QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Network Management & Monitoring Commands

www.qtech.ru

Оглавление

clear snmp locked-ip

Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures.

clear snmp locked-ip [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

Parameter Description

Parameter	Description
ipv4 *ipv4-address*	Clears a specified IPv4 address.
ipv6 *ipv6-address*	Clears a specified IPv6 address.

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures. You can clear the whole source IP address table or a specific source IP address.

After the source IP addresses locked are cleared, the SNMP packets with these source IP addresses could be authenticated again.

Configuration Examples

Related Commands

Platform Description

The following example clears the whole source IP address table locked after continuous SNMP authentication failures.

```
QTECH#clear snmp locked-ip
```

Command	Description

N/A	N/A

N/A

no snmp-server

Use this command to disable the SNMP agent function.

no snmp-server

Parameter

Parameter	Description
N/A	N/A

Description

Defaults

SNMP agent is enabled by default.

Command mode

Global configuration mode.

Usage Guide

This command disables the SNMP agent services of all versions supported on the device.

Configuration Examples

Related Commands

Platform Description

The following example disables the SNMP agent.

```
QTECH(config)# no snmp-server
```

Command	Description
N/A	N/A

N/

show snmp

Use this command to display the SNMP configuration.

show snmp **[** mib **|** user **|** view **|** group **|** host | locked-ip | process-mib-time **]**

Parameter Description

Parameter	Description
mib	Displays the SNMP MIBs supported.
user	Displays the SNMP user information.
view	Displays the SNMP view information.
group	Displays the SNMP user group information.
host	Displays the explicit host configuration.
locked-ip	Displays the source IP addresses locked after continuous SNMP authentication failures.
process-mib-time	Displays the MIB node requiring the longest processing time.

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show snmp Chassis: 60FF60
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: disabled SNMP logging: disabled SNMP agent:
enabled
```

The example below displays the SNMP configuration:

Command	Description
snmp-server chassis-id	Specifies the SNMP system sequence number.

Related Commands

Platform Description

N/A

snmp trap link-status

Use this command to enable the interface to send link traps. Use the **no** form of this command to disable the interface to send link traps.

snmp trap link-status no snmp trap link-status

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Sending link traps on the interface is enabled by default. If the interface link status changes, SNMP link traps will be sent.

Command mode

Interface configuration mode

Usage Guide

This command can be configured on the Ethernet interface, aggregate ports and SVI interfaces.

Configuration Examples

```
QTECH(config)# interface gigabitEthernet 1/1
QTECH(config-if-GigabitEthernet 1/1)# no snmp trap link-status
```

The following example disables the interface to send link traps.

```
QTECH(config)# interface gigabitEthernet 1/1
QTECH(config-if-GigabitEthernet 1/1)# snmp trap link-status
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

snmp-server authentication attempt

Use this command to configure the maximum number of continuous SNMP authentication failures, and specified the action policy for the authentication failure. Use the **no** form of this command to remove the limit of continuous SNMP authentication failures and the related action policies.

snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

no snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

Parameter Description

Parameter	Description
times	The maximum number of continuous SNMP authentication failures. The range is from 1 to 10.
exceed	Indicates the action policy in the case that the maximum number of continuous SNMP authentication failures is exceeded.
lock	Indicates that the source IP address is permanently locked to be authenticated and can be unlocked only by the administrator's manual configuration.
lock-time *minutes*	Indicates that the source IP address is locked for a period of time. The *minutes* indicates the lock time, ranging from 1 to 65,535. The unit is minute.
unlock	Indicates that no action policy is configured for the authentication failed user, that is, the SNMP authentication for this user is allowed.

Defaults

SNMP attack prevention is disabled by default.

Command mode

Global configuration mode

Usage Guide

The IP address of the SNMP authentication failed user is added to the blacklist. When the maximum number of continuous SNMP authentication failures is exceeded, the system will perform the related authentication limit actions according the configured policy.:

For the permanently locked IP addresses: The source IP addresses can be authenticated only after the administrator unlock them manually.

For the IP addresses locked for a period time: The source IP addresses can be authenticated only after the lock time expires or the administrator unlock them manually.

For the unlocked IP addresses: The source IP address can pass the authentication as long as the correct community (for SNMPv1 and SNMPv2) or username (for SNMPv3) is used.

Configuration Examples

Related Commands

Platform Description

The following example configures the maximum number of continuous SNMP authentication failures to 4, and sets the IP address lock time to 30 seconds.

```
QTECH(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

Command	Description
N/A	N/A

N/A

snmp-server chassis-id

Use this command to specify the SNMP chassis ID. Use the **no** form of this command to restore the default chassis ID.

snmp-server chassis-id ***text***

no snmp-server chassis-id

Parameter Description

Parameter	Description
text	SNMP chassis ID: numerals or characters.

Defaults

The default is 60FF60.

Command mode

Global configuration mode.

Usage Guide

The SNMP chassis ID is generally the serial number of the device to facilitate identification. The SNMP chassis ID can be displayed through the **show snmp** command.

Configuration Examples

Related Commands

Platform Description

The following example specifies the SNMP chassis ID as 123456:

```
QTECH(config)# snmp-server chassis-id 123456
```

Command	Description
show snmp	Displays the SNMP configuration.

N/A

snmp-server community

Use this command to specify the SNMP community access string. Use the **no** form of this command to remove the SNMP community access string.

snmp-server community [0 | 7] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*] [**ipv6**

ipv6-aclname] [*aclnum*] [*aclname*]

no snmp-server community [0 | 7] *string*

Parameter Description

Parameter	Description
0	Indicates that the community string is in plaintext.
7	Indicates that the community string is in ciphertext.

string	Community string, which is the communication password between the NMS and the SNMP agent
view-name	View name
ro	Indicates that the NMS can only read the variables of the MIB.
rw	Indicates that the NMS can read and write the variables of the MIB.
aclnum	Access list number (1 to 199, and 1300 to 2699), which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Access list name, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6-aclname	IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.
ipaddr	Specifies the IP address of the NMS to access the MIB.

Defaults

All communities are read only by default.

Command mode

Global configuration mode.

Usage Guide

This command is an essential command to enable the SNMP agent function, such as specifying the community attribute and IP addresses of NMS to access the MIB.

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

Configuration Examples

Related Commands

Platform Description

The following example defines a SNMP community access string named public, which can be read-only.

```
QTECH(config)# snmp-server community public ro
```

Command	Description
access-list	Defines an access list.

N/A

snmp-server contact

Use this command to specify the system contact string. Use the **no** form of this command to remove the system contact string.

snmp-server contact ***text***

no snmp-server contact

Parameter Description

Parameter	Description
text	Defines a system contact string.

Defaults

No system contact string is set by default.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example specifies the SNMP system contract i-net800@i-net.com.cn:

```
QTECH(config)# snmp-server contact i-net800@i-net.com.cn
```

Command	Description
show snmp-server	Displays the SNMP configuration.
no snmp-server	Disables the SNMP agent function.

N/A

snmp-server enable secret-dictionary-check

Use this command to enable the secret dictionary check for the **community** and **user** fields. Use the

no form of this command to disable the secret dictionary check.

snmp-server enable secret-dictionary-check no snmp-server enable secret-dictionary-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Secret dictionary check for the community and user fields is disabled by default.

Command mode

Global configuration mode.

Usage Guide

This command must be used together with the password policy command.

Configuration Examples

