Contents

1 Configuring SNMP

1.1 Introduction

1.1.1 Overview

The Simple Network Management Protocol (SNMP) is used for network monitoring and management. Because many vendors support SNMP, SNMP has become a network management standard and applies to the interconnected environment of systems of multiple vendors. By using SNMP, the network administrator can implement information query for network nodes, network configuration, fault locating, and capacity planning.

1.1.2 SNMP Versions

- SNMPv1

  SNMPv1 is the first official version of SNMP and is defined in RFC1157. Based on community names, SNMPv1 has simple structure of management information (SMI) and simple management information base (MIB) and lower security.

- SNMPv2C

  SNMPv2 is a community-based SNMP management architecture and is defined in RFC1901. SNMPv2 is compatible with SNMPv1. Compared with SNMPv1, SNMPv2 has two more protocol operations Get-Bulk and Inform and supports more data types and error code information.

- SNMPv3

  SNMPv3 defines security extension capability and provides the following security features by identifying and encrypting data.

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

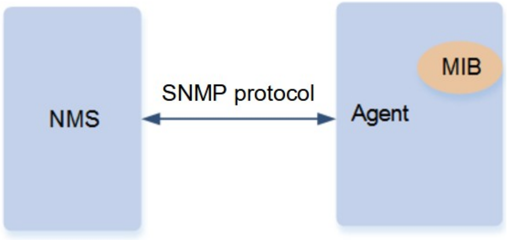
1.1.3 Principles

1. Basic Concepts

The SNMP management system has the following components:

- SNMP network manager
- SNMP agent
- MIB

Figure 1-1Relationship Between the NMS and Network Management Agent



- SNMP network manager

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

- SNMP agent

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

- MIB

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

- Operation types

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

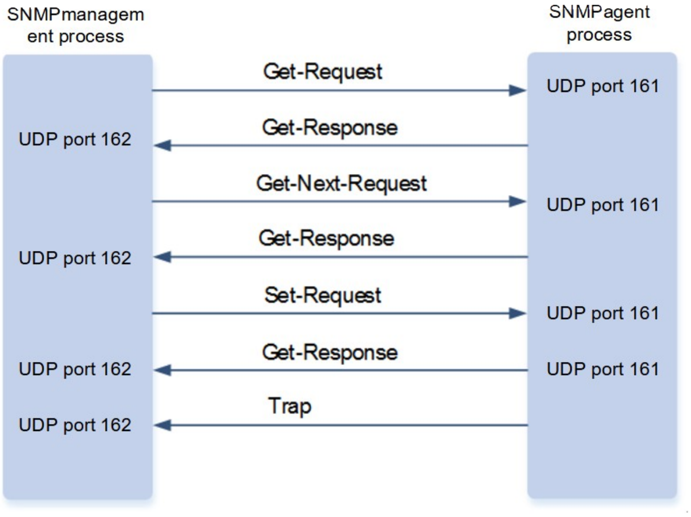
  - Get-Request: The NMS extracts one or more parameter values from the agent.
  - Get-Next-Request: The NMS extracts the parameter value next to one or more parameters from the agent.
  - Get-Bulk: The NMS extracts a batch of parameter values from the agent.
  - Set-Request: The NMS sets one or more parameter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

  The first four packets are sent by the NMS to the agent and the last two packets are sent by the agent to the NMS. The first three operations of the NMS and the response operations of the agent are based on UDP port 161. The Trap operation performed by the agent is based on UDP port 162. For details, see Figure 1-2.

⚠ **Caution**

SNMPv1 does not support the Get-Bulk operation.

Figure 1-2SNMP Packet Interaction



2. Basic SNMP Functions

SNMP interaction is response interaction (for interaction of packets, see Figure 1-2). The NMS actively sends requests to the agent, including Get-request, Get-next-request, Get-bulk, and Set-request. The agent receives the requests, completes operations, and returns a Get-response. Sometimes, the agent actively sends a Trap message and an Inform message to the NMS. The NMS does not need to respond to the Trap message but needs to return an Inform-response to the agent. Otherwise, the agent re-sends the Inform message.

