1 SNMP Commands

Command	Function
clear snmp locked-ip	Clear the list of source IP addresses that are locked after Simple Network Management Protocol (SNMP) authentication fails consecutively.
no snmp-server	Disable the SNMP agent function of a device.
show snmp	Display the SNMP status.
snmp trap link-status	Send a Link Trap message through an interface.
snmp-server authentication attempt	Configure the maximum number of consecutive SNMP authentication failures and specify the corresponding processing actions.
snmp-server chassis-id	Configure a system serial number.
snmp-server community	Configure an authentication name and access permission.
snmp-server contact	Configure a system contact mode.
snmp-server enable secret-dictionary-check	Configure password dictionary check for communities and users.
snmp-server enable traps	Enable the agent to actively send Trap messages to the NMS.
snmp-server enable version	Configure an SNMP version.
snmp-server flow-control pps	Configure SNMP traffic control.
snmp-server group	Configure an SNMP user group.
snmp-server host	Configure NMS host addresses for the agent to send messages.
snmp-server inform	Configure Inform message sending attempts and timeout time.
snmp-server location	Configure a system location.
snmp-server logging	Enable the SNMP logging function.
snmp-server net-id	Configure NE code information of a device.
snmp-server packetsize	Configure the maximum packet length of the SNMP

	agent.
snmp-server queue-length	Configure the queue of the Trap messages.
snmp-server source-interface	Configure the source port of a device to receive SNMP packets.
snmp-server system-shutdown	Enable the SNMP system reboot notification function.
snmp-server trap-format private	Include private fields in SNMP Trap messages.
snmp-server trap-source	Configure a source address for sending Trap messages.
snmp-server trap-timeout	Configure the timeout time of Trap message re-sending.
snmp-server udp-port	Configure the ID of a port that receives SNMP packets.
snmp-server user	Configure an SNMP user.
snmp-server view	Configure an SNMP view.

1.1 clear snmp locked-ip

Function

Run the **clear snmp locked-ip** command to clear the list of source IP addresses that are locked after Simple Network Management Protocol (SNMP) authentication fails consecutively.

Syntax

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

Parameter Description

ipv4 *ipv4-address*: Specifies the source IPv4 address to be cleared.

ipv6 *ipv6-address*: Specifies the source IPv6 address to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

- This command is used to manually clear source IP addresses that are locked after authentication fails consecutively. A list of source IP addresses or a specific source IP address can be cleared.
- After a source IP address is cleared, a request to authenticate the IP address can be initiated when SNMP access packets from this cleared IP address are received.

Examples

The following example clears the list of source IP addresses that are locked after SNMP authentication fails consecutively.

```
Hostname> enable
Hostname# clear snmp locked-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 no snmp-server

Function

Run the **no snmp-server** command to disable the SNMP agent function of a device.

The SNMP agent function is enabled by default.

Syntax

no snmp-server

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The SNMP agent function is enabled by default. When SNMP agent parameters (for example, Network Management System (NMS) host address, authentication name, and access permission) are configured, the SNMP agent service is automatically enabled. This command can be used to disable the agent service of all SNMP versions supported on a device.
- This command must be used with the **enable service snmp-agent** command to make the SNMP agent service take effect. Otherwise, the SNMP agent service will not take effect.
- After this command is run, all SNMP agent service configurations are shielded. In this case, running the **show running-config** will not display the configurations. The configurations can be restored after the SNMP agent service is enabled again. Running the **no enable service snmp-agent** will not shield the SNMP agent configurations.

Examples

The following example disables the SNMP agent service function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no snmp-server
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **enable service snmp-agent** (basic configuration/basic management)

1.3 show snmp

Function

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

Syntax

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

Parameter Description

group: Displays SNMP user group information.

host: Displays user configuration information.

locked-ip: Displays source IP address that is locked after consecutive SNMP authentication failure.

mib: Displays SNMP management information base (MIB) information supported in the system.

process-mib-time: Displays the MIB node with the longest processing time.

user: Displays SNMP user information.

version: Displays SNMP version.

view: Displays SNMP view information.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays SNMP statistics.

