Configurar SNMP y RMON

CAPITULOS

1. SNMP
2. Configuraciones SNMP
3. Configuraciones de Notificaciones
4. RMON
5. Configuraciones RMON
6. Ejemplo de configuracion
7. Apéndice: Parámetros predeterminados

Esta guía se aplica a:

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

1 SNMP

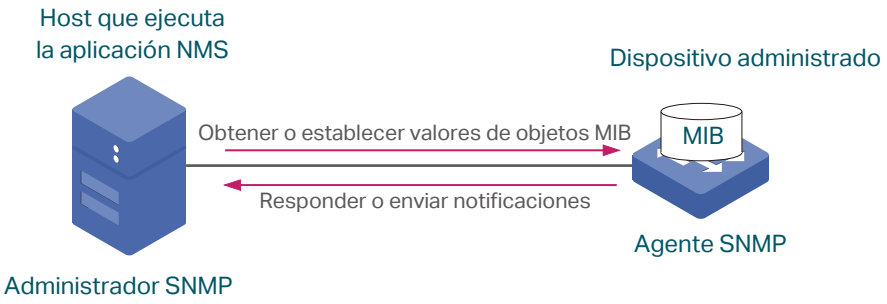
1.1 Visión general

SNMP (Simple Network Management Protocol) es un protocolo estándar de administración de red, ampliamente utilizado en redes TCP/IP. Facilita la gestión de dispositivos mediante aplicaciones NMS (Network Management System). Con SNMP, los administradores de red pueden ver o modificar la información de los dispositivos de red, y solucionar problemas de manera oportuna de acuerdo con las notificaciones enviadas por esos dispositivos.

Como se muestra en la siguiente figura, el sistema SNMP consta de un administrador SNMP, un agente SNMP y una MIB (Base de información de administración).

El administrador SNMP es un host que ejecuta aplicaciones NMS. El agente y la MIB residen en el dispositivo administrado, como el conmutador, el enrutador, el host o la impresora. Al configurar SNMP en el conmutador, usted define la relación entre el administrador y el agente.

Figure 1-1 Sistema SNMP



1.2 Conceptos básicos

Se presentarán los siguientes conceptos básicos de SNMP: administrador de SNMP, agente de SNMP, MIB (Management Information Base) significa Base de información de administración, entidad de SNMP, motor de SNMP, tipos de notificación y versión de SNMP.

Administrador/ Manager SNMP

El administrador SNMP usa SNMP para monitorear y controlar los agentes SNMP, proporcionando una interfaz de administración amigable para que el administrador administre los dispositivos de red de manera conveniente.

Puede obtener valores de objetos MIB de un agente o establecer valores para ellos. Además, recibe notificaciones de los agentes para conocer el estado de la red.

Agente/Agent SNMP

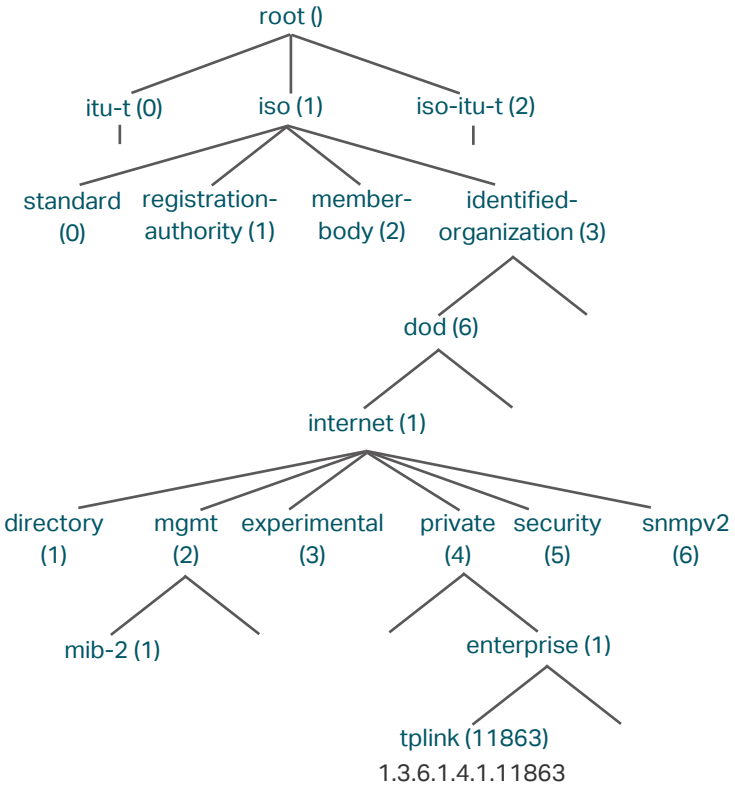
Un agente SNMP es un proceso que se ejecuta en el dispositivo administrado. Contiene objetos MIB cuyos valores pueden ser solicitados o establecidos por el administrador SNMP. Un agente puede enviar mensajes de captura no solicitados para notificar al administrador de SNMP que se ha producido un evento significativo en el agente.

MIB

Una MIB es una colección de objetos gestionados que se organiza jerárquicamente. Los objetos definen los atributos del dispositivo administrado, incluidos los nombres, el estado, los derechos de acceso y los tipos de datos. Cada objeto puede ser direccionado a través de un identificador de objeto (OID).

Como muestra la siguiente figura, la jerarquía MIB se puede representar como un árbol con una raíz sin nombre, cuyos niveles son asignados por diferentes organizaciones. Las ID de objeto MIB de nivel superior pertenecen a diferentes organizaciones estándar, mientras que las ID de objeto de nivel inferior son asignadas por organizaciones asociadas. Los proveedores pueden definir sucursales privadas que incluyen objetos administrados para sus propios productos.

Figure 1-2 MIB Tree



Los switches TP-Link proporcionan MIB privadas que pueden identificarse mediante el OID 1.3.6.1.4.1.11863. El archivo MIB se puede encontrar en el CD provisto o en el centro de descargas de nuestro sitio web oficial: *https://www.tp-link.com/download-center.html* .

Además, los switches TP-Link admiten las siguientes MIB públicas:

- 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

Para obtener información detallada sobre las MIB públicas compatibles, consulte *MIB públicas admitidas para Switches TP-Link*.

Entidad/Entity SNMP

Una entidad SNMP es un dispositivo que ejecuta el protocolo SNMP. Tanto el administrador SNMP como el agente SNMP son entidades SNMP.

Motor/Engine SNMP

Un motor SNMP es parte de la entidad SNMP. Cada entidad SNMP tiene un solo motor. Un motor SNMP proporciona servicios para enviar y recibir mensajes, autenticar y cifrar mensajes, y controlar el acceso a los objetos administrados.

Un motor SNMP puede identificarse de forma exclusiva mediante una ID de motor dentro de un dominio administrativo. Dado que existe una asociación uno a uno entre los motores SNMP y las entidades SNMP, también podemos usar la ID del motor para identificar de forma exclusiva la entidad SNMP dentro de ese dominio administrativo.

Tipos de notificaciones

Las notificaciones son mensajes que el switch envía al host NMS cuando ocurren eventos importantes. Las notificaciones facilitan el monitoreo y la gestión del NMS. Hay dos tipos de notificaciones:

- **Captura/Trap**: cuando el host NMS recibe un mensaje de captura, no enviará una respuesta al switch. Por lo tanto, el switch no puede determinar si se recibe un mensaje o no, y los mensajes que no se reciben no se reenviarán.

- **Informe/Inform**: cuando el host NMS recibe un mensaje de Informe, envía una respuesta al switch. Si el switch no recibe ninguna respuesta dentro del intervalo de tiempo de espera, reenviará el mensaje Informe. Por lo tanto, Informe es más confiable que Captura.

Versión SNMP

El dispositivo admite tres versiones de SNMP con un nivel de seguridad de menor a mayor: SNMPv1, SNMPv2c y SNMPv3. *Tabla 1-1* sus características son compatibles con diferentes versiones de SNMP, y *Tabla 1-2* muestra los escenarios de aplicación correspondientes.

Tabla 1-1 Funciones compatibles con diferentes versiones de SNMP

Feature	SNMPv1	SNMPv2c	SNMPv3
Control de acceso	Basado en la comunidad SNMP y la vista MIB	Basado en la comunidad SNMP y la vista MIB	Basado en la vista de usuario, grupo y MIB de SNMP
Autenticación y privacidad	Basado en el nombre de la comunidad	Basado en el nombre de la comunidad	Los modos de autenticación y privacidad admitidos son los siguientes: Autenticación: MD5 / SHA Privacidad: DES
Captura/Trap	Soportado	Soportado	Soportado
Informe/Inform	No soportado	Soportado	Soportado

Tabla 1-2 Escenarios de aplicación de diferentes versiones

Version	Escenario de aplicación
SNMPv1	SNMPv1 es aplicable a redes de pequeña escala con redes simples, buena estabilidad y requisitos de baja seguridad, como redes de campus y redes de pequeñas empresas.
SNMPv2c	SNMPv2c es aplicable a redes de mediana y gran escala con bajos requisitos de seguridad (o que ya son lo suficientemente seguras como las redes VPN) y tráfico pesado. La función agregada Inform ayuda a garantizar que el host NMS reciba las notificaciones del switch incluso cuando se produce una congestión de la red.
SNMPv3	SNMPv3 es aplicable a redes de varias escalas, particularmente aquellas que tienen requisitos de alta seguridad y requieren que los dispositivos sean administrados por administradores autenticados (como cuando los datos deben transferirse en redes públicas).

2 Configuraciones SNMP

Para completar la configuración de SNMP, elija una versión de SNMP de acuerdo con los requisitos de red y la compatibilidad de la aplicación NMS, y luego siga estos pasos:

■ Elija SNMPv1 o SNMPv2c

1) Habilitar SNMP.
2) Cree una vista SNMP para objetos gestionados.
3) Cree una comunidad, especifique la vista accesible y los derechos de acceso correspondientes.

■ Elija SNMPv3

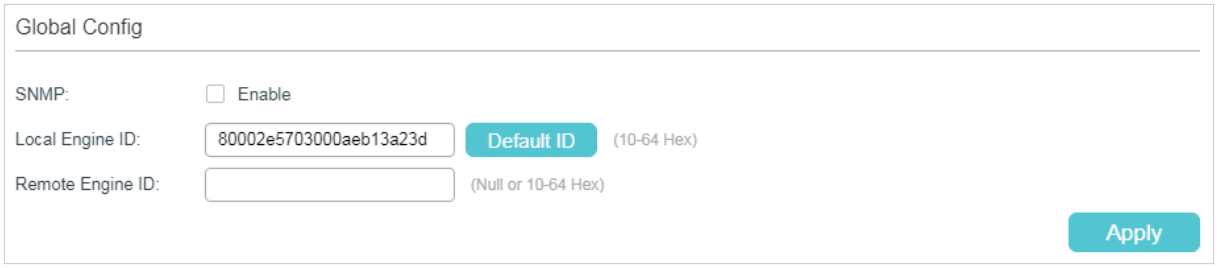
1) Habilitar SNMP.
2) Cree una vista SNMP para objetos gestionados.
3) Cree un grupo SNMP y especifique el nivel de seguridad y la vista accesible.
4) Cree usuarios SNMP y configure el modo de autenticación, el modo de privacidad y las contraseñas correspondientes.

2.1 Usando la GUI

2.1.1 Habilitar SNMP

Elija MAINTENANCE > SNMP > Global Config para cargar la siguiente página.

Figura 2-1 Configuración de parámetros globales



Siga estos pasos para configurar SNMP globalmente:

1) En la sección Configuración global, habilite SNMP y configure el ID del motor local y remoto.

SNMP	Habilitar o deshabilitar SNMP a nivel mundial.

Local Engine ID/ ID del motor local	Establezca la ID del motor del agente SNMP local (el switch) con 10 a 64 dígitos hexadecimales. Una ID de motor válida debe contener un número par de caracteres. De manera predeterminada, el switch genera la ID del motor utilizando el número de empresa de TP-Link (80002e5703) y su propia dirección MAC. La ID del motor local es una cadena alfanumérica única utilizada para identificar el motor SNMP. Como un agente SNMP contiene solo un motor SNMP, la ID del motor local puede identificar de forma exclusiva al agente SNMP.
Remote Engine ID/ ID remota del motor	Establezca la ID del motor del administrador SNMP remoto con 10 a 64 dígitos hexadecimales. Una ID de motor válida debe contener un número par de caracteres. Si no se necesita un administrador SNMP remoto, puede dejar este campo vacío. La ID remota del motor es una cadena alfanumérica única. Se utiliza para identificar el motor SNMP en el dispositivo remoto que recibe los mensajes Inform del switch.

2) Clic en **Apply**.

Nota:

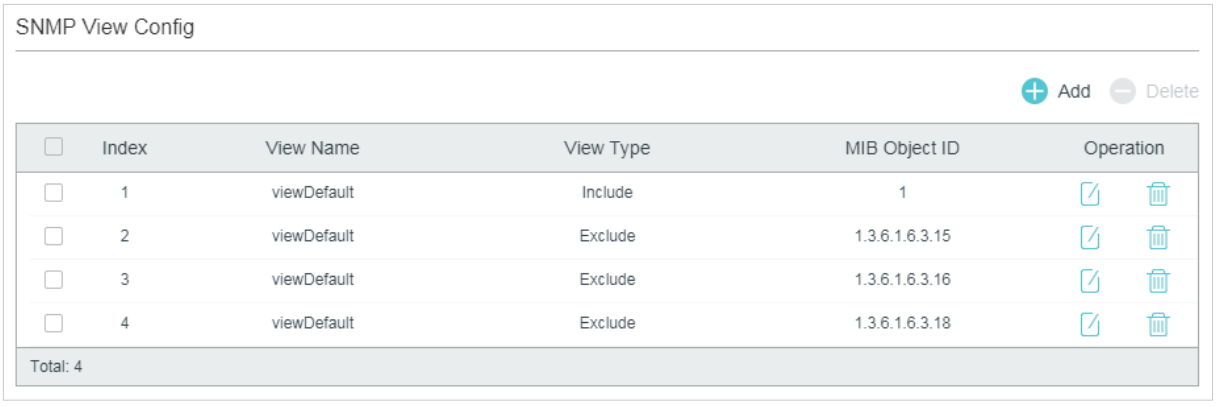
En SNMPv3, cambiar el valor de la ID del motor SNMP tiene importantes efectos secundarios. La contraseña de un usuario se convierte en un resumen de seguridad MD5 o SHA en función de la contraseña y la ID del motor. Si el valor de la ID del motor local cambia, el switch eliminará automáticamente todos los usuarios locales de SNMPv3 a medida que sus resúmenes de seguridad se vuelvan inválidos. Del mismo modo, todos los usuarios remotos de SNMPv3 se eliminarán si cambia el valor de la ID remota del motor.

2.1.2 Crear una vista SNMP

Una vista SNMP es una subred de una MIB. NMS gestiona objetos MIB basados en la vista. El sistema tiene una vista predeterminada llamada viewDefault. Puede crear una nueva o editar la vista predeterminada según sus necesidades.

