Contents

SNMP commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

The SNMP agent sends notifications (traps and informs) to inform the NMS of significant events, such as link state changes and user logins or logouts. Unless otherwise stated, the **trap** keyword in the command line includes both traps and informs.

display snmp-agent community

Use **display snmp-agent community** to display information about SNMPv1 or SNMPv2c communities.

Syntax

display snmp-agent community [**read** | **write**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

read: Specifies SNMP read-only communities.

write: Specifies SNMP read and write communities.

Usage guidelines

This command is not available in FIPS mode.

If you do not specify the **read** or **write** keyword, this command displays information about all SNMPv1 and SNMPv2c communities.

SNMPv1 and SNMPv2c communities can be created in the following ways:

- Created by using the **snmp-agent community** command.
- Automatically created by the system for SNMPv1 and SNMPv2c users that have been assigned to an existing SNMP group.

This command displays information only about communities created and saved in plaintext form.

Examples

# Display information about all SNMPv1 and SNMPv2c communities.

```
<Sysname> display snmp-agent community
   Community name: aa
       Group name: aa
       ACL:2001
       Storage-type: nonVolatile
       Context name: con1

   Community name: bb
       Role name: bb
       Storage-type: nonVolatile

   Community name: userv1
       Group name: testv1
       Storage-type: nonvolatile
Community name: cc
       Group name: cc
       ACL name: testacl
       Storage-type: nonVolatile
```

Table 1 Command output

Field	Description
Community name	Community name created by using the **snmp-agent community** command or username created by using the **snmp-agent usm-user** { **v1** | **v2c** } command.
Group name	SNMP group name. • If the community is created by using the **snmp-agent community** command in VACM mode, the group name is the same as the community name. • If the community is created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, the name of the group that has the user is displayed.
Role name	User role name for the community. If the community is created by using the **snmp-agent community** command in RBAC mode, a user role can be bound to the community name.
ACL	Number of the ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community.
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community.
IPV6 ACL	Number of the IPv6 ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an ACL is specified for the SNMPv1 or SNMPv2c community.
Storage-type	Storage type: • **volatile**—Settings are lost when the system reboots. • **nonVolatile**—Settings remain after the system reboots. • **permanent**—Settings remain after the system reboots and can be modified but not deleted. • **readOnly**—Settings remain after the system reboots and cannot be modified or deleted. • **other**—Any other storage type.
Context name	SNMP context: • If a mapping between the SNMP community and an SNMP context is configured, the SNMP context is displayed. • If no mapping between the SNMP community and an SNMP context exists, this field is empty.

Related commands

snmp-agent community

snmp-agent usm-user { **v1** | **v2c** }

display snmp-agent context

Use **display snmp-agent context** to display SNMP contexts.

Syntax

display snmp-agent context [*context-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

context-name: Specifies an SNMP context by its name, a case-sensitive string of 1 to 32 characters. If you do not specify this argument, the command displays all SNMP contexts.

Examples

# Display all SNMP contexts.

```
<Sysname> display snmp-agent context
   testcontext
```

Related commands

snmp-agent context

display snmp-agent group

Use **display snmp-agent group** to display information about SNMP groups.

Syntax

display snmp-agent group [*group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-name: Specifies an SNMPv1, SNMPv2c, or SNMPv3 group name in non-FIPS mode, and an SNMPv3 group name in FIPS mode. It is a case-sensitive string of 1 to 32 characters. If you do not specify a group, this command displays information about all SNMP groups.

Examples

# Display information about all SNMP groups.

```
<Sysname> display snmp-agent group
   Group name: groupv3
```

```
Security model: v3 noAuthnoPriv
Readview: ViewDefault
Writeview: <no specified>
Notifyview: <no specified>
Storage-type: nonvolatile
 ACL name: testacl
```

Table 2 Command output

Field	Description
Group name	SNMP group name.
Security model	Security model of the SNMP group: • **authPriv**—Authentication with privacy. • **authNoPriv**—Authentication without privacy. • **noAuthNoPriv**—No authentication, no privacy. Security model of an SNMPv1 or SNMPv2c group can only be noAuthNoPriv.
Readview	Read-only MIB view accessible to the SNMP group.
Writeview	Write MIB view accessible to the SNMP group.
Notifyview	Notify MIB view for the SNMP group. The SNMP users in the group can send notifications only for the nodes in the notify MIB view.
Storage-type	Storage type, including **volatile**, **nonvolatile**, **permanent**, **readOnly**, and **other**. For more information, see Table 1.
ACL	Number of the IPv4 ACL. This field appears only when an IPv4 ACL is specified for the SNMP group.
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMP group.
IPv6 ACL	Number of the IPv6 ACL. This field appears only when an IPv6 ACL is specified for the SNMP group.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an IPv6 ACL is specified for the SNMP group.

Related commands

snmp-agent group

display snmp-agent local-engineid

Use **display snmp-agent local-engineid** to display the local SNMP engine ID.

Syntax

display snmp-agent local-engineid

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Every SNMP entity has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP domain.

Examples

# Display the local SNMP engine ID.

```
<Sysname> display snmp-agent local-engineid
   SNMP local engine ID: 800063A2800084E52BED7900000001
```

Related commands

snmp-agent local-engineid

display snmp-agent mib-node

Use **display snmp-agent mib-node** to display SNMP MIB node information.

Syntax

display snmp-agent mib-node [**details** | **index-node** | **trap-node** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

details: Specifies detailed MIB node information, including node name, last octet of an OID string, and name of the next leaf node.

index-node: Specifies SNMP MIB tables, and node names and OIDs of MIB index nodes.

trap-node: Specifies node names and OIDs of MIB notification nodes, and node names and OIDs of notification objects.

verbose: Specifies detailed information about SNMP MIB nodes, including node names, OIDs, node types, permissions to MIB nodes, data types, MORs, and parent, child, and sibling nodes.

Usage guidelines

If you do not specify any keywords, this command displays information about all SNMP MIB nodes, including node name, OID, and permissions to MIB nodes.

The SNMP software package includes different MIB files. Support for MIBs varies by SNMP software versions.

Examples

# Display SNMP MIB node information.

```
<Sysname> display snmp-agent mib-node

iso<1>(NA)
  |-std<1.0>(NA)
   |-iso8802<1.0.8802>(NA)
    |-ieee802dot1<1.0.8802.1>(NA)
     |-ieee802dot1mibs<1.0.8802.1.1>(NA)
```

```
      ...
```

Table 3 Command output

Field	Description
-std	MIB node name
<1.0>	MIB node OID
(NA)	Access right to the MIB node: • **NA**—Not accessible • **NF**—Notifications • **RO**—Read-only access • **RW**—Read and write access • **RC**—Read-write-create access • **WO**—Write-only access
*	Leaf node or MIB table node

# Display detailed MIB node information.

```
<Sysname> display snmp-agent mib-node details

 iso(1)(dot1xPaeSystemAuthControl)
  |-std(0)(dot1xPaeSystemAuthControl)
   |-iso8802(8802)(dot1xPaeSystemAuthControl)
    |-ieee802dot1(1)(dot1xPaeSystemAuthControl)
     |-ieee802dot1mibs(1)(dot1xPaeSystemAuthControl)
      ...
```

Table 4 Command output

Field	Description
-std	MIB node name
(0)	Last bit of the MIB OID string
(lldpMessageTxInterval)	Name of the leaf node
*	Leaf node or MIB table node

# Display MIB table names, and node names and OIDs of MIB index nodes.

```
<Sysname> display snmp-agent mib-node index-node

Table          |dot1xPaePortTable
Index          ||dot1xPaePortNumber
OID            |||  1.0.8802.1.1.1.1.1.2.1.1
...
```

Table 5 Command output

Field	Description
Table	MIB table name
Index	MIB index node name
OID	MIB index node OID

