2)# ip verify urpf drop-rate notify

	QTECH-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	QTECH-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 QTECH-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 QTECH-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 QTECH-B#show ip urpf interface gigabitEthernet 0/2 IP verify source reachable-via RX IP verify URPF drop-rate notify enabled

❖ Configuring the Loose Mode

	On the egress device QTECH 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 12-4	
QTECH-A	QTECH-A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH-A (config)# interface gigabitEthernet3/1 QTECH-A (config-if-GigabitEthernet 3/1)# ip address 195.52.1.2 255.255.255.252 QTECH-A (config-if-GigabitEthernet 3/1)# ip verify unicast source reachable-via any QTECH-A (config-if-GigabitEthernet 3/1)# ip verify urpf drop-rate notify QTECH-A (config-if-GigabitEthernet 3/1)# exit QTECH-A (config)# interface gigabitEthernet3/2 QTECH-A (config-if-GigabitEthernet 3/2)# ip address 152.95.1.2 255.255.255.252 QTECH-A (config-if-GigabitEthernet 3/2)# ip verify unicast source reachable-via any QTECH-A (config-if-GigabitEthernet 3/2)# ip verify urpf drop-rate notify QTECH-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	QTECH #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

12.4.2 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.
- Global configuration mode

❖ **Configuring the Alarm Interval of the URPF Packet Loss Rate**

- Optional.
- 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 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 calculation interval of the URPF packet loss rate is configured in global configuration mode. The configuration is applied to the global and interface-based calculation of the URPF packet loss rate.

❖ 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 configuration mode. The configuration is applied to the global and interface-based alarms of the URPF packet loss rate.

❖ 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 mode.**
	QTECH#configure terminal QTECH(config)# ip verify urpf drop-rate compute interval 120 QTECH(config)# end
Verification	Run the **show ip urpf** command to check whether the configuration takes effect.
	QTECH# 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 configuration mode.**
	QTECH#configure terminal QTECH(config)# ip verify urpf drop-rate notify hold-down 120 QTECH(config)# end
Verification	Run the **show ip urpf** command to check whether the configuration takes effect.
	QTECH# show ip urpfIP verify URPF drop-rate notify hold-down is 120s

❖ Enabling the Function of Monitoring the IPv4 URPF Packet Loss Information on the Interface GigabitEthernet 0/1

Configuration	**Enable the function of monitoring the IPv4 URPF packet loss information on the interface GigabitEthernet 0/1.**
	QTECH#configure terminal QTECH(config)# interface gigabitEthernet0/1 QTECH(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via rx QTECH(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
Verification	Run the **show ip urpf** command to check whether the function of monitoring the IPv4 URPF packet loss information is enabled on the interface GigabitEthernet 0/1.
	QTECH# show ip urpf interface gigabitEthernet 0/1 IP verify source reachable-via RX IP verify URPF drop-rate notify is enabled IP verify URPF notification threshold is 1000pps Number of drop packets in this interface is 0 Number of drop-rate notification counts in this interface is 0

- Setting the Threshold of the IPv4 URPF Packet Loss Rate to 2,000 pps on the Interface GigabitEthernet 0/1

Configuration	**Set the threshold of the IPv4 URPF packet loss rate to 2,000 pps on the interface GigabitEthernet 0/1.**
	QTECH#configure terminal QTECH(config)# interface gigabitEthernet0/1 QTECH(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via rx QTECH(config-if-GigabitEthernet 0/1)#ip verify urpf notification threshold 2000

Verification	Run the **show ip urpf** command to check the threshold of the IPv4 URPF packet loss rate and the threshold of the IPv6 URPF packet loss rate. QTECH# show ip urpf interface gigabitEthernet 0/1 IP verify source reachable-via RX IP verify URPF drop-rate notify is enabled IP verify URPF notification threshold is 2000pps Number of drop packets in this interface is 0

12.5 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*]

Debugging

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

Description	Command
Debugs the URPF events.	**debug urpf event**
Debugs the URPF timers.	**debug urpf timer**

13.1 Overview

The CPU Protect Policy (CPP) provides policies for protecting the CPU of a switch.

In network environments, various attack packets spread, which may cause high CPU usages of the switches, affect protocol running and even difficulty in switch management. To this end, switch CPUs must be protected, that is, traffic control and priority-based processing must be performed for various incoming packets to ensure the processing capabilities of the switch CPUs.

CPP can effectively prevent malicious attacks in the network and provide a clean environment for legitimate protocol packets. CPP is enabled by default. It provides protection during the entire operation of switches.

13.2 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 Processing Bottlenecks	Even when no attacks exist, it would become a bottleneck for CPU to handle excessive normal traffic. CPP can limit the rate of packets being sent to the CPU to ensure normal operation of switches.

13.2.1 Preventing Malicious Attacks

Scenario

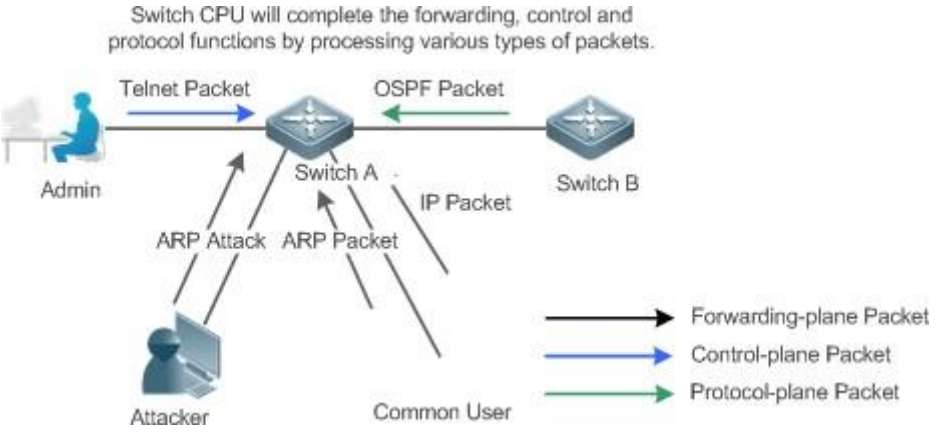
Network switches at all levels may be attacked by malicious packets, typically ARP attacks.

As shown in Figure 13-1, switch CPUs process three types of packets: forwarding-plane, control-plane and protocol-plane. Forwarding-plane packets are used for routing, including ARP packets and IP route disconnection packets. Control-plane packets are used to manage services on switches, including Telnet packets and HTTP packets. Protocol-plane packets serve for running protocols, including 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 be

discarded) and consume many CPU resources (for processing ARP attack packets). Consequently, the CPU fails to work normally. In the scenario as shown in Figure 13-1, possible consequences include: common users fail to access the network; administrators fail to manage switches; the OSPF link between switch A and the neighbor B is disconnected and route learning fails.

Figure 13-1 Networking Topology of Switch Services and Attacks



Deployment

- By default, CPP classifies ARP packets, Telnet packets, IP route disconnection packets, and OSFP packets into queues of different priorities. In this way, ARP packets will not affect other packets.
- By default, CPP limits the rates of ARP packets and the rates of the priority queue where the ARP packets reside to ensure that the attack packets do not occupy too many CPU resources.
- Packets in the same priority queue with ARP packets may be affected by ARP attack packets. You can divide the packets and the ARP packets into different priority queues by means of configuration.
- When ARP attack packets exist, CPP cannot prevent normal ARP packets from being affected. CPP can only differentiate the packet type but cannot distinguish attack packets from normal packets of the same type. In this case, the Network Foundation Protection Policy (NFPP) function can be used to provide higher-granularity attack prevention.

For description of NFPP configurations, see the *Configuring NFPP*.

13.2.2 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 and 802.1X authentication packets.

13.3 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 classifying service streams to provide differentiated services.

❖ Bandwidth, Rate

Bandwidth refers to the maximum allowable data rate, which refers to the rate threshold in this document. Packets whose rates exceed the threshold will be discarded.

The rate indicates an actual data rate. When the rate of packets exceeds the bandwidth, packets out of the limit will be discarded. The rate must be equal to or smaller than the bandwidth.

The bandwidth and rate units in this document are packets per second (pps).

❖ L2, L3, L4

The structure of packets is hierarchical based on the TCP/IP model.

L2 refers to layer-2 headers, namely, the Ethernet encapsulation part; L3 refers to layer-3 headers, namely, the IP encapsulation part; L4 refers to layer-4 headers, usually, the TCP/UDP encapsulation part.

❖ Priority Queue, SP

Packets are cached inside a switch and packets in the output direction are cached in queues. Priority queues are mapped to Strict Priorities (SPs). Queues are not equal but have different priorities.

The SP is a kind of QoS scheduling algorithm. When a higher priority queue has packets, the packets in this queue are scheduled first. Scheduling refers to

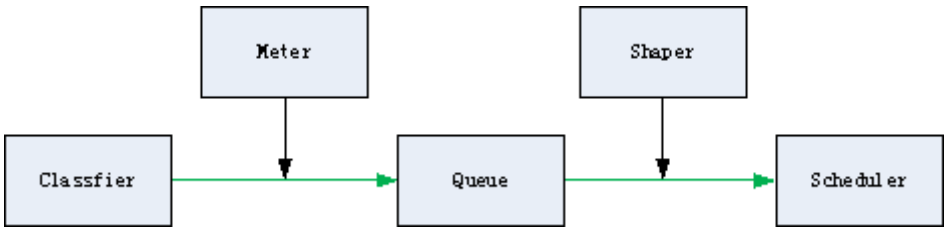
selecting packets from queues for output and refers to selecting and sending the packets to the CPU in this document.

- **CPU interface**

Before sending packets to the CPU, a switch will cache the packets. The process of sending packets to the CPU is similar to the process of packet output. The CPU interface is a virtual interface. When packets are sent to the CPU, the packets will be output from this virtual interface. The priority queue and SP mentioned above are based on the CPU interface.

Overview

CPP protects the CPU by using the standard QoS DiffServ model. Figure 13-2 CPP Implementation Model



Feature	Description
Classfier	Classifies packet types and provides assurance for the subsequent implementation of QoS 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.

Classifier

Working Principle

The Classifier classifies all packets to be sent to the CPU based on the L2, L3 and L4 information of the packets. Classifying packets is the basis for implementing QoS policies. In subsequent actions, different policies are implemented based on the classification to provide differentiated services. A switch provides fixed classification. The management function classifies packet types based on the protocols supported by the switch, for example, STP BPDU packets and ICMP packets. Packet types cannot be customized.

13.3.1 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.

13.3.2 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.

13.3.3 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.

13.3.4 Shaper

Working Principle

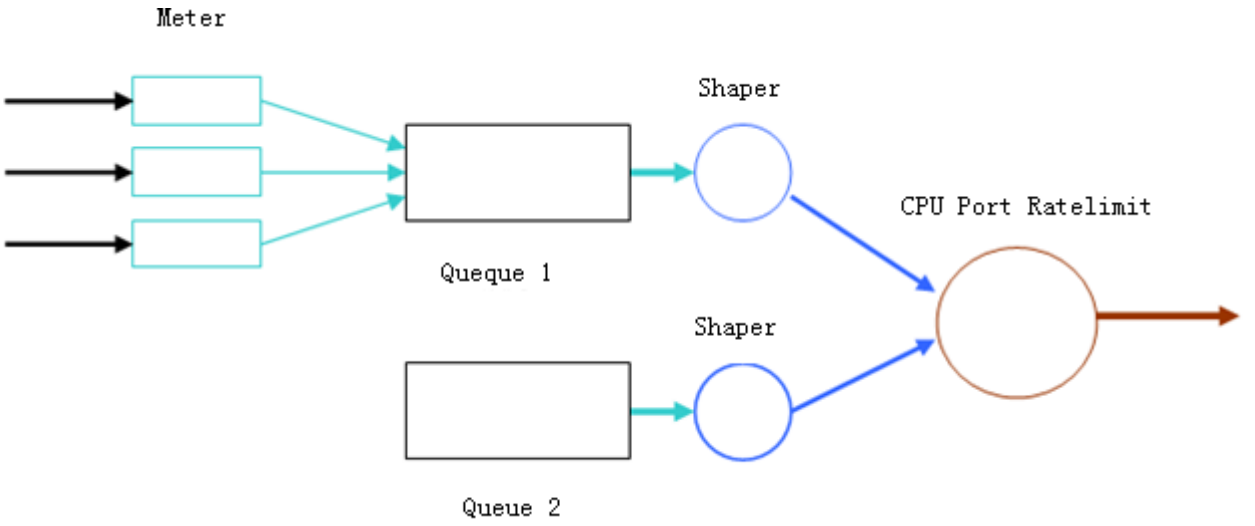
The Shaper is used to shape packets to be sent to the CPU, that is, when the actual rate of packets is greater than the shaping threshold, the packets must stay in the queue and cannot be scheduled. When packet rates fluctuate, the Shaper ensures that the rates of packets sent to the CPU are smooth (no more than the shaping threshold).

When the Shaper is available, packets in a queue with a lower priority may be scheduled before all packets in a queue with a higher priority are scheduled. If the rate of packets in a queue with certain priority exceeds the shaping threshold, scheduling of the packets in this queue may be stopped temporarily. Therefore, the Shaper can prevent packets in queues with lower priorities from starvation

(which means that only packets in queues with higher priorities are scheduled and packets in queues with higher priorities are not scheduled).

Since the Shaper limits the scheduling rates of packets, it actually plays the rate limit function. The Shaper provides level-2 rate limit for priority queues and all packets sent to the CPU (CPU interface). The Shaper and Meter functions provide 3-level rate limit together and provide level-3 protection for the CPU.

Figure 13-3 Level Rate Limit of the CPP



13.4 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.
	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 for the CPU

		interface.

13.4.1 Configuring CPP

Configuration Effect

- By configuring the Meter function, you can set the bandwidth and rate limit for a packet type. Packets out of the limit will be directly discarded.
- By configuring the Queue function, you can select a priority queue for a packet type. Packets in a queue with a higher priority will be scheduled first.
- By configuring the Shaper function, you can set the bandwidth and rate limit for a CPU interface and a priority queue. Packets out of the limit will be directly discarded.

Notes

- Pay special attention when the bandwidth of a packet type is set to a smaller value, which may affect the normal traffic of the same type. To provide per-user CPP, combine the NFPP function.
- When the Meter and Shaper functions are combined, 3-level protection will be provided. Any level protection fights alone may bring negative effects. For example, if you want to increase the Meter of a packet type, you also need to adjust the Shaper of the corresponding priority queue. Otherwise, the packets of this type may affect other types of packets in the same priority queue.

Configuration Steps

❖ **Configuring the Meter for a packet type**

- You can use or modify the default value but cannot disable it.
- You need to modify the configuration in the following cases: when packets of a type are not attackers but are discarded, you need to increase the Meter of this packet type. If attacks of a packet type cause abnormal CPU running, you need to decrease the Meter of this packet type.
- This configuration is available on all switches in a network environment.

❖ **Configuring the priority queue for a packet type**

- You can use or modify the default value but cannot disable it.
- You need to modify the configuration in the following cases: When attacks of a packet type cause abnormality of other packets in the same queue, you can put the packet type in an unused queue. If a packet type cannot be discarded but the packet type is in the same queue with other packet types in use, you can put this packet type in a queue with a higher priority.
- This configuration is available on all switches in a network environment.

❖ **Configuring the Shaper for a priority queue**

- You can use or modify the default value and cannot disable it.
- You need to modify the configuration in the following cases: If the Meter value of a packet type is greater which causes that other packets in the corresponding priority queue do not have sufficient bandwidth, you need to increase the Shaper for this priority queue. If attack packets are put in a priority queue and no other packets are in use, you need to increase the Shaper of this priority queue.
- This configuration is available on all switches in a network environment.

❖ **Configuring the Shaper for the CPU interface**

- You can use or modify the default value and cannot disable it.
- You are not advised to change the Shaper of the CPU interface.
- This configuration is available on all switches in a network environment.

Verification

- Modify the configurations when the system runs abnormally, and view the system running after the modification to check whether the configurations take effect.
- Check whether the configurations take effect by viewing corresponding configurations and statistic values. For details, see the following commands.