```
Hostname> enable
Hostname# 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
```

Table 1-1Output Fields of the show snmp Command

Field	Description
Chassis	System serial number
SNMP packets input	Total number of input packets
Bad SNMP version errors	Total number of packets with version error
Unknown community name	Total number of packets in which an unknown community name is used for access
Illegal operation for community name supplied	Total number of packets in which the community name is used for override operations
Encoding errors	Total number of packets with encoding error
Number of requested variables	Total number of read MIB objects
Number of altered variables	Total number of set MIB objects
Get-request PDUs	Total number of Get request packets
Get-next PDUs	Total number of Get-next request packets
Set-request PDUs	Total number of Set request packets
SNMP packets output	Total number of output packets
Too big errors (Maximum packet size 1472)	Total number of excessively long packets (more than 1,472 bytes)
No such name errors	Total number of packets that contains the no such name error
Bad values errors	Total number of packets that contains the bad values error
General errors	Total number of packets that contains the general error
Response PDU	Total number of packets that are normally returned
Trap PDUs	Total number of sent Trap packets

Field	Description
SNMP global trap	Global Trap enabling/disabling status
SNMP logging	Global SNMP log enabling/disabling status
SNMP agent	Global SNMP agent enabling/disabling status

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 snmp trap link-status

Function

Run the **snmp trap link-status** command to send a Link Trap message through an interface.

Run the **no** form of this command to disable this function.

The Link Trap message sending function is enabled on an interface by default.

Syntax

snmp trap link-status

no snmp trap link-status

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After this command is run, the SNMP sends a Link Trap message if the link status on the interfaces (Ethernet interface, AP interface, and SVI interface) changes. Otherwise, the SNMP does not send the message.

Examples

The following example disables the Link Trap sending function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no snmp trap link-status
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 snmp-server authentication attempt

Function

Run the **snmp-server authentication attempt** command to configure the maximum number of consecutive SNMP authentication failures and specify the corresponding processing actions.

Run the **no** form of this command to remove this configuration.

The SNMP attack prevention and detection function is disabled by default.

Syntax

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

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

Parameter Description

attempt-times: Maximum number of SNMP authentication failures. The value range is from 1 to 10.

exceed: Specifies the actions taken after the SNMP authentication failures exceed the threshold.

lock: Permanently forbids this source IP address from authentication. After this source IP address is placed on the blacklist, the administrator needs to manually unlock the IP address.

lock-time *lock time*: Specifies the lock time of a source IP address after this source IP address is forbidden from authentication, in minutes. The value range is from 1 to 65535.

unlock: Allows a user to log in though the user fails the authentication.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After a source IP address fails the SNMP authentication, the system adds the source IP address to the blacklist. When the number of consecutive authentication failures exceeds the limit, the system restricts subsequent access authentication of this source IP address based on the configured processing actions.

- The permanently forbidden source IP addresses can be authenticated for access again only after the administrator manually unlocks the IP addresses.
- The source IP addresses that are forbidden in a period of time can be authenticated again after the period expires or after the administrator manually unlocks the IP addresses.
- Unrestricted source IP addresses can be authenticated again based on the correct community name (for SNMPv1 and SNMPv2c) or username (for SNMPv3) so long as users access authentication again.

Examples

The following example sets the consecutive authentication failures of SNMP to 4 and IP address lock time to 30 minutes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

Notifications

After the SNMP attack prevention and detection function is enabled, if a source IP address is locked because an incorrect community name or username is used for access authentication, the following notification will be displayed.

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 snmp-server chassis-id

Function

Run the **snmp-server chassis-id** command to configure a system serial number.

Run the **no** form of this command to restore the default configuration.

The default system serial number is **60FF60**.

Syntax

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

no snmp-server chassis-id

Parameter Description

chassis-id-text: Text of the system serial number, which may be digits or characters. The maximum length is 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In general, the device serial number is used as the SNMP serial number to facilitate identification of the device. The system sequence number can be displayed by running the **show snmp** command.

