

Configuring SNMP & RMON

CHAPTERS

1. SNMP
2. SNMP Configurations
3. Notification Configurations
4. RMON
5. RMON Configurations
6. Configuration Example
7. Appendix: Default Parameters

✔ This guide applies to:

T1500G-8T v2 or above, T1500G-10PS v2 or above, T1500G-10MPS v2 or above, T1500-28PCT v3 or above, T1600G-18TS v2 or above, T1600G-28TS v3 or above, T1600G-28PS v3 or above, T1600G-52TS v3 or above, T1600G-52PS v3 or above, T1700X-16TS v3 or above, T1700G-28TQ v3 or above, T2500G-10TS v2 or above, T2600G-18TS v2 or above, T2600G-28TS v3 or above, T2600G-28MPS v3 or above, T2600G-28SQ v1 or above, T2600G-52TS v3 or above.

1 SNMP

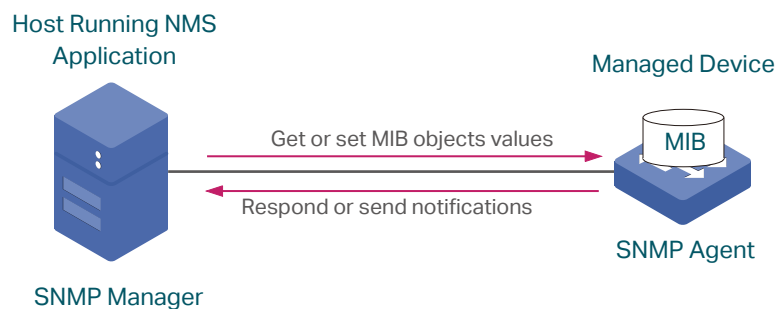
1.1 Overview

SNMP (Simple Network Management Protocol) is a standard network management protocol, widely used on TCP/IP networks. It facilitates device management using NMS (Network Management System) applications. With SNMP, network managers can view or modify the information of network devices, and timely troubleshoot according to notifications sent by those devices.

As the following figure shows, the SNMP system consists of an SNMP manager, an SNMP agent, and a MIB (Management Information Base).

The SNMP manager is a host that runs NMS applications. The agent and MIB reside on the managed device, such as the switch, router, host or printer. By configuring SNMP on the switch, you define the relationship between the manager and the agent.

Figure 1-1 SNMP System



1.2 Basic Concepts

The following basic concepts of SNMP will be introduced: SNMP manager, SNMP agent, MIB (Management Information Base), SNMP entity, SNMP engine, Notification types and SNMP version.

SNMP Manager

The SNMP manager uses SNMP to monitor and control SNMP agents, providing a friendly management interface for the administrator to manage network devices conveniently.

It can get values of MIB objects from an agent or set values for them. Also, it receives notifications from the agents so as to learn the condition of the network.

SNMP Agent

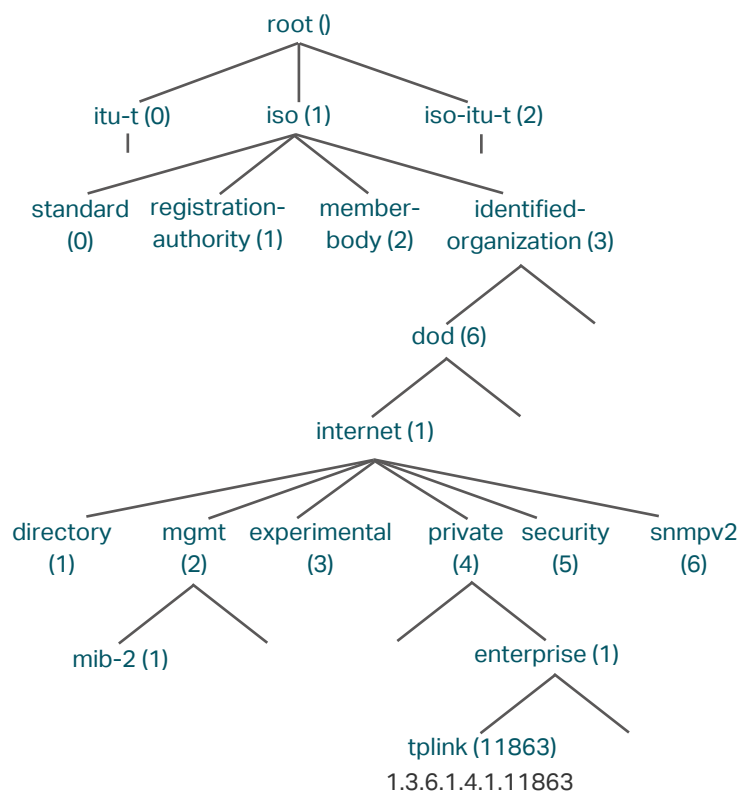
An SNMP agent is a process running on the managed device. It contains MIB objects whose values can be requested or set by the SNMP manager. An agent can send unsolicited trap messages to notify the SNMP manager that a significant event has occurred on the agent.

MIB

A MIB is a collection of managed objects that is organized hierarchically. The objects define the attributes of the managed device, including the names, status, access rights, and data types. Each object can be addressed through an object identifier (OID).

As the following figure shows, the MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. The top-level MIB object IDs belong to different standard organizations, while lower-level object IDs are allocated by associated organizations. Vendors can define private branches that include managed objects for their own products.

Figure 1-2 MIB Tree



TP-Link switches provide private MIBs that can be identified by the OID 1.3.6.1.4.1.11863. The MIB file can be found on the provided CD or in the download center of our official website: <https://www.tp-link.com/download-center.html>.

Also, TP-Link switches support the following public MIBs:

- LLDP.mib

- LLDP-Ext-Dot1.mib
- LLDP-Ext-MED.mib
- RFC1213.mib
- RFC1493-Bridge.mib
- RFC1757-RMON.mib
- RFC2618-RADIUS-Auth-Client.mib
- RFC2620-RADIUS-Acc-Client.mib
- RFC2674-pBridge.mib
- RFC2674-qBridge.mib
- RFC2863-pBridge.mib
- RFC2925-Disman-Ping.mib
- RFC2925-Disman-Traceroute.mib

For detail information about the supported public MIBs, see [Supported Public MIBs for TP-Link Switches](#).

SNMP Entity

An SNMP entity is a device running the SNMP protocol. Both the SNMP manager and SNMP agent are SNMP entities.

SNMP Engine

An SNMP engine is a part of the SNMP entity. Every SNMP entity has one and only one engine. An SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine can be uniquely identified by an engine ID within an administrative domain. Since there is a one-to-one association between SNMP engines and SNMP entities, we can also use the engine ID to uniquely identify the SNMP entity within that administrative domain.

Notification Types

Notifications are messages that the switch sends to the NMS host when important events occur. Notifications facilitate the monitoring and management of the NMS. There are two types of notifications:

- **Trap:** When the NMS host receives a Trap message, it will not send a response to the switch. Thus the switch cannot tell whether a message is received or not, and the messages that are not received will not be resent.
- **Inform:** When the NMS host receives an Inform message, it sends a response to the switch. If the switch does not receive any response within the timeout interval, it will resend the Inform message. Therefore, Inform is more reliable than Trap.

SNMP Version

The device supports three SNMP versions with the security level from low to high: SNMPv1, SNMPv2c and SNMPv3. *Table 1-1* lists features supported by different SNMP versions, and *Table 1-2* shows corresponding application scenarios.

Table 1-1 Features Supported by Different SNMP Versions

Feature	SNMPv1	SNMPv2c	SNMPv3
Access Control	Based on SNMP Community and MIB View	Based on SNMP Community and MIB View	Based on SNMP User, Group, and MIB View
Authentication and Privacy	Based on Community Name	Based on Community Name	Supported authentication and privacy modes are as follows: Authentication: MD5/SHA Privacy: DES
Trap	Supported	Supported	Supported
Inform	Not supported	Supported	Supported

Table 1-2 Application Scenarios of Different Versions

Version	Application Scenario
SNMPv1	SNMPv1 is applicable to small-scale networks with simple networking, good stability and low security requirements, such as campus networks and small enterprise networks.
SNMPv2c	SNMPv2c is applicable to medium and large-scale networks with low security requirements (or are already secure enough like VPN networks) and heavy traffic. The added feature Inform helps to ensure that the notifications from the switch are received by the NMS host even when network congestion occurs.
SNMPv3	SNMPv3 is applicable to networks of various scales, particularly those that have high security requirements and require devices to be managed by authenticated administrators (such as when data needs to be transferred on public networks).

2 SNMP Configurations

To complete the SNMP configuration, choose an SNMP version according to network requirements and supportability of the NMS application, and then follow these steps:

- Choose SNMPv1 or SNMPv2c

- 1) Enable SNMP.
- 2) Create an SNMP view for managed objects.
- 3) Create a community, specify the accessible view and the corresponding access rights.

- Choose SNMPv3

- 1) Enable SNMP.
- 2) Create an SNMP view for managed objects.
- 3) Create an SNMP group, and specify the security level and accessible view.
- 4) Create SNMP users, and configure the authentication mode, privacy mode and corresponding passwords.

2.1 Using the GUI

2.1.1 Enabling SNMP

Choose the **MAINTENANCE > SNMP > Global Config** to load the following page.

Figure 2-1 Configuring Global Parameters

Follow these steps to configure SNMP globally:

- 1) In the **Global Config** section, enable SNMP and configure the local and remote engine ID.

SNMP	Enable or disable SNMP globally.
------	----------------------------------

Local Engine ID Set the engine ID of the local SNMP agent (the switch) with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. By default, the switch generates the engine ID using TP-Link’s enterprise number (80002e5703) and its own MAC address.

The local engine ID is a unique alphanumeric string used to identify the SNMP engine. As an SNMP agent contains only one SNMP engine, the local engine ID can uniquely identify the SNMP agent.

Remote Engine ID Set the engine ID of the remote SNMP manager with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. If no remote SNMP manager is needed, you can leave this field empty.

The remote engine ID is a unique alphanumeric string. It is used to identify the SNMP engine on the remote device that receives Inform messages from the switch.

2) Click **Apply**.

 **Note:**









In SNMPv3, changing the value of the SNMP engine ID has important side effects. A user’s password is converted to an MD5 or SHA security digest based on the password itself and the engine ID. If the value of local engine ID changes, the switch will automatically delete all SNMPv3 local users as their security digests become invalid. Similarly, all SNMPv3 remote users will be deleted if the value of remote engine ID changes.

2.1.2 Creating an SNMP View

An SNMP view is a subnet of a MIB. NMS manages MIB objects based on the view. The system has a default view named viewDefault. You can create a new one or edit the default view according to your needs.

Choose the menu **MAINTENANCE > SNMP > Global Config** to load the following page.

Figure 2-2 SNMP View Config

SNMP View Config					
<input type="checkbox"/>	Index	View Name	View Type	MIB Object ID	Operation
<input type="checkbox"/>	1	viewDefault	Include	1	 
<input type="checkbox"/>	2	viewDefault	Exclude	1.3.6.1.6.3.15	 
<input type="checkbox"/>	3	viewDefault	Exclude	1.3.6.1.6.3.16	 
<input type="checkbox"/>	4	viewDefault	Exclude	1.3.6.1.6.3.18	 
Total: 4					

Follow these steps to create an SNMP view:


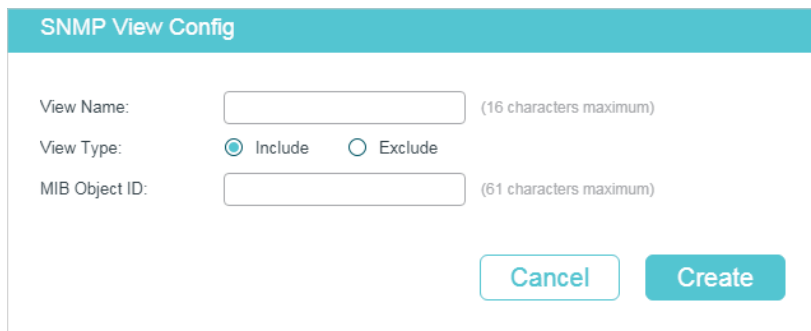
- 1) Click  **Add** to load the following page. Enter a view name, and specify the view type and a MIB object ID that is related to the view.

Figure 2-3 Creating an SNMP View



The image shows a web form titled "SNMP View Config". It contains three input fields: "View Name" with a text box and "(16 characters maximum)" label; "View Type" with two radio buttons, "Include" (selected) and "Exclude"; and "MIB Object ID" with a text box and "(61 characters maximum)" label. At the bottom right are two buttons: "Cancel" and "Create".

View Name Set the view name with 1 to 16 characters. A complete view consists of all MIB objects that have the same view name.

View Type Set the view to include or exclude the related MIB object.

Include: The NMS can view or manage the function indicated by the object.

Exclude: The NMS cannot view or manage the function indicated by the object.

