Conmutador Gigabit PoE administrado por Dahua

Manual de configuración web

V1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Prefacio

General

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

Instrucciones de seguridad

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

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

Revisión histórica

Versión	Contenido de la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Julio de 2019

Aviso de protección de privacidad

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

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida causada por las 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 el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más actualizado y la documentación complementaria.

- Todavía puede haber desviaciones en los datos técnicos, la descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final. Actualice el software del lector o pruebe con
- otro software de lectura convencional si no puede abrir el manual (en formato PDF).

- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Advertencias y medidas de seguridad importantes

El manual le ayuda a utilizar nuestro producto correctamente. Para evitar peligros y daños a la propiedad, lea atentamente el manual antes de usar el producto y le recomendamos que lo guarde en un lugar seguro para futuras consultas.

Requisitos operativos

- No exponga el dispositivo directamente a la luz solar y manténgalo alejado de fuentes de calor. No instale el
- dispositivo en un ambiente húmedo y evite el polvo y el hollín.
- Asegúrese de que el dispositivo esté en instalación horizontal e instálelo en una superficie sólida y plana para evitar que se caiga.
- Evite las salpicaduras de líquido en el dispositivo. No coloque objetos llenos de líquido sobre el dispositivo para evitar que el líquido fluya hacia el dispositivo.
- Instale el dispositivo en un ambiente bien ventilado. No bloquee la salida de aire del dispositivo.

- Utilice el dispositivo a la tensión nominal de entrada y salida.
- No desmonte el dispositivo sin instrucción profesional.
- Transporte, use y almacene el dispositivo en rangos permitidos de humedad y temperatura.

Requisitos de suministro de energía

- Utilice la batería correctamente para evitar incendios, explosiones y otros peligros.
- Reemplace la batería por una 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 la fuente de alimentación que cumpla con la fuente de alimentación limitada, de acuerdo con IEC60950-1. Consulte la etiqueta del dispositivo. Adopte la protección GND para dispositivos de tipo I.
-
- El acoplador es el aparato de desconexión. Manténgalo en ángulo para facilitar su operación.

Tabla de contenido

Prólogo ..... YO Advertencias y salvaguardias importantes .... III 1 Iniciar sesión 1

2 Configuración rápida 2

2.1 Información del sistema 2

2.2 Local 3

2.3 VLAN 3

2.4 Agregación 4

2.4.1 Configuración de agregación estática 5

2.4.2 Configuración de agregación dinámica 6

2.5 IP y ruta 6

3 Configuración avanzada 9

3.1 Configuración común 9

3.1.1 Configuración del sistema 9

3.1.2 Configuración del puerto 15

3.1.3 Configuración de VLAN ..... dieciséis

3.1.4 Agregación 18

3.1.5 Tabla MAC 20

3.1.6 Árbol de expansión 24

3.2 Configuraciones de uso poco frecuente 27

3.2.1 ERPS 27

3.2.2 ACL 35

3.2.3 Protección de bucle 38

3.2.4 Seguridad 38

3.2.5 Inspección IGMP 43

3.2.6 QoS 45

3.2.7 SNMP 54

3.2.8 Servidor DHCP 58

3.2.9 LLDP 60

3.2.10 Configuración 485 62

3.2.11 PoE 63

4 Mantenimiento 67

4.1 Reinicio del sistema 67

4.2 Restauración de la configuración predeterminada 67

4.3 Gestión de configuración 67

4.3.1 Exportar archivo de configuración 67

4.3.2 Carga de archivo de configuración 68

4.4 Actualización de software 68

4.5 Duplicación 68

4.6 Ping 70

Apéndice 1 Recomendaciones de ciberseguridad 71

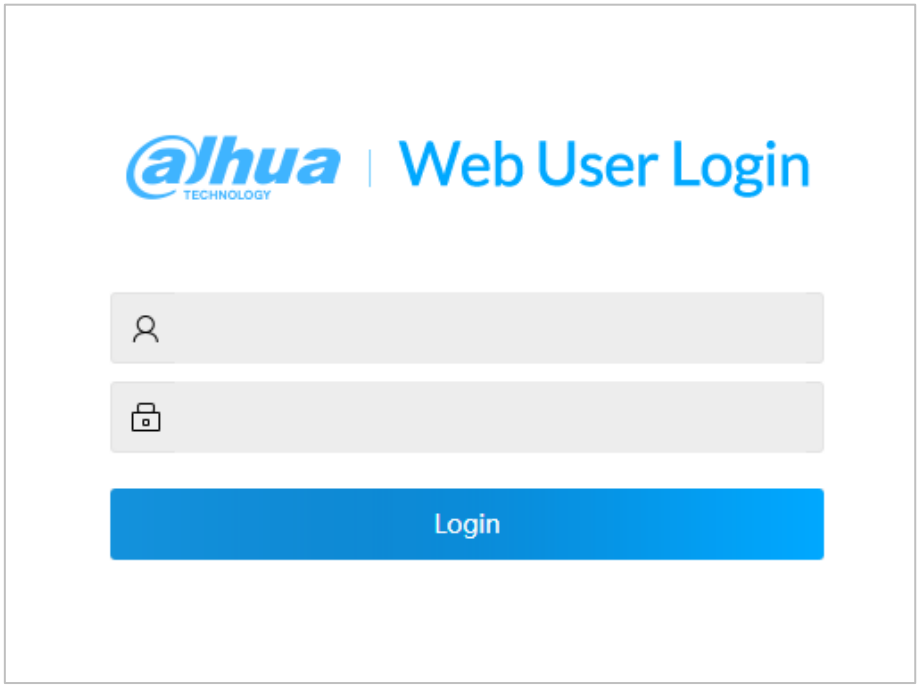
1 Iniciar sesión

Antes de iniciar sesión, asegúrese de:

- Ya configura la dirección IP del conmutador. 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 switch correctamente.

Paso 1 Introduzca la dirección IP (192.168.1.110 por defecto) del conmutador en la barra de direcciones del navegador web y luego presione Entrar. los **Iniciar sesión** se muestra la interfaz. Vea la Figura 1-1.

Figura 1-1 Inicio de sesión web



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

Paso 3 Haga clic en **Iniciar sesión.**

los **Ajuste rapido** se muestra la interfaz.

Modifique la contraseña después de iniciar sesión por primera vez. 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 '";: &).

2 Ajustes rápidos

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. La interfaz real prevalecerá.

2.1 Información del sistema

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

Después de iniciar sesión en el sistema, **Ajuste rapido** se muestra la interfaz. Vea 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 en gris, significa que el puerto no está conectado o la conexión falla. Consulte la Tabla 2-1.

Figura 2-1 Información del sistema

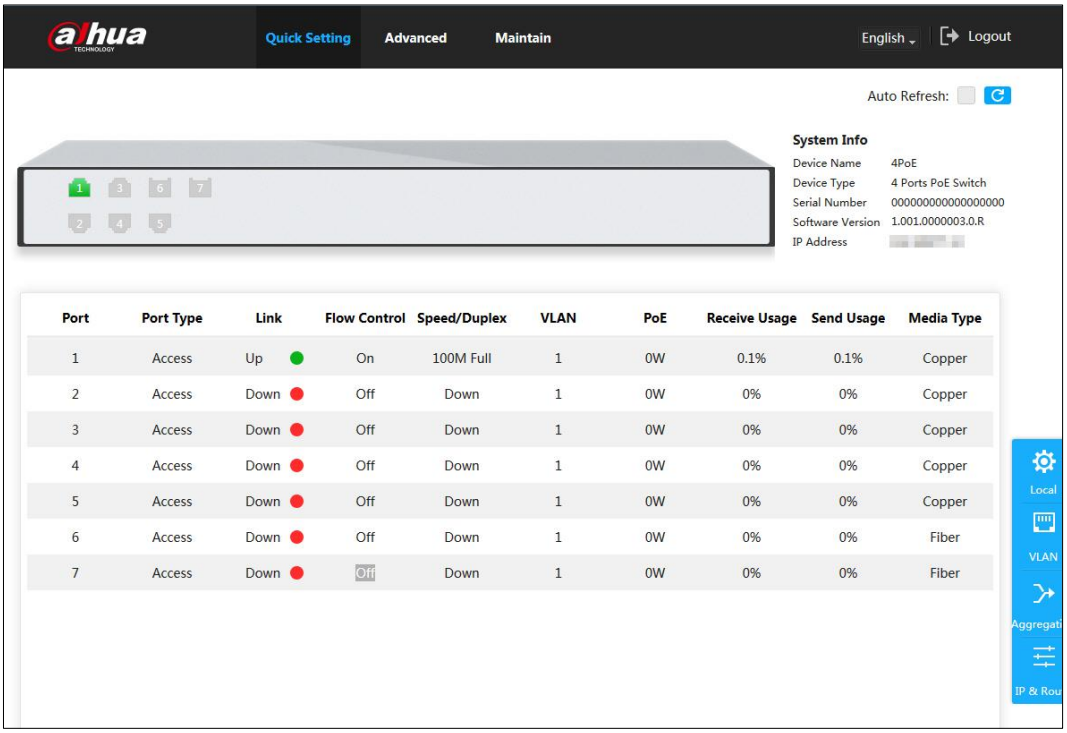


Tabla 2-1 Información del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador. Este conmutador contiene 7 puertos. La cantidad de puertos puede variar según el modelo que compró, y prevalecerá el producto real. Tres tipos: **Acceso, Híbrido,** y **Maletero.**
Tipo de puerto	
Enlace	Dos estados de enlace: **Arriba** y **Abajo. Arriba** indica que el puerto está conectado correctamente y **Abajo** indica que el puerto no está conectado o la conexión falla.
Control de flujo	Muestra el estado de control de flujo.

Parámetro	Descripción
Velocidad / Dúplex	• En línea: muestra la velocidad del puerto y el modo dúplex. Fuera de línea: • muestra **Abajo.**
VLAN	Puerto VLAN. Es la VLAN 1 de forma predeterminada.
POE	Muestra el consumo de energía de POE. Solo 1 a 4 puertos son puertos PoE. La velocidad de
Recibir uso	recepción actual se divide por la velocidad media en un período determinado (normalmente 5 minutos).
Enviar uso	La velocidad de envío actual se divide por la velocidad media en un período determinado (normalmente 5 minutos).
Tipo de medio	Dos tipos de medios: **Cobre** y **Fibra. Cobre** indica el puerto RJ-45 y **Fibra** indica puerto de fibra.

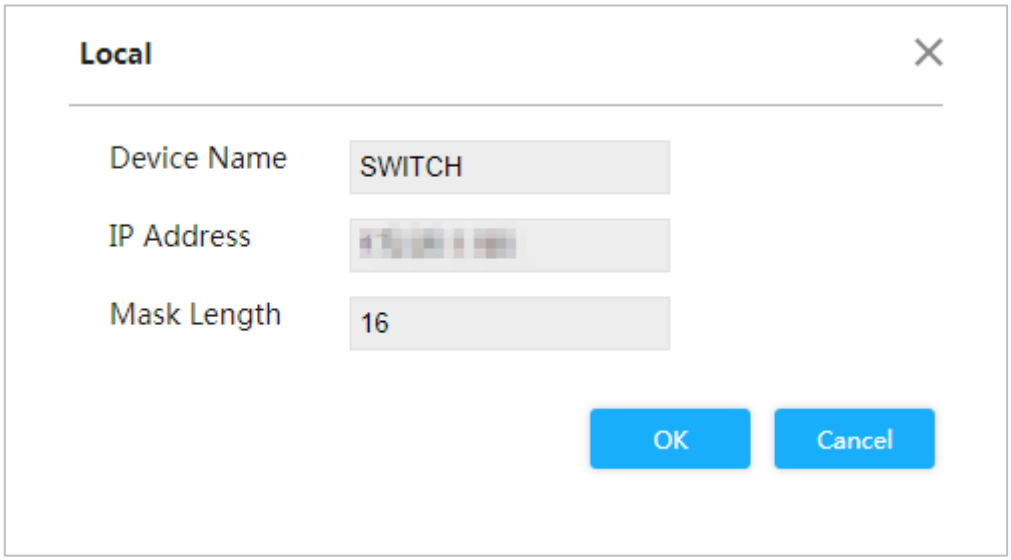
2.2 Local

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

Paso 1 clic **Local** a la derecha de **Ajuste rapido** interfaz.

los **Local** se muestra la interfaz. Vea la Figura 2-2.

Figura 2-2 Local



Paso 2 Introduzca el nombre del sistema, la dirección IP y la longitud de la máscara.

Paso 3 Haga clic en **OKAY.**

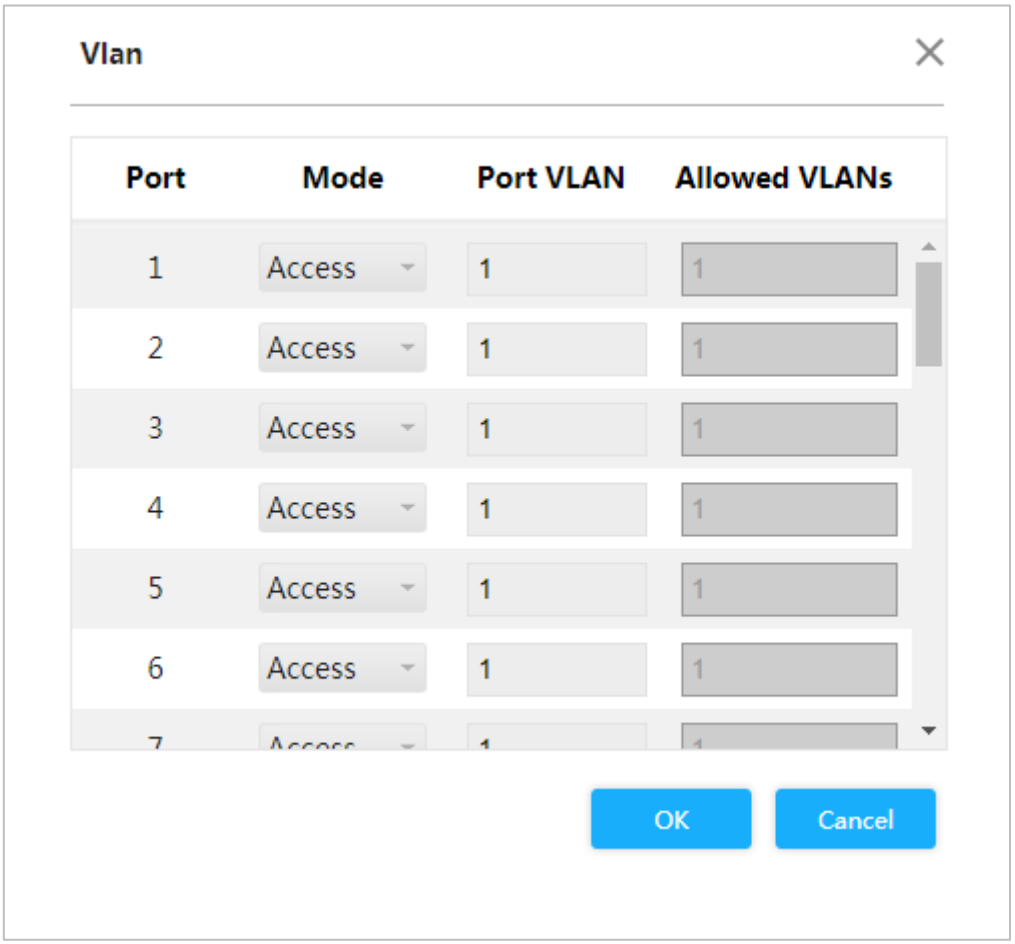
2.3 VLAN

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

Paso 1 clic **Vlan** sobre el **Ajuste rapido** interfaz.

los **Vlan** se muestra la interfaz. Vea la Figura 2-3.

Figura 2-3 VLAN



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

Tabla 2-2 Parámetro de configuración de la VLAN del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador. Tres modos: **Acceso,**
Modo	**Híbrido,** y **Maletero.** • **Acceso:** Cuando el puerto se conecta a dispositivos terminales (como PC e IPC), seleccione **Acceso.** • **Maletero:** Cuando el puerto se conecta al conmutador, seleccione **Maletero. 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 **Maletero,** puedes configurarlo.

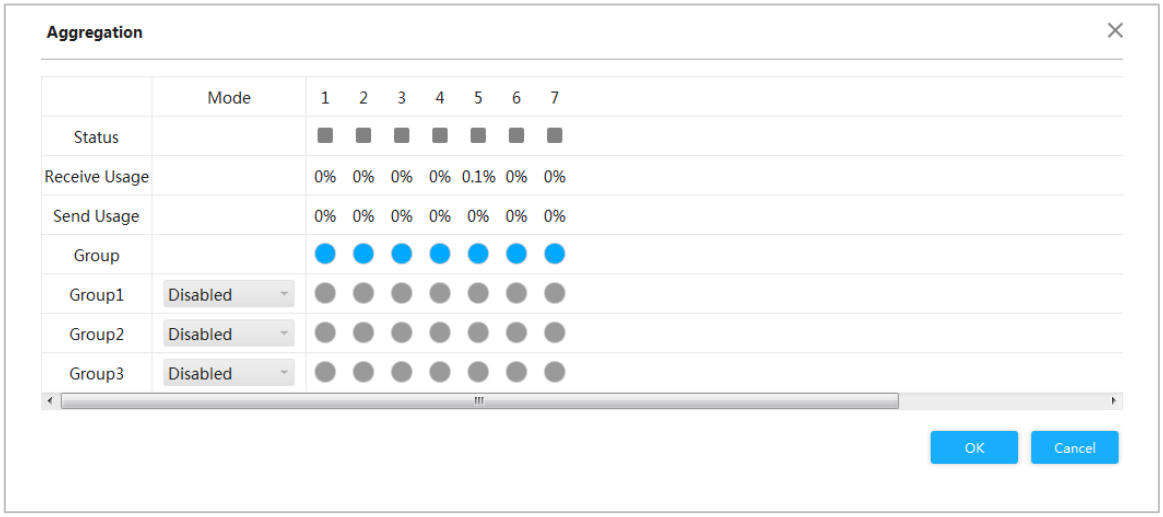
Paso 3 Haga clic en **OKAY.**

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. Vea la Figura 2-4.

Figura 2-4 Agregación



2.4.1 Configuración de agregación estática

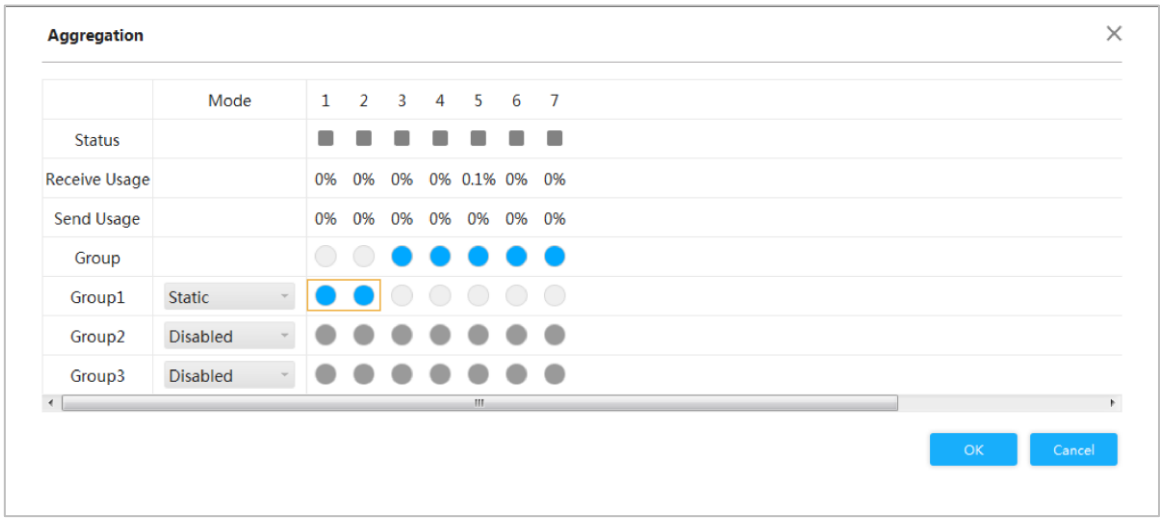
La agregación estática es un método para combinar o agrupar varios puertos de conmutador o NIC para formar un solo canal de ethernet. Por ejemplo, agregue el puerto 1 y el puerto 2 al Grupo estático 1.

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

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

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

Figura 2-5 Configuración estática



Paso 3 Haga clic en **OKAY.**

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

2.4.2 Configuración de agregación dinámica

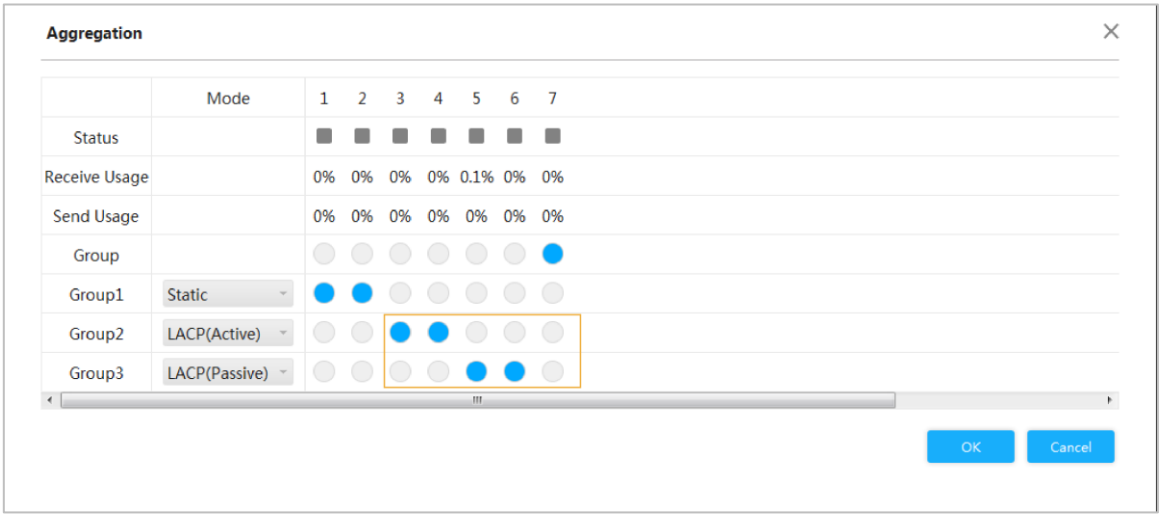
La agregación dinámica se diferencia de la agregación estática en que la cantidad de puerto se fija en la agregación estática, pero la cantidad de puerto realmente agregado se ajusta dinámicamente de acuerdo con la estrategia de caudal.

Paso 1 Agregue los puertos al grupo dinámico.