3. Principles of SNMPv1 and SNMPv2C

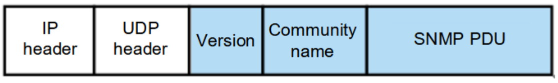
SNMPv1 and SNMPv2C adopt the community-based security architecture. The administrator who can perform operations on the MIB of the agent is limited by defining the host address and authentication name (community string).

SNMPv1 and SNMPv2 determine whether the administrator has the right to use MIB objects by using the authentication name. To be able to manage devices, the NMS must ensure that its authentication name is the same as an authentication name defined in devices.

In SNMPv2C, the Get-bulk operation enables more detailed error message types to be returned to the NMS. The Get-bulk operation allows all information from a table or lots of data to be obtained at a time, so as to reduce the request-response times. The enhanced error handling capabilities of SNMPv2C include extension of error codes to differentiate error types. In SNMPv1, however, only one error code is provided for the errors. In SNMPv2C, the error codes can be used to differentiate error types. Because management workstations on the network may support SNMPv1 and SNMPv2C at the same time, the SNMP agent must be able to identify SNMPv1 packets and SNMPv2C packets and return packets of the corresponding versions.

SNMPv1 and SNMPv2c packets are composed of version, community name, and SNMP protocol data unit (PDU). Figure 1-1 shows the structure of the packets.

Figure 1-1Structure of SNMPv1 and SNMPv2c Packets



- The main fields in packets are as follows:
  - Version: Indicates an SNMP version. For SNMPv1 packets, the corresponding field value is 0. For SNMPv2c packets, the field value is 1.
  - Community name: It is used for authentication between the agent and NMS. The field value is a string that can be customized. The community names include readable and writable community names. During Get-Request and Get-Next-Request operations, a readable community name is used for authentication. During Set operations, a writable community name is used for authentication.
  - SNMP PDU: Includes information such as PDU type, request identifier, and variable binding list. SNMPv1 PDUs include GetRequest PDU, GetNextRequest PDU, SetRequest PDU, Response PDU, and Trap PDU. Compared with SNMPv1, SNMPv2c has GetBulkRequest PDU and InformRequest PDU.
- Security

  An authentication name has the following attributes:
  - Read-only: Provides the read permission of all MIB variables for authorized management workstations.
  - Read-write: Provides the read/write permission of all MIB variables for authorized management workstations.

4. Principles of SNMPv3

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

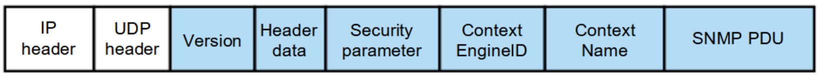
The NMS and SNMP agent are SNMP entities. In the SNMPv3 architecture, SNMP entities consist of the SNMP engine and SNMP applications. The SNMP engine is used to send and receive messages, identify and encrypt information, and control access to managed objects. SNMP applications refer to internal applications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

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

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

SNMPv3 defines a new packet format, which is shown in Figure 1-1.

Figure 1-1Structure of SNMPv3 Packets



- The main fields in SNMP packets are as follows:
  - Version: Indicates an SNMP version. For SNMPv3 packets, the field value is 2.
  - Header data: Mainly includes description information such as the maximum message size supported by the message sender and the security model of the message.
  - Security parameter: Includes such security information as SNMP engine-related information, username, authentication parameter, and encryption parameter.
  - Context EngineID: A unique identifier of SNMP. This field and the PDU type decide the application to which the packets are sent.
  - Context name: Decides the MIB view of the managed devices based on the Context EngineID.
  - SNMP PDU: Includes information such as PDU type, request identifier, and variable binding list. SNMPv3 PDUs include GetRequest PDU, GetNextRequest PDU, SetRequest PDU, Response PDU, Trap PDU, GetBulkRequest PDU, and InformRequest PDU.
- Security

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

Table 1-1Security Models and Security Levels of SNMPv1 and SNMPv2C

Security Model	Security Level	Authentication	Encryption
SNMPv1	noAuthNoPriv	Authentication name	N/A
SNMPv2c	noAuthNoPriv	Authentication name	N/A

Table 1-2Security Model and Security Level of SNMPv3

Security Model	Security Level	Authentica-tion	Encryp-tion	Description
SNMPv3	noAuthNoPriv	Username	N/A	Data validity is confirmed through username.
SNMPv3	authNoPriv	MD5 or SHA	N/A	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA is provided.
SNMPv3	authPriv	MD5 or SHA	DES	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA and the data encryption mechanism based on CBC-DES are provided.

