Interruptor de Eternet

Manual de operación web

V1.0.0

Prefacio

General

Este manual presenta las operaciones en la interfaz web del conmutador Ethernet (en adelante, "el conmutador"). Puede visitar el interruptor en el navegador web, configurar y administrar el interruptor.

Instrucciones de seguridad

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

Palabras de advertencia	Significado
DANGER	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrarle tiempo.
NOTE	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	abril 2021

Acerca del Manual

- El manual es sólo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por operaciones que no cumplan con el manual. El
- manual se actualizará de acuerdo con las últimas leyes y regulaciones 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 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. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria. Aún así
- puede haber desviaciones en los datos técnicos, funciones y descripción de operaciones, o errores de impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final.

- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema al usar el dispositivo.
- Si existe alguna incertidumbre o controversia, consulte nuestra explicación final.

Salvaguardias 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 consultarlo en el futuro.

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 instalación horizontal e instálelo en una superficie sólida y plana para evitar que se caiga.
- Evite salpicaduras de líquido sobre 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 con voltaje nominal de entrada y salida.
- No desmonte el dispositivo sin instrucción profesional.
- Transporte, utilice y almacene el dispositivo en los rangos permitidos de humedad y
- temperatura. Al retirar el cable, primero apague el dispositivo para evitar lesiones personales.
- El estabilizador de voltaje y el dispositivo de protección contra rayos son opcionales según la fuente de alimentación y el entorno circundante.

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 dentro del límite de las especificaciones nominales.
- Utilice el adaptador de corriente estándar. No asumiremos ninguna responsabilidad por cualquier problema causado por un adaptador de corriente no estándar.
- La fuente de alimentación deberá cumplir con el requisito SELV. Utilice una fuente de alimentación que cumpla con la fuente de alimentación limitada, según IEC62368-1. Consulte la etiqueta del dispositivo.
- Asegúrese de conectar a tierra el dispositivo (sección del cable de cobre: > 2,5 mm^2; resistencia a tierra: ≤ 4 Ω).
- El acoplador es el aparato de desconexión. Manténgalo en ángulo para una fácil operación.

Tabla de contenido

1 Iniciar sesión

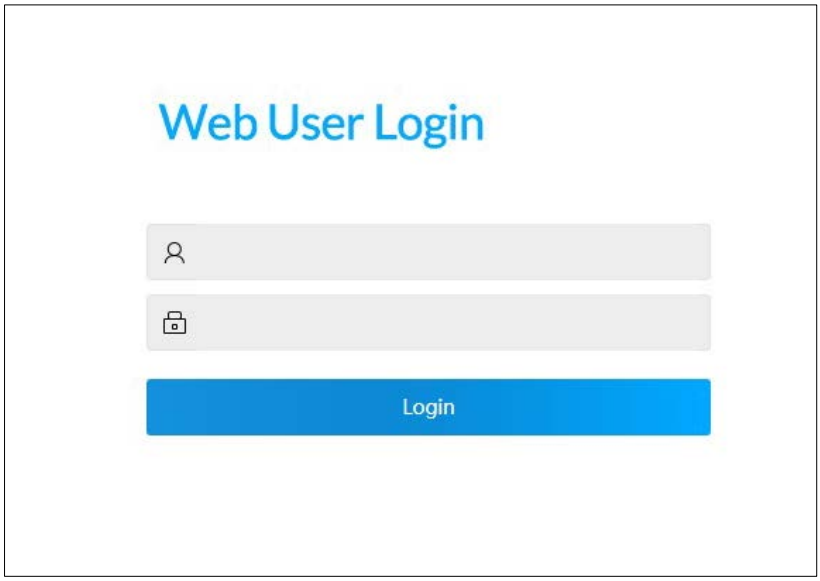
Antes de iniciar sesión, asegúrese de:

- Ya configuras 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 correctamente.

Paso 1 Ingrese la dirección IP (192.168.1.110 de forma predeterminada) del conmutador en la barra de direcciones del navegador web y luego presione la tecla Intro.

Figura 1-1 Inicio de sesión web



Paso 2 Ingrese el nombre de usuario y la contraseña. El nombre de usuario y la contraseña son admin de forma predeterminada. Hacer clic

Paso 3 **Acceso**.

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

2 configuraciones rápidas

Puede ver la información del sistema y configurar los parámetros del dispositivo, VLAN, agregación de enlaces, dirección IP y ruta. Tomemos como ejemplo el conmutador PoE de 4 puertos. 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, tipo, número de serie, versión de software, dirección IP, estado del puerto e información del puerto del dispositivo.

Después de iniciar sesión en el sistema, el**Ajuste rapido**Se 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 que la conexión falla.

Figura 2-1 Información del sistema

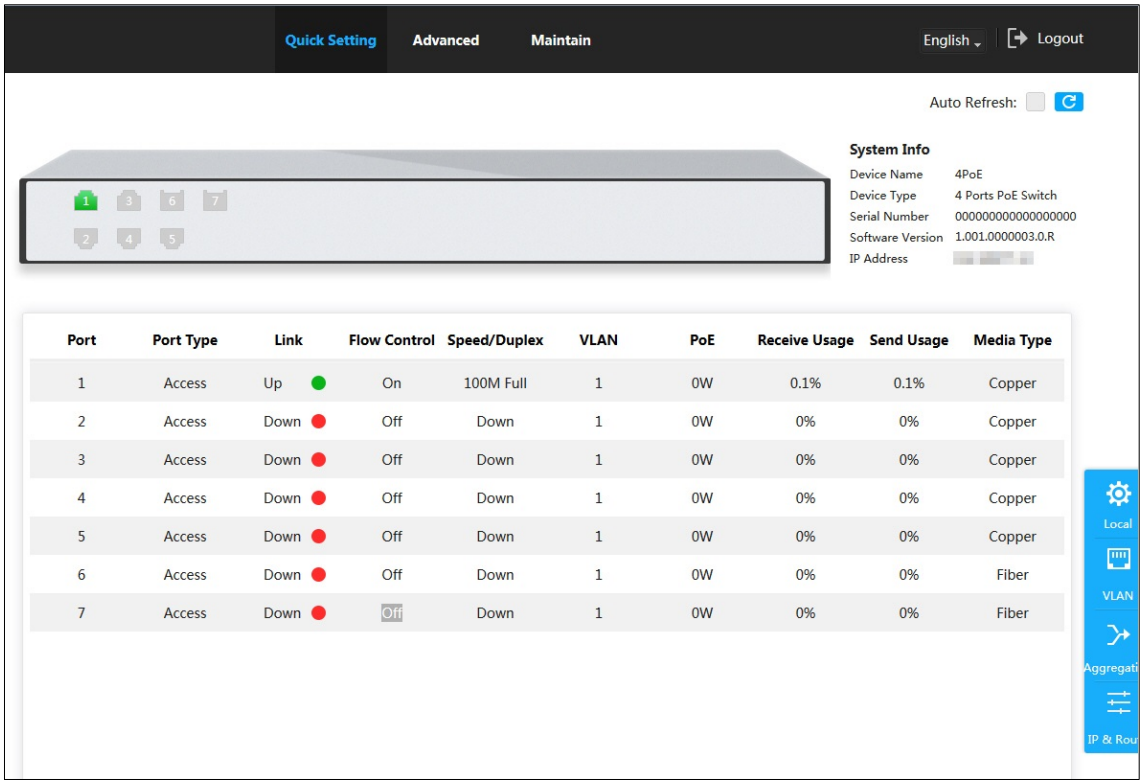


Tabla 2-1 Información del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador. El conmutador demostrado 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:**Acceso**,**Híbrido**, y**Trompa**.

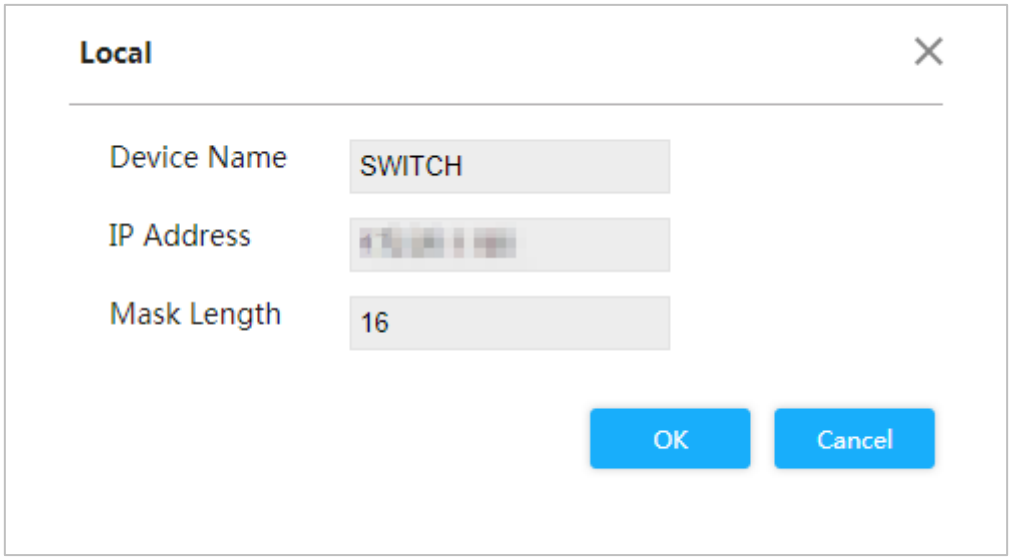
Parámetro	Descripción
Enlace	Dos estados de enlace:**Arriba**y**Abajo**.**Arriba**indica que el puerto está conectado exitosamente y**Abajo**indica que el puerto no está conectado o que la conexión falla.
Control de flujo	Muestra el estado del control de flujo.
Velocidad/Dúplex	- Online: Muestra la velocidad del puerto y el modo dúplex. Sin - conexión: muestra**Abajo**.
VLAN	Puerto VLAN. Es VLAN 1 de forma predeterminada.
PoE	Muestra el consumo de energía de POE. Sólo entre 1 y 4 puertos son puertos PoE. - Los conmutadores Ethernet que no son PoE no admiten esta función. - La cantidad de puertos PoE admitidos por diferentes modelos es diferente.
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 promedio en un período determinado (normalmente 5 minutos).
Tipo de medio	Dos tipos de medios:**Cobre**y**Fibra**.**Cobre**indica el puerto RJ-45 y **Fibra** indica puerto de fibra.

2.2 Locales

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

Paso 1 Hacer clic**Local**a la derecha de**Ajuste rapido**interfaz. El **Local**Se muestra la interfaz.

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**.

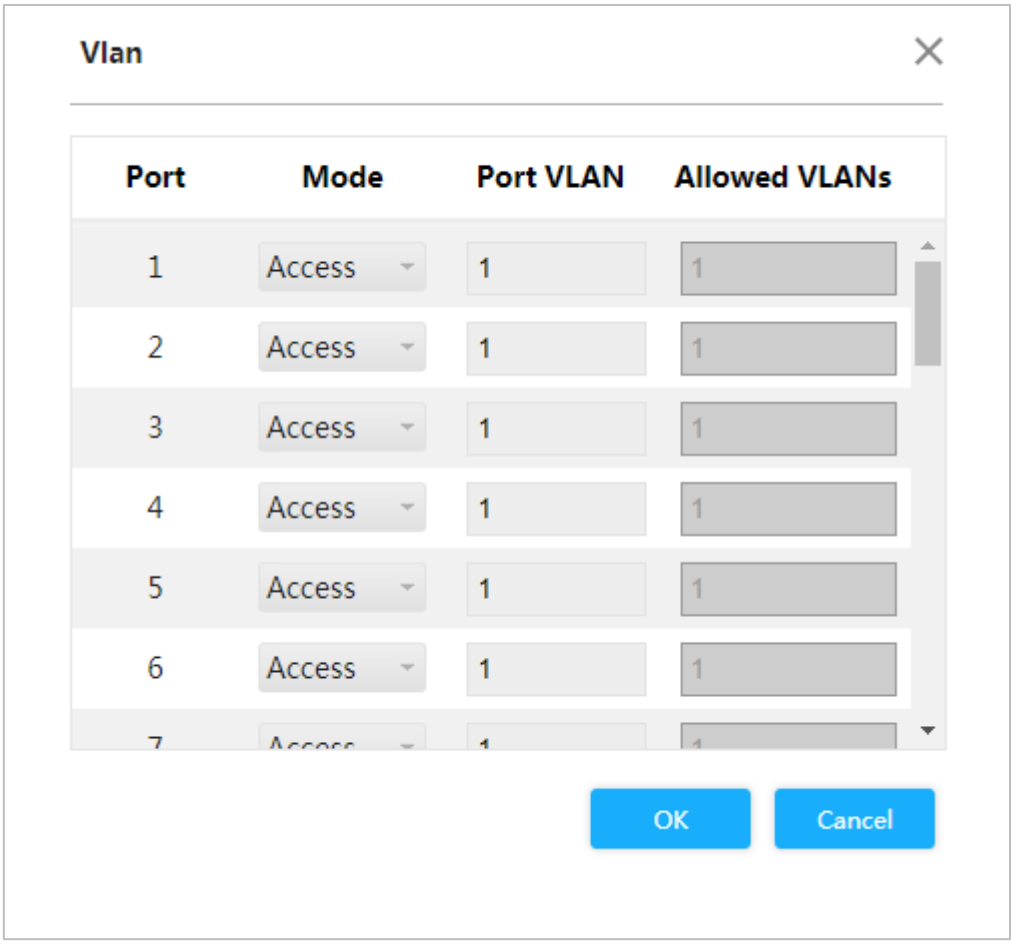
2.3 VLAN

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 rapido**interfaz.

El**VLAN**Se muestra la interfaz.

Figura 2-3 VLAN



Paso 2 Configure los parámetros de VLAN del puerto.

Tabla 2-2 Parámetro de configuración de VLAN del puerto

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

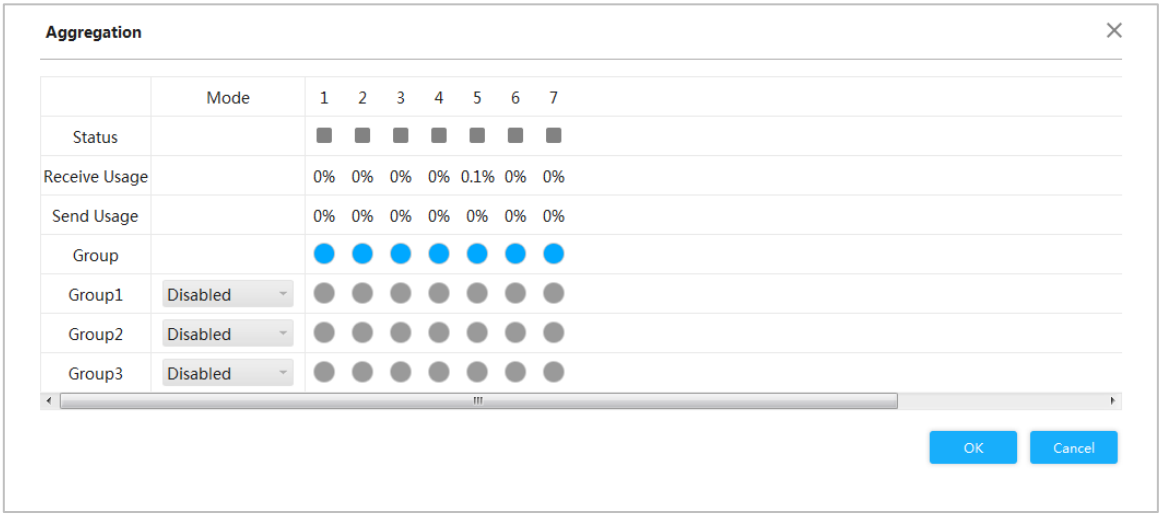
Paso 3 Hacer clic**DE ACUERDO**.

2.4 Agregación

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

Hacer clic**Agregación**en**Ajuste rapido**interfaz, y el**Agregación**Se muestra la interfaz.

Figura 2-4 Agregación



2.4.1 Configuración de agregación estática

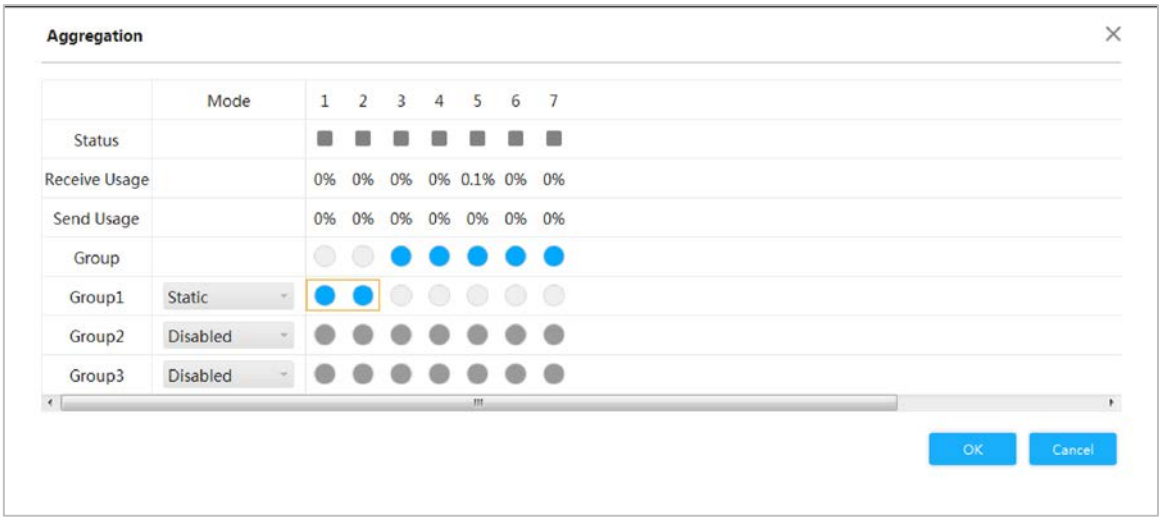
La agregación estática es un método de combinación o agrupación de múltiples puertos de conmutador o NIC para formar un único canal de éter. Por ejemplo, agregue el puerto 1 y el puerto 2 al grupo estático 1.

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

Paso 2 puerto 1 y el puerto 2 en el grupo 1 para agregar los dos puertos a la agregación estática.

Para un conmutador PoE de 4 puertos, puede configurar hasta 3 grupos de agregación estática. Estático La agregación es diferente dependiendo de los diferentes modelos de conmutador PoE. La interfaz real prevalecerá.

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

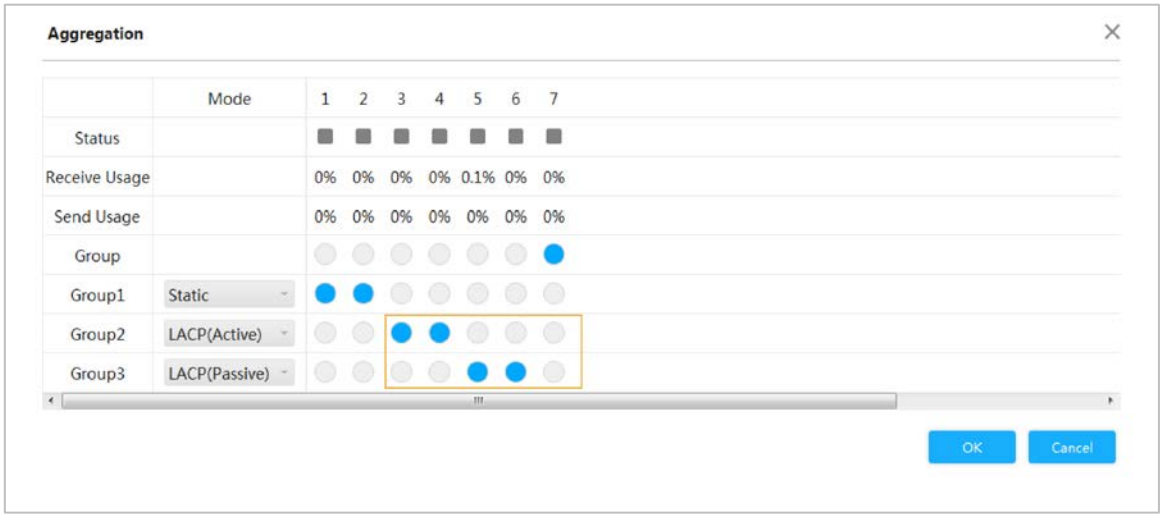
La agregación dinámica se diferencia de la agregación estática en que la cantidad del puerto se fija en la agregación estática, pero la cantidad del puerto realmente agregado se ajusta dinámicamente de acuerdo con la estrategia de caudal.

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.

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.

Figura 2-6 Configuración dinámica



Paso 2 Hacer clic**DE ACUERDO**.

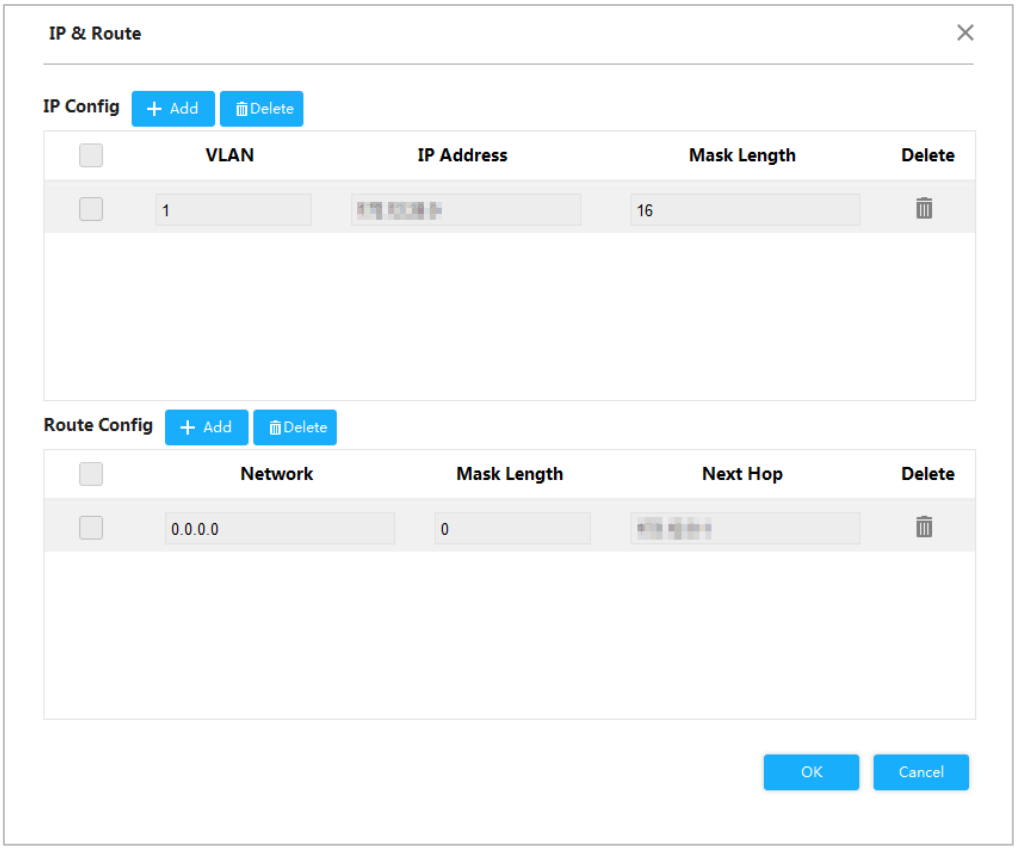
2.5 IP y Ruta

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 rapido**interfaz.

El**IP y ruta**Se muestra la interfaz.

Figura 2-7 IP y ruta



Paso 2 Agregue la interfaz VLAN.

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

Figura 2-8 Interfaz VLAN

2) Configurar los parámetros.

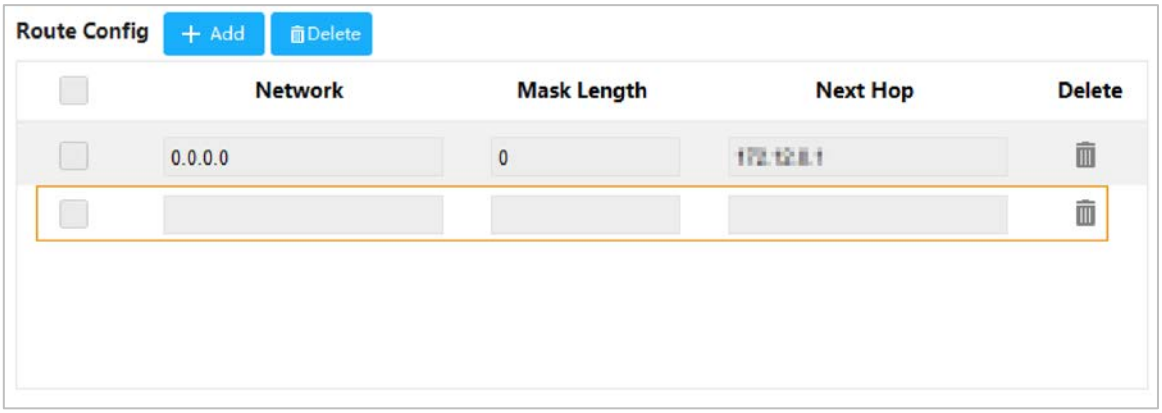
Tabla 2-3 Interfaz VLAN

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.

Figura 2-9 Ruta IP



2) Configurar los parámetros.

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 configuraciones avanzadas

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. Tomemos como ejemplo el conmutador PoE de 4 puertos.

3.1 Configuración común

3.1.1 Configuración del sistema

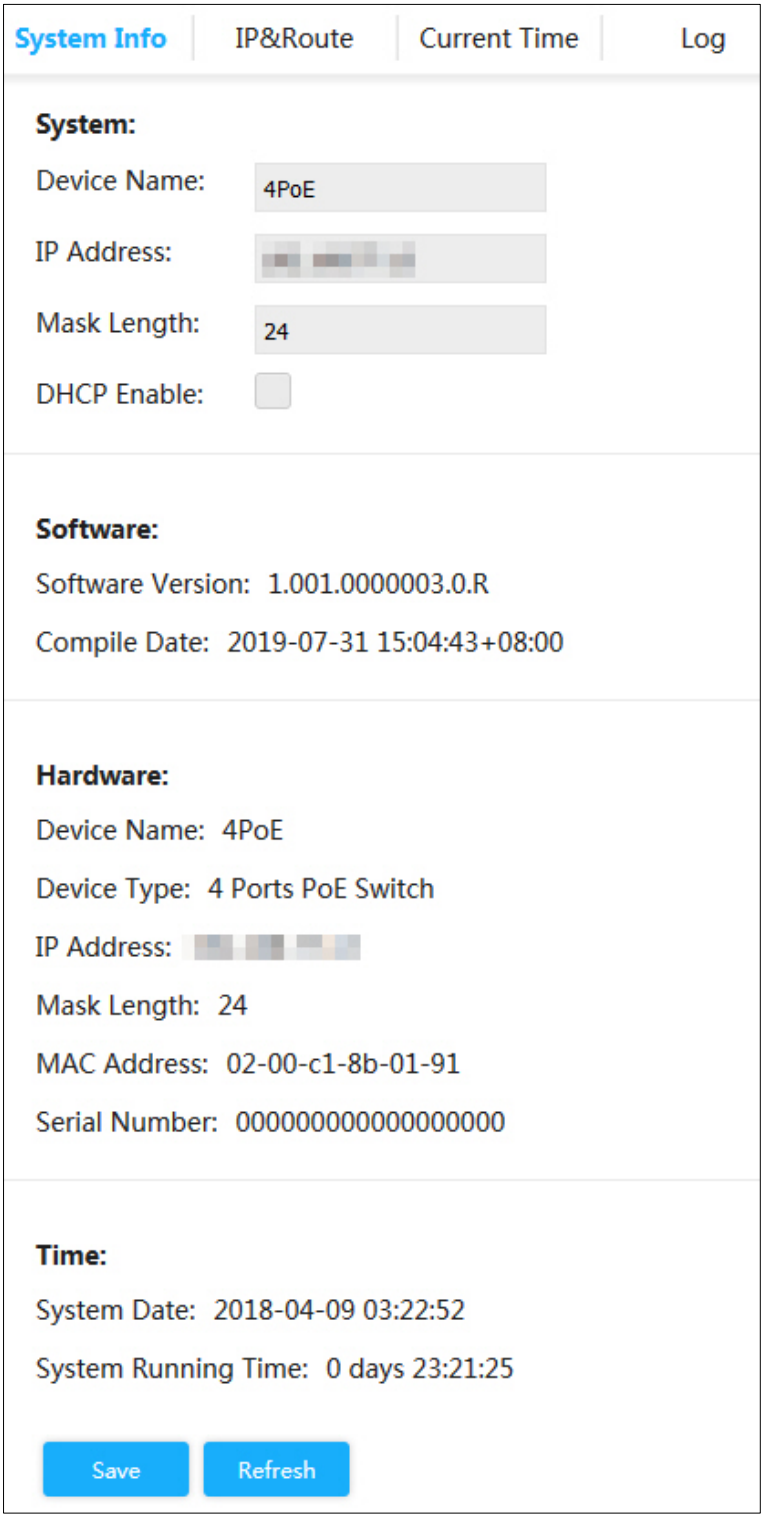
3.1.1.1 Información del sistema

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 al habilitar el cliente DHCP. Después de habilitar el Cliente DHCP, el enrutador IP o el servidor DHCP
La conexión al conmutador asignará la dirección IP al conmutador automáticamente y la IP existente
La dirección será invalidada y entonces 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.

Figura 3-1 Información del sistema



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

Paso 3 clic**Ahorrar**.

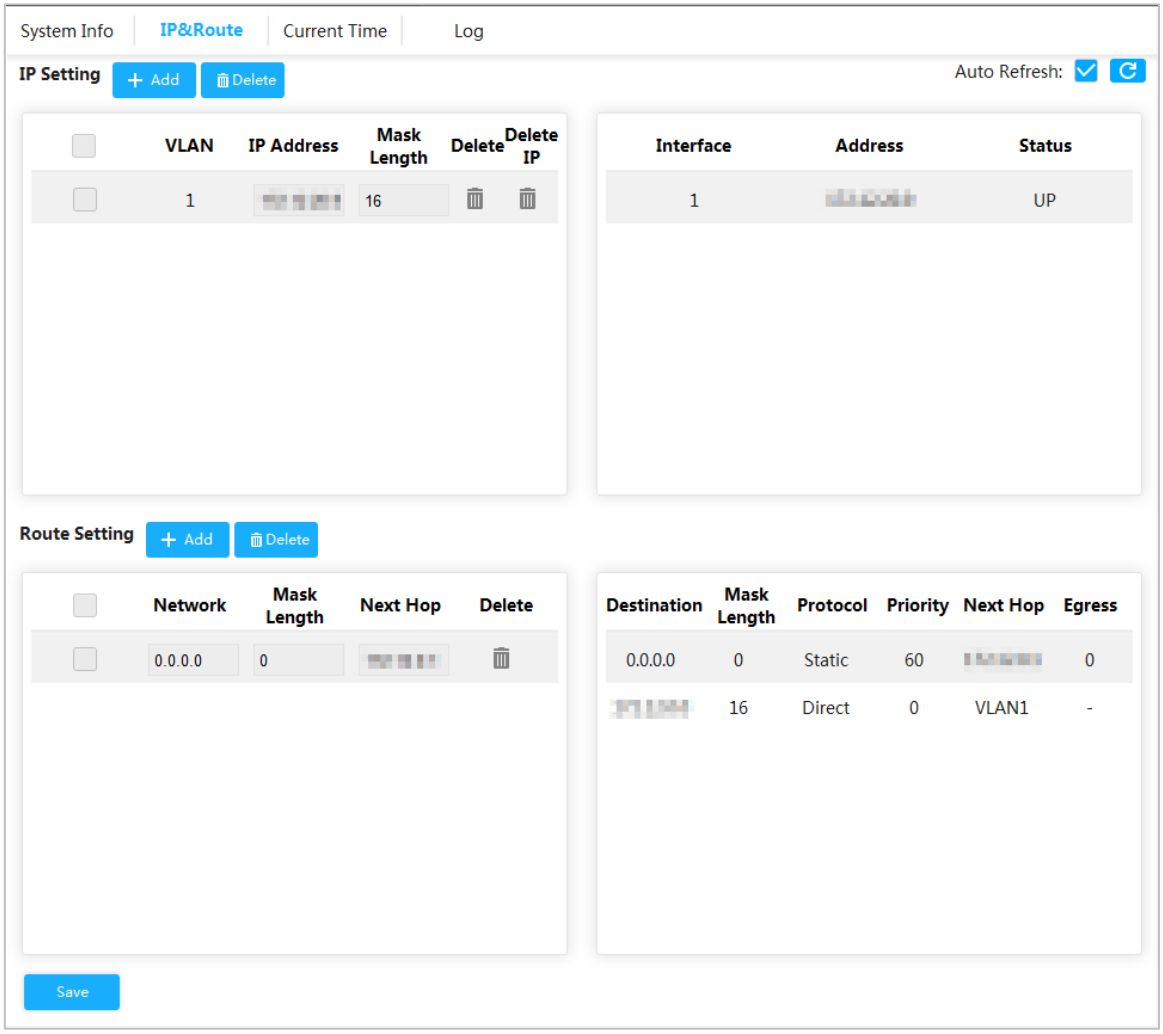
3.1.1.2 IP y Ruta

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 la entidad física 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**.

