

# Mamá Commutador PoE Gigabit integrado

Manual de configuración web

**V1.0.1**

# Prefacio

## General

Este Manual de configuración web (en lo sucesivo, "el manual") presenta las operaciones en la interfaz web del conmutador PoE Gigabit administrado (en lo sucesivo, "el conmutador"). Puede visitar el interruptor en el navegador web, configurar y administrar el interruptor.

## Instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con un significado definido pueden aparecer en el manual.

Palabras de advertencia	Significado
 <b>PELIGRO</b>	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 <b>ADVERTENCIA</b>	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 <b>PRECAUCIÓN</b>	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 <b>CONSEJOS</b>	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 <b>NOTA</b>	Proporciona información adicional como énfasis y complemento del texto.

## Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	julio 2019
V1.0.1	- Se agregaron funciones de vigilancia PoE y sistema de administración de red. Cifras actualizadas.	noviembre 2020

## Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como la cara, las huellas dactilares, el número de placa del automóvil, la dirección de correo electrónico, el número de teléfono, el GPS, etc. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: proporcionar una identificación clara y visible para informar al sujeto de los datos sobre la existencia de un área de vigilancia y proporcionar información relacionada. contacto.

## Sobre el Manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplen con el manual.
- El manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final. Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

# Medidas de seguridad y advertencias importantes

El manual le ayuda a utilizar nuestro producto correctamente. Para evitar peligros y daños a la propiedad, lea atentamente el manual antes de utilizar el producto y le recomendamos encarecidamente que lo conserve para futuras consultas.

## Requisitos operativos

- No exponga el dispositivo directamente a la luz solar y manténgalo alejado de fuentes de calor. No instale el dispositivo en un ambiente húmedo y evite el polvo y el hollín.
- Asegúrese de que el dispositivo esté en una instalación horizontal e instálelo en una superficie sólida y plana para evitar que se caiga.
- Evite las salpicaduras de líquido en el dispositivo. No coloque objetos llenos de líquido sobre el dispositivo para evitar que el líquido fluya hacia el dispositivo.
- Instale el dispositivo en un ambiente bien ventilado. No bloquee la salida de aire del dispositivo.
- Utilice el dispositivo a la tensión nominal de entrada y salida.
- No desmonte el dispositivo sin instrucción profesional.
- Transporte, use y almacene el dispositivo en los rangos permitidos de humedad y temperatura.

## Requisitos de fuente de alimentación

- Utilice la batería correctamente para evitar incendios, explosiones y otros peligros.
- Reemplace la batería con una batería del mismo tipo.
- Utilice el cable de alimentación recomendado localmente en el límite de las especificaciones nominales.
- Utilice el adaptador de corriente estándar. No asumiremos ninguna responsabilidad por ningún problema causado por un adaptador de corriente no estándar.
- La fuente de alimentación deberá cumplir con el requisito SELV. Utilice la fuente de alimentación que cumpla con la fuente de alimentación limitada, según IEC60950-1. Consulte la etiqueta del dispositivo.
- Adopte la protección GND para dispositivos tipo I.
- El acoplador es el aparato de desconexión. Manténgalo en ángulo para que sea fácil de operar.

# Tabla de contenido

<b>Prólogo</b> .....	<b>I Medidas de seguridad y advertencias importantes</b> .....
<b>sesión</b> .....	<b>III 1 Iniciar sesión</b> .....
<b>1</b>	<b>1</b>
<b>2 Ajustes rápidos</b> .....	<b>2</b>
2.1 Información del sistema .....	2
2.2 Locales.....	3
2.3 VLAN.....	3
2.4 Agregación .....	4
2.4.1 Configuración de agregación estática.....	5
2.4.2 Configuración de agregación dinámica.....	6
2.5 IP y Ruta .....	6
<b>3 Ajustes avanzados</b> .....	<b>9</b>
3.1 Configuración común .....	9
3.1.1 Configuración del sistema .....	9
3.1.2 Configuración de puertos .....	15
3.1.3 Configuración de VLAN .....	17
3.1.4 Agregación .....	18
3.1.5 Tabla MAC .....	20
3.1.6 Árbol de expansión .....	25
3.1.7 PoE de larga distancia .....	28
3.2 Configuraciones poco usadas .....	28
3.2.1 ERPS .....	28
3.2.2 LCA .....	36
3.2.3 Protección de bucle .....	39
3.2.4 Seguridad .....	39
3.2.5 Indagación IGMP .....	44
3.2.6 Calidad del servicio.....	46
3.2.7 SNMP.....	56
3.2.8 Servidor DHCP .....	59
3.2.9 LLDP .....	61
3.2.10 Configuración 485 .....	63
3.2.11 PoE .....	64
<b>4 Mantenimiento</b> .....	<b>69</b>
4.1 Reinicio del sistema .....	69
4.2 Restauración de la configuración predeterminada .....	69
4.3 Gestión de configuración .....	69
4.3.1 Exportación del archivo de configuración .....	69
4.3.2 Subir archivo de configuración .....	70
4.4 Actualización de software .....	70
4.5 Duplicación .....	71
4.6 Hacer ping .....	72
4.7 Función del Sistema de Gestión de Red.....	72
4.7.1 Habilitación de funciones e inicio de sesión .....	72
4.7.2 Exportación del archivo de configuración de gestión de red .....	73

4.7.3 Carga del archivo de configuración de gestión de red .....	73
<b>Apéndice 1 Recomendaciones sobre ciberseguridad .....</b>	<b>74</b>

## 1 Iniciar sesión

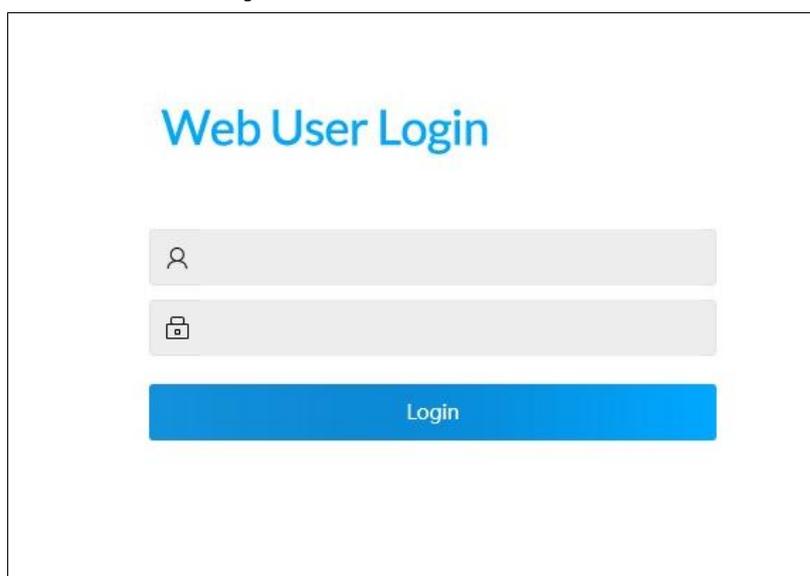
Antes de iniciar sesión, asegúrese de:

- Ya configuraste la dirección IP del switch. La dirección IP de la VLAN 1 es 192.168.1.110 de forma predeterminada.
- La PC con navegador web está conectada a la red y la PC puede hacer ping al conmutador con éxito.

**Paso 1** Ingrese la dirección IP (192.168.1.110 por defecto) del conmutador en la barra de direcciones del navegador web y luego presione Entrar.

El **Acceso** muestra la interfaz. Consulte la Figura 1-1.

Figura 1-1 Inicio de sesión web



**Paso 2** Introduzca el nombre de usuario y la contraseña. El nombre de usuario y la contraseña son admin por defecto.

**Paso 3** Hacer clic **Acceso**.

El **Ajuste rapido** muestra la interfaz.



Modifique la contraseña después del primer inicio de sesión. La contraseña debe constar de 8 a 32 no en blanco caracteres y contienen al menos dos tipos de caracteres entre mayúsculas, minúsculas, número y carácter especial (excepto ' " ; : &).

# 2 ajustes rápidos

Puede ver la información del sistema y configurar los parámetros del dispositivo, la VLAN, la agregación de enlaces, la dirección IP y la ruta. Tome el conmutador PoE de 4 puertos, por ejemplo. La interfaz de configuración rápida es diferente según los modelos de interruptor. Prevalecerá la interfaz real.

## 2.1 Información del sistema

Puede ver el nombre, el tipo, el número de serie, la versión del software, la dirección IP, el estado del puerto y la información del puerto del dispositivo.

Después de iniciar sesión en el sistema, el **Ajuste rápido** muestra la interfaz. Consulte la Figura 2-1. En el conmutador, si el puerto se muestra en verde, significa que el puerto está conectado correctamente. Y si el puerto se muestra gris, significa que el puerto no está conectado o la conexión falla. Consulte la Tabla 2-1.

Figura 2-1 Información del sistema

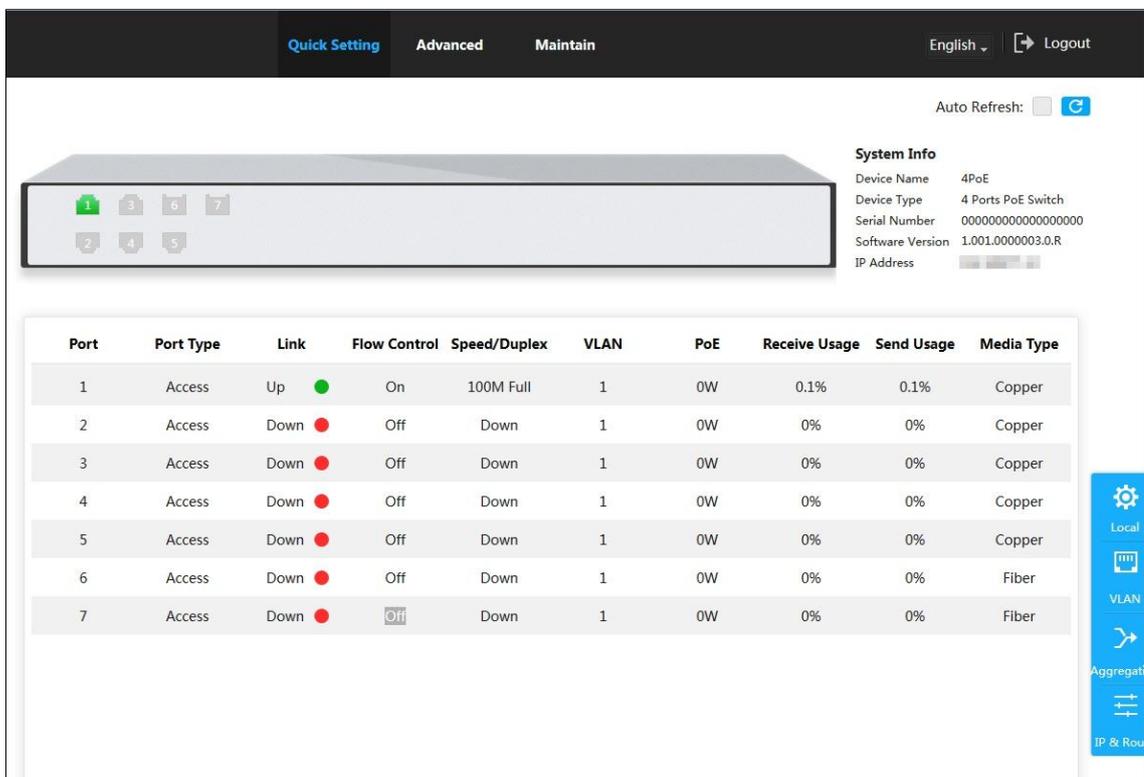


Tabla 2-1 Información del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.  Este interruptor contiene 7 puertos. La cantidad de puertos puede variar según el modelo que haya comprado y prevalecerá el producto real.
Tipo de puerto	Tres tipos: <b>Acceso</b> , <b>Híbrido</b> , y <b>Trompa</b> .
Enlace	Dos estados de enlace: <b>Arriba</b> y <b>Abajo</b> . <b>Arriba</b> indica que el puerto está conectado con éxito, y <b>Abajo</b> indica que el puerto no está conectado o la conexión falla.

Parámetro	Descripción
Control de flujo	Muestra el estado del control de flujo.
Velocidad/Dúplex	- Online: Muestra la tasa de puerto y el modo dúplex. - Desconectado: Muestra <b>Abajo</b> .
VLAN	puerto VLAN. Es VLAN 1 por defecto.
POE	Muestra el consumo de energía de POE. Solo de 1 a 4 puertos son puertos PoE.
Recibir uso	La velocidad de recepción actual se divide por la velocidad promedio en un período determinado (normalmente 5 minutos).
Enviar uso	La velocidad de envío actual se divide por la velocidad media en un período determinado (normalmente 5 minutos).
Tipo de medio	Dos tipos de medios: <b>Cobre</b> y <b>Fibra</b> . <b>Cobre</b> indica puerto RJ-45, y <b>Fibra</b> indica puerto de fibra.

## 2.2 locales

Puede establecer el nombre del sistema, la dirección IP y la máscara de subred.

**Paso 1** Hacer clic **Local** a la derecha de **Ajuste rápido** interfaz. El **Local** se muestra la interfaz. Consulte la Figura 2-2.

Figura 2-2 Locales

**Paso 2** Ingrese el nombre del sistema, la dirección IP y la longitud de la máscara. Hacer clic **DE**

**Paso 3** **ACUERDO**.

## 2.3 VLAN

Agregue el puerto a la VLAN y configure la VLAN. De forma predeterminada, el puerto es VLAN1.

**Paso 1** Hacer clic **VLAN** sobre el **Ajuste rápido** interfaz. El **VLAN** se muestra la interfaz. Consulte la Figura 2-3.

Figura 2-3 VLAN

Port	Mode	Port VLAN	Allowed VLANs
1	Access	1	1
2	Access	1	1
3	Access	1	1
4	Access	1	1
5	Access	1	1
6	Access	1	1
7	Access	1	1

**Paso 2** Configure los parámetros de la VLAN del puerto. Consulte la Tabla 2-2.

Tabla 2-2 Parámetro de configuración de VLAN de puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.
Modo	Tres modos: <b>Acceso</b> , <b>Híbrido</b> , y <b>Trompa</b> . - <b>Acceso</b> : Cuando el puerto se conecta a dispositivos terminales (como PC e IPC), seleccione <b>Acceso</b> . - <b>Trompa</b> : Cuando el puerto se conecte al conmutador, seleccione <b>Trompa</b> . - <b>Híbrido</b> : No se usa con frecuencia.
Puerto VLAN	Agregue el puerto a una VLAN. De manera predeterminada, el puerto pertenece a VLAN1 y el rango es 1-4094.
VLAN permitidas	Configure la VLAN permitida. Cuando el modo es <b>Trompa</b> , puede configurarlo.

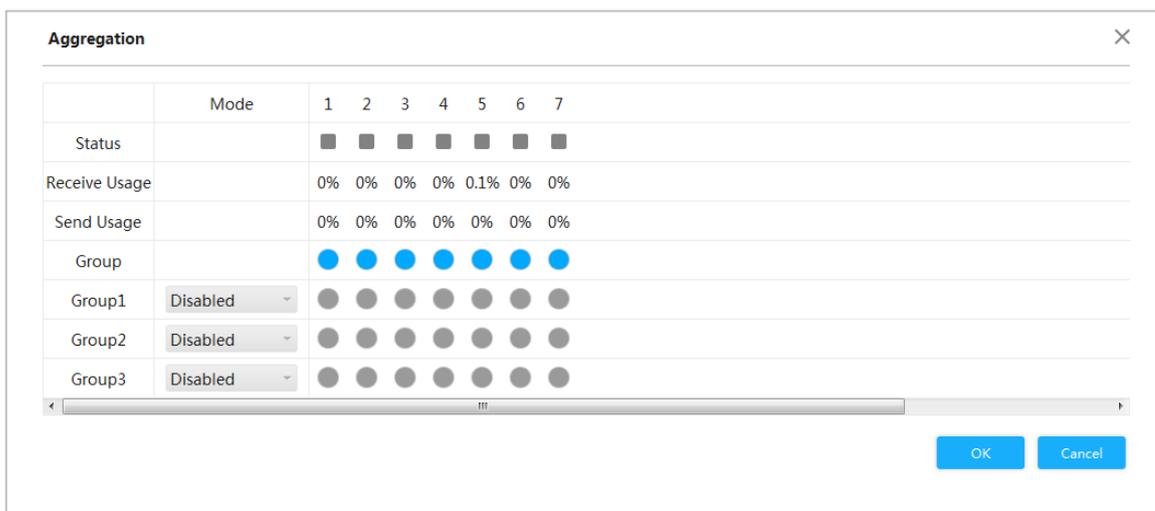
**Paso 3** Hacer clic**DE ACUERDO**.

## 2.4 Agregación

Agregue el puerto a la agregación. Para obtener más información, consulte "3.1.4 Agregación".

Hacer clic**Agregación**en**Ajuste rápido**interfaz, y la**Agregación**se muestra la interfaz. Consulte la Figura 2-4.

Figura 2-4 Agregación



### 2.4.1 Configuración de agregación estática

La agregación estática es un método para combinar o agrupar varios puertos de conmutador o NIC para formar un único canal ethernet. Por ejemplo, agregue el puerto 1 y el puerto 2 al grupo estático 1.

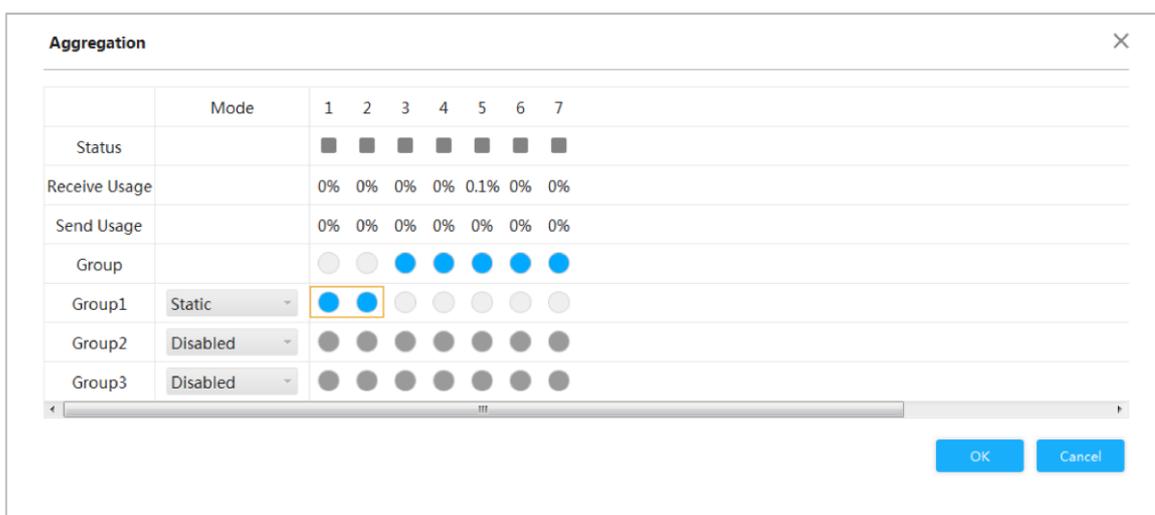
**Paso 1** Seleccionar **Modelo** como **Estático** en el grupo 1, lo que indica que el grupo es una agregación estática. Seleccione

**Paso 2** el puerto 1 y el puerto 2 en el grupo 1 para agregar los dos puertos a la agregación estática. Consulte la Figura 2-5.