- Engine ID

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

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

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

1.1.4 Protocols and Standards

- RFC 1157, Simple Network Management Protocol (SNMP)
- RFC 1901, Introduction to Community-based SNMPv2
- RFC 2578, Structure of Management Information Version 2 (SMIv2)
- RFC 2579, Textual Conventions for SMIv2
- RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413, Simple Network Management Protocol (SNMP) Applications
- RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

RFC 3419, Textual Conventions for Transport Addresses

1.2 Configuration Task Summary

SNMP configuration includes the following tasks:

(1) Configuring Basic SNMP Features

(2) (Optional) Configuring the Trap Function

(3) (Optional) Configuring the Agent Shielding Function

(4) (Optional) Configuring SNMP Control Parameters

1.3 Configuring Basic SNMP Features

1.3.1 Overview

After the basic SNMP function is configured, users can access the agent through the NMS.

1.3.2 Restrictions and Guidelines

- When an authentication name is configured, the default access permission is read-only if no access permission is specified.
- When the view-based access control model (VACM) is used, an SNMP user group must be configured. By associating users with a group and associating the group with a view, you can ensure that the users in the group have the same access permission. In this way, you can determine whether managed objects associated with an operation are in the allowable range of a view. Only managed objects in the range of a view can be accessed.
- When you configure users in SNMPv3, you can specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (DES at present), and encryption password.
- After the SNMP attack prevention and detection function is configured, the corresponding action can be taken after authentication fails consecutively.
- The permanently forbidden source IP addresses can be authenticated for access again only after the administrator manually unlocks the IP addresses. The source IP addresses that are forbidden in a period of time can be authenticated for access again after the period expires or after the administrator manually unlocks the IP addresses.
- By default, password dictionary check is not performed for communities and users. If community names and usernames are too simple and are easily cracked, enable password dictionary check for the communities and users. The configuration must be used with the **password policy** command in the global configuration mode.
- The SNMP logging function records the Get, Get-Next, and Set operations performed by the NMS on the SNMP Agent. When the Get and Get-Next operations are performed, the agent records the IP address of the NMS user, operation type, and OID of the operation node. When the Set operation is performed, the agent records the IP address of the NMS user, operation type, OID of the operation node, and set value. These logs are sent to the information center of devices. The level of these logs is informational, that is, the logs are used as prompt information of devices. A large number of logs will affect device performance. In normal conditions, you are advised to disable the SNMP logging function.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure an SNMP view.

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

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

The default view allows access to all MIB objects.

(4) (Optional) Configure an SNMP user group.

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

No user group is configured by default.

(5) Configure an authentication name and access permission.

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

No authentication name is configured and the access permission of all communities is read-only by default.

When SNMPv1 and SNMPv2C are used to manage network devices, an authentication name must be configured on the agent.

(6) Configure an SNMP user.

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

No SNMP user is configured by default.

When SNMPv3 is used to manage network devices, a user must be configured.

(7) (Optional) Enable the agent function.

enable service snmp-agent

The SNMP agent function is enabled by default.

(8) (Optional) Enable the SNMP attack prevention and detection function.

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

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

(9) (Optional) Configure password dictionary check for communities and users.

snmp-server enable secret-dictionary-check

Password dictionary check is not configured for communities and users by default.

(10) (Optional) Configure the SNMP logging function to record the Get, Get-Next, and Set Operations performed by the NMS on the SNMP Agent.

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

By default, the SNMP logging function is disabled.

1.4 Configuring the Trap Function

1.4.1 Overview

After the Trap function is configured, the agent actively sends Trap messages to the NMS.