```
QTECH(config)# password policy min-size 6  QTECH(config)# snmp-server
enable secret-dictionary-check QTECH(config)#snmp-server community abc12
% The community(abc12) is a weak community!
```

The following example enables the secret dictionary check for the **community** field.

Related Commands

Command	Description
snmp-server host	Specifies the SNMP host to send the SNMP trap message.

Platform Description

N/A

snmp-server enable traps

Use this command to enable the SNMP agent to send the SNMP trap massage to NMS. Use the **no**

form of this command to disable the SNMP agent to send the SNMP trap massage to NMS.

snmp-server enable traps [*notification-type*]

no snmp-server enable traps

Parameter Description

Parameter	Description
notification-type	Specifies the type of trap messages. snmp: SNMP trap message
	bgp: BGP trap message. bridge: Bridge trap message. isis: ISIS trap message. mac-notification: MAC trap message. ospf: OSPF trap message. urpf: uRPF trap message. vrrp: VRRP trap message. web-auth: Web authentication trap message.

Defaults

Sending trap message to the NMS is disabled by default.

Command mode

Global configuration mode.

Usage Guide

This command must be used together with the **snmp-server host** command to send the trap message. Specifying no trap type indicates all trap messages are sent.

Configuration Examples

```
QTECH(config)# snmp-server enable traps snmp
QTECH(config)# snmp-server host 192.168.12.219 public snmp
```

The following example enables the SNMP agent to send the SNMP trap message.

Related Commands

Command	Description
snmp-server host	Specifies the SNMP host to send the SNMP trap message.

Platform Description

N/A

snmp-server flow-control

Use this command to configure the SNMP flow control. Use the **no** form of this command to restore the default setting.

snmp-server flow-control pps [*count*]

no snmp-server flow-control pps

Parameter Description

Parameter	Description
count	Indicates the number of SNMP requests processed per second, ranging from 50 to 65,535.

Defaults

The default count is 300.

mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example configures the number of SNMP requests processed per second to 200.

```
QTECH(config)# snmp-server flow-control pps 200
```

Command	Description
N/A	N/A

N/A

snmp-server group

Use this command to configure a new SNMP group**.** Use the **no** form of this command to remove a specified SNMP group.

snmp-server group *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write**

writeview] [**access** { [**ipv6** *ipv6_aclname* | *aclnum* | *aclname* }]

no snmp-server group *groupname* {**v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }

Parameter Description

Parameter	Description
v1 | **v2c** | **v3**	Specifies the SNMP version
auth	Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only.
noauth	Specifies no authentication a packet. This applies to

	SNMPv3 only.
priv	Specifies authentication of a packet with encryption. This applies to SNMPv3 only.
readview	Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent.
writeview	Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
aclnum	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example configures a new SNMP group.

```
QTECH(config)# snmp-server group mib2user v3 priv read mib2
```

Command	Description
show snmp group	Displays the SNMP group configuration.

N/A

snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message. Use the **no** form of this command to remove the specified SNMP host.

snmp-server host [**oob**] { *host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps | informs**] [**version**

{ **1** | **2c** | **3** [**auth** | **noauth** | **priv**]] *community-string* [**udp-port** *port-num*] [**via** *mgmt-name*] [*notification-type*]

no snmp-server host [**oob**] { *host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps | informs**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [**via** *mgmt-name*]

Parameter Description

Parameter	Description
oob	Indicates the out of band communication, that is, the trap messages are sent to the alarm server through the MGMT port. This option is available only when the device is equipped with the MGMT port.
host-addr	SNMP host address
ipv6-addr	SNMP host address(ipv6)
vrfname	Set the name of vrf forwarding table
**trap	informs**	Enables the host to send the SNMP notification as traps or informs.
version	SNMP version: V1, V2C or V3
auth	**noauth**	**priv**	Security level of SNMPv3 users

community-string	Community string or username (SNMPv3 version)
port-num	Port of the SNMP host
via *mgmt-name*	Specifies the MGMT port.
notification-type	The type of the SNMP trap message, such as **snmp**. If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included.

Defaults

No SNMP host is specified by default.

Command mode

Global configuration mode.

Usage Guide

This command must be used together with the **snmp-server enable traps** command to send the SNMP trap messages to NMS.

Multiple SNMP hosts can be configured to receive the SNMP trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages can be configured.

The **via** parameter can take effect only when the **oob** parameter is configured. The **vrf** parameter cannot be used together with the **oob** parameter.

Configuration Examples

Related Commands

Platform Description

The following example specifies an SNMP host to receive the SNMP event trap:

QTECH(config)# **snmp-server host** *192.168.12.219* **publicsnmp**

Command	Description

snmp-server enable traps	Enables the SNMP agent to send the SNMP trap message.

N/A

snmp-server inform

Use this command to configure the resend times for inform requests and the inform request timeout**.** Use the **no** form of this command to restore the default settings.

snmp-server inform [**retries** *retry-time* | **timeout** *time*]

no snmp-server inform

Parameter Description

Parameter	Description
retry-num	Specifies the resend times for inform requests, ranging from 0 to 255.
time	Specifies the inform request timeout, ranging from 0 to 21,474,836.

Defaults

The default *retry-num* is 3, and the default **timeout** *time* is 15 seconds.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example configures the resend times of inform requests to 5.

```
QTECH(config)# snmp-server inform retries 5
```

The following example configures the inform request timeout to 20 seconds.

```
QTECH(config)# snmp-server inform timeout 20
```

Command	Description
N/A	N/A

N/A

snmp-server location

Use this command to set the system location string. Use the **no** form of this command to remove the system location string.

snmp-server location ***text***

no snmp-server location

Parameter Description

Parameter	Description
text	String that describes the system location information.

Defaults

No system location string is set by default.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example sets the system location information:

```
QTECH(config)# snmp-server location start-technology-city 4F of A Buliding
```

Command	Description
snmp-server contact	Sets the system contact information.

N/A

snmp-server logging

se this command to enable the system to log the GET, GET-NETX and SET operations of NMS. Use the **no** form of this command to disable the SNMP logging function.

snmp-server logging **{** get-operation | set-operation **}**

no snmp-server logging { **get-operation | set-operation** }

Parameter Description

Parameter	Description
get-operation	Logging function for the GET and GET-NEXT operations.
set-operation	Logging function for the SET operation.

Defaults

The SNMP logging function is disabled by default.

Command mode

Global configuration mode.

Usage Guide

This command is used to enable the logging function for the GET, GET-NETX and SET operations of NMS.

With the **get-operation** enabled, the SNMP agent logs the IP address of NMS, operation type and operation node OID during the GET and GET-NEXT operations.

With the **set-operation** enabled, the SNMP agent logs the IP address of NMS, operation type and operation node OID and related values during the SET operation.

A larger number of logs may affect the device performance. Under normal condition, it is recommended to disable the SNMP logging function.

Configuration Examples

The following example enables the logging function for the GET and SET operations:

```
QTECH(config)#snmp-server logging get-operation
QTECH(config)#snmp-server logging set-operation
```

he operation logs are displayed as below:

```
QTECH#*Feb 7 15:31:16: %SNMP-6-GET_OPER: NMS source-ip(13.12.11.7)
operation(GET) object(id=1.3.6.1.2.1.1.5.0)


QTECH#*Feb 7 15:32:16:%SNMP-6-GETN_OPER: NMS source-ip(13.12.11.7)
operation(GET-NEXT) object(id=1.3.6.1.2.1.1.5.0)


QTECH#*Feb 7 15:33:23: %SNMP-6-SET_OPER: NMS source-ip(13.12.11.7)
operation(SET) object(id=1.3.6.1.2.1.1.5.0, value=QTECH)
```

The following example disables the logging function for the GET and SET operations:

```
QTECH(config)#no snmp-server logging get-operation
QTECH(config)#no snmp-server logging set-operation
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

snmp-server net-id

Use this command to configure the network element coding information of the device. Use the **no**

form of this command to remove the network element coding information.

snmp-server net-id ***text***

no snmp-server net-id

Parameter **Description**

Parameter	Description
text	Configures the network element coding information of the device. The text length ranges from 1 to 255. The text is case-sensitive, and may contain spaces.

Defaults

No network element coding information is configured by default.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example configures the network element coding text to FZ_CDMA_MSC1.

```
QTECH(config)# snmp-server net-id FZ_CDMA_MSC1
```

Command	Description
N/A	N/A

N/

snmp-server packetsize

Use this command to specify the largest size of the SNMP packet. Use the no form of this command to restore the default value.

