

Security Configuration

Оглавление

1	CONFIGURING AAA	7
1.1	Overview	7
1.2	Applications	7
1.2.1	Configuring AAA in a Single-Domain Environment	8
1.2.2	Configuring AAA in a Multi-Domain Environment	9
1.3	Features	10
1.3.1	AAA Authentication	12
1.3.2	AAA Authorization	14
1.3.3	AAA Accounting	15
1.3.4	Multi-Domain AAA	16
1.3.5	Login Switch for the AAA Slave Device	18
1.3.6	Authorization Result Caching	18
1.3.7	Configuring AAA Authentication	22
1.3.8	Configuring AAA Authorization	30
1.3.9	Configuring AAA Accounting	40
1.3.10	Configuring an AAA Server Group	49
1.3.11	Configuring the Domain-Based AAA Service	53
1.3.12	Configuring a Login Switch for the AAA Slave Device	60
1.3.13	Configuring Authorization Result Caching	62
1.4	Monitoring	63
2	CONFIGURING RADIUS	65
2.1	Overview	65
2.2	Applications	66
2.2.1	Providing Authentication, Authorization, and Accounting Services for Access Users	66
2.2.2	Forcing Users to Go Offline	67
2.3	Features	67
2.3.1	RADIUS Authentication, Authorization, and Accounting	74
2.3.2	Source Address of RADIUS Packets	76
2.3.3	RADIUS Timeout Retransmission	77
2.3.4	RADIUS Server Accessibility Detection	77
2.3.5	RADIUS Forced Offline	78
2.4	Configuration	79
2.4.1	RADIUS Basic Configuration	80

1. Configuring AAA	3
2.4.2 Configuring the RADIUS Attribute Type	85
2.4.3 Configuring RADIUS Accessibility Detection	88
2.5 Monitoring	92
3 CONFIGURING TACACS+	94
3.1 Overview	94
3.2 Applications	94
3.2.1 Managing and Controlling Login of End Users	94
3.3 Features	95
3.3.1 TACACS+ Authentication, Authorization, and Accounting	96
3.4 Configuration	98
3.4.1 Configuring TACACS+ Basic Functions	99
3.4.2 Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+	103
3.5 Monitoring	108
4 CONFIGURING SCC	109
4.1 Overview	109
4.2 Application	109
4.2.1 Access Control of Extended Layer 2 Campus Networks	109
4.2.2 Authentication Mode	113
4.2.3 Authentication-Exemption VLAN	113
4.2.4 IPv4 User Capacity	114
4.2.5 Authenticated-User Migration	114
4.2.6 User Online-Status Detection	115
4.3 Configuration	117
4.3.1 Configuring the Authentication Mode	118
4.3.2 Configuring Authentication-Exemption VLANs	121
4.3.3 Configuring the IPv4 User Capacity	124
4.3.4 Configuring Authenticated-User Migration	126
4.3.5 Configuring User Online-Status Detection	129
4.4 Monitoring	131
5 CONFIGURING PASSWORD POLICY	132
5.1 Overview	132
5.2 Features	132
5.3 Configuration	133
5.3.1 Configuring the Password Security Policy	134

1. Configuring AAA	4
5.4 Monitoring	139
6 CONFIGURING STORM CONTROL	140
6.1 Overview	140
6.2 Applications	140
6.2.1 Network Attack Prevention	140
6.3 Features	141
6.3.1 Unicast Packet Storm Control	142
6.3.2 Multicast Packet Storm Control	142
6.3.3 Broadcast Packet Storm Control	143
6.4 Configuration	144
6.4.1 Configuring Basic Functions of Storm Control	144
6.5 Monitoring	147
7 CONFIGURING SSH	148
7.1 Overview	148
7.2 Applications	148
7.2.1 SSH Device Management	149
7.2.2 SSH Local Line Authentication	150
7.2.3 SSH AAA Authentication	151
7.2.4 SSH Public Key Authentication	152
7.2.5 SSH File Transfer	152
7.2.6 SSH Client Application	153
7.3 Features	153
7.3.1 SSH Server	155
7.3.2 SCP Service	157
7.3.3 SSH Client	158
7.3.4 SCP Client	158
7.4 Configuration	159
7.4.1 Configuring the SSH Server	160
7.4.2 Configuring the SCP Service	190
7.4.3 Configuring the SSH Client	193
7.4.4 Configuring SCP Client	199
7.5 Monitoring	204
8 CONFIGURING URPF	1
8.1 Overview	1
8.2 Applications	1

1. Configuring AAA	5
8.2.1 Strict Mode	2
8.2.2 Loose Mode	2
8.3 Features	3
8.3.1 Enabling URPF	4
8.3.2 Notifying the URPF Packet Loss Rate	6
8.4 Configuration	7
8.4.1 Enabling URPF	7
8.4.2 Configuring the Function of Monitoring the URPF Packet Loss Information	13
8.5 Monitoring	16
9 CONFIGURING CPP	18
9.1 Overview	18
9.2 Applications	18
9.2.1 Preventing Malicious Attacks	18
9.2.2 Preventing CPU Processing Bottlenecks	19
9.3 Features	20
9.3.1 Classifier	21
9.3.2 Meter	22
9.3.3 Queue	22
9.3.4 Scheduler	22
9.3.5 Shaper	23
9.4 Configuration	24
9.4.1 Configuring CPP	24
9.4.2 Configuring CPP Warning	31
9.5 Monitoring	33
10 CONFIGURING DHCP SNOOPING	1
10.1 Overview	1
10.2 Applications	1
10.2.1 Guarding Against DHCP Service Spoofing	2
10.2.2 Guarding Against DHCP Packet Flooding	2
10.2.3 Guarding Against Forged DHCP Packets	3
10.2.4 Guarding Against IP/MAC Spoofing	4
10.2.5 Preventing Lease of IP Addresses	5
10.2.6 Detecting ARP Attacks	6
10.3 Features	6
10.3.1 Filtering DHCP Packets	9
10.3.2 Building the Binding Database	10

1. Configuring AAA	6
10.4 Configuration	10
10.4.1 Configuring Basic Features	12
10.4.2 Configuring Option82	18
10.5 Monitoring	21
11 CONFIGURING NFPP	23
11.1 Overview	23
11.2 Applications	23
11.2.1 Attack Rate Limiting	23
11.2.2 Centralized Bandwidth Allocation	24
11.3 Features	25
11.3.1 Host-based Rate Limiting and Attack Identification	28
11.3.2 Port-based Rate Limiting and Attack Identification	29
11.3.3 Monitoring Period	29
11.3.4 Isolation Period	30
11.3.5 Trusted Hosts	31
11.3.6 Centralized Bandwidth Allocation	31
11.4 Configuration	32
11.4.1 Configuring ARP Guard	37
11.4.2 Configuring IP Guard	46
11.4.3 Configuring ICMP Guard	54
11.4.4 Configuring DHCP Guard	62
11.4.5 Configuring DHCPv6 Guard	68
11.4.6 Configuring ND Guard	74
11.4.7 Configuring a Self-Defined Guard	78
11.4.8 Configuring Centralized Bandwidth Allocation	89
11.4.9 Configuring NFPP Logging	91
11.5 Monitoring	94

1 CONFIGURING AAA

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.

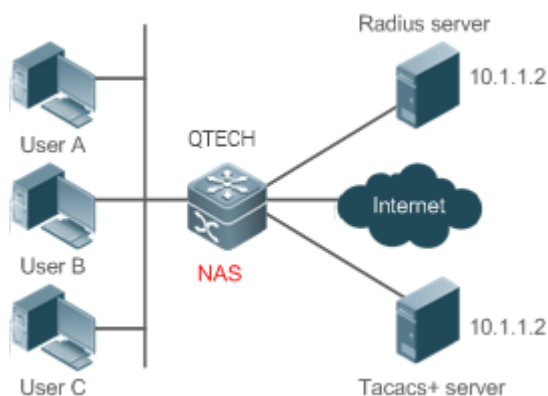
1.2.1 Configuring AAA in a Single-Domain Environment

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

Deployment

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

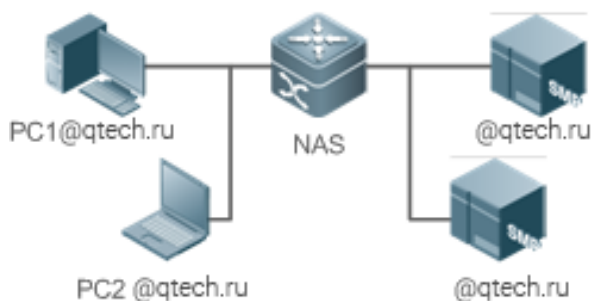
1.2.2 Configuring AAA in a Multi-Domain Environment

Scenario

Configure the domain-based AAA service on the NAS.

- A user can log in by entering the username PC1@QTECH.ru or PC2@QTECH.ru 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	<p>The clients with the usernames PC1@qtech.ru and PC2@qtech.ru are connected to the NAS in wired or wireless way.</p> <p>The NAS is an access or convergence switch.</p>
----------------	---

The Security Accounts Manager (SAM) server is a universal RADIUS server.

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

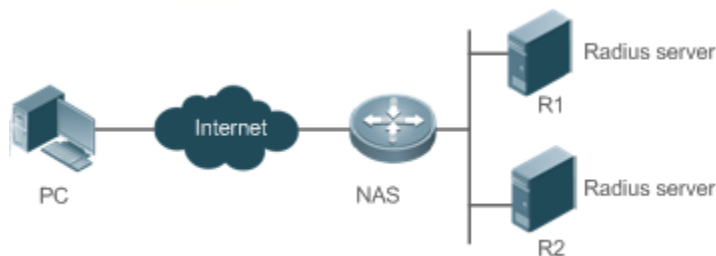


Figure 1-3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

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.

- i 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.
- i 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.
Login Switch for the AAA Slave Device	Provides a login switch to control login of the AAA slave device.
Authorization Result Caching	Caches authorization results returned from the server that can be used for later authorization at the same level.

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.

- i** 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).

[Related Configuration](#)

Enabling AAA

By default, AAA is disabled.

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

Configuring an AAA Authentication Scheme

By default, no AAA authentication scheme is configured.

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

Configuring an AAA Authentication Method List

By default, no AAA authentication method list is configured.

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

1.3.2 AAA Authorization

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

AAA Authorization Scheme

- Direct authorization (**none**)

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

- Local authorization (**local**)

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

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

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

AAA Authorization Types

- EXEC authorization

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

- Config-commands authorization

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

- Console authorization

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

- Command authorization

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

- Network authorization

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

Related Configuration

Enabling AAA

By default, AAA is disabled.

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

Configuring an AAA Authorization Scheme

By default, no AAA authorization scheme is configured.

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

Configuring an AAA Authorization Method List

By default, no AAA authorization method list is configured.

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

1.3.3 AAA Accounting

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

In AAA configuration, accounting scheme configuration is optional.

AAA Accounting Schemes

- No accounting (**none**)

Accounting is not performed on users.

- Local accounting (**local**)

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

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

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

AAA Accounting Types

- EXEC accounting

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

- Command accounting

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

- Network accounting

Records are kept on the sessions 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.

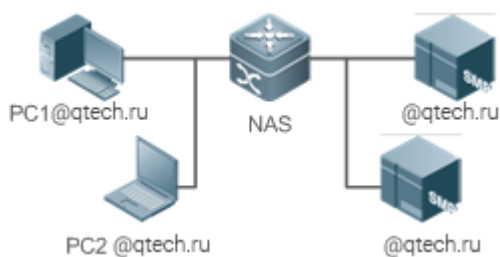
The NAS provides the domain-based AAA service based on the following principles:

- 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.

i 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.

1.3.5 Login Switch for the AAA Slave Device

A login switch is provided to control login of the AAA slave device. By default, the switch is off, so the slave device is not allowed to login. When the switch is turned on, the slave device can login.

Related Configuration

Enabling AAA

By default, AAA is disabled.

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

Configuring a Login Switch for the AAA Slave Device

By default, the slave device is not allowed to login.

Run the **aaa slave-login allow** command to permit login of the slave device.

1.3.6 Authorization Result Caching

The AAA module caches authorization results returned from the server. Therefore, later authorizations at the same level can be operated based on the cached resources.



Related Configuration



Configuring Authorization Result Caching




By default, authorization results are not cached.

To enable authorization result caching, run the **aaa command-author cache** command.

Configuration

Configuration	Description and Command	
Configuring AAA Authentication	 Mandatory if user identities need to be verified.	
	aaa new-model	Enables AAA.
	aaa authentication login	Defines a method list of login authentication.
	aaa authentication enable	Defines a method list of Enable authentication.
	aaa authentication ppp	Defines a method list of PPP authentication.
	aaa authentication sslvpn	Defines a method list of SSL VPN authentication.
	login authentication	Applies login authentication to a specific terminated line.
	aaa local authentication attempts	Sets the maximum number of login attempts.
	aaa local authentication lockout-time	Sets the lockout time for a login user.
Configuring 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	Defines a method list 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.
	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.
	username-format	Configures whether to contain the domain name in usernames.
	access-limit	Configures the maximum number of domain users.
Configuring a Login Switch for the AAA Slave Device	 Mandatory if a login switch needs to be configured for the AAA slave device.	
	aaa slave-login allow	Allows login of the slave device.
Configuring Authorization Result Caching	 Mandatory if later authorizations at the same level need to be operated based on the former results.	
	aaa command-author cache	Caches authorization results.

1.3.7 Configuring AAA Authentication

Configuration

Effect

Verify whether users are able to obtain access permission.

Notes

- If an authentication scheme contains multiple authentication methods, these methods are executed according to the configured sequence.
- The next authentication method is executed only when the current method does not respond. If the current AAA method fails, the next method will be not tried.
- When the **none** method is used, users can get access even when no authentication method gets response. Therefore, the **none** method is used only as standby.

i 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 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 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.

Applying Login Authentication to a Specific Terminated Line

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

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.

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

	<p>In a method list, the next method is executed only when the current method does not receive response.</p> <p>After you configure login authentication methods, apply the methods to the VTY lines that require login authentication; otherwise, the methods will not take effect.</p>
--	--

Defining a Method List of Enable Authentication

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

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

Command	aaa authentication { ppp sslvpn } { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]
Parameter Description	<p>ppp: Configures a method list of PPP authentication.</p> <p>sslvpn: Configures a method list of SSL VPN authentication.</p> <p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name</i>: Indicates the name of a PPP authentication method list in characters.</p>

	<p><i>method</i>: Indicates authentication methods from local, none, group, and subs. A method list contains up to four methods.</p> <p><i>local</i>: Indicates that the local user database is used for authentication.</p> <p><i>none</i>: Indicates that authentication is not performed.</p> <p><i>group</i>: Indicates that a server group is used for authentication. Currently, RADIUS and TACACS+ server groups are supported.</p> <p><i>subs</i>: Specifies the SUBS authentication method using the SUBS database.</p>
Command Mode	Global configuration mode
Usage Guide	<p>If the AAA PPP authentication service is enabled on the NAS, users must perform PPP authentication negotiation through AAA. Run the <code>aaa authentication ppp</code> command to configure the default or optional method lists for PPP authentication.</p> <p>In a method list, the next method is executed only when the current method does not receive response.</p>

Setting the Maximum Number of Login Attempts

Command	<code>aaa local authentication attempts <i>max-attempts</i></code>
Parameter Description	<i>max-attempts</i> : 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	<code>aaa local authentication lockout-time <i>lockout-time</i></code>
Parameter Description	<i>lockout-time</i> : Indicates the time during which a user is locked after entering wrong passwords up to the specified times. The value ranges from 1 to 2,147,483,647, in the unit of minutes.

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	
Configurati on Steps	<p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.)</p> <p>Step 3: Configure an AAA authentication method list for login authentication users. (This example uses group radius and local in order.)</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authentication method is used.</p>
NAS	<pre> 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 </pre>

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

Configuring AAA Enable Authentication

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

<p>Scenario</p> <p>Figure 1-6</p>	
<p>Configurati on Steps</p>	<p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. Configure Enable authentication passwords on the NAS if you use Enable password authentication.</p> <p>Step 3: Configure an AAA authentication method list for Enable authentication users.</p>

	<p>i 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.</p>
NAS	<pre>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</pre>
Verification	Run the show aaa method-list command on the NAS to display the configuration.
NAS	<pre>QTECH#show aaa method-list Authentication method-list: aaa authentication enable default group radius local enable Accounting method-list: Authorization method-list:</pre>
	The CLI displays an authentication prompt when the user level is updated to level 15. The user must enter the correct username and password to access the NAS.
NAS	<pre>QTECH>enable Username:user Password:pass QTECH#</pre>

Common

Errors

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

1.3.8 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.

i 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 <i>list-name</i> } <i>method1</i> [<i>method2...</i>]
Parameter Description	<p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name</i>: Indicates the name of an EXEC authorization method list in characters.</p> <p><i>method</i>: Specifies authentication methods from local, none, and group. A method list contains up to four methods.</p> <p>local: Indicates that the local user database is used for EXEC authorization.</p> <p>none: Indicates that EXEC authorization is not performed.</p> <p>group: Indicates that a server group is used for EXEC authorization. Currently, the RADIUS and TACACS+ server groups are supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>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.</p> <p>After you configure EXEC authorization methods, apply the methods to the VTY lines that require EXEC authorization; otherwise, the methods will not take effect.</p>

Defining a Method List of Command Authorization

Command	aaa authorization commands <i>level</i> { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]
----------------	---

Parameter Description	<p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name</i>: Indicates the name of a command authorization method list in characters.</p> <p><i>method</i>: Indicates authentication methods from none and group. A method list contains up to four methods.</p> <p>none: Indicates that command authorization is not performed.</p> <p>group: Indicates that a server group is used for command authorization. Currently, the TACACS+ server group is supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>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.</p> <p>When you configure command authorization, specify the command level, which is used as the default level. (For example, if a command above Level 14 is visible to users, the default level of the command is 14.)</p> <p>After you configure command authorization methods, apply the methods to the VTY lines that require command authorization; otherwise, the methods will not take effect.</p>

Configuring a Method List of Network Authorization

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

Usage Guide	<p>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.</p> <p>You can configure three different authorization methods. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried.</p> <p>RADIUS or TACACS+ servers return a series of AV pairs to authorize authenticated users. Network authorization is based on authentication. Only authenticated users can perform network authorization.</p>
-------------	---

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

Command	aaa authorization config-commands
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	<p>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.</p>

Enabling Authorization for the Console to Run Commands


Command	aaa authorization console
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	<p>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.</p>

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.

<p>Scenario Figure 1-7</p>	
<p>Configurati on Steps</p>	<p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.</p> <p>EXEC authorization is often used with login authentication, which can be implemented on the same line.</p>
<p>NAS</p>	<pre> 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 </pre>

Verification	Run the show run and show aaa method-list commands on the NAS to display the configuration.
NAS	<pre>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</pre>
	<pre>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</pre>

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.

<p>Scenario Figure 1-8</p>	
<p>Configurati on Steps</p>	<p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.</p>
<p>NAS</p>	<pre>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</pre>
<p>Verification</p>	<p>Run the show run and show aaa method-list commands on the NAS to display the configuration.</p>
<p>NAS</p>	<pre>QTECH#show aaa method-list Authentication method-list: aaa authentication login default local</pre>

Accounting method-list:

Authorization method-list:

```
aaa authorization commands 15 default group tacacs+ local
```

```
QTECH#show run
```

```
!
```

```
aaa new-model
```

```
!
```

```
aaa authorization console
```

```
aaa authorization commands 15 default group tacacs+ local
```

```
aaa authentication login default local
```

```
!
```

```
!
```

```
nfpp
```

```
!
```

```
vlan 1
```

```
!
```

```
username user1 password 0 pass1
```

```
username user1 privilege 15
```

```
no service password-encryption
```

```
!
```

```
tacacs-server host 192.168.217.10
```

```
tacacs-server key aaa
```

```
!
```

```
line con 0
```


```
line vty 0 4
```

```
!
```

```
!
```

```
end
```

Configuring AAA Network Authorization

<p>Scenario Figure 1-9</p>	
<p>Configuration Steps</p>	<p>Step 1: Enable AAA.</p> <p>Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.</p>
<p>NAS</p>	<pre>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</pre>
<p>Verification</p>	<p>Run the show aaa method-list command on the NAS to display the configuration.</p>
<p>NAS</p>	<pre>QTECH#show aaa method-list Authentication method-list: Accounting method-list: Authorization method-list: aaa authorization network default group radius none</pre>

Common Errors

N/A

1.3.9 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.

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 <i>list-name</i> } start-stop <i>method1</i> [<i>method2...</i>]
Parameter Description	<p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of an EXEC accounting method list in characters.</p> <p><i>method:</i> Indicates authentication methods from none and group. A method list contains up to four methods.</p> <p>none: Indicates that EXEC accounting is not performed.</p> <p>group: Indicates that a server group is used for EXEC accounting. Currently, the RADIUS and TACACS+ server groups are supported.</p>
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 <i>level</i> { default <i>list-name</i> } start-stop <i>method1</i> [<i>method2...</i>]
Parameter Description	<p><i>level</i>: 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.</p> <p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name</i>: Indicates the name of a command accounting method list in characters.</p> <p><i>method</i>: Indicates authentication methods from none and group. A method list contains up to four methods.</p> <p>none: Indicates that command accounting is not performed.</p> <p>group: Indicates that a server group is used for command accounting. Currently, the TACACS+ server group is supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>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.</p> <p>After you configure command accounting methods, apply the methods to the VTY lines that require command accounting; otherwise, the methods will not take effect.</p>

Defining a Method List of Network Accounting

Command	aaa accounting network { default <i>list-name</i> } start-stop <i>method1</i> [<i>method2...</i>]
----------------	--

Parameter Description	<p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of a network accounting method list in characters.</p> <p>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.</p> <p><i>method:</i> Indicates authentication methods from none and group. A method list contains up to four methods.</p> <p>none: Indicates that network accounting is not performed.</p> <p>group: Indicates that a server group is used for network accounting. Currently, the RADIUS and TACACS+ server groups are supported.</p>
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 <i>interval</i>
Parameter Description	<i>Interval:</i> 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 1-10	
Configuration Steps	<p>Step 1: Enable AAA.</p> <p>If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance.</p> <p>Step 2: Configure an AAA accounting method list according to different access modes and service types.</p> <p>Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.</p>
NAS	<pre> 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 </pre>

Verification	Run the show run and show aaa method-list commands on the NAS to display the configuration.
NAS	<pre>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:</pre>
	<pre>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</pre>

Configuring AAA Command Accounting

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

<p>Scenario Figure 1-11</p>	
<p>Configurati on Steps</p>	<p>Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance.</p> <p>Step 2: Configure an AAA accounting method list according to different access modes and service types.</p> <p>Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.</p>
<p>NAS</p>	<pre>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+</pre>
<p>Verification</p>	<p>Run the show aaa method-list command on the NAS to display the configuration.</p>
<p>NAS</p>	<pre>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:</pre>

```
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
```

Common

Errors

N/A

1.3.10 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	<code>aaa group server {radius tacacs+} name</code>

Parameter Description	<i>name</i> : 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 <i>ip-addr</i> [auth-port <i>port1</i>] [acct-port <i>port2</i>]
Parameter Description	<i>ip-addr</i> : Indicates the IP address of a server. <i>port1</i> : Indicates the authentication port of a server. (This parameter is supported only by the RADIUS server group.) <i>port2</i> : 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.

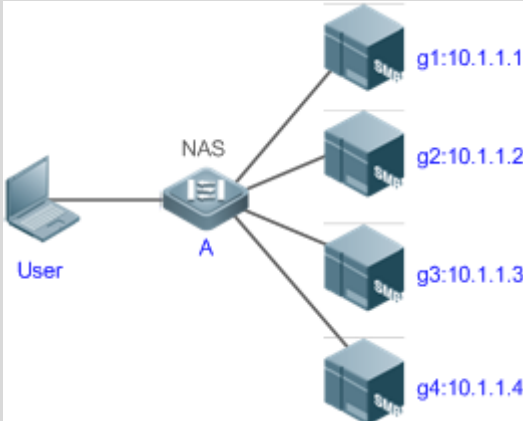
Configuring the VRF Attribute of an AAA Server Group

Command	ip vrf forwarding <i>vrf_name</i>
Parameter Description	<i>vrf_name</i> : 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.

<p>Scenario Figure 1-12</p>	
<p>Prerequisites</p>	<ol style="list-style-type: none"> 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.
<p>Configuration Steps</p>	<p>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.</p>
<p>NAS</p>	<pre> 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 </pre>

	<pre>QTECH(config-gs-radius)#server 10.1.1.3 QTECH(config-gs-radius)#server 10.1.1.4 QTECH(config-gs-radius)#exit</pre>
<p>Verification</p>	<p>Run the show aaa group and show run commands on the NAS to display the configuration.</p>
<p>NAS</p>	<pre>QTECH#show aaa group Type Reference Name ----- radius 1 radius tacacs+ 1 tacacs+ radius 1 g1 radius 1 g2</pre>
	<pre>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 ! !</pre>

Common Errors

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

1.3.11 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.
- 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 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 <i>domain-name</i> }
Parameter Description	default: Uses this parameter to configure the default domain. <i>domain-name</i> : 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 <i>domain-name</i> 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 a Network Accounting Method List

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

Usage Guide	
-------------	--

Configuring the Domain Status

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

Configuring Whether to Contain the Domain Name in Usernames

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

Configuring the Maximum Number of Domain Users

Command	access-limit <i>num</i>
Parameter Description	<i>num</i> : 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.

<p>Scenario Figure 1-13</p>	
<p>Configurati on Steps</p>	<p>The following example shows how to configure RADIUS authentication and accounting, which requires the configuration of a RADIUS server in advance.</p> <p>Step 1: Enable AAA.</p> <p>Step 2: Define an AAA method list.</p> <p>Step 3: Enable the domain-based AAA service.</p> <p>Step 4: Create a domain.</p> <p>Step 5: Associate the domain with the AAA method list.</p> <p>Step 6: Configure the domain attribute.</p>
<p>NAS</p>	<pre> 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 QTECH(config-aaa-domain)# username-format without-domain </pre>

<p>Verification</p>	<p>Run the show run and show aaa domain command on the NAS to display the configuration.</p>
<p>NAS</p>	<pre>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</pre>
	<pre>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 domain.com authentication dot1x default accounting network list3 ! aaa accounting network list3 start-stop group radius aaa authentication dot1x default group radius ! nfpp</pre>

```
!  
no service password-encryption  
!  
radius-server host 10.1.1.1  
radius-server key test  
!  
line con 0  
line vty 0 4  
!  
end
```

Common

Errors

N/A

1.3.12 Configuring a Login Switch for the AAA Slave Device

Configuration

Effect

When the switch is turned on, the slave device is allowed to login; otherwise, the slave device cannot login.

The configuration remains valid unless a change is made.

Notes

The **aaa new-model** command should be run first.

Configuration

Steps

Configuring a Login Switch for the AAA Slave Device

- Optional.
- By default, the slave device is not allowed to login.

Verification

Run the **show run** command to verify the configuration.

**Related
Commands**

Configuring a Login Switch for the AAA Slave Device

Command	<code>aaa slave-login allow</code>
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the switch is off, so the slave device is not allowed to login. When the switch is turned on, the slave device can login.

**Configuration
Example**

Configuring a Login Switch for the AAA Slave Device

Scenario Figure 1-14	
Configuration Steps	<p>The following example shows how to configure a login switch for the AAA slave device</p> <p>Step 1: Enable AAA.</p> <p>Step 2: Turn on the login switch.</p>
NAS	<pre>QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#aaa slave-login allow</pre>
Verification	Run the show run command on the NAS to display the configuration.
NAS	<pre>QTECH#sh run inc aaa</pre>
	<pre>aaa new-model aaa slave-login allow</pre>

Common Errors

N/A

1.3.13 Configuring Authorization Result Caching

Configuration

Effect

After this feature is configured, the AAA module caches authorization results returned from the server. Therefore, later authorizations at the same level can be operated based on the cache.

Notes

The cached authorization results, originating from specific levels of sessions and commands, can be applied only to sessions and commands at these levels.

Configuration

Steps

Configuring Authorization Result Caching

- Optional.
- By default, authorization results are not cached.

Verification

Run the **show run** command to verify the configuration.

Related


Commands

Configuring Authorization Result Caching

Command	aaa command-author cache
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The AAA device caches authorization results returned from the server. Therefore, later authorizations at the same level can be operated based on the cached resources.