Para el conmutador PoE de 4 puertos, puede configurar hasta 3 grupos de agregación estática. Estático la agregación es diferente según los diferentes modelos de conmutador PoE. El actual prevalecerá la interfaz.

Figura 2-5 Configuración estática



**Paso 3** Hacer clic **DE ACUERDO**.

El puerto 1 y el puerto 2 forman un puerto lógico.

## 2.4.2 Configuración de agregación dinámica

La agregación dinámica se diferencia de la agregación estática en que la cantidad de puertos se fija en la agregación estática, pero la cantidad de puertos realmente agregados se ajusta dinámicamente de acuerdo con la estrategia de tasa de flujo.

**Paso 1** Agregue los puertos al grupo dinámico.

- 1) Seleccionar **LACP (activo)** en el **Modo** y agregue los puertos al grupo de agregación. Por ejemplo, agregue el puerto 3 y el puerto 4 al grupo de agregación 2. Consulte la Figura 2-6.
- 2) Seleccionar **LACP (Pasivo)** en el **Modo** y agregue los puertos al grupo de agregación. Por ejemplo, agregue el puerto 5 y el puerto 6 al grupo de agregación 3. Consulte la Figura 2-6.

Figura 2-6 Configuración dinámica

The screenshot shows a configuration window titled 'Aggregation' with a table of port settings. The table has columns for Mode, ports 1-7, Status, Receive Usage, Send Usage, and Group. Three groups are defined: Group1 (Static), Group2 (LACP(Active)), and Group3 (LACP(Passive)). Group2 has ports 3 and 4 selected, and Group3 has ports 5 and 6 selected. A yellow box highlights the LACP(Active) and LACP(Passive) rows.

	Mode	1	2	3	4	5	6	7
Status		■	■	■	■	■	■	■
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		○	○	○	○	○	○	●
Group1	Static	●	●	○	○	○	○	○
Group2	LACP(Active)	○	○	●	●	○	○	○
Group3	LACP(Passive)	○	○	○	○	●	●	○

**Paso 2** Hacer clic **DE ACUERDO**.

## 2.5 IP y Ruta

Puede agregar la dirección IP de la interfaz virtual VLAN y la ruta IP. Para obtener más información, consulte "3.1.1.2 IP y ruta".

**Paso 1** Hacer clic **IP y ruta** sobre el **Ajuste rápido** interfaz. El **IP y ruta** se muestra la interfaz. Consulte la Figura 2-7.

Figura 2-7 IP y ruta

**IP & Route**
✕

---

**IP Config**
+ Add
Delete

	VLAN	IP Address	Mask Length	Delete
<input type="checkbox"/>	1	172.16.0.1	16	Delete

**Route Config**
+ Add
Delete

	Network	Mask Length	Next Hop	Delete
<input type="checkbox"/>	0.0.0.0	0	172.16.0.1	Delete

OK
Cancel

**Paso 2** Agregue la interfaz VLAN.

1) Haga clic **Agregar** en el **Configuración IP** área.

Se agrega un nuevo registro. Consulte la Figura 2-8.

Figura 2-8 Interfaz VLAN

**IP Config**
+ Add
Delete

	VLAN	IP Address	Mask Length	Delete
<input type="checkbox"/>	1	172.16.0.1	16	Delete
<input type="checkbox"/>				Delete

2) Para los parámetros, consulte la Tabla 2-3.

Tabla 2-3 Interfaz VLAN

Parámetro	Descripción
VLAN	Ingrese el número de VLAN.
dirección IP	Configure la dirección IP de la interfaz VLAN.
Longitud de la máscara	Establezca la longitud de la máscara de la interfaz VLAN.

**Paso 3** Agregue la ruta IP.

1) Haga clic **Agregar** en el **Configuración de ruta** área.

Se agrega un nuevo registro. Consulte la Figura 2-9.

Figura 2-9 Ruta IP

The screenshot shows a 'Route Config' interface with two buttons at the top: '+ Add' and 'Delete'. Below is a table with the following structure:

<input type="checkbox"/>	Network	Mask Length	Next Hop	Delete
<input type="checkbox"/>	0.0.0.0	0	172.12.0.1	
<input type="checkbox"/>				

2) Para los parámetros, consulte la Tabla 2-4.

Tabla 2-4 Rutas IP

Parámetro	Descripción
Red	Es el destino del paquete IP.
Longitud de la máscara	La longitud de la máscara, con la dirección de destino, sirve para identificar la dirección IP del host de destino o la ruta. Después del AND lógico entre la dirección de destino y la máscara de red, puede obtener la dirección IP del host de destino o la ruta.
Siguiente salto	La IP del siguiente salto de la ruta.

**Etapa 4** Hacer clic **DE ACUERDO**.

## 3 Configuración avanzada

Puede configurar el sistema, el puerto, la VLAN, la agregación, la tabla MAC y otros parámetros en la interfaz de configuración avanzada. La interfaz de configuración avanzada es diferente según los modelos de conmutador, y prevalecerá la interfaz real. Tome el conmutador PoE de 4 puertos, por ejemplo.

### 3.1 Configuración común

#### 3.1.1 Configuración del sistema

##### 3.1.1.1 Información del sistema

Puede configurar el nombre del dispositivo, la dirección IP, la longitud de la máscara y habilitar DHCP, y ver la información del software, la información del hardware y la hora.



Tenga cuidado cuando habilite el Cliente DHCP. Después de habilitar el Cliente DHCP, el enrutador IP o DHCP El servidor que se conecta al conmutador asignará la dirección IP al conmutador automáticamente y el la dirección IP existente se invalidará y no podrá acceder a la interfaz web.

**Paso 1** Seleccionar **Avanzado > Común > Configuración del sistema > Información del sistema**.

El **Información del sistema** se muestra la interfaz. Consulte la Figura 3-1.

Figura 3-1 Información del sistema

System Info	IP&Route	Current Time	Log
<b>System:</b>			
Device Name:	4PoE		
IP Address:	[Redacted]		
Mask Length:	24		
DHCP Enable:	<input type="checkbox"/>		
<b>Software:</b>			
Software Version:	1.001.0000003.0.R		
Compile Date:	2019-07-31 15:04:43+08:00		
<b>Hardware:</b>			
Device Name:	4PoE		
Device Type:	4 Ports PoE Switch		
IP Address:	[Redacted]		
Mask Length:	24		
MAC Address:	02-00-c1-8b-01-91		
Serial Number:	000000000000000000		
<b>Time:</b>			
System Date:	2018-04-09 03:22:52		
System Running Time:	0 days 23:21:25		
<input type="button" value="Save"/> <input type="button" value="Refresh"/>			

**Paso 2** Ingrese el nombre del dispositivo, la dirección IP y la longitud de la máscara y habilite DHCP. Hacer

**Paso 3** clic **Ahorrar**.

### 3.1.1.2 IP y Ruta

Los hosts de diferentes VLAN no pueden comunicarse. Se necesita la ruta o el conmutador de capa 3 para el reenvío.

El conmutador admite el reenvío de capa 3 a través de la interfaz VLAN. La interfaz VLAN es la interfaz virtual del modo de capa 3, para la comunicación de capa 3 entre las VLAN. no es el físico

entidad en el dispositivo. Cada VLAN está relacionada con una interfaz VLAN, y la interfaz VLAN puede reenviar paquetes para la VLAN. Generalmente, debido a que la VLAN puede aislar el dominio de transmisión, cada VLAN corresponde a un segmento de red. La interfaz VLAN es la puerta de enlace del segmento de red y admite el reenvío de capa 3 para el mensaje según la dirección IP. Paso 1

Seleccionar **Avanzado > Común > Configuración del sistema > IP y ruta**. El **IP y ruta** se muestra la interfaz. Consulte la Figura 3-2.

Figura 3-2 IP y ruta

The screenshot shows a web-based configuration interface for IP and routing. At the top, there are tabs for 'System Info', 'IP&Route', 'Current Time', and 'Log'. Below the tabs, there are buttons for '+ Add' and 'Delete' under the 'IP Setting' section. The 'IP Setting' section contains a table with the following data:

VLAN	IP Address	Mask Length	Delete	Delete IP
1	192.168.1.1	16	<input type="checkbox"/>	<input type="checkbox"/>

To the right of the IP Setting table is a table for the interface configuration:

Interface	Address	Status
1	192.168.1.1	UP

Below these tables is the 'Route Setting' section, which also has '+ Add' and 'Delete' buttons. It contains a table with the following data:

Network	Mask Length	Next Hop	Delete
0.0.0.0	0	192.168.1.1	<input type="checkbox"/>

To the right of the Route Setting table is another table for route details:

Destination	Mask Length	Protocol	Priority	Next Hop	Egress
0.0.0.0	0	Static	60	192.168.1.1	0
192.168.1.0	16	Direct	0	VLAN1	-

At the bottom left of the interface is a 'Save' button.

**Paso 2** Agregue la interfaz VLAN.

1) Haga clic **Agregar** en **Configuración de IP** región.

El **Agregar IP** se muestra la interfaz. Consulte la Figura 3-3.

Figura 3-3 Agregar IP

2) Para los parámetros, consulte la Tabla 3-1.

Tabla 3-1 Interfaz VLAN

Parámetro	Descripción
VLAN	Ingrese el número de VLAN.
dirección IP	Configure la dirección IP de la interfaz VLAN.
Longitud de la máscara	Configure la longitud de la máscara de la dirección IP.

3) Haga clic **DE ACUERDO**.

**Paso 3** Agregue la ruta IP.

1) Haga clic **Agregar** en el **Configuración de ruta** región.

El **Añadir ruta** se muestra la interfaz. Consulte la Figura 3-4.

Figura 3-4 Agregar ruta

2) Para los parámetros, consulte la Tabla 3-2.

Tabla 3-2 Rutas IP

Parámetro	Descripción
Red	Es el destino del paquete IP.
Longitud de la máscara	La longitud de la máscara, con la dirección de destino, es para identificar la dirección IP del host de destino o la ruta. Después del AND lógico entre la dirección de destino y la máscara de red, puede obtener la dirección IP del host de destino o la ruta.
Siguiente salto	La IP del siguiente salto de la ruta.

3) Haga clic **DE ACUERDO**.

### 3.1.1.3 Hora del sistema

Establezca la hora del sistema del cambio.

Seleccionar **Avanzado > Común > Configuración del sistema > Hora actual**.

El **Tiempo actual** se muestra la interfaz. Consulte la Figura 3-5.

Figura 3-5 Hora actual (1)

The screenshot shows a web interface for configuring the system's current time. It features a top navigation bar with four tabs: 'System Info', 'IP&Route', 'Current Time', and 'Log'. The 'Current Time' tab is active. Below the navigation bar, the title 'Current Time' is displayed. The configuration area includes a date input field showing '2018-12-17', a time input field showing '11 : 19 : 26', and a blue 'Sync PC' button. There is also an unchecked checkbox labeled 'NTP Enable'. Below this, there are two input fields for 'Server1' and 'Server2'. At the bottom of the configuration area, there are two blue buttons: 'Save' and 'Refresh'.

Puede configurar la hora del sistema a través de los siguientes tres métodos:

- Configurar la hora manualmente  
Configure la fecha y la hora en **Tiempo actual** interfaz y luego haga clic en **Ahorrar**. tiempo de sincronización
- Hacer clic **Sincronizar PC** y la hora del interruptor se sincroniza automáticamente con la hora de la PC local. Sincronizar la hora del servidor NTP

Solo con el servidor NTP configurado en la red puede habilitar esta función en los siguientes pasos:

Paso 1 Selecciona el **Habilitar NTP** cuadro para habilitar el servicio NTP.

Paso 2 Configure la dirección IP del servidor NTP. Consulte la Figura 3-6.

Figura 3-6 Hora actual (2)

The screenshot displays the 'Current Time' configuration interface. At the top, there are four tabs: 'System Info', 'IP&Route', 'Current Time' (which is selected and highlighted in blue), and 'Log'. Below the tabs, the title 'Current Time' is displayed. The interface includes a date selection field showing '2018-12-17' with a calendar icon to its right. Below the date is a time selection field showing '11 : 20 : 47' and a dark grey button labeled 'Sync PC'. A checkbox labeled 'NTP Enable' is checked. Below this are two input fields for 'Server1' and 'Server2'. At the bottom of the form are two blue buttons: 'Save' and 'Refresh'.

**Paso 3** Hacer clic **Ahorrar**.

La hora del interruptor se sincroniza automáticamente con la hora del servidor 1.

### 3.1.1.4 Registro

Puede ver registros, exportar registros y borrar registros.

Seleccionar **Avanzado** > **Común** > **Configuración del sistema** > **Registro**. El **Registro** se muestra la interfaz. Consulte la Figura 3-7.

Figura 3-7 Registro

The screenshot shows a web interface for viewing system logs. At the top, there are tabs for 'System Info', 'IP&Route', 'Current Time', and 'Log'. Below the tabs, there are input fields for 'Start Time' (1970-01-01 00:00:00) and 'End Time' (2018-05-13 10:17:27). A 'Log Level' dropdown is set to 'All', and a 'Search' button is present. The main area contains a table with the following data:

No.	Log Time	Log Level	Description
1	2018-03-31 03:16:59	Informational	SYS-BOOTING: Switch just made a cold boot.
2	2018-03-31 03:17:04	Informational	USERS: modify the password of user [admin]
3	2018-03-31 03:17:07	Notice	CHIP 1, PSE CHIP FOUND
4	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/1, changed state to up (MEP).
5	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/2, changed state to up (MEP).
6	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/3, changed state to up (MEP).
7	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/4, changed state to up (MEP).
8	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/5, changed state to up (MEP).
9	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/6, changed state to up (MEP).

At the bottom of the table, there are navigation controls showing '1 / 52' and '1' with arrows. Below the table, there are 'Export' and 'Clear' buttons.

- Ver los registros.  
Establezca la hora de inicio, la hora de finalización y el nivel de registro, y luego haga clic en **Buscar** para ver los detalles de los registros. **Nivel de registro** incluye **Error**, **Advertencia**, **Aviso** y **Información**. Hacer clic **Exportar** para exportar todos los registros. Hacer clic **Clear** para borrar todos los registros.
- 

### 3.1.2 Configuración de puertos

Puede configurar los parámetros del puerto, incluida la velocidad, dúplex completo y dúplex medio, etc. Paso

1 Seleccione Avanzado > Común > Puerto.

El **Configuración del puerto** se muestra la interfaz. Consulte la Figura 3-8.

Figura 3-8 Configuración de puertos

Port Configuration

Port	Link	Speed Duplex Status	Speed Duplex Setting	Flow Control Status	Flow Control Setting	Ingress Limit Enable	Ingress Limit (kbps)	Egress Limit Enable	Egress Limit (kbps)	Receive Usage	Send Usage
1	Down	Down	Auto	Off			500		500	0%	0%
2	Down	Down	Auto	Off			500		500	0%	0%
3	Down	Down	Auto	Off			500		500	0%	0%
4	Down	Down	Auto	Off			500		500	0%	0%
5	Up	1G Full	Auto	Off			500		500	0.1%	0%
6	Down	Down	Auto	Off			500		500	0%	0%
7	Down	Down	Auto	Off			500		500	0%	0%

Save Refresh

Paso 2 Para los parámetros, consulte la Tabla 3-3.

Tabla 3-3 Parámetro de puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.
Enlace	Verde <b>Arriba</b> indica que el puerto está conectado con éxito, y rojo <b>Abajo</b> indica que el puerto no está conectado o la conexión falla.
Estado de velocidad dúplex	<b>Abajo</b> significa desconexión, y la velocidad específica significa conexión exitosa. <b>Lleno</b> significa dúplex completo; <b>Medio</b> significa medio dúplex.
Configuración de velocidad dúplex	Configure la velocidad y el modo dúplex.  La velocidad y el modo dúplex del puerto combinado se fijan en <b>Auto</b> .
Estado de control de flujo	Muestra el estado real del negociador o habilitado del control de flujo, incluidos ON y OFF. - ENCENDIDO: La negociación tiene éxito. - APAGADO: La negociación falla.
Configuración de control de flujo	Función de control de flujo ON/OFF. -  : El control de flujo está activado. -  : El control de flujo está APAGADO.
Habilitar límite de ingreso	Habilitar/deshabilitar el límite de ingreso. -  : La habilitación de ingreso está habilitada. -  : La habilitación de ingreso está deshabilitada.

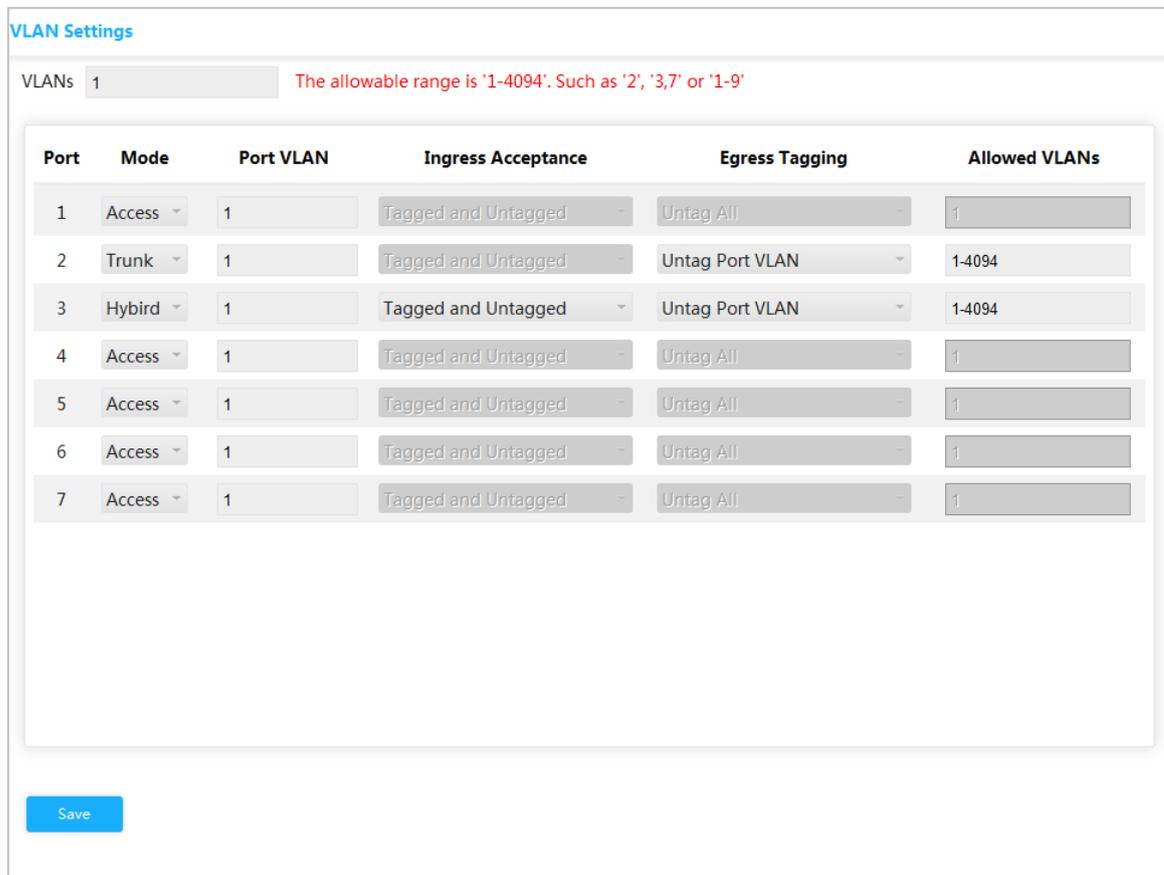
Parámetro	Descripción
Límite de ingreso (kbps)	Establecer el límite de entrada.
Habilitar límite de salida	Habilitar/deshabilitar el límite de salida.  : La habilitación de salida está habilitada.  : La habilitación de salida está deshabilitada.
Límite de salida (kbps)	Establecer el límite de salida.
Recibir uso	Muestra el uso de aceptación.
Enviar uso	Muestra el uso de envío.