1.4.2 Restrictions and Guidelines

- The host address of the NMS must be configured when the agent actively sends Trap messages to the NMS. That is, the **snmp-server host** command is used with the **snmp-server enable traps** command in the global configuration mode.
- Multiple SNMP hosts can be configured to receive Trap messages. A host can combine different types of Trap messages, ports, and VRF forwarding tables. If a host is configured with the same port and VRF in multiple configurations, the last configuration is combined with the previous configurations. To send different Trap messages to the same host, configure different types of Trap messages each time. These configurations are finally combined.
- The system reboot notification function must be enabled on the agent so that the RGOS system sends Trap messages to the NMS to notify system reboot before reloading or rebooting of the device.
- After the Link Trap message sending function is enabled on an interface, the SNMP sends a Link Trap message if the link status on the interface changes. Otherwise, the SNMP does not send the message.
- By default, the IP address of an interface that sends SNMP packets is used as the source address of the SNMP packets. If you want to use a fixed local IP address as the source address to facilitate management, configure the source address for sending Trap messages on the agent.
- The **snmp-server trap-format private** command can be run to include private fields in Trap messages. The supported private field is the alarm generation time. For the specific data types and data ranges of the fields, see the Orion_B26Q-TRAP-FORMAT-MIB.mib file.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure an NMS host address.

snmp-server host [**oob**] { *ipv4-addrress* | **ipv6** *ipv6-address* | **domain** *domain-name* } [**vrf** *vrf-name*] [**informs** | **traps**] [**version** { { **1** | **2c** } [**0** | **7**] *community* | **3** { **auth** | **noauth** | **priv** } *username* }] [**udp-port** *port-number*] [**via** *mgmt-name*] [*notification-type*] No SNMP host address is configured by default.

(4) (Optional) Enable the agent to actively send Trap messages to the NMS.

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

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

(5) (Optional) Enable the Link Trap message sending function on an interface.

snmp-server link-status

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

(6) (Optional) Configure the system reboot trap sending function.

snmp-server system-shutdown

The SNMP system reboot notification function is disabled by default.

(7) (Optional) Configure a source address for Trap messages.

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

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

(8) (Optional) Include private fields in sent Trap messages.

snmp-server trap-format private

SNMP Trap messages do not include private fields by default.

(9) Configure Inform message sending attempts and timeout time.

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

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

1.5 Configuring the Agent Shielding Function

1.5.1 Overview

After the agent shielding function is enabled, the port access frequency and network attack probability are reduced.

1.5.2 Restrictions and Guidelines

The SNMP agent function is disabled by default. When SNMP agent parameters (for example, NMS host address, authentication name, and access permission) are configured, the SNMP agent service is automatically enabled. The **enable service snmp-agent** command must be run so that the SNMP agent service can take effect. If the SNMP agent service is disabled or the **enable service snmp-agent** command is not run, the SNMP agent service does not take effect. The **no snmp-server** command is used to shield all SNMP agent service configurations. In this case, running the **show running-config** command will not display the configurations. The configurations can be restored after the SNMP agent service is enabled again. The **no enable service snmp-agent** command is used to disable the SNMP agent service. In this case, the SNMP agent function is disabled and packets and trap messages are not sent and received, but the SNMP agent configurations are not shielded.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SNMP agent shielding function.

no snmp-server

The SNMP agent function is enabled by default.

(4) Disable the SNMP agent function of a device.

no enable service snmp-agent

The SNMP agent function is enabled by default.

1.6 Configuring SNMP Control Parameters

1.6.1 Overview

After basic parameters such as device contact mode, device location, serial number, and Trap message sending are configured, the NMS can obtain information such as the contact person and physical location of the device by accessing the parameters.

1.6.2 Restrictions and Guidelines

- When too many SNMP request packets cause SUMP tasks to occupy a large CPU space, you can configure SNMP traffic control to limit the number of request packets processed per second in each SNMP task to control the CPU usage.
- SNMP contains three versions: v1, v2C, and v3. If only a specified version is used for MIB interaction management in a user scenario, you can disable unused SNMP versions by running the **no snmp-server enable version** [**v1** | **v2c** | **v3**] command.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the contact mode of the system.

snmp-server contact *contact-text*

The contact mode of the system is empty by default.