Related Commands

❖ **Configuring the Meter for a packet type**

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 packets or the 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. QTECH# configure terminal QTECH(config)# cpu-protect type arp traffic-class 1 QTECH(config)# cpu-protect type arp bandwidth 5000 QTECH(config)# cpu-protect type ospf traffic-class 5 QTECH(config)# cpu-protect type v4uc-route traffic-class 3 QTECH(config)# cpu-protect type traffic-class 3 bandwidth 5000 QTECH(config)# end QTECH# configure terminal QTECH(config)# cpu-protect type arp traffic-class 1 QTECH(config)# cpu-protect type arp bandwidth 5000 QTECH(config)# cpu-protect type ospf traffic-class 5 QTECH(config)# cpu-protect type v4uc-route traffic-class 3 QTECH(config)# cpu-protect type traffic-class 3 bandwidth 5000 QTECH(config)# end
Verification	Run the **show cpu-protect** command to view the configuration and statistics. QTECH#show cpu-protect %cpu port bandwidth: 100000(pps) Traffic-class Bandwidth(pps) Rate(pps) Drop(pps) 0 6000 0 0 1 6000 0 0 2 6000 0 0 3 6000 0 0 4 6000 0 0 5 6000 0 0 6 6000 0 0 7 6000 0 0 Packet Type Traffic-class Bandwidth(pps) Ra te(pps) Drop(pps) Total Total Drop bpdu 6 128 0 0 0 0 arp 1 3000 0 0 0 0 tpp 6 128 0 0 0 0 dot1x 2 1500 0 0 0

0	gvrp	5	128	0	0	0
0	rldp	5	128	0	0	0
0	lacp	5	256	0	0	0
0	rerp	5	128	0	0	0
0	reup	5	128	0	0	0
0	lldp	5	768	0	0	0
0	cdp	5	768	0	0	0
0	dhcps	2	1500	0	0	0
0	dhcps6	2	1500	0	0	0
0	dhcp6-client	2	1500	0	0	0
0	dhcp6-server	2	1500	0	0	0
0	dhcp-relay-c	2	1500	0	0	0
0	dhcp-relay-s	2	1500	0	0	0
0	option82	2	1500	0	0	0
0	tunnel-bpdu	2	128	0	0	0
0	tunnel-gvrp	2	128	0	0	0
0	unknown-v6mc		128	0	0	0
0	xgv6-ipmc	1	128	0	0	0
0	stargv6-ipmc	1	128	0	0	0
0	unknown-v4mc	1	128	0	0	0
0	xgv-ipmc	2	128	0	0	0
0	stargv-ipmc	2	128	0	0	0
0	udp-helper	1	128	0	0	0
0	dvmrp	4	128	0	0	0
0	igmp	2	1000	0	0	0
0	icmp	3	1600	0	0	0
0	ospf	4	2000	0	0	0
0	ospf3	4	2000	0	0	0
0	pim	4	1000	0	0	0
0	pimv6	4	1000	0	0	0
0	rip	4	128	0	0	0
0	ripng	4	128	0	0	0
0	vrrp	6	256	0	0	0
0	vrrpv6	6	256	0	0	0
0	ttl0	0	128	0	0	0
0	ttl1	0	2000	0	0	0
0	hop-limit	0	800	0	0	0
0	local-ipv4	3	4000	0	0	0
0	local-ipv6	3	4000	0	0	0
0	v4uc-route	1	800	0	0	0
0	v6uc-route	1	800	0	0	0
0	rt-host	4	3000	0	0	0
0	mld	2	1000	0	0	0
0	nd-snp-ns-na	1	3000	0	0	0
0	nd-snp-rs	1	1000	0	0	0
0	nd-snp-ra-redirect	1	1000	0	0	0
0	erps	5	128	0	0	0
0	mpls-ttl0	4	128	0	0	0
0	mpls-ttl1	4	128	0	0	0
0	mpls-ctrl	4	128	0	0	0
0	isis	4	2000	0	0	0
0	bgp	4	2000	0	0	0
0	cfm	5	512	0	0	0
0	web-auth	2	2000	0	0	0
0	fcoe-fip	4	1000	0	0	0
0	fcoe-local	4	1000	0	0	0

```
bfd                6          5120              0          0          0
0 micro-bfd        6          5120              0          0          0
0 micro-bfd-v6     6          5120              0          0          0
0 dldp             6          3200              0          0          0
0 other            0          4096              0          0          0
0 trill            4          1000              0          0          0
0 efm              5          1000              0          0          0
0 ipv6-all         0          2000              0          0          0
0 ip-option        0          800               0          0          0
0 mgmt 4000        4          4639              0          0          0
0  dns             2          200               0          0          0
0 sdn              0          5000              0          0          0
0 sdn_of_fetch     0          5000              0          0          0
0 sdn_of_copy      0          5000              0          0          0
0 sdn_of_trap      0          5000              0          0          0
0 vxlan-non-uc     1          512               0          0          0
0 local-telnet     3          1000              0          0          0
0 local-snmp       3          1000              0          0          0
0 local-ssh        3          1000              0          0          0
0
```

13.5 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	**show cpu-protect cpu**

interface.	
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. For chassis devices, the parameter **slot** is used to specify a line card; for cassette devices, **slot** is unavailable.
- In the VSU mode, the parameter **device** indicates a cassette device. If the **device** value is not specified, it indicates the master device.

14.1 Overview

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record and monitor users' IP addresses and filter out illegal DHCP packets, including client request packets and server response packets. The legal user database generated from DHCP Snooping records may serve security applications like IP Source Guard.

Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

14.2 Applications

Application	Description
Guarding against DHCP service spoofing	In a network with multiple DHCP servers, DHCP clients are allowed to obtain 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 example, DHCP-RELEASE packets.
Guarding against IP/MAC spoofing	Malicious network users may send forged IP packets, for example, tampered 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 normal users' communication.

14.2.1 Guarding Against DHCP Service Spoofing

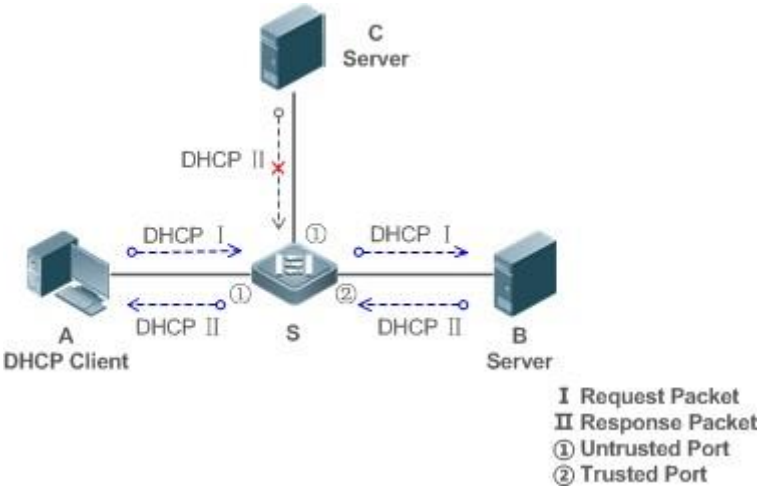
Scenario

Multiple DHCP servers may exist in a network. It is essential to ensure that user PCs obtain network configurations only from the DHCP servers within a controlled area.

Take the following figure as an example. The DHCP client can only communicate with trusted DHCP servers.

- Request packets from the DHCP client can be transmitted only to trusted DHCP servers.
- Only the response packets from trusted DHCP servers can be transmitted to the client.

Figure 14-1



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.

14.2.2 Guarding Against DHCP Packet Flooding

Scenario

Potential malicious DHCP clients in a network may send high-rate DHCP packets. As a result, legitimate users cannot obtain IP addresses, and access devices are highly loaded or even break down. It is necessary to take actions to ensure network stability.

With the DHCP Snooping rate limit function for DHCP packets, a DHCP client can only send DHCP request packets at a rate below the limit.

- The request packets from a DHCP client are sent at a rate below the limit.
- Packets sent at rates beyond the limit will be discarded.
- Enable DHCP Snooping correlation with ARP, and delete the non-existing entries.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Limit the rates of DHCP packets from the untrusted ports.
- Enable DHCP Snooping correlation with ARP, and detect whether the user is online.

14.2.3 Guarding Against Forged DHCP Packets

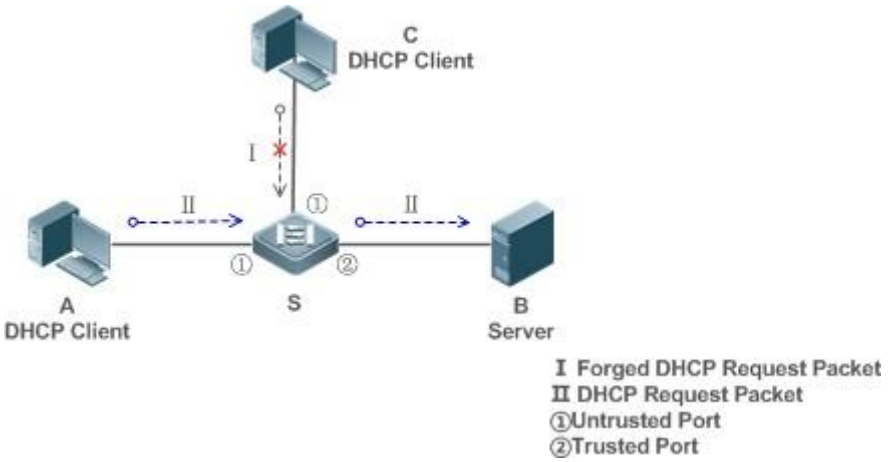
Scenario

Potential malicious clients in a network may forge DHCP request packets, consuming applicable IP addresses from the servers and probably preempting legal users' IP addresses. Therefore, it is necessary to filter out illegal DHCP packets.

For example, as shown in the figure below, the DHCP request packets sent from DHCP clients will be checked.

- The source MAC address fields of the request packets from DHCP clients must match the **chaddr** fields of DHCP packets.
- The Release packets and Decline packets from clients must match the entries in the DHCP Snooping binding database.

Figure 14-2



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.

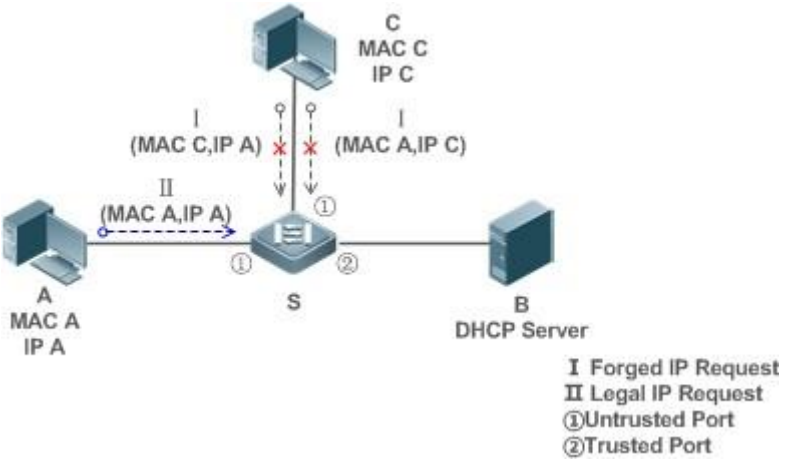
14.2.4 Guarding Against IP/MAC Spoofing

Scenario

Check IP packets from untrusted ports to filter out forged IP packets based on IP or IP-MAC fields. For example, in the following figure, the IP packets sent by DHCP clients are validated.

- The source IP address fields of IP packets must match the IP addresses assigned by DHCP.
- The source MAC address fields of layer-2 packets must match the **chaddr** fields in DHCP request packets from clients.

Figure 14-3



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.

14.2.5 Preventing Lease of IP Addresses

Scenario

Validate the source addresses of IP packets from untrusted ports compared with DHCP-assigned addresses.

If the source addresses, connected ports, and layer-2 source MAC addresses of ports in IP packets do not match the assignments of the DHCP server, such packets will be discarded.

The networking topology scenario is the same as that shown in the previous figure.

Deployment

- The same as that in the section "Guarding Against IP/MAC Spoofing".

14.2.6 Detecting ARP Attacks

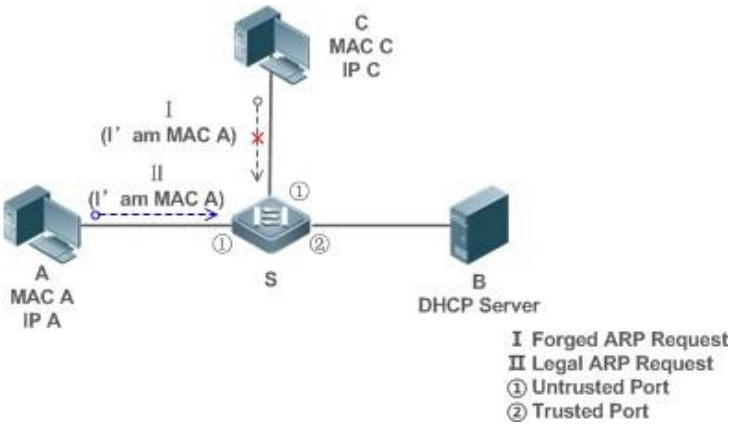
Scenario

Check the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

For example, in the following figure, the ARP packets sent from DHCP clients will be checked.

- The ports receiving ARP packets, the layer-2 MAC addresses, and the source MAC addresses of ARP packets senders shall be consistent with the DHCP Snooping histories.

Figure 14-4



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

14.3 Features

Basic Concepts

❖ **DHCP Request Packets**

Request packets are sent from a DHCP client to a DHCP server, including DHCP-DISCOVER packets, DHCP-REQUEST packets, DHCP-DECLINE packets, DHCP-RELEASE packets and DHCP-INFORM packets.

❖ **DHCP Response Packets**

Response packets are sent from a DHCP server to a DHCP client, including DHCP-OFFER packets, DHCP-ACK packets and DHCP-NAK packets.

❖ **DHCP Snooping Trusted Ports**

IP address request interaction is complete via broadcast. Therefore, illegal DHCP services will influence normal clients' acquisition of IP addresses and lead to service spoofing and stealing. To prevent illegal DHCP services, DHCP Snooping ports are divided into two types: trusted ports and untrusted ports. The access devices only transmit DHCP response packets received on trusted ports, while such packets from untrusted ports are discarded. In this way, we may configure the ports connected to a legal DHCP Server as trusted and the other ports as untrusted to shield illegal DHCP Servers.

On switches, all switching ports or layer-2 aggregate ports are defaulted as untrusted, while trusted ports can be specified. On wireless access points (APs), all the WLAN interfaces are untrusted and cannot be specified as trusted. In fat AP configuration mode, all the layer-2 switching ports and layer-2 encapsulation sub-interfaces are untrusted by default, and can be specified as trusted. In fit AP configuration mode, all the layer-2 switching ports are untrusted by default and can be specified as trusted, and all the layer-2 encapsulation sub-interfaces are trusted and cannot be specified as untrusted. On wireless access controllers (ACs), all WLAN interfaces are untrusted ports and cannot be specified as trusted, and all the switching ports and layer-2 aggregate ports are untrusted ports by default and can be specified as trusted.

❖ DHCP Snooping Packet Suppression

To shield all the DHCP packets on a specific client, we can enable DHCP Snooping packet suppression on its untrusted ports.

❖ VLAN-based DHCP Snooping

DHCP Snooping can work on a VLAN basis. By default, when DHCP Snooping is enabled, it is effective to all the VLANs of the current client. Specify VLANs help control the effective range of DHCP Snooping flexibly.

❖ DHCP Snooping Binding Database

In a DHCP network, clients may set static IP addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legal clients with IP addresses assigned by the DHCP server may fail to use the network normally due to address conflict. Through snooping packets between clients and servers, DHCP Snooping summarizes the user entries including IP addresses, MAC address, VLAN ID (VID), ports and lease time to build the DHCP

Snooping binding database. Combined with ARP detection and ARP check, DHCP Snooping controls the reliable assignment of IP addresses for legal clients.

❖ DHCP Snooping Rate Limit

DHCP Snooping rate limit function can be configured through the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see the *Configuring NFPP*.

❖ DHCP Option82

DHCP Option82, an option for DHCP packets, is also called DHCP Relay Agent Information Option. As the option number is 82, it is known as Option82. Option82 is developed to enhance the security of DHCP servers and improve the strategies of IP address assignment. The option is often configured for the DHCP relay services of a network access device like DHCP Relay and DHCP Snooping. This option is transparent to DHCP clients, and DHCP relay components realize the addition and deduction of the option.

❖ Illegal DHCP Packets

Through DHCP Snooping, validation is performed on the DHCP packets passing through a client. Illegal DHCP packets are discarded, user information is recorded into the DHCP Snooping binding database for further applications (for example, ARP detection). The following types of packets are considered illegal DHCP packets.

- The DHCP response packets received on untrusted ports, including DHCP-ACK, DHCP-NACK and DHCP-OFFER packets
- The DHCP request packets carrying gateway information **giaddr**, which are

received on untrusted ports

- When MAC verification is enabled, packets with source MAC addresses different with the value of the **chaddr** field in DHCP packets
- DHCP-RELEASE packets with the entry in the DHCP Snooping binding database Snooping while with untrusted ports inconsistent with settings in this binding database
- DHCP packets in wrong formats, or incomplete

verview

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 binding database	Snoop the interaction between DHCP clients and the server, and generate the DHCP Snooping binding database to provide basis for other filtering modules.

14.3.1 Filtering DHCP Packets

Perform validation on DHCP packets from untrusted ports. Filter out the illegal packets as introduced in the previous section "Basic Concepts".

Working Principle

During snooping, check the receiving ports and the packet fields of packets to realize packet filtering, and modify the destination ports of packets to realize control of transmit range of the packets.

- **Checking Ports**

In receipt of DHCP packets, a client first judges whether the packet receiving ports are DHCP Snooping trusted ports. If yes, legality check and binding entry addition are skipped, and packets are transferred directly. For not, both the check and addition are needed.

- **Checking Packet Encapsulation and Length**

A client checks whether packets are UDP packets and whether the destination port is 67 or 68. Check whether the packet length match the length field defined in protocols.

- **Checking Packet Fields and Types**

According to the types of illegal packet introduced in the section "Basic Concepts", check the fields **giaddr** and **chaddr** in packets and then check

whether the restrictive conditions for the type of the packet are met.

Related Configuration

- **Enabling Global DHCP Snooping**

By default, DHCP Snooping is disabled.

It can be enabled on a device using the **ip dhcp snooping** command.

Global DHCP Snooping must be enabled before VLAN-based DHCP Snooping is applied.

- **Configuring VLAN-based DHCP Snooping**

By default, when global DHCP Snooping is effective, DHCP Snooping is effective to all VLANs.

Use the [**no**] **ip dhcp snooping vlan** command to enable DHCP Snooping on specified VLANs or delete VLANs from the specified VLANs. The value range of the command parameter is the actual range of VLAN numbers.

- **Configuring DHCP Snooping Source MAC Verification**

By default, the layer-2 MAC addresses of packets and the **chaddr** fields of DHCP packets are not verified.

When the **ip dhcp snooping verify mac-address** command is used, the source MAC addresses and the **chaddr** fields of the DHCP request packets sent from untrusted ports are verified. The DHCP request packets with different MAC addresses will be discarded.