**Paso 3** Hacer clic **Ahorrar**.

### 3.1.3 Configuración de VLAN

Agregue el puerto a la VLAN y configure la VLAN. De forma predeterminada, el puerto pertenece a VLAN1. **Paso 1** Seleccionar **Avanzado > Común > Configuración de VLAN**. El **Configuración de VLAN** se muestra la interfaz. Consulte la Figura 3-9.

Figura 3-9 Configuración de VLAN



VLAN Settings

VLANs  The allowable range is '1-4094'. Such as '2', '3,7' or '1-9'

Port	Mode	Port VLAN	Ingress Acceptance	Egress Tagging	Allowed VLANs
1	Access	1	Tagged and Untagged	Untag All	1
2	Trunk	1	Tagged and Untagged	Untag Port VLAN	1-4094
3	Hybird	1	Tagged and Untagged	Untag Port VLAN	1-4094
4	Access	1	Tagged and Untagged	Untag All	1
5	Access	1	Tagged and Untagged	Untag All	1
6	Access	1	Tagged and Untagged	Untag All	1
7	Access	1	Tagged and Untagged	Untag All	1

**Paso 2** Ingrese 1, 2 en VLAN para crear VLAN 1 y VLAN 2. Configure

**Paso 3** los parámetros de VLAN del puerto. Consulte la Tabla 3-4.

Tabla 3-4 Parámetro de configuración de VLAN de puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.
Modo	Tres modos: <b>Acceso, Híbrido, y Trompa</b> .

Parámetro	Descripción
Puerto VLAN	Agregue el puerto a una VLAN. De forma predeterminada, el puerto pertenece a VLAN1. El rango es 1-4094.
Aceptación de ingreso	Muestra si los datos pueden fluir al puerto. Solo <b>Híbrido</b> admite la configuración (de manera predeterminada, toda la fecha fluye hacia el puerto en otros modelos). Ver las siguientes situaciones: <ul style="list-style-type: none"> <li>- <b>Etiquetado y sin etiquetar:</b> Todos los datos fluyen hacia el puerto. <b>Solo</b></li> <li>- <b>etiquetados:</b> Solo los datos etiquetados pueden fluir hacia el puerto. <b>Solo sin</b></li> <li>- <b>etiquetar:</b> solo los datos sin etiquetar pueden fluir al puerto.</li> </ul>
Etiquetado de salida	Muestra si etiquetar los datos que saldrán del puerto. Vea las siguientes tres situaciones: <ul style="list-style-type: none"> <li>- <b>Desetiquetar puerto VLAN:</b> Si la etiqueta de flujo de datos es la misma que PVID, la etiqueta se despegará.</li> <li>- <b>etiquetar todo:</b> Todos los datos serán etiquetados.</li> <li>- <b>Desetiquetar todo:</b> No se etiquetarán todos los datos.</li> </ul>
VLAN permitidas	Configure la VLAN permitida.

Etapa 4 Hacer clic **Ahorrar**.

## 3.1.4 Agregación

La agregación consiste en formar los múltiples puertos físicos del conmutador en el puerto lógico. Los enlaces múltiples en el mismo grupo se pueden considerar como un enlace lógico con el mayor ancho de banda.

A través de la agregación, los puertos en el mismo grupo pueden compartir el flujo de comunicación para generar un mayor ancho de banda. Además, los puertos del mismo grupo pueden realizar copias de seguridad de forma recíproca y dinámica para mejorar la fiabilidad del enlace.

### 3.1.4.1 Configuración estática

Paso 1 Seleccionar **Avanzado > Común > Agregación**.

El **Agregación** se muestra la interfaz. Consulte la Figura 3-10.

Figura 3-10 Agregación

Aggregation								
Aggregation Configuration <input checked="" type="checkbox"/> Source MAC Address <input type="checkbox"/> Destination MAC Address <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> TCP/UDP Port								
	Mode	1	2	3	4	5	6	7
Status		■	■	■	■	■	■	■
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		●	●	●	●	●	●	●
Group1	Disabled	●	●	●	●	●	●	●
Group2	Disabled	●	●	●	●	●	●	●
Group3	Disabled	●	●	●	●	●	●	●

Save Refresh

**Paso 2** Seleccione el modo de algoritmo de equilibrio de carga de agregación en **Configuración de agregación**. Hay cuatro tipos:

- Dirección MAC de origen: el algoritmo de equilibrio de carga de agregación basado en la dirección MAC.
- Dirección MAC de destino: el algoritmo de equilibrio de carga de agregación basado en la dirección MAC de destino.
- Dirección IP: el algoritmo de equilibrio de carga de agregación basado en la dirección IPv4 de origen y la dirección IPv4 de destino.
- Puerto TCP/UDP: el algoritmo de equilibrio de carga de agregación basado en el puerto TCP/UDP de origen y destino.

**Paso 3** Seleccione **Estático** en el **Modo** y agregue los puertos al grupo de agregación dinámica. Por ejemplo, agregue el puerto 1 y el puerto 2 al grupo de agregación. Consulte la Figura 3-11.



Con respecto al conmutador PoE de 4 puertos, se pueden configurar como máximo 3 grupos de agregación estática en el mismo tiempo. El grupo de agregación estática es diferente según los modelos de conmutador. Prevalecerá la interfaz real.

Figura 3-11 Configuración estática

Aggregation Configuration								
<input checked="" type="checkbox"/> Source MAC Address <input type="checkbox"/> Destination MAC Address <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> TCP/UDP Port								
	Mode	1	2	3	4	5	6	7
Status		■	■	■	■	■	■	■
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Group1	Static	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Group2	Disabled	<input type="radio"/>						
Group3	Disabled	<input type="radio"/>						

**Etapa 4** Hacer clic **Ahorrar**.

El puerto 1 y el puerto 2 forman un puerto lógico.

### 3.1.4.2 LACP

LACP (protocolo de control de agregación de enlaces) es el protocolo para la agregación dinámica de enlaces. LACP se comunica con otro puerto a través de LACPDU (Unidad de datos del protocolo de control de agregación de enlaces).

Seleccione la función del puerto de la lista desplegable en **Modo**. Hay dos tipos:

- **Activo:** El puerto puede enviar paquetes LACPDU activamente al puerto opuesto y analiza el LACP.
- **Pasivo:** El puerto no puede enviar el paquete LACPDU de forma activa. Después de recibir el paquete LACP enviado por el puerto opuesto, el puerto analiza el LACP.

**Paso 1** Seleccione Avanzado > Común > Agregación.

El **Agregación** se muestra la interfaz. Consulte la Figura 3-12.

Figura 3-12 LACP (1)

Aggregation								
Aggregation Configuration <input checked="" type="checkbox"/> Source MAC Address <input type="checkbox"/> Destination MAC Address <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> TCP/UDP Port								
	Mode	1	2	3	4	5	6	7
Status		<input type="checkbox"/>						
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		<input checked="" type="checkbox"/>						
Group1	Disabled	<input type="checkbox"/>						
Group2	Disabled	<input type="checkbox"/>						
Group3	Disabled	<input type="checkbox"/>						

**Paso 2** Seleccionar **LACP (Pasivo)** en el **Modo** y agregue el miembro del puerto al grupo de agregación dinámica. Por ejemplo, agregue el puerto 3 y el puerto 4 al grupo de agregación 2. Consulte la figura 3-13.

**Paso 3** Seleccionar **LACP (Pasivo)** en el **Modo** y agregue el miembro del puerto al grupo de agregación dinámica. Por ejemplo, agregue el puerto 5 y el puerto 6 al grupo de agregación 3. Consulte la figura 3-13.

Figura 3-13 LACP (2)

Aggregation								
Aggregation Configuration <input checked="" type="checkbox"/> Source MAC Address <input type="checkbox"/> Destination MAC Address <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> TCP/UDP Port								
	Mode	1	2	3	4	5	6	7
Status		<input type="checkbox"/>						
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group1	Disabled	<input type="checkbox"/>						
Group2	LACP(Active)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group3	LACP(Passive)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Etapa 4** Hacer clic **Ahorrar**.

### 3.1.5 Tabla MAC

La tabla MAC (Media Access Control) registra la relación entre la dirección MAC y el puerto, y la información, incluida la VLAN a la que pertenece el puerto. Cuando el dispositivo está reenviando el paquete, consulta en la tabla de direcciones MAC la dirección MAC de destino del paquete. Si la dirección MAC de destino del paquete está contenida en la tabla de direcciones MAC, el paquete se reenvía directamente a través del puerto de la tabla. Y si el destino MAC

La dirección del paquete no está contenida en la tabla de direcciones MAC, el dispositivo adopta la transmisión para reenviar el paquete a todos los puertos excepto al puerto de recepción en la VLAN.

### 3.1.5.1 Adición de una tabla MAC estática

**Paso 1** Seleccione **Avanzado > Común > Tabla MAC > Tabla de direcciones MAC**. El **Tabla de direcciones MAC** muestra la interfaz. Consulte la Figura 3-14.

Figura 3-14 Tabla de direcciones MAC

<input type="checkbox"/>	MAC Address	Type	VLAN	Port	Delete
<input type="checkbox"/>	00:00:00:00:00:01	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:02	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:03	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:04	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:05	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:06	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:07	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:08	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:09	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:0A	Dynamic	1	5	

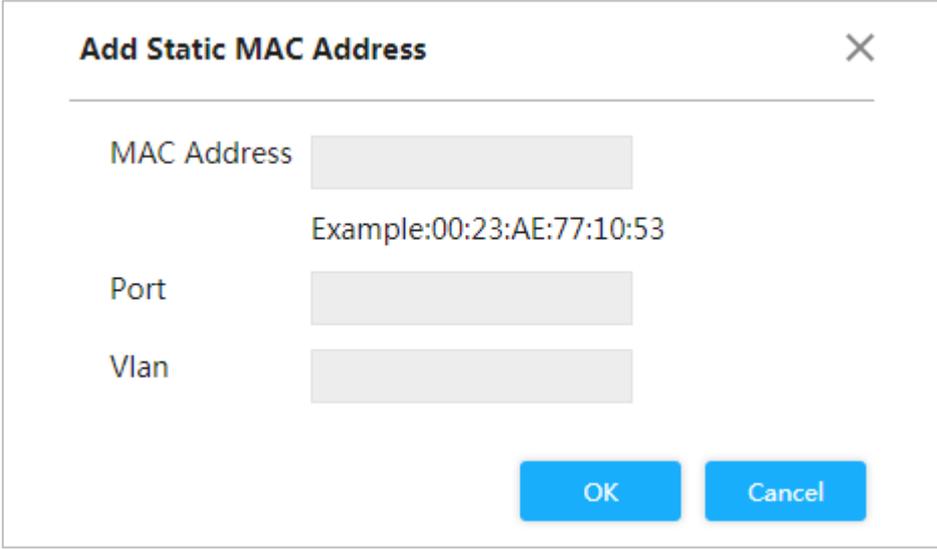
**Paso 2** Vincule la dirección MAC al puerto en la VLAN determinada. Por ejemplo, vincule la dirección MAC 00:00:00:00:00:01 al puerto 3 en la VLAN 2.

1) Haga clic **Agregar**.

El **Agregar dirección MAC estática** muestra la interfaz.

2) Configure la dirección MAC, el puerto y la VLAN. Consulte la Figura 3-15.

Figura 3-15 Adición de una tabla MAC estática



**Add Static MAC Address** [X]

MAC Address   
Example:00:23:AE:77:10:53

Port

Vlan

OK Cancel

3) Haga clic **DE ACUERDO**.

### 3.1.5.2 Filtrado de puertos MAC

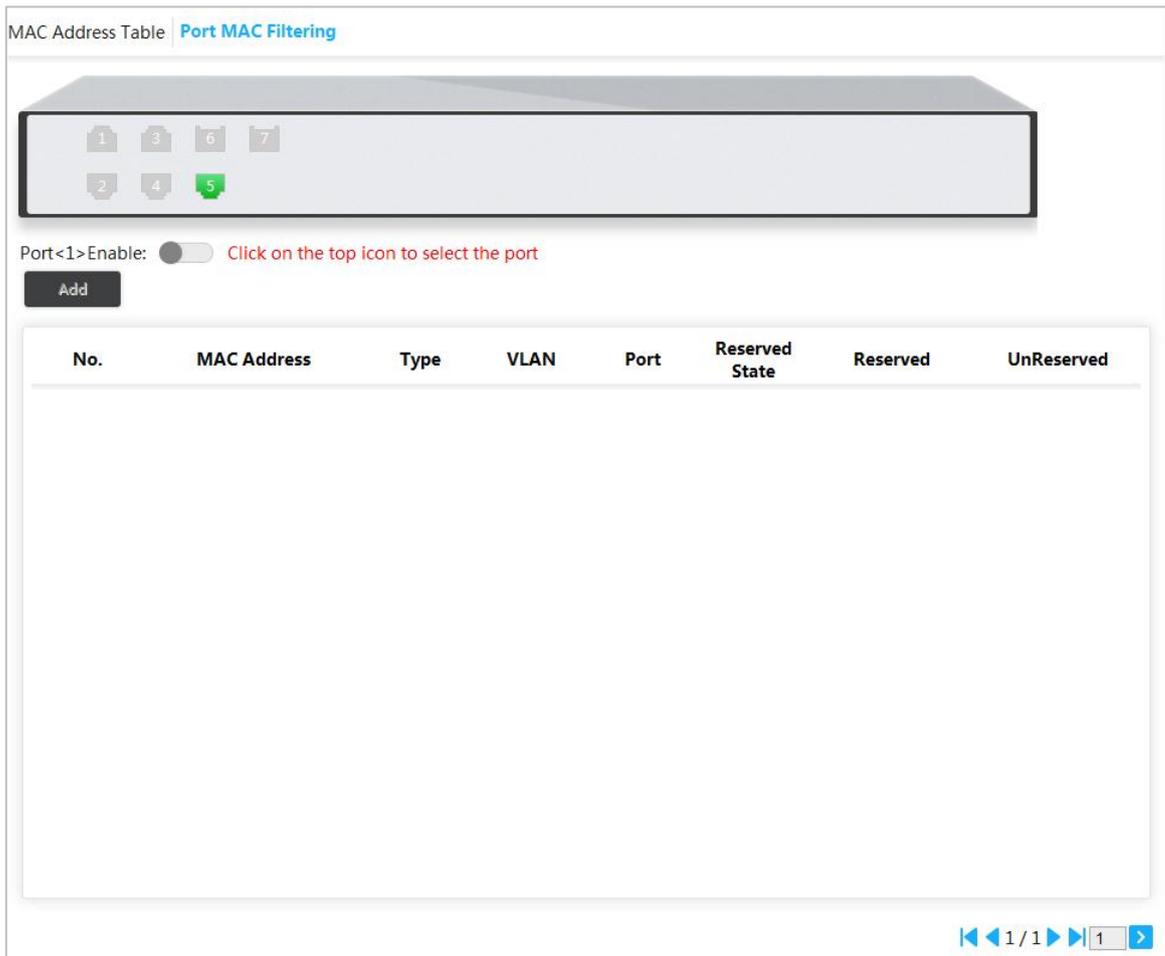
Después de habilitar el filtrado MAC del puerto, los siguientes dos dispositivos MAC pueden comunicarse con el puerto.

- Dispositivos en la lista blanca de MAC
- Los dispositivos MAC estáticos cambian de los dispositivos MAC dinámicos

**Paso 1** Seleccione Avanzado > Común > Tabla MAC > Filtrado de puertos MAC. El

**Filtrado de puertos MAC** se muestra la interfaz. Consulte la Figura 3-16.

Figura 3-16 Filtrado MAC de puertos

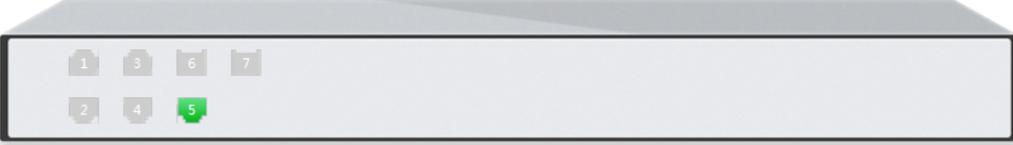


**Paso 2** Seleccione el puerto, como el puerto 5.

**Paso 3** Hacer clic  detrás **Puerto <5> Habilitar** para habilitar el puerto. Consulte la Figura 3-17.

Figura 3-17 Habilitar el filtrado MAC del puerto

MAC Address Table **Port MAC Filtering**



Port<5>Enable:  Click on the top icon to select the port

Add

No.	MAC Address	Type	VLAN	Port	Reserved State	Reserved	UnReserved
1	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
2	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
3	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
4	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
5	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
6	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
7	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
8	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
9	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
10	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved

Save

- Cambie el dispositivo MAC dinámico a estático.
- 1) Seleccione un registro y haga clic en **Reservado**.
- 2) Haga clic **Ahorrar**. El tipo cambia de **Dinámica** a **Estático**. Los dispositivos MAC estáticos pueden comunicarse con el puerto normalmente. Agregar lista blanca de MAC.
- Haga clic **Agregar**.

El **Agregar lista blanca de MAC** se muestra la interfaz. Consulte la Figura 3-18.