Parameter Description

Parameter	Description
byte-count	Packet size. The range is from 484 to 17,876 bytes

snmp-server packetsize *byte-count*

no snmp-server packetsize

Defaults

The default is 1,472 bytes.

Command mode

Global configuration mode.

Usage Guide

The following example specifies the largest size of SNMP packet as 1,492 bytes:

```
QTECH(config)# snmp-server packetsize 1492
```

Configuration Examples

Related Commands

Platform Description

N/A

Command	Description
snmp-server queue-length	Specifies the length of the message queue for

	each SNMP trap host.

N/A

snmp-server queue-length

Parameter Description

Use this command to specify the length of the message queue for each SNMP trap host. Use the **no**

form of this command to restore the default value.

snmp-server queue-length ***length***

no snmp-server queue-length

Defaults

The default is 10.

Parameter	Description
length	Queue length. The range is from 1 to 1000.

Command mode

Global configuration mode.

Usage Guide

Use this command to adjust the length of message queue for each SNMP trap host for the purposes of controlling the speed of sending the SNMP trap messages.

Configuration Examples

Related Commands

Platform Description

The following example specifies the length of message queue as 100.

```
QTECH(config)# snmp-server queue-length 100
```

Command	Description

snmp-server packetsize	Specifies the largest size of the SNMP packet.

N/A

snmp-server system-shutdown

Use this command to enable the SNMP message reload function. Use the **no** form of this command to disable the SNMP message reload function.

snmp-server system-shutdown no snmp-server system-shutdown

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The SNMP message reload function is disabled by default.

Command mode

Global configuration mode.

Usage Guide

Use this command to enable the SNMP message reload function which may enable the system to send the device reload traps to the NMS before the device is reloaded or rebooted.

Configuration Examples

The following example enables the SNMP message reload function:

```
QTECH(config)# snmp-server system-shutdown
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

snmp-server trap-format private

Use this command to configure the SNMP traps with private fields. Use the **no** form of this command to restore the default trap format.

Parameter Description

Parameter	Description
N/A	N/A

snmp-server trap-format private no snmp-server trap-format privateDefaults

The private field is not carried in the SNMP trap by default.

Command mode

Global configuration mode.

Usage Guide

Use this command to configure the SNMP trap format with the private field. Currently, the supported data in the private field is alarm occurrence time. For the specific data type and range of each field, refer to QTECH-TRAP-FORMAT-MIB.mib file.

This command does not work if the traps are sent with SNMPv1.

Configuration Examples

Related Commands

Platform Description

The following example configures the SNMP trap format with the private field.

```
QTECH(config)# snmp-server trap-format private
```

Command	Description
N/A	N/A

N/A

snmp-server trap-source

Use this command to specify the source interface of the SNMP trap message. Use the **no** form of this command to restore the default value.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter Description

Parameter	Description
interface	Specifies the source interface of the SNMP trap messages.

Defaults

By default, the IP address of the interface from which the SNMP packet is sent is just the source address.

Command

Global configuration mode.

mode

Usage Guide

For easy management and identification, you can use this command to fix a local IP address as the SNMP source address.

Configuration Examples

Related Commands

Platform Description

The following example specifies the IP address of Ethernet interface 0/1 as the source address of the SNMP trap message:

```
QTECH(config)# snmp-server trap-source fastethernet 0/1
```

Command	Description
snmp-server enable traps	Enables t the SNMP agent to send the SNMP

	trap massage to NMS.
snmp-server host	Specifies the NMS host to send the SNMP trap message.

N/A

snmp-server trap-timeout

Use this command to define the retransmission timeout time of the SNMP trap message. Use the **no**

form of this command to restore the default value.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter Description

Parameter	Description
seconds	Timeout (in seconds) of retransmit the SNMP trap message. The range is from 1 to 1,000.

Defaults

The default is 30 seconds.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Command	Description
snmp-server queue-length	Specifies the length of message queue for the
	SNMP trap host.
snmp-server host	Specifies the NMS host to send the SNMP trap message.
snmp-server trap-source	Specifies the source address of the SNMP trap message.

The following example specifies the timeout period as 60 seconds.

```
QTECH(config)# snmp-server trap-timeout 60
```

Platform Description

N/A

snmp-server udp-port

Use this command to specify a port to receive SNMP packets**.** Use the **no** form of this command to restore the default setting.

snmp-server udp port *port-number*

no snmp-server udp port

Parameter Description

Parameter	Description
port-number	Specifies a port to receive the SNMP packets.

Defaults

The default is 161.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example specifies port 15000 to receive the SNMP packets.

```
QTECH(config)# snmp-server udp-port 15000
```

Related Commands

Command	Description
N/A	N/A

Description

snmp-server user

Use this command to configure a new user to an SNMP group**.** Use the **no** form of this command to remove a user from an SNMP group.

snmp-server user *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { [**ipv6** *ipv6_aclname*] [*aclnum* | *aclname* }]]

no snmp-server user *username groupname* { **v1** | **v2c** | **v3** }

Parameter Description

Parameter	Description
username	Name of the user on the host that connects to the agent.
groupname	Name of the group to which the user belongs.
v1 | v2c | v3	Specifies the SNMP version. But only SNMPv3 supports the following security parameters.

encrypted	Specifies whether the password appears in cipher text. In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has a length of 16 bytes, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can be used only by the local SNMP engine on the switch.
auth	Specifies which authentication level should be used.
auth-password	Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.
priv	Encryption mode. des56 refers to 56-bit DES encryption protocol. *priv-password*: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.
md5	Enables the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol.
aclnumber	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
ipv6_aclname	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv
des56 despassstr
```

The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

Related Commands

Command	Description
show snmp user	Displays the SNMP user configuration.

Platform Description

N/A

snmp-server view

Use this command to configure an SNMP view**.** Use the **no** form of this command to remove an SNMP view.

snmp-server view *view-name oid-tree* { **include** | **exclude** }

no snmp-server view *view-name* [*oid-tree*]

Parameter Description

Parameter	Description
view-name	View name
oid-tree	Specifies the MIB object to associate with the view.
include	Includes the sub trees of the MIB object in the view.
exclude	Excludes the sub trees of the MIB object from the view.

Defaults

By default, a view is set to access all MIB objects.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Command	Description
show snmp view	Displays the SNMP view configuration.

The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).

```
QTECH(config)# snmp-server view mib2 1.3.6.1 include
```

Platform Description

N/A

rmon alarm

Use this command to monitor a MIB variable. Use the **no** form of this command to remove the alarm entry.

rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*]

falling-threshold *value* [*event-number*] [**owner** *ownername*]

no rmon alarm *number*

Parameter description

Parameter	Description
number	Alarm number. The value ranges from 1-65,535.
variable	Alarm variable. The value is a character string consisting of 1 to 255 characters in OID dotted format (the format is entry.integer.instance or a leaf node named .instance, for example. 1.3.6.1.2.1.2.1.10.1).
interval	Sampling interval. The valye ranges from 1 to 2,147,483,647 in the unit of second.
absolute	Absolute sampling. In this mode, when the sampling time arrives, the system directly invokes the variable value.
delta	Delta sampling. In this mode, when the sampling time arrives, the system invokes the delta value of the variable within the sampling interval.
rising-threshold *value*	Rising threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647.
event-number	The event number ranges from 1 to 65,535.
falling-threshold	Falling threshold and the corresponding event number when the threshold is

value	reached. The threshold ranges from -2,147,483,648 to +2,147,483,647
owner *ownername*	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

The RGOS allows you to modify the configured history information of the Ethernet network, including variable, absolute/delta, owner, rising-threshold/falling-threshold, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.