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

2)

Figura 2-6 Configuración dinámica



Paso 2 Haga clic en **OKAY.**

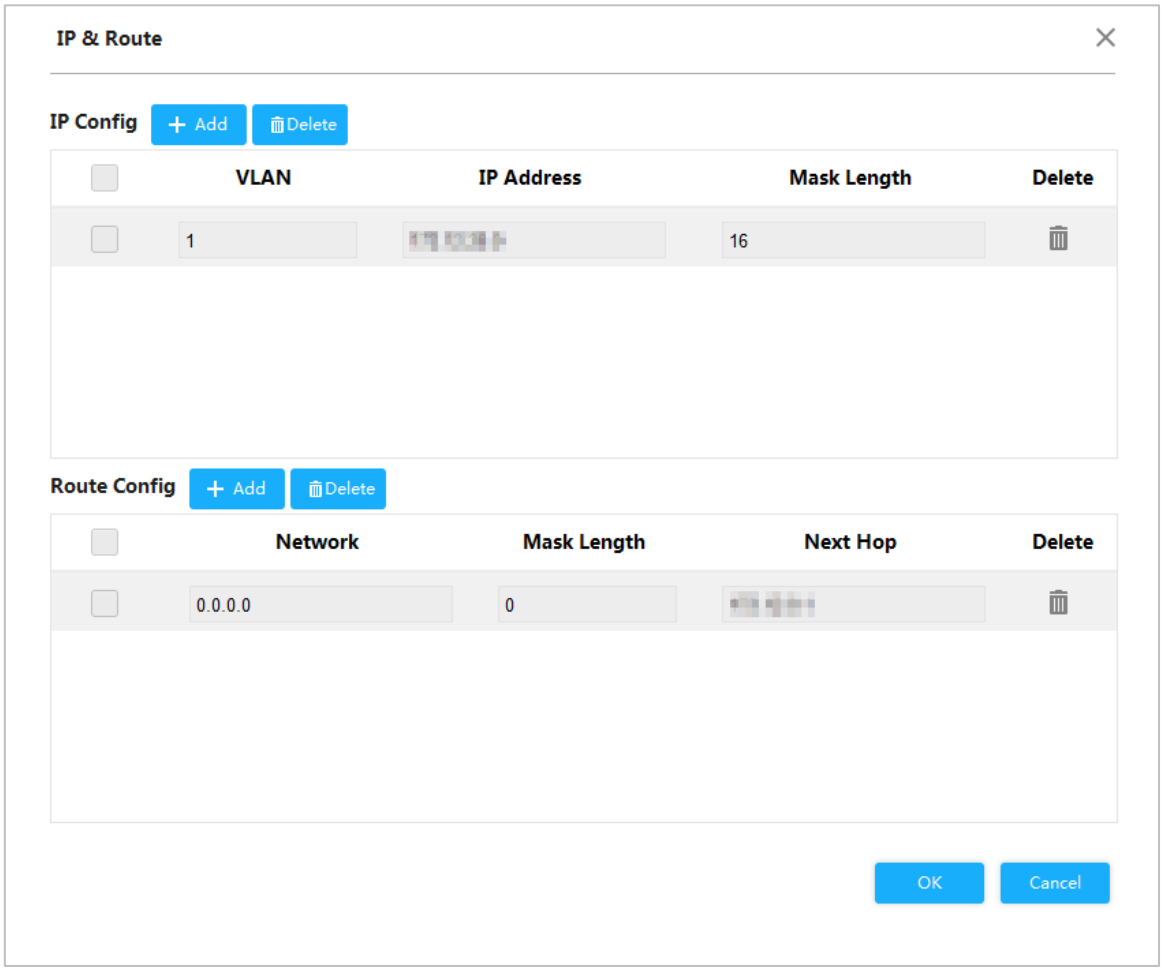
2.5 IP y ruta

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 clic **IP y ruta** sobre el **Ajuste rapido** interfaz.

los **IP y ruta** se muestra la interfaz. Vea la Figura 2-7.

Figura 2-7 IP y ruta



Paso 2 Agregue la interfaz VLAN.

1) Haga clic en **Añadir** en el **Configuración de IP** zona.

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

Figura 2-8 Interfaz VLAN

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

Tabla 2-3 Interfaz VLAN

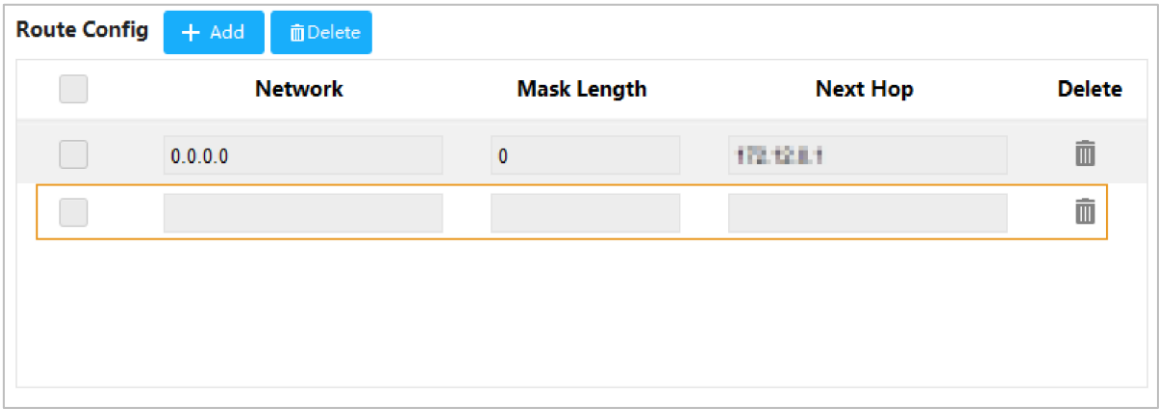
Parámetro	Descripción
VLAN	Ingrese el número de VLAN.
dirección IP	Configure la dirección IP de la interfaz VLAN. Configure la
Longitud de la máscara	longitud de la máscara de la interfaz VLAN.

Paso 3 Agregue la ruta IP.

1) Haga clic en **Añadir** en el **Configuración de ruta** zona.

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

Figura 2-9 Ruta IP



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

Tabla 2-4 rutas IP

Parámetro	Descripción
Red	Es el destino del paquete IP.
Longitud de la máscara	La longitud de la máscara, con la dirección de destino, es para identificar la dirección IP del host de destino o la ruta. Después de un 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.

Paso 4 Haga clic en **OKAY.**

3 Ajustes avanzados

Puede configurar el sistema, puerto, VLAN, agregación, 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

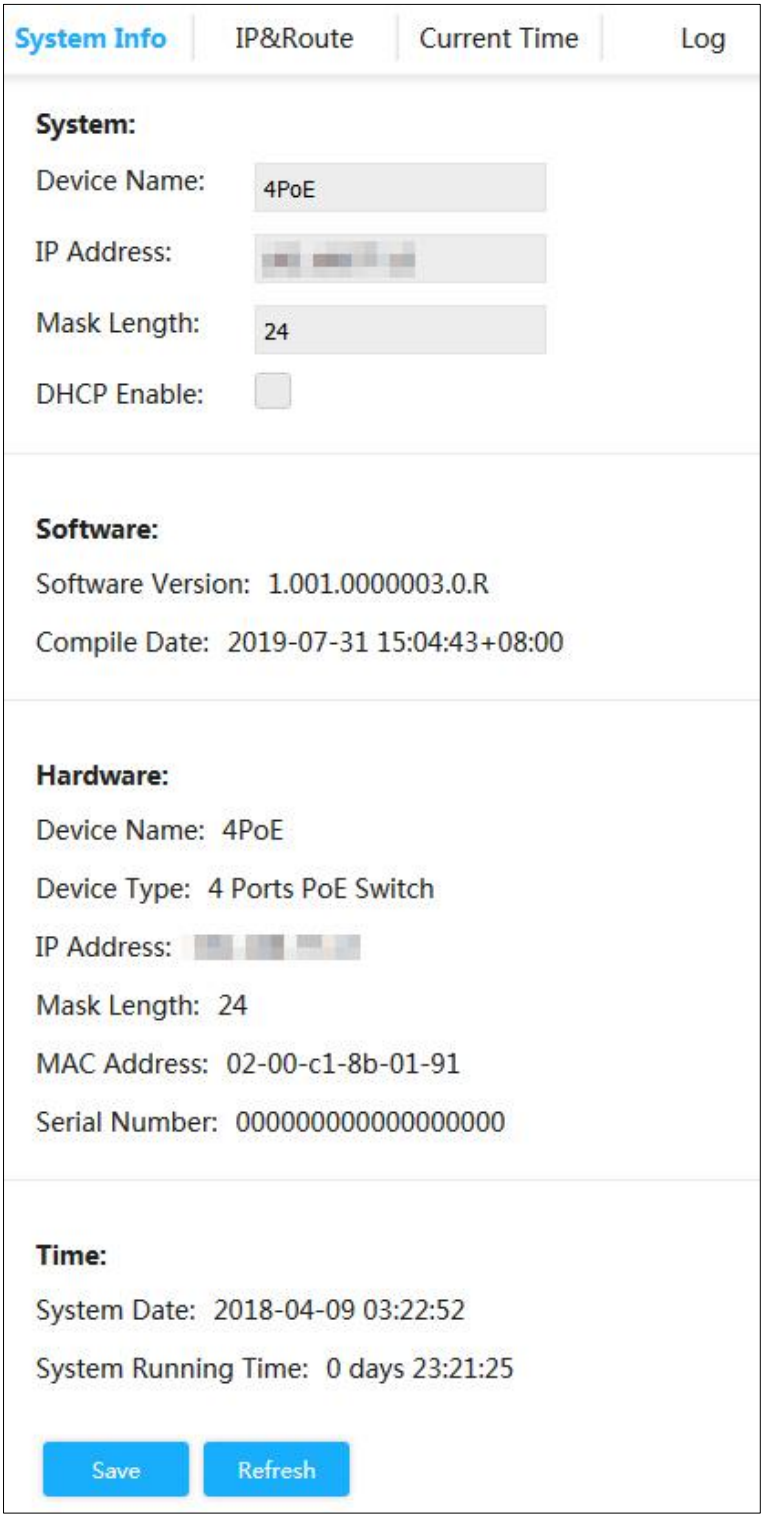
Puede configurar el nombre del dispositivo, la dirección IP, la longitud de la máscara y la activación de DHCP, y ver la información del software, la información del hardware y la hora.

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

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

los **Información del sistema** se muestra la interfaz. Vea la Figura 3-1.

Figura 3-1 Información del sistema



Paso 2 Introduzca el nombre del dispositivo, la dirección IP y la longitud de la máscara y la habilitación de DHCP.

Paso 3 Haga clic en **Salvar.**

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.

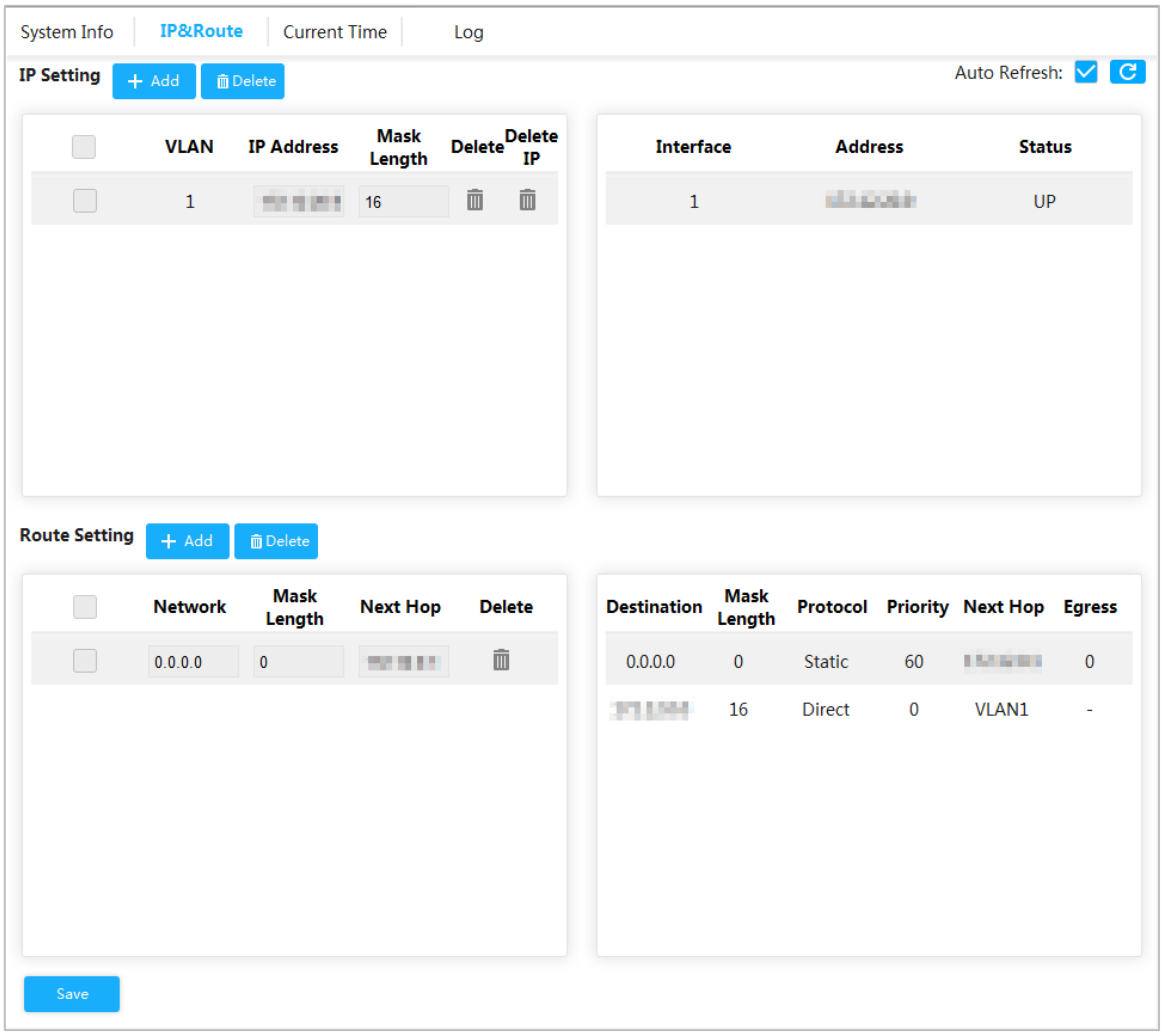
El conmutador admite el reenvío de capa 3 a través de la interfaz VLAN. La interfaz VLAN es la interfaz virtual del modo de capa 3, para la comunicación de capa 3 entre las VLAN. No es lo fisico

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

Paso 1 Seleccione **Avanzado> Común> Configuración del sistema> IP y ruta.**

los **IP y ruta** se muestra la interfaz. Vea la Figura 3-2.

Figura 3-2 IP y ruta

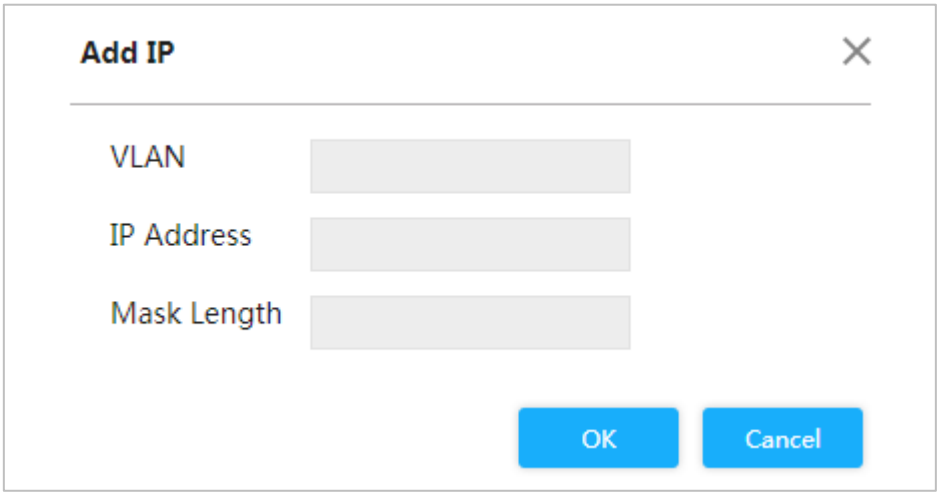


Paso 2 Agregue la interfaz VLAN.

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

los **Agregar IP** se muestra la interfaz. Vea la Figura 3-3.

Figura 3-3 Agregar IP



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

Tabla 3-1 Interfaz VLAN

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

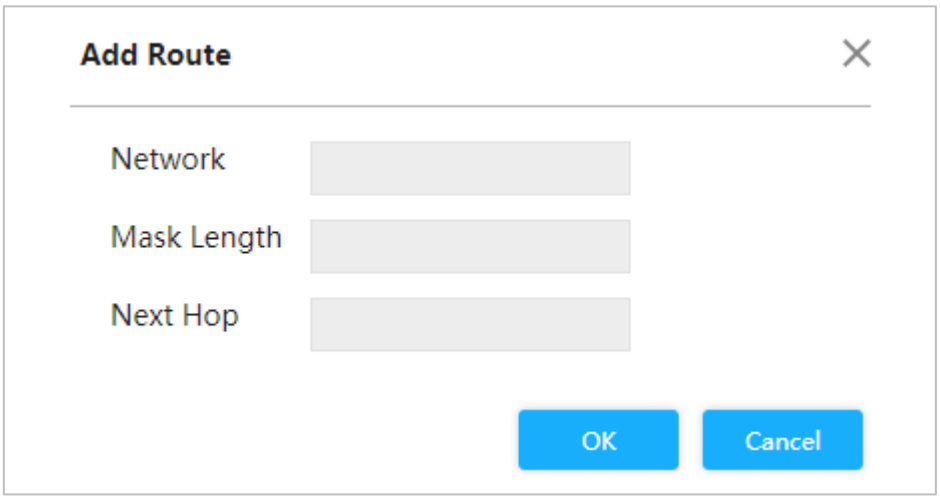
3) Haga clic en **OKAY.**

Paso 3 Agregue la ruta IP.

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

los **Agregar ruta** se muestra la interfaz. Vea la Figura 3-4.

Figura 3-4 Agregar ruta



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

Tabla 3-2 Rutas IP

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

3) Haga clic en **OKAY.**

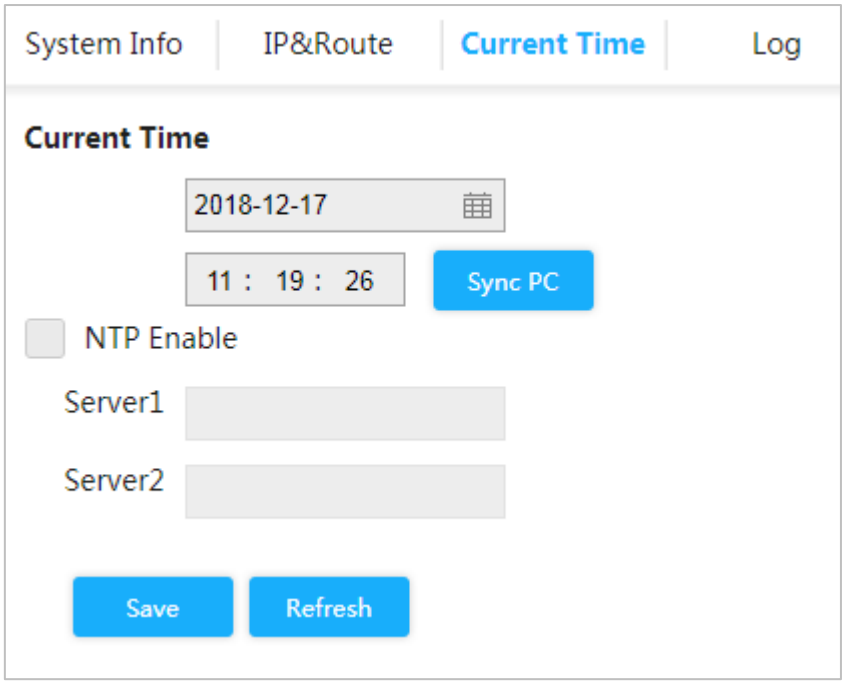
Paso 4 Haga clic en **Salvar.**

3.1.1.3 Hora del sistema

Establezca la hora del sistema de cambio. Seleccione **Avanzado> Común> Configuración del sistema> Hora actual.**

los **Tiempo actual** se muestra la interfaz. Vea la Figura 3-5.

Figura 3-5 Hora actual (1)



Puede configurar la hora del sistema mediante los siguientes tres métodos:

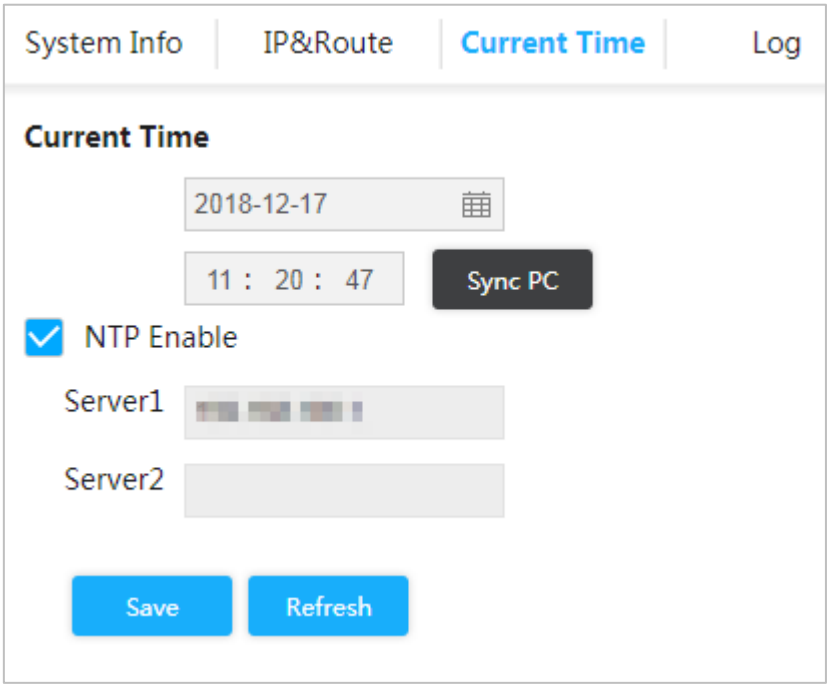
- Establecer la hora manualmente Establecer la fecha y la hora en **Tiempo actual** interfaz y luego haga clic en **Salvar.**
- Tiempo de sincronización

  Hacer clic **Sincronizar PC,** y la hora del cambio se sincroniza automáticamente con la hora local de la PC. Sincronizar la hora del servidor NTP
- Solo con el servidor NTP configurado en la red puede habilitar esta función en los siguientes pasos:

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

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

Figura 3-6 Hora actual (2)



Paso 3 Haga clic en **Salvar.**

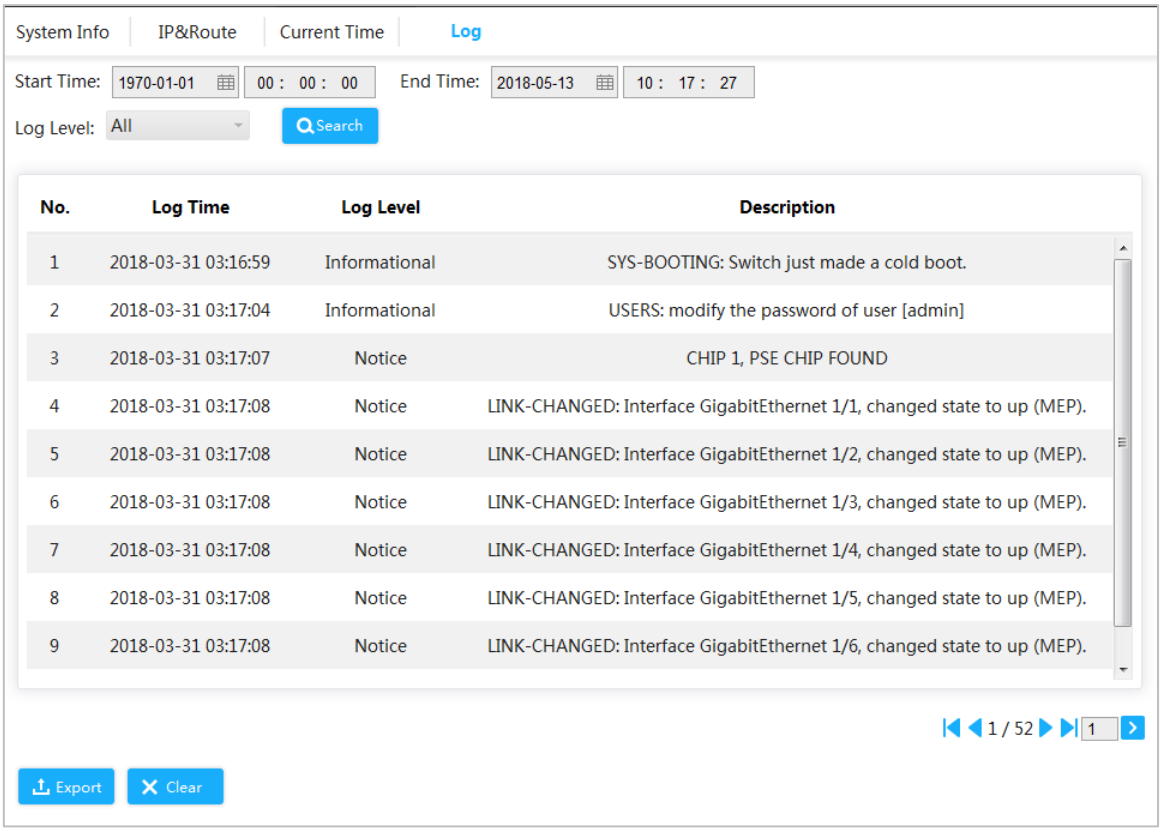
La hora de cambio se sincroniza automáticamente con la hora del servidor 1.

