Contents

Configuring SNMP

Overview

Simple Network Management Protocol (SNMP) is an Internet standard protocol widely used for a management station to access and operate the devices on a network, regardless of their vendors, physical characteristics, and interconnect technologies.

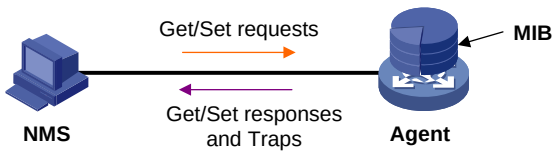
SNMP enables network administrators to read and set the variables on managed devices for state monitoring, troubleshooting, statistics collection, and other management purposes.

SNMP framework

The SNMP framework contains the following elements:

- **SNMP manager**—Works on an NMS to monitor and manage the SNMP-capable devices in the network.
- **SNMP agent**—Works on a managed device to receive and handle requests from the NMS, and sends notifications to the NMS when events, such as an interface state change, occur.
- **Management Information Base (MIB)**—Specifies the variables (for example, interface status and CPU usage) maintained by the SNMP agent for the SNMP manager to read and set.

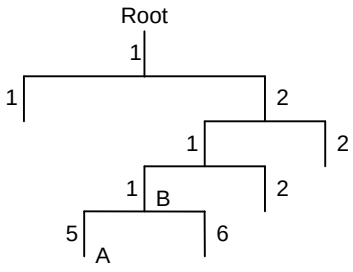
Figure 1 Relationship between NMS, agent, and MIB



MIB and view-based MIB access control

A MIB stores variables called "nodes" or "objects" in a tree hierarchy and identifies each node with a unique OID. An OID is a dotted numeric string that uniquely identifies the path from the root node to a leaf node. For example, object B in Figure 2 is uniquely identified by the OID {1.2.1.1}.

Figure 2 MIB tree



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

A MIB view can have multiple view records each identified by a *view-name oid-tree* pair.

You control access to the MIB by assigning MIB views to SNMP groups or communities.

SNMP operations

SNMP provides the following basic operations:

- **Get**—NMS retrieves the SNMP object nodes in an agent MIB.
- **Set**—NMS modifies the value of an object node in an agent MIB.
- **Notification**—SNMP agent sends traps or informs to report events to the NMS. The difference between these two types of notification is that informs require acknowledgment but traps do not. Traps are available in SNMPv1, SNMPv2c, and SNMPv3, but informs are available only in SNMPv2c and SNMPv3.

Protocol versions

SNMPv1, SNMPv2c, and SNMPv3 are supported in non-FIPS mode. Only SNMPv3 is supported in FIPS mode. An NMS and an SNMP agent must use the same SNMP version to communicate with each other.

- **SNMPv1**—Uses community names for authentication. To access an SNMP agent, an NMS must use the same community name as set on the SNMP agent. If the community name used by the NMS differs from the community name set on the agent, the NMS cannot establish an SNMP session to access the agent or receive traps from the agent.
- **SNMPv2c**—Uses community names for authentication. SNMPv2c is compatible with SNMPv1, but supports more operation types, data types, and error codes.
- **SNMPv3**—Uses a user-based security model (USM) to secure SNMP communication. You can configure authentication and privacy mechanisms to authenticate and encrypt SNMP packets for integrity, authenticity, and confidentiality.

Access control modes

SNMP uses the following modes to control access to MIB objects:

- **View-based Access Control Model**—VACM mode controls access to MIB objects by assigning MIB views to SNMP communities or users.
- **Role based access control**—RBAC mode controls access to MIB objects by assigning user roles to SNMP communities or users.
    - SNMP communities or users with predefined user role network-admin or level-15 have read and write access to all MIB objects.
    - SNMP communities or users with predefined user role network-operator have read-only access to all MIB objects.
    - SNMP communities or users with a non-predefined user role have user-assigned access rights. To create a non-predefined user role, use the **role** command. To assign MIB object rights to the user role, use the **rule** command.

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.

If you create the same SNMP community or user with both modes multiple times, the most recent configuration takes effect. For more information about RBAC, see *Fundamentals Command Reference*.

SNMP silence

SNMP silence enables the device to automatically detect and defend against SNMP attacks.

After you enable SNMP, the device automatically starts an SNMP silence timer and counts the number of packets that fail SNMP authentication within 1 minute.