Configuration Example

Configuring Authorization Result Caching

<p>Scenario Figure 1-15</p>	
<p>Configuration Steps</p>	<p>The following example shows how to configure authorization result caching</p> <p>Step 1: Enable AAA.</p> <p>Step 2: Turn on the login switch.</p> <p>Step 3: Configure authorization result caching.</p>
<p>NAS</p>	<pre>QTECH#configure terminal QTECH(config)#aaa new-model QTECH(config)#aaa command-author cache QTECH(config)# aaa authorization commands 15 default group tacacs+</pre>
<p>Verification</p>	<p>Run the show run command on the NAS to display the configuration.</p>
<p>NAS</p>	<pre>QTECH#sh run inc aaa</pre>
	<pre>aaa new-model aaa authorization commands 15 default group tacacs+ aaa command-author cache</pre>

1.4 Monitoring

Clearing

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

Displaying

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

2 CONFIGURING RADIUS

2.1 Overview

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

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

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

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

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

Protocols and Standards

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

2.2 Applications

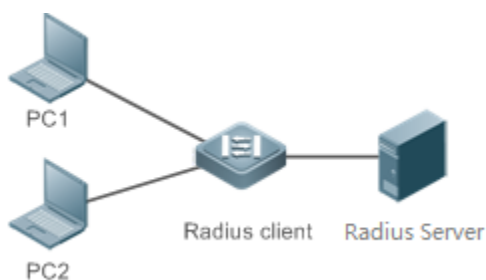
Application	Description
Providing Authentication, Authorization, and Accounting Services for Access Users	Authentication, authorization, and accounting are conducted on access users on a network, to prevent unauthorized access or operations.
Forcing Users to Go Offline	The server forces an authenticated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

2.2.1 Providing Authentication, Authorization, and Accounting 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

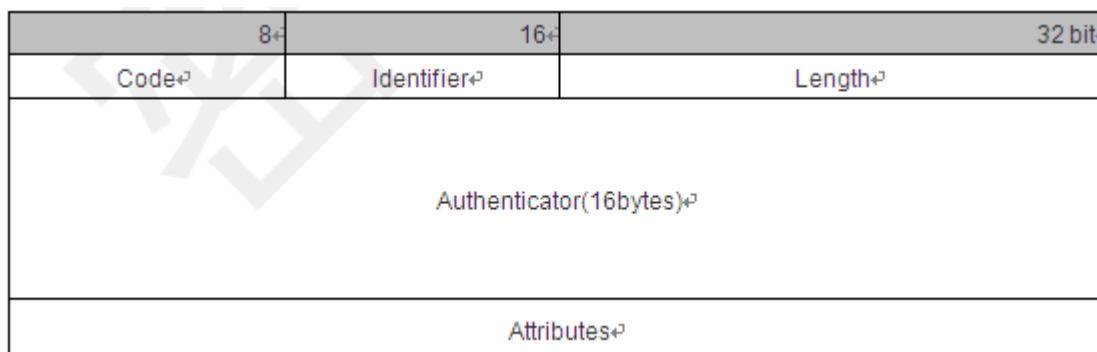
Basic Concepts

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-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference

39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

Shared Key

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

RADIUS Server Group

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

RADIUS Attribute Type

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

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

Format	Description
--------	-------------

ietf	Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 08-c6-b3-33-22-AC
Normal	Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 08c6.b333.22ac
Unformatted	Indicates the format without separators. This format is used by default. Example: 08c6b33322ac

- 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-supplciant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

Overview

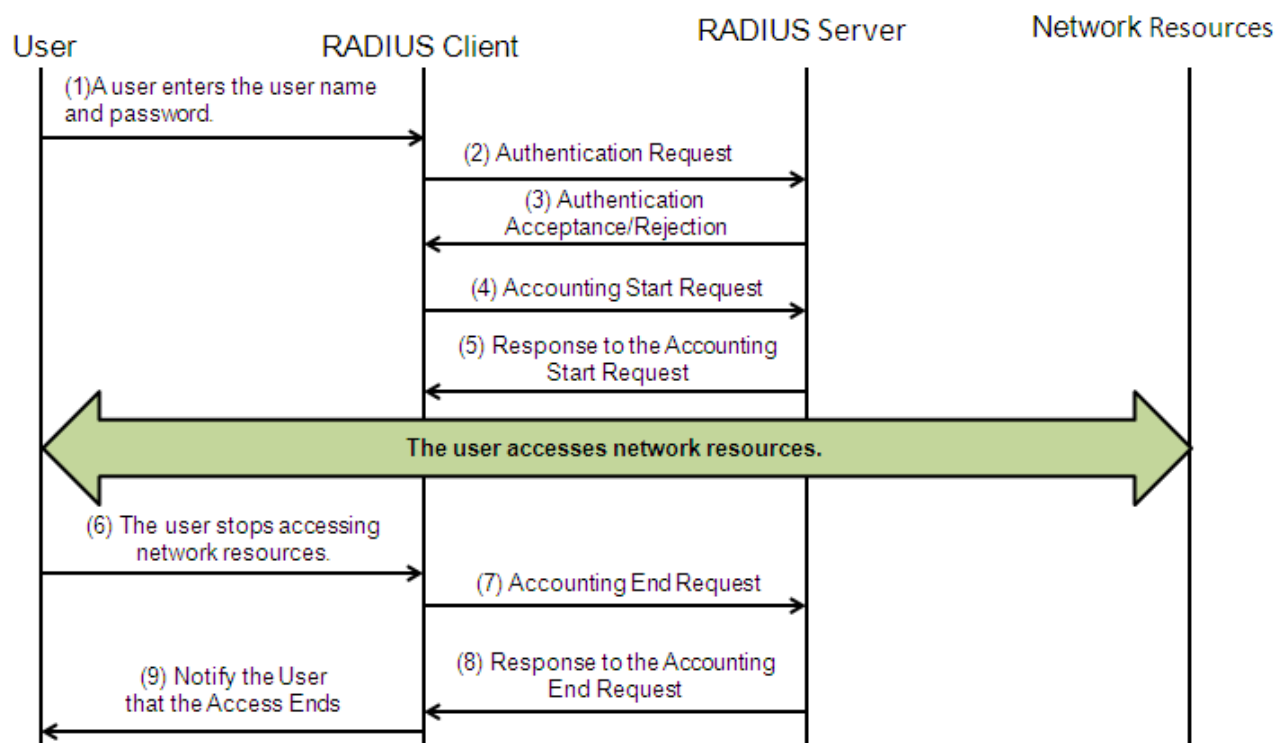
Feature	Description
RADIUS Authentication, Authorization, and Accounting	Conducts identity authentication and accounting on access users, safeguards network security, and facilitates management for network administrators.
Source Address of RADIUS Packets	Specifies the source IP address used by a RADIUS client to transmit packets to a RADIUS server.
RADIUS Timeout Retransmission	Specifies the packet retransmission parameter for a RADIUS client when a RADIUS server does not respond to packets transmitted from the RADIUS client within a period of time.
RADIUS Server Accessibility Detection	Enables a RADIUS client to actively detect whether a RADIUS server is reachable 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:

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

The RADIUS accounting process is described as follows:

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

Related Configuration

Configuring RADIUS Server Parameters

No RADIUS server is configured by default.

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

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

Configuring the AAA Authentication Method List

No AAA authentication method list is configured by default.

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

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

Configuring the AAA Authorization Method List

No AAA authorization method list is configured by default.

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

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

Configuring the AAA Accounting Method List

No AAA accounting method list is configured by default.

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

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

2.3.2 Source Address of RADIUS Packets

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

Working Principle

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

Related Configuration

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

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

2.3.3 RADIUS Timeout Retransmission

Working Principle

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

Related Configuration

Configuring the RADIUS Server Timeout Time

The default timeout time is 5 seconds.

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

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

Configuring the Retransmission Count

The default retransmission count is 3.

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

Configuring Whether to Retransmit Accounting Update Packets

Accounting update packets are not retransmitted by default.

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

2.3.4 RADIUS Server Accessibility Detection

Working Principle

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

Related Configuration

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

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

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

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

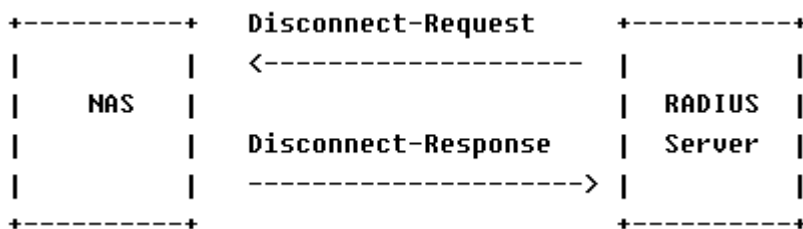
No test user name is specified for actively detecting the RADIUS security server by default.

You can run the **radius-server host x.x.x.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-serverhost Configures the IP address of the remote RADIUS security server.
	radius-serverkey Configures the shared key for communication between the device and the RADIUS server.
	radius-serverretransmit Configures the request transmission count, after which the device confirms that a RADIUS server is unreachable.
	radius-servertimeout 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 the RADIUS Attribute Type	 (Optional) It is used to define attribute processing adopted when the device encapsulates and parses RADIUS packets.
	radius-serverattribute31 Configures the MAC address format of RADIUS attribute No. 31 (Calling-Station-ID).
	radius set qoscos Sets the private attribute port-priority issued by the server to the COS value of an interface. For COS-relevant concepts, see the <i>Configuring QoS</i> .
	radius support cui Configures the device to support the CUI attribute.
	radius vendor-specific Configures the mode of parsing private attributes by the device.
Configuring 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 device to stop transmitting request packets to an unreachable RADIUS server.
	radius-server host Configures the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.

2.4.1 RADIUS Basic Configuration

Configuration

Effect

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

Notes

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

Configuration

Steps

Configuring the Remote RADIUS Security Server

- Mandatory.
- Configure the IP address, authentication port, accounting port, and shared 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 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	<code>radius-server host [oob [<i>viamgmt_name</i>]] { <i>ipv4-address</i> } [auth-port<i>port-number</i>] [acct-port<i>port-number</i>][test username<i>name</i> [idle-timetime] [ignore-auth-port] [ignore-acct-port]] [key [0 7] <i>text-string</i>]</code>
Parameter Description	<p><i>oob</i>: Indicates oob authentication, that is, the source interface for transmitting packets to the RADIUS server is an mgmt port.</p> <p><i>viamgmt_name</i>: Specifies a specific mgmt port when oob supports multiple mgmt ports.</p> <p><i>ipv4-address</i>: Indicates the IPv4 address of the RADIUS security server.</p> <p><i>auth-portport-number</i>: 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.</p> <p><i>acct-port port-number</i>: 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.</p> <p>test username <i>name</i>: Enables the function of actively detecting the RADIUS security server and specifies the user name used for active detection.</p> <p><i>idle-timetime</i>: Indicates the interval for the device to transmit test packets to a reachable RADIUS security server. The default value is 60 minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).</p> <p><i>ignore-auth-port</i>: Disables the function of detecting the authentication port of the RADIUS security server. It is enabled by default.</p> <p><i>ignore-acct-port</i>: Disables the function of detecting the accounting port of the RADIUS security server. It is enabled by default.</p>

	<code>key [0 7] text-string</code> : 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 <code>radius-server host</code> 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	<code>radius-server key [0 7] text-string</code>
Parameter Description	<i>text-string</i> : 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	<code>radius-server retransmitretries</code>
Parameter Description	<i>retries</i> : Indicates the RADIUS retransmission count. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	The prerequisite for AAA to use the next user authentication method is that the current security server used for authentication does not respond. The criteria for the device to judge that a security 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 timeoutseconds
Parameter Description	<i>seconds</i> : 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.

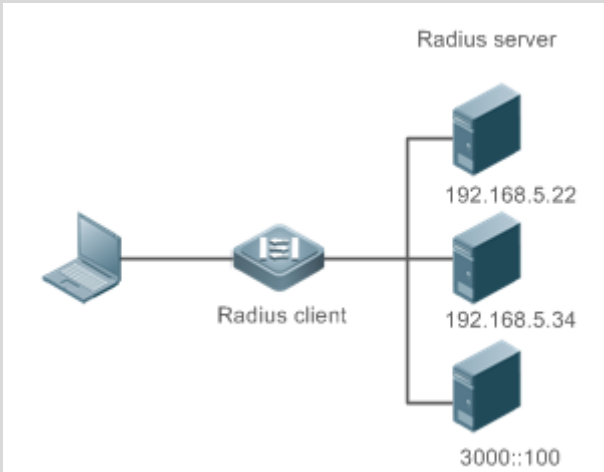
Configuring Retransmission of Accounting Update Packets for Authenticated Users

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 not retransmitted by default. The configuration does not affect users of other types.

Configuration

Example

Using RADIUS Authentication, Authorization, and Accounting for Login Users

<p>Scenario Figure 2-4</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ▪ 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.
<p>RADIUS Client</p>	<pre>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 authorizationexecetest group radius QTECH (config)#aaa accountingexecetest 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</pre>
<p>Verification</p>	<p>Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. After obtaining a certain access level granted by the server, only run commands under this access level. Display the authentication log of the user on the RADIUS server. Perform management operations on the device as the user and then log out. Display the accounting information on the user on the RADIUS server.</p>
	<pre>QTECH#show running-config ! radius-server host 192.168.5.22</pre>

```
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 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.

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	<code>radius-server attribute 31 mac format {ietf normal unformatted }</code>
Parameter Description	<p>ietf: Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 08-c6-b3-33-22-AC.</p> <p>normal: Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 08c6.b333.22ac.</p>

	unformatted: Indicates the format without separators. This format is used by default. Example: 08c6b33322ac.
Command Mode	Global configuration mode
Usage Guide	Some RADIUS security servers can identify only MAC addresses in the IETF format. In this case, set the MAC address format of Calling-Station-ID to IETF.

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

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

Configuration

Example

Configuring the RADIUS Attribute Type

Scenario	One authentication device
Configuration Steps	<ul style="list-style-type: none"> Configure the MAC address format of RADIUS Calling-Station-Id. 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.
	<pre>QTECH(config)#radius-server attribute 31 mac format ietf QTECH(config)#radiussetqoscos QTECH(config)#radiussupport cui QTECH(config)#radiusvendor-specific extend</pre>
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 timesecconds** 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 triesnumber**.

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 { <i>timeseconds</i> [<i>triesnumber</i>] <i>triesnumber</i> }
Parameter Description	<p><i>timeseconds</i>: Indicates the time condition parameter. If the device fails to receive a correct response packet from a RADIUS security server within the specified time, it is deemed that the RADIUS security server meets the inaccessibility duration condition. The value ranges from 1 second to 120 seconds.</p> <p><i>triesnumber</i>: Indicates the consecutive request timeout count. If the timeout count of request packets transmitted by the device to the same RADIUS security server reaches the preset count, it is deemed that the RADIUS security server meets the consecutive timeout count condition of inaccessibility. The value ranges from 1 to 100.</p>
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 deadtimeminutes
Parameter Description	<i>minutes</i> : Indicates the duration for the device to stop transmitting requests to an unreachable RADIUS security server, with the unit of minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).

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	<ul style="list-style-type: none"> 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	<pre>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</pre>
Verification	<p>Disconnect the network communication between the device and the server with the IP address of 192.168.5.22. Conduct RADIUS authentication through the device. After 120 seconds, run the show radius server command to check that the server state is dead.</p>
	<pre>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 ...</pre>

2.5 Monitoring

Clearing


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

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

Displaying

Description	Command
Displays global parameters of the RADIUS server.	<code>show radius parameter</code>
Displays the configuration of the RADIUS server.	<code>show radius server</code>
Displays the configuration of the RADIUS private attribute type.	<code>show radius vendor-specific</code>
Displays statistics relevant to the RADIUS dynamic authorization extension function.	<code>show radius dynamic-authorization-extension statistics</code>
Displays statistics relevant to RADIUS authentication.	<code>show radius auth statistics</code>
Displays statistics relevant to RADIUS accounting.	<code>show radius acct statistics</code>
Displays configuration of RADIUS server groups.	<code>show radius group</code>

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 CONFIGURING TACACS+

3.1 Overview

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

Protocols and Standards

- RFC 1492 Terminal Access Controller Access Control System

3.2 Applications

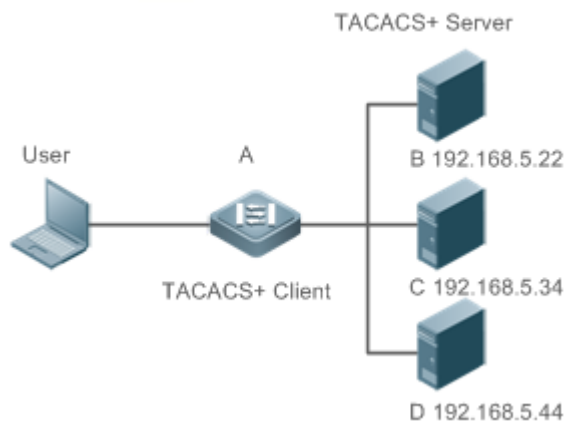
Application	Description
Managing and Controlling Login of End Users	Password verification and authorization need to be conducted on end users.

3.2.1 Managing and Controlling Login of End Users

Scenario

TACACS+ is typically applied in the login management and control of end users. A network device serves as the TACACS+ client and sends a user name and password to the TACACS+ server for verification. The user is allowed to log in 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.

3.3 Features

Basic Concepts

Format of TACACS+ Packets

Figure 3-2

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

- Major Version: Indicates the major TACACS+ version number.
- Minor Version: Indicates the minor TACACS+ version number.

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

Overview

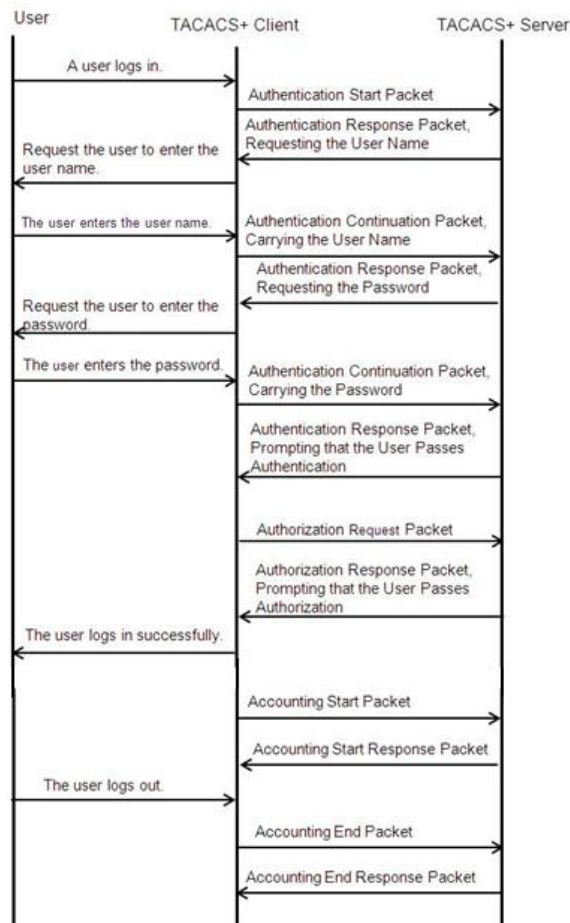
Feature	Description
TACACS+ Authentication, Authorization, and Accounting	Conducts authentication, authorization, and accounting on end users.

3.3.1 TACACS+ Authentication, Authorization, and Accounting

Working Principle

The following figure uses basic authentication, authorization, and accounting of user 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.

3.4 Configuration

Configuration	Description and Command
Configuring TACACS+ Basic Functions	 (Mandatory) It is used to enable the TACACS+ security service.
	tacacs-server host Configures the TACACS+ server.
	tacacs-server key Specifies the key shared by the server and network device.
	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.	
	aaa group server tacacs+	Configures TACACS+ server groups and divides TACACS+ servers into different groups.
	server	Adds servers to TACACS+ server groups.

3.4.1 Configuring TACACS+ Basic Functions

Configuration Effect

- The TACACS+ basic functions are available after the configuration is complete. When configuring the AAA method list, specify the method of using TACACS+ to implement TACACS+ authentication, authorization, and accounting.
- When authentication, authorization, and accounting operations are performed, TACACS+ initiates the 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 <i>mgmt_name</i>] <i>ipv4-address</i> [port <i>integer</i>] [timeout <i>integer</i>] [key [0 7] <i>text-string</i>]
Parameter Description	<p><i>ipv4-address</i>: Indicates the IPv4 address of the TACACS+ server.</p> <p><i>oob</i>: Uses an MGMT port as the source interface for communicating with the TACACS+ server. A non-MGMT port is used for communication by default.</p> <p>via <i>mgmt_name</i>: Specifies a specific MGMT port when <i>oob</i> supports multiple MGMT ports.</p> <p>port <i>integer</i>: Indicates the TCP port used for TACACS+ communication. The default TCP port is 49.</p> <p>timeout <i>integer</i>: Indicates the timeout time of the communication with the TACACS+ server. The global timeout time is used by default.</p> <p>key [0 7] <i>text-string</i>: 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.</p>
Defaults	No TACACS+ server is configured.
Command Mode	Global configuration mode
Usage Guide	<p>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 <code>tacacs-server key</code> command is used as the shared key of the server. The shared key must be completely the same as that configured on the server.</p> <p>You can specify the communication port of the server when configuring the IP address.</p>

	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	<i>text-string</i> : 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 timeoutseconds
Parameter Description	<i>seconds</i> : 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

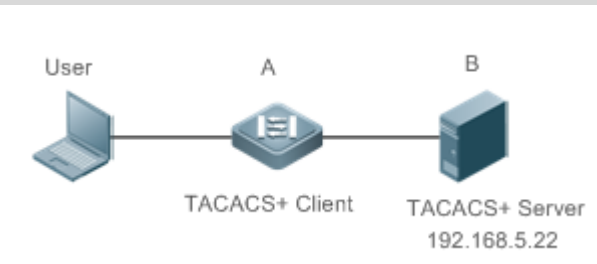
Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- 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

<p>Scenario Figure 3-4</p>	
Remarks	<ul style="list-style-type: none"> ▪ A is a client that initiates TACACS+ requests. ▪ B is a server that processes TACACS+ requests.
Configurati on Steps	<ul style="list-style-type: none"> ▪ Enable AAA. ▪ Configure the TACACS+ server information. ▪ Configure the method of using TACACS+ for authentication. ▪ Apply the configured authentication method on an interface.
A	<pre> 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 </pre>

	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.

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

Configuration Effect

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

Notes

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

Configuration Steps

Configuring TACACS+ Server Groups

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

Command	aaa group server tacacs+group-name
Parameter Description	<i>group-name</i> : Indicates the name of a group. A group name cannot be radius or tacacs+, which are the names of embedded groups.

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 <i>ipv4-address</i>
Parameter Description	<i>ipv4-address</i> : Indicates the IPv4 address of the TACACS+ server.
Defaults	No server is configured.
Command Mode	TACACS+ server group configuration mode
Usage Guide	<p>Before configuring this command, you must run the <code>aaa group server tacacs+</code> command to enter the TACACS+ server group configuration mode.</p> <p>For the address of a server configured in a TACACS+ server group, the server must be configured using the <code>tacacs-server host</code> command in global configuration mode.</p> <p>If multiple servers are added to one server group, when one server does not respond, the device continues to send a TACACS+ request to another server in the server group.</p>

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 <i>vrf-name</i>
----------------	--

Parameter Description	<i>vrf-name</i> : 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 <code>aaa group server tacacs+</code> 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 <code>vrf</code> 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	<code>ip oob via <i>mgmt_name</i></code>
Parameter Description	<i>mgmt-name</i> : Indicates the name of a management port.
Defaults	No oob is specified by default.
Command Mode	TACACS+ server group configuration mode
Usage Guide	Before configuring this command, you must run the <code>aaa group server tacacs+</code> command to enter the TACACS+ server group configuration mode. If no MGMT port is specified, the MGMT0 port is used by default.

Verification

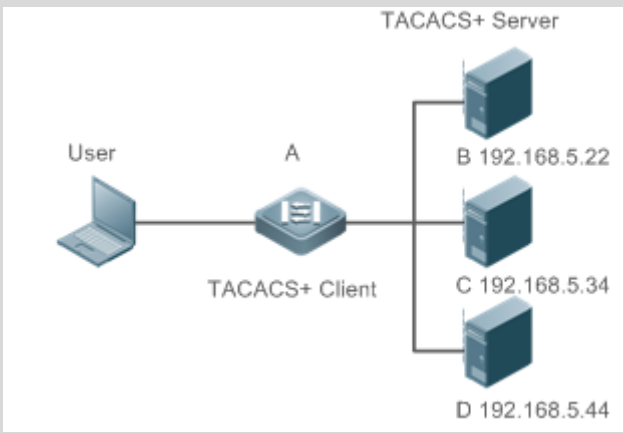
Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- 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

<p>Scenario Figure 3-5</p>	
<p>Remarks</p>	<ul style="list-style-type: none"> ▪ 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.
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ▪ 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.
	<pre> 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 </pre>

	<pre>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</pre>
Verification	<p>Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. Enter the 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.</p> <p>View the authentication log of the user on the server with the IP address of 192.168.5.22.</p> <p>View the enable authentication log of the user on the server with the IP address of 192.168.5.22.</p> <p>View the exec authorization log of the user on the server with the IP address of 192.168.5.34.</p> <p>View the command accounting log of the user on the server with the IP address of 192.168.5.44.</p>

Common

Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- Undefined servers are added to a server group.

- No method list is configured.

3.5 Monitoring

Displaying

Description	Command
Displays interaction with each TACACS+ server.	show tacacs

Debugging

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

Description	Command
Debugs TACACS+.	debug tacacs+

4 CONFIGURING SCC

4.1 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.

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.

- i** 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

4.2 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.

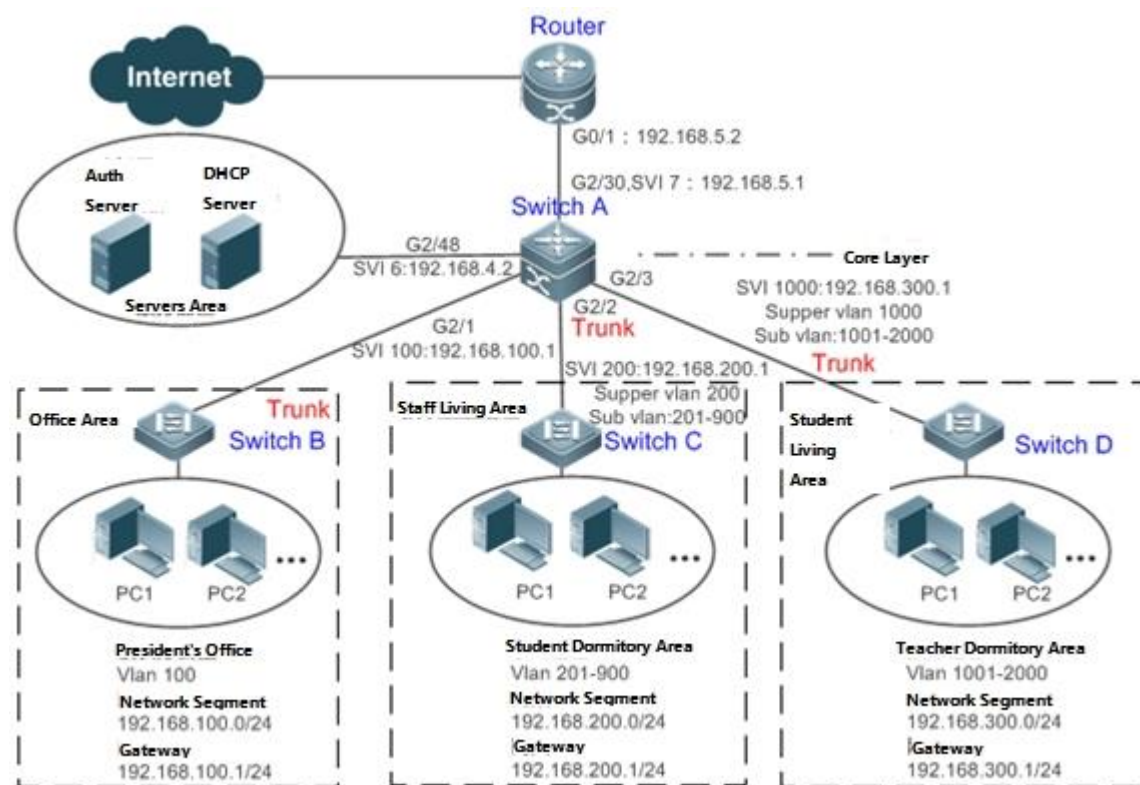
4.2.1 Access Control of Extended Layer 2 Campus Networks

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 4-1



Remark 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 1-1) are all trunk ports.

The user access switches B, C, and D connect to PCs in various departments via access ports, and VLANs correspond to sub VLANs configured on the downlink ports of the core switch, so that access users are 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.

Basic Concepts

Authentication Mode

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

Authentication-Exemption VLAN

Some special departments may be allocated to authentication-exemption VLANs to simplify network management, so 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.

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.

Features


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

4.2.2 Authentication Mode

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

Working Principle

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




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

4.2.3 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.

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

4.2.4 IPv4 User Capacity

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

Working Principle

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

- ℹ Only the switches support the restriction on the number of IPv4 access users.
- ℹ The number of IPv4 access users is not restricted on the device by default, but depends on the hardware capacity of the device.
- ⚠ The number of IPv4 access users includes 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.

4.2.5 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.

- ⚠ 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*.



4.2.6 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.

4.3 Configuration

Configuration Item	Suggestions and Related Commands	
Configuring the Authentication Mode	 Optional configuration, which is used to configure the authentication mode for the device.	
	[no] auth-mode gateway	Configures the authentication mode.
Configuring Authentication-Exemption VLANs	 Optional configuration, which is used to specify the users of which VLANs can access the Internet without authentication.	
	[no] direct-vlan	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.

4.3.1 Configuring the Authentication Mode

Configuration

Effect

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

Precautions

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

Configuration

Method

Configuring the Authentication Mode

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

Command	[no] auth-mode gateway
Parameter Description	no: If the command carries this parameter, it indicates that the authentication mode is restored to access authentication; that is, the local device is only an access device and not a gateway device any longer. auth-mode gateway: If the command carries this parameter, it indicates that the authentication mode is set to gateway authentication; that is, the local device is both a gateway device and an access device.
Defaults	Access authentication mode
Command Mode	Global configuration mode

Usage Guide	<p>Use this command to determine the access position of the device on the network. Perform this configuration or not perform this configuration, which depends on whether the access control function is deployed on access switches on the network or deployed on the gateway device.</p> <p>Use this command to change the authentication mode configured on the device from access authentication to gateway authentication. Use the no auth-mode gateway command to change the authentication mode configured on the device from gateway authentication back to access authentication.</p>
-------------	--

Verification

i Check the configuration using the following method:

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

Configuration

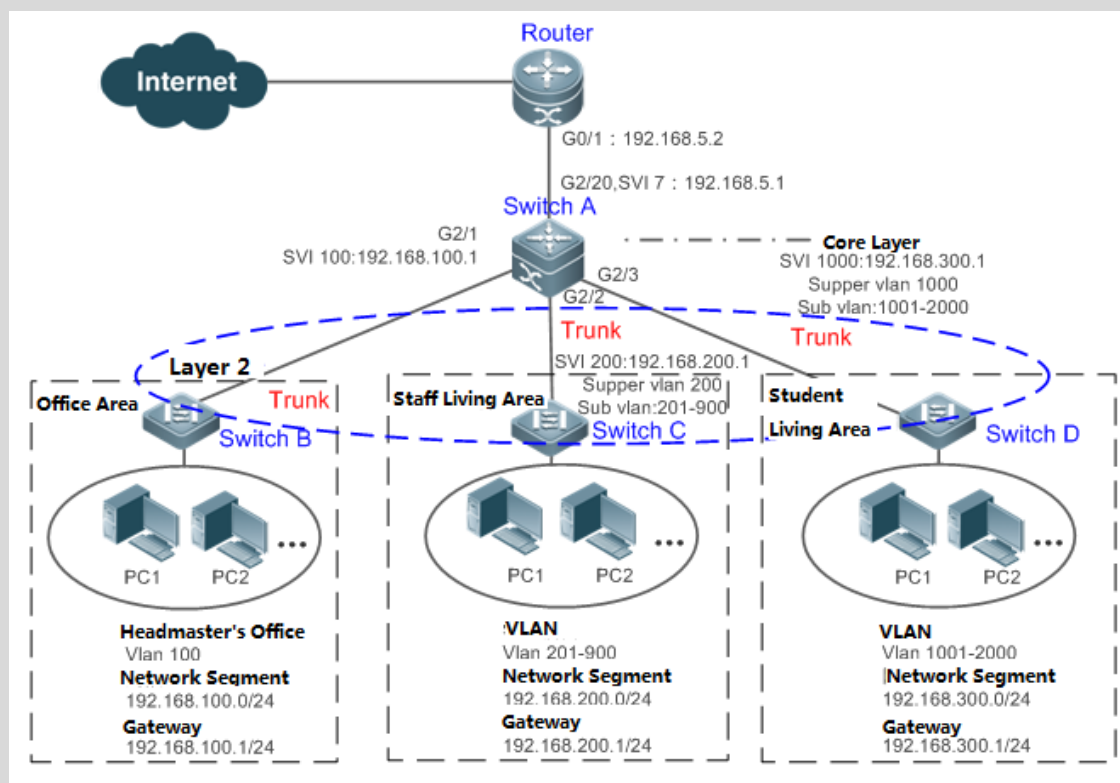
Examples

The following configuration example describes SCC-related configuration only.

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

Figure 4-2

Scenario
Figure 4-2



Configurati
on Steps

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

Switch A