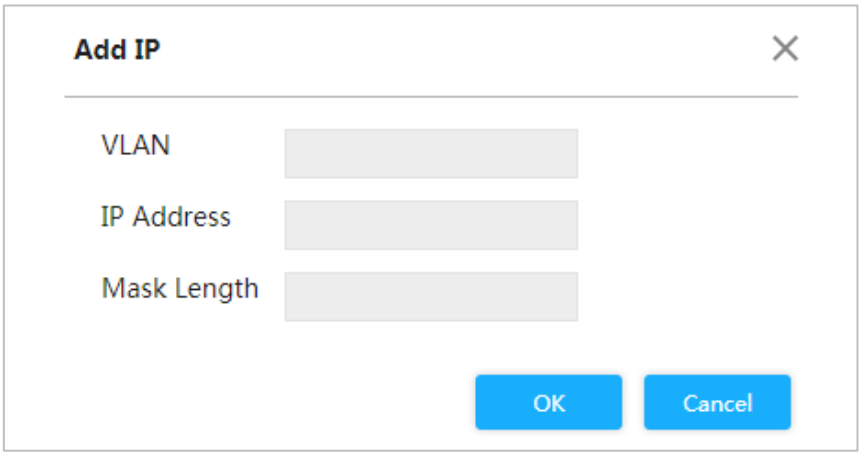
Figura 3-2 IP y ruta



Paso 2 Agregue la interfaz VLAN.

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

Figura 3-3 Agregar IP



2) Configurar los parámetros.

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	Establezca 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.

Figura 3-4 Agregar ruta

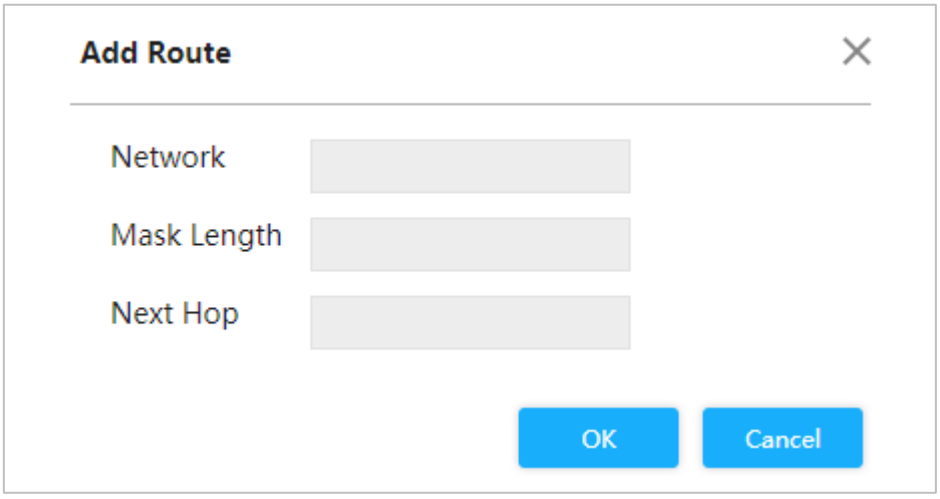


Tabla 3-2 Descripción de rutas IP

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.

2) Haga clic**DE ACUERDO**.

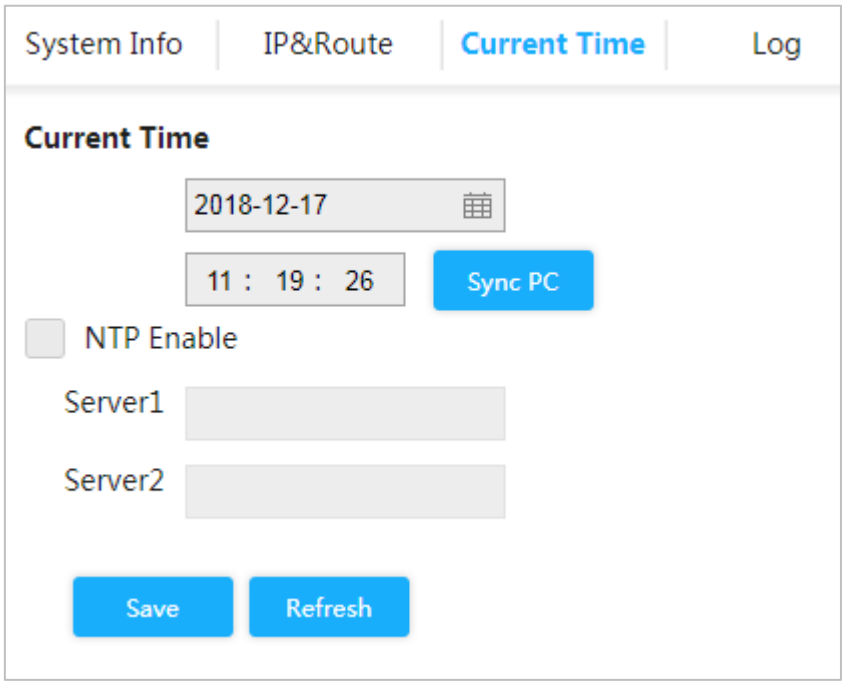
Etapa 4 Hacer clic**Ahorrar**.

3.1.1.3 Hora del sistema

Establezca la hora del sistema de conmutación.

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

Figura 3-5 Hora actual (1)



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

- Establecer la hora manualmente

  Establecer 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 del PC local. Sincronizar la

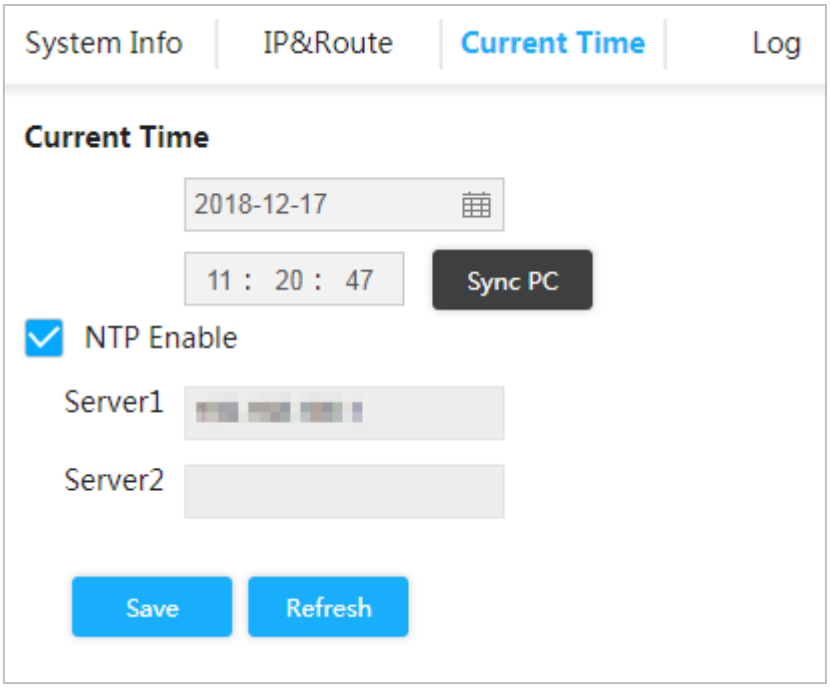
- hora del servidor NTP

  Sólo con el servidor NTP configurado en la red podrás habilitar esta función en los siguientes pasos:

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

Paso 2 Configure la dirección IP del servidor NTP.

Figura 3-6 Hora actual (2)



Paso 3 Hacer clic**Ahorrar**.

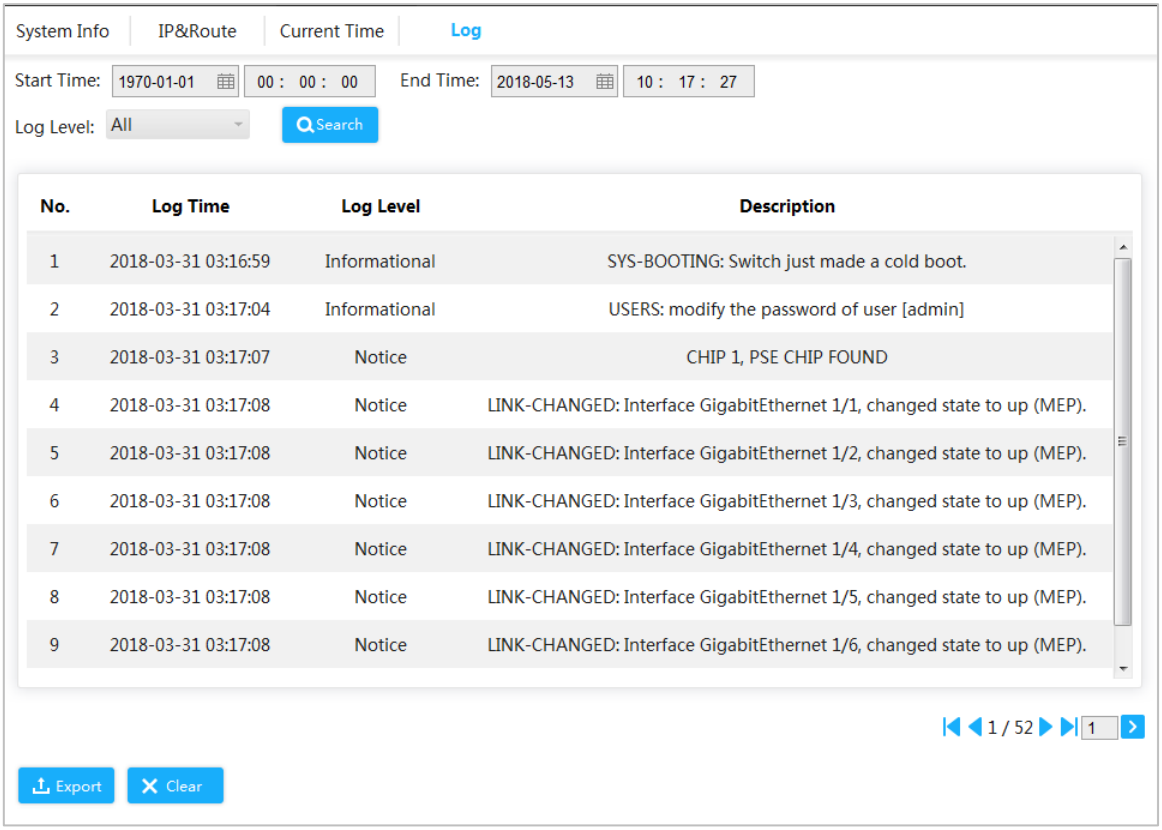
La hora del cambio se sincroniza automáticamente con la hora del servidor 1.

3.1.1.4 Registro

Puede ver registros, exportarlos y borrarlos.

Seleccionar**Avanzado > Común > Configuración del sistema > Registro**. El**Registro**Se muestra la interfaz.

Figura 3-7 Registro



- 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**Claro**para borrar todos los registros.
-

3.1.2 Configuración del puerto

Puede configurar los parámetros del puerto, incluida la velocidad, full duplex y half duplex, etc. Paso 1

Seleccionar**Avanzado > Común > Puerto**.

Figura 3-8 Configuración del puerto

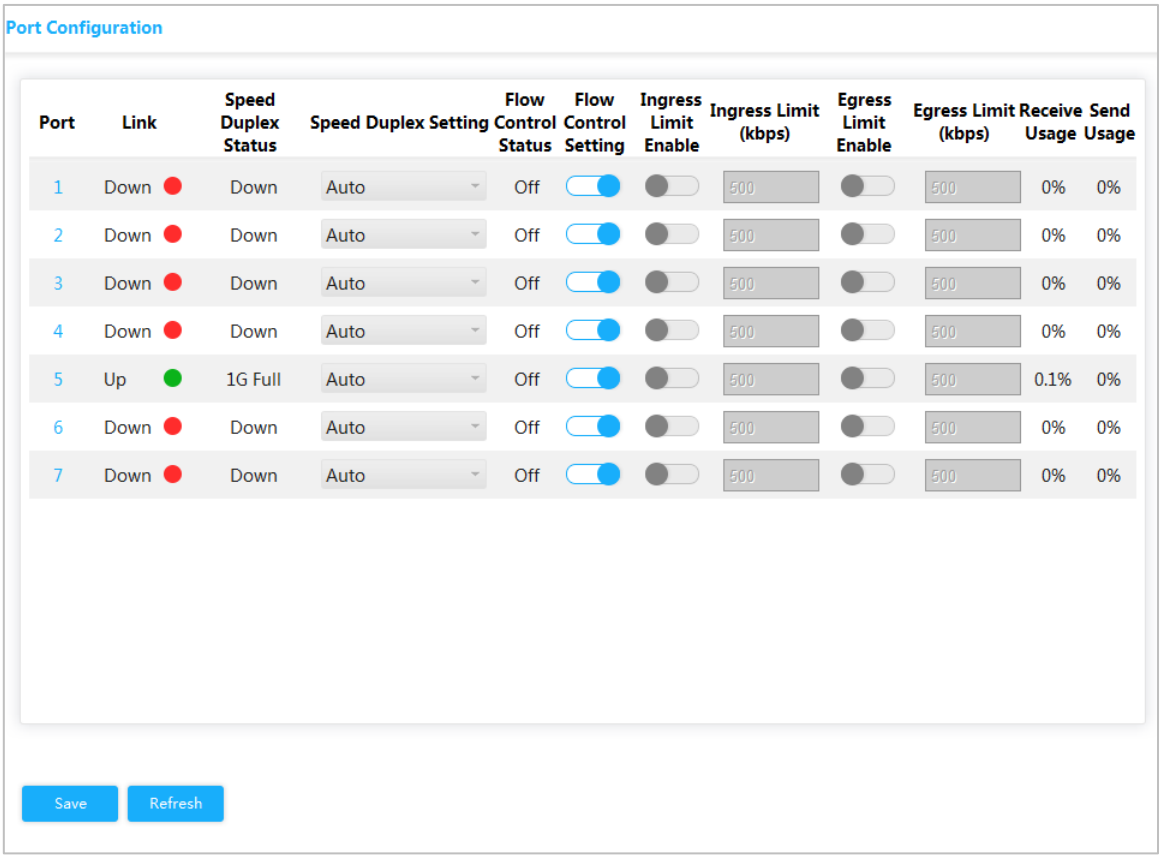


Tabla 3-3 Parámetro de puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.
Enlace	Verde**Arriba**indica que el puerto está conectado correctamente y el color rojo**Abajo** indica que el puerto no está conectado o que la conexión falla.
Estado de velocidad dúplex	**Abajo**significa desconexión, y la velocidad específica significa conexión exitosa. **Lleno**significa dúplex completo;**Medio**significa medio dúplex.
Configuración de velocidad dúplex	Configure la velocidad y el modo dúplex. La velocidad y el modo dúplex del puerto combinado están fijados en**Auto**.
Estado de control de flujo	Muestra el estado de habilitación o negociador real del control de flujo, incluidos ENCENDIDO y APAGADO. - ON: 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.
Límite de ingreso (kbps)	Establezca el límite de ingreso.

Parámetro	Descripción
Habilitar límite de salida	Activar/desactivar el límite de salida. - : La habilitación de salida está habilitada. - : La habilitación de salida está deshabilitada.
Límite de salida (kbps)	Establezca el límite de salida.
Recibir uso	Muestra el uso de aceptación.
Enviar uso	Muestra el uso de envío.

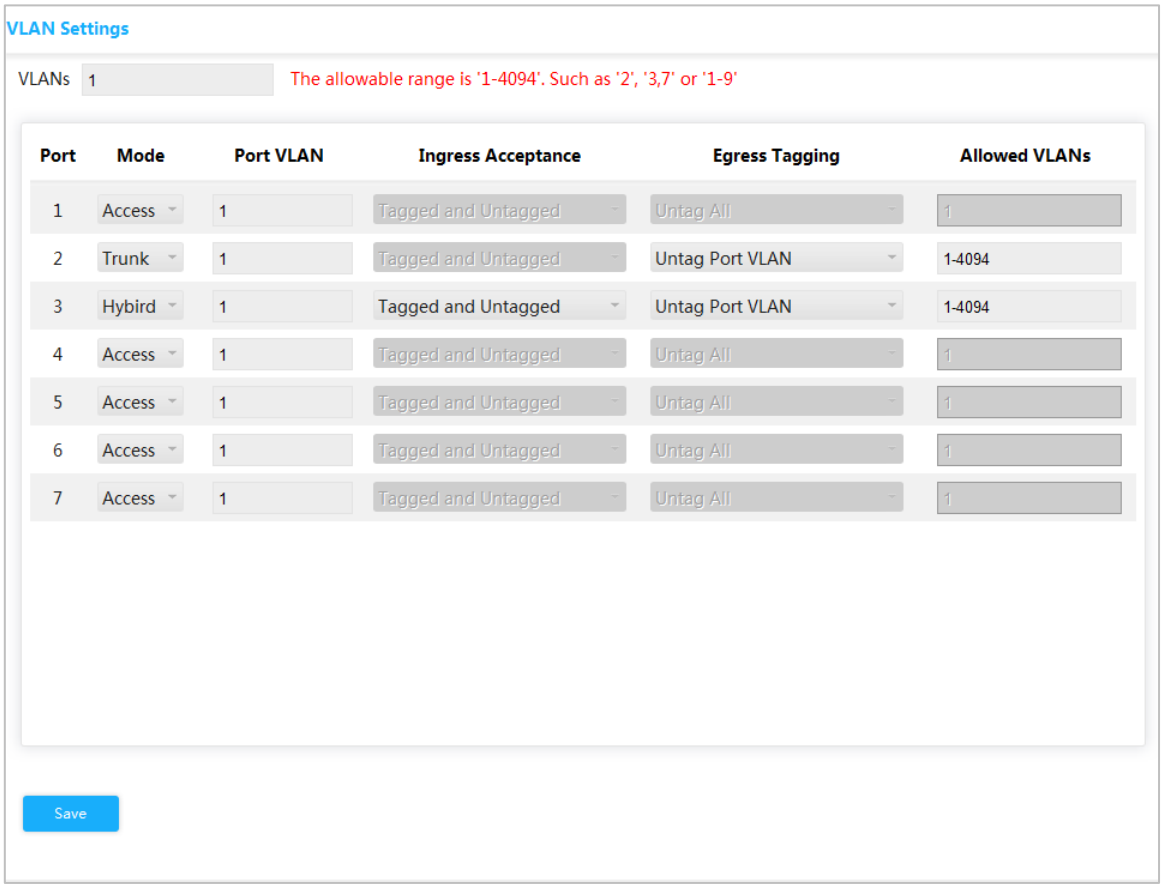
Paso 2 Hacer clic**Ahorrar**.

3.1.3 Configuración de VLAN

Agregue el puerto a la VLAN y configure la VLAN. Por defecto, el puerto pertenece a VLAN1. Paso 1 Seleccionar**Avanzado > Común > Configuración de VLAN**.

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

Figura 3-9 Configuración de VLAN



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

Paso 3 Configure los parámetros de VLAN del puerto.

Tabla 3-4 Parámetro de configuración de VLAN del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.
Modo	Tres modos:**Acceso**,**Híbrido**, y**Trompa**.
Puerto VLAN	Agregue el puerto a una VLAN. Por defecto, el puerto pertenece a VLAN1. El rango es 1–4094.

Parámetro	Descripción
Aceptación de ingreso	Muestra si los datos pueden fluir hacia el puerto. Solo**Híbrido**admite la configuración (de forma predeterminada, toda la fecha fluye hacia el puerto en otros modelos). Vea las siguientes situaciones: - **Etiquetado y sin etiquetar**: Todos los datos fluyen hacia el puerto. **Sólo** - **etiquetado**: Sólo los datos etiquetados pueden fluir hacia el puerto. **Sólo sin** - **etiquetar**: Sólo los datos sin etiquetar pueden fluir hacia el puerto.
Etiquetado de salida	Muestra si se deben etiquetar los datos que saldrán del puerto. Vea las siguientes tres situaciones: - **Desetiquetar puerto VLAN**: Si la etiqueta de flujo de datos es la misma que PVID, la etiqueta se eliminará. - **Etiquetar todo**: Todos los datos serán etiquetados. - **Desetiquetar todo**: No se etiquetarán todos los datos.
VLAN permitidas	Configure la VLAN permitida.

Etapa 4 Hacer clic**Ahorrar**.

3.1.4 Agregación

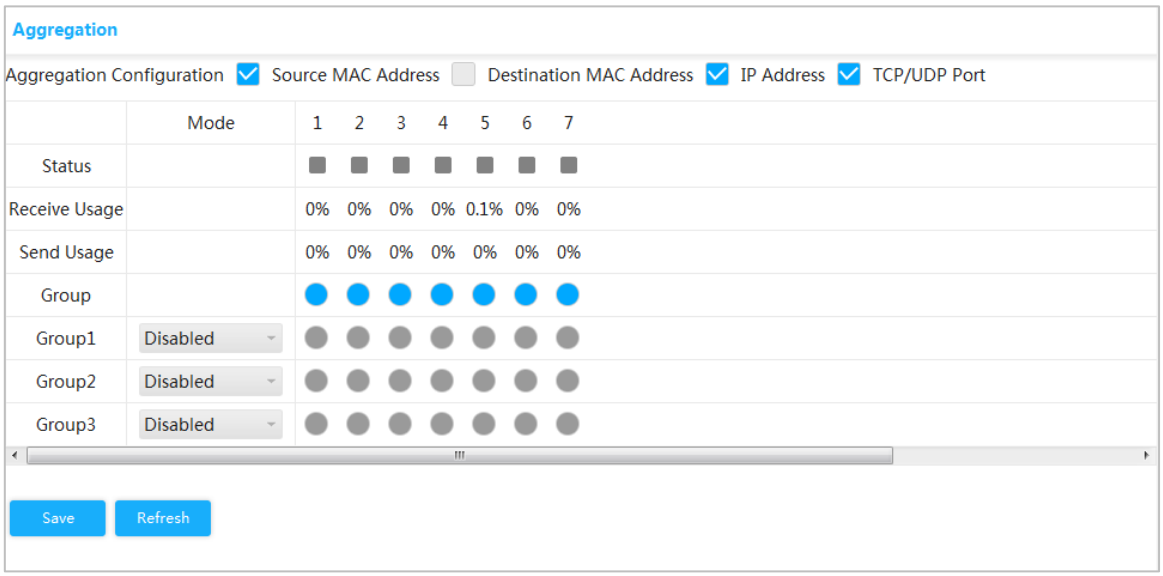
La agregación consiste en formar los múltiples puertos físicos del conmutador en el puerto lógico. Los múltiples enlaces en el mismo grupo pueden considerarse como un enlace lógico con mayor ancho de banda.

Mediante la agregación, los puertos del 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 recíprocas y dinámicas para mejorar la confiabilidad del enlace.

3.1.4.1 Configuración estática

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

Figura 3-10 Interfaz de agregación



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

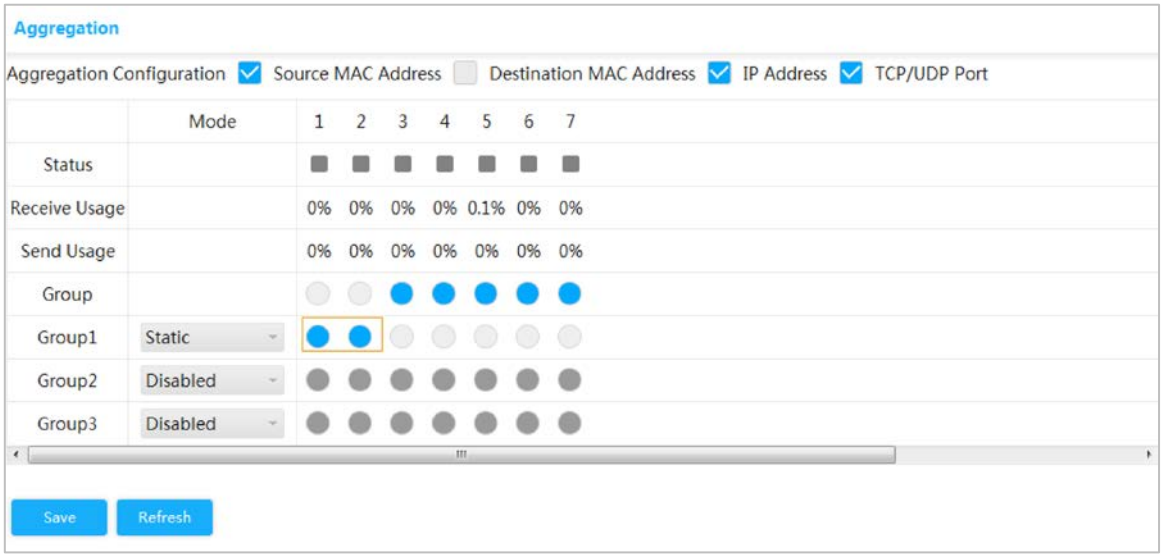
- Dirección MAC de origen: el algoritmo de equilibrio de carga de agregación basado en la dirección MAC.

- 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 Seleccionar**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.

En cuanto al conmutador PoE de 4 puertos, se pueden configurar como máximo 3 grupos de agregación estática al mismo tiempo.
tiempo. El grupo de agregación estática es diferente según los modelos de conmutador. El La interfaz real prevalecerá.

Figura 3-11 Configuración estática



Etapa 4 Hacer clic**Ahorrar**.

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

3.1.4.2 LACP

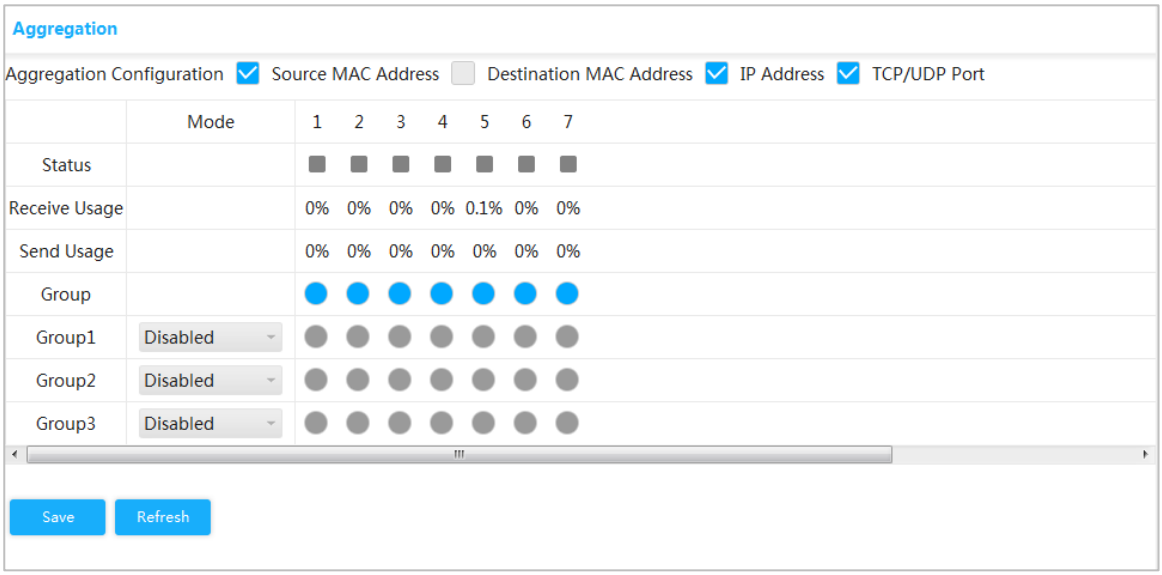
LACP (Protocolo de control de agregación de enlaces) es el protocolo para la agregación dinámica de enlaces. LACP se comunica con otro puerto a través de LACPDU (Unidad de datos del protocolo de control de agregación de enlaces).

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 paquetes LACPDU de forma activa. Después de recibir el paquete LACP enviado por el puerto opuesto, el puerto analiza el LACP.

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

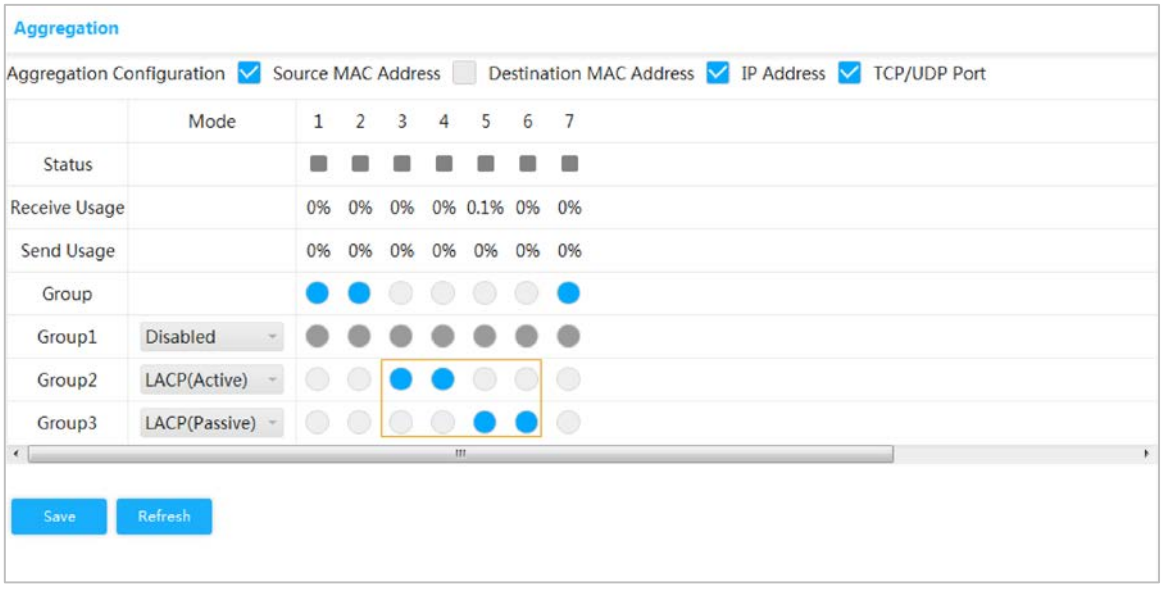
Figura 3-12 LACP (1)



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.