- If the number of the packets is smaller than 100, the device restarts the timer and counting.
- If the number of the packets is equal to or greater than 100, the SNMP module enters a 5-minute silence period, during which the device does not respond to any SNMP packets. After the 5 minutes expire, the device restarts the timer and counting.

FIPS compliance

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*.

Configuring SNMP basic parameters

SNMPv3 differs from SNMPv1 and SNMPv2c in many ways. Their configuration procedures are described in separate sections.

Configuring SNMPv1 or SNMPv2c basic parameters

SNMPv1 and SNMPv2c settings are not supported in FIPS mode.

Only users with the network-admin or level-15 user role can create SNMPv1 or SNMPv2c communities, users, or groups. Users with other user roles cannot create SNMPv1 or SNMPv2c communities, users, or groups even if these roles are granted access to related commands or commands of the SNMPv1 or SNMPv2c feature.

To configure SNMPv1 or SNMPv2c basic parameters:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Enable the SNMP agent.	**snmp-agent**	By default, the SNMP agent is disabled. The SNMP agent is enabled when you use any command that begins with **snmp-agent** except for the **snmp-agent calculate-password** command.
3. (Optional.) Configure the system contact.	**snmp-agent sys-info contact** *sys-contact*	By default, the system contact is **New H3C Technologies Co., Ltd.**.
4. (Optional.) Configure the system location.	**snmp-agent sys-info location** *sys-location*	By default, the system location is **Hangzhou, China**
5. Enable SNMPv1 or SNMPv2c.	**snmp-agent sys-info version** { **all** | { **v1** | **v2c** } *}	By default, SNMPv3 is enabled.
6. (Optional.) Set a local engine ID.	**snmp-agent local-engineid** *engineid*	By default, the local engine ID is the company ID plus the device ID. The device ID varies by device model.

Step	Command	Remarks
7. (Optional.) Set an engine ID for a remote SNMP entity.	**snmp-agent remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **engineid** *engineid*	By default, no remote entity engine IDs exist. This step is required for the device to send SNMPv1 or SNMPv2c notifications to a host, typically NMS.
8. (Optional.) Create or update a MIB view.	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	By default, the MIB view **ViewDefault** is predefined. In this view, all the MIB objects in the **iso** subtree but the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees are accessible. Each *view-name oid-tree* pair represents a view record. If you specify the same record with different MIB sub-tree masks multiple times, the most recent configuration takes effect.
9. Configure the SNMP access right.	• (Method 1.) Create an SNMP community: 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* }] * 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* }] * • (Method 2.) Create an SNMPv1/v2c group, and add users to the group: a. **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* }] * b. **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* }] *	By default, no SNMP group or SNMP community exists. The username in method 2 has the same purpose as the community name in method 1. Whichever method you use, make sure the configured name is the same as the community name on the NMS.
10. (Optional.) Create an SNMP context.	**snmp-agent context** *context-name*	By default, no SNMP contexts exist.

Step	Command	Remarks
11. (Optional.) Map an SNMP community to an SNMP context.	**snmp-agent community-map** *community-name* **context** *context-name*	By default, no mapping exists between an SNMP community and an SNMP context.
12. (Optional.) Configure the maximum SNMP packet size (in bytes) that the SNMP agent can handle.	**snmp-agent packet max-size** *byte-count*	By default, an SNMP agent can process SNMP packets with a maximum size of 1500 bytes,
13. Specify the UDP port for receiving SNMP packets.	**snmp-agent port** *port-num*	By default, the device uses UDP port 161 for receiving SNMP packets.
14. (Optional.) Configure SNMP agent alive notification sending and set the sending interval.	**snmp-agent trap periodical-interval** *interval*	By default, sending SNMP agent alive notifications is enabled and the sending interval is 60 seconds.
15. (Optional.) Set the DSCP value for SNMP responses.	**snmp-agent packet response dscp** *dscp-value*	By default, the DSCP value is 0 for SNMP responses.

Configuring SNMPv3 basic parameters

Only users with the network-admin or level-15 user role can create SNMPv3 users or groups. Users with other user roles cannot create SNMPv3 users or groups even if these roles are granted access to related commands or commands of the SNMPv3 feature.

SNMPv3 users are managed in groups. All SNMPv3 users in a group share the same security model, but can use different authentication and privacy 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 1 and match the settings on the NMS.

Table 1 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, privacy key	If the authentication key or the privacy key is not configured, SNMP communication will fail.
Authentication without privacy	**authentication**	Authentication key	If no authentication key is configured, SNMP communication will fail. The privacy key (if any) for the user does not take effect.