Figura 3-18 Agregar lista blanca de MAC.

### Add MAC Whitelist ✕

---

MAC Address

Example:00:23:AE:77:10:53

VLAN

2) Configure la dirección MAC y la VLAN.

3) Haga clic **DE ACUERDO**.

Los dispositivos en la lista blanca de MAC pueden comunicarse con el puerto normalmente.

### 3.1.6 Árbol de expansión

El protocolo de árbol de expansión es el protocolo de la capa 2. Puede eliminar el ciclo de anillo de la capa 2 eligiendo bloquear los enlaces redundantes en la red y puede respaldar los enlaces.

Al igual que otros protocolos, el protocolo de árbol de expansión se actualiza con el desarrollo de la red: de STP (Protocolo de árbol de expansión), a RSTP (Protocolo de árbol de expansión rápido) y al último MSTP (Protocolo de árbol de expansión múltiple).

**Paso 1** Seleccione **Avanzado > Común > Árbol de expansión > Configuración de puertos STP**. El

**Configuración de puertos STP** se muestra la interfaz. Consulte la Figura 3-19.

Figura 3-19 Configuración de puertos STP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
------	--	-----	-------	--------	-------------------	-----------------

**Paso 2** Seleccione el modo STP: **STP, RSTP y MSTP**.

- **STP**: El protocolo de árbol de expansión más básico.
- **RSTP**: Mejorado basado en STP y realiza una convergencia rápida de la topología de la red.
- **MSTP**: Remedia los defectos de STP y RSTP. MSTP no solo logra una rápida convergencia, sino que también proporciona un mejor mecanismo de reparto de carga para los enlaces redundantes al reenviar el flujo desde diferentes VLAN a través de sus propias rutas.

**Paso 3** Hacer clic **Ahorrrar**, y los resultados son varios según los diferentes modos. Consulte la Figura 3-20, la Figura 3-21 y la Figura 3-22.

Figura 3-20 STP

STP Port Settings

STP Mode: STP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
1	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
2	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
3	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
4	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
5	<input type="checkbox"/>	128	-	Non-STP	Forwarding	-
6	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
7	<input type="checkbox"/>	128	-	Non-STP	Discarding	-

Save

Figura 3-21 RSTP

STP Mode: RSTP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
1	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
2	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
3	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
4	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
5	<input type="checkbox"/>	128	-	Non-STP	Forwarding	-
6	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
7	<input type="checkbox"/>	128	-	Non-STP	Discarding	-

Save

Figura 3-22 MSTP

STP Port Settings

STP Mode: MSTP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
1	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
2	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
3	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
4	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
5	<input type="checkbox"/>	128	-	Non-STP	Forwarding	-
6	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
7	<input type="checkbox"/>	128	-	Non-STP	Discarding	-

Save

**Etapas 4** Seleccione al menos 3 puertos para combinar un snoop STP/RSTP/MSTP. Por ejemplo: Puerto 1, puerto 2 y puerto 3 combinan un snoop STP. Consulte la Figura 3-23.

Figura 3-23 Snoop STP

STP Port Settings

STP Mode: STP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
1	<input checked="" type="checkbox"/>	128	-	Non-STP	Discarding	-
2	<input checked="" type="checkbox"/>	128	-	Non-STP	Discarding	-
3	<input checked="" type="checkbox"/>	128	-	Non-STP	Discarding	-
4	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
5	<input type="checkbox"/>	128	-	Non-STP	Forwarding	-
6	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
7	<input type="checkbox"/>	128	-	Non-STP	Discarding	-

Save

**Paso 5** Hacer clic **Ahorrar**.

Los estados del puerto 1, puerto 2 y puerto 3 cambiarán.

## 3.1.7 PoE de larga distancia

Después de habilitar PoE de larga distancia, la distancia máxima de transmisión cambiará de 100 m a 250 m, y la velocidad de transmisión se reducirá de 1 Gbps a 10 Mbps.

Seleccionar **Avanzado > Configuración del sistema > PoE de larga distancia** y luego seleccione la casilla de verificación del puerto correspondiente para habilitar PoE de larga distancia. **Clic en Guardar.**

Figura 3-24 PoE de larga distancia

Port	Enable
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

Save

## 3.2 Configuraciones poco utilizadas

### 3.2.1 ERPS

ERPS (Ethernet Ring Protection Switching) es el estándar de protocolo de prevención de bucle de capa 2 definido por ITU-T, y el número estándar es ITU-T G.8032/Y1344. Por eso también se llama G.8032. Define el paquete de protocolo RAPS (Ring Auto Protection Switching) y el esquema de conmutación de protección.

ERPS admite dos versiones (V1 y V2). V1 fue lanzado por ITU-T en junio de 2008 y V2 fue lanzado por ITU-T en agosto de 2010. V2 es compatible con V1 y agrega las siguientes funciones:

1. Redes de anillos múltiples, incluido el anillo de cruce.
2. Paquete RAPS de conmutación de subanillo por canal virtual o canal no virtual.
3. Cambiar bloques de forma forzada y manual.
4. El interruptor de reversa de ERPS es configurable.

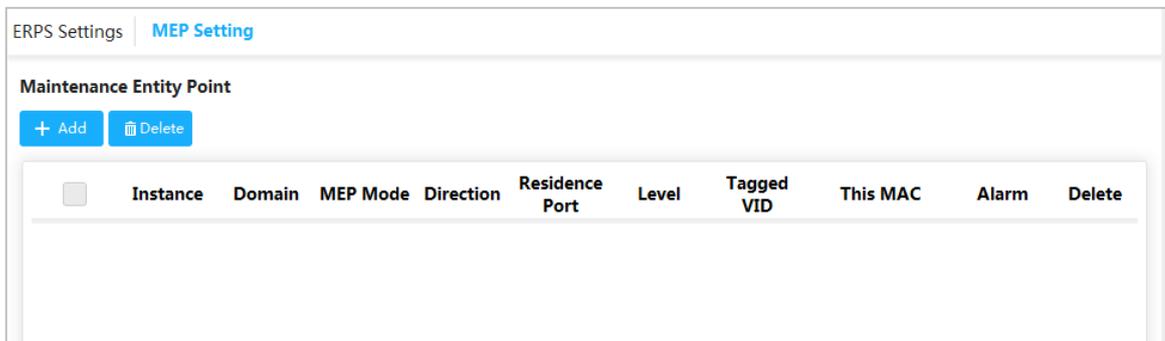
#### 3.2.1.1 Configuración MEP

MEP (Punto de entidad de mantenimiento) es una parte de ERPS.

El dispositivo de capa 2 agregado a ERPS se denomina nodo. No agregue más de 2 puertos en un ERPS para cada nodo.

**Paso 1** Seleccione Avanzado > Poco uso > ERPS > Configuración MEP. El **Configuración de MEP** se muestra la interfaz. Consulte la Figura 3-25.

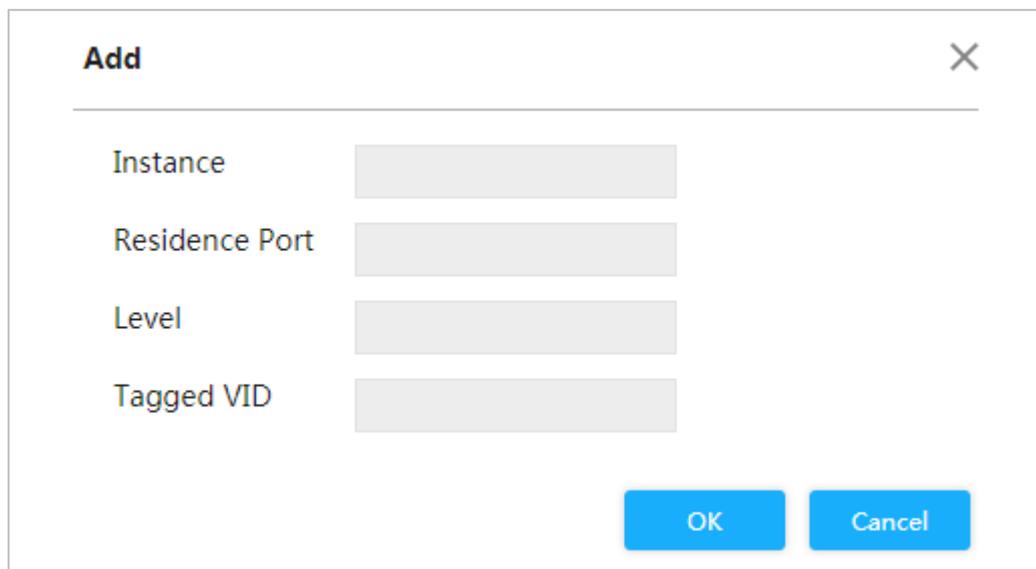
Figura 3-25 Configuración MEP



**Paso 2** Hacer clic **Agregar**.

El **Agregarse** se muestra la interfaz. Consulte la Figura 3-26.

Figura 3-26 Agregar



**Paso 3** Para los parámetros, consulte la Tabla 3-5.

Tabla 3-5 Parámetros MEP

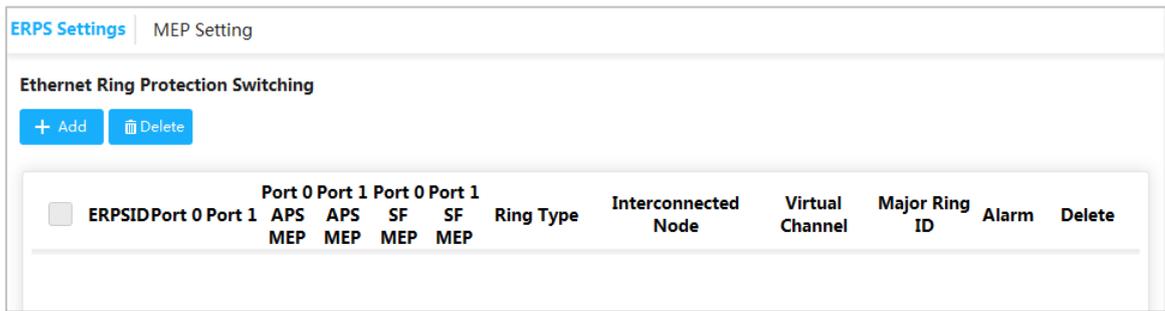
Parámetro	Descripción
Instancia	Ingrese el número de instancia de MEP, como 1.
Puerto de Residencia	Ingrese el número de puerto al que pertenece el MEP, como Puerto 1.
Nivel	Nivel de mantenimiento. Se recomienda configurarlo en 0.
VÍDEO etiquetado	Ingrese el protocolo VLAN, como VLAN 3.

**Etapa 4** Hacer clic **DE ACUERDO**.

### 3.2.1.2 Configuración de ERPS

**Paso 1** Seleccione Avanzado > Poco utilizado > ERPS > Configuración de ERPS. El **Configuración de ERPS** se muestra la interfaz. Consulte la Figura 3-27.

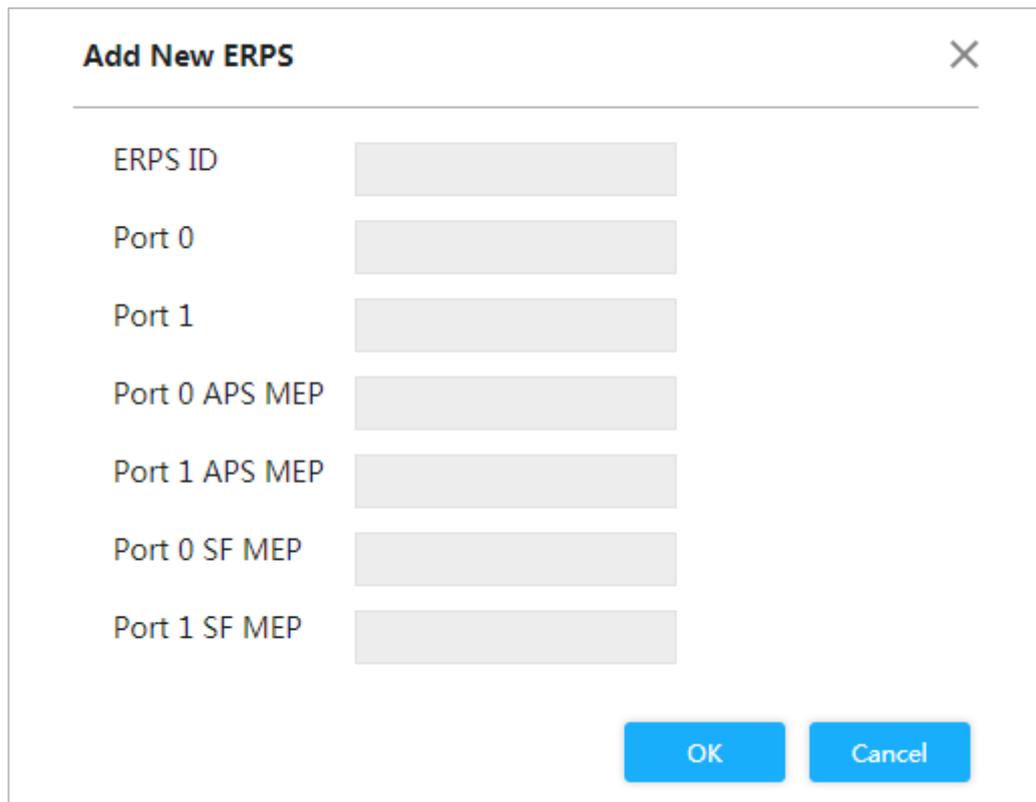
Figura 3-27 Configuración de ERPS



**Paso 2** Hacer clic **Agregar**.

El **Añadir ERPS** se muestra la interfaz. Consulte la Figura 3-28.

Figura 3-28 Agregar ERPS



**Paso 3** Para los parámetros, consulte la Tabla 3-6.

Tabla 3-6 Parámetros de ERPS

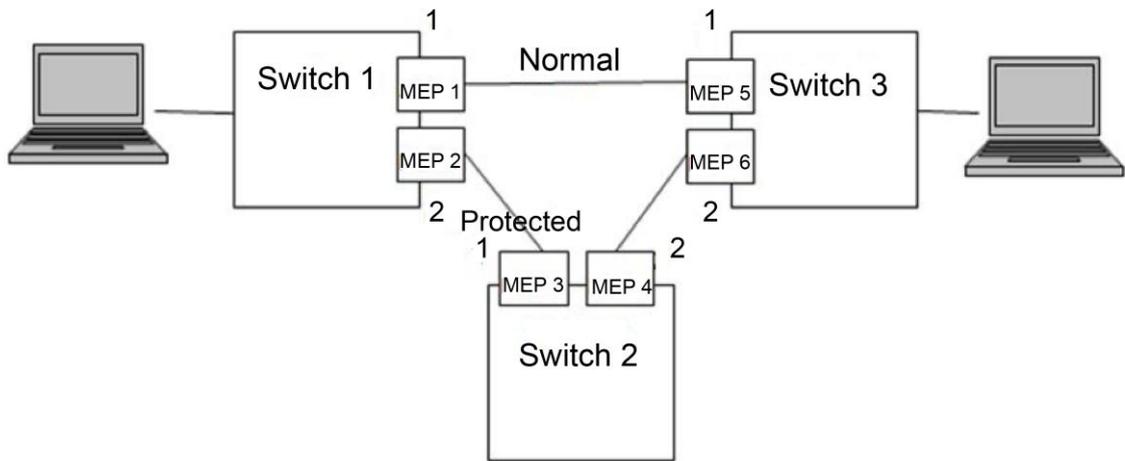
Parámetro	Descripción
ID de ERP	El número de identificación de ERPS.
Puerto 0	Los dos puertos se agregaron al ERPS.
Puerto 1	
Puerto 0 APS MEP	El paquete de protocolo correspondiente ERPS al puerto ERPS. Mantenga el puerto 0 APS MEP consistente con el puerto 0 SF MEP. Mantenga el puerto 1 APS MEP consistente con el puerto 1 SF MEP. Por ejemplo: Puerto 0 APS MEP es 1 y Puerto 1 APS MEP es 2.
Puerto 1 APS MEP	
Puerto 0 SF MEP	La correspondiente agregación de inspección MEP del puerto ERPS. Mantenga el puerto 0 APS MEP consistente con el puerto 0 SF MEP. Mantenga el puerto 1 APS MEP consistente con el puerto 1 SF MEP. Por ejemplo: Port 0 SF MEP es 1 y Port 1 SF MEP es 2.
Puerto 1 SF MEP	

### 3.2.1.3 Ejemplo: configuración de anillo único de ERPS

#### Requisito de red

Se solicitan tres conmutadores, puerto 1 y puerto 2 para combinar un ERPS. Consulte la Figura 3-29. La relación correspondiente: Switch 1: MEP 1 y MEP 2; Conmutador 2: MEP3 y MEP 4; Interruptor 3: MEP 5 y MEP 6.

Figura 3-29 Configuración de un solo anillo de ERPS



#### Configuración

Configure el ERPS con los siguientes pensamientos:

- 1) Confirme la topología y planifique la VLAN de protección y la VLAN de protocolo.
- 2) Confirme el puerto propietario de RPL.
- 3) Asegúrese de deshabilitar la función mutex de los puertos.
- 4) Configuración de VLAN
- 5) Crear eurodiputado.
- 6) Crear ERPS y configurar VLAN de control e instancia de protección.
- 7) Ver el estado.

#### Ejemplo

Planifique la VLAN de protección y la VLAN de protocolo para que sean 2 y 3. Configure el puerto 2 del conmutador 1 para que sea el puerto propietario de RPL. Asegúrese de deshabilitar la función mutex de los puertos, incluida la función STP y la función LLDP.

Las configuraciones del switch son las siguientes:

**Paso 1** Configure la protección VLAN y el protocolo VLAN son 2 y 3 por separado. 1)

Seleccione Avanzado > Común > Configuración de VLAN.

El **Configuración de VLAN** se muestra la interfaz.

- 2) Configure el modo del puerto 1 y el puerto 2 para que sea **Trompa**. Consulte la Figura 3-30.
- 3) Configure el puerto VLAN del puerto 1 y el puerto 2 para que sea 1.
- 4) Configure la VLAN permitida en 2 y 3.

5) Haga clic **Ahorrar**.

Figura 3-30 Agregue el puerto 1 y el puerto 2 en la VLAN 1

**VLAN Settings**

VLANs  The allowable range is '1-4094'. Such as '2', '3,7' or '1-9'

Port	Mode	Port VLAN	Ingress Acceptance	Egress Tagging	Allowed VLANs
1	Access	1	Tagged and Untagged	Untag All	1
2	Access	2	Tagged and Untagged	Untag All	2
3	Access	3	Tagged and Untagged	Untag All	3
4	Access	4	Tagged and Untagged	Untag All	4
5	Access	5	Tagged and Untagged	Untag All	5
6	Access	1	Tagged and Untagged	Untag All	1
7	Access	1	Tagged and Untagged	Untag All	1

## Paso 2 Crear MEP1 y MEP 2

1) Seleccione Avanzado > Poco utilizado > ERPS > Configuración MEP. El

**Configuración de eurodiputado** se muestra la interfaz.

2) Haga clic **Agregar**.