Examples

The example below monitors the MIB variable instance ifInNUcastPkts.6.

```
QTECH(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta

rising-threshold 20 1 falling-threshold 10 1 owner zhangsan
```

Related commands

Command	Description
rmon event *number* [log] [trap *community*] description *string* [owner *owner-string*]	Adds an event definition.

rmon collection history

Use this command to enable history statistics on the Ethernet interface. Use the **no** form of this command to remove the history entry.

rmon collection history *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

no rmon collection history ***index***

Parameter description

Parameter	Description
index	Index of a history entry. The value ranges from 1 to 65,535.
owner *ownername*	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.
buckets *bucket-number*	Capacity of a history entry (that is, the maximum number of history entries). The value ranges from 1 to 65,535. The default value is 10.
interval *seconds*	Statistics period. The unit is second. The value ranges from 1 to 3,600. The default value is 1,800 seconds.

Default

N/A.

Command mode

Interface configuration mode.

Usage guidelines

The configured history control entry parameters cannot be modified. And the history entry can be removed from the interface where the entry configured.

The example below enables log statistics on interface GigabitEthernet 0/1.

Examples

```
QTECH# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
QTECH(config)#interface gigabitEthernet 0/1
QTECH(config-GigabitEthernet0/1)#rmon collection history 1 owner UserA
buckets 5 interval 60
```

Related commands

Command	Description

rmon collection stats *index* [owner *owner-name*]	Adds a statistical entry on the Ethernet interface.

rmon collection stats

Use this command to monitor an Ethernet interface. Use the **no** form of this command to remove the configuration.

rmon collection stats index [**owner** owner-string]

no rmon collection stats **index**

Parameter description

Parameter	Description
index	Index of the statistic table. The value ranges from 1 to 65,535.
owner *ownername*	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive and do not contain spaces.

Default

N/A.

Command mode

Interface configuration mode.

Usage guidelines

N/A.

Examples

The example below enables monitoring the statistics of interface GigabitEthernet 0/1.

```
QTECH# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#interface
gigabitEthernet 0/1
QTECH(config-GigabitEthernet0/1)# rmon collection stats 1 owner UserA
```

Related commands

Command	Description

rmon collection history *index* [**owner** *owner-name*] [**buckets** *bucket-number*] [**interval** *seconds*]	Adds a history control entry.

rmon event

Use this command to define an event. Use the **no** form of this command to remove the event entry.

rmon event *number* [**log**] [**trap** *community*] [*description-string*] [**description** *description-string*] [**owner** *owner-name*]

no rmon event *number*

Parameter description

Parameter	Description
number	Event number. The value ranges from 1 to 65,535.
log	(Optional) Log event. When a log event is triggered, the system records a log.
trap *community*	(Optional) Trap event. When a trap event is triggered, the system sends trap with the group named “community”.
description *description-string*	(Optional) Description of the event. The value is a character string consisting of 1 to 127 characters.
owner *owner-name*	(Optional) Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.

Default

N/A.

Command mode

Global configuration mode.

Usage guidelines

N/A.

Examples

The example below defines the event actions: log event and send trap message.

```
QTECH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#rmon event 1
log trap public description "ifInNUcastPkts is abnormal" owner UserA
```

Related commands

Command	Description
rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Adds an alarm entry.

show rmon

Default

Use this command to display the RMON configuration.

show rmo

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The example below displays the RMON configuration.

```
QTECH#show rmon
ether statistic table:
                index = 1
                interface = GigabitEthernet 0/1 owner = admin
```

```
                status = 0
                dropEvents = 61
                octets = 170647461
                pkts = 580375
                broadcastPkts = 2135
                multiPkts = 3615
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 3254668
                packets65To127Octets = 1833370
                packets128To255Octets = 2098146
                packets256To511Octets = 126716
                packets512To1023Octets = 363621
                packets1024To1518Octets = 1077865

rmon history control table:
                index = 1
                interface = GigabitEthernet 0/1 bucketsRequested =
                5
                bucketsGranted = 5
                interval  =  60  owner  =  UserA
                stats = 1

rmon history table:
                index = 1
                sampleIndex = 2485 intervalStart = 7d:22h:56m:38s
                dropEvents = 0
                octets = 5840
                pkts = 27
                broadcastPkts = 0
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0 rmon alarm table:
                index: 1
```

```
                interval: 60
                oid = 1.3.6.1.2.1.2.2.1.12.6
                sampleType: 2
                alarmValue: 0
                startupAlarm: 3
                risingThreshold: 20
                fallingThreshold: 10
                risingEventIndex: 1
                fallingEventIndex: 1 owner:  UserA
                status: 1

rmon event table:
                index = 1
                description = ifInNUcastPkts is abnormal type = 4
                community = public lastTimeSent = 0d:0h:0m:0s
                owner =UserA
                status = 1

rmon log table:
                eventIndex = 1
                index = 1
                logTime = 6 d:19 h:21 m:48 s  logDescription = ifInNUcastPkts
                is abnormal
```

Related commands

Command	Description
N/A	N/A

show rmon alarm

Default

Use this command to display the RMON alarm table.

show rmon alarm

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The example below displays the RMON alarm table.

```
QTECH#show rmon alarm
rmon alarm table:
                index: 1
                interval: 60
                oid = 1.3.6.1.2.1.2.2.1.12.6
                sampleType: 2
                alarmValue: 0
                startupAlarm: 3
                risingThreshold: 20
                fallingThreshold: 10
                risingEventIndex: 1
                fallingEventIndex: 1 owner:  UserA
                status: 1
```

Related commands

Command	Description
rmon alarm *number variable interval* {**absolute** | **delta** } **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Adds an alarm entry.

show rmon event

Use this command to display the event configuration.

show rmon event

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The example below displays the event configuration.

```
QTECH#show rmon event rmon event table:
                index = 1
                description = ifInNUcastPkts is abnormal type = 4
                community = public lastTimeSent = 0d:0h:0m:0s
                owner =UserA
                status = 1
rmon log table:
                eventIndex = 1
                index = 1
                logTime = 6d:19h:21m:48s
                logDescription = ifInNUcastPkts is abnormal
```

Related commands

Command	Description
rmon event *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]	Adds an event entry.

show rmon history

Use this command to display the history information.

show rmon history

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The example below displays the history information.

```
QTECH#show rmon history rmon history control
table:
                index = 1
                interface = GigabitEthernet 0/1 bucketsRequested =
                5
                bucketsGranted = 5
                interval  =  60  owner  =  UserA
                stats = 1

rmon history table:
                index = 1
                sampleIndex = 2485 intervalStart = 7d:22h:56m:38s
                dropEvents = 0
                octets = 5840
                pkts = 27
                broadcastPkts = 0
                multiPkts = 0
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
```

Related commands

Command	Description
rmon collection history *index* [owner *ownername*] **[buckets** *bucket-number*] **[interval** *seconds*]	Adds a history control entry.

show rmon statistics

Use this command to display the RMON statistics.

show rmon statistics

Default

N/A.

Command mode

Privileged EXEC mode.

Usage guidelines

N/A.

Examples

The example below displays the RMON statistics.

```
QTECH#show rmon statistics ether statistic
table:
                index = 1
                interface = GigabitEthernet 0/1 owner = admin
                status = 0
                dropEvents = 61
                octets = 170647461
                pkts = 580375
                broadcastPkts = 2135
                multiPkts = 3615
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                packets64Octets = 3254668
                packets65To127Octets = 1833370
                packets128To255Octets = 2098146
                packets256To511Octets = 126716
                packets512To1023Octets = 363621
                packets1024To1518Octets = 1077865
```

Related commands

Command	Description
rmon collection stats *index* [**owner** *owner-string*]	Adds a statistical entry.

no ntp

Use this command to disable Network Time Protocol (NTP), and clear all NTP configuration.

no ntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

NTP is disabled by default.

Command mode

Global configuration mode.

Usage Guide

By default, NTP is disabled. However, once the NTP server or the NTP primary clock is configured, the NTP service will be enabled.