Security model	Security model keyword for the group	Security key settings for the user	Remarks
No authentication, no privacy	Neither **authentication** nor **privacy**	None	The authentication and privacy keys, if configured, do not take effect.

To configure SNMPv3 basic parameters:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Enable the SNMP agent.	**snmp-agent**	By default, the SNMP agent is disabled. The SNMP agent is enabled when you use any command that begins with **snmp-agent** except for the **snmp-agent calculate-password** command.
3. (Optional.) Configure the system contact.	**snmp-agent sys-info contact** *sys-contact*	By default, the system contact is **New H3C Technologies Co., Ltd.**.
4. (Optional.) Configure the system location.	**snmp-agent sys-info location** *sys-location*	By default, the system location is **Hangzhou, China**.
5. Enable SNMPv3.	**snmp-agent sys-info version** { **all** | { **v1** | **v2c** | **v3** } *	By default, SNMPv3 is enabled.
6. (Optional.) Set a local engine ID.	**snmp-agent local-engineid** *engineid*	By default, the local engine ID is the company ID plus the device ID. The device ID varies by device model. IMPORTANT: After you change the local engine ID, the existing SNMPv3 users and encrypted keys become invalid, and you must reconfigure them.
7. (Optional.) Set an engine ID for a remote SNMP entity.	**snmp-agent remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **engineid** *engineid*	By default, no remote entity engine IDs exist. This step is required for the device to send SNMPv3 notifications to a host, typically NMS.

Step	Command	Remarks
8. (Optional.) Create or update a MIB view.	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	By default, the MIB view **ViewDefault** is predefined. In this view, all the MIB objects in the **iso** subtree but the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees are accessible. Each *view-name oid-tree* pair represents a view record. If you specify the same record with different MIB sub-tree masks multiple times, the most recent configuration takes effect.
9. (Optional.) Create an SNMPv3 group.	• In non-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* }] * • 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* }] *	By default, no SNMP groups exist.
10. (Optional.) Calculate the encrypted form for a key in plaintext form.	• 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* }	N/A

Step	Command	Remarks
11. Create an SNMPv3 user.	• 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* }] * • In non-FIPS mode (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* }] * • 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* }] * • In FIPS mode (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* }] *	To send notifications to an SNMPv3 NMS, you must specify the **remote** keyword.
12. (Optional.) Assign a user role to an SNMPv3 user created in RBAC mode.	**snmp-agent usm-user v3** *user-name* **user-role** *role-name*	By default, an SNMPv3 user has the user role assigned to it at its creation.
13. (Optional.) Create an SNMP context.	**snmp-agent context** *context-name*	By default, no SNMP contexts exist

Step	Command	Remarks
14. (Optional.) Configure the maximum SNMP packet size (in bytes) that the SNMP agent can handle.	**snmp-agent packet max-size** *byte-count*	By default, an SNMP agent can process SNMP packets with a maximum size of 1500 bytes.
15. (Optional.) Specify the UDP port for receiving SNMP packets.	**snmp-agent port** *port-num*	By default, the device uses UDP port 161 for receiving SNMP packets.
16. (Optional.) Configure SNMP agent alive notification sending and set the sending interval.	**snmp-agent trap periodical-interval** *interval*	By default, sending SNMP agent alive notifications is enabled and the sending interval is 60 seconds.
17. (Optional.) Set the DSCP value for SNMP responses.	**snmp-agent packet response dscp** *dscp-value*	By default, the DSCP value is 0 for SNMP responses.

Configuring SNMP logging

Enable SNMP logging only if necessary. SNMP logging is memory-intensive and might impact device performance.

The SNMP agent logs Get requests, Set requests, Set responses, SNMP notifications, and SNMP authentication failures, but does not log Get responses.

- **Get operation**—The agent logs the IP address of the NMS, name of the accessed node, and node OID.
- **Set operation**—The agent logs the NMS' IP address, name of accessed node, node OID, variable value, and error code and index for the Set operation.
- **Notification tracking**—The agent logs the SNMP notifications after sending them to the NMS.
- **SNMP authentication failure**—The agent logs related information when an NMS fails to be authenticated by the agent.