MIB Object ID Enter a MIB Object ID to specify a specific function of the device. When a MIB Object ID is specified, all its child Object IDs are specified. For specific ID rules, refer to the device related MIBs.

2) Click **Create**.

2.1.3 Creating SNMP Communities (For SNMP v1/v2c)

Choose the menu **MAINTENANCE > SNMP > SNMP v1/v2c** and click  **Add** to load the following page.

Figure 2-4 Creating an SNMP Community



The image shows a web form titled "SNMP Community Config". It contains three input fields: "Community Name" with a text box and "(16 characters maximum)" label; "Access Mode" with two radio buttons, "Read Only" (selected) and "Read & Write"; and "MIB View" with a dropdown menu showing "viewDefault". At the bottom right are two buttons: "Cancel" and "Create".

Follow these steps to create an SNMP community:

1) Set the community name, access rights and the related view.

Community Name Configure the community name. This community name is used like a password and the NMS can access the specified MIB objects of the switch using the same community name.

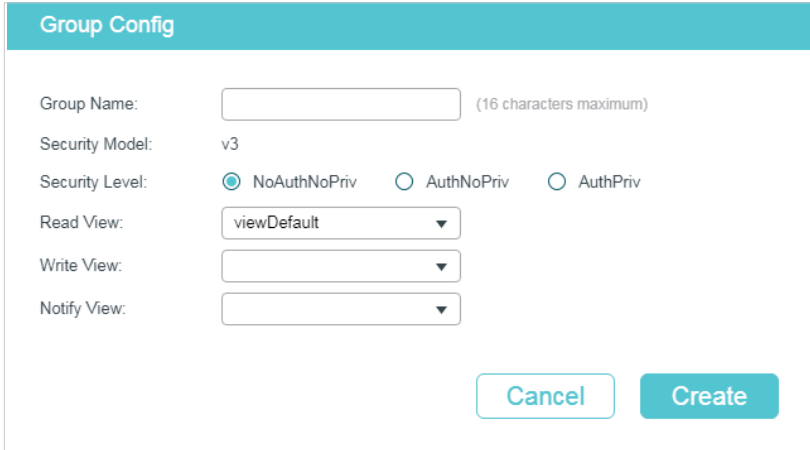
Access Mode	Specify the access right to the related view. Read Only: The NMS can view but not modify parameters of the specified view. Read & Write: The NMS can view and modify parameters of the specified view.
MIB View	Choose an SNMP view that allows the community to access.

2) Click **Create**.

2.1.4 Creating an SNMP Group (For SNMP v3)

Choose the menu **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** and click  Add to load the following page.

Figure 2-5 Creating an SNMP Group



Follow these steps to create an SNMP Group and configure related parameters.

1) Assign a name to the group, then set the security level and the read view, write view and notify view.

Group Name	Set the SNMP group name using 1 to 16 characters. The identifier of a group consists of a group name, security model and security level. Groups of the same identifier are recognized as being in the same group.
Security Model	Displays the security model. SNMPv3 uses v3, the most secure model.
Security Level	Set the security level for the SNMPv3 group. NoAuthNoPriv: No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them. AuthNoPriv: An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them. AuthPriv: An authentication algorithm and a privacy algorithm are applied to check and encrypt packets.

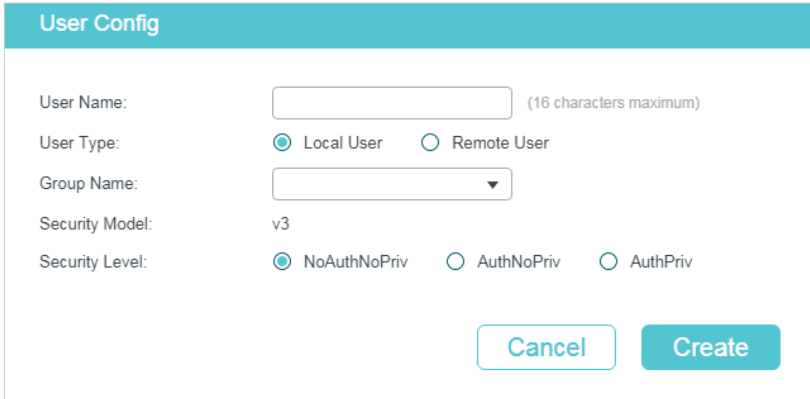
Read View	Choose a view to allow parameters to be viewed but not modified by the NMS. The view is necessary for any group.
Write View	Choose a view to allow parameters to be modified by the NMS. The view in Write View should also be added to Read View.
Notify View	Choose a view to allow it to send notifications to the NMS.

2) Click **Create**.

2.1.5 Creating SNMP Users (For SNMP v3)

Choose the menu **MAINTENANCE > SNMP > SNMP v3 > SNMP User** and click  Add to load the following page.

Figure 2-6 Creating an SNMP User



Follow these steps to create an SNMP user:

1) Specify the user name and user type as well as the group which the user belongs to. Then configure the security level.

User Name	Set the SNMP user name using 1 to 16 characters. For different entries, user names cannot be the same.
User Type	Choose a user type based on the location of the user. Local User: The user resides on the local engine, which is the SNMP agent of the switch. Remote User: The user resides on the NMS. Before configuring a remote user, you need to set the remote engine ID first. The remote engine ID and user password are used when computing the authentication and privacy digests.
Group Name	Choose the name of the group that the user belongs to. Users with the same Group Name, Security Model and Security Level will be in the same group.
Security Model	Displays the security model. SNMPv3 uses v3, the most secure model.

Security Level	<p>Set the security level. The security level from lowest to highest is: NoAuthNoPriv, AuthNoPriv, AuthPriv. The security level of the user should not be lower than the group it belongs to.</p> <p>NoAuthNoPriv: No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them.</p> <p>AuthNoPriv: An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them.</p> <p>AuthPriv: An authentication algorithm and a privacy algorithm are applied to check and encrypt packets.</p>
-----------------------	---

- 2) If you have chosen **AuthNoPriv** or **AuthPriv** as the security level, you need to set corresponding Authentication Mode or Privacy Mode. If not, skip this step.

Authentication Mode	<p>With AuthNoPriv or AuthPriv selected, configure the authentication mode and password for authentication. Two authentication modes are provided:</p> <p>MD5: Enable the HMAC-MD5 algorithm for authentication.</p> <p>SHA: Enable the SHA (Secure Hash Algorithm) algorithm for authentication. SHA algorithm is securer than MD5 algorithm.</p>
----------------------------	--

Authentication Password	Set the password for authentication.
--------------------------------	--------------------------------------

Privacy Mode	With AuthPriv selected, configure the privacy mode and password for encryption. The switch uses the DES (Data Encryption Standard) algorithm for encryption.
---------------------	--

Privacy Password	Set the password for encryption.
-------------------------	----------------------------------

- 3) Click **Create**.

2.2 Using the CLI

2.2.1 Enabling SNMP

Step 1	<p>configure</p> <p>Enter Global Configuration Mode.</p>
--------	---

Step 2	<p>snmp-server</p> <p>Enabling SNMP.</p>
--------	---

Step 3 **snmp-server engineID** {[*local local-engineID*] [*remote remote-engineID*]}

Configure the local engine ID and the remote engine ID.

local-engineID: Enter the engine ID of the local SNMP agent (the switch) with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. By default, the switch generates the engine ID using TP-Link's enterprise number (80002e5703) and its own MAC address.

The local engine ID is a unique alphanumeric string used to identify the SNMP engine. As an SNMP agent contains only one SNMP engine, the local engine ID can uniquely identify the SNMP agent.

remote-engineID: Enter the remote engine ID with 10 to 64 hexadecimal digits. A valid engine ID must contain an even number of characters. The remote engine ID is a unique alphanumeric string. It is used to identify the SNMP engine on the remote device that receives inform messages from switch.

Note:

In SNMPv3, changing the value of the SNMP engine ID has important side effects. A user's password is converted to an MD5 or SHA security digest based on the password itself and the engine ID. If the value of local engine ID changes, the switch will automatically delete all SNMPv3 local users as their security digests become invalid. Similarly, all SNMPv3 remote users will be deleted if the value of remote engine ID changes.

Step 4 **show snmp-server**

Displays the global settings of SNMP.

Step 5 **show snmp-server engineID**

Displays the engine ID of SNMP.

Step 6 **end**

Return to Privileged EXEC Mode.

Step 7 **copy running-config startup-config**

Save the settings in the configuration file.

The following example shows how to enable SNMP and set 123456789a as the remote engine ID:

Switch#configure

Switch(config)#snmp-server

Switch(config)#snmp-server engineID remote 123456789a

Switch(config)#show snmp-server

SNMP agent is enabled.

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 1500)
 - 0 No such name errors
 - 0 Bad value errors
 - 0 General errors
 - 0 Response PDUs
 - 0 Trap PDUs

Switch(config)#show snmp-server engineID

Local engine ID: 80002e5703000aeb13a23d

Remote engine ID: 123456789a

Switch(config)#end**Switch#copy running-config startup-config**

2.2.2 Creating an SNMP View

Specify the OID (Object Identifier) of the view to determine objects to be managed.

-
- | | |
|--------|----------------------------------|
| Step 1 | configure |
| | Enter Global Configuration Mode. |
-

Step 2	<p>snmp-server view <i>name mib-oid</i> {include exclude}</p> <p>Configure the view.</p> <p><i>name</i>: Enter a view name with 1 to 16 characters. You can create multiple entries with each associated to a MIB object. A complete view consists of all MIB objects that have the same view name.</p> <p><i>mib-oid</i>: Enter the MIB object ID with 1 to 61 characters. When a MIB Object ID is specified, all its child Object IDs are specified. For specific ID rules, refer to the device related MIBs.</p> <p><i>include exclude</i>: Specify a view type. Include indicates that objects of the view can be managed by the NMS, while exclude indicates that objects of the view cannot be managed by the NMS.</p>
Step 3	<p>show snmp-server view</p> <p>Displays the view table.</p>
Step 4	<p>end</p> <p>Return to Privileged EXEC Mode.</p>
Step 5	<p>copy running-config startup-config</p> <p>Save the settings in the configuration file.</p>

The following example shows how to set a view to allow the NMS to manage all function. Name the view as View:

Switch#configure

Switch(config)#snmp-server view View 1 include

Switch(config)#show snmp-server view

No.	View Name	Type	MOID
---	-----	-----	----
1	viewDefault	include	1
2	viewDefault	exclude	1.3.6.1.6.3.15
3	viewDefault	exclude	1.3.6.1.6.3.16
4	viewDefault	exclude	1.3.6.1.6.3.18
5	View	include	1

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Creating SNMP Communities (For SNMP v1/v2c)

For SNMPv1 and SNMPv2c the Community Name is used for authentication, functioning as the password.

Step 1	configure Enter Global Configuration Mode.
Step 2	snmp-server community <i>name</i> { read-only read-write } [<i>mib-view</i>] Configure the community. <i>name</i> : Enter a group name with 1 to 16 characters. <i>read-only</i> <i>read-write</i> : Choose an access permissions for the community. Read-only indicates that the NMS can view but cannot modify parameters of the view, while read-write indicates that the NMS can both view and modify. <i>mib-view</i> : Enter a view to allow it to be accessed by the community. The name contains 1 to 61 characters. The default view is viewDefault.
Step 3	show snmp-server community Displays community entries.
Step 4	end Return to Privileged EXEC Mode.
Step 5	copy running-config startup-config Save the settings in the configuration file.

The following example shows how to set an SNMP community. Name the community as the nms-monitor, and allow the NMS to view and modify parameters of View:

Switch#configure

Switch(config)#snmp-server community nms-monitor read-write View

Switch(config)#show snmp-server community

Index	Name	Type	MIB-View
-----	-----	-----	-----
1	nms-monitor	read-write	View

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Creating an SNMP Group (For SNMPv3)

Create an SNMP group and set user access control with read, write and notify views. Meanwhile, set the authentication and privacy modes to secure the communication between the NMS and managed devices.