Elija el menú **MAINTENANCE > SNMP > Global Config** para cargar la siguiente página.

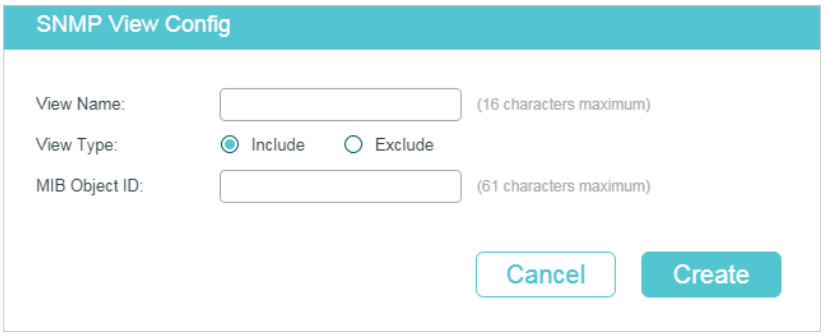
Figura 2-2 Configuración de vista SNMP



Siga estos pasos para crear una vista SNMP:

1) Clic Add para cargar la siguiente página. Ingrese un nombre de vista y especifique el tipo de vista y un ID de objeto MIB relacionado con la vista.

Figura 2-3 Crear una vista SNMP



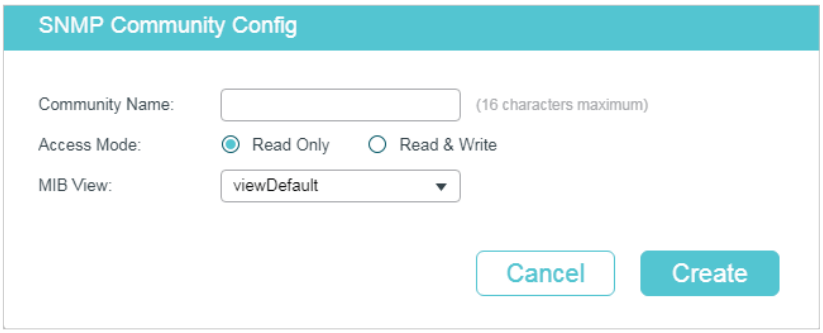
View Name	Establezca el nombre de la vista con 1 a 16 caracteres. Una vista completa consta de todos los objetos MIB que tienen el mismo nombre de vista.
View Type	Configure la vista para incluir o excluir el objeto MIB relacionado. **Include**: el NMS puede ver o administrar la función indicada por el objeto. **Exclude**: el NMS no puede ver ni administrar la función indicada por el objeto.
MIB Object ID	Ingrese una ID de objeto MIB para especificar una función específica del dispositivo. Cuando se especifica una ID de objeto MIB, se especifican todas sus ID de objeto hijo. Para conocer las reglas de identificación específicas, consulte las MIB relacionadas con el dispositivo.

2) clic en **Create**.

2.1.3 Creación de comunidades SNMP (para SNMP v1 / v2c)

Elija el menú MAINTENANCE > SNMP > SNMP v1/v2c y haga clic en la Add para cargar la página siguiente.

Figura 2-4 Creación de una comunidad SNMP



Siga estos pasos para crear una comunidad SNMP:

1) Establezca el nombre de la comunidad, los derechos de acceso y la vista relacionada.

Community Name	Configurar el nombre de la comunidad. Este nombre de comunidad se usa como una contraseña y el NMS puede acceder a los objetos MIB especificados del switch utilizando el mismo nombre de comunidad.

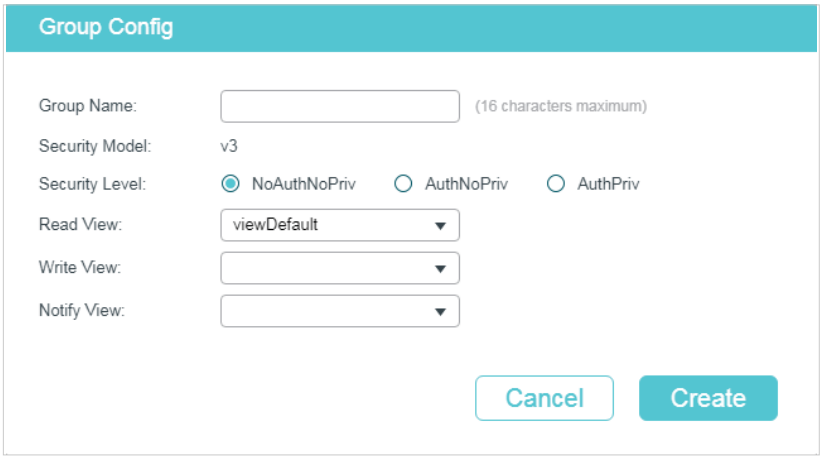
Access Mode	Especifique el derecho de acceso a la vista relacionada. **Read Only**: el NMS puede ver pero no modificar los parámetros de la vista especificada. **Read & Write**: el NMS puede ver y modificar los parámetros de la vista especificada.
MIB View	Elija una vista SNMP que permita el acceso de la comunidad.

2) clic en **Create**.

2.1.4 Crear un grupo SNMP (para SNMP v3)

Elija el menú **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** haga clic en para Add cargar la siguiente página.

Figura 2-5 Creación de un grupo SNMP



Siga estos pasos para crear un grupo SNMP y configurar parámetros relacionados.

1) Asigne un nombre al grupo, luego establezca el nivel de seguridad y la vista de lectura, vista de escritura y vista de notificación.

Group Name	Establezca el nombre del grupo SNMP con 1 a 16 caracteres. El identificador de un grupo consta de un nombre de grupo, modelo de seguridad y nivel de seguridad. Los grupos del mismo identificador se reconocen como pertenecientes al mismo grupo.
Security Model	Muestra el modelo de seguridad. SNMPv3 usa v3, el modelo más seguro.
Security Level	Establezca el nivel de seguridad para el grupo SNMPv3. **NoAuthNoPriv:** No hay algoritmo de autenticación, pero se aplica una coincidencia de nombre de usuario para verificar los paquetes, y no se aplica ningún algoritmo de privacidad para cifrarlos. **AuthNoPriv:**Se aplica un algoritmo de autenticación para verificar los paquetes, pero no se aplica ningún algoritmo de privacidad para cifrarlos. **AuthPriv:** Se aplican un algoritmo de autenticación y un algoritmo de privacidad para verificar y cifrar paquetes.

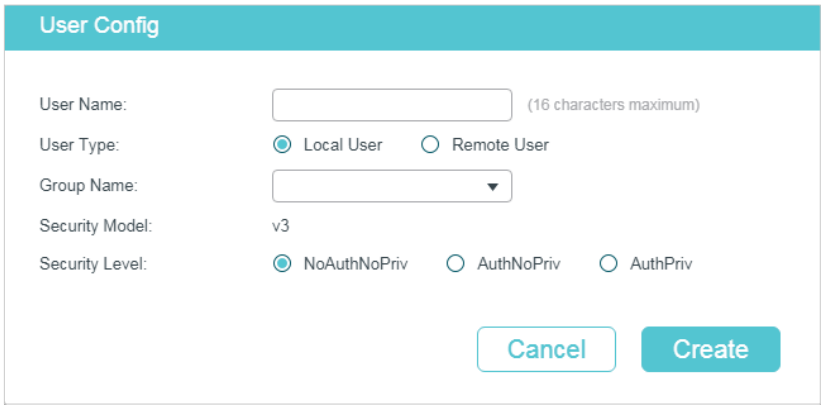
Read View	Elija una vista para permitir que los parámetros sean vistos pero no modificados por el NMS. La vista es necesaria para cualquier grupo.
Write View	Elija una vista para permitir que los parámetros sean modificados por el NMS. La vista en la Vista de escritura también se debe agregar a la Vista de lectura.
Notify View	Elija una vista para permitirle enviar notificaciones al NMS.

2) clic en **Create**.

2.1.5 Creación de usuarios SNMP (para SNMP v3)

Elija el menú MAINTENANCE > SNMP > SNMP v3 > SNMP User y haga clic para Add cargar la siguiente página.

Figura 2-6 Creación de un usuario SNMP



Siga estos pasos para crear un usuario SNMP:

1) Especifique el nombre de usuario y el tipo de usuario, así como el grupo al que pertenece el usuario. Luego configure el nivel de seguridad.

User Name	Establezca el nombre de usuario SNMP con 1 a 16 caracteres. Para diferentes entradas, los nombres de usuario no pueden ser iguales.
User Type	Elija un tipo de usuario basado en la ubicación del usuario. **Local User:** El usuario reside en el motor local, que es el agente SNMP del switch. **Remote User:** El usuario reside en el NMS. Antes de configurar un usuario remoto, primero debe configurar la ID remota del motor. La identificación remota del motor y la contraseña del usuario se utilizan al calcular los resúmenes de autenticación y privacidad.
Group Name	Elija el nombre del grupo al que pertenece el usuario. Los usuarios con el mismo nombre de grupo, modelo de seguridad y nivel de seguridad estarán en el mismo grupo.
Security Model	Muestra el modelo de seguridad. SNMPv3 usa v3, el modelo más seguro.

Security Level	Establecer el nivel de seguridad. El nivel de seguridad de menor a mayor es: NoAuthNoPriv, AuthNoPriv, AuthPriv. El nivel de seguridad del usuario no debe ser inferior al grupo al que pertenece. **NoAuthNoPriv:** No hay algoritmo de autenticación, pero se aplica una coincidencia de nombre de usuario para verificar los paquetes, y no se aplica ningún algoritmo de privacidad para cifrarlos. **AuthNoPriv:** Se aplica un algoritmo de autenticación para verificar los paquetes, pero no se aplica ningún algoritmo de privacidad para cifrarlos. **AuthPriv:** Se aplican un algoritmo de autenticación y un algoritmo de privacidad para verificar y cifrar paquetes.

2) Si has elegido **AuthNoPriv** o **AuthPriv** como nivel de seguridad, debe configurar el modo de autenticación o el modo de privacidad correspondientes. Si no, omita este paso.

Authentication Mode	With AuthNoPriv o AuthPriv seleccionado, configure el modo de autenticación y la contraseña para la autenticación. Se proporcionan dos modos de autenticación: **MD5:** Habilite el algoritmo HMAC-MD5 para la autenticación. **SHA:** Habilite el algoritmo SHA (algoritmo de hash seguro) para la autenticación. El algoritmo SHA es más seguro que el algoritmo MD5.
Authentication Password	Establece la contraseña para la autenticación.
Privacy Mode	With AuthPriv seleccionado, configure el modo de privacidad y la contraseña para el cifrado. El conmutador utiliza el algoritmo DES (estándar de cifrado de datos) para el cifrado.
Privacy Password	Establezca la contraseña para el cifrado.

3) Clic en **Create**.

2.2 Usando CLI

2.2.1 Habilitando SNMP

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**snmp-server** Habilitar SNMP.

Paso 3	**snmp-server engineID** {[**local** *local-engineID*] [**remote***remote-engineID*]} Configure la ID del motor local y la ID del motor remoto. *local-engineID:* Ingrese la ID del motor del agente SNMP local (el Switch) con 10 a 64 dígitos hexadecimales. Una ID de motor válida debe contener un número par de caracteres. De manera predeterminada, el switch genera la ID del motor utilizando el número de empresa de TP-Link (80002e5703) y su propia dirección MAC El local engine ID es una cadena alfanumérica única utilizada para identificar el motor SNMP. Como un agente SNMP contiene solo un motor SNMP, la ID del motor local puede identificar de forma exclusiva al agente SNMP. *remote-engineID:* Ingrese la ID remota del motor con 10 a 64 dígitos hexadecimales. Una ID de motor válida debe contener un número par de caracteres. La ID remota del motor es una cadena alfanumérica única. Se utiliza para identificar el motor SNMP en el dispositivo remoto que recibe mensajes de información del Switch. *Nota:* En SNMPv3, cambiar el valor de la ID del motor SNMP tiene importantes efectos secundarios. La contraseña de un usuario se convierte en un resumen de seguridad MD5 o SHA en función de la contraseña y la ID del motor. Si el valor de la ID del motor local cambia, el switch eliminará automáticamente todos los usuarios locales de SNMPv3 a medida que sus resúmenes de seguridad se vuelvan inválidos. Del mismo modo, todos los usuarios remotos de SNMPv3 se eliminarán si cambia el valor de la ID remota del motor.
Paso 4	**show snmp-server** Muestra la configuración global de SNMP.
Paso 5	**show smnp-server engineID** Muestra la ID del motor de SNMP.
Paso 6	**end** Regrese al modo EXEC privilegiado.
Paso 7	**copy running-config startup-config** Guarde la configuración en el archivo de configuración

El siguiente ejemplo muestra cómo habilitar SNMP y configurar 123456789a como la ID remota del motor:

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 Crear una vista SNMP

Especifique el OID (Object Identifier) de la vista para determinar los objetos que se administrarán.

Paso 1	**configure** Ingrese al modo de configuración global.

Paso 2	**snmp-server view** *name mib-oid* {include | exclude} Configura la vista. *name:* Ingrese un nombre de vista con 1 a 16 caracteres. Puede crear múltiples entradas con cada una asociada a un objeto MIB. Una vista completa consta de todos los objetos MIB que tienen el mismo nombre de vista. *mib-oid:* Ingrese la ID del objeto MIB con 1 a 61 caracteres. Cuando se especifica una ID de objeto MIB, se especifican todas sus ID de objeto hijo. Para conocer las reglas de identificación específicas, consulte las MIB relacionadas con el dispositivo. include | exclude: Especifique un tipo de vista. Incluir indica que los objetos de la vista pueden ser administrados por el NMS, mientras que la exclusión indica que los objetos de la vista no pueden ser administrados por el NMS.
Paso 3	**show snmp-server view** Muestra la tabla de vista.
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración

El siguiente ejemplo muestra cómo configurar una vista para permitir que el NMS administre todas las funciones. Asigne un nombre a la vista como Vista:

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 Creación de comunidades SNMP (para SNMP v1 / v2c)

Para SNMPv1 y SNMPv2c, el Nombre de comunidad se utiliza para la autenticación, que funciona como contraseña.

Paso 1	**configure** Ingrese al modo de configuración global
Paso 2	**snmp-server community** *name* { read-only | read-write } [*mib-view*] Configura la comunidad. *name:* Ingrese un nombre de grupo con 1 a 16 caracteres *read-only | read-write:* Elija un permisos de acceso para la comunidad. Solo lectura indica que el NMS puede ver pero no puede modificar los parámetros de la vista, mientras que la lectura y escritura indica que el NMS puede ver y modificar. *mib-view:* Ingrese una vista para permitir que la comunidad acceda a ella. El nombre contiene de 1 a 61 caracteres. La vista predeterminada es viewDefault.
Paso 3	**show snmp-server community** Muestra entradas de la comunidad.
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración

El siguiente ejemplo muestra cómo configurar una comunidad SNMP. Asigne un nombre a la comunidad como nms-monitor y permita que el NMS vea y modifique los parámetros de Vista:

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 Crear un grupo SNMP (para SNMPv3)

Cree un grupo SNMP y configure el control de acceso del usuario con vistas de lectura, escritura y notificación. Mientras tanto, configure los modos de autenticación y privacidad para asegurar la comunicación entre el NMS y los dispositivos administrados.

