QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Network Management & Monitoring Configuration

www.qtech.ru

Оглавление

1. Configuring SNMP 1
1.1 Overview 1
1.2 Applications 2
1.2.1 Managing Network Devices Based on SNMP 2
1.3 Features 3
1.3.1 Basic SNMP Functions 5
1.3.2 SNMPv1 and SNMPv2C 7
1.3.3 SNMPv3 8
1.4 Configuration 10
1.4.1 Configuring Basic SNMP Functions 11
1.4.2 Enabling the Trap Function 20
1.4.3 Shielding the Agent Function 25
1.4.4 Setting SNMP Control Parameters 27
1.5 Monitoring 32
2. Configuring RMON 33
2.1 Overview 33
2.2 Applications 33
2.2.1 Collecting Statistics on Information of a Monitored Interface 33
2.3 Features 34
2.3.1 RMON Ethernet Statistics 36
2.3.2 RMON History Statistics 37
2.3.3 RMON Alarm 37
2.4 Configuration 38
2.4.1 Configuring RMON Ethernet Statistics 38
2.4.2 Configuring RMON History Statistics 40
2.4.3 Configuring RMON Alarm 45
2.5 Monitoring 49
3. Configuring NTP 50
3.1 Overview 50
3.2 Applications 50
3.2.1 Synchronizing Time Based on an External Reference Clock Source 50

3.2.2 Synchronizing Time Based on a Local Reference Clock Source 51
3.3 Features 51
3.3.1 NTP Time Synchronization 53
3.3.2 NTP Security Authentication 55
3.3.3 NTP Access Control 56
3.4 Configuration 56
3.4.1 Configuring Basic Functions of NTP 57
3.4.2 Configuring NTP Security Authentication 61
3.4.3 Configuring NTP Access Control 64
3.5 Monitoring 66
4. Configuring SNTP 67
4.1 Overview 67
4.2 Applications 67
4.2.1 Synchronizing Time with an NTP Server 67
4.3 Features 68
4.3.1 SNTP Time Synchronization 69
4.4 Configuration 71
4.4.1 Configuring SNTP 71
4.5 Monitoring 73
5. Configuring SPAN-RSPAN 74
5.1 Overview 74
5.2 Applications 75
5.2.1 Stream-based SPAN 75
5.2.2 One-to-Many RSPAN 76
5.2.3 RSPAN Basic Applications 76
5.3 Features 77
5.3.1 SPAN 79
5.3.2 RSPAN 80
5.4 Configuration 83
5.4.1 Configuring SPAN Basic Functions 84
5.4.2 Configuring RSPAN Basic Functions 87
5.5 Monitoring 92
6. Configuring sFlow 93
6.1 Overview 93

6.2 Applications 93
6.2.1 Monitoring the LAN Traffic 93
6.3 Features 94
6.3.1 Flow Sampling 97
6.3.2 Counter Sampling 98
6.4 Configuration 98
6.4.1 Configuring Basic Functions of sFlow 98
6.4.2 Configuring Optional Parameters of sFlow 103
6.5 Monitoring 106

1. CONFIGURING SNMP

1.1 Overview

Simple Network Management Protocol (SNMP) became a network management standard RFC1157 in August 1988. At present, because many vendors support SNMP, SNMP has in fact become a network management standard and is applicable to the environment where systems of multiple vendors are interconnected. By using SNMP, the network administrator can implement basic functions such as information query for network nodes, network configuration, fault locating, capacity planning, and network monitoring and management.

❖ SNMP Versions

Currently, the following SNMP versions are supported:

- SNMPv1: The first official version of SNMP, which is defined in RFC1157.
- SNMPv2C: Community-based SNMPv2 management architecture, which is defined in RFC1901.
- SNMPv3: SNMPv3 provides the following security features by identifying and encrypting data.

1. Ensuring that data is not tampered during transmission.
2. Ensuring that data is transmitted from legal data sources.
3. Encrypting packets and ensuring data confidentiality.

Protocols and Standards

- RFC 1157, Simple Network Management Protocol (SNMP)
- RFC 1901, Introduction to Community-based SNMPv2
- RFC 2578, Structure of Management Information Version 2 (SMIv2)
- RFC 2579, Textual Conventions for SMIv2
- RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413, Simple Network Management Protocol (SNMP) Applications
- RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

- RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3419, Textual Conventions for Transport Addresses

1.2 Applications

Application	Description
Managing Network Devices Based on SNMP	Network devices are managed and monitored based on SNMP.

1.2.1 Managing Network Devices Based on SNMP

Scenario

Take the following figure as an example. Network device A is managed and monitored based on SNMP network manager.

Figure 1-1

Remarks	A is a network device that needs to be managed. PC is a network management station.

Deployment

The network management station is connected to the managed network devices. On the network management station, users access the Management Information Base (MIB) on the network devices through the SNMP network manager and receive messages actively sent by the network devices to manage and monitor the network devices.

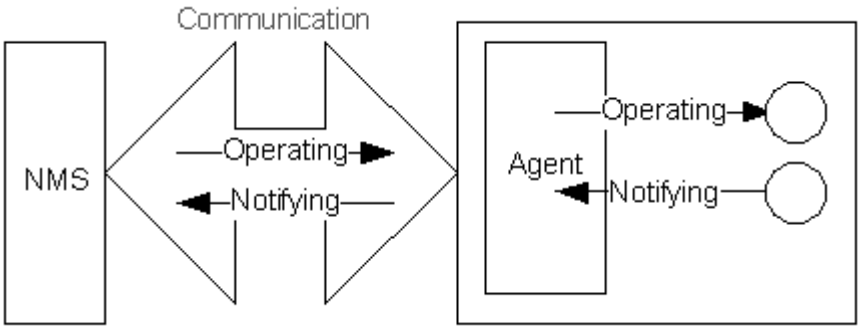
1.3 Features

Basic Concepts

SNMP is an application layer protocol that works in C/S mode. It consists of three parts:

- SNMP network manager
- SNMP agent
- MIB

Figure 1-2 shows the relationship between the network management system (NMS) and the network management agent.



❖ SNMP Network Manager

The SNMP network manager is a system that controls and monitors the network based on SNMP and is also called the NMS.

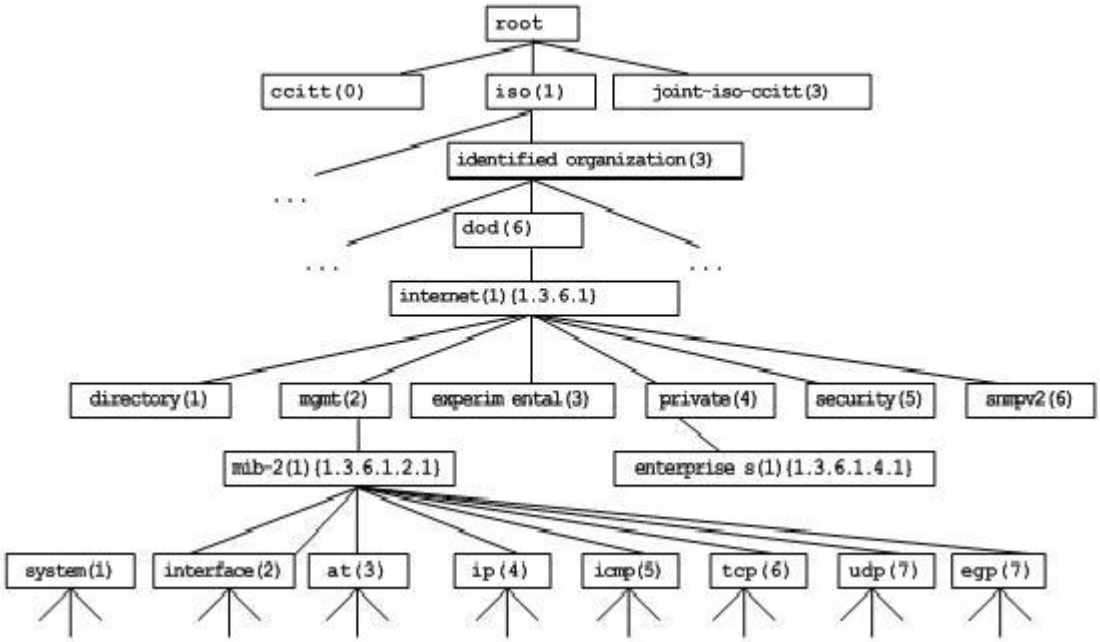
❖ SNMP Agent

The SNMP agent (hereinafter referred to as the agent) is software running on the managed devices. It is responsible for receiving, processing, and responding to monitoring and control packets from the NMS. The agent may also actively send messages to the NMS.

❖ MIB

The MIB is a virtual network management information base. The managed network devices contain lots of information. To uniquely identify a specific management unit among SNMP packets, the MIB adopts the tree hierarchical structure. Nodes in the tree indicate specific management units. A string of digits may be used to uniquely identify a management unit system among network devices. The MIB is a collection of unit identifiers of network devices.

Figure 1-3 Tree Hierarchical Structure



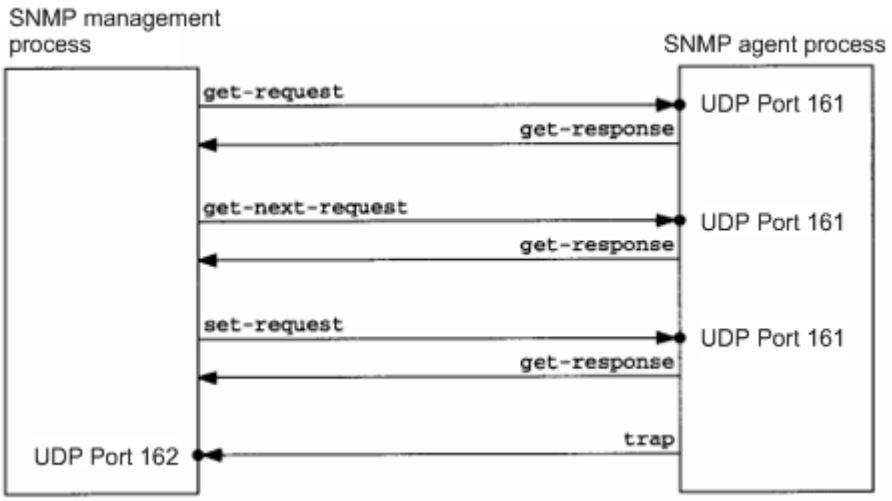
❖ Operation Types

Six operation types are defined for information exchange between the NMS and the agent based on SNMP:

- Get-request: The NMS extracts one or more parameter values from the agent.
- Get-next-request: The NMS extracts the parameter value next to one or more parameters from the agent.
- Get-bulk: The NMS extracts a batch of parameter values from the agent.
- Set-request: The NMS sets one or more parameter values of the agent.
- Get-response: The agent returns one or more parameter values, which are the operations in response to the three operations performed by the agent on the NMS.
- Trap: The agent actively sends a message to notify the NMS of something that happens.

The first four packets are sent by the NMS to the agent and the last two packets are sent by the agent to the NMS. (Note: SNMPv1 does not support the Get-bulk operation.) Figure 1-4 describes the operations.

Figure 1-4 SNMP Packet Types



The three operations performed by the NMS on the agent and the response operations of the agent are based on UDP port 161. The trap operation performed by the agent is based on UDP port 162.

Overview

Feature	Description
Basic SNMP Functions	The SNMP agent is configured on network devices to implement basic functions such as information query for network nodes, network configuration, fault locating, and capacity planning.
SNMPv1 and SNMPv2C	SNMPv1 and SNMPv2C adopt the community-based security architecture, including authentication name and access permission.
SNMPv3	SNMPv3 redefines the SNMP architecture, namely, it enhances security functions, including the security model based on users and access control model based on views. The SNMPv3 architecture already includes all functions of SNMPv1 and SNMPv2C.

1.3.1 Basic SNMP Functions

Working Principle

❖ Working Process

SNMP protocol interaction is response interaction (for exchange of packets, see Figure 1-4). The NMS actively sends requests to the agent, including Get-request, Get-next-request, Get-bulk, and Set-request. The agent receives the requests, completes operations, and returns a Get-response.

Sometimes, the agent actively sends a trap message and an Inform message to the NMS. The NMS does not need to respond to the trap message but needs to return an Inform-response to the agent. Otherwise, the agent re-sends the Inform message.

Related Configuration

❖ Shielding or Disabling the SNMP Agent

By default, the SNMP function is enabled.

The **no snmp-server** command is used to disable the SNMP agent.

The **no enable service snmp-agent** command is used to directly disable all SNMP services.

❖ Setting Basic SNMP Parameters

By default, the system contact mode, system location, and device Network Element (NE) information are empty. The default serial number is 60FF60, the default maximum packet length is 1,572 bytes, and the default UDP port ID of the SNMP service is 161.

The **snmp-server contact** command is used to configure or delete the system contact mode.

The **snmp-server location** command is used to configure or delete the system location.

The **snmp-server chassis-id** command is used to configure the system serial number or restore the default value.

The **snmp-server packetsize** command is used to configure the maximum packet length of the agent or restore the default value.

The **snmp-server net-id** command is used to configure or delete the device NE information.

The **snmp-server udp-port** command is used to set the UDP port ID of the SNMP service or restore the default value.

❖ Configuring the SNMP Host Address

By default, no SNMP host is configured.

The **snmp-server host** command is used to configure the NMS host address to which the agent actively sends messages or to delete the specified SNMP host address. In the messages sent to the host, the SNMP version, receiving port, authentication name, or user can be bound. This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS.

❖ Setting Trap Message Parameters

By default, SNMP is not allowed to actively send a trap message to the NMS, the function of sending a Link Trap message on an interface is enabled, the function of sending a system reboot trap message is disabled, and a trap message does not carry any private field.

By default, the IP address of the interface where SNMP packets are sent is used as the source address.

By default, the length of a trap message queue is 10 and the interval for sending a trap message is 30s.

The **snmp-server enable traps** command is used to enable or disable the agent to actively send a trap message to the NMS.

The **snmp trap link-status** command is used to enable or disable the function of sending a Link Trap message on an interface.

The **snmp-server trap-source** command is used to specify the source address for sending messages or to restore the default value.

The **snmp-server queue-length** command is used to set the length of a trap message queue or to restore the default value.

The **snmp-server trap-timeout** command is used to set the interval for sending a trap message or to restore the default value.

The **snmp-server trap-format private** command is used to set or disable the function of carrying private fields in a trap message when the message is sent.

The **snmp-server system-shutdown** command is used to enable or disable the function of sending a system reboot trap message.

1.3.2 SNMPv1 and SNMPv2C

SNMPv1 and SNMPv2C adopt the community-based security architecture. The administrator who can perform operations on the MIB of the agent is limited by defining the host address and authentication name (community string).

Working Principle

SNMPv1 and SNMPv2 determine whether the administrator has the right to use MIB objects by using the authentication name. The authentication name of the NMS must be the same as an authentication name defined in devices.

SNMPv2C adds the Get-bulk operation mechanism and can return more detailed error message types to the management workstation. The Get-bulk operation is performed to obtain all information from a table or obtain lots of data at a time, so as to reduce the number of request responses. The enhanced error handling capabilities of SNMPv2C include extension of error codes to differentiate error types. In SNMPv1, however, only one error code is provided for errors. Now, errors can be differentiated based on error codes. Because management workstations supporting SNMPv1 and SNMPv2C may exist on the network, the SNMP agent must be able to identify SNMPv1 and SNMPv2C packets and return packets of the corresponding versions.

❖ Security

One authentication name has the following attributes:

- Read-only: Provides the read permission of all MIB variables for authorized management workstations.

- Read-write: Provide the read/write permission of all MIB variables for authorized management workstations.

Related Configuration

❖ Setting Authentication Names and Access Permissions

The default access permission of all authentication names is read-only.

The **snmp-server community** command is used to configure or delete an authentication name and access permission.

This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed.

1.3.3 SNMPv3

SNMPv3 redefines the SNMP architecture and includes functions of SNMPv1 and SNMPv2 into the SNMPv3 system.

Working Principle

The NMS and SNMP agent are SNMP entities. In the SNMPv3 architecture, SNMP entities consist of the SNMP engine and SNMP applications. The SNMP engine is used to send and receive messages, identify and encrypt information, and control access to managed objects. SNMP applications refer to internal applications of SNMP, which work by using the services provided by the SNMP engine.

SNMPv3v determines whether a user has the right to use MIB objects by using the User-based Security Model (USM). The security level of the NMS user must be the same as that of an SNMP user defined in devices so as to manage devices.

SNMPv3 requires the NMS to obtain the SNMP agent engine IDs on devices when the NMS manages devices. SNMPv3 defines the discover and report operation mechanisms. When the NMS does not know agent engine IDs, the NMS may first send a discover message to the agent and the agent returns a report message carrying an engine ID. Later, management operations between the NMS and the agent must carry the engine ID.

❖ Security

- SNMPv3 determines the data security mechanism based on the security model and security level. At present, security models include: SNMPv1, SNMPv2C, and SNMPv3. SNMPv3 includes SNMPv1 and SNMPv2C into the security model.

SNMPv1 and SNMPv2C Security Models and Security Levels

Security Model	Security Level	Authentication	Encryption	Description
SNMPv1	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.
SNMPv2c	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.

SNMPv3 Security Model and Security Level

Security Model	Security Level	Authentication	Encryption	Description
SNMPv3	noAuthNoPriv	User name.	N/A	Data validity is confirmed through user name.
SNMPv3	authNoPriv	MD5 or SHA	N/A	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA is provided.
SNMPv3	authPriv	MD5 or SHA	DES	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA and data encryption mechanism based on CBC-DES are provided.

❖ Engine ID

An engine ID is used to uniquely identify an SNMP engine. Because each SNMP entity includes only one SNMP engine, one SNMP engine uniquely identifies an SNMP entity in a management domain. Therefore, the SNMPv3 agent as an entity must has a unique engine ID, that is, SnmpEngineID.

An engine ID is an octet string that consists of 5 to 32 bytes. RFC3411 defines the format of an engine ID:

- The first four bytes indicate the private enterprise ID (allocated by IANA) of a vendor, which is expressed in hexadecimal.
- The fifth byte indicates remaining bytes:
- 0: Reserved.
- 1: The later four bytes indicate an IPv4 address.
- 2: The later 16 bytes indicate an IPv6 address.
- 3: The later six bytes indicate a MAC address.
- 4: Text consisting of 27 bytes, which is defined by the vendor.
- 5: Hexadecimal value consisting of 27 bytes, which is defined by the vendor.
- 6-127: Reserved.
- 128-255: Formats specified by the vendor.

Related Configuration

❖ Configuring an MIB View and a Group

By default, one view is configured and all MIB objects can be accessed.

By default, no user group is configured.

The **snmp-server view** command is used to configure or delete a view and the **snmp-server group** command is used to configure or delete a user group.

One or more instructions can be configured to specify different community names so that network devices can be managed by NMSs of different permissions.

❖ Configuring an SNMP User

By default, no user is configured.

The **snmp-server user** command is used to configure or delete a user.

The NMS can communicate with the agent by using only legal users.

An SNMPv3 user can specify the security level (whether authentication and encryption are required), authentication algorithm (MD5 or SHA), authentication password, encryption password (only DES is available currently), and encryption password.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic SNMP Functions	(Mandatory) It is used to enable users to access the agent through the NMS.	
	enable service snmp-agent	Enables the agent function.
	snmp-server community	Sets an authentication name and access permission.
	snmp-server user	Configures an SNMP user.
	snmp-server view	Configures an SNMP view.
	snmp-server group	Configures an SNMP user group.
	snmp-server authentication	Configures the SNMP attack protection and detection function.
	snmp-server enable secret-dictionary-check	Configures password dictionary check for communities and users.
Enabling the Trap Function	(Optional) It is used to enable the agent to actively send a trap message to the NMS.	
	snmp-server host	Configures the NMS host address.