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.

Figura 3-13 LACP (2)



Etapa 4 Hacer clic**Ahorrar**.

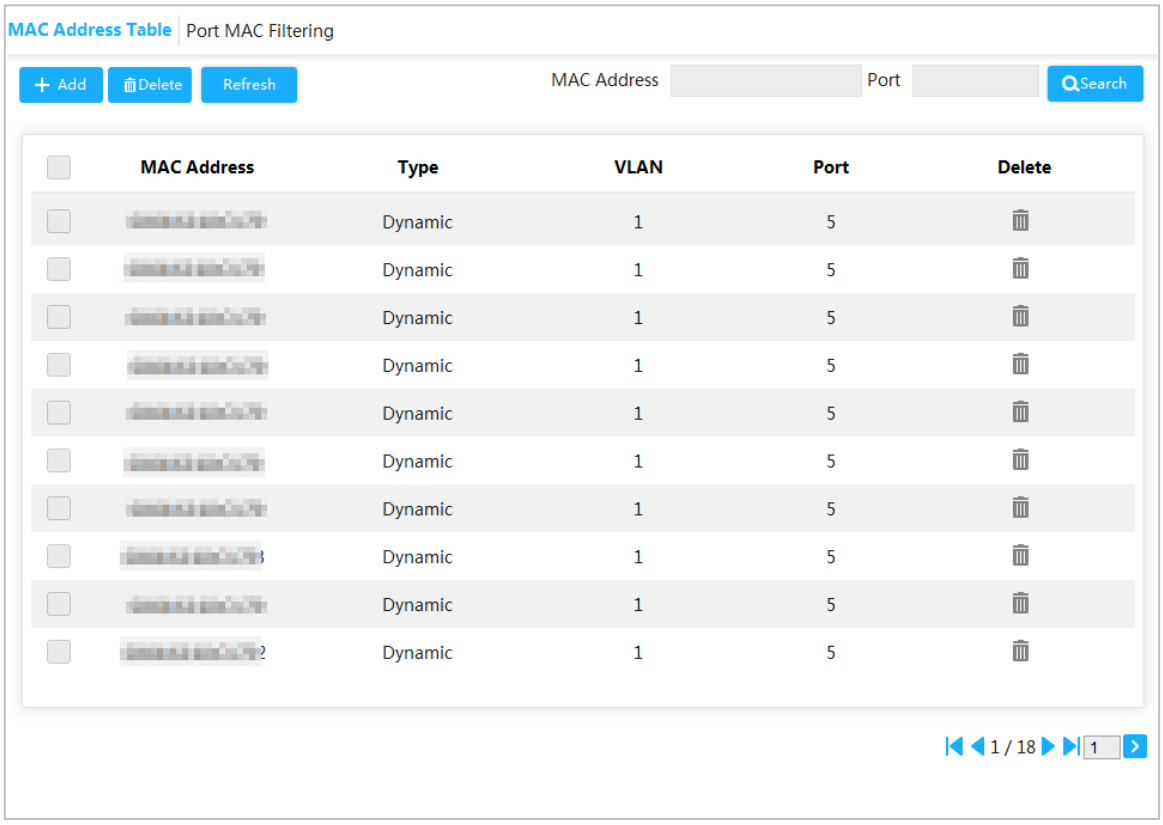
3.1.5 Tabla MAC

La tabla MAC (Control de acceso a medios) 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 reenvía 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 la dirección MAC de destino 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 Agregar tabla MAC estática

Paso 1 Seleccionar**Avanzado > Común > Tabla MAC > Tabla de direcciones MAC**.

Figura 3-14 Tabla de direcciones MAC



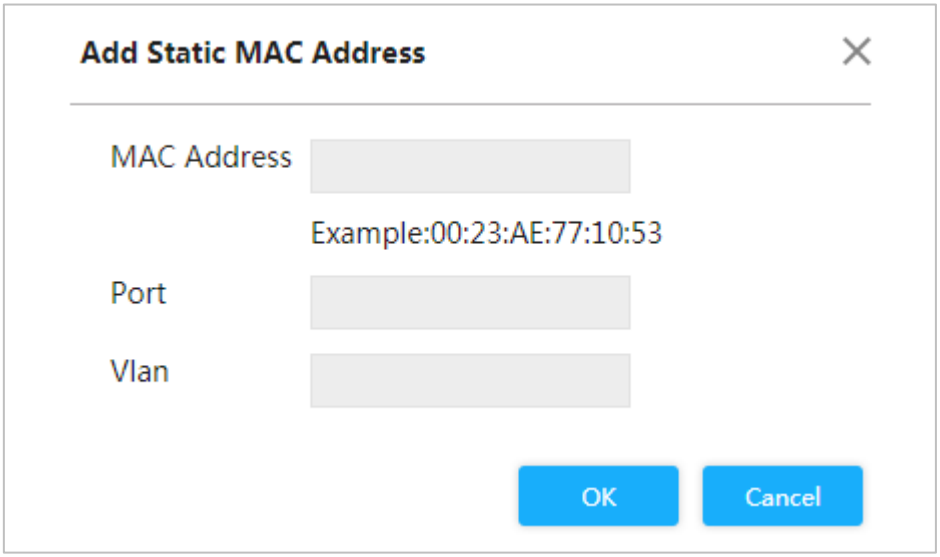
Paso 2 Vincule la dirección MAC al puerto en una VLAN determinada. Por ejemplo, vincule la dirección MAC 00:00:00:00:00:01 al puerto 3 en la VLAN 2.

1) Haga clic**Agregar**.

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

2) Configure la dirección MAC, el puerto y la VLAN.

Figura 3-15 Agregar una tabla MAC estática



3) Haga clic**DE ACUERDO**.

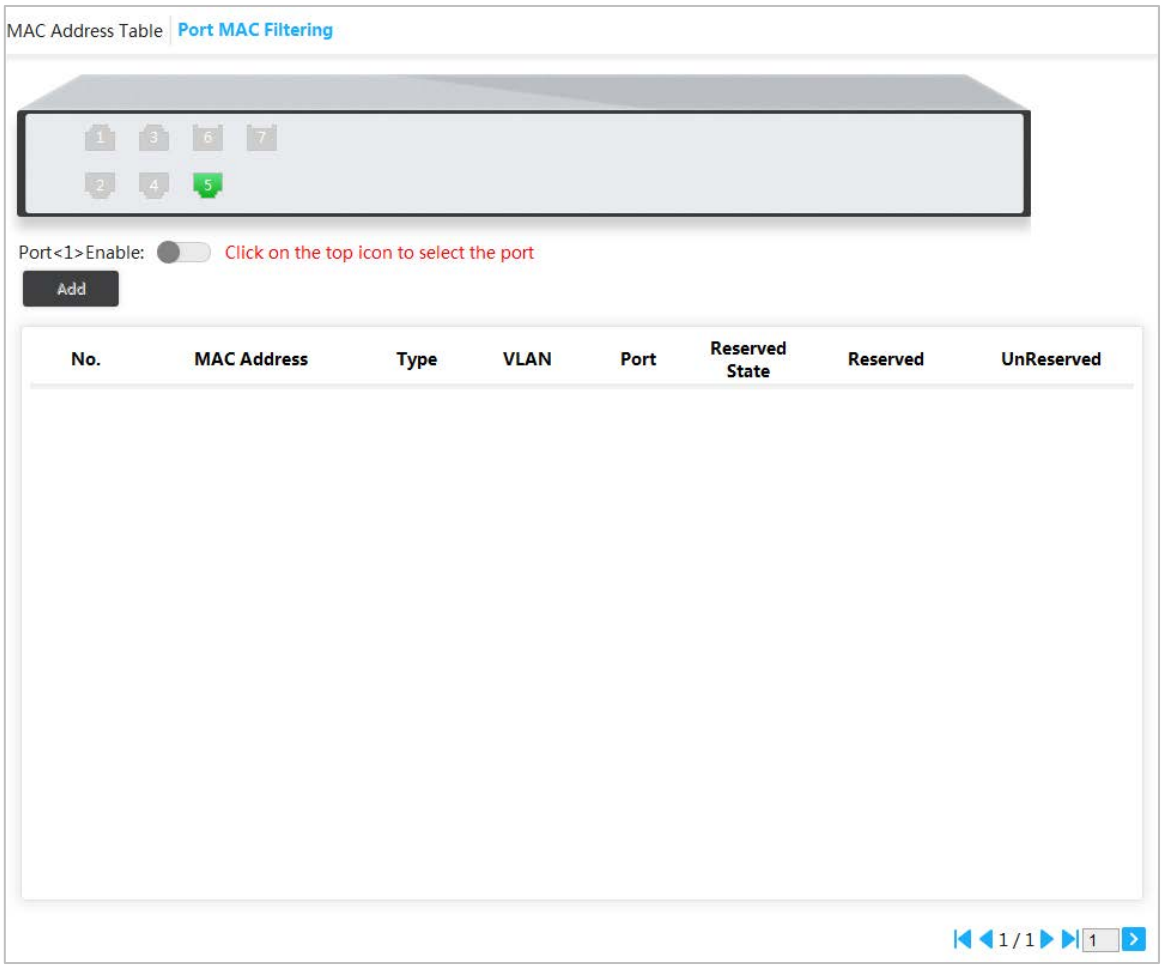
3.1.5.2 Filtrado de puerto MAC

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

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

Paso 1 Seleccionar**Avanzado > Común > Tabla MAC > Filtrado de puerto MAC**. El **Filtrado de puerto MAC**Se muestra la interfaz.

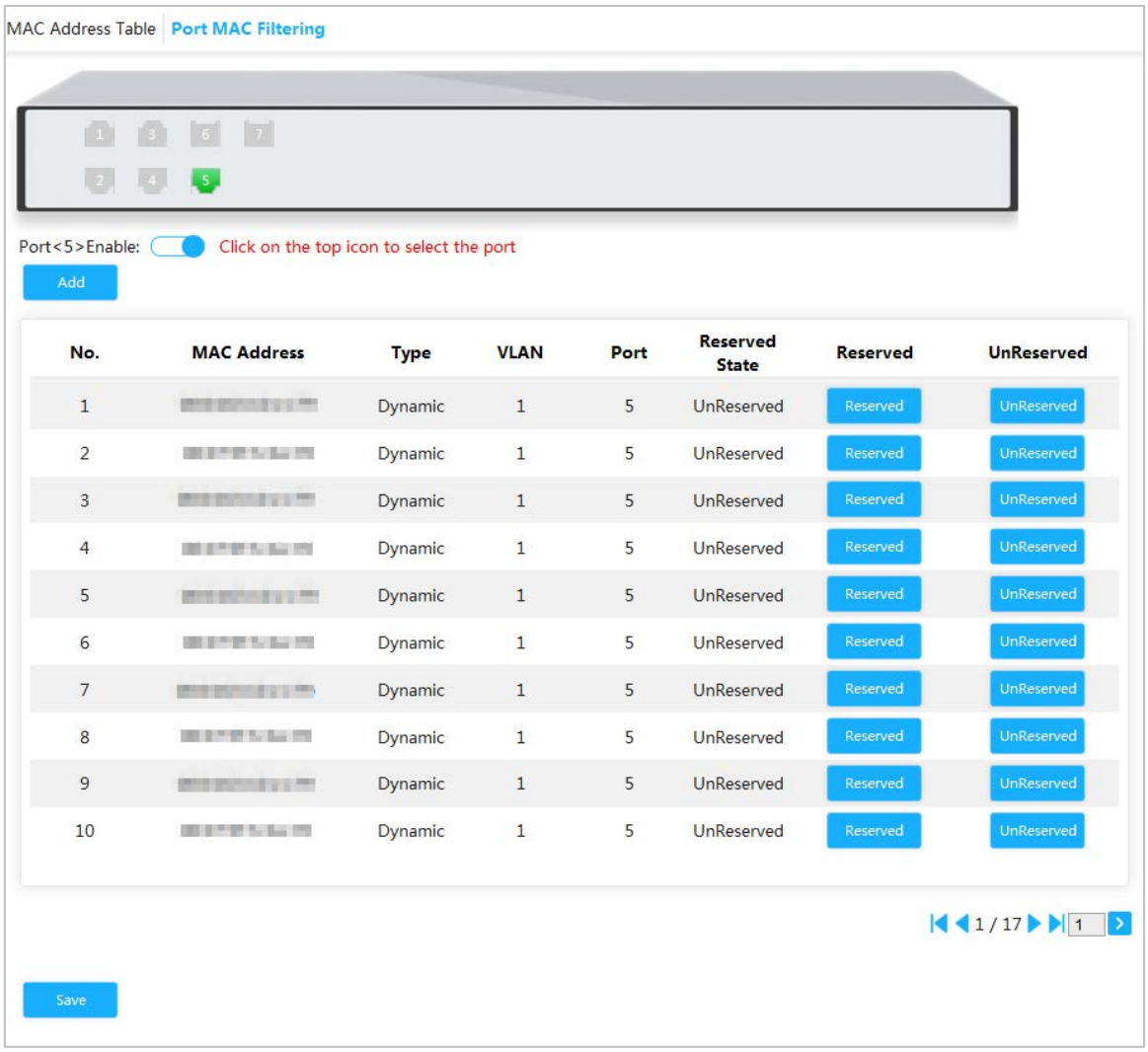
Figura 3-16 Filtrado de puerto MAC



Paso 2 Seleccione el puerto, como el puerto 5.

Paso 3 Hacer clic  detrás**Puerto <5> habilitado**para habilitar el puerto.

Figura 3-17 Habilitar el filtrado MAC del puerto



- Cambie el dispositivo MAC dinámico a estático.

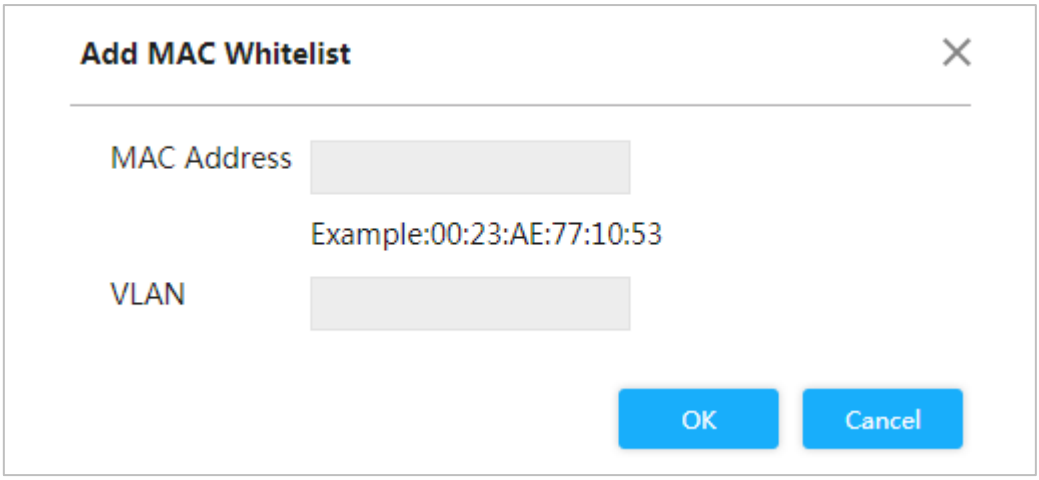
1) Seleccione un registro y haga clic**Reservado**.

2) Haga clic**Ahorrar**. El tipo cambia de**Dinámica**a**Estático**. Los dispositivos MAC estáticos pueden comunicarse con el puerto normalmente. Agregue la lista de

- permitidos de MAC.

1) Haga clic**Agregar**.

Figura 3-18 Agregar lista permitida de MAC



2) Configure la dirección MAC y VLAN.

3) Haga clic**DE ACUERDO**.

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

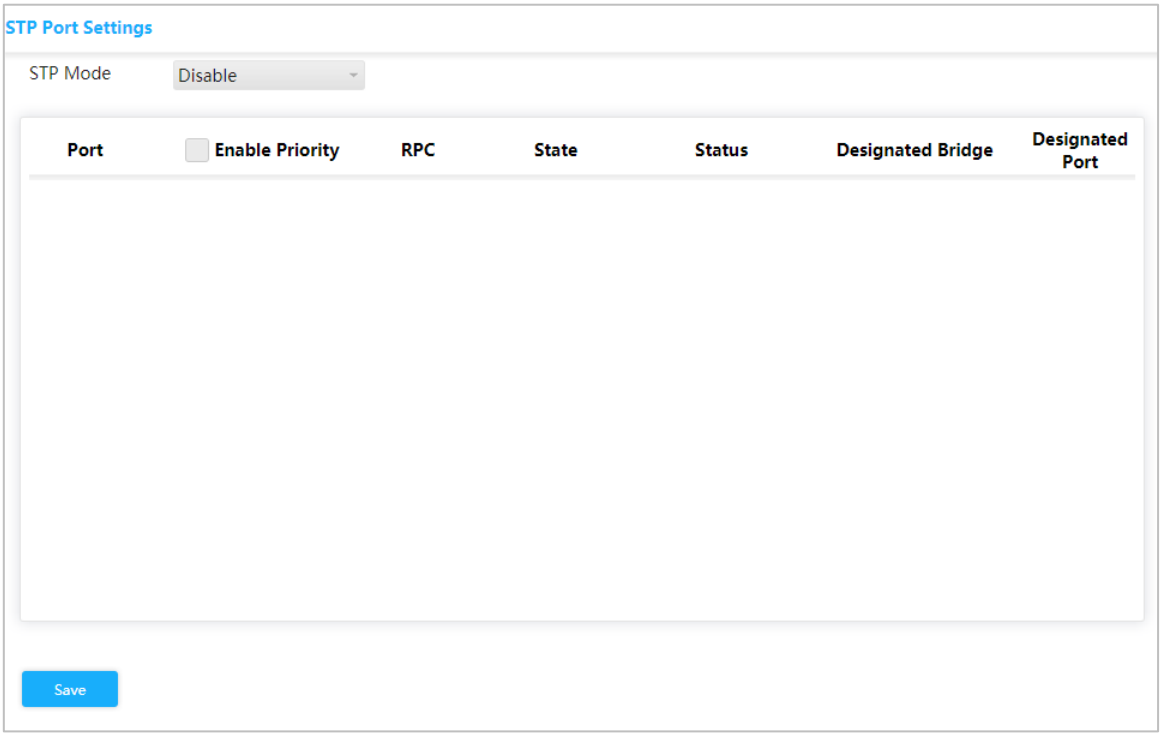
3.1.6 Árbol de expansión

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 realizar copias de seguridad de los enlaces.

Al igual que otros protocolos, el protocolo de árbol de expansión se actualiza con el desarrollo de la red: desde 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 Seleccionar**Avanzado > Común > Árbol de expansión > Configuración de puertos STP**.

Figura 3-19 Configuración de puertos STP



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

- **STP**: El protocolo de árbol de expansión más básico.
- **RSTP**: Mejorado en base a STP y logra una rápida convergencia de la topología de la red. **MSTP**:
- Soluciona los defectos de STP y RSTP. MSTP no sólo logra una convergencia rápida, 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**Ahorrar**, y los resultados son diversos según los diferentes modos.

Figura 3-20 PTS

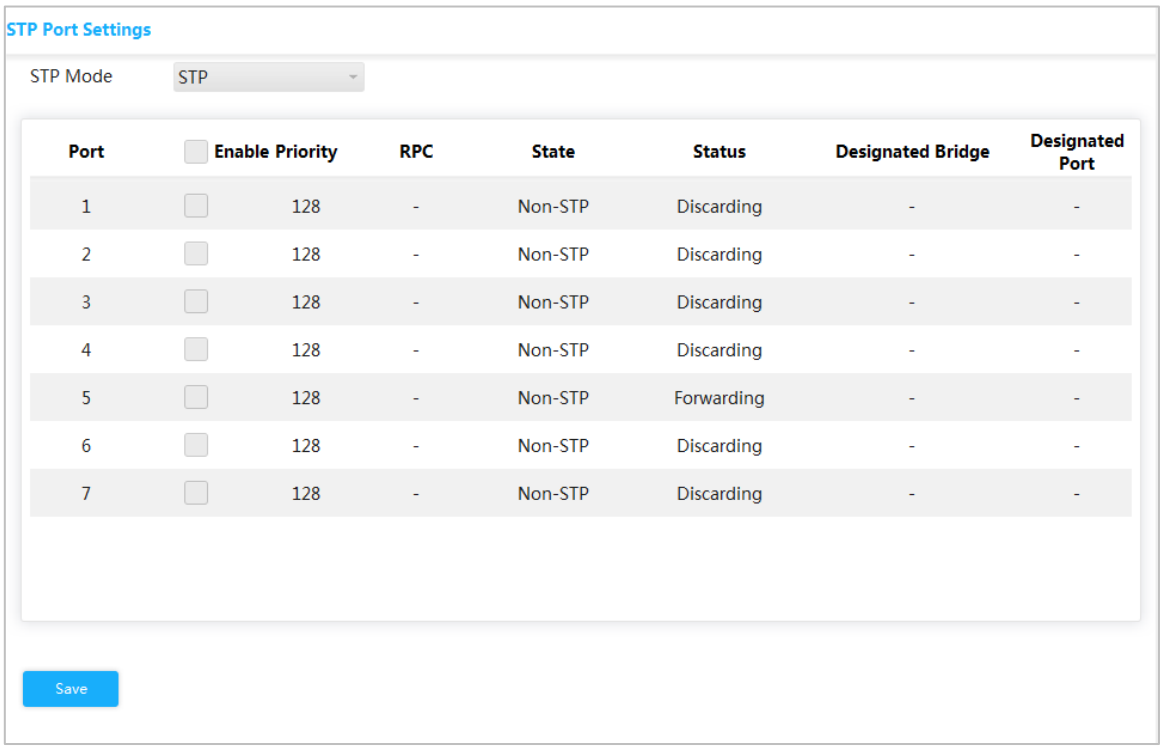


Figura 3-21 RSTP

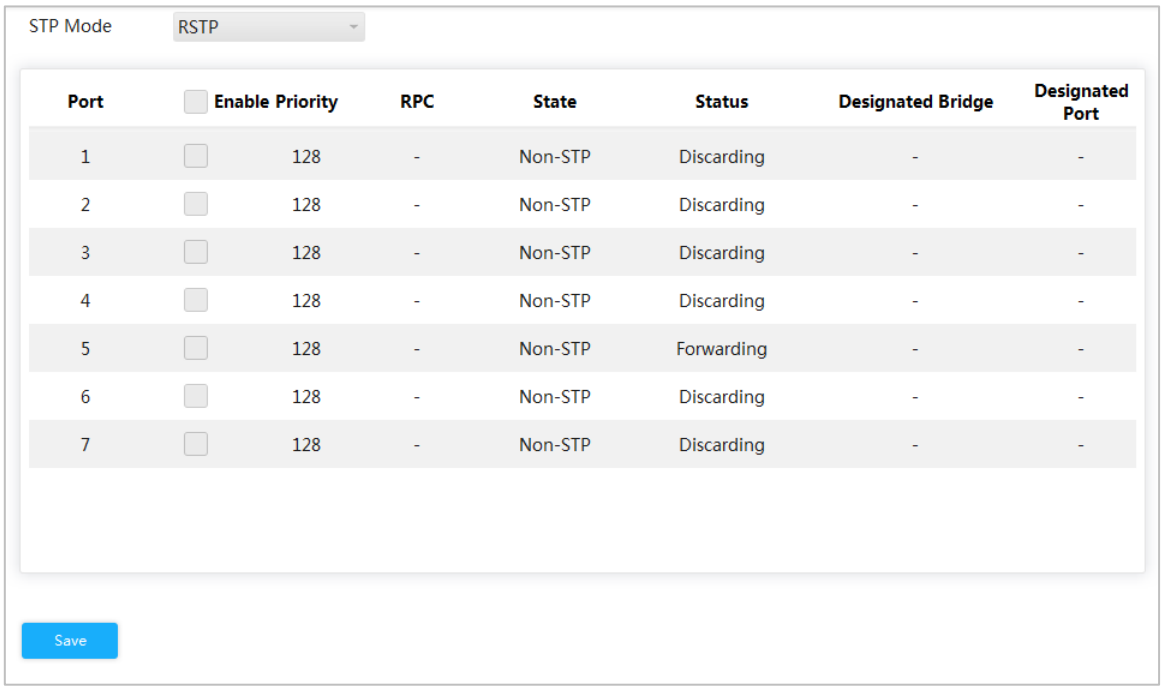
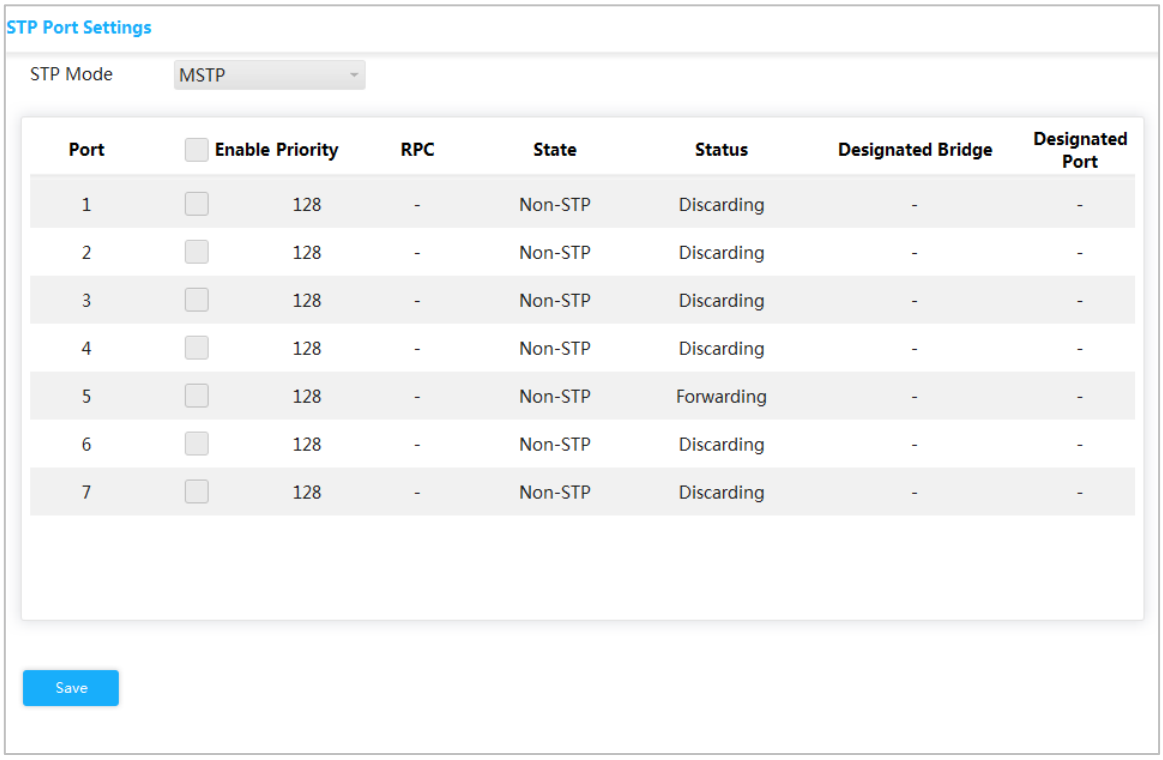
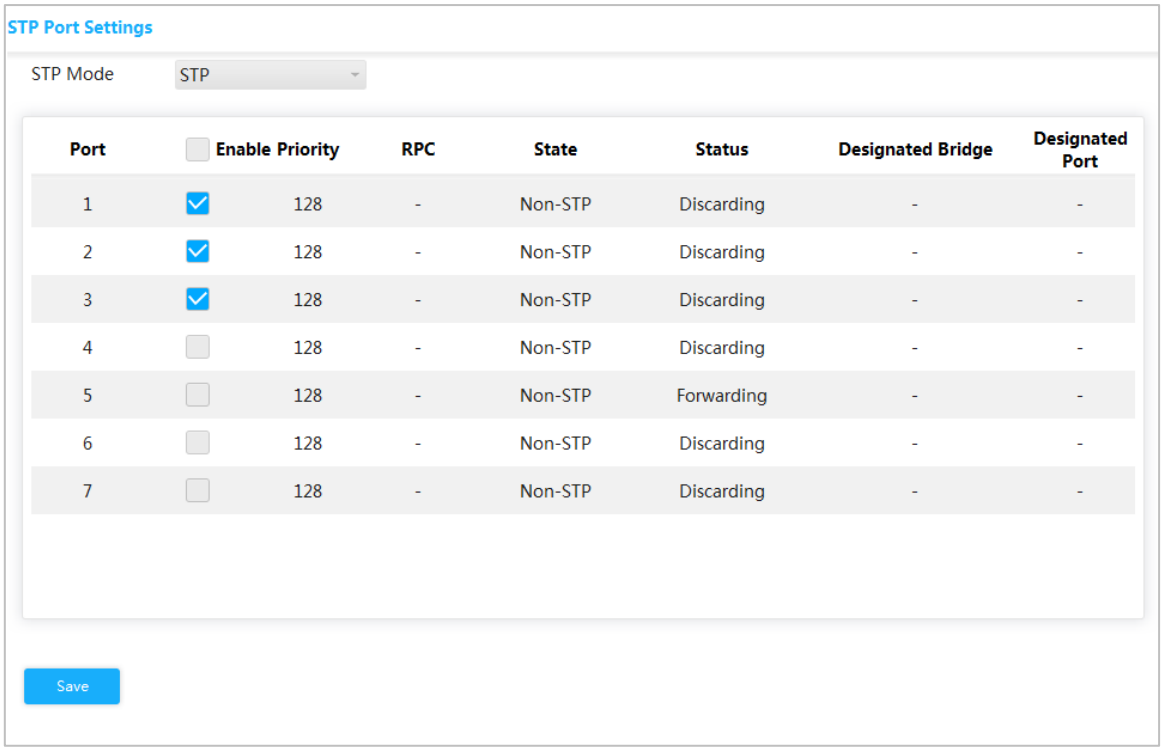


Figura 3-22 MSTP



Etapa 4 Seleccione al menos 3 puertos para combinar un rastreo STP/RSTP/MSTP. Por ejemplo: el puerto 1, el puerto 2 y el puerto 3 combinan un rastreo STP.

Figura 3-23 Vigilancia STP



Paso 5 Hacer clic**Ahorrar**.