14.3.2 Building the Binding Database

DHCP Snooping detects the interactive packets between DHCP clients and the DHCP server, and generate entries of the DHCP Snooping binding database according to the information of legal DHCP packets. All these legal entries are provided to other security modules of a client as the basis of filtering packets from network.

Working Principle

During snooping, the binding database is updated timely based on the types of DHCP packets.

- **Generating Binding Entries**

When a DHCP-ACK packet on a trusted port is snooped, the client's IP address, MAC address, and lease time field are extracted together with the port ID (a wired interface index or WLAN ID) 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.

14.4 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 Snooping packet 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 Snooping binding database to Flash periodically.
	ip dhcp snooping database write-to-flash	Writes the DHCP Snooping binding database to Flash manually.
	renew ip dhcp snooping database	Imports Flash storage to the DHCP Snooping Binding database.
	ip dhcp snooping database	Configures file backup of the DHCP Snooping binding database.
	ip dhcp snooping trust	Configures DHCP Snooping trusted ports.

	ip dhcp snooping bootp	Enables BOOTP support.
	ip dhcp snooping check-giaddr	Enables DHCP Snooping to support the function of processing Relay requests.
	ip dhcp snooping monitor	Enables DHCP Snooping monitoring.
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 sub-potion **remote-id** of Option82 as a user-defined characterstring.

14.4.1 Configuring Basic Features

Configuration Effect

- Enable DHCP Snooping.
- Generate the DHCP Snooping binding database.
- Control the transmit range of DHCP packets.
- Filter out illegal DHCP packets.

Notes

- The ports on clients connecting a trusted DHCP server must be configured as trusted.
- DHCP Snooping is effective on the wired switching ports, layer-2 aggregate ports, and layer-2 encapsulation sub-interfaces as well as WLAN interfaces. The configuration can be implemented in interface configuration mode and WLAN security configuration mode.
- DHCP Snooping and DHCP Relay are mutually exclusive in VRF scenarios.

Configuration Steps

❖ **Enabling Global DHCP Snooping**

- Mandatory.
- Unless otherwise noted, the feature should be configured on access devices.

❖ **Enabling or Disabling VLAN-based DHCP Snooping**

- DHCP Snooping can be disabled if not necessary for some VLANs.
- Unless otherwise noted, the feature should be configured on access devices.

❖ **Configuring DHCP Snooping Trusted Ports**

- Mandatory.
- Configure the ports connecting a trusted DHCP server as trusted.

❖ **Enabling DHCP Snooping Source MAC Validation**

- This configuration is required if the **chaddr** fields of DHCP request packets match the layer-2 source MAC addresses of data packets.
- Unless otherwise noted, the feature should be enabled on all the untrusted ports of access devices.

❖ **Writing the DHCP Snooping Binding Database to Flash Periodically**

- Enable this feature to timely save the DHCP Snooping binding database information in case that client reboot.
- Unless otherwise noted, the feature should be configured on access devices.

❖ **Enabling BOOTP Support**

- Optional
- Unless otherwise noted, the feature should be configured on access devices.

❖ **Enabling DHCP Snooping to Process Relay Requests**

- Optional.
- Unless otherwise noted, the feature should be enabled on access devices.

❖ **Enabling DHCP Snooping Monitoring**

- Optional.
- If DHCP Snooping binding entries need to be generated on a routing port, the feature should be enabled on Layer-3 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/WLAN security 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 Snooping database to the 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 device 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 FLASH documents in real time. If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored from FLASH documents because of version differences between FLASH documents.

❖ Importing Backep File 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 backup file to the DHCP Snooping binding database.

❖ Configure File Backup of the DHCP Snooping Binding Database

Command	ip dhcp snooping database sata0 [interval *time*]
Parameter Description	*time*: the interval of storing the database in the unit of second. The range is from 10s to 86,400s. The default value is 300s.
Command Mode	Global configuration mode
Usage Guide	After this feature is enabled, the DHCP Snooping database can be written to the backup file of a specified type. In this way, users are able to resume communication immediately after restart of the device.

❖ 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.

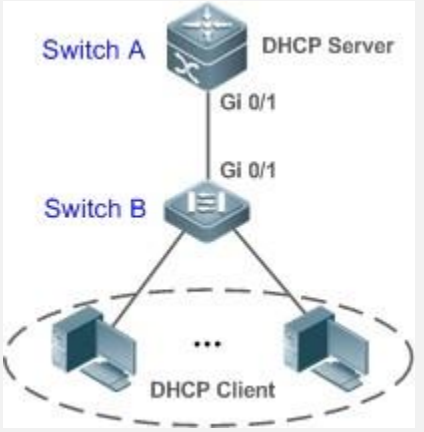
❖ Enabling DHCP Snooping to Process Relay Requests

Command	[no] ip dhcp snooping check-giaddr
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet. After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

❖ Enabling DHCP Snooping Loose Forwarding

Command	ip dhcp snooping loose-forward
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this feature is enabled, when the capacity of DHCP Snooping binding entries is reached, DHCP packets of new users are forwarded and obtain addresses, but DHCP Snooping does not record binding entries of new users.

❖ Enabling DHCP Snooping Monitoring

Command	▪ [no] ip dhcp snooping monitor
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, DHCP Snooping generates binding entries according to the interaction process by copying DHCP packets. It, however, does not check the validity of packets.
Scenario Figure 14-5	
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

Configuration Example

❖ DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

Common Errors

- The uplink port is not configured as a DHCP trusted port.
- Another access security option is already configured for the uplink port, so that a DHCP trusted port cannot be configured.

14.4.2 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	**string** *ASCII-string*: Indicates the content of the extensible format, the Option82 option **remote-id**, is a
Description	user-defined character string ▪ hostname: Indicates the content of the extensible format, the Option82 option 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

	according to Option82 information.

Configuration Example

❖ Configuring Option82 to DHCP Request Packets

Configuration Steps	▪ **Configuring basic functions of DHCP Snooping.** ▪ **Configuring Option82.**
B	`QTECH# configure terminal` `QTECH(config)# ip dhcp snooping information option QTECH(config)# end`
Verification	Check the DHCP Snooping configuration.
B	`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`

Common Errors

▪ N/A

14.5 Monitoring

Clearing

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

Description	Command
Clears dynamic user inforamtion of DHCP Snooping 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**
Enables debugging MAC-based DHCP Snooping.	**debug snooping ipv4 mac-address** *H.H.H*
Disables debugging MAC-based DHCP Snooping.	**no debug snooping ipv4 mac-address** *H.H.H*
Enables debugging all DHCP Snooping	**debug snooping ipv4 all**
Disables debugging all DHCP Snooping	**no debug snooping ipv4 all**

15.1 Overview

DHCPv6 Snooping: Dynamic Host Configuration Protocol version 6 (DHCPv6) snooping enables recording and monitoring of IPv6 address usage by snooping DHCPv6 packets exchanged between the client and the server, and filters illegal DHCPv6 packets, including request packets from the client and response packets from the server. The user data entries generated by DHCPv6 snooping recording can serve security applications such as IPv6 Source Guard.

Protocols and Standards

- RFC3315 Dynamic Host Configuration Protocol For IPv6
- RFC5007 DHCPv6 Leasequery
- RFC5460 DHCPv6 Bulk Leasequery

15.2 Applications

Application	Description
Prevention of DHCPv6 Spoofing	There is more than one DHCPv6 server on the network, and DHCPv6 clients can obtain network configuration parameters only from legal DHCPv6 servers.
Prevention of Forged DHCPv6 Packet Attacks	Malicious users on the network frequently send DHCPv6 request packets.
Prevention of Forged DHCPv6 Packet Attacks	Malicious users on the network send forged DHCPv6 request packets such as DHCPv6 release packets.
Prevention of IPv6/MAC Spoofing	Malicious users on the network send forged IPv6 request packets that temper the source address fields.
Prevention of Unauthorized IPv6 Configuration	Users do not obtain IPv6 addresses from the DHCPv6 server as required and configure IPv6 addresses without authorization.

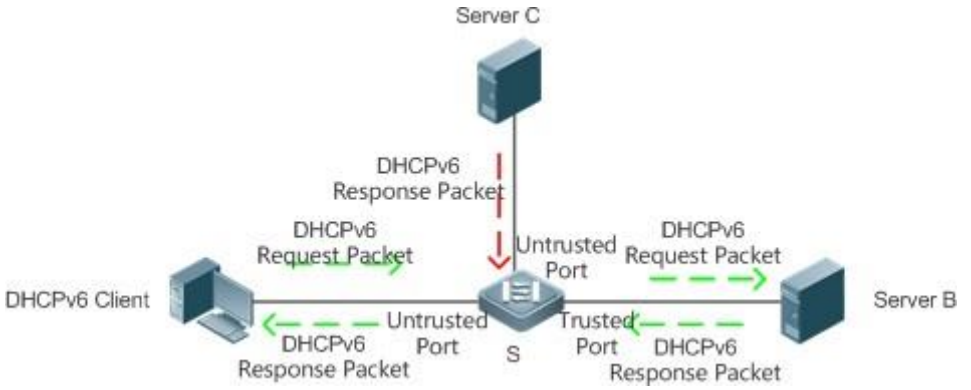
15.2.1 Prevention of DHCPv6 Spoofing

Scenario

There may exist more than one DHCPv6 server on the network, and it is necessary to ensure that user PCs obtain network configuration parameters only from the controlled DHCPv6 servers.

As shown in the following figure, the DHCPv6 client only communicates with trusted DHCPv6 servers.

- The request packets from the DHCPv6 client are transmitted only to a trusted DHCPv6 server.
- Only the response packets from the trusted DHCPv6 server can be transmitted to the client.



Remarks	**S is an access device. A is a user PC.** **B is a controlled DHCPv6 server.** **C is an uncontrolled DHCPv6 server**

Deployment

- Enable DHCPv6 snooping on the access device S for DHCPv6 packet monitoring.
- Set the port connecting the access device S to the DHCPv6 server B as a DHCPv6 trusted port to forward response packets.
- Set the other ports of the access device S as DHCPv6 untrusted ports to filter response packets.

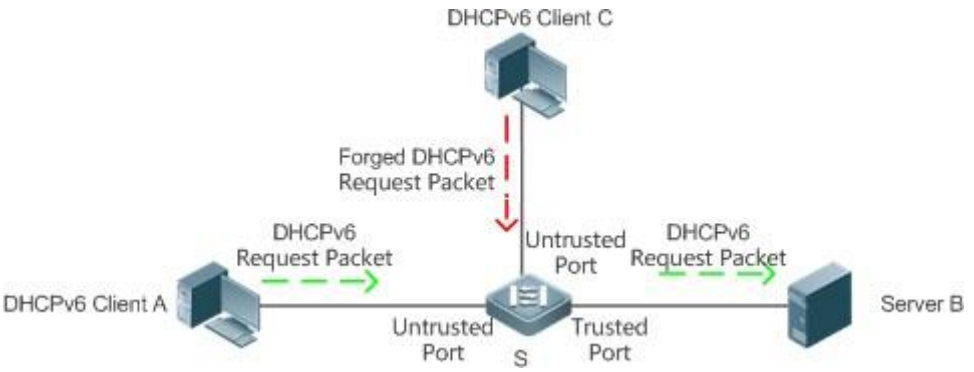
15.2.2 Prevention of Forged DHCPv6 Packet Attacks

Scenario

There may exist malicious users on the network who forge DHCPv6 request packets. The packets not only consume available IPv6 addresses of the server but may also snatch IPv6 addresses from legal users. Therefore, such packets on the network must be filtered.

As shown in the following figure, the DHCPv6 request packets sent by the DHCPv6 client will be checked.

- Release packets and decline packets from the client must match those recorded in the internal snooping database.



Remarks	**S is an access device. A and C are user PCs.** **B is a controlled DHCPv6 server.**

Deployment

- Enable DHCPv6 snooping on the access device S for DHCPv6 monitoring.
- Set the port connecting the access device S to the DHCPv6 server as a DHCPv6 trusted port to forward response packets.
- Set the other ports of the access device S as DHCPv6 untrusted ports to filter DHCPv6 packets.

15.2.3 Prevention of IPv6/MAC Spoofing

Scenario

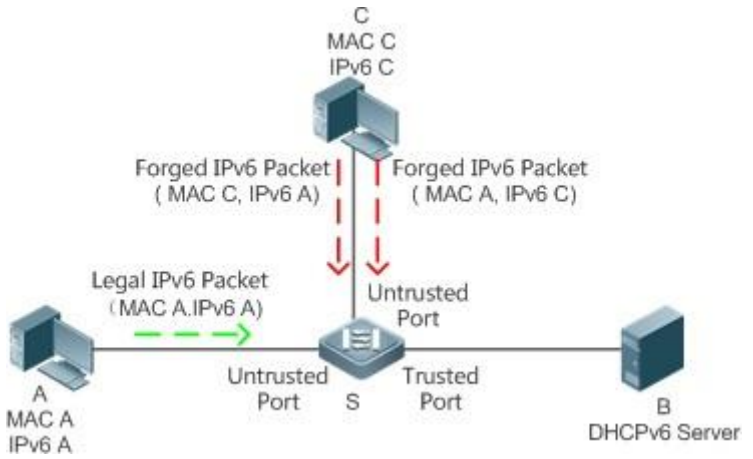
When checking IPv6 packets from the untrusted port, you may check IP address fields only or IP+MAC fields to filter forged IPv6 packets.

As shown in the following figure, IPv6 packets sent from the DHCPv6 client will be

checked.

- The source address fields of IPv6 packets must match IPv6 addresses assigned by the DHCPv6 client.
- The source Media Access Control (MAC) addresses of Layer-2 packets must match the client MAC addresses in DHCPv6 request packets of the client.

Figure 15-3



Remarks	S is an access device. A and C are user PCs. B is a controlled DHCPv6 server.

Deployment

- Enable DHCPv6 snooping on the access device S for DHCPv6 monitoring.
- Set all downstream ports on the access device S as DHCPv6 untrusted ports.
- Enable IPv6 Source Guard on the access device S to filter IPv6 packets.
- On the access device S, set the match mode of IPv6 Source Guard as IPv6+MAC to check both MAC fields and IPv6 fields of IPv6 packets.

15.2.4 Prevention of Unauthorized IPv6 Configuration

Scenario

When checking IPv6 packets from untrusted ports, you need to check whether source IPv6 addresses of the packets are consistent with the IPv6 addresses assigned by the DHCPv6.

If the source IPv6 addresses, connection ports, or Layer-2 MAC addresses of IPv6 packets fail to match the assignment records of the DHCPv6 server snooped

by the device, the packets should be discarded.

The operating process of the device in the scenario is the same as that in the preceding figure.

Deployment

- See section 15.2.3 "Prevention of IPv6/MAC Spoofing".

15.3 Features

Basic Concepts

❖ **DHCPv6 Request Packet**

A DHCPv6 request packet is the packet sent from the DHCPv6 client to the DHCPv6 server. It includes DHCPv6 solicit packet, DHCPv6 request packet, DHCPv6 confirm packet, DHCPv6 rebind packet, DHCPv6 release packet, DHCPv6 decline packet, DHCPv6 renew packet, DHCPv6 inform-req packet, and DHCPv6 leasequery packet.

❖ **DHCPv6 Response Packet**

A DHCPv6 response packet is the packet sent from the DHCPv6 server to the DHCPv6 client. It includes DHCPv6 advertise packet, DHCPv6 reply packet, DHCPv6 reconfigure packet, DHCPv6 relay-reply packet, DHCPv6 leasequery-reply packet, DHCPv6 leasequery-done packet, and DHCPv6 leasequery-data packet.

❖ **DHCPv6 Snooping Trusted Port**

As the interactive packets used by DHCPv6 to obtain IPv6 addresses or prefixes are multicast packets, there may exist illegal DHCPv6 services affecting IPv6 acquisition, and user information may even be stolen by such illegal services. To prevent such issues, DHCPv6 snooping classifies ports into trusted and untrusted ports, and the devices forwards only the DHCPv6 response packets received by the trusted port and discards all DHCPv6 response packets from the untrusted port. By setting the ports connected to a legal DHCPv6 server as trusted ports and the others as untrusted ports, illegal DHCPv6 servers will be shielded.

On a switch, all switch ports or Layer-2 aggregate ports (APs) are untrusted ports by default, which can be configured as trusted ports. In fat AP configuration mode, all the layer-2 switching ports and layer-2 encapsulation sub-interfaces are untrusted by default, and can be specified as trusted. In fit AP configuration mode, all the layer-2 switching ports are untrusted by default and can be specified as trusted, and all the layer-2 encapsulation sub-interfaces are trusted and cannot be specified as untrusted. All switching ports and layer-2 aggregate ports are untrusted ports by default and can be specified as trusted.

❖ **Filtering DHCPv6 Snooping Request Packets**

When DHCPv6 packets are disabled for an individual user, any DHCPv6 packets sent from the user's device shall be shielded. DHCPv6 request packet filtering can be configured on an untrusted port to filter all DHCPv6 request packets received by the port.

- **VLAN-based DHCPv6 Snooping**

DHCPv6 snooping takes effect in the unit of VLAN. If DHCPv6 snooping is enabled by default, the function is enabled on all VLANs of the device. The VLAN on which DHCPv6 snooping takes effect can be flexibly controlled through configuration.

- **DHCPv6 Snooping User Database**

On a DHCPv6 network, a frequently encountered problem is that users may arbitrarily set static IPv6 addresses. Such addresses are difficult to maintain and may conflict with legal user addresses, making the users unable to access the Internet. By snooping the packets exchanged between the client and the server, DHCPv6 snooping forms IPv6 information obtained by users, user MAC, VID, PORT, and lease time into a user record, thus making a DHCPv6 snooping user database to control legal use of IPv6 addresses.