**El Agregar** se muestra la interfaz.

3) Establezca Instancia en 1. Consulte la Figura 3-31.

4) Establezca el puerto de residencia en 1.

5) Establezca el nivel en 0.

6) Establezca el VID etiquetado en 3, es decir, el protocolo VLAN.

7) Haga clic **DE ACUERDO**.

Figura 3-31 Agregar MEP

**Add** [Close]

Instance: 1

Residence Port: 1

Level: 0

Tagged VID: 3

[OK] [Cancel]

Agregue MEP2 de la misma manera. Establezca Instancia en 2, Puerto de residencia en 2, Nivel en 0 y VID etiquetado en 3.

**Paso 3** Hacer clic **1y2** por separado bajo **Instancia** para entrar en la interfaz de configuración. Modifique la ID de MEP y agregue la ID de pares. Consulte la Figura 3-32 y la Figura 3-33.

Figura 3-32 Configure la ID de par del MEP 1

**MEP Configuration** [Close]

**Instance Data**

Instance	Domain	MEP Mode	Direction	Residence Port	This MAC	Oper State
1	Port	MEP	ingress	1	90-02-A9-DA-67-CD	<span style="color: red;">■</span>

**Instance Configuration**

Level: 0 | MEP ID: 1 | Tagged VID: 3

**Peer MEP Configuration** [Add]

<input type="checkbox"/>	Peer MEP ConfigId	Unicast Peer MAC	Delete
<input type="checkbox"/>	5	00:00:00:00:00:00	[Delete]

[OK] [Cancel]

Figura 3-33 Configure la ID de par de MEP 2

The screenshot displays the 'MEP Configuration' window with the following sections:

- Instance Data:** A table with columns: Instance, Domain, MEP Mode, Direction, Residence Port, This MAC, and Oper State. The row shows Instance 2, Domain Port, MEP Mode MEP, Direction ingress, Residence Port 2, This MAC 90-02-A9-DA-67-CE, and Oper State with a red square icon.
- Instance Configuration:** A form with three input fields: Level (set to 0), MEP ID (set to 1), and Tagged VID (set to 3).
- Peer MEP Configuration:** A table with columns: Peer MEP ConfigId, Unicast Peer MAC, and Delete. The first row has a checkbox, Peer MEP ConfigId 3, Unicast Peer MAC 00:00:00:00:00:00, and a Delete button. There are 'Add', 'Delete', 'OK', and 'Cancel' buttons.

**Etapa 4** Hacer clic **DE ACUERDO**.

**Paso 5** Crear ERP.

1) Seleccione Avanzado > Poco uso > ERPS > Configuración de ERPS. El

**Configuración de ERPS** se muestra la interfaz.

2) Haga clic **Agregar**.

El **Añadir nuevo ERPS** se muestra la interfaz.

3) Establezca el ID de ERPS en 1. Consulte la Figura 3-34.

4) Establezca el puerto 0 en 1 y el puerto 1 en 2.

5) Establezca Puerto 0 APS MEP en 1 y Puerto 1 APS MEP en 2.

6) Establezca Port 0 SF MEP en 1 y Port 1 SF MEP en 2.

7) Haga clic **DE ACUERDO**.

Figura 3-34 Agregar ERPS

### Add New ERPS ✕

---

ERPS ID

Port 0

Port 1

Port 0 APS MEP

Port 1 APS MEP

Port 0 SF MEP

Port 1 SF MEP

**Paso 6** Hacer clic **1** bajo **ERPSID** para entrar en la interfaz de configuración. Para la configuración de ERPS, consulte la Figura 3-35.

Figura 3-35 Configuración de ERPS

### ERPS Configuration ✕

---

**Instance Data**

ERPSID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type
1	1	2	1	2	1	2	Major Ring

**Instance Configuration**

Configured	Guard Time(Ms)	WTR Time	Hold Off Time(Ms)	Version	Revertive	VLANconfig
●	500	1min	0	v2	<input checked="" type="checkbox"/>	<input style="background-color: #00aaff; color: white; padding: 2px 5px; border: none;" type="button" value="VLANconfig"/>

**RPL Configuration**

RPL Role	RPL Port	RPLClear
None	None	<input type="checkbox"/>

**Instance Command**

Command	CommandPort
None	None

**Instance State**

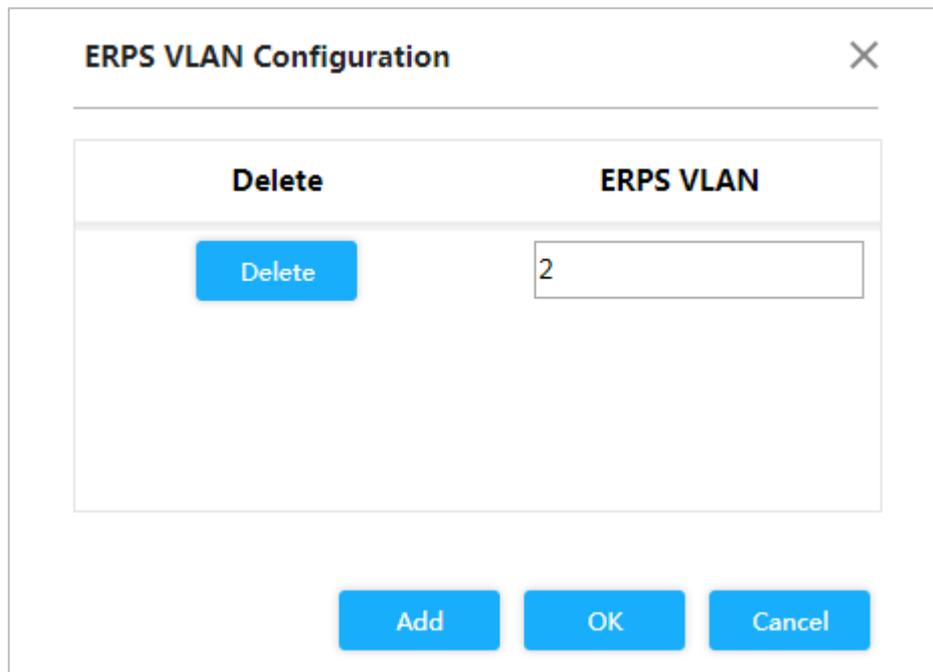
Protection State	State Port0	State Port1	Transmit APS	Port0 ReceiveAPS	Port1 Receive APS	WTR Remaining	RPL Unblocked	No APS Received	Port0 BlockStatus	Port1 BlockStatus	FOP Alarm
Protected	OK	SF	2	0	0	0	●	●	Blocked	Unblocked	●

1) Haga clic en Configuración de VLAN.

El **Configuración de VLAN de ERPS** se muestra la interfaz.

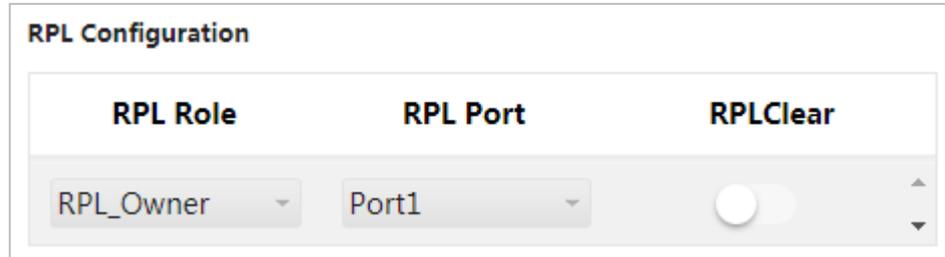
- 2) Haga clic **Agregar**.
- 3) Configure la VLAN de ERPS en 2. Consulte la Figura 3-36.
- 4) Haga clic **DE ACUERDO**.

Figura 3-36 Configuración de VLAN de ERPS



- 5) Configure el puerto 2 del conmutador 1 para que sea propietario de RPL en la configuración de RPL. Consulte la Figura 3-37.

Figura 3-37 Configuración del puerto propietario



**Paso 7** Hacer clic DE ACUERDO.

**Paso 8** Configure el interruptor 2 y el interruptor 3 de la misma manera.

**Paso 9** Ver el estado en **Estado de instancia** sobre el **Configuración de ERP** interfaz.

Figura 3-38 Estado de la instancia

Instance State											
Protection State	State Port0	State Port1	Transmit APS	Port0 Receive	Port1 Receive	WTR APS Remaining	RPL Unblocked	No APS Received	Port0 BlockStatus	Port1 BlockStatus	FOP Alarm
Pending	OK	SF	2	0	0	48680	●	●	Unblocked	Blocked	●

### 3.2.2 LCA

ACL (Lista de control de acceso) es para la identificación de flujo. Para filtrar el paquete, el dispositivo de red necesita configurar una serie de condiciones coincidentes para clasificar los paquetes. Las condiciones pueden ser la dirección de origen, la dirección de destino y el número de puerto del paquete.

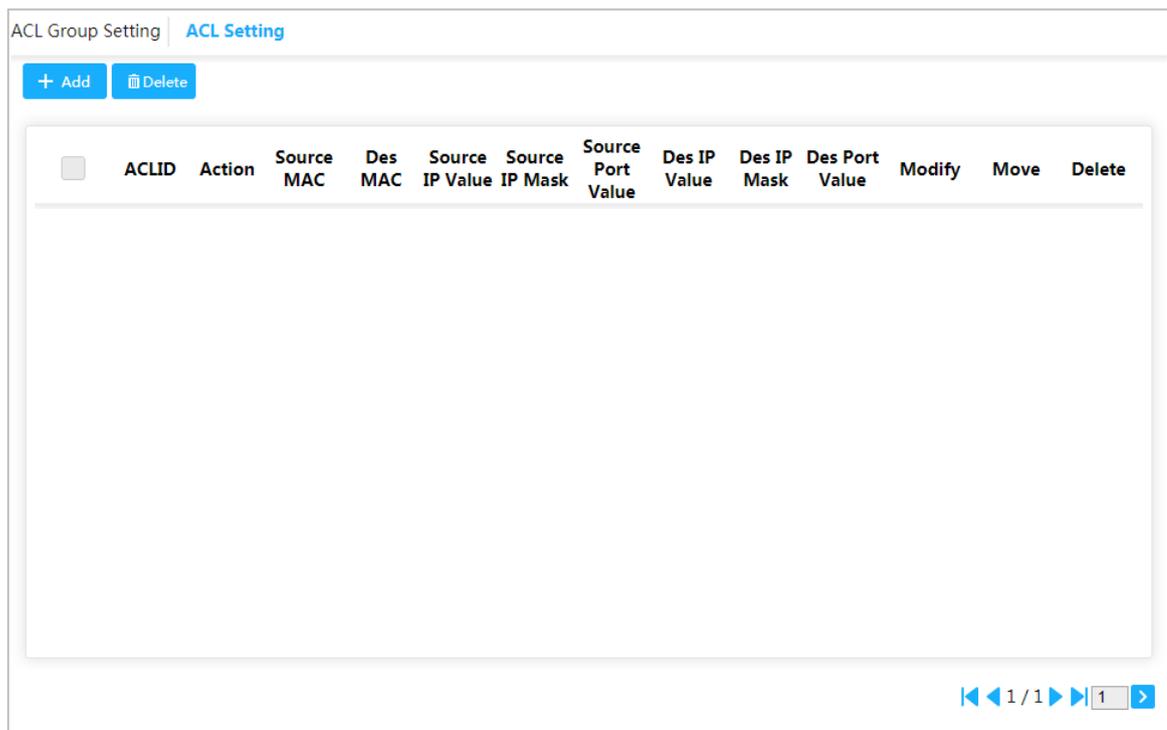
Cuando el puerto del dispositivo recibe el paquete, puede analizar el campo del paquete de acuerdo con la regla ACL del puerto actual. Y después de identificar el paquete específico, se permite o prohíbe el paso del paquete de acuerdo con la regla preestablecida.

### 3.2.2.1 Configuración de ACL

**Paso 1** Seleccione Avanzado > Usado raramente > ACL > Configuración de ACL. El

**Configuración de ACL** muestra la interfaz. Consulte la Figura 3-39.

Figura 3-39 Configuración de ACL



**Paso 2** Hacer clic **Agregar**.

El **Agregarse** muestra la interfaz. Consulte la Figura 3-40.

Figura 3-40 Agregar

**Add** [Close]

Mode: MAC ACL

ACL ID: [Text Input]

Action: Permit

Source MAC: any

Source MAC Address: [Text Input]  
such as 00:23:AE:77:10:53

Des MAC: any

Destination MAC Address: [Text Input]

[OK] [Cancel]

**Paso 3** Establezca el ID de ACL y el rango es de 1 a 128. Hacer clic **DE**

**Etapa 4** **ACUERDO.**

### 3.2.2.2 Configuración del grupo ACL

**Paso 1** Seleccione Avanzado > Usado raramente > ACL > Configuración de grupo de ACL. El

**Configuración del grupo ACL** se muestra la interfaz. Consulte la Figura 3-41.

Figura 3-41 Configuración del grupo ACL

ACL Group Setting | ACL Setting

Port	ACLID
1	[Text Input]
2	[Text Input]
3	[Text Input]
4	[Text Input]
5	[Text Input]
6	[Text Input]
7	[Text Input]

[Save] [Refresh]

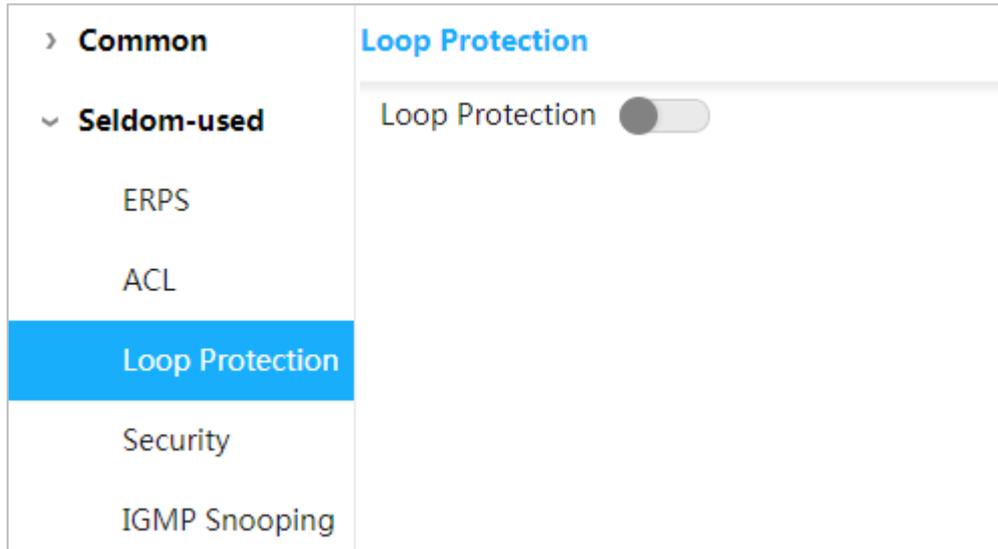
**Paso 2** Ingrese la identificación de ACL. Asegúrese de que la ID de ACL se haya agregado durante la configuración de ACL. Hacer clic

**Paso 3** **Ahorrar.**

### 3.2.3 Protección de bucle

Detectar el bucle entre los puertos. Después de que el dispositivo haya detectado el bucle, romperá el bucle. Paso 1 Seleccione Avanzado > Usado raramente > Protección de bucle. El **Protección de bucle** se muestra la interfaz. Consulte la Figura 3-42.

Figura 3-42 Protección de bucle



Paso 2 Hacer clic  para habilitar la protección de bucle

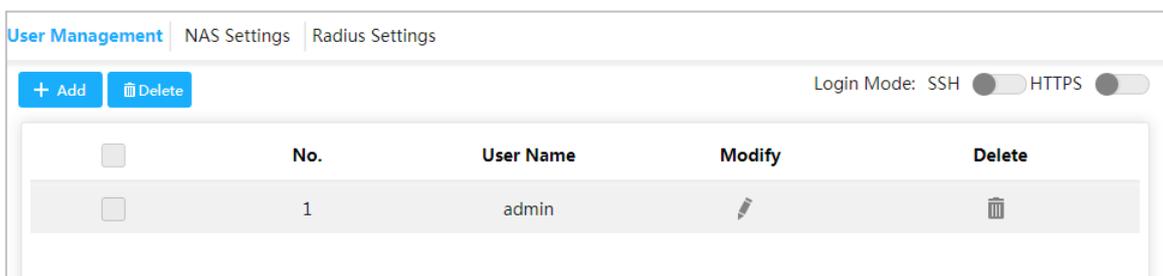
### 3.2.4 Seguridad

#### 3.2.4.1 Gestión de usuarios

Puede agregar, editar y eliminar el usuario.

Seleccionar **Avanzado > Poco utilizado > Seguridad > Gestión de usuarios**. Y el **Gestión de usuarios** se muestra la interfaz. Consulte la Figura 3-43.

Figura 3-43 Gestión de usuarios

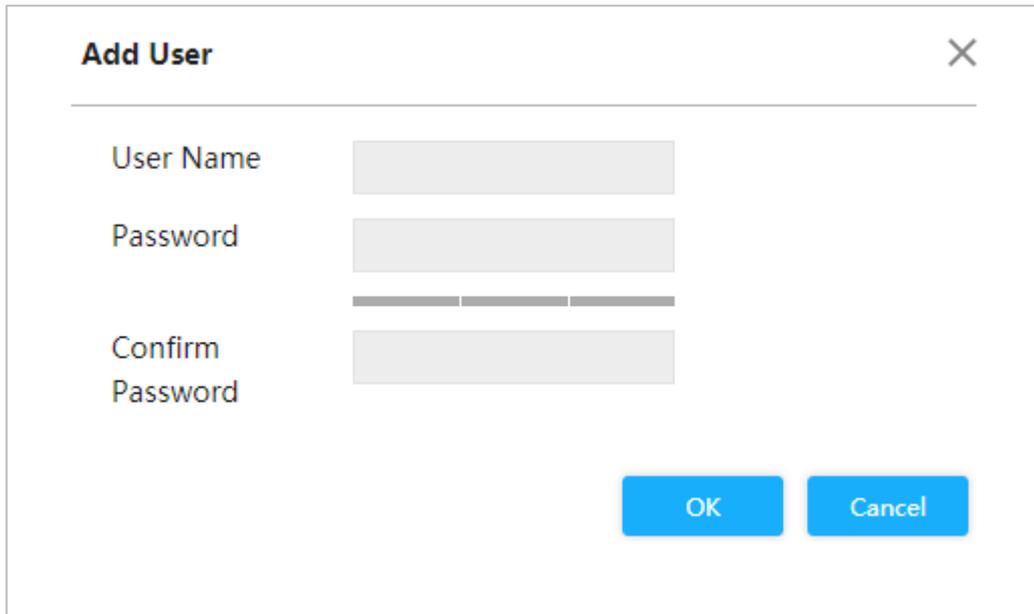


Agregar usuario

Paso 1 Hacer clic **Agregar**.