# Display names and OIDs of MIB notification nodes, and names and OIDs of notification objects.

```
<Sysname> display snmp-agent mib-node trap-node


Name          |lldpRemTablesChange
OID           ||1.0.8802.1.1.2.0.0.1
Trap Object
Name          |||lldpStatsRemTablesInserts
OID           ||||1.0.8802.1.1.2.1.2.2
Name          |||lldpStatsRemTablesDeletes
OID           ||||1.0.8802.1.1.2.1.2.3
Name          |||lldpStatsRemTablesDrops
OID           ||||1.0.8802.1.1.2.1.2.4
Name          |||lldpStatsRemTablesAgeouts
OID           ||||1.0.8802.1.1.2.1.2.5
...
```

Table 6 Command output

Field	Description
Name	MIB notification node name
OID	MIB notification node OID
Trap Object	Name and OID of a notification object

# Display detailed information about SNMP MIB nodes, including node names, OIDs, node types, permissions to MIB nodes, data types, MORs, and parent, child, and sibling nodes.

```
<Sysname> display snmp-agent mib-node verbose


Name          |iso
OID           ||1
Properties    ||NodeType:   Other
              ||AccessType: NA
              ||DataType:   NA
              ||MOR:        0x00000000
Parent        ||
First child   ||std
Next leaf     ||dot1xPaeSystemAuthControl
Next sibling  ||
...
```

Table 7 Command output

Field	Description
Name	MIB node name.
OID	MIB node OID.
Properties	MIB node properties.
NodeType	MIB node type:

Field	Description
	• **Table**—Table node. • **Row**—Row node in a MIB table. • **Column**—Column node in a MIB table. • **Leaf**—Leaf node. • **Group**—Group node (parent node of a leaf node). • **Trapnode**—Notification node. • **Other**—Other node type.
AccessType	Access right to the MIB node: • **NA**—Not accessible. • **NF**—Supports notifications. • **RO**—Supports read-only access. • **RW**—Supports read and write access. • **RC**—Supports read-write-create access. • **WO**—Supports write-only access.
DataType	Data type of the MIB node: • **Integer**—An integer. • **Integer32**—A 32-bit integer. • **Unsigned32**—A 32-bit integer with no mathematical sign. • **Gauge**—A non-negative integer that might increase or decrease. • **Gauge32**—A 32-bit non-negative integer that might increase or decrease. • **Counter**—A non-negative integer that might increase but not decrease. • **Counter32**—A 32-bit non-negative integer that might increase but not decrease. • **Counter64**—A 64-bit non-negative integer that might increase but not decrease. • **Timeticks**—A non-negative integer for time keeping. • **Octstring**—An octal string. • **OID**—Object identifier. • **IPaddress**—A 32-bit IP address. • **Networkaddress**—A network IP address. • **Opaque**—Any data. • **Userdefined**—User-defined data. • **BITS**—Bit enumeration. • **NA**—Other data type.
MOR	MOR for the MIB node.
Parent	Name of the parent node.
First child	Name of the first leaf node.
Next leaf	Name of the next leaf node.
Next sibling	Name of the next sibling node.
Allow	Operation types allowed: • **get/set/getnext**—All operations. • **get**—Get operation. • **set**—Set operation. • **getnext**—GetNext operation.
Value range	Value range of the MIB node.
Index	Table index. This field appears only for a table node.

display snmp-agent mib-view

Use **display snmp-agent mib-view** to display MIB views.

Syntax

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

exclude: Displays the subtrees excluded from any MIB view.

include: Displays the subtrees included in any MIB view.

viewname *view-name*: Displays information about the specified MIB view. The *view-name* argument is a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify any parameters, this command displays all MIB views.

Examples

# Display all MIB views.

```
<Sysname> display snmp-agent mib-view
   View name: ViewDefault
       MIB Subtree: iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type: included
       View status: active

   View name: ViewDefault
       MIB Subtree: snmpUsmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type: excluded
       View status: active

   View name: ViewDefault
       MIB Subtree: snmpVacmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type: excluded
       View status: active

   View name: ViewDefault
       MIB Subtree: snmpModules.18
       Subtree mask:
```

```
Storage-type: nonVolatile
View Type: excluded
View status: active
```

ViewDefault is the default MIB view. The output shows that except for the MIB objects in the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees, all the MIB objects in the **iso** subtree are accessible.

Table 8 Command output

Field	Description
View name	MIB view name.
MIB Subtree	MIB subtree covered by the MIB view.
Subtree mask	MIB subtree mask.
Storage-type	Type of the medium (see Table 1) where the subtree view is stored.
View Type	Access privilege for the MIB subtree in the MIB view: • **Included**—All objects in the MIB subtree are accessible in the MIB view. • **Excluded**—None of the objects in the MIB subtree is accessible in the MIB view.
View status	Status of the MIB view: • **active**—MIB view is effective. • **inactive**—MIB view is ineffective. The objects in the MIB view are not accessible, but they can send notifications.

Related commands

snmp-agent mib-view

display snmp-agent remote

Use **display snmp-agent remote** to display engine IDs of the remote SNMP entities.

Syntax

display snmp-agent remote [{ *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv4-address: Specifies a remote SNMP entity by its IPv4 address.

ipv6 *ipv6-address*: Specifies a remote SNMP entity by its IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the remote SNMP entity belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the remote SNMP entity belongs to the public network, do not specify this option.

Usage guidelines

Every SNMP entity has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP domain.

If you do not specify a remote SNMP entity, this command displays the engine IDs of all remote SNMP entities.

Examples

# Display engine IDs of all remote SNMP entities.

```
<Sysname> display snmp-agent remote
   Remote engineID: 800063A28000A0FC00580400000001
       IPv4 address: 1.1.1.1
       VPN instance: vpn1
```

Table 9 Command output

Field	Description
Remote engineID	Remote SNMP engine ID you have configured using the **snmp-agent remote** command.
IPv4 address	IPv4 address of the remote SNMP entity.
IPv6 address	IPv6 address of the remote SNMP entity. This field is displayed if the remote SNMP entity is configured with an IPv6 address.
VPN instance	This field is available only if a VPN instance has been specified for the remote SNMP entity in the **snmp-agent remote** command.

Related commands

snmp-agent remote

display snmp-agent statistics

Use **display snmp-agent statistics** to display SNMP message statistics.

Syntax

display snmp-agent statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

# Display SNMP message statistics.

```
<Sysname> display snmp-agent statistics
  1684 messages delivered to the SNMP entity.
  5 messages were for an unsupported version.
  0 messages used an unknown SNMP community name.
  0 messages represented an illegal operation for the community supplied.
  0 ASN.1 or BER errors in the process of decoding.
```

```
1679 messages passed from the SNMP entity.
0 SNMP PDUs had badValue error-status.
0 SNMP PDUs had genErr error-status.
0 SNMP PDUs had noSuchName error-status.
0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
16544 MIB objects retrieved successfully.
2 MIB objects altered successfully.
7 GetRequest-PDU accepted and processed.
7 GetNextRequest-PDU accepted and processed.
1653 GetBulkRequest-PDU accepted and processed.
1669 GetResponse-PDU accepted and processed.
2 SetRequest-PDU accepted and processed.
0 Trap PDUs accepted and processed.
0 alternate Response Class PDUs dropped silently.
0 forwarded Confirmed Class PDUs dropped silently.
```

Table 10 Command output

Field	Description
messages delivered to the SNMP entity	Number of messages that the SNMP agent has received.
messages were for an unsupported version	Number of messages that are not supported by the SNMP agent version.
messages used an unknown SNMP community name	Number of messages that used an unknown SNMP community name.
messages represented an illegal operation for the community supplied	Number of messages carrying an operation that the community has no right to perform.
ASN.1 or BER errors in the process of decoding	Number of messages that had ASN.1 or BER errors during decoding.
messages passed from the SNMP entity	Number of messages sent by the SNMP agent.
SNMP PDUs had badValue error-status	Number of PDUs with a BadValue error.
SNMP PDUs had genErr error-status	Number of PDUs with a genErr error.
SNMP PDUs had noSuchName error-status	Number of PDUs with a NoSuchName error.
SNMP PDUs had tooBig error-status	Number of PDUs with a TooBig error (the maximum packet size is 1500 bytes).
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved.
MIB objects altered successfully	Number of MIB objects that have been successfully modified.
GetRequest-PDU accepted and processed	Number of GetRequest requests that have been received and processed.
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed.
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed.
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed.
SetRequest-PDU accepted and processed	Number of set requests that have been received

Field	Description
	and processed.
Trap PDUs accepted and processed	Number of notifications that have been received and processed.
alternate Response Class PDUs dropped silently	Number of dropped response packets.
forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped.

display snmp-agent sys-info

Use **display snmp-agent sys-info** to display SNMP agent system information.