Configuration	Description and Command	
	snmp-server enable traps	Enables the agent to actively send a trap message to the NMS.
	snmp trap link-status	Enables the function of sending a Link Trap message on an interface.
	snmp-server system-shutdown	Enables the function of sending a system reboot trap message.
	snmp-server trap-source	Specifies the source address for sending a trap message.
	snmp-server trap-format private	Enables a trap message to carry private fields when the message is sent.
Shielding the Agent Function	(Optional) It is used to shield the agent function when the agent service is not required.	
	no snmp-server	Shields the agent function.
Setting SNMP Control Parameters	(Optional) It is used to set or modify SNMP control parameters.	
	snmp-server contact	Sets the device contact mode.
	snmp-server location	Sets the device location.
	snmp-server chassis-id	Sets the serial number of the device.
	snmp-server net-id	Sets NE information about the device.
	snmp-server packetsize	Modifies the maximum packet length.
	snmp-server udp-port	Modifies the UDP port ID of the SNMP service.
	snmp-server queue-length	Modifies the length of a trap message queue.
	snmp-server trap-timeout	Modifies the interval for sending a trap message.

1.4.1 Configuring Basic SNMP Functions

Configuration Effect

Enable users to access the agent through the NMS.

Notes

- By default, no authentication name is set on network devices and SNMPv1 or SNMPv2C cannot be used to access the MIB of network devices. When an authentication name is set, if no access permission is specified, the default access permission is read-only.

Configuration Steps

❖ Configuring an SNMP View

- Optional
- An SNMP view needs to be configured when the View-based Access Control Model (VACM) is used.

❖ Configuring an SNMP User Group

- Optional
- An SNMP user group needs to be configured when the VACM is used.

❖ Configuring an Authentication Name and Access Permission

- Mandatory
- An authentication name must be set on the agent when SNMPv1 and SNMPv2C are used to manage network devices.

❖ Configuring an SNMP User

- Mandatory
- A user must be set when SNMPv3 is used to manage network devices.

❖ Enabling the Agent Function

- Optional
- By default, the agent function is enabled. When the agent function needs to be enabled again after it is disabled, this command must be used.

Verification

Run the **show snmp** command to check the SNMP function on devices.

Related Commands

❖ Configuring an SNMP View

Command	**snmp-server view** *view-name oid-tree* { **include** | **exclude** }
Parameter Description	*view-name*: View name *oid-tree*: MIB objects associated with a view, which are displayed as an MIB subtree. **include:** Indicates that the MIB object subtree is included in the view. **exclude:** Indicates that the MIB object subtree is not included in the view.
Command Mode	Global configuration mode
Usage Guide	Specify a view name and use it for view-based management.

❖ Configuring an SNMP User Group

Command	**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]

Parameter Description	**v1** | **v2c** |**v3:** Specifies the SNMP version. **auth:** Messages sent by users in the group need to be verified but data confidentiality is not required. This configuration is valid for SNMPv3 only. **noauth:** Messages sent by users in the group do not need to be verified and data confidentiality is not required. This configuration is valid for SNMPv3 only. **priv:** Messages sent by users in the group need to be verified and confidentiality of transmitted data is required. This configuration is valid for SNMPv3 only. *readview*: Associates one read-only view. *writeview*: Associates one read/write view. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: IPv6 ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified.
Command Mode	Global configuration mode
Usage Guide	Associate certain users with a group and associate the group with a view. Users in a group have the same access permission. In this way, you can determine whether managed objects associated with an operation are in the allowable range of a view. Only managed objects in the range of a view can be accessed.

❖ Configuring an Authentication Name and Access Permission

Command	**snmp-server community** [*0* | *7*] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [**ipv6** *ipv6-aclname*] [*aclnum* | *aclname*]
Parameter Description	*0*: Indicates that the input community string is a plaintext string. *7*: Indicates that the input community string is a ciphertext string. *string*: Community string, which is equivalent to the communication password between the NMS and the SNMP agent. *view-name*: Specifies a view name for view-based management. **ro:** Indicates that the NMS can only read variables of the MIB. **rw:** The NMS can read and write variables of the MIB. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified. *ipaddr*: Associates NMS addresses and specifies NMS addresses for accessing the MIB.
Command Mode	Global configuration mode
Usage Guide	This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed.

	To disable the SNMP agent function, run the **no snmp-server** command.

❖ Configuring an SNMP User

Command	**snmp-server user** *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]
Parameter Description	*username*: User name. *groupname*: Specifies the group name for a user. **v1** | **v2c** | **v3:** Specifies the SNMP version. Only SNMPv3 supports later security parameters. **encrypted:** The specified password input mode is ciphertext input. Otherwise, plaintext is used for input. If ciphertext input is selected, enter a key consisting of continuous hexadecimal digits. An MD5 protocol authentication key consists of 16 bytes and an SHA authentication protocol key consists of 20 bytes. Two characters stand for one byte. Encrypted keys are valid for this engine only. **auth:** Specifies whether authentication is used. **md5:** Specifies the MD5 authentication protocol. **sha** specifies the SHA authentication protocol. *auth-password*: Configures a password string (not more than 32 characters) used by the authentication protocol. The system converts the passwords into the corresponding authentication keys. **priv:** Specifies whether confidentiality is used. **des56** specifies the use of the 56-bit DES encryption protocol. *priv-password*: Configures a password string (not more than 32 characters) used for encryption. The system converts the password into the corresponding encryption key. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: IPv6 ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified.
Command Mode	Global configuration mode
Usage Guide	Configure user information so that the NMS can communicate with the agent by using a valid user. For an SNMPv3 user, you can specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (at present, only DES is available), and encryption password.

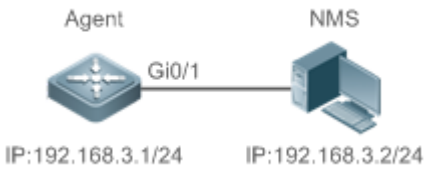
❖ Enabling the Agent Function

Command	**enable service snmp-agent**
Parameter Description	
Configuration mode	Privileged mode.
Usage Guide	This command is used to enable the SNMP agent function of a device.

❖ Displaying the SNMP Status Information

Command	**show snmp** [**mib** | **user** | **view** | **group| host | process-mib-time**]
Parameter Description	**mib:** Displays information about the SNMP MIB supported in the system. **user:** Displays information about an SNMP user. **view:** Displays information about an SNMP view. **group:** Displays information about an SNMP user group. **host:** Displays information about user configuration. **process-mib-time:** Displays the MIB node with the longest processing time.
Configuration mode	Privileged mode.
Usage Guide	N/A

❖ Configuration Example Configuring SNMP v1/2c

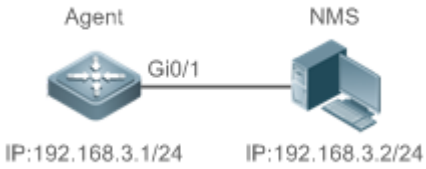
Scenario Figure 1-5	 ● The NMS is connected to an agent through the Ethernet. The IP address of the agent is 192.168.3.1/24, and the IP address of the NMS is 192.168.3.2/24. ● The NMS monitors and manages the agent through SNMP v1 or SNMP v2c.
	● When the agent is faulty or an error occurs, the agent can actively reports the related information to the NMS.
Configuration Steps	➢ Configure the SNMP basic information, including the version and community name. ➢ Allow the NMS (192.168.3.2/24) to send Trap messages. ➢ Configure the IP address of the agent, and set the IP address of the Gi0/1 interface to 192.168.3.1/24.

Agent	`Qtech(config)#snmp-server community public rw`
	`Qtech(config)#snmp-server host 192.168.3.2 traps version 2c public`
	`Qtech(config)#snmp-server enable traps`
	`Qtech(config)#interface gigabitEthernet 0/1`
	`Qtech(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0`
	`Qtech(config-if-gigabitEthernet 0/1)#exit`

Verification	➢ Run the **show running-config** command to display configuration information of the device.

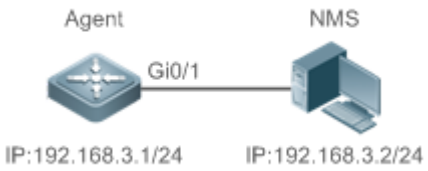
	➢ Run the **show snmp host** command to display the host information configured by the user.
NMS	On the NMS that uses the SNMP v1/v2c, configure the read/write community name, timeout time, and retry times. You can use the NMS to query and configure the device. Configurations on the NMS must be consistent with those on the device; otherwise, related operations cannot be performed.

❖ Configuring SNMP v3 (Default View)

Scenario **Figure 1-6**	 ● The NMS manages network devices (agents) based on the user authentication and encryption mode, for example, the NMS uses user1 as the user name, MD5 as the authentication mode, 123 as the authentication password, DES56 as the encryption algorithm, and 321 as the encryption password. ● You can access all MIB nodes. ("read default write default" indicates that all MIB nodes can be accessed.) ● Network devices can actively send authentication and encryption messages to the NMS.
Configuration Steps	➢ Configure an MIB group. Create a group “g1”, select the version “v3”, set the security level to the authentication and encryption mode “priv”, and configure permissions to read and write the view “default”. "Default" indicates that all MIB nodes can be accessed. ➢ Configure an SNMP user. Create a user named “user1” under group “g1”, select “v3” as the version, and set the authentication mode to “md5”, authentication password to “123”, encryption mode to “DES56”, and encryption password to “321”. ➢ Configure the SNMP host address. Set the host address to 192.168.3.2, select “3” as the version, set the security level to the authentication and encryption mode “priv”, and associate the user name “user1”. Enable the agent to actively send a trap message to the NMS. ➢ Configure the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	`Qtech(config)#snmp-server group g1 v3 priv read default write default` `Qtech(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321`

	Qtech(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 Qtech(config)#snmp-server enable traps Qtech(config)#interface gigabitEthernet 0/1 Qtech(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 Qtech(config-if-gigabitEthernet 0/1)#exit
Verification	➢ Run the **show running-config** command to display configuration information of the device. ➢ Run the **show snmp user** command to display the SNMP user. ➢ Run the **show snmp view** command to display the SNMP view. ➢ Run the **show snmp group** command to display the SNMP group. ➢ Run the **show snmp host** command to display the host information configured by the user. ➢ Install MIB-Browser.
NMS	SNMP v3 adopts the authentication and encryption security mechanisms. On the NMS, configure the user name, and select a security level. Based on the selected security level, configure the authentication mode, authentication password, encryption mode, and encryption password. In addition, configure the timeout time and retry times. You can use the NMS to query and configure the device. \ Configurations on the NMS must be consistent with those on the device; otherwise, related operations cannot be performed.

❖ Configuring SNMPv3 Configuration (Specified View)

Scenario **Figure 1-7**	 ● The NMS manages network devices (agents) based on the user authentication and encryption mode, for example, the NMS uses user1 as the user name, MD5 as the authentication mode, 123 as the authentication password, DES56 as the encryption algorithm, and 321 as the encryption password. ● Network devices can control the operation permission of users to access MIB objects. For example, the user named user1 can read MIB objects under the system node (1.3.6.1.2.1.1) and can only write MIB objects under the SysContact node (1.3.6.1.2.1.1.4.0).

	● Network devices can actively send authentication and encryption messages to the NMS.
Configuration Steps	➢ Configure a MIB view and a MIB group. Create a MIB view “view1”, which includes the associated MIB object (1.3.6.1.2.1.1); then create a MIB view “view2”, which includes the associated MIB object (1.3.6.1.2.1.1.4.0). Create a group “g1”, select the version “v3”, set the security level to the authentication and encryption mode “priv”, and configure permissions to read the view “view1” and write the view “view2”. ➢ Configure an SNMP user. Create a user named “user1” under group “g1”, select “v3” as the version, and set the authentication mode to “md5”, authentication password to “123”, encryption mode to “DES56”, and encryption password to “321”. ➢ Configure the SNMP host address. Set the host address to 192.168.3.2, select “3” as the version, set the security level to the authentication and encryption mode “priv”, and associate the user name “user1”. Enable the agent to actively send a trap message to the NMS. ➢ Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.

Agent	`Qtech(config)#snmp-server view view1 1.3.6.1.2.1.1 include`
	`Qtech(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include`
	`Qtech(config)#snmp-server group g1 v3 priv read view1 write view2`
	`Qtech(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321`
	`Qtech(config)#snmp-server host 192.168.3.2 traps version 3 priv user1`
	`Qtech(config)#snmp-server enable traps`
	`Qtech(config)#interface gigabitEthernet 0/1`
	`Qtech(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0`
	`Qtech(config-if-gigabitEthernet 0/1)#exit`

Verification	1. Run the **show running-config** command to display configuration information of the device. 2. Run the **show snmp user** command to display the SNMP user. 3. Run the **show snmp view** command to display the SNMP view. 4. Run the **show snmp group** command to display the SNMP group. 5. Run the **show snmp host** command to display the host information configured by the user. 6. Install MIB-Browser.
Agent	`Qtech# show running-config` `!`

```
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56
D5CEC4884360373ABBF30AB170E42D03
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
snmp-server enable traps
```

```
Qtech# show snmp user
User name: user1
Engine ID: 800013110308c6b3221120
storage-type: permanent     active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

```
Qtech#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

```
Qtech# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