Paso 1	**configure** Ingrese al modo de configuración global

Paso 2	**snmp-server group** *name* [**smode** v3] [**slev** {noAuthNoPriv | authNoPriv | authPriv}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] Crea un grupo SNMP. *name:* Ingrese el nombre del grupo con 1 a 16 caracteres. El identificador de un grupo consta de un nombre de grupo, modelo de seguridad y nivel de seguridad. Los grupos del mismo identificador se reconocen como pertenecientes al mismo grupo. v3: Configure el modelo de seguridad para el grupo. v3 indica SNMPv3, el modelo más seguro. noAuthNoPriv | authNoPriv | authPriv: Elige un nivel de seguridad. Los niveles de seguridad se ordenan de menor a mayor, y el valor predeterminado es noAuthNoPriv. noAuthNoPriv indica que no hay algoritmo de autenticación, pero se aplica una coincidencia de nombre de usuario para verificar los paquetes, y no se aplica ningún algoritmo de privacidad para cifrarlos. authNoPriv indica que se aplica un algoritmo de autenticación para verificar los paquetes, pero no se aplica ningún algoritmo de privacidad para cifrarlos. authPriv indica que se aplica un algoritmo de autenticación y un algoritmo de privacidad para verificar y cifrar paquetes. *read-view:* Configure la vista para que sea la vista de lectura. Entonces el NMS puede ver los parámetros de la vista especificada. *write-view:* Configure la vista para que sea la vista de escritura. Luego, el NMS puede modificar los parámetros de la vista especificada. Tenga en cuenta que la vista en la vista Escribir también debe estar en la vista Leer. *notify-view:* Configure la vista para que sea la vista Notificar. Luego, el NMS puede recibir notificaciones de la vista especificada del agente.
Paso 3	**show snmp-server group** Muestra entradas de grupo SNMP.
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo crear un grupo SNMPv3 con el nombre del grupo como nms1, el nivel de seguridad como authPriv y la vista Leer y Notificar son ambas Vistas:

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 Creación de usuarios SNMP (para SNMPv3)

Cree usuarios SNMP y agréguelos al grupo SNMP. Los usuarios en el mismo grupo tienen los mismos derechos de acceso, que se definen al crear el grupo.

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	Elija un nivel de seguridad para el usuario y ejecute el comando correspondiente para crear el usuario. Los niveles de seguridad de menor a mayor son NoAuthNoPriv, AuthNoPriv y AuthPriv. El nivel de seguridad de un usuario no debe ser inferior al del grupo al que pertenece. Para crear un usuario con el nivel de seguridad como NoAuthNoPriv: **snmp-server user** *name* { local | remote } *group-name* [**smode** v3] **slev** noAuthNoPriv *name:* Ingrese el nombre de usuario con 1 a 16 caracteres local | remote: Elija un tipo de usuario basado en la ubicación del usuario. Local indica que el usuario reside en el motor SNMP local (el switch), mientras que remoto indica que el usuario reside en el NMS. Antes de configurar un usuario remoto, primero debe configurar la ID remota del motor. La identificación remota del motor y la contraseña del usuario se utilizan al calcular los resúmenes de autenticación y privacidad. *group-name:* Ingrese el nombre del grupo al que pertenece el usuario. Los usuarios con el mismo nombre de grupo, modelo de seguridad y nivel de seguridad estarán en el mismo grupo. *v3:* Configure el modelo de seguridad para el usuario. v3 indica SNMPv3, el modelo más seguro. noAuthNoPriv: Configure el nivel de seguridad como noAuthNoPriv. Para este nivel, no se aplica ningún algoritmo de autenticación, pero se aplica una coincidencia de nombre de usuario para verificar los paquetes, y no se aplica ningún algoritmo de privacidad para cifrarlos. Para crear un usuario con el nivel de seguridad como AuthNoPriv: **snmp-server user** *name* { local | remote } *group-name* [**smode** v3] **slev** authNoPriv **cmode** {MD5 | SHA } **cpwd** *confirm-pwd* authNoPriv: Configure el nivel de seguridad como authNoPriv. Para este nivel, se aplica un algoritmo de autenticaciÐn para verificar los paquetes, pero no se aplica ningĕn algoritmo de MD5|SHA: elija un algoritmo de autenticación cuando el nivel de seguridad esté configurado como authNoPriv o authPriv. El modo de autenticación SHA tiene una mayor seguridad que el modo MD5. Por defecto, el modo de autenticación es ninguno *confirm-pwd:* Ingrese una contraseña de autenticación con 1 a 16 caracteres excluyendo el signo de interrogación y el espacio. Esta contraseña en el archivo de configuración se mostrará en forma cifrada simétrica. Para crear un usuario con la seguridad como AuthPriv: **snmp-server user** *name* { local | remote } *group-name* [**smode** v3] **slev** authPriv **cmode** {MD5 | SHA } **cpwd** *confirm-pwd* **emode** DES **epwd** *encrypt-pwd* authPriv:Configure el nivel de seguridad como authPriv. Para este nivel, se aplican un algoritmo de autenticación y un algoritmo de privacidad para verificar y cifrar paquetes. DES:Configure el modo de privacidad como DES. El switch utilizará el algoritmo DES para cifrar los paquetes. Por defecto, el modo de privacidad es ninguno. *encrypt-pwd:* Ingrese una contraseña de privacidad con 1 a 16 caracteres excluyendo el signo de interrogación y el espacio. Esta contraseña en el archivo de configuración se mostrará en forma cifrada simétrica.

Paso 3	**show snmp-server user** Muestra la información de los usuarios de SNMP..
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo crear un usuario SNMP remoto llamado admin y agregarlo al grupo nms1. La configuración de seguridad es la Tabla 2-1:

Tabla 2-1 Configuración de seguridad para el usuario

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 Configuraciones de notificaciones

Con la Notificación habilitada, el switch puede enviar notificaciones al NMS sobre eventos importantes relacionados con el funcionamiento del dispositivo. Esto facilita el monitoreo y la gestión del NMS.

Para configurar la notificación SNMP, siga estos pasos:

1) Configure la información de los hosts NMS.
2) Habilitar trampas SNMP.

Pautas de configuración

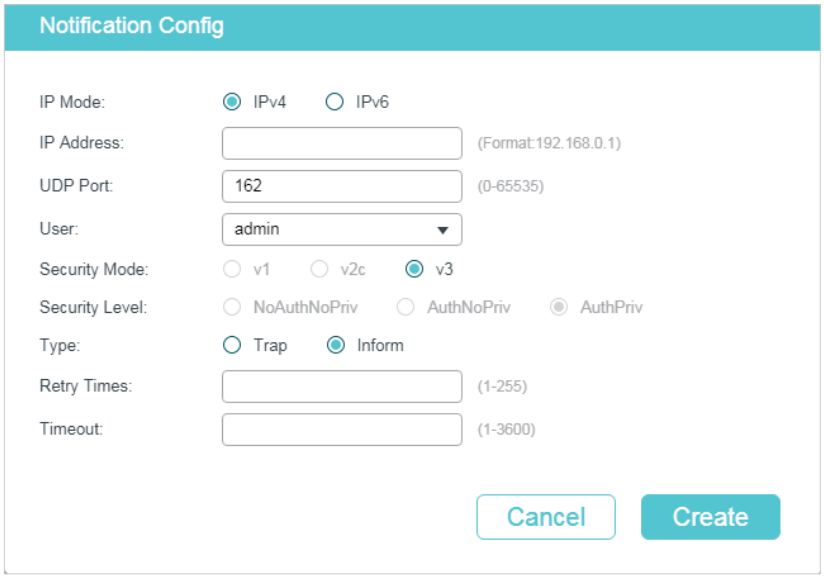
Para garantizar la comunicación entre el switch y el NMS, asegúrese de que el switch y el NMS puedan comunicarse entre sí

3.1 Usando la GUI

3.1.1 Configuración de la información de hosts NMS

Elige el menu **MAINTENANCE > SNMP > Notification > Notification Config** y haga clic en Add para cargar la siguiente página.

Figura 3-1 Agregar un host NMS



Siga estos pasos para agregar un host NMS:

1) Elija el modo IP de acuerdo con el entorno de red y especifique la dirección IP del host NMS y el puerto UDP que recibe las notificaciones.

IP Mode	Elija un modo IP para el host NMS.
IP Address	Si configura el Modo IP como IPv4, especifique una dirección IPv4 para el host NMS. Si configura el Modo IP como IPv6, especifique una dirección IPv6 para el host NMS.
UDP Port	Especifique un puerto UDP en el host NMS para recibir notificaciones. Por seguridad, le recomendamos que cambie el número de puerto bajo la condición de que las comunicaciones en otros puertos UDP no se vean afectadas.

2) Especifique el nombre de usuario o el nombre de la comunidad que usa el host NMS y configure el modelo de seguridad y el nivel de seguridad según el usuario o la comunidad.

User	Elija el nombre de usuario o el nombre de comunidad utilizado por el host NMS.
Security Model	Si se selecciona un nombre de comunidad (creado para SNMPv1 / v2c) en Usuario, especifique el modelo de seguridad como v1 o v2c. Si se selecciona un nombre de usuario (creado para SNMPv3) en Usuario, aquí se muestra el modelo de seguridad como v3. *Nota:* El host NMS debe usar la versión SNMP correspondiente.
Security Level	Si el modelo de seguridad es v3, aquí se muestra el nivel de seguridad del usuario.

3) Elija un tipo de notificación basado en la versión SNMP. Si elige el tipo de informe, debe establecer los tiempos de reintento y el intervalo de tiempo de espera.

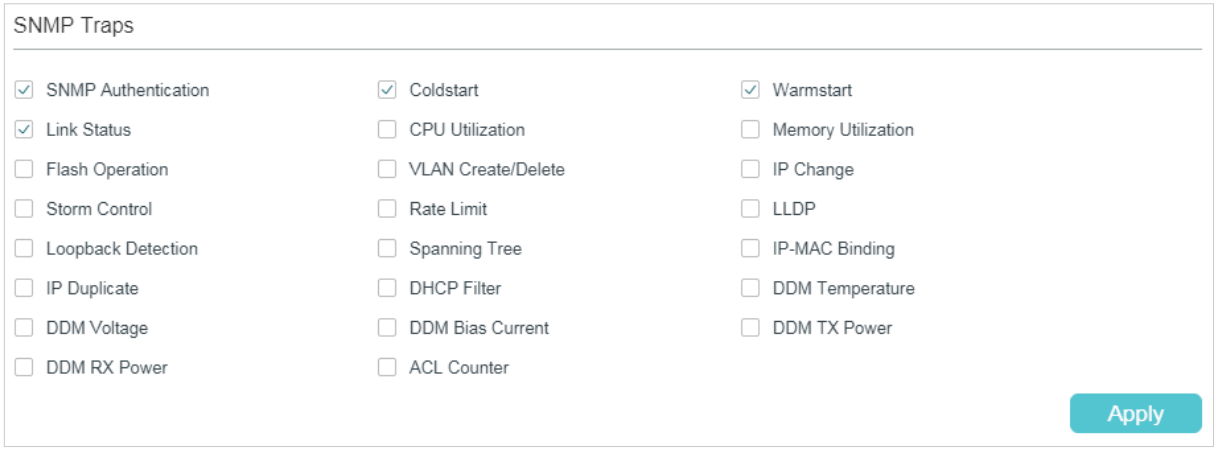
Type	Elija un tipo de notificación para el host NMS. Para SNMPv1, el tipo admitido es Trap. Para SNMPv2c y SNMPv3, puede configurar el tipo como Trap o Inform. **Trap:** El switch enviará mensajes de captura al host NMS cuando ocurran ciertos eventos. Cuando el host NMS recibe un mensaje de captura, no enviará una respuesta al switch. Por lo tanto, el switch no puede determinar si se recibe un mensaje o no, y los mensajes que no se reciben no se reenviarán. **Inform:** El switch enviará mensajes Inform al host NMS cuando ocurran ciertos eventos. Cuando el host NMS recibe un mensaje de Informe, envía una respuesta al switch. Si el switch no recibe ninguna respuesta dentro del intervalo de tiempo de espera, reenviará el mensaje Inform. Por lo tanto, Inform es más confiable que Trap.
Retry	Establezca los tiempos de reintento para Informes. El switch reenviará el mensaje Informar si no recibe ninguna respuesta del host NMS dentro del intervalo de tiempo de espera. Dejará de enviar mensajes de informe cuando el tiempo de reintento alcance el límite.
Timeout	Establezca el tiempo que el switch espera una respuesta del host NMS después de enviar un mensaje de informe.

4) Clic en **Create**.

3.1.2 Habilitación de SNMP Traps

Elige el menu **MAINTENANCE > SNMP > Notification > Trap Config** para cargar la siguiente página.

Figura 3-2 Habilitación de capturas SNMP



Siga estos pasos para habilitar algunas o todas las traps compatibles:

1) Seleccione las traps que se habilitarán según sus necesidades. Con una traps habilitada, el switch enviará el mensaje de trap correspondiente al NMS cuando se active la trap.

SNMP Authentication	Se activa cuando una solicitud SNMP recibida falla la autenticación.
Coldstart	Indica que la entidad SNMP se está reinicializando a sí misma de modo que sus configuraciones pueden cambiarse. La trap se puede activar cuando reinicia el interruptor.
Warmstart	Indica que la entidad SNMP se está reinicializando con sus configuraciones sin cambios. Para un conmutador que ejecuta SNMP, la trap se puede activar si deshabilita y luego habilita SNMP sin cambiar ningún parámetro.
Link Status	Active o desactive la trampa de estado de enlace de forma global. La trap incluye las siguientes dos sub-traps: **Linkup Trap**: Indica que el estado de un puerto cambia de linkdown a linkup. **Linkdown Trap**: Indica que el estado de un puerto cambia de linkup a linkdown. Link Status Trap se puede activar cuando está habilitado globalmente y en el puerto, y conecta un nuevo dispositivo al puerto o desconecta un dispositivo del puerto. Para habilitar la Trap en un puerto, ejecute el comando snmp-server traps link-status en el Modo de configuración de interfaz del puerto. Para deshabilitarlo, ejecute el comando no correspondiente. De forma predeterminada, la trap está habilitada tanto globalmente como en todos los puertos, lo que significa que los cambios en el estado del enlace en cualquier puerto activarán la trap. Si no desea recibir mensajes de notificación sobre algunos puertos específicos, desactive la captura en esos puertos.