```
SwitchA(config)#auth-mode gateway
Please save config and reload system.
SwitchA(config)#exit
*Nov 7 10:13:27: %SYS-5-CONFIG_I: Configured from console by console
SwitchA#reload
Reload system?(Y/N)y
SwitchA#
```

Verification

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

Switch A

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


4.3.2 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.

Notices

Authentication-exemption VLANs only mean that users in these VLANs do not need to experience a check related to access authentication, but still need to experience a check based on a security ACL. If specified users or 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

Steps

Configuring Authentication-Exemption VLANs

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

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

Verification

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

- Enable dot1x authentication on downlink ports that connect to user terminals, add the downlink ports that connect to the user terminals to a specific VLAN, and configure the VLAN as an authentication-exemption VLAN. Then open the Internet Explorer, and enter a valid extranet address (such as www.baidu.com). If the users can open the corresponding webpage on the Internet, it indicates that the authentication-exemption VLAN is valid; otherwise, the 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

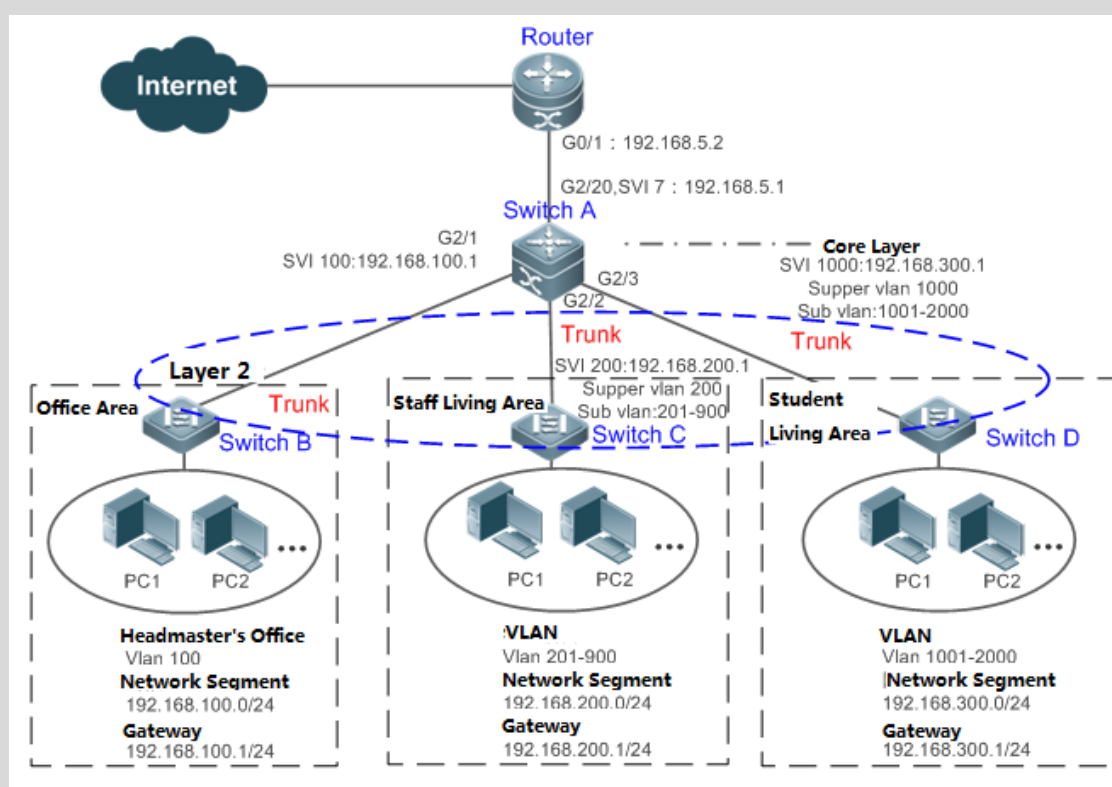
Configuration

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 4-3



Configurati
on 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
----------	---

4.3.3 Configuring the IPv4 User Capacity

Configuration

Effect

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

Precautions

N/A

Configuration

Method

Configuring the IPv4 User Capacity

- Optional configuration. To limit the maximum of users who are allowed to access an access port, configure the 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 <i>max-user-num</i> 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.

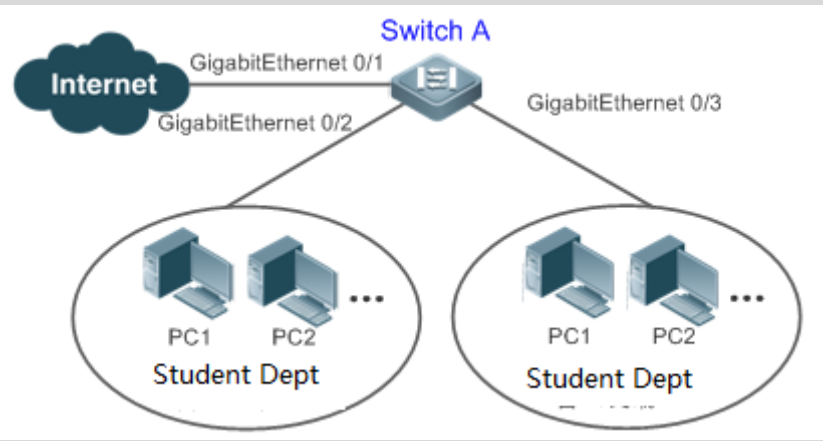
Command	show nac-author-user [interface <i>interface-name</i>]
Parameter Description	<i>interface-name</i> : This parameter indicates the interface name.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Global configuration mode
Usage Example	<pre>QTECH#show nac-author-user interface GigabitEthernet 0/1 Port Cur_num Max_num ----- Gi0/1 0 4</pre>

Configuration

Examples

i 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

<p>Scenario Figure 4-4</p>	
<p>Configurati on Steps</p>	<ul style="list-style-type: none"> 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.
<p>Switch A</p>	<pre>SwitchA(config)#int GigabitEthernet 0/2 SwitchA(config-if-GigabitEthernet 0/2)#nac-author-user maximum 4</pre>
<p>Verification</p>	<ul style="list-style-type: none"> 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.
<p>Switch A</p>	<pre>SwitchA(config)#show nac-author-user Port Cur_num Max_num ----- ----- ----- Gi0/1 0 4</pre>

4.3.4 Configuring Authenticated-User Migration

Configuration

Effect

By default, when a user gets online after passing dot1x or Web authentication at a physical location (which is represented by a specific access port plus the VLAN number) and quickly moves to another physical location without getting offline, the user cannot get online through dot1x or Web

authentication from the new physical location, 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, 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.

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

i 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

<p>Scenario Figure 4-5</p>	
<p>Configurati on Steps</p>	<ul style="list-style-type: none"> ▪ 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.
<p>Switch A</p>	<pre>sw1(config)#station-move permit</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ▪ 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.
<p>Switch A</p>	<pre>sw1(config)#show running-config include station station-move permit</pre>

4.3.5 Configuring User Online-Status Detection

Configuration

Effect

After the user online-status detection function is enabled, if a user's traffic is lower than a certain 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 by default.
- Perform this configuration on access, convergence, or core switches depending on user distribution. The configuration acts on only the configured device instead of other devices on the network.
- If the traffic threshold parameter `threshold` is set to 0, it indicates that zero-traffic detection will be performed.

Command	<code>offline-detect interval interval threshold threshold</code> <code>no offline-detect</code> <code>default offline-detect</code>
Parameter Description	<p><i>interval</i>: 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.</p> <p><i>threshold</i>: This parameter indicates the traffic threshold. The value range is from 0 to 4294967294 in bytes. The default value is 0, indicating that the user is disconnected when no traffic of the user is detected.</p> <p>no offline-detect: Disables the user online-status detection function.</p> <p>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.</p>
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:

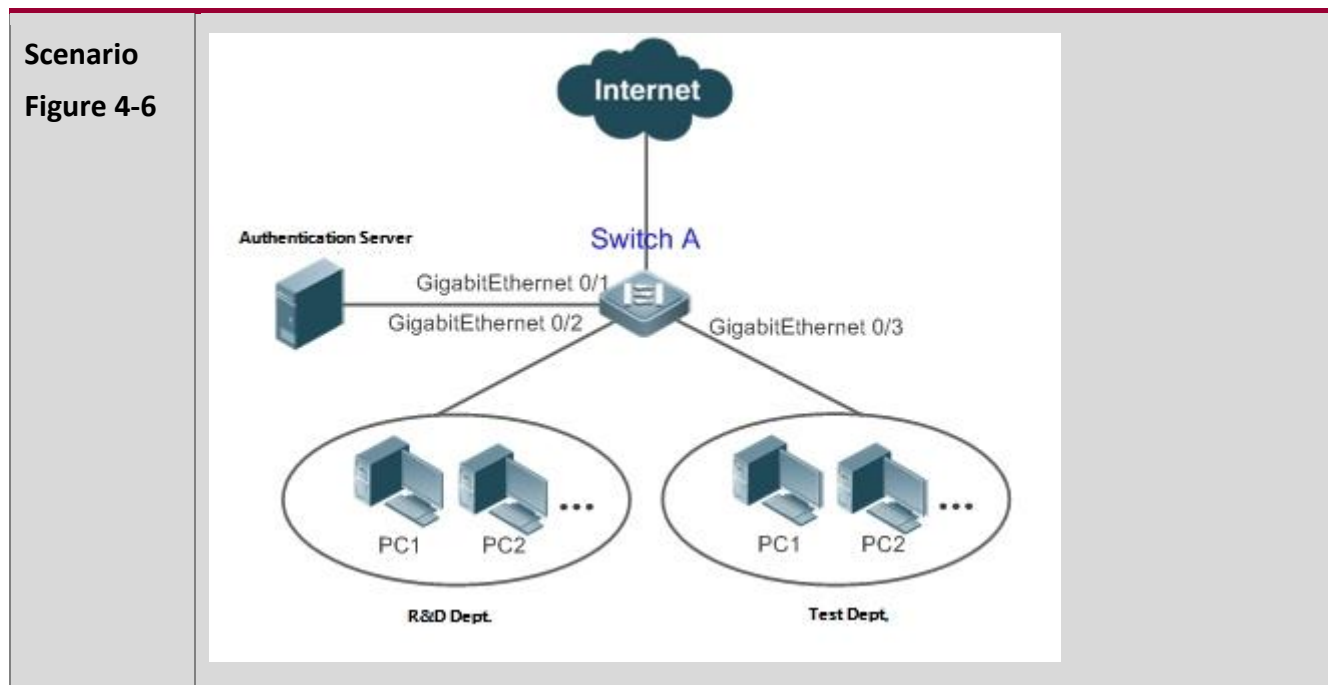
- After the user online-status detection function is enabled, power off the specified authenticated terminal after the corresponding user gets online. Then wait for the specified period of time, and run the online user query command associated with dot1x or Web authentication on the device to confirm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

Configuration

Examples

i 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



Configuration Steps	<ul style="list-style-type: none"> 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	<code>sw1(config)# offline-detect interval 5 threshold 0</code>
Verification	<ul style="list-style-type: none"> 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	<code>sw1(config)#show running-config include offline-detect offline-detect interval 5</code>

4.4 Monitoring

Displaying

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

Debugging

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

Command	Function
<code>debug scc event</code>	Debugs the SCC running process.
<code>debug scc user [mac author mac]</code>	Debugs SCC user entries.
<code>debug scc acl-show summary</code>	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.

5 CONFIGURING PASSWORD POLICY

5.1 Overview

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

i The following sections introduce password policy only.

Protocols and Standards

N/A

5.2 Features

Basic Concepts

Minimum Password Length

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

Strong Password Detection

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

1. Passwords that are the same as corresponding accounts;
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.

5.3 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.

5.3.1 Configuring the Password Security Policy

Networking Requirements

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

Notes

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

Configuration Steps

Configuring the Password Life Cycle

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

Configuring the Minimum Length of User Passwords

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

Setting the No-Repeat Times of Latest Password Configuration

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

Enabling the Strong Password Detection Function

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

Setting the Storage of Encrypted Passwords

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

Verification

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

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

Related Commands

Configuring the Password Life Cycle

Command	password policy life-cycle <i>days</i>
Parameter Description	life-cycle <i>days</i> : 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	password policy min-size <i>length</i>
Parameter Description	min-size <i>length</i> : 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	<code>password policy no-repeat-times <i>times</i></code>
Parameter Description	<code>no-repeat-times <i>times</i></code> : Indicates the no-repeat times of latest password configuration. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	<p>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.</p> <p>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.</p>

Enabling the Strong Password Detection Function

Command	<code>password policy strong</code>
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	<p>After the strong password detection function is enabled, a prompt is displayed for the following types of passwords:</p> <ol style="list-style-type: none">1. Passwords that are the same as corresponding accounts;2. Simple passwords that contain characters or digits only.

Setting the Storage of Encrypted Passwords

Command	service password-encryption
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Before the storage of encrypted passwords is set, all passwords used in the configuration process will be displayed and stored in plaintext format, unless the passwords are configured in cipher text format. You can enable the storage of encrypted passwords for security 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	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.

Configuration

Examples

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

Configuring Password Security Check on the Device

Typical Application	Assume that the following password security requirements arise in a network environment: 1. The minimum length of passwords is 8 characters;
----------------------------	---

	<ol style="list-style-type: none"> 2. The password life cycle is 90 days; 3. Passwords are stored and transmitted in cipher text format; 4. The number of no-repeat times of password history records is 3; 5. Passwords shall not be the same as user names, and shall not contain simple characters or digits only.
<p>Configurati on Steps</p>	<ul style="list-style-type: none"> ▪ 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. <pre> 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 </pre>
<p>Verification</p>	<p>When you create a user and the corresponding password after configuring the password security policy, the system will perform relevant detection according to the password security policy.</p> <ul style="list-style-type: none"> ▪ Run the show password policy command to display user-configured password security policy information. <pre> 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) </pre>

**Common
Errors**

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

5.4 Monitoring

Displaying

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

6 CONFIGURING STORM CONTROL

6.1 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.

6.2 Applications

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

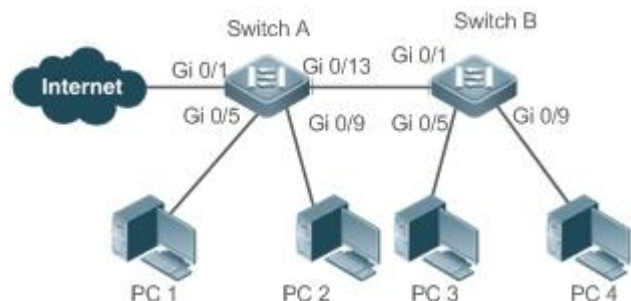
6.2.1 Network Attack Prevention

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 6-1



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).

6.3 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.

6.3.1 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.

6.3.2 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.

6.3.3 Broadcast Packet Storm Control

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

Working Principle

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

Related Configuration

Enabling Broadcast Packet Storm Control on Ports


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

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

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

The default command parameters are determined by related products.

6.4 Configuration

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

6.4.1 Configuring Basic Functions of Storm Control

Configuration

Effect

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

Notes

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

Configuration

Steps

Enabling Unicast Packet Storm Control

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

Enabling Multicast Packet Storm Control

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

Enabling Broadcast Packet Storm Control

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

Verification

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

Related Commands

Enabling Unicast Packet Storm Control

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

Enabling Multicast Packet Storm Control

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

Enabling Broadcast Packet Storm Control

Command	storm-control broadcast [{ level percent pps packets rate-bps }]
Parameter Description	level percent: Indicates the bandwidth percentage. pps packets: Indicates the number of packets per second. rate-bps: Indicates the packet rate.

Command Mode	Interface configuration mode
Usage Guide	Storm control can be enabled only on switch ports.

Configuration Example

Enabling Storm Control on Devices

Scenario	
Figure 6-2	
Configuration Step	<ul style="list-style-type: none"> Enable storm control on Switch A and Switch B.
Switch A	<pre>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</pre>
Switch B	<pre>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</pre>
Verification	Check whether storm control is enabled on Switch A and Switch B.
Switch A	<pre>QTECH# sho storm-control Interface Broadcast Control Multicast Control Unicast Control Action</pre>

	<pre>----- GigabitEthernet 0/1 Disabled Disabled Disabled none GigabitEthernet 0/5 default default default none GigabitEthernet 0/9 default default default none GigabitEthernet 0/13 default default default none -----</pre>
Switch B	<pre>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 GigabitEthernet 0/9 default default default none</pre>

6.5 Monitoring

Displaying

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

7 CONFIGURING SSH

7.1 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.

- i** 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.
- i** 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.

7.2 Applications

Application	Description
-------------	-------------

SSH Device Management	Use SSH to manage devices.
SSH Local Line Authentication	Use the local line password authentication for SSH user authentication.
SSH AAA Authentication	Use the authentication, authorization and accounting (AAA) mode for SSH 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.
SSH Client Application	Use the SSH client to safely log in to a remote device for management.

7.2.1 SSH Device Management

Scenario

You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows system does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client. Figure 7-1 shows the network topology.

Figure 7-1 Networking Topology of SSH Device Management



Deployment

Configure the SSH client as follows:

- Start the PuTTY software.
- On the **Session** option tab of PuTTY, type in the host IP address of the SSH server and SSH port number **22**, and select the connection type **SSH**.
- On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**.
- On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**.

- Click **Open** to connect to the SSH server.
- Type in the correct user name and password to enter the terminal login interface.

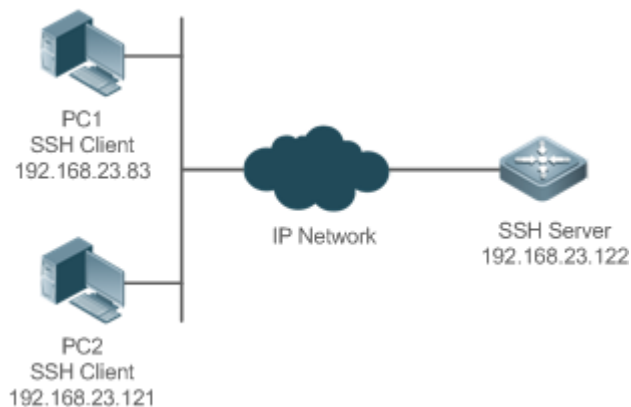
7.2.2 SSH Local Line Authentication

Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 7-2. 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 7-2 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:

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.

1. Open the PuTTY connection tab, and select SSHv1 for authenticated login. (The method is similar if SSHv2 is selected.)

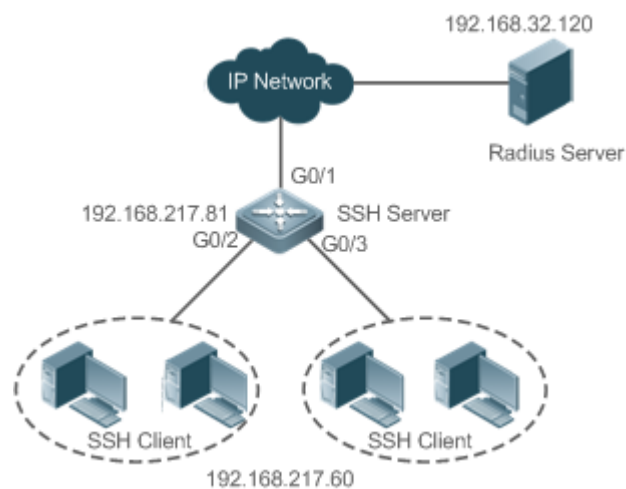
2. Set the IP address and connected port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22. Click **Open** to start the connection. As the current authentication mode does not require a user name, you can type in any user name, but cannot be null. (In this example, the user name is "anyname".)

7.2.3 SSH AAA Authentication

Scenario

SSH users can use the AAA authentication mode for user authentication, as shown in Figure 7-3. To ensure security of data exchange, the PCs function as the SSH clients, and use 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 7-3 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.

7.2.4 SSH Public Key Authentication

Scenario

SSH clients can use the public keys for authentication, and the public key algorithm can be RSA or DSA, as shown in Figure 7-4. SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 7-4 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.

7.2.5 SSH File Transfer

Scenario

The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server, as shown in Figure 7-5.

Figure 7-5 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.

7.2.6 SSH Client Application

Scenario

The SSH service is enabled on a remote SSH server, and the **ssh** command is used on the local client to set up an SSH connection with the server for secure data transmission, as shown in Figure 7-6.

Figure 7-6 Networking Topology of SSH Client Application



Deployment

- Enable the SSH service on the server.
- On the client, run the **ssh** command to set up an SSH connection with the server for secure data transmission.

7.3 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.

i 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 server. 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.
SSH Client	You can use the SSH client on the device to set up a secure connection with the SSH server on a network device.

7.3.1 SSH Server

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

Working Principle

For details about the working principle of the SSH server, see the "SSH Communication" in "Basic Concepts." In practice, after enabling the SSH server function, you can configure the following parameters according to the application requirements:

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

Related Configuration

Enabling the SSH Server

By default, the SSH server is disabled.

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

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

Specifying the SSH Version

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

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

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

Configuring the SSH Authentication Timeout

By default, the user authentication timeout is 120s.

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

Configuring the Maximum Number of SSH Authentication Retries

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

Run the **ip ssh authentication-retries** command to configure the maximum number of user authentication retries on the SSH server. Use the **no** form of the command to restore the default number of user authentication retries. If authentication still does not succeed when the maximum number of user authentication retries is reached, user authentication fails.

Specifying the SSH Encryption Mode

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

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

Specifying the SSH Message Authentication Algorithm

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

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

Configuring Support for Diffie-Hellman(DH) Key Exchange Algorithm on the SSH Server

By default, QTECH's SSHv2 server supports `diffie-hellman-group-exchange-sha1`, `diffie-hellman-group14-sha1`, and `diffie-hellman-group1-sha1` for keyexchange while the SSHv1 server support none. Run the **ip ssh key-exchange** command to configure support for Diffie-Hellman on the SSH server. Use the **no ip ssh key-exchange** command to restore the default setting.

Setting ACL Filtering of the SSH Server

By default, ACL filtering is not performed for all connections to the SSH server.

Run the **{ip | ipv6} ssh access-class** command to perform ACL filtering for all connections to the SSH server. Run **no {ip | ipv6} ssh access-class** to restore the default settings.

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.

7.3.2 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.

7.3.3 SSH Client

The SSH client is used to set up a secure connection with a remote network device on which the SSH server runs.

Working

Principle

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

Related

Configuration

Specifying the Source Interface of the SSH Client

By default, the source address of SSH packets is searched based on the destination address.

Run the **ip ssh source-interface *interface-name*** command to specify the source interface of the SSH client.

Establishing a Session with the SSH Server

Run the **ssh** command to log in to a remote device that supports the SSH Server

Recovering an Established SSH Session

- Run the **ssh-session *session-id*** command to recover an established SSH session.

Disconnecting a Suspended SSH Session

- Run the **disconnect ssh-session *session-id*** command to disconnect a specified SSH session.

7.3.4 SCP Client

The SCP client is used to support file transfer with the remote network device on which the SCP server is enabled.

Working

Principle

SCP is a protocol that supports online file transfer. It runs on Port 22 based on BSD RCP, while RCP provides the encryption and authentication functions based on the SSH protocol. RCP implements file transfer, and SSH implements authentication and encryption.

When you use an SCP client to upload or download files, the SCP client first parses 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 serves as a data provider in source mode and reads and sends files to the peer end through the SSH connection, while serving as the destination of data in sink mode and receives the files through the SSH connection.

Related Configuration

Specifying Source Interface of SCP Client


By default, configure the IP address of the source interface as the source address in SSH packets.



Run the **ip scp client source-interface** *interface-name* command to specify the source interface of the SCP client.

Establishing Connection with the SCP Server via SCP Client to Implement File Transfer

Run the **scp** command to implement file transfer with the SSH server.

7.4 Configuration

Configuration	Description and Command	
Configuring the SSH Server	 It is mandatory to enable the SSH server.	
	enable service ssh-server	Enables the SSH server.
	disconnect ssh [vty] <i>session-id</i>	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 <i>time</i>	Configures the SSH authentication timeout.
	ip ssh authentication-retries <i>retry times</i>	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	Configures support for Diffie-Hellman on the SSH server.	

	dh_group14_sha1 dh_group1_sha1 }	
	{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 Service	 Mandatory.	
	ip scp server enable	Enables the SCP server.
Configuring the SSH Client	 (Optional)It is used to set up a secure connection with a remote network device that supports the SSH server.	
	ip ssh source-interface interface-name	Specifies the source interface of the SSH client.
	ssh [oob] [-v {1 2}][-c {3des aes128-cbc aes192-cbc aes256-cbc}] [-l username][-m {hmac-md5-96 hmac-md5-128 hmac-sha1-96 hmac-sha1-160}] [-p port-num]{ ip-addr hostname}[via mgmt-name][/source {ipA.B.C.D ipv6 X:X:X::X interface interface-name}] [/vrf vrf-name]	Establishes an encrypted session with a remote network device.

7.4.1 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 <i>time</i>
Parameter Description	<i>time</i> : 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 <i>retry times</i>
Parameter Description	<i>retry times</i> : Indicates the maximum number of user authentication retries. The value ranges from 0 to 5.

Command Mode	Global configuration mode
Usage Guide	Run the <code>no ip ssh authentication-retries</code> command to restore the default number of user authentication retries, which is 3.

Specifying the SSH Encryption Mode

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

Specifying the SSH Message Authentication Algorithm

Command	<code>ip ssh hmac-algorithm{md5 md5-96 sha1 sha1-96}</code>
Parameter Description	<code>md5</code> : Indicates that the message authentication algorithm supported by the SSH server is MD5.

	<p>md5-96: Indicates that the message authentication algorithm supported by the SSH server is MD5-96.</p> <p>sha1: Indicates that the message authentication algorithm supported by the SSH server is SHA1.</p> <p>sha1-96: Indicates that the message authentication algorithm supported by the SSH server is SHA1-96.</p>
Command Mode	Global configuration mode
Usage Guide	<p>This command is used to configure the message authentication algorithm supported by the SSH server.</p> <p>On QTECH devices, the SSHv1 server does not 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.</p>

Configuring Support for DH Key Exchange Algorithm on the SSH Server

Command	<code>ip ssh key-exchange { dh_group_exchange_sha1 dh_group14_sha1 dh_group1_sha1 }</code>
Parameter Description	<p>dh_group_exchange_sha1: Indicates configuration of diffie-hellman-group-exchange-sha1 for keyexchange. The key has 2,048 bytes, which cannot be edited.</p> <p>dh_group14_sha1: Indicates configuration of diffie-hellman-group14-sha1 for keyexchange. The key has 2,048 bytes.</p> <p>dh_group1_sha1: Indicates configuration of diffie-hellman-group1-sha1 for keyexchange. The key has 1,024 bytes.</p>
Command Mode	Global configuration mode
Usage Guide	<p>Use this command to configure a DH key exchange method on the SSH.</p> <p>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 keyexchange.</p>

Configuring ACL Filtering of the SSH Server

Command	{ip ipv6} ssh access-class { <i>access-list-number</i> <i>access-list-name</i> }
Parameter Description	<p><i>access-list-number</i>: 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.</p> <p>Only IPv4 addresses are supported.</p> <p><i>access-list-name</i>: Indicates an ACL name. Both IPv4 and IPv6 addresses are supported.</p>
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 <i>test</i> public-key rsaflash:<i>rsa.pub</i>
Parameter Description	<p><i>test</i>: Indicates the user name.</p> <p><i>rsa</i>: Indicates that the public key type is RSA.</p> <p><i>rsa.pub</i>: Indicates the name of a public key file.</p>
Command Mode	Global configuration mode
Usage Guide	<p>This command is used to configure the RSA public key file associated with user <i>test</i>.</p> <p>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.</p>

Configuring DSA Public Key Authentication

Command	ip ssh peer <i>test</i> public-key dsaflash:<i>dsa.pub</i>
Parameter Description	<p><i>test</i>: Indicates the user name.</p> <p><i>dsa</i>: Indicates that the public key type is DSA.</p> <p><i>dsa.pub</i>: Indicates the name of a public key file.</p>

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

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

Generating a Public Key on the SSH Server

Configuration Steps	<ul style="list-style-type: none"> Run the crypto key generate { rsa dsa } command to generate a RSA public key for the server.
SSH Server	<pre>QTECH#configure terminal QTECH(config)# crypto key generate rsa</pre> <p>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.</p> <p>How many bits in the modulus [512]:</p> <ul style="list-style-type: none"> If the generation of the RSA key is successful, the following information is displayed: <pre>% Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok]</pre> If the generation of the RSA key fails, the following information is displayed: <pre>% Generating 512 bit RSA1 keys ...[fail] % Generating 512 bit RSA keys ...[fail]</pre>
Verification	<ul style="list-style-type: none"> 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	<pre> 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 OdKBCfN trOr/CT+ cs5tIGKV S0ICGifz oB+pYaE= % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEAAQAAAHJfLwKnzOgO F3RIKhTN /7PmQYoE v0a2VXTX 8ZCa7SII EghLDLJc w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISglfZ9 8o5No3Zz MPM0LnQR G4c7/28+ GOHzYkTk 4liQuTIL HRgtbyEYXCFaaxU= </pre>
------------	---

Specifying the SSH Version

Configurati on Steps	<ul style="list-style-type: none"> ▪ Run the ip ssh version { 1 2 } command to set the version supported by the SSH server to SSHv2.
SSH Server	<pre> QTECH#configure terminal QTECH(config)#ip ssh version 2 </pre>
Verification	<ul style="list-style-type: none"> ▪ Run the show ip ssh command to display the SSH version currently supported by the SSH server.
SSH Server	<pre> QTECH(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 120 secs </pre>

	<pre>Authentication retries: 3 SSH SCP Server: disabled</pre>
--	---

Configuring the SSH Authentication Timeout

Configurati on Steps	<ul style="list-style-type: none"> Run the ip ssh time-out <i>time</i> command to set the SSH authentication timeout to 100s.
SSH Server	<pre>QTECH#configure terminal QTECH(config)#ip sstime-out100</pre>
Verification	<ul style="list-style-type: none"> Run the show ip ssh command to display the configured SSH authentication timeout.
SSH Server	<pre>QTECH(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled</pre>

Configuring the Maximum Number of SSH Authentication Retries

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

Specifying the SSH Encryption Mode

Configurati on Steps	<ul style="list-style-type: none"> Run the <code>ip ssh cipher-mode {cbc ctr others }</code> command to set the encryption mode supported by the SSH server to CTR.
SSH Server	<pre>QTECH#configure terminal QTECH(config)# ip ssh cipher-mode ctr</pre>
Verification	<ul style="list-style-type: none"> 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

Configurati on Steps	<ul style="list-style-type: none"> Run the <code>ip ssh hmac-algorithm {md5 md5-96 sha1 sha1-96 }</code> command to set the message authentication algorithm supported by the SSH server to SHA1.
SSH Server	<pre>QTECH#configure terminal QTECH(config)# ip ssh hmac-algorithmsha1</pre>
Verification	<ul style="list-style-type: none"> 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


Configurati on Steps	<ul style="list-style-type: none"> Run the <code>ip ssh key-exchange { dh_group_exchange_sha1 dh_group14_sha1 dh_group1_sha1 }</code> command to configure a key exchange method on the SSH server.
SSH Server	<pre>QTECH# configure terminal QTECH(config)# ip ssh key-exchange dh_group14_sha1</pre>
Verification	<ul style="list-style-type: none"> Choose <code>diffie-hellman-group14-sha1</code> on the client terminal and check if successful login is performed.

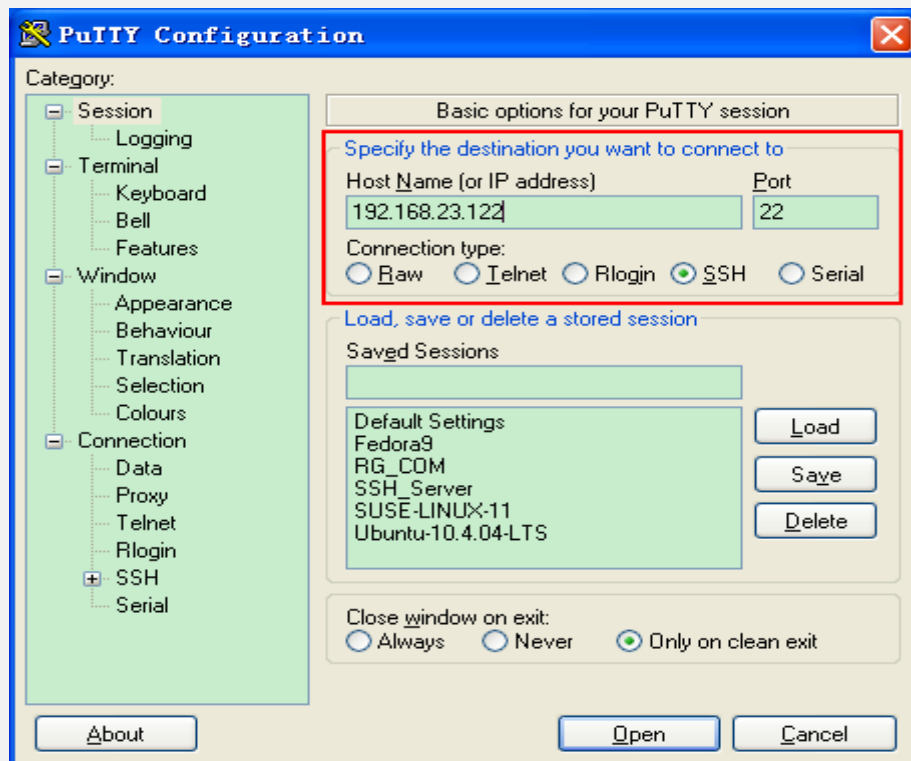
Configuring the Public Key Authentication

Configurati on Steps	<ul style="list-style-type: none"> Run the <code>ip ssh peer <i>username</i> public-key { rsa dsa } <i>filename</i></code> command to associate a public key file of the client with a user name. When the client is authenticated upon login, a public key file (for example, RSA) is specified based on the user name.
-------------------------	---

SSH Server	<pre>QTECH#configure terminal QTECH(config)# ip ssh peer test public-key rsaflash:rsa.pub</pre>
Verification	<ul style="list-style-type: none"> 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.

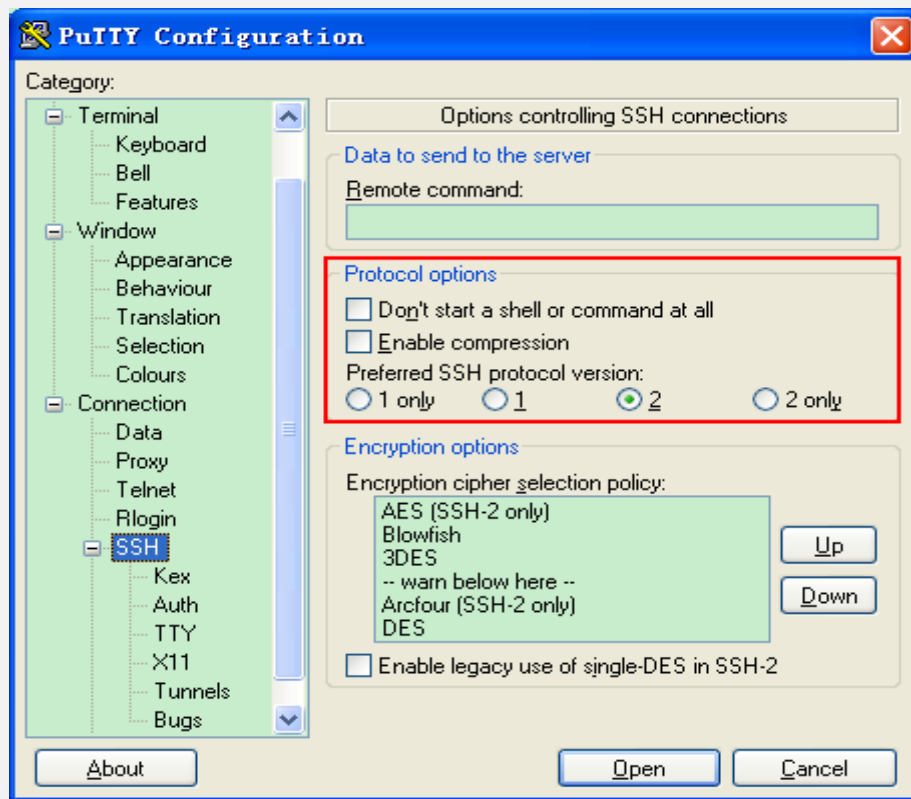
Configuring SSH Device Management

<p>Scenario Figure 7-1</p>	 <p>You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible client software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> Start the PuTTY software. On the Session option tab of PuTTY, type in the host IP address 192.168.23.122 and SSH port number 22, and select the connection type SSH. On the SSH option tab of PuTTY, select the preferred SSH protocol version 2. On the SSH authentication option tab of PuTTY, select the authentication method Attempt "keyboard-interactive" auth. Click Open to connect to the SSH server. Type in the correct user name and password to enter the terminal login interface.
<p>SSH Client</p>	<p>Figure 7-7</p>



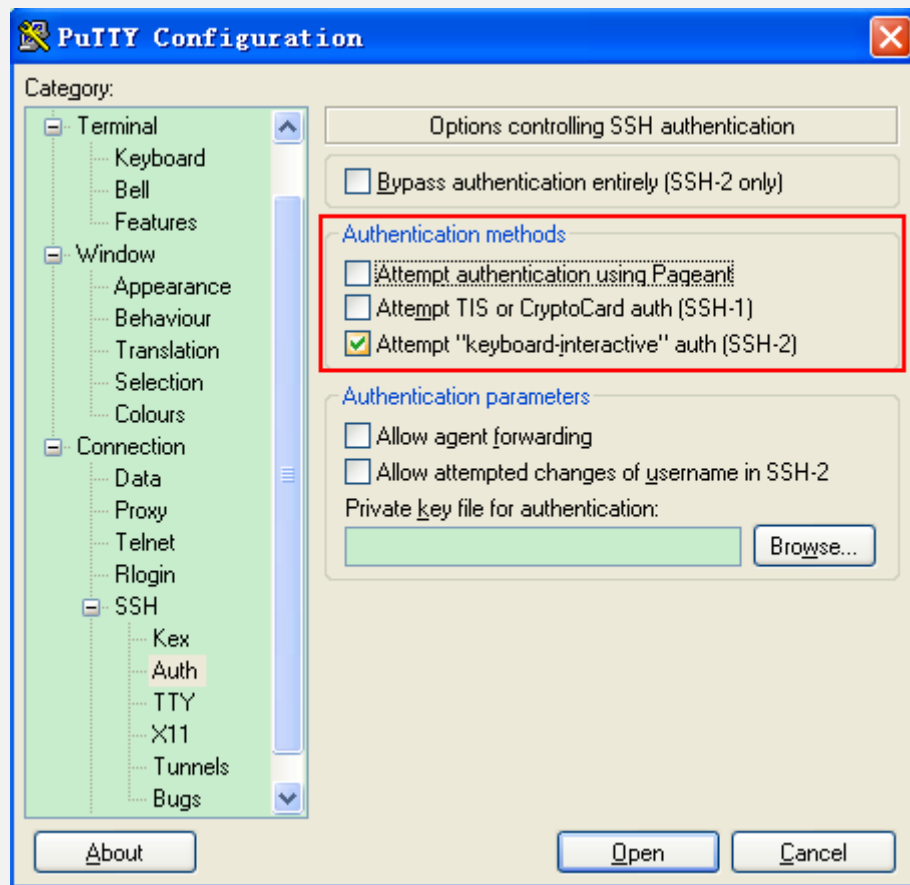
Host Name (or IP address) indicates the IP address of the host to be logged in. In this example, the IP address is **192.168.23.122**. **Port** indicates the port ID 22, that is, the default ID of the port listened by SSH. **Connection type** is **SSH**.

Figure 7-8



As shown in Figure 7-8, select **2** as the preferred SSH protocol version in the **Protocol options** pane because SSHv2 is used for login.

Figure 7-9



As shown in Figure 7-2, select **Attempt "keyboard-interactive" auth** as the authentication method to support authentication based on the user name and password.

Then, click **Open** to connect to the configured server host, as shown in Figure 7-10.

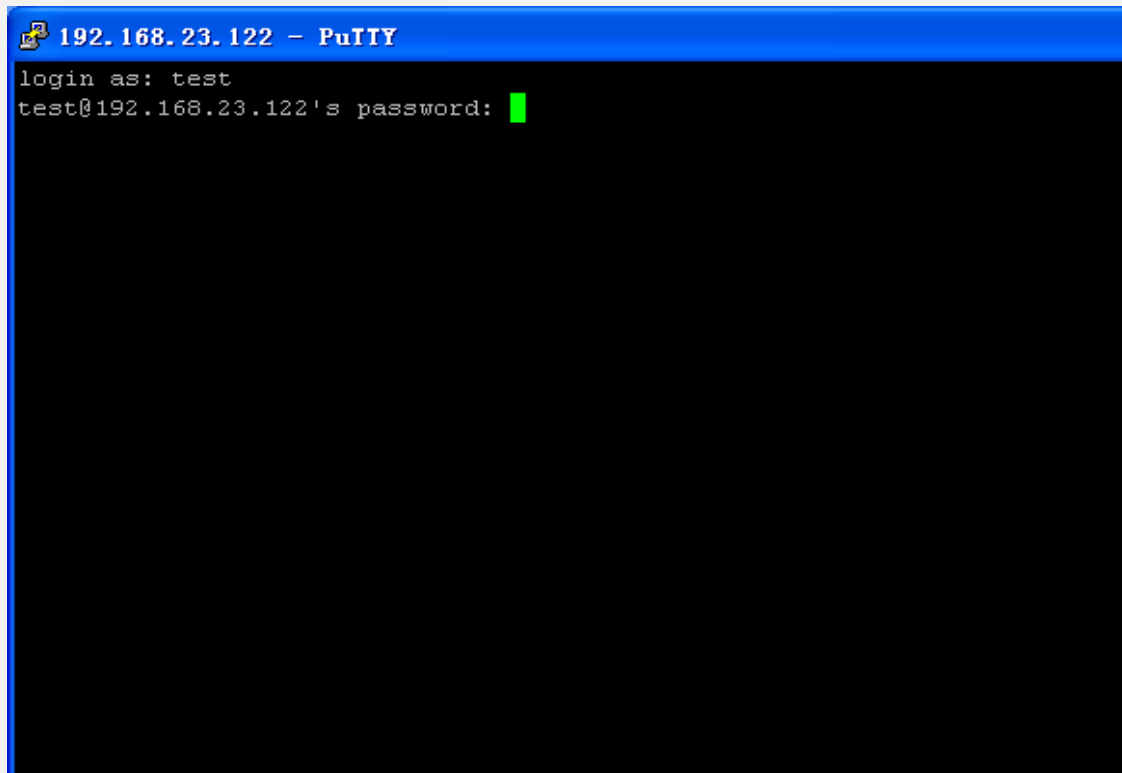
Figure 7-10



The **PuTTY Security Alert** box indicates that you are logging in to the client of the server 192.168.23.122, and asks you whether to receive the key sent from the server.

If you select **Yes**, a login dialog box is displayed, as shown in Figure 7-11.

Figure 7-11



Type in the correct user name and password, and you can log in to the SSH terminal interface, as shown in Figure 7-12.

Figure 7-12