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

contact: Displays the system contact.

location: Displays the physical location of the device.

version: Displays the SNMP agent version.

Usage guidelines

If you do not specify any keywords, this command displays all SNMP agent system information.

Examples

# Display all SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
   The contact information of the agent:
       New H3C Technologies Co., Ltd.

   The location information of the agent:
       Hangzhou, China

   The SNMP version of the agent:
       SNMPv3
```

Related commands

snmp-agent sys-info

display snmp-agent trap queue

Use **display snmp-agent trap queue** to display basic information about the trap queue.

Syntax

display snmp-agent trap queue

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

# Display the trap queue configuration and usage status.

```
<Sysname> display snmp-agent trap queue
   Queue size: 100
   Message number: 6
```

Related commands

snmp-agent trap life

snmp-agent trap queue-size

display snmp-agent trap-list

Use **display snmp-agent trap-list** to display SNMP notifications enabling status for modules.

Syntax

display snmp-agent trap-list

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

If a module has multiple sub-modules and SNMP notifications are enabled for one of its sub-modules, the command output shows that the module is SNMP notifications-enabled.

To determine whether a module supports SNMP notifications, execute the **snmp-agent trap enable ?** command.

The **display snmp-agent trap-list** command output varies by the **snmp-agent trap enable** command configuration and the module configuration.

Examples

# Display SNMP notifications enabling status for modules.

```
<Sysname> display snmp-agent trap-list
   arp notification is disabled.
   configuration notification is enabled.
   mac-address notification is enabled.
   radius notification is disabled.
   standard notification is enabled.
   syslog notification is disabled.
   system notification is enabled.

   Enabled notifications: 4; Disabled notifications: 3
```

Related commands

snmp-agent trap enable

display snmp-agent usm-user

Use **display snmp-agent usm-user** to display SNMPv3 user information.

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

engineid *engineid*: Specifies an SNMP engine ID. The engine ID is case insensitive. When an SNMPv3 user is created, the system records the local SNMP entity engine ID. The user becomes invalid when the engine ID changes, and it becomes valid again when the recorded engine ID is restored.

group *group-name*: Specifies an SNMP group by its name. The group name is case sensitive.

username *user-name*: Specifies an SNMPv3 user by its name. The username is case sensitive.

Usage guidelines

This command displays only SNMPv3 users that you have created by using the **snmp-agent usm-user v3** command. To display SNMPv1 or SNMPv2c users created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, use the **display snmp-agent community** command.

Examples

# Display information about all SNMPv3 users.

```
<Sysname> display snmp-agent usm-user
   Username: userv3
   Group name: mygroupv3
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active
       ACL: 2000

   Username: userv3
   Group name: mygroupv3
       Engine ID: 8000259503000BB3100A508
       Storage-type: nonVolatile
       UserStatus: active
```

```
    ACL name: testacl

Username: userv3code
Role name: groupv3code
           network-operator
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active

Username: userv3code
Role name: snmprole
           network-operator
    Engine ID: 800063A280000002BB0001
    Storage-type: nonVolatile
    UserStatus: active
```

Table 11 Command output

Field	Description
Username	SNMP username.
Group name	SNMP group name.
Role name	SNMP user role name.
Engine ID	Engine ID that the SNMP agent used when the SNMP user was created.
Storage-type	Storage type: • **volatile**. • **nonvolatile**. • **permanent**. • **readOnly**. • **other**. For more information about these storage types, see Table 1.
UserStatus	SNMP user status: • **active**—The SNMP user is effective. • **notInService**—The SNMP user is correctly configured but not activated. • **notReady**—The SNMP user configuration is incomplete. • **other**—Any other status.
ACL	Number of the ACL. This field appears only when an ACL is specified for the SNMPv3 user.
ACL name	Name of the ACL. This field appears only when an ACL is specified for the SNMPv3 user.
IPV6 ACL	Number of the IPv6 ACL. This field appears only when an ACL is specified for the SNMPv3 user.
IPV6 ACL name	Name of the IPv6 ACL. This field appears only when an ACL is specified for the SNMPv3 user.

Related commands

snmp-agent usm-user v3

enable snmp trap updown

Use **enable snmp trap updown** to enable link state notifications on an interface.

Use **undo enable snmp trap updown** to disable link state notifications on an interface.

Syntax

enable snmp trap updown

undo enable snmp trap updown

Default

Link state notifications are enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

For an interface to generate linkUp/linkDown notifications when its state changes, you must also enable the linkUp/linkDown notification function globally by using the **snmp-agent trap enable standard** [**linkdown** | **linkup**] * command.

Examples

# Enable Ten-GigabitEthernet 1/0/1 to send linkUp/linkDown SNMP traps to 10.1.1.1 in the community **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] enable snmp trap updown
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent

Use **snmp-agent** to enable the SNMP agent.

Use **undo snmp-agent** to disable the SNMP agent.

Syntax

snmp-agent

undo snmp-agent

Default

The SNMP agent is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The SNMP agent is automatically enabled when you execute any command that begins with **snmp-agent** except for the **snmp-agent calculate-password** command.

The SNMP agent will fail to be enabled when the port that the agent will listen on is used by another service. You can use the **snmp-agent port** command to specify a listening port. To view the UDP port use information, execute the **display udp verbose** command.

If you disable the SNMP agent, the SNMP settings do not take effect. The **display current-configuration** command does not display the SNMP settings. The SNMP settings will not be saved in the configuration file. For the SNMP settings to take effect, enable the SNMP agent.

Examples

# Enable the SNMP agent.

```
<Sysname> system-view
[Sysname] snmp-agent
```

Related commands

display udp verbose (see IP performance optimization commands in *Layer 3—IP Services Configuration Guide*)

snmp-agent port

snmp-agent { inform | trap } source

Use **snmp-agent** { **inform** | **trap** } **source** to specify a source IP address for the informs or traps sent by the SNMP agent.

Use **undo snmp-agent** { **inform** | **trap** } **source** to restore the default.

Syntax

snmp-agent { **inform** | **trap** } **source** *interface-type* { *interface-number* | *interface-number*.*subnumber* }

undo snmp-agent { **inform** | **trap** } **source**

Default

The SNMP agent uses the IP address of the outgoing interface as the source IP address of notifications.

Views

System view

Predefined user roles

network-admin

Parameters

inform: Specifies informs.

trap: Specifies traps.

interface-type { *interface-number* | *interface-number.subnumber* }: Specifies an interface by its type and number. The *interface-number* argument specifies a main interface number. The *subnumber* argument specifies a subinterface number in the range of 1 to 4094.

Usage guidelines

The **snmp-agent source** command enables the SNMP agent to use the primary IP address of an interface or subinterface as the source IP address in all its SNMP informs or traps, regardless of their outgoing interfaces. An NMS can use this IP address to filter all the informs or traps sent by the SNMP agent.

Make sure the specified interface has been created and assigned a valid IP address. The configuration will fail if the interface has not been created and will take effect only after a valid IP address is assigned to the specified interface.

Examples

# Configure the primary IP address of Ten-GigabitEthernet 1/0/1 as the source address of SNMP traps.