Step 1	configure Enter Global Configuration Mode.
--------	--

Step 2	<p>snmp-server group <i>name</i> [smode v3] [slev {noAuthNoPriv authNoPriv authPriv}] [read <i>read-view</i>] [write <i>write-view</i>] [notify <i>notify-view</i>]</p> <p>Create an SNMP group.</p> <p><i>name</i>: Enter the group name with 1 to 16 characters. The identifier of a group consists of a group name, security model and security level. Groups of the same identifier are recognized as being in the same group.</p> <p>v3: Configure the security model for the group. v3 indicates SNMPv3, the most secure model.</p> <p>noAuthNoPriv authNoPriv authPriv: Choose a security level. The security levels are sorted from low to high, and the default is noAuthNoPriv.</p> <p>noAuthNoPriv indicates no authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them. authNoPriv indicates an authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them. authPriv indicates an authentication algorithm and a privacy algorithm are applied to check and encrypt packets.</p> <p><i>read-view</i>: Set the view to be the Read view. Then the NMS can view parameters of the specified view.</p> <p><i>write-view</i>: Set the view to be the Write view. Then the NMS can modify parameters of the specified view. Note that the view in the Write view should also be in the Read view.</p> <p><i>notify-view</i>: Set the view to be the Notify view. Then the NMS can get notifications of the specified view from the agent.</p>
Step 3	<p>show snmp-server group</p> <p>Displays SNMP group entries.</p>
Step 4	<p>end</p> <p>Return to Privileged EXEC Mode.</p>
Step 5	<p>copy running-config startup-config</p> <p>Save the settings in the configuration file.</p>

The following example shows how to create an SNMPv3 group with the group name as nms1, the security level as authPriv, and the Read and Notify view are both View:

Switch#configure

Switch(config)#snmp-server group nms1 **smode** v3 **slev** authPriv **read** View **notify** View

Switch(config)#show snmp-server group

No.	Name	Sec-Mode	Sec-Lev	Read-View	Write-View	Notify-View
---	-----	-----	-----	-----	-----	-----
1	nms1	v3	authPriv	View		View

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Creating SNMP Users (For SNMPv3)

Create SNMP users and add them to the SNMP group. Users in the same group have the same access rights, which are defined when creating the group.

Step 1	<p>configure</p> <p>Enter Global Configuration Mode.</p>
Step 2	<p>Choose a security level for the user and run the corresponding command to create the user. The security levels from low to high are NoAuthNoPriv, AuthNoPriv, and AuthPriv. The security level of a user should not be lower than that of the group it belongs to.</p> <p>To create a user with the security level as NoAuthNoPriv:</p> <pre>snmp-server user <i>name</i> { <i>local</i> <i>remote</i> } <i>group-name</i> [smode <i>v3</i>] slev noAuthNoPriv</pre> <p><i>name</i>: Enter the user name with 1 to 16 characters.</p> <p><i>local</i> <i>remote</i>: Choose a user type based on the location of the user. Local indicates that the user resides on the local SNMP engine (the switch), while remote indicates that the user resides on the NMS. Before configuring a remote user, you need to set the remote engine ID first. The remote engine ID and user password are used when computing the authentication and privacy digests.</p> <p><i>group-name</i>: Enter the name of the group which the user belongs to. Users with the same Group Name, Security Model and Security Level will be in the same group.</p> <p><i>v3</i>: Configure the security model for the user. <i>v3</i> indicates SNMPv3, the most secure model.</p> <p><i>noAuthNoPriv</i>: Configure the security level as noAuthNoPriv. For this level, no authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them.</p> <p>To create a user with the security level as AuthNoPriv:</p> <pre>snmp-server user <i>name</i> { <i>local</i> <i>remote</i> } <i>group-name</i> [smode <i>v3</i>] slev authNoPriv cmode {MD5 SHA} cpwd <i>confirm-pwd</i></pre> <p><i>authNoPriv</i>: Configure the security level as authNoPriv. For this level, an authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them.</p> <p><i>MD5</i> <i>SHA</i>: Choose an authentication algorithm when the security level is set as authNoPriv or authPriv. SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is none.</p> <p><i>confirm-pwd</i>: Enter an authentication password with 1 to 16 characters excluding question mark and space. This password in the configuration file will be displayed in the symmetric encrypted form.</p> <p>To create a user with the security as AuthPriv:</p> <pre>snmp-server user <i>name</i> { <i>local</i> <i>remote</i> } <i>group-name</i> [smode <i>v3</i>] slev authPriv cmode {MD5 SHA} cpwd <i>confirm-pwd</i> emode DES epwd <i>encrypt-pwd</i></pre> <p><i>authPriv</i>: Configure the security level as authPriv. For this level, an authentication algorithm and a privacy algorithm are applied to check and encrypt packets.</p> <p><i>DES</i>: Configure the privacy mode as DES. The switch will use the DES algorithm to encrypt the packets. By default, the Privacy Mode is none.</p> <p><i>encrypt-pwd</i>: Enter a privacy password with 1 to 16 characters excluding question mark and space. This password in the configuration file will be displayed in the symmetric encrypted form.</p>

Step 3	show snmp-server user Displays the information of SNMP users.
Step 4	end Return to Privileged EXEC Mode.
Step 5	copy running-config startup-config Save the settings in the configuration file.

The following example shows how to create a remote SNMP user named admin and add it to group nms1. The security settings are as *Table 2-1*:

Table 2-1 Security Settings for the User

Parameter	Value
Security Level	v3
Authentication Mode	SHA
Authentication Password	1234
Privacy Mode	DES
Privacy Password	5678

Switch#configure

```
Switch(config)#snmp-server user admin remote nms1 smode v3 slev authPriv cmode
SHA cpwd 1234 emode DES epwd 5678
```

Switch(config)#show snmp-server user

```
No. U-Name  U-Type  G-Name  S-Mode  S-Lev  A-Mode  P-Mode
--- -----  -----  -----  -----  -----  -----
1  admin    remote  nms1    v3      authPriv  SHA    DES
```

Switch(config)#end

Switch#copy running-config startup-config

3 Notification Configurations

With Notification enabled, the switch can send notifications to the NMS about important events relating to the device's operation. This facilitates the monitoring and management of the NMS.

To configure SNMP notification, follow these steps:

- 1) Configure the information of NMS hosts.
- 2) Enable SNMP traps.

Configuration Guidelines

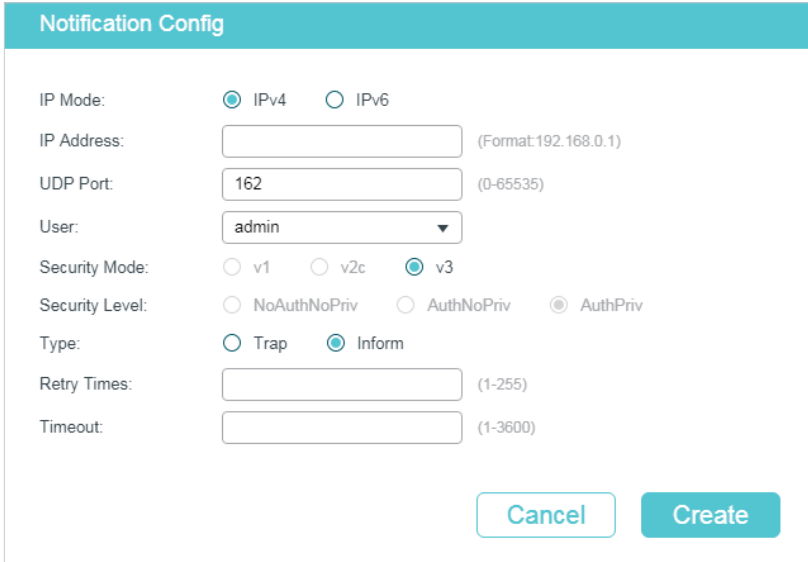
To guarantee the communication between the switch and the NMS, ensure the switch and the NMS can reach one another.

3.1 Using the GUI

3.1.1 Configuring the Information of NMS Hosts

Choose the menu **MAINTENANCE > SNMP > Notification > Notification Config** and click  **Add** to load the following page.

Figure 3-1 Adding an NMS Host



Notification Config

IP Mode: IPv4 IPv6

IP Address: (Format:192.168.0.1)

UDP Port: (0-65535)

User:

Security Mode: v1 v2c v3

Security Level: NoAuthNoPriv AuthNoPriv AuthPriv

Type: Trap Inform

Retry Times: (1-255)

Timeout: (1-3600)

Follow these steps to add an NMS host:

- 1) Choose the IP mode according to the network environment, and specify the IP address of the NMS host and the UDP port that receives notifications.

IP Mode	Choose an IP mode for the NMS host.
IP Address	If you set IP Mode as IPv4, specify an IPv4 address for the NMS host. If you set IP Mode as IPv6, specify an IPv6 address for the NMS host.
UDP Port	Specify a UDP port on the NMS host to receive notifications. For security, we recommend that you change the port number under the condition that communications on other UDP ports are not affected.

- 2) Specify the user name or community name used by the NMS host, and configure the security model and security level based on the user or community.

User	Choose the user name or community name used by the NMS host.
Security Model	If a community name (created for SNMPv1/v2c) is selected in User, specify the security model as v1 or v2c. If a user name (created for SNMPv3) is selected in User, here displays the security model as v3. <i>Note:</i> The NMS host should use the corresponding SNMP version.
Security Level	If Security model is v3, here displays the security level of the user.

- 3) Choose a notification type based on the SNMP version. If you choose the Inform type, you need to set retry times and timeout interval.

Type	Choose a notification type for the NMS host. For SNMPv1, the supported type is Trap. For SNMPv2c and SNMPv3, you can configure the type as Trap or Inform. Trap: The switch will send Trap messages to the NMS host when certain events occur. When the NMS host receives a Trap message, it will not send a response to the switch. Thus the switch cannot tell whether a message is received or not, and the messages that are not received will not be resent. Inform: The switch will send Inform messages to the NMS host when certain events occur. When the NMS host receives an Inform message, it sends a response to the switch. If the switch does not receive any response within the timeout interval, it will resend the Inform message. Therefore, Inform is more reliable than Trap.
Retry	Set the retry times for Informs. The switch will resend the Inform message if it does not receive any response from the NMS host within the timeout interval. It will stop sending Inform messages when the retry time reaches the limit.
Timeout	Set the time that the switch waits for a response from the NMS host after sending an inform message.

- 4) Click **Create**.

3.1.2 Enabling SNMP Traps

Choose the menu **MAINTENANCE > SNMP > Notification > Trap Config** to load the following page.

Figure 3-2 Enabling SNMP Traps

SNMP Traps

<input checked="" type="checkbox"/> SNMP Authentication	<input checked="" type="checkbox"/> Coldstart	<input checked="" type="checkbox"/> Warmstart
<input checked="" type="checkbox"/> Link Status	<input type="checkbox"/> CPU Utilization	<input type="checkbox"/> Memory Utilization
<input type="checkbox"/> Flash Operation	<input type="checkbox"/> VLAN Create/Delete	<input type="checkbox"/> IP Change
<input type="checkbox"/> Storm Control	<input type="checkbox"/> Rate Limit	<input type="checkbox"/> LLDP
<input type="checkbox"/> Loopback Detection	<input type="checkbox"/> Spanning Tree	<input type="checkbox"/> IP-MAC Binding
<input type="checkbox"/> IP Duplicate	<input type="checkbox"/> DHCP Filter	<input type="checkbox"/> DDM Temperature
<input type="checkbox"/> DDM Voltage	<input type="checkbox"/> DDM Bias Current	<input type="checkbox"/> DDM TX Power
<input type="checkbox"/> DDM RX Power	<input type="checkbox"/> ACL Counter	

Apply

Follow these steps to enable some or all of the supported traps:

- 1) Select the traps to be enabled according to your needs. With a trap enabled, the switch will send the corresponding trap message to the NMS when the trap is triggered.

SNMP Authentication	Triggered when a received SNMP request fails the authentication.
Coldstart	Indicates that the SNMP entity is reinitializing itself such that its configurations may be changed. The trap can be triggered when you reboot the switch.
Warmstart	Indicates that the SNMP entity is reinitializing itself with its configurations unchanged. For a switch running SNMP, the trap can be triggered if you disable and then enable SNMP without changing any parameters.
Link Status	<p>Enable or disable Link Status Trap globally. The trap includes the following two sub-traps:</p> <p>Linkup Trap: Indicates that a port status changes from linkdown to linkup.</p> <p>Linkdown Trap: Indicates that a port status changes from linkup to linkdown.</p> <p>Link Status Trap can be triggered when it is enabled both globally and on the port, and you connect a new device to the port or disconnect a device from the port.</p> <p>To enable the trap on a port, run the command snmp-server traps link-status in Interface Configuration Mode of the port. To disable it, run the corresponding no command.</p> <p>By default, the trap is enabled both globally and on all ports, which means that link status changes on any ports will trigger the trap. If you do not want to receive notification messages about some specific ports, disable the trap on those ports.</p>

CPU Utilization	Triggered when the CPU utilization exceeds 80%.
Memory Utilization	Triggered when the memory utilization exceeds 80%.
Flash Operation	Triggered when flash is modified during operations such as backup, reset, firmware upgrade, and configuration import.
VLAN Create/Delete	Triggered when certain VLANs are created or deleted successfully.
IP Change	Monitors the changes of interfaces' IP addresses. The trap can be triggered when the IP address of any interface is changed.
Storm Control	Monitors whether the storm rate has reached the limit that you have set. The trap can be triggered when the Storm Control feature is enabled and broadcast/multicast/unknown-unicast frames are sent to the port with a rate higher than what you have set.
Rate Limit	Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.
LLDP	<p>The trap includes the following sub-traps:</p> <p>LLDP RemTablesChange: Indicates that the switch senses an LLDP topology change. The trap can be triggered when adding or removing a remote device, and when the information of some remote devices is aged out or cannot be stored into the switch because of insufficient resources. This trap can be used by an NMS to trigger LLDP remote systems table maintenance polls.</p> <p>LLDP TopologyChange: Indicates that the switch senses an LLDP-MED topology change (the topology change of media endpoints). The trap can be triggered when adding or removing a media endpoint that supports LLDP, such as an IP Phone. An LLDP Remtableschange trap will be also triggered every time LLDP Topologychange trap is triggered.</p>
Loopback Detection	Triggered when the Loopback Detection feature is enabled and a loopback is detected or cleared.
Spanning Tree	Indicates spanning tree changes. The trap can be triggered in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a TCN (Topology Change Notification) BPDU or a Configuration BPDU with the TC (Topology Change) bit set.