- **DHCPv6 Option 18 and Option 37**

When managing user IP addresses, some network administrators expect to determine the IP addresses to be assigned according to the user locations; that is, they expect to assign IP addresses to users according to the information on the connected network devices, thereby adding user-related device information to DHCP request packets through DHCPv6 option while performing DHCPv6 snooping. The option number for RFC3315 is 18; the option number for RFC4649, the option number used is 37. After the content of Option 18 and Option 37 is parsed on the DHCPv6 server, the server can obtain information of more users according to the content uploaded by Option 18 and option 37 so as to assign IP addresses more accurately.

- Option 18: Interface ID

The default content of Interface ID include the number of the VLAN to which the port receiving request packets from the DHCPv6 client belongs, and the port index (the values of the port index are the slot number and port number); the extension content is a customized character string. Default and extension fillings take effect only for wired interfaces, including switch ports, Layer-2 APs, or Layer-2 encapsulation sub-interfaces.

The Interface ID filling format can be classified into standard and extension formats, only one of which can be used on the same network. When the standard filling format is used, only default content can be filled in for sub-options of Interface ID, as shown in the following figure:

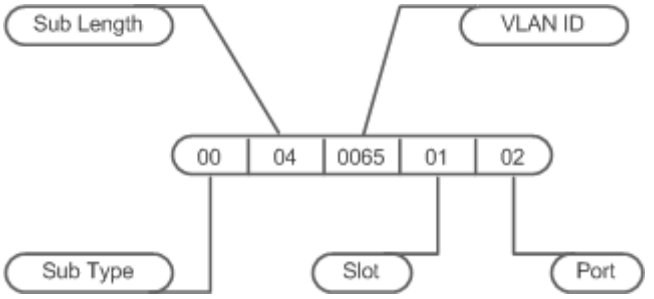
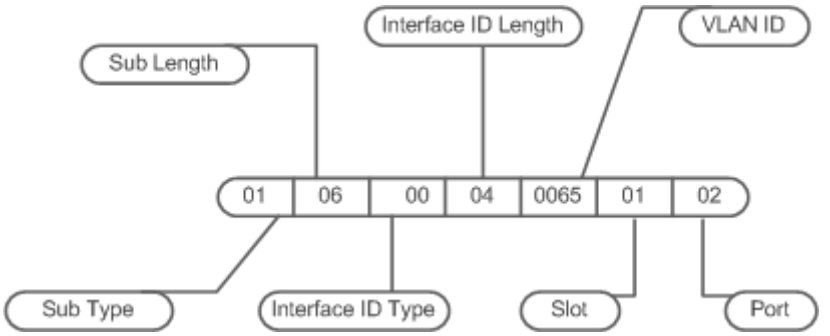


Figure 15-4

To use customized content, the extension filling format can be used. The content filled in by extension can be default or extension content. To distinguish between the content, add a content type field and a content length field of one byte respectively following the sub-option length. For default content, set the content type as 0; for extension content, set the content type as 1.

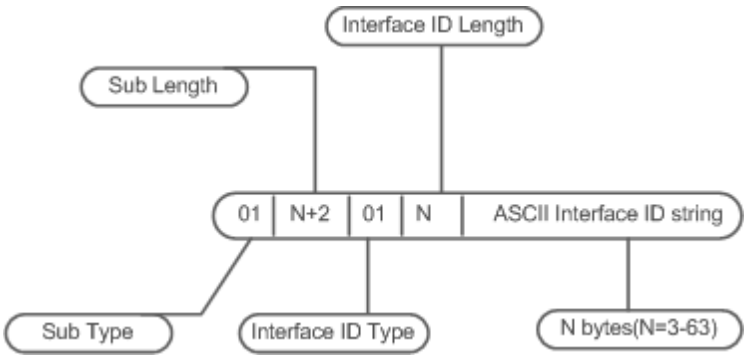
The format of default content is as follows:

Figure 15-5



The format of extension content is as follows:

Figure 15-6



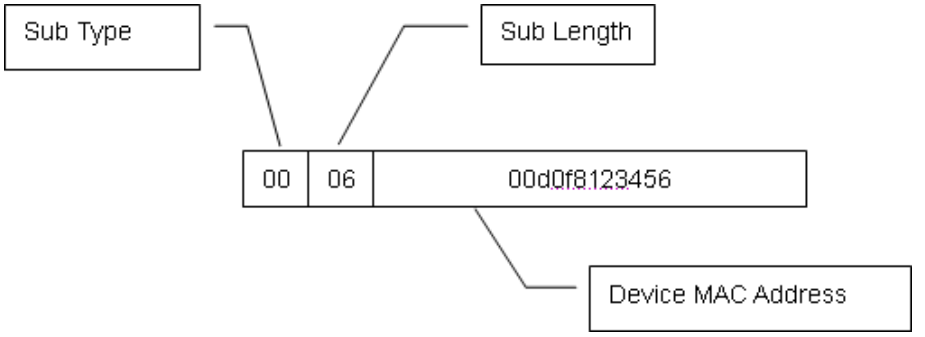
- Option 37: Remote ID

The default content of Remote ID is the bridge MAC address of the DHCPv6 relay that receives request packets from the DHCPv6 client, and the extension content is a customized character string.

The Remote ID filling format can be classified into standard and extension

formats, only one of which can be used on the same network. When the standard filling format is used, only default content are filled in for sub-options of Remote ID, as shown in the following figure:

Figure 15-7

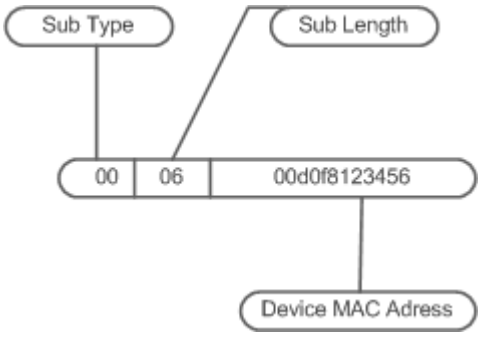


To use customized content, the extension filling format can be used. The content filled in by extension can be default or extension content. To distinguish between the content, add a content type field and a content length field of one byte

respectively following the sub-option length. For default content, set the content type as 0; for extension content, set the content type as 1.

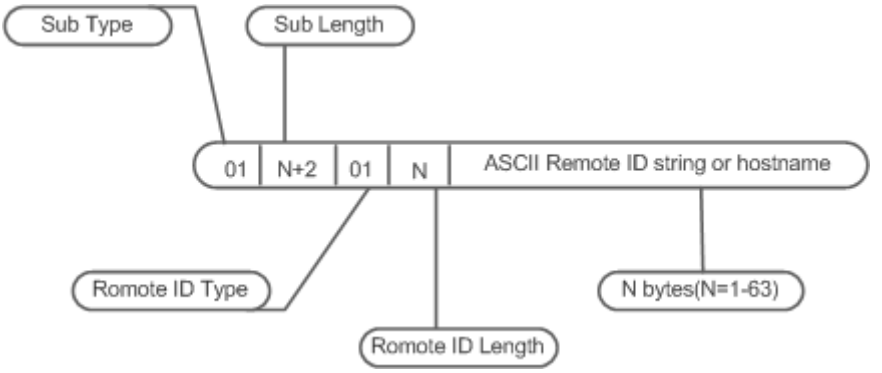
The format of default content is as follows:

Figure 15-8



The format of extension content is as follows:

Figure 15-9



- Note

Option 18: The values of port index for Interface ID are the slot number and port number. The port can be a wired switch port, Layer-2 AP, or Layer-2 encapsulation sub-interface. The port number refers to the sequence number of the port in the slot. The port number of a Layer-2 AP is an AP number. For example, the port number of Fa0/10 is 10, the port number of AP 11 is 11;

Slot numbers are the sequence numbers of all slots on a device (one device in stack mode). The slot number of an AP is the last one. The sequence numbers of slots start from 0. Run the **show slots** command to display the numbers. For example:

Example 1:

```
QTECH#show slots (only Dev and slot displayed)

 Dev Slot

  1   0 ----------------> The slot number is 0.
1   1    ------> The slot number is 1.
 1   2  > The slot number is 2.
```

In this case, the slot number of an AP is 3.

Example 2:

```
QTECH #show slots (only Dev and slot displayed)
Dev Slot
  1   0 ----------------> The slot number is 0.

  1   1    ------> The slot number is 1.

  1   2    ------> The slot number is 2.
```

In this case, the slot number of an AP is 6.

❖ Illegal DHCPv6 Packet

DHCPv6 snooping checks the validity of DHCPv6 packets passing through the device, discards illegal DHCPv6 packets, records user information, and generates a DHCPv6 snooping binding database for query of other functions. The following packets are considered as illegal DHCPv6 packets.

- DHCPv6 response packets received by untrusted ports. For details, see the section DHCPv6 Response Packet.
- Relayed DHCPv6 packets received by untrusted ports, namely DHCPv6 relay-forw packets and DHCPv6 relay-reply packets.
- DHCPv6 relay-reply packets received by trusted ports. The egress for these packets is an untrusted ports according to the entry.
- DHCPv6 release packets; no corresponding users are found in the DHCPv6

snooping user database according to the Layer-2 source MAC and VID of these packets.

- DHCPv6 release packets. The IPv6 addresses or prefixes of these packets do not exist in the DHCPv6 snooping user database.
- DHCPv6 release packets. The IPv6 addresses or prefixes of these packets all exist in the DHCPv6 snooping user database but the untrusted ports of DHCPv6 release packets are inconsistent with those untrusted ports in the DHCPv6 snooping user database.
- DHCPv6 packets in incorrect formats or incomplete packets.

Overview

Features	Description
Filtering Illegal DHCPv6 Packets	Checks the validity of exchanged DHCPv6 packets, and discards illegal packets (see the preceding section for instructions for illegal packets). Forwards only legal response packets to trusted ports.
Establishing a User Database	Snoops interaction between the client and the server, and generates the DHCPv6 snooping user database to provide a basis for other security filtering modules.

15.3.1 Filtering Illegal DHCPv6 Packets

This function is to check the validity of DHCPv6 packets from untrusted ports, filter the packets according to the types of illegal packets described in Basic Concepts above, and control the transmission scope of packets to prevent malicious users from spoofing.

Working Principle

During snooping, the receipt ports of packets and packet fields are checked to filter the packets; the destination ports of packets are modified to control the transmission scope of packets.

❖ **Checking Ports**

When receiving DHCPv6 packets, the device first determines whether the port receiving packets is a DHCPv6 trusted port. If the port is a trusted port, the packets will be forwarded without validity check, binding, or prefix record generation. If the port is an untrusted port, validity check is required.

❖ **Checking whether Packet Encapsulation and Length are Complete**

Check whether the packets are User Datagram Protocol (UDP) packets and the destination port is 546 or 547. Check whether the actual length of a packet matches the length field described in the protocol.

❖ **Checking Whether DHCPv6 Packet Field and Packet Type are Correct**

Check whether the packets are relayed according to the types of illegal packets described in the preceding section Basic Concepts, and then check whether the restrictions specific to a type of packets are met according to the actual type of packets.

Related Configuration

❖ **Enabling Global DHCPv6 Snooping**

By default, DHCPv6 snooping is disabled.

Run the [**no**] **ipv6 dhcp snooping** command to enable or disable DHCPv6 snooping.

To enable or disable DHCPv6 snooping on different VLANs, global DHCPv6 snooping must be enabled first.

❖ **Setting DHCPv6 Snooping on a VLAN**

By default, when global DHCPv6 snooping is enabled, DHCPv6 snooping takes effect on all VLANs.

Run the [**no**] **ipv6 dhcp snooping vlan** command to enable or disable DHCPv6 snooping on a VLAN. The range of command parameter values is the actual range of VLAN numbers.

15.3.2 Establishing a User Database

The packets exchanged between the DHCPv6 client and the DHCPv6 server are snooped, and DHCPv6 snooping binding entries and prefix entries are generated according to the information on legal DHCPv6 packets. All the entries are provided for other security configuration modules as an information list of legal users and a basis for network packet filtering.

Working Principle

During snooping, binding database and prefix database are continuously updated according to the types of DHCPv6 packets.

❖ **Generating Binding or Prefix Records**

When DHCPv6 reply packets are snooped on a trusted port, client IPv6 addresses or prefixes, client MAC addresses, and lease time fields of the packets are extracted, and a binding or prefix record is generated according to the client port ID recorded by the device (wired interface index), and the client VLAN.

❖ **Deleting Binding or Prefix Records**

When the recorded lease time is over, or the legal DHCPv6 release/DHCPv6 decline packets sent from the client are snooped, or users run the clear command to delete binding or prefix records, the corresponding binding or prefix records are deleted.

Related Configuration

Enable DHCPv6 snooping without extra configuration.

15.4 Configuration

Configuration	Description and Command	
Configuring Basic DHCPv6 Snooping Functions	(Mandatory) It is used to establish DHCPv6 snooping.	
	ipv6 dhcp snooping	Enables DHCPv6 snooping.
	ipv6 dhcp snooping binding-delay	Delays assignment of the DHCPv6 snooping binding entries to the hardware filtering entries.
	ipv6 dhcp snooping filter-dhcp-pkt	Enables DHCPv6 request packet filtering.
	ipv6 dhcp snooping vlan	Enables and disables DHCPv6 snooping for specified VLANs.
	ipv6 dhcp snooping database write-delay	Enables the function for regularly saving DHCPv6 snooping binding and prefix records.
	ipv6 dhcp snooping database write-to-flash	Manually saves DHCPv6 snooping binding and prefix records.
	renew ipv6 dhcp snooping database	Manually imports the user records saved in flash to the DHCPv6 snooping user database.
	ipv6 dhcp snooping trust	Configures DHCPv6 snooping trusted ports.
	ipv6 dhcp snooping link-detection	Clears dynamical biding entries on a port when the port is configured into Link Down state.
	(Optional) It is used to optimize assignment of DHCPv6 server addresses.	

Configuring Option 18 and Option 37	ipv6 dhcp snooping Information option [standard-format]	Adds Option 18 or Option 37 to DHCPv6 request packets. **standard-format**: Fills in content in a standard format if such keyword exists; otherwise, fills in content in an extension format.
	ipv6 dhcp snooping information option format remote-id [**string** *ASCII-string* | **hostname**]	Configures Remote ID in an extension format. **string**: Indicates that the content filled in is a customized character string. **hostname**: Indicates that the content filled in is hostname.
	ipv6 dhcp snooping vlan *vlan-id* **information option** *ASCII-string*	Configures the customized character string of Interface ID in an extension format.
	ipv6 dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*	Configures VLAN mapping for Interface ID in an extension format, which is exclusive from the [**no**] **ipv6 dhcp snooping vlan** *vlan-id* **information option format-type** *interface-id* **string** *ASCII-string* command.

15.4.1 Configuring Basic DHCPv6 Snooping Functions

Configuration Effect

- Enable DHCPv6 snooping.
- Generate DHCPv6 snooping binding and prefix databases.
- Control the transmission scope of DHCPv6 packets.
- Filter illegal DHCPv6 packets.

Notes

- The port connecting the device to a trusted DHCPv6 server must be set as a trusted port.
- The port on which DHCPv6 snooping takes effect can be a wired switch port, Layer-2 AP or Layer-2 encapsulation sub-interface. Configuration on a port can be classified into configuration in interface mode and configuration in wireless security mode.
- The Link Down entry clearing function applies only to wired ports.

Configuration Steps

- **Enabling Global DHCPv6 Snooping**
  - Mandatory.
  - If not specified, configure this function on an access device.
- **Delaying Assignment of DHCPv6 Snooping Binding Entries to Hardware Filtering Entries**
  - Configure the function if assignment needs to be delayed. Assignment is not delayed by default.
  - If not specified, configure this function on an access device.
- **Enabling DHCPv6 Request Packet Filtering**
  - Enable the function if users' DHCPv6 requests need to be restricted on a port.
  - If not specified, disable the function on the access device.
- **Enabling and Disabling VLAN-based DHCPv6 Snooping**
  - Disable DHCPv6 snooping if the function is not needed on a VLAN.
  - If not specified, configure this function on an access device.
- **Enabling Regular Saving of DHCPv6 Snooping Binding Records**
  - This function should be enabled if DHCPv6 snooping binding records need to be maintained after the device is restarted.
  - If not specified, enable the function on the access device.
- **Configuring DHCPv6 Trusted Ports**
  - Mandatory.
  - Set the port connecting the device to a trusted DHCPv6 device as a DHCPv6 trusted port.
- **Enabling and Disabling Clearing of Dynamically Bound Entries When the Port is Configured into Link Down State**
  - On a stable network, enable the function to release spaces occupied by hardware entries and timely clear the entries on the Link Down port.
  - If not specified, disable the function on the access device.

Verification

Enable the device to use DHCPv6 to obtain network configuration parameters.

- Check whether user records are generated in the DHCPv6 snooping binding

database.

Related Commands

- **Enabling and Disabling DHCPv6 Snooping**

Command	[no] ipv6 dhcp snooping
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After global DHCPv6 snooping is enabled, run the **show ipv6 dhcp snooping** command to check whether DHCPv6 snooping is enabled.

- Delaying Assignment of the DHCPv6 Snooping Binding Entries to the Hardware Filtering Entries

Command	[no] ipv6 dhcp snooping binding-delay
Parameter Description	***seconds***: Indicates the time for delaying assignment of binding entries to hardware filtering entries, in the unit of seconds. The value is 0 by default.
Command Mode	Global configuration mode
Usage Guide	By default, dynamically bound entries are added to hardware filtering entries in real time. After the function is configured, the dynamically generated binding entries are bound to hardware filtering entries only when no IPv6 address conflicts are detected within a specified time period.