(4) Configure the system location.

snmp-server location *location-text*

The system location is empty by default.

(5) Configure the system serial number.

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

The default system serial number is 60FF60.

In general, the device serial number is used as the SNMP serial number to facilitate identification of the device.

(6) Configure NE information of a device.

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

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

(7) Configure the maximum packet length of the SNMP agent.

snmp-server packetsize *packetsize*

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

(8) Configure the UDP port ID of the SNMP service.

snmp-server udp-port *port-number*

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

(9) Configure the source port of the device on which the SNMP service is deployed.

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

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

(10) Configure the queue length of Trap messages.

snmp-server queue-length *queue-length*

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

(11) Configure the sending interval of Trap messages.

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

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

(12) Configure SNMP traffic control.

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

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

(13) Configure the status of SNMP versions.

no snmp-server enable version [**v1** | **v2c** | **v3**]

All SNMP versions are enabled by default.

1.7 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

⚠ **Caution**

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1Monitoring

Command	Purpose
clear snmp locked-ip [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]	Clears the list of source IP addresses that are locked after authentication fails consecutively.
show snmp [**group** | **host** | **locked-ip** | **process-mib-time** | **mib** | **user** | **version** | **view**]	Displays the SNMP status information.

1.8 Configuration Examples

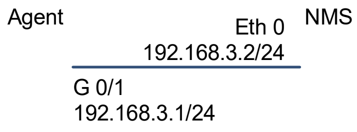
1.8.1 Configuring Basic SNMPv2c Function

1. Requirements

Network devices are managed and monitored through the SNMP network manager, as shown in Figure 1-1.

2. Topology

Figure 1-1Topology of Basic SNMPv2 Function



3. Procedure

Enable the SNMP agent function.

```
Orion_B26Q> enable
Orion_B26Q# configure terminal
Orion_B26Q(config)# enable service snmp-agent
```

Configure a read/write community with the name comm_v1.

```
Orion_B26Q(config)# snmp-server community comm_v2 rw
```

Configure an IP address for the agent. Set the address of GigabitEthernet 0/1 to 192.168.3.1/24.

```
Orion_B26Q(config)# interface gigabitEthernet 0/1
Orion_B26Q(config-if-gigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
Orion_B26Q(config-if-gigabitEthernet 0/1)# exit
```

4. Verification

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Orion_B26Q# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **show service** command to check whether the SNMP agent function is enabled.

```
Orion_B26Q# show service
snmp-agent    : enabled
ssh-server    : disabled
telnet-server : enabled
```

5. Configuration Files

Agent configuration file

```
interface GigabitEthernet 0/1
```

```
 ip address 192.168.2.1 255.255.255.0
!
snmp-server community comm_v2 rw
!
end
```

1.8.2 Configuring Basic SNMPv3 Function

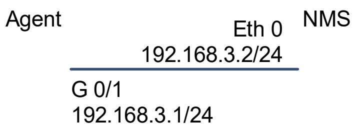
1. Requirements

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

- The management workstation (NMS) manages network devices (agents) based on the authentication and encryption mode of users.
- Network devices can control the operation permission of users to access MIB objects.
- Network devices can actively send authentication and encryption messages to the NMS.

2. Topology

Figure 1-1Topology of Basic SNMPv3 Function



3. Notes

- Configure an MIB view and an SNMP user group.
- Configure an SNMP user.
- Configure an SNMP host.
- Configure an IP address for the agent.