```
<Sysname> system-view
[Sysname] snmp-agent trap source ten-gigabitethernet 1/0/1
```

# Configure the primary IP address of Ten-GigabitEthernet 1/0/2 as the source address of SNMP informs.

```
<Sysname> system-view
[Sysname] snmp-agent inform source ten-gigabitethernet 1/0/2
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent calculate-password

Use **snmp-agent calculate-password** to calculate the encrypted form for a key in plaintext form.

Syntax

In non-FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **aes192md5** | **aes192sha** | **aes256md5** | **aes256sha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

In FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **aes192sha** | **aes256sha** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

Views

System view

Predefined user roles

network-admin

Parameters

plain-password: Specifies a key in plaintext form. The *plain-password* argument is a case-sensitive string of 1 to 64 characters.

mode: Specifies an authentication algorithm and encryption algorithm. The device supports the HMAC-MD5 and HMAC-SHA1 authentication algorithms. The HMAC-MD5 algorithm is faster than the HMAC-SHA1 algorithm. The HMAC-SHA1 algorithm provides more security than the HMAC-MD5 algorithm. The AES256, AES192, AES, 3DES, and DES encryption algorithms (in descending order of security strength) are available for the device. A more secure algorithm calculates slower. DES is enough to meet general security requirements.

- **3desmd5**: Calculates the encrypted form for the encryption key by using the 3DES encryption algorithm and HMAC-MD5 authentication algorithm.
- **3dessha**: Calculates the encrypted form for the encryption key by using the 3DES encryption algorithm and HMAC-SHA1 authentication algorithm.
- **aes192md5**: Calculates the encrypted form for the encryption key by using the AES192 encryption algorithm and the HMAC-MD5 authentication algorithm.
- **aes192sha**: Calculates the encrypted form for the encryption key by using the AES192 encryption algorithm and the HMAC-SHA1 authentication algorithm.
- **aes256md5**: Calculates the encrypted form for the encryption key by using the AES256 encryption algorithm and the HMAC-MD5 authentication algorithm.
- **aes256 sha**: Calculates the encrypted form for the encryption key by using the AES256 encryption algorithm and the HMAC-SHA1 authentication algorithm.
- **md5**: Calculates the encrypted form for the authentication key or encryption key by using the HMAC-MD5 authentication algorithm and AES or DES encryption algorithm. When the HMAC-MD5 authentication algorithm is used, you can get the same authentication key or encryption key in encrypted form regardless of whether the AES or DES encryption algorithm is used.
- **sha**: Calculates the encrypted form for the authentication key or encryption key by using HMAC-SHA1 authentication algorithm and AES or DES encryption algorithm. When the HMAC-SHA1 authentication algorithm is used, you can get the same authentication key or encryption key in encrypted form regardless of whether the AES or DES encryption algorithm is used.

local-engineid: Uses the local engine ID to calculate the encrypted form for the key. You can configure the local engine ID by using the **snmp-agent local-engineid** command.

specified-engineid *engineid*: Uses a user-defined engine ID to calculate the encrypted form for the key. The *engineid* argument is an even number of case-insensitive hexadecimal characters. All-zero and all-F strings are invalid. The even number is in the range of 10 to 64.

Usage guidelines

Make sure the SNMP agent is enabled before you execute the **snmp-agent calculate-password** command.

For security purposes, use the encrypted-form key generated by using this command when you create SNMPv3 users by specifying the **cipher** keyword in the **snmp-agent usm-user v3** command.

The encrypted form of the key is valid only under the engine ID specified for key conversion.

Examples

# Use the local engine ID and the HMAC-SHA1 algorithm to calculate the encrypted form for key **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode sha local-engineid
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

Related commands

snmp-agent local-engineid

snmp-agent usm-user v3

snmp-agent community

Use **snmp-agent community** to configure an SNMPv1 or SNMPv2c community.

Use **undo snmp-agent community** to delete an SNMPv1 or SNMPv2c community.

Syntax

In VACM mode:

snmp-agent community { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

In RBAC mode:

snmp-agent community [**simple** | **cipher**] *community-name* **user-role** *role-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

Default

No SNMPv1 or SNMPv2c communities exist.

Views

System view

Predefined user roles

network-admin

Parameters

read: Assigns the specified community read-only access to MIB objects. A read-only community can only inquire MIB information.

write: Assigns the specified community read and write access to MIB objects. A read and write community can configure MIB information.

simple: Specifies a community name in plaintext form. For security purposes, the community name specified in plaintext form will be stored in encrypted form.

cipher: Specifies a community name in encrypted form.

community-name: Specifies the community name. The plaintext form is a case-sensitive string of 1 to 32 characters. The encrypted form is a case-sensitive string of 33 to 73 characters. Input a string as escape characters after a backslash (\).

mib-view *view-name*: Specifies the MIB view available for the community. The *view-name* argument represents a MIB view name, a case-sensitive string of 1 to 32 characters. A MIB view represents a set of accessible MIB objects. If you do not specify a view, the specified community can access the MIB objects in the default MIB view **ViewDefault**.

user-role *role-name*: Specifies a user role name for the community, a case-sensitive string of 1 to 63 characters.

acl: Specifies a basic or advanced IPv4 ACL for the community.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the community.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command is not available in FIPS mode.

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

An SNMP community is identified by a community name. It contains a set of NMSs and SNMP agents. Devices in an SNMP community authenticate each other by using the community name. An NMS and an SNMP agent can communicate only when they use the same community name.

Typically, **public** is used as the read-only community name and **private** is used as the read and write community name. To enhance security, you can assign your SNMP communities a name other than **public** and **private**.

The **snmp-agent community** command allows you to use either of the following modes to control SNMP community access to MIB objects:

- **View-based access control model**—The VACM mode controls access to MIB objects by assigning MIB views to SNMP communities.
- **Role based access control**—The RBAC mode controls access to MIB objects by assigning user roles to SNMP communities.
  -
  - The network-admin and level-15 user roles have the read and write access to all MIB objects.
  - The network-operator user role has the read-only access to all MIB objects.

  For more information about user roles, see *Fundamentals Configuration Guide*.

RBAC mode controls access on a per MIB object basis, and VACM mode controls access on a MIB view basis. As a best practice to enhance MIB security, use RBAC mode.

You can create a maximum of 10 SNMP communities by using the **snmp-agent community** command.

If you execute the command multiple times to specify the same community name but different other settings each time, the most recent configuration takes effect.

To set and save a community name in plain text, do not specify the **simple** or **cipher** keyword.

The ACL is used to filter illegitimate NMSs.

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the community name can access the SNMP agent.
- If you specify an ACL and the ACL has rules, only NMSs permitted by the ACL can access the SNMP agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

You can also create an SNMP community by using the **snmp-agent usm-user** { **v1** | **v2c** } and **snmp-agent group** { **v1** | **v2c** } commands. These two commands create an SNMPv1 or SNMPv2c user and the group to which the user is assigned. The system automatically creates an SNMP community by using the SNMPv1 or SNMPv2c username.

The **display snmp-agent community** command displays information only about communities created and saved in plaintext form.

Examples

# Create the read-only community with the plaintext form name **readaccess** so an SNMPv1 or SNMPv2c NMS can use the community name **readaccess** to read the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read simple readaccess
```

# Create the read and write community with the plaintext form name **writeaccess** so only the SNMPv2c NMS at 1.1.1.1 can use the community name **writeaccess** to read or set the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl 2001
```

# Create the read and write community with the plaintext form name **writeaccess** so only the SNMPv2c NMS at 1.1.1.2 can use the community name **writeaccess** to read or set the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl name testacl
```

# Create the read and write community with the plaintext form name **wr-sys-acc** so an SNMPv1 or SNMPv2c NMS can use the community name **wr-sys-acc** to read or set the MIB objects in the system subtree (OID 1.3.6.1.2.1.1).

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] undo snmp-agent mib-view ViewDefault
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write simple wr-sys-acc mib-view test
```

Related commands

display snmp-agent community

snmp-agent mib-view

snmp-agent community-map

Use **snmp-agent community-map** to map an SNMP community to an SNMP context.