Configuration Examples

Related Commands

Platform Description

The following example disables NTP.

```
QTECH(config)#no ntp
```

Command	Description
ntp server	Specifies an NTP server.

N/A

ntp access-group

Use this command to configure an access group to control NTP access. Use the **no** form of this command to remove the peer access group.

ntp access-group { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*

no ntp access-group { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*

Parameter Description

Parameter	Description
peer	Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list.
serve	Allows the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers.
serve-only	Allows the device to receive only time requests from the servers specified in the access list.
query-only	Allows the device to receive only NTP control queries from servers specified in the access list.
access-list-number	Access control list number, ranging from 1 to 99 and 1300 to 1999.
access-list-name	Access control list name.

Defaults

No access rule to control NTP access is configured by default, namely, NTP access is granted to all devices.

Command mode

Global configuration mode.

Usage Guide

Use this command to configure an access group to control NTP access, providing a minimal security measures (more secure way is to use the NTP authentication mechanism).

The NTP service enables the access group options to be scanned in the following order, from least restrictive to most restrictive: peer, serve, serve-only, query-only.

If you do not configure any access groups, NTP access is granted to all devices. However, once you configure the access rule, NTP access is granted only to the devices specified in the access list.

NTP control query is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

Configuration Examples

```
QTECH(config)# access-list 1 permit 192.168.1.1
QTECH(config)# ntp access-group serve-only 1
```

The following example shows how to allow the device to only receive time requests from the device of 192.168.1.1.

Related Commands

Command	Description
ip access-list	Creates an IP access control list.

Platform Description

N/A

ntp authenticate

Use this command to enable NTP authentication. Use the **no** form of this command to disable NTP

Parameter Description

Parameter	Description
N/A	N/A

authentication.

ntp authenticate

no ntp authenticate

Defaults

Disabled.

Command mode

Global configuration mode.

Usage Guide

If NTP authentication is disabled, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the NTP authentication and configure other keys globally.

NTP authentication is implemented through the trusted key specified by the **ntp authentication-key**

and **ntp trusted-key** commands.

Configuration Examples

```
QTECH(config)#ntp authentication-key 6 md5 wooooop
QTECH(config)#ntp trusted-key 6
QTECH(config)#ntp authenticate
```

After an authentication key is configured and specified as the global trusted key, enable NTP authentication.

Related Commands

Command	Description
ntp authentication-key	Sets the global authentication key.
ntp trusted-key	Configures the global trusted key.

Platform Description

N/A

ntp authentication-key

Use this command to configure an NTP authentication key. Use the **no** form of this command to remove the NTP authentication key.

ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

no ntp authentication-key ***key-id***

Parameter Description

Parameter	Description
key-id	Key ID, ranging from 1 to 4294967295.
key-string	Key string
	An encrypted key supports up to 64 bytes of length, while a non-encrypted key supports up to 31 bytes.
enc-type	(Optional) Whether this key is encrypted, where, 0 indicates the key is not encrypted, 7 indicates the key is encrypted simply. The key is not encrypted by default.

Defaults

NTP authentication key is not configured by default.

Command mode

Global configuration mode.

Usage Guide

Use this command to configure an NTP authentication key and enables the md5 algorithm for authentication. Each key presents a unique key ID, which can be configured as a trusted key using the ntp trusted-key command..

You can configure up to 1024 NTP authentication keys. However, each server can support only one key.

Configuration Examples

The following example configures an NTP authentication key.

```
QTECH(config)ntp authentication-key 6 md5 wooooop
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp trusted-key	Configures an NTP trusted key.

ntp server	Specifies an NTP server.

Platform Description

N/A

ntp disable

Use this command to disable the device to receive NTP packets on the specified interface.

ntp disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

All NTP packets can be received by default.

Command mode

Interface configuration mode.

Usage Guide

The NTP message received on any interface can be provided to the client to carry out the clock

adjustment. The function can be set to shield the NTP message received from the corresponding interface.

By default, the device receives NTP packets on all interfaces, and adjust clock for the client. You can use this command to disable the device to receive NTP packets on the specified interface.

This command is configured only the interface that can receive and send IP packets.

Configuration Examples

Related Commands

Platform Description

The following example disables the device to receive the NTP packets.

```
QTECH(config-if)# no ntp disable
```

Command	Description
N/A	N/A

N/A

ntp interval

Use this command to set the interval for time synchronization between the NTP client and the NTP server. Use the **no** form of this command to restore the default time synchronization interval.

ntp interval *seconds*

no ntp interval

Parameter Description

Parameter	Description
seconds	Sets the time synchronization interval in seconds. The value ranges from 10 to 2,592,000.

Defaults

The default value is 64.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

The configuration does not take effect immediately. For immediate validation, enable NTP and then set the interval. If the NTP client has never synchronized the time successfully, it rapidly synchronizes the time at an interval of 5s. Then, it synchronizes time at the preset interval after the first successful time synchronization.

Configuration Examples

The following example configures the NTP time synchronization interval to 3,600 seconds.

```
QTECH(config)# ntp interval 3600
```

ntp master

Use this command to configure the device to act as an authoritative NTP server, synchronizing time to other devices. Use the **no** form of this command to remove the device as an authoritative NTP server.

ntp master [*stratum*]

no ntp master

Parameter Description

Parameter	Description
stratum	Stratum level. The range is from 1 to 15. The default is 8.

Defaults

N/A

Command mode

Global configuration mode.

Usage Guide

In general, the local device synchronizes time from the external time source directly or indirectly.

However, if the time synchronization fails due to network connection trouble, you can use this command to configure the local device to act as an authoritative NTP server to synchronize time to t other devices. Once configured, the device will not perform time synchronization with the time source which is of a higher stratum.

Configuring the device to act as an authoritative NTP server (in particular, specify a lower stratum level), may be likely to overwrite the effective time. If multiple devices in the same network are configured with this command, the time synchronization may be instable due to the time difference between the devices.

Before configuring this command, you need to manually correct the system clock to avoid too much bias if the device has never performed time synchronization with the external clock

source.

Configuration Examples

Related Commands

Platform Description

The following example configures the device to act as an authoritative NTP server, and sets the stratum level to 12:

```
QTECH(config)# ntp master 12
```

Command	Description
N/A	N/A

N/A

ntp server

Use this command to specify a NTP server for the NTP client. Use the **no** form of this command to delete the specified NTP server.

ntp server [**oob** | **vrf** *vrf-name*] { *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain* } [**version** *version*] [**source** *if-name*] [**key** *keyid*] [**prefer**] [**via** *mgmt-name*]

no ntp server *ip-addr*

Parameter Description

Parameter	Description
oob	(Optional) Accesses the NTP server from the MGMT interface. By default, this option is disabled.
vrf *vrf-name*	Specifies the virtual routing and forwarding (VRF) name. By default, this parameter is disabled.
ip-addr	Sets the IP address of the NTP server. The address can be in IPv4 or IPv6 format.
domain	Sets the domain name of the NTP server, supporting IPv4 and IPv6.
version	(Optional) Specifies the NTP version (1-3). The

	default is NTPv3.
if-name	(Optional) Specifies the source interface from which the NTP message is sent (L3 interface).
keyid	(Optional) Specifies the encryption key adopted when communication with the corresponding server. The key ID range is from 1 to 4,294,967,295.
prefer	(Optional) Specifies the given NTP server as the preferred one.
mgmt-name	(Optional) Specifies the egress MGMT interface for the packets in oob mode.

Defaults

No NTP server is configured by default.

Command mode

Global configuration mode.

Usage Guide

At present, RGOS system only supports clients other than servers. Up to 20 servers can be synchronized.

To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server.

In the same condition (for instance, precision), the prefer clock is used for synchronization.

The source interface of NTP packets must be configured with the IP address and can be communicated with the peer.

Configuration

The following example configures an NTP server.

Examples

For IPv4: `QTECH(config)# ntp server 192.168.210.222`

For IPv6: `QTECH(config)# ntp server 10::2`

Related Commands

Command	Description
no ntp	Disables NTP.

Platform Description

N/A

ntp trusted-key

Use this command to set a global trusted key. Use the **no** form of this command to remove the global trusted key.

ntp trusted-key *key-id*

no ntp trusted-key *key-id*

Parameter Description

Parameter	Description
key-id	Global trusted key ID, ranging from 1 to 4294967295.

Defaults

N/A

Command mode

Global configuration mode.

Usage Guide

The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

Configuration Examples