PoE	<p>Only for products that support PoE. The trap includes the following sub-traps:</p> <p>Over-max-pwr-budget: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply.</p> <p>Port-pwr-change: Triggered when a port starts to supply power or stops supplying power.</p> <p>Port-pwr-deny: Triggered when the switch powers off PDs on low-priority PoE ports. The switch powers off them to ensure stable running of the other PDs when the total power required by the connected PDs exceeds the system power limit.</p> <p>Port-pwr-over-30w: Triggered when the power required by the connected PD exceeds 30 watts.</p> <p>Port-pwr-overload: Triggered when the power required by the connected PD exceeds the maximum power the port can supply.</p> <p>Port-short-circuit: Triggered when a short circuit is detected on a port.</p> <p>Thermal-shutdown: Triggered when the PSE chip overheats. The switch will stop supplying power in this case.</p>
IP-MAC Binding	Triggered in the following two situations: the ARP Inspection feature is enabled and the switch receives an illegal ARP packet; or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.
IP Duplicate	Triggered when the switch detects an IP conflict.
DHCP Filter	Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server.
DDM Temperature	<p>Monitors the temperature of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold.</p> <p><i>Note:</i> T2600G-52TS does not support this trap.</p>
DDM Voltage	<p>Monitors the voltage of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold.</p> <p><i>Note:</i> T2600G-52TS does not support this trap.</p>
DDM Bias Current	<p>Monitors the bias current of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold.</p> <p><i>Note:</i> T2600G-52TS does not support this trap.</p>
DDM TX Power	<p>Monitors the TX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold.</p> <p><i>Note:</i> T2600G-52TS does not support this trap.</p>

DDM RX Power	Monitors the RX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold. <i>Note:</i> T2600G-52TS does not support this trap.
ACL Counter	Monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in the ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.

2) Click **Apply**.

3.2 Using the CLI

3.2.1 Configuring the NMS Host

Configure parameters of the NMS host and packet handling mechanism.

Step 1	configure
	Enter Global Configuration Mode.

Step 2

snmp-server host *ip udp-port user-name* [**smode** { v1 | v2c | v3 }] [**slev** {noAuthNoPriv | authNoPriv | authPriv }] [**type** { trap | inform}] [**retries** *retries*] [**timeout** *timeout*]

Configure parameters of the NMS host and packet handling mechanism.

ip: Specify the IP address of the NMS host in IPv4 or IPv6. Make sure the NMS host and the switch can reach each other.

udp-port: Specify a UDP port on the NMS host to receive notifications. The default is port 162. For communication security, we recommend that you change the port number under the condition that communications on other UDP ports are not affected.

user-name: Enter the name used by the NMS host. When the NMS host uses SNMPv1 or SNMPv2c, enter the Community Name; when the NMS host uses SNMPv3, enter the User Name of the SNMP Group.

v1 | v2c | v3: Choose the security model used by the user from the following: SNMPv1, SNMPv2c, SNMPv3. The NMS host should use the corresponding SNMP version.

noAuthNoPriv | authNoPriv | authPriv: For SNMPv3 groups, choose a security level from noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption), authPriv (authorization and encryption). The default is noAuthNoPriv. Note that if you have chosen v1 or v2c as the security model, the security level cannot be configured.

trap | inform: Choose a notification type for the NMS host. For SNMPv1, the supported type is Trap. For SNMPv2c and SNMPv3, you can configure the type as Trap or Inform.

Trap: The switch will send Trap messages to the NMS host when certain events occur. When the NMS host receives a Trap message, it will not send a response to the switch. Thus the switch cannot tell whether a message is received or not, and the messages that are not received will not be resent.

Inform: The switch will send Inform messages to the NMS host when certain events occur. When the NMS host receives an Inform message, it sends a response to the switch. If the switch does not receive any response within the timeout interval, it will resend the Inform message. Therefore, Inform is more reliable than Trap.

retries: Set the retry times for Inform messages. The range is between 1 to 255 and the default is 3. The switch will resend the Inform message if it does not receive any response from the NMS host within the timeout interval. And it will stop sending Inform message when the retry times reaches the limit.

timeout: Set the time that the switch waits for a response. Valid values are from 1 to 3600 seconds; the default is 100 seconds. The switch will resend the Inform message if it does not receive a response from the NMS host within the timeout interval.

Step 3

show snmp-server host

Verify the information of the host.

Step 4

end

Return to Privileged EXEC Mode.

Step 5

copy running-config startup-config

Save the settings in the configuration file.

The following example shows how to configure an NMS host with the parameters shown in *Table 3-1*.

Table 3-1 Parameters for the NMS Hosts

Parameter	Value
IP Address	172.16.1.222
UDP Port	162
User Name	admin
Security Model	v3
Security Level	authPriv
Notification Type	Inform
Retry Times	3
Timeout Interval	100 seconds

Switch#configure

```
Switch(config)#snmp-server host 172.16.1.222 162 admin smode v3 slev authPriv type
inform retries 3 timeout 100
```

Switch(config)#show snmp-server host

No.	Des-IP	UDP	Name	SecMode	SecLev	Type	Retry	Timeout
---	-----	-----	----	-----	-----	----	-----	-----
1	172.16.1.222	162	admin	v3	authPriv	inform	3	100

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Enabling SNMP Traps

The switch supports many types of SNMP traps, like SNMP standard traps, ACL traps, and VLAN traps, and the corresponding commands are different. With a trap enabled, the switch will send the corresponding trap message to the NMS when the trap is triggered. Follow these steps to enable the traps according to your needs.

■ Enabling the SNMP Standard Traps Globally

-
- Step 1 **configure**
Enter Global Configuration Mode.
-

Step 2	<p>snmp-server traps snmp [linkup linkdown warmstart coldstart auth-failure]</p> <p>Enable the corresponding SNMP standard traps. The command without any parameter enables all SNMP standard traps. By default, all SNMP standard traps are enabled.</p> <p>linkup linkdown: Enable Linkup Trap and Linkdown Trap globally.</p> <p>Linkup Trap indicates that a port status changes from linkdown to linkup. The trap can be triggered when you connect a new device to the port, and the trap is enabled both globally and on the port.</p> <p>Linkdown Trap indicates that a port status changes from linkup to linkdown. The trap can be triggered when you disconnect a device from the port, and the trap is enabled both globally and on the port.</p> <p>To enable Linkup Trap and Linkdown Trap on a port, run the command snmp-server traps link-status in Interface Configuration Mode of the port. To disable them, run the corresponding no command.</p> <p>By default, the traps are enabled both globally and on all ports, which means that the traps will be triggered when a device is connected to or disconnected from any port of the switch. If you do not want to receive notification messages about some specific ports, disable the traps on those ports.</p> <p>warmstart: Indicates that the SNMP entity is reinitializing itself with its configurations unchanged. For a switch running SNMP, the trap can be triggered if you disable and then enable SNMP without changing any parameters.</p> <p>coldstart: Indicates that the SNMP entity is reinitializing itself such that its configurations may be changed. The trap can be triggered when you reboot the switch.</p> <p>auth-failure: Triggered when a received SNMP request fails the authentication.</p>
--------	---

Step 3	<p>end</p> <p>Return to Privileged EXEC Mode.</p>
--------	--

Step 4	<p>copy running-config startup-config</p> <p>Save the settings in the configuration file.</p>
--------	--

The following example shows how to configure the switch to send linkup traps:

```

Switch#configure
Switch(config)#snmp-server traps snmp linkup
Switch(config)#end
Switch#copy running-config startup-config

```

■ Enabling the SNMP Extended Traps Globally

Step 1	<p>configure</p> <p>Enter Global Configuration Mode.</p>
--------	---

Step 2	snmp-server traps { rate-limit cpu flash lldp remtableschange lldp topologychange loopback-detection storm-control spanning-tree memory }
	<p>Enable the corresponding SNMP extended traps. By default, all SNMP extended traps are disabled.</p> <p>rate-limit: Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.</p> <p>cpu: Monitors the load status of the switch CPU. The trap can be triggered when the utilization rate of the CPU exceeds 80%.</p> <p>flash: Triggered when flash is modified during operations such as backup, reset, firmware upgrade, and configuration import.</p> <p>lldp remtableschange: Indicates that the switch senses an LLDP topology change. The trap can be triggered when adding or removing a remote device, and when the information of some remote devices is aged out or cannot be stored into the switch because of insufficient resources. This trap can be used by an NMS to trigger LLDP remote systems table maintenance polls.</p> <p>lldp topologychange: Indicates that the switch senses an LLDP-MED topology change (the topology change of media endpoints). The trap can be triggered when adding or removing a media endpoint that supports LLDP, such as an IP Phone. An LLDP Remtableschange trap will be also triggered every time LLDP Topologychange trap is triggered.</p> <p>loopback-detection: Triggered when the Loopback Detection feature is enabled and a loopback is detected or cleared.</p> <p>storm-control: Monitors whether the storm rate has reached the limit that you have set. The trap can be triggered when the Storm Control feature is enabled and broadcast/multicast/unknown-unicast frames are sent to the port with a rate higher than what you have set.</p> <p>spanning-tree: Indicates spanning tree changes. The trap can be triggered in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a TCN (Topology Change Notification) BPDU or a Configuration BPDU with the TC (Topology Change) bit set.</p> <p>memory: Monitors the load status of the switch memory. The trap can be triggered when the memory utilization exceeds 80%.</p>
Step 3	end Return to Privileged EXEC Mode.
Step 4	copy running-config startup-config Save the settings in the configuration file.

The following example shows how to configure the switch to enable bandwidth-control traps:

```
Switch#configure
```

```
Switch(config)#snmp-server traps bandwidth-control
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

■ Enabling the DDM Traps Globally

Note:

T2600G-52TS does not support DDM traps.

Step 1	configure Enter Global Configuration Mode.
Step 2	snmp-server traps ddm [temperature voltage bias_current tx_power rx_power] Enable the corresponding DDM traps. DDM function is used to monitor the status of the SFP modules inserted into the SFP ports on the switch. The command without parameter enables all SNMP DDM traps. By default, all DDM traps are disabled. temperature: Monitors the temperature of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold. voltage: Monitors the voltage of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold. bias_current: Monitors the bias current of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold. tx_power: Monitors the TX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold. rx_power: Monitors the RX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold.
Step 3	end Return to Privileged EXEC Mode.
Step 4	copy running-config startup-config Save the settings in the configuration file.

The following example shows how to configure the switch to enable DDM temperature trap:

```
Switch#configure
```

```
Switch(config)#snmp-server traps ddm temperature
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

■ Enabling the VLAN Traps Globally

Step 1	configure Enter Global Configuration Mode.
--------	--

Step 2	<p>snmp-server traps vlan [create delete]</p> <p>Enable the corresponding VLAN traps. The command without parameter enables all SNMP VLAN traps. By default, all VLAN traps are disabled.</p> <p>create: Triggered when certain VLANs are created successfully.</p> <p>delete: Triggered when certain VLANs are deleted successfully.</p>
Step 3	<p>end</p> <p>Return to Privileged EXEC Mode.</p>
Step 4	<p>copy running-config startup-config</p> <p>Save the settings in the configuration file.</p>

The following example shows how to configure the switch to enable all the SNMP VLAN traps:

Switch#configure

Switch(config)#snmp-server traps vlan

Switch(config)#end

Switch#copy running-config startup-config

■ Enabling the SNMP Security Traps Globally

Step 1	<p>configure</p> <p>Enter Global Configuration Mode.</p>
Step 2	<p>snmp-server traps security { dhcp-filter ip-mac-binding }</p> <p>Enable the corresponding security traps. By default, all security traps are disabled.</p> <p>dhcp-filter: Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server.</p> <p>ip-mac-binding: Triggered when the ARP Inspection feature is enabled and the switch receives an illegal ARP packet, or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.</p>
Step 3	<p>end</p> <p>Return to Privileged EXEC Mode.</p>
Step 4	<p>copy running-config startup-config</p> <p>Save the settings in the configuration file.</p>

The following example shows how to configure the switch to enable DHCP filter trap:

Switch#configure

Switch(config)#snmp-server traps security dhcp-filter

Switch(config)#end

Switch#copy running-config startup-config

■ Enabling the ACL Trap Globally

Step 1	configure Enter Global Configuration Mode.
Step 2	snmp-server traps security acl Enable the ACL trap. By default, it is disabled. The trap monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in the ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.
Step 3	end Return to Privileged EXEC Mode.
Step 4	copy running-config startup-config Save the settings in the configuration file.