Examples

The following example sets the system serial number of SNMP to 123456.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server chassis-id 123456
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 snmp-server community

Function

Run the **snmp-server community** command to configure an authentication name and access permission.

Run the **no** form of this command to remove this configuration.

The default access permission of all communities is read-only.

Syntax

snmp-server community [**0** | **7** | **secret** [**0** | **8**]] *community-string* [**view** *view-name*] [**ro** | **rw**] [**host** *ipv4-address* | **host** *ipv6-address*] [**ipv6** *ipv6-acl-name*] [*acl-name* | *acl-number*]

no snmp-server community [**0** | **7** | **secret** [**0** | **8**]] *community-string*

Parameter Description

0: Indicates that the input community string is a plaintext string.

7: Indicates that the input community string is a ciphertext string.

secret [**0** | **8**]: Indicates that the input community string is encrypted. **0** indicates that the input community string is a plaintext string and is encrypted with the default algorithm. **8** indicates that the input community string is a ciphertext string and is encrypted with the SHA256 algorithm. The default encryption algorithm is SHA256.

community-string: Community string. This parameter is case sensitive and does not support special characters or Chinese characters. The maximum length is 32. It is equivalent to the communication password used between the NMS and SNMP agent.

view *view-name*: Specifies a view name for view-based management.

ro: Specifies that the NMS can only read variables of the MIB.

rw: Specifies that the NMS can read and write variables of the MIB.

host *ipv4-address*: Configures IPv4 host address of SNMP.

host *ipv6-address*: Configures IPv6 host address of SNMP.

ipv6 *ipv6-acl-name*: Specifies the name of a list of IPv6 addresses and the range of the addresses that are allowed to access the MIB.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an ACL. The value range of the ACL list of standard IP addresses is from 1 to 99 or from 1300 to 1999. The value range of the ACL list of extended IP addresses is from 100 to 199 or from 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used to enable the SNMP agent function. It specifies community attributes and NMS scope that is allowed to access the MIB.
- Run the **no snmp-server** command to disable the SNMP agent function.

Examples

The following example allows the NMS to access the MIB with the read-only permission using the SNMP community string named public1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server community public1 ro
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 snmp-server contact

Function

Run the **snmp-server contact** command to configure a system contact mode.

Run the **no** form of this command to remove this configuration.

The contact mode of the system is empty by default.

Syntax

snmp-server contact *contact-text*

no snmp-server contact

Parameter Description

contact-text: String that describes the system contact mode. This parameter is case sensitive and does not support Chinese characters. The maximum length is 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the system contact mode to i-net800@i-net.com.cn.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server contact i-net800@i-net.com.cn
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 snmp-server enable secret-dictionary-check

Function

Run the **snmp-server enable secret-dictionary-check** command to configure password dictionary check for communities and users.

Run the **no** form of this command to remove this configuration.

No password dictionary check is configured for communities and users by default.

Syntax

snmp-server enable secret-dictionary-check

no snmp-server enable secret-dictionary-check

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command must be used with the **password policy** command in global configuration mode.

Examples

The following example sets the password length to be no less than six characters and configures password dictionary check for communities.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **password policy min-size** (security/PASSWORD-POLICY)

1.10 snmp-server enable traps

Function

Run the **snmp-server enable traps** command to enable the agent to actively send Trap messages to the NMS.

Run the **no** form of this command to disable this function.

The SNMP agent is forbidden to send Trap messages to the NMS by default.

Syntax

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

no snmp-server enable traps

Parameter Description

notification-type: Type of Trap messages that are actively sent. The following types of Trap messages are supported:

authentication: Enables Trap notification for authentication events.

bgp: Enables Trap notification for Border Gateway Protocol (BGP) events.

bridge: Enables Trap notification for bridge events.

entity: Enables Trap notification for entity events.

isis: Enables Trap notification for intermediate system to intermediate system (ISIS) events.

mac-notification: Enables Trap notification for MAC events.

nfpp: Enables Trap notification for Network Foundation Protection Policy (NFPP) events.