4. Procedure

Create an MIB view with the name view1, which includes the associated MIB object 1.3.6.1.2.1.1. Create an MIB view with the name view2, which includes the associated MIB object 1.3.6.1.2.1.1.4.0.

```
Orion_B26Q> enable
Orion_B26Q# configure terminal
Orion_B26Q(config)# snmp-server view view1 1.3.6.1.2.1.1 include
```

Create an MIB view with the name view2, which includes the associated MIB object 1.3.6.1.2.1.1.4.0.

```
Orion_B26Q(config)# snmp-server view view2 1.3.6.1.2.1.1.4.0 include
```

Create an SNMP user group with the name g1, select v3 as the version, and configure an authentication and encryption mode with the security level priv. Configure view1 as a readable view and view2 as a writable view.

```
Orion_B26Q(config)# snmp-server group g1 v3 priv read view1 write view2
```

Configure an SNMP user. Create a user with the name **user1** under the group g1, select v3 as the version, and set the authentication mode to md5, authentication password to 123, encryption mode to DES56, and encryption password to 321.

```
Orion_B26Q(config)# snmp-server user user1 g1 v3 auth md5 123 priv des56 321
```

Configure the SNMP host: Set the host address to 192.168.3.2, and the version to v3, configure an authentication and encryption mode with the security level priv, and associate the username **user1**.

```
Orion_B26Q(config)# snmp-server host 192.168.3.2 traps version 3 priv user1
```

Enable the agent to actively send Trap messages to the NMS.

```
Orion_B26Q(config)# snmp-server enable traps
```

Configure an IP address for the agent. Set the address of GigabitEthernet 0/1 to 192.168.3.1/24.

```
Orion_B26Q(config)# interface gigabitEthernet 0/1
Orion_B26Q(config-if-gigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
Orion_B26Q(config-if-gigabitEthernet 0/1)# exit
```

5. Verification

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Orion_B26Q# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

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

```
Orion_B26Q# show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent     active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

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

```
Orion_B26Q# show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

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

```
Orion_B26Q# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
```

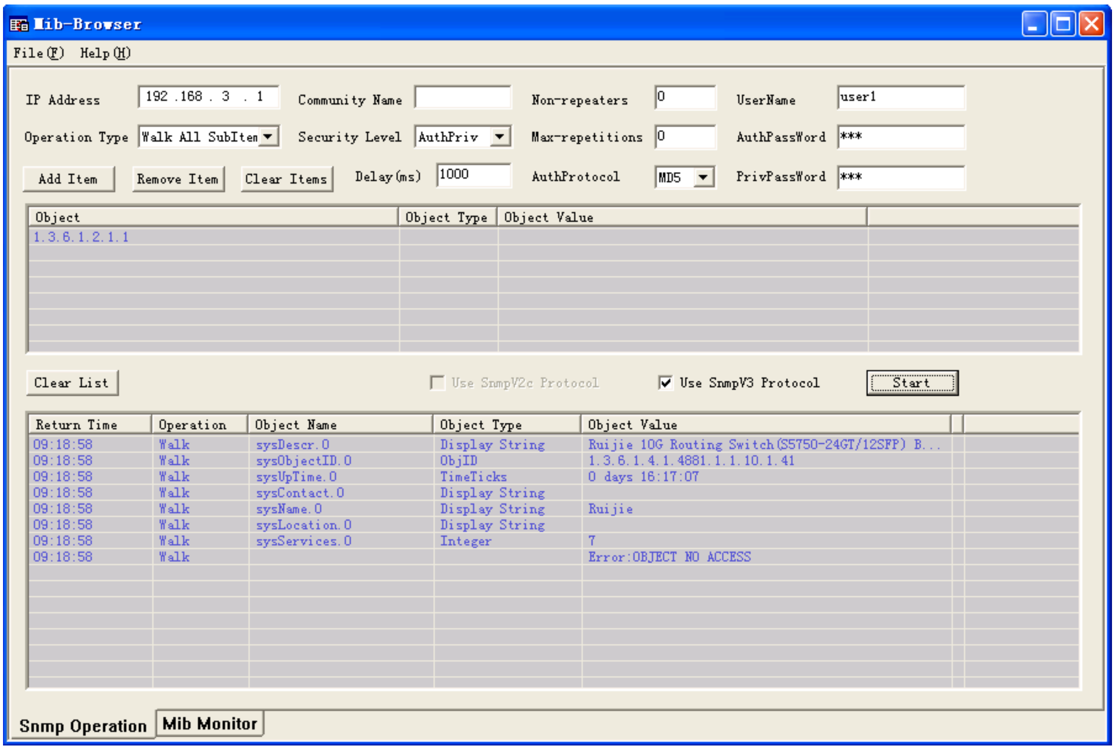
```
writeview: view2
notifyview:
```

Run the **show snmp host** command to display the host information configured by the user.

```
Orion_B26Q# show snmp host
Notification host: 192.168.3.2
udp-port: 162
type: trap
user: user1
security model: v3 authPriv
```