El **Agregar usuario** se muestra la interfaz. Consulte la Figura 3-44.

Figura 3-44 Agregar usuario



The image shows a dialog box titled "Add User" with a close button (X) in the top right corner. It contains three input fields: "User Name", "Password", and "Confirm Password". The "Password" field has a strength indicator below it. At the bottom right, there are two buttons: "OK" and "Cancel".

**Paso 2** Introduzca el nombre de usuario, la contraseña y confirme la contraseña. La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; &). Por ejemplo, agregue la prueba de usuario nuevo 01 .

**Paso 3** Hacer clic **Ahorrar**.

Se agrega la nueva prueba de usuario 01. Consulte la Figura 3-45.

Figura 3-45 Nuevo usuario agregado



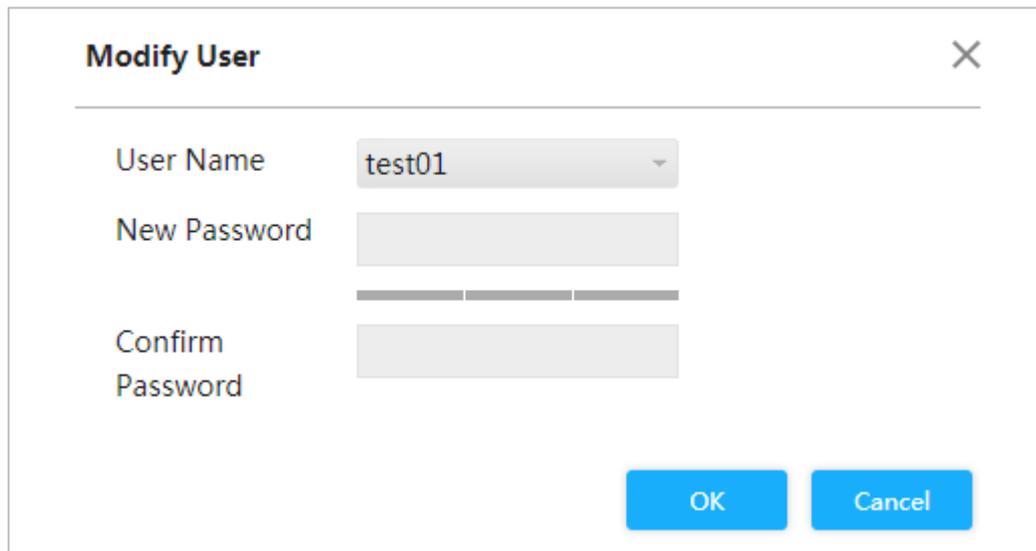
The image shows a "User Management" interface with tabs for "User Management", "NAS Settings", and "Radius Settings". It includes "+ Add" and "Delete" buttons, and a "Login Mode" section with "SSH" and "HTTPS" toggle switches. Below is a table of users:

<input type="checkbox"/>	No.	User Name	Modify	Delete
<input type="checkbox"/>	1	admin		
<input type="checkbox"/>	2	test01		

## Modificar y Eliminar Usuario

- Hacer clic  , y el **Modificar usuario** se muestra la interfaz. Consulte la Figura 3-46.

Figura 3-46 Modificar usuario



- Hacer clic  para eliminar el usuario.



No puede eliminar el usuario administrador.

## SSH

Puede habilitar o deshabilitar la función SSH.

Hacer clic  correspondiente a SSH en la esquina superior derecha de la **Gestión de usuarios** interfaz.

## HTTPS

HTTPS (Protocolo de transferencia de hipertexto sobre capa de conexión segura) es el canal HTTP para el objetivo de seguridad. La capa SSL y la capa TLS se agregan a HTTP. SSL y TLS son la base de seguridad de HTTP, por lo que se solicita SSL/TLS para el cifrado. HTTPS es el esquema URI, y la sintaxis es similar a HTTP, y se utiliza para la transmisión de datos HTTP de seguridad. Construido en la web Netscape Navigator, proporciona comunicación de autenticación y encriptación. Se aplica ampliamente en la red mundial para comunicaciones sensibles a la seguridad. Por ejemplo, proteger la seguridad de la cuenta y la información del usuario.

Hacer clic  correspondiente a HTTPS en la esquina superior derecha de la **Gestión de usuarios** interfaz para habilitar el servicio HTTPS.

### 3.2.4.2 Configuración del NAS

NAS (Servidor de acceso a la red) es un servidor que permite que el ISP proporcione un servicio de acceso a Internet.

Paso 1 Seleccione Avanzado > Poco uso > Seguridad > Configuración de NAS. El

**Configuración de NAS** se muestra la interfaz. Consulte la Figura 3-47.

Figura 3-47 Configuración de NAS

User Management | **NAS Settings** | Radius Settings

Mode

Reauthentication  Enabled

Port	Admin State	Port State
1	<input type="text" value="Force Authorized"/>	Globally Disabled
2	<input type="text" value="Force Authorized"/>	Globally Disabled
3	<input type="text" value="Force Authorized"/>	Globally Disabled
4	<input type="text" value="Force Authorized"/>	Globally Disabled
5	<input type="text" value="Force Authorized"/>	Globally Disabled
6	<input type="text" value="Force Authorized"/>	Globally Disabled
7	<input type="text" value="Force Authorized"/>	Globally Disabled

**Paso 2** Seleccionar **Activado** en el **Modo** área para habilitar la función de duplicación. Selecciona

**Paso 3** el **Reautenticación habilitada** caja para permitir la reautenticación.

**Etapas 4** Establecer estado de administrador: Forzar autorizado, Forzar no autorizado, basado en puerto 802.1X o

Autenticación basada en MAC.

**Paso 5** Hacer clic **Ahorrar**.

### 3.2.4.3 Configuración de radio

RADIUS (Servicio de Usuario de Acceso Telefónico de Autenticación Remota) es un protocolo común para realizar AAA (Autenticación, Autorización y Contabilidad).

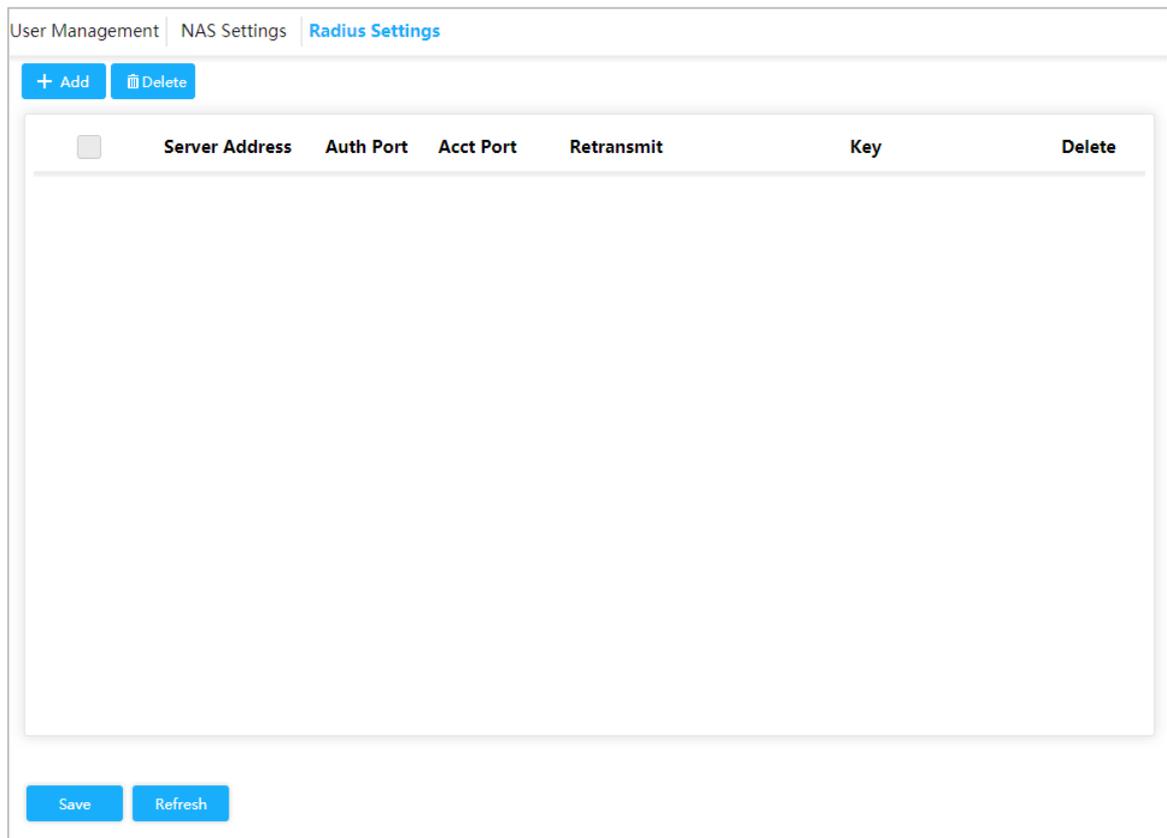
RADIUS es un protocolo de interacción de información de construcción distribuida y C/S. Puede proteger la red de visitas no autorizadas. Se utiliza en la red que permite visitas remotas pero solicita la mayor seguridad. Define el formato del paquete RADIUS y el mecanismo de transmisión del mensaje. Estipula que el uso de UDP como protocolo de capa de transporte para encapsular el paquete RADIUS.

Al principio, RADIUS es el protocolo AAA solo para usuarios de acceso telefónico. Con el desarrollo de los accesos de usuario, RADIUS se adapta a varios accesos, incluidos el acceso Ethernet y el acceso ADSL. Accede al servidor a través de la autenticación y la autorización, y recopila registros del uso de la fuente de la red a través de la contabilidad.

**Paso 1** Seleccione Avanzado > Usado raramente > Seguridad > Configuración de radio. El

**Configuración de radio** se muestra la interfaz. Consulte la Figura 3-48.

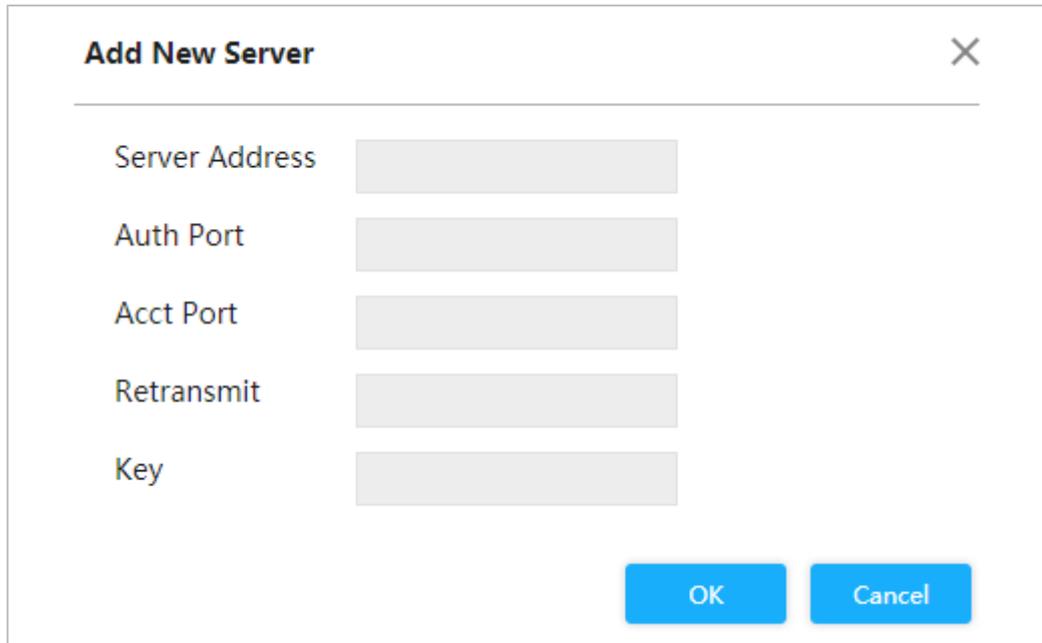
Figura 3-48 Configuración de radio



**Paso 2** Hacer clic **Agregar**.

El **Agregar nuevo servidor** se muestra la interfaz. Consulte la Figura 3-49.

Figura 3-49 Agregar nuevo servidor



The image shows a dialog box titled "Add New Server" with a close button (X) in the top right corner. The dialog contains five input fields, each with a label to its left: "Server Address", "Auth Port", "Acct Port", "Retransmit", and "Key". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

**Paso 3** Configure la dirección del servidor, el puerto de autenticación, el puerto de cuenta, la retransmisión y la clave. Hacer clic **DE**

**Etapa 4** **ACUERDO.**

### 3.2.5 Indagación IGMP

IGMP Snooping (Internet Group Management Protocol Snooping) es el mecanismo de restricción de multidifusión que se ejecuta en el dispositivo de la capa 2, para administrar y controlar la multidifusión. Mediante el análisis del paquete IGMP recibido, el dispositivo de la capa 2, que ejecuta IGMP Snooping, crea la asignación entre el puerto y la dirección de multidifusión MAC, y reenvía los datos de multidifusión de acuerdo con la asignación.

**Paso 1** Seleccione Avanzado > Usado raramente > IGMP Snooping. El

**Indagación IGMP** se muestra la interfaz. Consulte la Figura 3-50.

Figura 3-50 Indagación de IGMP

**IGMP Snooping**

IGMP Snooping  Disable  Enable

Discarding Unknown IGMP Packets  Disable  Enable

<input type="checkbox"/>	VLAN ID	Querier Election	Querier Address	Delete
--------------------------	---------	------------------	-----------------	--------

**Paso 2** Seleccionar **Permitir** en el **Indagación IGMP** área para habilitar la función. Seleccione

**Paso 3** Deshabilitar o Habilitar en el área Descartar paquetes IGMP desconocidos. Hacer clic

**Etapa 4** **Agregar**.

El **Agregar VLAN** se muestra la interfaz. Consulte la Figura 3-51.

Figura 3-51 Agregar VLAN

**Add VLAN** ✕

---

VLAN ID

Querier Election

Querier Address

**Paso 5** Establezca la ID de VLAN y la dirección del solicitante, y seleccione el **Elección del interrogador** casilla para habilitar el buscador

**Paso 6** Hacer clic **DE ACUERDO**.

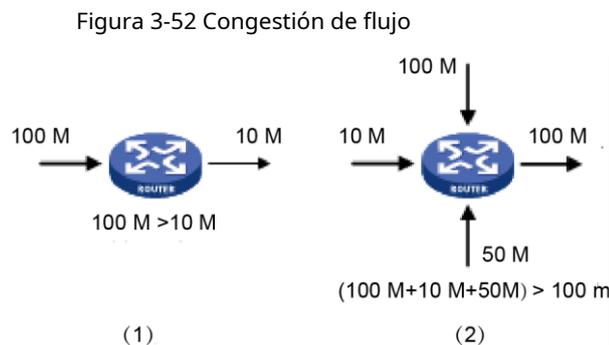
### 3.2.6 Calidad del servicio

QoS (Calidad de servicio) se utiliza para evaluar la capacidad de que el servidor cumpla con las demandas de servicio del cliente. En Internet, lo que QoS evalúa es la capacidad del servicio de reenvío de red y paquetes.

QoS puede evaluar desde los diferentes aspectos de acuerdo con los diversos servicios proporcionados por la red. QoS evalúa el ancho de banda, la demora, el tramado y la pérdida de paquetes durante el paquete y el reenvío.

## Congestión

La congestión es común en un entorno de conmutación de paquetes de Internet complejo. Vea el siguiente ejemplo:



- 1) El paquete entra al dispositivo por el enlace de alta velocidad y sale por el enlace de baja velocidad.
- 2) El paquete ingresa al dispositivo desde múltiples puertos y sale de un puerto (la tasa de velocidad de múltiples puertos es mayor que la del puerto de salida).

Si el flujo llega a una velocidad lineal, se encontrará con el punto de inmovilización del recurso y luego se generará la congestión.

Además del ancho de banda de agresión, cualquier otra escasez de recursos (como la escasez de tiempo de procesamiento distributivo, búfer y recursos de memoria) causará congestión. Adicionalmente, el mal control del flujo que llega en un tiempo determinado, lo que lleva a que el flujo exceda el recurso de la red distributiva, también es un factor generador de congestión.

### 3.2.6.1 Puerto

Mediante la configuración de CoS, se puede decidir la prioridad para el paso de paquetes por el puerto de salida del conmutador. Si la congestión se produce en el puerto de salida, el conmutador otorgará un valor de CoS al paquete después de que pase por el puerto de entrada. Cuanto mayor sea el valor de CoS, mayor será la prioridad.

**Paso 1** Seleccione Avanzado > Poco utilizado > QoS > Clasificación de puertos. El

**Clasificación de puertos** se muestra la interfaz. Consulte la Figura 3-53.

Figura 3-53 Clasificación de puertos

**Port Classification** | Port Schedulers | Port Shapers | DSCP-Based | Storm Policer

Port	CoS	<input type="checkbox"/> DSCP
1	0	<input type="checkbox"/>
2	0	<input type="checkbox"/>
3	0	<input type="checkbox"/>
4	0	<input type="checkbox"/>
5	0	<input type="checkbox"/>
6	0	<input type="checkbox"/>
7	0	<input type="checkbox"/>

**Paso 2** Establecer CoS. Por ejemplo: Configure el puerto 1 como 1 y el puerto 2 como 2. Consulte la Figura 3-54. El puerto 1 y el puerto 2 son puertos de entrada y el puerto 3 es el puerto de salida. El valor CoS del puerto 2 es mayor que el del puerto 1, por lo que los datos del puerto 2 pasarán primero por el puerto 3.

Figura 3-54 Establecer CoS

Port	CoS	<input type="checkbox"/> DSCP
1	1	<input type="checkbox"/>
2	2	<input type="checkbox"/>
3	0	<input type="checkbox"/>
4	0	<input type="checkbox"/>
5	0	<input type="checkbox"/>
6	0	<input type="checkbox"/>
7	0	<input type="checkbox"/>

Save

Paso 3 Hacer clic **Ahorrar**.

### 3.2.6.2 Programadores de puertos

Los dos modos de programadores de puertos:

- **prioridad estricta**. Cuando se produce una congestión, la prioridad de los paquetes que pasan por el puerto de salida del conmutador depende del valor de CoS en **Clasificación de puertos**.
- **2-8 colas ponderadas**. Cuando se produce una congestión, la prioridad de los paquetes que pasan por el puerto de salida del conmutador depende de la proporción de la tasa total.