```

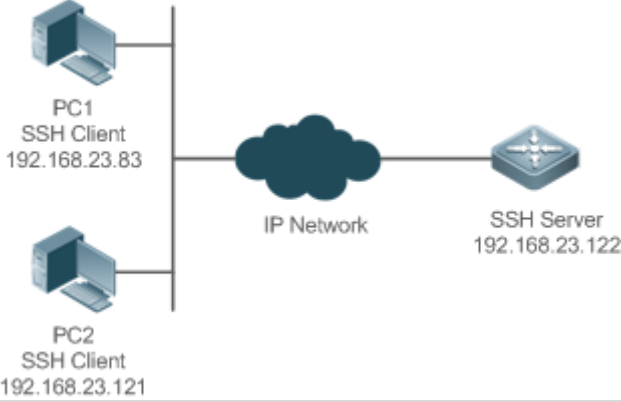
192.168.23.122 - PuTTY
login as: test
test@192.168.23.122's password:
QTECH #
    
```

- Verification**
- Run the **show ip ssh** command to display the configurations that are currently effective on the SSH server.
 - Run the **show ssh** command to display information about every SSH connection that has been established.

```

QTECH#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
QTECH#show ssh
Connection Version Encryption Hmac State Username
0 2.0 aes256-cbc hmac-sha1 Session started test
    
```

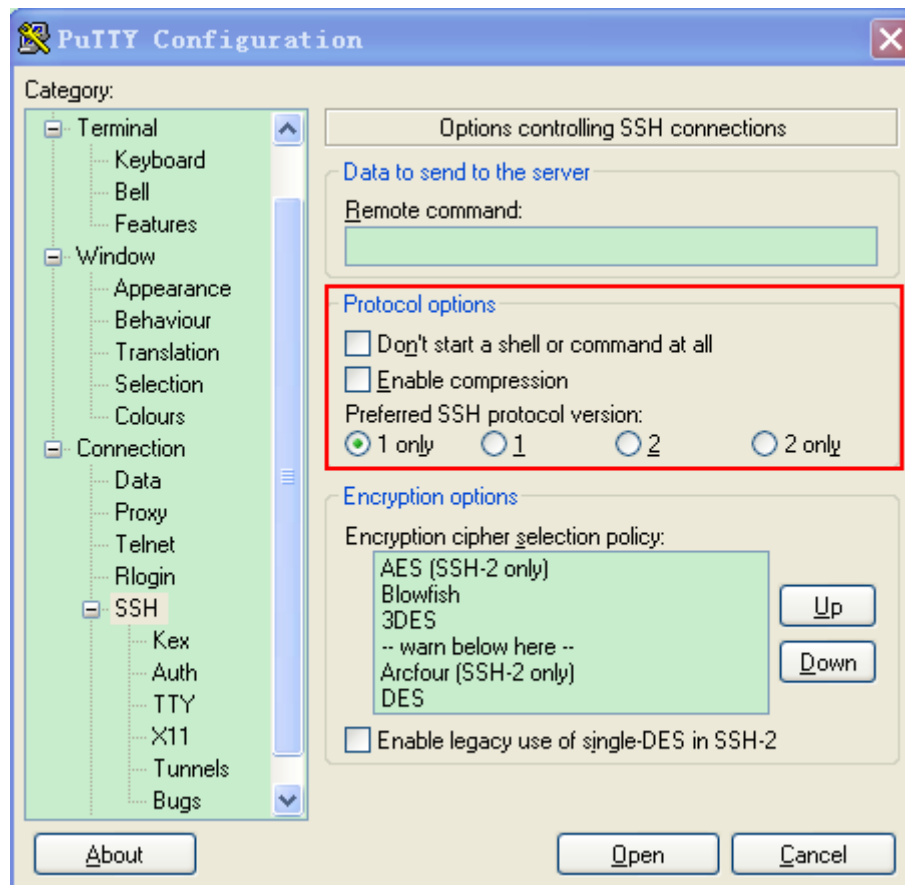
Configuring SSH Local Line Authentication

<p>Scenario Figure 7-13</p>	 <p>SSH users can use the local line password for user authentication, as shown in Figure 7-13. 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:</p> <ul style="list-style-type: none"> ▪ 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.
<p>Configuration Steps</p>	<p>Configure the SSH server as follows:</p> <ul style="list-style-type: none"> ▪ Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. ▪ Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses the RSA key, whereas SSHv2 uses the RSA or DSA key. ▪ Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server based on this IP address. The route from the SSH client to the SSH server is reachable. ▪ Configure the SSH client as follows: ▪ Diversified SSH client software is available, including PuTTY, Linux, and SecureCRT. This document takes PuTTY as an example to explain the method for configuring the SSH client. For details about the configuration method, see "Configuration Steps."
<p>SSH Server</p>	<p>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 7-14. The detailed procedures for configuring IP addresses and routes are omitted.</p> <pre>QTECH(config)# enable service ssh-server</pre>

```
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
```

SSH
Client(PC1/
PC2)

Figure 7-14



Set the IP address and port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22 (For details about the configuration method, see "Configuring SSH Device Management."). Click Open to start the SSH server. As the current authentication mode does not require a user name, you can type in any user name, but cannot leave the user name unspecified. (In this example, the user name is "anyname".)

- Verification
- Run the **show running-config** command to display the current configurations.
 - Verify that the SSH client configurations are correct.

SSH Server

```

QTECH#show running-config
Building configuration...

!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server

!
interface fastEthernet0/1
    
```

```
ip address 192.168.23.122 255.255.255.0
!
line vty 0
privilege level 15
login
password passzero
line vty 1 4
privilege level 15
login
password pass
!
end
```

SSH Client

Set up a connection, and enter the correct password. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Then, the SSH server operation interface is displayed, as shown in Figure 7-15.

Figure 7-15

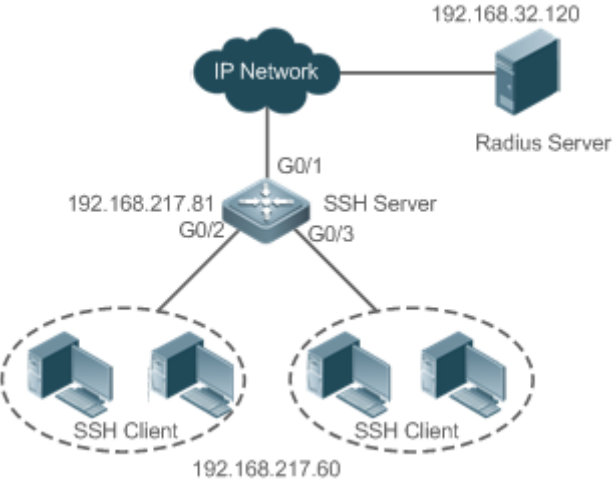


QTECH#show users

Line	User	Host(s)	Idle	Location

	* 0 con 0	---	idle	00:00:00	---
	1 vty 0	---	idle	00:08:02	192.168.23.83
	2 vty 1	---	idle	00:00:58	192.168.23.121

Configuring AAA Authentication of SSH Users

<p>Scenario</p> <p>Figure 7-16</p>	 <p>SSH users can use the AAA authentication mode for user authentication, as shown in Figure 7-16. 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.</p>
<p>Configurati on Steps</p>	<ul style="list-style-type: none"> ▪ 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.
<p>SSH Server</p>	<pre>QTECH(config)# enable service ssh-server QTECH(config)#crypto key generate rsa % You already have RSA keys.</pre>

	<pre> % 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 </pre>
Verification	<ul style="list-style-type: none"> ▪ 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 $1$hbz$ArCsyqty6yyzpz03
enable service ssh-server
!
interface gigabitEthernet1/1
 no ip proxy-arp
 ip address 192.168.217.81 255.255.255.0
!
 ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
End
```

On the SSH client, choose **System Management>Device Management**, and add the device IP address **192.168.217.81** and the device key **aaaradius**.

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

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

Configure the SSH client and set up a connection to the SSH server. For details, see the previous example.

Type in the user name **user** and password **pass**. Verify that you can log in to the SSH server successfully.

```
QTECH#show users
```

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:31	
* 1 vty 0	user	idle	00:00:33	192.168.217.60

Configuring Public Key Authentication of SSH Users

Scenario
Figure 7-17



SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in Figure 7-17. SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

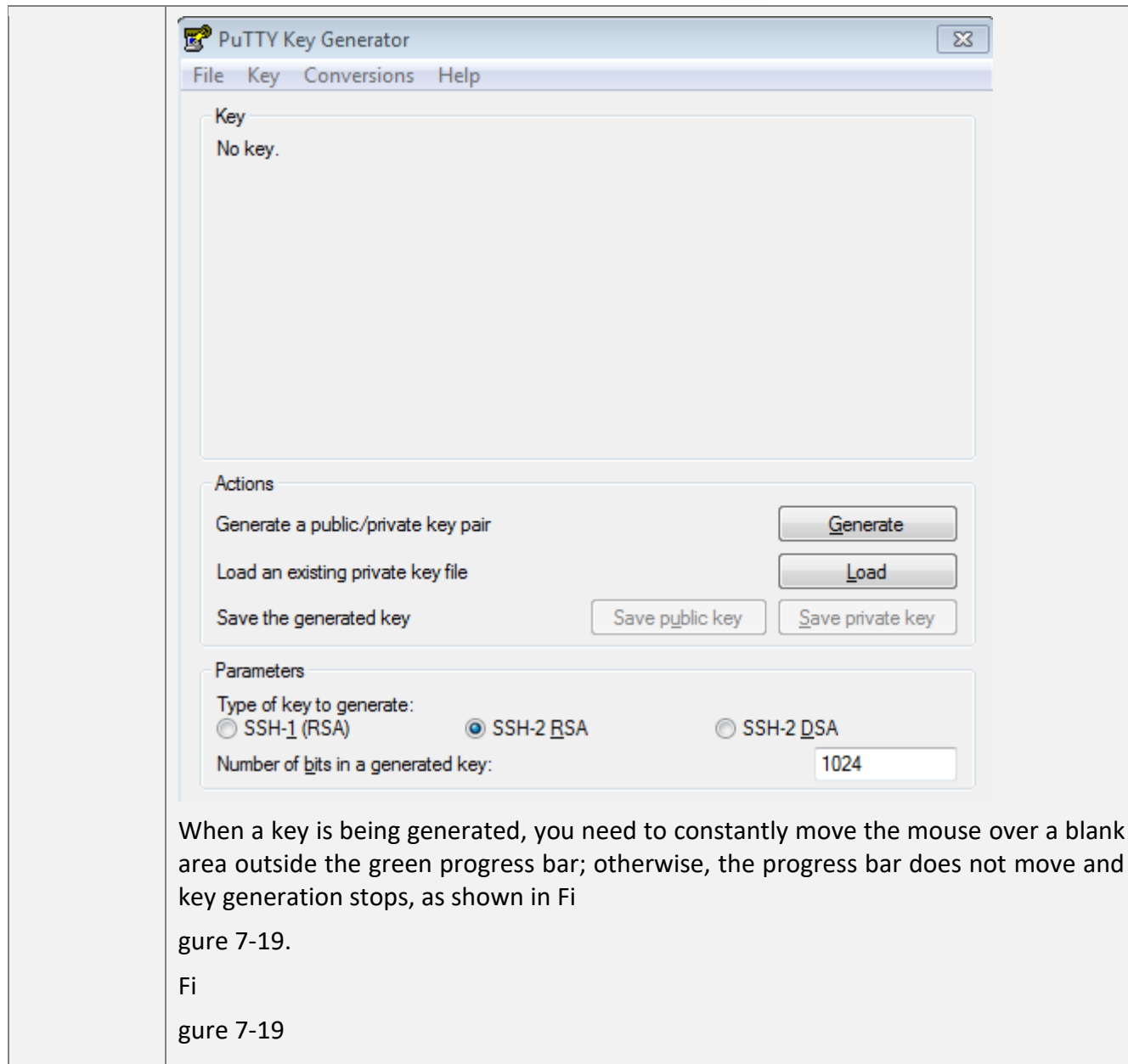
Configuration Steps

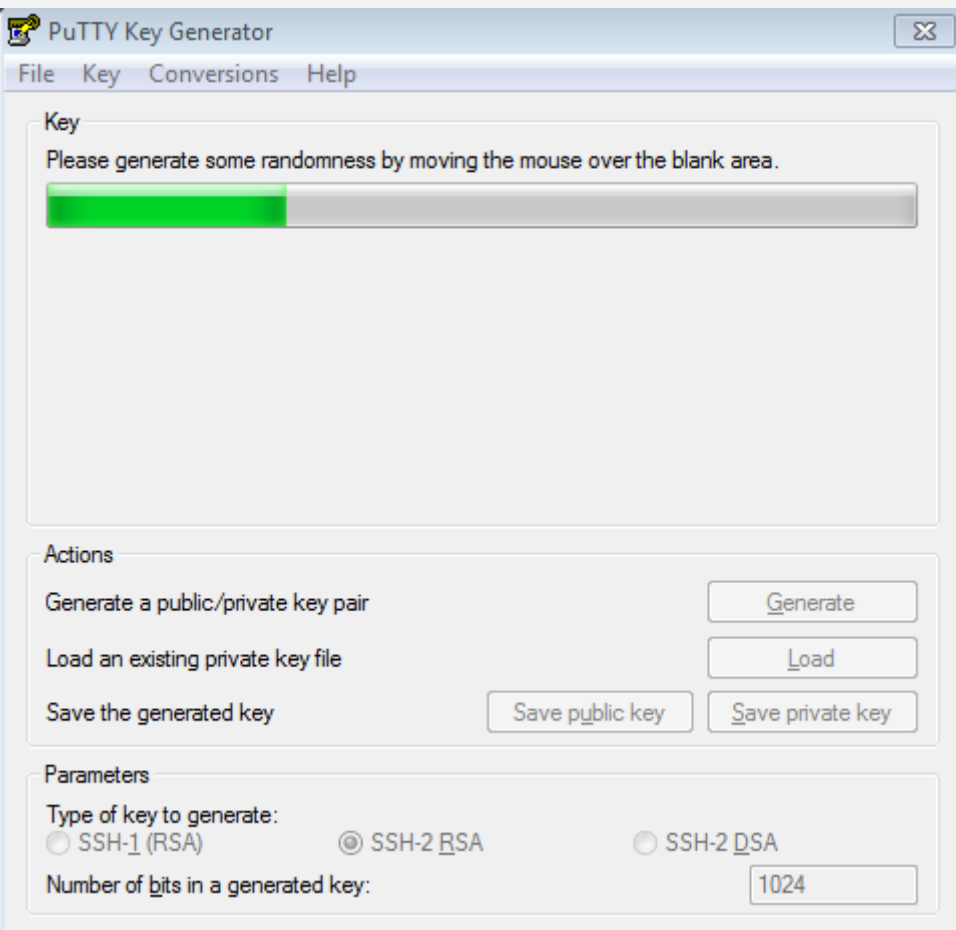
- To implement public key authentication on the client, generate a key pair (for example, RSA key) on the client, place the public key on the SSH server, and select the public key authentication mode.
- i After the key pair is generated on the client, you must save and upload the public key file to the server and complete the server-related settings before you can continue to configure the client and connect the client with the server.
- After the key is generated on the client, copy the public key file from the client to the flash of the SSH server, and associate the file with an SSH user name. A user can be associated with one RSA public key and one DSA public key.