- Configuring a VLAN on Which DHCPv6 Snooping Takes Effect

Command	[no] ipv6 dhcp snooping vlan { *vlan-rng* | {*vlan-min* [*vlan-max*] } }
Parameter Description	*vlan-rng*: Indicates the VLAN scope in which DHCPv6 snooping takes effect. *vlan-min*: Indicates the lower VLAN limit where DHCPv6 snooping takes effect. *vlan-max*: Indicates the upper VLAN limit where DHCPv6 snooping takes effect.

Command Mode	Global configuration mode
Usage Guide	DHCPv6 snooping is enabled or disabled on a specified VLAN by configuring the command. This function takes effect only if global DHCPv6 snooping is enabled.

❖ Filtering DHCPv6 Request Packets on a Port

Command	▪ **[no] ipv6 dhcp snooping filter-dhcp-pkt**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	All DHCPv6 request packets can be prohibited on the port by configuring the command; that is, all users are prohibited from applying for addresses on the port.

❖ Regularly Writing DHCPv6 Snooping Database Information into Flash

Command	**[no] ipv6 dhcp snooping database write-delay [*time*]**
Parameter Description	*time*: Indicates the interval for regularly writing the DHCPv6 snooping database into flash.
Command Mode	Global configuration mode
Usage Guide	The DHCPv6 snooping database can be written into a flash file by configuring the command. The function prevents user information loss after the device restarts. If user information is lost, users have to re-obtain IP addresses for normal communication.

❖ Manually Writing DHCPv6 Snooping Database Information into Flash

Command	**ipv6 dhcp snooping database write-to-flash**
Parameter Description	N/A

Command Mode	Global configuration mode
Usage Guide	Dynamic user information in the DHCPv6 snooping database can be written into a flash file in real time by running the command.

❖ Manually Importing Information in Flash to the DHCPv6 Snooping Binding Database

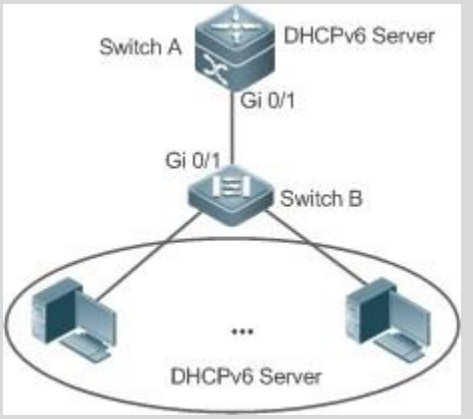
Command	**renew ipv6 dhcp snooping database**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Flash file information can be written into the DHCPv6 snooping database in real time by running the command.

❖ Configuring a Port as a Trusted Port

Command	▪ **[no] ipv6 dhcp snooping trust**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The port connecting to a legal DHCPv6 server is configured as a trusted port by configuring the command. The DHCPv6 response packets received by a trusted port are forwarded, while the DHCPv6 response packets received by an untrusted port are discarded.

Configuration Example

❖ Dynamically obtaining IPv6 addresses through the legal DHCPv6 server on a DHCPv6 client

Scenario Figure 15-10	
Configuration Steps	▪ Enable DHCPv6 snooping on the access device (Switch B). ▪ Set the uplink port (Gi 0/1) as a trusted port.
B	B#configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)#ipv6 dhcp snooping B(config)#interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ipv6 dhcp snooping trust B(config-if-GigabitEthernet 0/1)#end
Verification	QTECH#show ipv6 dhcp snooping DHCPv6 snooping status : ENABLE DHCPv6 snooping database write-delay time : 0 seconds DHCPv6 snooping binding-delay time : 0 seconds DHCPv6 snooping option18/37 status : DISABLE DHCPv6 snooping link detection : DISABLE Interface Trusted Filter DHCPv6 GigabitEthernet 0/1 YES DISABLE QTECH#show ipv6 dhcp snooping binding Total number of bindings: 1 NO. MacAddress IPv6 Address Lease(sec) VLAN Interface 1 00d0.f801.0101 2001::10 42368 2 GigabitEthernet 0/1

Common Errors

- The uplink port is not set as a DHCPv6 trusted port.
- Other access security options are configured on the uplink port, resulting in failure of DHCPv6 trusted port configuration.

15.4.2 Configuring Option 18 and Option 37

Configuration Effect

- The DHCPv6 server can obtain more information during address assignment, thus improving address assignment.
- The option is transparent to the DHCPv6 client, and such function is perception-free to the client.

Configuration Steps

- Run the configuration if the optimization is needed.
- If not specified, enable the function on the device where DHCPv6 snooping is enabled.

Verification

Check the configuration of DHCPv6 snooping to ensure that such function is enabled.

Related Commands

❖ **Adding Option18 and Option 37 to DHCPv6 Request Packets**

Command	▪ **[no] ipv6 dhcp snooping information option [standard-format]**
Parameter Description	**standard-format**: Fills in content in a standard format if such keyword exists; otherwise, fills in content in an extension format.
Command Mode	Global configuration mode
Usage Guide	Information on Option 18 and Option 37 is added to DHCPv6 request packets by configuring the command, and the DHCPv6 server assigns addresses according to information on Option 18 and Option 37.

❖ Setting Option 37 (Remote ID) as a Customized Character String

Command	**[no] ipv6 dhcp snooping information option format remote-id { string *ASCII-string* | hostname }**
Parameter Description	**string** *ASCII-string*: Indicates that the content of Remote ID in an extension format is a customized character string. **hostname**: Indicates that the content of Remote ID in an extension format is hostname.

Command Mode	Global configuration mode
Usage Guide	Remote ID is configured in an extension format by configuring the command. Remote ID is customized, and the DHCPv6 server assigns addresses according to information on Option 37.

❖ Setting Option 18 (Interface ID) as a Customized Character String

Command	**[no] ipv6 dhcp snooping vlan *vlan-id* information option format-type *interface-id* string *ASCII-string***
Parameter Description	*vlan-id*: Indicates the VLAN to which DHCPv6 request packets belong. *ASCII-string*: Indicates the user-customized content to be filled in for Interface-ID.
Command Mode	Interface configuration mode
Usage Guide	Customized character strings of Interface ID are configured in an extension format by configuring the command, and the DHCPv6 server assigns addresses according to information on Option 18.

❖ Setting Option 18 (Interface ID) as a Modified VLAN

Command	**[no] ipv6 dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id***
Parameter Description	*vlan-id* (the first one): Indicates the VLAN to which DHCPv6 request packets belong. *vlan-id* (the second one): Indicates the VLAN after modification.
Command Mode	Interface configuration mode
Usage Guide	Interface ID is configured as VLAN mapping in an extension format by configuring the command, and the DHCPv6 server assigns addresses according to information on Option 18.

Configuration Example

❖ The following example shows how to add Option 18 and Option 37 to DHCPv6 request packets.

Configuration Steps	▪ **Configure basic DHCPv6 snooping functions.(Omitted)** ▪ **Enable the function for adding Option 18 and Option 37.**
B	`QTECH# configure terminal` `QTECH(config)# ipv6 dhcp snooping information option QTECH(config)# end`
Verification	Display the DHCPv6 snooping configuration.

B	`QTECH #show ipv6 dhcp snooping`
	
	`DHCPv6 snooping status :ENABLE`
	`DHCPv6 snooping database write-delay time : 0 seconds DHCPv6 snooping binding-delay time : 0 seconds DHCPv6 snooping option 18/37 status : ENABLE`
	`DHCPv6 snooping link detection : DISABLE Interface Trusted Filter DHCPv6`
	`FastEthernet0/10 YES DISABLE`

15.5 Monitoring and Maintenance

Clearing

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

Description	Command
Clears dynamic user information in the DHCPv6 snooping database.	**clear ipv6 dhcp snooping binding**[**vlan** *vlan-id*| *ipv6* **interface** [*mac interface-id*]
Clears all entries in the DHCPv6 snooping prefix database.	**clear ipv6 dhcp snooping prefix**
Clears statistics about DHCPv6 snooping handling DHCPv6 packets.	**clear ipv6 dhcp snooping statistics**

Displaying

Description	Command
Displays DHCPv6 snooping configuration.	**show ipv6 dhcp snooping**
Displays the VLANs on which DHCPv6 snooping fails to take effect.	**show ipv6 dhcp snooping vlan**
Displays all dynamically bound entries in the DHCPv6 snooping binding database.	show ipv6 dhcp snooping binding
Displays all entries in the DHCPv6 snooping prefix database.	**show ipv6 dhcp snooping prefix**
Displays the counters of DHCPv6 snooping handling packets.	**show ipv6 dhcp snooping statistics**
Displays all statically bound entries added manually and all dynamically bound entries in the DHCPv6 snooping binding database.	**show ipv6 source binding**

Debugging

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

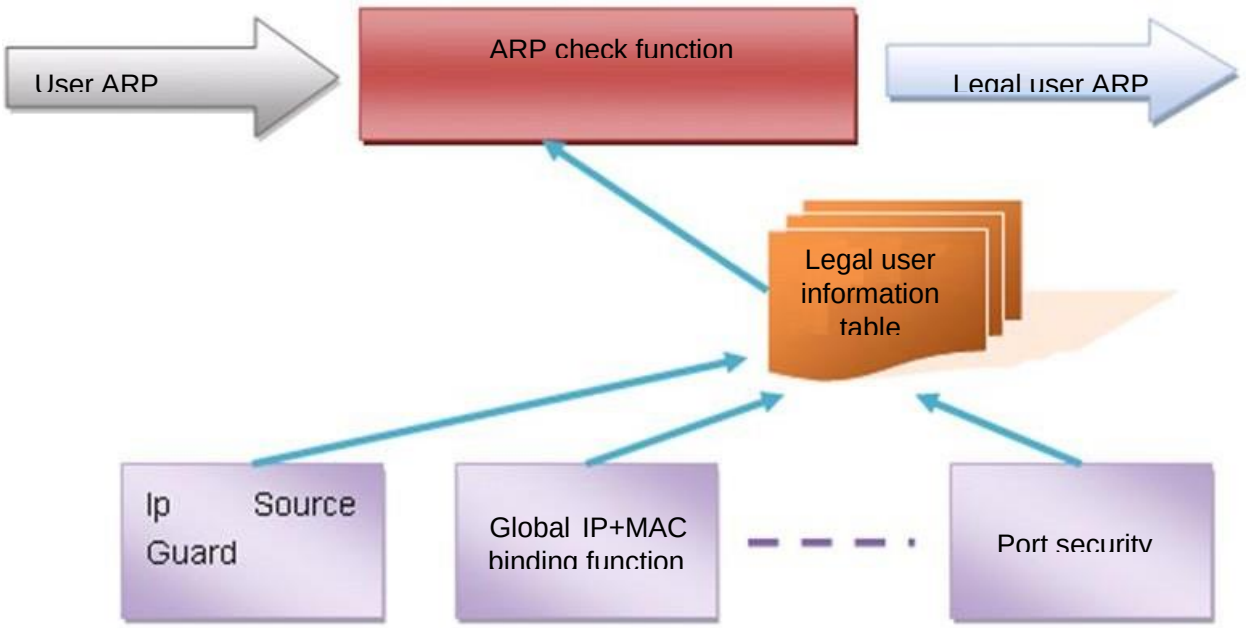
Description	Command
Debugs DHCPv6 snooping events.	**debug snooping ipv6 event**
Disables debugging of DHCPv6 snooping events.	**no debug snooping ipv6 event**
Debugs DHCPv6 snooping packets.	**debug snooping ipv6 packet**

Disables debugging of DHCPv6 snooping packets.	**no debug snooping ipv6 packet**

16.1 Overview

The Address Resolution Protocol (ARP) packet check filters all ARP packets under ports (including wired layer-2 switching ports, layer-2 aggregate ports (APs), and layer-2 encapsulation sub-interfaces) and discards illegal ARP packets, so as to effectively prevent ARP deception via networks and to promote network stability. On devices supporting ARP check, illegal ARP packets in networks will be ignored according to the legal user information (IP-based or IP-MAC based) generated by security application modules such as IP Source Guard, global IP+MAC binding, 802.1X authentication, GSN binding, Web authentication and port security.

Figure 16-1



The above figure shows that security modules generate legal user information (IP-based or IP-MAC based). ARP Check uses the information to detect whether the Sender IP fields or the <Sender IP, Sender MAC>fields in all ARP packets at ports matches those in the list of legal user information. If not, all unlisted ARP packets will be discarded.

Protocols and Standards

- RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

16.2 Applications

Application	Description
Filtering ARP packets in Networks	Illegal users in networks launch attacks using forged ARP packets.

16.2.1 Filtering ARP Packets in Networks

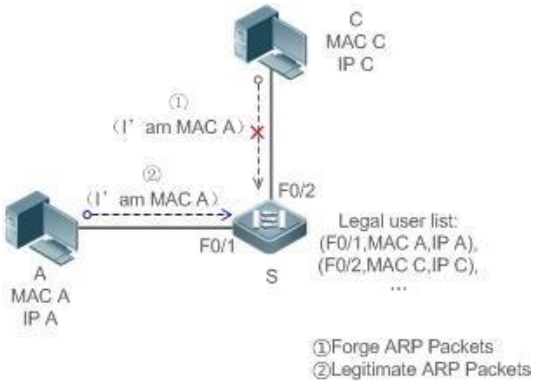
Scenario

Check ARP packets from distrusted ports and filter out ARP packets with addresses not matching the results assigned by the DHCP server.

For example, in the following figure, the ARP packets sent by DHCP clients are checked.

- The ports receiving ARP packets, the source MAC addresses of ARP packets, and the source IP addresses of ARP packets shall be consistent with the snooped DHCP-assigned records.

Figure 16-2



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.

16.3 Features

Basic Concepts

❖ Compatible Security Modules

Presently, the ARP Check supports the following security modules.

- IP-based: IP-based mode: port security, and static configuration of IP Source Guard.
- IP-MAC based: IP-MAC based mode: port security, global IP+MAC binding, 802.1X authorization, IP Source Guard, GSN binding, and Web authentication.

❖ Two Modes of APR Check

The ARP Check has two modes: Enabled and Disabled. The default is Enabled.

1. Enabled Mode

Through ARP Check, ARP packets are detected based on the IP/IP-MAC based binding information provided by the following modules.

- Global IP-MAC binding
- 802.1X authorization
- IP Source Guard
- GSN binding
- Port security
- Web authentication
- Port security IP+MAC binding or IP binding

When only ARP Check is enabled on a port but the above-mentioned modules are not enabled, legal user information cannot be generated, and thereby all ARP packets from this port will be discarded.

When the ARP Check and VRRP functions are enabled on an interface, if the physical IP address and virtual IP address of the interface can be used as the gateway address, the physical IP address and VRRP IP address need to be permitted to pass. Otherwise, ARP packets sent to the gateway will be filtered out.

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.

16.3.1 Filtering ARP Packets

Enable ARP Check on specified ports to realize filtration of illegal ARP packets.

Working Principle

A device matches the source IP and source MAC addresses of the ARP packets received at its ports with the legal user information of the device. With successful matching, packets will be transferred, or otherwise they will be discarded.

Related Configuration

- **Enabling ARP Check on Ports**

By default, the ARP Check is disabled on ports.

Use the **arp-check** command to enable ARP Check.

Unless otherwise noted, this function is usually configured on the ports of access devices.

16.4 Configuration

Configuration	Description and Command	
Configuring ARP Check	(Mandatory) It is used to enable APR Check.	
	arp-check	Enables ARP Check.

16.4.1 Configuring ARP Check

Configuration Effect

- Illegal ARP packets are filtered out.

Notes

- When ARP Check is enabled, the number of policies or users of related security applications may decrease.
- ARP Check cannot be configured on mirrored destination ports.
- ARP Check cannot be configured on the trusted ports of DHCP Snooping.
- ARP Check cannot be configured on global IP+MAC exclude ports.
- ARP Check can be enabled only on wired switching ports, layer-2 APs, layer-2 encapsulation sub-interfaces. Enable ARP check for the wired in interface configuration mode

Configuration Steps

❖ **Enabling ARP Check**

- (Mandatory) The function is disabled by default. To use the ARP Check function, an administrator needs to run a command to enable it.

Verification

- Use the **show run** command to display the system configuration.
- Use the **show interfaces** { *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
Usage Guide	Generate ARP filtration information according to the legal user information of security application modules to filter out illegal ARP packets in networks.

Configuration Example

The following configuration example introduces only ARP Check related configurations

❖ Enabling ARP Check on ports

Configuration Steps	**Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard, port security, or global IP+MAC binding.**

	QTECH# configure terminal QTECH(config)#address-bind 192.168.1.3 00D0.F800.0003 QTECH(config)#address-bind install QTECH(config)#ip source binding 00D0.F800.0002 vlan 1 192.168.1.4 interface gigabitEthernet 0/1 QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#arp-check QTECH(config-if-GigabitEthernet 0/1)#ip verify source port-security QTECH(config-if-GigabitEthernet 0/1)#switchport port-security QTECH(config-if-GigabitEthernet 0/1)#switchport port-security binding 00D0.F800.0001 vlan 1 192.168.1.1 QTECH(config-if-GigabitEthernet 0/1)#exit QTECH(config)#interface gigabitEthernet 0/4 QTECH(config-if-GigabitEthernet 0/4)#switchport port-security QTECH(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5 QTECH(config-if-GigabitEthernet 0/4)#arp-check QTECH(config-if-GigabitEthernet 0/4)#exit QTECH(config)#interface gigabitEthernet 0/5 QTECH(config-if-GigabitEthernet 0/5)#arp-check QTECH(config-if-GigabitEthernet 0/5)#end QTECH# configure terminal QTECH#conf
Verification	Use the show interfaces arp-check list command to display the effective ARP Check list for interfaces.
	QTECH# show interface arp-check list INTERFACE SENDER MAC SENDER IP POLICY SOURCE snooping GigabitEthernet 0/4 00d0.f800.0003 192.168.1.3 address-bind GigabitEthernet 0/4 192.168.1.5 port-security GigabitEthernet 0/5 00d0.f800.0003 192.168.1.3 address-bind

Common Errors

- If ARP packets at a port need to be checked but APR-Check is disabled, then APR-Check will not be effective.