The following example shows how to configure the switch to enable ACL trap:

Switch#configure

Switch(config)#snmp-server traps acl

Switch(config)#end

Switch#copy running-config startup-config

■ Enabling the IP Traps Globally

Step 1	configure Enter Global Configuration Mode.
Step 2	snmp-server traps ip { change duplicate } Enable the IP traps. By default, all IP traps are disabled. change: Monitors the changes of interfaces' IP addresses. The trap can be triggered when the IP address of any interface is changed. duplicate: Triggered when the switch detects an IP conflict.
Step 3	end Return to Privileged EXEC Mode.
Step 4	copy running-config startup-config Save the settings in the configuration file.

The following example shows how to configure the switch to enable IP-Change trap:

```
Switch#configure
Switch(config)#snmp-server traps ip change
Switch(config)#end
Switch#copy running-config startup-config
```

■ Enabling the SNMP PoE Traps Globally

Note:

Only T2600G-28MPS supports PoE traps.

Step 1	<p>configure</p> <p>Enter Global Configuration Mode.</p>
Step 2	<p>snmp-server traps power [over-max-pwr-budget port-pwr-change port-pwr-deny port-pwr-over-30w port-pwr-overload port-short-circuit thermal-shutdown]</p> <p>Enable the PoE traps. The command without any parameter enables all PoE traps. By default, all PoE traps are disabled.</p> <p>over-max-pwr-budget: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply.</p> <p>port-pwr-change: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply.</p> <p>port-pwr-deny: Triggered when the switch powers off PDs on low-priority PoE ports. The switch powers off them to ensure stable running of the other PDs when the total power required by the connected PDs exceeds the system power limit.</p> <p>port-pwr-over-30w: Triggered when the power required by the connected PD exceeds 30 watts.</p> <p>port-pwr-overload: Triggered when the power required by the connected PD exceeds the maximum power the port can supply.</p> <p>port-short-circuit: Triggered when a short circuit is detected on a port.</p> <p>thermal-shutdown: Triggered when the PSE chip overheats. The switch will stop supplying power in this case.</p>
Step 3	<p>end</p> <p>Return to Privileged EXEC Mode.</p>
Step 4	<p>copy running-config startup-config</p> <p>Save the settings in the configuration file.</p>

The following example shows how to configure the switch to enable all PoE traps:

```
Switch#configure
Switch(config)#snmp-server traps power
Switch(config)#end
```


Switch#copy running-config startup-config

■ Enabling the Link-status Trap for Ports

Step 1	configure Enter Global Configuration Mode.
Step 2	interface {fastEthernet <i>port</i> range fastEthernet <i>port-list</i> gigabitEthernet <i>port</i> range gigabitEthernet <i>port-list</i> ten-gigabitEthernet <i>port</i> range ten-gigabitEthernet <i>port-list</i> } Configure notification traps on the specified ports. <i>port/port-list</i> : The number or the list of the Ethernet ports that you desire to configure notification traps. To configure multiple ports, enter a list of port numbers separated by commas, or use a hyphen to indicate a range of port numbers. For example, 1-3, 5 indicates port 1, 2, 3, 5.
Step 3	snmp-server traps link-status Enable Link Status Trap for the port. By default, it is enabled. Link Status Trap (including Linkup Trap and Linkdown Trap) can be triggered when the link status of a port changes, and the trap is enabled both globally and on the port. To enable Linkup Trap and Linkdown Trap globally, run the command snmp-server traps snmp [linkup linkdown] in Global Configuration Mode. To disable it, run the corresponding no command.
Step 4	end Return to Privileged EXEC Mode.
Step 5	copy running-config startup-config Save the settings in the configuration file.

The following example shows how to configure the switch to enable link-status trap:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#snmp-server traps link-status
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

4 RMON

RMON (Remote Network Monitoring) together with the SNMP system allows the network manager to monitor remote network devices efficiently. RMON reduces traffic flow between the NMS and managed devices, which is convenient to manage large networks.

RMON includes two parts: the NMS and the Agents running on every network device. The NMS is usually a host that runs the management software to manage Agents of network devices. The Agent is usually a switch or router that collects traffic statistics (such as the total number of packets on a network segment during a certain time period, or total number of correct packets that are sent to a host). Based on SNMP protocol, the NMS collects network data by communicating with Agents. However, the NMS cannot obtain every datum of RMON MIB because the device resources are limited. Generally, the NMS can only get information of the following four groups: Statistics, History, Event and Alarm.

- **Statistics:** Collects Ethernet statistics (like the total received bytes, the total number of broadcast packets, and the total number of packets with specified size) on an interface.
- **History:** Collects a history group of statistics on Ethernet ports for a specified polling interval.
- **Event:** Specifies the action to be taken when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.
- **Alarm:** Monitors a specific MIB object for a specified interval, and triggers an event at a specified value (rising threshold or falling threshold).

5 RMON Configurations

With RMON configurations, you can:

- Configuring the Statistics group.
- Configuring the History group.
- Configuring the Event group.
- Configuring the Alarm group.

Configuration Guidelines

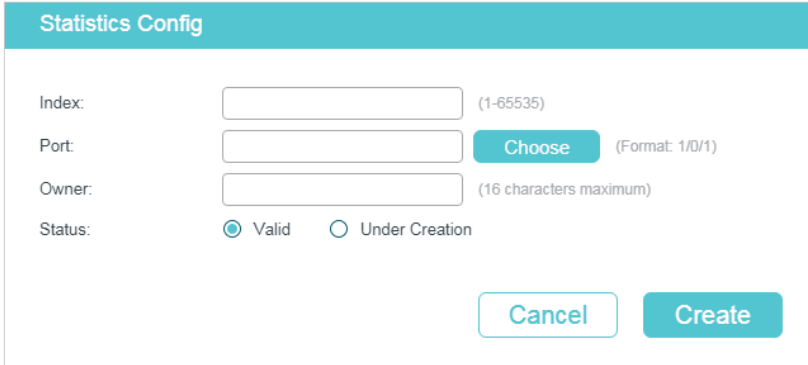
To ensure that the NMS receives notifications normally, complete configurations of SNMP and SNMP Notification before configuring RMON.

5.1 Using the GUI

5.1.1 Configuring the Statistics Group

Choose the menu **MAINTENANCE > SNMP > RMON > Statistics** and click  Add to load the following page.

Figure 5-1 Creating a Statistics Entry



Follow these steps to configure the Statistics group:

- 1) Specify the entry index, the port to be monitored, and the owner name of the entry. Set the entry as Valid or Under Creation.

Index	Enter the index of the entry.
Port	Specify an Ethernet port to be monitored in the entry. You can click Choose to choose a port from the list or manually enter the port number, for example, 1/0/1 in the input box.
Owner	Enter the owner name of the entry with 1 to 16 characters.

Status Set the entry as Valid or Under Creation. By default, it is Valid. The switch start to collect Ethernet statistics for a Statistics entry since the entry status is configured as valid.

Valid: The entry is created and valid.

Under Creation: The entry is created but invalid.

2) Click **Create**.

5.1.2 Configuring History Group

Choose the menu **MAINTENANCE > SNMP > RMON > History** to load the following page.

Figure 5-2 Configuring the History Entry

History Control Config						
<input type="checkbox"/>	Index	Port	Interval (seconds)	Maximum Buckets	Owner	Status
<input checked="" type="checkbox"/>	1	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	2	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	3	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	4	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	5	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	6	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	7	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	8	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	9	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	10	1/0/1	1800	50	monitor	Disabled
Total: 12			1 entry selected.		<input type="button" value="Cancel"/>	<input type="button" value="Apply"/>

Follow these steps to configure the History group:

1) Select a History entry, and specify a port to be monitored.

Index Displays the index of History entries. The switch supports up to 12 History entries.

Port Specify a port to be monitored.

2) Set the sample interval and the maximum buckets of History entries.

Interval (seconds) Specify the number of seconds in each polling cycle. Valid values are from 10 to 3600 seconds. Every history entry has its own timer. For the monitored port, the switch samples packet information and generates a record in every interval.

Maximum Buckets Set the maximum number of records for the History entry. Valid values are from 10 to 130. When the number of records exceeds the limit, the earliest record will be overwritten.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

Owner	Enter the owner name of the entry with 1 to 16 characters. By default, it is monitor.
Status	Enable or disable the entry. By default, it is disabled. Enable: The entry is enabled. Disable: The entry is disabled.

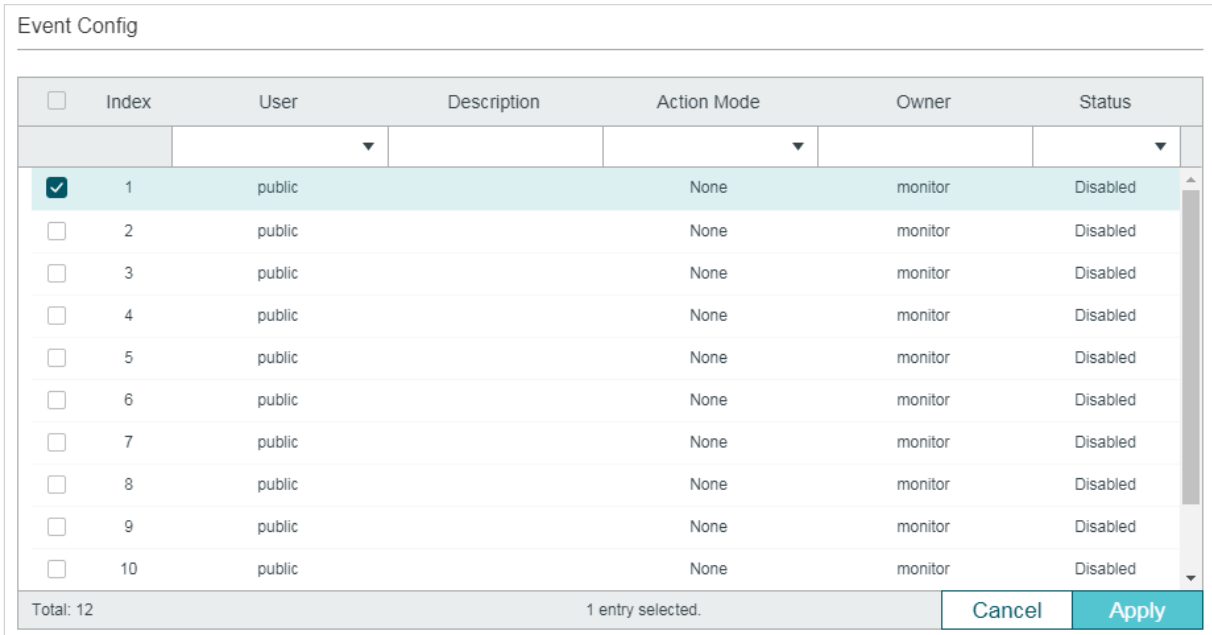
 **Note:**

To change the parameters of a History entry, enable the entry at the same time; otherwise, the change cannot take effect.

5.1.3 Configuring Event Group

Choose the menu **MAINTENANCE > SNMP > RMON > Event** to load the following page.

Figure 5-3 Configuring the Event Entry



<input type="checkbox"/>	Index	User	Description	Action Mode	Owner	Status
<input checked="" type="checkbox"/>	1	public		None	monitor	Disabled
<input type="checkbox"/>	2	public		None	monitor	Disabled
<input type="checkbox"/>	3	public		None	monitor	Disabled
<input type="checkbox"/>	4	public		None	monitor	Disabled
<input type="checkbox"/>	5	public		None	monitor	Disabled
<input type="checkbox"/>	6	public		None	monitor	Disabled
<input type="checkbox"/>	7	public		None	monitor	Disabled
<input type="checkbox"/>	8	public		None	monitor	Disabled
<input type="checkbox"/>	9	public		None	monitor	Disabled
<input type="checkbox"/>	10	public		None	monitor	Disabled

Total: 12 1 entry selected. **Cancel** **Apply**

Follow these steps to configure the Event group:

1) Choose an Event entry, and specify an SNMP User for the entry.

Index	Displays the index of Event entries. The switch supports up to 12 Event entries.
User	Choose an SNMP user name or community name for the entry. Only the specified user can access the log messages or receive the notification messages related to the event.

2) Set the description and action to be taken when the event is triggered.

Description	Enter an brief description of this event to make it easier to be identified.
--------------------	--

Action Mode Specify the action for the switch to take when the event is triggered.

None: No action.

Log: The switch records the event in the log, and the NMS should initiate requests to get notifications.