The SNMP module sends these logs to the information center. You can configure the information center to output these messages to certain destinations, such as the console and the log buffer. The total output size for the node field (MIB node name) and the value field (value of the MIB node) in each log entry is 1024 bytes. If this limit is exceeded, the information center truncates the data in the fields. For more information about the information center, see "Configuring the information center."

To configure SNMP logging:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Enable SNMP logging.	**snmp-agent log** { **all** | **authfail** | **get-operation** | **set-operation** }	By default, SNMP logging is disabled.
3. (Optional.) Enable SNMP notification logging.	**snmp-agent trap log**	By default, SNMP notification logging is disabled.

Configuring SNMP notifications

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.

Enabling SNMP notifications

Enable an SNMP notification only if necessary. SNMP notifications are memory-intensive and might affect device performance.

To generate linkUp or linkDown notifications when the link state of an interface changes, you must perform the following tasks:

- Enable linkUp or linkDown notification globally by using the **snmp-agent trap enable standard** [**linkdown** | **linkup**] * command.
- Enable linkUp or linkDown notification on the interface by using the **enable snmp trap updown** command.

After you enable notifications for a module, whether the module generates notifications also depends on the configuration of the module. For more information, see the configuration guide for each module.

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

To enable SNMP notifications:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SNMP notifications.	**snmp-agent trap enable** [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]	By default, SNMP configuration notifications, standard notifications, and system notifications are enabled. Whether other SNMP notifications are enabled varies by modules.
3. Enter interface view.	**interface** *interface-type interface-number*	N/A
4. Enable link state notifications.	**enable snmp trap updown**	By default, link state notifications are enabled.

Configuring parameters for sending SNMP notifications

You can configure the SNMP agent to send notifications as traps or informs to a host, typically an NMS, for analysis and management. Traps are less reliable and use fewer resources than informs, because an NMS does not send an acknowledgment when it receives a trap.

Configuration guidelines

When network congestion occurs or the destination is not reachable, the SNMP agent buffers notifications in a queue. You can set the queue size and the notification lifetime (the maximum time that a notification can stay in the queue). A notification is deleted when its lifetime expires. When the notification queue is full, the oldest notifications are automatically deleted.

You can extend standard linkUp/linkDown notifications to include interface description and interface type, but must make sure the NMS supports the extended SNMP messages.

To send informs, make sure of the following information:

- The SNMP agent and the NMS use SNMPv2c or SNMPv3.
- If SNMPv3 is used, you must configure the SNMP engine ID of the NMS when you configure SNMPv3 basic settings. Also, specify the IP address of the SNMP engine when you create the SNMPv3 user.

Configuration prerequisites

Configure the SNMP agent with the same basic SNMP settings as the NMS. If SNMPv1 or SNMPv2c is used, you must configure a community name. If SNMPv3 is used, you must configure an SNMPv3 user, a MIB view, and a remote SNMP engine ID associated with the SNMPv3 user for notifications.

Make sure the SNMP agent and the NMS can reach each other.

Configuration procedure

To configure the SNMP agent to send notifications to a host:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a target host.	• (In non-FIPS mode.) Send traps to the target host: **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**]] • (In FIPS mode.) Send traps to the target host: **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** } • (In non-FIPS mode.) Send informs to the target host: **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**] } • (In FIPS mode.) Send informs to the target host: **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** }	By default, no target host is configured.
3. (Optional.) Configure a source address for notifications.	**snmp-agent** { **inform** | **trap** } **source** *interface-type* { *interface-number* | *interface-number.subnumber* }	By default, SNMP uses the IP address of the outgoing routed interface as the source IP address.
4. (Optional.) Enable extended linkUp/linkDown notifications.	**snmp-agent trap if-mib link extended**	By default, the SNMP agent sends standard linkup/linkDown notifications.

Step	Command	Remarks
5. (Optional.) Set the notification queue size.	**snmp-agent trap queue-size** *size*	By default, the notification queue can hold 100 notification messages.
6. (Optional.) Set the notification lifetime.	**snmp-agent trap life** *seconds*	The default notification lifetime is 120 seconds.

Displaying the SNMP settings

Execute **display** commands in any view.