16.5 Monitoring

Displaying

Description	Command
Displays the effective ARP Check list based on ports.	**show interfaces** [*interface-type interface-number*] **arp-checklist**

17.1. Overview

Dynamic Address Resolution Protocol (ARP) inspection (DAI) checks the validity of received ARP packets. Invalid ARP packets will be discarded.

DAI ensures that only valid ARP packets can be forwarded by devices. DAI mainly performs the following steps:

- Intercepts all ARP request packets and ARP reply packets on untrusted ports in the virtual local area networks (VLANs) where the DAI function is enabled.
- Checks the validity of intercepted ARP packets according to user records stored in a security database.
- Discards the ARP packets that do not pass the validity check.
- Sends the ARP packets that pass the validity check to the destination.
- The DAI validity criteria are the same as those of ARP Check. For details, see the *Configuring ARP Check*.

DAI and ARP Check have same functions. The only difference is that DAI takes effect by VLAN whereas ARP Check takes effect by port.

Protocols and Standards

- RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

17.2 Applications

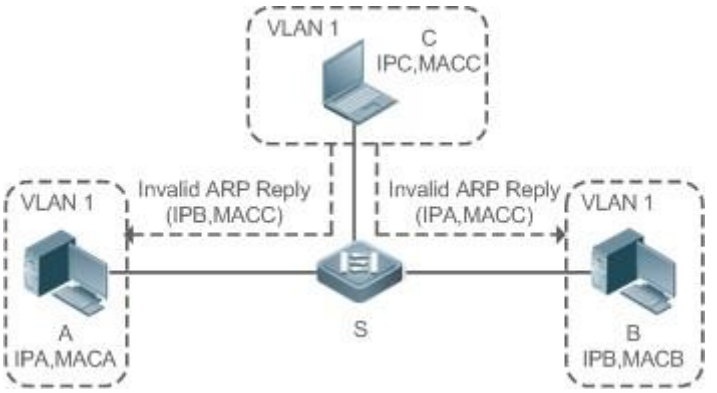
Application	Description
ARP Spoofing Prevention	Prevent ARP spoofing that is mounted by taking advantage of ARP defects.

17.2.1 ARP Spoofing Prevention

Scenario

Due to inherent defects, ARP does not check the validity of received ARP packets. Attackers can take advantage of the defects to mount ARP spoofing. A typical example is man-in-the-middle (MITM) attack. See Figure 17-1.

Figure 17-1



Remarks	**Device S is a QTECH 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 reply. Upon receiving the ARP reply packet, User A updates its ARP cache with IP B and MAC B.

In this model, User C can make the ARP entry mapping between User A and User B incorrect by continuously broadcasting ARP reply packets to the network. The reply packets contain IP A, IP B, and MAC C, After receiving these reply packets, User A stores the ARP entry (IP B, MAC C), and User B stores the ARP entry (IP A, MAC C). As a result, the communication between User A and User B is directed to User C, without the knowledge of User A and User B. Here User C acts as the man in the middle by modifying received packets and forwarding them to User A or User B.

If Device S is enabled with DAI, it will filter out forged ARP packets to prevent ARP spoofing as long as the IP addresses of User A and User B meet the validity criteria described in section 17.1 Overview. Figure 17-2 shows the working process of DAI.

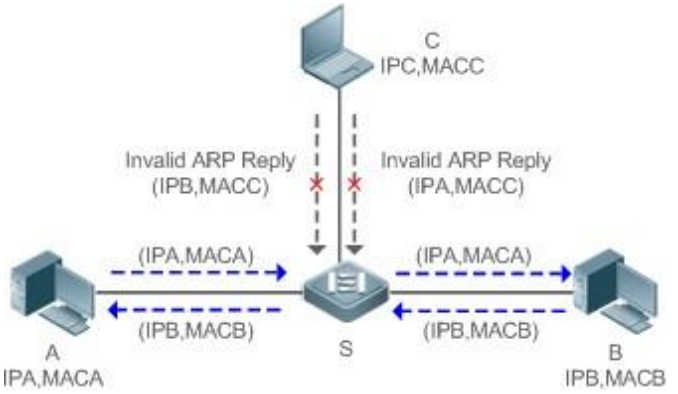


Figure 17-2

Remarks	**Device S is a QTECH 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 User C are discarded because the packets do not match the records in the security database of Device S.

Deployment

- Enable DHCP Snooping on Device S.
- Enable DAI and IP Source Guard on Device S.

17.3 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 through without checking their validity.

17.3.1 Invalid ARP Packet Filter

Enable DAI in a specific VLAN to filter out invalid ARP packets. The DAI validity criteria are the same as those of ARP Check.

Working Principle

Upon receiving an ARP packet, the device matches the IP address and MAC address of the packet with the valid user records in its security database. If the packet matches a record, it will be forwarded normally. If it does not match any record, it will be discarded.

DAI and ARP Check use the same set of valid user records. For details, see the packet validity check description in the *Configuring ARP Check*.

Related Configuration

- **Enabling DAI in a VLAN**

By default, DAI is disabled in VLANs.

Run the **ip arp inspection vlan** *vlan-id* command to enable DAI in a specific VLAN.

After DAI is enabled in a VLAN, DAI may not take effect on all ports in the VLAN. A DHCP Snooping trusted port does not perform DAI check.

- **Disabling DAI in a VLAN**

By default, DAI is disabled in VLANs.

After DAI is enabled in a VLAN, you can run the **no ip arp inspection vlan** *vlan-id* command to disable DAI.

Disabling DAI in a VLAN does not mean disabling packet validity check on all ports in the VLAN. The ports with ARP Check effective still check the validity of received ARP packets.

17.3.2 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.

17.4 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.

17.4.1 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 QTECH access devices unless otherwise specified.

❖ **Configuring DAI Trusted Ports**

- Optional.
- It is recommended to configure uplink ports as DAI trusted ports after DAI is enabled. Otherwise, the uplink ports enabled with other security features and set to trusted state accordingly may filter out valid ARP packets due to the absence of DAI user entries.
- Perform this configuration on QTECH 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

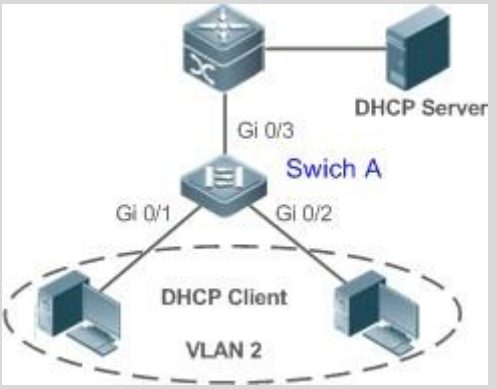
❖ Configuring DAI Trusted Ports

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 17-3	
Configuration Steps	Enable DHCP Snooping on the access switch (Switch A) and configure its uplink port (GigabitEthernet 0/3) connected to the valid DHCP server as a trusted port. 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.

17.5 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**

18.1. Overview

The IP Source Guard function realizes hardware-based IP packet filtering to ensure that only the users having their information in the binding database can access networks normally, preventing users from forging IP packets.

18.2 Applications

Application	Description
Guarding Against IP/MAC Spoofing Attack	In network environments, users set illegal IP addresses and malicious users launch attacks through forging IP packets.

18.2.1 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.

Remarks	**S is a network access server (NAS). A and C are user PCs.** **B is a DHCP server within the control area.**

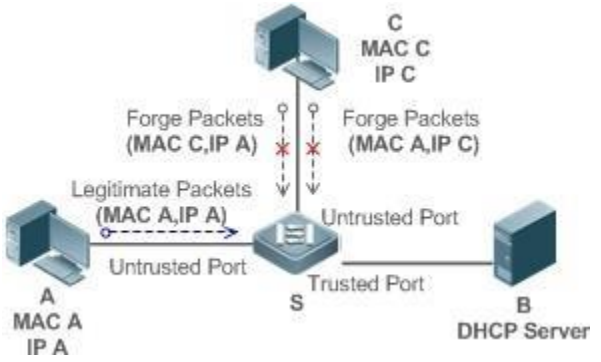


Figure 18-1

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.

18.3 Features

Basic Concepts

❖ **Source IP Address**

Indicate the source IP address field of an IP packet.

❖ **Source MAC Address**

Indicate the source MAC address field of an IP packet.

❖ **IP-based Filtering**

Indicate a policy of IP packet filtering, where only the source IP addresses of all IP packets (except DHCP packets) passing through a port are checked. It is the default filtering policy of IP Source Guard.

❖ **IP-MAC based Filtering**

A policy of IP packet filtering, where both the source IP addresses and source MAC addresses of all IP packets are checked, and only those user packets with these IP addresses and MAC addresses existing in the binding database are permitted.

❖ **Address Binding Database**

As the basis of security control of the IP Source Guard function, the data in the

address binding database comes from two ways: the DHCP Snooping binding database and static configuration. When IP Source Guard is enabled, the data of the DHCP Snooping binding database is synchronized to the address binding database of IP Source Guard, so that IP packets can be filtered strictly through IP Source Guard on a device with DHCP Snooping enabled.

- **Excluded VLAN**

By default, when IP Source Guard is enabled on a port, it is effective to all the VLANs under the port. Users may specify excluded VLANs, within which IP packets are not checked and filtered, which means that such IP packets are not controlled by IP Source Guard. At most 32 excluded VLANs can be specified for a port.

Overview

Feature	Description
Checking Source Address Fields of Packets	Filter the IP packets passing through ports by IP-based or IP-MAC based filtering.

18.3.1. Checking Source Address Fields of Packets

Filter the IP packets passing through ports based on source IP addresses or on both source IP addresses and source MAC addresses to prevent malicious attack by forging packets. When there is no need to check and filter IP packets within a VLAN, an excluded VLAN can be specified to release such packets.

Working Principle

When IP Source Guard is enabled, the source addresses of packets passing through a port will be checked. The port can be a wired switching port, a layer-2 aggregate port (AP), or a layer-2 encapsulation sub-interface. Such packets will pass the port only when the source address fields of the packets match the set of the address binding records generated by DHCP Snooping, or the static configuration set by the administrator. There are two matching modes as below.

- **IP-based Filtering**

Packets are allowed to pass a port only if the source IP address fields of them belong to the address binding database.

- **IP-MAC Based Filtering**

Packets are allowed to pass a port only when both the layer-2 source MAC addresses and layer-3 source IP addresses of them match an entry in the address binding database.

- **Specifying Excluded VLAN**

Packets within such a VLAN are allowed to pass a port without check or filtering.

Related Configuration

- **Enabling IP Source Guard on a Port**

By default, the IP Source Guard is disabled on ports.

It can be enabled using the **ip verify source** command.

Usually IP Source Guard needs to work with DHCP Snooping. Therefore, DHCP Snooping should also be enabled.

DHCP Snooping can be enabled at any time on QTECH devices, either before or after IP Source Guard is enabled.

- **Configuring a Static Binding**

By default, legal users passing IP Source Guard check are all from the binding database of DHCP Snooping. Bound users can be added using the **ip source binding** command.

- **Specifying an Excluded VLAN**

By default, IP Source Guard is effective to all the VLANs under a port.

Excluded VLANs may be specified which are exempted from IP Source Guard using the **ip verify source exclude-vlan**

command.

Excluded VLANs can be specified only after IP Source Guard is enabled on a port. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on a port.

The above-mentioned port can be a wired switching port, a layer-2 AP port or a layer-2 encapsulation sub-interface..

18.4 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.

18.4.1 Configuring IP Source Guard

Configuration Effect

- Check the source IP addresses of input IP packets.

Notes

- When IP Source Guard is enabled, IP packets forwarding may be affected. In general case, IP Source Guard is enabled together with DHCP Snooping.
- IP Source Guard cannot be configured on the trusted ports controlled by DHCP Snooping.
- IP Source Guard cannot be configured on the global IP+MAC exclusive ports.
- IP Source Guard can be configured and enabled only on wired switch ports, Layer-2 AP ports, Layer-2 encapsulation sub-ports. In a wired access scenario, it is supposed to be configured in the interface configuration mode.

Configuration Steps

- Enable DHCP Snooping.
- Enable IP Source Guard.

Verification

Use the monitoring commands to display the address binding database of IP Source Guard.

Related Commands

❖ **Enabling IP Source Guard on a Port**

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. It indicates the outer VLAN ID of a QINQ-termination user. **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.**
	`QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ip verify source` `QTECH(config-if-GigabitEthernet 0/1)# end`
Verification	Displays the address filtering table of IP Source Guard.
	`QTECH# show ip verify source`

❖ Configuring a Static Binding

Configuration Steps	▪ **Enable DHCP Snooping.** ▪ **Enable IP Source Guard.** ▪ **Configure a static binding.**
	QTECH# configure terminal QTECH(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface GigabitEthernet 0/3 QTECH(config)# end
Verification	Displays the address filtering table of IP Source Guard.
	QTECH# show ip verify source NO. INTERFACE FilterType FilterStatus IPADDRESS MACADDRESS VLAN TYPE 1 GigabitEthernet 0/3 UNSET Inactive-restrict-off 192.168.4.243 00d0.f801.0101 1 Static 2 GigabitEthernet 0/1 IP-ONLY Active Deny-All

❖ Specifying an Excluded VLAN

Configuration Steps	▪ **Enable DHCP Snooping.** ▪ **Enable IP Source Guard.**
	QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ip verify source QTECH(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1 QTECH(config-if)# end
Verification	Display the configuration of excluded VLANs specified on a port.
	QTECH# 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.

18.5 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**

19.1. Overview

IPv6 Source Guard binding allows IPv6 packets to be filtered by hardware so as to ensure that only the users having corresponding information in the IPv6 packet hardware filtering database can access the Internet, thus preventing users from configuring IP addresses without authorization or fabricating IPv6 packets.

19.2 Applications

Application	Description
Prevention of IPv6/MAC Spoofing	There are malicious users on a network who fabricate IPv6 packets to launch an attack.

19.2.1 Prevention of IPv6/MAC Spoofing

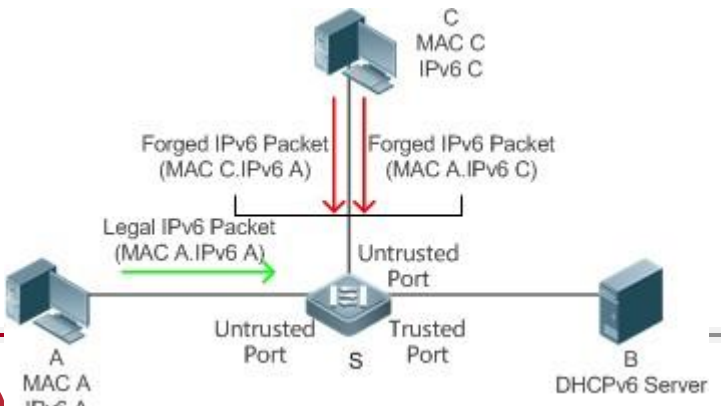
Scenario

When checking the IPv6 packets from the untrusted DHCPv6 ports, you may check IPv6 fields only or IPv6+MAC fields, thereby filtering fabricated IPv6 packets.

As shown in the following figure, IPv6 packets sent from the Dynamic Host Configuration Protocol version 6 (DHCPv6) client will be checked.

- The source address fields of IPv6 packets must match IPv6 addresses assigned by the DHCPv6 client.
- The source media access control (MAC) addresses of Layer-2 packets must match those assigned by DHCPv6 Snooping to hardware filtering records.

Figure 20-1



Remarks	**S is an access device. A and C are user PCs.** **B is a controlled DHCPv6 server.**

Deployment

- Enable DHCPv6 Snooping on the access device S for DHCPv6 monitoring.
- Set all the downstream interfaces on the access device S as untrusted DHCPv6 ports.
- On the access device S, enable IPv6 Source Guard for IPv6 packet filtering.
- On the access device S, set the match mode of IPv6 Source Guard as IPv6+MAC for checking MAC fields and IPv6 fields of IPv6 packets.

19.3 Features

Basic Concepts

❖ **Source IPv6**

Indicates the source IPv6 address fields of IPv6 packets

❖ **Source MAC**

Indicates the source MAC address fields of Layer-2 packets

❖ **Source IPv6-based Filtering**

The source IPv6-based filtering policy checks only the source IPv6 addresses of all IPv6 packets (except DHCP packets) passing through the interface. The source IPv6-based filtering policy is the default filtering policy of IPv6 Source Guard.

❖ **Source IPv6+Source MAC-based Filtering**

The source IPv6-based filtering policy checks the source IPv6+source MAC of all IPv6 packets, and only the user packets saved in the database for binding user records are allowed to pass through.

❖ **Database for Binding User Records**

The database for binding user records is the basis for IPv6 Source Guard security control. Currently, the data in the database binding user records come from the following two sources. One is the DHCPv6 Snooping binding database. After IPv6 Source Guard is enabled, the information in the DHCPv6 Snooping binding database is synchronized to the user binding database of IPv6 Source Guard so that IPv6 Source Guard can filter the IPv6 packets of the client on the device where DHCPv6 Snooping is enabled. The other is users' static configuration.

Overview

Feature	Description
Checking the Source Address Fields of	Filters the IPv6 packets passing through the interface based on source IPv6 or source IPv6+source MAC.

19.3.1 Checking the Source Address Fields of Packets

Filter the IPv6 packets transiting the port based on source IPv6 or source IPv6+source MAC, thereby preventing malicious users from fabricating packets to launch an attack.