```
Qtech#show snmp host
Notification host: 192.168.3.2
udp-port: 162
```

	type: trap user: user1 security model: v3 authPriv
	Install MIB-Browser, enter IP address **192.168.3.1** in **IP Address** and **user1** in **UserName**, select **AuthPriv** for **Security Level**, enter **123** in **AuthPassWord**, select **MD5** for **AuthProtocol**, and enter **321** in **PrivPassWord**. Click **Add Item** and select a management unit for which the MIB needs to be queried, for example, **System** in the following figure. Click **Start**. The MIB is queried for network devices.

Common Errors

-

1.4.2 Enabling the Trap Function

Configuration Effect

Enable the agent to actively send a trap message to the NMS.

Notes

N/A

Configuration Steps

- ❖ Configuring the SNMP Host Address
- Optional
- Configure the host address of the NMS when the agent is required to actively send messages.
- ❖ Enabling the Agent to Actively Send a Trap Message to the NMS
- Optional
- Configure this item on the agent when the agent is required to actively send a trap message to the NMS.
- ❖ Enabling the Function of Sending a Link Trap Message on an Interface
- Optional
- Configure this item on the agent when a link trap message needs to be sent on an interface.
- ❖ Enabling the Function of Sending a System Reboot Trap Message
- Optional

- Configure this item on the agent when the QOS system is required to send a trap message to the NMS to notify system reboot before reloading or reboot of the device.

❖ Specifying the Source Address for Sending a Trap Message

- Optional
- Configure this item on the agent when it is required to permanently use a local IP address as the source SNMP address to facilitate management.

❖ Enabling a Trap Message to Carry Private Fields when the Message Is Sent

- Optional
- Configure this item on the agent when private fields need to be carried in a trap message.

Verification

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

❖ Setting the NMS Host Address

Command	**snmp-server host** { *host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps | inrorms**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]
Parameter Description	*host-addr*: Address of the SNMP host. *ipv6-addr*: (IPv6) address of the SNMP host. *Vrfname*: Configures a VRF forwarding table name. **traps | informs:** Configures the host to send a trap message or an inform message. **version:** SNMP version, which can be set to **V1**, **V2C**, or **V3**. **auth** | **noauth** | **priv:** Sets the security level of V3 users. *community-string*: Community string or user name (V3). *port-num*: Configures the port ID of the SNMP host. *notification-type*: Type of trap messages that are actively sent, for example, snmp. ➢ If no trap type is specified, all trap messages are sent.
Command Mode	Global configuration mode
Usage Guide	This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS. You can configure different SNMP hosts to receive trap messages. A host can support different traps, ports, and VRF forwarding tables. If the same host is configured (the port and VRF configuration are the same), the last configuration is combined with the previous configurations, that is, to send different trap messages to the same host, configure one type of trap messages each time. These configurations are finally combined.

❖ Enabling the Agent to Actively Send a Trap Message to the NMS

Command	**snmp-server enable traps** [*notification-type*]
Parameter Description	*notification-type*: Enables trap notification for the corresponding events, including the following types: snmp: Enables trap notification for SNMP events. bgp: Enables trap notification for BGP events. bridge: Enables trap notification for bridge events. isis: Enables trap notification for ISIS events. mac-notification: Enables trap notification for MAC events. ospf: Enables trap notification for OSPF events. urpf: Enables trap notification for URPF events. vrrp: Enables trap notification for VRRP events. web-auth: Enables trap notification for Web authentication events.
Command Mode	Global configuration mode
Usage Guide	This command must be used with the **snmp-server host** command to so that trap messages can be actively sent.

❖ Enabling the Function of Sending a Link Trap Message on an Interface

Command	**snmp trap link-status**
Parameter Description	**-**
Configuration mode	Interface configuration mode
Usage Guide	For interfaces (Ethernet interface, AP interface, and SVI interface), when this function is enabled, the SNMP sends a Link Trap message if the link status on the interfaces changes. Otherwise, the SNMP does not send the message.

❖ Enabling the Function of Sending a System Reboot Trap Message

Command	**snmp-server system-shutdown**
Parameter Description	-
Configuration mode	Global configuration mode
Usage Guide	When the function of notification upon SNMP system reboot is enabled, a trap message is sent to the NMS to notify system reboot before reloading or reboot of the device.

❖ Specifying the Source Address for Sending a Trap Message

Command	**snmp-server trap-source** *interface*
Parameter Description	*interface*: Used as the interface for the SNMP source address.

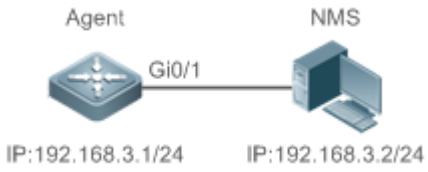
Configuration mode	Global configuration mode
Usage Guide	By default, the IP address of the interface where SNMP packets are sent is used as the source address. To facilitate management and identification, this command can be run to permanently use one local IP address as the source SNMP address.

❖ Enabling a Trap message to Carry Private Fields when the Message Is Sent

Command	**snmp-server trap-format private**
Parameter Description	-
Configuration mode	Global configuration mode
Usage Guide	This command can be used to enable a trap message to carry private fields when the message is sent. At present, supported private fields include the alarm generation time. For the specific data types and data ranges of the fields, see QTECH-TRAP-FORMAT-MIB.mib.

Configuration Example

❖ Enabling the Trap Function

Scenario Figure 1-8	 ● The NMS manages network devices (agents) based on the community authentication mode, and network devices can actively send messages to the NMS.
Configuration Steps	1. Perform configuration to enable the agent to actively send messages to the NMS. Set the SNMP host address to 192.168.3.2, the message format to Version2c, and the authentication name to user1. Enable the agent to actively send trap messages. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.

Agent	`Qtech(config)#snmp-server host 192.168.3.2 traps version 2c user1`
	`Qtech(config)#snmp-server enable traps`
	`Qtech(config)#interface gigabitEthernet 0/1`
	`Qtech(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0`
	`Qtech(config-if-gigabitEthernet 0/1)#exit`

Verification	● Run the **show running-config** command to display configuration information of the device. ● Run the **show snmp** command to display the SNMP status.
Agent	Qtech# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 snmp-server view v1 1.3.6.1.2.1.1 include snmp-server location snmp-server host 192.168.3.2 traps version 2c user1 snmp-server enable traps snmp-server contact Qtech.ru snmp-server community user1 view v1 rw a1 snmp-server chassis-id 1234567890
	Qtech#show snmp Chassis: 1234567890 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1472) 0 No such name errors 0 Bad values errors 0 General errors

	0 Response PDUs 0 Trap PDUs SNMP global trap: enabled SNMP logging: disabled SNMP agent: enabled

Common Errors

N/A

1.4.3 Shielding the Agent Function

Configuration Effect

Shield the agent function when the agent service is not required.

Notes

- Run the **no snmp-server** command to shield the SNMP agent function when the agent service is not required.
- Different from the shielding command, after the **no enable service snmp-agent** command is run, all SNMP services are directly disabled (that is, the SNMP agent function is disabled, no packet is received, and no response packet or trap packet is sent), but configuration information of the agent is not shielded.

Configuration Steps

❖ Shielding the SNMP Agent Function for the Device

- Optional
- To shield the configuration of all SNMP agent services, use this configuration.

❖ Disabling the SNMP Agent Function for the Device

- Optional
- To directly disable all services, use this configuration.

Verification

Run the **show services** command to check whether SNMP services are enabled or disabled.

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

❖ Shielding the SNMP Agent Function for the Device

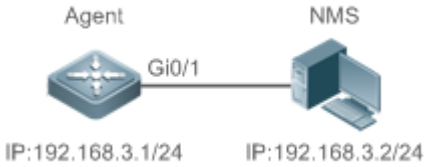
Command	no snmp-server
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the SNMP agent function is disabled. When SNMP agent parameters (for example, NMS host address, authentication name, and access permission) are set, the SNMP agent service is automatically enabled. The **enable service snmp-agent** command must also be run at the same time so that the SNMP agent service can take effect. If the SNMP agent service is disabled or the **enable service snmp-agent** command is not run, the SNMP agent service does not take effect. Run the **no snmp-server** command to disable SNMP agent services of all versions supported by the device. After this command is run, all SNMP agent service configurations are shielded (that is, after the **show running-config** command is run, no configuration is displayed. Configurations are restored after the SNMP agent service is enabled again). After the **enable service snmp-agent** command is run, the SNMP agent configurations are not shielded.

❖ Disabling the SNMP Agent Function for the Device

Command	no enable service snmp-agent
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	This command can be used to disable the SNMP service, but it will not shield SNMP agent parameters.

Configuration Example

❖ Enabling the SNMP Service

Scenario Figure 1-1	 After the SNMP service is enabled and the SNMP agent server is set, the NMS can access devices based on SNMP.

Configuration Steps	1. Enable the SNMP service. 2. Set parameters for the SNMP agent server to make the SNMP service take effect.
A gent	`Qtech(config)#enable service snmp-agent`
Verification	1. Run the **show services** command to check whether the SNMP service is enabled or disabled.

Agent	`Qtech#show service`
	`web-server : disabled`
	`web-server(https): disabled`
	`snmp-agent : enabled`
	`ssh-server : disabled`
	`telnet-server : enabled`

Common Errors

N/A

1.4.4 Setting SNMP Control Parameters

Configuration Effect

Set basic parameters of the SNMP agent, including the device contact mode, device location, serial number, and parameters for sending a trap message. By accessing the parameters, the NMS can obtain the contact person of the device and physical location of the device.

Notes

N/A

Configuration Steps

- ❖ Setting the System Contact Mode
- Optional
- When the contact mode of the system needs to be modified, configure this item on the agent.
- ❖ Setting the System Location
- Optional
- When the system location needs to be modified, configure this item on the agent.
- ❖ Setting the System Serial Number

- Optional
- When the system serial number needs to be modified, configure this item on the agent.

❖ Setting NE Information about the Device

- Optional
- When the NE code needs to be modified, configure this item on the agent.

❖ Setting the Maximum Packet Length of the SNMP Agent

- Optional
- When the maximum packet length of the SNMP agent needs to be modified, configure this item on the agent.

❖ Setting the UDP Port ID of the SNMP Service

- Optional
- When the UDP port ID of the SNMP service needs to be modified, configure this item on the agent.

❖ Setting the Queue Length of Trap Messages

- Optional
- When the size of the message queue needs to be adjusted to control the message sending speed, configure this item on the agent.

❖ Setting the Interval for Sending a Trap Message

- Optional
- When the interval for sending a trap message needs to be modified, configure this item o the agent.

❖ Configuring SNMP Flow Control

- Optional
- If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Verification

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

❖ Setting the System Contact Mode

Command	**snmp-server contact** *text*
Parameter Description	*text*: String that describes the system contact mode.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Setting the System Location

Command	**snmp-server location** *text*
Parameter Description	*text*: String that describes system information.
Configuration mode	Global configuration mode
Usage Guide	N/A

❖ Setting the System Serial Number

Command	**snmp-server chassis-id** *text*
Parameter Description	*text*: Text of the system serial number, which may be digits or characters.
Configuration mode	Global configuration mode
Usage Guide	In general, the device serial number is used as the SNMP serial number to facilitate identification of the device.

❖ Setting NE Information about the Device

Command	**snmp-server net-id** *text*
Parameter Description	*text*: Text that is used to set the device NE code. The text is a string that consists of 1 to 255 characters that are case-sensitive and may include spaces.
Configuration mode	Global mode.
Usage Guide	Set the NE code of the device.

❖ Setting the Maximum Packet Length of the SNMP Agent

Command	**snmp-server packetsize** *byte-count*
Parameter Description	*byte-count*: Packet size, ranging from 484 bytes to 17,876 bytes.
Configuration mode	Global mode.
Usage Guide	N/A

❖ Setting the UDP Port ID of the SNMP Service

Command	**snmp-server udp-port** *port-num*

Parameter Description	*port-num*: Specifies the UDP port ID of the SNMP service, that is, the ID of the protocol port that receives SNMP packets.
Configuration mode	Global mode.
Usage Guide	Specify the protocol port ID for receiving SNMP packets.

❖ Setting the Length of a Trap Message Queue

Command	**snmp-server queue-length** *length*
Parameter Description	*length*: Queue length, ranging from 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the size of the message queue to control the message sending speed.

❖ Setting the Interval for Sending a Trap Message

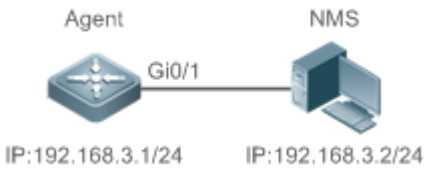
Command	**snmp-server trap-timeout** *seconds*
Parameter Description	*seconds*: Interval (unit: second). The value range is 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the interval for sending a message to control the message sending speed.

❖ Configuring SNMP Flow Control

Command	**snmp-server flow-control pps** [count]
Parameter Description	count**:** Number of SNMP request packets processed per second. The value range is 50 to 65,535.
Command Mode	Global configuration mode
Usage Guide	If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Configuration Example

❖ Setting SNMP Control Parameters

Scenario Figure 1-2	

	• The NMS manages network devices (agents) based on the community authentication mode and can obtain basic system information about the devices, for example, system contact mode, location, and serial number.
Configuration Steps	1. Set SNMP agent parameters. Set the system location, contact mode, and serial number. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.

Agent	`Qtech(config)#snmp-server location Moscow`
	`Qtech(config)#snmp-server contact Qtech.ru`
	`Qtech(config)#snmp-server chassis-id 1234567890`
	`Qtech(config)#interface gigabitEthernet 0/1`
	`Qtech(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0`
	`Qtech(config-if-gigabitEthernet 0/1)#exit`

Verification	1. Check the configuration information of the device. 2. Check the SNMP view and group information.

Agent	`Qtech# show running-config`
	`ip access-list standard a1`
	`10 permit host 192.168.3.2`
	`interface gigabitEthernet 0/1`
	`no ip proxy-arp`
	`ip address 192.168.3.1 255.255.255.0`
	`snmp-server view v1 1.3.6.1.2.1.1 include`
	`snmp-server location Moscow`
	`snmp-server host 192.168.3.2 traps version 2c user1`
	`snmp-server enable traps`
	`snmp-server contact Qtech.ru`
	`snmp-server community user1 view v1 rw a1`
	`snmp-server chassis-id 1234567890`

	`Qtech#show snmp view`
	`v1(include) 1.3.6.1.2.1.1`
	`default(include) 1.3.6.1`
	`Qtech#show snmp group`

```
groupname: user1
securityModel: v1
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
groupname: user1
securityModel: v2c
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
```

Common Errors

N/A

1.5 Monitoring

Displaying

Description	Command
Displays the SNMP status.	**show snmp** [**mib** | **user** | **view** | **group**| **host**]

2. CONFIGURING RMON

2.1 Overview

The Remote Network Monitoring (RMON) aims at resolving problems of managing local area networks (LANs) and remote sites by using one central point. In RMON, network monitoring data consists of a group of statistics and performance indicators, which can be used for monitoring the network utilization, so as to facilitate network planning, performance optimization, and network error diagnosis.

RMON is mainly used by a managing device to remotely monitor and manage managed devices.

Protocols and Standards

STD 0059 / RFC 2819: Remote Network Monitoring Management Information Base

RFC4502: Remote Network Monitoring Management Information Base Version 2

RFC 3919: Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)

RFC 3737: IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB Modules

RFC 3434: Remote Monitoring MIB Extensions for High Capacity Alarms

RFC 3395: Remote Network Monitoring MIB Protocol Identifier Reference Extensions

RFC 3287: Remote Monitoring MIB Extensions for Differentiated Services

RFC 3273: Remote Network Monitoring Management Information Base for High Capacity Networks

RFC 2896: Remote Network Monitoring MIB Protocol Identifier Macros

RFC 2895: Remote Network Monitoring MIB Protocol Identifier Reference

2.2 Applications

Application	Description
Collecting Statistics on Information of a Monitored Interface	Applies four functions of RMON to an interface to monitor the network communication of the interface.

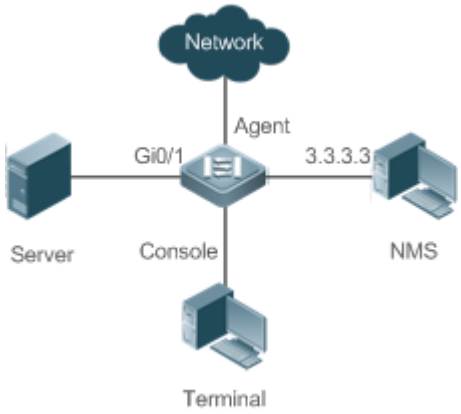
2.2.1 Collecting Statistics on Information of a Monitored Interface

Scenario

The RMON Ethernet statistics function is used to monitor accumulated information of an interface, the history statistics function is used to monitor the packet count of an interface within each

monitoring interval, and the alarm function is used to immediately acquire packet count exceptions of an interface. The following figure shows the networking topology.

Figure 2-1



Deployment

Interface x is monitored to accumulatively collect statistics on the packet count of the interface and collect statistics on the packet count and bandwidth utilization of the interface within the monitoring interval. If a packet count exception occurs on the interface, an alarm is reported to the network management system (NMS). The configuration key points are as follows:

- Configure the RMON Ethernet statistics function on interface x.
- Configure the RMON history statistics function on interface x.
- Configure the RMON alarm table and define RMON event processing actions in configuration mode. Monitored objects of alarms are the object identifier (OID) values of specific fields in the RMON Ethernet statistical table configured for interface x.

2.3 Features

Basic Concepts

RMON defines multiple RMON groups. Qtech products support the statistics group, history group, alarm group, and event group, which are described as follows:

❖ Statistics Group

The statistics group is used to monitor and collect statistics on Ethernet interface traffic information, which is accumulated from the entry creation time to the current time. The statistical items include discarded data packets, broadcast data packets, cyclic redundancy check (CRC) errors, large and small blocks, and collisions. Statistical results are stored in the Ethernet statistical table.

❖ History Group

The history group is used to periodically collect network traffic information. It records accumulated values of network traffic information and the bandwidth utilization within each interval, and saves them in the history control table. It includes two small groups:

- The HistoryControl group is used to set the sampling interval, sampling data source, and other control information.
- The EthernetHistory group provides administrators with historical data, including statistics on network segment traffic, error packets, broadcast packets, utilization, and number of collisions.

❖ Alarm Group

The alarm group is used to monitor a specified Management Information Base (MIB) object. When the value of a MIB object exceeds the preset upper limit or is lower than the preset lower limit, an alarm is triggered and the alarm is processed as an event.

❖ Event Group

The event group is used to define the event processing mode. When a monitored MIB object meets alarm conditions, an event is triggered. An event can be processed in any of the following modes:

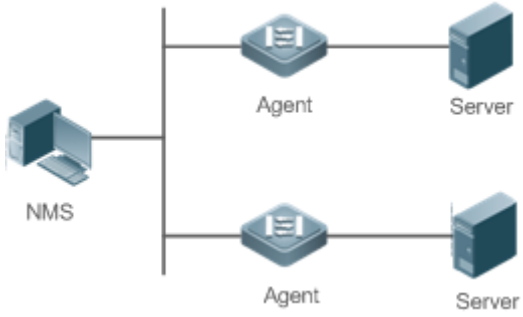
- none: No action is taken.
- log: Event-relevant information is recorded in the log record table so that administrators can view it at any time.
- snmp-trap: A trap message is transmitted to the NMS to notify the NMS of the event occurrence.
- log-and-trap: Event-relevant information is recorded in the log record table and a trap message is transmitted to the NMS.

Working Principle

RMON supports multiple monitors and two data collection methods. Method 1: A dedicated RMON probe is used to collect data and the NMS can directly acquire all information about the RMON MIB from the RMON probe. Method 2: RMON agents are built into network devices so that the devices have the RMON probe function. The NMS uses basic commands of the Simple Network Management Protocol (SNMP) to exchange data with the RMON agents and collect network management information. This method, however, is limited by device resources and information of only four groups rather than all data of the RMON MIB is acquired.

The following figure shows an example of communication between the NMS and RMON agents. The NMS, through the RMON agents running on devices, can acquire information about overall traffic, error statistics, and performance statistics of the network segment where a managed network device interface is, thereby implementing remote management of network devices.

Figure 2-2



Overview

Feature	Description
RMON Ethernet Statistics	Collects statistics on the packet count, byte count, and other data of a monotored Ethernet interface accumulatively.
RMON History Statistics	Records the counts of packets, bytes, and other data communicated by an Ethernet interface within the configured interval and calculates the bandwidth utilization within the interval.
RMON Alarm	Samples values of monitored variables at intervals. The alarm table is used in combination with the event table. When the upper or lower limit is reached, a relevant event table is triggered to perform event processing or no processing is performed.

2.3.1 RMON Ethernet Statistics

Working Principle

The RMON Ethernet statistics function accumulatively collects statistics on network traffic information of an Ethernet interface from the entry creation time to the current time.

Related Configuration

❖ Configuring RMON Statistical Entries

- The RMON Ethernet statistics function is disabled by default.
- Run the **rmon collection stats** command to create Ethernet statistical entries on a specified Ethernet interface.
- After statistical entries are successfully created on a specified interface, the statistics group collects statistics on the traffic information of the current interface. The statistical items are variables defined in the RMON Ethernet statistical table, and recorded information is the accumulated values of variables from the creation time of the RMON statistical table to the current time.

2.3.2 RMON History Statistics

Working Principle

The RMON history statistics function records accumulated statistics on traffic information of an Ethernet interface within each interval.

Related Configuration

❖ Configuring RMON Historical Control Entries

- The RMON history statistics function is disabled by default.
- Run the **rmon collection history** command to create historical control entries on an Ethernet interface.
- The RMON history group collects statistics on variables defined in the RMON history table and records accumulated values of variables within each interval.

2.3.3 RMON Alarm

Working Principle

The RMON alarm function periodically monitors value changes of alarm variables. If the value of an alarm variable reaches the specified upper threshold or lower threshold, a corresponding event is triggered for processing, for example, a trap message is transmitted or one logTable entry record is generated. If a lower threshold or upper threshold is reached multiple times consecutively, only one corresponding event is triggered and another event is triggered till a reverse threshold is reached.

Related Configuration

❖ Configuring the Event Table

- The RMON event group function is disabled by default.
- Run the **rmon event** command to configure the event table.

❖ Configuring Alarm Entries

- The RMON alarm group function is disabled by default.
- Run the **rmon event** command to configure the event table and run the **rmon alarm** command to configure the RMON alarm table.
- The RMON alarm function is implemented by the alarm table and event table jointly. If a trap message needs to be transmitted to a managing device in the case of an alarm event, the SNMP

agent must be correctly configured first. For the configuration of the SNMP agent, see the *Configuring SNMP*.

- If a configured alarm object is a field node in the RMON statistics group or history group, the RMON Ethernet statistics function or RMON history statistics function need to be configured on a monitored Ethernet interface first.

2.4 Configuration

Configuration	Description and Command	
Configuring RMON Ethernet Statistics	(Mandatory) It is used to accumulatively collect statistics on traffic information of an Ethernet interface.	
	rmon collection stats	Configures Ethernet statistical entries.
Configuring RMON History Statistics	(Mandatory) It is used to collect, at intervals, statistics on traffic information of an Ethernet interface and the bandwidth utilization within the interval.	
	rmon collection history	Configures historical control entries.
Configuring RMON Alarm	(Mandatory) It is used to monitor whether data changes of a variable is within the valid range.	
	rmon event	Configures event entries.
	rmon alarm	Configures alarm entries.

2.4.1 Configuring RMON Ethernet Statistics

Configuration Effect

Acquire accumulated statistics on traffic information of a monitored Ethernet interface from the entry creation time to the current time.

Notes

This function cannot be configured in batch interface configuration mode.

Configuration Steps

❖ Configuring RMON Statistical Entries

- Mandatory.
- If statistics and monitoring are required for a specified interface, Ethernet statistical entries must be configured on this interface.

Verification

Run the **show rmon stats** command to display Ethernet statistics.

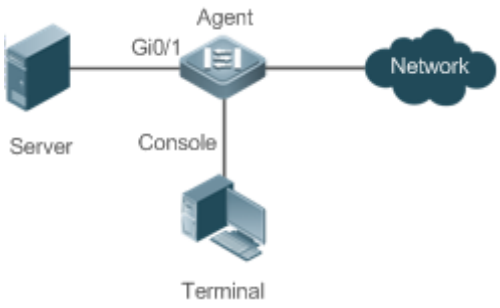
Related Commands

❖ Configuring RMON Statistical Entries

Command	**rmon collection stats** *index* [**owner** *ownername*]
Parameter Description	*index*: Indicates the index number of a statistical entry, with the value ranging from 1 to 65,535. **owner** *ownername*: Indicates the entry creator, that is, *ownername*, which is a case-sensitive string of 1-63 characters.
Command Mode	Interface configuration mode
Usage Guide	The values of statistical entry parameters cannot be changed.

Configuration Example

❖ Configuring RMON Ethernet Statistics

Scenario **Figure 2-3**	
	As shown in the preceding figure, the RMON agent is connected to the server, and the NMS requires the RMON statistics group to conduct performance statistics on received packets of interface Gi0/1. Administrators can view the statistics at any time to understand data about received packets of an interface and take measures in a timely manner to handle network exceptions.
Configuration Steps	➢ Configure a statistical table instance on interface GigabitEthernet 0/1 to collect statistics on the traffic of this interface.

Agent	`Qtech# configure terminal`
	`Qtech (config)# interface gigabitEthernet 0/1`
	`Qtech (config-if-GigabitEthernet 0/1)# rmon collection stats 1 owner admin`

Verification	Run the **show rmon stats** command to display Ethernet statistics.
Agent	`Qtech# show rmon stats` `ether statistic table:`