3.1.1.4 Registro

Puede ver registros, exportar registros y borrar registros.

Seleccione **Avanzado> Común> Configuración del sistema> Registro.** los **Iniciar sesión** se muestra la interfaz. Vea la Figura 3-7.

Figura 3-7 Registro



- Ver los registros.

  Configure 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.

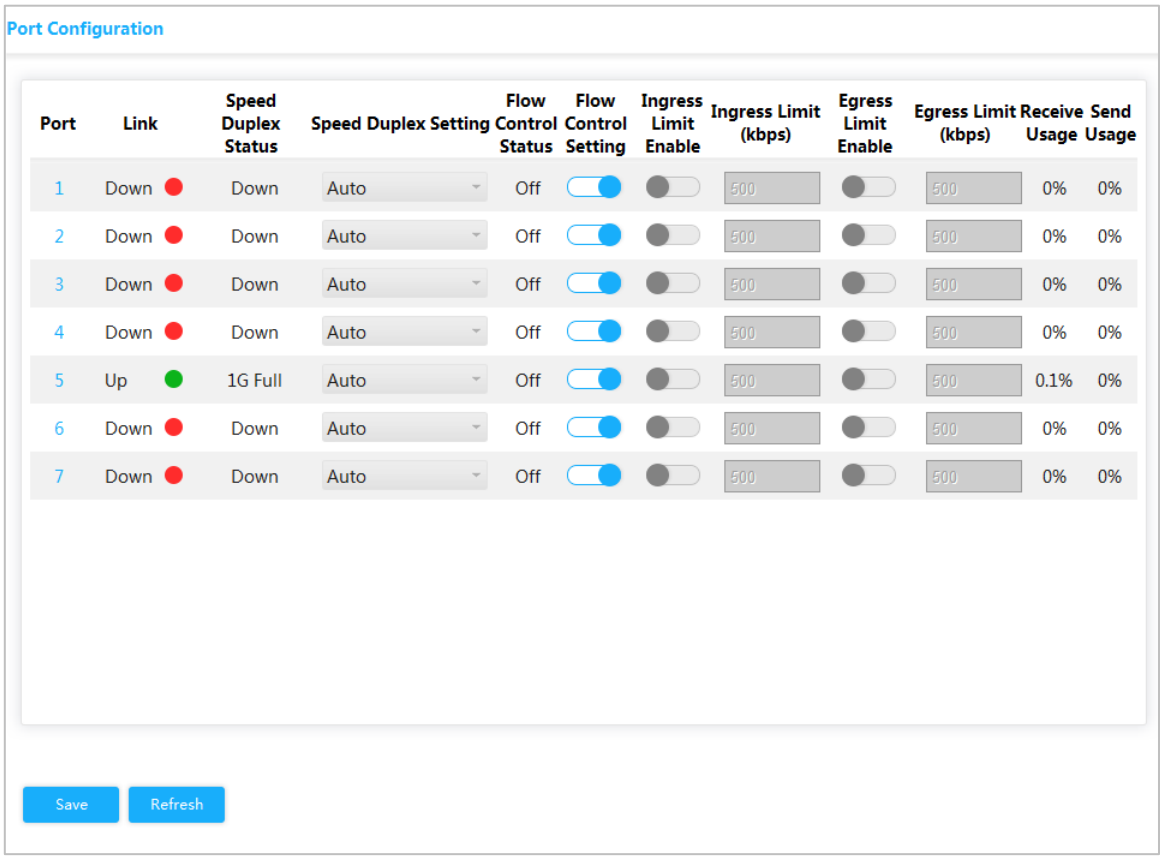
3.1.2 Configuración de puerto

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

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

los **Configuración del puerto** se muestra la interfaz. Vea la Figura 3-8.

Figura 3-8 Configuración del puerto



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

Tabla 3-3 Parámetro de puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador. Verde **Arriba** indica que el puerto está conectado
Enlace	correctamente y rojo **Abajo** indica que el puerto no está conectado o la conexión falla.
Estado dúplex de velocidad	**Abajo** significa desconexión, y la velocidad específica significa conexión exitosa. **Completo** significa dúplex completo; **Medio** significa semidúplex. Configure
Ajuste de velocidad dúplex	la velocidad y el modo dúplex.

Parámetro	Descripción
Estado de control de flujo	Muestra el negociador real del control de flujo o el estado de habilitación, incluidos ON y OFF. • ON: La negociación se realiza correctamente. • APAGADO: La negociación falla.
Configuración de control de flujo	Función de control de flujo ON / OFF. • : El control de flujo está encendido. • : El control de flujo está APAGADO.
Límite de ingreso habilitado	Activar / desactivar 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.
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. Muestra el
Enviar uso	uso de envío.

Paso 3 Haga clic en **Salvar.**

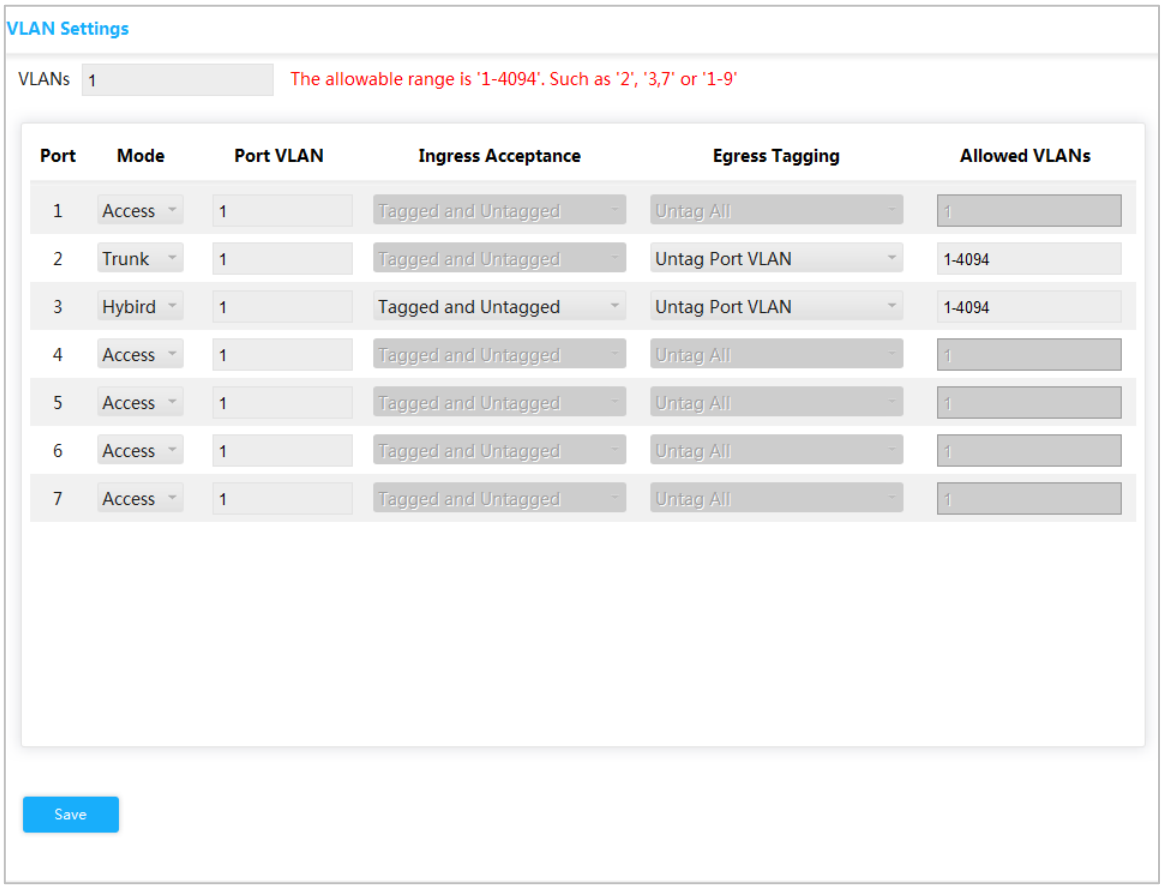
3.1.3 Configuración de VLAN

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

Paso 1 Seleccione **Avanzado> Común> Configuración de VLAN.**

los **Configuración de VLAN** se muestra la interfaz. Vea la Figura 3-9.

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 la VLAN del puerto. Consulte la Tabla 3-4.

Tabla 3-4 Parámetro de configuración de la VLAN del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador. Tres modos: **Acceso,**
Modo	**Híbrido,** y **Maletero.**
Puerto VLAN	Agregue el puerto a una VLAN. De forma predeterminada, el puerto pertenece a VLAN1. El rango es 1–4094.
Aceptación de ingreso	Muestra si los datos pueden fluir hacia el puerto. Solamente **Híbrido** admite la configuración (por defecto, 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. • **Solo etiquetado:** Solo los datos etiquetados pueden fluir hacia el puerto. • **Solo sin etiquetar:** Solo los datos sin etiquetar pueden ingresar al puerto. Muestra si se
Etiquetado de salida	deben etiquetar los datos que saldrán del puerto. Vea las siguientes tres situaciones: • **Desmarcar VLAN del puerto:** Si la etiqueta de flujo de datos es la misma que PVID, la etiqueta se despegará. • **Etiquetar todo:** Todos los datos serán etiquetados. • **Desmarcar todo:** No se etiquetarán todos los datos. Configure
VLAN permitidas	la VLAN permitida.

Paso 4 Haga clic en **Salvar.**

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 se pueden considerar como un enlace lógico con mayor ancho de banda.

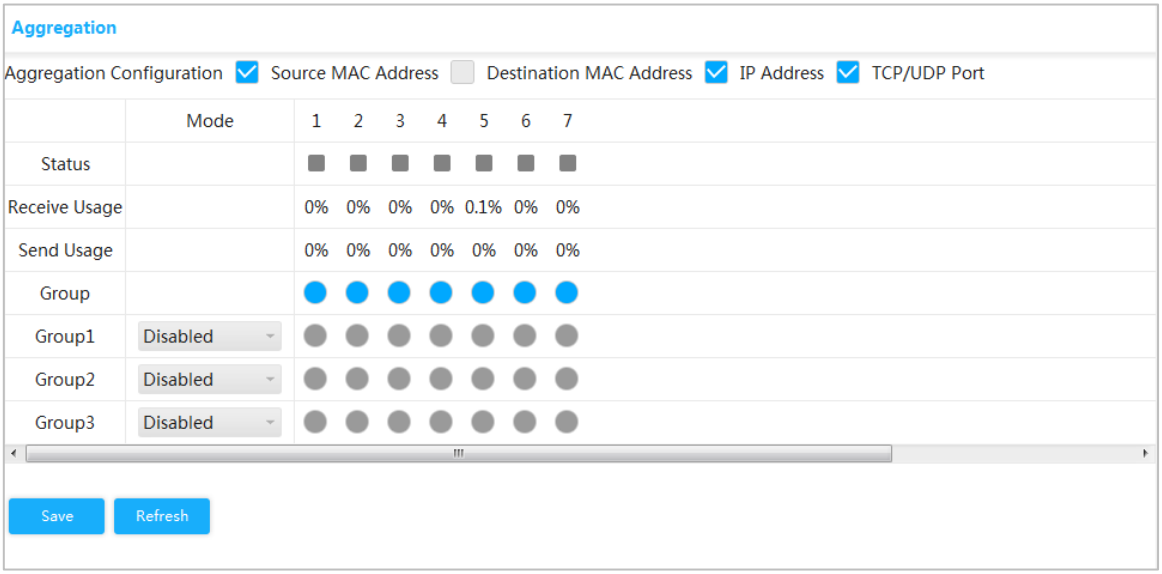
A través de la agregación, los puertos del mismo grupo pueden compartir el flujo de comunicación para hacer un ancho de banda mayor. Además, los puertos del mismo grupo pueden realizar copias de seguridad de forma recíproca y dinámica para mejorar la fiabilidad del enlace.

3.1.4.1 Configuración estática

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

los **Agregación** se muestra la interfaz. Vea la Figura 3-10.

Figura 3-10 Agregación



Paso 2 Seleccione el modo de algoritmo de equilibrio de carga de agregación en **Configuración de agregación.**

Hay cuatro tipos:

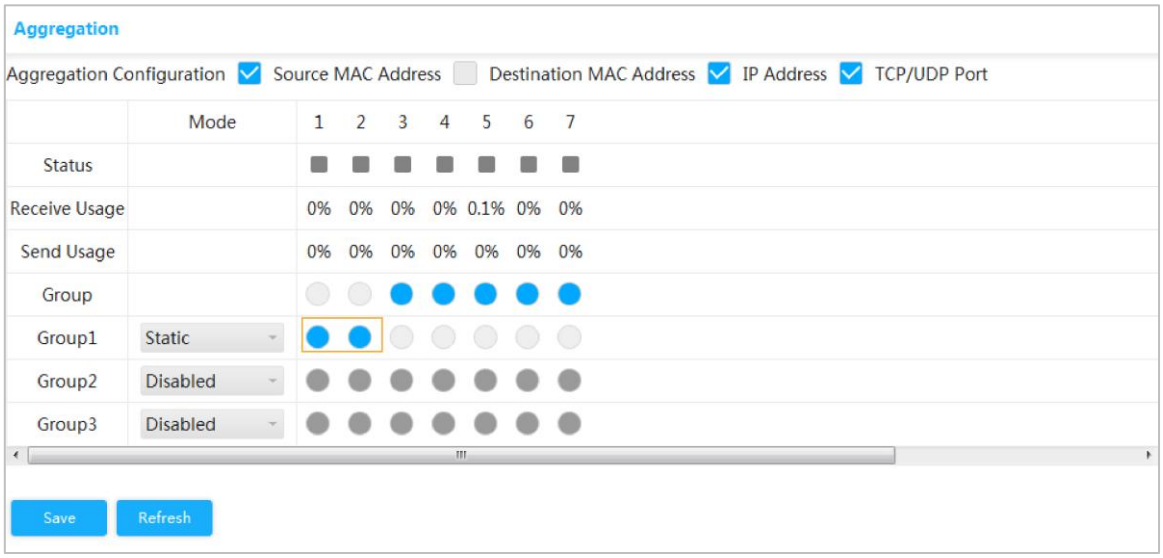
- Dirección MAC de origen: el algoritmo de equilibrio de carga de agregación basado en la dirección MAC.
- Dirección MAC de destino: el algoritmo de equilibrio de carga de agregación basado en la dirección MAC de destino.
- Dirección IP: el algoritmo de equilibrio de carga de agregación basado en la 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 Seleccione **Estático** en el **Modo** área y agregue los puertos al grupo de agregación dinámica.

Por ejemplo, agregue el puerto 1 y el puerto 2 al grupo de agregación. Vea la Figura 3-11.

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

Figura 3-11 Configuración estática



Paso 4 Haga clic en **Salvar.**

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:

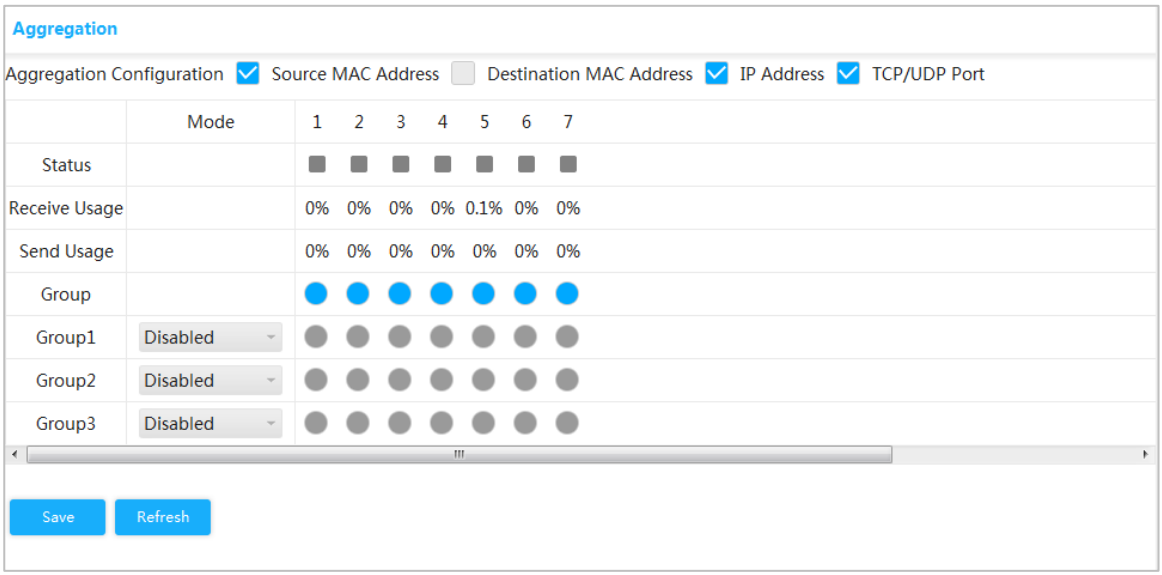
- **Activo:** El puerto puede enviar paquetes LACPDU activamente al puerto opuesto y analiza el LACP.

- **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 Seleccione **Avanzado> Común> Agregación.**

los **Agregación** se muestra la interfaz. Vea la Figura 3-12.

Figura 3-12 LACP (1)



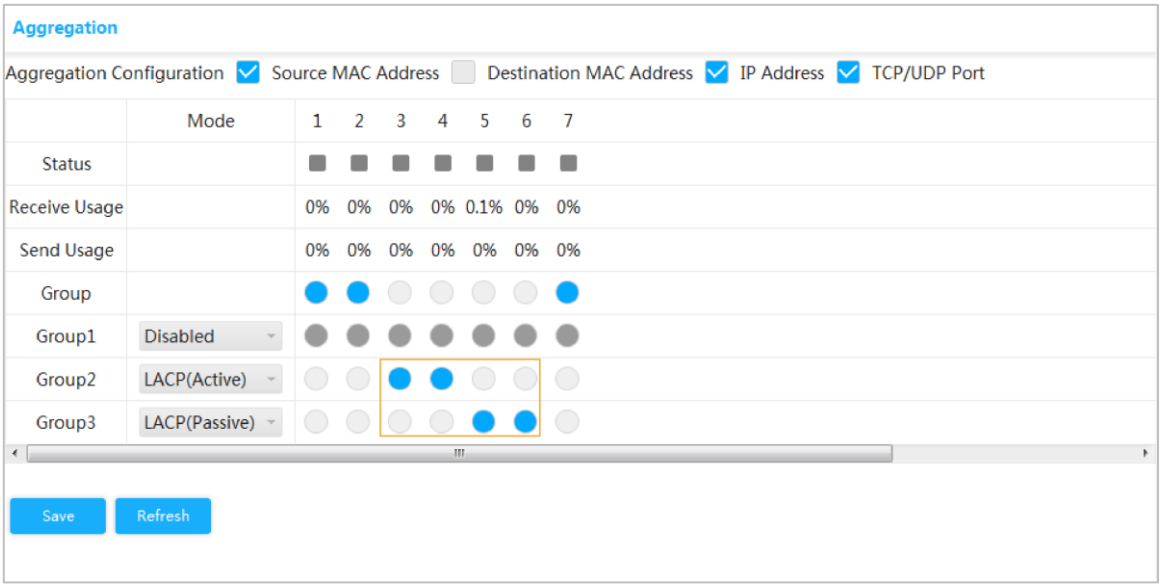
Paso 2 Seleccione **LACP (pasivo)** en el **Modo** área y agregue el miembro del puerto a la dinámica

grupo de agregación. Por ejemplo, agregue el puerto 3 y el puerto 4 al Grupo de agregación 2. Consulte la Figura 3-13.

Paso 3 Seleccione **LACP (pasivo)** en el **Modo** área y agregue el miembro del puerto a la dinámica

grupo de agregación. Por ejemplo, agregue el puerto 5 y el puerto 6 al Grupo de agregación 3. Consulte la Figura 3-13.