SSH Client

Run the puttygen.exe software on the client. Select SSH-2 RSA in the Parameters pane, and click Generate to generate a key, as shown in Figure 7-18.

Figure 7-18



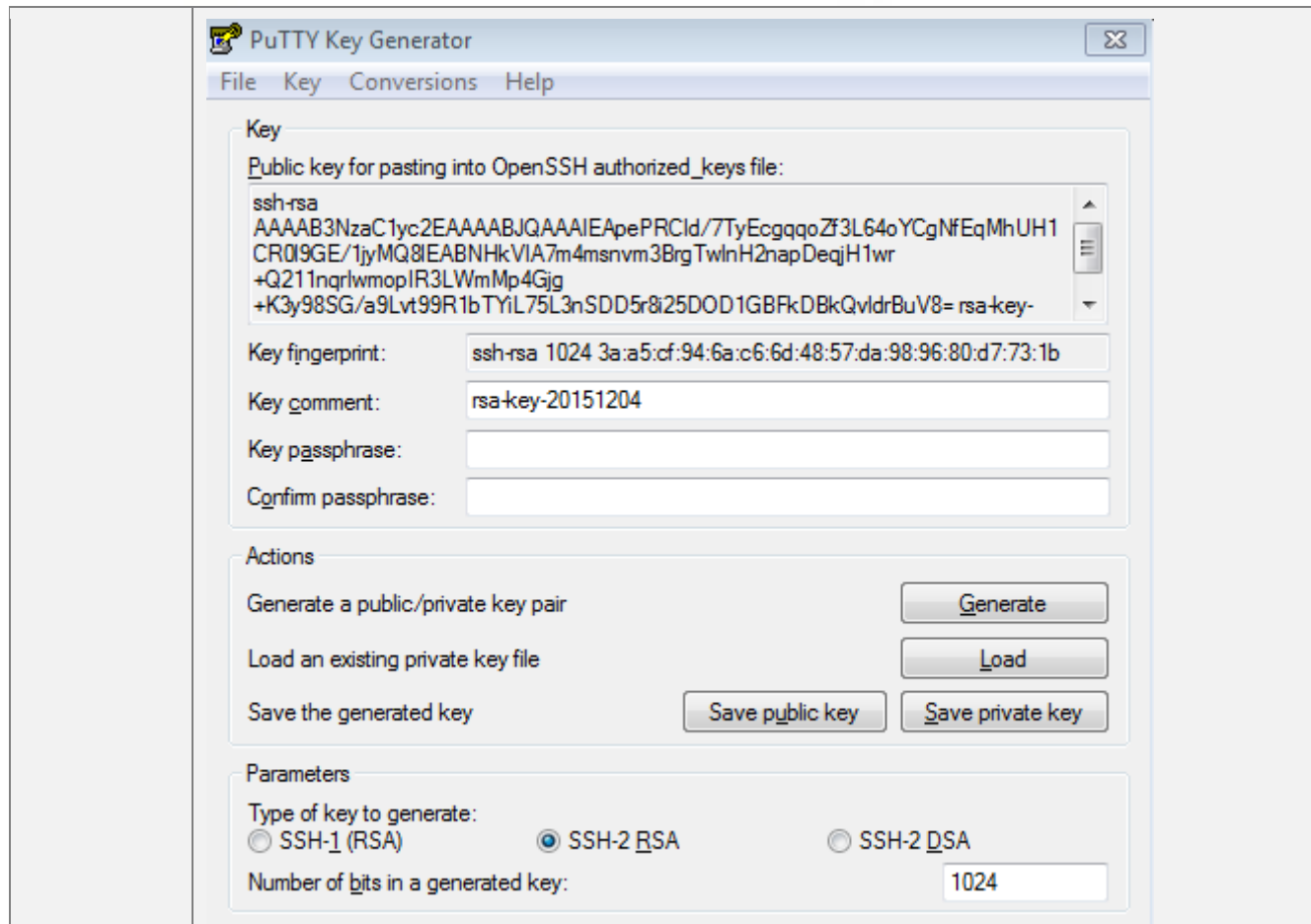


The screenshot shows the PuTTY Key Generator application window. The title bar reads "PuTTY Key Generator" with a close button. The menu bar includes "File", "Key", "Conversions", and "Help". The main area is divided into three sections: "Key", "Actions", and "Parameters".

- Key:** A text box with the instruction "Please generate some randomness by moving the mouse over the blank area." Below it is a horizontal bar with a green segment on the left.
- Actions:** Three buttons: "Generate", "Load", and "Save the generated key". The "Save the generated key" button is associated with "Save public key" and "Save private key" sub-buttons.
- Parameters:** "Type of key to generate:" with radio buttons for "SSH-1 (RSA)", "SSH-2 RSA" (selected), and "SSH-2 DSA". Below it, "Number of bits in a generated key:" is set to "1024".

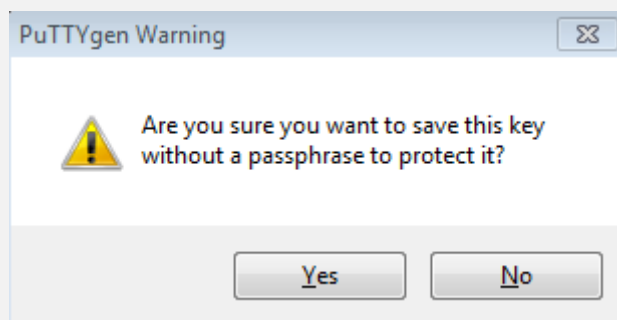
To ensure security of the RSA public key authentication, the length of the generated RSA key pair must be equal to or larger than 768 bits. In this example, the length is set to 1024 bits.

Figure 7-20



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

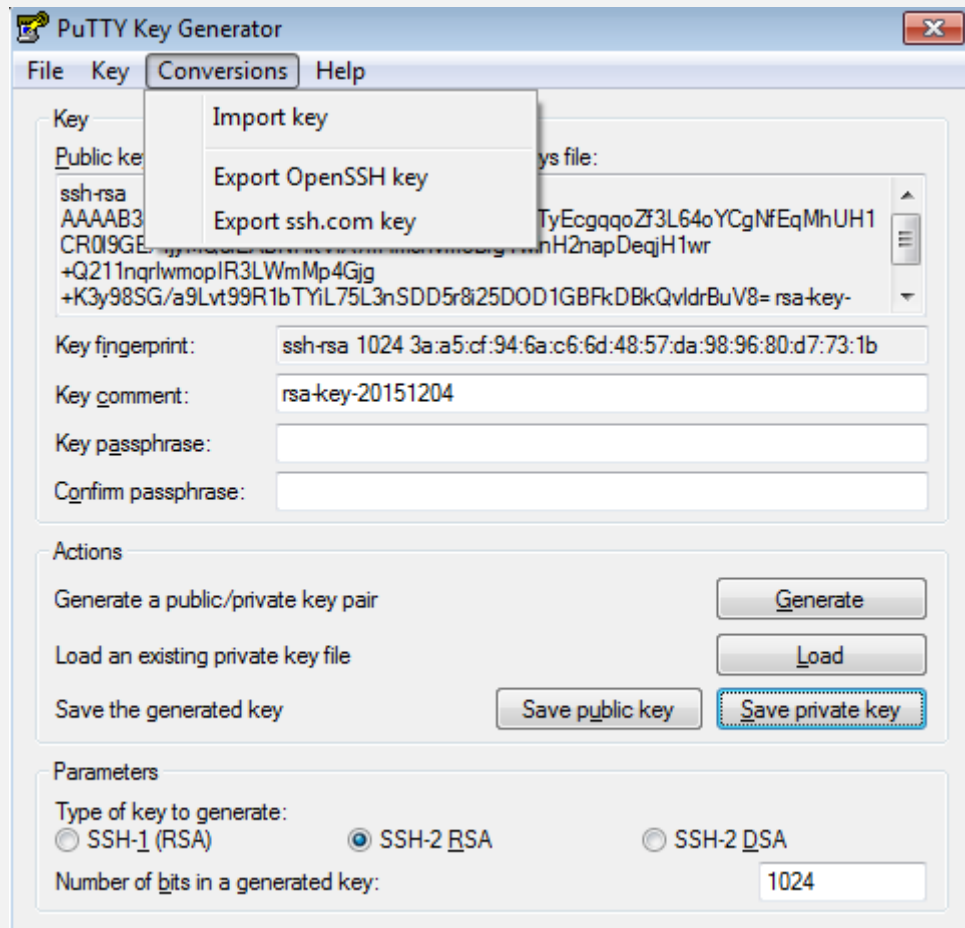
Figure 7-21



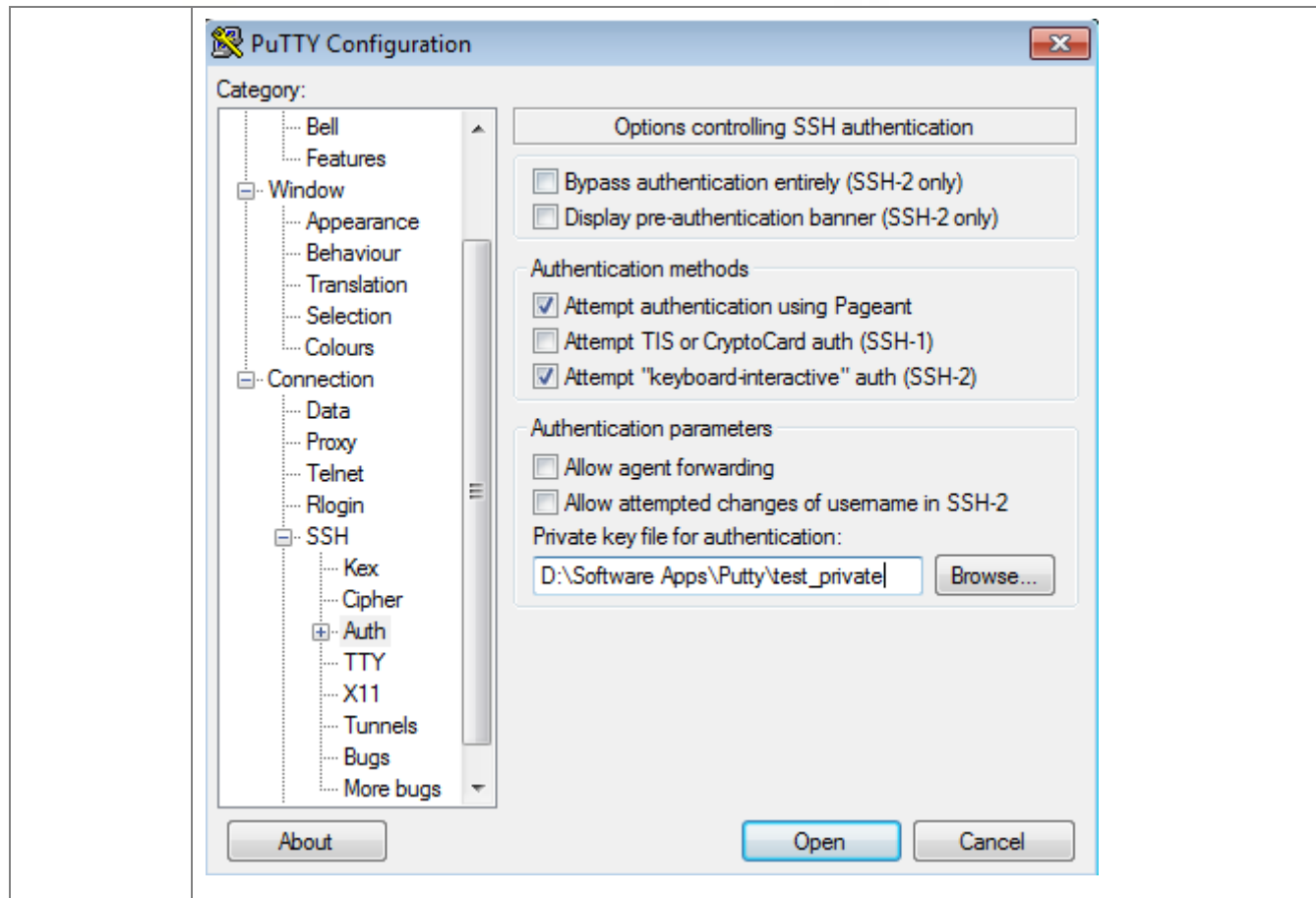
You must select the OpenSSH key file; otherwise, the key file cannot be used. The puttygen.exe software can be used to generate a key file in OpenSSH format, but this file cannot be directly used by the PuTTY client. You must use puttygen.exe to convert the private key to the PuTTY format. Format conversion is not required for the public

key file stored on the server, and the format of this file is still OpenSSH, as shown in Figure 7-20.

Figure 7-22



<p>SSH Server</p>	<pre>QTECH#configure terminal QTECH(config)# ip ssh peer test public-key rsaflash:test_key.pub</pre>
<p>Verification</p>	<ul style="list-style-type: none"> 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.
	<p>Figure 7-23</p>



Common Errors

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

7.4.2 Configuring the SCP Service

Configuration Effect

After the SCP function is enabled on a network device, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

Notes

- The SSH server must be enabled in advance.

Configuration Steps

Enabling the SCP Server

- Mandatory.
- By default, the SCP server function is disabled. Run the **ip scp server enable** command to enable the SCP server function in global configuration mode.

Verification

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

Related

Commands

Enabling the SCP Server

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

Configuration


Example

Enabling the SCP Server

Configuration Steps	<ul style="list-style-type: none"> ▪ Run the ip scp server enable command to enable the SCP server.
	<pre>QTECH#configure terminal QTECH(config)#ip scp server enable</pre>
Verification	<ul style="list-style-type: none"> ▪ Run the show ip ssh command to check whether the SCP server function is enabled.
	<pre>QTECH(config)#show ipssh SSH Enable - version 1.99 Authentication timeout: 120 secs</pre>

Authentication retries: 3
 SSH SCP Server: enabled

Configuring SSH File Transfer

<p>Scenario Figure 7-24</p>	 <p>The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ▪ Enable the SCP service on the server. <p>i The SCP server uses SSH threading. When connecting to a network device for SCP transmission, the client occupies a VTY session (You can find out that the user type is SSH by running the show user command).</p> <ul style="list-style-type: none"> ▪ On the client, use SCP commands to upload files to the server, or download files from the server. <p>Syntax of the SCP command:</p> <pre>scp [-1246BCpqr] [-c cipher] [-F ssh_config] [-i identity_file] [-l limit] [-o ssh_option] [-P port] [-S program] [[user@]host1:]file1 [...] [[user@]host2:]file2</pre> <p>Descriptions of some options:</p> <ul style="list-style-type: none"> -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). <p>For other parameters, see the filescp.0.</p>
<p>SSH Server</p>	<pre>QTECH#configure terminal QTECH(config)# ip scp server enable</pre>

Verification	<ul style="list-style-type: none"> ▪ 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.
	<pre>root@dhcpd:~#scp test@192.168.23.122:/config.text /root/config.text test@192.168.195.188's password: config.text 100% 1506 1.5KB/s 00:00 Read from remote host 192.168.195.188: Connection reset by peer</pre>

7.4.3 Configuring the SSH Client

Configuration

Effect

On the network device that supports the SSH server, enable the SSH server function, and specify the user authentication method and supported SSH versions. Then, you can use the built-in SSH client function of the device to set up a secure connection with the SSH server, implementing remote device management.

Notes

- The SSH server function must be configured in advance on the device that needs to remotely support the SSH server.
- The SSH client must communicate with the SSH server properly.

Configuration

Steps

Specifying the Source Interface of the SSH Client

- (Optional) This configuration must be performed on the SSH-client device.

Establishing a Session with the SSH Server

- (Optional) Use the **ssh** command on the client to set up a connection with a remote server.
- Before using this command, enable the SSH server function and configure the SSH key and authentication mode on the server.

Recovering an Established SSH Session

- (Optional) Run the related command to recover a session after temporary stop if necessary.

Disconnecting a Suspended SSH Session

- (Optional) This configuration must be performed on the SSH client if you need to disconnect a specified SSH session.

Verification

Run the **show ssh-session** command to display information about every established SSH client session.

Related


Commands

Specifying the Source Interface of the SSH Client

Command	ip ssh source-interface <i>interface-name</i>
Parameter Description	<i>interface-name</i> : Specifies an interface, the IP address of which will be used as the source address of an SSH client session.
Command Mode	Global configuration mode
Usage Guide	This command is used to specify an interface, the IP address of which will be used as the global source address of an SSH client session. When the ssh command is used to connect to an SSH server, this global configuration will be used if a source interface or a source address is not specified for this connection. Run the no ip ssh source-interface command to restore the default setting.

Establishing a Session with the SSH Server

Command	ssh [oob] [-v {1 2}][-c {3des aes128-cbc aes192-cbc aes256-cbc}] [-l <i>username</i>][-m {hmac-md5-96 hmac-md5-128 hmac-sha1-96 hmac-sha1-160}] [-p <i>port-num</i>][{ <i>ip-addr</i> <i>hostname</i>}[<i>via mgmt-name</i>][/source {ip <i>A.B.C.D</i> ipv6 <i>X:X:X:X::X</i> <i>interface interface-name</i>}] [/vrf <i>vrf-name</i>]
Parameter Description	<p>oob: Connects to the SSH server remotely via outband communication (generally via the MGMT interface). This option is available only when the device has the MGMT interface.</p> <p>-v: (Optional) Specifies the SSH version used for connecting to the server. SSHv2 is used by default.</p> <ul style="list-style-type: none"> ▪ 1: uses SSHv1 for connection. ▪ 2: uses SSHv2 for connection. <p>-c { 3des aes128-cbc aes192-cbc aes256-cbc }: (Optional) Specifies the data encryption algorithm, which can be the Data Encryption Standard (DES), Triple Data</p>

	<p>Encryption Standard (3DES), and Advanced Encryption Standard (AES). The AES algorithm supports three key lengths: aes128-cbc (128-bit key), aes192-cbc (192-bit key), and aes256-cbc (256-bit key).</p> <ul style="list-style-type: none"> ▪ If -c is not specified, a list of all algorithms supported by the SSH client is sent to the server during algorithm negotiation. ▪ If -c is specified, the SSH client sends only the specified encryption algorithm to the server during algorithm negotiation. If the server does not support the specified encryption algorithm, the connection will be disabled. <p>-l username: (Mandatory) Specifies the login username.</p> <p>-m { hmac-md5-96 hmac-md5-128 hmac-sha1-96 hmac-sha1-160 }: (Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm.</p> <ul style="list-style-type: none"> ▪ SSHv1 does not support HMACs. If both SSHv1 and HMACs are specified, HMACs are ignored. ▪ If -m is not specified, a list of all algorithms supported by the SSH client is sent to the server during algorithm negotiation. ▪ If -m is specified, the SSH client sends only the specified HMAC algorithm to the server during algorithm negotiation. If the server does not support the specified HMAC algorithm, the connection will be disabled. <p>-p port-num: (Optional) Specifies the ID of a port on the client for connecting to the remote server. The default port ID is 22.</p> <p>ip-addr hostname: (Mandatory) Specifies the IPv4/IPv6 address or host name of the remote server.</p> <p>via mgmt-name: Indicates the MGMT interface used when oob is specified.</p> <p>/source: Specifies the source IP address or source interface used by the SSH client.</p> <p>ip A.B.C.D: Specifies the source IPv4 address used by the SSH client.</p> <p>ipv6 X:X:X:X: Specifies the source IPv6 address used by the SSH client.</p> <p>interface interface-name: Specifies the source interface used by the SSH client.</p> <p>/vrf vrf-name: Specifies the VRF routing table used for searches.</p>
Command Mode	User EXEC mode
Usage Guide	<p>The ssh command is used to set up a secure and encrypted connection from the local device (an SSH client) to another device (an SSH server) or any other server that supports SSHv1 or SSHv2. This connection provides a mechanism similar to the Telnet connection except that all data transmitted over this connection is encrypted. Based on authentication and encryption, the SSH client can set up a secure connection on an insecure network.</p> <hr/> <p> SSHv1 supports only the DES (56-bit key) and 3DES (168-bit key) encryption algorithms.</p>

- ⚠ SSHv2 supports the following Advanced Encryption Standards (AES): AES128-CBC, AES192-CBC, AES256-CBC, AES128-CTR, AES192-CTR, and AES256-CTR.
- ⚠ SSHv1 does not support the Hashed Message Authentication Code (HMAC).
- ⚠ If you specify an unmatched encryption or authentication algorithm when selecting an SSH version, the unmatched algorithm will be ignored when a connection is set up.

Recovering an Established SSH Client Session

Command	ssh-session <i>session-id</i>
Parameter Description	<i>session-id</i> : Indicates the ID of an established SSH client session.
Command Mode	User EXEC mode
Usage Guide	This command is used to restore the use of an established SSH client session. When the ssh command is used to initiate an SSH client session, you can press Ctrl+Shift+6+X to temporarily exit the session. To recover this session, run the ssh-session command. In addition, if the session is already established, you can run the show ssh-session command to display information about the established session.

Disconnecting a Suspended SSH Session

Command	disconnect ssh-session <i>session-id</i>
Parameter Description	<i>session-id</i> : Indicates the ID of a suspended SSH client session.
Command Mode	User EXEC mode
Usage Guide	You can specify an SSH client session ID to disconnect the specified SSH client session.


Configuration

Example

Specifying the Source Interface of the SSH Client

Configurati on Steps	<ul style="list-style-type: none"> Run the <code>ip ssh source-interface <i>interface-name</i></code> command to specify an interface, the IP address of which will be used as the global source address of an SSH client session.
	<pre>QTECH#configure terminal QTECH(config)#ipsshsource-interface gigabitEthernet 0/1</pre>
Verification	N/A

Establishing a Session with the SSH Server

Scenario Figure 7-25	 <p>The SSH server function is enabled on the server. The <code>ssh</code> command is used on the client to set up a secure connection with the server.</p>
Configurati on Steps	<ul style="list-style-type: none"> Enable the SSH server function on the server. Configure the SSH key on the server. Configure the authentication mode of the SSH server, and use the local line authentication mode for Line 0 to Line 4. Configure the IP address of the Gi 0/1 interface of the SSH server. The client will use this address as the source address to connect to the SSH server. Configure the SSH client, and specify the source address of the SSH client. <p>i By default, the SSH server supports two SSH versions: SSHv1 and SSHv2.</p> <p>i 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 an RSA key, whereas SSHv2 uses an RSA or DSA key.</p> <p>i The authentication mode used by the SSH server is local line authentication. The local user name is admin, and the password is 123456.</p> <p>i The SSH client is connected to the SSH server based on this IP address. The routes from the SSH clients to the SSH server are reachable.</p> <p>i Configure the IP address of the Gi 0/1 interface of the SSH server. The client will use this address as the source address to connect to the SSH server.</p>
SSH Server	<pre>QTECH#configure terminal QTECH(config)#enable service ssh-server</pre>

	<pre> 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)#line vty 0 4 QTECH(config-line)#login local QTECH(config-line)#exit QTECH(config)#username admin password 123456 QTECH(config)#username admin privilege 15 QTECH(config-line)#exit QTECH(config)#interface gigabitEthernet0/1 QTECH(config-if-gigabitEthernet0/1)#ip address 192.168.23.122 255.255.255.0 QTECH(config-if-gigabitEthernet0/1)#exit </pre>
SSH Client	<pre> QTECH(config)#interface gigabitEthernet0/1 QTECH(config-if-gigabitEthernet0/1)#ip address 192.168.23.83 255.255.255.0 QTECH(config-if-gigabitEthernet0/1)#exit QTECH(config)#ipsshsource-interface gigabitEthernet 0/1 </pre>
Verification	<ul style="list-style-type: none"> ▪ Run the show running-config include username and show ip ssh commands to verify whether the SSH server configurations are correct. ▪ On the SSH client, set up a connection with a remote SSH server. After the connection is set up, type in the correct password 123456. The SSH server operation interface is displayed. Check the login user on the Console of the SSH client.
	<pre> QTECH(config)#sh running-config include username username admin password admin username admin privilege 15 QTECH(config)#sh running-config begin line </pre>

	<pre>line con 0 line vty 0 4 login local ! ! end</pre>
	<ul style="list-style-type: none"> Verify whether the SSH client configurations are correct.
	<pre>QTECH#ssh -l admin 192.168.23.122 %Trying 192.168.23.122, 22,...open admin@192.168.23.122's password: QTECH# QTECH#sh users Line User Host(s) Idle Location 0 con 0 idle 00:00:00 * 1 vty 0 admin idle 00:00:36 192.168.217.20</pre>

7.4.4 Configuring SCP Client

Configuration

Effect

On the network device that supports the SCP server, enable the SCP service so that users can directly download files from the network device and upload local files to the network device. In addition, all exchanged data is encrypted, featuring authentication and security.

Notes

- The SSH server function must be configured and the SCP service must be enabled on the device in order to remotely support the SCP server.
- The SCP client must communicate with the SCP server properly.

Configuration

Steps

Specifying Source Interface of SCP Client

- (Optional) Specify a source interface of the SCP client.

Implementing File Transfer with SCP Server via SCP Client

- (Optional) Run the **scp** command to implement file transfer with the remote SCP server via the SCP client.
- Before running this command, enable the SSH server function, configure an SSH key and authentication mode, and enable the SCP server function.

Verification

Check whether file transfer is successful.

Related

Commands

Specifying Source Interface of SCP Client

Command	ip scp client source-interface <i>interface-name</i>
Parameter Description	<i>interface-name</i> : Indicates a source interface. Set the IP address of the interface to the source IP address of the SCP client.
Command Mode	Global configuration mode
Usage Guide	Run this command to specify the IP address of the designated interface as the global source address of the SCP client. During interaction with the remote SSH server via the scp command, global settings are used if no source interface or source address is specified. Run the no ip ssh source-interface command to restore the default settings.