```
index = 1
interface = GigabitEthernet 0/1
owner = admin
status = 1
dropEvents = 0
octets = 25696
pkts = 293
broadcastPkts = 3
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
packets640ctets = 3815
packets65To1270ctets = 1695
packets128To2550ctets = 365
packets256To5110ctets = 2542
packets512To10230ctets = 152
packets1024To15180ctets = 685
```

Common Errors

Statistical table entries are re-configured or configured statistical table entries are modified.

2.4.2 Configuring RMON History Statistics

Configuration Effect

Acquire accumulated statistics on the traffic of a monitored Ethernet interface and the bandwidth utilization within each interval.

Notes

This function cannot be configured in batch interface configuration mode.

Configuration Steps

- Mandatory.
- If network statistics on a specified interface need to be collected, RMON historical control entries must be configured on the interface.

Verification

Run the **show rmon history** command to display history group statistics.

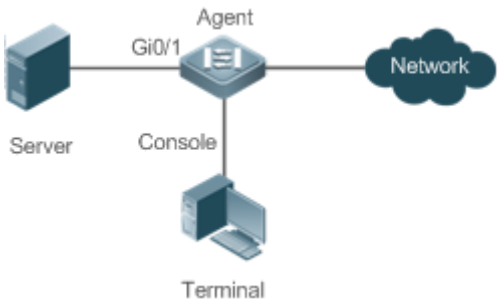
Related Commands

❖ Configuring RMON Historical Control Entries

Command	**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]
Parameter Description	*index*: Indicates the index number of a history statistical entry, with the value ranging from 1 to 65,535. **owner** *ownername*: Indicates the entry creator, that is, *ownername*, which is a case-sensitive string of 1-63 characters. **buckets** *bucket-number*: Sets the capacity of the history table in which a history statistical entry exists, that is, sets the maximum number of records (*bucket-number*) that can be accommodated in the history table. The value of *bucket-number* ranges from 1 to 65,535 and the default value is **10**. **interval** *seconds*: Sets the statistical interval, with the unit of seconds. The value ranges from 1 second to 3,600 seconds and the default value is **1,800** seconds.
Command Mode	Interface configuration mode
Usage Guide	The values of history statistical entry parameters cannot be changed.

Configuration Example

❖ Configuring RMON History Statistics

Scenario **Figure 2-4**	
	As shown in the preceding figure, the RMON agent is connected to the server, and the NMS needs to collect statistics on received packets of interface Gi0/1 through the RMON history group at an interval of 60 seconds, in an effort to monitor the network and understand emergency data.

Configuration Steps	➢ Configure the history control table on interface GigabitEthernet 0/1 to periodically collect statistics on the traffic of this interface.
Agent	Qtech# configure terminal Qtech(config)# interface gigabitEthernet 0/1 Qtech(config-if-GigabitEthernet 0/1)# rmon collection history 1 buckets 5 interval 300 owner admin
Verification	Run the **show rmon history** command to display history group statistics.
Agent	Qtech# show rmon history rmon history control table: index = 1 interface = GigabitEthernet 0/1 bucketsRequested = 5 bucketsGranted = 5 interval = 60 owner = admin stats = 1 rmon history table: index = 1 sampleIndex = 786 intervalStart = 6d:18h:37m:38s dropEvents = 0 octets = 2040 pkts = 13 broadcastPkts = 0 multiPkts = 0 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 jabbers = 0 collisions = 0 utilization = 0

```
index = 1
sampleIndex = 787
intervalStart = 6d:18h:38m:38s
dropEvents = 0
octets = 1791
pkts = 16
broadcastPkts = 1
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
sampleIndex = 788
intervalStart = 6d:18h:39m:38s
dropEvents = 0
octets = 432
pkts = 6
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
```

```
sampleIndex = 789
intervalStart = 6d:18h:40m:38s
dropEvents = 0
octets = 432
pkts = 6
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
sampleIndex = 790
intervalStart = 6d:18h:41m:38s
dropEvents = 0
octets = 86734
pkts = 934
broadcastPkts = 32
multiPkts = 23
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0
```

Common Errors

History control table entries are re-configured or configured history control table entries are modified.

2.4.3 Configuring RMON Alarm

Configuration Effect

Periodically monitor whether value changes of alarm variables are within the specified valid range.

Notes

If a trap message needs to be transmitted to a managing device when an alarm event is triggered, the SNMP agent must be correctly configured. For the configuration of the SNMP agent, see the *Configuring SNMP*.

If an alarm variable is a MIB variable defined in the RMON statistics group or history group, the RMON Ethernet statistics function or RMON history statistics function must be configured on the monitored Ethernet interface. Otherwise, an alarm table fails to be created.

Configuration Steps

❖ Configuring Event Entries

- Mandatory.
- Complete the configuration in global configuration mode.

❖ Configuring Alarm Entries

- Mandatory.
- Complete the configuration in global configuration mode.

Verification

- Run the **show rmon event** command to display the event table.
- Run the **show rmon alarm** command to display the alarm table.

Related Commands

❖ Configuring the Event Table

Command	**rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]
Parameter Description	*number*: Indicates the index number of an event table, with the value ranging from 1 to 65,535. **log**: Indicates a log event. The system logs a triggered event. **trap** *community*: Indicates a trap event. When an event is triggered, the system transmits a trap message with the community name of *community*. **description** *description-string*: Sets the description information about an event, that is, *description-string*. The value is a string of 1-127 characters. **owner** *ownername*: Indicates the entry creator, that is, *ownername*, which is a case-sensitive string of 1-63 characters.

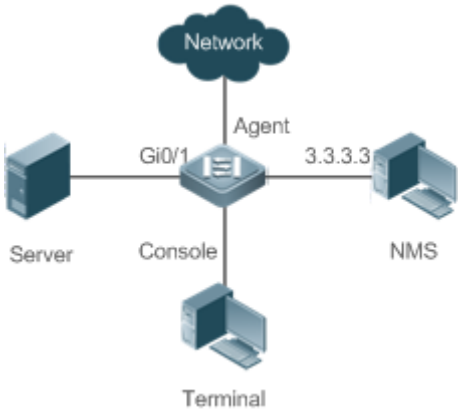
Command Mode	Global configuration mode
Usage Guide	The values of configured event entry parameters can be changed, including the event type, trap community name, event description, and event creator.

❖ Configuring the RMON Alarm Group

Command	**rmon alarm** *number variable interval* {**absolute	delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]
Parameter Description	*number*: Indicates the index number of an alarm entry, with the value ranging from 1 to 65,535. *variable*: Indicates an alarm variable, which is a string of 1-255 characters and is represented in dotted format using the node OID (format: entry.integer.instance; example: 1.3.6.1.2.1.2.1.10.1). *Interval*: Indicates the sampling interval, with the unit of seconds and the value ranging from 1 to 2,147,483,647. **absolute**: Indicates that the sampling type is absolute value sampling, that is, variable values are directly extracted when the sampling time is up. **delta**: Indicates that the sampling type is changing value sampling, that is, changes in the variable values within the sampling interval are extracted when the sampling time is up. **rising-threshold** *value*: Sets the upper limit of the sampling quantity (*value*), with the value ranging from -2,147,483,648 to +2,147,483,647. *event-number:* Indicates that an event with the event number of *event-number* is triggered when the upper limit or lower limit is reached. **falling-threshold** *value*: Sets the lower limit of the sampling quantity (*value*), with the value ranging from -2,147,483,648 to +2,147,483,647. **owner** *ownername*: Indicates the entry creator, that is, *ownername*, which is a case-sensitive string of 1-63 characters.
Command Mode	Global configuration mode
Usage Guide	Values of configured alarm entry parameters can be changed, including alarm variables, sampling type, entry creator, sampling interval, upper/lower limit of the sampling quantity, and relevant trigger events.

Configuration Example

❖ Configuring RMON Alarm

Scenario **Figure 2-5**	
	Assume that SNMPv1 runs on the NMS, the community name used for accessing the settings is public, with the attribute of read-write, and the IP address used by the NMS to receive trap messages is 3.3.3.3. Assume that the OID value of unknown protocol packets received by monitored interface GigabitEthernet0/3 is 1.3.6.1.2.1.2.2.1.15.3, the sampling mode is relative sampling, and the sampling interval is 60 seconds. When the relative sampling value is larger than 100 or lower than 10, event 1 and event 2 are triggered respectively. In event 1, a trap message is transmitted and the event is logged. In event 2, the event is only logged. The configuration of the RMON agent is completed on the terminal. The RMON agent is connected to the NMS and is connected to the server through interface GI0/1. The RMON agent needs to monitor the count of unknown protocol packets received by interface GI0/1. The sampling interval is 60 seconds. When the absolute sampling value is smaller than 10, the event is only logged. When the absolute sampling value is larger than 100, the event is logged and a trap message is transmitted to the NMS.
Configuration Steps	➢ Configure the host address for receiving trap messages. ➢ Configure an event group to process alarm trigger. ➢ Configure the alarm function.

Agent	`Qtech# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Qtech(config)# snmp-server community public rw`
	`Qtech(config)# snmp-server host 3.3.3.3 trap public`
	`Qtech(config)# rmon event 1 description rising-threshold-event log trap public owner admin`
	`Qtech(config)# rmon event 2 description falling-threshold-event log owner admin`
	`Qtech(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.15.3 60 delta rising-threshold 100 1 falling-threshold 10 2 owner admin`

Verification	➢ Run the **show rmon event** command to display the event table. ➢ Run the **show rmon alarm** command to display the alarm table.

Agent

```
Qtech# show rmon event
rmon event table:
                    index = 1
                    description = rising-threshold-event
                    type = 4
                    community = public
                    lastTimeSent = 0d:0h:0m:0s
                    owner = admin
                    status = 1

                    index = 2
                    description = falling-threshold-event
                    type = 2
                    community =
                    lastTimeSent = 6d:19h:21m:48s
                    owner = admin
                    status = 1