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

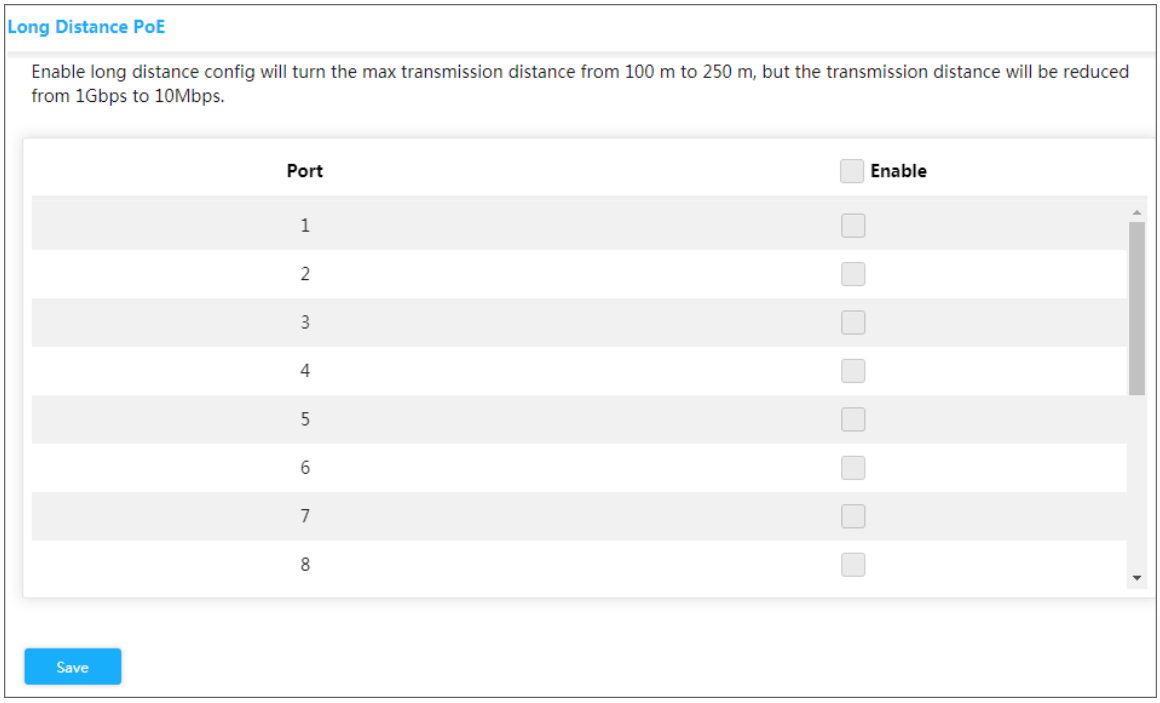
3.1.7 PoE de larga distancia

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

Los conmutadores Ethernet que no son PoE no admiten esta función.

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



3.2 Configuraciones poco utilizadas

3.2.1 ERPS

ERPS (Ethernet Ring Protection Switching) es el estándar de protocolo de prevención de bucles de capa 2 definido por ITU-T, y el número de 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). La UIT-T lanzó la V1 en junio de 2008 y la UIT-T lanzó la V2 en agosto de 2010. La V2 es compatible con la V1 y agrega las siguientes funciones:

- Redes multianillo incluyendo anillo cruzado.
- Paquete RAPS de conmutación de subanillo por canal virtual o canal no virtual. Cambiar
- bloques de forma forzada y manual.
- El interruptor inverso ERPS es configurable.

Sólo algunos modelos de conmutadores admiten ERPS.

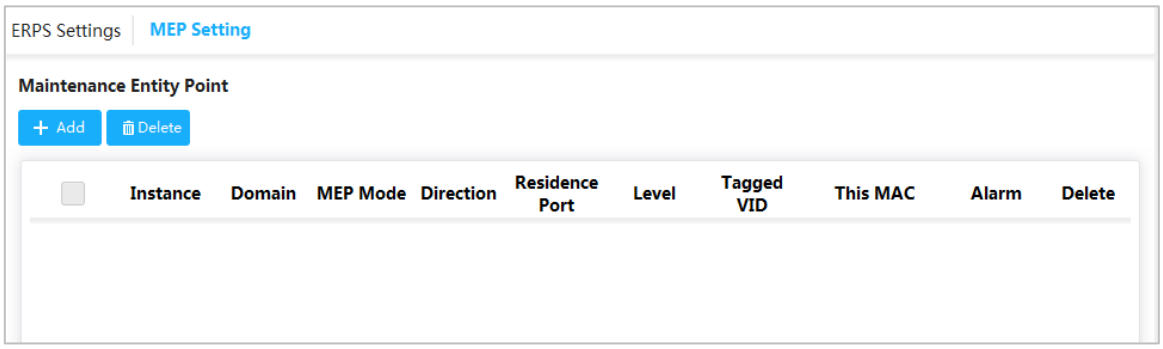
3.2.1.1 Configuración MEP

MEP (Punto de Entidad de Mantenimiento) es parte de ERPS.

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

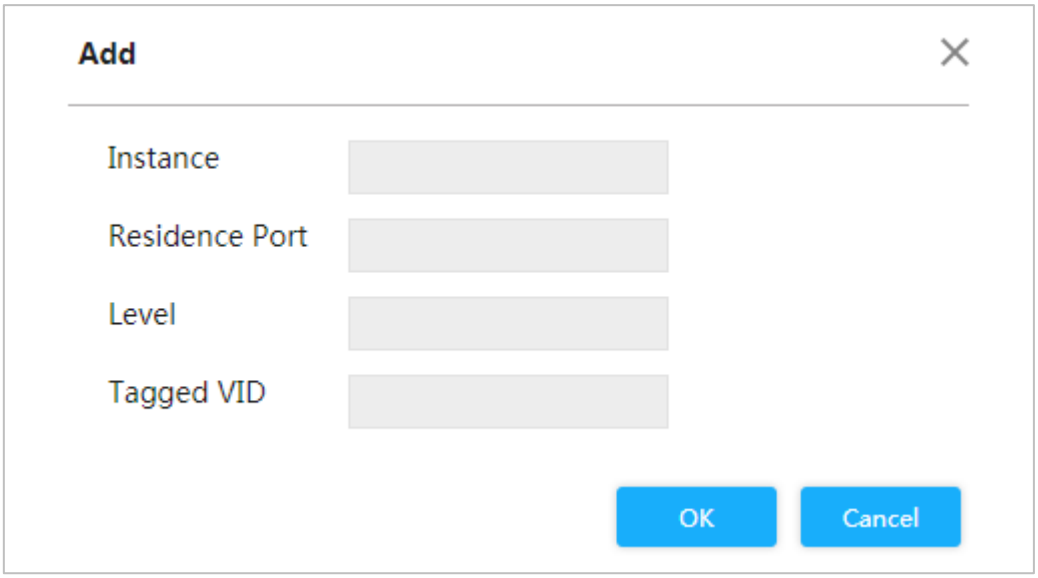
Paso 1 Seleccionar**Avanzado > Usado poco > ERPS > Configuración MEP**.

Figura 3-25 Configuración MEP



Paso 2 Hacer clic**Agregar**.

Figura 3-26 Agregar



Paso 3 Configure los parámetros.

Tabla 3-5 Parámetros MEP

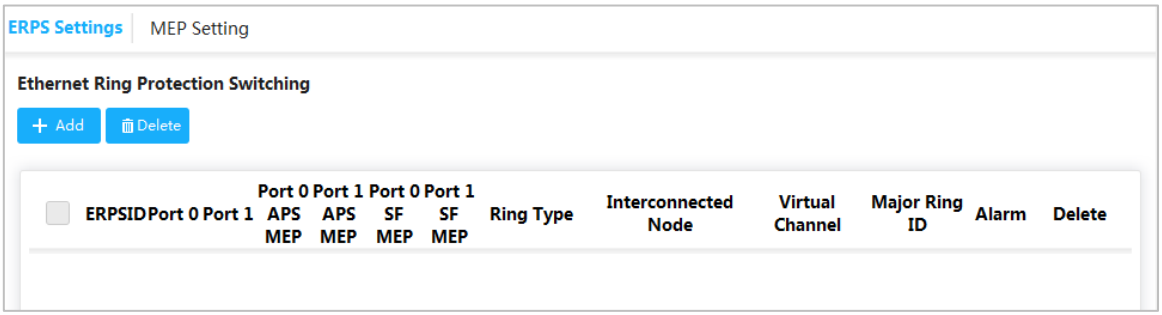
Parámetro	Descripción
Instancia	Ingrese el número de instancia MEP, como 1.
Puerto residencial	Ingrese el número de puerto al que pertenece MEP, como Puerto 1.
Nivel	Nivel de mantenimiento. Se recomienda configurarlo en 0.
Etiquetado VID	Ingrese el protocolo VLAN, como VLAN 3.

Etapa 4 Hacer clic**DE ACUERDO**.

3.2.1.2 Configuración ERPS

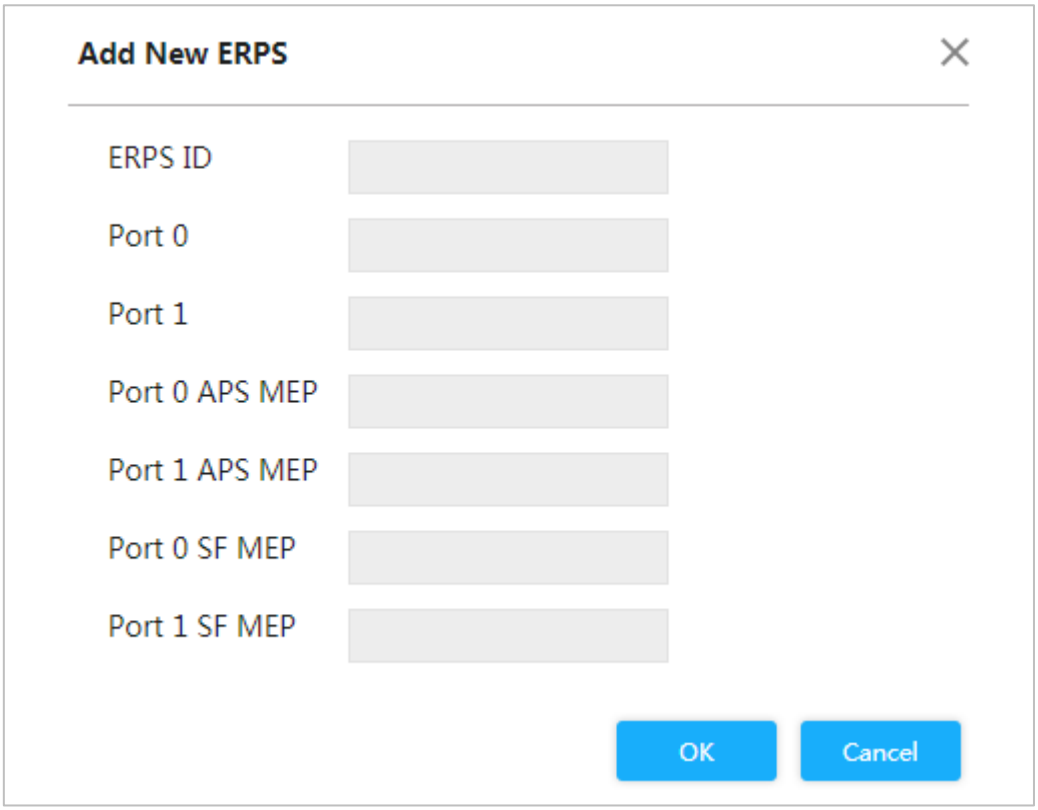
Paso 1 Seleccionar**Avanzado > Usado poco > ERPS > Configuración de ERPS**.

Figura 3-27 Configuración de ERPS



Paso 2 Hacer clic**Agregar**.

Figura 3-28 Agregar ERPS



Paso 3 Configure los parámetros.

Tabla 3-6 Parámetros ERPS

Parámetro	Descripción
ID de ERPS	El número de identificación de ERPS.
Puerto 0	Los dos puertos agregados al ERPS.
Puerto 1	
Puerto 0 APS eurodiputado	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: el puerto 0 APS MEP es 1 y el puerto 1 APS MEP es 2.
Puerto 1 APS eurodiputado	
Puerto 0 SF MEP	El MEP de inspección de agregación correspondiente 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: el puerto 0 SF MEP es 1 y el puerto 1 SF MEP es 2.
Puerto 1 SF eurodiputado	

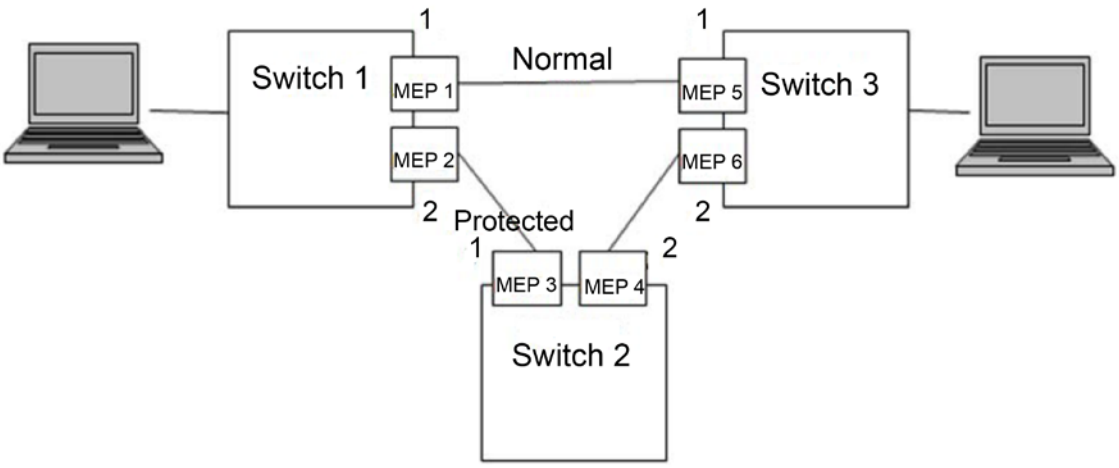
Etapa 4 Hacer clic**DE ACUERDO**.

3.2.1.3 Ejemplo: Configuración de anillo único 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; Switch 3: MEP 5 y MEP 6.

Figura 3-29 Configuración de anillo único ERPS



Configuración

Configure el ERPS con las siguientes ideas:

1) Confirme la topología y planifique la VLAN de protección y el protocolo VLAN.

2) Confirme el puerto propietario de RPL.

3) Asegúrese de desactivar la función mutex de los puertos.

4) Configuración de VLAN

5) Crear eurodiputado.

6) Crear ERPS y configurar la VLAN de control y la 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 como puerto propietario de RPL. Asegúrese de desactivar la función mutex de los puertos, incluida la función STP y la función LLDP.

Las configuraciones del conmutador son las siguientes:

Paso 1 Configure la VLAN de protección y el protocolo VLAN son 2 y 3 por separado. 1) Seleccionar**Avanzado > Común > Configuración de VLAN**.

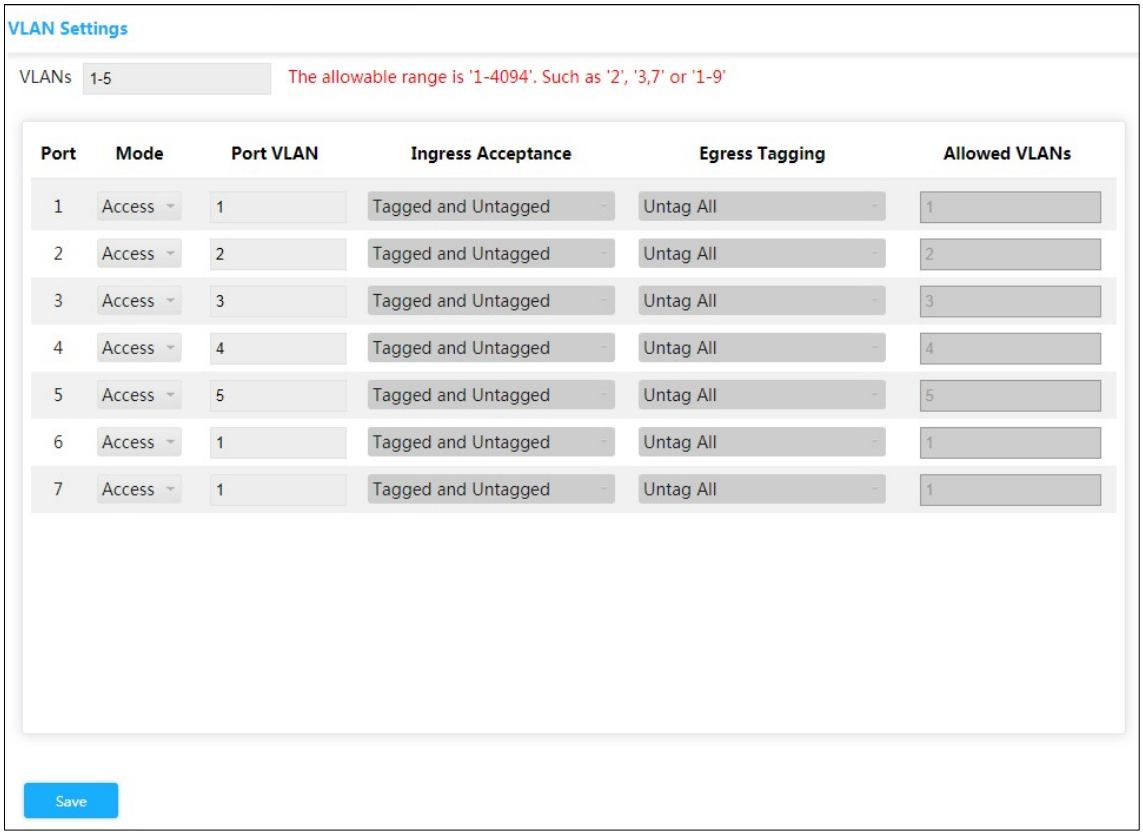
2) Configure el modo del puerto 1 y del puerto 2 para que sea**Trompa**. Consulte la Figura 3-30.

3) Configure la VLAN del puerto 1 y el puerto 2 en 1.

4) Configure la VLAN permitida en 2 y 3.

5) Haga clic**Ahorrar**.

Figura 3-30 Agregar el puerto 1 y el puerto 2 a la VLAN 1



Paso 2 Crear MEP1 y MEP 2

1) Seleccionar**Avanzado > Usado poco > ERPS > Configuración MEP**.

2) Haga clic**Agregar**.

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

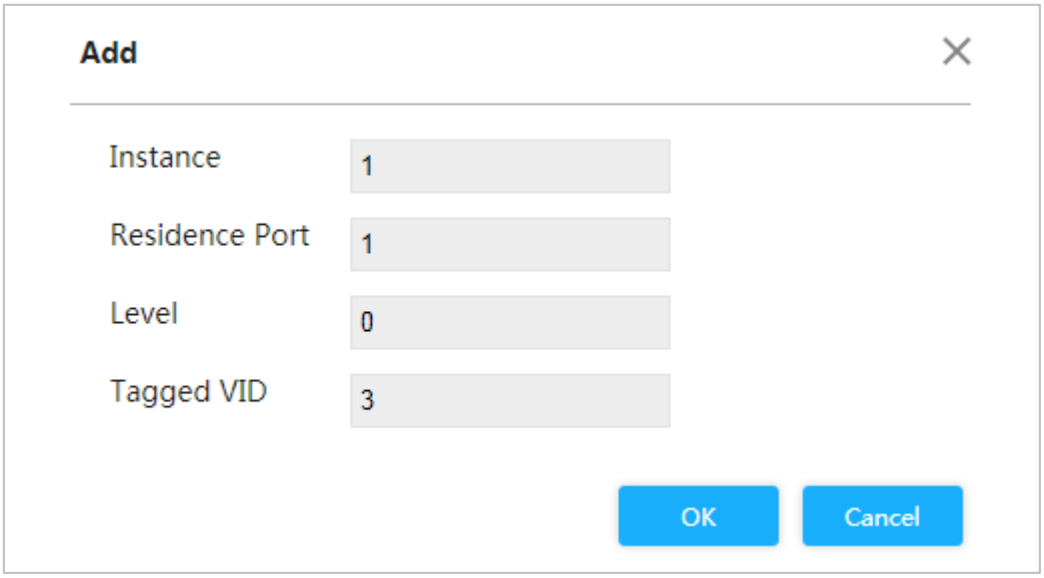
4) Establezca el Puerto de residencia en 1.

5) Establezca el nivel en 0.

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

7) Haga clic**DE ACUERDO**.

Figura 3-31 Agregar MEP



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**1**y**2**por separado bajo**Instancia**para ingresar a la interfaz de configuración. Modifique la ID del MEP y agregue la ID del par.

Figura 3-32 Configurar el ID del par de MEP 1

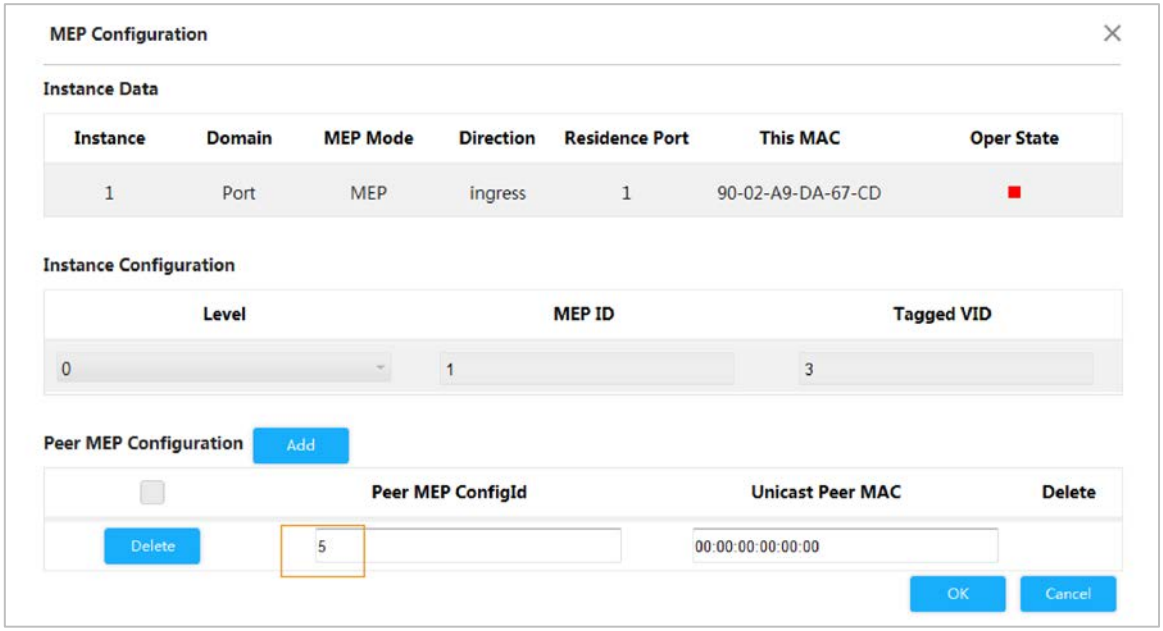
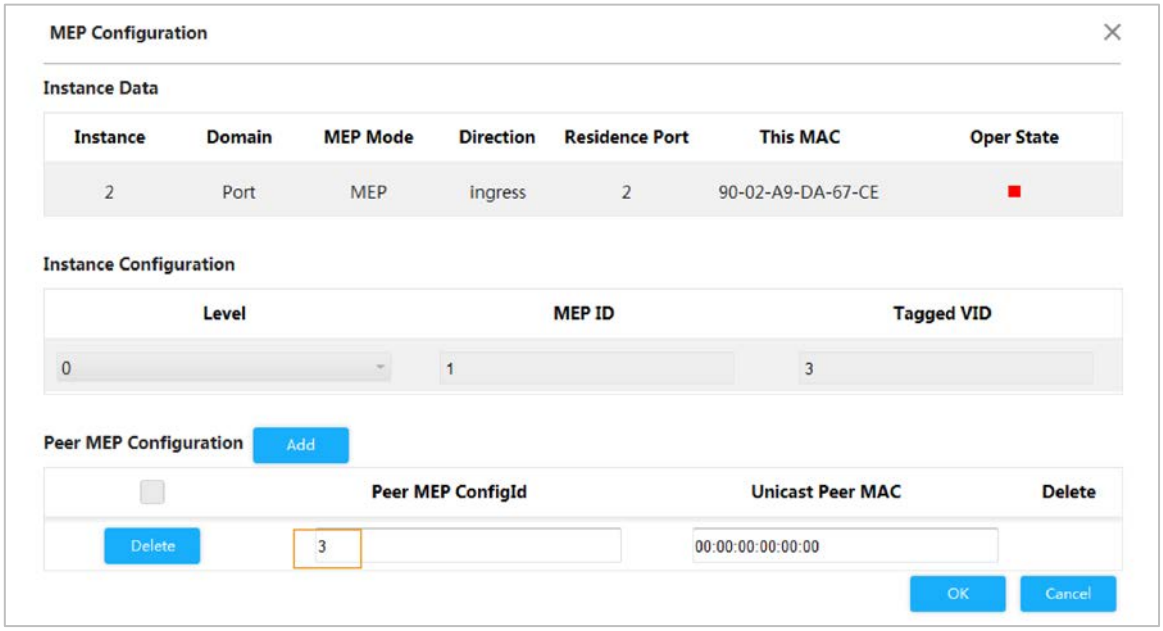


Figura 3-33 Configurar el ID del par de MEP 2



Etapa 4 Hacer clic**DE ACUERDO**.

Paso 5 Crear ERPS.

1) Seleccionar**Avanzado > Usado poco > ERPS > Configuración de ERPS**. El **Configuración ERPS**Se muestra la interfaz.

2) Haga clic**Agregar**. El**Agregar nuevo ERPS**Se muestra la interfaz.

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

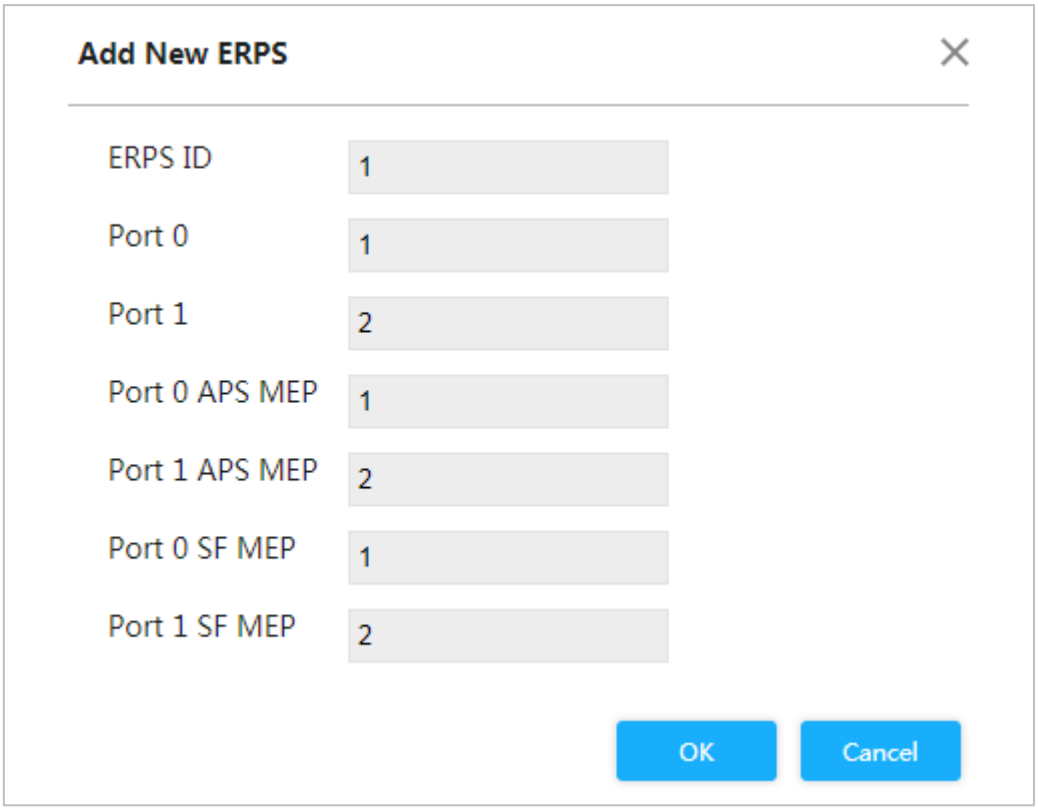
4) Configure el Puerto 0 como 1 y el Puerto 1 como 2.

5) Configure el Puerto 0 APS MEP en 1 y el Puerto 1 APS MEP en 2.

6) Configure el Puerto 0 SF MEP como 1 y el Puerto 1 SF MEP como 2.

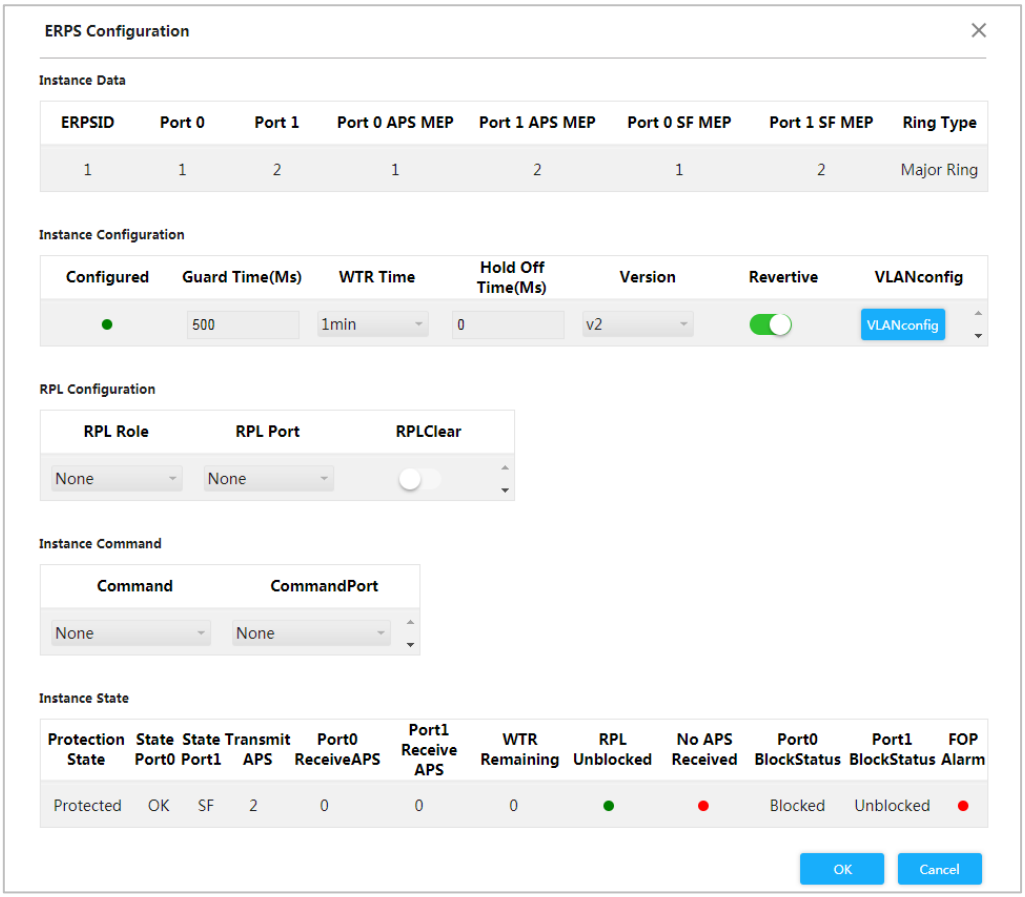
7) Haga clic**DE ACUERDO**.

Figura 3-34 Agregar ERPS



Paso 6 Hacer clic**1**bajo**ERPSID**para ingresar a la interfaz de configuración.