Figura 3-13 LACP (2)



Paso 4 Haga clic en **Salvar.**

3.1.5 Tabla MAC

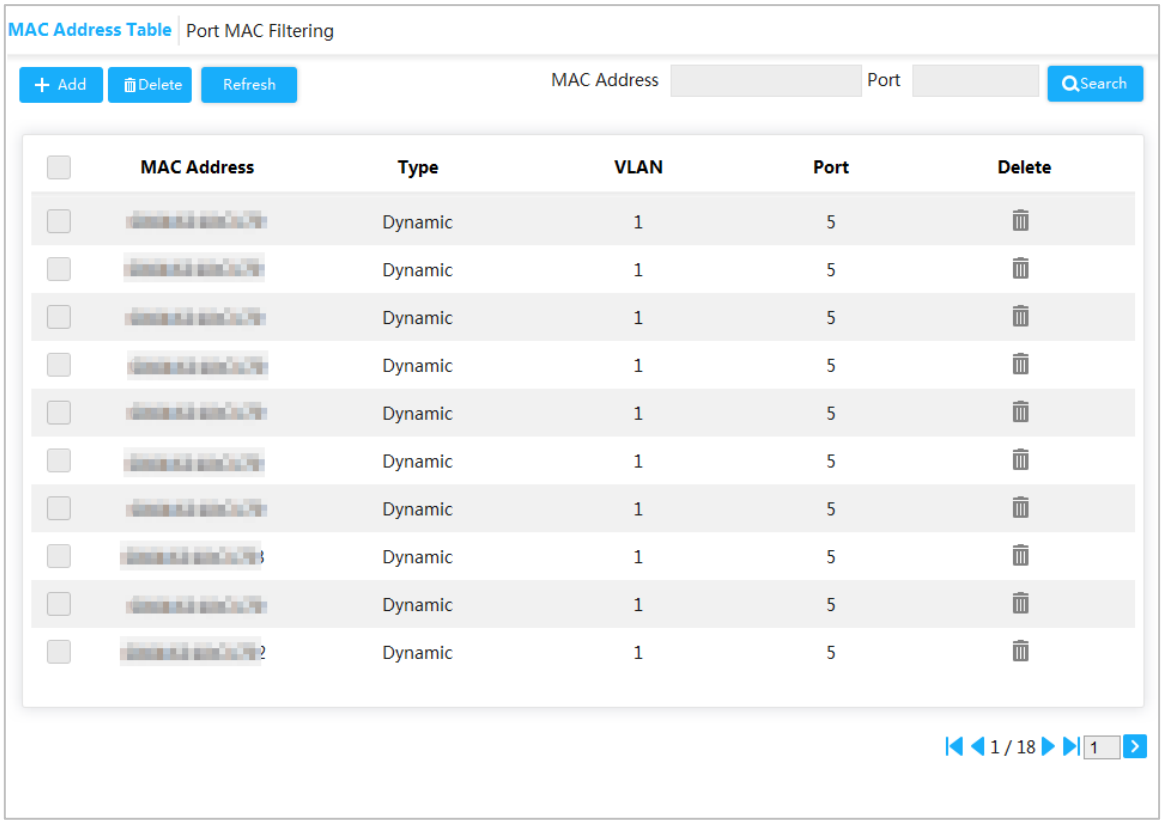
La tabla MAC (Media Access Control) registra la relación entre la dirección MAC y el puerto, y la información, incluida la VLAN a la que pertenece el puerto. Cuando el dispositivo reenvía el paquete, consulta en la tabla de direcciones MAC la dirección MAC de destino del paquete. Si la dirección MAC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

3.1.5.1 Agregar tabla MAC estática

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

los **Tabla de direcciones MAC** se muestra la interfaz. Vea la Figura 3-14.

Figura 3-14 Tabla de direcciones MAC



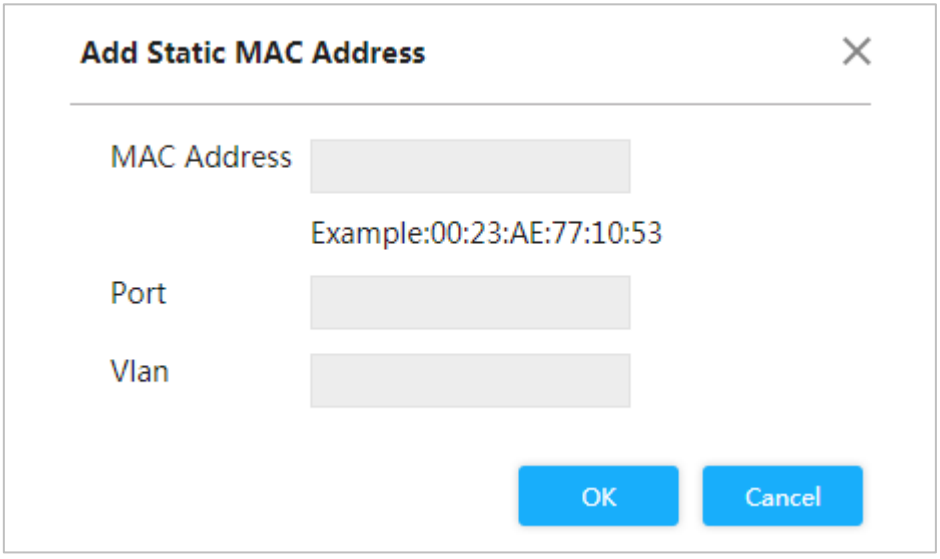
Paso 2 Vincule la dirección MAC al puerto en la VLAN determinada. Por ejemplo, vincula el MAC dirección 00: 00: 00: 00: 00: 01 al puerto 3 en la VLAN 2.

1) Haga clic en **Añadir.**

los **Agregar dirección MAC estática** se muestra la interfaz.

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

Figura 3-15 Agregar una tabla MAC estática



3) Haga clic en **OKAY.**

3.1.5.2 Filtrado MAC de puerto

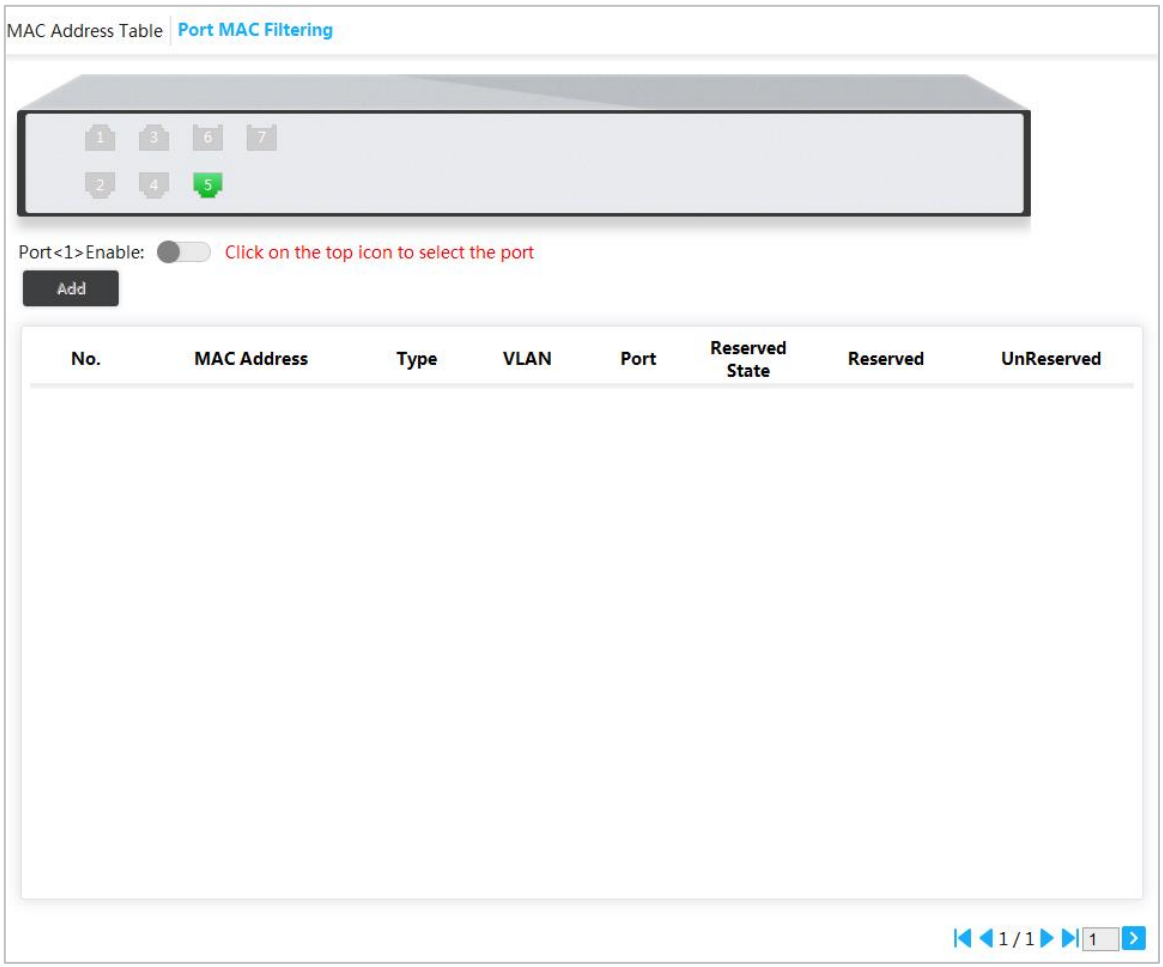
Después de habilitar el filtrado MAC del puerto, los siguientes dos dispositivos MAC pueden comunicarse con el puerto.

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

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

los **Filtrado MAC de puerto** se muestra la interfaz. Vea la Figura 3-16.

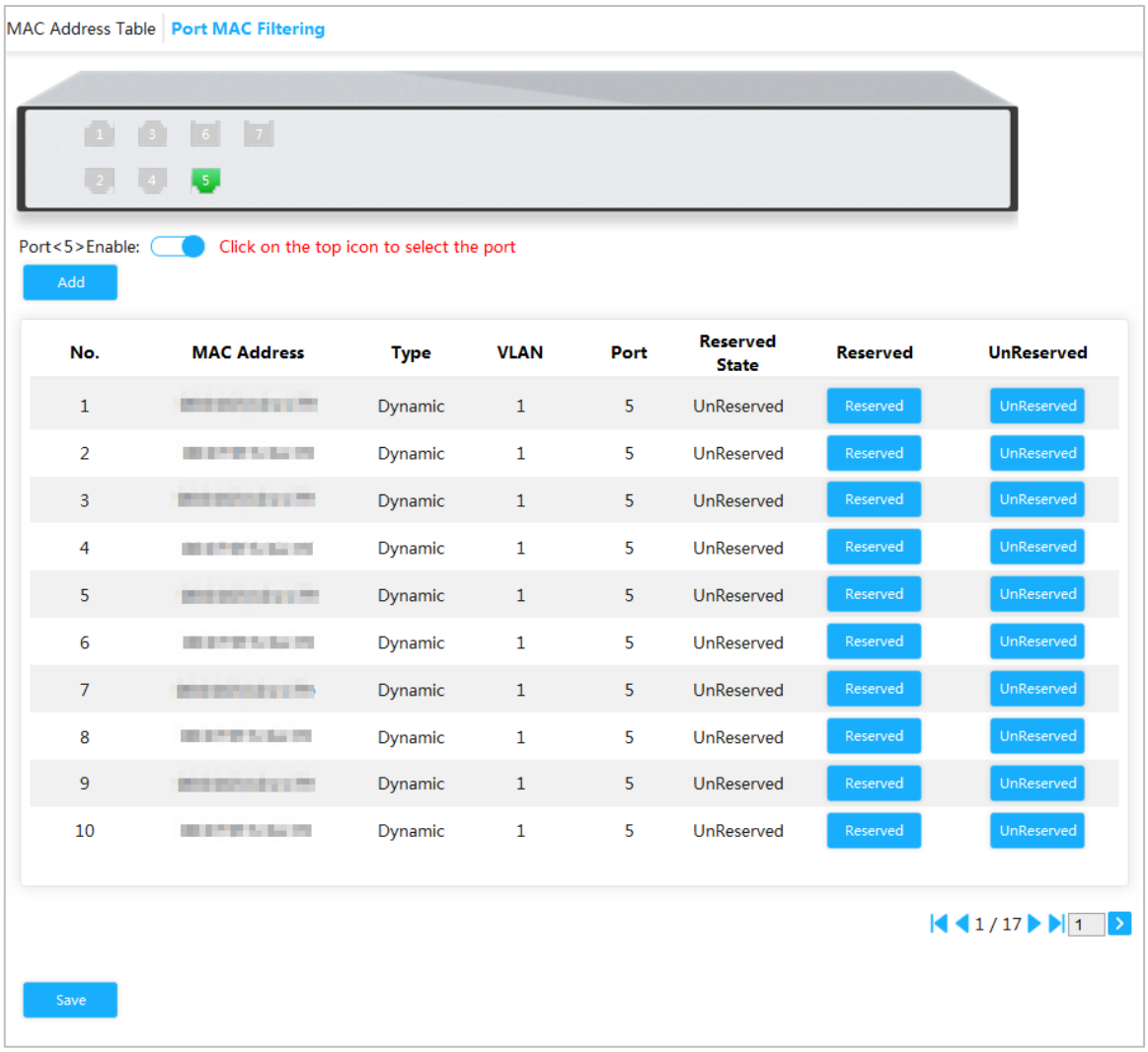
Figura 3-16 Filtrado MAC de puerto



Paso 2 Seleccione el puerto, como el puerto 5.

Paso 3 Haga clic en detrás **Puerto <5> Habilitar** para habilitar el puerto. Vea la Figura 3-17.

Figura 3-17 Habilitar el filtrado MAC del puerto



- Cambie el dispositivo MAC dinámico a estático. Seleccione

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

2) Hacer clic **Salvar.** El tipo cambia de **Dinámica** a **Estático.**

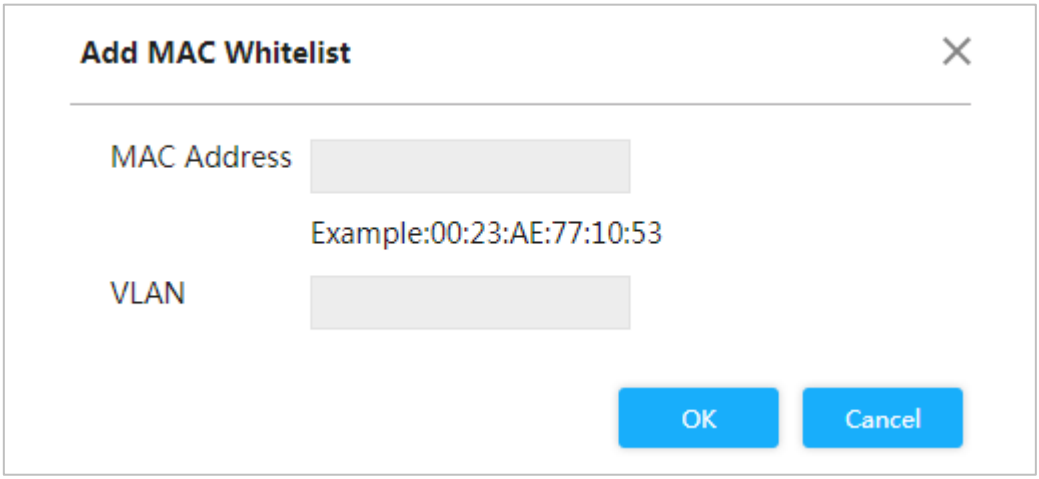
Los dispositivos MAC estáticos pueden comunicarse con el puerto normalmente. Agregar lista blanca de

- MAC.

1) Hacer clic **Añadir.**

los **Agregar lista blanca de MAC** se muestra la interfaz. Vea la Figura 3-18.

Figura 3-18 Agregar lista blanca de MAC.



2) Configure la dirección MAC y la VLAN.

3) Haga clic en **OKAY.**

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

3.1.6 Árbol de expansión

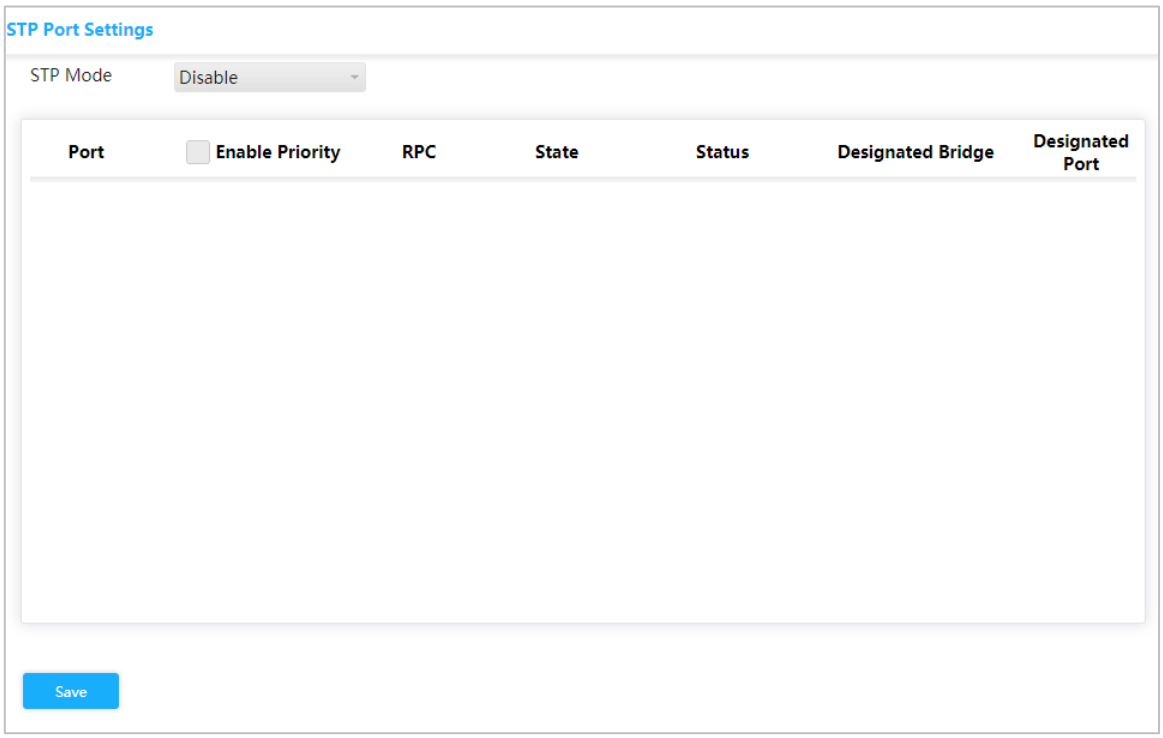
El protocolo de árbol de expansión es el protocolo de la capa 2. Puede eliminar el ciclo de anillo de la capa 2 eligiendo bloquear los enlaces redundantes en la red y puede hacer una copia de seguridad de los enlaces.

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), hasta RSTP (Protocolo de árbol de expansión rápido) y hasta el último MSTP (Protocolo de árbol de expansión múltiple).

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

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

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

Paso 3 Haga clic en **Salvar,** y los resultados son diversos según los diferentes modos. Ver figura 3-20, Figura 3-21 y Figura 3-22.