rmon log table:
                    eventIndex = 2
                    index = 1
                    logTime = 6d:19h:21m:48s
                    logDescription = falling-threshold-event
Qtech# show rmon alarm
rmon alarm table:
           index: 1,
           interval: 60,
           oid = 1.3.6.1.2.1.2.2.1.15.3
           sampleType: 2,
           alarmValue: 0,
           startupAlarm: 3,
           risingThreshold: 100,
           fallingThreshold: 10,
```

	risingEventIndex: 1, fallingEventIndex: 2, owner: admin, stauts: 1

Common Errors

- The entered OID of a monitored object is incorrect, the variable corresponding to the OID does not exist, or the type is not an integer or unsigned integer.
- The upper threshold is smaller than or equal to the lower threshold.

2.5 Monitoring

Displaying

Description	Command
Displays all RMON configuration information.	**show rmon**
Displays the Ethernet statistical table.	**show rmon stats**
Displays the history control table.	**show rmon history**
Displays the alarm table.	**show rmon alarm**
Displays the event table.	**show rmon event**

3. CONFIGURING NTP

3.1 Overview

The Network Time Protocol (NTP) is an application-layer protocol that enables network devices to synchronize time. NTP enables network devices to synchronize time with their servers or clock sources and provides high-precision time correction (the difference from the standard time is smaller than one millisecond in a LAN and smaller than decades of milliseconds in a WAN). In addition, NTP can prevent attacks by using encrypted acknowledgment.

Currently, Qtech devices can be used both as NTP clients and NTP servers. In other words, a Qtech device can synchronize time with a time server, and be used as a time server to provide time synchronization for other devices. When a Qtech device is used as a server, it supports only the unicast server mode.

Protocols and Standards

- RFC 1305 : Network Time Protocol (Version 3)

3.2 Applications

Application	Description
Synchronizing Time Based on an External Reference Clock Source	A device is used as a client that synchronizes time with an external clock source. After successful synchronization, it is used as a server to provide time synchronization for other devices.
Synchronizing Time Based on a Local Reference Clock Source	A device uses a local clock as a reliable NTP reference clock source and is also used as a server to provide time synchronization for other devices.

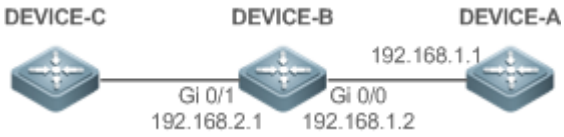
3.2.1 Synchronizing Time Based on an External Reference Clock Source

Scenario

As shown in Figure 3-1

- DEVICE-A is used as a reliable reference clock source to provide time synchronization for external devices.
- DEVICE-B specifies DEVICE-A as the NTP server and synchronizes time with DEVICE-A.
- After successful synchronization, DEVICE-B provides time synchronization for DEVICE-C.

Figure 3-1



Deployment

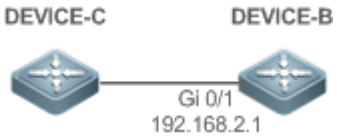
Configure DEVICE-B to the NTP external reference clock mode.

3.2.2 Synchronizing Time Based on a Local Reference Clock Source

Scenario

As shown in Figure 3-2, DEVICE-B uses a local clock as the NTP reference clock source and provides time synchronization for DEVICE-C.

Figure 3-2



Deployment

Configure DEVICE-B to the NTP local reference clock mode.

3.3 Features

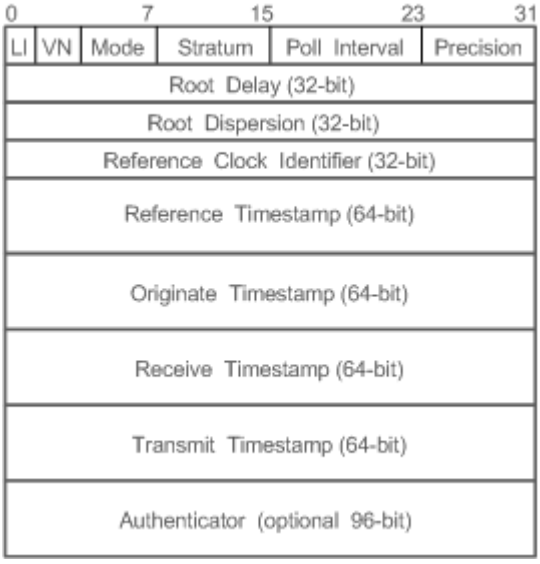
Basic Concepts

❖ NTP Packet

As defined in RFC1305, NTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 3-3 shows the format of an NTP time synchronization packet.

Figure 3-3 Format of an NTP Time Synchronization Packet



- Leap Indicator(LI): indicates a 2-bit leap second indicator.

➢ 00: indicates no warning information; 01: indicates that there are 61 seconds in the previous minute; 10: indicates that there are 59 seconds in the previous minute; 11: indicates that the clock is not synchronized.

- Version Number(VN): indicates a 3-bit NTP version number. The current version number is 3.
- Mode: indicates a 3-bit NTP working mode.

➢ 0: indicates no definition; 1: indicates symmetric active; 2: indicates symmetric passive; 3: indicates a client; 4: indicates a server; 5: indicates broadcasting; 6: indicates control information; 7: reserved.

- Stratum: indicates the 8-bit stratum of a local clock. 0: indicates no definition; 1: indicates the master reference clock source; other values: indicate slave reference clock sources.
- Poll Interval: indicates the poll interval (seconds), which is a 8-bit integer.
- Precision: indicates the time precision (seconds) of a local clock, which is a 8-bit integer.
- Root Delay: indicates the round-trip time to the master reference clock source, which is a 32-bit integer.
- Root Dispersion: indicates the largest difference from the master reference clock source, which is a 32-bit integer.
- Reference Clock Identifier: indicates the 32-bit identifier of a reference clock source.
- Reference Timestamp: indicates a 64-bit timestamp, namely, the time that is set or corrected at the last time.
- Originate Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request leaves from a client.

- Receive Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request packet arrives at a server.
- Transmit Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization response packet leaves from a server.
- Authenticator (optional): indicates authentication information.

❖ NTP Server

A device uses a local clock as the reference clock source to provide time synchronization for other devices in the network.

❖ NTP Client

A device is used as an NTP client that synchronizes time with an NTP server in the network.

❖ Stratum

In NTP, "stratum" is used to describe the hops from a device to an authority clock source. An NTP server whose stratum is 1 has a directly connected atomic clock or radio controlled clock; an NTP server whose stratum is 2 obtains time from the server whose stratum is 1; an NTP server whose stratum is 3 obtains time from the server whose stratum is 2; and so on. Therefore, clock sources with lower stratums have higher clock precisions.

❖ Hardware Clock

A hardware clock operates based on the frequency of the quartz crystal resonator on a device and is powered by the device battery. After the device is shut down, the hardware clock continues running. After the device is started, the device obtains time information from the hardware clock as the software time of the device.

Overview

Feature	Description
NTP Time Synchronization	Network devices synchronize time with their servers or reliable clock sources to implement high-precision time correction.
NTP Security Authentication	The NTP packet encryption authentication is used to prevent unreliable clock sources from time synchronization interference on a device.
NTP Access Control	An Access Control List (ACL) is used to filter sources of received NTP packets.

3.3.1 NTP Time Synchronization

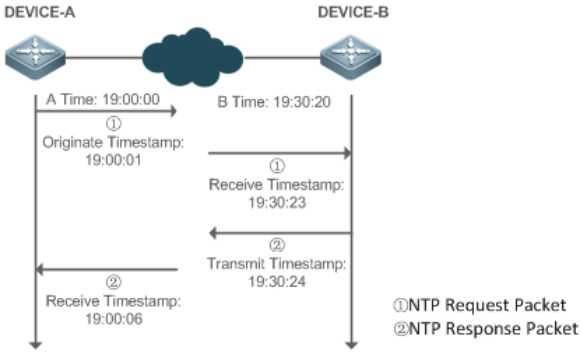
Working Principle

NTP time synchronization is implemented by interaction of NTP packets between a client and a server:

- The client sends a time synchronization packet to all servers every 64 seconds. After receiving response packets from the servers, the client filters and selects the response packets from all servers, and synchronizes time with an optimum server.
- After receiving the time synchronization request packet, a server uses the local clock as the reference source, and fills the local time information into the response packet to be sent to the client based on the protocol requirement.

Figure 3-4 shows the format of an NTP time synchronization packet.

Figure 3-4 Working Principle of NTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an NTP client that synchronizes time with DEVICE-B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

1. A sends an NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.
2. After a 2-second network delay, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.
3. B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.
4. After a 2-second network delay, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

- A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

❖ NTP Working Mode

- External clock reference mode

In this mode, a device is used as both a server and a client. If receiving time synchronization requests from other clients, the device must synchronize time with the specified server first and provide time synchronization for the clients after successful synchronization.

- Local clock reference mode

In this mode, a device uses the default local clock as the reliable clock source and provides time synchronization directly for other clients.

Related Configuration

❖ Configuring an NTP Server

- The NTP function is disabled by default.
- Run the **ntp server** command to specify an NTP server (external clock reference source), which can enable NTP.
- After the configuration, the device works in the external clock reference mode.

❖ Real-time Synchronization

- A device performs time synchronization every 64 seconds by default.

❖ Updating a Hardware Clock

- By default, a device does not update synchronized time to the hardware clock.
- Run the **ntp update-calendar** command to enable a device to automatically update the hardware clock after successfully synchronizing time each time.

❖ Configuring the NTP Master Clock

- By default, a device works in the external clock reference mode.
- Run the **ntp master** command to configure a device to the local clock reference mode.

3.3.2 NTP Security Authentication

To prevent malicious damage on an NTP server, NTP uses the authentication mechanism to check whether the time synchronization information is really from the announced server and check the information return path to provide an anti-interference protection mechanism.

Working Principle

An NTP client and an NTP server are configured with the same key. When sending request and response packets, a device calculates the hash values of the packets by using the MD5 algorithm based on the specified key and NTP packet content, and fills the hash values into the packet authentication information. The receiving device checks whether the packets are sent by a trusted device or modified based on the authentication information.

Related Configuration

- ❖ Configuring a Global Security Authentication Mechanism for NTP
- By default, no NTP security authentication mechanism is enabled.
- Run the **ntp authenticate** command to enable the NTP security authentication mechanism.
- ❖ Configuring a Global Authentication Key for NTP
- By default, no global authentication key is configured.
- Run the **ntp authentication-key** command to enable an NTP global authentication key.
- ❖ Configuring a Globally Trusted Key ID for NTP
- By default, no globally trusted key is configured.
- Run the **ntp trusted-key** command to configure a device as the reference clock source to provide a trusted key for time synchronization externally.
- ❖ Configuring a Trusted Key ID for an External Reference Clock Source
- Run the **ntp server** command to specify an external reference source and the trusted key of this clock source as well.

3.3.3 NTP Access Control

Working Principle

Provide a minimum security measure by using an ACL.

Related Configuration

- ❖ Configuring the Access Control Rights for NTP Services
- By default, there is no access control right for NTP.
- Run the **ntp access-group** command to configure the access control rights for NTP.

3.4 Configuration

Configuration	Description and Command
Configuring Basic Functions of NTP	(Mandatory) It is used to enable NTP. After NTP is enabled, a device works in the external clock reference mode.

	ntp server	Configures an NTP server.
	ntp update-calendar	Automatically updates a hardware clock.
	(Optional) It is used to configure a device to the local clock reference mode.	
	ntp master	Configures the NTP master clock.
	(Optional) It is used to disable NTP.	
	no ntp	Disables all functions of NTP and clears all NTP configurations.
	ntp disable	Disables receiving of NTP packets from a specified interface.
Configuring NTP Security Authentication	(Optional) It is used to prevent unreliable clock sources from performing time synchronization interference on a device.	
	ntp authenticate	Enables a security authentication mechanism.
	ntp authentication-key	Configures a global authentication key.
	ntp trusted-key	Configures a trusted key for time synchronization.
	ntp server	Configures a trusted key for an external reference clock source.
Configuring NTP Access Control	(Optional) It is used to filter the sources of received NTP packets.	
	ntp access-group	Configures the access control rights for NTP.

3.4.1 Configuring Basic Functions of NTP

Configuration Effect

❖ External Clock Reference Mode

- Use a device as a client to synchronize time from an external reference clock source to the local clock.
- After the time synchronization is successful, use the device as a time synchronization server to provide time synchronization.

❖ Local Clock Reference Mode

- Use the local clock of a device as the NTP reference clock source to provide time synchronization.

Notes

- In the client/server mode, a device can be used as a time synchronization server to provide time synchronization only after successfully synchronizing time with a reliable external clock source.
- Once the local clock reference mode is configured, the system will not synchronize time with a clock source with a higher stratum.
- Configuring a local clock as the master clock (especially when specifying a lower stratum) may overwrite an effective clock source. If this command is used for multiple devices in a network, the clock difference between the devices may cause unstable time synchronization of the network.
- Before a local clock is configured as the master clock, if the system never synchronizes time with an external clock source, you may need to manually calibrate the system clock to ensure that there is no excessive difference. For details about how to manually calibrate the system clock, refer to the system time configuration section in the configuration guide.

Configuration Steps

❖ Configuring an NTP Server

- (Mandatory) At least one external reference clock source must be specified (A maximum of 20 different external reference clock sources can be configured).
- If it is necessary to configure an NTP key, you must configure NTP security authentication before configuring the NTP server.

❖ Automatically Updating a Hardware Clock

- Optional.
- By default, the system updates only the system clock, but not the hardware clock after successful time synchronization.
- After this command is configured, the system automatically updates the hardware clock after successful time synchronization.

❖ Configuring the NTP Master Clock

- To switch a device to the local clock reference mode, run this command.

❖ Disabling NTP

- To disable NTP and clear NTP configurations, run the **no ntp** command.
- By default, all interfaces can receive NTP packets after NTP is enabled. To disable NTP for a specified interface, run the **ntp disable** command.

Verification

- Run the **show ntp status** command to display the NTP configuration.

- Run the **show clock** command to check whether time synchronization is completed.

Related Commands

❖ Configuring an NTP Server

Command	**ntp server**[**oob | vrf** *vrf-name*]{ *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain*}[**version** *version*] [**key** *keyid*][**prefer**] [**via** *mgmt-name*]
Parameter Description	oob: Indicates whether a reference clock source is bound to the MGMT interface. *vrf-name:* Indicates the name of the VRF that is bound to the reference clock source. *ip-addr*: Indicates the IPv4/IPv6 address of the reference clock source. *domain*: Indicates the IPv4/IPv6 domain name of the reference clock source. *version*: Indicates the NTP version number, ranging from 1 to 3. *keyid*: Indicates the key used for communicating with the reference clock source, ranging from 1 to 4294967295. **prefer**: Indicates whether the reference clock source has a high priority. *mgmt-name:* Specifies the egress management interface for packets in the oob mode.
Command Mode	Global configuration mode
Usage Guide	By default, no NTP server is configured. Qtech client system supports interaction with up to 20 NTP servers. You can configure an authentication key for each server (after configuring global authentication and the related key) to initiate encrypted communication with the servers. If it is necessary to configure an authentication key, you must configure NTP security authentication before configuring an NTP server. The default version of NTP for communicating with a server is NTP version 3. In addition, you can specify that the NTP packets from a corresponding server can be received only on the transmitting interface.

❖ Updating a Hardware Clock

Command	**ntp update-calendar**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	**N/A**

❖ Configuring a Local Reference Clock Source

Command	**ntp master**[*stratum*]
Parameter Description	*stratum*: specifies the stratum of a local clock, ranging from 1 to 15. The default value is 8.
Command Mode	Global configuration mode

Usage Guide	N/A

❖ Disabling NTP

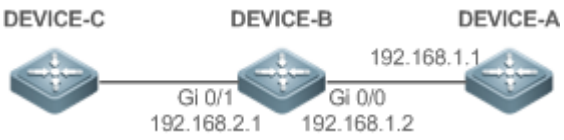
Command	no ntp
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command can be used to fast disable all functions of NTP and clear all NTP configurations.

❖ Disabling Receiving of NTP Packets on an Interface

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

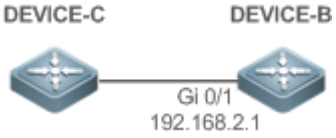
Configuration Example

❖ External Clock Reference Mode of NTP

Scenario **Figure 3-5**	
	➢ DEVICE-B is configured to the NTP external clock reference mode. ➢ DEVICE-A is used as the reference clock source of DEVICE-B. ➢ DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	➢ DEVICE-A configures the local clock as the NTP reference clock source. ➢ DEVICE-B configures DEVICE-A as the reference clock source. ➢ DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-A	A#configure terminal A(config)# ntp master A(config)#exit
DEVICE-B	B#configure terminal B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal

	C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	➢ Run the **show ntp status** command on DEVICE-B to display the NTP configuration. ➢ DEVICE-B sends a time synchronization packet to 192.168.1.1 in order to synchronize time with DEVICE-A. ➢ After successfully synchronizing time with DEVICE-A, DEVICE-B can respond to the time synchronization request from DEVICE-C. ➢ Run the **show clock** command on DEVICE-B and DEVICE-C to check whether the time synchronization is successful.

❖ Local Clock Reference Mode of NTP

Scenario Figure 3-6	
	➢ DEVICE-B configures the local clock as the NTP reference clock source. ➢ DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	➢ DEVICE-B configures the local clock as the NTP reference clock source. ➢ DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp master B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	➢ Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful.

3.4.2 Configuring NTP Security Authentication

Configuration Effect

❖ Synchronizing Time from a Trusted Reference Clock Source

Use a device as a client to synchronize time only from a trusted external reference clock source to the local clock.

❖ Providing Time Synchronization for a Trusted Device

Use the local clock of a device as the NTP reference clock source to provide time synchronization for only a trusted device.

Notes

The authentication keys of the client and server must be the same.

Configuration Steps

❖ Configuring a Global Security Authentication Mechanism for NTP

- Mandatory.
- By default, a device disables the security authentication mechanism.

❖ Configuring a Global Authentication Key for NTP

- Mandatory.
- By default, a device is not configured with an authentication key.

❖ Configuring a Globally Trusted Key ID for NTP

- Optional.
- To provide time synchronization for a trusted device, you must specify a trusted authentication key by using the key ID.
- Only one trusted key can be configured. The specified authentication key must be consistent with that of the trusted device.

❖ Configuring an Authentication Key ID for an External Reference Clock Source

- Optional.
- To synchronize time with a trusted reference clock source, you must specify a trusted authentication key by using the key ID.
- Each trusted reference clock source is mapped to an authentication key. The authentication keys must be consistent with the keys of trusted reference clock sources.

Verification

- Run the **show run** command to verify the NTP configuration.
- Run the **show clock** command to check whether time is synchronized only with a trusted device.

Related Commands

❖ Enabling a Security Authentication Mechanism

Command	ntp authenticate

Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	By default, a client does not use a global security authentication mechanism. If no security authentication mechanism is used, communication will not be encrypted. A global security indicator is not enough to imply that the communication between the client and server is implemented in an encrypted manner. Other global keys and an encryption key for the server must also be configured for initiating encrypted communication between the client and server.

❖ Configuring a Global Authentication Key

Command	**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]
Parameter Description	*key-id*: indicates the ID of a global authentication key, ranging from 1 to 4294967295. *key-string*: indicates a key string. *enc-type*: (optional) indicates whether an entered key is encrypted. 0 indicates no encryption, and 7 indicates simple encryption. The default setting is no encryption.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring a Trusted Key for NTP

Command	**ntp trusted-key** *key-id*
Parameter Description	*key-id*: Indicates the ID of a trusted key, ranging from 1 to 4294967295.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring a Trusted Key for an External Reference Clock Source

Refer to the section "**Ошибка! Источник ссылки не найден.**".

Configuration Example

❖ Security Authentication

Scenario **Figure 3-7**	
	➢ DEVICE-B is configured to the NTP client/server mode and provides NTP services requiring security authentication for DEVICE-C. The authentication key is "abcd". ➢ DEVICE-A is used as the reference clock source of DEVICE-B.

	➢ DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	➢ DEVICE-B configures DEVICE-A as the reference clock source. ➢ DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp authentication-key 1 md5 abcd B(config)# ntp trusted-key 1 B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp authentication-key 1 md5 abcd C(config)# ntp server 192.168.2.1 key 1 C(config)# exit
Verification	➢ DEVICE-B sends a time synchronization packet that carries authentication information to 192.168.1.1 in order to synchronize time with DEVICE-A. ➢ Run the **show clock** command on DEVICE-B to check whether the time synchronization is successful.

3.4.3 Configuring NTP Access Control

Configuration Effect

Access control for NTP services provides a minimum security measure. A more secure method is to use an NTP authentication mechanism.

Notes

- Currently, the system does not support control query (used to control NTP servers by using network management devices, such as setting the leap second indicator or monitoring its working status). Though rule matching is implemented in the preceding sequence, no request related to control query is supported.
- ➢ If no access control rule is configured, all accesses are allowed. If any access control rule is configured, only accesses allowed by the rule can be implemented.

Related Configuration

- ❖ Configuring the Access Control Rights for NTP
- Optional.

- Run the **ntp access-group** command to configure the access control rights and a corresponding ACL for NTP.

Verification

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

Related Commands

❖ Configuring the Access Control Rights for NTP Services

Command	**ntp access-group** { **peer** | **serve** |**serve-only** | **query-only** }*access-list-number* | *access-list-name*
Parameter Description	**peer**: allows time request and control query for local NTP services, and allows a local device to synchronize time with a remote system (full access rights). **serve**: allows time request and control query for local NTP services, but does not allow a local device to synchronize time with a remote system. **serve-only**: allows only time request for local NTP services. **query-only**: allows only control query for local NTP services. *access-list-number*: indicates the number of an IP ACL, ranging from 1 to 99 and from 1300 to 1999. For details about how to create an IP ACL, refer to the *Configuring ACL*. *access-list-name*: indicates the name of an IP ACL. For details about how to create an IP ACL, refer to the *Configuring ACL*.
Command Mode	Global configuration mode
Usage Guide	Configure NTP access control rights. When an access request arrives, the NTP service matches rules in the sequence from the minimum access restriction to the maximum access restriction and uses the first matched rule. The matching sequence is peer, serve, serve-only, and query-only.

Configuration Example

❖ Configuring NTP Access Control Rights

Configuration Steps	Allow only the device with the IP address of 192.168.1.1 to send a time synchronization request to a local device.
	Qtech(config)# access-list 1 permit 192.168.1.1 Qtech(config)# ntp access-group serve-only 1

3.5 Monitoring

Displaying

Description	Command
show ntp status	Displays the current NTP information.

Debugging

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

Description	Command
debug ntp	Enables debugging.
no debug ntp	Disables debugging.

4. CONFIGURING SNTP

4.1 Overview

The Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol (NTP), which is used to synchronize the clocks of computers on the Internet. SNTP is applied in scenarios where it is unnecessary to use all NTP functions.

NTP uses a complex algorithm and has higher requirements for the system whereas SNTP uses a simpler algorithm and provides higher performance. Generally, SNTP precision can reach about 1s, which meets the basic requirements of most scenarios. Since SNTP packets are the same as NTP packets, the SNTP client implemented on a device is fully compatible with an NTP server.