```
QTECH(config)#ntp authentication-key 6 md5 wooooop
QTECH(config)#ntp trusted-key 6
QTECH(config)#ntp server 192.168.210.222 key 6
```

The following example configures an authentication key and sets it as a trusted key.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Configures an NTP authentication key.
ntp server	Configures an NTP server.

Platform Description

N/A

ntp update-calendar

Use this command to enable the NTP client to periodically update the device clock with the time synchronized from the external source clock. Use the no form of this command to remove this function.

ntp update-calendar no ntp update-calendar

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, update the calendar periodically is not configured.

Command mode

Global configuration mode.

Usage Guide

By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

Configuration Examples

The following example configures the NTP update calendar periodically.

```
QTECH(config)# ntp update-calendar
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show ntp server

Use this command to display the NTP server configuration.

show ntp server

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command

Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration

mode

mode

Usage Guide

N/A

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description

The following example displays the NTP server.

```
QTECH#  show  ntp  server  ntp-
server
                              source          keyid      prefer      version
-------------------------------------------------------------------------
--------------

10::2                         None            None       FALSE      3
192.168.210.222               None            None       FALSE
                                                                       3
```

N/A

show ntp status

Use this command to display the NTP configuration.

show ntp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

Usage Guide

Use this command to display the NTP configuration. No configuration is displayed before the synchronization server is configured for the first time.

Configuration Examples

```
QTECH# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24 reference
time is D4BD819B.433892EE (01:27:55.000 UTC )
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

The following example displays the NTP configuration.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

show sntp

Use this command to display the SNTP configuration.

show sntp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode.

Usage Guide

N/A

Configuration Examples

```
QTECH# show sntp
SNTP state           : Enable

SNTP server          : 192.168.4.12
 SNTP sync interval  : 60
 Time zone           : +8
```

The following example displays the SNTP configuration.

Related mmands

Command	Description
ntp enable	Enables SNTP.

Platform Description

N/A

sntp enable

Use this command to enable the SNTP function. Use the no form of this command to restore the default value.

sntp enable no sntp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

SNTP is disabled by default.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example enables SNTP.

```
QTECH(config)# sntp enable
```

Command	Description
show sntp	Displays the SNTP configuration.

N/A

sntp interval

Use this command to set the interval for the SNTP client to synchronize its clock with the NTP/SNTP server. Use the **no** form of this command to restore the default synchronization interval.

sntp interval *seconds*

no sntp interval

Parameter Description

Parameter	Description
seconds	Synchronization interval. The unit is second, and the range is from 60 to 65,535.

Defaults

The default synchronization interval is 1,800 seconds.

Command mode

Global configuration mode.

Usage Guide

To make the synchronization interval configuration effective, run the **sntp enable** command.

Configuration Examples

Command	Description
sntp enable	Enables SNTP.
show sntp	Displays the SNTP configuration.

Related Commands

The following example configures the synchronization interval to 3,600 seconds.

```
QTECH(config)# sntp interval 3600
```

Platform Description

N/A

sntp server

Use this command to specify an SNTP server. Use the **no** form of this command to remove the SNTP server.

sntp server [**oob**] { *ip- address* | *domain* } [**via** *mgmt-name*] [**source** *source-ip-address*]

no sntp server

Parameter Description

Parameter	Description
ip-address	IP address of the SNTP server.
oob	(Optional) Accesses the SNTP server from the MGMT interface.
domain	Specifies the domain name of the SNTP server.
source-ip-address	(Optional) Indicates the specified source IP address.
mgmt-name	(Optional) Specifies the egress MGMT interface for the packets in oob mode.

Defaults

No SNTP server is configured by default.

Command mode

Global configuration mode.

Usage Guide

As SNTP is fully compatible with NTP, the SNTP server can be used as an NTP server in Internet.

Configuration Examples

Related Commands

Platform Description

The following example specifies an SNTP server in Internet.

```
QTECH(config)# sntp server 192.168.4.12
```

Command	Description
show sntp	Displays the SNTP configuration.
sntp enable	Enables SNTP.

N/A

mac-loopback

Use this command to enable MAC loopback. Use the **no** form of this command to disable MAC loopback.

mac-loopback

no mac-loopback

Parameter Description

Parameter	Description
N/A	N/A

Defaults

MAC loopback is disabled by default.

Command mode

Interface configuration mode.

Usage Guide

The MAC loopback feature must be enabled on the interfaces for purposes of local one-to-many mirroring. (Please enable the MAC loopback feature on the down interface, and do not add other configurations to the interface.)

Configuration Examples

The following example configures a remote VLAN.

```
QTECH(config)#vlan 100 QTECH(config-
vlan)#remote-span
QTECH(config-vlan)#exit
```

The following example configures a session and specifies the mirrored port.

```
QTECH(config)#monitor session 1 remote-source
QTECH(config)#monitor session 1 source interface gigabitEthernet 4/1 both
```

The following example configures the mirroring port, and enables MAC loopback on the port.

```
QTECH(config)#monitor session 1 destination remote vlan 100 interface gigabitEthernet 4/2
switch
QTECH(config)#interface gigabitEthernet 4/2
QTECH(config-if-GigabitEthernet 4/2)#switchport access vlan 100 QTECH(config-
if-GigabitEthernet 4/2)#mac-loopback
```

The following example adds interfaces GigabitEthernet 4/3-4 to the remote VLAN.

```
QTECH(config)#interface range gigabitEthernet 4/3-4
QTECH(config-if-range)#switchport access vlan 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

monitor session

Use this command to configure the SPAN session and specify the source port (monitored port).

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

Use this command to configure the SPAN session mirroring only the traffic permitted by the access list

monitor session *session-num* **source interface** *interface-id* **rx acl** *acl-name*

Use this command to configure the SPAN session and specify the destination port (monitoring port).

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

Use this command to configure the SPAN session monitoring the CPU packets.

monitor session *session-num* **source interface** *interface-id* **tx cpu**

Use this command to configure the remote SPAN session ID on the source device..

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

Use this command to configure the remote SPAN session ID on the destination device.

monitor session *session-num* **remote-destination**

Use this command to configure the remote SPAN session and specify the remote SPAN destination VLAN.

monitor session *session-num* **destination remote vlan** *remote-vlan-id* **interface** *interface-id*

[**switch**]

Use this command to configure the SPAN session and specify the source VLAN to monitor. Note that the source VLAN should not be a remote VLAN.

monitor session *session-num* **source vlan** *vlan-id* [**rx**]

Use this command to limit the SPAN source traffic to specific VLANs.

monitor session *session-num* **filter vlan** *vlan-id-list*

Use this command to remove the specified SPAN session, or remove the source port or destination port of the specified SPAN session.

no monitor session *session-num* [**source interface** *interface-id* | **destination interface** *interface-id*]

Use this command to remove the specified remote SPAN session, or remove the destination port of the remote SPAN session.

no monitor session *session-num* [**destination remote vlan** *remote-vlan-id* **interface** *interface-id*]

Use this command to remove the specified remote SPAN session, or remote the destination port of the remote SPAN session.

default monitor session *session-num* [**destination remote vlan** *remote-vlan-id* **interface** *interface-id*]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the SPAN session.

default monitor session *session-num* { **source interface** *interface-id* | **destination interface** *interface-id* }

Parameter Description

Parameter	Description
session_number	SPAN session number
interface-id	Interface name
acl *acl-name*	Access list name

remote-vlan-id	Remote VLAN ID
vlan-id	VLAN ID (remote VLAN excluded)
vlan-id-list	VLAN list (remote VLAN excluded)
rx	Monitors the only received traffic.
tx	Monitors the only transmitted traffic.
both	Monitors both received and transmitted traffic. This is the default.
switch	Enables switching on the destination port. Switching function is disabled by default.
cpu	Monitors the CPU packets. This is disabled by default.