Figura 3-20 STP

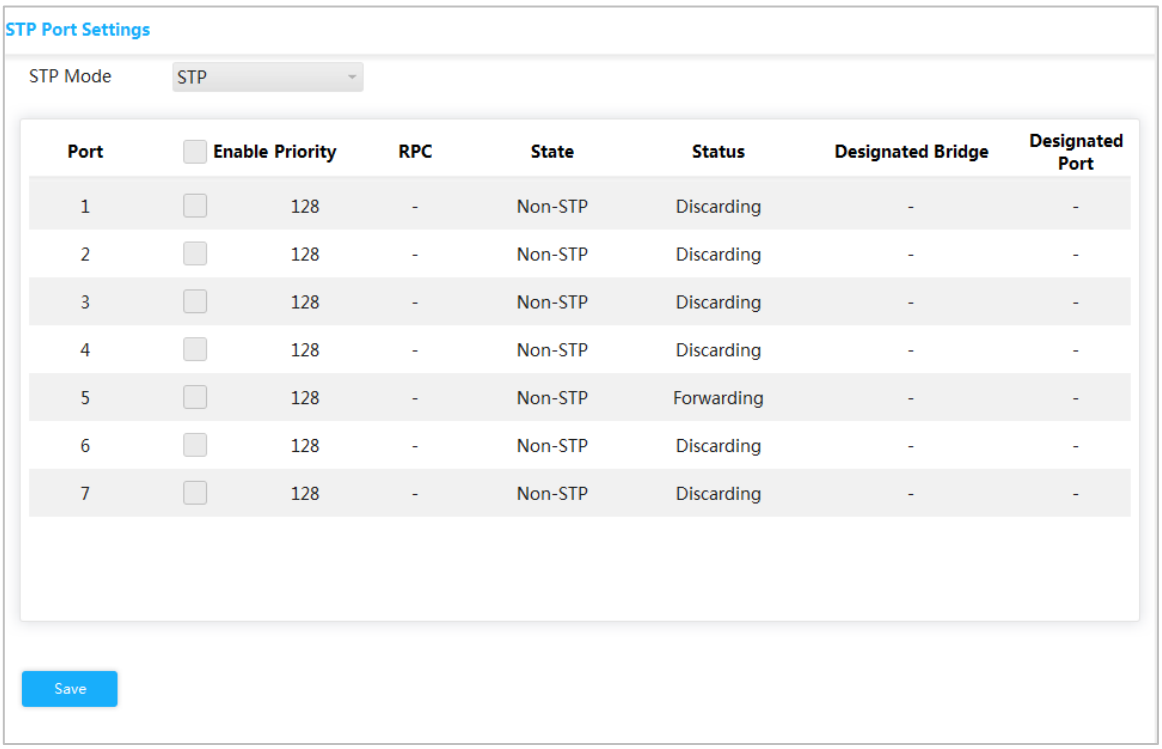


Figura 3-21 RSTP

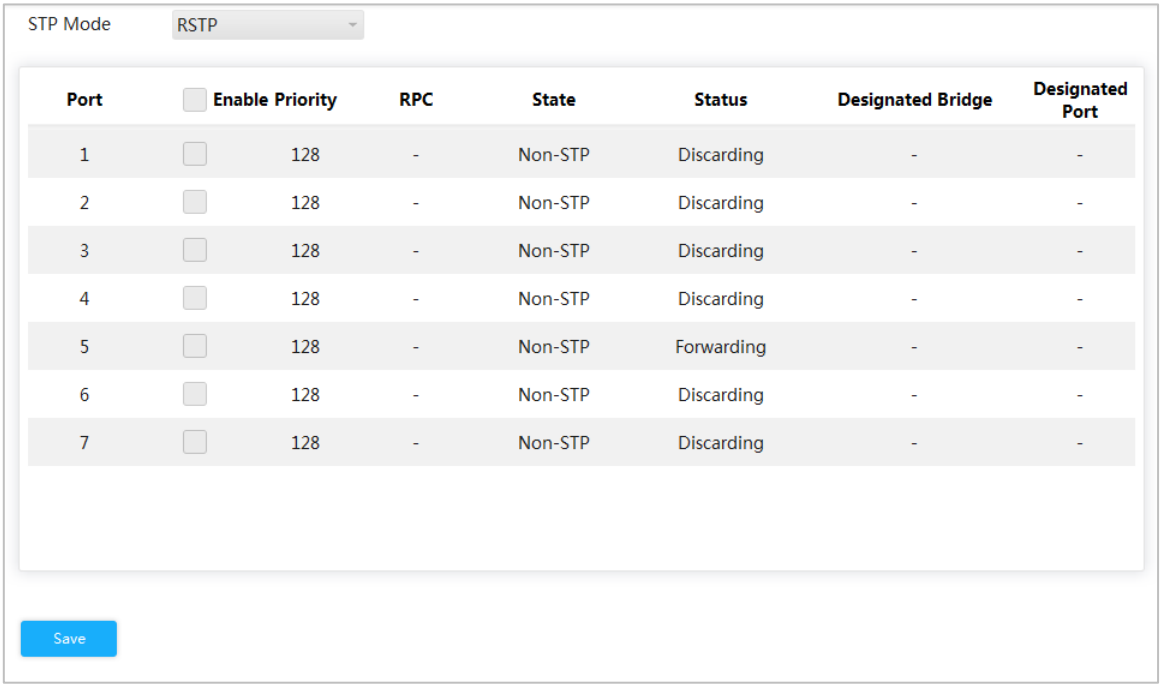
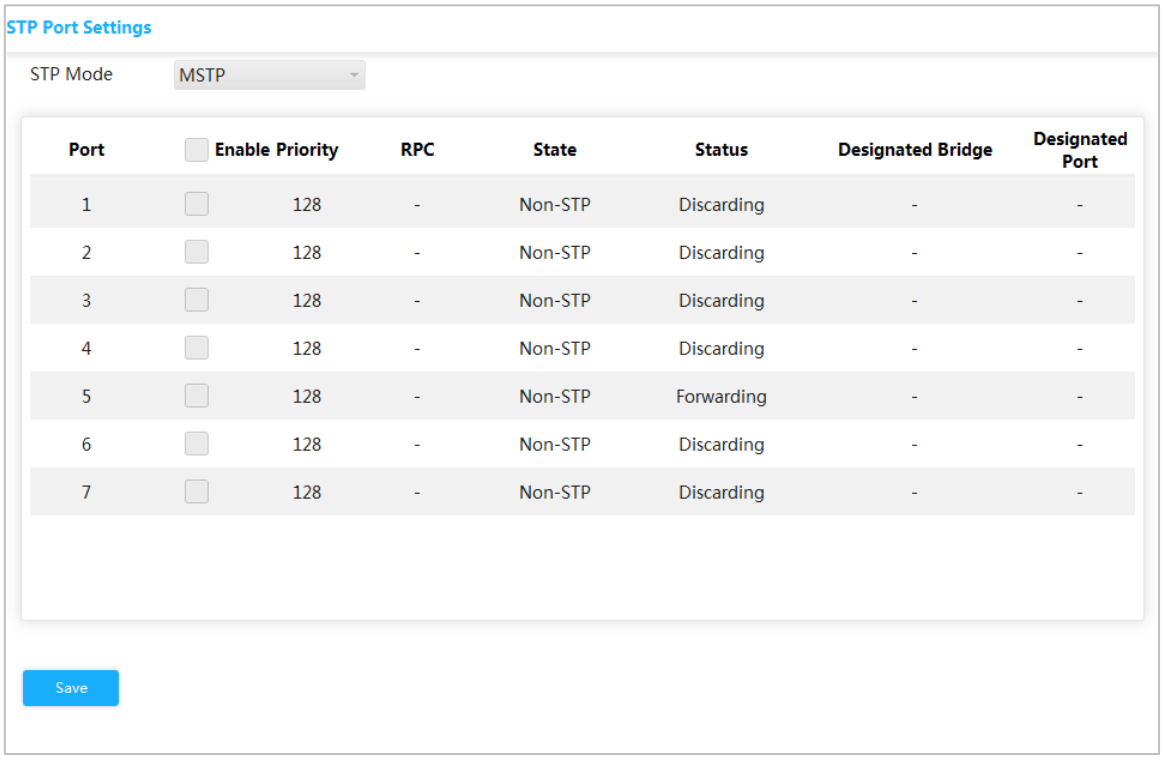
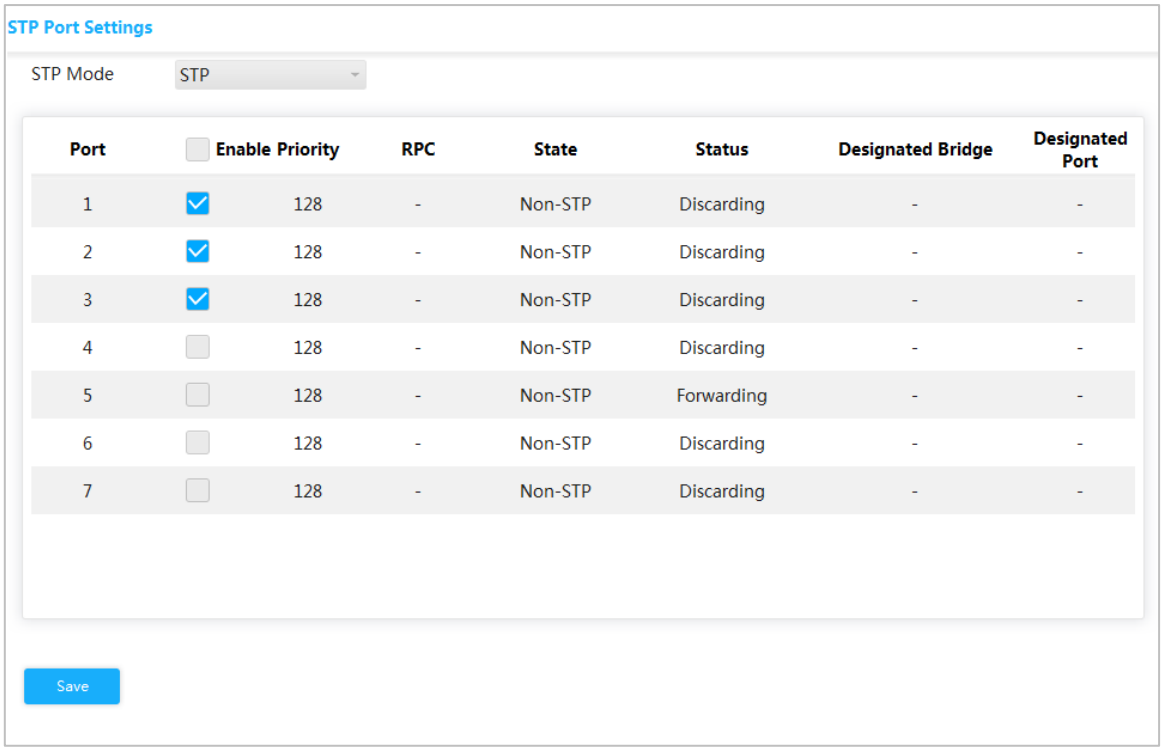


Figura 3-22 MSTP



Paso 4 Seleccione 3 puertos como mínimo para combinar un snoop STP / RSTP / MSTP. Por ejemplo: Puerto 1, el puerto 2 y el puerto 3 combinan un snoop STP. Vea la Figura 3-23.

Figura 3-23 Snoop de STP



Paso 5 Haga clic en **Salvar.**

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

3.2 Configuraciones de uso poco frecuente

3.2.1 ERPS

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

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

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

3.2.1.1 Configuración MEP

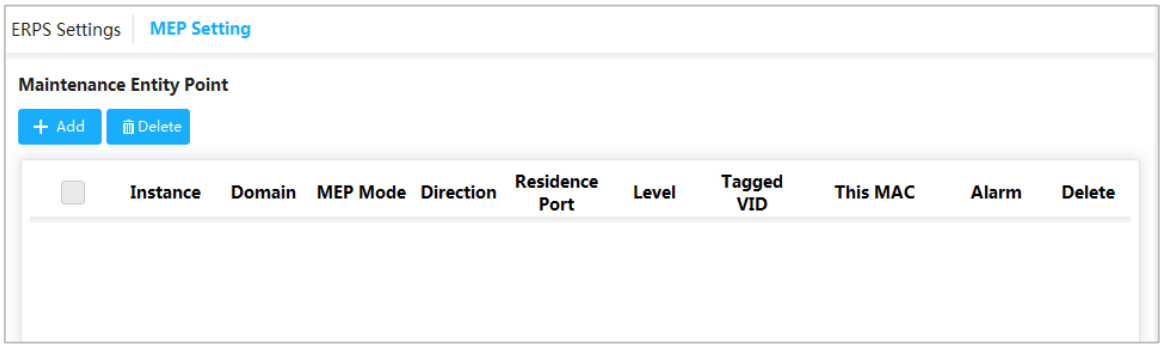
MEP (Maintenance Entity Point) es parte de ERPS.

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

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

los **Configuración MEP** se muestra la interfaz. Vea la Figura 3-24.

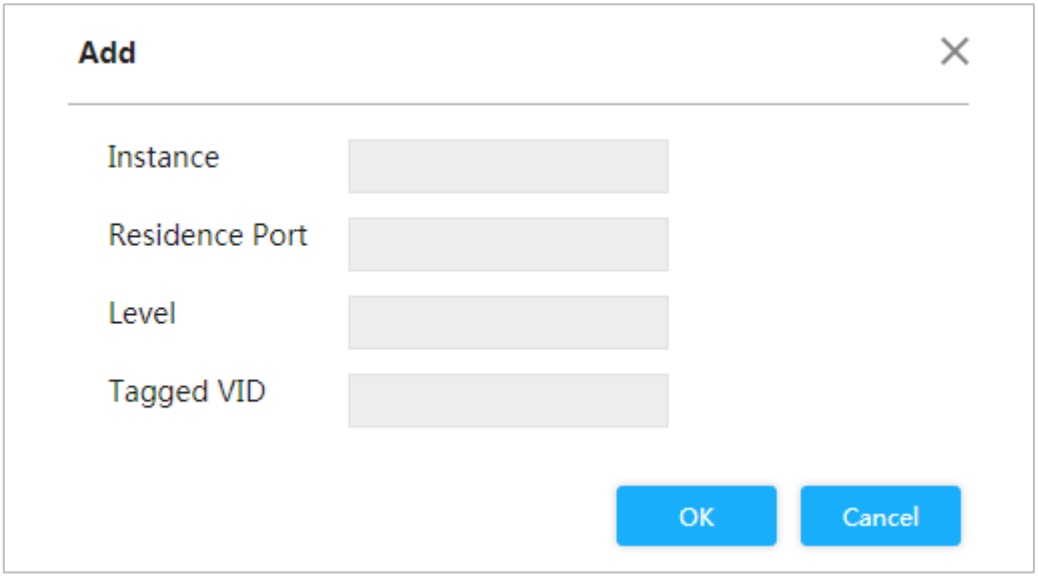
Figura 3-24 Configuración MEP



Paso 2 Haga clic en **Añadir.**

los **Añadir** se muestra la interfaz. Vea la Figura 3-25.

Figura 3-25 Agregar



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

Tabla 3-5 Parámetros MEP

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

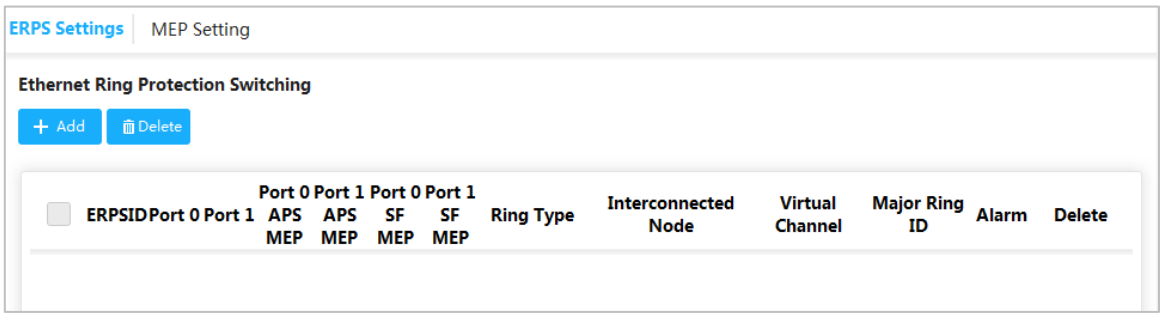
Paso 4 Haga clic en **OKAY.**

3.2.1.2 Configuración de ERPS

Paso 1 Seleccione **Avanzado> Poco usado> ERPS> Configuración de ERPS.**

los **Configuración de ERPS** se muestra la interfaz. Vea la Figura 3-26.

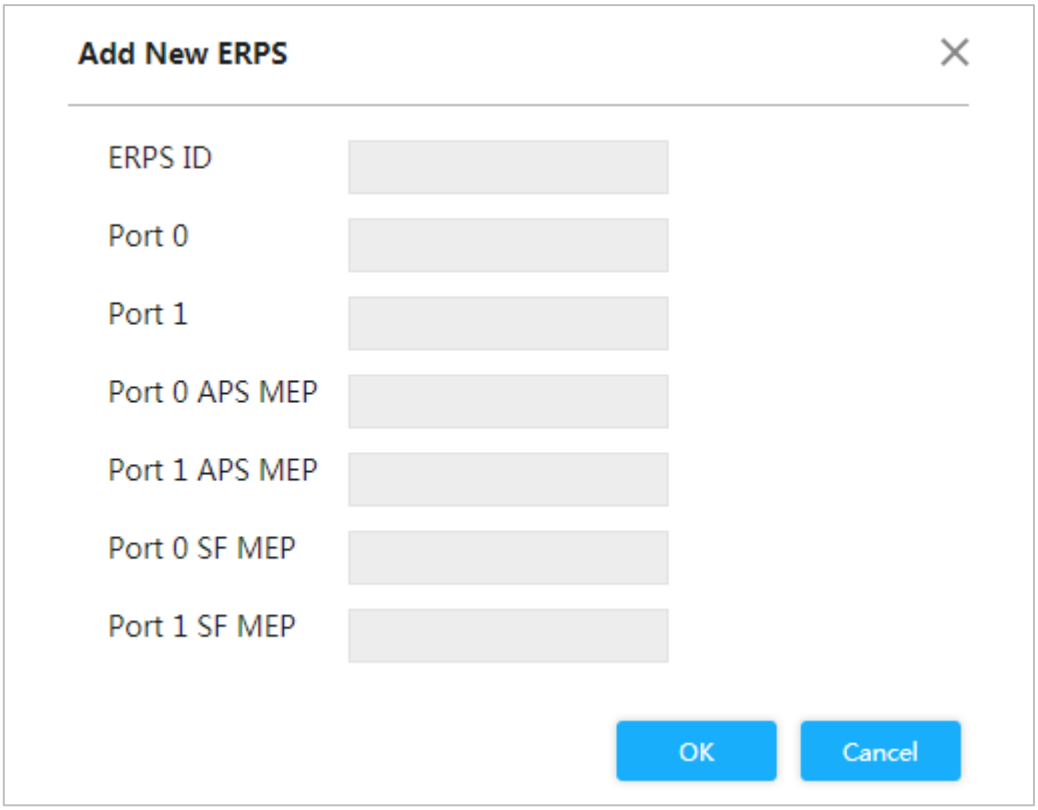
Figura 3-26 Configuración de ERPS



Paso 2 Haga clic en **Añadir.**

los **Agregar ERPS** se muestra la interfaz. Vea la Figura 3-27.

Figura 3-27 Agregar ERPS



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

Tabla 3-6 Parámetros de ERPS

Parámetro	Descripción
ID ERPS	El número de identificación de ERPS.
Puerto 0	Los dos puertos agregados al ERPS.
Puerto 1	
Puerto 0 APS MEP	El paquete de protocolo correspondiente ERPS al puerto ERPS. Mantenga el puerto 0 APS MEP coherente con el puerto 0 SF MEP. Mantenga el puerto 1 APS MEP coherente 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 MEP	
Puerto 0 SF MEP	La correspondiente inspección de agregación MEP del puerto ERPS. Mantenga el puerto 0 APS MEP coherente con el puerto 0 SF MEP. Mantenga el puerto 1 APS MEP coherente 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 MEP	

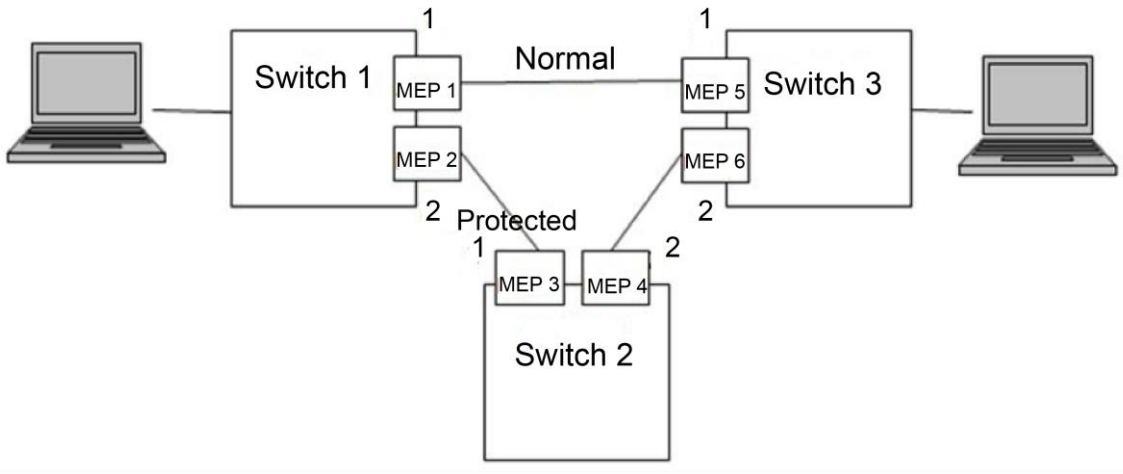
Paso 4 Haga clic en **OKAY.**

3.2.1.3 Ejemplo: configuración de anillo único ERPS

Requisito de red

Se solicitan tres conmutadores, el puerto 1 y el puerto 2 para combinar un ERPS. Vea la Figura 3-28. La relación correspondiente: Switch 1: MEP 1 y MEP 2; Switch 2: MEP3 y MEP 4; Switch 3: MEP 5 y MEP 6.

Figura 3-28 Configuración de anillo único ERPS



Configuración

Configure el ERPS con los siguientes pensamientos:

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

2) Confirme el puerto del propietario de RPL.

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

4) Configuración de VLAN

5) Crear MEP.

6) Cree ERPS y configure la VLAN de control y la instancia de protección.

7) Ver el estado.

Ejemplo

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

Las configuraciones del conmutador son las siguientes:

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

1) Seleccione Avanzado> Común> Configuración de VLAN. los **Configuración de VLAN** se muestra la interfaz. Configure el modo del puerto 1 y el puerto 2 para **Maletero.** Vea la Figura 3-29. Configure la

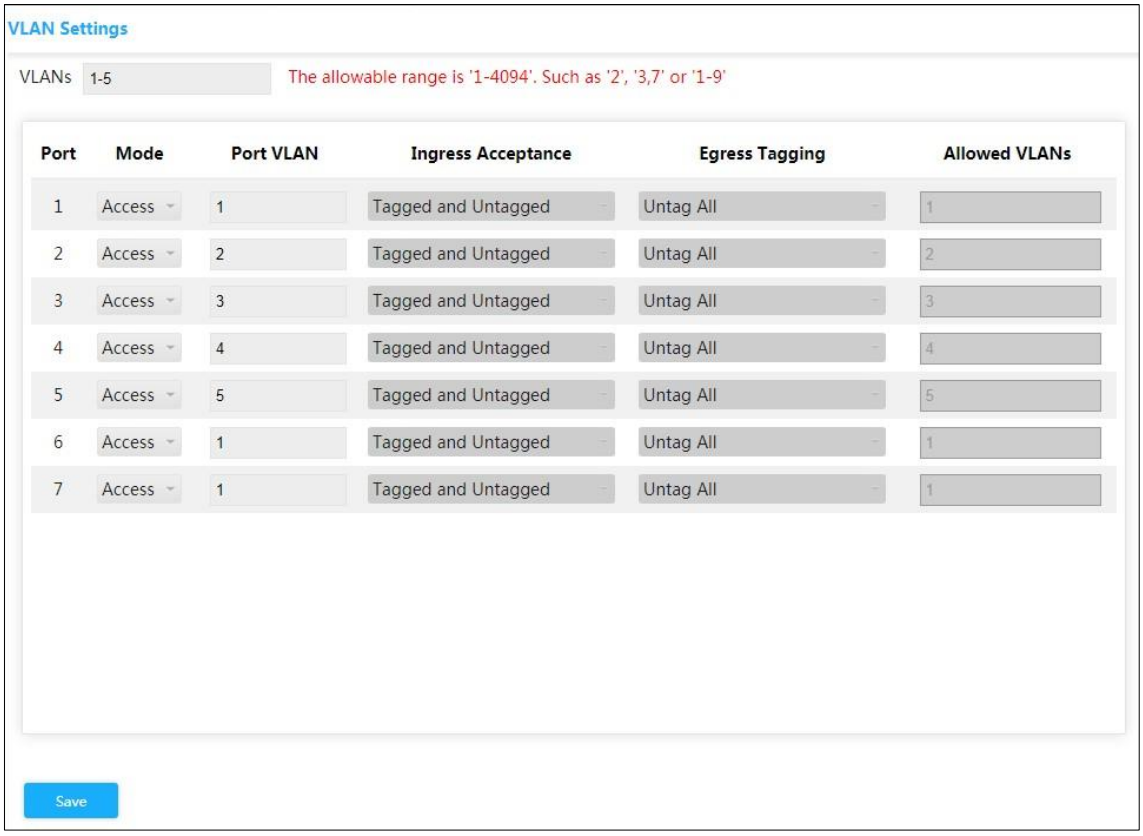
2) VLAN del puerto del puerto 1 y el puerto 2 en 1.

3)

4) Configure la VLAN permitida en 2 y 3. Haga clic en **Salvar.**

5)

Figura 3-29 Agregue el puerto 1 y el puerto 2 a la VLAN 1



Paso 2 Crear MEP1 y MEP 2

1) Seleccione Avanzado> Usado con poca frecuencia> ERPS> Configuración MEP. los **Configuración MEP** se muestra la interfaz. Hacer clic **Añadir.**

2) los **Añadir** se muestra la interfaz.

3) Establezca Instancia en 1. Consulte la Figura 3-30. Establezca el

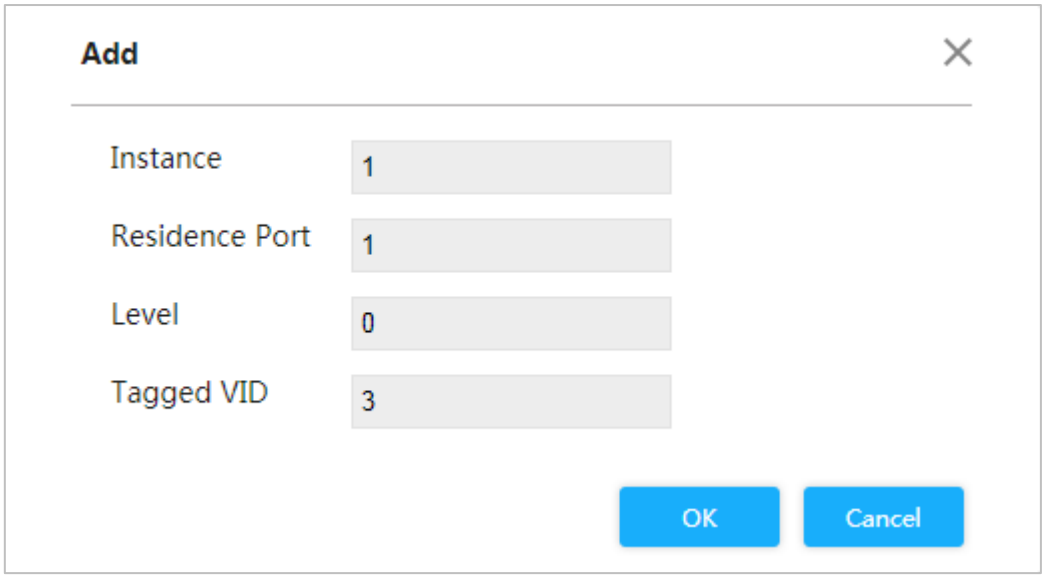
4) puerto de residencia en 1.