Figura 3-35 Configuración de ERPS



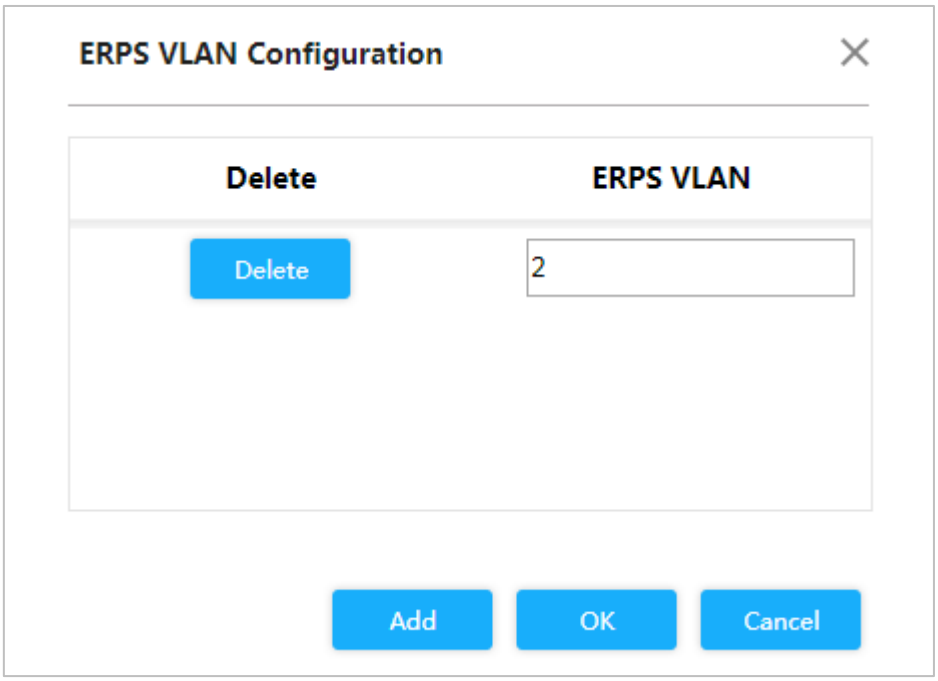
1) Haga clic**VLANconfig**.

2) Haga clic**Agregar**.

3) Configure ERPS VLAN en 2. Consulte la Figura 3-36.

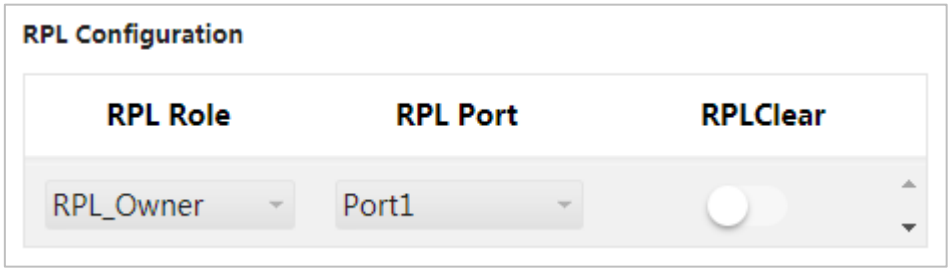
4) Haga clic**DE ACUERDO**.

Figura 3-36 Configuración de VLAN de ERPS



5) Configure el puerto 2 del conmutador 1 como propietario de RPL en Configuración de RPL.

Figura 3-37 Configuración del puerto propietario

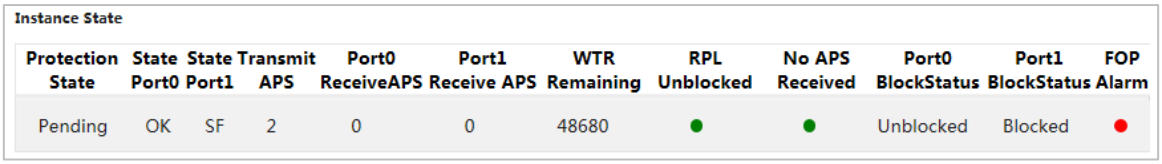


Paso 7 Hacer clic**DE ACUERDO**.

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 ERPS**interfaz.

Figura 3-38 Estado de instancia



3.2.2 LCA

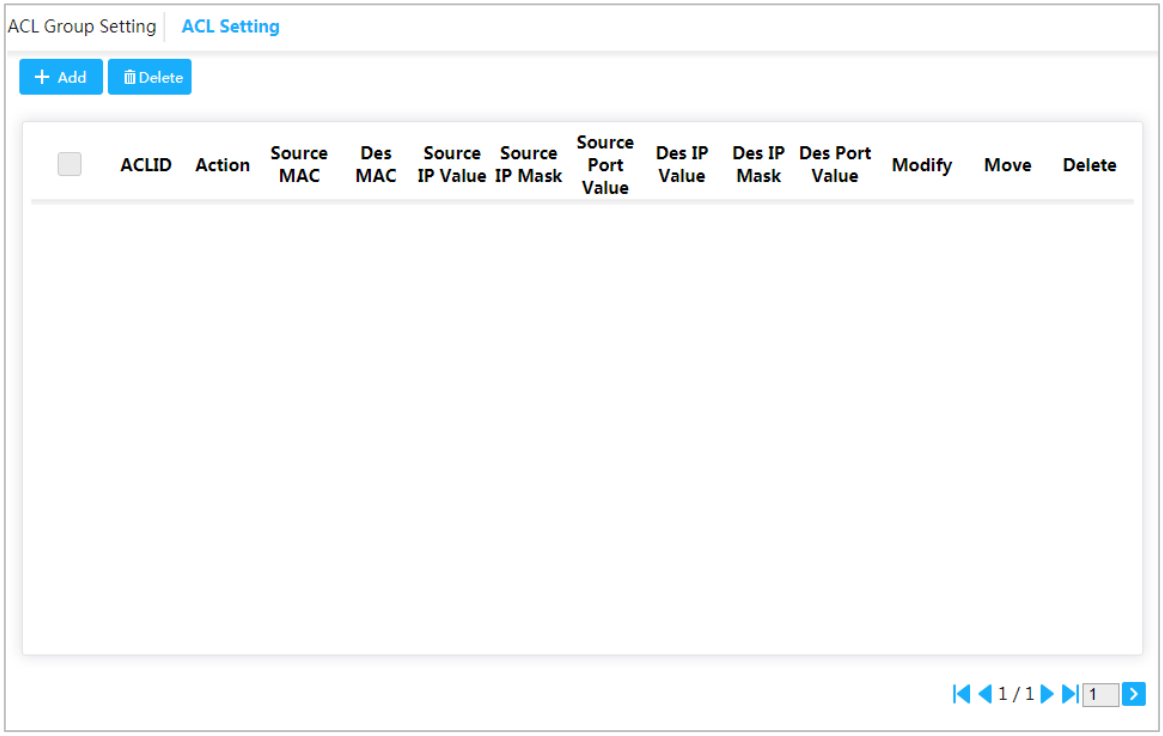
ACL (Lista de control de acceso) es para la identificación de flujo. Para filtrar el paquete, el dispositivo de red necesita configurar una serie de condiciones coincidentes para clasificar los paquetes. Las condiciones pueden ser la dirección de origen, la dirección de destino y el número de puerto 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 una vez identificado el paquete específico, se permite o prohíbe el paso del paquete según la regla preestablecida.

3.2.2.1 Configuración de ACL

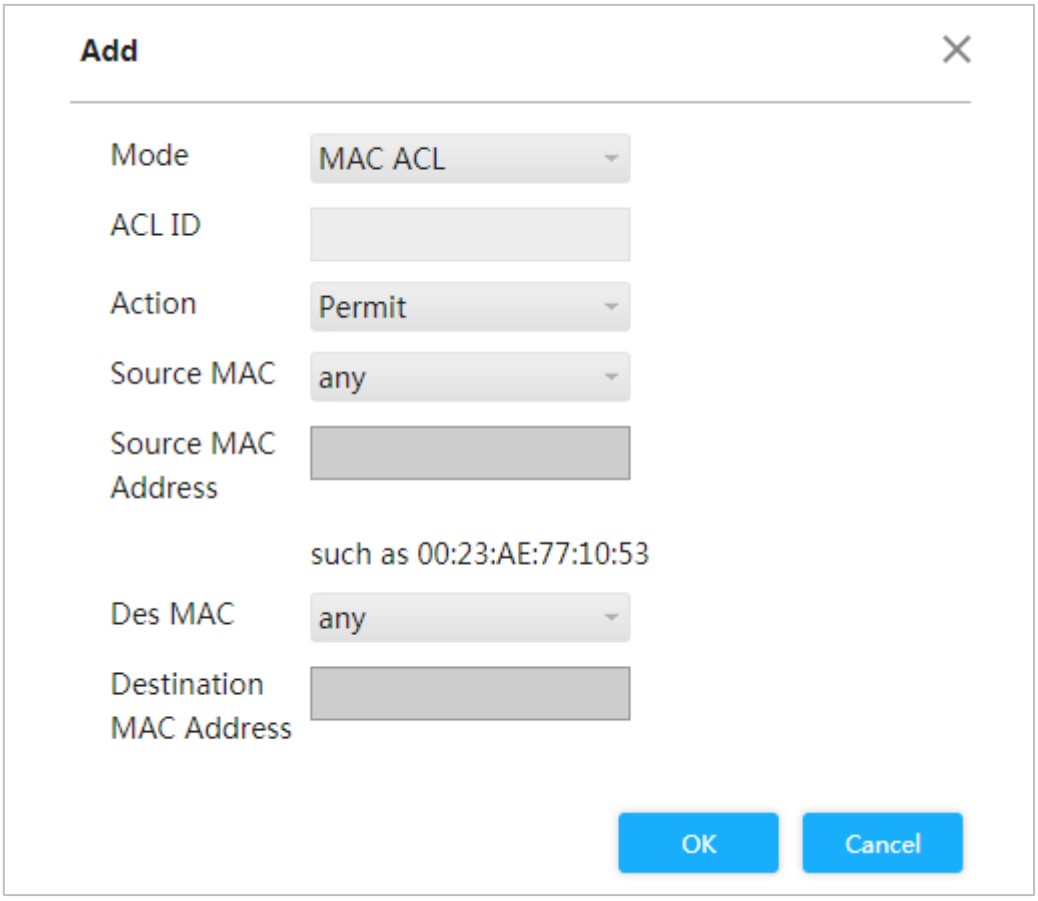
Paso 1 Seleccionar**Avanzado > Usado poco > ACL > Configuración de ACL**. El **Configuración de ACL**Se muestra la interfaz.

Figura 3-39 Configuración de ACL



Paso 2 Hacer clic**Agregar**.

Figura 3-40 Agregar



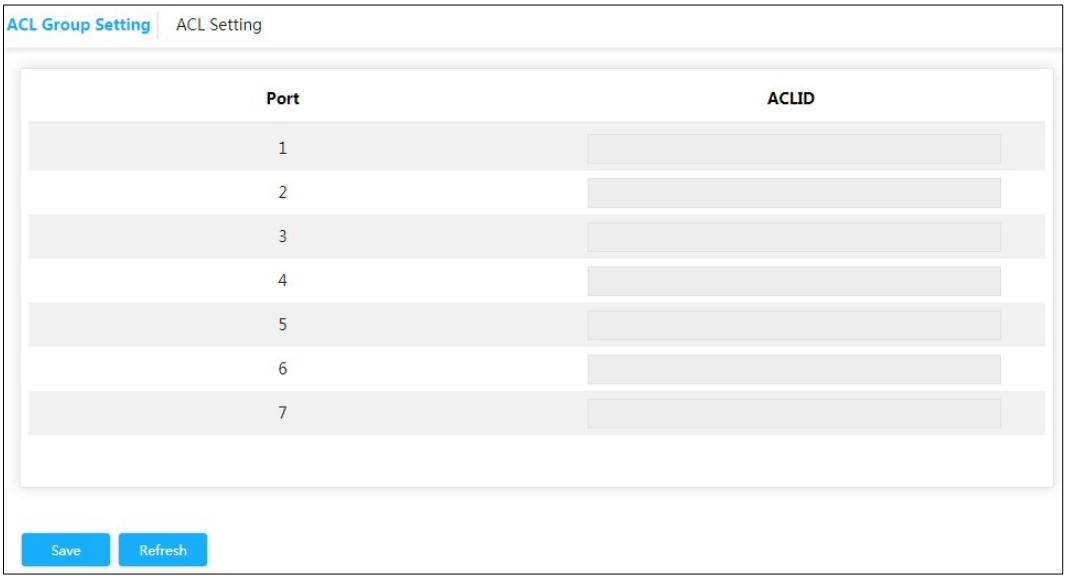
Paso 3 Configure la ID de ACL y el rango es 1–128. Hacer clic**DE**

Etapa 4 **ACUERDO**.

3.2.2.2 Configuración del grupo ACL

Paso 1 Seleccionar**Avanzado > Usado poco > ACL > Configuración de grupo de ACL**.

Figura 3-41 Configuración del grupo ACL



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

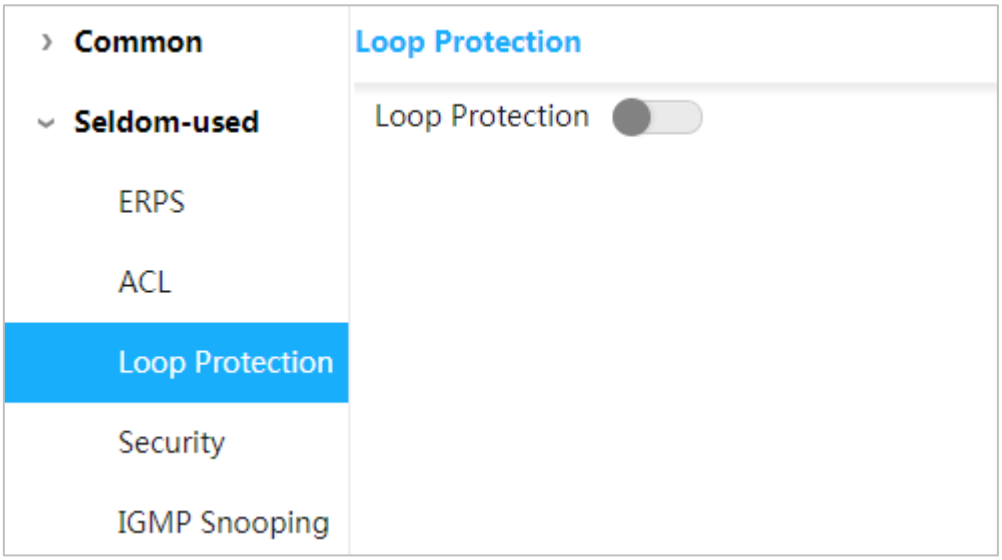
Paso 3 **Ahorrar**.

3.2.3 Protección de bucle

Detecta el bucle entre los puertos. Una vez que el dispositivo haya detectado el bucle, lo romperá. Paso 1

Seleccionar**Avanzado > Usado poco > Protección de bucle**.

Figura 3-42 Protección de bucle



Paso 2 Hacer clic  para habilitar la protección de bucle

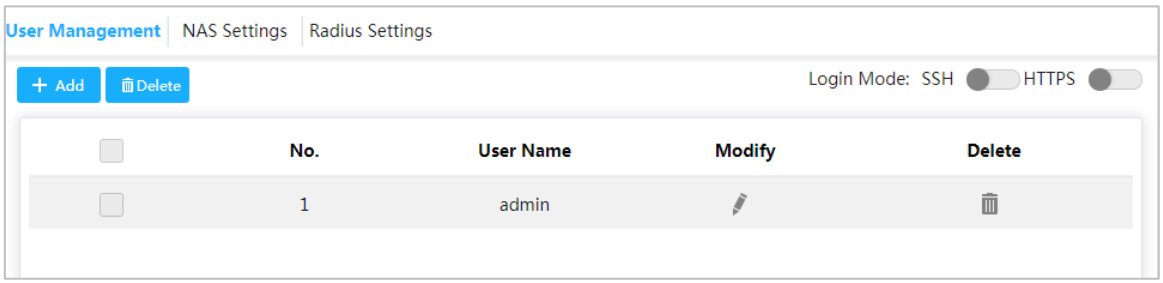
3.2.4 Seguridad

3.2.4.1 Gestión de usuarios

Puede agregar, editar y eliminar el usuario.

Seleccionar**Avanzado > Poco utilizado > Seguridad > Gestión de usuarios**.

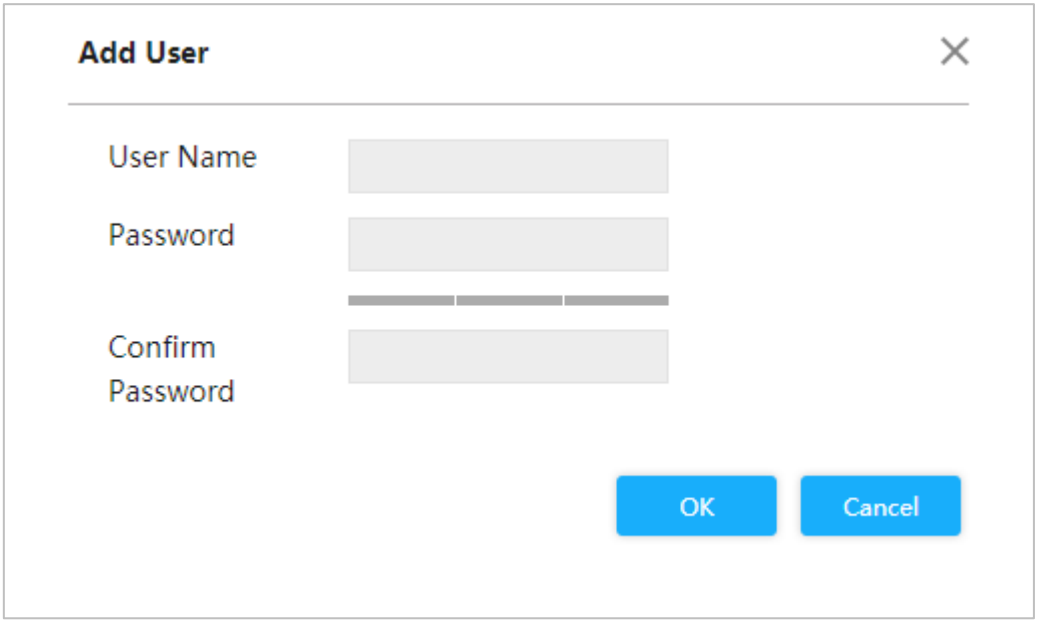
Figura 3-43 Gestión de usuarios



Agregar usuario

Paso 1 Hacer clic**Agregar**.

Figura 3-44 Agregar usuario

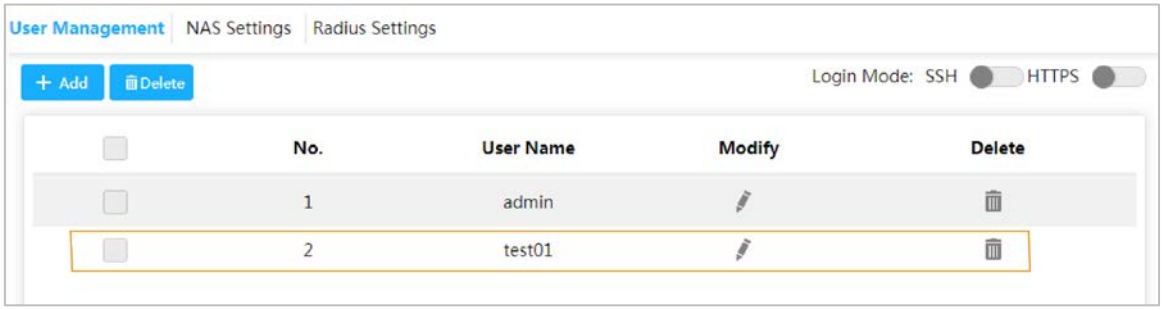


Paso 2 Ingrese el nombre de usuario, la contraseña y confirme la contraseña. La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' "; : &). Por ejemplo, agregue el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

Paso 3 Hacer clic**Ahorrar**.

Se agrega la nueva prueba de usuario 01.

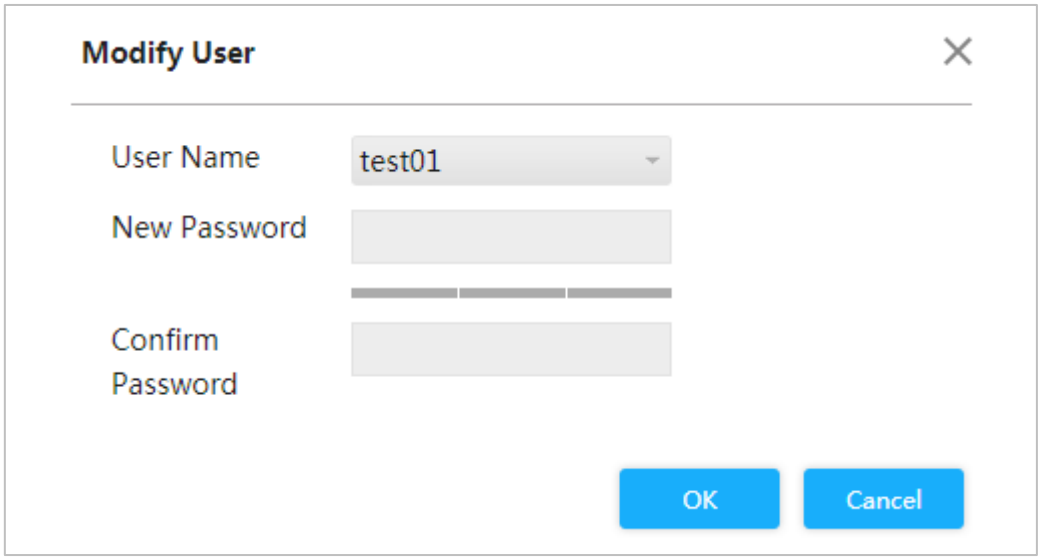
Figura 3-45 Nuevo usuario agregado



Modificar y eliminar usuario

- Hacer clic , y luego el**Modificar usuario**Se muestra la interfaz.

Figura 3-46 Modificar usuario



- Hacer clic para eliminar al 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. Integrado en la web Netscape Navigator, proporciona

comunicación de autenticación y cifrado. Se aplica ampliamente en la World Wide Web para comunicaciones sensibles a la seguridad. Por ejemplo, proteja la seguridad de la cuenta y la información del usuario.

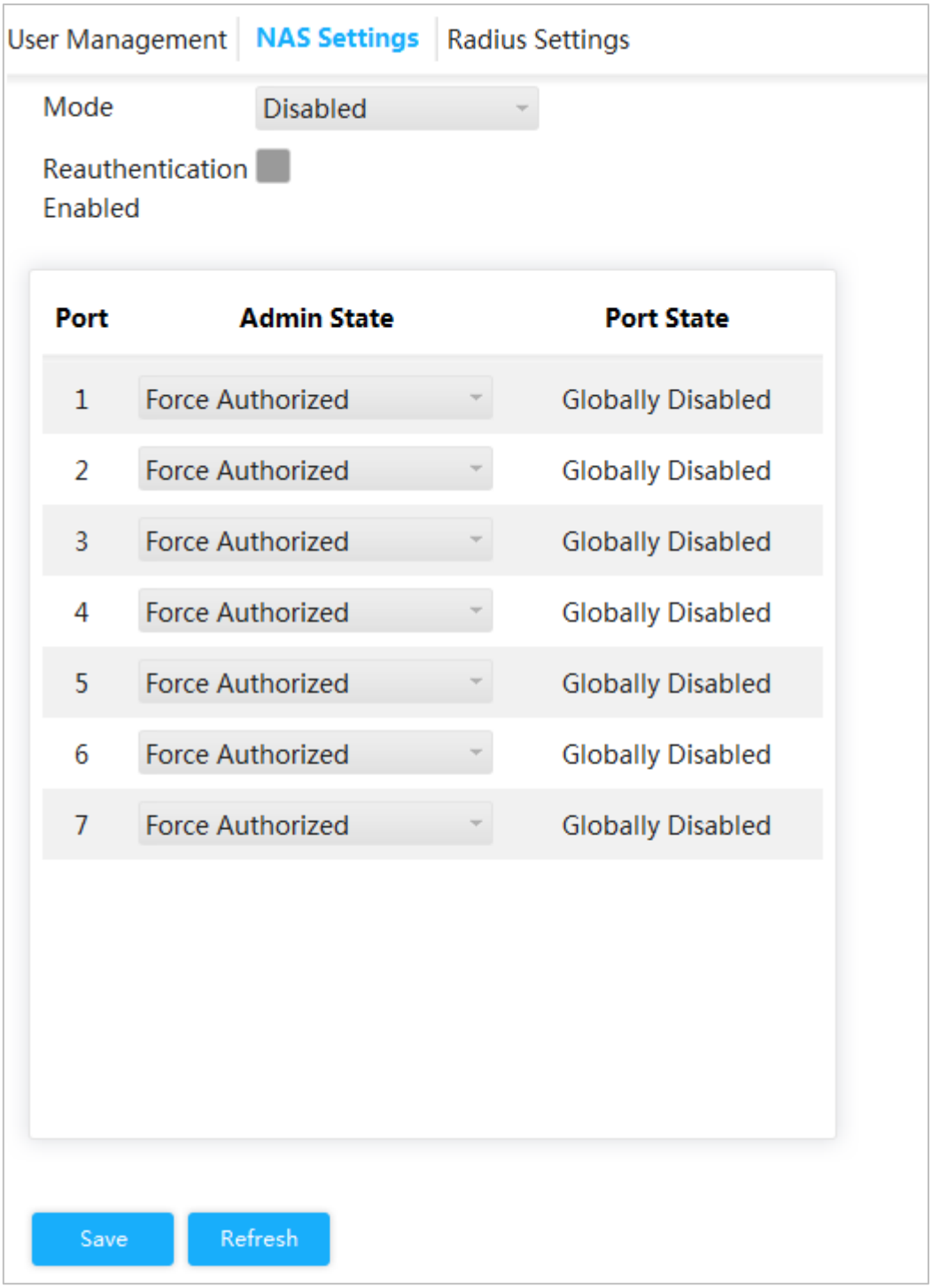
Hacer clic correspondiente a HTTPS en la esquina superior derecha de la**Gestión de usuarios**interfaz para habilitar el servicio HTTPS.

3.2.4.2 Configuración NAS

NAS (Network Access Server) es un servidor que permite al ISP proporcionar un servicio de acceso a Internet. Paso 1

Seleccionar**Avanzado > Usado poco > Seguridad > Configuración NAS**. El **Configuración del NAS**Se muestra la interfaz. Consulte la Figura 3-47.

Figura 3-47 Configuración NAS



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

Paso 3 el**Reautenticación habilitada**casilla para habilitar la reautenticación.

Etapa 4 Establecer estado de administrador: Forzar autorización, Forzar no autorizada, autenticación basada en puerto 802.1X o basada en MAC.

Paso 5 Hacer clic**Ahorrar**.

3.2.4.3 Configuración del radio

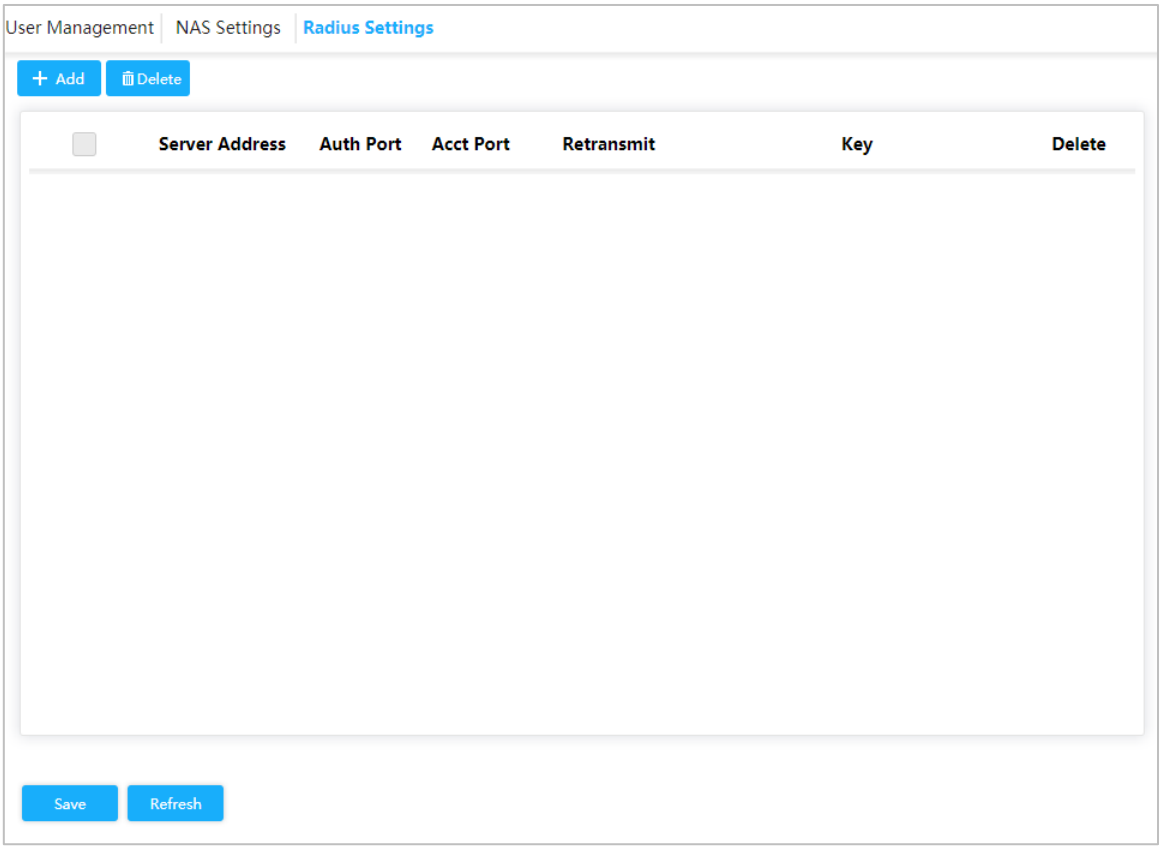
RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) es un protocolo común para realizar AAA (Autenticación, Autorización y Contabilidad).

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 mayor seguridad. Define el formato del paquete RADIUS y el mecanismo de transmisión del mensaje. Estipula el uso de UDP como protocolo de capa de transporte para encapsular el paquete RADIUS.

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

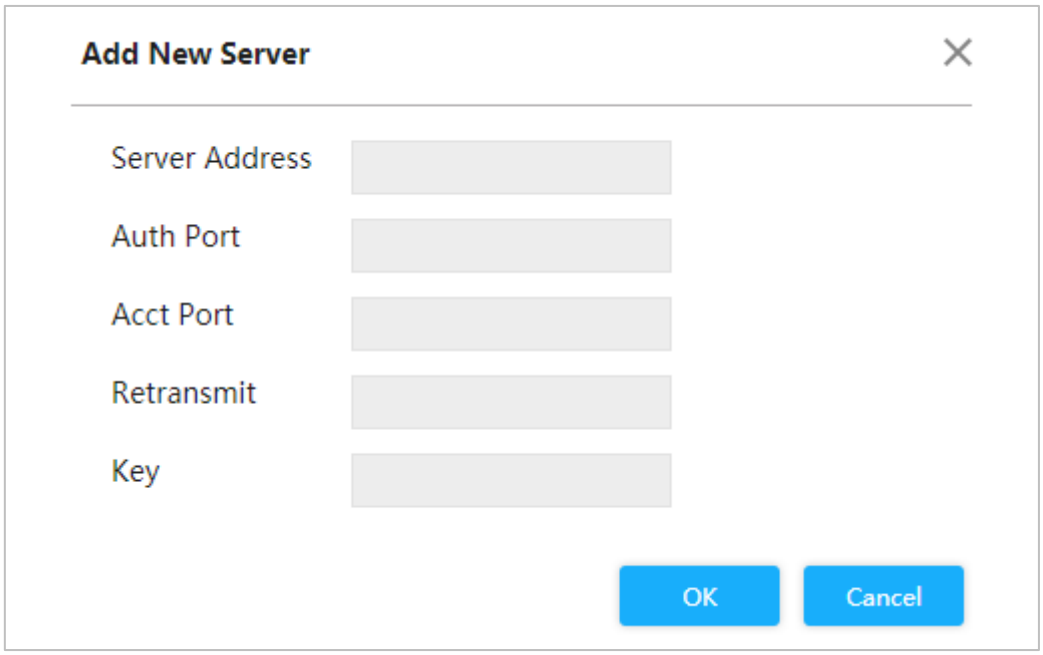
Paso 1 Seleccionar**Avanzado > Usado poco > Seguridad > Configuración de radio**.