Protocols and Standards

- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

4.2 Applications

Application	Description
Synchronizing Time with an NTP Server	A device is used as a client to synchronize time with an NTP server.

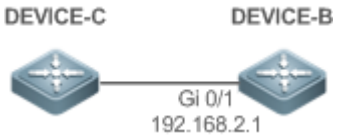
4.2.1 Synchronizing Time with an NTP Server

Scenario

As shown in Figure 4-1, DEVICE-B uses a local clock as the NTP clock reference source and provides time synchronization for DEVICE-C.

DEVICE-C is used as an SNTP client to synchronize time with DEVICE-B.

Figure 4-1



Deployment

- Specify DEVICE-B as the SNTP server of DEVICE-C.
- Enable SNTP for DEVICE-C.

4.3 Features

Basic Concepts

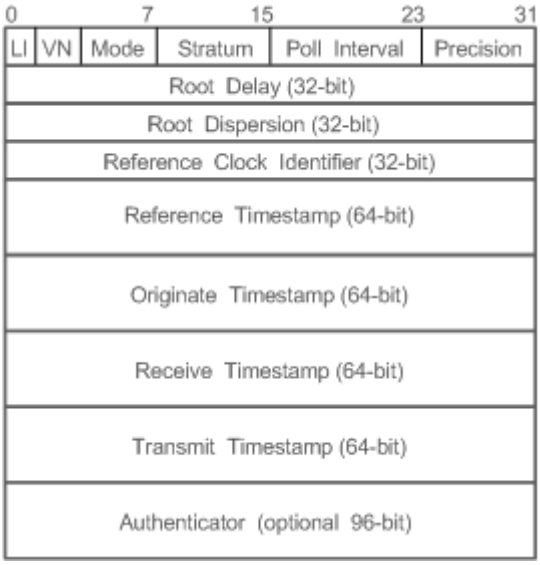
❖ SNTP Packet

SNTPV4 is developed from NTP, which is intended to simplify the functions of NTP. It does not change the NTP specifications and the original implementation of NTP. The message format of SNTPV4 is the same as that of NTP defined in RFC1305, with only some data fields initialized into preset values.

As defined in RFC1305, SNTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 4-2 shows the format of an SNTP time synchronization packet.

Figure 4-2 Format of an SNTP Time Synchronization Packet



- Leap Indicator(LI): indicates a 2-bit leap second indicator.

➢ 00: indicates no warning information; 01: indicates that there are 61 seconds in the previous minute; 10: indicates that there are 59 seconds in the previous minute; 11: indicates that the clock is not synchronized.

- Version Number(VN): indicates a 3-bit NTP/SNTP version number. The current version number is 3.
- Mode: indicates a 3-bit SNTP/NTP working mode.

➢ 0: indicates no definition; 1: indicates symmetric active; 2: indicates symmetric passive; 3: indicates a client; 4: indicates a server; 5: indicates broadcasting; 6: indicates control information; 7: reserved.

- Stratum: indicates the 8-bit stratum of a local clock. 0: indicates no definition; 1: indicates the master clock reference source; other values: indicate slave clock reference sources.
- Poll Interval: indicates the poll interval (seconds), which is a 8-bit integer.
- Precision: indicates the time precision (seconds) of a local clock, which is a 8-bit integer.
- Root Delay: indicates the round-trip time to the master clock reference source, which is a 32-bit integer.
- Root Dispersion: indicates the largest difference from the master reference clock source, which is a 32-bit integer.
- Reference Clock Identifier: indicates the 32-bit identifier of a reference clock source.
- Reference Timestamp: indicates a 64-bit timestamp, namely, the time that is set or corrected at the last time.
- Originate Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request leaves from a client.
- Receive Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request packet arrives at a server.
- Transmit Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization response packet leaves from a server.
- Authenticator (optional): indicates authentication information.

Overview

Feature	Description
SNTP Time Synchronization	Synchronizes time from an SNTP/NTP server to a local device.

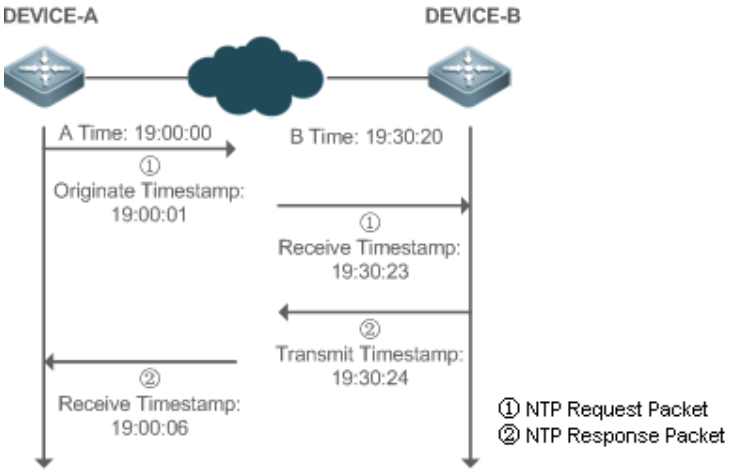
4.3.1 SNTP Time Synchronization

Working Principle

SNTP time synchronization is implemented by interaction of SNTP/NTP packets between a client and a server. The client sends a time synchronization packet to the server at intervals (half an hour by default). After receiving a response packet from the server, the client synchronizes time.

Figure 4-3 shows the format of an SNTP time synchronization packet.

Figure 4-3 Working Principle of SNTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an SNTP client that synchronizes time with DEVICE-B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

1. A sends an SNTP/NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.
2. After a 2-second network delay, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.
3. B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.
4. After a 2-second network delay, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

- A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

Related Configuration

❖ Enabling SNTP

- SNTP is disabled by default.
- Run the **sntp enable** command to enable SNTP.

❖ Configuring an SNTP Server

- By default, no SNTP server is configured.

- Run the s**ntp server** command to specify an SNTP server.

❖ Configuring the SNTP Time Synchronization Interval

- By default, the SNTP time synchronization interval is 1,800s.
- Run the **sntp interval** command to specify the time synchronization interval.

4.4 Configuration

Configuration	Description and Command	
Configuring SNTP	(Mandatory) It is used to enable SNTP.	
	sntp enable	Enables SNTP.
	sntp server	Configures the IP address of an SNTP server.
	(Optional) It is used to configure the SNTP time synchronization interval.	
	sntp interval	Configures the SNTP time synchronization interval.

4.4.1 Configuring SNTP

Configuration Effect

An SNTP client accesses an NTP server at fixed intervals to correct the clock regularly.

Notes

All time obtained through SNTP communication is Greenwich Mean Time (GMT). To obtain precise local time, you need to set the local time zone for alignment with GMT.

Configuration Steps

❖ Enabling SNTP

- (Mandatory) SNTP is disabled by default.

❖ Configuring the IP address of an SNTP Server

- (Mandatory) No SNTP/NTP server is configured by default.

❖ Configuring the SNTP Time Synchronization Interval

- Optional.
- By default, a device synchronizes time every half an hour.

Verification

Run the **show sntp** command to display SNTP-related parameters.

Related Commands

❖ Enabling SNTP

Command	**sntp enable**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	SNTP is disabled by default. Run the **no sntp enable** global configuration command to disable SNTP.

❖ Configuring the IP address of an SNTP/NTP Server

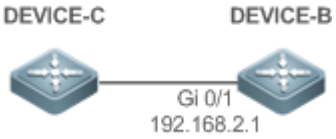
Command	**sntp server** [**oob**] *ip-address* [**via** *mgmt-name*]
Parameter Description	*ip-address*: indicates the IP address of an NTP/SNTP server. No NTP/SNTP server is configured by default.
	oob: indicates that the NTP/SNTP server supports an out-band management interface (interface of mgmt). *mgmt-name:* Specifies the egress management interface for packets in the oob mode.
Command Mode	Global configuration mode
Usage Guide	Since SNTP is fully compatible with NTP, the server can be configured as a public NTP server on the Internet. Since SNTP packets are the same as NTP packets, the SNTP client is fully compatible with the NTP server. There are many NTP servers on the Internet. You can select an NTP server with a shorter delay as the SNTP server on your device.

❖ Configuring the SNTP Time Synchronization Interval

Command	**sntp interval** *seconds*
Parameter Description	*seconds*: Indicates the time synchronization interval, ranging from 60s to 65,535s. The default value is 1,800s.
Command Mode	Global configuration mode
Usage Guide	Run this command to set the interval for an SNTP client to synchronize time with an NTP/SNTP server. The interval configured here does not take effect immediately. To make it take effect immediately, run the **sntp enable** command.

Configuration Example

❖ SNTP Time Synchronization

Scenario **Figure 4-4**	
	➢ DEVICE-B indicates an NTP server on the Internet. ➢ DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	Enable SNTP for DEVICE-C and configure DEVICE-B as an NTP server.
DEVICE-C	C#configure terminal C(config)# sntp server 192.168.2.1 C(config)# sntp enable C(config)# exit
Verification	➢ Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful. ➢ Run the **show sntp** command on DEVICE-C to display the SNTP status and check whether the server is successfully configured.

4.5 Monitoring

Displaying

Description	Command
show sntp	Displays SNTP-related parameters.

Debugging

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

Description	Command
debug sntp	Enables debugging.

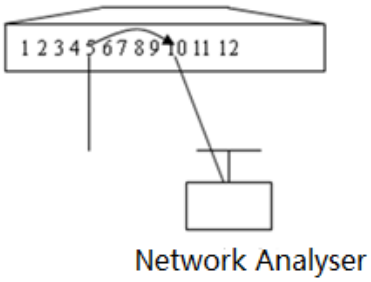
5. CONFIGURING SPAN-RSPAN

5.1 Overview

The Switched Port Analyzer (SPAN) is to copy packets of a specified port to another switch port that is connected to a network monitoring device, so as to achieve network monitoring and troubleshooting.

All input and output packets of a source port can be monitored through SPAN. For example, as shown in the following figure, all packets on Port 5 are mapped to Port 10, and the network analyzer connected to Port 10 receives all packets that pass through Port 5.

Figure 5-1 SPAN Configuration Instance



The SPAN function is mainly applied in network monitoring and troubleshooting scenarios, to monitor network information and rectify network faults.

The Remote SPAN (RSPAN), an extension to SPAN, is capable of remotely monitoring multiple devices. Each RSPAN session is established in a specified remote VLAN. RSPAN breaks through the limitation that a mirrored port and a mirroring port must reside on the same device, and allows a mirrored port to be several network devices away from a mirroring port. Users can observe data packets of the remote mirrored port by using an analyzer in the central equipment room.

The application scenarios of RSPAN are similar to those of SPAN. RSPAN allows users to conduct real-time data monitoring without staying in the equipment room, providing great convenience for users.

VLAN SPAN (VSPAN) considers data streams of some VLANs as data sources and mirrors them to a destination port. The configuration is similar to that of the port-based SPAN. VSPAN has the following features:

- A VLAN that is not a remote VLAN can be specified as the data source of VSPAN.
- Some VLANs that are not remote VLANs can be specified as the data sources of VSPAN.
- When a VLAN is configured as a data source, packets only in the Rx direction can be mirrored.

5.2 Applications

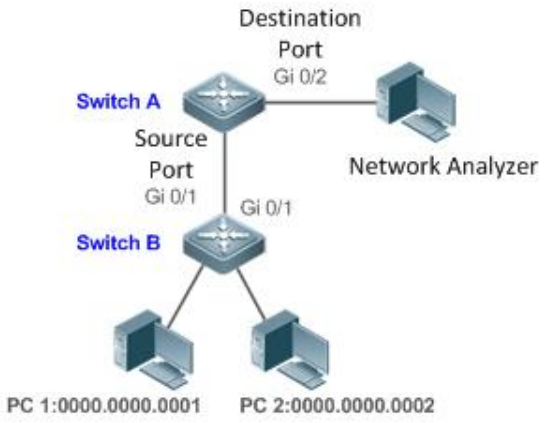
Application	Description
Stream-based SPAN	Data streams with certain characteristics need to be monitored, for example, data streams using a specified access control list (ACL) policy need to be monitored.
One-to-Many RSPAN	Multiple users need to monitor data of the same port.
RSPAN Basic Applications	Packets on the mirroring source device need to be mirrored to the destination device for monitoring.

5.2.1 Stream-based SPAN

Scenario

As shown in the following figure, the network analyzer can be configured to can monitor all data streams forwarded by Switch A to Switch B and specific data streams of Switch B (for example, data streams from PC1 and PC2).

Figure 5-2 SPAN Simple Application Topology



Remarks

0000.0000.0001 is the MAC address of PC1.
0000.0000.0002 is the MAC address of PC2.

Deployment

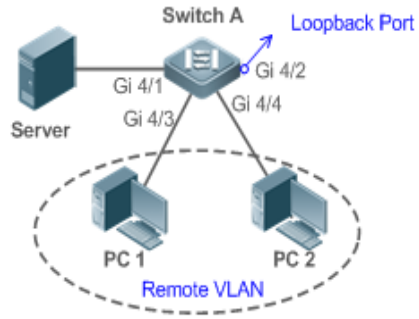
- In the preceding figure, configure the SPAN function on Switch A connected to the network analyzer, set port Gi 0/1 connected to Switch B as the SPAN source port, and set port Gi 0/2 that is directly connected to the network analyzer as the SPAN destination port.
- Configure stream-based SPAN (only data streams of PC1and PC2 are allowed) for the source port Gi 0/1 of SPAN.

5.2.2 One-to-Many RSPAN

Scenario

As shown in the following figure, one-to-many RSPAN can be implemented on a single device, that is, both PC 1 and PC 2 can be configured to monitor the transmitted and received traffic of the port connected to the server. Users can make proper configuration (for example, remote VLAN and port MAC loopback) to monitor data streams that pass through port Gi 4/1 on PC 1 and PC 2, thereby monitoring data streams of the server.

Figure 5-3 Application Topology of One-to-Many RSPAN



Deployment

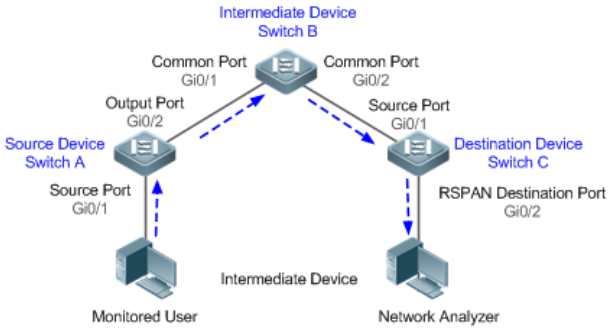
- Create a remote VLAN on Switch A.
- Configure Switch A as the source device of RSPAN and configure the port Gi 4/1 that is directly connected to the server as the RSPAN source port. Select a port that is in the Down state, Gi 4/2 in this example, as the RSPAN output port, add this port to the remote VLAN, and configure MAC loopback (run the **mac-loopback** command in interface configuration mode).
- Add ports that are directly connected to PC 1 and PC 2 to the remote VLAN.

5.2.3 RSPAN Basic Applications

Scenario

As shown in the following figure, the RSPAN function enables the network analyzer to monitor the STA connected to the source device Switch A from the destination device Switch C through the intermediate device Switch B. The devices can normally exchange data with each other.

Figure 5-4 Basic Application Topology of RSPAN



Deployment

- Configure a remote VLAN on Switch A, Switch B, and Switch C.
- On Switch A, configure port Gi 0/1 directly connected to the STA as the source port, configure port Gi 0/2 connected to Switch B as the output port, and configure the switching function for the output port.
- On Switch B, configure port Gi 0/1 connected to Switch A and port Gi 0/2 connected to Switch C as common ports.
- On Switch C, configure port Gi0/1 connected to Switch B as a common source port, configure port Gi 0/2 connected to the network analyzer as the RSPAN destination port, and configure the switching function for the RSPAN destination port.

5.3 Features

Basic Concepts

❖ SPAN Session

A SPAN session is data streams between the SPAN source port and the destination port, which can be used to monitor the packets of one or more ports in the input, output, or both directions. Switched ports, routed ports, and aggregate ports (APs) can be configured as source ports or destination ports of SPAN sessions. Normal operations on a switch are not affected after ports of the switch are added to a SPAN session.

Users can configure a SPAN session on a disabled port but the SPAN session is inactive. A SPAN session is in the active state only after the port on which the SPAN session is configured is enabled. In addition, a SPAN session does not take effect after a switch is powered on. It is active only after the destination port is in the operational state. Users can run the **show monitor** [**session** *session-num*] command to display the operation status of a SPAN session.

❖ SPAN Data Streams

A SPAN session covers data streams in three directions:

- Input data streams: All packets received by a source port are copied to the destination port. Users can monitor input packets of one or more source ports in a SPAN session. Some input packets of a source port may be discarded for some reasons (for example, for the sake of port security). It does not affect the SPAN function and such packets are still mirrored to the destination port.
- Output data streams: All packets transmitted by a source port are copied to the destination port. Users can monitor output packets of one or more source ports in a SPAN session. Packets transmitted from other ports to a source port may be discarded for some reasons and such packets will not be transmitted to the destination port. The format of output packets of a source port may be changed for some reasons. For example, after routing, packets transmitted from the source port are changed in source MAC addresses, destination MAC addresses, VLAN IDs, and TTLs, and their formats are also changed after copied to the destination port.
- Bidirectional data streams: Bidirectional data streams include input data streams and output data streams. In a SPAN session, users can monitor data streams of one or more source ports in the input and output directions.

❖ Source Port

A source port is called a monitored port. In a SPAN session, data streams of the source port are monitored for network analysis and troubleshooting. In a single SPAN session, users can monitor the input, output, and bidirectional data streams, and the number of source ports is not restricted.

A source port has the following features:

- A source port can be a switched port, routed port, or AP.
- A source port cannot be used as a destination port simultaneously.
- A source port and a destination port can belong to the same VLAN or different VLANs.

❖ Destination Port

A SPAN session has one destination port (called a monitoring port) for receiving packets copied from a source port.

A destination port has the following features:

- A destination port can be a switched port, routed port, or AP.
- A destination port cannot be used as a source port simultaneously.

Overview

Feature	Description
SPAN	Configures mirroring of ports on the same device.
RSPAN	Configures mirroring of ports on different devices.

5.3.1 SPAN

SPAN is used to monitor data streams on switches. It copies frames on one port to another switch port that is connected to a network analyzer or RMON analyzer so as to analyze the communication of the port.

Working Principle

When a port transmits or receive packets, SPAN, after checking that the port is configured as a SPAN source port, copies the packets transmitted and received by the port to the destination port.

❖ Configuring a SPAN Source Port

Users need to specify a SPAN session ID and source port ID to configure a SPAN source port, and set the optional SPAN direction item to determine the direction of SPAN data streams or specify an ACL policy to mirror specific data streams.

❖ Configuring a SPAN Destination Port

Users need to specify a SPAN session ID and destination port ID to configure a SPAN destination port, and set the optional switching function item to determine whether to enable the switching function and tag removal function on the SPAN destination port.

Related Configuration

The SPAN function is disabled by default. It is enabled only after a session is created, and the SPAN source and destination ports are configured. A SPAN session can be created when a SPAN source port or destination port is configured.

❖ Configuring a SPAN Source Port

A SPAN session does not have a SPAN source port by default. Users can run the following command to configure a SPAN source port:

monitor session *session-num* **source interface** *interface-id* [**both** | **rx** | **tx**] [**acl** *name*]

In the preceding command:

session-num: Indicates the SPAN session ID. The number of supported SPAN sessions varies with products.

interface-id: Indicates the SPAN source port to be configured.

rx: Indicates that only packets received by the source port are monitored after **rx** is configured.

tx: Indicates that only packets transmitted by the source port are monitored after **tx** is configured.

both: Indicates that packets transmitted and received by the source port are copied to the destination port for monitoring after **both** is configured, that is, **both** includes **rx** and **tx**. If none of **rx**, **tx**, and **both** is selected, **both** is enabled by default.

acl: Specifies an ACL policy. After this option is configured, packets allowed by the ACL policy on the source port are monitored. This function is disabled by default.

❖ Configuring a SPAN Destination Port

A SPAN session does not have a SPAN destination port by default. Users can run the following command to configure a SPAN destination port:

monitor session *session-num* **destination interface** *interface-id* [**switch**]

In the preceding command:

switch: Indicates that the SPAN destination port only receives packets mirrored from the SPAN source port and discards other packets if this option is disabled, and receives both packets mirrored from the SPAN source port and packets from non-source ports if this option is enabled, that is, the communication between this destination port and other devices is not affected.

When the SPAN destination port is configured, the relevant function is disabled by default if **switch** is not configured.

❖ Configuring Stream-based SPAN

This function is disabled by default. Users can run the **monitor session** *session-num* **source interface** *interface-id***rxacl***acl-name* command to configure stream-based SPAN.

Pay attention to the following points when using SPAN:

The SPAN destination port is used for the Spanning Tree Protocol (STP) calculation.

SPAN is unavailable if a source port or destination port is disabled.

If a source port or destination port is added to an AP, the source port or destination port exits from a SPAN session.

If a VLAN (or VLAN list) is used as a SPAN source, ensure that the destination port has sufficient bandwidth for receiving mirrored data of the VLAN (or VLAN list).

Not all products support all options of the preceding commands because of product differences.

5.3.2 RSPAN

RSPAN is capable of monitoring multiple devices. Each RSPAN session is established in a specified remote VLAN. RSPAN breaks through the limitation that a mirrored port and a mirroring port must reside on the same device, and allows a mirrored port to be several network devices away from a mirroring port.

Working Principle

A remote VLAN is created for the source device, intermediate device, and destination device, all ports involved in an RSPAN session need to be added to the remote VLAN. Mirrored packets are

broadcasted in the remote VLAN so that they are transmitted from the source port of the source switch to the destination port of the destination switch.

❖ Configuring a Remote VLAN

Packets from an RSPAN source port are broadcasted in a remote VLAN so as to be copied from the local switch to the remote switch. The RSPAN source port, output port, reflection port, transparent transmission ports of the intermediate device (packet input port and output port of the intermediate device), destination port and input port of the destination port must be added to the remote VLAN. The RSPAN function requires configuring a VLAN as a remote VLAN in VLAN mode.

❖ Configuring an RSPAN Session

The configuration of the RSPAN source port and destination port are similar to that of the SPAN source port and destination port, but the mirroring session ID specified during configuration must be the ID of an RSPAN session.

❖ Configuring an RSPAN Source Port

The configuration of an RSPAN source port is the same as that of a SPAN source port, but the specified mirroring session ID must be the ID of an RSPAN session.

❖ Configuring an RSPAN Output Port

The output port is located on the source device and must be added to a remote VLAN. Mirrored packets of a source port are broadcasted in this remote VLAN. The source device transmits packets to the intermediate switch or destination switch through the output port.

❖ Configuring an RSPAN Destination Port

When an RSPAN destination port is configured, an RSPAN session ID, remote VLAN, and port name must be specified so that packets from the source port are copied to the destination port through the remote VLAN.

❖ Configuring Stream-based RSPAN

RSPAN is an extension to SPAN and also supports stream-based mirroring. The configuration is the same as that of stream-based SPAN. Stream-based RSPAN does not affect normal communication.

Users can configure an ACL in the input direction of a source port on an RSPAN source device. Standard ACLs, extended ACLs, MAC ACLs, and user-defined ACLs are supported.

Users can configure a port ACL in the input direction of a source port on an RSPAN source device, and configure a port ACL in the output direction of the destination port on the RSPAN destination device. Users can also configure an ACL in the output direction of a remote VLAN on an RSPAN source switch and configure an ACL in the input direction of the remote VLAN on the RSPAN destination switch.

❖ Configuring One-to-Many RSPAN

If data streams of one source port need to be mirrored to multiple destination ports, users can configure an RSPAN session, configure the source port of the RSPAN session as a one-to-many

mirroring source port and select another Ethernet port as the forwarding port (output port on the source device).In addition, the MAC loopback function needs to be configured on the RSPAN forwarding port in interface configuration mode, the expected RSPAN output port and RSPAN forwarding port need to be added to the remote VLAN. Then, mirrored packets are looped back on the RSPAN forwarding port and then broadcasted in the remote VLAN, thereby implementing one-to-many RSPAN.

Related Configuration

The RSPAN function is disabled by default. It is enabled only after an RSPAN session is created, and a remote VLAN, RSPAN source port, and RSPAN destination port are configured.

❖ Configuring a Remote VLAN

No remote VLAN is specified for RSPAN by default. Users can run the **remote-span** command in VLAN mode to configure a VLAN as a remote VLAN. One remote VLAN corresponds to one RSPAN session.

❖ Configuring an RSPAN Source Device

This function is disabled by default. Users can run the **monitor session** *session-num***remote-source** command in global configuration mode to configure a device as the remote source device of a specified RSPAN session.

❖ Configuring an RSPAN Destination Device

This function is disabled by default. Users can run the **monitor session** *session-num***remote-destination** command in global configuration mode to configure a device as the remote destination device of a specified RSPAN session.

❖ Configuring an RSPAN Source Port

A source port of an RSPAN session is configured on the source device. The configuration is the same as that of a SPAN source port but an RSPAN session ID needs to be specified. This function is disabled by default.

❖ Configuring an Output Port on the RSPAN Source Device

This function is disabled by default. Users can run the **monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-name* [**switch**] command in global configuration mode to configure an output port on the RSPAN source device. If the option **switch** is configured, the output port can participate in normal data packet switching. It is not configured by default. The output port must be added to a remote VLAN.

❖ Configuring a Destination Port on the RSPAN Destination Device

This function is disabled by default. Users can run the **monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-name* [**switch**] command in global configuration mode to configure a destination port on the RSPAN destination device. If the option **switch** is configured,

the destination port can participate in normal data packet switching. It is not configured by default. The destination port must be added to a remote VLAN.

Pay attention to the following points when using RSPAN:

A remote VLAN must be configured on each device, their VLAN IDs must be consistent, and all ports that participate in a session must be added to the VLAN.