5) Establezca el nivel en 0.

6) Configure el VID etiquetado en 3, es decir, el protocolo VLAN. Hacer clic **OKAY.**

7)

Figura 3-30 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 Haga clic en **1** y **2** por separado bajo **Ejemplo** para ingresar a la interfaz de configuración. Modificar MEP ID y agregue peer ID. Consulte la Figura 3-31 y la Figura 3-32.

Figura 3-31 Configure el ID de peer de MEP 1

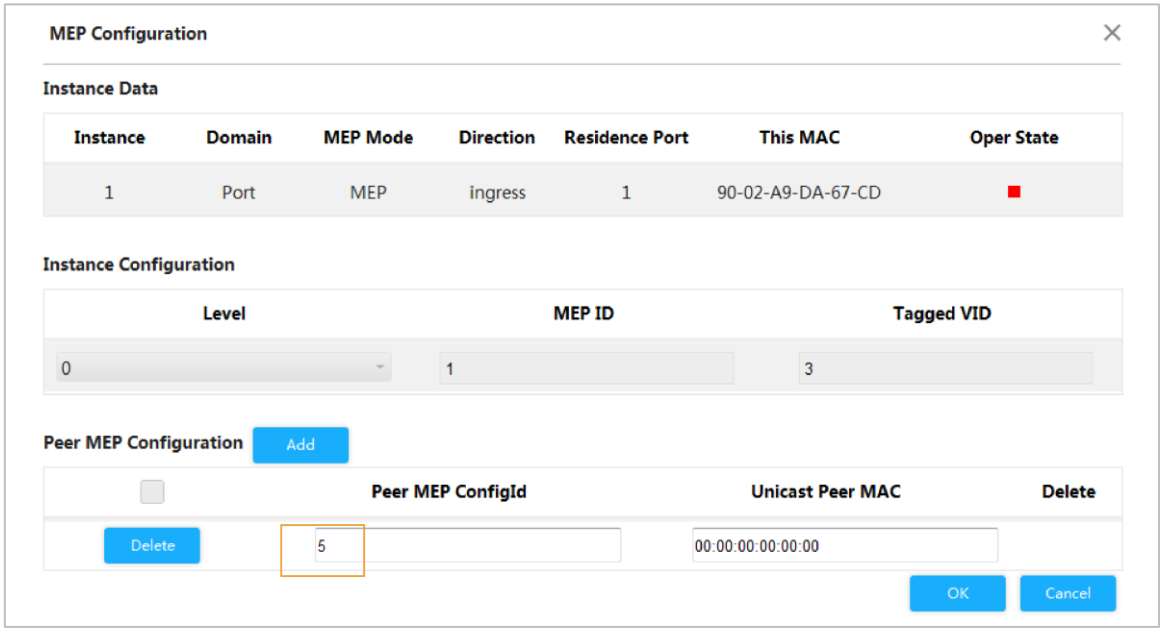
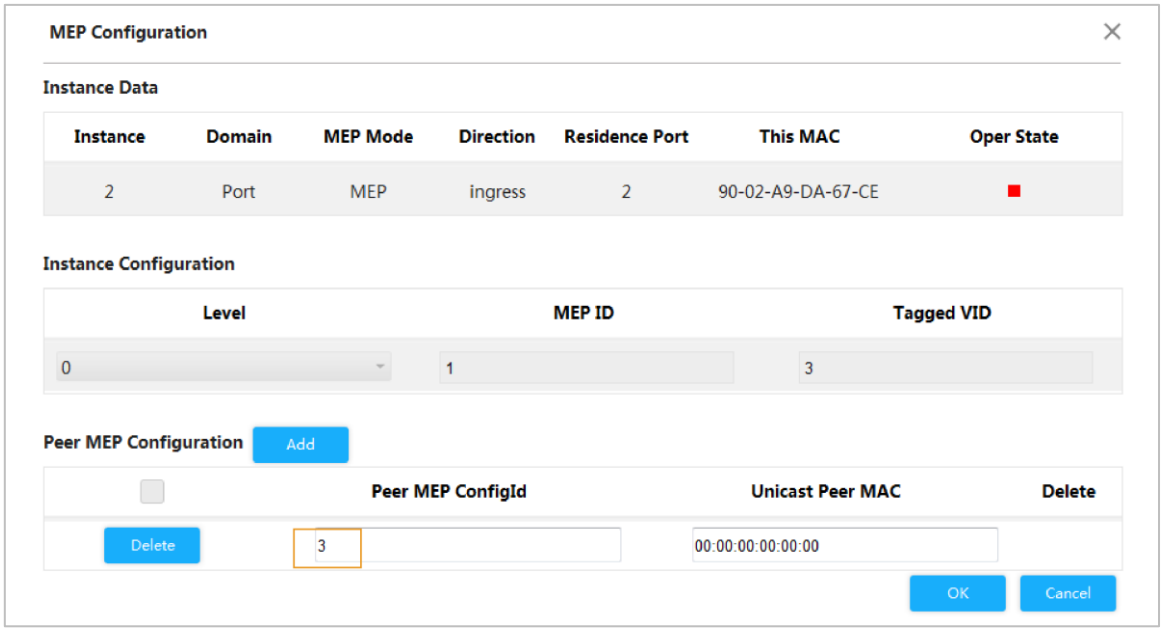


Figura 3-32 Configure el ID de peer de MEP 2



Paso 4 Hacer clic **OKAY.**

Paso 5 Crea ERPS.

1) Seleccione Avanzado> Usado con poca frecuencia> ERPS> Configuración de ERPS. los **Configuración ERPS** se muestra la interfaz. Hacer clic **Añadir.**

2) los **Agregar nuevo ERPS** se muestra la interfaz. Configure la ID de

3) ERPS en 1. Consulte la Figura 3-33. Establezca el puerto 0 en 1 y el

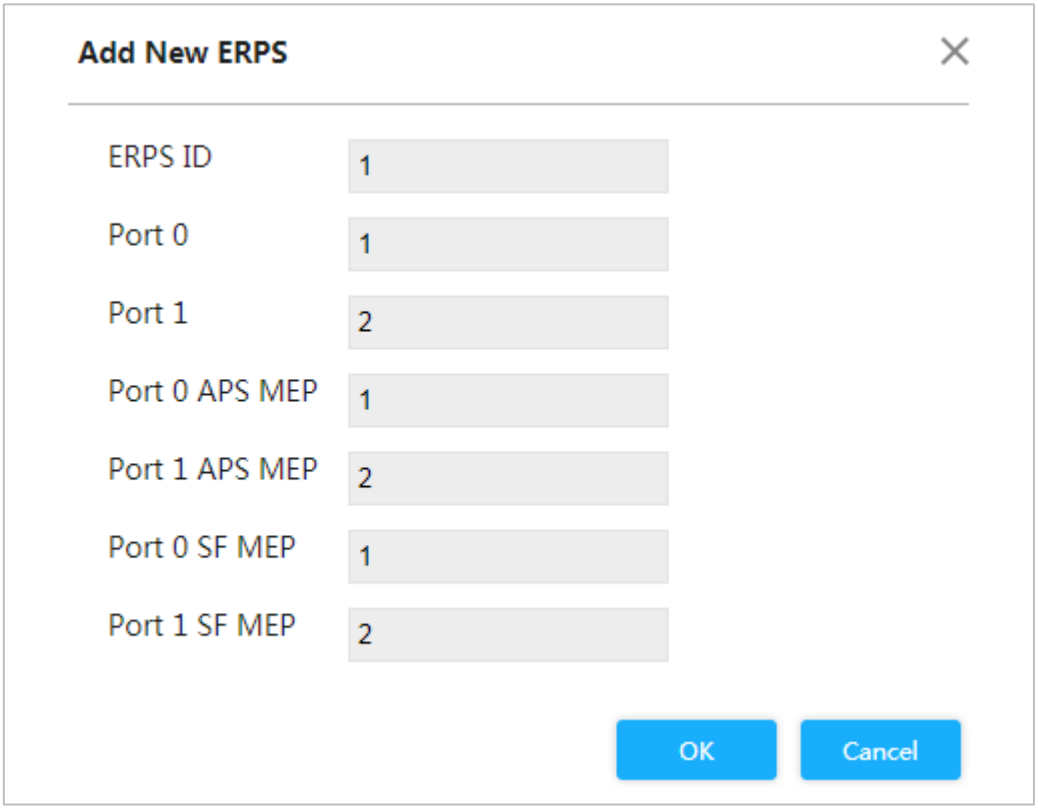
4) puerto 1 en 2.

5) Establezca el puerto 0 APS MEP en 1 y el puerto 1 APS MEP en 2.

6) Establezca el puerto 0 SF MEP en 1 y el puerto 1 SF MEP en 2.

7) Haga clic en **OKAY.**

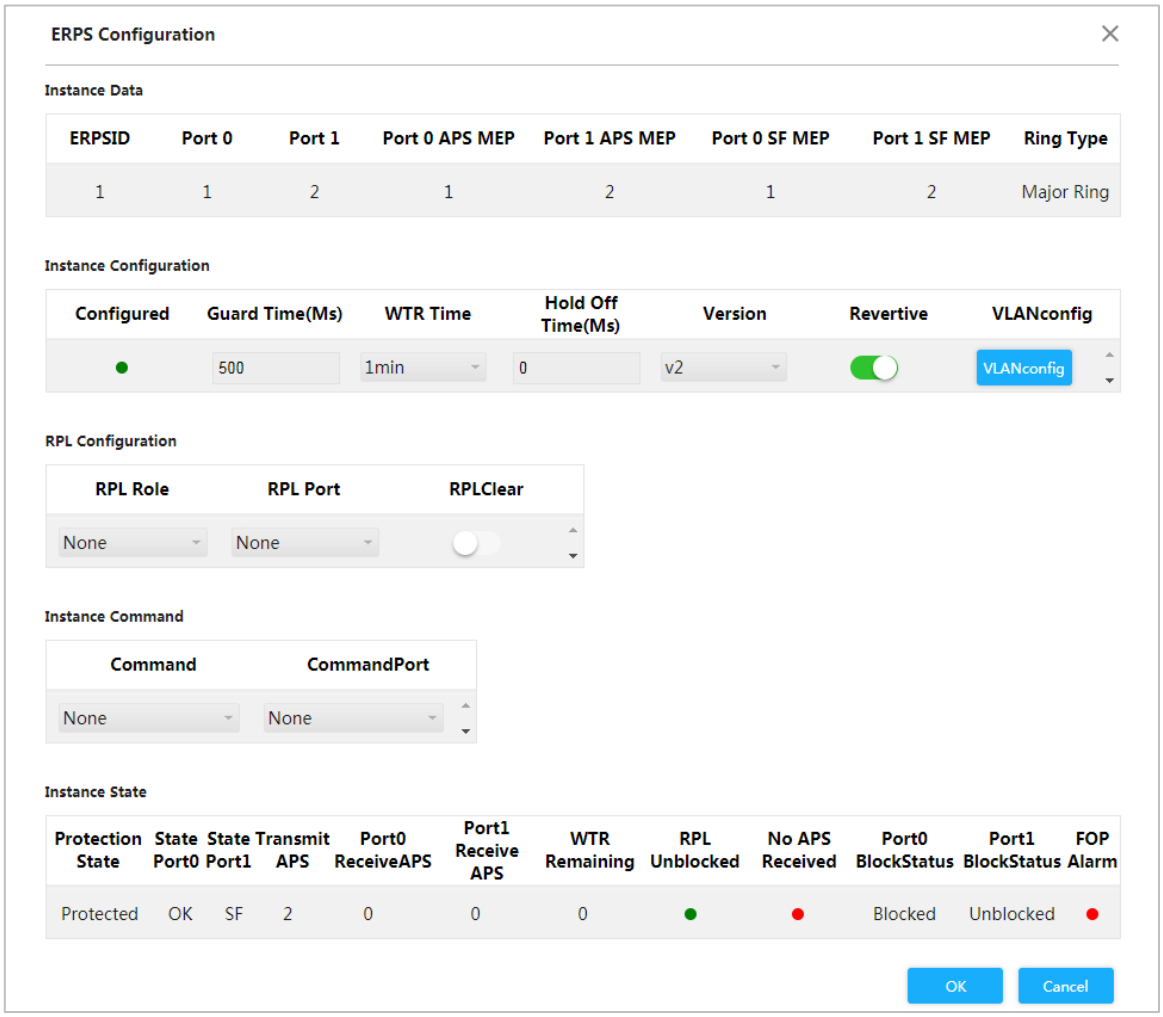
Figura 3-33 Agregar ERPS



Paso 6 Haga clic en **1** debajo **ERPSID** para ingresar a la interfaz de configuración. Para la configuración de ERPS, consulte

Figura 3-34.

Figura 3-34 Configuración de ERPS



1) Haga clic en VLANconfig.

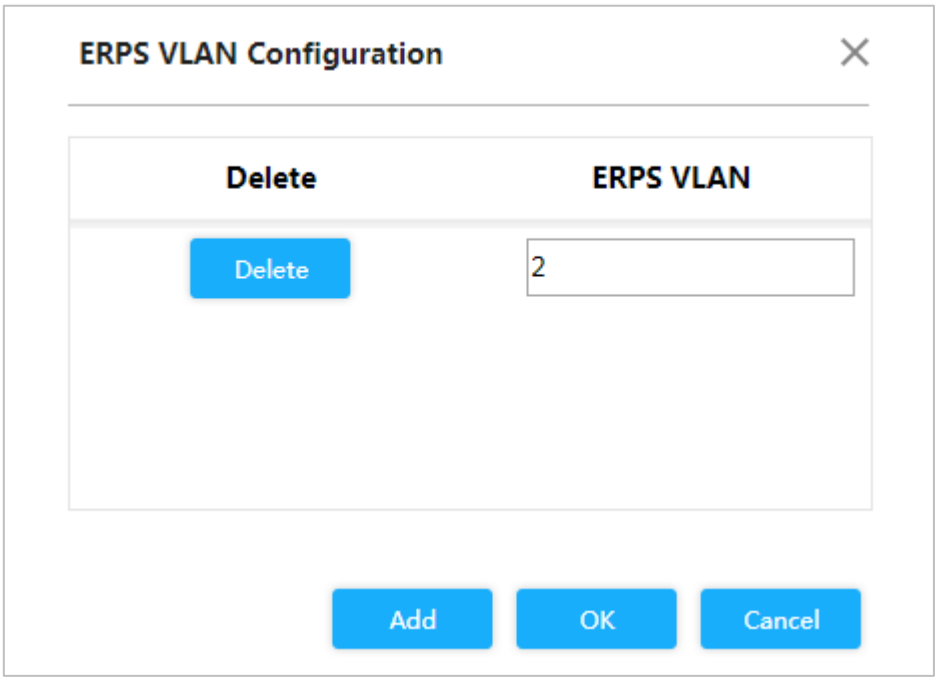
   los **Configuración de ERPS VLAN** se muestra la interfaz. Hacer clic **Añadir.**

2)

3) Configure la VLAN de ERPS en 2. Consulte la Figura 3-35. Hacer clic **OKAY.**

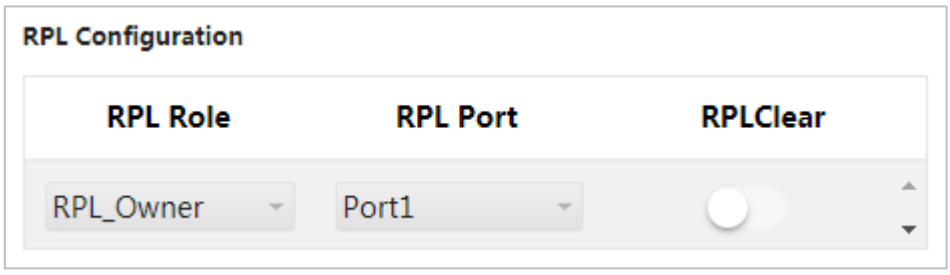
4)

Figura 3-35 Configuración de VLAN ERPS



5) Configure el puerto 2 del conmutador 1 para que sea propietario de RPL en Configuración de RPL. Vea la Figura 3-36.

Figura 3-36 Configuración del puerto del propietario



Paso 7 Haga clic en **OKAY.**

Paso 8 Configure el conmutador 2 y el conmutador 3 de la misma forma.

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

Figura 3-37 Estado de la instancia

Instance State

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

3.2.2 ACL

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

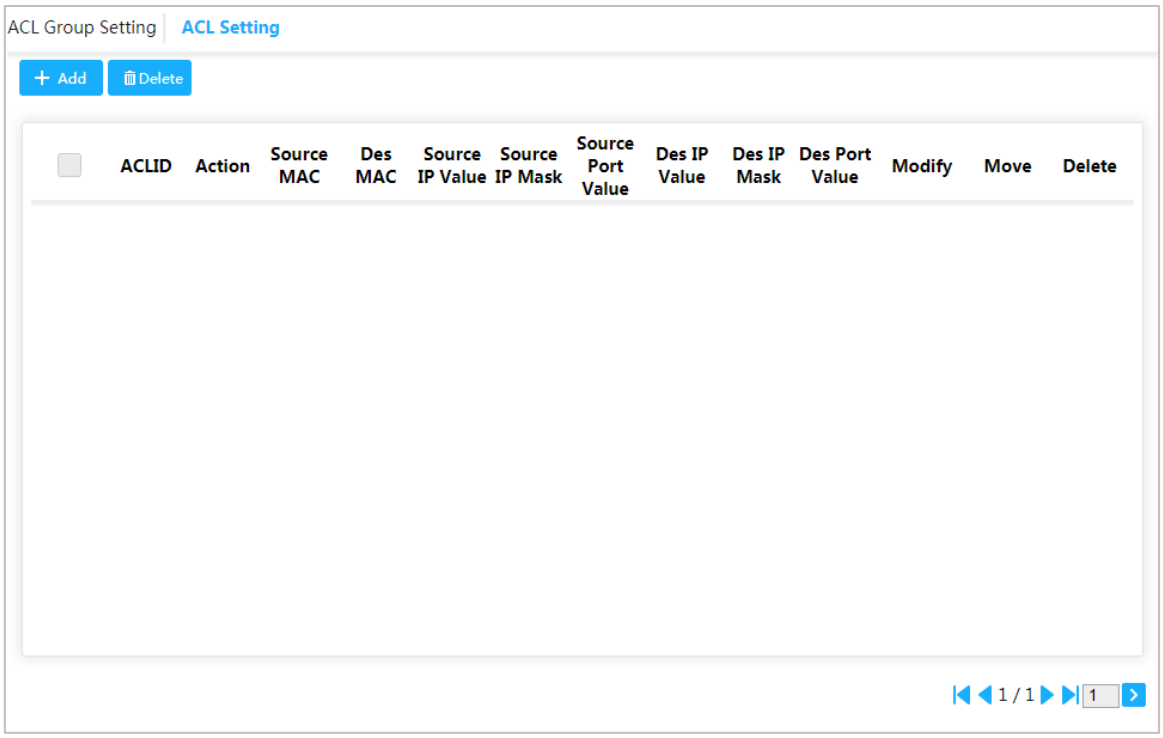
Cuando el puerto del dispositivo recibe el paquete, puede analizar el campo del paquete de acuerdo con la regla ACL del puerto actual. Y después de que se identifica el paquete específico, se permite o se prohíbe el paso del paquete según la regla preestablecida.

3.2.2.1 Configuración de ACL

Paso 1 Seleccione **Avanzado> Rara vez usado> ACL> Configuración de ACL.**

los **Configuración de ACL** se muestra la interfaz. Vea la Figura 3-38.

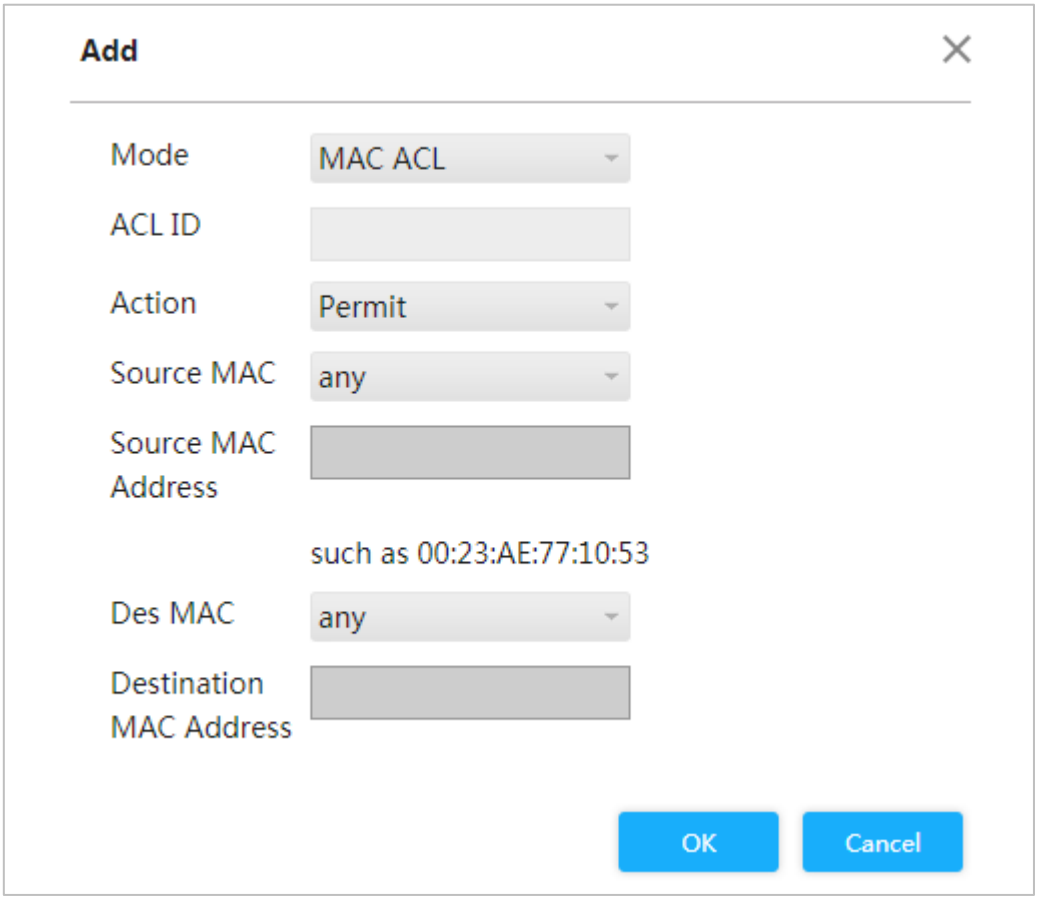
Figura 3-38 Configuración de ACL



Paso 2 Haga clic en **Añadir.**

los **Añadir** se muestra la interfaz. Vea la Figura 3-39.