CPU Utilization	Se activa cuando la utilización de la CPU supera el 80%.
Memory Utilization	Se activa cuando la utilización de la memoria supera el 80%.
Flash Operation	Se activa cuando se modifica el flash durante operaciones como copia de seguridad, restablecimiento, actualización de firmware e importación de configuración.
VLAN Create/Delete	Se activa cuando ciertas VLAN se crean o eliminan correctamente.
IP Change	Supervisa los cambios de las direcciones IP de las interfaces. La trap se puede activar cuando se cambia la dirección IP de cualquier interfaz.
Storm Control	Supervisa si la velocidad de storm rate ha alcanzado el límite que ha establecido. La trap se puede activar cuando la función Strom Control está habilitada y las tramas de broadcast/multicast/unknown-unicast se envían al puerto con una velocidad superior a la establecida.
Rate Limit	Supervisa si el ancho de banda ha alcanzado el límite establecido. La trap se puede activar cuando la función Límite de velocidad está habilitada y los paquetes se envían al puerto con una velocidad superior a la establecida.
LLDP	La trap incluye las siguientes sub-traps: **LLDP RemTablesChange**: Indica que el switch detecta un cambio de topología LLDP. La trap se puede activar al agregar o quitar un dispositivo remoto, y cuando la información de algunos dispositivos remotos caduca o no se puede almacenar en el switch debido a recursos insuficientes. Esta trap puede ser utilizada por un NMS para activar encuestas de mantenimiento de tablas de sistemas remotos LLDP. **LLDP TopologyChange**: Indica que el switch detecta un cambio de topología LLDP-MED (el cambio de topología de los puntos finales de medios). La trap se puede activar al agregar o quitar un punto final de medios que admita LLDP, como un teléfono IP. Una trap LLDP Remtableschange también se activará cada vez que se active la trap LLDP Topologychange.
Loopback Detection	Se activa cuando la función de detección de bucle invertido está habilitada y se detecta o borra un bucle invertido.
Spanning Tree	Indica cambios en el árbol de expansión. La trap se puede activar en las siguientes situaciones: un puerto cambia de estado de no reenvío a estado de reenvío o viceversa; un puerto recibe una BPDU TCN (Notificación de cambio de topología) o una BPDU de configuración con el conjunto de bits TC (Cambio de topología).

PoE	Solo para productos que admiten PoE. La trap incluye las siguientes sub-trapa: **Over-max-pwr-budget**: Se activa cuando la potencia total requerida por los PD conectados excede la potencia máxima que puede suministrar el switch PoE. **Port-pwr-change**: Se activa cuando un puerto comienza a suministrar energía o deja de suministrar energía. **Port-pwr-deny**: Se activa cuando el switch apaga los PD en los puertos PoE de baja prioridad. El switch los apaga para garantizar un funcionamiento estable de los otros PD cuando la potencia total requerida por los PD conectados excede el límite de potencia del sistema. **Port-pwr-over-30w**: Se activa cuando la potencia requerida por el PD conectado supera los 30 vatios. **Port-pwr-overload**: Se activa cuando la potencia requerida por el PD conectado excede la potencia máxima que el puerto puede suministrar. **Port-short-circuit**: Se activa cuando se detecta un cortocircuito en un puerto. **Thermal-shutdown**: Se activa cuando el chip PSE se sobrecalienta. El switch dejará de suministrar energía en este caso.
IP-MAC Binding	Triggered in the following two situations: la función de inspección ARP está habilitada y el switch recibe un paquete ARP ilegal; o la función IPv4 Source Guard está habilitada y el conmutador recibe un paquete IP ilegal.
IP Duplicate	Se activa cuando el switch detecta un conflicto de IP.
DHCP Filter	Se activa cuando la función Filtro DHCPv4 está habilitada y el switch recibe paquetes DHCP de un servidor DHCP ilegal.
DDM Temperature	Supervisa la temperatura de los módulos SFP insertados en los puertos SFP del conmutador. La trap se puede activar cuando la temperatura de cualquier módulo SFP ha alcanzado el umbral de advertencia o alarma. *Nota:* T2600G-52TS no es compatible con trap.
DDM Voltage	Supervisa el voltaje de los módulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando el voltaje de cualquier módulo SFP ha alcanzado el umbral de advertencia o alarma. *Nota:* T2600G-52TS no es compatible con esta trap.
DDM Bias Current	Supervisa la corriente de polarización de los módulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando la corriente de polarización de cualquier módulo SFP ha alcanzado el umbral de advertencia o alarma. *Nota:* T2600G-52TS no es compatible con esta trap.
DDM TX Power	Supervisa la potencia TX de los módulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando la potencia TX de cualquier módulo SFP ha alcanzado el umbral de advertencia o alarma. *Nota:* T2600G-52TS no es compatible con esta trap.

DDM RX Power	Supervisa la potencia RX de los módulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando la potencia RX de cualquier módulo SFP ha alcanzado el umbral de advertencia o alarma. *Nota:* T2600G-52TS no es compatible con esta trap.
ACL Counter	Supervisa la información de ACL coincidente, incluida la ID de ACL coincidente, la ID de regla y el número de paquetes coincidentes. Con esta trap y la función de Registro en la configuración de la regla de ACL habilitada, el switch verificará la información de ACL coincidente cada cinco minutos y enviará traps SNMP si hay información actualizada.

2) Clic en **Apply**.

3.2 Uso de la CLI

3.2.1 Configurando el NMS Host

Configure los parámetros del host NMS y el mecanismo de manejo de paquetes.

Paso 1	**configure** Ingrese al modo de configuración global.

Paso 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 los parámetros del host NMS y el mecanismo de manejo de paquetes. *ip:* Especifique la dirección IP del host NMS en IPv4 o IPv6. Asegúrese de que el host NMS y el switch puedan comunicarse entre sí. *udp-port:* Especifique un puerto UDP en el host NMS para recibir notificaciones. El valor predeterminado es el puerto 162. Para la seguridad de la comunicación, le recomendamos que cambie el número de puerto bajo la condición de que las comunicaciones en otros puertos UDP no se vean afectadas. *user-name:* Ingrese el nombre utilizado por el host NMS. Cuando el host NMS usa SNMPv1 o SNMPv2c, ingrese el Nombre de comunidad; cuando el host NMS use SNMPv3, ingrese el Nombre de usuario del Grupo SNMP. v1 | v2c | v3: Elija el modelo de seguridad utilizado por el usuario entre los siguientes: SNMPv1, SNMPv2c, SNMPv3. El host NMS debe usar la versión SNMP correspondiente. noAuthNoPriv | authNoPriv | authPriv: Para grupos SNMPv3, elija un nivel de seguridad de noAuthNoPriv (sin autorización y sin cifrado), authNoPriv (autorización y sin cifrado), authPriv (autorización y cifrado). El valor predeterminado es noAuthNoPriv. Tenga en cuenta que si ha elegido v1 o v2c como modelo de seguridad, el nivel de seguridad no se puede configurar. trap | inform: Elija un tipo de notificación para el host NMS. Para SNMPv1, el tipo admitido es Trap. Para SNMPv2c y SNMPv3, puede configurar el tipo como Trap o Inform. **Trap:** El switch enviará mensajes de captura al host NMS cuando ocurran ciertos eventos. Cuando el host NMS recibe un mensaje de captura, no enviará una respuesta al switch. Por lo tanto, el switch no puede determinar si se recibe un mensaje o no, y los mensajes que no se reciben no se reenviarán. **Inform:** El switch enviará mensajes Inform al host NMS cuando ocurran ciertos eventos. Cuando el host NMS recibe un mensaje de Inform, envía una respuesta al switch. Si el switch no recibe ninguna respuesta dentro del intervalo de tiempo de espera, reenviará el mensaje Inform. Por lo tanto, Inform es más confiable que Trap. *retries:* Establezca los tiempos de reintento para los mensajes Inform. El rango está entre 1 y 255 y el valor predeterminado es 3. El switch volverá a enviar el mensaje Inform si no recibe ninguna respuesta del host NMS dentro del intervalo de tiempo de espera. Y dejará de enviar el mensaje Inform cuando los tiempos de reintento alcancen el límite. *timeout:* Establezca el tiempo que el interruptor espera una respuesta. Los valores válidos son de 1 a 3600 segundos; El valor predeterminado es 100 segundos. El switch reenviará el mensaje Inform si no recibe una respuesta del host NMS dentro del intervalo de tiempo de espera.
Paso 3	**show snmp-server host** Verifique la información del host.
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar un host NMS con los parámetros que se muestran en *Tabla 3-1* .

Tabla 3-1 Parámetros para los hosts NMS

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 Habilitando SNMP Traps

El switch admite muchos tipos de SNMP Traps, como el estándar SNMP traps, las ACL traps y las VLAN traps, y los comandos correspondientes son diferentes. Con una trap habilitada, el switch enviará el mensaje de trap correspondiente al NMS cuando se active la trap. Siga estos pasos para habilitar las traps según sus necesidades.

■ Habilitar las SNMP Standard Traps Globalmente

Paso 1	**configure** Ingrese al modo de configuración global.

Paso 2	**snmp-server traps snmp [** linkup | linkdown | warmstart | coldstart | auth-failure **]** Habilite las trampas estándar SNMP correspondientes. El comando sin ningún parámetro habilita todas las trampas estándar SNMP. Por defecto, todas las trampas estándar SNMP están habilitadas. linkup | linkdown: Active Linkup Trap y Linkdown Trap globalmente. Linkup Trap indica que el estado de un puerto cambia de linkdown a linkup. La trap se puede activar cuando conecta un nuevo dispositivo al puerto, y la trap se habilita tanto globalmente como en el puerto. Linkdown Trap indica que el estado de un puerto cambia de linkup a linkdown. La trap se puede activar cuando desconecta un dispositivo del puerto, y la trap se habilita tanto globalmente como en el puerto. Para habilitar Linkup Trap y Linkdown Trap en un puerto,**ejecuta el comando snmp-server traps link-status** en el modo de configuración de interfaz del puerto. Para deshabilitarlos, ejecute el comando no correspondiente. De forma predeterminada, las traps están habilitadas globalmente y en todos los puertos, lo que significa que las traps se activarán cuando un dispositivo esté conectado o desconectado de cualquier puerto del switch. Si no desea recibir mensajes de notificación sobre algunos puertos específicos, desactive las traps en esos puertos. warmstart: Indica que la entidad SNMP se está reinicializando con sus configuraciones sin cambios. Para un switch que ejecuta SNMP, el trap se puede activar si deshabilita y luego habilita SNMP sin cambiar ningún parámetro. coldstart: Indica que la entidad SNMP se está reinicializando a sí misma de modo que sus configuraciones pueden cambiarse. La trampa se puede activar cuando reinicia el switch. auth-failure: Se activa cuando una solicitud SNMP recibida falla la autenticación.
Paso 3	**end** Regrese al modo EXEC privilegiado.
Paso 4	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el switch para enviar traps de enlace:

Switch#configure

Switch(config)#snmp-server traps snmp linkup

Switch(config)#end

Switch#copy running-config startup-config

■ Habilitar el SNMP Extended Traps Globalmente

Paso 1	**configure** Ingrese al modo de configuración global.

Paso 2	**snmp-server traps** { rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory } Habilite las SNMP extended traps correspondientes. Por defecto, todas las traps extendidas SNMP están deshabilitadas. rate-limit: Supervisa si el ancho de banda ha alcanzado el límite establecido. La trap se puede activar cuando la función Límite de velocidad está habilitada y los paquetes se envían al puerto con una velocidad superior a la establecida. cpu: Supervisa el estado de carga de la CPU del switch. La trap se puede activar cuando la tasa de utilización de la CPU supera el 80%. flash: Se activa cuando se modifica el flash durante operaciones como copia de seguridad, restablecimiento, actualización de firmware e importación de configuración. lldp remtableschange: Indica que el switch detecta un cambio de topología LLDP. La trap se puede activar al agregar o quitar un dispositivo remoto, y cuando la información de algunos dispositivos remotos caduca o no se puede almacenar en el switch debido a recursos insuficientes. Esta trap puede ser utilizada por un NMS para activar encuestas de mantenimiento de tablas de sistemas remotos LLDP. lldp topologychange: Indica que el switch detecta un cambio de topología LLDP-MED (el cambio de topología de los puntos finales de medios). La trap se puede activar al agregar o quitar un punto final de medios que admita LLDP, como un teléfono IP. Una trap LLDP Remtableschange también se activará cada vez que se active la trap LLDP Topologychange. loopback-detection: Se activa cuando la función de detección de bucle invertido está habilitada y se detecta o borra un bucle invertido. storm-control: Supervisa si la velocidad storm rate ha alcanzado el límite que ha establecido. La trap se puede activar cuando la función Control de Strom está habilitada y las tramas de broadcast/multicast/unknown-unicast se envían al puerto con una velocidad superior a la establecida. spanning-tree: Indica cambios en el árbol de expansión. La trap se puede activar en las siguientes situaciones: un puerto cambia de estado de no reenvío a estado de reenvío o viceversa; un puerto recibe una BPDU TCN (Notificación de cambio de topología) o una BPDU de configuración con el conjunto de bits TC (Cambio de topología). memory: Supervisa el estado de carga de la memoria del switch. La trap se puede activar cuando la utilización de la memoria supera el 80%.
Paso 3	**end** Regresar al modo EXEC privilegiado.
Paso 4	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el switch para habilitar traps de control de ancho de banda:

Switch#configure

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

Switch(config)#end

Switch#copy running-config startup-config

■ Habilitar el DDM Traps Globalmente

Note:

T2600G-52TS no es compatible con DDM traps.

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**snmp-server traps ddm** [temperature | voltage | bias_current | tx_power | rx_power] Habilite las DDM Traps correspondientes. La función DDM se usa para monitorear el estado de los módulos SFP insertados en los puertos SFP en el switch. El comando sin parámetro habilita todas las traps SNMP DDM. Por defecto, todas las traps DDM están deshabilitadas. temperature: Supervisa la temperatura de los mĎdulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando la temperatura de cualquier mĎdulo SFP ha alcanzado el umbral de advertencia o alarma. voltage: Supervisa el voltaje de los mĎdulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando el voltaje de cualquier mĎdulo SFP ha alcanzado el umbral de advertencia o alarma. bias_current: Supervisa la corriente de polarizaciĎn de los mĎdulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando la corriente de polarizaciĎn de cualquier mĎdulo SFP ha alcanzado el umbral de advertencia o alarma. tx_power: Supervisa la potencia TX de los mĎdulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando la potencia TX de cualquier mĎdulo SFP ha alcanzado el umbral de advertencia o alarma. rx_power: Supervisa la potencia RX de los mĎdulos SFP insertados en los puertos SFP del switch. La trap se puede activar cuando la potencia RX de cualquier mĎdulo SFP ha alcanzado el umbral de advertencia o alarma.
Paso 3	**end** Regrese al modo EXEC privilegiado.
Paso 4	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el switch para habilitar la trap de temperatura DDM:

Switch#configure

Switch(config)#snmp-server traps ddm temperature

Switch(config)#end

Switch#copy running-config startup-config

■ Habilitar VLAN Traps Globalmente

Paso 1	**configure** Ingrese al modo de configuración global.