Figura 3-48 Configuración del radio



Paso 2 Hacer clic**Agregar**.

Figura 3-49 Agregar nuevo servidor



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

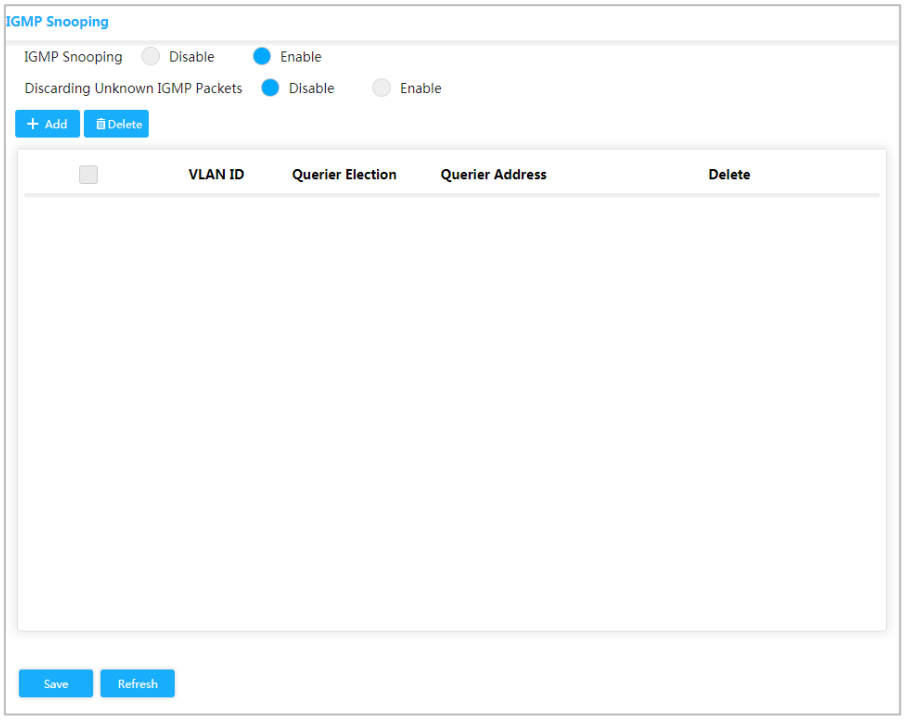
Etapa 4 clic**DE ACUERDO**.

3.2.5 Espionaje IGMP

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

Paso 1 Seleccionar**Avanzado > Poco utilizado > IGMP Snooping**.

Figura 3-50 Espionaje IGMP

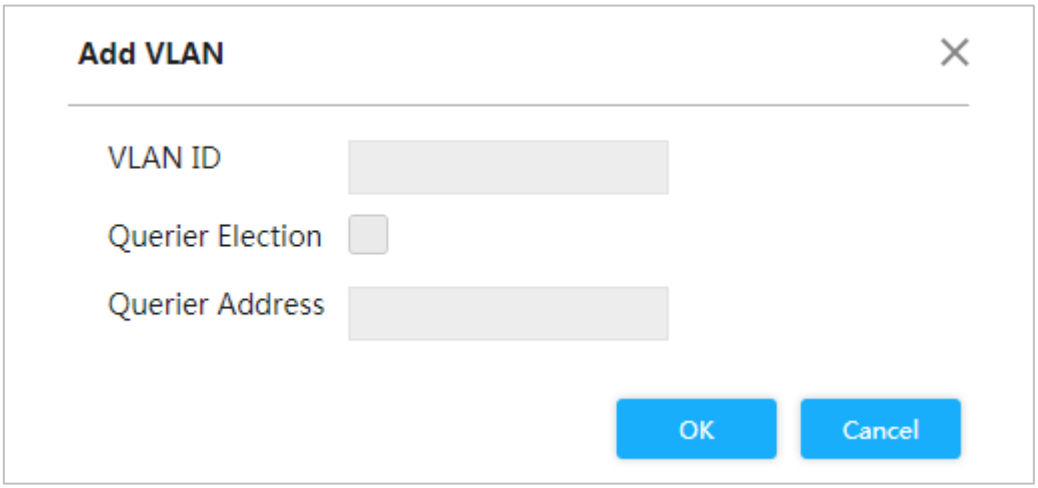


Paso 2 Seleccionar**Permitir**en el**Espionaje IGMP**área para habilitar la función. Seleccione

Paso 3 Desactivar o Activar en el área Descartar paquetes IGMP desconocidos. Hacer clic

Etapa 4 **Agregar**.

Figura 3-51 Agregar VLAN



Paso 5 Establezca el ID de VLAN y la dirección del interrogador y seleccione el**Elección de interrogadores**casilla para habilitar el buscador. Haga clic en**DE**

Paso 6 **ACUERDO**.

3.2.6 Calidad de servicio

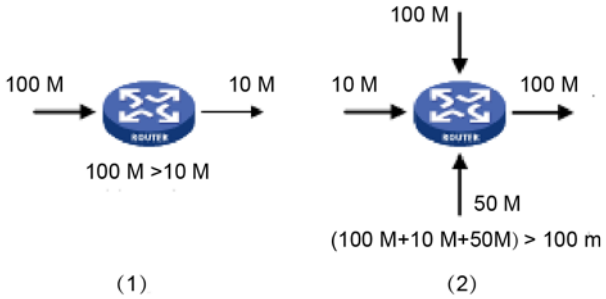
QoS (Calidad de Servicio) se utiliza para evaluar la capacidad que tiene el servidor para satisfacer las demandas de servicio del cliente. En Internet, lo que evalúa QoS es la capacidad del servicio de reenvío de red y paquetes.

La QoS se puede evaluar desde diferentes aspectos según los diversos servicios proporcionados por la red. QoS evalúa el ancho de banda, el retraso, el difuminado y la pérdida de paquetes durante el envío y el envío de paquetes.

Congestión

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

Figura 3-52 Congestión de flujo



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 por un puerto (la velocidad de múltiples puertos es mayor que la del puerto de salida).

Si el flujo llega a velocidad lineal, encontrará el punto de bloqueo de recursos 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, buffer y recursos de memoria) causará congestión. Además, el

El mal control del flujo llegado en un tiempo determinado, lo que lleva a que el flujo supere el recurso de la red distributiva, también es un factor para generar congestión.

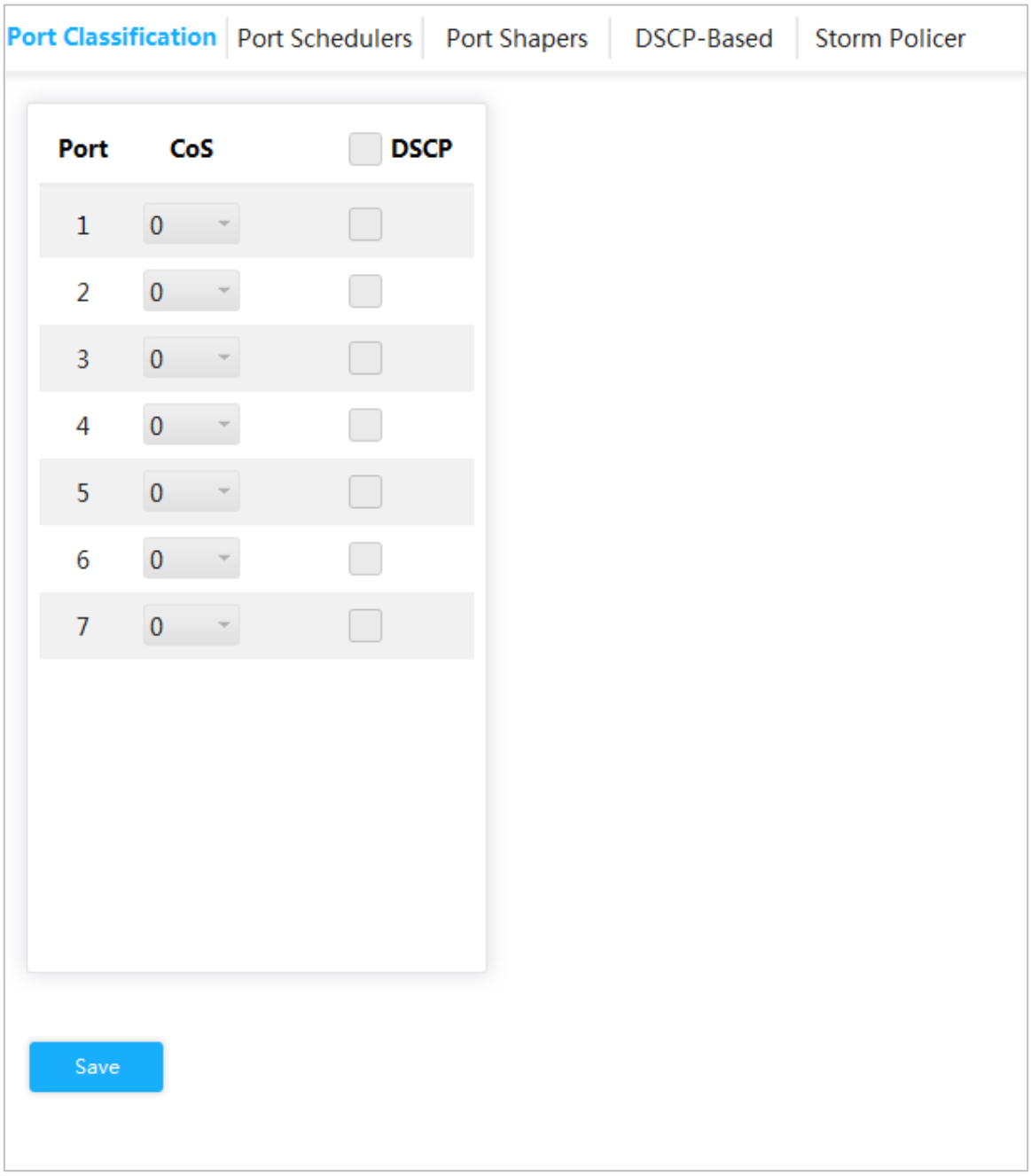
3.2.6.1 Puerto

Mediante la configuración de CoS, se puede decidir la prioridad para los paquetes que pasan por el puerto de salida del conmutador.

Si la congestión ocurre en el puerto de salida, el conmutador le dará un valor 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 Seleccionar**Avanzado > Poco utilizado > QoS > Clasificación de puertos**.

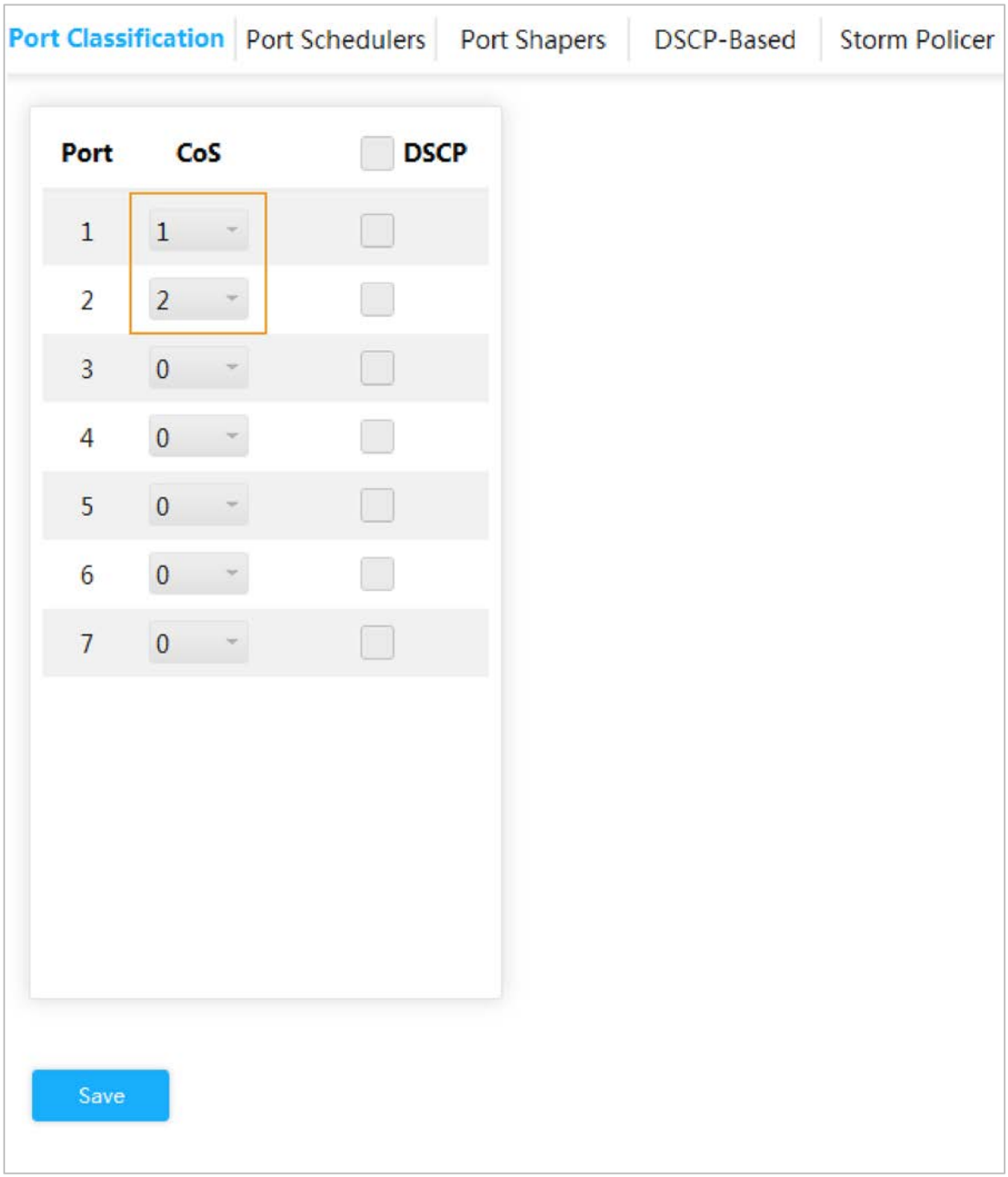
Figura 3-53 Clasificación de puertos



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



Paso 3 Hacer clic**Ahorrar**.

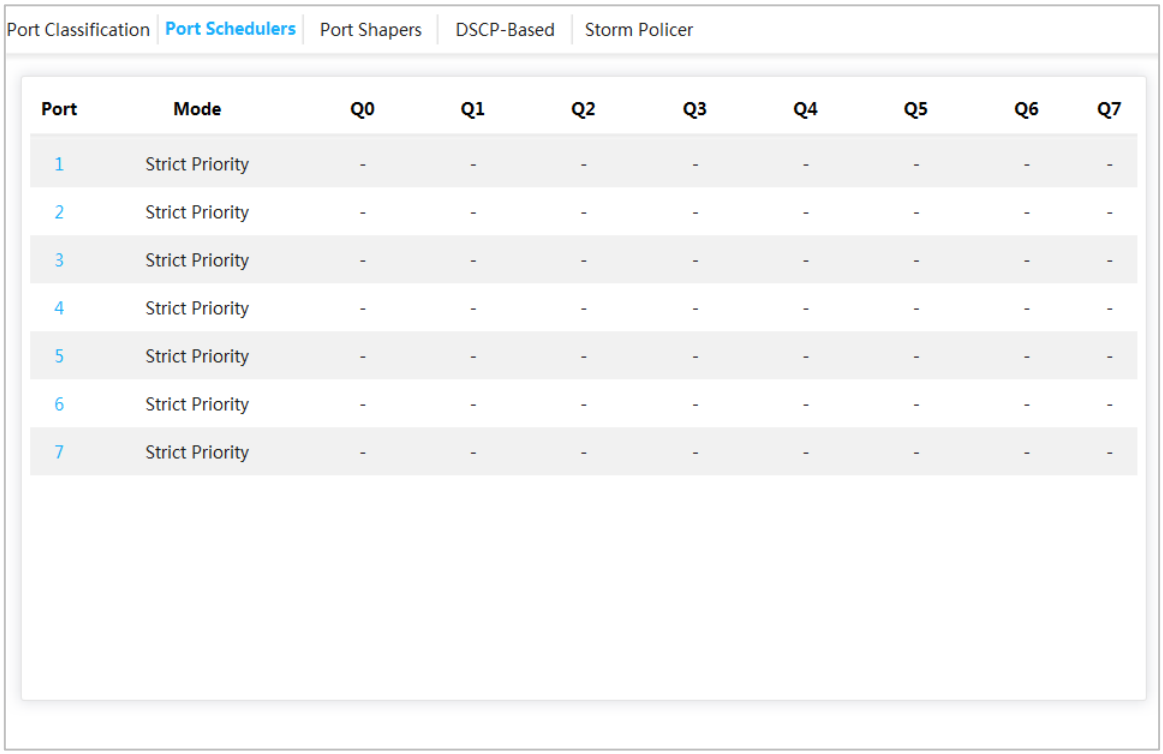
3.2.6.2 Programadores de puertos

Los dos modos de programadores de puertos:

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

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

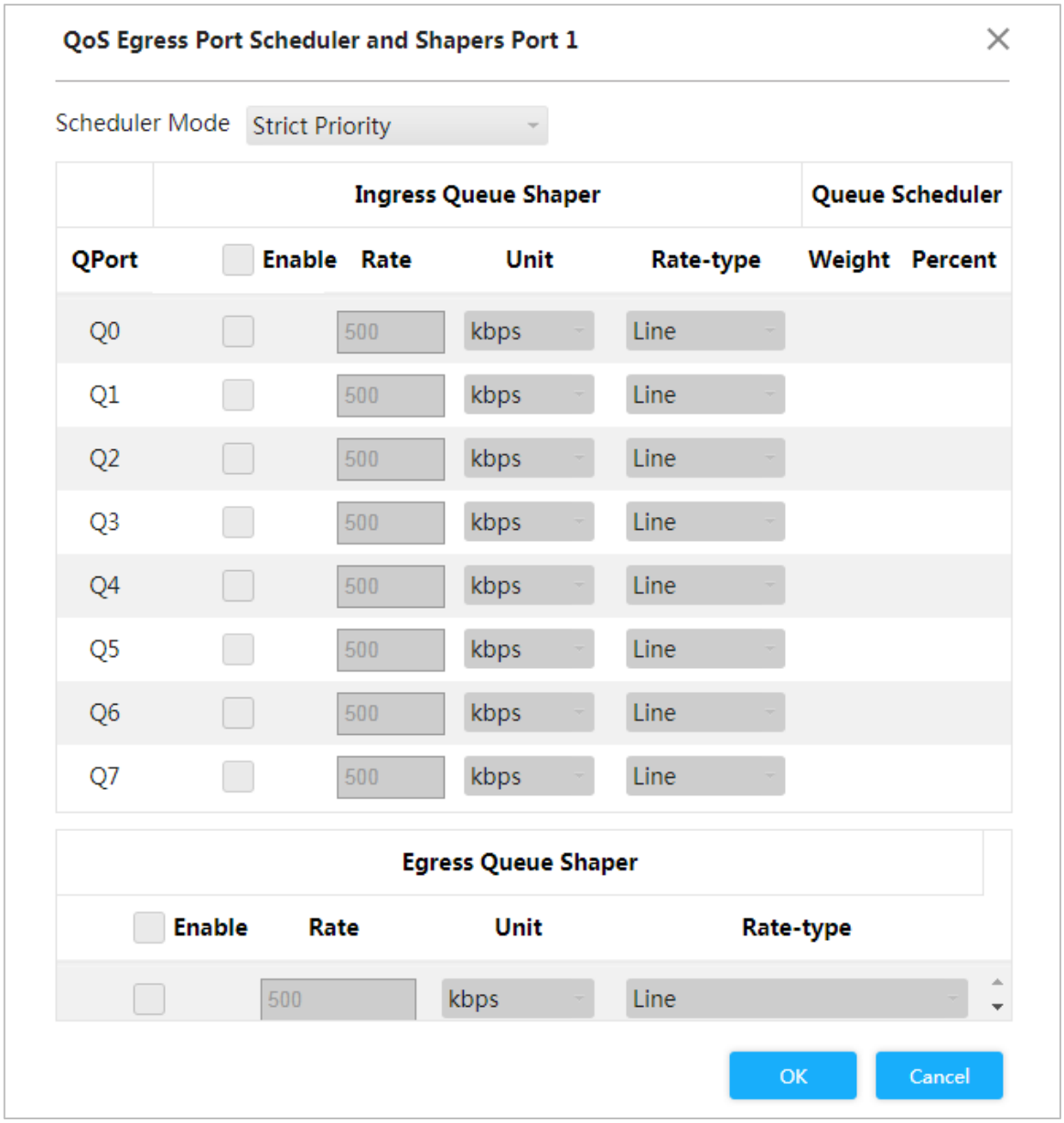
Figura 3-55 Programadores de puertos



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

El**Programadores y modeladores de puertos de salida de QoS Puerto 1**Se muestra la interfaz. El CoS de Q0 es 0, y así sucesivamente.

Figura 3-56 Configuración del puerto



Paso 3 Seleccionar modo.

- **Prioridad estricta**. La prioridad para los paquetes que pasan por el puerto de salida del conmutador depende del valor CoS en**Clasificación de puertos**.
- **2 a 8 colas ponderadas**. Cuando se produce congestión, la prioridad para los paquetes que pasan por el puerto de salida del conmutador depende de la proporción de la velocidad 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 congestión, el 50% de los paquetes del puerto de entrada pasarán por el puerto de salida.

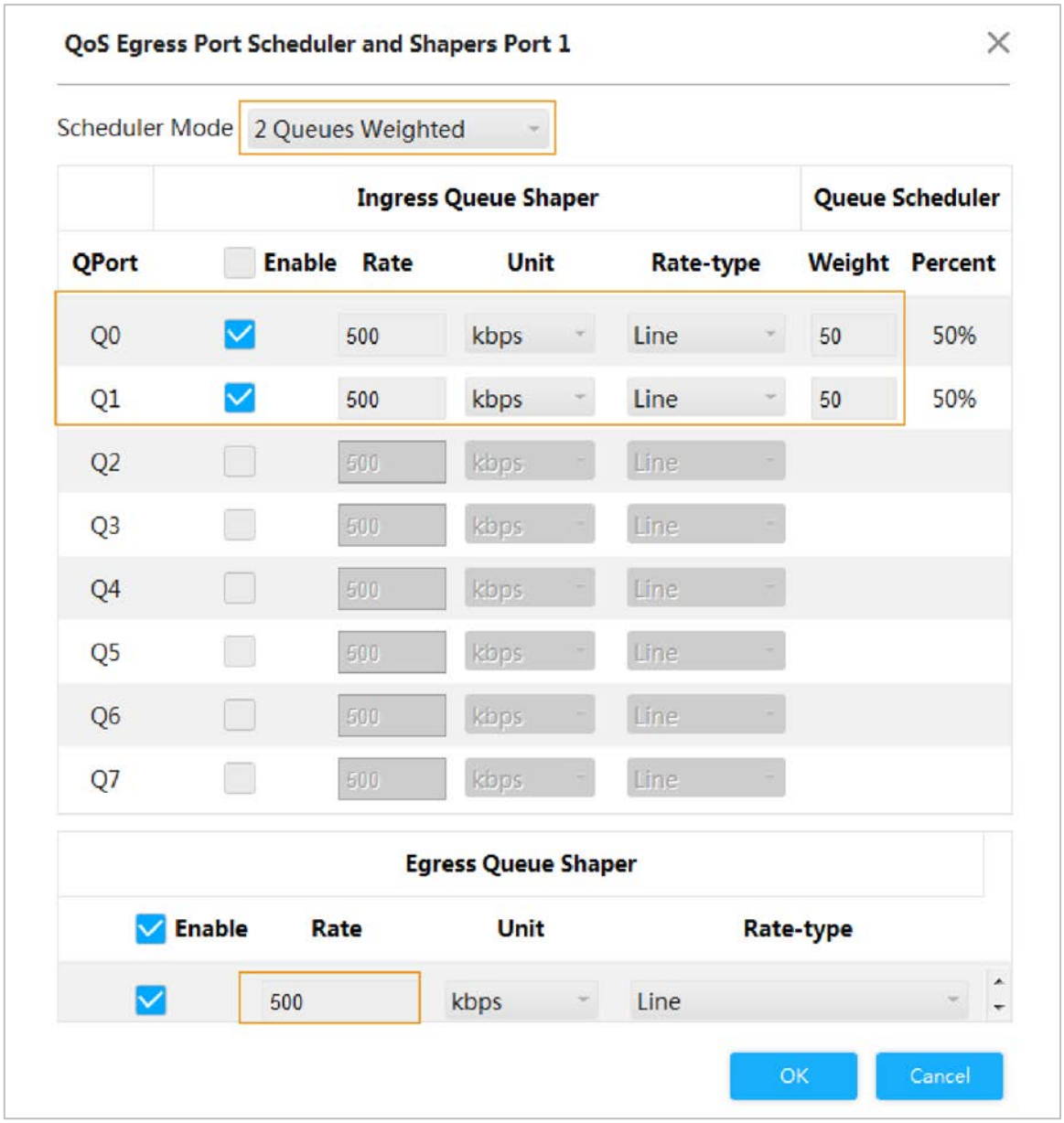
Consulte lo siguiente para la configuración:

1) Seleccionar**Modo de programador**como**2 colas ponderadas**. Consulte la Figura 3-57.

2) en**Modelador de cola de ingreso**, selecciona el**Tasa**de**Q0**y**Q1**ser 500 kbps, y**Tipo de cambio**ser Línea.

3 en**Modelador de cola de salida**, selecciona el**Tasa**ser 500 kbps, y**Tipo de cambio**ser**Línea**. Cuando se produce 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



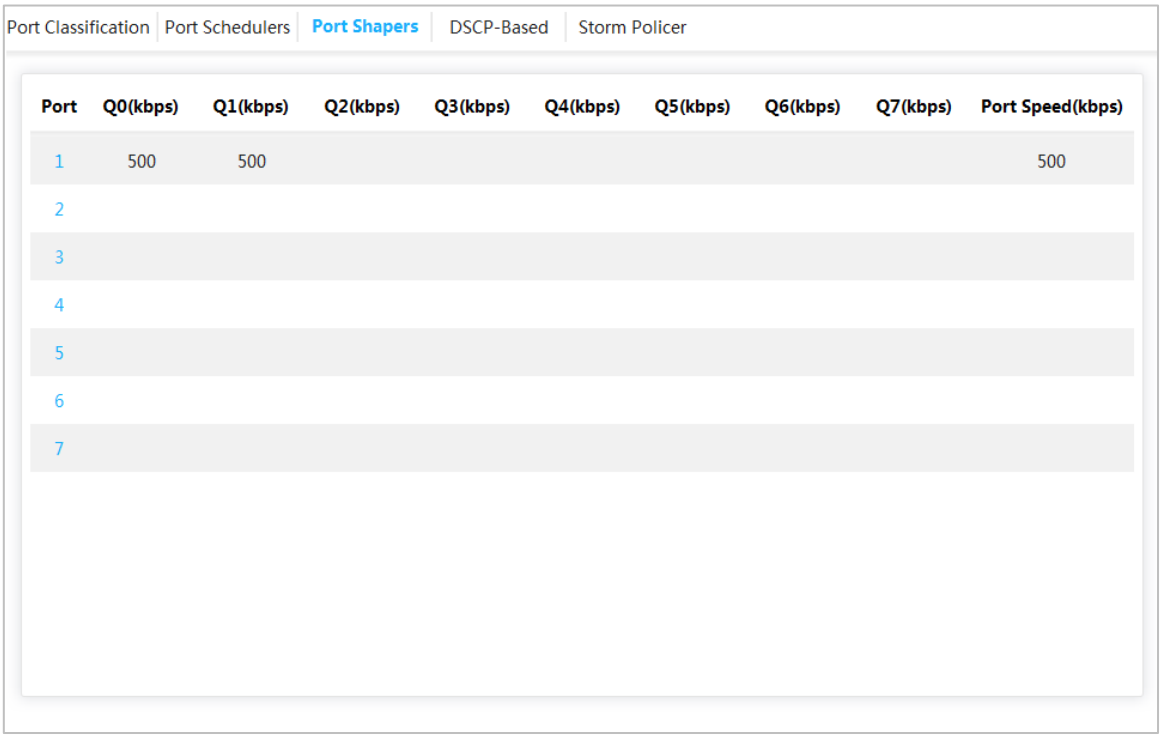
Etapa 4 Hacer clic**DE ACUERDO**.

3.2.6.3 Formadores de puertos

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

Seleccionar**Avanzado > Poco utilizado > QoS > Port Shapers**.

Figura 3-58 Formadores de puertos



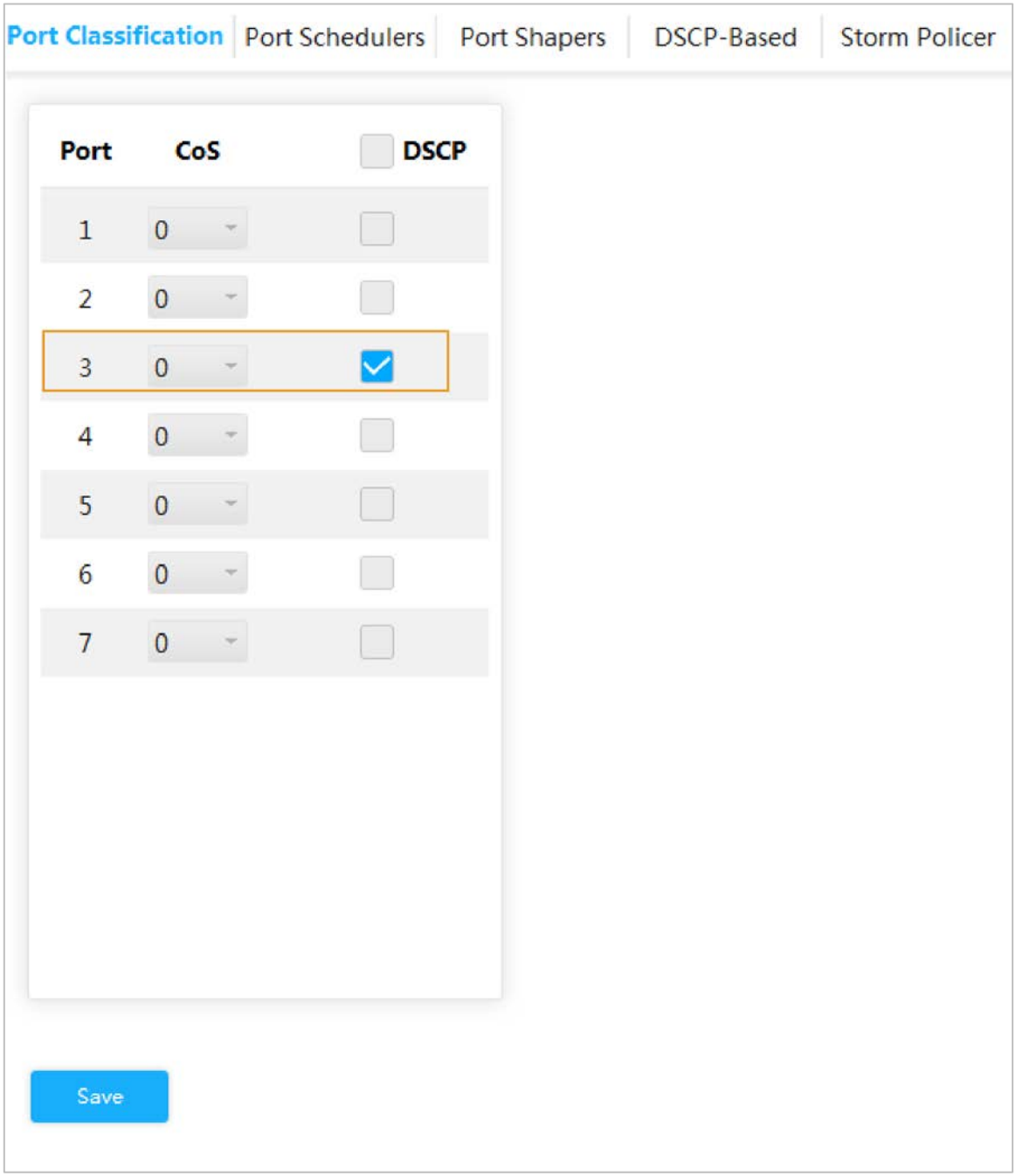
3.2.6.4 Basado en DSCP

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

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

Paso 2 DSCP en el puerto DSCP. Supongamos que el puerto 3 es el puerto de salida.