Task	Command
Display SNMP agent system information.	**display snmp-agent sys-info** [**contact** | **location** | **version**] *
Display SNMP agent statistics.	**display snmp-agent statistics**
Display the local engine ID.	**display snmp-agent local-engineid**
Display SNMP group information.	**display snmp-agent group** [*group-name*]
Display remote engine IDs.	**display snmp-agent remote** [{ *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]]
Display basic information about the notification queue.	**display snmp-agent trap queue**
Display SNMP notifications enabling status for modules.	**display snmp-agent trap-list**
Display SNMPv3 user information.	**display snmp-agent usm-user** [**engineid** *engineid* | **username** *user-name* | **group** *group-name*] *
Display SNMPv1 or SNMPv2c community information. (This command is not supported in FIPS mode.)	**display snmp-agent community** [**read** | **write**]
Display MIB view information.	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]
Display SNMP MIB node information.	**display snmp-agent mib-node** [**details** | **index-node** | **trap-node** | **verbose**]
Display SNMP contexts.	**display snmp-agent context** [*context-name*]

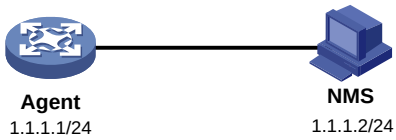
SNMPv1/SNMPv2c configuration example

The SNMPv1 configuration procedure is the same as the SNMPv2c configuration procedure. This example uses SNMPv1, and is not available in FIPS mode.

Network requirements

As shown in Figure 3, the NMS (1.1.1.2/24) uses SNMPv1 to manage the SNMP agent (1.1.1.1/24), and the agent automatically sends notifications to report events to the NMS.

Figure 3 Network diagram



Configuration procedure

1. Configure the SNMP agent:

   # Configure the IP address of the agent and make sure the agent and the NMS can reach each other. (Details not shown.)

   # Specify SNMPv1, and create read-only community **public** and read and write community **private**.

   ```
   <Agent> system-view
   [Agent] snmp-agent sys-info version v1
   [Agent] snmp-agent community read public
   [Agent] snmp-agent community write private
   ```

   # Configure contact and physical location information for the agent.

   ```
   [Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
   [Agent] snmp-agent sys-info location telephone-closet,3rd-floor
   ```

   # Enable SNMP notifications, specify the NMS at 1.1.1.2 as an SNMP trap destination, and use **public** as the community name. (To make sure the NMS can receive traps, specify the same SNMP version in the **snmp-agent target-host** command as is configured on the NMS.)

   ```
   [Agent] snmp-agent trap enable
   [Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname
   public v1
   ```

2. Configure the SNMP NMS:
   - Specify SNMPv1.
   - Create read-only community **public**, and create read and write community **private**.
   - Set the timeout timer and maximum number of retries as needed.

   For information about configuring the NMS, see the NMS manual.

   NOTE:

   The SNMP settings on the agent and the NMS must match.

Verifying the configuration

Try to get the MTU value of NULL0 interface from the agent. The attempt succeeds.

```
Send request to 1.1.1.1/161 ...
Protocol version: SNMPv1
Operation: Get
Request binding:
1: 1.3.6.1.2.1.2.2.1.4.135471
Response binding:
1: Oid=ifMtu.135471 Syntax=INT Value=1500
Get finished
```

Use a wrong community name to get the value of a MIB node on the agent. You can see an authentication failure trap on the NMS.

```
1.1.1.1/2934 V1 Trap = authenticationFailure
SNMP Version = V1
Community = public
Command = Trap
Enterprise = 1.3.6.1.4.1.43.1.16.4.3.50
GenericID = 4
SpecificID = 0
Time Stamp = 8:35:25.68
```

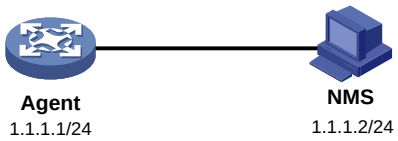
SNMPv3 configuration example

Network requirements

As shown in Figure 4, the NMS (1.1.1.2/24) uses SNMPv3 to monitor and manage the interface status of the agent (1.1.1.1/24). The agent automatically sends notifications to report events to the NMS. The default UDP port 162 is used for SNMP notifications.

The NMS and the agent perform authentication when they establish an SNMP session. The authentication algorithm is SHA-1 and the authentication key is **123456TESTauth&!**. The NMS and the agent also encrypt the SNMP packets between them by using the AES algorithm and the privacy key **123456TESTencr&!**.

Figure 4 Network diagram



Configuration procedure

Configuring SNMPv3 in RBAC mode

1. Configure the agent:

   # Assign IP address **1.1.1.1/24** to the agent and make sure the agent and the NMS can reach each other. (Details not shown.)