Paso 2	**snmp-server traps vlan** [create | delete] Habilite las VLAN traps correspondientes. El comando sin parámetro habilita todas las VLAN SNMP traps. Por defecto, todas las traps de VLAN están deshabilitadas. create: Se activa cuando ciertas VLAN se crean con éxito. delete: Se activa cuando ciertas VLAN se eliminan correctamente.
Paso 3	**end** Regrese al modo EXEC privilegiado.
Paso 4	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el switch para habilitar todas las VLAN SNMP Traps:

Switch#configure

Switch(config)#snmp-server traps vlan

Switch(config)#end

Switch#copy running-config startup-config

■ Habiltar SNMP Security Traps Globalmente

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**snmp-server traps security** { dhcp-filter | ip-mac-binding } Habilite las traps de seguridad correspondientes. Por defecto, todas las traps de seguridad están deshabilitadas. dhcp-filter: Se activa cuando la función Filtro DHCPv4 está habilitada y el switch recibe paquetes DHCP de un servidor DHCP ilegal. ip-mac-binding: Se activa cuando la función de inspección ARP está habilitada y el switch recibe un paquete ARP ilegal, o la función de protección de fuente IPv4 está habilitada y el switch recibe un paquete IP ilegal.
Paso 3	**end** Regrese al modo EXEC privilegiado.
Paso 4	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el switch para habilitar la captura de filtro DHCP:

Switch#configure

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

Switch(config)#end

Switch#copy running-config startup-config

■ Habilitar ACL Trap Globalmente

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**snmp-server traps security acl** Habilitar el ACL trap. por defecto, este viene deshabilitado. La trap supervisa la información de ACL coincidente, incluida la ID de ACL coincidente, la ID de regla y el número de paquetes coincidentes. Con esta trap y la función de Registro en la configuración de la regla de ACL habilitada, el switch verificará la información de ACL coincidente cada cinco minutos y enviará traps SNMP si hay información actualizada.
Paso 3	**end** Regresar al modo EXEC privilegiado.
Paso 4	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el switch para habilitar la ACL trap:

Switch#configure

Switch(config)#snmp-server traps acl

Switch(config)#end

Switch#copy running-config startup-config

■ Habilitar la IP Traps Globalmente

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**snmp-server traps ip** { change | duplicate } Habilite las IP traps. Por defecto, todas las traps de IP están deshabilitadas. change: Supervisa los cambios de las direcciones IP de las interfaces. La trap se puede activar cuando se cambia la dirección IP de cualquier interfaz. duplicate: Se activa cuando el switch detecta un conflicto de IP.
Paso 3	**end** Regrese al modo EXEC privilegiado.
Paso 4	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el conmutador para habilitar la trampa de cambio de IP:

Switch#configure

Switch(config)#snmp-server traps ip cambio

Switch(config)#end

Switch#copy running-config startup-config

Habilitar el SNMP PoE Traps Globalmente

Nota:

Solo el T2600G-28MPS es compatible con PoE traps.

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**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] Habilite las traps PoE. El comando sin ningún parámetro habilita todas las PoE Traps. Por defecto, todas las traps PoE están deshabilitadas. over-max-pwr-budget: Se activa cuando la potencia total requerida por los PD conectados excede la potencia máxima que puede suministrar el switch PoE. port-pwr-change: Se activa cuando la potencia total requerida por los PD conectados excede la potencia máxima que puede suministrar el switch PoE. port-pwr-deny: Se activa cuando el switch apaga los PD en los puertos PoE de baja prioridad. El switch los apaga para garantizar un funcionamiento estable de los otros PD cuando la potencia total requerida por los PD conectados excede el límite de potencia del sistema. port-pwr-over-30w: Se activa cuando la potencia requerida por el PD conectado supera los 30 vatios. port-pwr-overload: Se activa cuando la potencia requerida por el PD conectado excede la potencia máxima que el puerto puede suministrar. port-short-circuit: Se activa cuando se detecta un cortocircuito en un puerto. thermal-shutdown: Se activa cuando el chip PSE se sobrecalienta. El switch dejará de suministrar energía en este caso.
Paso 3	**end** Regrese al modo EXEC privilegiado.
Paso 4	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el switch para habilitar todas las PoE traps:

Switch#configure

Switch(config)#snmp-server traps power

Switch(config)#end

Switch#copy running-config startup-config

■ Habilitando Link-status Trap para los puertos

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Configurar traps de notificación en los puertos especificados. *port/port-list:* El número o la lista de los puertos Ethernet que desea configurar para capturar notificaciones. Para configurar múltiples puertos, ingrese una lista de números de puerto separados por comas, o use un guión para indicar un rango de números de puerto. Por ejemplo, 1-3, 5 indica el puerto 1, 2, 3, 5.
Paso 3	**snmp-server traps link-status** Habilite la trap de estado de enlace para el puerto. Por defecto, está habilitado. La trap de estado de enlace (Linkup Trap y Linkdown Trap) se puede activar cuando cambia el estado del enlace de un puerto, y la trap se habilita tanto globalmente como en el puerto. Para habilitar Linkup Trap y Linkdown Trap globalmente, ejecute el comando **snmp-server traps snmp [** linkup | linkdown **]** en modo de configuración global. Para deshabilitarlo, ejecute el comando no correspondiente.
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar el conmutador para habilitar la captura de estado de enlace:

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) junto con el sistema SNMP permite que el administrador de red monitoree los dispositivos de red remotos de manera eficiente. RMON reduce el flujo de tráfico entre el NMS y los dispositivos administrados, lo cual es conveniente para administrar redes grandes.

RMON incluye dos partes: el NMS y los agentes que se ejecutan en cada dispositivo de red. El NMS suele ser un host que ejecuta el software de administración para administrar agentes de dispositivos de red. El agente suele ser un swith o router que recopila estadísticas de tráfico (como el número total de paquetes en un segmento de red durante un cierto período de tiempo o el número total de paquetes correctos que se envían a un host). Basado en el protocolo SNMP, el NMS recopila datos de red comunicándose con los agentes. Sin embargo, el NMS no puede obtener todos los datos de RMON MIB porque los recursos del dispositivo son limitados. En general, el NMS solo puede obtener información de los siguientes cuatro grupos: Statistics, History, Event and Alarm.

- **Statistics:** Recopila estadísticas de Ethernet (como el total de bytes recibidos, el número total de paquetes de difusión y el número total de paquetes con un tamaño especificado) en una interfaz.
- **History:** Recopila un grupo histórico de estadísticas en puertos Ethernet para un intervalo de sondeo especificado.
- **Event:** Especifica la acción a tomar cuando un evento es activado por una alarma. La acción puede ser generar una entrada de registro o una captura SNMP.
- **Alarm:** Supervisa un objeto MIB específico durante un intervalo específico y activa un evento en un valor específico (umbral ascendente o umbral descendente).

5 RMON Configuraciones

Con las configuraciones de RMON, puede:

- Configuración del Statistics group.
- Configuración del History group.
- Configuración del Event group.
- Configuración del Alarm group.

Pautas de configuración

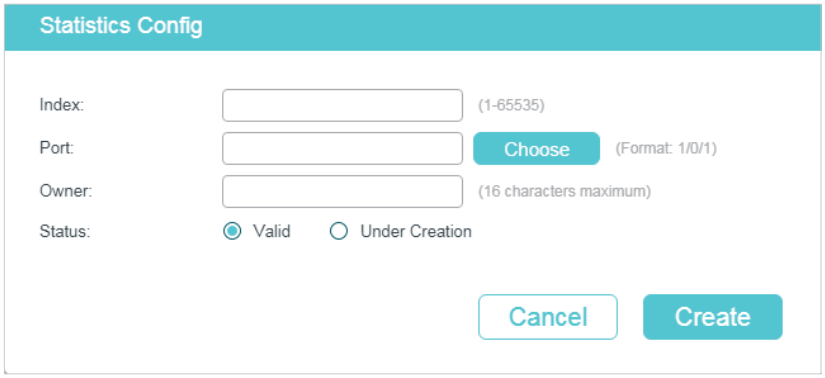
Para asegurarse de que el NMS recibe notificaciones normalmente, complete las configuraciones de SNMP y SNMP Notification antes de configurar RMON.

5.1 Usando la GUI

5.1.1 Configuración del Statistics group

Elige el menu**MAINTENANCE > SNMP > RMON > Statistics** y haga clic en Add para cargar la siguiente página.

Figura 5-1 Crear una entrada de estadísticas



Siga estos pasos para configurar el Statistics group:

1) Especifique el índice de entrada, el puerto que se supervisará y el nombre del propietario de la entrada. Establezca la entrada como Válida o En creación.

Index	Ingrese el índice de la entrada.
Port	Especifique un puerto Ethernet para monitorear en la entrada. Puede hacer clic en Elegir para elegir un puerto de la lista o ingresar manualmente el número de puerto, por ejemplo, 1/0/1 en el cuadro de entrada.
Owner	Ingrese el nombre del propietario de la entrada con 1 a 16 caracteres.

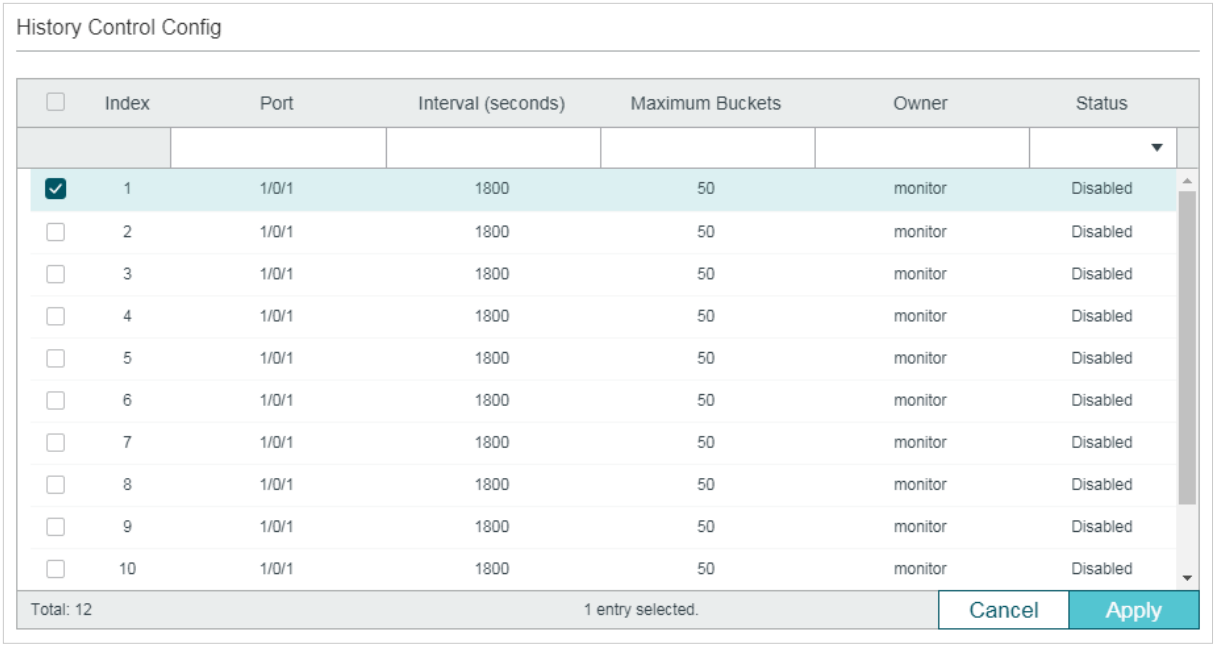
Status	Establezca la entrada como Valid o under Creation. Por defecto, es Valid. El switch comienza a recopilar estadísticas de Ethernet para una entrada de Estadísticas ya que el estado de la entrada está configurado como Valid. **Valid**: La entrada es creada y válida. **Under Creation**: La entrada se crea pero no es válida.

2) Clic en **Create**.

5.1.2 Configuración del History Group

Elige el menu **MAINTENANCE > SNMP > RMON > History** para cargar la siguiente página.

Figura 5-2 Configuración de la entrada del historial



Siga estos pasos para configurar el History group:

1) Seleccione una entrada del historial y especifique un puerto para supervisar.

Index	Muestra el índice de entradas del historial. El switch admite hasta 12 entradas del historial.
Port	Especifique un puerto para ser monitoreado.

2) Establezca el intervalo de muestra y los segmentos máximos de las entradas del historial.

Interval (seconds)	Especifique el número de segundos en cada ciclo de sondeo. Los valores válidos son de 10 a 3600 segundos. Cada entrada del historial tiene su propio temporizador. Para el puerto monitoreado, el switch muestra información del paquete y genera un registro en cada intervalo.
Maximum Buckets	Establezca el número máximo de registros para la entrada del historial. Los valores válidos son de 10 a 130. Cuando el número de registros excede el límite, se sobrescribirá el registro más antiguo.

3) Ingrese el nombre del propietario y establezca el estado de la entrada. Clic en **Apply**.

Owner	Ingrese el nombre del propietario de la entrada con 1 a 16 caracteres. Por defecto, es monitor.
Status	Habilita o deshabilita la entrada. Por defecto, está deshabilitado. Enable: la entrada está habilitada. Disable: la entrada está deshabilitada.

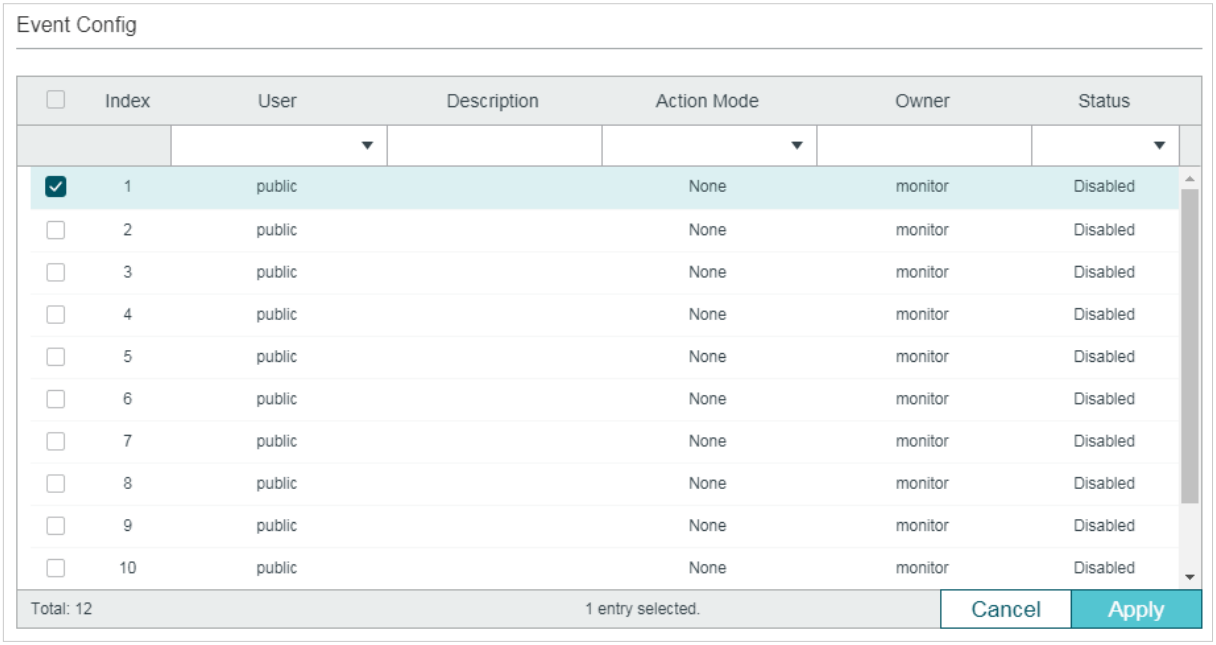
Nota:

Para cambiar los parámetros de una entrada de Historial, habilite la entrada al mismo tiempo; de lo contrario, el cambio no puede tener efecto.