Use **undo snmp-agent community-map** to delete the mapping between an SNMP community and an SNMP context.

Syntax

snmp-agent community-map *community-name* **context** *context-name*

undo snmp-agent community-map *community-name* **context** *context-name*

Default

No mapping exists between an SNMP community and an SNMP context.

Views

System view

Predefined user roles

network-admin

Parameters

community-name: Specifies an SNMP community, a case-sensitive string of 1 to 32 characters.

context-name: Specifies an SNMP context, a case-sensitive string of 1 to 32 characters.

Usage guidelines

This command enables a module on an agent to obtain the context mapped to a community name when an NMS accesses the agent by using SNMPv1 or SNMPv2c.

You can configure a maximum of 10 community-context mappings on the device.

Examples

# Map SNMP community **private** to SNMP context **trillcontext**.

```
<Sysname> system-view
[Sysname] snmp-agent community-map private context testcontext
```

Related commands

display snmp-agent community

snmp-agent context

Use **snmp-agent context** to create an SNMP context.

Use **undo snmp-agent context** to delete an SNMP context.

Syntax

snmp-agent context *context-name*

undo snmp-agent context *context-name*

Default

No SNMP contexts exist.

Views

System view

Predefined use roles

network-admin

Parameters

context-name: Specifies an SNMP context, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For an NMS and an SNMP agent to communicate, configure the same SNMP context for them or do not configure a context for the NMS.

You can create a maximum of 20 SNMP contexts.

Examples

# Create SNMP context **trillcontext**.

```
<Sysname> system-view
[Sysname] snmp-agent context testcontext
```

Related commands

display snmp-agent context

snmp-agent group

Use **snmp-agent group** to create an SNMP group.

Use **undo snmp-agent group** to delete an SNMP group.

Syntax

In non-FIPS mode:

- SNMPv1 and SNMP v2c:

  snmp-agent group { **v1** | **v2c** } *group-name* [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent group { **v1** | **v2c** } *group-name*

- SNMPv3:

  snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

In FIPS mode:

snmp-agent group v3 *group-name* { **authentication** | **privacy** } [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent group v3 *group-name* { **authentication** | **privacy** }

Default

No SNMP groups exist.

Views

System view

Predefined use roles

network-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

group-name: Specifies an SNMP group name, a case-sensitive string of 1 to 32 characters.

authentication: Specifies the authentication without privacy security model for the SNMPv3 group.

privacy: Specifies the authentication with privacy security model for the SNMPv3 group.

read-view *view-name*: Specifies a read-only MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. If you do not specify a read-only MIB view, the SNMP group has read access to the default view **ViewDefault**.

notify-view *view-name*: Specifies a notify MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. The SNMP agent sends notifications to the users in the specified group only for the MIB objects included in the notify view. If you do not specify a notify view, the SNMP agent does not send any notification to the users in the specified group.

write-view *view-name:* Specifies a read and write MIB view. The *view-name* represents a MIB view name, a case-sensitive string of 1 to 32 characters. If you do not specify a read and write view, the SNMP group cannot set any MIB object on the SNMP agent.

acl: Specifies a basic or advanced IPv4 ACL for the group.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the group.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

SNMPv1 and SNMPv2c settings in this command are not supported in FIPS mode.

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

All users in an SNMP group share the security model and access rights of the group.

You can create a maximum of 20 SNMP groups, including SNMPv1, SNMPv2c, and SNMPv3 groups.

All SNMPv3 users in a group share the same security model, but can use different authentication and encryption key settings. To implement a security model for a user and avoid SNMP communication failures, make sure the security model configuration for the group and the security key settings for the user are compliant with Table 12 and match the settings on the NMS.

Table 12 Basic security setting requirements for different security models

Security model	Security model keyword for the group	Security key settings for the user	Remarks
Authentication with privacy	**privacy**	Authentication key, encryption key	If the authentication key or the encryption key is not configured, SNMP communication will fail.
Authentication without privacy	**authentication**	Authentication key	If no authentication key is configured, SNMP

Security model	Security model keyword for the group	Security key settings for the user	Remarks
			communication will fail. The encryption key (if any) for the user does not take effect.
No authentication, no privacy	Neither **authentication** nor **privacy**	None	The authentication and encryption keys, if configured, do not take effect.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

# Create the SNMPv3 group **group1**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

Related commands

display snmp-agent group

snmp-agent mib-view

snmp-agent usm-user

snmp-agent local-engineid

Use **snmp-agent local-engineid** to set an SNMP engine ID.

Use **undo snmp-agent local-engineid** to restore the default.

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

Default

The engine ID of a device is the combination of the company ID and the device ID.

Views

System view

Predefined user roles

network-admin

Parameters

engineid: Specifies an SNMP engine ID, a case-insensitive hexadecimal string. Its length is an even number in the range of 10 to 64. All-zero and all-F strings are invalid.

Usage guidelines

An SNMP engine ID uniquely identifies a device in an SNMP managed network. Make sure the local SNMP engine ID is unique within your SNMP managed network to avoid communication problems.

If you have configured SNMPv3 users, change the local SNMP engine ID only when necessary. The change can void the SNMPv3 usernames and encrypted keys you have configured.

You can use the default engine ID or configure an easy-to-remember engine ID based on the network plan. For example, you can set the engine ID for device 1 on the first floor of building A to 000Af0010001 and device 2 to 000Af0010002.

Examples

# Set the local SNMP engine ID to **123456789A**.

```
<Sysname> system-view
[Sysname] snmp-agent local-engineid 123456789A
```

Related commands

display snmp-agent local-engineid

snmp-agent usm-user

snmp-agent log

Use **snmp-agent log** to enable SNMP logging.

Use **undo snmp-agent log** to disable SNMP logging.

Syntax

snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

Default

SNMP logging operations are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Enables logging SNMP authentication failures, Get operations, and Set operations.

authfail: Enables logging SNMP authentication failures.

get-operation: Enables logging SNMP Get operations.

set-operation: Enables logging SNMP Set operations.

Usage guidelines

Use SNMP logging to record the SNMP operations performed on the SNMP agent or authentication failures from the NMS to the agent for auditing NMS behaviors. The SNMP agent sends log data to the information center. You can configure the information center to output the data to a destination as needed.

Examples

# Enable logging SNMP Get operations.

```
<Sysname> system-view
[Sysname] snmp-agent log get-operation
```

# Enable logging SNMP Set operations.

```
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

# Enable logging SNMP authentication failures.

```
<Sysname> system-view
[Sysname] snmp-agent log authfail
```

snmp-agent mib-view

Use **snmp-agent mib-view** to create or update a MIB view.

Use **undo snmp-agent mib-view** to delete a MIB view.

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

Default

The system creates the **ViewDefault** view when the SNMP agent is enabled. In this default MIB view, all MIB objects in the **iso** subtree but the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees are accessible.

Views

System view

Predefined user roles

network-admin

Parameters

excluded: Denies access to any node in the specified MIB subtree.

included: Permits access to all the nodes in the specified MIB subtree.

view-name: Specifies a view name, a case-sensitive string of 1 to 32 characters.

oid-tree: Specifies a MIB subtree by its root node's OID (for example, **1.3.6.1.2.1.1**) or object name (for example, **system**). The *oid-tree* argument is a case-sensitive string of 1 to 255 characters. An OID is a dotted numeric string that uniquely identifies an object in the MIB tree.

mask *mask-value*: Sets a MIB subtree mask, a case-insensitive hexadecimal string. Its length is an even number in the range of 1 to 32.

Usage guidelines

A MIB view represents a set of MIB objects (or MIB object hierarchies) with certain access privilege. The MIB objects included in the MIB view are accessible while those excluded from the MIB view are inaccessible.

Each *view-name oid-tree* pair represents a view record. If you specify the same record with different MIB subtree masks multiple times, the most recent configuration takes effect.

Be cautious with deleting the default MIB view. The operation blocks the access to any MIB object on the device from NMSs that use the default view.

Examples

# Include the **mib-2** (OID 1.3.6.1.2.1) subtree in the **mibtest** view and exclude the **system** subtree from this view.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1.2.1
[Sysname] snmp-agent mib-view excluded mibtest system
[Sysname] snmp-agent community read public mib-view mibtest
```

An SNMPv1 NMS in the **public** community can query the objects in the **mib-2** subtree but not any object (for example, the **sysDescr or sysObjectID** node) in the **system** subtree.