Working Principle

After IPv6 Source Guard is enabled, the device checks the source addresses of the packets passing through the port. The port can be a wired switch port, Layer-2 aggregate port (AP) or Layer-2 encapsulation sub interface. Only the packets whose source address fields match the user binding record set generated by DHCPv6 Snooping or the user set statically configured by the administrator can pass through the port. There are two matching methods:

- **Source IPv6 Address-based Filtering**

If IPv6 fields of a packet belong to the identity association in the user binding records, the packet is allowed to pass through the port.

- **IPv6+MAC Address-based Filtering**

Only when Layer-2 MAC and Layer-3 IPv6 of a packet completely match a certain record in the set of authenticated users can the packet pass through the port.

Related Configuration

- **Enabling IPv6 Source Guard on a Port**

By default, IPv6 Source Guard is disabled on a port.

IPv6 Source Guard of the port can be enabled or disabled by running the **ipv6 verify source** command.

Typically, DHCPv6 Snooping is used together with IPv6 Source Guard , so DHCPv6 Snooping needs to be enabled. Timing for enabling DHCPv6 Snooping is not limited on QTECH devices. You can enable DHCPv6 Snooping before or after IPv6 Source Guard is enabled.

- **Configuring Static IPv6 Source Guard Users**

By default, all sets of authenticated users checked by IPv6 Source Guard are from the bound users of DHCPv6 Snooping. Run the **ipv6 source binding** command to add extra user binding records.

19.4 Configuration

Configuration	Description and Command	
Configuring IPv6 Source Guard	(Mandatory) It is used to enable IPv6 Source Guard.	
	ipv6 verify source	Enables IPv6 Source Guard on a port.
	ipv6 source binding	Configure statically bound users.

19.4.1 Configuring IPv6 Source Guard

Configuration Effect

- Check the source IPv6 fields entered into IPv6 packets.

Notes

- IPv6 Source Guard is based on DHCPv6 Snooping; that is to say, interface-based IPv6 Source Guard takes effect only on the untrusted ports controlled by DHCPv6 Snooping. If configured on trusted ports or the interfaces on VLANs not controlled by DHCPv6 Snooping, the function will not take effect.

Configuration Steps

- Enable DHCPv6 Snooping.
- Enable IPv6 Source Guard.

Verification

Use the monitoring command provided by the device to view the user filtering entries of IPv6 Source Guard.

Related Commands

❖ **Enabling IPv6 Source Guard on a Port**

Command	**ipv6 verify source [port-security]**
Parameter Description	**port-security**: Configures IPv6 Source Guard to perform IPv6+MAC-based detection.
Command Mode	Interface mode

Usage Guide	By enabling IPv6 Source Guard on a port through this command, you can detect users based on IPv6 or IPv6+MAC.

❖ Adding Information on Static Users to Ipv6 Source Address Binding Database

Command	**ipv6 source binding *mac-address* vlan *vlan-id ipv6-address* { interface *interface-id* | ip-mac | ip-only }**
Parameter Description	***mac-address***: Indicates the MAC address of a statically added user. ***vlan-id***: Indicates the VLAN ID of a statically added user. ***ipv6-address***: Indicates the IPv6 addresses of a statically added user. ***interface-id***: Indicates the wired access interface for a statically added user. **wlan-id**: Indicates the wireless access WLAN for a statically added user. **ip-mac**: Indicates that the global binding mode is IPv6+MAC binding mode. ▪ ip-only: Indicates that the global binding mode is IPv6 binding mode only.
Command Mode	Global configuration mode
Usage Guide	By running this command, some users can pass the check of IPv6 Source Guard without being controlled by DHCPv6.

Configuration Example

❖ Enabling IPv6 Source Guard on a Port

Configuration Steps	▪ **Enable DHCPv6 Snooping.**
	`QTECH(config)# ipv6 access-list v6-list QTECH(config-ipv6-nacl)# permit ipv6 fe80::/10 any QTECH(config-ipv6-nacl)# permit ipv6 ::/128 any QTECH(config-ipv6-nacl)# exit`
	`QTECH(config)# security global access-group v6-list`
	▪ **Enable IPv6 Source Guard.**
	`QTECH(config)# interface GigabitEthernet 0/1`
	`QTECH(config-if-GigabitEthernet 0/1)# ipv6 verify source QTECH(config-if-GigabitEthernet 0/1)# end`

Verification	View the user filtering entries of IPv6 Source Guard.
	`QTECH# show ipv6 source binding`

❖ Adding a Statically Bound User

Configuration Steps	▪ **Enable DHCPv6 Snooping.(Omitted)** ▪ **Enable IPv6 Source Guard.(Omitted)** ▪ **Add a static user.**
	QTECH# configure terminal QTECH(config)# ipv6 source binding 0001.0002.0006 vlan 1 2008::1 ip-mac QTECH(config)# end
Verification	View the user filtering entries of IPv6 Source Guard.
	QTECH# show ipv6 source binding Total number of bindings: 7 NO. Filter Type Filter Status IPv6 Address MACAddress VLAN Type Interface 1 IPv6+MAC Inactive-system-error 2000::127 0001.0002.0003 1 Static Global 2 IPv6-ONLY Active 2008::4 0001.0002.0004 1 DHCPv6-Snooping GigabitEthernet 0/5 3 IPv6-ONLY Active 2008::7 0001.0002.0007 1 Static Global 4 IPv6+MAC Active 2008::1 0001.0002.0006 1 Static Global 5 UNSET Inactive-restrict-off 2008::9 0001.0002.0009 1 DHCPv6-Snooping GigabitEthernet 0/1 6 IPv6-ONLY Active Deny-All GigabitEthernet 0/5

Common Errors

- IPv6 Source Guard is enabled on the trusted DHCPv6 Snooping port.

19.5 Monitoring

Displaying

Description	Command
Displays information on the IPv6	**show ipv6 source binding**

source address binding database.	

20. CONFIGURING GATEWAY-TARGETED ARP SPOOFING PREVENTION

20.1. Overview

Gateway-targeted Address Resolution Protocol (ARP) spoofing prevention effectively prevents gateway-targeted ARP 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

20.2 Applications

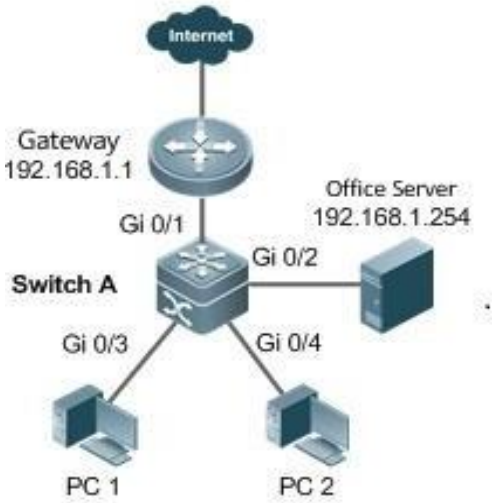
Application	Description
Typical Application of Prevention	Blocks ARP spoofing packets with forged gateway address and intranet server IP addresses to ensure that users can access the Internet.

20.2.1 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 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 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 20-1 Typical Topology of Gateway-targeted ARP Spoofing Prevention



Deployment

- 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 intranet server address.

20.3 Features

Basic Concepts

❖ ARP

ARP is a TCP/IP protocol that obtains physical addresses according to IP addresses. Its function is as follows: The host broadcasts ARP requests to all hosts on the network and receives the returned packets to determine physical 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 requests. On 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 hosts receive the response packets and record them in the local ARP cache without detecting their authenticity. In this way, 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 communications are 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.

20.3.1 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 wrong ARP 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.

20.4 Configuration

Configuration	Description and Command
Configuring	Optional.

Gateway-targeted Spoofing Prevention	**anti-arp-spoofing ip**	Configures gateway-targeted ARP spoofing prevention on the logical port and specifies the gateway IP address.

20.4.1 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 spoofing prevention.

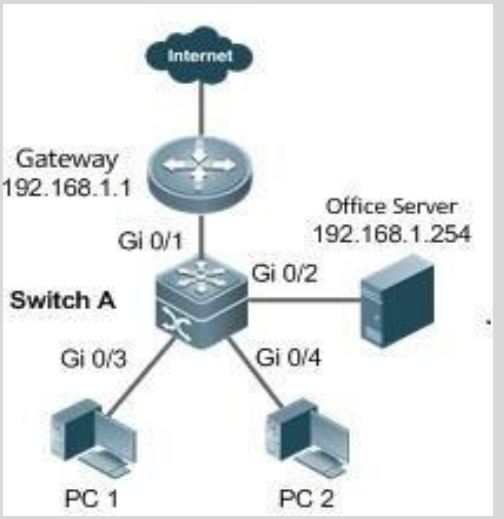
Related Commands

- **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/Wireless Security Configuration Mode
Usage Guide	Supported only on Layer-2 ports. Supported on AC/AP only in wireless security configuration mode.

Configuration Example

- Configuring Gateway-targeted Spoofing Prevention

Scenario Figure 20-2	
	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 0/3-4 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 spoofing prevention.

	`SwitchA#show anti-arp-spoofing`
	
	`NO PORT IP STATUS`
	
	`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

20.5 Monitoring

Displaying

Description	Command
Displays all data on gateway-targeted ARP spoofing prevention.	**show anti-arp-spoofing**

21.1. 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.

21.2 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.

21.2.1 Attack Rate Limiting

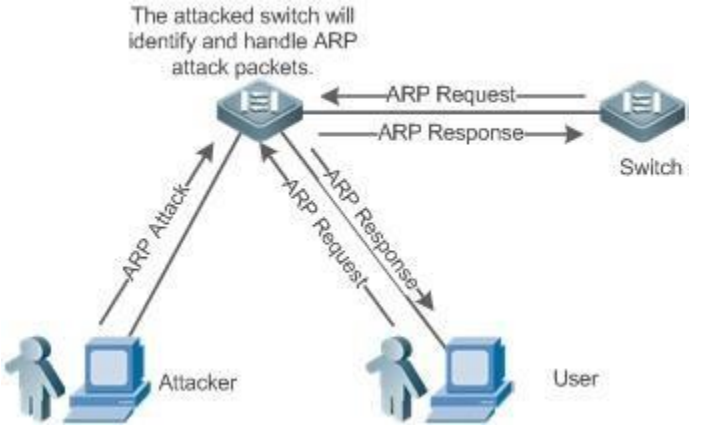
Scenario

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 describe the 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 22-1, normal hosts will fail to access the network, and the switch will fail to send ARP replies to other devices.

Figure 22-1



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 in CPP based on the application environment or use the configurations recommended by the system. You can run the **show cpu-protect summary** command to display the configurations.

21.3 Features

Basic Concepts

❖ **ARP Guard**

In local area networks (LANs), IP addresses are mapped to MAC addresses

through ARP, which has a significant role in 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 start from scanning active hosts in the network. Therefore, many scanning packets rapidly occupy the network bandwidth, causing network communication failure.

To solve this problem, QTECH 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 consumes 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 mainly designed for consuming the CPU load. For a Layer-3 device, if the destination IP address exists, packets are directly forwarded by the switching chip without occupying CPU resources. If the destination IP address does not exist, IP packets are sent to the 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 switch or router returns an ICMP echo reply. The preceding process requires the CPU to process the packets, thereby definitely consuming part of CPU resources. If an attacker sends a large number of ICMP echo requests to the destination device, 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 DHCP requests. Various attack tools on the Internet can easily complete this type of attack. A network attacker can send sufficient DHCP 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 send a large number of DHCPv6 requests to use up the address space provided by the DHCPv6 server within a period. In this case, 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 and isolate 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 IPv6 hosts in the 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 exchange packets through different protocols. These packets must be sent to the CPU and processed by appropriate protocols. Once the network 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 to work properly.

Since various protocols are being continuously developed, protocols in use vary with the user environments. QTECH devices hereby provide self-defined guard. Users can customize and flexibly configure guard types to meet 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.

21.3.1. 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 period 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 address continuously changes.

Among IP packets beyond the scanning threshold received in the configured period, if the source IP address remains the 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 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 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.

21.3.2. 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.

21.3.3. Monitoring Period

Working Principle

The monitoring user provides information about attackers in the current system. If the isolation period is 0 (that is, not 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.

During software monitoring, if the isolation period is set to a non-zero value, the guard module automatically isolates the attacker 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.

21.3.4. Isolation Period

Working Principle

Isolation is performed by the guard policies after attacks are detected. Isolation is implemented using the filter of the 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 guard supports port-based hardware isolation.

A policy is configured in the hardware to isolate attackers. However, hardware

resources are limited. When hardware 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 period. If it is set to **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

21.3.5 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.

21.4 Configuration

Configuration	Description and Command	
Configuring ARP Guard	**arp-guard enable**	Enables ARP guard globally.
	arp-guard isolate-period	Configures the global ARP-guard isolation 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 monitoring 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 ARP-guard attack threshold.
	arp-guard scan-threshold	Configures the global ARP-guard scanning 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-guard monitoring 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-guard scanning threshold.
	ip-guard trusted-host	Configures IP-guard trusted hosts.
	nfpp ip-guard enable	Enables IP guard on an interface.
	nfpp ip-guard policy	Configures the IP-guard rate limit and attack 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-guard isolation period.
	icmp-guard monitor-period	Configures the global ICMP-guard monitoring period.
	icmp-guard monitored-host-limit	Configuresthe 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 ICMP-guard attack 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.
	dhcp-guard enable	Enables DHCP guard globally.
	dhcp-guard isolate-period	Configures the global DHCP-guard isolation period.
	dhcp-guard monitor-period	Configures the global DHCP-guard monitoring

Configuring DHCP Guard		period.
	dhcp-guard monitored-host-limit	Configuresthe maximum number of DHCP-guard monitored hosts.
	dhcp-guard rate-limit	Configures the global DHCP-guard rate limit.
	dhcp-guard attack-threshold	Configures the global DHCP-guard attack 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.
	dhcpv6-guard monitor-period	Configures the global DHCPv6-guard monitoring period.
	dhcpv6-guard monitored-host-limit	Configuresthe 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-guard attack threshold.
	nfpp dhcpv6-guard enable	EnablesDHCPv6 guard on an interface.
	nfpp dhcpv6-guard policy	Configures the DHCPv6-guard rate limit and

		attack threshold on an interface.
	nfpp dhcpv6-guard isolate-period	Configures the DHCPv6-guard isolation period 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 global ND-guard attack 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 and attack threshold of a self-defined guard.
	isolate-period	Configures the global isolation period of a self-defined guard.
	monitor-period	Configures the global monitoring period of a 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 self-defined 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.

21.4.1 Configuring ARP Guard

Configuration Effect

- ARP attacks are identified based on hosts or ports. Host-based ARP attack identification supports two modes: 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. If the ARP 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 system also isolates the attack source.
- ARP guard can also detect ARP scanning attacks. ARP scanning attacks indicate that the link-layer source MAC 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 possibly 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 attack packets are 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, preventing false positive of ARP traffic over the trusted ports. For details about DAI trusted ports, see the Configuring Dynamic ARP 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 isolated entries on 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 packets while not 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 period, and the configured 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 increases, 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 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 "% 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 threshold is smaller than rate limit 300pps." to

notify the administrator.

- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ARP_GUARD-4-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 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 address continuously 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 configured in NFPP configuration mode.

❖ Configuring the ARP-Guard Isolation Period on an Interface

Command	**nfpp 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. 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.
	`QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#arp-guard rate-limit per-src-mac 5 QTECH (config-nfpp)#arp-guard attack-threshold per-src-mac 10 QTECH (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

21.4.2 Configuring IP Guard

Configuration Effect

- IP attacks are identified based on hosts or physical interfaces. In host-based IP attack identification, IP attacks are 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 attack

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 CPP 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 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 "% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to 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 threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_IP_GUARD-4-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 within 10 seconds meet the following 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 system 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 delete trusted host 1.1.1.0 255.255.255.0." 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 1.1.1.0 255.255.255.0 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 threshold, an attack log is 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 this command to trust the host. 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 that configured in NFPP 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	**per-src-ip**: Configures the attack threshold of each source IP address.

Description	**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 routed and 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 passthrough.**
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.

	`QTECH# configure terminal QTECH(config)# nfpp`
	`QTECH (config-nfpp)#ip-guard rate-limit per-src-ip 20 QTECH (config-nfpp)#ip-guard attack-threshold per-src-ip 30 QTECH (config-nfpp)#ip-guard isolate-period 180`
	`QTECH (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

21.4.3 Configuring ICMP Guard

Configuration Effect

- ICMP attacks are identified based on hosts or ports. In host-based attack identification, ICMP attacks are 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 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 attack
identification, the system also isolates the attack source.
- Configure ICMP guard isolation to assign hardware-isolated entries against host attacks so that attack packets are 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 period, and the configured 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 monitored hosts 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 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 "% 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 threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ ICMP_GUARD-4-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 system 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 delete trusted host 1.1.1.0 255.255.255.0." 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 1.1.1.0 255.255.255.0 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 whether these 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-zero value, the system automatically performs hardware isolation against monitored attackers and sets the 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 part of 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 "% NFPP_ICMP_GUARD-4-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 Mode	NFPP configuration 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 configured in NFPP 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 passthrough.**
Configuration Steps	▪ Configure the host-based attack threshold. ▪ Set the isolation period to a non-zero value.
	Configure trusted hosts.