Install the MIB browser query. Enter the IP address 192.168.3.1 in IP Address and **user1** in UserName, select AuthPriv for Security Level, enter 123 in AuthPassWord, select MD5 for AuthProtocol, and enter 321 in PrivPassWord. Click **Add Item** and select an MIB management unit to be queried, for example, System. Click **Start** to query the MIB of the network devices. The query results are displayed in the lowest pane of the dialog box, as shown in Figure 1-1.

Figure 1-1MIB-browser Query Example



IP Address: 192 .168 . 3 . 1
Community Name:
Non-repeaters: 0
UserName: user1
Operation Type: Walk All SubIten
Security Level: AuthPriv
Max-repetitions: 0
AuthPassWord: ***
Delay(ms): 1000
AuthProtocol: MD5
PrivPassWord: ***

Object	Object Type	Object Value
1.3.6.1.2.1.1		

□ Use SnmpV2c Protocol ☑ Use SnmpV3 Protocol

Return Time	Operation	Object Name	Object Type	Object Value
09:18:58	Walk	sysDescr.0	Display String	Ruijie 10G Routing Switch(S5750-24GT/12SFP) B...
09:18:58	Walk	sysObjectID.0	ObjID	1.3.6.1.4.1.4881.1.1.10.1.41
09:18:58	Walk	sysUpTime.0	TimeTicks	0 days 16:17:07
09:18:58	Walk	sysContact.0	Display String	
09:18:58	Walk	sysName.0	Display String	Ruijie
09:18:58	Walk	sysLocation.0	Display String	
09:18:58	Walk	sysServices.0	Integer	7
09:18:58	Walk			Error:OBJECT NO ACCESS

6. Configuration Files

Agent configuration file

```
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5 DE8E9D1158A057A69EF73D1C12C51CC5
priv des56 C767B705F9B261E6D359D4BFBDAF9CF4
```

```
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
snmp-server enable traps
!
end
```

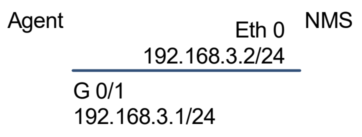
1.8.3 Configuring Basic Trap Function

1. **Requirements**

The network management station (NMS) manages network devices (agents) based on the community authentication mode, and the network devices can actively send messages to the network management station.

2. **Topology**

Figure 1-1Topology of Basic Trap Function



3. **Procedure**

Set the agent and NMS to be reachable via L3 routes, and set the IP address of GigabitEthernet 0/1 on the agent to 192.168.3.1.

```
Orion_B26Q> enable
Orion_B26Q# configure terminal
Orion_B26Q(config)#interface gigabitEthernet 0/1
Orion_B26Q(config-if-GigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Orion_B26Q(config-if-GigabitEthernet 0/1)#exit
```

Set the SNMP host address to 192.168.3.2, the message format to Version 2c, and the authentication name to user1. Enable the agent to actively send Trap messages to the NMS.

```
Orion_B26Q> enable
Orion_B26Q# configure terminal
Orion_B26Q(config)# snmp-server host 192.168.3.2 traps version 2c user1
Orion_B26Q(config)# snmp-server enable traps
```

4. **Verification**

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Orion_B26Q# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

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

```
Orion_B26Q# show snmp
Chassis: 1234567890
0 SNMP packets input
        0 Bad SNMP version errors
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
0 SNMP packets output
        0 Too big errors (Maximum packet size 1472)
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 Response PDUs
        0 Trap PDUs
SNMP global trap: enabled
SNMP logging: disabled
SNMP agent: enabled
```

5. Configuration Files

Agent configuration file

```
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
!
end
```