5.1.3 Configuración del Event Group

Elige el menu **MAINTENANCE > SNMP > RMON > Event** para cargar la siguiente página.

Figura 5-3 Configuración de la entrada de evento



Siga estos pasos para configurar el Event group:

1) Elija una entrada de evento y especifique un usuario SNMP para la entrada.

Index	Muestra el índice de entradas de eventos. El conmutador admite hasta 12 entradas de eventos.
User	Elija un nombre de usuario SNMP o un nombre de comunidad para la entrada. Solo el usuario especificado puede acceder a los mensajes de registro o recibir los mensajes de notificación relacionados con el evento.

2) Establezca la descripción y la acción que se tomarán cuando se active el evento.

Description	Ingrese una breve descripción de este evento para facilitar su identificación.

Action Mode	Especifique la acción que debe realizar el cambio cuando se desencadena el evento. **None**: ninguna acción. **Log**: el switch registra el evento en el registro y el NMS debe iniciar solicitudes para recibir notificaciones. **Notify**: el switch envía notificaciones al NMS. **Log & Notify**: el switch registra el evento en el registro y envía notificaciones al NMS.

3) Ingrese el nombre del propietario y establezca el estado de la entrada. Clic en **Apply**.

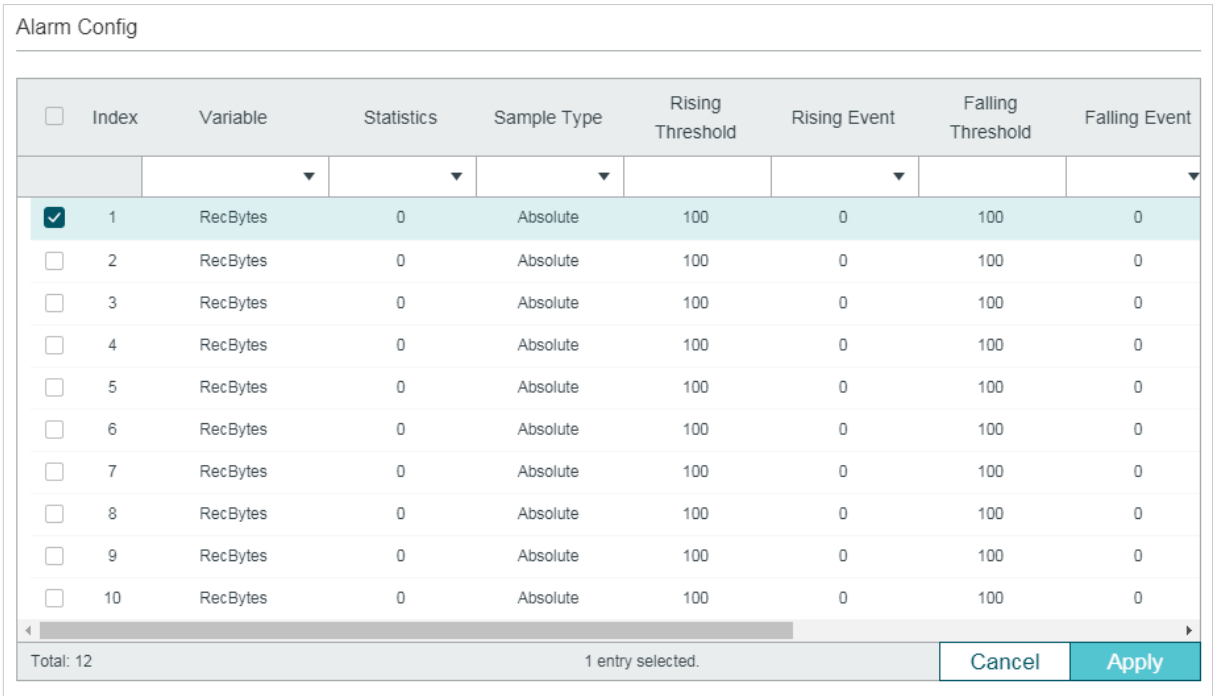
Owner	Ingrese el nombre del propietario de la entrada con 1 a 16 caracteres.
Status	Habilita o deshabilita la entrada. **Enable**: la entrada está habilitada. **Disable**: la entrada está deshabilitada.

5.1.4 Configuración de Alarm Group

Antes de comenzar, complete las configuraciones de las entradas de Statistics y entradas de Event , ya que las entradas de alarma deben estar asociadas con las entradas de estadísticas y eventos.

Elige el menu **MAINTENANCE > SNMP > RMON > Alarm** para cargar la siguiente página.

Figura 5-4 Configuración de la entrada de alarma



Siga estos pasos para configurar el Alarm group:

1) Seleccione una entrada de alarma, elija una variable para monitorear y asocie la entrada con una entrada de estadísticas.

Index	Muestra el índice de entradas de alarma. El switch admite hasta 12 entradas de alarma.
Variable	Establezca la variable de alarma a monitorear. El switch monitoreará la variable especificada en intervalos de muestra y actuará de la manera establecida cuando se active la alarma. **RecBytes**: Número total de bytes recibidos. **RecPackets**: Número total de paquetes recibidos. **BPackets**: Número total de paquetes de difusión. **MPackets**: Número total de paquetes de multidifusión. **CRC&Align ERR**: Paquetes que contienen error FCS o error de alineación, dentro de un tamaño de 64 a 1518 bytes. **Undersize**: Paquetes que son más pequeños que 64 bytes. **Oversize**: Paquetes que son mayores de 1518 bytes. **Jabbers**: Paquetes que se envían cuando se producen colisiones de puertos. **Collisions**: Tiempos de colisión en el segmento de red. **64, 65-127, 128-255, 256-511, 512-1023, 1024-1518**: número total de paquetes del tamaño especificado.
Statistics	Asociar la entrada de alarma con una entrada de estadísticas. Luego, el switch monitorea la variable especificada de la entrada Estadísticas.

2) Establezca el tipo de muestra, el umbral ascendente y descendente, las entradas de eventos correspondientes y el tipo de alarma de la entrada.

Sample Type	Especifique el método de muestreo de la variable especificada. **Absolute**: Compare el valor de muestreo con el umbral preestablecido. **Delta**: El switch obtiene la diferencia entre los valores de muestreo del intervalo actual y el intervalo anterior, y luego compara la diferencia con el umbral preestablecido.
Rising Threshold	Especifique el umbral ascendente de la variable. Los valores válidos son de 1 a 2147483647. Cuando el valor de muestreo o el valor de diferencia excede el umbral, el sistema activará el Evento ascendente correspondiente. *Nota:* El umbral ascendente debe ser mayor que el umbral descendente.
Rising Event	Especifique el índice de la entrada de evento que se activará cuando el valor de muestreo o el valor de diferencia exceda el umbral preestablecido. La entrada de evento especificada aquí debe habilitarse primero.

Falling Threshold	Establecer el umbral descendente de la variable. Los valores válidos son de 1 a 2147483647. Cuando el valor de muestreo o el valor de diferencia está por debajo del umbral, el sistema activará el Evento de caída correspondiente. *Nota:* El umbral descendente debe ser menor que el umbral ascendente.
Falling Event	Especifique el índice de la entrada del evento que se activará cuando el valor de muestreo o el valor de diferencia esté por debajo del umbral preestablecido. La entrada de evento especificada aquí debe habilitarse primero.
Alarm Type	Especifique el tipo de alarma para la entrada. **Rising**: La alarma se activa solo cuando el valor de muestreo o el valor de diferencia excede el umbral ascendente. **Falling**: La alarma se activa solo cuando el valor de muestreo o el valor de diferencia está por debajo del umbral descendente. **All**: La alarma se activa cuando el valor de muestreo o el valor de diferencia excede el umbral ascendente o está por debajo del umbral descendente.

3) Ingrese el nombre del propietario y establezca el estado de la entrada. Clic en **Apply**.

Interval (seconds)	Establecer el intervalo de muestreo. Los valores válidos son de 10 a 3600 segundos.
Owner	Ingrese el nombre del propietario de la entrada con 1 a 16 caracteres.
Status	Habilita o deshabilita la entrada. **Enable**: La entrada está habilitada. **Disable**: La entrada está deshabilitada.

5.2 Uso de la CLI

5.2.1 Configuración de Statistics

Paso 1	**configure** Ingrese al modo de configuración global.

Paso 2	**rmon statistics** *index* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } [**owner** *owner-name*] [**status** { underCreation | valid }] Configure las entradas estadisticas de RMON. *index:* Especifique el índice de la entrada Estadísticas, que varía de 1 a 65535. Para configurar varios índices, ingrese una lista de índices separados por comas, o use un guión para indicar un rango de índices. Por ejemplo, 1-3, 5 indica 1, 2, 3, 5. *port:* Especifique el puerto que se vinculará a la entrada. *owner-name:* Ingrese el nombre del propietario de la entrada con 1 a 16 caracteres. El nombre predeterminado es monitor. underCreation | valid: Ingrese el estado de la entrada. UnderCreation indica que la entrada se creó pero no es válida, mientras que Valid indica que la entrada se creó y es válida. Por defecto, es válido. El switch comienza a recopilar estadísticas de Ethernet para una entrada de Estadísticas ya que el estado de la entrada está configurado como válido.
Paso 3	**show rmon statistics** [*index*] Muestra las entradas de estadísticas y sus configuraciones. *index:* Ingrese el índice de entrada de estadísticas que desea ver. Los valores válidos son de 1 a 65535. El comando sin ningún parámetro muestra todas las entradas de estadísticas existentes.
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo crear entradas de estadísticas 1 y 2 en el switch para monitorear los puertos 1/0/1 y 1/0/2, respectivamente. El propietario de las entradas es monitor y el estado es válido:

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 Configuración de History

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**rmon history** *index* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*} [**interval** *seconds*] [**owner** *owner-name*] [**buckets** *number*] Configuración de entradas del historial de RMON. *index:* Especifique el índice de la entrada Historial, que varía de 1 a 12. Para configurar varios índices, ingrese una lista de índices separados por comas, o use un guión para indicar un rango de índices. Por ejemplo, 1-3, 5 indica 1, 2, 3, 5. *port:* Especifique el puerto que se vinculará a la entrada. *seconds:* Establecer el intervalo de muestra. Los valores son de 10 a 3600 segundos, y el valor predeterminado es 1800 segundos. *owner-name:* Ingrese el nombre del propietario de la entrada con 1 a 16 caracteres. El nombre predeterminado es monitor. *number:* Establezca el número máximo de registros para la entrada del historial. Cuando el número de registros excede el límite, se sobrescribirá el registro más antiguo. Los valores son de 10 a 130; el valor predeterminado es 50.
Paso 3	**show rmon history** [*index*] Muestra la entrada del historial especificada y las configuraciones relacionadas. Para mostrar múltiples entradas, ingrese una lista de índices separados por comas, o use un guión para indicar un rango de índices. Por ejemplo, 1-3, 5 indica 1, 2, 3, 5. *index:* Ingrese el índice de la entrada del historial que desea ver. Los valores válidos son de 1 a 12 El comando sin ningún parámetro muestra todas las entradas de estadísticas existentes..
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo crear una entrada de Historial en el switch para monitorear el puerto 1/0/1. Establezca el intervalo de muestra en 100 segundos, los intervalos máximos en 50 y el propietario como 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 Configuración de Event

Paso 1	**configure** Ingrese al modo de configuración global.
Paso 2	**rmon event** *index* [**user** *user-name*] [**description** *description*] [**type** { none | log | notify | log-notify }] [**owner** *owner-name*] Configuración de entradas de eventos RMON. *index*:Especifique el índice de la entrada Evento, que varía de 1 a 12. Para configurar varios índices, ingrese una lista de índices separados por comas, o use un guión para indicar un rango de índices. Por ejemplo, 1-3, 5 indica 1, 2, 3, 5. *user-name:* Ingrese el nombre de usuario SNMP o el nombre de comunidad de la entrada. El nombre debe ser el que configuró en SNMP anteriormente. El nombre predeterminado es public. *description:* Dé una descripción a la entrada con 1 a 16 caracteres. Por defecto, la descripción está vacía. none | log | notify | log-notify*:* Especifique el tipo de acción del evento; entonces el switch tomará la acción especificada para lidiar con el evento. Por defecto, el tipo es none. Ninguno indica que el switch no realiza ninguna acción, el registro indica que el switch registra solo el evento, la notificación indica que el switch envía notificaciones solo al NMS y la notificación de registro indica que el switch registra el evento y envía notificaciones al NMS. *owner-name:* Ingrese el nombre del propietario de la entrada con 1 a 16 caracteres. El nombre predeterminado es monitor
Paso 3	**show rmon event** [*index*] Muestra la entrada de evento especificada y las configuraciones relacionadas. Para mostrar múltiples entradas, ingrese una lista de índices separados por comas, o use un guión para indicar un rango de índices. Por ejemplo, 1-3, 5 indica 1, 2, 3, 5. *index:* Ingrese el índice de la entrada del evento que desea ver. Los valores válidos son de 1 a 12. El comando sin ningún parámetro muestra todas las entradas de estadísticas existentes.
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo crear una entrada de evento en el switch. Establezca el nombre de usuario como administrador, el tipo de evento como Notificar (configure el switch para iniciar notificaciones en el NMS) y el propietario como 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 Configuración de Alarm

Paso 1 **configure**

Ingrese al modo de configuración global.