Defaults

Port monitoring is disabled by default.

Global configuration mode.

Usage Guide

Use this command to configure SPAN or remote SPAN, and specify the source port or destination port.

If the both, rx or tx is not specified for the source port, the both parameter is the default. Configuring an access list for the source port indicates that only the traffic permitted by the access list is monitored.

The switch feature is disabled on the destination port.

CPU packet monitoring, which is enabled through the cpu parameter, is disabled by default.

Configuration Examples

The following example configures the source port and destination port of the SPAN session.

```
QTECH(config)# monitor session 1 source interface gigabitEthernet 0/1
QTECH(config)# monitor session 1 destination interface gigabitEthernet 0/2
```

The following example configures the SPAN session mirroring only the traffic permitted by the access list.

```
QTECH(config)# monitor session 3 source interface gigabitEthernet 0/3 rx acl
90
```

The following example configures a remote SPAN session.

```
QTECH(config)# monitor session 10 remote-source
```

The following example configures the destination port of the remote SPAN session.

```
QTECH(config)# monitor session 4 destination remote vlan 10 interface
gigabitEthernet 0/5
```

The following example configures the source VLAN of the SPAN session.

```
QTECH(config)# monitor session 1 source vlan 1
```

The following example removes the SPAN session.

```
QTECH(config)# no monitor session 1
```

The following example removes the source port and destination port of the SPAN session.

```
QTECH(config)# no monitor session 1 source interface gigabitEthernet 0/18
QTECH(config)# no monitor session 1 destination interface gigabitEthernet 0/18
```

The following example configures the SPAN session monitoring only the traffic sent from CPU.

```
QTECH(config)# monitor session 3 source interface gigabitEthernet 0/3 tx cpu
```

The following example configures the SPAN session monitoring traffic, including the traffic sent from CPU.

```
QTECH(config)# monitor session 3 source interface gigabitEthernet 0/3 tx cpu
QTECH(config)# monitor session 3 source interface gigabitEthernet 0/3 tx
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

remote-span

Use this command to configure a remote SPAN VLAN in VLAN configuration mode. Use the **no** form of this command to disable the remote SPAN VLAN.

remote-span

no remote-span

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Remote SPAN VLAN is disabled by default.

Command mode

VLAN configuration mode.

Usage Guide

N/A

Configuration Examples

The following example configures a remote SPAN VLAN.

```
QTECH(config)# vlan 100
QTECH(config-vlan)# remote-span
```

Related Commands

Command	Description
show vlan	Displays VLAN configuration.

Platform Description

N/A

show monitor

Use this command to display the SPAN configurations.

show monitor [**session** *session_number*]

Parameter Description

Parameter	Description
session_number	Displays the specified SPAN session.

Defaults

N/A

Command mode

Privileged EXEC mode, global configuration mode and interface configuration mode

Usage Guide

N/A

Configuration Examples

```
QTECH(config)# show monitor sess-num: 2
span-type: LOCAL_SPAN
src-intf:
TenGigabitEthernet 0/5   frame-type Both
dest-intf:
TenGigabitEthernet 0/6
sess-num: 1
span-type:
LOCAL_SPAN src-intf:
TenGigabitEthernet 0/3   frame-type Both
dest-intf:
```

This following example displays all SPAN sessions.

he following example displays SPAN session 1.

```
QTECH(config)# show monitor session 1 sess-num: 1
span-type: LOCAL_SPAN src-intf:
TenGigabitEthernet 0/3     frame-type Both dest-intf:
TenGigabitEthernet 0/4
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

sflow agent

Use this command to configure the address of the sFlow Agent.

sflow agent { **address** { *ip-address* **| ipv6** *ipv6-address* }} | { **interface** { *interface-name* | **ipv6**
interface-name }}

Use this command to delete the address of the sFlow Agent.

no sflow agent { address | interface }

Use this command to restore the default setting.

default sflow agent { address | interface }

Parameter Description

Parameter	Description
address	Configures the IP address of the sFlow Agent.
ip-address	sFlow Agent IPv4 address.
ipv6 *ipv6-address*	sFlow Agent IPv6 address.
interface	Configures the interface of the sFlow Agent.
interface-name	Interface of IPv4 address.
ipv6 *interface-name*	Interface of IPv6 address.

Defaults

Command Mode

Global configuration mode

Default Level

14

Usage Guide

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.

Configuration Examples

The following example configures 192.168.2.1 as the sFlow Agent address.

```
QTECH(config)# sflow agent address 192.168.2.1
```

Verification

Use the show sflow command to display the sFlow configuration.

Prompt

Prompt an error message when the address is invalid.

Messages

```
invalid host address.
```

Common Errors

N/A

Platforms

N/A

sflow collector *collector-id* destination

Use this command to configure the address of the sFlow Collector.

sflow collector *collector-id* **destination** { *ip-address* | **ipv6** *ipv6_address* } *udp-port* **[vrf** *vrf-name* **] |**

[**description** *collector-name*]

Use this command to delete the address of the sFlow Collector.

no sflow collector *collector-id* **destination** { *ip-address* | **ipv6** *ipv6_address* } *udp-port* **[vrf** *vrf-name* **]**

[**description** *collector-name*]

Use this command to delete the address of the sFlow Collector.

default sflow collector *collector-id* **destination** { *ip-address* | **ipv6** *ipv6_address* } *udp-port* **[vrf**

vrf-name] **|** [**description** *collector-name*]

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.
ip-address	sFlow Collector IPv4 address
ipv6 *ipv6-address*	sFlow Collector IPv6 address
udp-port	sFlow Collector listening port number
vrf *vrf-name*	VRF instance name. It is not configured by default.
description *collector-name*	Description of the sFlow Collector.

Defaults

Command Mode

Global configuration mod

Default Level

14

Usage Guide

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.

Configuration Examples

The following example configures 192.168.1.100 as the address of sFlow Collector 1, 6343 as the port number and vpn 1 as the VRF instance.

```
QTECH(config)# sflow collector 1 destination 192.168.2.100 6343 vrf vpn1
```

Verification

Use the **show sflow** command to display the sFlow Collector.

Prompt Messages

Prompt an error message when the address is invalid.

```
invalid host address.
```

No VPN exists.

```
vpn is not exist
```

Common Errors

N/A

Platforms

N/A

sflow collector *collector-id* max-datagram-size

Use this command to configure the maximum length of the output sFlow datagram.

sflow collector *collector-id* max-datagram-size *datagram-size*

Use this command to restore the default maximum length of the output sFlow datagram.

no sflow collector *collector-id* max-datagram-size

Use this command to restore the default maximum length of the output sFlow datagram.

default sflow collector *collector-id* max-datagram-size

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.
max-datagram-size *datagram-size*	The maximum length of the output sFlow datagram. The range is from 200 to 9,000.

Defaults

The default maximum length of the output sFlow datagram is 1,400.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration

The following example configures 1,000 as the maximum length of the output sFlow datagram for sFlow

Examples

Collector.

```
QTECH(config)# sflow collector 1 max-datagram-size 1000
```

Verification

Use the show sflow command to display the maximum length of the output sFlow datagram.