Figura 3-39 Agregar



Paso 3 Configure la ID de ACL y el rango es 1–128.

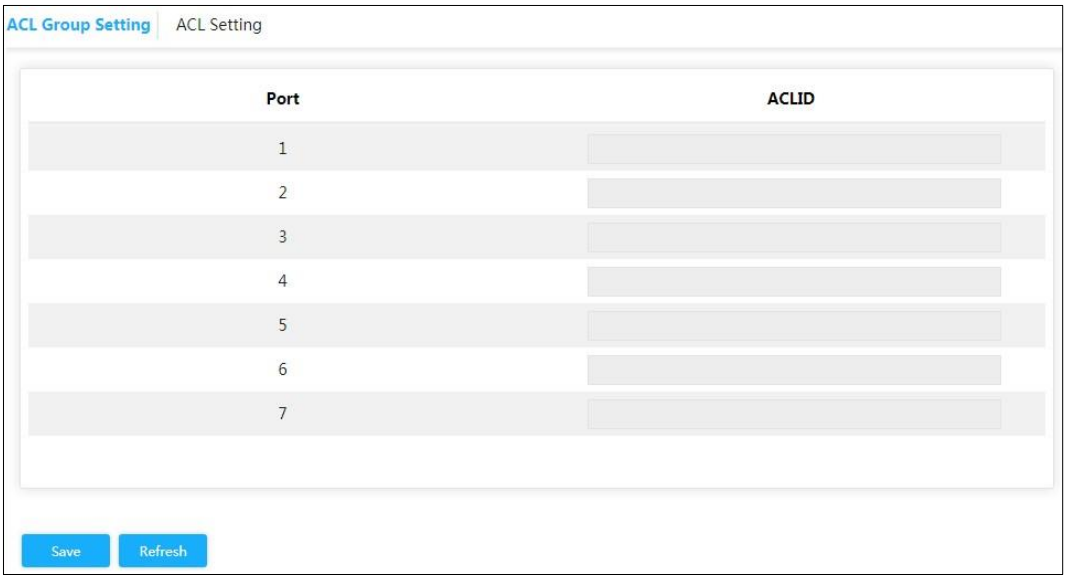
Paso 4 Haga clic en **OKAY.**

3.2.2.2 Configuración del grupo de ACL

Paso 1 Seleccione **Avanzado> Usado con poca frecuencia> ACL> Configuración de grupo de ACL.**

los **Configuración de grupo de ACL** se muestra la interfaz. Vea la Figura 3-40.

Figura 3-40 Configuración del grupo de ACL



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

Paso 3 Haga clic en **Salvar.**

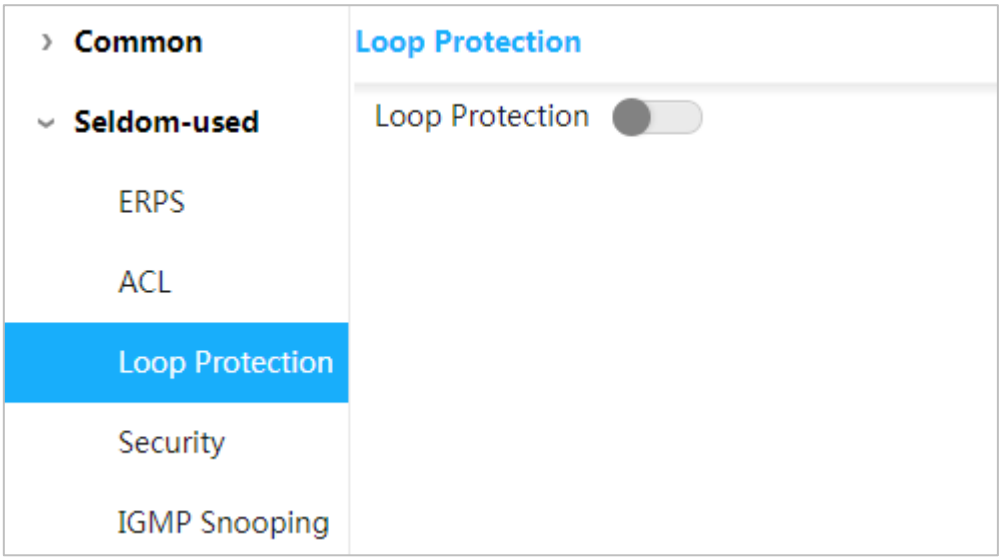
3.2.3 Protección de bucle

Detecta el bucle entre los puertos. Una vez que el dispositivo ha detectado el bucle, lo romperá.

Paso 1 Seleccione **Avanzado> Poco usado> Protección de bucle.**

los **Protección de bucle** se muestra la interfaz. Vea la Figura 3-41.

Figura 3-41 Protección de bucle



Paso 2 Haga clic en para habilitar la protección de bucle

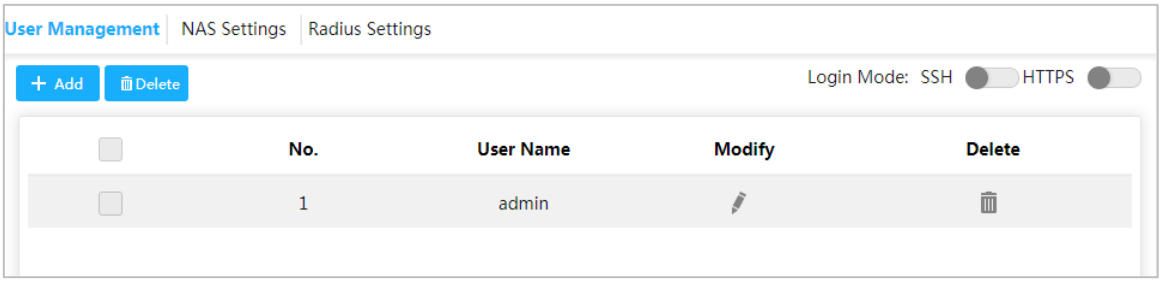
3.2.4 Seguridad

3.2.4.1 Gestión de usuarios

Puede agregar, editar y eliminar el usuario.

Seleccione **Avanzado> Poco usado> Seguridad> Gestión de usuarios.** Y el **Gestión de usuarios** se muestra la interfaz. Vea la Figura 3-42.

Figura 3-42 Gestión de usuarios

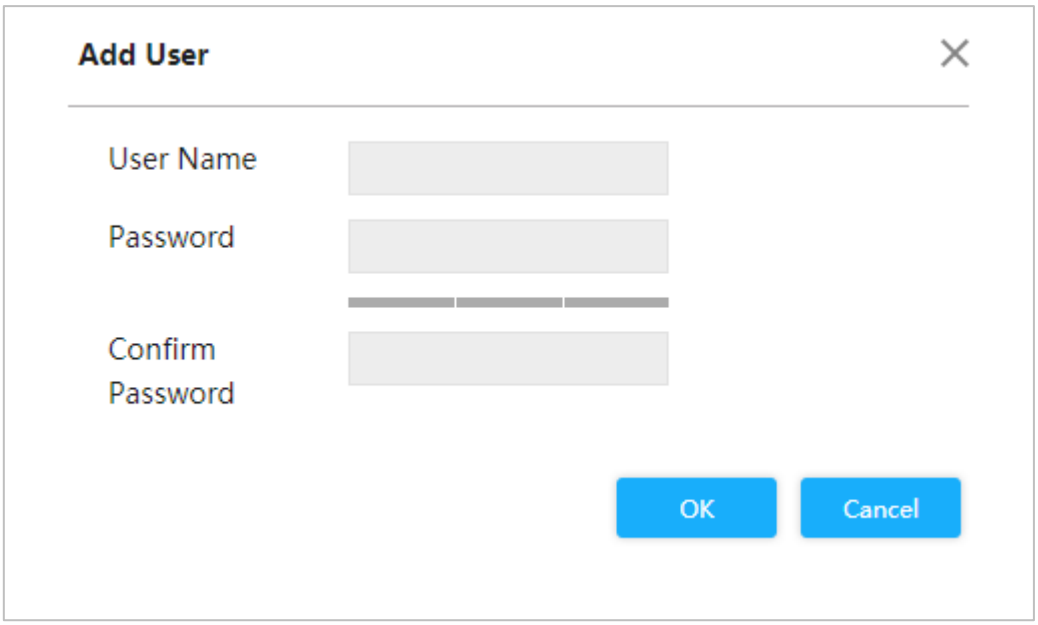


Agregar usuario

Paso 1 clic **Añadir.**

los **Agregar usuario** se muestra la interfaz. Vea la Figura 3-43.

Figura 3-43 Agregar usuario

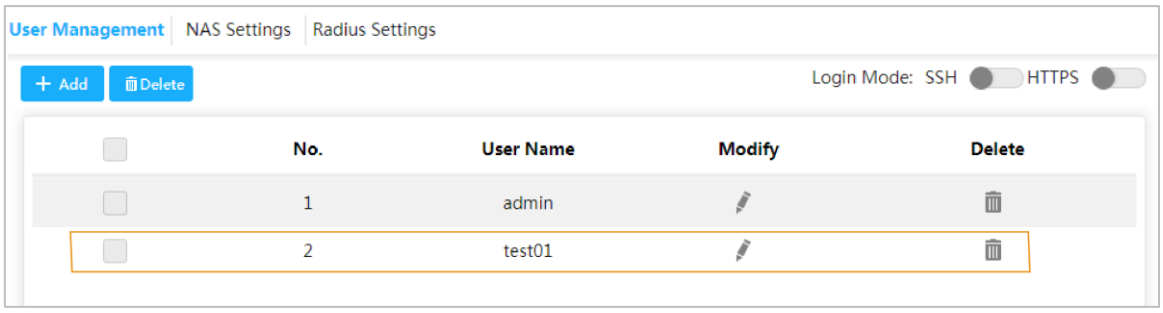


Paso 2 Ingrese el nombre de usuario, la contraseña y confirme la contraseña. La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo "';: &). Por ejemplo, agregue la nueva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

Paso 3 Hacer clic **Salvar.**

Se agrega la nueva prueba de usuario 01. Vea la Figura 3-44.

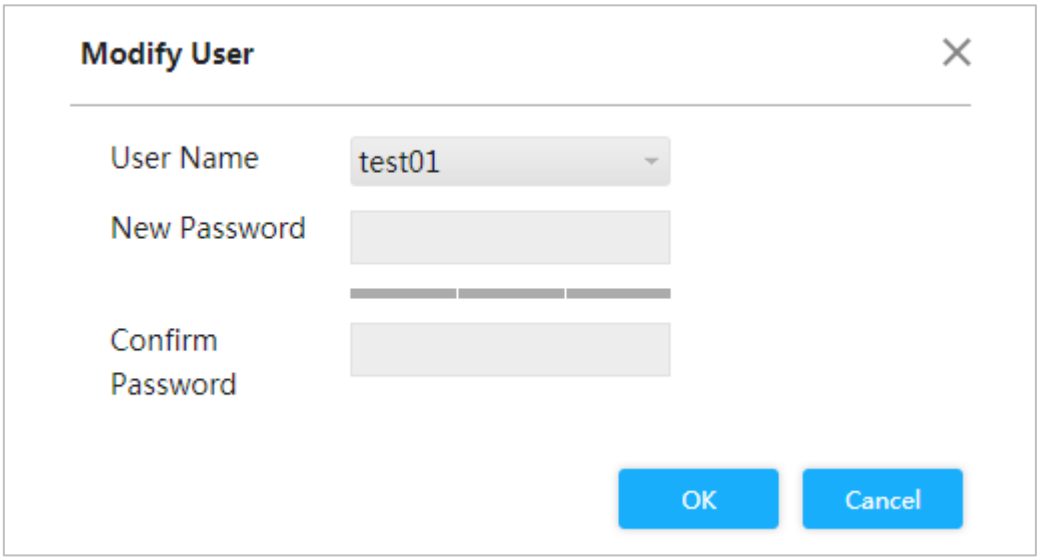
Figura 3-44 Nuevo usuario agregado



Modificar y eliminar usuario

- Hacer clic , y el **Modificar usuario** se muestra la interfaz. Vea la Figura 3-45.

Figura 3-45 Modificar usuario



- Hacer clic para eliminar el usuario.

No puede eliminar el usuario administrador.

SSH

Puede habilitar o deshabilitar la función SSH.

Hacer clic correspondiente a SSH en la esquina superior derecha del **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 solicitan 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 el navegador web Netscape, proporciona comunicación de autenticación y cifrado. Se aplica ampliamente en la red mundial 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 del **Gestión de usuarios** interfaz para habilitar el servicio HTTPS.

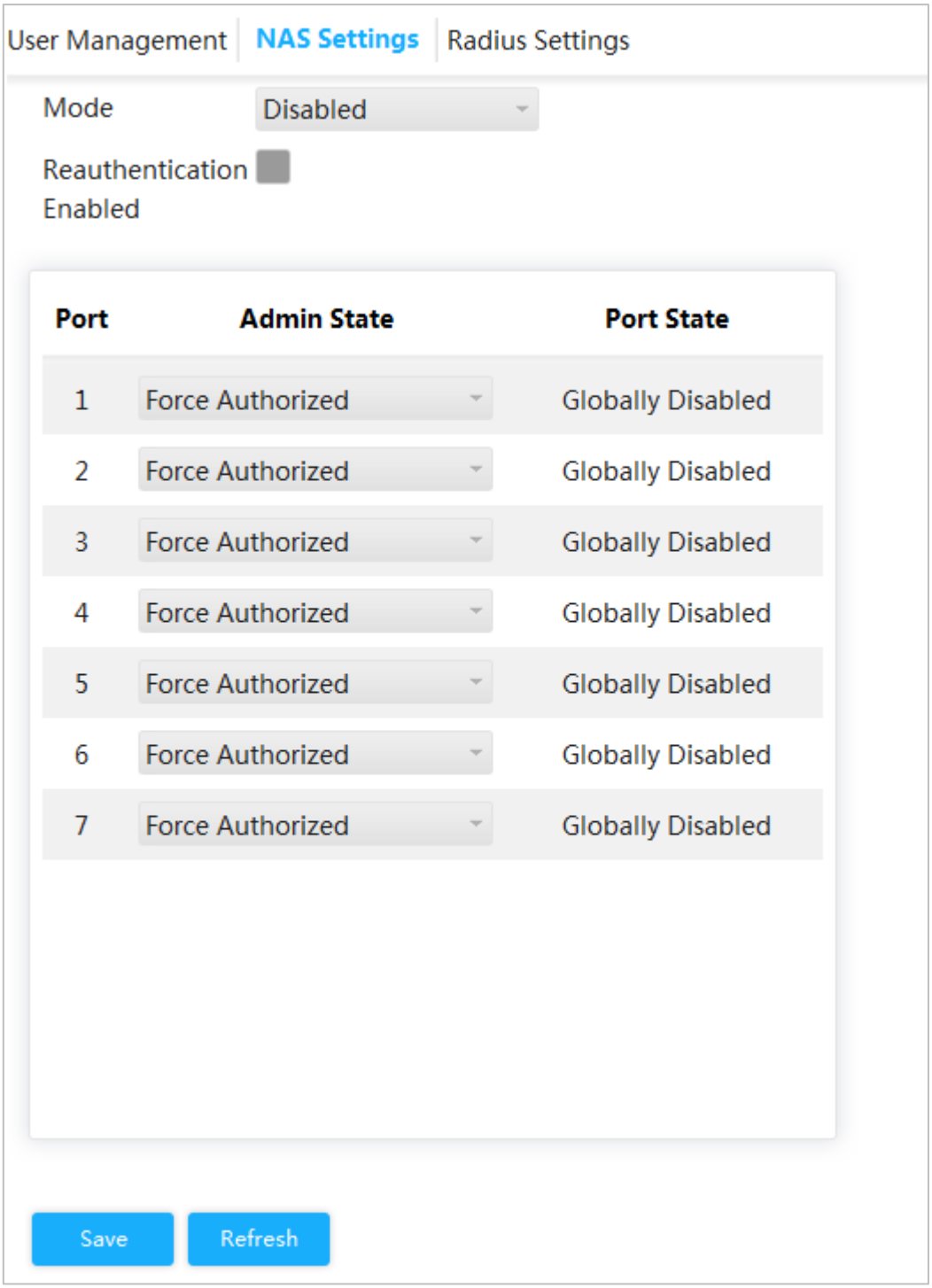
3.2.4.2 Configuración NAS

NAS (servidor de acceso a la red) es un servidor que permite al ISP proporcionar un servicio de acceso a Internet.

Paso 1 Seleccione **Avanzado> Poco usado> Seguridad> Configuración NAS.**

los **Configuración NAS** se muestra la interfaz. Vea la Figura 3-46.

Figura 3-46 Configuración del NAS



Paso 2 Seleccione **Habilitado** en el **Modo** área para habilitar la función de espejo.

Paso 3 Seleccione el **Reautenticación habilitada** cuadro para habilitar la reautenticación.

Paso 4 Establecer estado de administración: Forzar autorizado, Forzar no autorizado, 802.1X basado en puerto o Autenticación basada en MAC

Paso 5 Haga clic en **Salvar.**

3.2.4.3 Configuración de radio

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

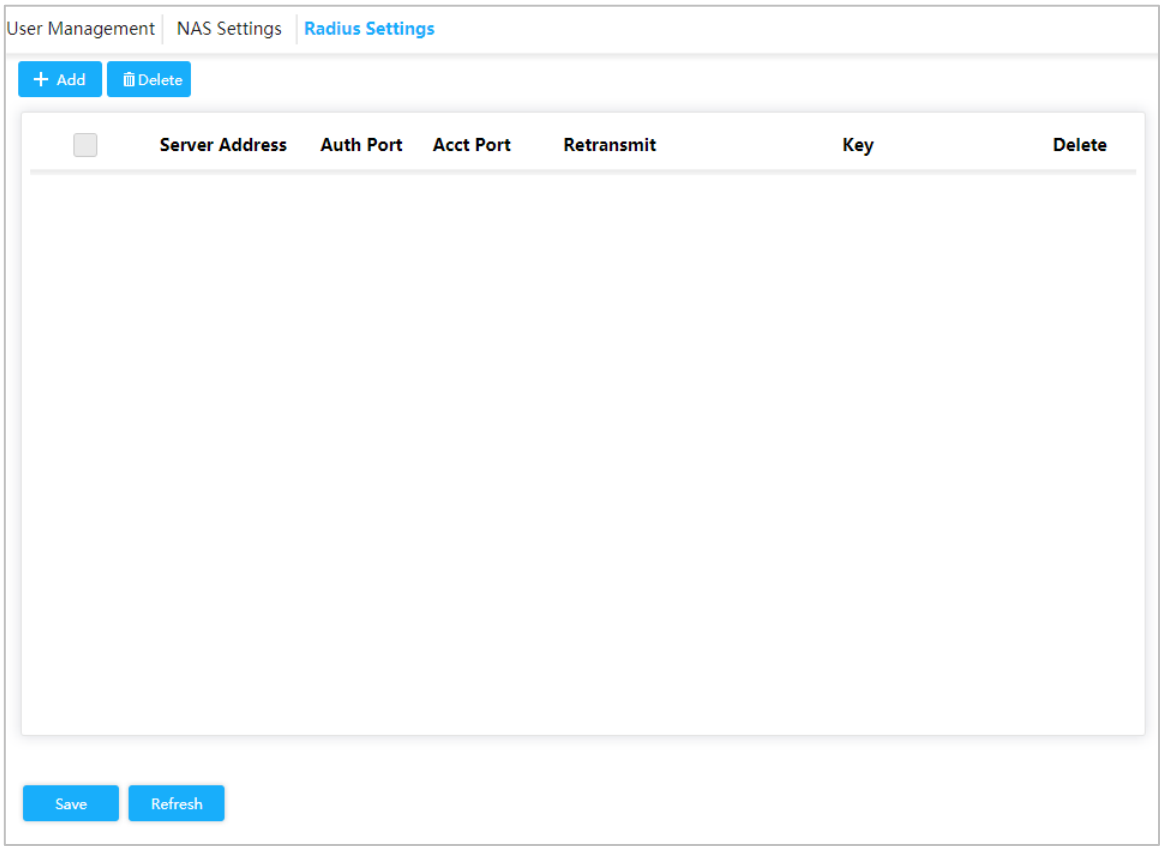
RADIUS es un protocolo de interacción de información de construcción distribuida y C / S. Puede proteger la red de visitas no autorizadas. Se utiliza en la red que permite visitas remotas pero solicita mayor seguridad. Define el formato de paquete RADIUS y el mecanismo de transmisión de mensajes. Estipula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

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

Paso 1 Seleccione **Avanzado> Poco usado> Seguridad> Configuración de radio.**

los **Configuración de radio** se muestra la interfaz. Vea la Figura 3-47.

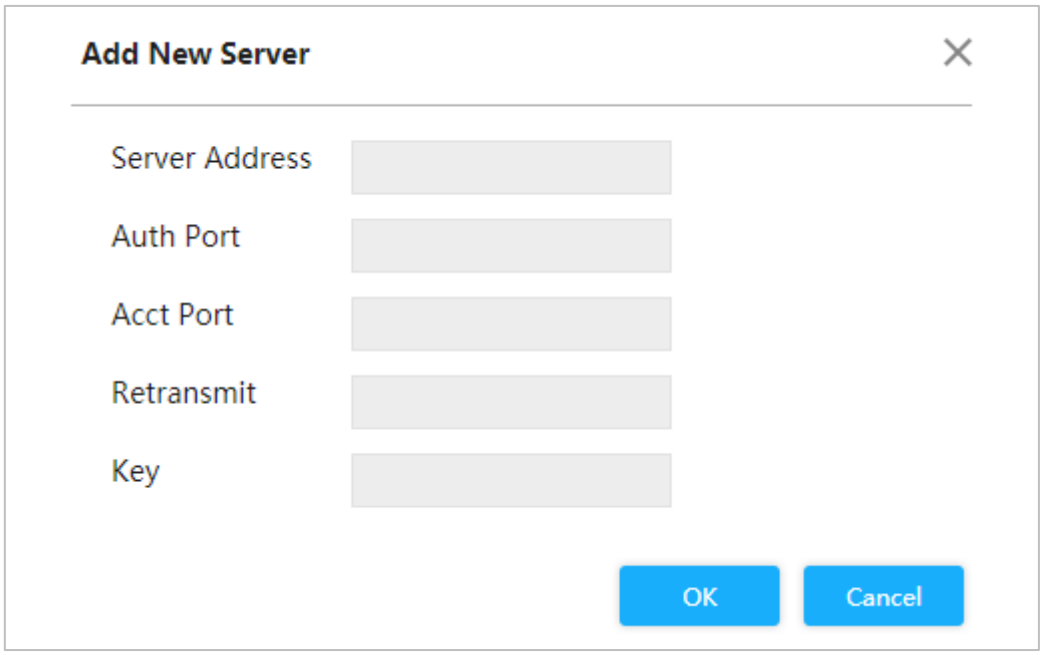
Figura 3-47 Configuración de radio



Paso 2 Haga clic en **Añadir.**

los **Agregar nuevo servidor** se muestra la interfaz. Vea la Figura 3-48.