ospf: Enables Trap notification for Open Shortest Path First (OSPF) events.

snmp: Enables Trap notification for SNMP events.

urpf: Enables Trap notification for unicast reverse path forwarding (URPF) events.

vrrp: Enables Trap notification for Virtual Router Redundancy Protocol (VRRP) events.

web-auth: Enables Trap notification for Web authentication events.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command must be used with the **snmp-server host** command so that Trap messages can be sent.
- If no Trap type is specified, all types of Trap messages are sent.

Examples

The following example configures the function of actively sending Trap messages for SNMP events.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server enable traps snmp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- snmp-server host

1.11 snmp-server enable version

Function

Run the **snmp-server enable version** command to configure an SNMP version.

Run the **no** form of this command to disable this version.

All SNMP versions are enabled by default.

Syntax

snmp-server enable version { **v1** | **v2c** | **v3** }

no snmp-server enable version { **v1** | **v2c** | **v3** }

Parameter Description

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

v3: Uses SNMPv3.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the SNMPv1 function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server enable version v1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 snmp-server flow-control pps

Function

Run the **snmp-server flow-control pps** command to configure SNMP traffic control.

Run the **no** form of this command to restore the default configuration.

About 300 SNMP request packets are processed every second by default.

Syntax

snmp-server flow-control pps *packet-count*

no snmp-server flow-control pps

Parameter Description

packet-count: Number of SNMP request packets processed per second. The value range is from 50 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the number of SNMP request packets processed per second to 200.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server flow-control pps 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 snmp-server group

Function

Run the **snmp-server group** command to configure an SNMP user group.

Run the **no** form of this command to remove this configuration.

No user group is configured by default.

Syntax

snmp-server group *group-name* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { [**ipv6** *ipv6-acl-name*] *acl-name* | *acl-number* }]

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

Parameter Description

group-name: Name of a user group.

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

v3: Uses SNMPv3.

auth | **noauth** | **priv**: Configures the security level of SNMPv3 users. **auth** indicates that the messages transmitted by users in this group need authentication but the data does not need encryption. **noauth** indicates that the messages transmitted by users in this group do not need authentication and the data does not need encryption. This security level is valid for SNMPv3 only. **priv** indicates that the messages transmitted by users in this group need authentication and the data needs encryption. This security level is valid for SNMPv3 only.

read *readview*: Associates a read-only view.

write *writeview*: Associates a read/write view.

ipv6 *ipv6-acl-name*: Specifies the name of a list of IPv6 addresses and the range of the addresses that are allowed to access the MIB.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an ACL. The value range of the ACL list of standard IP addresses is from 1 to 99 or from 1300 to 1999. The value range of the ACL list of extended IP addresses is from 100 to 199 or from 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a user group with the name mib2user.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server group mib2user v3 priv read mib2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 snmp-server host

Function

Run the **snmp-server host** command to configure NMS host addresses for the agent to send messages.

Run the **no** form of this command to remove this configuration.

No SNMP host address is configured by default.

Syntax

snmp-server host [**oob**] { *ipv4-addrress* | **ipv6** *ipv6-address*

| **domain** *domain-name*

} [**vrf** *vrf-name*] [**informs** | **traps**] [**version** { { **1** | **2c** } [**0** | **7**] *community* | **3** { **auth** | **noauth** | **priv** } *username* }] [**udp-port** *port-number*] [**via** *mgmt-name*] [*notification-type*]

no snmp-server host [**oob**] { *ipv4-address* | **ipv6** *ipv6-address*

| **domain** *domain-name*

} [**vrf** *vrf-name*] [**informs** | **traps**] [**version** { { **1** | **2c** } [**0** | **7**] *community* | **3** { **auth** | **noauth** | **priv** } *username* }] [**udp-port** *port-numer*] [**via** *mgmt-name*]

Parameter Description

oob: Specifies out-of-band communication for the alarm server (sending logs to the alarm server through the management interface).

ipv4-address: IPv4 address of the SNMP host.

ipv6 *ipv6-address*: Specifies the IPv6 address of the SNMP host.

domain *domain-name*: Domain name of the SNMP host.

vrf *vrf-name*: Configures the name of the VRF forwarding table.

informs: Configures the host to send Inform messages.

traps: Configures the host to send Trap messages.