Figura 3-59 Clasificación de puertos



Paso 3 Hacer clic**Ahorrar**.

Etapa 4 Seleccionar**Avanzado > Usado poco > QoS > Basado en DSCP**.

Paso 5 Cuando se configura DSCP en 4 y 8, CoS es 2 y DPL son 2 y 1.

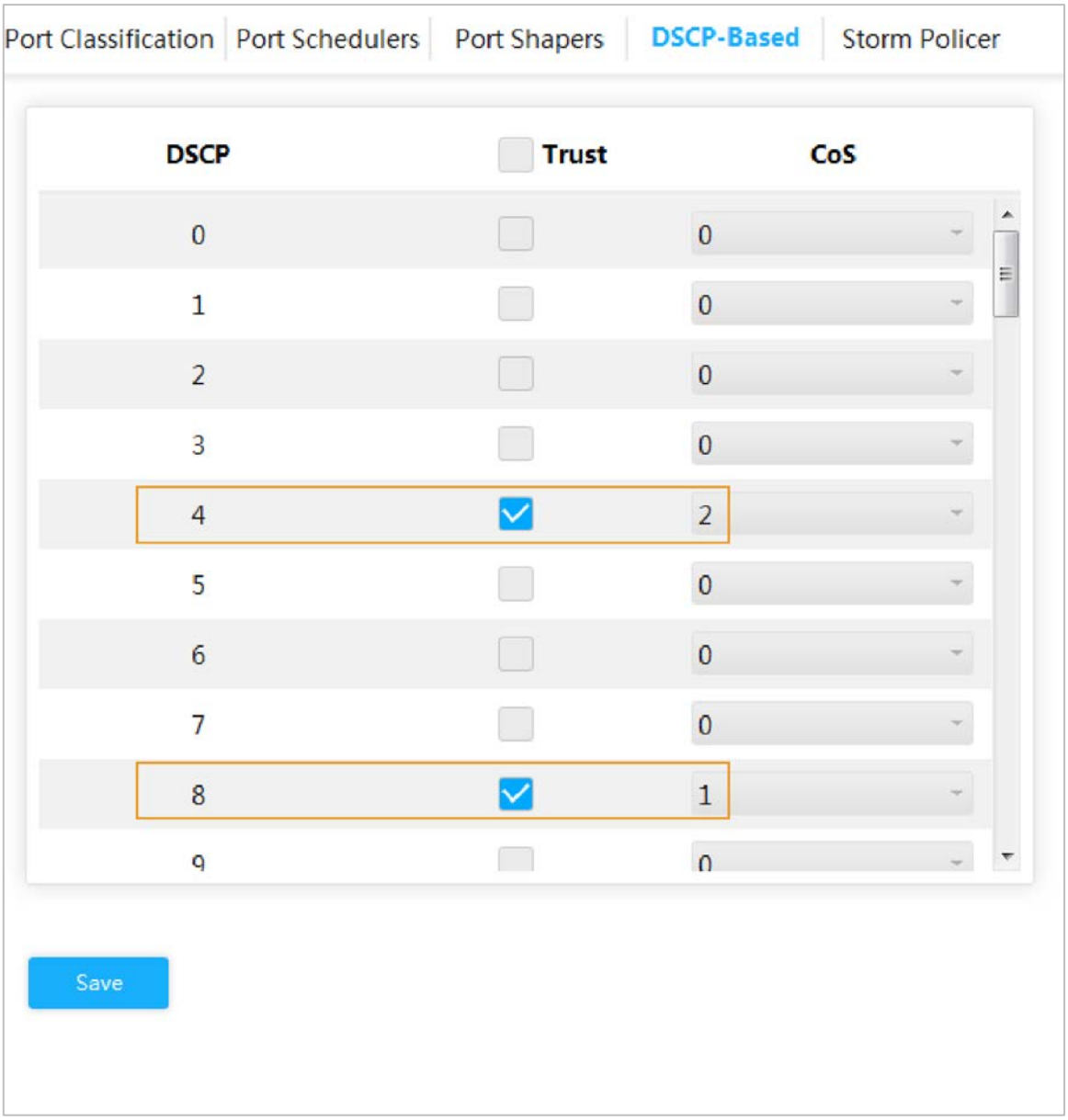
1) Cuando DSCP sea 4 y 8, seleccione**Confianza**para habilitar la función. Consulte la Figura 3-60.

2) Cuando se configura DSCP en 4, CoS es 2 y DPL es 2.

3) Cuando se configura DSCP en 8, CoS es 2 y DPL es 1.

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

Figura 3-60 Basado en DSCP



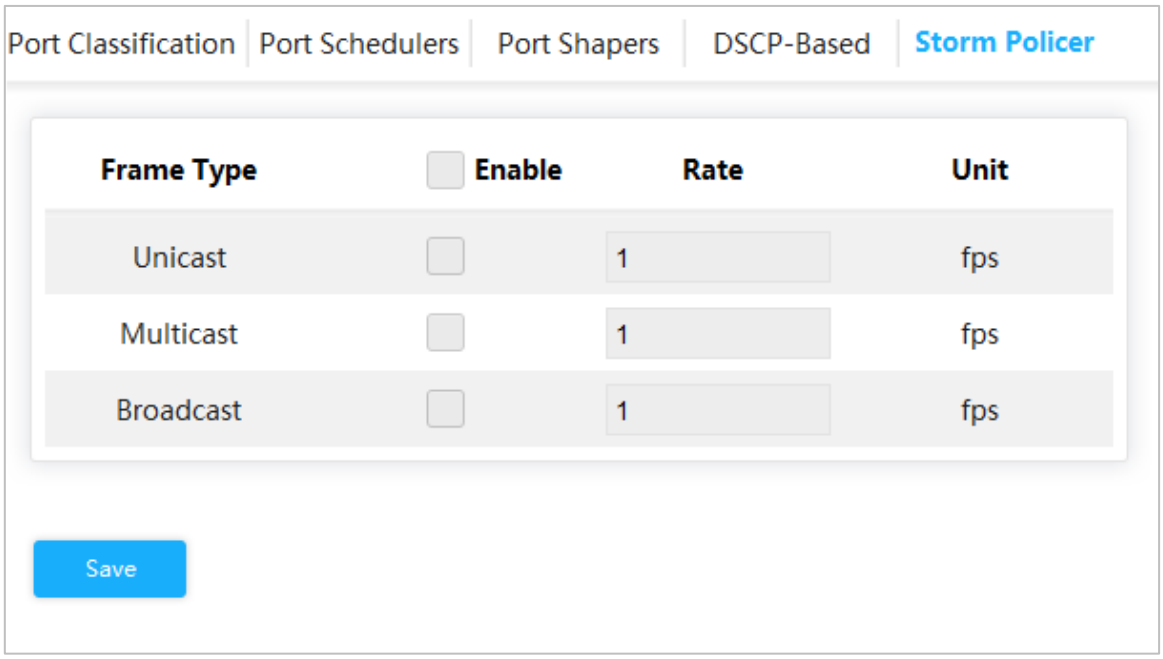
Paso 6 Hacer clic**Ahorrar**.

3.2.6.5 Policía de tormentas

Inhibe los tres paquetes, incluidos unidifusión, multidifusión y difusión.

Paso 1 Seleccionar**Avanzado > Usado poco > QoS > Storm Policer**.

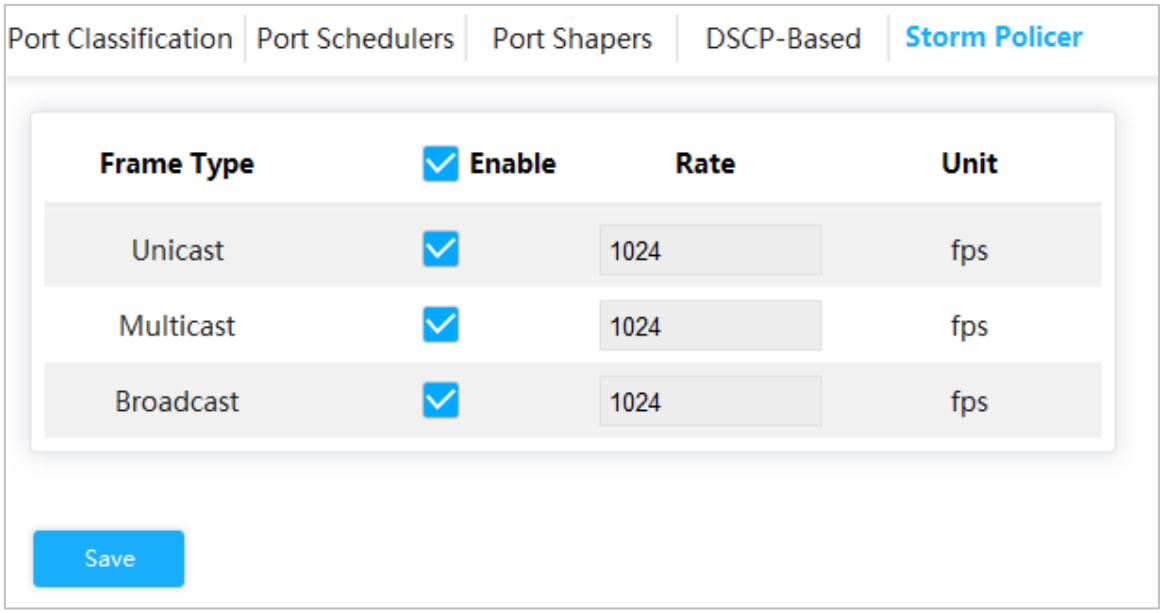
Figura 3-61 Policía de tormentas



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

- En**Unidifusión**, Selecciona el**Permitir**e ingrese 1024 en**Tasa**. Significa que el puerto puede recibir una velocidad de hasta 1024 fps de paquetes de unidifusión.
- En**Multidifusión**, Selecciona el**Permitir**e ingrese 1024 en**Tasa**. Significa que el puerto puede recibir una velocidad de hasta 1024 fps de paquetes de multidifusión.
- En**Transmisión**, Selecciona el**Permitir**e ingrese 1024 en**Tasa**. Significa que el puerto puede recibir una velocidad de hasta 1024 fps de paquete de transmisión.

Figura 3-62 Configuración del policía de tormentas



Paso 3 Hacer clic**Ahorrar**.

3.2.7 SNMP

SNMP (Protocolo simple de administración de red) 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:

- Admite la gestión inteligente de dispositivos de red. Al utilizar la plataforma de administración de red basada en SNMP, el administrador de la 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 sólo la biblioteca de funciones más básica. Independiente la tarea de gestión y la característica física y la tecnología de red del dispositivo gestionado, para gestionar los dispositivos de diferentes fabricantes.

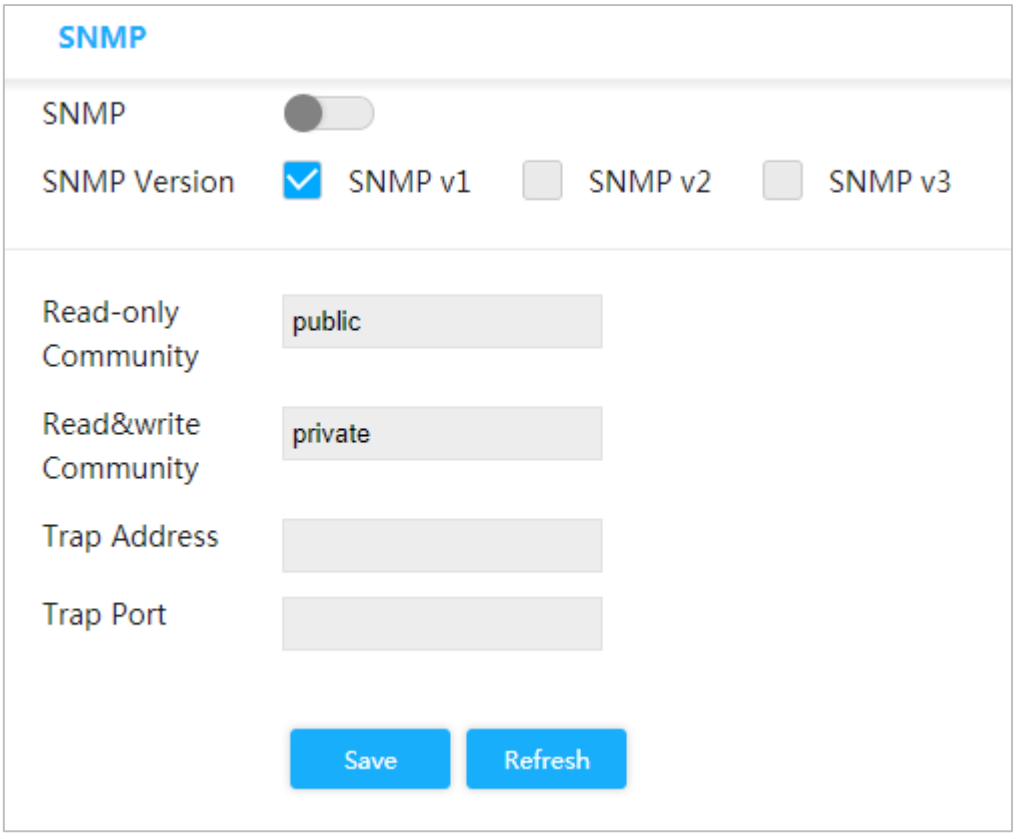
La red SNMP proporciona dos elementos, NMS y Agente.

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

3.2.7.1 Habilitación de la función SNMP

Paso 1 Seleccionar**Avanzado > Poco utilizado > SNMP**.

Figura 3-63 SNMP



Paso 2 Hacer clic  en**SNMP**para habilitar SNMP.

Cada agente SNMP v3 tiene un 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**.

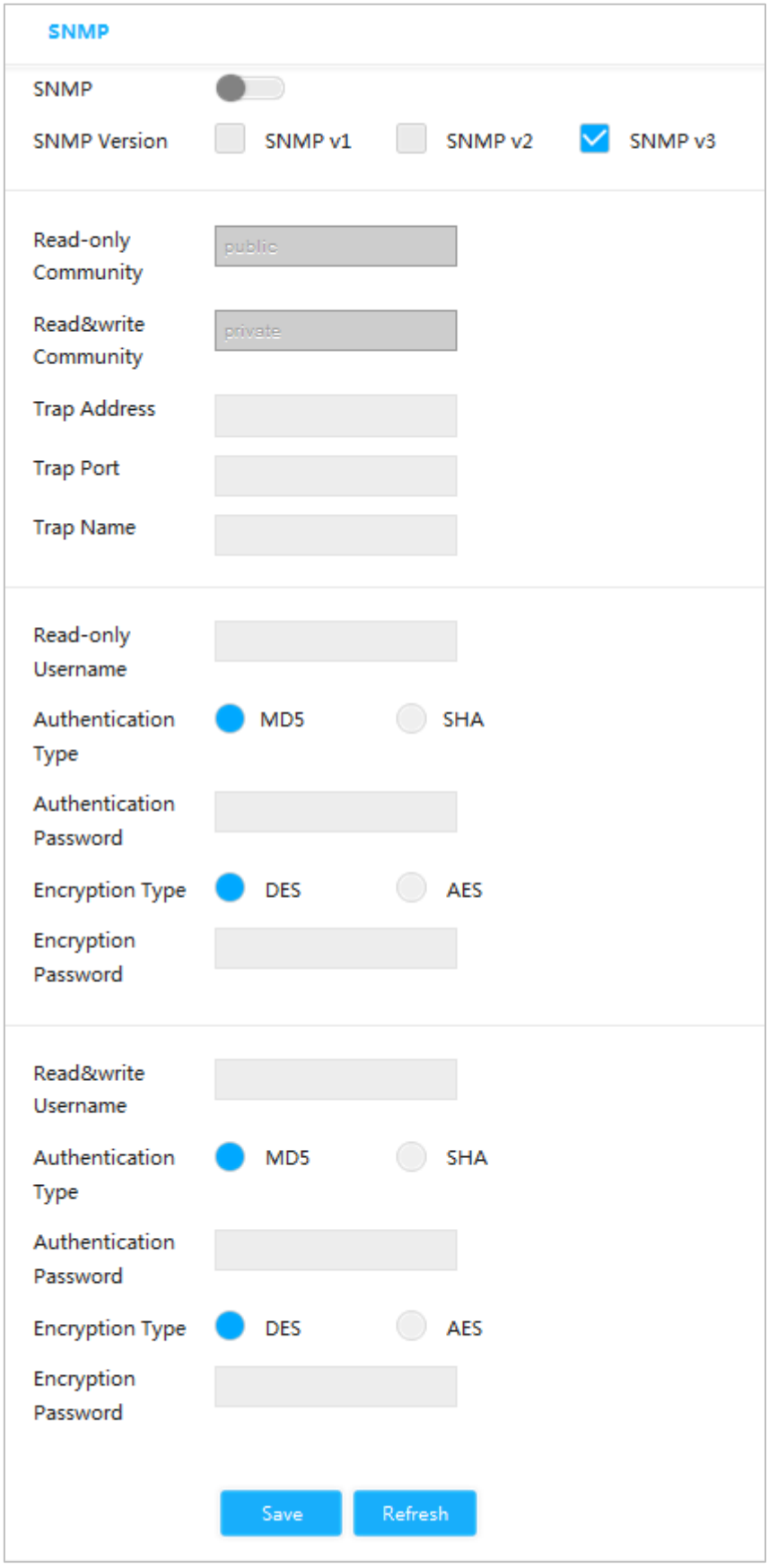
Paso 2 Configure la comunidad de solo lectura, la comunidad de lectura y escritura, la dirección de captura y el puerto de captura. Hacer clic

Paso 3 **Ahorrar**.

3.2.7.3 Configuración de SNMP v3

Paso 1 Seleccionar**SNMPv3**en**Versión SNMP**.

Figura 3-64 SNMP v3



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

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

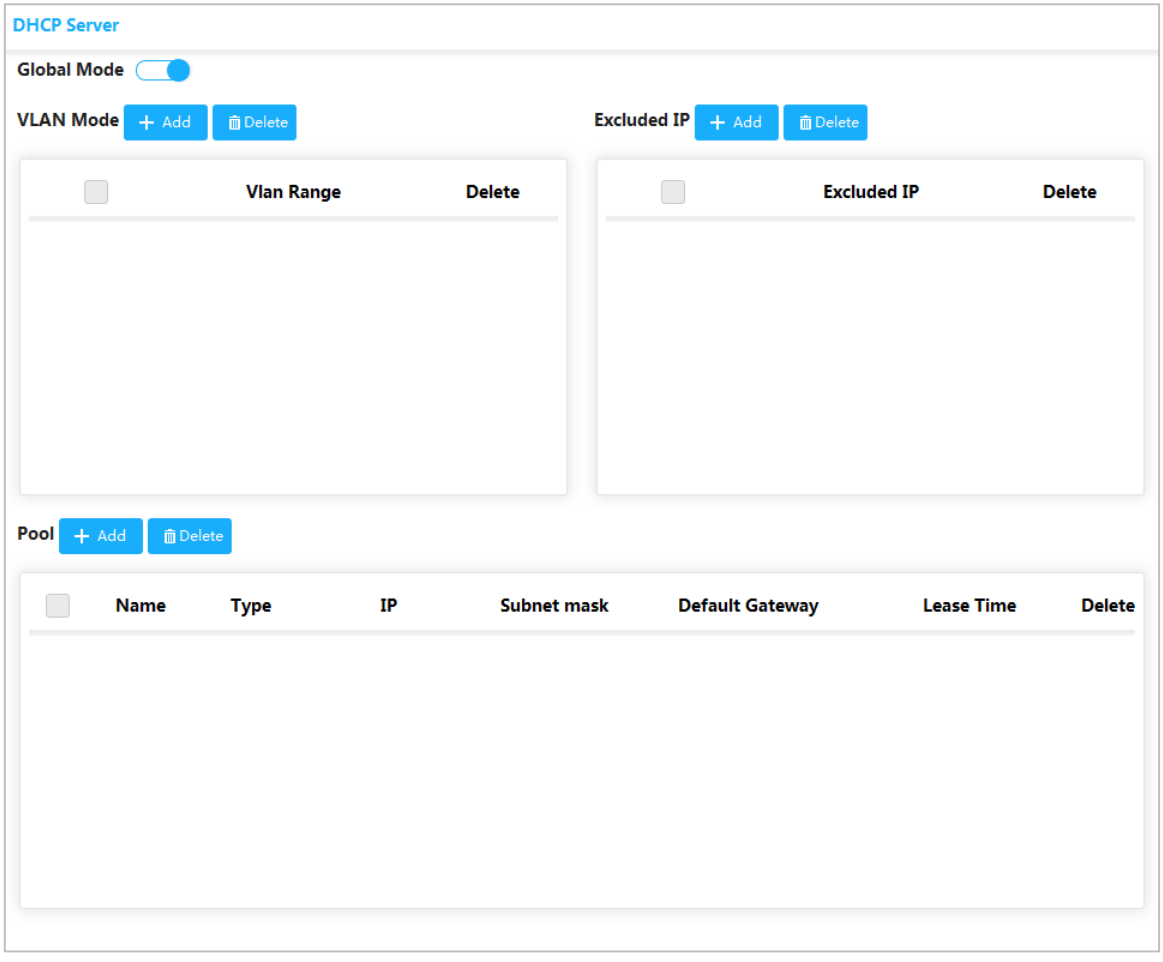
El servidor DHCP es el servidor para administrar el estándar DHCP en la red específica. El servidor DHCP debe asignar una dirección IP para la estación de trabajo y asegurarse de que la dirección IP para cada estación de trabajo sea diferente. El servidor DHCP simplifica la tarea de administración de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

Generalmente, en los siguientes escenarios, 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 debe 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 excluida**y**Piscina**. Paso 1 Seleccionar**Avanzado > Usado poco > DHCP > Servidor DHCP**.

Figura 3-65 Servidor DHCP



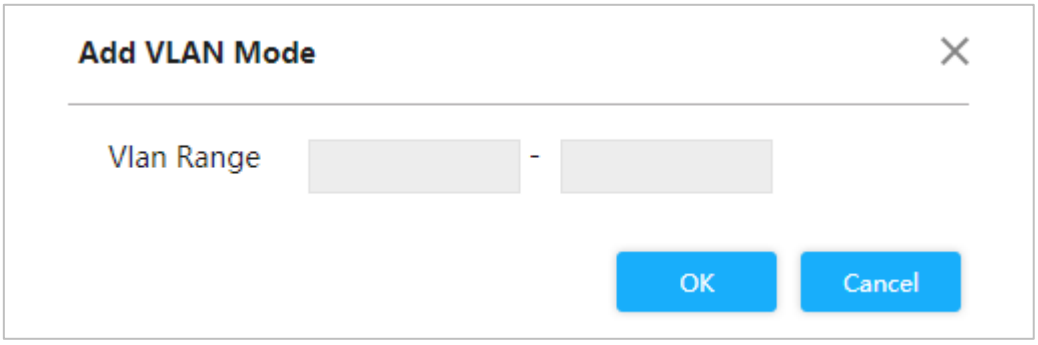
Paso 2 Hacer clic  en**Modo global**, para habilitar la función del servidor DHCP.

Paso 3 Configure el modo DHCP.

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

1) Haga clic**Agregar**en modo VLAN.

Figura 3-66 Modo Agregar VLAN



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

3) Haga clic**DE ACUERDO**.

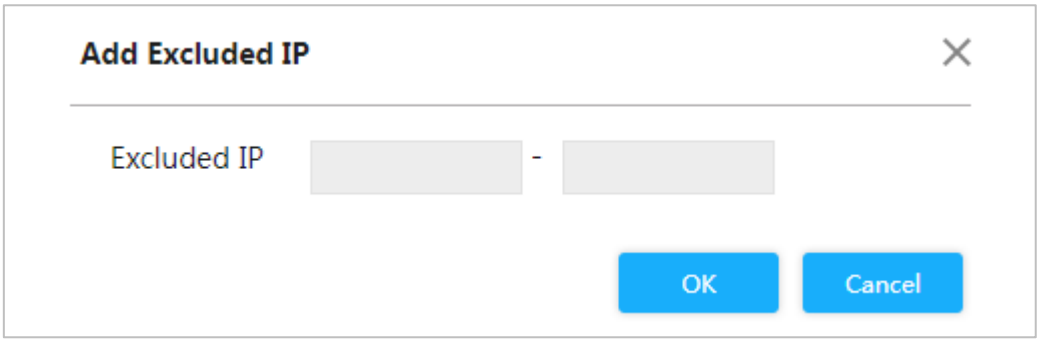
Etapa 4 Configurar el segmento de red de IP excluida.

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

1) Haga clic en Agregar en IP excluida.

El**Agregar IP excluida**Se muestra la interfaz. Consulte la Figura 3-67.

Figura 3-67 Agregar IP excluida



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

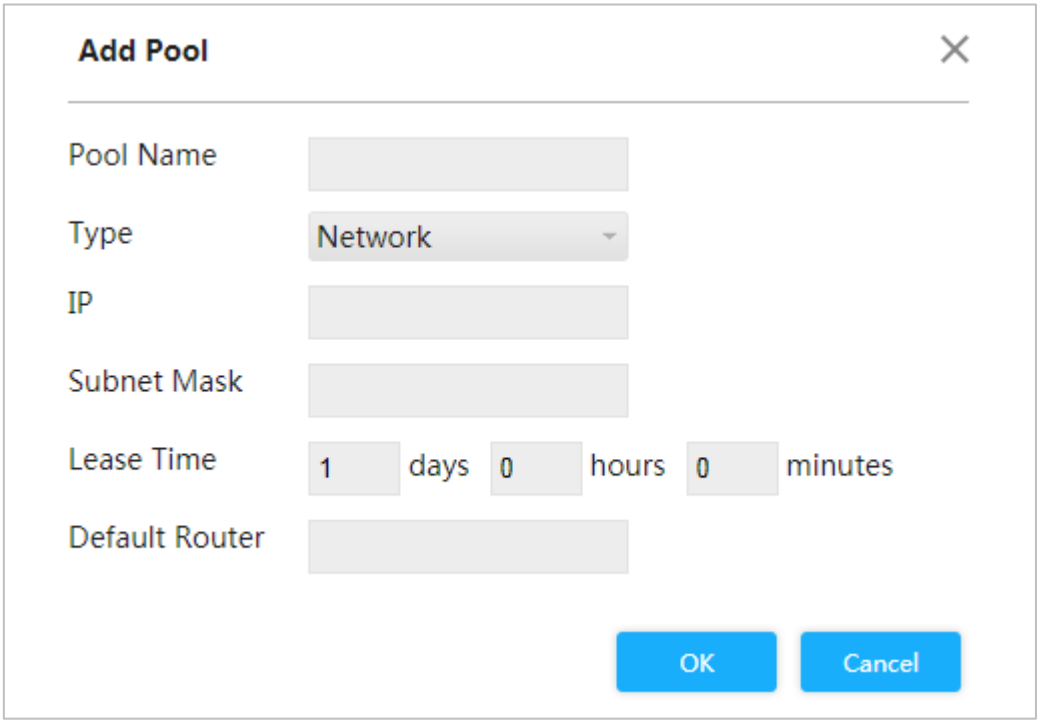
3) Haga clic**DE ACUERDO**.

Paso 5 Agregue el grupo de direcciones

DHCP. 1) Haga clic**Agregar**en**Piscina**.

El**Agregar grupo**Se muestra la interfaz.

Figura 3-68 Agregar grupo



2) Configurar los parámetros.

Tabla 3-7 Parámetros del grupo

Parámetro	Descripción
Nombre de la piscina	Nombre del grupo de direcciones DHCP, como "pool01". Sólo se pueden ingresar números o letras y la longitud de la cadena está limitada a 1 ~ 32.
Tipo	Dos tipos:**Red**y**Anfitrión**. - Red: El segmento de red de una IP. Host: - una IP específica
IP	La dirección IP del host o de la red.
Máscara de subred	La máscara de subred del host o de la red.
Tiempo de arrendamiento	Ingrese 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 estándar de descubrimiento de capa de enlace. 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 del protocolo de descubrimiento de capa de enlace) y liberarlo a su vecino. El vecino mantendrá la información recibida en forma de MIB (Base de información de gestión) estándar, para que la gestión de la red pueda consultar y juzgar el estado de comunicación del enlace.

LLDP

Paso 1 Seleccionar**Avanzado > Poco utilizado > LLDP**.

Figura 3-69 LLDP

Paso 2 Configure el modo LLDP.

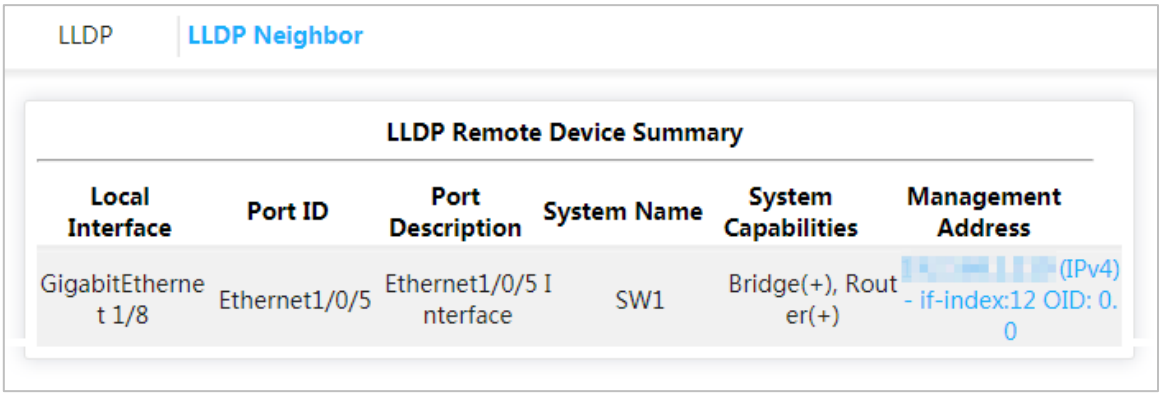
- Seleccionar**Permitir**: envían y reciben paquetes LLDP. Seleccionar
- **Desactivar**: No envía ni recibe paquetes LLDP. Seleccionar**Rx**
- **encendido**yo**y**: Sólo recibe paquetes LLDP. Seleccionar**solo**
- **transmisión**: Sólo envía paquetes LLDP.