Paso 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*]

Configuración de entradas de alarma RMON.

index: Especifique el índice de la entrada de alarma, que varía de 1 a 12. Para configurar varios índices, ingrese una lista de índices separados por comas, o use un guión para indicar un rango de índices. Por ejemplo, 1-3, 5 indica 1, 2, 3, 5.

sindex: Especifique el índice de la entrada de estadísticas relacionada, que varía de 1 a 65535.

revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65- 127 | 128-255 | 256-511 | 512-1023 | 1024-1518: Elija una variable de alarma para monitorear. El switch monitoreará la variable especificada en intervalos de muestra y actuará de la manera establecida cuando se active la alarma. La variable predeterminada es revbyte.

revbyte significa el número total de bytes recibidos; revpkt significa el número total de paquetes recibidos; bpkt significa el número total de paquetes de difusión. mpkt significa el número total de paquetes de multidifusión; crc-align significa paquetes que contienen error FCS o error de alineación, dentro de un tamaño de 64 a 1518 bytes; undersize significa paquetes que son más pequeños que 64 bytes; oversize significa paquetes que son mayores de 1518 bytes; jabber significa paquetes que se envían cuando se producen colisiones de puertos; collision significa los tiempos de colisión en el segmento de red; 64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-1518 significa el número total de paquetes del tamaño especificado.

absolute | delta: Elija el método de muestreo de la variable especificada. El valor predeterminado es absoluto. En el modo absoluto, el switch compara el valor de muestreo con el umbral preestablecido; en el modo delta, el switch obtiene la diferencia entre los valores de muestreo del intervalo actual y el intervalo anterior, y luego compara la diferencia con el umbral preestablecido.

r-threshold: Ingrese el umbral ascendente. Los valores válidos son de 1 a 2147483647, y el valor predeterminado es 100. El umbral ascendente debe ser mayor que el umbral descendente.

r-event: Ingrese el índice de la entrada del evento que se activará cuando el valor de muestreo o el valor de diferencia exceda el umbral preestablecido. Los valores válidos son de 1 a 12. La entrada de evento especificada aquí debe habilitarse primero.

f-threshold: Ingrese un umbral descendente. Los valores válidos son de 1 a 2147483647, y el valor predeterminado es 100. El umbral descendente debe ser menor que el umbral ascendente.t

f-event: Ingrese el índice de la entrada del evento que se activará cuando el valor de muestreo o el valor de diferencia esté por debajo del umbral preestablecido. Los valores válidos son de 1 a 12. La entrada de evento especificada aquí debe habilitarse primero.

rise | fall | all: Elija un tipo de alarma; El valor predeterminado es todo. Rise indica que la alarma se activa solo cuando el valor de muestreo o el valor de diferencia excede el umbral ascendente. La caída indica que la alarma se activa solo cuando el valor de muestreo o el valor de diferencia está por debajo del umbral de caída. Todo indica que la alarma se activa cuando el valor de muestreo o el valor de diferencia excede el umbral ascendente o está por debajo del umbral descendente.

owner-name: Ingrese el nombre del propietario de la entrada con 1 a 16 caracteres. El nombre predeterminado es monitor.

interval: Establecer el intervalo de muestreo. El valor varía de 10 a 3600 segundos; El valor predeterminado es 1800 segundos.

Paso 3	**show rmon alarm** [*index*] Muestra la entrada de alarma especificada y las configuraciones relacionadas. Para mostrar múltiples entradas, ingrese una lista de índices separados por comas, o use un guión para indicar un rango de índices. Por ejemplo, 1-3, 5 indica 1, 2, 3, 5. *index:* Ingrese el índice de entrada de alarma que desea ver. Los valores válidos son de 1 a 12 El comando sin ningún parámetro muestra todas las entradas de estadísticas existentes.
Paso 4	**end** Regrese al modo EXEC privilegiado.
Paso 5	**copy running-config startup-config** Guarde la configuración en el archivo de configuración.

El siguiente ejemplo muestra cómo configurar una entrada de alarma para monitorear BPackets en el switch. Establezca el índice de entrada de Estadística relacionado en 1, el tipo de muestra como Absoluto, el umbral ascendente como 3000, el índice de entrada de evento ascendente relacionado como 1, el umbral descendente como 2000, el índice de evento descendente relacionado como 2, el tipo de alarma como todo, el intervalo de notificación como 10 segundos, y el propietario de la entrada como 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 Ejemplo de configuración

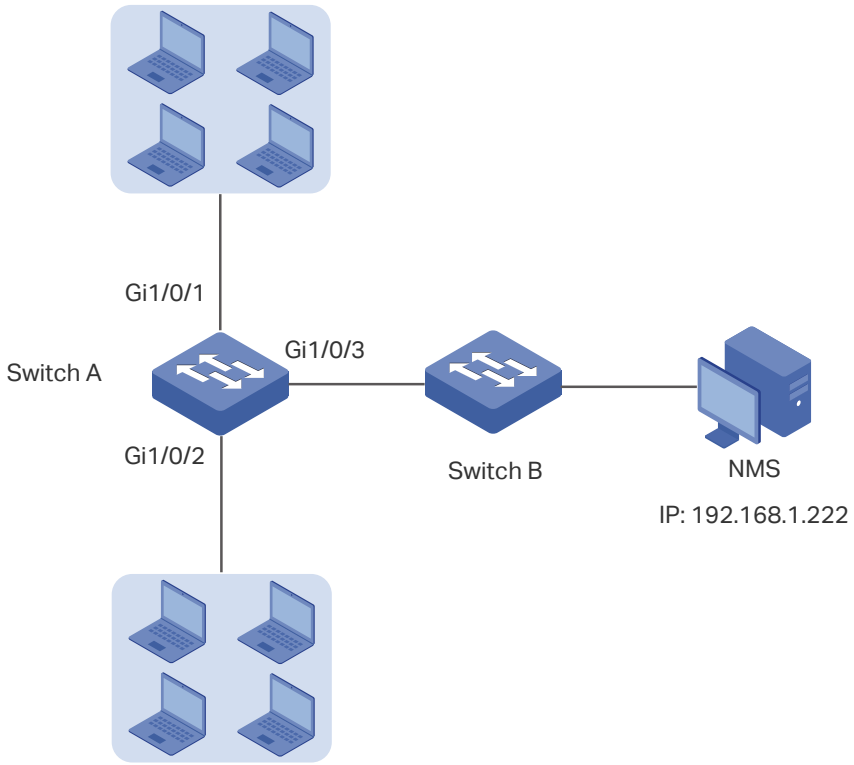
6.1 Requisitos de red

La siguiente figura muestra la topología de red de una empresa. La empresa tiene los siguientes requisitos:

1) Monitoree el tráfico de tormentas de los puertos 1/0/1 y 1/0/2 en el Switch A, y envíe notificaciones al NMS cuando la tasa real de paquetes de difusión, multidifusión o unidifusión desconocida exceda el umbral preestablecido.
2) Supervise el tráfico de los puertos 1/0/1 y 1/0/2 en el conmutador A, y recopile y guarde regularmente datos para las comprobaciones de seguimiento. Específicamente, el Switch A debe notificar al NMS cuando el número de paquetes transmitidos y recibidos en los puertos durante el intervalo de muestra excede el umbral ascendente preestablecido, y debe registrar pero no notificar al NMS cuando está por debajo del umbral descendente preestablecido.

El host NMS con la dirección IP 192.168.1.222 está conectado al switch central, el switch B. El switch A está conectado al switch B a través del puerto 1/0/3. El puerto 1/0/3 y el NMS pueden comunicarse entre sí.

Figura 6-1 Topología de red



6.2 Esquema de configuración

1) En el Switch A, establezca umbrales para paquetes de difusión, multidifusión y unidifusión desconocida en los puertos 1/0/1 y 1/0/2. Habilite SNMP y configure los parámetros correspondientes. Habilite las notificaciones de trampa en los puertos. El switch A puede enviar notificaciones al NMS cuando la tasa de tráfico de tormentas excede el umbral preestablecido.

2) Después de las configuraciones de SNMP y notificación, cree entradas de estadísticas en los puertos para monitorear la transmisión y recepción de paquetes en tiempo real y cree entradas de historial para recopilar y guardar regularmente datos relacionados. Cree dos entradas de evento: una es el tipo de notificación utilizada para notificar al NMS y la otra es el tipo de registro utilizado para registrar eventos relacionados.

3) Cree una entrada de alarma para supervisar RecPackets (paquetes recibidos). Configure los umbrales ascendentes y descendentes. Configure el evento ascendente como la entrada del evento Notificar y el evento descendente como la entrada del evento Log.

Demostrado con T2600G-28TS, este capítulo proporciona procedimientos de configuración de dos maneras: usando la GUI y usando la CLI.

6.3 Usando la GUI

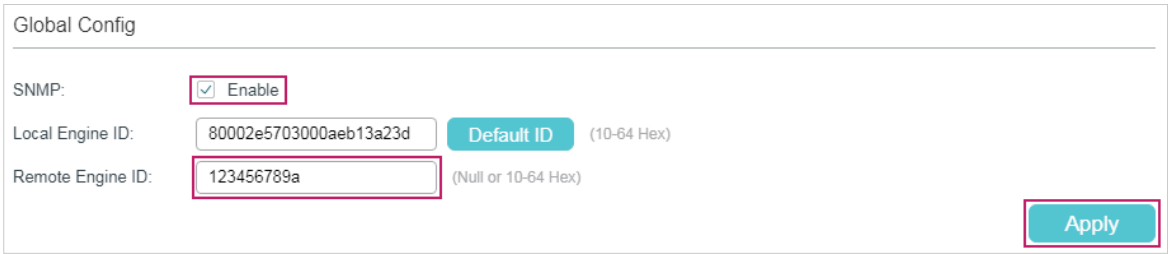
■ Configuración de control de tormentas en puertos

Configure Storm Control en los puertos requeridos. Para una configuración detallada, consulte *Configurar QoS* .

■ Configurar SNMP

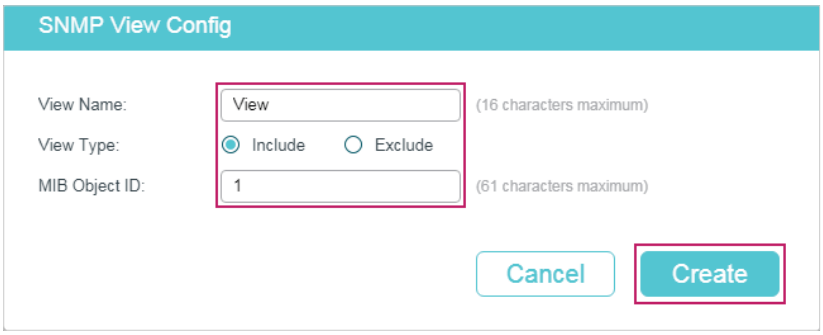
1) Selecciona **MAINTENANCE > SNMP > Global Config** para cargar la siguiente página. En la seccion **Global Config**, habilitar SNMP, y configure la ID del motor remoto como 123456789a. Hacer clic **Apply**.

Figura 6-2 Habilitación de SNMP



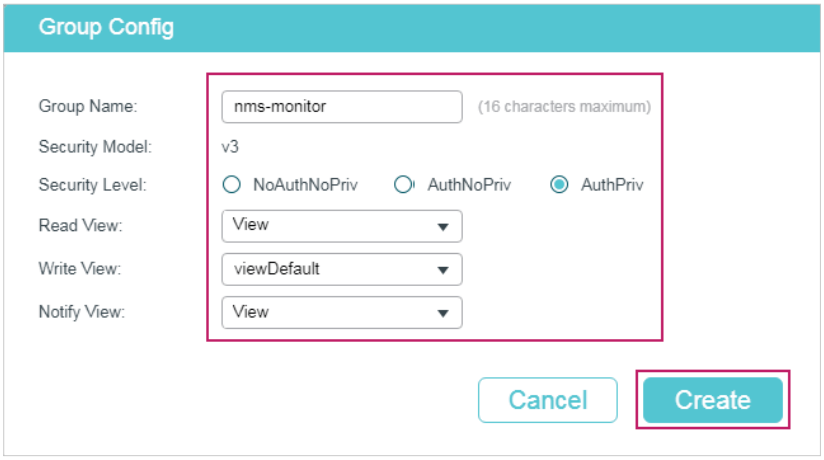
2) En la sección **SNMP View Config**, haga clic en Add para cargar la siguiente página. Asigne un nombre a la vista SNMP como Vista, establezca el tipo de vista como Incluir y establezca el ID de objeto MIB en 1 (lo que significa todas las funciones). Haz clic en Crear.

Figura 6-3 Crear una vista SNMP



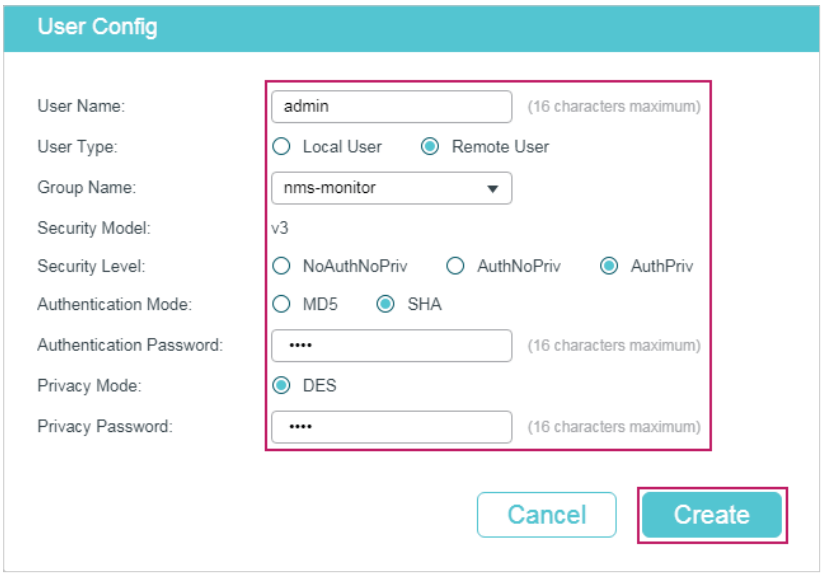
3) Selecciona **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** y haga clic Add para cargar la siguiente pügina. Cree un grupo llamado nms-monitor, habilite la autenticaciĎn y la privacidad, y agregue Vista a Vista de lectura y Vista de notificaciĎn. Hacer clic **Create**.

Figura 6-4 ConfiguraciĎn de un grupo SNMP



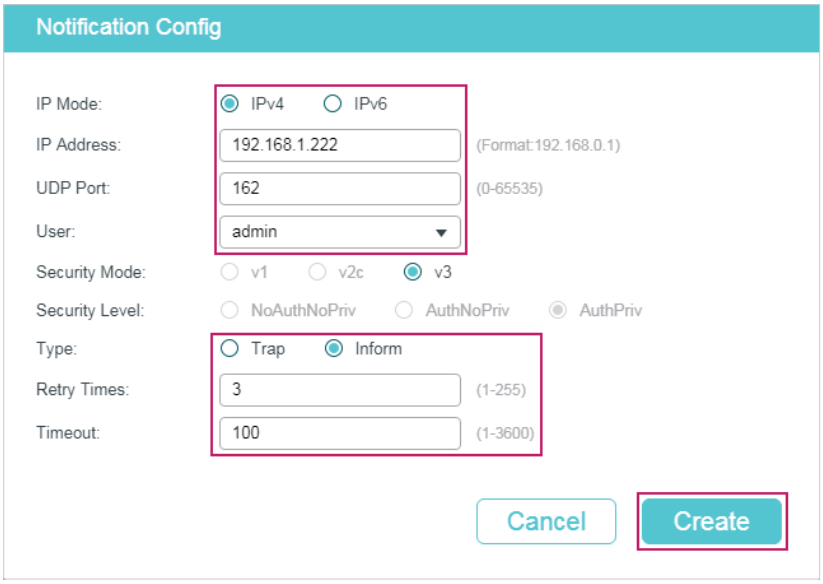
4) Selecciona **MAINTENANCE > SNMP > SNMP v3 > SNMP User** y haga clic en Add para cargar la siguiente pügina. Cree un usuario llamado admin para el NMS, establezca el tipo de usuario como Usuario remoto y especifique el nombre del grupo. Establezca el nivel de seguridad de acuerdo con el del grupo nms-monitor. Elija el algoritmo de autenticaciĎn SHA y el algoritmo de privacidad DES, y configure las contraseČas correspondientes. Hacer clic en **Create**.