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

0: Indicates that the input community string is a plaintext string.

7: Indicates that the input community string is a ciphertext string.

community: Community string.

v3: Uses SNMPv3.

auth | **noauth** | **priv**: Configures the security level of SNMPv3 users. **auth** indicates that the messages transmitted by users in this group need authentication but the data does not need encryption. **noauth** indicates that the messages transmitted by users in this group do not need authentication and the data does not need encryption. This security level is valid for SNMPv3 only. **priv** indicates that the messages transmitted by users in this group need authentication and the data needs encryption. This security level is valid for SNMPv3 only.

username: Username used in SNMPv3 configuration.

udp-port *port-number*: Configures the port ID of the SNMP host. The value range is from 0 to 65535.

via *mgmt-name*: Specifies a management port when OOB is configured. *mgmt-name* indicates the name of the management port.

notification-type: Type of Trap packets, for example, SNMP.

Note

Parameter **0** is not supported if SNMPv3 is used.

Parameter **7** is not supported if SNMPv3 is used.

If no Trap type is specified for the *notification-type* parameter, all types of Trap messages are sent.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used with the **snmp-server enable traps** command to actively send Trap messages to the NMS.
- Multiple SNMP hosts can be configured to receive Trap messages. A host can combine different types of Trap messages, ports, and VRF forwarding tables. If a host is configured with the same port and VRF in multiple configurations, the last configuration is combined with the previous configurations. To send different Trap messages to the same host, configure different types of Trap messages each time. These configurations are finally combined.
- Note: The **via** parameter can be specified only when **oob** is enabled in the command. In this case, the VRF parameter is unavailable.

Examples

The following example sets the SNMP host address to 192.168.12.219 and the community name to public1 and receives Trap messages for SNMP events.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server host 192.168.12.219 public1 snmp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- snmp-server enable traps

1.15 snmp-server inform

Function

Run the **snmp-server inform** command to configure Inform message sending attempts and timeout time.

Run the **no** form Inform this command to restore the default configuration.

The number of default Inform message sending attempts is **3** and the default Inform message timeout time is **15** seconds.

Syntax

snmp-server inform { **retries** *retry-number* | **timeout** *timeout* }

no snmp-server inform

Parameter Description

retries *retry-number*: Specifies the number of Inform message sending attempts. The value range is from 0 to 255.

timeout *timeout*: Specifies the Inform message timeout time, in seconds. The value range is from 0 to 21474836.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the number of Inform message sending attempts to 5 and Inform message timeout time to 20 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server inform retries 5
Hostname(config)# snmp-server inform timeout 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 snmp-server location

Function

Run the **snmp-server location** command to configure a system location.

Run the **no** form of this command to remove this configuration.

The system location is empty by default.

Syntax

snmp-server location *location-text*

no snmp-server location

Parameter Description

location-text: String that describes the system information. This parameter is case sensitive and does not support Chinese characters. The maximum length is 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the system location as snmp-server location start-technology-city 4F of A Building.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server location start-technology-city 4F of A Building
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 snmp-server logging

Function

Run the **snmp-server logging** command to enable the SNMP logging function.

Run the **no** form of this command to disable this function.

By default, the SNMP logging function is disabled.

Syntax

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

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

Parameter Description

get-operation: Enables the Get and Get-Next operation logging function.

set-operation: Enables the Set operation logging function.

trap-info: Enables the Trap message logging function

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After this command is run, the NMS Get, Get-Next, and Set operations on the SNMP agent are logged. When the Get and Get-Next operations are performed, the agent records the IP address of the NMS user, operation type, and OID of the operation node. When the Set operation is performed, the agent records the IP address of the NMS user, operation type, OID of the operation node, and set value.
- Normally, you are advised to disable the SNMP logging function to avoid large amount of logs from affecting device performance.

Examples

The following example enables the Get operation logging function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server logging get-operation
```