Implementing File Transfer with SCP Server via SCP Client

Command	scp [oob] [-v { 1 2 }] [-c { 3des aes128-cbc aes192-cbc aes256-cbc }] [-m { hmac-md5-96 hmac-md5-128 hmac-sha1-96 hmac-sha1-160 }] [-p <i>port-num</i>] { <i>filename</i> <i>username@host:/filename</i> <i>username@host:/filename filename</i> } [via <i>mgmt-name</i>] [/source { ip <i>A.B.C.D</i> ipv6 <i>X:X:X:X::X</i> interface <i>interface-name</i> }] [/vrf <i>vrf-name</i>]
Parameter Description	<p>oob: Connects to the SCP server remotely via outband communication (generally via the MGMT interface). This option is available only when the device has the MGMT interface.</p> <p>-v: (Optional) Specifies the SSH version used for connecting to the server. SSHv2 is used by default.</p> <ul style="list-style-type: none"> ▪ 1: uses SSHv1 for connection.

- **2:** uses SSHv2 for connection.

-c { 3des | aes128-cbc | aes192-cbc | aes256-cbc }: (Optional) Specifies the data encryption algorithm, which can be the Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). The AES algorithm supports three key lengths: aes128-cbc (128-bit key), aes192-cbc (192-bit key), and aes256-cbc (256-bit key).

- If **-c** is not specified, a list of all algorithms supported by the SSH client is sent to the server during algorithm negotiation.
- If **-c** is specified, the SSH client sends only the specified encryption algorithm to the server during algorithm negotiation. If the server does not support the specified encryption algorithm, the connection will be disabled.

-m { hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 }: (Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm.

- SSHv1 does not support HMACs. If both SSHv1 and HMACs are specified, HMACs are ignored.
- If **-m** is not specified, a list of all algorithms supported by the SCP client is sent to the server during algorithm negotiation.
- If **-m** is specified, the SCP client sends only the specified HMAC algorithm to the server during algorithm negotiation. If the server does not support the specified HMAC algorithm, the connection will be disabled.

-p port-num: (Optional) Specifies the ID of a port on the client for connecting to the remote server. The default port ID is 22.

filename username@host:/filename | username@host:/filename filename: (Mandatory) **filename username@host:/filename** indicates uploading a file from the device to the remote SCP server.

username@host:/filename filename indicates downloading a file from the remote SCP server to the device.

Files on the device support the following storage media:

flash:/filename: extended flash memory

flash2:/filename: extended flash memory 2

usb0:/filename: extended USB flash drive 0. It is supported only when the device has one USB port and an extended USB flash drive is inserted.

usb1:/filename: extended USB flash drive 1. It is supported only when the device has two USB ports and extended USB flash drives are inserted.

sd0:/filename: extended SD card. It is supported only when the device has one SD card port and an extended SD card is inserted.

sata0:/filename: extended hard disk device.

tmp:/filename: temporary directory **tmp/vsd/**.

ip-addr | hostname: (Mandatory) Specifies the IPv4/IPv6 address or host name of the remote server.

via mgmt-name: Indicates the MGMT interface used when **oob** is specified.

/source: Specifies the source IP address or source interface used by the SCP client.

	<p>ip A.B.C.D: Specifies the source IPv4 address used by the SCP client.</p> <p>ipv6 X:X:X:X::X: Specifies the source IPv6 address used by the SCP client.</p> <p>interface <i>interface-name</i>: Specifies the source interface used by the SCP client.</p> <p>/vrf <i>vrf-name</i>: Specifies the VRF routing table used for searches.</p>
Command Mode	Common user mode
Usage Guide	Run the scp command to establish a secure and encrypted connection from the local device (SCP client) to another device (SCP server) to implement file transfer.


Configuration

Example

Specifying Source Interface of SCP Client

Configuration Steps	<ul style="list-style-type: none"> Run the ip scp client source-interface <i>interface-name</i> command to specify the IP address of the interface as the global source address of the SCP client.
	<pre>QTECH# configure terminal QTECH(config)# ip scp client source-interface gigabitEthernet 0/1</pre>
Verification	N/A

Implementing File Transfer with SCP Server via SCP Client

<p>Scenario Figure 7-3</p>	 <p>Enable the SSH server and SCP server functions on the server end, and run the scp command on the SCP client to implement file transfer with the server.</p>
Configuration Steps	<ul style="list-style-type: none"> Enable the SSH server function on the server end. Configure an SSH key on the server end. Configure an authentication mode for the SSH server, and configure the local authentication mode for lines 0 to 4. Enable the SCP server function. Configure the IP address of the Gi 0/1 interface of the SSH server, so that the client uses this address as the source address to connect to the SSH server. Configure the SSH client, and specify the source address of the SSH client.

	<ul style="list-style-type: none"> i By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. i 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 an authentication success or failure message. SSHv1 uses an RSA key, while SSHv2 uses an RSA or DSA key. i The SSH server uses the local authentication mode. The local username is admin, and the password is 123456. i The SSH client connects to the SSH server at this IP address. The route from the SSH client to the SSH server is reachable. i Configure the IP address of the Gi 0/1 interface of the SSH client, so that the client uses this address as the source address to connect to the SSH server.
SCP Server	<pre> QTECH# configure terminal 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)#line vty 0 4 QTECH(config-line)#login local QTECH(config-line)#exit QTECH(config)#username admin password 123456 QTECH(config)#username admin privilege 15 QTECH(config-line)#exit QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.23.122 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit </pre>
SSH Client	<pre> QTECH(config)#interface gigabitEthernet 0/1 </pre>

	<pre>QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.23.83 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit QTECH(config)# ip scp server enable QTECH(config)#ip ssh source-interface gigabitEthernet 0/1</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ▪ Run the show running-config include username and show ip ssh commands to verify the SSH server configuration. ▪ On the SSH client, set up a connection with the remote SSH server. After the connection is set up, enter the password 123456. The SSH server operation interface is displayed. Check the logged-in user on the console of the SSH client.
	<pre>QTECH(config)#sh running-config include username username admin password admin username admin privilege 15 QTECH(config)#sh running-config begin line line con 0 line vty 0 4 login local ! ! end</pre>
	<ul style="list-style-type: none"> ▪ Verify the SCP client configuration.
	<pre>QTECH#scp config.text admin@192.168.23.122:/config.text %Trying 192.168.23.122, 22,...open admin@192.168.23.122's password: QTECH#</pre>

7.5 Monitoring

Displaying

Description	Command
-------------	---------

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

Debugging

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

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

8 CONFIGURING URPF

8.1 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

8.2 Applications

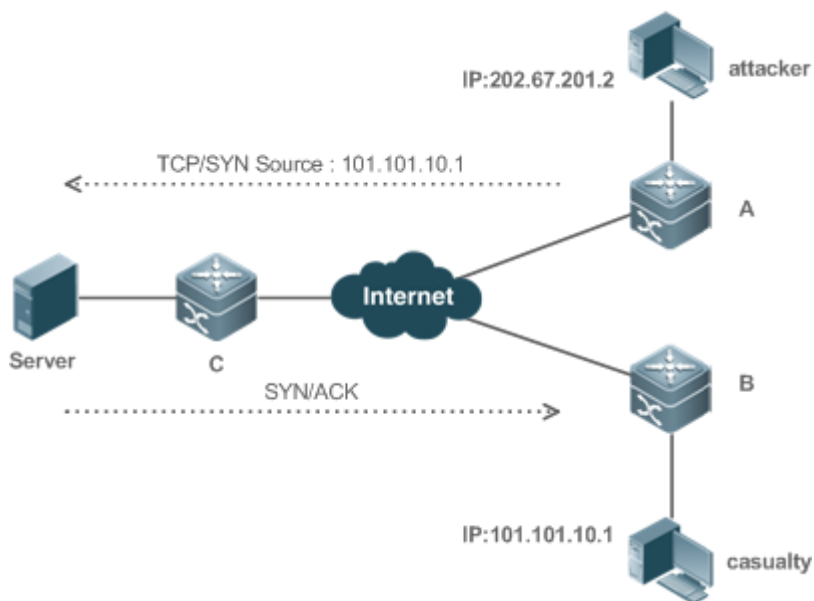
Application	Description
Strict Mode	Block the packets with spoofed sourced addresses at the access layer or aggregation layer to prevent sending these packets from PCs to the core network.
Loose Mode	On a multihomed network, the user network is connected to multiple Internet service providers (ISPs), 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.

8.2.1 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 8-1



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.

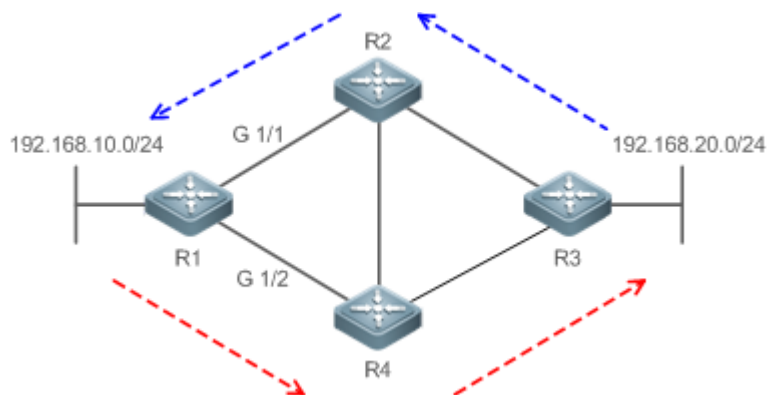
8.2.2 Loose Mode

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 8-2, 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 8-2



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.

8.3 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.

8.3.1 Enabling URPF

Enable URPF to perform a URPF check on IP 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 an IPv4/IPv6 unicast address, and is not checked if the packet is a multicast packet or an IP 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 is performed on packets received on the configured interface. Configurations in interface configuration mode and those in global configuration mode cannot coexist.

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

✔ A switch supports configuration of URPF on a routed port of L3 aggregate port (AP). In some cases, the configuration is also supported on an SVI. The following constraints exist:

- URPF does not support association with the ACL option.
- 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 URPF function for a specified interface.

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

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

8.3.2 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 monitoring the URPF packet loss information is disabled.



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

Configuring the Threshold of the URPF Packet Loss Rate

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

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

8.4 Configuration

Configuration Item	Description and Command		
Enabling URPF	 (Mandatory) It is used to enable URPF.		
	<table border="1"> <tr> <td><code>ip verify unicast source reachable-via { rx any } [allow-default] [<i>acl_name</i>] (Interface configuration mode)</code></td> <td>Enables URPF for a specified interface.</td> </tr> </table>	<code>ip verify unicast source reachable-via { rx any } [allow-default] [<i>acl_name</i>] (Interface configuration mode)</code>	Enables URPF for a specified interface.
<code>ip verify unicast source reachable-via { rx any } [allow-default] [<i>acl_name</i>] (Interface configuration mode)</code>	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.		
	<table border="1"> <tr> <td><code>ip verify urpf drop-rate compute interval <i>seconds</i></code></td> <td>Configures the calculation interval of the URPF packet loss rate.</td> </tr> </table>	<code>ip verify urpf drop-rate compute interval <i>seconds</i></code>	Configures the calculation interval of the URPF packet loss rate.
	<code>ip verify urpf drop-rate compute interval <i>seconds</i></code>	Configures the calculation interval of the URPF packet loss rate.	
	<table border="1"> <tr> <td><code>ip verify urpf drop-rate notify</code></td> <td>Configures the function of monitoring URPF packet loss information.</td> </tr> </table>	<code>ip verify urpf drop-rate notify</code>	Configures the function of monitoring URPF packet loss information.
<code>ip verify urpf drop-rate notify</code>	Configures the function of monitoring URPF packet loss information.		
<table border="1"> <tr> <td><code>ip verify urpf drop-rate notify hold-down <i>seconds</i></code></td> <td>Configures the alarm interval of the URPF packet loss rate.</td> </tr> </table>	<code>ip verify urpf drop-rate notify hold-down <i>seconds</i></code>	Configures the alarm interval of the URPF packet loss rate.	
<code>ip verify urpf drop-rate notify hold-down <i>seconds</i></code>	Configures the alarm interval of the URPF packet loss rate.		
<table border="1"> <tr> <td><code>ip erify urpf notification threshold <i>rate-value</i></code></td> <td>Configures the threshold of the URPF packet loss rate.</td> </tr> </table>	<code>ip erify urpf notification threshold <i>rate-value</i></code>	Configures the threshold of the URPF packet loss rate.	
<code>ip erify urpf notification threshold <i>rate-value</i></code>	Configures the threshold of the URPF packet loss rate.		

8.4.1 Enabling URPF

Configuration

Effect

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

Configuration

Steps

Enabling IPv4 URPF for a Specified Interface

- Mandatory.

Verification

Enable URPF and check the source address as follows:

- If the strict mode is used, check whether a packet is forwarded only when the forwarding table contains the source address of the received IP 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 IP packet; otherwise, the packet is dropped.

Related

Commands

Enabling IPv4 URPF for a Specified Interface

Command	<code>ip verify unicast source reachable-via { rx any } [allow-default] [acl-id]</code>
Parameter Description	<p>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.</p> <p>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.</p> <p>allow-default: (Optional) Indicates that the default route can be used for the URPF check.</p> <p>acl-id: (Optional) Indicates the ID of the ACL. Values include 1 to 99 (IP standard access list), 100 to 199 (IP extended access list), 1300 to 1999 (IP standard access list, expanded range), and 2000 to 2699 (IP extended access list, expanded range).</p>
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. If the ACL (*acl-name*) is configured, the packet is matched against the ACL after it fails in the URPF check. If no ACL exists, or a packet matches a deny ACE, the packet will be dropped. If the packet matches a permit ACE, the packet will be forwarded.

i A switch supports configuration of URPF on a routed port or L3 AP port. In addition, the following constraints exist:

1. URPF does not support association with the ACL option.
2. 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.
3. After URPF is enabled, the route forwarding capacity of the device will be reduced by half.
4. 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.
5. If URPF is configured in global configuration mode, the default route cannot be used for the URPF check.

i URPF configured in global configuration mode is mutually exclusive with URPF configured in interface configuration mode.

Configuration

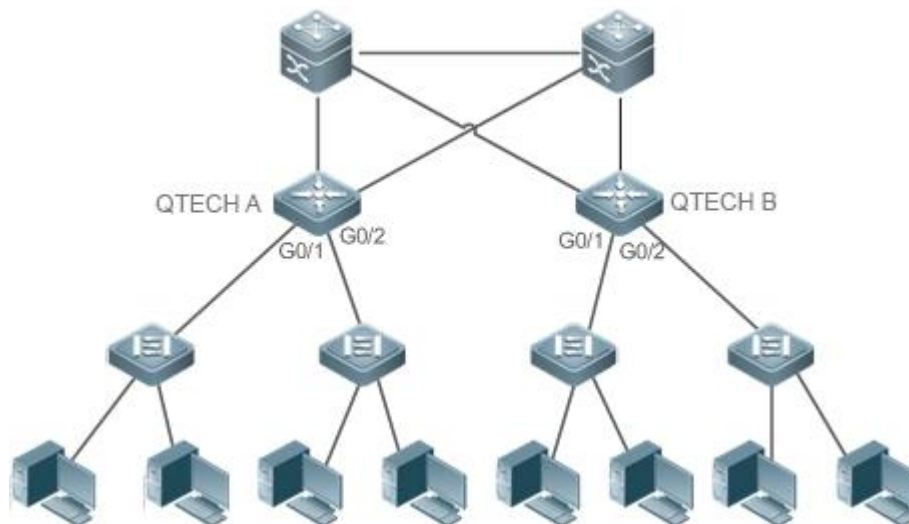
Example

Configuring the Strict Mode

Block the packets with spoofed sourced addresses at the access layer or aggregation layer to prevent sending these packets from PCs to the core network.

To meet the preceding requirement, enable URPF in strict mode on the interface between the aggregation device and the access device.

Scenario
Figure 8-3



Verification

As shown in Figure 8-3, 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
```

	<pre> 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 </pre>
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	<pre> 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 </pre>
B	<pre> 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 </pre>

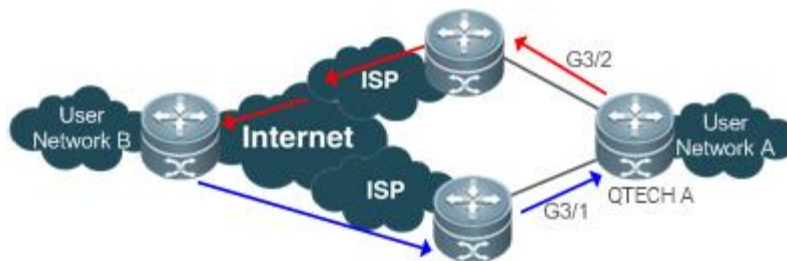

```

IP verify source reachable-via RX
IP verify URPF drop-rate notify enabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 250
Number of drop-rate notification counts in this interface is 0
    
```

Configuring the Loose Mode

On the egress device 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 8-4



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
```

8.4.2 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 <i>seconds</i>
Parameter Description	interval <i>seconds</i> : 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 <i>seconds</i>
Parameter Description	hold-down <i>seconds</i> : 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 <i>rate-value</i>
Parameter Description	threshold <i>rate-value</i> : 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.
---------------------	---

	<pre>QTECH#configure terminal QTECH(config)# ip verify urpf drop-rate compute interval 120 QTECH(config)# end</pre>
Verification	Run the show ip urpf command to check whether the configuration takes effect.
	<pre>QTECH# show ip urpf IP verify URPF drop-rate compute interval is 120s</pre>

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

Configurati on Steps	Set the alarm interval of the URPF packet loss rate to 120s in global configuration mode. The configuration takes effect on both IPv4 URPF and IPv6 URPF.
	<pre>QTECH#configure terminal QTECH(config)# ip verify urpf drop-rate notify hold-down 120 QTECH(config)# end</pre>
Verification	Run the show ip urpf command to check whether the configuration takes effect.
	<pre>QTECH# show ip urpfIP verify URPF drop-rate notify hold-down is 120s</pre>

8.5 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.	<code>clear ip urpf [interface <i>interface-name</i>]</code>

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

9 CONFIGURING CPP

9.1 Overview

The CPU Protect Policy (CPP) provides policies for protecting the CPU of a switch.

In network environments, various attack packets spread, which may cause high CPU usages of the switches, affect protocol running and even difficulty in switch management. To this end, switch CPUs must be protected, that is, traffic control and priority-based processing must be performed for various incoming packets to ensure the processing capabilities of the switch CPUs.

CPP can effectively prevent malicious attacks in the network and provide a clean environment for legitimate protocol packets.

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

9.2 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.

9.2.1 Preventing Malicious Attacks

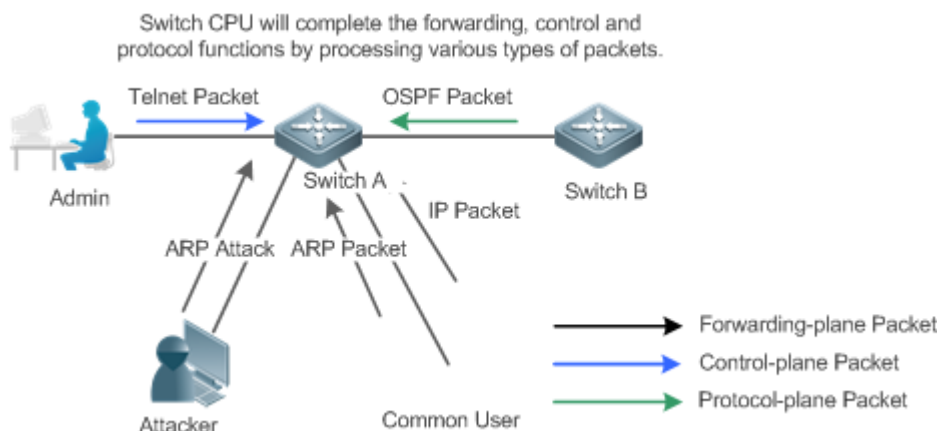
Scenario

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

As shown in Figure 9-1, 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 9-1, 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 9-1 Networking Topology of Switch Services and Attacks



Deployment

- By default, CPP classifies ARP packets, Telnet packets, IP route disconnection packets, and OSPF packets into queues of different priorities. In this way, ARP packets will not affect other packets.
- By default, CPP limits the rates of ARP packets and the rates of the priority queue where the ARP packets reside to ensure that the attack packets do not occupy too many CPU resources.
- Packets in the same priority queue with ARP packets may be affected by ARP attack packets. You can divide the packets and the ARP packets into different priority queues by means of configuration.
- When ARP attack packets exist, CPP cannot prevent normal ARP packets from being affected. CPP can only differentiate the packet type but cannot distinguish attack packets from normal packets of the same type. In this case, the Network Foundation Protection Policy (NFPP) function can be used to provide higher-granularity attack prevention.

i For description of NFPP configurations, see the *Configuring NFPP*.

9.2.2 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.

9.3 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.

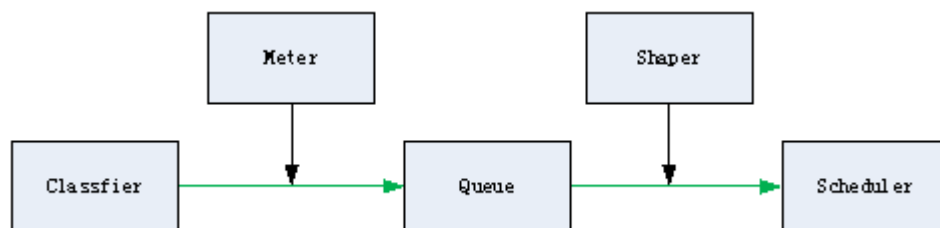
CPU interface

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 9-2 CPP Implementation Model



Feature	Description
Classifier	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.

9.3.1 Classifier

Working Principle

The Classifier classifies all packets to be sent to the CPU based on the L2, L3 and L4 information of the packets. Classifying packets is the basis for implementing QoS policies. In subsequent actions, different policies are implemented based on the classification to provide differentiated services. A switch provides fixed classification. The management function classifies packet types based on the protocols supported by the switch, for example, STP BPDU packets and ICMP packets. Packet types cannot be customized.

9.3.2 Meter

Working Principle

The Meter limits the rates of different packets based on the preset rate thresholds. You can set different rate thresholds for different packet types. When the rate of a packet type exceeds the corresponding threshold, the packets out of the limit will be discarded.

By using the Meter, you can control the rate of a packet type sent to the CPU within a threshold to prevent specific attack packets from exerting large impacts on the CPU resources. This is the level-1 protection of the CPP.

Related Configuration

- By default, each packet type corresponds to a rate threshold (bandwidth) and Meter policies are implemented based on the rate threshold.
- In application, you can run the **cpu-protect type** *packet-type* **bandwidth** *bandwidth-value* command to set Meter policies for specified packet types.

9.3.3 Queue

Working Principle

Queues are used to classify packets at level 2. You can select the same queue for different packet types; meanwhile, queues cache packets inside switches and provide services for the Scheduler and Shaper.

CPP queues are SP queues. The SPs of the packets are determined based on the time when they are added to a queue. Packets with a larger queue number have a higher priority.

Related Configuration

- By default, each packet type is mapped to an SP queue.
- In application, you can run the **cpu-protect type** *packet-type* **traffic-class** *traffic-class-num* command to select SP queues for specific packet types.

9.3.4 Scheduler

Working Principle

The Scheduler schedules packets based on SPs of queues. That is, packets in a queue with a higher priority are scheduled first.

Before being scheduled, packets to be sent to the CPU are cached in queues. When being scheduled, the packets are sent to the CPU for processing.

i Only the SP scheduling policy is supported and cannot be modified.

9.3.5 Shaper

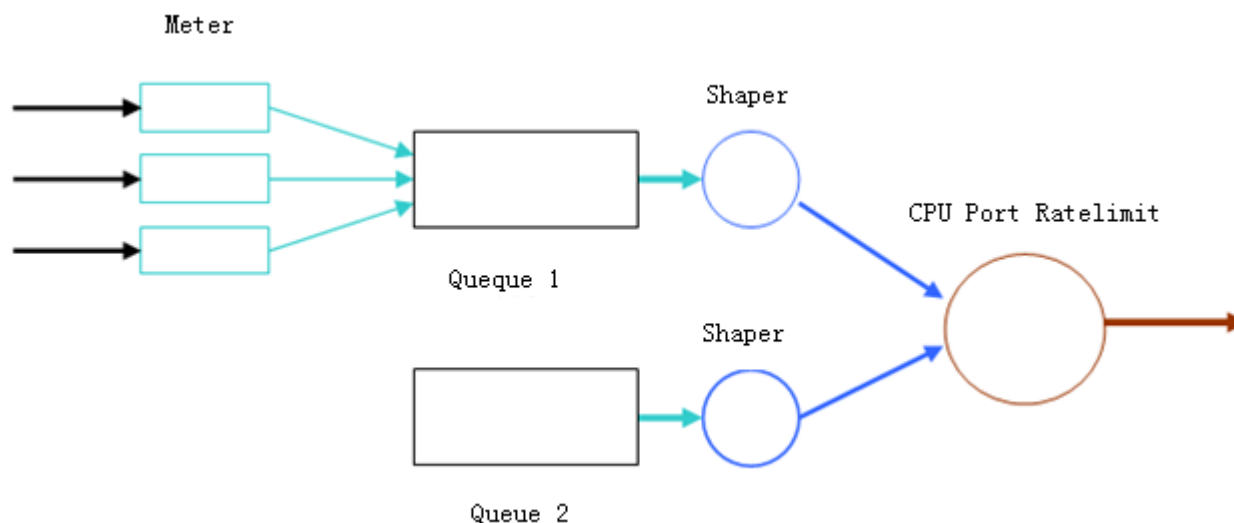
Working Principle

The Shaper is used to shape packets to be sent to the CPU, that is, when the actual rate of packets is greater 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 9-3 3-Level Rate Limit of the CPP



Related Configuration


Configuring the Shaper for priority queues

- By default, each priority queue determines a shaping threshold (bandwidth).
- In application, you can run the **cpu-protect traffic-class traffic-class-num bandwidth bandwidth_value** command to perform Shaper configuration for a specific priority queue.

Configuring the Shaper for the CPU Interface

- By default, the CPU interface determines a shaping threshold (bandwidth).
- Run the **cpu-protect cpu bandwidth bandwidth_value** command to perform Shaper configuration for the CPU interface.

9.4 Configuration

Configuration	Description and Command
Configuring CPP	<p> (Optional and configured by default) It is used to adjust the configuration parameters of CPP.</p>
	<p>cpu-protect type packet-type bandwidth Configures the Meter for a packet type.</p>
	<p>cpu-protect type packet-type traffic-class Configures the priority queue for a packet type.</p>
	<p>cpu-protect traffic-class traffic-class-num bandwidth Configures the Shaper for a priority queue.</p>
	<p>cpu-protect cpu bandwidth Configures the Shaper for the CPU interface.</p>

9.4.1 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 <i>packet-type</i> bandwidth <i>bandwidth_value</i>
Parameter Description	<i>packet-type</i> : Specifies a packet type. Packet types are defined. <i>bandwidth_value</i> : 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 <i>packet-type</i> traffic-class <i>traffic-class-num</i>
Parameter Description	<i>packet-type</i> : Specifies a packet type. Packet types are defined. <i>traffic-class-num</i> : 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 <i>traffic-class-num</i> bandwidth <i>bandwidth_value</i>
----------------	--

Parameter Description	<i>traffic-class-num</i> : Specifies a priority queue. <i>bandwidth_value</i> : 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 <i>bandwidth_value</i>
Parameter Description	<i>bandwidth_value</i> : 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	<ul style="list-style-type: none"> 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.
----------	---

<p>Configuration Steps</p>	<ul style="list-style-type: none"> 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.
	<pre> 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 </pre>
<p>Verification</p>	<p>Run the show cpu-protect command to view the configuration and statistics.</p>
	<pre> 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) Rate(pps) Drop(pps) Total Total Drop ----- </pre>

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	1	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	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
lldp	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	0	4639	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

9.4.2 Configuring CPP Warning

Configuration

Effect

- By configuring CPP warning, periodic detection is enabled to check whether protocol packets or packets in queues are lost.
- By configuring CPP warning of protocol packet loss, when protocol packets are lost, alarm logs are printed.
- By configuring CPP warning of packet loss in a queue, when packets in a queue are lost, alarm logs are printed.

Notes

N/A

Configuration

Steps

Enabling CPP Warning and Configuring Time Interval Between Two Detections of Packet Loss

- You can run the `cpp-warn warn-period value` command to enable CPP warning and configure time interval between two detections of packet loss.
- By default, CPP warning is disabled.

Enabling CPP Warning of Protocol Packet Loss

- You can run the **cpp-warn type *packet-type* warn** command to enable CPP warning of protocol packet loss.
- By default, CPP warning of protocol packet loss is disabled.

Enabling CPP Warning of Packet Loss in a Queue

- You can run the **cpp-warn traffic-class *traffic-class-num* warn** command to enable CPP warning of packet loss in a queue.
- By default, CPP warning of packet loss in a queue is disabled.