It is not recommended that common ports be added to a remote VLAN.

Do not configure a port that is connected to an intermediate switch or destination switch as an RSPAN source port. Otherwise, traffic on the network may be in chaos.

5.4 Configuration

Configuration	Description and Command	
Configuring SPAN Basic Functions	(Mandatory) It is used to create SPAN.	
	monitor session *session-num* **source interface** *interface-id* [**both | rx | tx**]	Configures a SPAN source port.
	monitor session *session-num* **destination interface** *interface-id*[**switch**]	Configures a SPAN destination port.
	monitor session *session-num* **source interface** *interface-id***rxacl***acl-name*	Configures stream-based SPAN.
	monitor session *session-num* **source filter vlan** *vlan-id-list*	Specifies some VLANs as the data sources of SPAN.
Configuring RSPAN Basic Functions	(Mandatory) It is used to create RSPAN.	
	monitor session *session-num* **remote-source**	Configures an RSPAN session ID and specifies a source device.
	monitor session *session-num* **remote-destination**	Configures an RSPAN session ID and specifies a destination device.
	remote-span	Configures a remote VLAN.
	monitor session *session-num* **source interface** *interface-id* [**both | rx | tx**]	Configures an RSPAN source port.

	monitor session *session-num* **destination remote vlan** *remote-vlan-id* **interface** *interface-id* [**switch**]	Configures an output port on the RSPAN source device or a destination port on the RSPAN destination device.

5.4.1 Configuring SPAN Basic Functions

Configuration Effect

- Configure a source and destination ports for a SPAN session.
- Configure a destination port to monitor any packets transmitted and received by a source port.

Notes

- If a source port or destination port is added to an AP, the source port or destination port exits from a SPAN session.
- If the switch function is disabled on a SPAN destination port, the destination port receives only mirrored packets and discards other packets that pass through the port. After the switch function is enabled, the destination port can receive non-mirrored packets.

Configuration Steps

❖ Configuring a SPAN Session

- Global configuration mode. Mandatory.
- You can configure a SPAN session when configuring a SPAN source port or destination port, or when configuring a specified VLAN or some VLANs as a data source or data sources of SPAN.

❖ Configuring a SPAN Source Port

- Global configuration mode. Mandatory.
- You can select the SPAN direction when configuring a SPAN source port. The **both** direction is configured by default, that is, both transmitted and received packets are monitored.

❖ Configuring a SPAN Destination Port

Global configuration mode. Mandatory.

A SPAN session is active only when a SPAN source port is configured (or a VLAN is specified as the data source of SPAN) and a SPAN destination port is configured.

Verification

- Run the **show monitor** command or the **show running** command to verify the SPAN configuration. Alternatively, conduct packet capture analysis on the SPAN destination port and check whether the SPAN function takes effect according to the captured packets.

Related Commands

❖ Configuring a SPAN Source Port

Command	**monitor session** *session-num* **source interface** *interface-id* [**both** | **rx** |**tx**]
Parameter Description	*session-num:* Indicates the ID of a SPAN session. *interface-id:* Indicates the interface ID. **both**: Indicates that packets in the input and output directions are monitored. It is the default value. **rx**: Indicates that packets in the input direction are monitored. **tx**: Indicates that packets in the output direction are monitored.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring a SPAN Destination Port

Command	**monitor session** *session-num* **destination interface** *interface-id*[**switch**]
Parameter Description	*session-num:* Indicates the ID of a SPAN session. *interface-id:* Indicates the interface ID. **switch:** Indicates that the switching function is enabled on the SPAN destination port. It is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring Stream-based SPAN

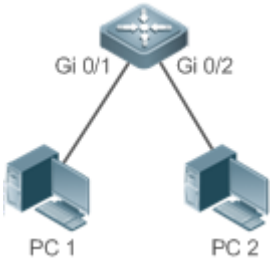
Command	**monitor session** *session-num* **source interface** *interface-id* **rx acl** *acl-name*
Parameter Description	*session-num:* Indicates the ID of a SPAN session. *interface-id:* Indicates the interface ID. *acl-name*: Indicates an ACL name.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Specifying Some VLANs as the Data Sources of SPAN

Command	**monitor session** *session-num* **source filter vlan** *vlan-id-list*
Parameter Description	*session-num:* Indicates the ID of a SPAN session. *vlan-id-list*: Indicates some specified VLAN IDs.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

❖ The following uses SPAN as an example.

Scenario **Figure 5-5**	
Configuration Steps	➢ As shown in Figure 5-5, add ports Gi 0/1 and Gi 0/2 of Device A to VLAN 1. ➢ Create SVI 1 and set the address of SVI 1 to 10.10.10.10/24. ➢ Set IP addresses of PC 1 and PC 2 to 10.10.10.1/24 and 10.10.10.2/24 respectively. ➢ Configure SPAN for Device A and configure ports Gi 0/1 and Gi 0/2 as the source port and destination port of SPAN respectively.

A	`Qtech# configure`
	`Qtech(config)# vlan 1`
	`Qtech(config-vlan)# exit`
	`Qtech(config)# interface vlan 1`
	`Qtech(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0`
	`Qtech(config-if-VLAN 1)# exit`
	`Qtech(config)# monitor session 1 source interface gigabitEthernet 0/1`
	`Qtech(config)# monitor session 1 destination interface gigabitEthernet 0/2`

Verification	Run the **show monitor** command to check whether SPAN is configured correctly. After successful configuration, PC 1 sends ping packets to SVI 1 and PC 2 conducts monitoring by using the packet capture tool.

A	Qtech# show monitor sess-num: 1 span-type: LOCAL_SPAN src-intf: GigabitEthernet 0/1 frame-type Both dest-intf: GigabitEthernet 0/2

Common Errors

- The session ID specified during configuration of the SPAN source port is inconsistent with that specified during configuration of the SPAN destination port.
- Packet loss may occur if packets of a port with large bandwidth are mirrored to a port with small bandwidth.

5.4.2 Configuring RSPAN Basic Functions

Configuration Effect

- Configure a source port and destination port on the source device of an RSPAN session and configure the destination port on the destination device.
- Configure the destination port on the RSPAN destination device to monitor any packets that are transmitted or received by the source port.

Notes

- If a source port or destination port is added to an AP, the source port or destination port exits from a SPAN session.
- If the switch function is disabled on an RSPAN destination port, the destination port receives only mirrored packets and discards other packets that pass through the port. After the switch function is enabled, the destination port can receive non-mirrored packets.
- All ports involved in RSPAN must be added to a remote VLAN.
- A remote VLAN must be created on an intermediate device and transparent transmission ports must be added to the remote VLAN.

Configuration Steps

❖ Configuring an RSPAN Session

- Global configuration mode. Mandatory.

- The same session ID needs to be configured on the RSPAN source device and RSPAN destination device.

❖ Configuring an RSPAN Source Device

- Global configuration mode. Mandatory.
- It is used to specify a device to be monitored by RSPAN.

❖ Configuring an RSPAN Destination Device

- Global configuration mode. Mandatory.
- It is used to specify the destination device for outputting RSPAN packets.

❖ Configuring an RSPAN Source Port

- Global configuration mode. Mandatory.
- Complete the configuration on an RSPAN source device. After configuration, RSPAN monitoring can be conducted on packets of the RSPAN source port. You can specify RSPAN to monitor remote VLAN packets in the input direction, output direction, or both directions of the RSPAN source port.

❖ Configuring an RSPAN Output Port

- Global configuration mode. Mandatory.
- Complete the configuration on an RSPAN source device. After configuration, mirrored packets received by the ports added to the remote VLAN can be transmitted to the RSPAN destination device through the output port.

❖ Configuring an RSPAN Destination Port

- Global configuration mode. Mandatory.
- Complete the configuration on the RSPAN destination device. After configuration, the RSPAN destination device forwards mirrored packets received by the ports added to the remote VLAN to the monitoring device through the destination port.

Verification

- Run the **show monitor** command or the **show running** command to check whether RSPAN is successfully configured on each device, or conduct packet capture on the destination mirroring port on the RSPAN destination device to check whether packets mirrored from the source port of the RSPAN source device are captured.

Related Commands

❖ Configuring an RSPAN Source Device

Command	**monitor session** *session-num* **remote-source**

Parameter Description	*session-num:* Indicates the ID of an RSPAN session.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring an RSPAN Destination Device

Command	**monitor session** *session-num* **remote-destination**
Parameter Description	*session-num:* Indicates the ID of an RSPAN session.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring a Remote VLAN

Command	**remote-span**
Parameter Description	N/A
Command Mode	VLAN mode
Usage Guide	N/A

❖ Configuring an RSPAN Source Port

Command	**monitor session** *session-num* **source interface** *interface-id* [**both | rx | tx**][**acl** *acl-name*]
Parameter Description	*session-num:* Indicates the ID of an RSPAN session. *interface-id:* Indicates the interface ID. **both**: Indicates that packets in the input and output directions are monitored. It is the default value. **rx**: Indicates that packets in the input direction are monitored. **tx**: Indicates that packets in the output direction are monitored. *acl-name*: Indicates an ACL name.
Command Mode	Global configuration mode
Usage Guide	The configuration is the same as that of a SPAN source port but an RSPAN session ID needs to be specified.

❖ Configuring an Output Port on the RSPAN Source Device

Command	**monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-id* [**switch**]
Parameter Description	*session-num:* Indicates the ID of an RSPAN session. *remote-vlan*: Indicates a remote VLAN. *interface-id:* Indicates the interface ID. ***switch***: Indicates whether the port participates in packet switching.

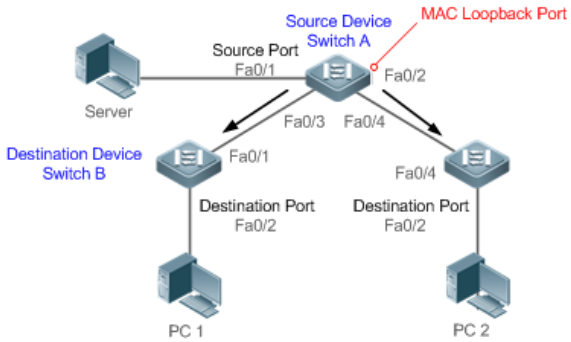
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring a Destination Port on the RSPAN Destination Device

Command	**monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-id* [**switch**]
Parameter Description	*session-num:* Indicates the ID of an RSPAN session. *remote-vlan*: Indicates a remote VLAN. *interface-id:* Indicates the interface ID. ***switch***: Indicates whether the port participates in packet switching.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring One-to-Many RSPAN

Scenario Figure 5-6	
Configuration Steps	➢ As shown in the preceding figure, configure a remote VLAN on Switch A, Switch B, and Switch C. ➢ Configure the source port and output port on Switch A. ➢ Configure the destination port on Switch B and Switch C.

A	`Qtech# configure`
	`Qtech(config)# vlan 7`
	`Qtech(config-vlan)# remote-span`
	`Qtech(config-vlan)# exit`

	Qtech(config)# monitor session 1 remote-source Qtech(config)# monitor session 1 source interface fa 0/1 both Qtech(config)# interface range fa0/3-4 Qtech(config-if-range)# switchport mode trunck
B, C	Qtech(config)# vlan 7 Qtech(config-vlan)# remote-span Qtech(config-vlan)# exit Qtech(config)# monitor session 1 remote-destination Qtech(config)# monitor session 1 destination remote vlan 7 interface fa 0/2 Qtech(config)# interface fa0/1 Qtech(config-if)#switchport mode trunck
Verification	Run the **show monitor** command or the **show running** command on Switch A, Switch B, and Switch C to check whether RSPAN is configured successfully.
A	Qtech# show monitor sess-num: 1 span-type: SOURCE_SPAN src-intf: FastEthernet 0/1 frame-type Both dest-intf: FastEthernet 0/2 Remote vlan 7 mtp_switch on
B	Qtech# show monitor sess-num: 1 span-type: DEST_SPAN dest-intf: FastEthernet 0/2 Remote vlan 7 mtp_switch on
C	Qtech# show monitor sess-num: 1 span-type: DEST_SPAN

	dest-intf: FastEthernet 0/2 Remote vlan 7 mtp_switch on

Common Errors

- A remote VLAN must be configured on the source device, intermediate device, and destination device, and their VLAN IDs must be consistent.
- Packet loss may occur if packets of a port with large bandwidth are mirrored to a port with small bandwidth.
- Multiple output ports need to be configured to implement one-to-many RSPAN.

5.5 Monitoring

Displaying

Description	Command
Displays all mirroring sessions existing in the system.	**show monitor**
Displays a specified mirroring session.	**show monitor session** *session-id*

Debugging

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

Description	Command
Debugs SPAN.	**debug span**

6. CONFIGURING SFLOW

6.1 Overview

sFlow is a network monitoring technology jointly developed by InMon, HP, and FoundryNetworks in 2001. This technology has been standardized. It can provide complete traffic flows of Layer 2 to Layer 4, and it is applicable to traffic analysis in the extra-large network. This technology helps users analyze the performance, trend, and existence of network traffic flows in a detailed manner in real time.

sFlow has the following advantages:

- Accurate: sFlow supports accurate monitoring of traffic on a Gigabit network or a network with higher bandwidth.
- Scalable: One sFlow Collector can monitor thousands of sFlow Agents, and it has high scalability.
- Low cost: sFlow Agent is embedded in a network device, and its cost is low.

Protocol Specification

- sFlow Version 5
- RFC 1014

6.2 Applications

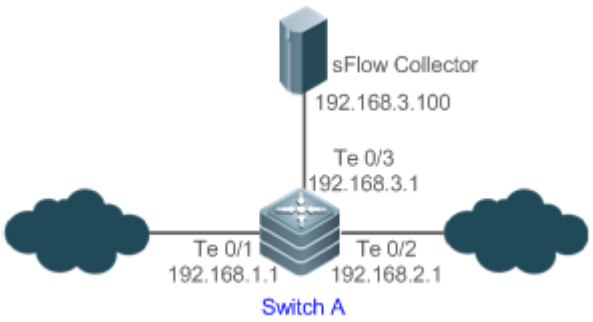
Typical Application	Scenario
Monitoring the LAN Traffic	Regard the device as an sFlow Agent, perform sampling of interface traffic in the LAN, and send the sFlow datagrams to an sFlow Collector for traffic analysis, thereby achieving the purpose of network monitoring.

6.2.1 Monitoring the LAN Traffic

Application Scenario

As shown in Figure 7-1, start switch A that serves as an sFlow Agent, enable flow sampling and counter sampling on port Te 0/1, monitor the traffic in the 192.168.1.0 network segment, encapsulate the sampling data into sFlow datagrams at regular intervals or when the buffer is full, and sent the sFlow data to the sFlow Collector for traffic analysis.

Figure 7-1



Function Deployment

- Configure the addresses of sFlow Agent and sFlow Collector on switch A.
- Enable flow sampling and counter sampling on port Te 0/1 of switch A.

➢ Lots of server software supports sFlow. You can obtain software supporting sFlow at http://www.sflow.org/products/collectors.php. The software sflowtrend is free of charge.

6.3 Features

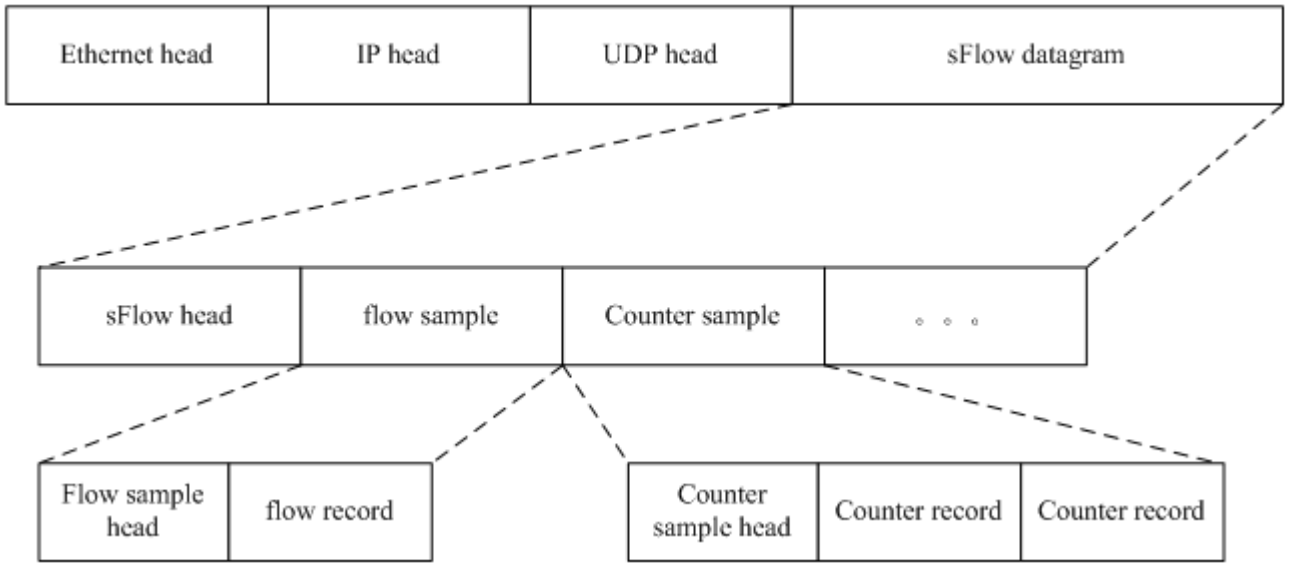
Basic Concepts

❖ sFlow Agent

sFlow Agent is embedded in a network device. Generally, one network device can serves as an sFlow Agent. sFlow Agent can perform flow sampling and counter sampling, encapsulate sampled data into sFlow datagrams, and send the sFlow datagrams to the sFlow Collector.

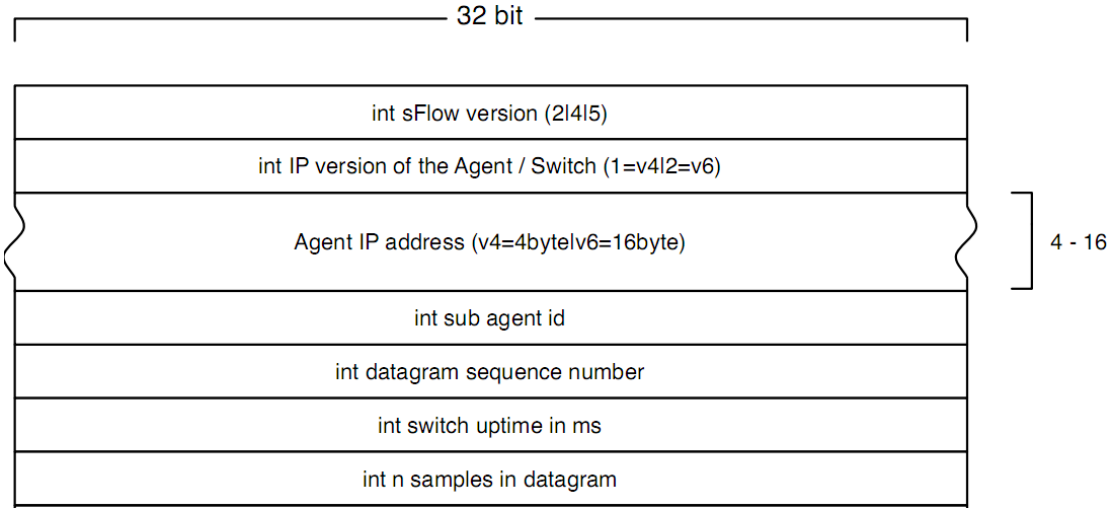
sFlow datagrams are encapsulated in UDP. Figure 7-2 shows the sFlow datagram format.

Figure 7-2 sFlow Datagram Format



One sFlow datagram may contain one or multiple flow samples and counter samples.

Figure 7-3 sFlow Header



sFlow Geader Description:

Field	Description
sFlow version	sFlow version. V2, V4, and V5 are available. Currently, Qtech supports V5 only.
IP version of the agent/switch	IP address version of the sFlow Agent
Agent IP address	IP address of the sFlow Agent
Sub agent id	Sub-agent ID
Datagram sequence number	Serial number of the sFlow datagram
Switch uptime	Duration from the startup time of the switch to the current time

n samples in datagram	The number of samples in the an sFlow datagram. One sFlow datagram may contain one or multiple flow samples and counter samples.

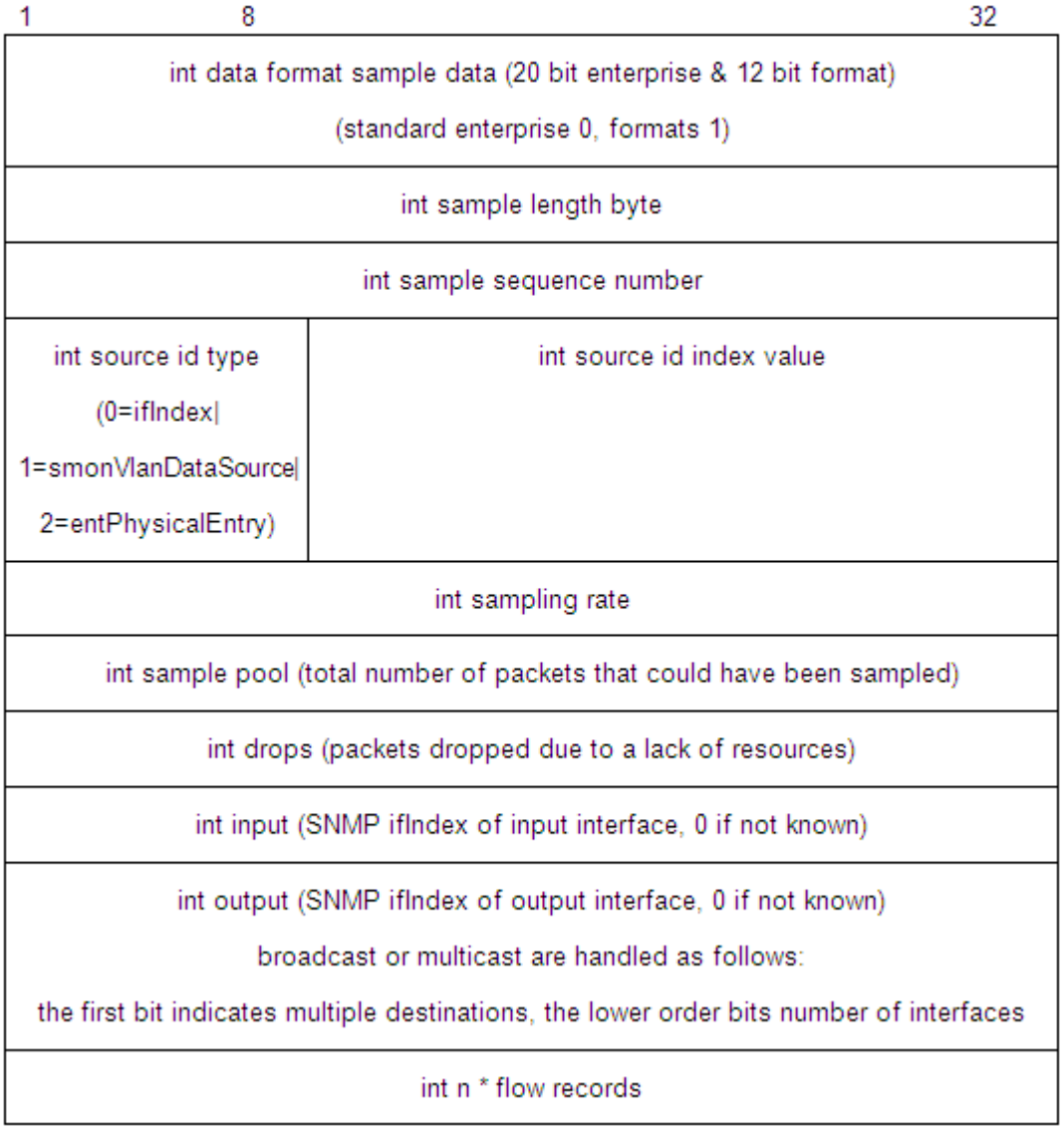
❖ sFlow Collector

sFlow Collector receives and analyzes the sFlow datagram sent from the sFlow Agent. sFlow Collector may be a PC or server. A PC or server installed with the application software for sFlow datagram analysis can be regarded as an sFlow Collector.

❖ Flow Sampling

Based on the specified sampling rate, the sFlow Agent device performs flow sampling on the traffic flowing through an interface, including copying the header of the packet, extracting the Ethernet header and IP header of the packet, and obtaining the route information of the packet.

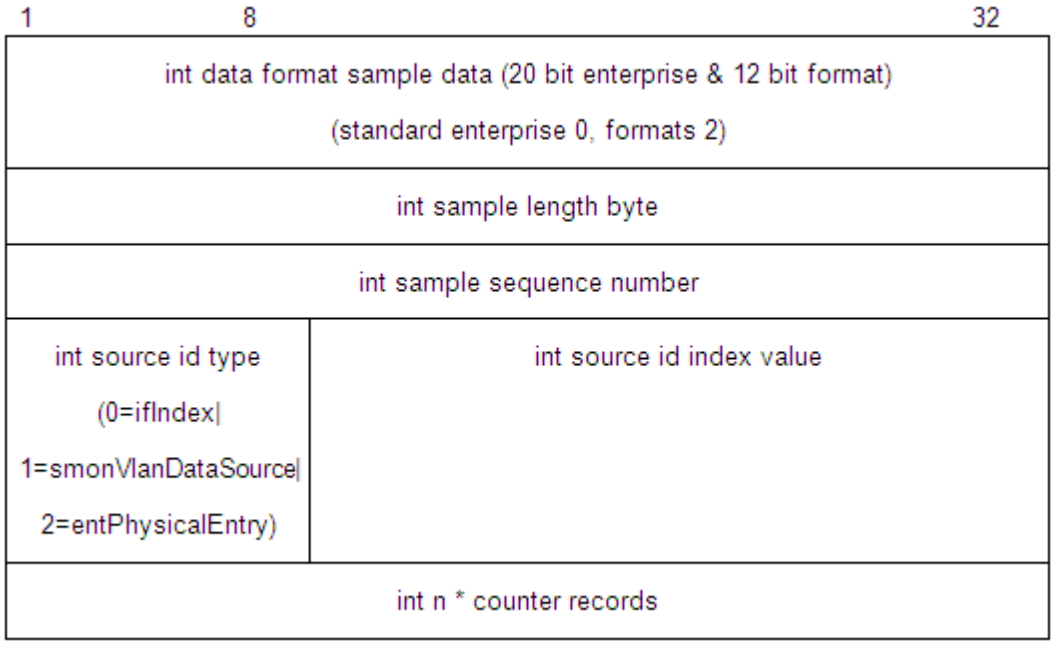
Figure 7-4 Flow Sample Header



❖ Counter Sampling

In counter sampling, an sFlow Agent periodically obtains the statistics and CPU usage on a specified interface. The statistics on the interface include the number of packets input through the interface and the number of packets output through the interface.

Figure 7-5 Counter Sample Header



Functions and Features

Feature	Description
Flow Sampling	Sample the traffic flowing through the interface, and send the encapsulated sFlow datagram to the sFlow Collector for analysis.
Counter Sampling	Periodically send the statistics on the interface to the sFlow Collector for analysis.

6.3.1 Flow Sampling

Sample the traffic flowing through the interface, and send the encapsulated sFlow datagram to the sFlow Collector for analysis.

Working Principle

Based on the specified sampling rate, the sFlow Agent device performs flow sampling on the traffic flowing through an interface, including copying the header of the packet, extracting the Ethernet header and IP header of the packet, and obtaining the route information of the packet. Then, the sFlow Agent encapsulates the flow sampling data into an sFlow datagram and sends the datagram to the sFlow Collector for analysis.

6.3.2 Counter Sampling

Periodically send the statistics on the interface to the sFlow Collector for analysis.

Working Principle

The sFlow Agent performs interface polling on a regular basis. For an interface whose counter sampling interval expires, the sFlow Agent obtains the statistics on this interface, encapsulates the statistics into an sFlow datagram, and sends the datagram to the sFlow Collector for analysis.

6.4 Configuration

Configuration Item	Suggestion & Related Command	
Configuring Basic Functions of sFlow	Mandatory configuration. Establish communication connections between sFlow Agent and sFlow Collector.	
	sflow agent {address }	Configures the sFlow Agent address.
	sflow collector *collector-id* **destination**	Configures the sFlow Collector address.
	Mandatory configuration. Enable flow sampling and counter sampling.	
	sflow counter collector	Enables the sFlow Agent to send counter samples to the sFlow Collector.
	sflow flow collector	Enables the sFlow Agent to send flow samples to the sFlow Collector .
	sflow enable	Enables sFlow sampling for the configuration interface, that is, enables counter sampling and flow sampling.
Configuring Optional Parameters of sFlow	Optional configuration. Sets the optional parameter attributes of sFlow.	
	sflow collector *collector-id* **max-datagram-size**	Configures the maximum length of the sFlow datagram.
	sflow counter interval	Configures the counter sampling interval.
	sflow flow max-header	Configures the maximum length of the packet header copied during flow sampling.
	sflow sampling-rate	Configures the sampling rate of flow sampling.

6.4.1 Configuring Basic Functions of sFlow

Configuration Effect

- sFlow Agent and sFlow Collector can communicate with each other.

- Traffic flowing through the interface are sampled based on the default sampling rate and sent to the sFlow Collector for analysis.
- Statistics of the interface are periodically sent to the sFlow Collector based on the default sampling interval for analysis.

Notes

- Flow sampling can be configured on only physical interfaces.
- To enable the sFlow Collector to analyze the flow sampling results, the IP address of the sFlow Collector on the sFlow Agent device is required.

Configuration Method

❖ Configuring sFlow Agent Address

- Mandatory configuration.
- Use the **sflow agent address** command to configure the address of the sFlow Agent.
- The sFlow Agent address must be a valid address. That is, the sFlow Agent address must not be a multicast or broadcast address. It is recommended that the IP address of the sFlow Agent device be used.

Command Syntax	**sflow agent address** {*ip-address* **| ipv6** *ipv6-address* }}
Parameter Description	**address**: Configures the IP address of the sFlow agent. *ip-address*: sFlow Agent IPv4 address **ipv6** *ipv6-address*: sFlow Agent IPv6 address
Defaults	No sFlow Agent address is configured by default
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the **Agent IP address** field in the output sFlow datagram. The datagram not configured with this filed cannot be output. The sFlow Agent address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Agent address, a message indicating configuration failure is displayed. It is recommended that the IP address of the sFlow Agent device be configured as the sFlow Agent address.

❖ Configuring sFlow Collector Address

- Mandatory configuration.
- Use the **sflow collector** command to configure the address of the sFlow Collector.
- The sFlow Collector address must be a valid address. That is, the sFlow Collector address must not be a multicast or broadcast address. sFlow Collector must exist, and the route to it must be reachable.

Command Syntax	**sflow collector** *collector-id* **destination** { *ip-address* | **ipv6** *ipv6_address* } *udp-port* **[[vrf** *vrf-name* **] | [oob]]**
Parameter Description	*collector-id*: sFlow Collector ID. The range is from 1 to 2. *ip-address*: sFlow Agent IPv4 address. It is not configured by default **ipv6** *ipv6-address*: sFlow Agent IPv6 address. It is not configured by default *udp-port*: sFlow Collector listening port number **vrf** *vrf-name*: VRF instance name. It is not configured by default **oob**: The sampled traffics are output through the management interface. By default, this parameter is not configured.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the sFlow Collector address. The sFlow Collector address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Collector address, a message indicating configuration failure is displayed. The sFlow Collector monitors the sFlow datagram on the specified port. When the **vrf** parameter is configured, the corresponding VRF instance must exist. When you remove the a VRF instance, the sFlow Collector address will be removed if this VRF instance is also configured for an sFlow Collector address. When the **oob** parameter is configured, a datagram is sent to the sFlow Collector through the management interface.

❖ Enabling sFlow Samples Output to the sFlow Collector

- Mandatory configuration.
- You can use the **sflow flow collector** command to enable the sFlow Agent to send flow samples to the sFlow Collector.
- This function must be enabled on the interface to send flow samples to the sFlow Collector. In addition, sFlow Collector must exist, the route to it must be reachable, and the IP address of the corresponding sFlow Collector has been configured on the sFlow Agent device.

Command Syntax	**sflow flow collector** *collector-id*
Parameter Description	*collector-id*: sFlow Collector ID. The range is from 1 to 2.
Defaults	Sending the flow samples to the sFlow Collector is disabled by default.
Command Mode	Interface configuration mode
Configuration Usage	This command can be used for physical ports and aggregate ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

❖ Enabling Counter Samples Output to the sFlow Collector

- Mandatory configuration.

- You can use the **sflow counter collector** command to enable the sFlow Agent to send counter samples to the sFlow Collector.
- This must be enabled on the interface to send counter samples to the sFlow Collector. In addition, sFlow Collector must exist, the route to it must be reachable, and the IP address of the corresponding sFlow Collector has been configured on the sFlow Agent device.

Command Syntax	**sflow counter collector** *collector-id*
Parameter Description	*collector-id*: sFlow Collector ID. The range is from 1 to 2.
Defaults	Sending counter samples to the sFlow Collector is disabled by default.
Command Mode	Interface configuration mode
Configuration Usage	This command can be used for physical ports and aggregate ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

❖ Enabling Counter Sampling and Flow Sampling

- Mandatory configuration.
- You can use the **sflow enable** command to enable the flow sampling and counter sampling on an interface.
- The forwarding performance of an interface may be affected after flow sampling is enabled.

Command Syntax	**sflow enable**
Parameter Description	N/A
Defaults	The sFlow sampling function on an interface is disabled by default.
Command Mode	Interface configuration mode
Configuration Usage	This command can be used to enable counter sampling and flow sampling for physical ports and aggregate ports.

Check Method

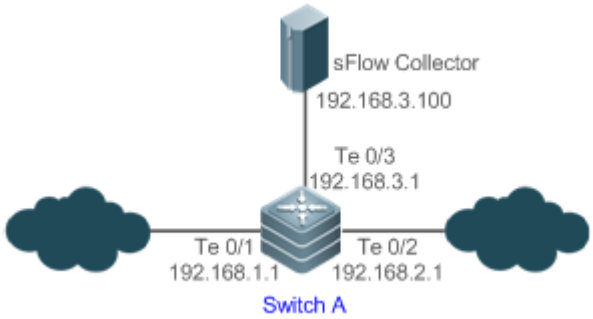
- Use the **show sflow** command to display the sFlow configuration, and check whether the displayed information is consistent with the configuration.

Configuration Examples

❖ Configuring Flow Sampling and Counter Sampling for sFlow Agent

Network Environment

Figure 7-6



As shown in Figure 7-6, start switch A that serves as the sFlow Agent, enable flow sampling and counter sampling on port Te 0/1, monitor the traffic in the 192.168.1.0 network segment, encapsulate the sampling traffic into sFlow datagrams at regular intervals or when the buffer is full, and send the sFlow datagrams to the sFlow Collector for traffic analysis.

Configuration Method

- Configure 192.168.1.1 as the sFlow Agent address.
- Configure 192.168.3.100 as the address of sFlow Collector 1, and 6343 as the port number.
- Configure interface TenGigabitEthernet 0/1 to output flow samples and counter samples to sFlow Collector 1, and enable the sFlow sampling function on this interface.

Switch A