The following example performs Get, Get-Next, and Set operations on the sysname node (.1.3.6.1.2.1.1.5.0) through the NMS and prints the following log information on the console:

```
Hostname#*Feb  7 15:31:16: %SNMP-GET_OPER: NMS source-ip(13.12.11.7)
operation(GET) object(id=1.3.6.1.2.1.1.5.0)
Hostname#*Feb  7 15:32:16:%SNMP-GETN_OPER: NMS source-ip(13.12.11.7)
operation(GET-NEXT) object(id=1.3.6.1.2.1.1.5.0)
Hostname#*Feb  7 15:33:23: %SNMP-SET_OPER: NMS source-ip(13.12.11.7)
operation(SET) object(id=1.3.6.1.2.1.1.5.0, value=Hostname)
```

The following example disables the Get and Set operation logging function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no snmp-server logging get-operation
Hostname(config)# no snmp-server logging set-operation
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 snmp-server net-id

Function

Run the **snmp-server net-id** command to configure NE code information of a device.

Run the **no** form of this command to remove this configuration.

The NE code information of a device is empty by default.

Syntax

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

no snmp-server net-id

Parameter Description

net-id-text: NE code text of a device. The text is a case-sensitive string of 1 to 255 characters. Space is supported.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the NE code of the device as FZ_CDMA_MSC1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server net-id FZ_CDMA_MSC1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 snmp-server packetsize

Function

Run the **snmp-server packetsize** command to configure the maximum packet length of the SNMP agent.

Run the **no** form of this command to restore the default configuration.

The maximum packet length of the SNMP agent is 1,472 bytes by default.

Syntax

snmp-server packetsize *packetsize*

no snmp-server packetsize

Parameter Description

packetsize: Packet size, in bytes. The value range is from 484 to 17876.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the maximum SNMP packet size to 1,492 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server packetsize 1492
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 snmp-server queue-length

Function

Run the **snmp-server queue-length** command to configure the queue of the Trap messages.

Run the **no** form of this command to restore the default configuration.

The default queue length of the Trap messages is **100**.

Syntax

snmp-server queue-length *queue-length*

no snmp-server queue-length

Parameter Description

queue-length: Queue length. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Adjust the size of the message queue to control the message sending speed.

Examples

The following example sets the queue length of Trap messages to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server queue-length 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 snmp-server source-interface

Function

Run the **snmp-server source-interface** command to configure the source port of a device to receive SNMP packets.

Run the **no** form of this command to restore the default configuration.

The source port of a device with a valid IP address is used to receive SNMP packets by default.

Syntax

snmp-server source-interface *interface-type interface-number*

no snmp-server source-interface

Parameter Description

interface-type interface-number: Interface type and interface number of the source port of a device that receives SNMP packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the source port of a device to receive SNMP packets as Mgmt 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server source-interface Mgmt 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 snmp-server system-shutdown

Function

Run the **snmp-server system-shutdown** command to enable the SNMP system reboot notification function.

Run the **no** form of this command to disable this function.

The SNMP system reboot notification function is disabled by default.

Syntax

snmp-server system-shutdown

no snmp-server system-shutdown

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enable the SNMP system reboot notification function. The system sends Trap messages to the NMS to notify system reboot before reboot of the device.

Examples

The following example enables the SNMP system reboot notification function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server system-shutdown
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 snmp-server trap-format private

Function

Run the **snmp-server trap-format private** command to include private fields in SNMP Trap messages.

Run the **no** form of this command to restore the default configuration.

SNMP Trap messages do not include private fields by default.

Syntax

snmp-server trap-format private

no snmp-server trap-format private

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is used to include private fields in Trap messages. The supported private field is the alarm generation time. For the specific data types and data ranges of the fields, see the ORION-TRAP-FORMAT-MIB.mib file.
- When SNMPv1 is used to send Trap messages, this configuration does not take effect.

Examples

The following example includes private fields in SNMP Trap messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server trap-format private
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 snmp-server trap-source

Function

Run the **snmp-server trap-source** command to configure a source address for sending Trap messages.

Run the **no** form of this command to restore the default configuration.

The IP address of the interface that sends SNMP packets is used as the source address by default.

Syntax

snmp-server trap-source *interface-type interface-number*

no snmp-server trap-source

Parameter Description

interface-type interface-number: Interface type and interface number of the source port of a device that sends Trap messages.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

By default, the IP address of an interface that sends SNMP packets is used as the source address of the SNMP packets. To manage and identify the source address, you can run this command to configure a fixed local IP address as the source address of the SNMP packets.

Examples

The following example configures the IP address of GigabitEthernet 0/1 as the source address of Trap messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server trap-source gigabitEthernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 snmp-server trap-timeout

Function

Run the **snmp-server trap-timeout** command to configure the timeout time of Trap message re-sending.

Run the **no** form of this command to restore the default configuration.

The Trap messages are resent with a timeout time of 300 milliseconds by default.