Related

Commands

Configuring Time Interval Between Two Detections of Packet Loss

Command	cpp-warn warn-period <i>value</i>
Parameter Description	<i>value</i> : Specifies the interval between two detections of packet loss in the unit of second. The default value is 0, which means this detection is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling CPP Warning of Protocol Packet Loss

Command	cpp-warn type <i>packet-type</i> warn
Parameter Description	<i>packet-type</i> : Specifies a packet type. Packet types are defined.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling CPP Warning of Packet Loss in a Queue

Command	cpp-warn traffic-class <i>traffic-class-num</i> warn
----------------	---

Parameter Description	<i>traffic-class-num</i> : Specifies a priority queue.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring CPP Warning

Configuration Steps	<ul style="list-style-type: none"> ▪ RFC 2131: Dynamic Host Configuration Protocol ▪ RFC 2132: DHCP Options and BOOTP Vendor Extensions
	<pre>QTECH# configure terminal QTECH(config)# cpp-warn warn-period 10 QTECH(config)# cpp-warn traffic-class 1 warn QTECH(config)# cpp-warn type arp warn</pre>
Verification	Run the show run command to view the configuration.
	<pre>QTECH# show run inc cpp cpp-warn warn-period 10 cpp-warn type arp warn cpp-warn traffic-class 1 warn</pre>

9.5 Monitoring

Clearing

Description	Command
Clears the CPP statistics.	<code>clear cpu-protect counters [device <i>device_num</i>]</code>
Clears the CPP statistics on the master device.	<code>clear cpu-protect counters mboard</code>

Displaying

Description	Command
Displays the configuration and statistics of a packet type.	show cpu-protect type <i>packet-type</i> [device <i>device_num</i>]
Displays the configuration and statistics of a priority queue.	show cpu-protect traffic-class <i>traffic-class-num</i> [device <i>device_num</i>]
Displays the configuration on a CPU interface.	show cpu-protect cpu
Displays all configurations and statistics on the master device.	show cpu-protect {mboard summary }
Displays all configurations and statistics of CPP.	show cpu-protect [device <i>device_num</i>]
Displays CPP statistics of an interface.	show cpu-protect statistics [interface <i>interface-id</i>]
Displays a CPP statistics type.	show cpu-protect statistics type <i>packet-type</i>

Debugging

N/A

- i** The preceding monitoring commands are available on both chassis and cassette devices in the standalone mode.
- i** 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.
- i** In the standalone mode, the parameter **device** is unavailable.

10 CONFIGURING DHCP SNOOPING

10.1 Overview

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record and monitor users' IP addresses and filter out illegal DHCP packets, including client request packets and server response packets. The legal user database generated from DHCP Snooping records may serve security applications like IP Source Guard.

Protocols and Standards

- Detect whether protocol packets or packets in queues are lost every 10s.
- Print alarm logs if ARP packets are lost.
- Print alarm logs if packets in queue 1 are lost.

10.2 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.

10.2.1 Guarding Against DHCP Service Spoofing

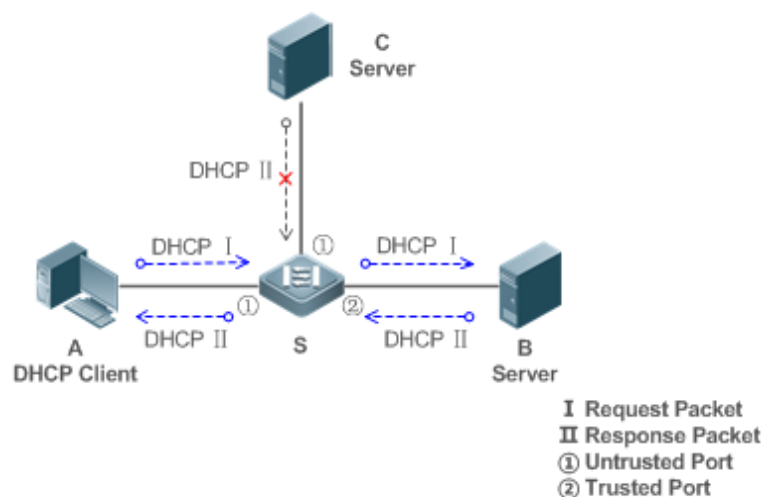
Scenario

Multiple DHCP servers may exist in a network. It is essential to ensure that user PCs obtain network configurations only from the DHCP servers within a controlled area.

Take the following figure as an example. The DHCP client can only communicate with trusted DHCP servers.

- Request packets from the DHCP client can be transmitted only to trusted DHCP servers.
- Only the response packets from trusted DHCP servers can be transmitted to the client.

Figure 10–1



Remark	S is an access device.
S:	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.

10.2.2 Guarding Against DHCP Packet Flooding

Scenario

Potential malicious DHCP clients in a network may send high-rate DHCP packets. As a result, legitimate users cannot obtain IP addresses, and access devices are highly loaded or even break down. It is necessary to take actions to ensure network stability.

With the DHCP Snooping rate limit function for DHCP packets, a DHCP client can only send DHCP request packets at a rate below the limit.

- The request packets from a DHCP client are sent at a rate below the limit.
- Packets sent at rates beyond the limit will be discarded.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Limit the rates of DHCP packets from the untrusted ports.

10.2.3 Guarding Against Forged DHCP Packets

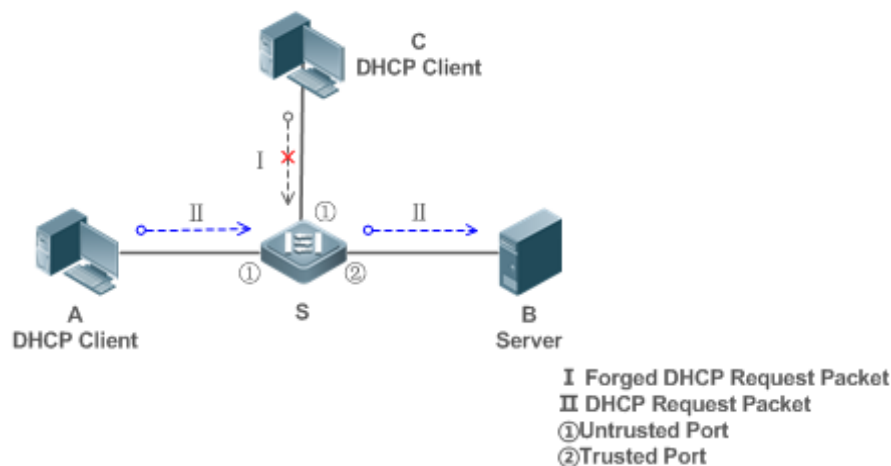
Scenario

Potential malicious clients in a network may forge DHCP request packets, consuming applicable IP addresses from the servers and probably preempting legal users' IP addresses. Therefore, it is necessary to filter out illegal DHCP packets.

For example, as shown in the figure below, the DHCP request packets sent from DHCP clients will be checked.

- The source MAC address fields of the request packets from DHCP clients must match the **chaddr** fields of DHCP packets.
- The Release packets and Decline packets from clients must match the entries in the DHCP Snooping binding database.

Figure 10–2



Remark s:	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.

10.2.4 Guarding Against IP/MAC Spoofing

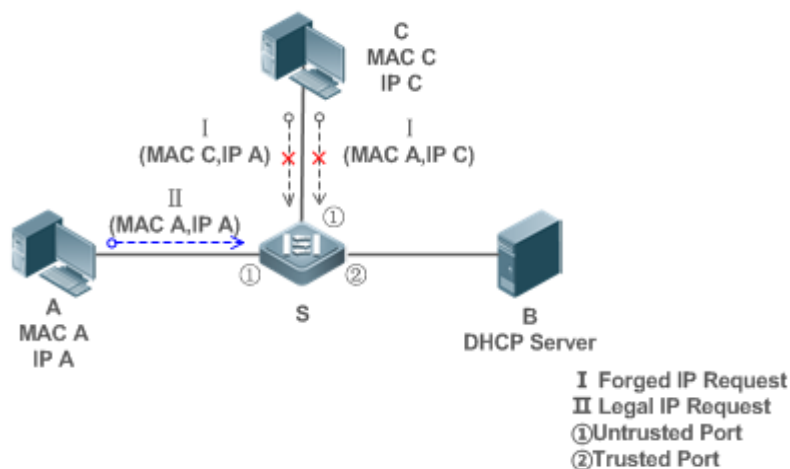
Scenario

Check IP packets from untrusted ports to filter out forged IP packets based on IP or IP-MAC fields.

For example, in the following figure, the IP packets sent by DHCP clients are validated.

- The source IP address fields of IP packets must match the IP addresses assigned by DHCP.
- The source MAC address fields of layer-2 packets must match the **chaddr** fields in DHCP request packets from clients.

Figure 10-3



Remark S:	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.

10.2.5 Preventing Lease of IP Addresses

Scenario

Validate the source addresses of IP packets from untrusted ports compared with DHCP-assigned addresses.

If the source addresses, connected ports, and layer-2 source MAC addresses of ports in IP packets do not match the assignments of the DHCP server, such packets will be discarded.

The networking topology scenario is the same as that shown in the previous figure.

Deployment

- The same as that in the section "Guarding Against IP/MAC Spoofing".

10.2.6 Detecting ARP Attacks

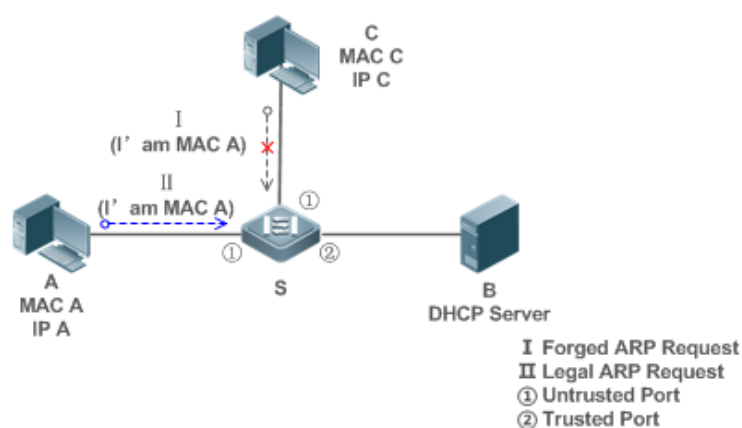
Scenario

Check the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

For example, in the following figure, the ARP packets sent from DHCP clients will be checked.

- The ports receiving ARP packets, the layer-2 MAC addresses, and the source MAC addresses of ARP packets senders shall be consistent with the DHCP Snooping histories.

Figure 10-4



Remark S:	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.

10.3 Features

Basic Concepts

DHCP Request Packets

Request packets are sent from a DHCP client to a DHCP server, including DHCP-DISCOVER packets, DHCP-REQUEST packets, DHCP-DECLINE packets, DHCP-RELEASE packets and DHCP-INFORM packets.

DHCP Response Packets

Response packets are sent from a DHCP server to a DHCP client, including DHCP-OFFER packets, DHCP-ACK packets and DHCP-NAK packets.

DHCP Snooping Trusted Ports

IP address request interaction is complete via broadcast. Therefore, illegal DHCP services will influence normal clients' acquisition of IP addresses and lead to service spoofing and stealing. To prevent illegal DHCP services, DHCP Snooping ports are divided into two types: trusted ports and untrusted ports.

The access devices only transmit DHCP response packets received on trusted ports, while such packets from untrusted ports are discarded. In this way, we may configure the ports connected to a legal DHCP Server as trusted and the other ports as untrusted to shield illegal DHCP Servers.

On switches, all switching ports or layer-2 aggregate ports are defaulted as untrusted, while trusted ports can be specified.

DHCP Snooping Packet Suppression

To shield all the DHCP packets on a specific client, we can enable DHCP Snooping packet suppression on its untrusted ports.

VLAN-based DHCP Snooping

DHCP Snooping can work on a VLAN basis. By default, when DHCP Snooping is enabled, it is effective to all the VLANs of the current client. Specify VLANs help control the effective range of DHCP Snooping flexibly.

DHCP Snooping Binding Database

In a DHCP network, clients may set static IP addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legal clients with IP addresses assigned by the DHCP server may fail to use the network normally due to address conflict. Through snooping packets between clients and servers, DHCP Snooping summarizes the user entries including IP addresses, MAC address, VLAN ID (VID), ports and lease time to build the DHCP Snooping binding database. Combined

with ARP detection and ARP check, DHCP Snooping controls the reliable assignment of IP addresses for legal clients.

DHCP Snooping Rate Limit

DHCP Snooping rate limit function can be configured through the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see the *Configuring NFPP*.

DHCP Option82

DHCP Option82, an option for DHCP packets, is also called DHCP Relay Agent Information Option. As the option number is 82, it is known as Option82. Option82 is developed to enhance the security of DHCP servers and improve the strategies of IP address assignment. The option is often configured for the DHCP relay services of a network access device like DHCP Relay and DHCP Snooping. This option is transparent to DHCP clients, and DHCP relay components realize the addition and deduction of the option.

Illegal DHCP Packets

Through DHCP Snooping, validation is performed on the DHCP packets passing through a client. Illegal DHCP packets are discarded, user information is recorded into the DHCP Snooping binding database for further applications (for example, ARP detection). The following types of packets are considered illegal DHCP packets.

- The DHCP response packets received on untrusted ports, including DHCP-ACK, DHCP-NACK and DHCP-OFFER packets
- The DHCP request packets carrying gateway information **giaddr**, which are received on untrusted ports
- When MAC verification is enabled, packets with source MAC addresses different with the value of the **chaddr** field in DHCP packets
- DHCP-RELEASE packets with the entry in the DHCP Snooping binding database Snooping while with untrusted ports inconsistent with settings in this binding database
- DHCP packets in wrong formats, or incomplete

Overview

Feature	Description
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.

10.3.1 Filtering DHCP Packets

Perform validation on DHCP packets from untrusted ports. Filter out the illegal packets as introduced in the previous section "Basic Concepts".

[Working Principle](#)

During snooping, check the receiving ports and the packet fields of packets to realize packet filtering, and modify the destination ports of packets to realize control of transmit range of the packets.

Checking Ports

In receipt of DHCP packets, a client first judges whether the packet receiving ports are DHCP Snooping trusted ports. If yes, legality check and binding entry addition are skipped, and packets are transferred directly. For not, both the check and addition are needed.

Checking Packet Encapsulation and Length

A client checks whether packets are UDP packets and whether the destination port is 67 or 68. Check whether the packet length match the length field defined in protocols.

Checking Packet Fields and Types

According to the types of illegal packet introduced in the section "Basic Concepts", check the fields **giaddr** and **chaddr** in packets and then check whether the restrictive conditions for the type of the packet are met.

[Related Configuration](#)

Enabling Global DHCP Snooping

By default, DHCP Snooping is disabled.

It can be enabled on a device using the **ip dhcp snooping** command.

Global DHCP Snooping must be enabled before VLAN-based DHCP Snooping is applied.

Configuring VLAN-based DHCP Snooping

By default, when global DHCP Snooping is effective, DHCP Snooping is effective to all VLANs.

Use the [**no**] **ip dhcp snooping vlan** command to enable DHCP Snooping on specified VLANs or delete VLANs from the specified VLANs. The value range of the command parameter is the actual range of VLAN numbers.

Configuring DHCP Snooping Source MAC Verification

By default, the layer-2 MAC addresses of packets and the **chaddr** fields of DHCP packets are not verified. When the **ip dhcp snooping verify mac-address** command is used, the source MAC addresses and the **chaddr** fields of the DHCP request packets sent from untrusted ports are verified. The DHCP request packets with different MAC addresses will be discarded.

10.3.2 Building the Binding Database

DHCP Snooping detects the interactive packets between DHCP clients and the DHCP server, and generate entries of the DHCP Snooping binding database according to the information of legal DHCP packets. All these legal entries are provided to other security modules of a client as the basis of filtering packets from network.

Working Principle

During snooping, the binding database is updated timely based on the types of DHCP packets.

Generating Binding Entries

When a DHCP-ACK packet on a trusted port is snooped, the client's IP address, MAC address, and lease time field are extracted together with the port ID (a wired interface index) and VLAN ID. Then, a binding entry of it is generated.


Deleting Binding Entries


When the recorded lease time of a binding entry is due, it will be deleted if a legal DHCP-RELEASE/DHCP-DECLINE packet sent by the client or a DHCP-NCK packet received on a trusted port is snooped, or the **clear** command is used.

Related Configuration

No configuration is needed except enabling DHCP Snooping.

10. 4 Configuration

Configuration	Description and Command
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 the backup file manually.
	renew ip dhcp snooping database	Imports Flash storage to 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.
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-option remote-id of Option82 as a user-defined character string.

	ip dhcp snooping vlan information option format-type circuit-id string	Configures the sub-option circuit-id of Option82 as a user-defined character string.
--	---	---

10.4.1 Configuring Basic Features

Configuration

Effect

- Enable DHCP Snooping.
- Generate the DHCP Snooping binding database.
- Control the transmit range of DHCP packets.
- Filter out illegal DHCP packets.

Notes

- The ports on clients connecting a trusted DHCP server must be configured as trusted.
- DHCP Snooping is effective on the wired switching ports, layer-2 aggregate ports, and layer-2 encapsulation sub-interfaces. The configuration can be implemented in interface configuration mode.
- DHCP Snooping and DHCP Relay are mutually exclusive in VRF scenarios.

Configuration

Steps

Enabling Global DHCP Snooping

- Mandatory.
- Unless otherwise noted, the feature should be configured on access devices.

Enabling or Disabling VLAN-based DHCP Snooping

- DHCP Snooping can be disabled if not necessary for some VLANs.
- Unless otherwise noted, the feature should be configured on access devices.

Configuring DHCP Snooping Trusted Ports

- Mandatory.
- Configure the ports connecting a trusted DHCP server as trusted.

Enabling DHCP Snooping Source MAC Validation

- This configuration is required if the **chaddr** fields of DHCP request packets match the layer-2 source MAC addresses of data packets.
- Unless otherwise noted, the feature should be enabled on all the untrusted ports of access devices.

Writing the DHCP Snooping Binding Database to Flash Periodically

- Enable this feature to timely save the DHCP Snooping binding database information in case that client reboot.
- Unless otherwise noted, the feature should be configured on access devices.

Enabling BOOTP Support

- Optional
- Unless otherwise noted, the feature should be configured on access devices.

Enabling DHCP Snooping to Process Relay Requests

- Optional.
- Unless otherwise noted, the feature should be enabled on access devices.

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 { <i>vlan-rng</i> { <i>vlan-min</i> [<i>vlan-max</i>] } }
Parameter Description	<i>vlan-rng</i> : Indicates the range of VLANs <i>vlan-min</i> : The minimum VLAN ID <i>vlan-max</i> : The maximum VLAN ID

Command Mode	Global configuration mode
Usage Guide	Use this command to enable or disable DHCP Snooping on specified VLANs. This feature is available only after global DHCP Snooping is enabled.

Configuring DHCP Snooping Packet Suppression

Command	[no] ip dhcp snooping suppression
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Use this command to reject all DHCP request packets at the port, that is, to forbid all users under the port to apply for addresses via DHCP.

Configuring DHCP Snooping Source MAC Verification

Command	[no] ip dhcp snooping verify mac-address
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Through the source MAC address verification, the MAC addresses in link headers and the CLIENT MAC fields in the request packets sent by a DHCP CLIENT are checked for consistence. When the source MAC address verification fails, packets will be discarded.

Writing DHCP Snooping Database to Flash Periodically

Command	[no] ip dhcp snooping database write-delay [<i>time</i>]
Parameter Description	<i>time</i> : 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	<p>Use this command to write the dynamic user information in the DHCP Snooping database in FLASH documents in real time.</p> <p>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.</p>

Importing the Backup 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 the backup file to the DHCP Snooping binding database.

Configuring DHCP Snooping Trusted Ports

Command	[no] ip dhcp snooping trust
----------------	--------------------------------------

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure a port connected to a legal DHCP server as a trusted port. The DHCP response packets received by trusted ports are transferred, while those received by untrusted ports are discarded.

Enabling or Disabling BOOTP Support

Command	[no] ip dhcp snooping bootp
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to support the BOOTP protocol.

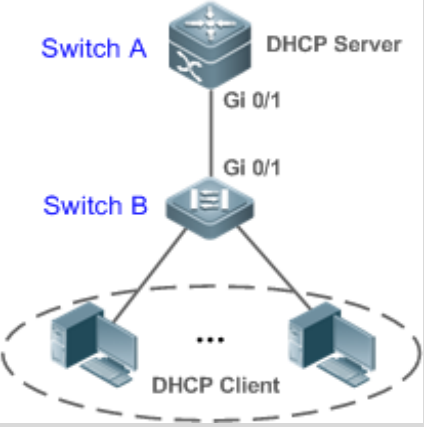
Enabling DHCP Snooping to Process Relay Requests

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.

Configuration Example

DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

<p>Scenario Figure 10-5</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ▪ 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.
<p>B</p>	<pre>B#configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)#ip dhcp snooping B(config)#interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust B(config-if-GigabitEthernet 0/1)#end</pre>
<p>Verification</p>	<p>Check the configuration on Switch B.</p> <ul style="list-style-type: none"> ▪ 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.
<p>B</p>	<pre>B#show running-config !</pre>


```
ip dhcp snooping
!
interface GigabitEthernet 0/1
B#show ip dhcp snooping
Switch DHCP Snooping status          : ENABLE
DHCP Snooping Verification of hwaddr status : DISABLE
DHCP Snooping database write-delay time  : 0 seconds
DHCP Snooping option 82 status        : DISABLE
DHCP Snooping Support BOOTP bind status : DISABLE
Interface          Trusted    Rate limit (pps)
-----
GigabitEthernet 0/1    YES      unlimited
B#show ip dhcp snooping binding
Total number of bindings: 1
MacAddress    IpAddress    Lease(sec)  Type         VLAN  Interface
-----
0013.2049.9014  172.16.1.2  86207      DHCP-Snooping 1   GigabitEthernet 0/11
```

Common Errors

- The uplink port is not configured as a DHCP trusted port.
- Another access security option is already configured for the uplink port, so that a DHCP trusted port cannot be configured.

10.4.2 Configuring Option82

Configuration Effect

- Enable a DHCP server to obtain more information and assign addresses better.
- The Option82 function is client-oblivious.

Notes

- The Option82 functions for DHCP Snooping and DHCP Relay are mutually exclusive.

Configuration Steps

- To realize optimization of address allocation, implement the configuration.
- Unless otherwise noted, enable this function on access devices with DHCP Snooping enabled.

Verification

Check whether the DHCP Snooping configuration options are configured successfully.

Related Commands

Adding Option82 to DHCP Request Packets

Command	[no] ip dhcp snooping information option [standard-format]
Parameter Description	standard-format : Indicates a standard format of the Option82 options
Command Mode	Global configuration mode
Usage Guide	Use this command to add Option82 to DHCP request packets so that a DHCP server assigns addresses according to such information.

Configuring Sub-option remote-id of Option82 as User-defined Character String

Command	[no] ip dhcp snooping information option format remote-id { string ASCII-string hostname }
Parameter Description	string ASCII-string : Indicates the content of the extensible format, the Option82 option remote-id , is a 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.

Configuring Sub-Option circuit-id of Option82 as User-defined Character String

Command	[no] ip dhcp snooping vlan <i>vlan-id</i> information option format-type circuit-id string <i>ascii-string</i>
Parameter Description	<i>vlan-id</i> : Indicates the VLAN where a DHCP request packet is <i>ascii-string</i> : Indicates the user-defined string
Configuration mode	Interface configuration mode
Usage Guide	Use this command to configure the sub-option circuit-id of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

Configuration

Example

Configuring Option82 to DHCP Request Packets

Configuration Steps	<ul style="list-style-type: none"> ▪ Configuring basic functions of DHCP Snooping. ▪ Configuring Option82.
B	<pre>QTECH# configure terminal QTECH(config)# ip dhcp snooping information option QTECH(config)# end</pre>
Verification	Check the DHCP Snooping configuration.
B	<pre>B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : ENABLE DHCP Snooping Support bootp bind status : DISABLE Interface Trusted Rate limit (pps) ----- GigabitEthernet 0/1 YES unlimited</pre>

Common Errors

- N/A

10.5 Monitoring

Clearing

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

Description	Command
Clears the DHCP Snooping binding database.	clear ip dhcp snooping binding [<i>ip</i>] [<i>mac</i>] [vlan <i>vlan-id</i>] [interface <i>interface-id</i>]

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

11 CONFIGURING NFPP

11.1 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.

11.2 Applications

Application	Description
Attack Rate Limiting	Due to various malicious attacks such as ARP attacks and IP scanning attacks in the network, the CPU cannot process normal protocol and management traffics, causing protocol flapping or management failure. The NFPP attack rate limiting function is used to limit the rate of attack traffic or isolate attack traffic to recover the network.
CentralizedBandwidth Allocation	If normal service traffics are too large, you need to classify and prioritize the traffics. When a large number of packets are directed to the CPU, the CPU will be highly loaded, thereby causing device management or device running failure. The centralized bandwidth distribution function is used to increase the priority of such traffics so that switches can run stably.

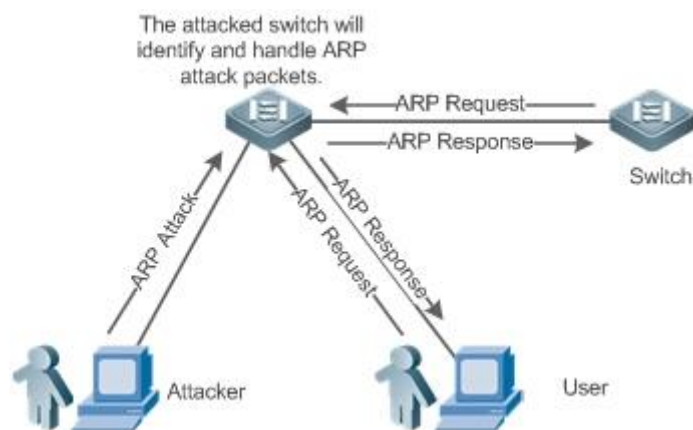
11.2.1 Attack Rate Limiting

[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 11-1, normal hosts will fail to access the network, and the switch will fail to send ARP replies to other devices.

Figure 11-1



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.

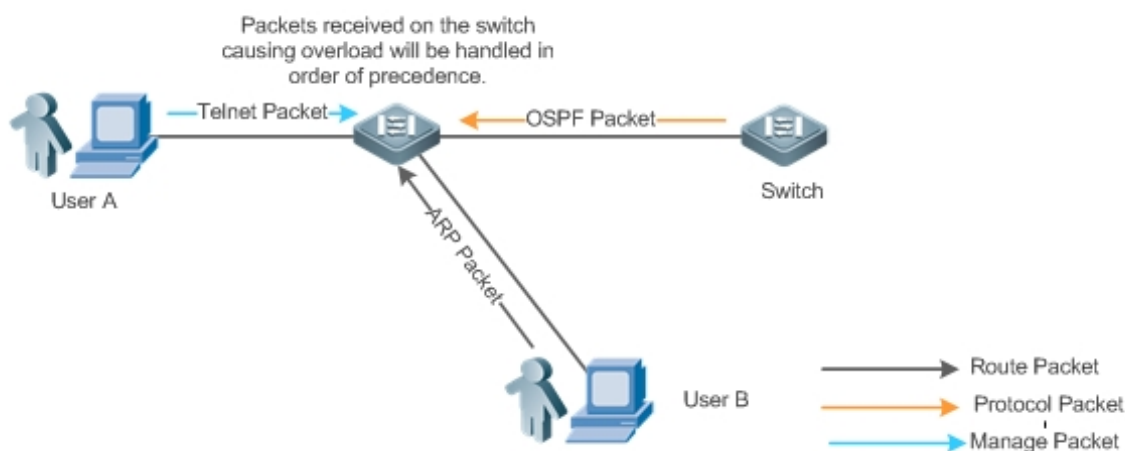
11.2.2 Centralized Bandwidth Allocation

Scenario

A switch classifies services defined in CPP into three types: Manage, Route, and Protocol. Each type of services has an independent bandwidth. Different types of services cannot share their bandwidths. Traffics with bandwidths exceeding the thresholds will be discarded. By such service classification, service packets are processed by orders of precedence.

As shown in Figure 11-2, the switch receives a large number of Telnet packets, OSPF packets, and ARP packets, causing CPU overload. In this case, the CPU cannot process all packets, and a large quantity of packets are backlogged in the queue, causing various problems such as frequent Telnet disconnection, OSPF protocol flapping, and ARP access failure on hosts.

Figure 11-2



Deployment

- By default, CPU centralized bandwidth allocation is enabled to assign an independent bandwidth and bandwidth ratio to each type of services. At the time, the CPU first processes Telnet packets to ensure uninterrupted connection of Telnet service, and then processes OSPF packets to maintain OSPF protocol stability, and finally processes ARP packets.
- If the preceding problems still occur in default configurations, you can accordingly adjust the bandwidths and bandwidth ratios of various types of services.

11.3 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 router or switch 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 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.

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.
Centralized Bandwidth Allocation	Classifies and prioritizes packets.

11.3.1 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.

11.3.2 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.

11.3.3 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 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.

11.3.4 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 or ND 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.

i At present, only ARP guard supports the configuration of isolate forwarding and ratelimit forwarding.

11.3.5 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.

11.3.6 Centralized Bandwidth Allocation

Working Principle

Services defined in CPP are classified into three types: Manage, Route, and Protocol. (For details, see the following table.) Each type of service has an independent bandwidth. Different types of services cannot share their bandwidths. Traffics exceeding the bandwidth thresholds are discarded. By such service classification, service packets are processed by orders of precedence.

NFPP allows the administrator to flexibly assign bandwidth for three types of packets based on the actual network environment so that Protocol and Manage packets can be first processed. Prior processing of Protocol packets ensures proper running of protocols, and prior processing of Manage packets ensures proper management for the administrator, thereby ensuring proper running of important device functions and improving the guard capability of the device.