Prompt Messages

N/A

Common Errors

N/A

Platforms

N/A

sflow counter collector

Use this command to enable the sFlow Agent to send counter samples to the sFlow Collector.

sflow counter collector *collector-id*

Use this command to disable the sFlow Agent to send counter samples to the sFlow Collector.

no sflow counter collector

Use this command to disable the sFlow Agent to send counter samples to the sFlow Collector.

default sflow counter collector

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.

Defaults

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

This command can be used for physical ports, SVI ports and sub routed ports and aggregate ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

Configuration Examples

The following example enables interface TenGigabitEthernet 0/5 to send counter samples to sFlow Collector 2.

```
QTECH(config-if-TenGigabitEthernet 0/5)# sflow counter collector 2
```

Verification

Use the **show sflow** command to display the sFlow counter sampling configuration.

Prompt Messages

N/A

Common Errors

N/A

Platforms

N/A

sflow counter interval

Use this command to configure the sFlow counter sampling interval.

sflow counter interval *seconds*

Use this command to restore the default sFlow counter sampling interval.

no sflow counter interval

Use this command to restore the default sFlow counter sampling interval.

default sflow counter interval

Parameter Description

Parameter	Description
seconds	sFlow counter sampling interval. The range is form 3 to 2,147,483,647. The unit is second.

Defaults

The default sFLow counter sampling interval is 30 seconds.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to configure the global sFlow counter sampling interval, and sFlow Counter sampling of all interfaces uses this sampling interval.

Configuration Examples

The following example configures the sFlow counter sampling interval to 60 seconds.

```
QTECH(config)# sflow counter interval 60
```

Verification

Use the **show sflow** command to display the sFlow counter sampling interval.

Prompt Messages

N/A

Common

N/A

Errors

Platforms

N/A

sflow enable

Use this command to enable flow sampling and counter sampling on the interface.
sflow enable [ingress | egress]

Use this command to disable flow sampling and counter sampling on the interface.
no sflow enable

Use this command to disable flow sampling and counter sampling on the interface.
default sflow enable

Parameter Description

Parameter	Description
ingress	Enables sFlow sampling in ingress direction.
egress	Enables sFlow sampling in egress direction.

Defaults

The sFlow sampling function on an interface is disabled by default.

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

If the direction parameter is not specified, sampling on both directions are enabled.

The SVI ports and sub routed ports support only the **ingress** parameter.

The ACL should be configured and applied on the interface before the flow sampling based on ACL matching is enabled.

Configuration Examples

The following example enables the sFlow sampling on interface TenGigabitEthernet 0/5.

```
QTECH(config-if-TenGigabitEthernet 0/5)# sflow enable
```

Verification

Use the **show sflow** command to display the status of the sFlow sampling function.

Prompt Messages

N/A

Common Errors

N/A

Platforms

N/A

sflow flow collector

Use this command to enable the sFlow Agent to send flow samples to the sFlow Collector.

sflow flow collector *collector-id*

Use this command to disable the sFlow Agent to send flow samples to the sFlow Collector.

no sflow flow collector

Use this command to disable the sFlow Agent to send flow samples to the sFlow Collector.

default sflow flow collector

Parameter Description

Parameter	Description
collector-id	sFlow Collector ID. The range is from 1 to 2.

Defaults

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

This command can be used for physical ports, SVI ports, sub routed ports and aggregate ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

Configuration Examples

The following example enables interface TenGigabitEthernet 0/5 to send flow samples to sFlow Collector 2.

```
QTECH(config-if-TenGigabitEthernet 0/5)# sflow flow collector 2
```

Verification

Use the **show sflow** command to display the sFlow flow sampling configuration.

Prompt Messages

N/A

Common Errors

N/A

Platforms

N/A

sflow flow max-header

Use this command to configure the maximum length of the packet header copied during flow sampling.

Parameter Description

sflow flow max-header *length*

Use this command to restore the default maximum length of the packet header copied during flow sampling.

no sflow flow max-header

Use this command to restore the default maximum length of the packet header copied during flow sampling.

default sflow flow max-header

Parameter	Description
length	Maximum length of the packet header to be copied. The range is from 18 to 256. The unit is byte.

Defaults

The default length is 64 bytes.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

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.

Configuration Examples

The following example sets the maximum length of the packet header copied during sFlow flow sampling to 128 bytes.

```
QTECH(config)# sflow flow max-header 128
```

Verification

Use the **show sflow** command to display the maximum length of the packet header copied during sFlow flow sampling.

Prompt Messages

N/A

Common Errors

N/A

Platforms N/A

sflow sampling-rate

Use this command to configure the sampling rate of sFlow flow sampling.

sflow sampling-rate ***rate***

Parameter Description

Use this command to restore the default the sampling rate of sFlow flow sampling.

no sflow sampling-rate

Use this command to restore the default sampling rate of sFlow flow sampling.

default sflow sampling-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 to 65,535.

Defaults

The default sFlow flow sampling rate is 8,192.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

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.

Configuration Examples

The following example sets the sFlow flow sampling rate to 4,096.

```
QTECH(config)# sflow sampling-rate 4096
```

Verification

Use the show sflow command to display the sFlow flow sampling rate.

Prompt Messages

N/A

Common Errors

N/A

Platforms

N/A

sflow source

Use this command to configure the source address of the output packets.

sflow source { address {*ip-address* **| ipv6** *ipv6-address* }} | { **interface** { *interface-name* | **ipv6**

interface-name }}

Use this command to remove the source address of the output packets.

no sflow source { address | interface }

Parameter Description

Use this command to restore the default source address of the output packets.

default sflow source { address | interface }

Parameter	Description
address	Configures the source IP address of sFlow output packets
ip-address	sFlow Source IPv4 address
ipv6 *ipv6-address*	sFlow Source IPv6 address
interface	Configures the source interface of sFlow output packets

interface-name	sFlow Source interface (configured with an IPv4 address)
ipv6 *interface-name*	sFlow Source interface (configured with an IPv6 address)

Defaults

The default sFlow Source address is the local device IP address which is used to ping the destination IP

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to configure the source IP address of the output packets. If a source interface is specified, the primary address of the interface will be the source IP address of the outputs packets. If the source interface is not specified or the IP address of the source interface is unreachable, for example, the interface is shutdown, the default source address will be used.

Configuration Examples

The following example configures the source address of the sFlow output packets as 192.168.2.1.

```
QTECH(config)# sflow source address 192.168.2.1
```

Verification

Use the **show sflow** command to display the status of the sFlow sampling function.

Prompt Messages

N/A

Common Errors

N/A

Platforms

N/A

show sflow

Use this command to display the sFlow configuration.

show sflow

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode/global configuration mode/interface configuration mode

Default Level

14

Usage Guide N/A

Configuration Examples

```
QTECH(config)#show sflow sFlow datagram version 5
Global information:
Agent IP: 10.10.10.10
sflow counter interval:30 sflow flow max-header:64
sflow sampling-rate:8192 Collector information:
ID   IP               Port Size VPN
1    NULL             6343 1400

2    192.168.2.100    0    1400


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

The following example displays the sFlow configuration.

Field Description:

Field	Description

sFlow datagram version	sFlow datagram version. Currently, QTECH supports V5 only.
Agent IP	IP address of the sFlow Agent. It can be configured by using the sflow Agent address {*ip-address* | ipv6 *ipv6-address* } command.
sflow counter interval	Counter sampling interval
sflow flow max-header	The maximum length of bytes of the packet header to be copied
sflow sampling-rate	Flow sampling rate
ID	sFlow Collector ID
IP	The IP address of the sFlow Colletor to receive sFlow datagram
Port	Port No. of the sFlow Collector to receive sFlow datagram
Size	The maximum length of the output sFlow datagram
VPN	VPN instance name of sFlow Collector
Interface	An interface configured with sFlow function
CID	The destination sFlow Collector ID to which the sFlow Agent sends the counter samples.
FID	The destination sFlow Collector ID to which the sFlow Agent sends the flow samples.
Enable	The status of the sFlow sampling function

Prompt Messages

N/A

Platforms

N/A