Syntax

snmp-server trap-timeout *trap-timeout-time*

no snmp-server trap-timeout

Parameter Description

trap timeout-time: Timeout time of Trap message re-sending, in 10 milliseconds. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the timeout time of Trap message re-sending to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server trap-timeout 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 snmp-server udp-port

Function

Run the **snmp-server udp-port** command to configure the ID of a port that receives SNMP packets.

Run the **no** form of this command to restore the default configuration.

The default UDP port ID of the SNMP service is **161**.

Syntax

snmp-server udp-port *port-number*

no snmp-server udp-port

Parameter Description

port-number: ID of a port that receives SNMP packets. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the ID of the UDP port that receives SNMP packets to 15000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server udp-port 15000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 snmp-server user

Function

Run the **snmp-server user** command to configure an SNMP user.

Run the **no** form of this command to remove this configuration.

No SNMP user is configured by default.

Syntax

snmp-server user *username group-name* { **v1** | **v2c** | **v3** [**encrypted** | **interactive**] [**auth** { **md5** | **sha** | **sha2-256** | **sha2-512** } *auth-password*] [**priv** { **des56 | acs128** } *priv-password*] } [**access** { [**ipv6** *ipv6-acl-name*] *acl-name* | *acl-number* }]

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

Parameter Description

username: Username.

group-name: Name of the user group to which this user belongs.

v1: Uses SNMPv1.

v2c: Uses SNMPv2c.

v3: Uses SNMPv3.

encrypted: Ciphertext input as the password input mode. Otherwise, plaintext is used for input. If ciphertext input is selected, enter a key consisting of continuous hexadecimal digits. An MD5 authentication key consists of 16 bytes and an SHA authentication key consists of 20 bytes. Two characters stand for one byte. Encrypted keys are valid for this engine only.

interactive: Uses the interactive method to configure the authentication and encrypted password string.

auth { **md5** | **sha** | **sha2-256** | **sha2-512** } *auth-password*: Specifies a protocol used for user authentication when an SNMPv3 user is configured.

md5 indicates that MD5 is used for authentication, **sha** indicates that SHA is used for authentication, **sha2-256** indicates that 256-bit SHA2 is used for authentication, **sha2-512** indicates that 512-bit SHA2 is used for authentication, and *auth-password* indicates a password string that is used for authentication protocol configuration. The value range is from 1 to 32 characters. The system converts the passwords into the corresponding authentication keys.

priv { **des56 | acs128** } *priv-password*: Specifies an encryption protocol when an SNMPv3 user is configured.

des56 indicates that 56-bit DES encryption protocol is used, **acs128** indicates that 128-bit ACS encryption protocol is used, and *priv-password* indicates a password string used for encryption. The value is a string of 1 to 32 characters. The system converts the password into the corresponding encryption key.

ipv6 *ipv6-acl-name*: Associates a specified list of IPv6 addresses and specifies the range of the IPv6 NMS addresses that are allowed to access the MIB.

acl-name: ACL name. The value is a case-sensitive string of 1 to 99 characters.

acl-number: Number of an ACL. The value range of the ACL list of standard IP addresses is from 1 to 99 or from 1300 to 1999. The value range of the ACL list of extended IP addresses is from 100 to 199 or from 2000 to 2699.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example creates an SNMPv3 user user-2 and configures MD5 as an authentication protocol and DES as an encryption protocol.

```
Hostname> enable
Hostname# configure terminal
```

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

The following example creates an SNMPv3 user in interaction mode and configures MD5 as an authentication protocol DES and DES as an encryption protocol.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server user mib2user mib2group v3 interactive auth md5
priv des56
Please configure the authentication password (1-32)
Enter Password:************
Confirm Password:************

Please configure the privacy password (1-32)
Enter Password:**********
Confirm Password:**********
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 snmp-server view

Function

Run the **snmp-server view** command to configure an SNMP view.

Run the **no** form of this command to remove this configuration.

The default view allows access to all MIB objects.

Syntax

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

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

Parameter Description

view-name: View name.

oid-tree: MIB objects associated with a view, which are displayed as an MIB subtree.

exclude: Indicates that the MIB object subtree is not included in the view.

include: Indicates that the MIB object subtree is included in the view.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a view named mib2 and includes all MIB-2 subtrees with OID 1.3.6.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# snmp-server view mib2 1.3.6.1 include
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A