Notify: The switch sends notifications to the NMS.

Log & Notify: The switch records the event in the log and sends notifications to the NMS.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

Owner Enter the owner name of the entry with 1 to 16 characters.

Status Enable or disable the entry.

Enable: The entry is enabled.

Disable: The entry is disabled.

5.1.4 Configuring Alarm Group

Before you begin, complete configurations of Statistics entries and Event entries, because the Alarm entries must be associated with Statistics and Event entries.

Choose the menu **MAINTENANCE > SNMP > RMON > Alarm** to load the following page.

Figure 5-4 Configuring the Alarm Entry

<input type="checkbox"/>	Index	Variable	Statistics	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event
<input checked="" type="checkbox"/>	1	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	2	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	3	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	4	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	5	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	6	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	7	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	8	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	9	RecBytes	0	Absolute	100	0	100	0
<input type="checkbox"/>	10	RecBytes	0	Absolute	100	0	100	0

Total: 12 1 entry selected.

Follow these steps to configure the Alarm group:

- 1) Select an alarm entry, choose a variable to be monitored, and associate the entry with a statistics entry.

Index	Displays the index of Alarm entries. The switch supports up to 12 Alarm entries.
Variable	<p>Set the alarm variable to be monitored. The switch will monitor the specified variable in sample intervals and act in the set way when the alarm is triggered.</p> <p>RecBytes: Total number of received bytes.</p> <p>RecPackets: Total number of received packets.</p> <p>BPackets: Total number of broadcast packets.</p> <p>MPackets: Total number of multicast packets.</p> <p>CRC&Align ERR: Packets that contain FCS Error or Alignment Error, within a size of 64 to 1518 bytes.</p> <p>Undersize: Packets that are smaller than 64 bytes.</p> <p>Oversize: Packets that are larger than 1518 bytes.</p> <p>Jabbers: Packets that are sent when port collisions occur.</p> <p>Collisions: Collision times in the network segment.</p> <p>64, 65-127, 128-255, 256-511, 512-1023, 1024-1518: Total number of packets of the specified size.</p>
Statistics	Associate the Alarm entry with a Statistics entry. Then the switch monitors the specified variable of the Statistics entry.

- 2) Set the sample type, the rising and falling threshold, the corresponding event entries, and the alarm type of the entry.

Sample Type	<p>Specify the sampling method of the specified variable.</p> <p>Absolute: Compare the sampling value against the preset threshold.</p> <p>Delta: The switch obtains the difference between the sampling values of the current interval and the previous interval, and then compares the difference against the preset threshold.</p>
Rising Threshold	<p>Specify the rising threshold of the variable. Valid values are from 1 to 2147483647. When the sampling value or the difference value exceeds the threshold, the system will trigger the corresponding Rising Event.</p> <p><i>Note:</i> The rising threshold should be larger than the falling threshold.</p>
Rising Event	Specify the index of the Event entry that will be triggered when the sampling value or the difference value exceeds the preset threshold. The Event entry specified here should be enabled first.

Falling Threshold	Set the falling threshold of the variable. Valid values are from 1 to 2147483647. When the sampling value or the difference value is below the threshold, the system will trigger the corresponding Falling Event. <i>Note:</i> The falling threshold should be less than the rising threshold.
Falling Event	Specify the index of the Event entry that will be triggered when the sampling value or the difference value is below the preset threshold. The Event entry specified here should be enabled first.
Alarm Type	Specify the alarm type for the entry. Rising: The alarm is triggered only when the sampling value or the difference value exceeds the rising threshold. Falling: The alarm is triggered only when the sampling value or the difference value is below the falling threshold. All: The alarm is triggered when the sampling value or the difference value exceeds the rising threshold or is below the falling threshold.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

Interval (seconds)	Set the sampling interval. Valid values are from 10 to 3600 seconds.
Owner	Enter the owner name of the entry with 1 to 16 characters.
Status	Enable or disable the entry. Enable: The entry is enabled. Disable: The entry is disabled.

5.2 Using the CLI

5.2.1 Configuring Statistics

Step 1	configure Enter Global Configuration Mode.
--------	--

Step 2 **rmon statistics** *index* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } [**owner** *owner-name*] [**status** { **underCreation** | **valid** }]

Configure RMON Statistic entries.

index: Specify the index of the Statistics entry, which ranges from 1 to 65535. To configure multiple indexes, enter a list of indexes separated by commas, or use a hyphen to indicate a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5.

port: Specify the port to be bound to the entry.

owner-name: Enter the owner name of the entry with 1 to 16 characters. The default name is monitor.

underCreation | **valid**: Enter the status of the entry. UnderCreation indicates that the entry is created but invalid, while Valid indicates the entry is created and valid. By default, it is valid.

The switch starts to collect Ethernet statistics for a Statistics entry since the entry status is configured as valid.

Step 3 **show rmon statistics** [*index*]

Displays the statistics entries and their configurations.

index: Enter the index of statistics entry that you want to view. Valid values are from 1 to 65535. The command without any parameters displays all existing statistics entries.

Step 4 **end**

Return to Privileged EXEC Mode.

Step 5 **copy running-config startup-config**

Save the settings in the configuration file.

The following example shows how to create Statistics entries 1 and 2 on the switch to monitor port 1/0/1 and 1/0/2, respectively. The owner of the entries are both monitor and the status are both valid:

Switch#configure

Switch(config)#rmon statistics 1 interface gigabitEthernet 1/0/1 owner monitor status valid

Switch(config)#rmon statistics 2 interface gigabitEthernet 1/0/2 owner monitor status valid

Switch(config)#show rmon statistics

Index	Port	Owner	State
-----	----	-----	-----
1	Gi1/0/1	monitor	valid
2	Gi1/0/2	monitor	valid

Switch(config)#end

Switch#copy running-config startup-config**5.2.2 Configuring History**

Step 1	configure Enter Global Configuration Mode.
Step 2	rmon history <i>index</i> interface { fastEthernet <i>port</i> gigabitEthernet <i>port</i> ten-gigabitEthernet <i>port</i> } [interval <i>seconds</i>] [owner <i>owner-name</i>] [buckets <i>number</i>] Configuring RMON History entries. <i>index</i> : Specify the index of the History entry, which ranges from 1 to 12. To configure multiple indexes, enter a list of indexes separated by commas, or use a hyphen to indicate a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. <i>port</i> : Specify the port to be bound to the entry. <i>seconds</i> : Set the sample interval. The values are from 10 to 3600 seconds, and the default is 1800 seconds. <i>owner-name</i> : Enter the owner name of the entry with 1 to 16 characters. The default name is monitor. <i>number</i> : Set the maximum number of records for the history entry. When the number of records exceeds the limit, the earliest record will be overwritten. The values are from 10 to 130; the default is 50.
Step 3	show rmon history [<i>index</i>] Displays the specified History entry and related configurations. To show multiple entries, enter a list of indexes separated by commas, or use a hyphen to indicate a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5. <i>index</i> : Enter the index of History entry that you want to view. Valid values are from 1 to 12. The command without any parameters displays all existing statistics entries.
Step 4	end Return to Privileged EXEC Mode.
Step 5	copy running-config startup-config Save the settings in the configuration file.

The following example shows how to create a History entry on the switch to monitor port 1/0/1. Set the sample interval as 100 seconds, maximum buckets as 50, and the owner as monitor:

Switch#configure

```
Switch(config)#rmon history 1 interface gigabitEthernet 1/0/1 interval 100 owner monitor buckets 50
```

Switch(config)#show rmon history

Index	Port	Interval	Buckets	Owner	State
1	Gi1/0/1	100	50	monitor	Enable

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

5.2.3 Configuring Event

Step 1	<p>configure</p> <p>Enter Global Configuration Mode.</p>
Step 2	<p>rmon event <i>index</i> [user <i>user-name</i>] [description <i>description</i>] [type { none log notify log-notify }] [owner <i>owner-name</i>]</p> <p>Configuring RMON Event entries.</p> <p><i>index</i>: Specify the index of the Event entry, which ranges from 1 to 12. To configure multiple indexes, enter a list of indexes separated by commas, or use a hyphen to indicate a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5.</p> <p><i>user-name</i>: Enter the SNMP user name or community name of the entry. The name should be what you have set in SNMP previously. The default name is public.</p> <p><i>description</i>: Give a description to the entry with 1 to 16 characters. By default, the description is empty.</p> <p>none log notify log-notify: Specify the action type of the event; then the switch will take the specified action to deal with the event. By default, the type is none. None indicates the switch takes no action, log indicates the switch records the event only, notify indicates the switch sends notifications to the NMS only, and log-notify indicates the switch records the event and sends notifications to the NMS.</p> <p><i>owner-name</i>: Enter the owner name of the entry with 1 to 16 characters. The default name is monitor.</p>
Step 3	<p>show rmon event [<i>index</i>]</p> <p>Displays the specified Event entry and related configurations. To show multiple entries, enter a list of indexes separated by commas, or use a hyphen to indicate a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5.</p> <p><i>index</i>: Enter the index of Event entry that you want to view. Valid values are from 1 to 12. The command without any parameters displays all existing statistics entries.</p>
Step 4	<p>end</p> <p>Return to Privileged EXEC Mode.</p>
Step 5	<p>copy running-config startup-config</p> <p>Save the settings in the configuration file.</p>

The following example shows how to create an Event entry on the switch. Set the user name as admin, the event type as Notify (set the switch to initiate notifications to the NMS), and the owner as monitor:

Switch#configure

```
Switch(config)#rmon event 1 user admin description rising-notify type notify owner monitor
```

Switch(config)#show rmon event

Index	User	Description	Type	Owner	State
-----	----	-----	----	-----	-----
1	admin	rising-notify	Notify	monitor	Enable

Switch(config)#end

```
Switch#copy running-config startup-config
```

5.2.4 Configuring Alarm

Step 1

configure

Enter Global Configuration Mode.

Step 2

```
rmon alarm index stats-index sindex [alarm-variable { revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-1518}] [s-type {absolute | delta}] [rising-threshold r-threshold] [rising-event-index r-event] [falling-threshold f-threshold] [falling-event-index f-event] [a-type {rise | fall | all}] [owner owner-name] [interval interval]
```

Configuring RMON alarm entries.

index: Specify the index of the Alarm entry, which ranges from 1 to 12. To configure multiple indexes, enter a list of indexes separated by commas, or use a hyphen to indicate a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5.

sindex: Specify the index of the related Statistics entry, which ranges from 1 to 65535.

revbyte | *revpkt* | *bpkt* | *mpkt* | *crc-align* | *undersize* | *oversize* | *jabber* | *collision* | *64* | *65-127* | *128-255* | *256-511* | *512-1023* | *1024-1518*: Choose an alarm variable to monitor. The switch will monitor the specified variable in sample intervals and act in the set way when the alarm is triggered. The default variable is revbyte.

revbyte means total number of received bytes; *revpkt* means total number of received packets; *bpkt* means total number of broadcast packets. *mpkt* means total number of multicast packets; *crc-align* means packets that contain FCS Error or Alignment Error, within a size of 64 to 1518 bytes; *undersize* means packets that are smaller than 64 bytes; *oversize* means packets that are larger than 1518 bytes; *jabber* means packets that are sent when port collisions occur; *collision* means the collision times in the network segment; *64* | *65-127* | *128-255* | *256-511* | *512-1023* | *1024-1518* means total number of packets of the specified size.

absolute | delta: Choose the sampling method of the specified variable. The default is absolute. In the absolute mode, the switch compares the sampling value against the preset threshold; in the delta mode, the switch obtains the difference between the sampling values of the current interval and the previous interval, and then compares the difference against the preset threshold.

r-threshold: Enter the rising threshold. Valid values are from 1 to 2147483647, and the default is 100. The rising threshold should be larger than the falling threshold.

r-event: Enter the index of the Event entry that will be triggered when the sampling value or the difference value exceeds the preset threshold. Valid values are from 1 to 12. The Event entry specified here should be enabled first.

f-threshold: Enter a falling threshold. Valid values are from 1 to 2147483647, and the default is 100. The falling threshold should be less than the rising threshold.

f-event: Enter the index of the Event entry that will be triggered when the sampling value or the difference value is below the preset threshold. Valid values are from 1 to 12. The Event entry specified here should be enabled first.

rise | fall | all: Choose an alarm type; the default is all. Rise indicates that the alarm is triggered only when the sampling value or difference value exceeds the rising threshold. Fall indicates that the alarm is triggered only when the sampling value or difference value is below the falling threshold. All indicates that the alarm is triggered when the sampling value or difference value either exceeds the rising threshold or is below the falling threshold.

owner-name: Enter the owner name of the entry using 1 to 16 characters. The default name is monitor.

interval: Set the sampling interval. The value ranges from 10 to 3600 seconds; the default is 1800 seconds.