Paso 3 Hacer clic**Ahorrar**.

Vea la información del vecino LLDP.

Seleccionar**Avanzado > Usado poco > LLDP > Vecino LLDP**.

Figura 3-70 Vecino LLDP

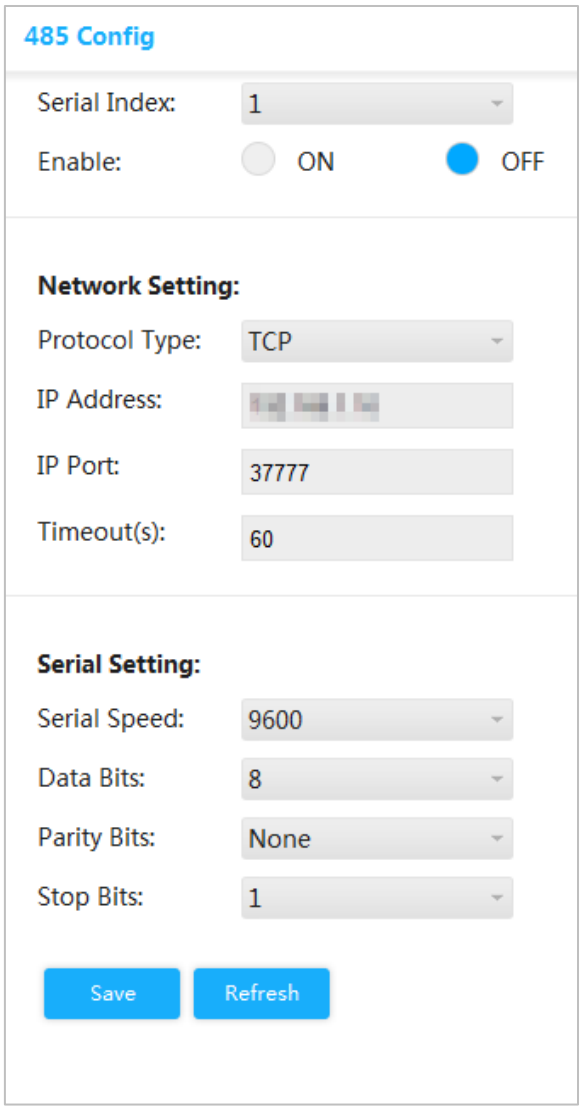


3.2.10 Configuración 485

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

Seleccionar**Avanzado > Poco utilizado > 485 Config**.

Figura 3-71 Configuración 485



3.2.11 PoE

PoE (Power over Ethernet) es la función que a través del puerto Ethernet RJ-45, el dispositivo puede proporcionar energía al PD (Powered Device) externo de forma remota con par trenzado. La función PoE ayuda a centralizar el suministro de energía y facilitar la copia de seguridad. El terminal de red ya no necesita una 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, AP (punto de acceso) inalámbrico, cargadores de dispositivos portátiles, lectores de tarjetas, cámaras de red, recopilación de fechas, etc.

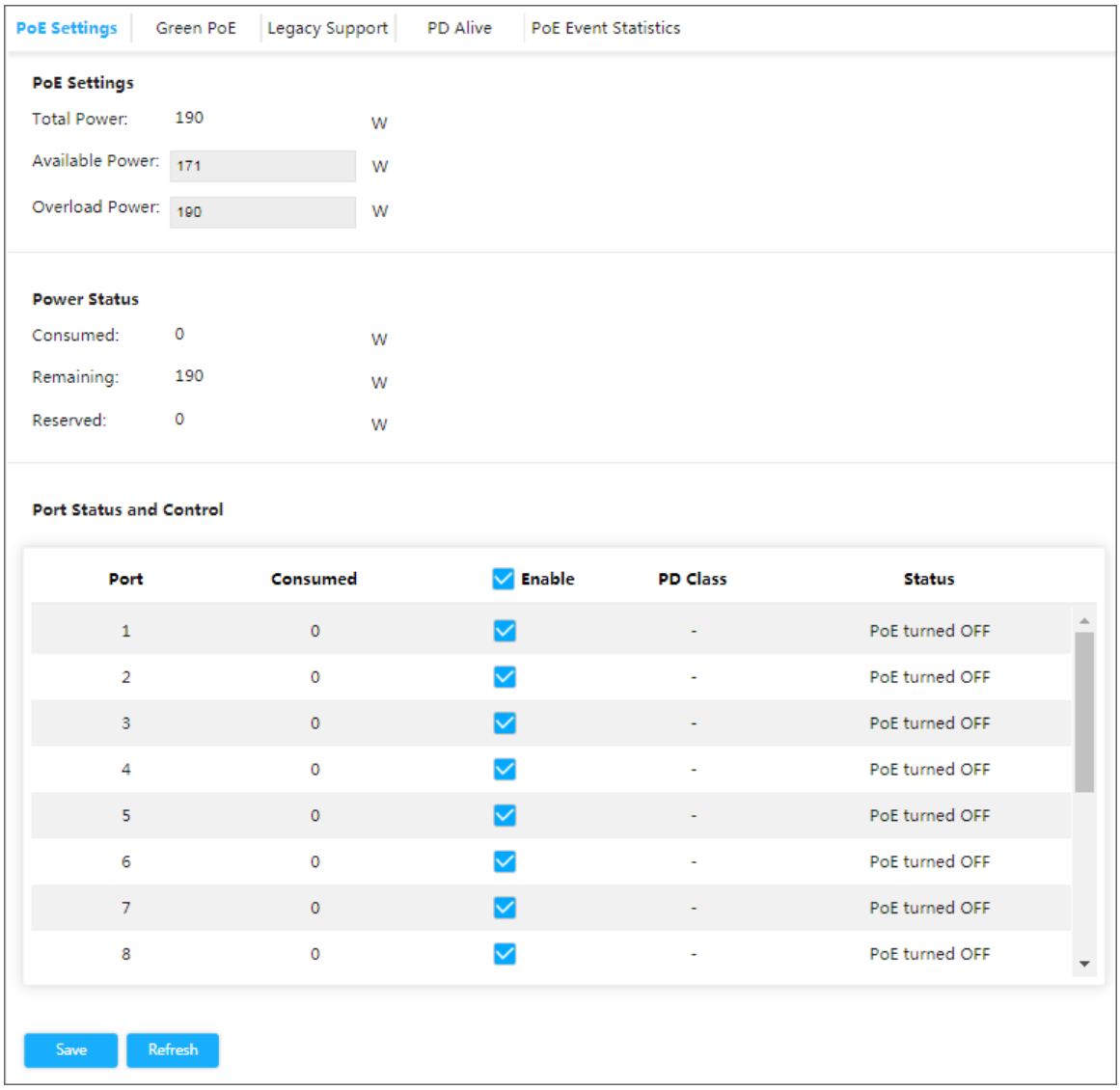
- Los conmutadores que no son PoE no admiten esta función.
- Solo algunos modelos de conmutadores PoE cumplen con el estándar IEEE 802.3bt y BT admite Max. 90W. Consulte la situación real.

3.2.11.1 Parámetros PoE

Configure la energía reservada, la energía de advertencia y habilite o deshabilite PoE. Paso 1

Seleccionar**Avanzado > Usado poco > PoE > Configuración de PoE**.

Figura 3-72 Configuración de PoE



Paso 2 En**Configuración de 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. En

Etapa 4 **Estado y control del puerto**, Selecciona el**Permitir**para habilitar o deshabilitar PoE del puerto correspondiente.

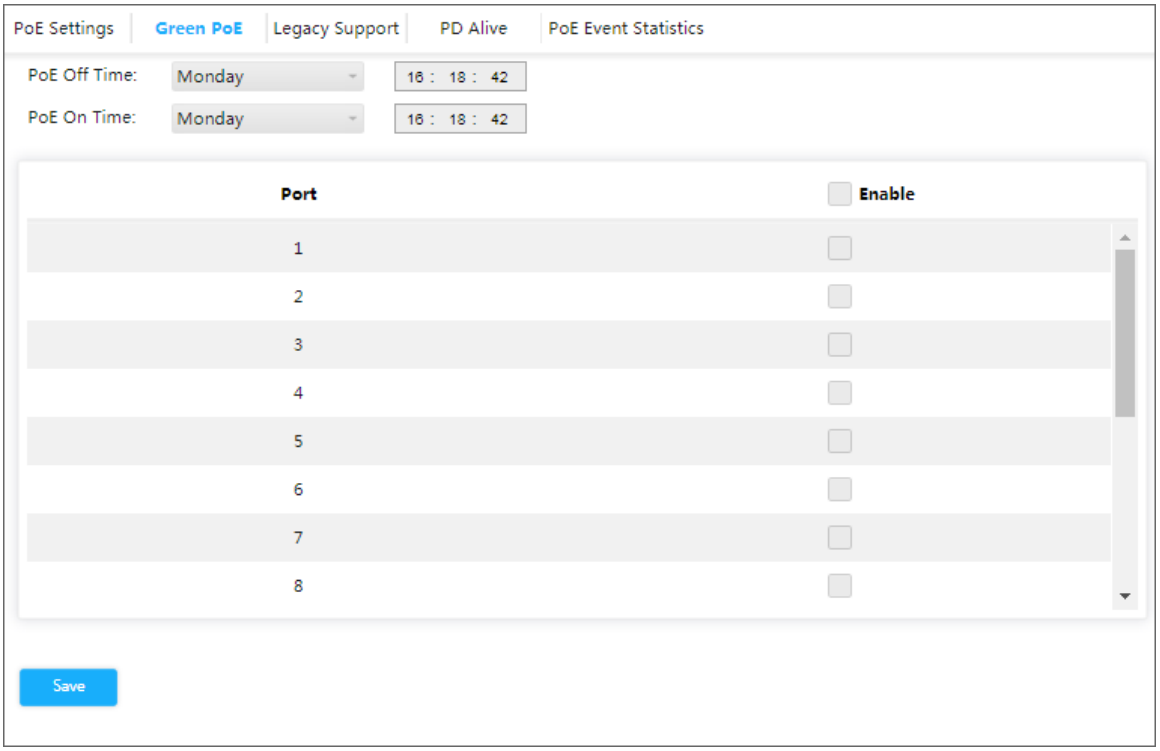
Paso 5 Hacer clic**Ahorrar**.

3.2.11.2 PoE verde

Active y desactive PoE a tiempo.

Paso 1 Seleccionar**Avanzado > Poco utilizado > PoE > PoE verde**.

Figura 3-73 PoE verde



Paso 2 Colocar**Tiempo de apagado de PoE**y**PoE a tiempo**.

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

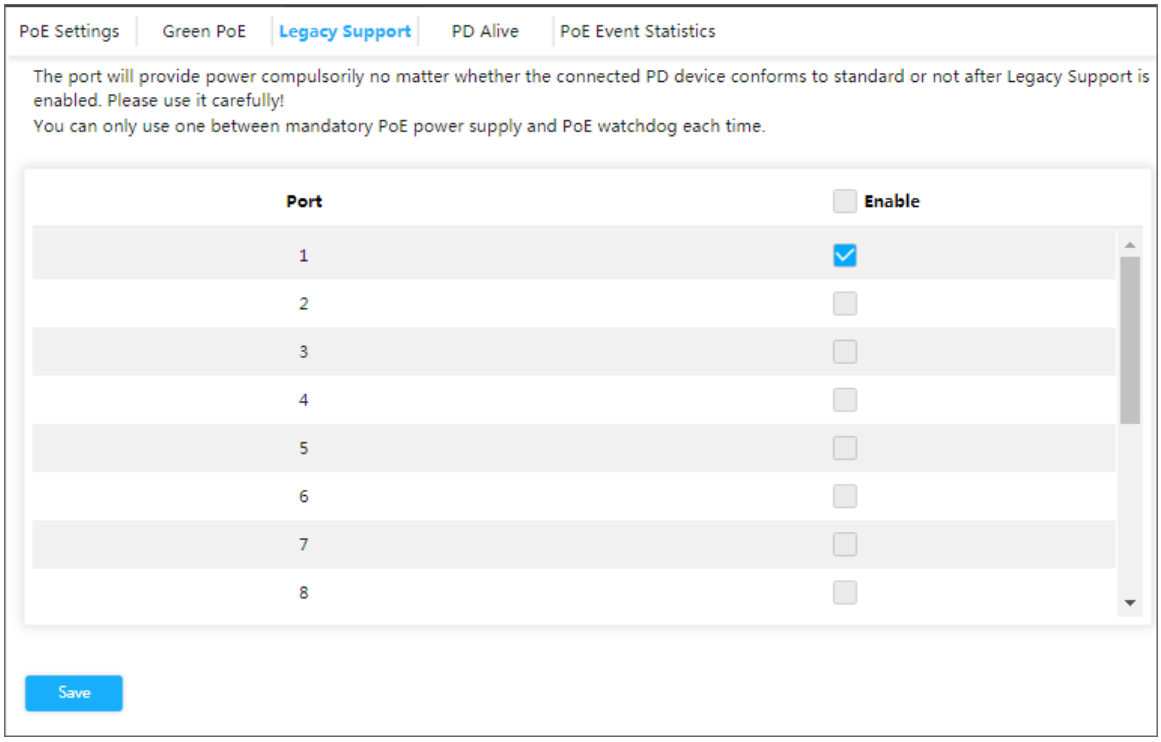
3.2.11.3 Soporte heredado

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

Dispositivo con alimentación 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**.

Figura 3-74 Soporte heredado



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

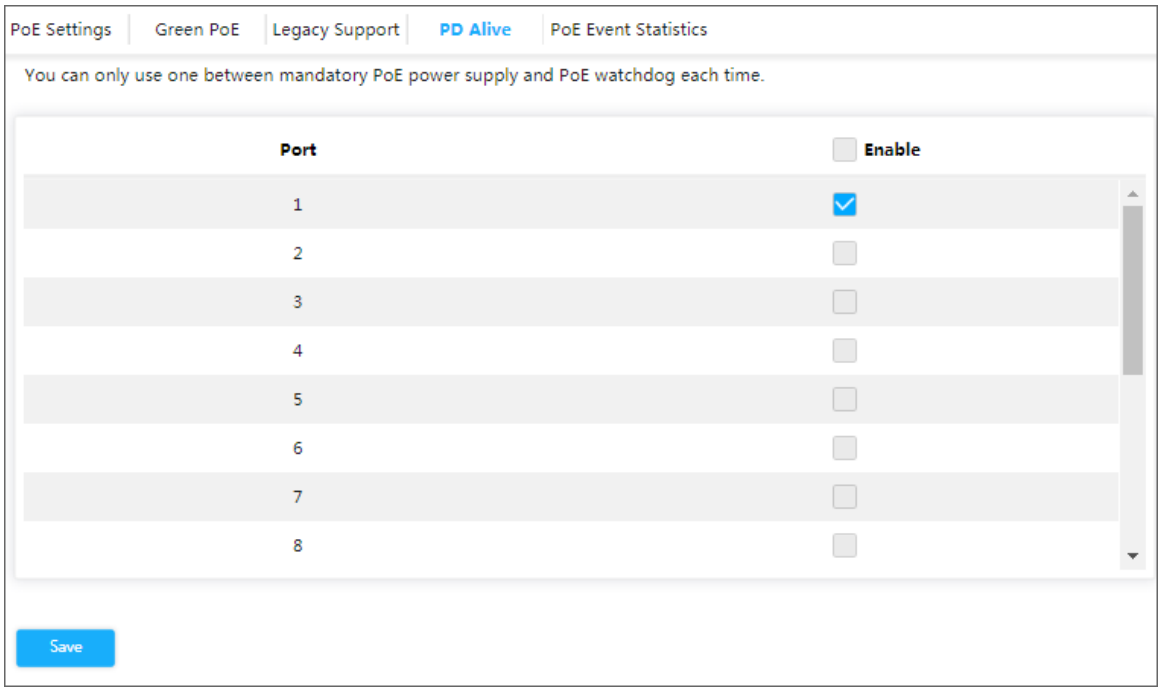
Paso 3 clic**Ahorrar**.

3.2.11.4 Vigilancia de PoE

Con el perro guardián PoE habilitado, puede monitorear PD y mantenerlo 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 > Usado poco > PoE > PD Alive**, seleccione la casilla de verificación del puerto correspondiente y luego haga clic en**Ahorrar**.

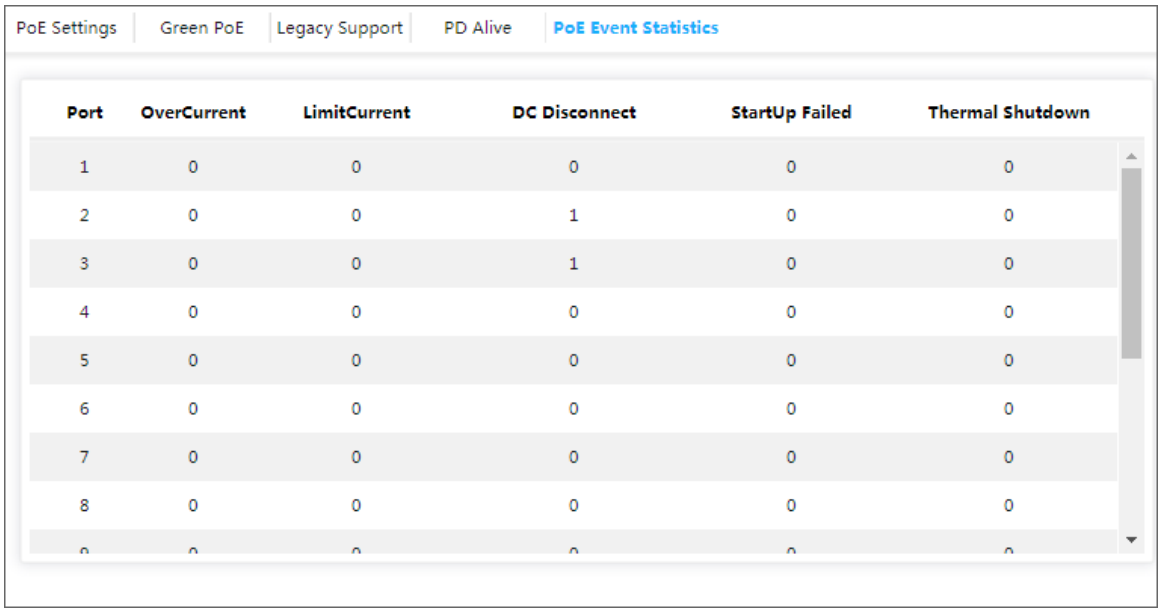
Figura 3-75 Vigilancia PoE



3.2.11.5 Visualización de estadísticas de eventos PoE

Seleccionar**Avanzado > Usado poco > PoE > Estadística de eventos PoE**para ver estadísticas de eventos PoE**.**

Figura 3-76 Estadística de eventos PoE



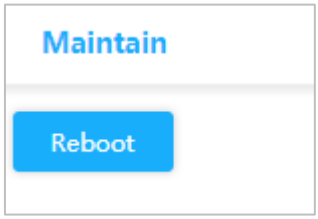
4 Mantenimiento

Tomemos como ejemplo el conmutador PoE de 4 puertos. La interfaz de mantenimiento es diferente según los modelos de interruptor. Prevalecerá la interfaz real.

4.1 Reinicio del sistema

Paso 1 Seleccionar**Mantenimiento > Común > Reinicio del sistema**.

Figura 4-1 Reinicio del sistema



Paso 2 Hacer clic**Reiniciar**.

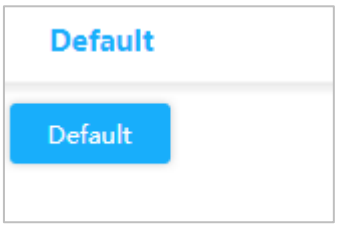
Paso 3 Hacer clic**Confirmar**y el dispositivo se reinicia.

4.2 Restaurar la configuración predeterminada

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

Paso 1 Seleccionar**Mantener > Común > Restaurar valor predeterminado**.

Figura 4-2 Restaurar valor predeterminado



Paso 2 Hacer clic**Por defecto**.

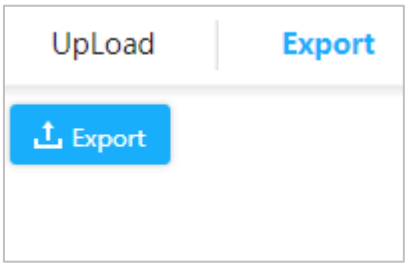
Todas las configuraciones, excepto la dirección IP VLAN1 del conmutador, se han restaurado a los valores predeterminados de fábrica.

4.3 Gestión de la configuración

4.3.1 Exportar archivo de configuración

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

Figura 4-3 Exportar

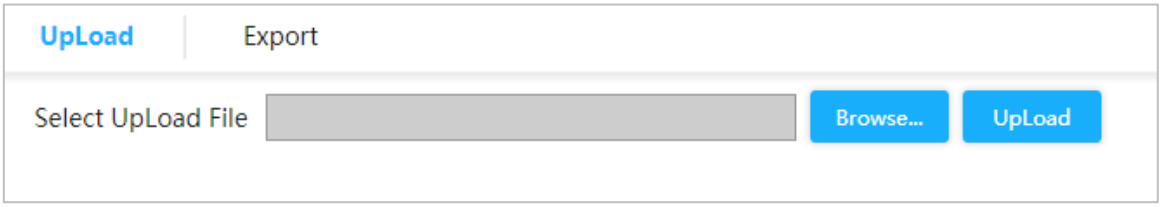


Paso 2 Hacer clic**Exportar**para exportar el archivo de configuración.

4.3.2 Carga del archivo de configuración

Paso 1 Seleccionar**Mantener > Común > Administrar configuración > Cargar**.

Figura 4-4 Carga



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

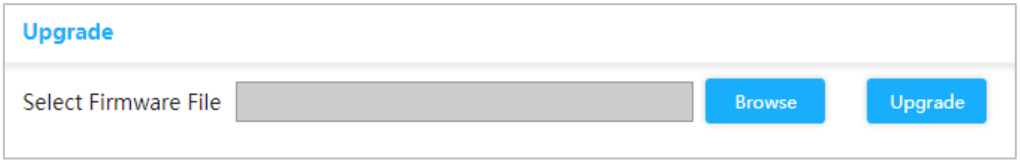
Paso 3 Hacer clic**Subir**.

Etapa 4 Reinicie el dispositivo y la configuración surtirá efecto.

4.4 Actualización de software

Paso 1 Seleccionar**Mantener > Común > Actualización de software**.

Figura 4-5 Actualización



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

Si el formato del archivo de actualización es incorrecto, el sistema mostrará el siguiente mensaje.

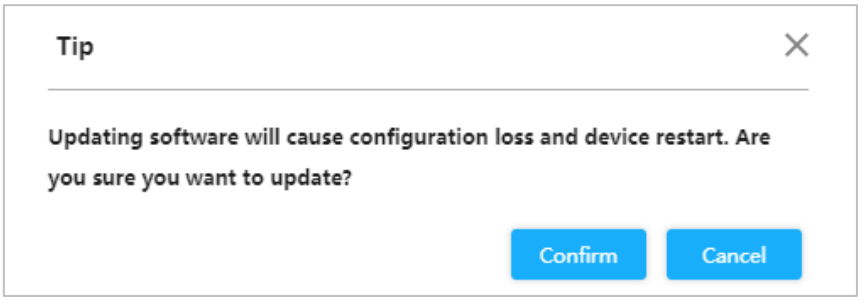
Figura 4-6 Mensaje de error

Paso 3 Hacer clic**Mejora**.

Etapa 4 Hacer clic**Confirmar**en el cuadro emergente.

El dispositivo se reinicia una vez finalizada la actualización.

Figura 4-7 Confirmar actualización

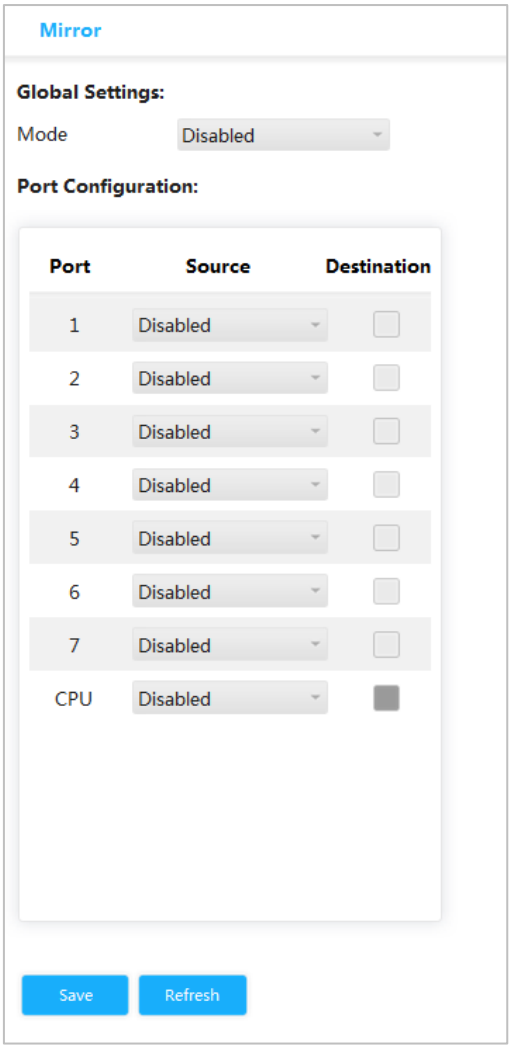


4.5 Duplicación

La duplicación de puertos también se denomina monitoreo 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 reflejados) se puede copiar a un puerto específico (puerto de destino reflejado). El puerto de destino de la 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 Seleccionar**Mantener > Común > Espejo**.

Figura 4-8 Espejo



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 dirección de origen del espejo.
  - Deshabilitar: deshabilita el puerto como dirección de origen del espejo.
  - Solo Rx: el puerto solo refleja la recepción de datos, en lugar de enviarlos.
  - Solo Tx: el puerto solo refleja el envío de datos, en lugar de recibirlos.
- Selecciona el**Destino**para configurar el puerto como destino.

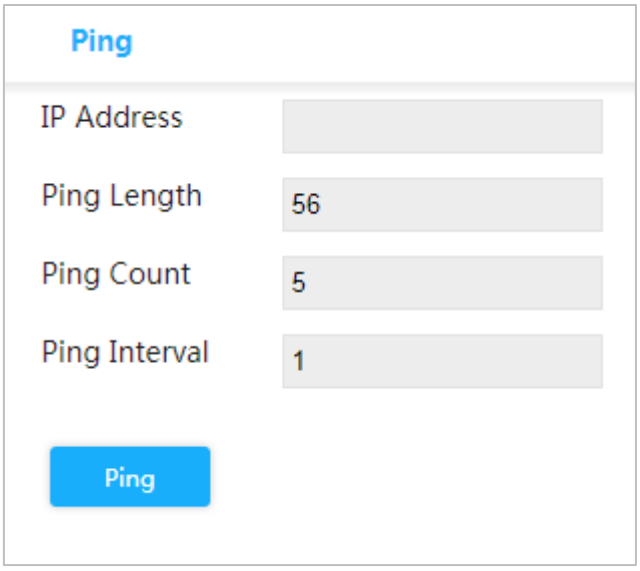
Etapa 4 Hacer clic**Ahorrar**.

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 Seleccionar**Mantener > Común > Ping**.

Figura 4-9 Hacer ping



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

4.7 Funciones del sistema de gestión de red

4.7.1 Habilitación de la función e inicio de sesión en la plataforma

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

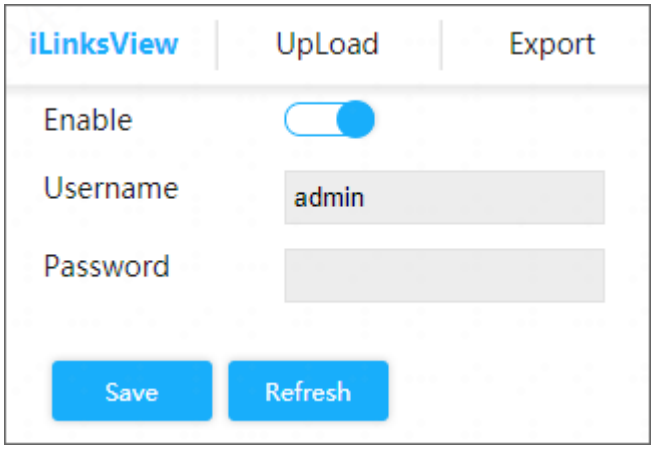
El nombre de usuario y contraseña deben ser los mismos que los de administración de red ILinksView plataforma.

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

Nombre de usuario: administrador

Contraseña: lt_91_il_02_nmp

Figura 4-10 Vista iLinks

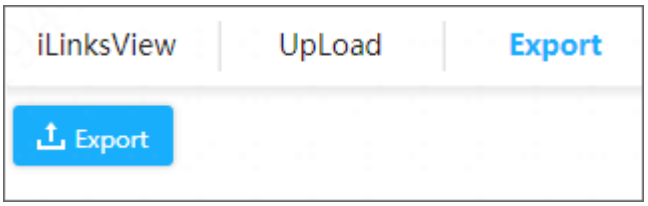


4.7.2 Exportación del archivo de configuración de administración de red

Puede exportar el archivo de configuración de administración de red.

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

Figura 4-11 Exportar archivo de configuración



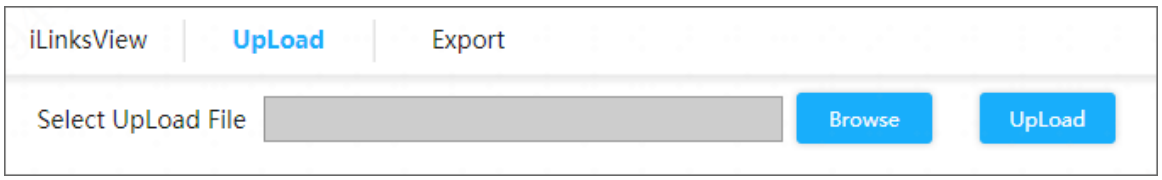
Paso 2 Hacer clic**Exportar**.

4.7.3 Carga del archivo de configuración de administración de red

Puede cargar el archivo de configuración de administración de red.

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

Figura 4-12 Cargar archivo de configuración



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

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

Etapa 4 Reinicie el dispositivo y la configuración surtirá efecto.

Apéndice 1Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple palabra de moda: es algo que pertenece a todos los dispositivos 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 conectados 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.

Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de personajes; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contener 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 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 "autoverificación 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 "es bueno tenerlas" para mejorar la seguridad de la red de su equipo: 1. Protección física

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

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3. Establecer y actualizar contraseñas Restablecer información oportuna

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 sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar preguntas de protección con contraseña, se sugiere no utilizar aquellas que puedan adivinarse fácilmente.

4. Habilite el bloqueo de cuenta

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

5. Cambie HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie 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. Habilite HTTPS

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

7. Vinculación de direcciones MAC

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

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9. Deshabilite los servicios innecesarios y elija modos seguros

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir 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 cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión cifrada de audio y vídeo

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

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de la transmisión.

11. Auditoría segura

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

12. Registro de red

Debido a la capacidad de almacenamiento limitada del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13. 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 asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar 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.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.