	`QTECH# configure terminal QTECH(config)# nfpp`
	`QTECH (config-nfpp)#icmp-guard rate-limit per-src-ip 20 QTECH (config-nfpp)#icmp-guard attack-threshold per-src-ip 30 QTECH (config-nfpp)#icmp-guard isolate-period 180`
	`QTECH (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

21.4.4 Configuring DHCP Guard

Configuration Effect

- DHCP attacks are identified based on hosts or ports. In host-based attack identification, DHCP attacks are identified 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-based
  attack identification, the system also isolates the attack source.
- Configure DHCP guard isolation to assign hardware-isolated entries against host attacks so that attack packets are 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 Functions of 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 period, and the configured 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 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 "% 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 threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCP_GUARD-4-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 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 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-zero value, the system automatically performs hardware isolation against monitored attackers and sets the 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 part of 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 "% NFPP_DHCP_GUARD-4-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	**per-src-mac**: Limits the rate of each source MAC address.
Description	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 configured in NFPP 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.
	`QTECH# configure terminal QTECH(config)# nfpp QTECH (config-nfpp)#dhcp-guard rate-limit per-src-mac 8 QTECH (config-nfpp)#dhcp-guard attack-threshold per-src-mac 16 QTECH (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

21.4.5 Configuring DHCPv6 Guard

Configuration Effect

- DHCPv6 attacks are identified based on hosts or ports. In host-based attack identification, DHCPv6 attacks are identified 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 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 and sends traps.
- In host-based attack identification, the system also isolates the attack source.

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 positive of DHCPv6 traffic on the trusted ports. For details about trusted ports of DHCPv6 snooping, see "Configuring Basic 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 the configured 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 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 "% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: 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 threshold is smaller than rate limit 300pps." to notify the administrator.

- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCPV6_GUARD-4-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-zero value, the system automatically performs hardware isolation against monitored attackers and sets the 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 part of 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 "% NFPP_DHCPV6_GUARD-4-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 NFPP configuration mode.

❖ Configuring the DHCPv6-Guard Isolation Period on an Interface

Command	**nfpp dhcpv6-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 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.
	`QTECH# configure terminal QTECH(config)# nfpp`
	`QTECH (config-nfpp)#dhcpv6-guard rate-limit per-src-mac 8`
	`QTECH (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 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 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`

Common Errors

N/A

21.4.6 Configuring ND Guard

Configuration Effect

- AR ND guard classifies ND packets into three types based on their purposes: 1. NS and NA; 2. RS; 3. RA and 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 are 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 attack thresholds for these three types of packets respectively. If the ND packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ND packet rate exceeds the attack threshold, the system prints logs and 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.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.

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 packets while not 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 threshold is 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 Description	N/A
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 that configured in NFPP 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 trusted ports (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 administrator 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.
	`QTECH# configure terminal QTECH(config)# nfpp`
	`QTECH (config-nfpp)# nd-guard rate-limit per-port ns-na 30`
	`QTECH (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

21.4.7 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 guard configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.
- 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 MAC 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)." to 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 attack thresholds listed below can meet the requirements in most network scenarios and are for reference only. You can 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.c200.00	Not applicable to this policy	rate-limit 20 attatch-threshold	rate-limit 100 attatch-threshold

	00		40	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
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, self-defined guards allow hosts to freely combine type fields of packets. If the configuration is inappropriate, the network may 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 self-defined guard 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 configured 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-based host 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_DEFINE_GUARD-4-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 threshold is smaller than rate limit 300pps." to notify the administrator.

❖ **Configuring the Global Isolation Period**

- (Optional) 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 self-defined guard 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 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 the 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 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 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, more CPU 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 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 "% NFPP_DEFINE-4-SESSION_LIMIT: Attempt to 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 packet type is IPv4 in the **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 **etype** 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 **etype** 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 system automatically deletes this entry.
- If a trusted host cannot be deleted, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0." 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 1.1.1.0 255.255.255.0 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-defined 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 is 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 whether these 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 identification, 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 Isolation Period of a Self-defined Guard

Command	**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	Self-defined guard configuration mode
Usage Guide	If the isolation period is not 0, a host is isolated and its packets of the self-defined guard type are discarded when the packet rate of the self-defined guard exceeds the attack threshold.

❖ 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

❖ Configuring the Isolation Period of a Self-defined Guard on an Interface

Command	**nfpp define name isolate-period {*seconds*	permanent}**
Parameter Description	*name*: Indicates the name of a self-defined guard. *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

❖ 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 after you have configured **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 the isolation period.
	▪ Configure trusted hosts.
	`QTECH# configure terminal QTECH(config)# nfpp`
	`QTECH (config-nfpp)#define rip`
	`QTECH (config-nfpp-define)#match etype 0x0800 protocol 17 dst-port 520`
	`QTECH (config-nfpp-define)#global-policy per-src-ip 100 150`
	`QTECH (config-nfpp-define)# isolate-period 180`
	`QTECH (config-nfpp-define)#trusted-host 192.168.201.46 255.255.255.255`
	`QTECH (config-nfpp-define)#exit`
	`QTECH (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 Isolate-period Rate-limit Attack-threshold`
	`Global Enable 180 100/-/- 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

21.4.8 Enabling/Disabling All Guards

Configuration Effect

- Use the (no) all-guard enable command to enable or disable all attack guards so that you do not need to disable or enable them one by one.

Notes

- Only basic guards (ARP, ICMP, IP, DHCP, DHCPv6, and ND) are applied.
- Only the global configuration is applied. Interface-based guard configuration remains the same.
- After the command is executed, basic guards are displayed by using the **show running-config** command.
- The **no all-guard enable** command just packs the **no** commands of all basic guards together. After you run the disabling command, the **no** commands of all basic guards are displayed under the **show running-config** command. After you run the enabling command, the default conditions are displayed under the **show running-config** command.

Configuration Steps

❖ **Running (no) all-guard enable in Global Configuration Mode**

Verification

When a host sends a large number of packets corresponding to basic guards to a switch, such as ARP/ICMP packets, NFPP guard detection takes effect by default.

- Run the **no all-guard enable** command. With the **show cpu-protect** command used, NFPP ratelimit failure is displayed. With the **show nfpp xx-guard host** command used, no attacker is displayed. With the **show nfpp xx-guard summary** command used, the "disabled" status of guards is displayed.

Related Commands

❖ **Running (no) all-guard enable in Global Configuration Mode**

Command	no all-guard enable
Parameter Description	
Command Mode	NFPP configuration mode
Usage Guide	1. By default, all basic guards are enabled. 2. Supported guards: ARP-GUARD / IP-GUARD / ICMP-GUARD / DHCP-GUARD / DHCPv6-GUARD / ND-GUARD 3. After disabling globally, the no xx-guard enable command is run automatically for all basic guards, which is visible by command show running-config. After enabling globally, the xx-guard enable command is run automatically for all basic guards, 4. Global enabling/disabling self-defined guards is not supported and does not affect the guard enabling status on interface. Global disabling/enabling does not support saving the configuration, but its results will take effect after saving and restart.

Configuration Example

❖ Prioritizing Packets Sent to the CPU Through Centralized Bandwidth Allocation

Scenario	N/A
Configuration Steps	N/A

	QTECH(config)#show running-config | begin nfpp nfpp log-buffer enable arp-guard rate-limit per-port 201 arp-guard attack-threshold per-port 210 ! QTECH(config)# nfpp QTECH(config-nfpp)#no all-guard enable QTECH(config-nfpp)#show running-config | begin nfpp nfpp log-buffer enable no arp-guard enable arp-guard rate-limit per-port 201 arp-guard attack-threshold per-port 210 no icmp-guard enable no ip-guard enable no dhcp-guard enable no dhcpv6-guard enable no nd-guard enable ! QTECH(config-nfpp)#all-guard enable QTECH(config-nfpp)#show running-config | begin nfpp nfpp log-buffer enable arp-guard rate-limit per-port 201 arp-guard attack-threshold per-port 210 ! no service password-encryption !
Verification	N/A

Common Errors

N/A

21.4.9 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 the previous ones with all attributes marked with a hyphen (-) is displayed in the log buffer. The administrator needs to increase the log buffer size or the system message 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 to export the log 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 instantly generated. This also applies to *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 VLAN range are recorded. 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 specified interface are recorded. 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, which requires restriction.**

Configuration Steps	▪ Configure the log buffer size.
	▪ Configure the log buffer rate.
	▪ Configure VLAN-based log filtering.
	`QTECH# configure terminal QTECH(config)# nfpp`
	`QTECH (config-nfpp)#log-buffer entries 1024`
	`QTECH (config-nfpp)#log-buffer logs 3 interval 5 QTECH (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
```

21.5 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*]
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**]

22.1. Overview

Denial of Service (DoS) attacks refer to attacks that cause DoS and aim to put computers or networks out of service.

DoS attacks are diversified in types and can be implemented in many ways, but have one common purpose, that is, prevent victim hosts or networks cannot receive, respond, or process external requests in time. In particular, on a layer-2 (L-2) network, DoS attack packets can be spread in the entire broadcast domain. If hackers maliciously initiate DoS attacks, some operating systems (OSs) may collapse. QTECH products supports the following anti DoS attack functions:

- Denying land attacks
- Denying invalid TCP packets
- Denying invalid layer-4 (L4) ports

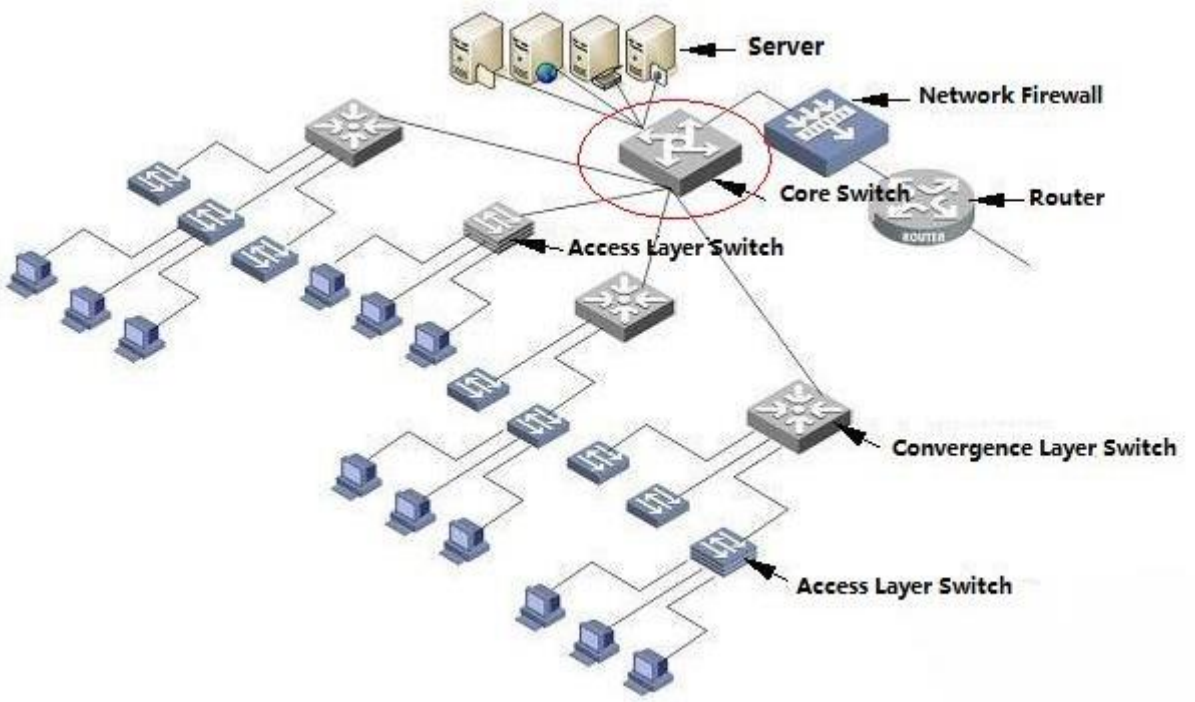
22.2 Applications

Application	Description
Protecting Attacks Servers Against DoS	On a campus network, configure the anti DoS attack function on the devices connected to servers to effectively reduce the negative impacts brought by DoS attacks to servers.

22.2.1 Protecting Servers Against DoS Attacks

As show in Figure 23-1, 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 23-1



Deployment

Enable the function of denying land attacks on the core switch to protect servers against land attacks.

Enable the function of denying invalid TCP packets on the core switch to protect servers against invalid TCP packets.

Enable the function of denying invalid L4 ports on the core switch to protect servers against attacks caused by invalid L4 ports.

22.3 Features

Overview

Feature	Description
Denying Land Attacks	Drop packets with the same source and destination IP addresses or the same L4 source and destination port IDs on the device to prevent these packets from attacking OSs on the network.
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.

22.3.1 Denying Land Attacks

This function protects servers against land attacks.

Working Principle

In a land attack, the attacker sets the source and destination IP addresses or the L4 source and destination port IDs in a SYN packet to the same address of the target host. Consequently, the attacked host will be trapped in an infinite loop or even collapse when attempting to set up a TCP connection with itself.

If the function of denying land attacks is enabled, the device checks packets based on characteristics of land packets (that is, SYN packets with the same source and destination IP addresses), and drops invalid packets.

22.3.2 Denying Invalid TCP Packets

This function protects servers against invalid TCP packets.

Working Principle

There are several flag fields in the TCP packet header:

- SYN: Connection establishment flag. The TCP SYN packet is used to set this flag to 1 to request establishment of a connection.
- ACK: Acknowledgement flag. In a TCP connection, this field must be available in every flag (except the first packet, that is, the TCP SYN packet) as the acknowledgement of the previous packet.
- FIN: Finish flag. When a host receives the TCP packet with the FIN flag, the host disconnects the TCP connection.
- RST: Reset flag. When the IP protocol stack receives a TCP packet that contains a non-existent destination port, it responds with a packet with the RST flag.
- PSH: This flag notifies the protocol stack to submit TCP data to the upper-layer program for processing as soon as possible.

In invalid TCP packets, flag fields are set improperly so that the processing resources of hosts are exhausted or even the system collapses. The following lists several common methods for setting flag fields in invalid TCP packets:

- TCP packets with both the SYN and FIN flags

Normally, a TCP packet cannot contain both the SYN and FIN flags. In addition, RFC does not stipulate how the IP protocol stack should process such invalid packets containing both the SYN and FIN flags. Therefore, the protocol stack of

each OS may process such packets in different ways when receiving these packets. Attackers can use this feature to send packets containing both the SYN and FIN flags to identify the OS type and initiate attacks on this OS.

- TCP packets without any flag

Normally, a TCP packet contains at least one of the five flags, including SYN, FIN, ACK, RST, and PSH. The first TCP packet (TCP SYN packet) must contain the SYN flag, and the subsequent packets contain the ACK flag. Based on such assumptions, some protocol stack does not specify the method for processing TCP packets without any flag, and therefore may collapse if such protocol stack receives TCP packets without any flag. Attackers use this feature to initiate attacks on target hosts.

- TCP packets with the FIN flag but without the ACK flag

Normally, except the first packet (TCP SYN packet), all other packets, including the packets with the FIN flag, contain the ACK flag. Some attackers may send TCP packets with the FIN flag but without the ACK flag to the target hosts, causing breakdown of the target hosts.

- TCP packets with the SYN flag and the source port ID set to a value between 0 and 1,023

Port IDs 0 to 1,023 are known port IDs allocated by the Internet Assigned Numbers Authority (IANA). In most systems, these port IDs can be used only by the system (or root) processes or programs run by privileged users. These ports (0–1023) cannot be used as the source port IDs in the first TCP packets (with the SYN flag) sent by clients.

If the function of denying invalid TCP packets is enabled, the device checks packets based on characteristics of invalid TCP packets, and drops invalid TCP packets.

22.3.3 Denying Invalid L4 Ports

This function protects servers against invalid L4 ports.

Working Principle

Attackers sends packets in which the IP address of the target host is the same as the L4 port ID of the host to the host target. As a result, the target host sends TCP connection setup requests to itself. Under such attacks, resources of the target host will soon be exhausted and the system will collapse.

If the function of denying invalid L4 ports is enabled, the device checks the L4 source port ID and destination port ID in the packets. If they are the same, the device drops the packets.

22.4 Configuration

Configuration Item	Description and Command

Configuring the Function of Denying Land Attacks	Optional.	
	ip deny land	Enables the function of denying land attacks globally.
Configuring the Function of Denying Invalid TCP Packets	Optional.	
	ipdeny invalid-tcp	Enables the function of denying invalid TCP packets globally.
Configuring the Function of Denying Invalid L4 Ports	Optional.	
	ip deny invalid-l4port	Enables the function of denying invalid L4 ports globally.

22.4.1 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.**
	`QTECH# configure terminal QTECH(config)# ip deny land` `QTECH(config)# end`

Verification	Run the **showipdenyland** command to display the status of the function of denying land attacks. The following example shows how to display the status of the function of denying land attacks:
	`QTECH#show ip deny land`
	`DoS Protection Mode State`
	
	`protect against land attack On`

22.4.2 Configuring the Function of Denying Invalid TCP Packets

Configuration Effect

Enable the function of denying invalid TCP packets. Then, the device checks packets based on characteristics of invalid TCP packets, and drops invalid TCP packets.

Configuration Steps

❖ **Enables the Function of Denying Invalid TCP Packets**

- Mandatory.
- Perform this configuration on a device connected to a server.

Verification

- Run the **show ip deny invalid-tcp** command to display the status of the function of denying invalid TCP packets.
- After this function is enabled, construct an invalid TCP packet and confirm that this packet cannot be forwarded.

Related Commands

❖ **Configuring the Function of Denying Invalid TCP Packets**

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.**
	`QTECH# configure terminal QTECH(config)# ip deny invalid-tcp` `QTECH(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:
	`QTECH#show ip deny invalid-tcp` `DoS Protection Mode State protect against invalid tcp attack On`

22.4.3 Configuring the Function of Denying Invalid L4

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.**
	QTECH# configure terminal QTECH(config)# ip deny invalid-l4port QTECH(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: QTECH#show ip deny invalid-l4port DoS Protection Mode State protect against invalid l4port attack On

22.5 Monitoring

Displaying

Description	Command
Displays the status of the function of denying land attacks.	**Showipdeny land**
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 antiDoS attack functions.	**show ip deny**