```
Qtech# configure terminal
Qtech(config)# sflow agent address 192.168.1.1
Qtech(config)# sflow collector 1 destination 192.168.3.100 6343
Qtech(config)# interface TenGigabitEthernet 0/1
Qtech(config-if-TenGigabitEthernet 0/1)# sflow flow collector 1
Qtech(config-if-TenGigabitEthernet 0/1)# sflow counter collector 1
Qtech(config-if-TenGigabitEthernet 0/1)# sflow enable
Qtech(config-if-TenGigabitEthernet 0/1)# end
```

Check Method

Use the **show sflow** command to check whether the command output is consistent with the configuration.

```
Qtech# show sflow
sFlow datagram version 5
Global information:
Agent IP: 192.168.1.1
sflow counter interval:30
sflow flow max-header:64
sflow sampling-rate:8192
Collector information:
ID   IP                              Port Size VPN
1    192.168.3.100                   6343 1400
```

```
2    NULL                          0    1400
Port information
Interface                     CID  FID  Enable
TenGigabitEthernet 0/1        1    1    Y
```

6.4.2 Configuring Optional Parameters of sFlow

Configuration Effect

You can adjust the data sampling accuracy by modifying relevant parameter attributes of sFlow.

Notes

- The forwarding performance may be affected when the sampling rate is too low.

Configuration Method

❖ Configuring the Maximum Length of the Output sFlow Datagram

- Optional configuration.
- You can use the **sflow collector** command to configure the length of the sFlow datagram, excluding the Ethernet header, IP header, and UDP header. An sFlow datagram may contain one or multiple flow samples and counter samples. Configuration of the output sFlow datagram's maximum length may lead to the result that the number of sFlow datagrams output during processing of a certain number of flow samples differs from the number of sFlow datagrams output during processing of the same number of counter packets. If the maximum length is greater than MTU, the output sFlow datagrams will be segmented.

Command Syntax	**sflow collector** *collector-id* **max-datagram-size** *datagram-size*
Parameter Description	*collector-id*: sFlow Collector ID. The range is from 1 to 2 **max-datagram-size** *datagram-size*: maximum length of the output sFlow datagram. The range is from 200 to 9,000.
Defaults	The default value is 1,400.
Command Mode	Global configuration mode
Configuration Usage	-

❖ Configuring the Flow Sampling Rate

- Optional configuration.
- You can use the **sflow sampling-rate** command to configure the global flow sampling rate.

- Configuration of flow sampling rate my affect the sFlow sampling accuracy. A lower sampling rate means a higher accuracy and larger CPU consumption. Therefore, the forwarding performance of the interface may be affected when the sampling rate is low.

Command Syntax	**sflow sampling-rate** *rate*
Parameter Description	*rate*: Sampling rate of sFlow sampling. One packet is sampled from every *n* packets (*n* equals the value of **rate**). The range is from 4,096 to16,777,215.
Defaults	The default global flow sampling rate is 8,192.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the global sampling rate of sFlow flow sampling, and sFlow flow sampling of all interfaces uses this sampling rate.

❖ Configuring the Maximum Length of the Packet Header Copied During Flow Sampling

- Optional configuration.
- You can use the **sflow flow max-header** command to configure the length of the packet header copied during flow sampling globally.
- Users can use this command to modify the datagram information to be sent to the sFlow Collector. For example, if a user concerns about the IP header, this user can configure the length to 56 bytes. During encapsulation of flow samples, the first 56 bytes of the sample packet are copied to the sFlow datagram.

Command Syntax	**sflow flow max-header** *length*
Parameter Description	*length*: maximum length of the packet header to be copied. The range is from 18 to 256.
Defaults	The default length of the packet header to be copied during global flow sampling is 64 bytes.
Command Mode	Global configuration mode
Configuration Usage	Configure the maximum number of bytes of the packet content copied from the header of the original packet. The copied content is recorded in the generated sample.

❖ Configuring the Sampling Interval

- Optional configuration.
- You can use the **sflow counter interval** command to configure the global counter sampling interval.
- Enable the counter sampling interface to send the statistics on it to the sFlow Collector at the sampling interval.

Command Syntax	**sflow counter interval** *seconds*

Parameter Description	*seconds*: time interval. The range is form 3 to 2,147,483,647. The unit is second.
Defaults	The default global counter sampling interval is 30 seconds.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the global sFlow counter sampling interval, and sFlow Counter sampling of all interfaces uses this sampling interval.

Check Method

- Check whether an sFlow datagram with the flow samples is received on the sFlow Collector.
- Use the **show sflow** command to display the sFlow configuration, and check whether the displayed information is consistent with the configuration.

Configuration Examples

❖ Configuring Optional Parameters of sFlow

Network Environment

See Figure 7-6.

Configuration Method

- ➢ Set the flow sampling rate to 4,096 in global configuration mode.
- ➢ Configure the length of the packet header copied during flow sampling to 128 bytes in global configuration mode.
- ➢ Set the sampling interval to 10 in global configuration mode.

```
Qtech# configure terminal
Qtech(config)# sflow sampling-rate 4096
Qtech(config)# sflow flow max-header 128
Qtech(config)# sflow counter interval 10
```

Make traffic pass through interface TenGigabitEthernet 0/1.

- ➢ Check whether there is traffic on interface TenGigabitEthernet 0/1 on sFlow Collector 1.
- ➢ Use the **show sflow** command to check whether the command output is consistent with the configuration.

Check Method

```
Qtech# show sflow
sFlow datagram version 5
Global information:
Agent IP: 10.10.10.10
sflow counter interval:10
sflow flow max-header:128
sflow sampling-rate:4096
Collector information:
ID   IP                                Port Size VPN
1    192.168.2.100                     6343 1400
2    NULL                              0    1400
Port information
Interface                         CID  FID  Enable
TenGigabitEthernet 0/1            0    1    Y
```

6.5 Monitoring

Displaying

Function	Command
Displays the sFlow configuration.	**show sflow**