Step 3 **show rmon alarm [index]**

Displays the specified alarm entry and related configurations. To show multiple entries, enter a list of indexes separated by commas, or use a hyphen to indicate a range of indexes. For example, 1-3, 5 indicates 1, 2, 3, 5.

index: Enter the index of Alarm entry that you want to view. Valid values are from 1 to 12. The command without any parameters displays all existing statistics entries.

Step 4 **end**

Return to Privileged EXEC Mode.

Step 5 **copy running-config startup-config**

Save the settings in the configuration file.

The following example shows how to set an alarm entry to monitor BPPackets on the switch. Set the related Statistics entry index as 1, the sample type as Absolute, the rising threshold as 3000, the related rising event entry index as 1, the falling threshold as 2000, the related falling event index as 2, the alarm type as all, the notification interval as 10 seconds, and the owner of the entry as monitor:

Switch#configure

```
Switch(config)#rmon alarm 1 stats-index 1 alarm-variable bpkt s-type absolute rising-  
threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2 a-type  
all interval 10 owner monitor
```

```
Switch(config)#show rmon alarm
```

```
Index-State:    1-Enabled  
Statistics index: 1  
Alarm variable: BPkt  
Sample Type:   Absolute  
RHold-REvent: 3000-1  
FHold-FEvent: 2000-2  
Alarm startup: All  
Interval:      10  
Owner:         monitor
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

6 Configuration Example

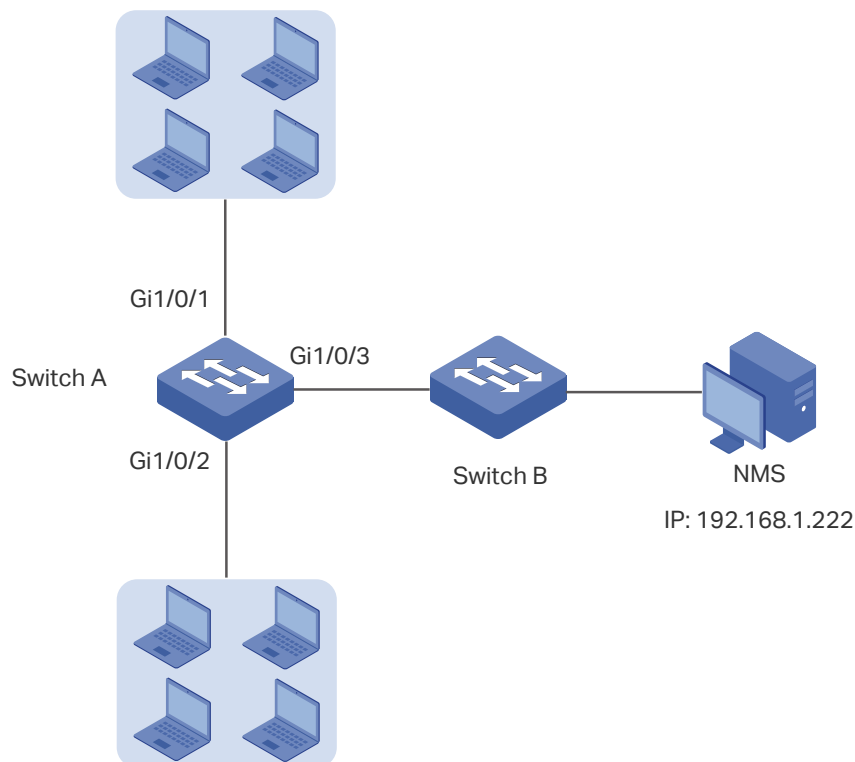
6.1 Network Requirements

The following figure shows the network topology of a company. The company has requirements as follows:

- 1) Monitor storm traffic of ports 1/0/1 and 1/0/2 on Switch A, and send notifications to the NMS when the actual rate of broadcast, multicast or unknown-unicast packets exceeds the preset threshold.
- 2) Monitor the traffic of ports 1/0/1 and 1/0/2 on Switch A, and regularly collect and save data for follow-up checks. Specifically, Switch A should notify the NMS when the number of packets transmitted and received on the ports during the sample interval exceeds the preset rising threshold, and should record but not notify the NMS when that is below the preset falling threshold.

The NMS host with IP address 192.168.1.222 is connected to the core switch, Switch B. Switch A is connected to Switch B via port 1/0/3. Port 1/0/3 and the NMS can reach one another.

Figure 6-1 Network Topology



6.2 Configuration Scheme

- 1) On Switch A, set thresholds for broadcast, multicast and unknown-unicast packets on ports 1/0/1 and 1/0/2. Enable SNMP and configure the corresponding parameters. Enable Trap notifications on the ports. Switch A can then send notifications to the NMS when the rate of storm traffic exceeds the preset threshold.
- 2) After SNMP and Notification configurations, create Statistic entries on the ports to monitor the real-time transmitting and receiving of packets and create History entries to regularly collect and save related data. Create two Event entries: one is the Notify type used to notify the NMS, and the other is the Log type used to record related events.
- 3) Create an Alarm entry to monitor RecPackets (Received Packets). Configure the rising and falling thresholds. Configure the rising event as the Notify event entry, and the falling event as the Log event entry.

Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

6.3 Using the GUI

■ Configuring Storm Control on Ports

Configure Storm Control on the required ports. For detailed configuration, refer to *Configuring QoS*.

■ Configuring SNMP

- 1) Choose **MAINTENANCE > SNMP > Global Config** to load the following page. In the **Global Config** section, enable SNMP, and set the Remote Engine ID as 123456789a. Click **Apply**.

Figure 6-2 Enabling SNMP

Global Config

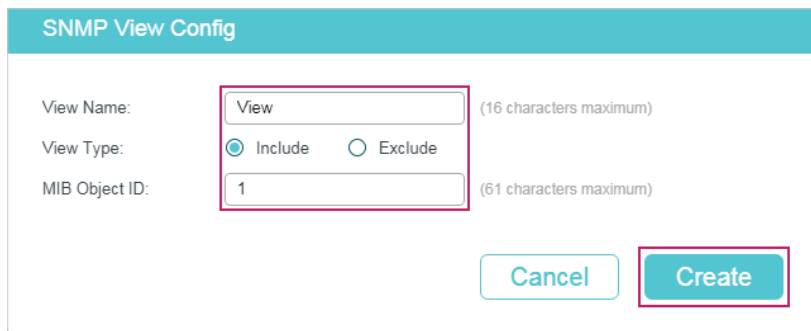
SNMP: Enable

Local Engine ID: Default ID (10-64 Hex)

Remote Engine ID: (Null or 10-64 Hex)

- 2) In the **SNMP View Config** section, click **+ Add** to load the following page. Name the SNMP view as View, set the view type as Include, and set MIB Object ID as 1 (which means all functions). Click **Create**.

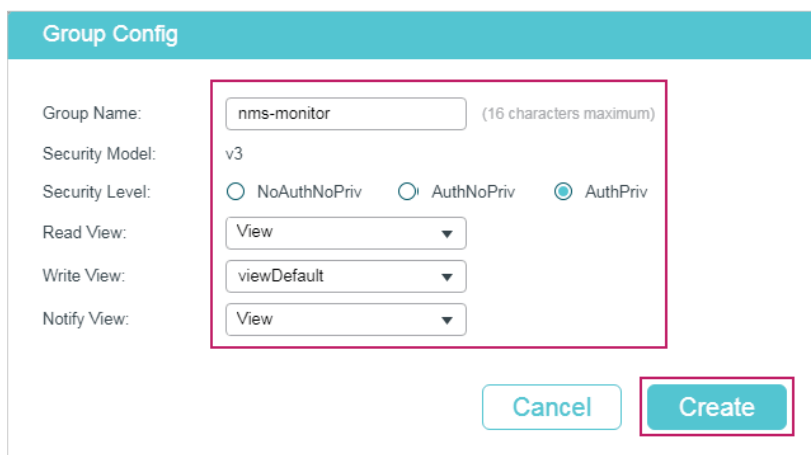
Figure 6-3 Creating an SNMP View



The image shows the 'SNMP View Config' form. It has a teal header. The form contains three input fields: 'View Name' with the value 'View' and a note '(16 characters maximum)', 'View Type' with radio buttons for 'Include' (selected) and 'Exclude', and 'MIB Object ID' with the value '1' and a note '(61 characters maximum)'. At the bottom right, there are two buttons: 'Cancel' and 'Create'.

- 3) Choose **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** and click **+** Add to load the following page. Create a group named nms-monitor, enable authentication and privacy, and add View to Read View and Notify View. Click **Create**.

Figure 6-4 Configuring an SNMP Group



The image shows the 'Group Config' form. It has a teal header. The form contains several fields: 'Group Name' with the value 'nms-monitor' and a note '(16 characters maximum)', 'Security Model' set to 'v3', 'Security Level' with radio buttons for 'NoAuthNoPriv', 'AuthNoPriv', and 'AuthPriv' (selected), 'Read View' with a dropdown menu showing 'View', 'Write View' with a dropdown menu showing 'viewDefault', and 'Notify View' with a dropdown menu showing 'View'. At the bottom right, there are two buttons: 'Cancel' and 'Create'.

- 4) Choose **MAINTENANCE > SNMP > SNMP v3 > SNMP User** and click **+** Add to load the following page. Create a user named admin for the NMS, set the user type as Remote User and specify the group name. Set the Security Level in accordance with that of the group nms-monitor. Choose SHA authentication algorithm and DES privacy algorithm, and set corresponding passwords. Click **Create**.

Figure 6-5 Creating an SNMP User

The screenshot shows the 'User Config' form with the following fields and values:

- User Name: admin (16 characters maximum)
- User Type: Local User Remote User
- Group Name: nms-monitor
- Security Model: v3
- Security Level: NoAuthNoPriv AuthNoPriv AuthPriv
- Authentication Mode: MD5 SHA
- Authentication Password: **** (16 characters maximum)
- Privacy Mode: DES
- Privacy Password: **** (16 characters maximum)

Buttons: Cancel, Create

- 5) Choose **MAINTENANCE > SNMP > Notification > Notification Config** and click Add to load the following page. Choose the IP Mode as IPv4, and specify the IP address of the NMS host and the port of the host for transmitting notifications. Specify the User as admin and choose the type as Inform. Set the retry times as 3, with the timeout period as 100 seconds. Click **Create**.

Figure 6-6 Creating an SNMP Notification Entry

The screenshot shows the 'Notification Config' form with the following fields and values:

- IP Mode: IPv4 IPv6
- IP Address: 192.168.1.222 (Format: 192.168.0.1)
- UDP Port: 162 (0-65535)
- User: admin
- Security Mode: v1 v2c v3
- Security Level: NoAuthNoPriv AuthNoPriv AuthPriv
- Type: Trap Inform
- Retry Times: 3 (1-255)
- Timeout: 100 (1-3600)

Buttons: Cancel, Create

- 6) Choose **MAINTENANCE > SNMP > Notification > Trap Config** to load the following page. Enable Storm Control trap and click **Apply**.

Figure 6-7 Enabling Storm Control Trap

SNMP Traps

<input checked="" type="checkbox"/> SNMP Authentication	<input checked="" type="checkbox"/> Coldstart	<input checked="" type="checkbox"/> Warmstart
<input checked="" type="checkbox"/> Link Status	<input type="checkbox"/> CPU Utilization	<input type="checkbox"/> Memory Utilization
<input type="checkbox"/> Flash Operation	<input type="checkbox"/> VLAN Create/Delete	<input type="checkbox"/> IP Change
<input checked="" type="checkbox"/> Storm Control	<input type="checkbox"/> Rate Limit	<input type="checkbox"/> LLDP
<input type="checkbox"/> Loopback Detection	<input type="checkbox"/> Spanning Tree	<input type="checkbox"/> IP-MAC Binding
<input type="checkbox"/> IP Duplicate	<input type="checkbox"/> DHCP Filter	<input type="checkbox"/> DDM Temperature
<input type="checkbox"/> DDM Voltage	<input type="checkbox"/> DDM Bias Current	<input type="checkbox"/> DDM TX Power
<input type="checkbox"/> DDM RX Power	<input type="checkbox"/> ACL Counter	

Apply

7) Click Save to save the settings.

■ **Configuring RMON**

1) Choose **MAINTENANCE > SNMP > RMON > Statistics** and click Add to load the following page. Create Statistics entries 1 and 2, and bind them to ports 1/0/1 and 1/0/2, respectively. Set the owner of the entries as monitor and the status as Valid.

Figure 6-8 Configuring Statistics Entry 1

Statistics Config

Index: (1-65535)

Port: **Choose** (Format: 1/0/1)

Owner: (16 characters maximum)

Status: Valid Under Creation

Cancel **Create**

Figure 6-9 Configuring Statistics Entry 2

Statistics Config

Index: (1-65535)

Port: **Choose** (Format: 1/0/1)

Owner: (16 characters maximum)

Status: Valid Under Creation

Cancel **Create**

2) Choose the menu **MAINTENANCE > SNMP > RMON > History** to load the following page. Configure entries 1 and 2. Bind entries 1 and 2 to ports 1/0/1 and 1/0/2, respectively. Set the Interval as 100 seconds, Maximum Buckets as 50, the owner of the entries as monitor, and the status as enabled.

Figure 6-10 Configuring the History Entries

History Control Config						
<input type="checkbox"/>	Index	Port	Interval (seconds)	Maximum Buckets	Owner	Status
<input type="checkbox"/>	1	1/0/1	100	50	monitor	Enabled
<input type="checkbox"/>	2	1/0/2	100	50	monitor	Enabled
<input type="checkbox"/>	3	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	4	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	5	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	6	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	7	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	8	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	9	1/0/1	1800	50	monitor	Disabled
<input type="checkbox"/>	10	1/0/1	1800	50	monitor	Disabled
Total: 12						

- Choose the menu **MAINTENANCE > SNMP > RMON > Event** to load the following page. Configure entries 1 and 2. For entry 1, set the SNMP user name as admin, type as Notify, description as "rising_notify", owner as monitor, and status as enable. For entry 2, set the SNMP user name as admin, type as Log, description as "falling_log", owner as monitor, and status as enabled.

Figure 6-11 Configuring the Event Entries

Event Config						
<input type="checkbox"/>	Index	User	Description	Action Mode	Owner	Status
<input type="checkbox"/>	1	admin	rising_notify	Notify	monitor	Enabled
<input type="checkbox"/>	2	admin	falling_log	Log	monitor	Enabled
<input type="checkbox"/>	3	public		None	monitor	Disabled
<input type="checkbox"/>	4	public		None	monitor	Disabled
<input type="checkbox"/>	5	public		None	monitor	Disabled
<input type="checkbox"/>	6	public		None	monitor	Disabled
<input type="checkbox"/>	7	public		None	monitor	Disabled
<input type="checkbox"/>	8	public		None	monitor	Disabled
<input type="checkbox"/>	9	public		None	monitor	Disabled
<input type="checkbox"/>	10	public		None	monitor	Disabled
Total: 12						

- Choose **MAINTENANCE > SNMP > RMON > Alarm** to load the following page. Configure entries 1 and 2. For entry 1, set the alarm variable as RecPackets, related statistics entry ID as 1 (bound to port 1/0/1), the sample type as Absolute, the rising threshold as 3000, associated rising event entry ID as 1 (which is the notify type), the falling threshold as 2000, the associated falling event entry ID as 2 (which is the log type), the alarm type as All, the interval as 10 seconds, the owner name as monitor. For entry 2, set the associated statistics entry ID as 2 (bound to port 1/0/2). Other configurations are the same as those of entry 1.

Figure 6-12 Configuring the Alarm Entries

<input type="checkbox"/>	Index	Variable	Statistics	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Alarm Type	Interval (seconds)	Owner	Status
<input type="checkbox"/>	1	RecPackets	1	Absolute	3000	1	2000	2	All	10	monitor	Enabled
<input type="checkbox"/>	2	RecPackets	2	Absolute	3000	1	2000	2	All	10	monitor	Enabled
<input type="checkbox"/>	3	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	Disabled
<input type="checkbox"/>	4	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	Disabled
<input type="checkbox"/>	5	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	Disabled
<input type="checkbox"/>	6	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	Disabled
<input type="checkbox"/>	7	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	Disabled
<input type="checkbox"/>	8	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	Disabled
<input type="checkbox"/>	9	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	Disabled
<input type="checkbox"/>	10	RecBytes	0	Absolute	100	0	100	0	All	1800	monitor	Disabled

Total: 12

- 5) Click  to save settings.

6.4 Using the CLI

■ Configuring Storm Control on ports

Configure the Storm Control on the required ports of Switch A. For detailed configuration, refer to *Configuring QoS*.

■ Configuring SNMP

- 1) Enable SNMP and specify the remote engine ID.