Figure 6-5 Creating an SNMP User



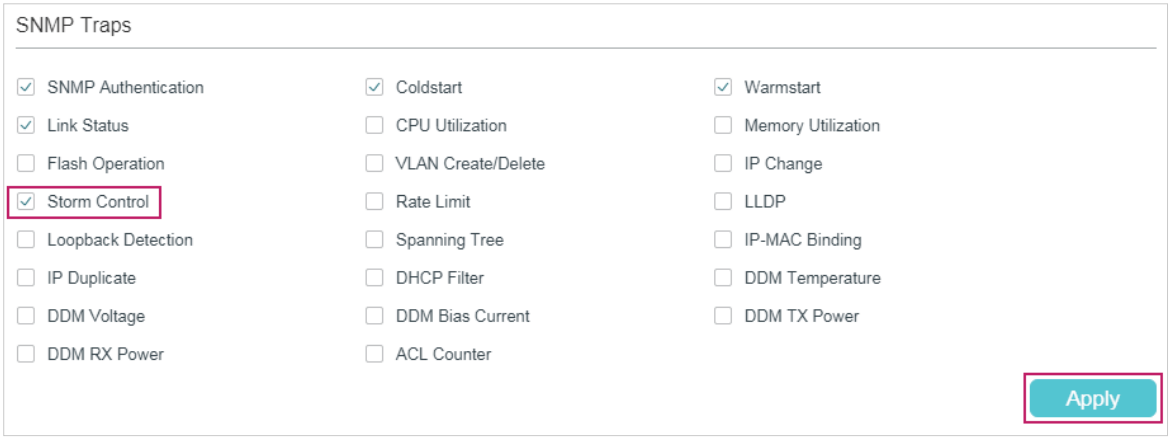
5) Seleciona **MAINTENANCE > SNMP > Notification > Notification Config** y haga clic en Add para cargar la siguiente página. Elija el Modo IP como IPv4 y especifique la dirección IP del host NMS y el puerto del host para transmitir las notificaciones. Especifique el Usuario como administrador y elija el tipo como Informar. Establezca los tiempos de reintento como 3, con el período de tiempo de espera como 100 segundos. Hacer clic en **Create**.

Figura 6-6 Creación de una entrada de notificación SNMP



6) Selecciona **MAINTENANCE > SNMP > Notification > Trap Config** para cargar la siguiente página. Habilite la trap de Control de tormentas y haga clic en **Apply**.

Figura 6-7 **Habilitar** Storm Control Trap



7) Clic Save para guardar la configuración.

■ Configuración de RMON

1) Selecciona **MAINTENANCE > SNMP > RMON > Statistics** y Haga Add clic para cargar la siguiente página. Cree entradas de estadísticas 1 y 2, y enlácelas a los puertos 1/0/1 y 1/0/2, respectivamente. Establezca el propietario de las entradas como monitor y el estado como Valid.

Figura 6-8 Configuración de entrada de estadísticas 1

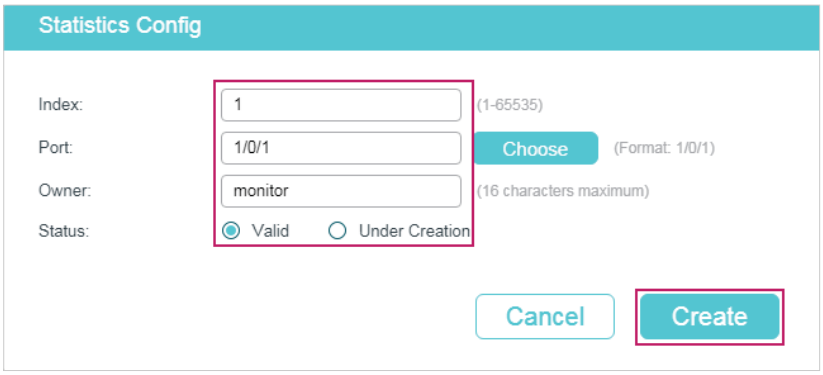
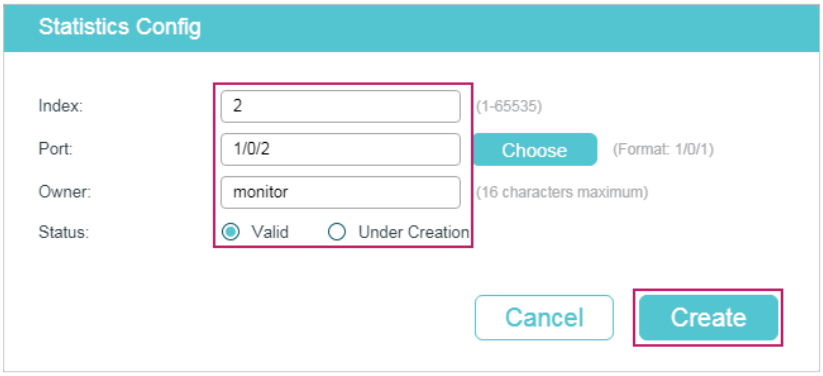


Figura 6-9 Configuración de la entrada de estadísticas 2



2) Seleccione el menú **MAINTENANCE > SNMP > RMON > History** para cargar la siguiente página. Configure las entradas 1 y 2. Enlace las entradas 1 y 2 a los puertos 1/0/1 y 1/0/2, respectivamente. Establezca el intervalo como 100 segundos, los depósitos máximos como 50, el propietario de las entradas como monitor y el estado como habilitado.

Figura 6-10 Configuración de las entradas del historial

History Control Config

Index	Port	Interval (seconds)	Maximum Buckets	Owner	Status
1	1/0/1	100	50	monitor	Enabled
2	1/0/2	100	50	monitor	Enabled
3	1/0/1	1800	50	monitor	Disabled
4	1/0/1	1800	50	monitor	Disabled
5	1/0/1	1800	50	monitor	Disabled
6	1/0/1	1800	50	monitor	Disabled
7	1/0/1	1800	50	monitor	Disabled
8	1/0/1	1800	50	monitor	Disabled
9	1/0/1	1800	50	monitor	Disabled
10	1/0/1	1800	50	monitor	Disabled

Total: 12

3) Seleccionar el meún **MAINTENANCE > SNMP > RMON > Event** para cargar la siguiente página. Configure las entradas 1 y 2. Para la entrada 1, establezca el nombre de usuario SNMP como administrador, escriba como Notificar, la descripción como "rising_notify", el propietario como monitor y el estado como habilitado. Para la entrada 2, configure el nombre de usuario SNMP como admin, escriba como Log, la descripción como "falling_log", el propietario como monitor y el estado como habilitado.

Figura 6-11 Configuración de las entradas de evento

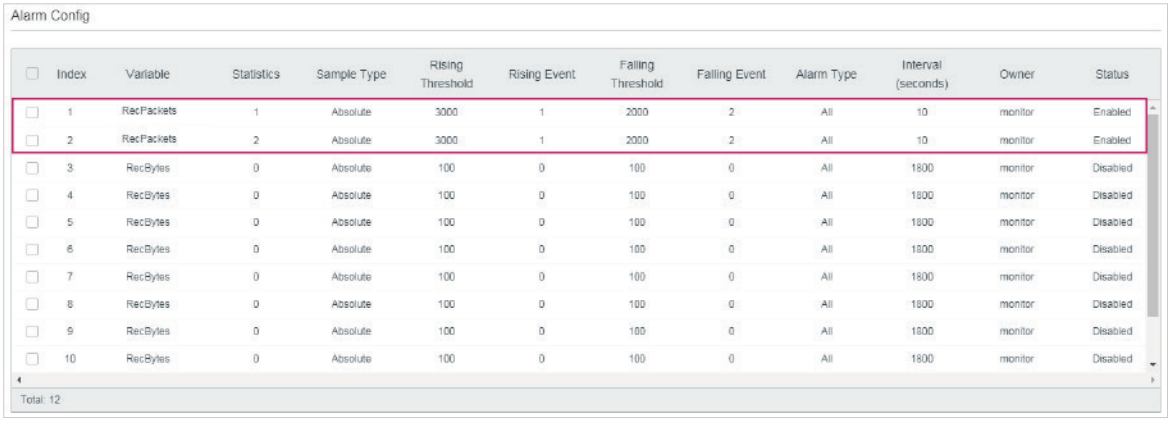
Event Config

Index	User	Description	Action Mode	Owner	Status
1	admin	rising_notify	Notify	monitor	Enabled
2	admin	falling_log	Log	monitor	Enabled
3	public		None	monitor	Disabled
4	public		None	monitor	Disabled
5	public		None	monitor	Disabled
6	public		None	monitor	Disabled
7	public		None	monitor	Disabled
8	public		None	monitor	Disabled
9	public		None	monitor	Disabled
10	public		None	monitor	Disabled

Total: 12

4) Seleccione **MAINTENANCE > SNMP > RMON > Alarm** para cargar la siguiente página. Configure las entradas 1 y 2. Para la entrada 1, configure la variable de alarma como RecPackets, el ID de entrada de estadísticas relacionadas como 1 (vinculado al puerto 1/0/1), el tipo de muestra como Absoluto, el umbral ascendente como 3000, la entrada de evento ascendente asociada ID como 1 (que es el tipo de notificación), el umbral descendente como 2000, el ID de entrada de evento descendente asociado como 2 (que es el tipo de registro), el tipo de alarma como Todo, el intervalo como 10 segundos, el nombre del propietario como monitor . Para la entrada 2, establezca el ID de entrada de estadísticas asociado como 2 (vinculado al puerto 1/0/2). Otras configuraciones son las mismas que las de la entrada 1.

Figura 6-12 Configuración de las entradas de alarma



5) Clic Save para guardar la configuración.

6.4 Uso de la CLI

■ Configurando Storm Control en los puertos

Configure Storm Control en los puertos requeridos del Switch A. Para obtener una configuración detallada, consulte *Configurar QoS* .

■ Configurar SNMP

1) Habilite SNMP y especifique el remote engine ID.

Switch_A#configure

Switch_A(config)#snmp-server

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

2) Cree una vista con el nombre Ver; establezca el MIB Object ID como 1 (que representa todas las funciones) y el tipo de vista como Include.

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

3) Cree un grupo de SNMPv3 con el nombre de nms-monitor. Habilite el Modo de autenticación y el Modo de privacidad, y configure Read y Notify views como Vista.

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

4) Cree un usuario SNMP llamado admin. Configure al usuario como usuario remoto y configure el modelo de seguridad y el nivel de seguridad según el grupo. Establezca el Modo de autenticación como algoritmo SHA, la contraseña como 1234, el Modo de privacidad como DES y la contraseña como 1234.

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

5) Para configurar la Notificación, especifique la dirección IP del host NMS y el puerto UDP. Establezca el Usuario, el Modelo de seguridad y el Nivel de seguridad de acuerdo con las configuraciones del Usuario SNMP.

Elija el tipo como Informar y establezca los tiempos de reintento en 3 y el tiempo de espera en 100 segundos.

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

■ Habilite storm-control Trap

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

■ Configuración de RMON

1) Cree entradas de estadísticas 1 y 2 para monitorear los puertos 1/0/1 y 1/0/2, respectivamente. El propietario de las entradas se establece como monitor y el estado se establece como 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) Cree entradas de historial 1 y 2 y asócielas a los puertos 1/0/1 y 1/0/2, respectivamente. Establezca el intervalo de muestra en 100 segundos, los intervalos máximos en 50 y el propietario como 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) Cree entradas de evento 1 y 2 para el administrador de usuarios SNMP. Establezca la entrada 1 como el tipo de notificación y su descripción como "rising_notify". Establezca la entrada 2 como el tipo de registro y su descripción como "falling_log". Establecer el propietario de ellos como 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) Cree las entradas de alarma 1 y 2. Para la entrada 1, configure la variable de alarma como RecPackets, el ID de entrada de estadísticas asociado como 1 (vinculado al puerto 1/0/1), el tipo de muestra como Absolute, el umbral ascendente como 3000, el aumento asociado ID de entrada de evento como 1 (Notify type), el umbral descendente como 2000, la ID de entrada de evento descendente asociada como 2 (the log type), el tipo de alarma como todo, el intervalo como 10 segundos y el nombre del propietario como monitor. Para la entrada 2, configure el ID de entrada de estadísticas asociado como 2 (vinculado al puerto 1/0/2), mientras que todas las demás configuraciones son las mismas que las de la entrada 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

Verificar las configuraciones

Verifique las configuraciones globales de SNMP:

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

Verifique el SNMP engine ID:

Switch_A(config)#show snmp-server engineID

Local engine ID: 80002e5703000aeb13a23d

Remote engine ID: 123456789a

Verifique las configuraciones SNMP view:

```
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
```

Verifique las configuraciones SNMP group:

```
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
```

Verifique las configuraciones de usuario SNMP:

```
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
```

Verifique las configuraciones de host SNMP:

```
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
```

Verifique las configuraciones de las estadísticas de RMON:

```
Switch_A(config)#show rmon statistics
```

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

Verifique las configuraciones del historial de RMON:

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

Verifique las configuraciones de eventos de RMON:

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

Verifique las configuraciones de alarma RMON:

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 Apéndice: Parámetros predeterminados

La configuración predeterminada de SNMP se enumera en las siguientes tablas.

Tabla 7-1 Configuración de configuración global predeterminada

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

Tabla 7-2 Configuración de tabla de vista SNMP predeterminada

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

Tabla 7-3 Configuración predeterminada de SNMP v1 / v2c

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

Tabla 7-4 Configuración predeterminada de SNMP v3

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

La configuración predeterminada de Notificación se enumera en la siguiente tabla.

Tabla 7-5 Configuración de notificación predeterminada

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

La configuración predeterminada de RMON se enumera en las siguientes tablas.

Tabla 7-6 Configuración de configuración de estadísticas predeterminada

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

Tabla 7-7 Configuración predeterminada para entradas de historial

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

Tabla 7-8 Configuración predeterminada para entradas de eventos

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

Tabla 7-9 Configuración predeterminada para entradas de alarma

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