After classified rate limiting, all types of packets are centralized in a queue. When one type of service is processed inefficiently, packets of this service will be backlogged in the queue and may finally use up resources of the queue. NFPP allows the administrator to configure the percentages of these three types of packets in the queue. When the queue length occupied by one type of packets exceeds the value of the total queue length multiplied by the percentage of

this packet type, the excessive packets will be discarded. This efficiently prevents one type of packets from exclusively occupying queue resources.

Packet Type	Service Type Defined in CPP
Protocol	tp-guard, dot1x, rldp, rerp, slow-packet, bpdu, isis dhcps, gvrp, ripng, dvmrp, igmp, mpls, ospf, pim, pimv6, rip, vrrp, ospf3, dhcp-relay-s, dhcp-relay-c, option82, tunnel-bpdu, tunnel-gvrp
Route	unknown-ipmc, unknown-ipmcv6, ttl1, ttl0, udp-helper, ip4-packet-other, ip6-packet-other, non-ip-packet-other, arp
Manage	ip4-packet-local, ip6-packet-local

 For the definitions of service types, see the Configuring CPU Protection.

[Related Configuration](#)

Configuring the Maximum Bandwidth of Specified Packets

In global configuration mode:

Run the **cpu-protect sub-interface { manage | protocol | route} pps *pps_value*** command to configure the maximum bandwidth of specified packets.

Configuring the Maximum Percentage of Specified Packets in the Queue

In global configuration mode:

Run the **cpu-protect sub-interface { manage | protocol | route} percent *percent_value*** command to configure the maximum percentage of specified packets in the queue.

11.4 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	Configures the maximum number of ICMP-guard monitored hosts.
	icmp-guard rate-limit	Configures the global ICMP-guard rate limit.
	icmp-guard attack-threshold	Configures the global 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.
Configuring DHCP Guard	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 period.
	dhcp-guard monitored-host-limit	Configures the 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.
	dhcpv6-guard enable	Enables DHCPv6 guard globally.

Configuring DHCPv6 Guard	dhcpv6-guard monitor-period	Configures the global DHCPv6-guard monitoring period.
	dhcpv6-guard monitored-host-limit	Configures the maximum number of DHCPv6-guard monitored hosts.
	dhcpv6-guard rate-limit	Configures the global DHCPv6-guard rate limit.
	dhcpv6-guard attack-threshold { per-src-mac per-port } pps	Configures the global DHCPv6-guard attack threshold.
	nfpp dhcpv6-guard enable	Enables DHCPv6 guard on an interface.
	nfpp dhcpv6-guard policy	Configures the DHCPv6-guard rate limit and attack threshold on an interface.
Configuring ND Guard	nd-guard enable	Enables ND guard globally.
	nd-guard ratelimit-forwarding enable	Enables ND-guard ratelimit forwarding.
	nd-guard rate-limit per-port	Configures the global ND-guard rate limit.
	nd-guard attack-threshold per-port	Configures the 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.
	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 <i>name</i> enable	Enables a self-defined guard globally.
	nfpp define <i>name</i> 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.

11.4.1 Configuring ARP Guard

[Configur
ation
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 [<i>seconds</i> permanent]
---------	--

Parameter Description	<i>seconds</i> : 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 <i>seconds</i>
---------	--

Parameter Description	<i>seconds</i> : 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 <i>number</i>
Parameter Description	<i>number</i> : 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} <i>pps</i>
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. <i>pps</i> : 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	<code>arp-guard attack-threshold {per-src-ip per-src-mac per-port} pps</code>
Parameter Description	<p>per-src-ip: Configures the attack threshold of each source IP address.</p> <p>per-src-mac: Configures the attack threshold of each source MAC address.</p> <p>per-port: Configures the attack threshold of each port.</p> <p>pps: Indicates the attack threshold, ranging from 1 to 19,999. The unit is packets per second (pps).</p>
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	<code>arp-guard scan-threshold pkt-cnt</code>
Parameter Description	<i>pkt-cnt</i> : 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	<code>nfpp arp-guard enable</code>
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 [<i>seconds</i> permanent]
Parameter Description	<i>seconds</i> : 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 { <i>per-src-ip</i> <i>per-src-mac</i> <i>per-port</i> } <i>rate-limit-pps</i> <i>attack-threshold-pps</i>
Parameter Description	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. <i>rate-limit-pps</i> : Indicates the rate limit, ranging from 1 to 19,999. <i>attack-threshold-pps</i> : 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 <i>pkt-cnt</i>
---------	---

Parameter Description	<i>pkt-cnt</i> : 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Set the host-based attack threshold to 5 pps. Set the ARP scanning threshold to 10 pps. Set the isolation period to 180 pps. 												
	<pre> 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 </pre>												
Verification	<ul style="list-style-type: none"> Run the show nfpp arp-guard summary command to display the configuration. 												
	<p>(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)</p> <table border="1"> <thead> <tr> <th>Interface</th> <th>Status</th> <th>Isolate-period</th> <th>Rate-limit</th> <th>Attack-threshold</th> <th>Scan-threshold</th> </tr> </thead> <tbody> <tr> <td>Global</td> <td>Disable</td> <td>180</td> <td>4/5/100</td> <td>8/10/200</td> <td>15</td> </tr> </tbody> </table> <p>Maximum count of monitored hosts: 1000 Monitor period: 600s</p>	Interface	Status	Isolate-period	Rate-limit	Attack-threshold	Scan-threshold	Global	Disable	180	4/5/100	8/10/200	15
Interface	Status	Isolate-period	Rate-limit	Attack-threshold	Scan-threshold								
Global	Disable	180	4/5/100	8/10/200	15								

	<ul style="list-style-type: none"> Run the show nfpp arp-guard hosts command to display the monitored hosts.
	<p>If col_filter 1 shows '*', it means "hardware do not isolate host".</p> <pre> VLAN interface IP address MAC address remain-time(s) ----- - 1 Gi0/43 5.5.5.16 - 175 Total: 1 host </pre>
	<ul style="list-style-type: none"> Run the show nfpp arp-guard scan command to display the scanned hosts.
	<pre> VLAN interface IP address MAC address timestamp ----- - 1 Gi0/5 - 08c6.b3c2.4609 2013-4-30 23:50:32 1 Gi0/5 192.168.206.2 08c6.b3c2.4609 2013-4-30 23:50:33 1 Gi0/5 - 08c6.b3c2.4609 2013-4-30 23:51:33 1 Gi0/5 192.168.206.2 08c6.b3c2.4609 2013-4-30 23:51:34 Total: 4 record(s) </pre>

Common Errors

N/A

11.4.2 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	<code>ip-guard enable</code>
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global IP-Guard Isolation Period

Command	<code>ip-guard isolate-period [seconds permanent]</code>
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	<code>ip-guard monitor-period seconds</code>
---------	--

Parameter Description	<i>seconds</i> : 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 <i>number</i>
Parameter Description	<i>number</i> : 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} <i>pps</i>
Parameter Description	per-src-ip : Limits the rate of each source IP address. per-port : Limits the rate of each port. <i>pps</i> : 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} <i>pps</i>
---------	---

Parameter Description	<p><i>per-src-ip</i>: Configures the attack threshold of each source IP address.</p> <p><i>per-port</i>: Configures the attack threshold of each port.</p> <p><i>pps</i>: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.</p>
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 <i>pkt-cnt</i>
Parameter Description	<i>pkt-cnt</i> : 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 <i>ip mask</i>
Parameter Description	<p><i>ip</i>: Indicates the IP address.</p> <p><i>mask</i>: Indicates the mask of an IP address.</p> <p>all: Used with no to delete all trusted hosts.</p>
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 [<i>seconds</i> permanent]
Parameter Description	<i>seconds</i> : 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. <i>permanent</i> : 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} <i>rate-limit-pps attack-threshold-pps</i>
Parameter Description	<i>per-src-ip</i> : Configures the attack threshold of each source IP address. <i>per-port</i> : Configures the attack threshold of each port. <i>rate-limit-pps</i> : Indicates the rate limit, ranging from 1 to 19,999. <i>attack-threshold-pps</i> : 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 <i>pkt-cnt</i>
Parameter Description	<i>pkt-cnt</i> : 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	<ul style="list-style-type: none"> 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 pass through.
Configuration Steps	<ul style="list-style-type: none"> Configure the host-based attack threshold. Configure the IP scanning threshold. Set the isolation period to a non-zero value. Configure trusted hosts.
	<pre>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</pre>
Verification	<ul style="list-style-type: none"> Run the show nfpp ip-guard summary command to display the configuration.

<p>(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)</p> <pre>Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold Global Disable 180 20/-/100 30/-/200 100</pre> <p>Maximum count of monitored hosts: 1000 Monitor period: 600s</p>
<ul style="list-style-type: none"> Run the show nfpp ip-guard hosts command to display the monitored hosts.
<p>If col_filter 1 shows '*', it means "hardware do not isolate host".</p> <pre>VLAN interface IP address Reason remain-time(s) ----- 1 Gi0/5 192.168.201.47 ATTACK 160</pre> <p>Total: 1 host</p>
<ul style="list-style-type: none"> Run the show nfpp ip-guard trusted-host command to display the trusted hosts.
<pre>IP address mask ----- 192.168.201.46 255.255.255.255</pre> <p>Total: 1 record(s)</p>

Common Errors

N/A

11.4.3 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 [<i>seconds</i> permanent]
Parameter Description	<i>seconds</i> : 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. <i>permanent</i> : 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 <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode

Usage Guide	<p>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.</p> <p>If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.</p>
-------------	--

Configuring the Maximum Number of ICMP-Guard Monitored Hosts

Command	icmp-guard monitored-host-limit <i>number</i>
Parameter Description	<i>number</i> : Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	<p>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.</p> <p>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.</p>

Configuring the Global ICMP-Guard Rate Limit

Command	icmp-guard rate-limit {per-src-ip per-port} <i>pps</i>
Parameter Description	<p>per-src-ip: Limits the rate of each source IP address.</p> <p>per-port: Limits the rate of each port.</p> <p><i>pps</i>: Indicates the rate limit, ranging from 1 to 19,999.</p>
Command Mode	NFPP configuration mode

Usage Guide	N/A
-------------	-----

Configuring the Global ICMP-Guard Attack Threshold

Command	<code>icmp-guard attack-threshold {per-src-ip per-port} pps</code>
Parameter Description	<p><code>per-src-ip</code>: Configures the attack threshold of each source IP address.</p> <p><code>per-port</code>: Configures the attack threshold of each port.</p> <p><code>pps</code>: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.</p>
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring ICMP-Guard Trusted Hosts

Command	<code>icmp-guard trusted-host ip mask</code>
Parameter Description	<p><code>ip</code>: Indicates the IP address.</p> <p><code>mask</code>: Indicates the mask of an IP address.</p> <p>all: Used with no to delete all trusted hosts.</p>
Command Mode	NFPP configuration mode
Usage Guide	<p>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.</p> <p>You can configure a maximum of 500 trusted hosts.</p>

Enabling ICMP Guard on an Interface

Command	<code>nfpp icmp-guard enable</code>
---------	-------------------------------------

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	<i>seconds</i> : 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. <i>rate-limit-pps</i> : Indicates the rate limit, ranging from 1 to 19,999. <i>attack-threshold-pps</i> : 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.

**Configur
ation
Example**

CPU Protection Based on ICMP Guard

Scenario	<ul style="list-style-type: none"> ▪ ICMP host attacks exist in the system, and some hosts cannot successfully ping devices. ▪ Packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	<ul style="list-style-type: none"> ▪ Configure the host-based attack threshold. ▪ Set the isolation period to a non-zero value. ▪ Configure trusted hosts.
	<pre> 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 </pre>
Verification	<ul style="list-style-type: none"> ▪ Run the show nfpp icmp-guard summary command to display the configuration.
	<pre> (Formate 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 </pre>
	<ul style="list-style-type: none"> ▪ Run the show nfpp icmp-guard hosts command to display the monitored hosts.
	<pre> 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 </pre>

	Total: 1 host
	<ul style="list-style-type: none"> Run the show nfpp icmp-guard trusted-host command to display the trusted hosts.
	<pre> IP address mask ----- - 192.168.201.46 255.255.255.255 Total: 1 record(s) </pre>

Common Errors

N/A

11.4.4 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	<code>dhcp-guard enable</code>
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global DHCP-Guard Isolation Period

Command	<code>dhcp-guard isolate-period [seconds permanent]</code>
Parameter Description	<p>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.</p> <p>permanent: Indicates permanent isolation.</p>
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	<code>dhcp-guard monitor-period seconds</code>
---------	--

Parameter Description	<i>seconds</i> : Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	<p>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.</p> <p>If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.</p>

Configuring the Maximum Number of DHCP-Guard Monitored Hosts

Command	dhcp-guard monitored-host-limit <i>number</i>
Parameter Description	<i>number</i> : Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	<p>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.</p> <p>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.</p>

Configuring the Global DHCP-Guard Rate Limit

Command	dhcp-guard rate-limit {per-src-mac per-port} <i>pps</i>
---------	--

Parameter Description	per-src-mac : Limits the rate of each source MAC address. per-port : Limits the rate of each port. <i>pps</i> : 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. <i>pps</i> : 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	<code>nfpp dhcp-guard isolate-period [seconds permanent]</code>
Parameter Description	<i>seconds</i> : 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. <i>permanent</i> : 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	<code>nfpp dhcp-guard policy {per-src-mac per-port} rate-limit-pps attack-threshold-pps</code>
Parameter Description	<i>per-src-ip</i> : Configures the rate limit and attack threshold of each source IP address. <i>per-port</i> : Configures the rate limit and attack threshold of each port. <i>rate-limit-pps</i> : Indicates the rate limit, ranging from 1 to 19,999. <i>attack-threshold-pps</i> : 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	<ul style="list-style-type: none"> DHCP host attacks exist in the system, and some hosts fail to request IP addresses.
Configuration Steps	<ul style="list-style-type: none"> Configure the host-based attack threshold. Set the isolation period to a non-zero value.

	<pre>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</pre>
<p>Verification</p>	<ul style="list-style-type: none"> Run the show nfpp dhcp-guard summary command to display the configuration.
	<pre>(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</pre>
	<ul style="list-style-type: none"> Run the show nfpp dhcp-guard hosts command to display the monitored hosts.
	<pre>If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ----- *1 Gi0/5 08c6.b3c2.4609 160 Total: 1 host</pre>

Common Errors

N/A

11.4.5 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.

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 <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.

Command Mode	NFPP configuration mode
Usage Guide	<p>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.</p> <p>If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.</p>

↘ Configuring the Maximum Number of DHCPv6-Guard Monitored Hosts

Command	dhcpv6-guard monitored-host-limit <i>number</i>
Parameter Description	<i>number</i> : Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	<p>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.</p> <p>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.</p>

Configuring the Global DHCPv6-Guard Rate Limit

Command	dhcpv6-guardrate-limit { per-src-mac per-port} <i>pps</i>
Parameter Description	<p>per-src-mac: Limits the rate of each source MAC address.</p> <p>per-port: Limits the rate of each port.</p>

	<i>pps</i> : 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	<code>dhcpv6-guard attack-threshold { per-src-mac per-port} pps</code>
Parameter Description	per-src-mac: Configures the attack threshold of each source MAC address. per-port: Configures the attack threshold of each port. <i>pps</i> : 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	<code>nfpp dhcpv6-guard enable</code>
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 DHCP-Guard Rate Limit and Attack Threshold on an Interface

Command	<code>nfpp dhcpv6-guard policy {per-src-mac per-port} rate-limit-pps attack-threshold-pps</code>
----------------	---

Parameter Description	<p>per-src-ip: Configures the rate limit and attack threshold of each source IP address.</p> <p>per-port: Configures the rate limit and attack threshold of each port.</p> <p><i>rate-limit-pps:</i> Indicates the rate limit, ranging from 1 to 19,999.</p> <p><i>attack-threshold-pps:</i> Indicates the attack threshold, ranging from 1 to 19,999.</p>
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	<ul style="list-style-type: none"> DHCPv6 host attacks exist in the system, and DHCPv6 neighbor discovery fails on some hosts.
Configuration Steps	<ul style="list-style-type: none"> Configure the host-based attack threshold.
	<pre>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</pre>
Verification	<ul style="list-style-type: none"> Run the show nfpp dhcpv6-guard summary command to display the configuration.
	<p>(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)</p> <pre>Interface Status Rate-limit Attack-threshold Global Disable -/8/150 -/16/300</pre> <p>Maximum count of monitored hosts: 1000 Monitor period: 600s</p>

	<ul style="list-style-type: none"> Run the show nfpp dhcpv6-guard hosts command to display the monitored hosts.
	<pre>If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ----- - *1 Gi0/5 08c6.b3c2.4609 160 Total: 1 host</pre>

Common Errors

N/A

11.4.6 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.

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	<code>nfpp nd-guard policy per-port [ns-na rs ra-redirect] rate-limit-pps attack-threshold-pps</code>
Parameter Description	ns-na: Indicates NSs and NAs. rs: Indicates RSs. ra-redirect: Indicates RAs and Redirect packets. <i>rate-limit-pps</i> : Indicates the rate limit, ranging from 1 to 19,999. <i>attack-threshold-pps</i> : 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 ND Guard

Scenario	<ul style="list-style-type: none"> ND host attacks exist in the system, and neighbor discovery fails on some hosts.
Configuration Steps	<ul style="list-style-type: none"> Configure the host-based attack threshold.
	<pre>QTECH# configure terminal QTECH(config)# nfpp</pre>

	<pre>QTECH (config-nfpp)# nd-guard rate-limit per-port ns-na 30 QTECH (config-nfpp)# nd-guard attack-threshold per-port ns-na 50</pre>
Verification	<ul style="list-style-type: none"> Run the show nfpp nd-guard summary command to display the configuration.
	<pre>(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</pre>

Common Errors

N/A

11.4.7 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.
- 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 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 attach-threshold 150	Not applicable to this policy	rate-limit 300 attach-threshold 500
RIPng	etype 0x86dd protocol 17 dst-port 521	rate-limit 100 attach-threshold 150	Not applicable to this policy	rate-limit 300 attach-threshold 500
BGP	etype 0x0800 protocol 6 dst-port 179	rate-limit 1000 attach-threshold 1200	Not applicable to this policy	rate-limit 2000 attach-threshold 3000
BPDU	dst-mac 08c6.b300.0000	Not applicable to this policy	rate-limit 20 attach-threshold 40	rate-limit 100 attach-threshold 100
RERP	dst-mac 08c6.b300.0001	Not applicable to this policy	rate-limit 20	rate-limit 100

			attach-threshold 40	attach-threshold 100
REUP	dst-mac 08c6.b300.0007	Not applicable to this policy	rate-limit 20 attach-threshold 40	rate-limit 100 attach-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 attach-threshold 1200	Not applicable to this policy	rate-limit 2000 attach-threshold 3000
OSPFv3	etype 0x86dd protocol 89	rate-limit 800 attach-threshold 1200	Not applicable to this policy	rate-limit 2000 attach-threshold 3000
VRRP	etype 0x0800 protocol 112	rate-limit 64 attach-threshold 100	Not applicable to this policy	rate-limit 1024 attach-threshold 1024
IPv6 VRRP	etype 0x86dd protocol 112	rate-limit 64 attach-threshold 100	Not applicable to this policy	rate-limit 1024 attach-threshold 1024
SNMP	etype 0x0800 protocol 17 dst-port 161	rate-limit 1000 attach-threshold 1200	Not applicable to this policy	rate-limit 2000 attach-threshold 3000
RSVP	etype 0x0800 protocol 46	rate-limit 800 attach-threshold 1200	Not applicable to this policy	rate-limit 1200 attach-threshold 1500
LDP (UDP hello)	etype 0x0800 protocol 17	rate-limit 10 attach-threshold 15	Not applicable to this policy	rate-limit 100 attach-threshold 150

	dst-port 646			
--	--------------	--	--	--

- 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 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 <i>name</i>
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	<code>match [etypetype] [src-macsmac [src-mac-masksmac_mask]] [dst-macdmac [dst-mac-maskdst_mask]] [protocolprotocol] [src-ipsip [src-ip-masksip-mask]] [src-ipv6sipv6 [src-ipv6-masklensipv6-masklen]] [dst-ipdip[dst-ip-maskdip-mask]] [dst-ipv6dipv6 [dst-ipv6-masklendipv6-masklen]][src-portsport] [dst-port dport]</code>
Parameter Description	<p><i>type</i>: Indicates the type of Ethernet link-layer packets.</p> <p><i>smac</i>: Indicates the source MAC address.</p> <p><i>smac_mask</i>: Indicates the mask of the source MAC address.</p> <p><i>dmac</i>: Indicates the destination MAC address.</p> <p><i>dst_mask</i>: Indicates the mask of the destination MAC address.</p> <p><i>protocol</i>: Indicates the protocol number of IPv4/IPv6 packets.</p> <p><i>sip</i>: Indicates the source IPv4 address.</p> <p><i>sip-mask</i>: Indicates the mask of the source IPv4 address.</p> <p><i>sipv6</i>: Indicates the source IPv6 address.</p> <p><i>sipv6-masklen</i>: Indicates the mask length of the source IPv6 address.</p> <p><i>dip</i>: Indicates the destination IPv4 address.</p> <p><i>dip-mask</i>: Indicates the mask of the destination IPv4 address.</p> <p><i>dipv6</i>: Indicates the destination IPv6 address.</p> <p><i>dipv6-masklen</i>: Indicates the mask length of the destination IPv6 address.</p> <p><i>sport</i>: Indicates the ID of the source transport-layer port.</p> <p><i>dsport</i>: Indicates the ID of the destination transport-layer port.</p>
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	<p>per-src-ip: Collects rate statistics for host identification based on the source IP address, VLAN ID, and port.</p> <p>per-src-mac: Collects rate statistics for host identification based on the source MAC address, VLAN ID, and port.</p> <p>per-port: Collects rate statistics based on each packet receiving port.</p> <p><i>rate-limit-pps:</i> Indicates the rate limit.</p> <p><i>attack-threshold-pps:</i> Indicates the attack threshold.</p>
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 Monitoring Period of a Self-defined Guard

Command	monitor-period <i>seconds</i>
Parameter Description	<i>seconds:</i> 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 <i>number</i>
---------	---

Parameter Description	<i>number</i> : 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 { <i>mac mac_mask</i> <i>ip mask</i> <i>IPv6/prefixlen</i> }
Parameter Description	<i>mac</i> : Indicates the MAC address. <i>mac_mask</i> : Indicates the mask of a MAC address. <i>ip</i> : Indicates the IP address. <i>mask</i> : Indicates the mask of an IP address. <i>IPv6/prefixlen</i> : Indicates the IPv6 address and its mask length. all : Used with no to delete all trusted hosts.
Command Mode	Self-defined guard configuration mode
Usage Guide	N/A

Enabling a Self-Defined Guard Globally

Command	define <i>name</i> enable
Parameter Description	<i>name</i> : 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 <i>name</i> enable
Parameter Description	<i>name</i> : 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 <i>name</i> policy {per-src-ip per-src-mac per-port} <i>rate-limit-pps</i> <i>attack-threshold-pps</i>
Parameter Description	<p><i>name</i>: Indicates the name of a self-defined guard.</p> <p>per-src-ip: Configures the rate limit and attack threshold of each source IP address.</p> <p>per-src-mac: Configures the rate limit and attack threshold of each source MAC address.</p> <p>per-port: Configures the rate limit and attack threshold of each port.</p> <p><i>rate-limit-pps</i>: Indicates the rate limit, ranging from 1 to 19,999.</p> <p><i>attack-threshold-pps</i>: Indicates the attack threshold, ranging from 1 to 19,999.</p>
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	<ul style="list-style-type: none"> Basic guards cannot protect the system with RIP attacks.
Configuration Steps	<ul style="list-style-type: none"> Configure a self-defined guard, with the key fields matching RIP packets. Configure the rate limit. Configure trusted hosts.
	<pre> 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)#trusted-host 192.168.201.46 255.255.255.255 QTECH (config-nfpp-define)#exit QTECH (config-nfpp)#define rip enable </pre>
Verification	<ul style="list-style-type: none"> Run the show nfpp define summary rip command to display the configuration.
	<pre> Define rip summary: match etype 0x800 protocol 17 dst-port 520 Maximum count of monitored hosts: 1000 Monitor period:600s (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) Interface Status Rate-limit Attack-threshold Global Enable 100/-/ 150/-/ </pre>
	<ul style="list-style-type: none"> Run the show nfpp define trusted-host rip command to display the trusted hosts.
	<pre> Define rip: IP trusted host number is 1: IP address IP mask ----- 192.168.201.46 255.255.255.255 </pre>

	Total: 1 record(s)Global Enable 180 100/-/- 150/-/-
	<ul style="list-style-type: none"> Run the show nfpp define hosts rip command to display the monitored hosts.
	<p>If col_filter 1 shows '*', it means "hardware do not isolate host".</p> <pre> VLAN interface IP address remain-time(s) ---- - 1 Gi0/5 192.168.201.47 160 Total: 1 host </pre>

Common Errors

N/A

11.4.8 Configuring Centralized Bandwidth Allocation

Configuration Effect

- Configure centralized bandwidth allocation so that Manage and Protocol packets are first processed when the network is busy.

Notes

- The following condition must be met: Valid percentage range of a type of packets ≤ 100% – Percentage of the sum of the other two types

Configuration Steps

Configuring the Maximum Bandwidth of Specified Packets

- (Mandatory) Manage, Route, and Protocol packets share the same default bandwidth.

Configuring the Maximum Percentage of Specified Packets in the Queue

- (Mandatory) By default, Manage packets occupy 30% of the bandwidth, Route packets occupy 25%, and Protocol packets occupy 45%.

Verification

Send a large number of protocol packets such as OSPF packets to a switch, causing high CPU utilization.

- When the host pings the switch, the pinging must be successful and no packet is lost.

Related Commands

Configuring the Maximum Bandwidth of Specified Packets

Command	<code>cpu-protect sub-interface { manage protocol route} pps <i>pps_value</i></code>
Parameter Description	<i>pps_value</i> : Indicates the rate limit, ranging from 1 to 100,000.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Maximum Percentage of Specified Packets in the Queue

Command	<code>cpu-protect sub-interface { manage protocol route} percent <i>percent_value</i></code>
Parameter Description	<i>percent_value</i> : Indicates the percentage of a type of packets in the queue, ranging from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	The following condition must be met: Valid percentage range of a type of packets $\leq 100\%$ – Percentage of the sum of the other two types

Configuration Example

Prioritizing Packets Sent to the CPU Through Centralized Bandwidth Allocation

Scenario	Various types of mass packets exist in the network and belong to different centralized types.
Configuration Steps	<ul style="list-style-type: none"> ▪ Configure the maximum bandwidth of specified packets. ▪ Configure the maximum percentage of specified packets in the queue.

	<pre>QTECH# configure terminal QTECH(config)# cpu-protect sub-interface manage pps 5000 QTECH(config)# cpu-protect sub-interface manage percent 25</pre>
Verification	N/A

Common Errors

N/A

11.4.9 Configuring NFPP Logging

Configuration Effect

- NFPP obtains a log from the dedicated log buffer at a certain rate, generates a system message, and clears this log from the dedicated log buffer.

Notes

- Logs are continuously printed in the log buffer, even if attacks have stopped.

Configuration Steps

Configuring the Log Buffer Size

- Mandatory.
- If the log buffer is full, new logs replace the old ones.
- If the log buffer overflows, subsequent logs replace previous logs, and an entry with all attributes marked with a hyphen (-) is displayed in the log buffer. The administrator needs to increase the log buffer size or the 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	<code>log-buffer entries <i>number</i></code>
Parameter Description	<i>number</i> : 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	<code>log-buffer logs <i>number_of_message</i> interval <i>length_in_seconds</i></code>
Parameter Description	<p><i>number_of_message</i>: 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.</p> <p><i>length_in_seconds</i>: 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 <i>number_of_message</i> and <i>length_in_seconds</i>.</p> <p><i>number_of_message/length_in_second</i> indicates the system message generation rate.</p>
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring VLAN-based Log Filtering

Command	logging vlan <i>vlan-range</i>
Parameter Description	<i>vlan-range</i> : 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 <i>interface-id</i>
Parameter Description	<i>interface-id</i> : 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	<ul style="list-style-type: none"> Configure the log buffer size. Configure the log buffer rate. Configure VLAN-based log filtering.
	<pre> 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 </pre>
Verification	<ul style="list-style-type: none"> Run the show nfpp log summary command to display the configuration.
	<pre> Total log buffer size : 1024 Syslog rate : 3 entry per 5 seconds Logging: VLAN 1 </pre>
	<ul style="list-style-type: none"> Run the show nfpp log buffer command to display logs in the log buffer.
	<pre> Protocol VLAN Interface IP address MAC address Reason Timestamp ----- ARP 1 Gi0/5 192.168.206.2 08c6.b3c2.4609 SCAN 2013-5-15:4:24 </pre>

11.5 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 <i>name</i> 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 [<i>name</i>]
Displays the monitored hosts.	show nfpp define hosts <i>name</i>
Displays the trusted hosts.	show nfpp define trusted-host <i>name</i>
Displays NFPP logs.	show nfpp log summary

Displays the NFPP log buffer.

```
show nfpp log buffer [statistics]
```