```
Switch_A#configure
```

```
Switch_A(config)#snmp-server
```

```
Switch_A(config)#snmp-server engineID remote 123456789a
```

- 2) Create a view with the name View; set the MIB Object ID as 1 (which represents all functions), and the view type as Include.

```
Switch_A(config)#snmp-server view View 1 include
```

- 3) Create a group of SNMPv3 with the name of nms-monitor. Enable Auth Mode and Privacy Mode, and set both the Read and Notify views as View.

```
Switch_A(config)#snmp-server group nms-monitor smode v3 slev authPriv read View notify View
```

- 4) Create an SNMP user named admin. Set the user as a remote user and configure the security model and security level based on the group. Set the Auth Mode as SHA algorithm, password as 1234, the Privacy Mode as DES, and password as 1234.

```
Switch_A(config)#snmp-server user admin remote nms-monitor smode v3 slev authPriv cmode SHA cpwd 1234 emode DES epwd 1234
```

- 5) To configure Notification, specify the IP address of the NMS host and UDP port. Set the User, Security Model and Security Level according to configurations of the SNMP User.

Choose the type as Inform, and set the retry times as 3, and the timeout period as 100 seconds.

```
Switch_A(config)#snmp-server host 192.168.1.222 162 admin smode v3 slev authPriv  
type inform retries 3 timeout 100
```

■ Enable storm-control Trap

```
Switch_A(config)#snmp-server traps storm-control
```

■ Configuring RMON

- 1) Create Statistics entries 1 and 2 to monitor ports 1/0/1 and 1/0/2, respectively. The owner of the entries is set as monitor, and the status is set as valid.

```
Switch_A(config)#rmon statistics 1 interface gigabitEthernet 1/0/1 owner monitor  
status valid
```

```
Switch_A(config)#rmon statistics 2 interface gigabitEthernet 1/0/2 owner monitor  
status valid
```

- 2) Create History entries 1 and 2 and bind them to ports 1/0/1 and 1/0/2, respectively. Set the sample interval as 100 seconds, max buckets as 50, and the owner as monitor.

```
Switch_A(config)#rmon history 1 interface gigabitEthernet 1/0/1 interval 100 owner  
monitor buckets 50
```

```
Switch_A(config)#rmon history 2 interface gigabitEthernet 1/0/2 interval 100 owner  
monitor buckets 50
```

- 3) Create Event entries 1 and 2 for the SNMP user admin. Set entry 1 as the Notify type and its description as "rising_notify". Set entry 2 as the Log type and its description as "falling_log". Set the owner of them as monitor.

```
Switch_A(config)#rmon event 1 user admin description rising_notify type notify owner  
monitor
```

```
Switch_A(config)#rmon event 2 user admin description falling_log type log owner  
monitor
```

- 4) Create Alarm entries 1 and 2. For entry 1, set the alarm variable as RecPackets, associated Statistics entry ID as 1 (bound to port 1/0/1), the sample type as Absolute, the rising threshold as 3000, the associated rising event entry ID as 1 (Notify type), the falling threshold as 2000, the associated falling event entry ID as 2 (the log type), the alarm type as all, the interval as 10 seconds, and the owner name as monitor. For entry 2, set the associated statistics entry ID as 2 (bound to port 1/0/2), while all other configurations are the same as those of entry 1.

```
Switch_A(config)#rmon alarm 1 stats-index 1 alarm-variable revpkt s-type absolute  
rising-threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2  
a-type all interval 10 owner monitor
```

```
Switch_A(config)#rmon alarm 2 stats-index 2 alarm-variable revpkt s-type absolute  
rising-threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2  
a-type all interval 10 owner monitor
```

Verify the Configurations

Verify global SNMP configurations:

```
Switch_A(config)#show snmp-server
```

SNMP agent is enabled.

```
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 1500)  
    0  No such name errors  
    0  Bad value errors  
    0  General errors  
    0  Response PDUs  
    0  Trap PDUs
```

Verify SNMP engine ID:

```
Switch_A(config)#show snmp-server engineID
```

Local engine ID: 80002e5703000aeb13a23d

Remote engine ID: 123456789a

Verify SNMP view configurations:

Switch_A(config)#show snmp-server view

No.	View Name	Type	MOID
1	viewDefault	include	1
2	viewDefault	exclude	1.3.6.1.6.3.15
3	viewDefault	exclude	1.3.6.1.6.3.16
4	viewDefault	exclude	1.3.6.1.6.3.18
5	View	include	1

Verify SNMP group configurations:

Switch_A(config)#show snmp-server group

No.	Name	Sec-Mode	Sec-Lev	Read-View	Write-View	Notify-View
1	nms-monitor	v3	authPriv	View		View

Verify SNMP user configurations:

Switch_A(config)#show snmp-server user

No.	U-Name	U-Type	G-Name	S-Mode	S-Lev	A-Mode	P-Mode
1	admin	remote	nms-monitor	v3	authPriv	SHA	DES

Verify SNMP host configurations:

Switch_A(config)#show snmp-server host

No.	Des-IP	UDP	Name	SecMode	SecLev	Type	Retry	Timeout
1	172.168.1.222	162	admin	v3	authPriv	inform	3	100

Verify RMON statistics configurations:

Switch_A(config)#show rmon statistics

Index	Port	Owner	State
1	Gi1/0/1	monitor	valid
2	Gi1/0/2	monitor	valid

Verify RMON history configurations:

Switch_A(config)#show rmon history

Index	Port	Interval	Buckets	Owner	State
1	Gi1/0/1	100	50	monitor	Enable
2	Gi1/0/2	100	50	monitor	Enable

Verify RMON event configurations:

Switch_A(config)#show rmon event

Index	User	Description	Type	Owner	State
1	admin	rising_notify	Notify	monitor	Enable
2	admin	falling_log	Log	monitor	Enable

Verify RMON alarm configurations:

Switch_A(config)#show rmon alarm

```

Index-State:      1-Enabled
Statistics index: 1
Alarm variable:   RevPkt
Sample Type:     Absolute
RHold-REvent:    3000-1
FHold-FEvent:    2000-2
Alarm startup:    All
Interval:         10
Owner:            monitor

```

Index-State: 2-Enabled
Statistics index: 2
Alarm variable: RevPkt
Sample Type: Absolute
RHold-REvent: 3000-1
FHold-FEvent: 2000-2
Alarm startup: All
Interval: 10
Owner: monitor

7 Appendix: Default Parameters

Default settings of SNMP are listed in the following tables.

Table 7-1 Default Global Config Settings

Parameter	Default Setting
SNMP	Disabled
Local Engine ID	Automatically
Remote Engine ID	None

Table 7-2 Default SNMP View Table Settings

View Name	View Type	MIB Object ID
viewDefault	Include	1
viewDefault	Exclude	1.3.6.1.6.3.15
viewDefault	Exclude	1.3.6.1.6.3.16
viewDefault	Exclude	1.3.6.1.6.3.18

Table 7-3 Default SNMP v1/v2c Settings

Parameter	Default Setting
Community Entry	No entries
Community Name	None
Access	Read-only
MIB View	viewDefault

Table 7-4 Default SNMP v3 Settings

Parameter	Default Setting
SNMP Group	
Group Entry	No entries
Group Name	None
Security Model	v3
Security Level	NoAuthNoPriv
Read View	viewDefault
Write View	None
Notify View	None

Parameter	Default Setting
SNMP User	
User Entry	No entries
User Name	None
User Type	Local User
Group Name	None
Security Model	v3
Security Level	noAuthNoPriv
Authentication Mode	MD5 (when Security Level is configured as AuthNoPriv or AuthPriv)
Authentication Password	None
Privacy Mode	DES (when Security Level is configured as AuthPriv)
Privacy Password	None

Default settings of Notification are listed in the following table.

Table 7-5 Default Notification Settings

Parameter	Default Setting
Notification Config	
Notification Entry	No entries
IP Mode	IPv4
IP Address	None
UDP Port	162
User	None
Security Model	v1
Security Level	noAuthNoPriv
Type	Trap
Retry	None
Timeout	None
Trap Config	
Enabled SNMP Traps	SNMP Authentication, Coldstart, Warmstart, Link Status

Default settings of RMON are listed in the following tables.

Table 7-6 Default Statistics Config Settings

Parameter	Default Setting
Statistics Entry	No entries
ID	None
Port	None
Owner	None
IP Mode	Valid

Table 7-7 Default Settings for History Entries

Parameter	Default Setting
Port	1/0/1
Interval	1800 seconds
Max Buckets	50
Owner	monitor
Status	Disabled

Table 7-8 Default Settings for Event Entries

Parameter	Default Setting
User	public
Description	None
Type	None
Owner	monitor
Status	Disabled

Table 7-9 Default Settings for Alarm Entries

Parameter	Default Setting
Variable	RecBytes
Statistics	0, means no Statistics entry is selected.
Sample Type	Absolute
Rising Threshold	100
Rising Event	0, means no event is selected.
Falling Threshold	100
Falling Event	0, means no event is selected.
Alarm Type	All

Parameter	Default Setting
Interval	1800 seconds
Owner	monitor
Status	Disabled