Related commands

display snmp-agent mib-view

snmp-agent group

snmp-agent packet max-size

Use **snmp-agent packet max-size** to set the maximum size (in bytes) of SNMP packets that an SNMP agent can receive or send.

Use **undo snmp-agent packet max-size** to restore the default.

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

Default

An SNMP agent can process SNMP packets with a maximum size of 1500 bytes.

Views

System view

Predefined user roles

network-admin

Parameters

byte-count: Sets the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send. The value range is 484 to 17940.

Usage guidelines

If any device on the path to the NMS does not support packet fragmentation, limit the SNMP packet size to prevent large-sized packets from being discarded. For most networks, the default value is sufficient.

Examples

# Set the maximum SNMP packet size to 1024 bytes.

```
<Sysname> system-view
[Sysname] snmp-agent packet max-size 1024
```

snmp-agent packet response dscp

Use **snmp-agent packet response dscp** to set the DSCP value for SNMP responses.

Use **undo snmp-agent packet response dscp** to restore the default.

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

Default

The DSCP value for SNMP responses is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for SNMP responses, in the range of 0 to 63. A greater DSCP value represents a higher priority.

Usage guidelines

The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet for transmission.

Examples

Set the DSCP value to 40 for SNMP responses.

```
<Sysname> system-view
[Sysname] snmp-agent packet response dscp 40
```

snmp-agent port

Use **snmp-agent port** to specify an SNMP listening port.

Use **undo snmp-agent port** to restore the default.

Syntax

snmp-agent port *port-number*

undo snmp-agent port

Default

The SNMP listening port is UDP port 161.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies an SNMP listening port by its number in the range of 1 to 65535.

Usage guidelines

The SNMP agent will fail to be enabled when the port that the agent will listen on is used by another service. You can use the **snmp-agent port** command to change the SNMP listening port. As a best practice, execute the **display udp verbose** command to view the UDP port use information before specifying a new SNMP listening port.

After changing the SNMP listening port, the NMS can perform SNMP set and get operations on the device only after reconnecting the device by using the new port number.

Examples

# Specify **5555** as the SNMP listening port..

```
<Sysname> system-view
[Sysname] snmp-agent port 5555
```

Related commands

display udp verbose (see IP performance optimization commands in *Layer 3—IP Services Configuration Guide*)

snmp-agent remote

Use **snmp-agent remote** to set an SNMP engine ID for a remote SNMP entity.

Use **undo snmp-agent remote** to delete the SNMP engine ID of a remote SNMP entity.

Syntax

snmp-agent remote { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **engineid** *engineid*

undo snmp-agent remote *ip-address*

Default

No SNMP engine IDs are configured for remote SNMP entities.

Views

System view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies a remote SNMP entity by its IPv4 address.

ipv6 *ipv6-address*: Specifies a remote SNMP entity by its IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the remote SNMP entity belongs. The *vpn-instance-name* argument represents the VPN instance name. a case-sensitive string of 1 to 31 characters. If the SNMP entity belongs to the public network, do not specify this option.

engineid: Specifies the SNMP engine ID of the remote SNMP entity. This argument is a case-insensitive hexadecimal string. Its length is an even number in the range of 10 to 64. All-zero and all-F strings are invalid.

Usage guidelines

To send informs to an NMS, you must configure the SNMP engine ID of the NMS on the SNMP agent.

The NMS accepts the SNMPv3 informs from the SNMP agent only if the engine ID in the informs is the same as its local engine ID.

You can configure a maximum of 20 remote SNMP engine IDs.

Examples

# Set the SNMP engine ID to **123456789A** for the remote entity **10.1.1.1**.

```
<Sysname> system-view
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
```

Related commands

display snmp-agent remote

snmp-agent sys-info contact

Use **snmp-agent sys-info contact** to configure the system contact.

Use **undo snmp-agent sys-info contact** to restore the default contact.

Syntax

snmp-agent sys-info contact *sys-contact*

undo snmp-agent sys-info contact

Default

The system contact is **New H3C Technologies Co., Ltd.**.

Views

System view

Predefined user roles

network-admin

Parameters

sys-contact: Specifies the system contact, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the system contact for system maintenance and management.

Examples

# Configure the system contact as **Dial System Operator # 27345**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator # 27345
```

Related commands

display snmp-agent sys-info

snmp-agent sys-info location

Use **snmp-agent sys-info location** to configure the system location.

Use **undo snmp-agent sys-info location** to restore the default location.

Syntax

snmp-agent sys-info location *sys-location*

undo snmp-agent sys-info location

Default

The system location is **Hangzhou, China**.

Views

System view

Predefined user roles

network-admin

Parameters

sys-location: Specifies the system location, a case-sensitive string of 1 to 255 characters.

Usage guidelines

Configure the location of the device for system maintenance and management.

Examples

# Configure the system location as **Room524-row1-3**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info location Room524-row1-3
```

Related commands

display snmp-agent sys-info

snmp-agent sys-info version

Use **snmp-agent sys-info version** to enable SNMP versions.

Use **undo snmp-agent sys-info version** to disable SNMP versions.

Syntax

In non-FIPS mode:

snmp-agent sys-info contact version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

In FIPS mode:

snmp-agent sys-info version v3

undo snmp-agent sys-info version v3

Default

SNMPv3 is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

all: Specifies SNMPv1, SNMPv2c, and SNMPv3.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

Usage guidelines

SNMPv1 and SNMPv2c settings in this command are not supported in FIPS mode.

Configure the SNMP agent with the same SNMP version as the NMS for successful communications between them.

To use SNMP notifications in IPv6, enable SNMPv2c or SNMPv3.

Examples

# Enable SNMPv3.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v3
```

Related commands

display snmp-agent sys-info

snmp-agent target-host

Use **snmp-agent target-host** to configure an SNMP notification target host.

Use **undo snmp-agent target-host** to remove an SNMP notification target host.

Syntax

In non-FIPS mode:

snmp-agent target-host inform address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6-target-host* } **params securityname** *security-string* [**vpn-instance** *vpn-instance-name*]

In FIPS mode:

snmp-agent target-host inform address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

snmp-agent target-host trap address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6-target-host* } **params securityname** *security-string* [**vpn-instance** *vpn-instance-name*]

Default

No SNMP notification target hosts exist.

Views

System view

Predefined user roles

network-admin

Parameters

inform: Specifies a host that receives informs.

trap: Specifies a host that receives traps.

address: Specifies the destination address of SNMP notifications.

udp-domain: Specifies UDP as the transport protocol.

ipv4-target-host: Specifies a target host by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. The string can only contain letters, numbers, hyphens (-), underscores (_), and dots (.). If you specify a host name, the IPv4 address of the target host can be obtained.

ipv6 *ipv6-target-host*: Specifies a target host by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters, which only contains letters, numbers, hyphens (-), underscores (_), and dots (.). If you specify a host name, the IPv6 address of the target host can be obtained. If you specify an IPv6 address, the address cannot be a link local address.

udp-port *port-number*: Specifies the UDP port for SNMP notifications. The default port number is 162.

dscp-value: Sets the DSCP value for traps sent to the target host, in the range of 0 to 63. The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet and affects the transmission priority of the packet. A greater DSCP value represents a higher priority. The default DSCP value for traps is 0.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the target host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the target host belongs to the public network, do not specify this option.

params securityname *security-string*: Specifies the authentication parameter. The *security-string* argument specifies an SNMPv1 or SNMPv2c community name or an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

- **authentication**: Specifies the security model to be authentication without privacy. You must specify the authentication key when you create the SNMPv3 user.
- **privacy**: Specifies the security model to be authentication with privacy. You must specify the authentication key and encryption key when you create the SNMPv3 user.

Usage guidelines

You can specify multiple SNMP notification target hosts.

Make sure the SNMP agent uses the same UDP port for SNMP notifications as the target host. Typically, NMSs, for example, IMC and MIB Browser, use port 162 for SNMP notifications as defined in the SNMP protocols.

If none of the keywords **v1**, **v2c**, or **v3** is specified, SNMPv1 is used. Make sure the SNMP agent uses the same SNMP version as the target host so the host can receive the notification.

If neither **authentication** nor **privacy** is specified, the security model is no authentication, no privacy.

Examples

# Configure the SNMP agent to send SNMPv3 traps to 10.1.1.1 by using the username **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
public v3
```