Paso 1 Seleccione Avanzado > Poco utilizado > QoS > Programadores de puertos. El

**Programadores de puertos** se muestra la interfaz. Consulte la Figura 3-55.

Figura 3-55 Programadores de puertos

Port Classification	Port Schedulers	Port Shapers	DSCP-Based	Storm Policer					
Port	Mode	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-

**Paso 2** Haga clic en el puerto, como el puerto 1.

El **Programadores y modeladores de puerto de salida de QoS Puerto 1** se muestra la interfaz. Consulte la Figura 3-56. El CoS de Q0 es 0, y así sucesivamente.

Figura 3-56 Configuración de puertos

**QoS Egress Port Scheduler and Shapers Port 1** ✕

---

Scheduler Mode Strict Priority

QPort	Ingress Queue Shaper				Queue Scheduler	
	<input type="checkbox"/> Enable	Rate	Unit	Rate-type	Weight	Percent
Q0	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>		
Q1	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>		
Q2	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>		
Q3	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>		
Q4	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>		
Q5	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>		
Q6	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>		
Q7	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>		

**Egress Queue Shaper**

<input type="checkbox"/> <b>Enable</b>	<b>Rate</b>	<b>Unit</b>	<b>Rate-type</b>
<input type="checkbox"/>	<input style="width: 50px;" type="text" value="500"/>	<span>kbps</span>	<span>Line</span>

OK
Cancel

**Paso 3** Seleccionar modo.

- **prioridad estricta.** La prioridad para el paso de paquetes por el puerto de salida del switch depende del valor de CoS en **Clasificación de puertos**.
- **2-8 colas ponderadas.** Cuando se produce una congestión, la prioridad de los paquetes que pasan por el puerto de salida del conmutador depende de la proporción de la tasa total.

Por ejemplo, seleccione **Modo de programador** como **2 colas ponderadas**. El límite de velocidad máxima del puerto 1 y el puerto 2 es de 500 kbps. Cuando se produce una congestión, el 50 % del paquete del puerto de entrada pasará por el puerto de salida. Consulte lo siguiente para la configuración:

- 1) Seleccione **Modo de programador** como **2 colas ponderadas**. Consulte la Figura 3-57.
- 2) en **Moldeador de cola de entrada**, selecciona el **Tasa** de **Q0** y **Q1** ser de 500 kbps, y **Tipo de cambio** ser Línea.
- 3) en **Moldeador de cola de salida**, selecciona el **Tasa** ser de 500 kbps, y **Tipo de cambio** ser Línea. Cuando se produce una congestión y la velocidad de los dos puertos es de 400 kbps, la velocidad que pasa por el puerto de salida es de 250 kbps.

Figura 3-57 Programadores de puertos

**QoS Egress Port Scheduler and Shapers Port 1**
✕

Scheduler Mode 2 Queues Weighted

Ingress Queue Shaper					Queue Scheduler	
QPort	<input type="checkbox"/> Enable	Rate	Unit	Rate-type	Weight	Percent
Q0	<input checked="" type="checkbox"/>	500	kbps	Line	50	50%
Q1	<input checked="" type="checkbox"/>	500	kbps	Line	50	50%
Q2	<input type="checkbox"/>	500	kbps	Line		
Q3	<input type="checkbox"/>	500	kbps	Line		
Q4	<input type="checkbox"/>	500	kbps	Line		
Q5	<input type="checkbox"/>	500	kbps	Line		
Q6	<input type="checkbox"/>	500	kbps	Line		
Q7	<input type="checkbox"/>	500	kbps	Line		

**Egress Queue Shaper**

<input checked="" type="checkbox"/> Enable	Rate	Unit	Rate-type
<input checked="" type="checkbox"/>	500	kbps	Line

OK
Cancel

**Etapa 4** Hacer clic **DE ACUERDO**.

### 3.2.6.3 Modeladores de puertos

La configuración es la misma para programadores de puertos y modeladores de puertos. La única diferencia es que la interfaz de programadores de puertos muestra el valor de peso y la interfaz de modeladores de puertos muestra la tasa de velocidad.

Seleccionar **Avanzado** > **Poco utilizado** > **QoS** > **Modeladores de puertos**. El **Modeladores de puertos** se muestra la interfaz. Consulte la Figura 3-58.

Figura 3-58 Moldeadores de puertos

Port	Q0(kbps)	Q1(kbps)	Q2(kbps)	Q3(kbps)	Q4(kbps)	Q5(kbps)	Q6(kbps)	Q7(kbps)	Port Speed(kbps)
1	500	500							500
2									
3									
4									
5									
6									
7									

### 3.2.6.4 Basado en DSCP

Asegúrese de haber habilitado DSCP antes de configurar la función DSCP.

**Paso 1** Seleccionar **Avanzado > Poco utilizado > QoS > Clasificación de puertos**.

El **Clasificación de puertos** se muestra la interfaz.

**Paso 2** Habilite DSCP en el puerto DSCP. Suponga que el puerto 3 es el puerto de salida, vea la Figura 3-59.

Figura 3-59 Clasificación de puertos

Port Classification | Port Schedulers | Port Shapers | DSCP-Based | Storm Policer

Port	CoS	<input type="checkbox"/> DSCP
1	0	<input type="checkbox"/>
2	0	<input type="checkbox"/>
3	0	<input checked="" type="checkbox"/>
4	0	<input type="checkbox"/>
5	0	<input type="checkbox"/>
6	0	<input type="checkbox"/>
7	0	<input type="checkbox"/>

Save

**Paso 3** Hacer clic **Ahorrar**.

**Etapas 4** Seleccionar **Avanzado > Poco utilizado > QoS > Basado en DSCP**

. El **Basado en DSCP** se muestra la interfaz.

**Paso 5** Al configurar DSCP en 4 y 8, CoS es 2 y DPL son 2 y 1.

1) Cuando DSCP son 4 y 8, seleccione **Confianza** para habilitar la función. Consulte la Figura 3-60.

2) Al configurar DSCP en 4, CoS es 2 y DPL es 2.

3) Al configurar DSCP en 8, CoS es 2 y DPL es 1.

Cuanto mayor sea el CoS de DSCP, mayor será la prioridad. El paquete de puerto correspondiente pasará primero por el puerto de salida.

Figura 3-60 Basado en DSCP

Port Classification | Port Schedulers | Port Shapers | **DSCP-Based** | Storm Policer

DSCP	<input type="checkbox"/> Trust	CoS
0	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0
4	<input checked="" type="checkbox"/>	2
5	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0
7	<input type="checkbox"/>	0
8	<input checked="" type="checkbox"/>	1
9	<input type="checkbox"/>	0

Save

Paso 6 Hacer clic **Ahorrar**.

### 3.2.6.5 Policía de tormentas

Inhibir los tres paquetes, incluyendo unidifusión, multidifusión y difusión. Paso

- 1 Seleccionar **Avanzado > Poco utilizado > QoS > Storm Policer**. El **Policía de tormentas** se muestra la interfaz. Consulte la Figura 3-61.

Figura 3-61 Policia de tormentas

Port Classification | Port Schedulers | Port Shapers | DSCP-Based | **Storm Policer**

Frame Type	<input type="checkbox"/> Enable	Rate	Unit
Unicast	<input type="checkbox"/>	1	fps
Multicast	<input type="checkbox"/>	1	fps
Broadcast	<input type="checkbox"/>	1	fps

[Save](#)

**Paso 2** El puerto puede recibir la tasa de hasta 1024 fps. Consulte la Figura 3-62.

- En **unidifusión**, Selecciona el **Permitire** ingrese 1024 en **Tasa**. Significa que el puerto puede recibir la tasa de hasta 1024 fps de paquete de unidifusión.
- En **multidifusión**, Selecciona el **Permitire** ingrese 1024 en **Tasa**. Significa que el puerto puede recibir la tasa de hasta 1024 fps de paquete de multidifusión.
- En **Transmisión**, Selecciona el **Permitire** ingrese 1024 en **Tasa**. Significa que el puerto puede recibir una tasa de hasta 1024 fps de paquete de transmisión.

Figura 3-62 Configuración de Storm Policer

Port Classification | Port Schedulers | Port Shapers | DSCP-Based | **Storm Policer**

Frame Type	<input checked="" type="checkbox"/> Enable	Rate	Unit
Unicast	<input checked="" type="checkbox"/>	1024	fps
Multicast	<input checked="" type="checkbox"/>	1024	fps
Broadcast	<input checked="" type="checkbox"/>	1024	fps

[Save](#)

**Paso 3** Hacer clic **Ahorrar**.

## 3.2.7 SNMP

SNMP (Protocolo simple de administración de redes) es el protocolo estándar para la administración de redes en Internet, y se aplica ampliamente para que los dispositivos de administración accedan y administren los dispositivos administrados. SNMP tiene las siguientes características:

- Es compatible con la gestión inteligente para dispositivos de red. Mediante el uso de la plataforma de administración de red basada en SNMP, el administrador de red puede consultar el estado de ejecución y los parámetros del dispositivo de red, y puede configurar el parámetro, encontrar el error, realizar un diagnóstico de fallas y luego planificar la capacidad y crear el informe.
- SNMP admite la gestión de dispositivos de diferentes características físicas. SNMP proporciona solo la biblioteca de funciones más básica. Hace que la tarea de administración y la característica física y la tecnología de red del dispositivo administrado sean independientes, para administrar los dispositivos de diferentes fabricantes.

La red SNMP proporciona dos elementos, NMS y Agente.

- NMS (Sistema de administración de red) es el administrador de la red SNMP y proporciona una interfaz hombre-máquina amigable para ayudar al administrador de la red a terminar la mayor parte del trabajo de administración de la red.
- El agente es el rol administrado en la red SNMP y recibe y maneja el paquete de solicitud de NMS. En algunas circunstancias de emergencia, por ejemplo, si cambia el estado del puerto, el agente puede enviar un paquete de alarma a NMS de manera proactiva.

### 3.2.7.1 Activación de la función SNMP

Paso 1 Seleccione Avanzado > Poco utilizado > SNMP. El **SNMP** se muestra la interfaz. Consulte la Figura 3-63.

Figura 3-63 SNMP

SNMP

SNMP

SNMP Version  SNMP v1  SNMP v2  SNMP v3

Read-only Community

Read&write Community

Trap Address

Trap Port

Paso 2 Hacer clic



en **SNMP** para habilitar SNMP.



Cada agente SNMP v3 tiene una ID de motor como identificador único.

### 3.2.7.2 Configuración de SNMP v1/v2

Ejemplo: Configurar SNMP v1. La configuración de SNMP v2 es la misma que la de SNMP v1. Paso

1 Seleccione SNMP v1 en **Versión SNMP**.

Paso 2 Configure la comunidad de solo lectura, la comunidad de lectura y escritura, la dirección de captura y el puerto de captura. Hacer

Paso 3 clic **Ahorrar**.

### 3.2.7.3 Configuración de SNMP v3

Paso 1 Seleccione SNMP v3 en **Versión SNMP**. Consulte la Figura 3-64.

Figura 3-64 SNMP v3

### SNMP

SNMP

SNMP Version  SNMP v1  SNMP v2  SNMP v3

---

Read-only Community

Read&write Community

Trap Address

Trap Port

Trap Name

---

Read-only Username

Authentication Type  MD5  SHA

Authentication Password

Encryption Type  DES  AES

Encryption Password

---

Read&write Username

Authentication Type  MD5  SHA

Authentication Password

Encryption Type  DES  AES

Encryption Password

**Paso 2** Configure la dirección de captura, el puerto de captura y el nombre de captura.

**Paso 3** Configure el nombre de usuario de solo lectura, el tipo de autenticación, la contraseña de autenticación, el tipo de cifrado y la contraseña de cifrado.

**Etapa 4** Configure el nombre de usuario de lectura y escritura, el tipo de autenticación, la contraseña de autenticación, el tipo de cifrado y la contraseña de cifrado.

**Paso 5** Hacer clic **Ahorrar**.

## 3.2.8 Servidor DHCP

El servidor DHCP es el servidor para administrar el estándar DHCP en la red específica. El servidor DHCP es asignar la dirección IP para la estación de trabajo y asegurarse de que la dirección IP para cada estación de trabajo sea diferente. El servidor DHCP simplifica la tarea de administración de la red que antes debería hacerse manualmente.

En general, en las siguientes escenas, se adopta el servidor DHCP para asignar la dirección IP.

- La escala de la red es grande. La carga de trabajo es demasiado pesada si se configura manualmente y la administración centralizada de la red será difícil.
- La cantidad de PC es mayor que la cantidad de direcciones IP en la red y es imposible asignar una dirección IP estática para cada PC. Por ejemplo, la cantidad de usuarios que pueden acceder a la red al mismo tiempo está limitada por el ISP y el usuario necesita adquirir la dirección IP de forma dinámica.
- Solo una pequeña cantidad de PC necesita la dirección IP estática, y la mayoría de las PC no necesitan la dirección IP estática.

Hay tres partes de la configuración del servidor DHCP: **Modo VLAN, IP excluidas y Piscina**. **Paso 1** Seleccionar **Avanzado > Poco utilizado > DHCP > Servidor DHCP**. El **servidor DHCP** se muestra la interfaz. Consulte la Figura 3-65.

Figura 3-65 Servidor DHCP

The screenshot displays the DHCP Server configuration interface. At the top, there is a 'Global Mode' toggle switch which is turned on. Below this, there are two main sections: 'VLAN Mode' and 'Excluded IP'. Each section has '+ Add' and 'Delete' buttons. Under 'VLAN Mode', there is a table with columns for 'Vlan Range' and 'Delete'. Under 'Excluded IP', there is a table with columns for 'Excluded IP' and 'Delete'. At the bottom, there is a 'Pool' section with '+ Add' and 'Delete' buttons, followed by a table with columns: 'Name', 'Type', 'IP', 'Subnet mask', 'Default Gateway', 'Lease Time', and 'Delete'. All tables are currently empty.

**Paso 2**

Hacer clic



en **Modo global**, para habilitar la función del servidor DHCP.

**Paso 3**

Configurar el modo DHCP.



Agregue primero la interfaz VLAN. Consulte "3.1.1.2 IP y ruta".

1) Haga clic en Agregar en modo VLAN.

El **Agregar modo VLAN** se muestra la interfaz. Consulte la Figura 3-66.

Figura 3-66 Agregar modo VLAN

**Add VLAN Mode** [Close]

Vlan Range [ ] - [ ]

[OK] [Cancel]

2) Ingrese el rango de VLAN, como 2-4.

3) Haga clic **DE ACUERDO**.

**Etapa 4**

Configurar segmento de red de IP excluida.



La IP excluida se refiere a la IP reservada para el servidor, que no se asignará al cliente.

1) Haga clic en Agregar en IP excluida.

El **Añadir IP Excluidase** muestra la interfaz. Consulte la Figura 3-67.

Figura 3-67 Agregar IP excluida

**Add Excluded IP** [Close]

Excluded IP [ ] - [ ]

[OK] [Cancel]

2) Ingrese el rango de direcciones IP, como 192.168.100.2-192.168.100.50.

3) Haga clic **DE ACUERDO**.

**Paso 5**

Agregar grupo de direcciones DHCP.

1) Haga clic **AgregarenPiscina**.

El **Agregar grupo** se muestra la interfaz. Consulte la Figura 3-68.

Figura 3-68 Agregar grupo

The image shows a dialog box titled "Add Pool" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Pool Name:** A text input field.
- Type:** A dropdown menu currently showing "Network".
- IP:** A text input field.
- Subnet Mask:** A text input field.
- Lease Time:** Three input fields for "1" days, "0" hours, and "0" minutes.
- Default Router:** A text input field.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

2) Para los parámetros, consulte la Tabla 3-7.

Tabla 3-7 Parámetros de piscina

Parámetro	Descripción
Nombre del grupo	Nombre del grupo de direcciones DHCP, como vlan2_test.
Tipo	Dos tipos: <b>RedyAnfitrión.</b> - Red: El segmento de red de una IP. - Anfitrión: una IP específica
IP	La dirección IP del host o la red.
Máscara de subred	La máscara de subred del host o la red.
Tiempo de arrendamiento	Introduzca el tiempo de concesión del grupo de direcciones.
Puerta	Configure la puerta de enlace predeterminada del grupo de direcciones.

3) Haga clic **DE ACUERDO**.

### 3.2.9 LLDP

LLDP (Protocolo de descubrimiento de capa de enlace) es una forma de descubrimiento de capa de enlace estándar. Puede formar sus capacidades principales, dirección de administración, número de dispositivo y número de puerto como TLV (valor de longitud de tipo), encapsularlo en LLDPDU (unidad de datos de protocolo de descubrimiento de capa de enlace) y liberarlo a su vecino. El vecino mantendrá la información recibida en forma de MIB estándar (Base de información de administración), de modo que la administración de la red pueda consultar y juzgar el estado de comunicación del enlace.

### LLDP

**Paso 1** Seleccionar **Avanzado > Poco utilizado > LLDP**. El LLDP se muestra la interfaz. Consulte la Figura 3-69.

Figura 3-69 LLDP

Interface	Mode
1	Enable
2	Enable
3	Enable
4	Enable
5	Enable
6	Enable
7	Enable

Save

**Paso 2** Configure el modo LLDP.

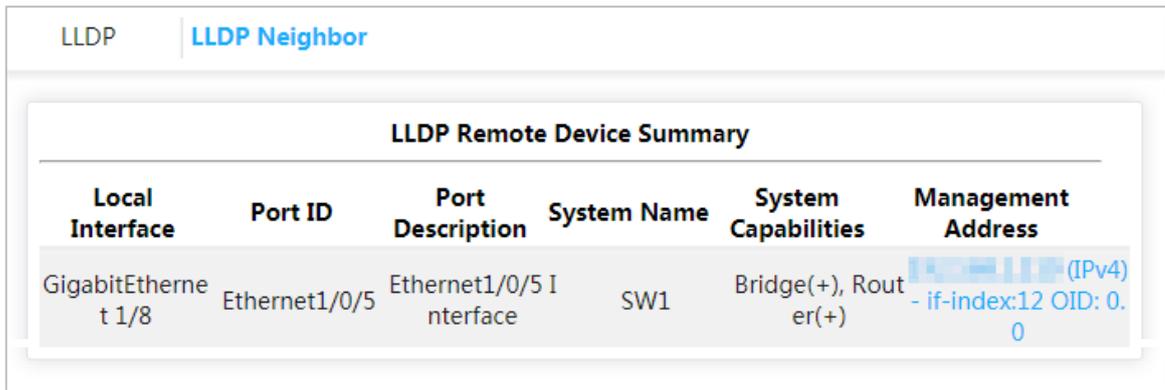
- Seleccionar **Permitir**: Ambos envían y reciben paquetes LLDP.
- Seleccionar **Desactivar**: Ni enviar ni recibir paquetes LLDP. Seleccionar
- **prescripción enoy**: Solo recibe paquetes LLDP. Seleccionar **solo**
- **transmisión**: Solo envía paquetes LLDP.

**Paso 3** Hacer clic **Ahorrar**.

Ver la información del vecino LLDP.