   # Create user role **test**, and assign **test** read-only access to the objects under the **snmpMIB** node (OID: 1.3.6.1.6.3.1), including the **linkUp** and **linkDown** objects.

   ```
   <Agent> system-view
   [Agent] role name test
   [Agent-role-test] rule 1 permit read oid 1.3.6.1.6.3.1
   ```

   # Assign user role **test** read-only access to the **system** node (OID: 1.3.6.1.2.1.1) and read-write access to the **interfaces** node (OID: 1.3.6.1.2.1.2).

   ```
   [Agent-role-test] rule 2 permit read oid 1.3.6.1.2.1.1
   [Agent-role-test] rule 3 permit read write oid 1.3.6.1.2.1.2
   [Agent-role-test] quit
   ```

   # Create SNMPv3 user **RBACtest**. Assign user role **test** to **RBACtest.** Set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and privacy key to **123456TESTencr&!**.

```
[Agent] snmp-agent usm-user v3 RBACtest user-role test simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

Enable notifications on the agent. Specify the NMS at 1.1.1.2 as the notification destination, and **RBACtest** as the username.

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname
RBACtest v3 privacy
```

2. Configure the NMS:

- Specify SNMPv3.
- Create SNMPv3 user **RBACtest**.
- Enable both authentication and privacy functions.
- Use SHA-1 for authentication and AES for encryption.
- Set the authentication key to **123456TESTauth&!** and the privacy key to **123456TESTencr&!**.
- Set the timeout timer and maximum number of retries.

For information about configuring the NMS, see the NMS manual.

NOTE:

The SNMP settings on the agent and the NMS must match.

Configuring SNMPv3 in VACM mode

1. Configure the agent:

Assign IP address 1.1.1.1/24 to the agent, and make sure the agent and the NMS can reach each other. (Details not shown.)

Create SNMPv3 group **managev3group** and assign **managev3group** read-only access to the objects under the **snmpMIB** node (OID: 1.3.6.1.6.3.1) in the **test** view, including the **linkUp** and **linkDown** objects.

```
<Agent> system-view
[Agent] undo snmp-agent mib-view ViewDefault
[Agent] snmp-agent mib-view included test snmpMIB
[Agent] snmp-agent group v3 managev3group privacy read-view test
```

Assign SNMPv3 group **managev3group** read-write access to the objects under the **system** node (OID: 1.3.6.1.2.1.1) and **interfaces** node (OID: 1.3.6.1.2.1.2) in the **test** view.

```
[Agent] snmp-agent mib-view included test 1.3.6.1.2.1.1
[Agent] snmp-agent mib-view included test 1.3.6.1.2.1.2
[Agent] snmp-agent group v3 managev3group privacy read-view test write-view test
```

Add user VACMtest to SNMPv3 group **managev3group**, and set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and privacy key to **123456TESTencr&!**.

```
[Agent] snmp-agent usm-user v3 VACMtest managev3group simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

Enable notifications on the agent. Specify the NMS at 1.1.1.2 as the trap destination, and **VACMtest** as the username.

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params VACMtest v3
privacy
```

2. Configure the SNMP NMS:
   - Specify SNMPv3.
   - Create SNMPv3 user VACMtest.
   - Enable both authentication and privacy functions.
   - Use SHA-1 for authentication and AES for encryption.
   - Set the authentication key to **123456TESTauth&!** and the privacy key to **123456TESTencr&!**.
   - Set the timeout timer and maximum number of retries.

   For information about configuring the NMS, see the NMS manual.

NOTE:

The SNMP settings on the agent and the NMS must match.

Verifying the configuration

- Use username **RBACtest** to access the agent.

  # Retrieve the value of the **sysName** node. The value **Agent** is returned.

  # Set the value for the **sysName** node to **Sysname**. The operation fails because the NMS does not have write access to the node.

  # Shut down or bring up an interface on the agent. The NMS receives linkUP (OID: 1.3.6.1.6.3.1.1.5.4) or linkDown (OID: 1.3.6.1.6.3.1.1.5.3) notifications.

- Use username **VACMtest** to access the agent.

  # Retrieve the value of the **sysName** node. The value **Agent** is returned.

  # Set the value for the **sysName** node to **Sysname**. The operation succeeds.

  # Shut down or bring up an interface on the agent. The NMS receives **linkUP** (OID: 1.3.6.1.6.3.1.1.5.4) or **linkDown** (OID: 1.3.6.1.6.3.1.1.5.3) notifications.