Related commands

snmp-agent { **inform** | **trap** } **source**

snmp-agent trap enable

snmp-agent trap life

snmp-agent trap enable

Use **snmp-agent trap enable** to enable SNMP notifications.

Use **undo snmp-agent trap enable** to disable SNMP notifications.

Syntax

snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

undo snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

Default

SNMP configuration notifications, standard notifications, and system notifications are enabled. Whether other SNMP notifications are enabled varies by module.

Views

System view

Predefined user roles

network-admin

Parameters

configuration: Specifies configuration notifications. If configuration notifications are enabled, the system checks the running configuration and the startup configuration every 10 minutes for any change and generates a notification for the most recent change.

protocol: Specifies protocol module notifications. You can use the **snmp-agent trap enable ?** command to obtain the value of this argument. For more information about this argument, see the command reference for each module.

standard: Specifies SNMP standard notifications.

Table 13 Standard SNMP notifications

Keyword	Definition
authentication	Authentication failure notification sent when an NMS fails to be authenticated by the SNMP agent.
coldstart	Notification sent when the device restarts.
linkdown	Notification sent when the link of a port goes down.
linkup	Notification sent when the link of a port comes up.

Keyword	Definition
warmstart	Notification sent when the SNMP agent restarts.

system: Specifies system notifications sent when the system time is modified, the system reboots, or the main system software image is not available.

Usage guidelines

To report critical protocol events to an NMS, first enable the protocol and then enable SNMP notifications for the protocol.

To use SNMP notifications in IPv6, enable SNMPv2c or SNMPv3.

For SNMP notifications to be sent correctly, you must also configure the notification sending parameters as required.

If no optional parameters are specified, this command or its **undo** form enables or disables all SNMP notifications supported by the device.

Examples

# Enable the SNMP agent to send SNMP authentication failure notifications.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard authentication
```

Related commands

snmp-agent sys-info version

snmp-agent target-host

snmp-agent trap if-mib link extended

Use **snmp-agent trap if-mib link extended** to configure the SNMP agent to send extended linkUp/linkDown notifications.

Use **undo snmp-agent trap if-mib link extended** to restore the default.

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

Default

The SNMP agent sends standard linkUp/linkDown notifications.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Extended linkUp and linkDown notifications add interface description and interface type to the standard linkUp/linkDown notifications for fast failure point identification.

When you use this command, make sure the NMS supports the extended linkup and linkDown notifications.

Examples

# Enable extended linkUp/linkDown notifications.

```
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

snmp-agent trap life

Use **snmp-agent trap life** to set the lifetime of notifications in the SNMP notification queue.

Use **undo snmp-agent trap life** to restore the default notification lifetime.

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

Default

The SNMP notification lifetime is 120 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Sets a lifetime in the range of 1 to 2592000, in seconds.

Usage guidelines

When congestion occurs, the SNMP agent buffers notifications in a queue. The notification lifetime sets how long a notification can stay in the queue. A notification is deleted when its lifetime expires.

Examples

# Set the SNMP notification lifetime to 60 seconds.

```
<Sysname> system-view
[Sysname] snmp-agent trap life 60
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent trap queue-size

snmp-agent trap log

Use **snmp-agent trap log** to enable SNMP notification logging.

Use **undo snmp-agent trap log** to disable SNMP notification logging.

Syntax

snmp-agent trap log

undo snmp-agent trap log

Default

SNMP notification logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use SNMP notification logging to record SNMP notifications sent by the SNMP agent for notification tracking. The SNMP agent sends the logs to the information center. You can configure the information center to output the logs to a destination as needed.

Examples

# Enable SNMP notification logging.

```
<Sysname> system-view
[Sysname] snmp-agent trap log
```

snmp-agent trap queue-size

Use **snmp-agent trap queue-size** to set the SNMP notification queue size.

Use **undo snmp-agent trap queue-size** to restore the default queue size.

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

Default

The SNMP notification queue can store a maximum of 100 notifications.

Views

System view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum number of notifications that the SNMP notification queue can hold. The value range is 1 to 1000.

Usage guidelines

When congestion occurs, the SNMP agent buffers notifications in a queue. SNMP notification queue size sets the maximum number of notifications that this queue can hold.

When the queue size is reached, the system discards the new notification it receives.

If modification of the queue size causes the number of notifications in the queue to exceed the queue size, the oldest notifications are dropped for new notifications.

Examples

# Set the SNMP notification queue size to 200.

```
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

Related commands

snmp-agent target-host

snmp-agent trap enable

snmp-agent trap life

snmp-agent usm-user { v1 | v2c }

Use **snmp-agent usm-user** { **v1** | **v2c** } to create an SNMPv1 or SNMPv2c user.

Use **undo snmp-agent usm-user** { **v1** | **v2c** } to delete an SNMPv1 or SNMPv2c user.

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

undo snmp-agent usm-user { **v1** | **v2c** } *user-name*

Default

No SNMPv1 or SNMPv2c users exist.

Views

System view

Predefined user roles

network-admin

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

user-name: Specifies an SNMP username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies an SNMPv1 or SNMPv2c group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. The user takes effect only after you create the group.

acl: Specifies a basic or advanced IPv4 ACL for the user.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the user.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command is not available in FIPS mode.

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

On an SNMPv1 or SNMPv2c network, NMSs and agents authenticate each other by using the community name. On an SNMPv3 network, NMSs and agents authenticate each other by using the username.

You can create an SNMPv1 or SNMPv2c community by using either of the following ways:

- Execute the **snmp-agent community** command.
- Execute the **snmp-agent usm-user** { **v1** | **v2c** } and **snmp-agent group** { **v1** | **v2c** } commands to create an SNMPv1 or SNMPv2c user and the group that the user is assigned to. The system automatically creates an SNMP community by using the SNMPv1 or SNMPv2c username.

The **display snmp-agent community** command displays information only about communities created and saved in plaintext form.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

# Add the user **userv2c** to the SNMPv2c group **readCom** so an NMS can use the protocol SNMPv2c and the read-only community name **userv2c** to access the device.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

# Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.1 can use the protocol SNMPv2c and read-only community name **userv2c** to access the device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

# Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.2 can use the protocol SNMPv2c and read-only community name **userv2c** to access the device.

```
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl name testacl
```

Related commands

display snmp-agent community

snmp-agent community

snmp-agent group

snmp-agent usm-user v3

Use **snmp-agent usm-user v3** to create an SNMPv3 user.

Use **undo snmp-agent usm-user v3** to delete an SNMPv3 user.