Seleccionar **Avanzado > Poco utilizado > LLDP > Vecino LLDP**. El **Vecino LLDP** se muestra la interfaz. Consulte la Figura 3-70.

Figura 3-70 Vecino LLDP



The screenshot shows a web interface for LLDP configuration. At the top, there are two tabs: 'LLDP' and 'LLDP Neighbor'. Below the tabs is a section titled 'LLDP Remote Device Summary' containing a table with the following data:

Local Interface	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/8	Ethernet1/0/5	Ethernet1/0/5 Interface	SW1	Bridge(+), Router(+)	192.168.1.1 (IPv4) - if-index:12 OID: 0.0

### 3.2.10 485 Configuración

Transmite los datos del puerto serie asíncrono RS-232/485 de forma transparente a través de Ethernet.

Seleccionar **Avanzado > Poco utilizado > 485 Config.** El **485 Configuración** se muestra la interfaz. Consulte la Figura 3-71.

Figura 3-71 Configuración 485

### 485 Config

Serial Index:

Enable:  ON  OFF

---

**Network Setting:**

Protocol Type:

IP Address:

IP Port:

Timeout(s):

---

**Serial Setting:**

Serial Speed:

Data Bits:

Parity Bits:

Stop Bits:

## 3.2.11 PoE

PoE (Power over Ethernet) es la función que a través del puerto Ethernet RJ-45, el dispositivo puede proporcionar energía para el PD (Powered Device) externo de forma remota con par trenzado. La función PoE ayuda a centralizar el suministro de energía y facilita la copia de seguridad. El terminal de red ya no necesita la fuente de alimentación externa, y un cable de red es suficiente. Cumple con los estándares de IEEE 802.3af, IEEE 802.3at e IEEE 802.3bt, adoptando el puerto de alimentación acordado globalmente. Se puede aplicar en teléfonos IP, puntos de acceso (AP) inalámbricos, cargadores de dispositivos portátiles, lectores de tarjetas, cámaras de red, recolección de datos, etc.



Solo algunos modelos de conmutadores PoE cumplen con el estándar IEEE 802.3bt y admiten BT máx. 90W. Por favor refiérase a la situación real.

### 3.2.11.1 Parámetros PoE

Configure la energía reservada, la energía de advertencia y habilite o deshabilite PoE.

**Paso 1** Seleccionar **Avanzado > Poco utilizado > PoE > Configuración de PoE**. El

**Configuración PoE** muestra la interfaz.

Figura 3-72 Configuración de PoE

The screenshot shows the PoE configuration interface with the following sections:

- PoE Settings:** Total Power: 190 W, Available Power: 171 W, Overload Power: 190 W.
- Power Status:** Consumed: 0 W, Remaining: 190 W, Reserved: 0 W.
- Port Status and Control:** A table with 8 rows and 5 columns: Port, Consumed, Enable, PD Class, and Status.

Port	Consumed	Enable	PD Class	Status
1	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
2	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
3	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
4	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
5	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
6	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
7	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
8	0	<input checked="" type="checkbox"/>	-	PoE turned OFF

Buttons: Save, Refresh

**Paso 2** En **Configuración PoE**, puede ver la potencia total de los 4 puertos y configurar la potencia disponible y la potencia de sobrecarga.

**Paso 3** En **Estado de energía**, puede ver la energía consumida, la energía restante y la energía reservada.

**Etapas 4** En **Estado y control de puertos**, selecciona el **Permitir** casilla para habilitar o deshabilitar PoE del puerto correspondiente.

**Paso 5** Hacer clic **Ahorrar**.

### 3.2.11.2 PoE verde

Establezca PoE Off time y PoE On time.

**Paso 1** Seleccionar **Avanzado > Poco utilizado > PoE > PoE verde**. El **PoE verde** muestra la interfaz.

Figura 3-73 PoE verde

Port	Enable
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

**Paso 2** Colocar **Tiempo de inactividad de PoE** a tiempo.

**Paso 3** Selecciona el **Permitir** cuadro y haga clic **Ahorrar**.

### 3.2.11.3 Soporte heredado

Permitir **Soporte heredado** en el caso de un dispositivo alimentado no estándar.



Dispositivo alimentado no estándar significa que el dispositivo admite una fuente de alimentación PoE de 48 V, pero no cumple con IEEE 802.3af/at.

**Paso 1** Seleccionar **Avanzado > Poco utilizado > PoE > Soporte heredado**.

El **Soporte heredado** se muestra la interfaz.

Figura 3-74 Soporte heredado

Port	Enable
1	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

**Paso 2** Selecciona el **Permitir** para el puerto correspondiente. Hacer

**Paso 3** clic **Ahorrar**.

### 3.2.11.4 Vigilancia PoE

Con PoE watchdog habilitado, puede monitorear dispositivos PD y mantenerlos en línea, y verificar el estado de los dispositivos PD cada 60 s. Si no hay transmisión de datos, el puerto PoE se apagará y reiniciará automáticamente. La fuente de alimentación PoE obligatoria y el mecanismo de vigilancia PoE no se pueden utilizar al mismo tiempo.

Seleccionar **Avanzado > Poco utilizado > PoE > PD Alive**, seleccione la casilla de verificación del puerto correspondiente y, a continuación, haga clic en **Ahorrar**.

El **perro guardián PoE** muestra la interfaz.

Figura 3-75 Vigilancia PoE

PoE Settings | Green PoE | Legacy Support | **PD Alive** | PoE Event Statistics

You can only use one between mandatory PoE power supply and PoE watchdog each time.

Port	Enable
1	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

[Save](#)

### 3.2.11.5 Visualización de estadísticas de eventos PoE

Seleccionar **Avanzado > Poco utilizado > PoE > Estadística de eventos de PoE** para ver estadísticas de eventos PoE.

Figura 3-76 Estadística de eventos PoE

PoE Settings | Green PoE | Legacy Support | PD Alive | **PoE Event Statistics**

Port	OverCurrent	LimitCurrent	DC Disconnect	StartUp Failed	Thermal Shutdown
1	0	0	0	0	0
2	0	0	1	0	0
3	0	0	1	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0

# 4 Mantenimiento

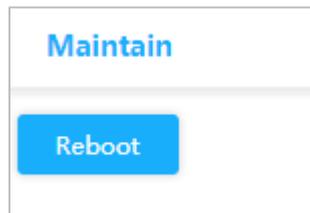
Tome el conmutador PoE de 4 puertos, por ejemplo. La interfaz de mantenimiento es diferente según los modelos de conmutador. Prevalecerá la interfaz real.

## 4.1 Reinicio del sistema

**Paso 1** Seleccione Mantener > Común > Reinicio del sistema.

El **Reinicio del sistema** se muestra la interfaz. Consulte la Figura 4-1.

Figura 4-1 Reinicio del sistema



**Paso 2** Hacer clic **Reiniciar**.

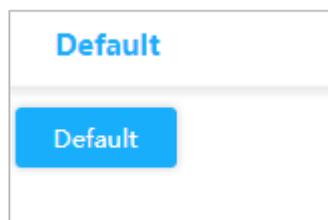
**Paso 3** Hacer clic **Confirmar** y el dispositivo se reinicia.

## 4.2 Restauración de la configuración predeterminada

Puede restaurar todas las configuraciones del conmutador a los valores predeterminados de fábrica, excepto la dirección IP de VLAN1 del conmutador.

**Paso 1** Seleccione Mantener > Común > Restaurar predeterminado. El **Por defecto** se muestra la interfaz. Consulte la Figura 4-2.

Figura 4-2 Restaurar predeterminado



**Paso 2** Hacer clic **Por defecto**.

Todas las configuraciones, excepto la dirección IP de VLAN1 del conmutador, se restauraron a los valores predeterminados de fábrica.

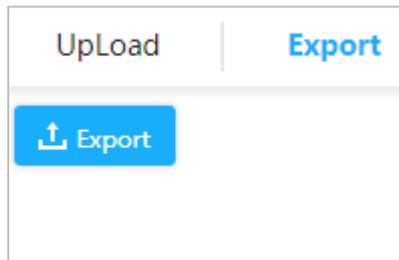
## 4.3 Gestión de configuración

### 4.3.1 Exportación del archivo de configuración

**Paso 1** Seleccione Mantener > Común > Administrar configuración > Exportar.

El **Exportarse** muestra la interfaz. Consulte la Figura 4-3.

Figura 4-3 Exportar



Paso 2 Hacer clic **Exportar**. Exportar archivo de configuración.

### 4.3.2 Subir archivo de configuración

Paso 1 Seleccione Mantener > Común > Administrar configuración > Cargar. El **Subirse** muestra la interfaz. Consulte la Figura 4-4.

Figura 4-4 Carga



Paso 2 Hacer clic **Browse...** y seleccione el archivo de configuración para cargar.

Paso 3 Hacer clic **Subir**.

Etapa 4 Reinicie el dispositivo y la configuración surtirá efecto.

## 4.4 Actualización de software

Paso 1 Seleccione Mantener > Común > Actualización de software. El **Actualizarse** muestra la interfaz. Consulte la Figura 4-5.

Figura 4-5 Actualización



Paso 2 Hacer clic **Navegar...** y seleccione el archivo en formato .mif para cargar.

Paso 3 Hacer clic **Subir**.

El dispositivo se reinicia una vez finalizada la actualización. Vuelva a iniciar sesión en el conmutador y todas las configuraciones anteriores no cambiarán.

## 4.5 Duplicación

La duplicación de puertos también se denomina supervisión de puertos. El monitoreo de puertos es la tecnología de adquisición de paquetes de datos que a través de la configuración del conmutador, el paquete de datos de uno o varios puertos (puertos de origen de duplicación) se puede copiar a un puerto específico (puerto de destino de duplicación). El puerto de destino de duplicación se conecta a una PC donde está instalado el software de análisis de paquetes de datos, y puede analizar el paquete de datos recibido para monitorear la red y solucionar problemas.

**Paso 1** Seleccione Mantener > Común > Duplicar.

El **Espejo** muestra la interfaz. Consulte la Figura 4-6.

Figura 4-6 Espejo

Port	Source	Destination
1	Disabled	<input type="checkbox"/>
2	Disabled	<input type="checkbox"/>
3	Disabled	<input type="checkbox"/>
4	Disabled	<input type="checkbox"/>
5	Disabled	<input type="checkbox"/>
6	Disabled	<input type="checkbox"/>
7	Disabled	<input type="checkbox"/>
CPU	Disabled	<input checked="" type="checkbox"/>

**Paso 2** En **Ajustes globales**, seleccionar **Activado** en **Modo** para habilitar la duplicación.

**Paso 3** En **Configuración del puerto**, seleccionar **Fuente** o **Destino** según la situación real.

- Seleccione las siguientes cuatro formas para el puerto de origen.
  - Ambos: habilite el puerto como la dirección de origen del espejo.
  - Deshabilitar: deshabilite el puerto como la dirección de origen del espejo.
  - Solo Rx: el puerto solo refleja la recepción de datos, en lugar de enviar datos.
  - Solo Tx: el puerto solo refleja el envío de datos, en lugar de recibir datos.
- Seleccione el **Destino** casilla para configurar el puerto como destino.

**Etapas** 4 Hacer clic **Ahorrar**.

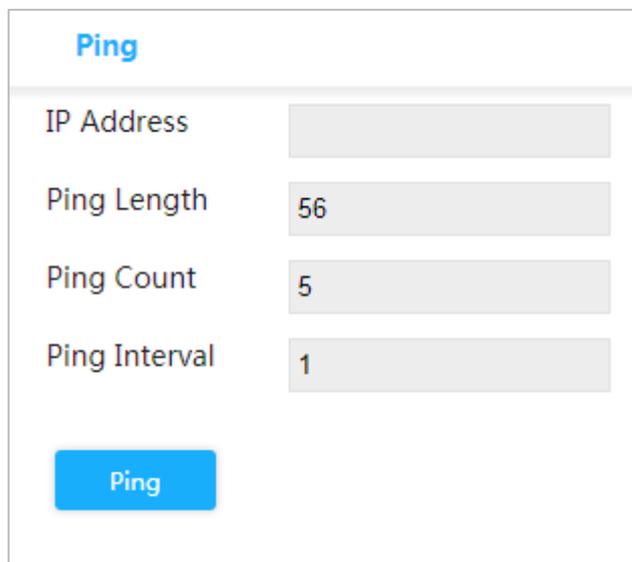
## 4.6 Hacer ping

Con el protocolo Ping, puede verificar si se puede acceder al dispositivo con una dirección IP específica y verificar si falla la conexión de red.

**Paso 1** Seleccione Mantener > Común > Ping.

El **Silbido** muestra la interfaz. Consulte la Figura 4-7.

Figura 4-7 Hacer ping



IP Address	<input type="text"/>
Ping Length	<input type="text" value="56"/>
Ping Count	<input type="text" value="5"/>
Ping Interval	<input type="text" value="1"/>

**Paso 2** Introduzca la dirección IP y haga clic en **Silbido**.

## 4.7 Funciones del Sistema de Gestión de Red

### 4.7.1 Activación de la función e inicio de sesión en la plataforma

Las funciones del sistema de administración de red son admitir la plataforma de administración de red iLinksView. Puede habilitar o deshabilitar la función de administración de red y cambiar el nombre de usuario y la contraseña.



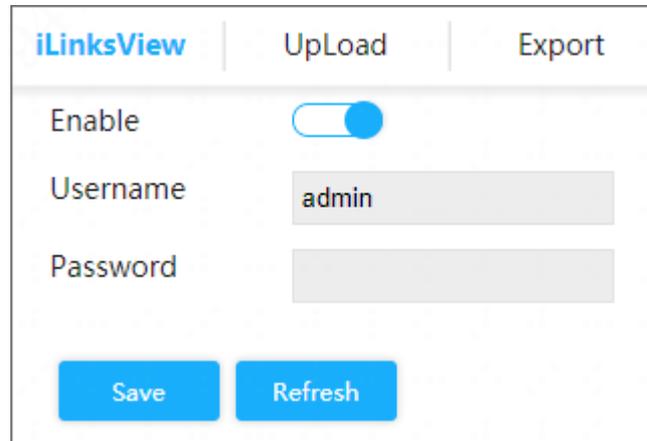
El nombre de usuario y la contraseña deben ser los mismos que los de la administración de red de iLinksView.  
plataforma.

La función de administración de red está habilitada de manera predeterminada. Aquí están el nombre de usuario y la contraseña predeterminados.

Nombre de usuario: administrador

Contraseña: lt\_91\_il\_02\_nmp

Figura 4-8 iLinksView



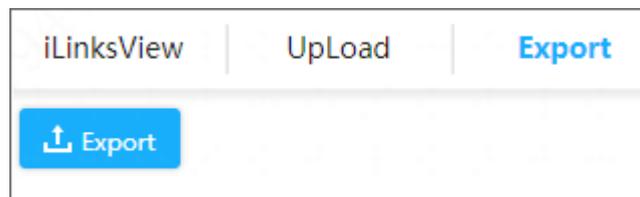
The screenshot shows the iLinksView configuration interface. At the top, there are three tabs: 'iLinksView', 'UpLoad', and 'Export'. The 'Export' tab is currently selected. Below the tabs, there is a section for configuration. The 'Enable' option is a toggle switch that is turned on. The 'Username' field is a text input containing the text 'admin'. The 'Password' field is a text input that is currently empty. At the bottom of the configuration section, there are two blue buttons: 'Save' and 'Refresh'.

## 4.7.2 Exportación del archivo de configuración de gestión de red

Puede exportar el archivo de configuración de administración de red.

Paso 1 Seleccionar **Mantener > Común > iLinksView > Exportar**.

Figura 4-9 Archivo de configuración de exportación



The screenshot shows the iLinksView configuration interface. At the top, there are three tabs: 'iLinksView', 'UpLoad', and 'Export'. The 'Export' tab is currently selected. Below the tabs, there is a blue button with an upward arrow icon and the text 'Export'.

Paso 2 Hacer clic **Exportar**.

## 4.7.3 Carga del archivo de configuración de gestión de red

Puede cargar el archivo de configuración de administración de red.

Paso 1 Seleccionar **Mantener > Común > iLinksView > Cargar**.

Figura 4-10 Cargar archivo de configuración



The screenshot shows the iLinksView configuration interface. At the top, there are three tabs: 'iLinksView', 'UpLoad', and 'Export'. The 'UpLoad' tab is currently selected. Below the tabs, there is a text input field labeled 'Select UpLoad File'. To the right of the input field are two blue buttons: 'Browse' and 'UpLoad'.

Paso 2 Hacer clic **Navegar** para seleccionar el archivo de

Paso 3 configuración. Hacer clic **Subir**.

Etapas 4 Reinicie el dispositivo y la configuración surtirá efecto.

# Apéndice 1 Recomendaciones sobre ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

## **Acciones obligatorias a tomar para la seguridad de la red de equipos básicos: 1.**

### **Usar contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso; No utilice caracteres continuos, como 123, abc, etc.;
- No utilice caracteres superpuestos, como 111, aaa, etc.;

### **2. Actualice el firmware y el software del cliente a tiempo**

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su equipo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el equipo está conectado a la red pública, se recomienda habilitar la función de "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

## **Recomendaciones "agradables de tener" para mejorar la seguridad de su red de equipos: 1. Protección física**

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en un gabinete y una sala de computadoras especiales, e implemente una administración de claves y un permiso de control de acceso bien hecho para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de equipos extraíbles (como un disco flash USB), puerto serie), etc.

### **2. Cambie las contraseñas regularmente**

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

### **3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo**

El equipo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

### **4. Habilitar bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada de forma predeterminada y le recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión varias veces con la contraseña incorrecta, la cuenta correspondiente y la dirección IP de origen se bloquearán.

### **5. Cambiar HTTP predeterminado y otros puertos de servicio**

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

## **6. Habilitar HTTPS**

Le sugerimos que habilite HTTPS, para que visite el servicio web a través de un canal de comunicación seguro.

## **7. Habilitar lista blanca**

Le sugerimos que habilite la función de lista blanca para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista blanca.

## **8. Enlace de dirección MAC**

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al equipo, reduciendo así el riesgo de suplantación de ARP.

## **9. Asigne cuentas y privilegios de manera razonable**

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

## **10. Deshabilite los servicios innecesarios y elija modos seguros**

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

Si es necesario, se recomienda encarecidamente que utilice modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP: Elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de encriptación WPA2-PSK y configure contraseñas seguras.

## **11. Transmisión encriptada de audio y video**

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión encriptada para reducir el riesgo de robo de datos de audio y video durante la transmisión.

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

## **12. Auditoría segura**

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del equipo: al ver los registros, puede conocer las direcciones IP que se usaron para iniciar sesión en sus dispositivos y sus operaciones clave.

## **13. Registro de red**

Debido a la limitada capacidad de almacenamiento del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

## **14. Construya un entorno de red seguro**

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, es

sugirió usar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.