Syntax

In non-FIPS mode:

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

In FIPS mode:

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] { **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

Default

No SNMPv3 users exist.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies an SNMPv3 group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. The user takes effect only after you create the group.

user-role *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters.

remote { *ipv4-address* | **ipv6** *ipv6-address* }: Specifies a target host by its IPv4 or IPv6 address, typically the NMS, to receive the notifications. To send SNMPv3 notifications to a target host, you need to specify this option and use the **snmp-agent remote** command to bind the IPv4 or IPv6 address to the remote engine ID.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the target host belongs to. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the target host belongs to the public network, do not specify this option.

cipher: Specifies an authentication key and an encryption key in encrypted form. The keys will be converted to a digest in encrypted form and stored in the device.

simple: Specifies an authentication key and an encryption key in plaintext from. The keys will be converted to a digest in encrypted form and stored in the device.

authentication-mode: Specifies an authentication algorithm. If you do not specify the keyword, the system does not perform authentication. For more information about authentication algorithms, see IPSec configuration in *Security Configuration Guide*.

- **md5**: Specifies the HMAC-MD5 authentication algorithm.
- **sha**: Specifies the HMAC-SHA1 authentication algorithm.

auth-password: Specifies an authentication key. This argument is case sensitive.

- The plaintext form of the key in non-FIPS mode is a string of 1 to 64 characters. The plaintext form of the key in FIPS mode is a string of 15 to 64 characters, which must contain numbers, uppercase letters, lowercase letters, and special characters.
- The encrypted form of the key can be calculated by using the **snmp-agent calculate-password** command.

privacy-mode: Specifies an encryption algorithm. If you do not specify this keyword, the system does not perform encryption.

- **3des**: Specifies the 3DES encryption algorithm that uses a 168-bit key.
- **aes128**: Specifies the AES encryption algorithm that uses a 128-bit key.
- **aes192**: Specifies the AES encryption algorithm that uses a 192-bit key.
- **aes256**: Specifies the AES encryption algorithm that uses a 256-bit key.
- **des56**: Specifies the DES encryption algorithm that uses a 56-bit key.

priv-password: Specifies an encryption key. This argument is case sensitive.

- The plaintext form of the key in non-FIPS mode is a string of 1 to 64 characters. The plaintext form of the key in FIPS mode is a string of 15 to 64 characters, which must contain numbers, uppercase letters, lowercase letters, and special characters.

- The encrypted form of the key can be calculated by using the **snmp-agent calculate-password** command.

acl: Specifies a basic or advanced IPv4 ACL for the user.

ipv4-acl-number: Specifies a basic or advanced IPv4 ACL by its number. The basic IPv4 ACL number is in the range of 2000 to 2999. The advanced IPv4 ACL number is in the range of 3000 to 3999.

name *ipv4-acl-name*: Specifies a basic or advanced IPv4 ACL by its name, a case-insensitive string of 1 to 63 characters.

acl ipv6: Specifies a basic or advanced IPv6 ACL for the user.

ipv6-acl-number: Specifies a basic or advanced IPv6 ACL by its number. The basic IPv6 ACL number is in the range of 2000 to 2999. The advanced IPv6 ACL number is in the range of 3000 to 3999.

name *ipv6-acl-name*: Specifies a basic or advanced IPv6 ACL by its name, a case-insensitive string of 1 to 63 characters.

local: Specifies the local SNMP engine. By default, an SNMPv3 user is associated with the local SNMP engine.

engineid *engineid-string*: Specifies an SNMP engine ID. The *engineid-string* argument is an even number of hexadecimal characters. All-zero and all-F strings are invalid. The even number is in the range of 10 to 64. If you change the local engine ID, the existing SNMPv3 users and keys become invalid. To delete an invalid username, specify the engine ID associated with the username in the **undo snmp-agent usm-user v3** command.

Usage guidelines

Only users with the network-admin or level-15 user role can execute this command. Users with other user roles cannot execute this command even if these roles are granted access to commands of the SNMP feature or this command.

You can use either of the following modes to control SNMPv3 user access to MIB objects.

- **VACM**—Controls user access to MIB objects by assigning the user to an SNMP group. To make sure the user takes effect, make sure the group has been created. An SNMP group contains one or multiple users and specifies the MIB views and security model for the users. The authentication and encryption algorithms for each user are specified when they are created.
- **RBAC**—Controls user access to MIB objects by assigning user roles to the user. A user role specifies the MIB objects accessible to the user and the operations that the user can perform on the objects. After you create a user in RBAC mode, you can use the **snmp-agent usm-user v3 user-role** command to assign more user roles to the user. You can assign a maximum of 64 user roles to a user.

RBAC mode controls access on a per MIB object basis, and VACM mode controls access on a MIB view basis. As a best practice to enhance MIB security, use RBAC mode.

You can execute the **snmp-agent usm-user v3** command multiple times to create different SNMPv3 users in VACM mode. If you do not change the username each time, the most recent configuration takes effect.

You can execute the **snmp-agent usm-user v3** command in RBAC mode multiple times to assign different user roles to an SNMPv3 user. The following restrictions and guidelines apply:

- If you specify only user roles but do not change any other settings each time, the **snmp-agent usm-user v3** command assigns different user roles to the user. Other settings remain unchanged.
- If you specify user roles and also change other settings each time, the **snmp-agent usm-user v3** command assigns different user roles to the user. The most recent configuration for other settings takes effect.

You can specify an ACL for the user and group, respectively, to filter illegitimate NMSs from accessing the agent. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

For more information about ACL, see *ACL and QoS Configuration Guide*.

Examples

In VACM mode:

# Add user **testUser** to SNMPv3 group **testGroup**, and enable authentication for the group. Specify authentication algorithm **HMAC-SHA1** and plaintext-form authentication key **123456TESTplat&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTplat&!
```

# For an NMS to access the MIB objects in the default view **ViewDefault**, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm and key.

# Add user **testUser** to SNMPv3 group **testGroup**, and enable authentication and encryption for the group. Specify authentication algorithm **HMAC-SHA1**, encryption algorithm **AES**, plaintext-form authentication key **123456TESTauth&!**, and plaintext-form encryption key **123456TESTencr&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

# For an NMS to access the MIB objects in the default view **ViewDefault**, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm.
- Privacy algorithm.
- Plaintext authentication and encryption keys.

# Add user **remoteUser** for the SNMP remote engine at 10.1.1.1 to SNMPv3 group **testGroup**, and enable authentication and encryption for the group. Specify authentication algorithm **HMAC-SHA1**, encryption algorithm **AES**, plaintext-form authentication key **123456TESTauth&!**, and plaintext-form encryption key **123456TESTencr&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 remoteUser testGroup remote 10.1.1.1 simple
authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

In RBAC mode:

# Create SNMPv3 user **testUser** with user role **network-operator** and enable authentication for the user. Specify authentication algorithm **HMAC-SHA1** and plaintext-form authentication key **123456TESTplat&!** for the user.

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser user-role network-operator simple
authentication-mode sha 123456TESTplat&!
```

For an NMS to have read-only access to all MIB objects, make sure the following configurations on the NMS are the same as the SNMP agent:

- SNMPv3 username.
- SNMP protocol version.
- Authentication algorithm and key.

Related commands

display snmp-agent usm-user

snmp-agent calculate-password

snmp-agent group

snmp-agent remote

snmp-agent usm-user v3 user-role

snmp-agent usm-user v3 user-role

Use **snmp-agent usm-user v3 user-role** to assign a user role to an SNMPv3 user created in RBAC mode.

Use **undo snmp-agent usm-user user-role** to remove a user role.

Syntax

snmp-agent usm-user v3 *user-name* **user-role** *role-name*

undo snmp-agent usm-user v3 *user-name* **user-role** *role-name*

Default

An SNMPv3 user has the user role assigned to it at its creation.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies an SNMPv3 username, a case-sensitive string of 1 to 32 characters.

user-role *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can assign a maximum of 64 user roles to an SNMPv3 user.

An SNMPv3 user must have a minimum of one user role.

Examples

# Assign the user role **network-admin** to the SNMPv3 user **testUser**.

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v3 testUser user-role network-admin
```

Related commands

```
snmp-agent usm-user v3
```