Figura 3-48 Agregar nuevo servidor



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

Paso 4 Haga clic en **OKAY.**

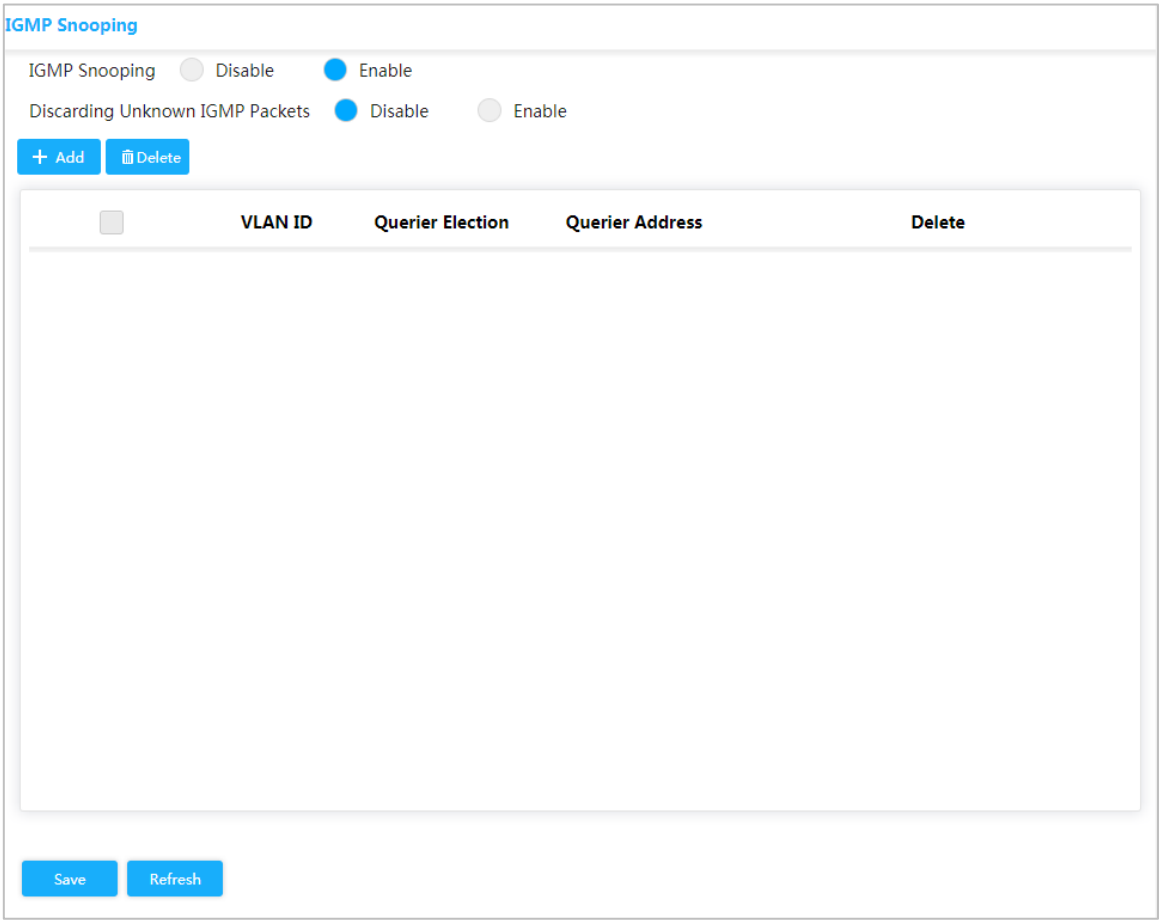
3.2.5 Inspección IGMP

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

Paso 1 Seleccione **Avanzado> Rara vez utilizado> IGMP Snooping.**

los **Inspección IGMP** se muestra la interfaz. Vea la Figura 3-49.

Figura 3-49 Inspección de IGMP



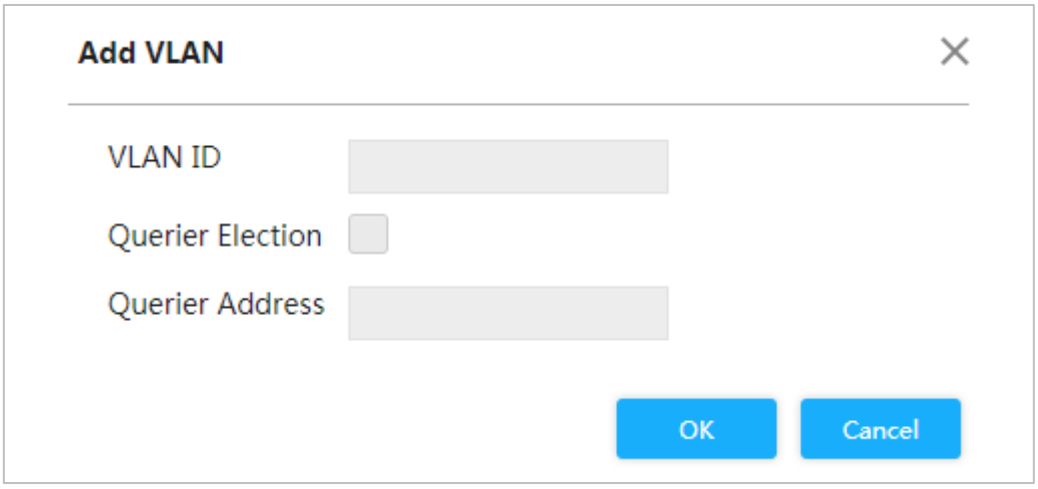
Paso 2 Seleccione **Habilitar** en el **Inspección IGMP** área para habilitar la función.

Paso 3 Seleccione **Inhabilitar** o **Habilitar** en el **Descartar paquetes IGMP desconocidos** zona.

Paso 4 Haga clic en **Añadir.**

los **Agregar VLAN** se muestra la interfaz. Vea la Figura 3-50.

Figura 3-50 Agregar VLAN



Paso 5 Configure el ID de VLAN y la dirección de consulta, y seleccione **Elección de Querier** caja para habilitar el

querier

Paso 6 Haga clic en **OKAY.**

3.2.6 QoS

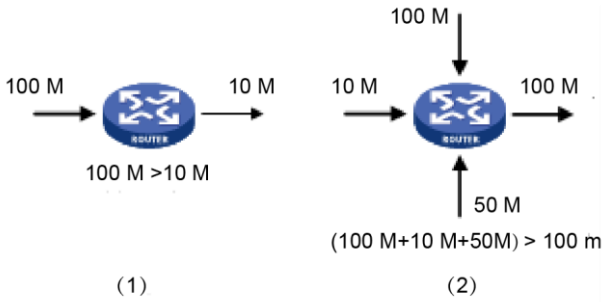
QoS (Calidad de servicio) se utiliza para evaluar la capacidad que el servidor cumple con las demandas de servicio del cliente. En Internet, lo que QoS evalúa es la capacidad del servicio de reenvío de red y paquetes.

QoS puede evaluarse desde los diferentes aspectos según los distintos servicios que brinda la red. QoS evalúa el ancho de banda, el retardo, el dithering 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 3-51 Congestión del flujo



1) El paquete llega al dispositivo por el enlace de alta velocidad y sale por el enlace de baja velocidad.

2) El paquete llega al dispositivo desde varios puertos y sale de un puerto (la velocidad de varios puertos es mayor que la del puerto de salida).

Si el flujo llega a una velocidad lineal, se encontrará con 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, búfer y recursos de memoria) provocará congestión. Adicionalmente, el mal control del flujo arribado en un tiempo determinado, que lleva a que el flujo exceda el recurso de la red distributiva, también es un factor para generar congestión.

3.2.6.1 Puerto

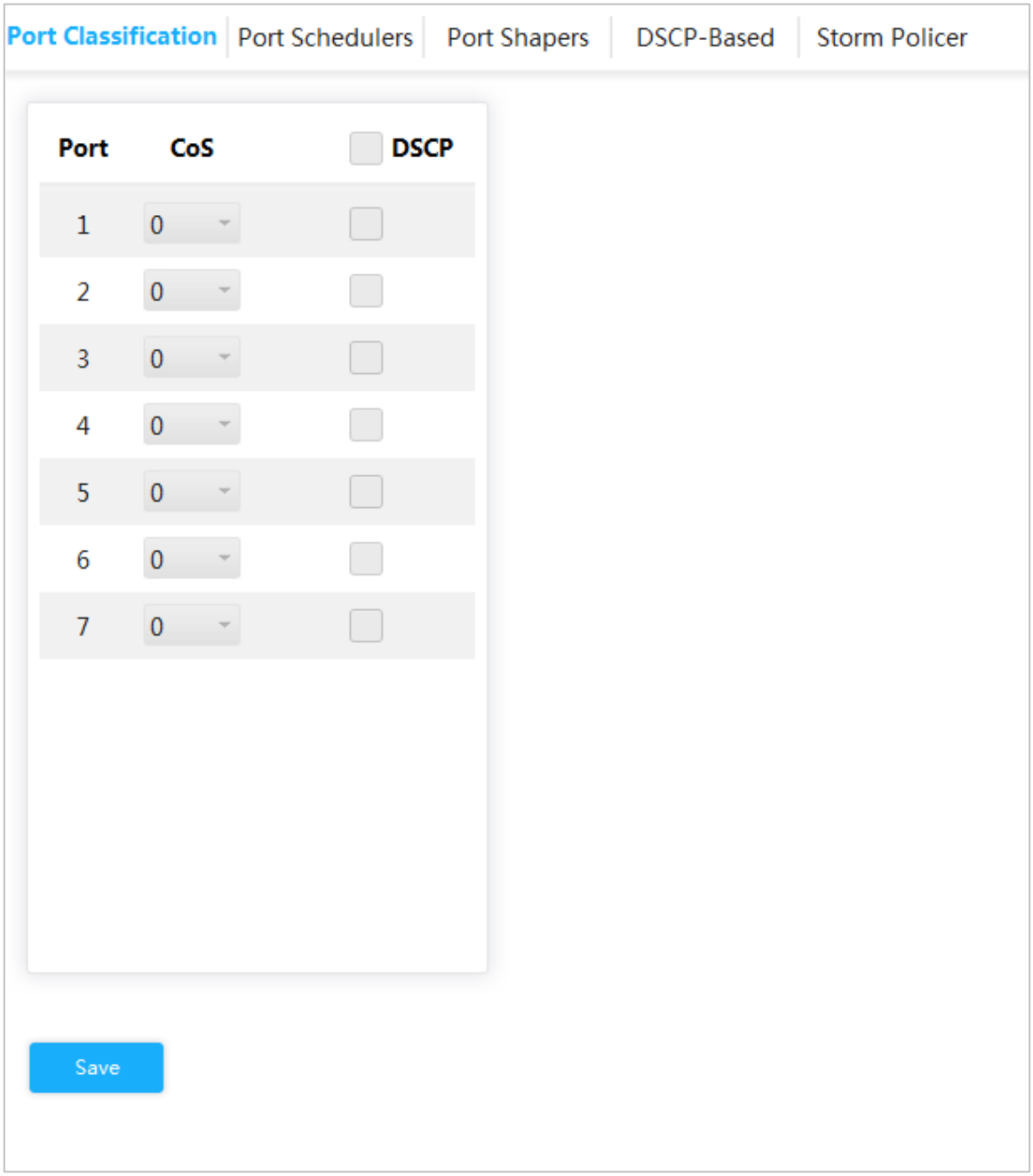
Mediante la configuración de CoS, se puede decidir la prioridad para el puerto de salida del conmutador que pasa paquetes.

Si la congestión ocurre en el puerto de salida, el switch le dará un valor de CoS al paquete después de que pase por el puerto de entrada. Cuanto mayor sea el valor de CoS, mayor será la prioridad.

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

los **Clasificación de puertos** se muestra la interfaz. Vea la Figura 3-52.

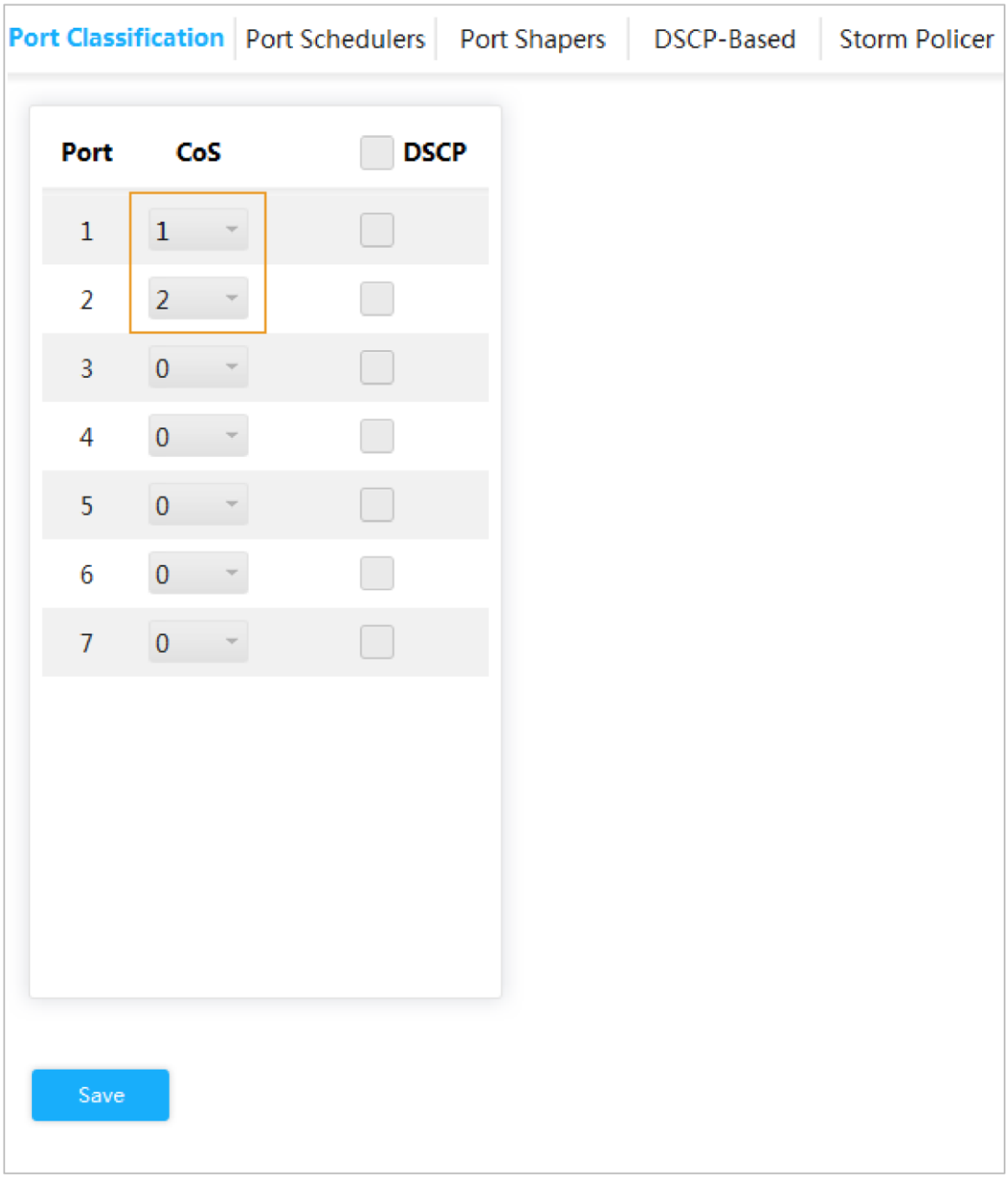
Figura 3-52 Clasificación de puertos



Paso 2 Configure CoS. Por ejemplo: Configure el puerto 1 como 1 y el puerto 2 como 2. Consulte la Figura 3-53.

El puerto 1 y el puerto 2 son puertos de entrada y el puerto 3 es el puerto de salida. El valor de 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 3-53 Establecer CoS



Paso 3 Haga clic en **Salvar.**

3.2.6.2 Programadores de puertos

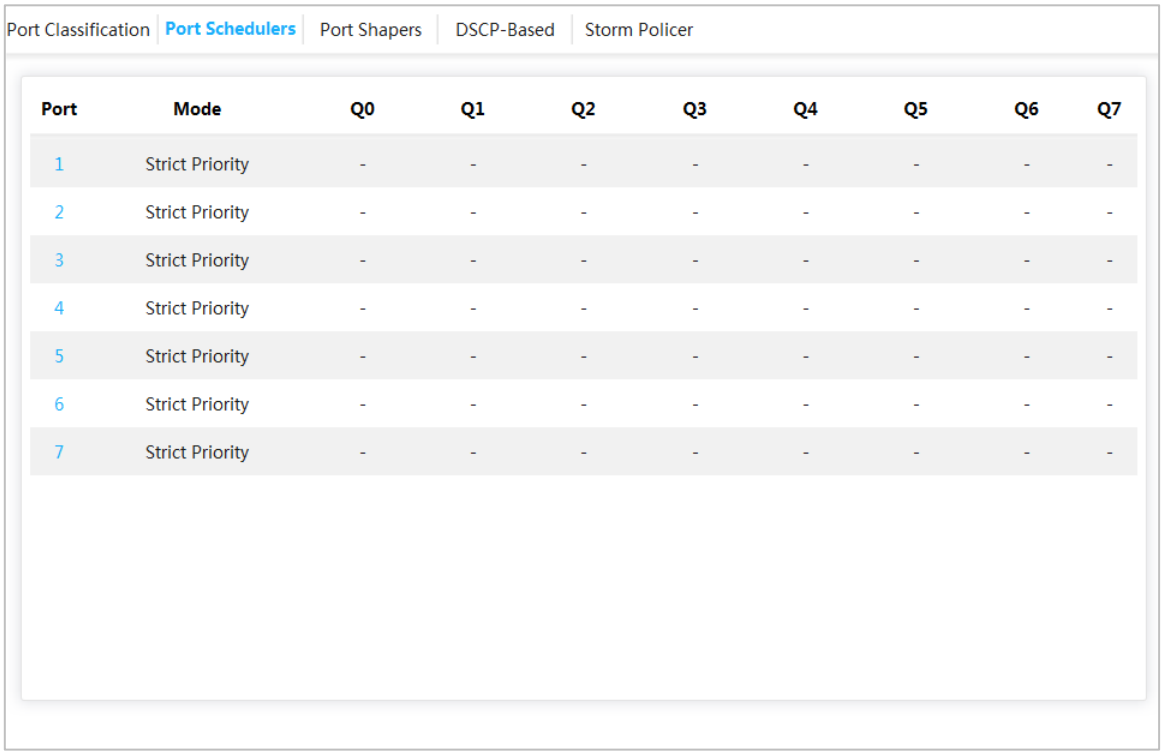
Los dos modos de los programadores de puertos:

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

Paso 1 Seleccione **Avanzado> De uso poco frecuente> QoS> Programadores de puertos.**

los **Programadores de puertos** se muestra la interfaz. Vea la Figura 3-54.

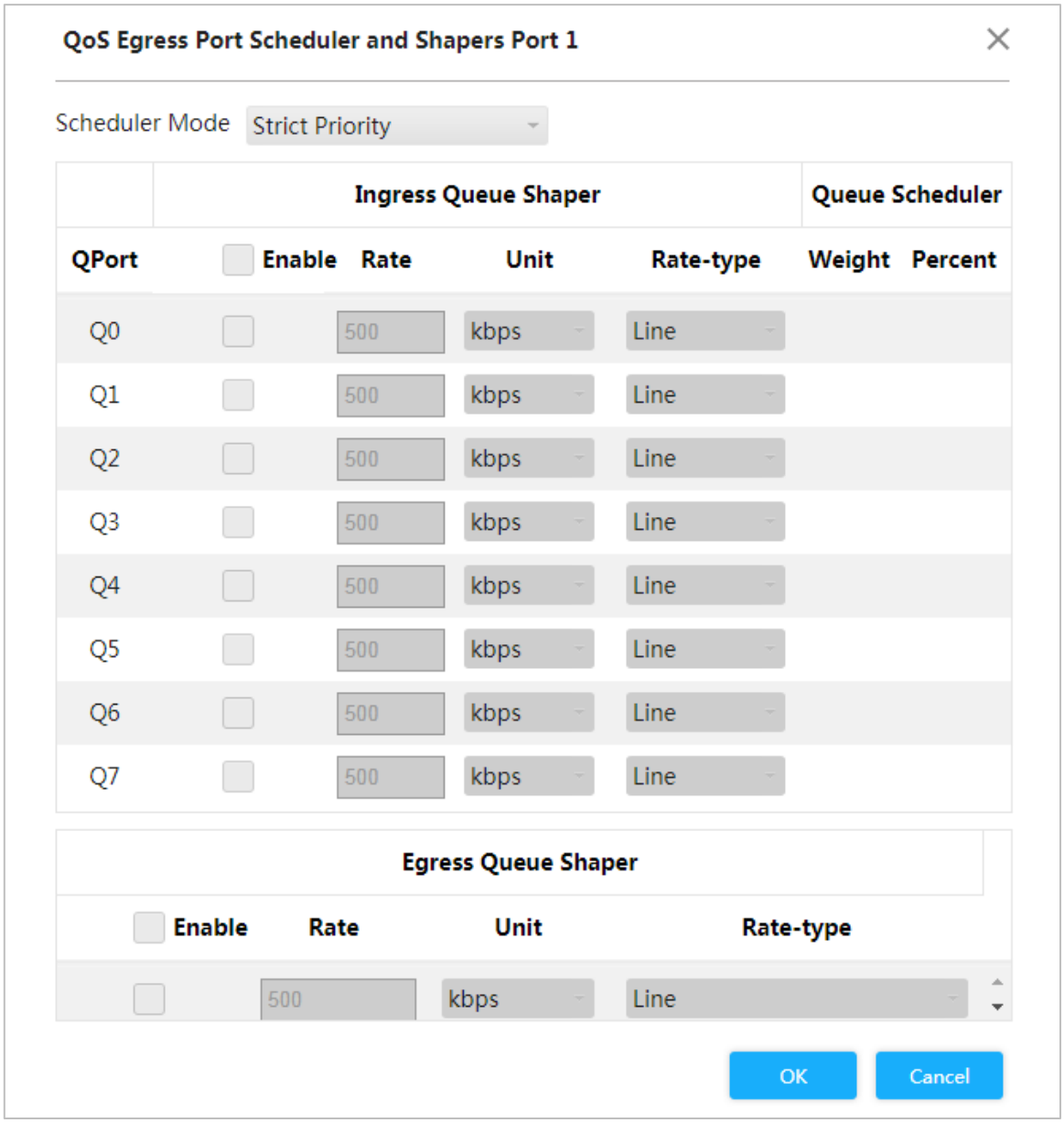
Figura 3-54 Programadores de puertos



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

los **Programadores y modeladores de puertos de salida de QoS Puerto 1** se muestra la interfaz. Vea la Figura 3-55. El CoS de Q0 es 0, y así sucesivamente.

Figura 3-55 Configuración del puerto



Paso 3 Seleccione el modo.

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

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

1) Seleccionar **Modo de programador** como **2 colas ponderadas.** Vea la Figura 3-56.

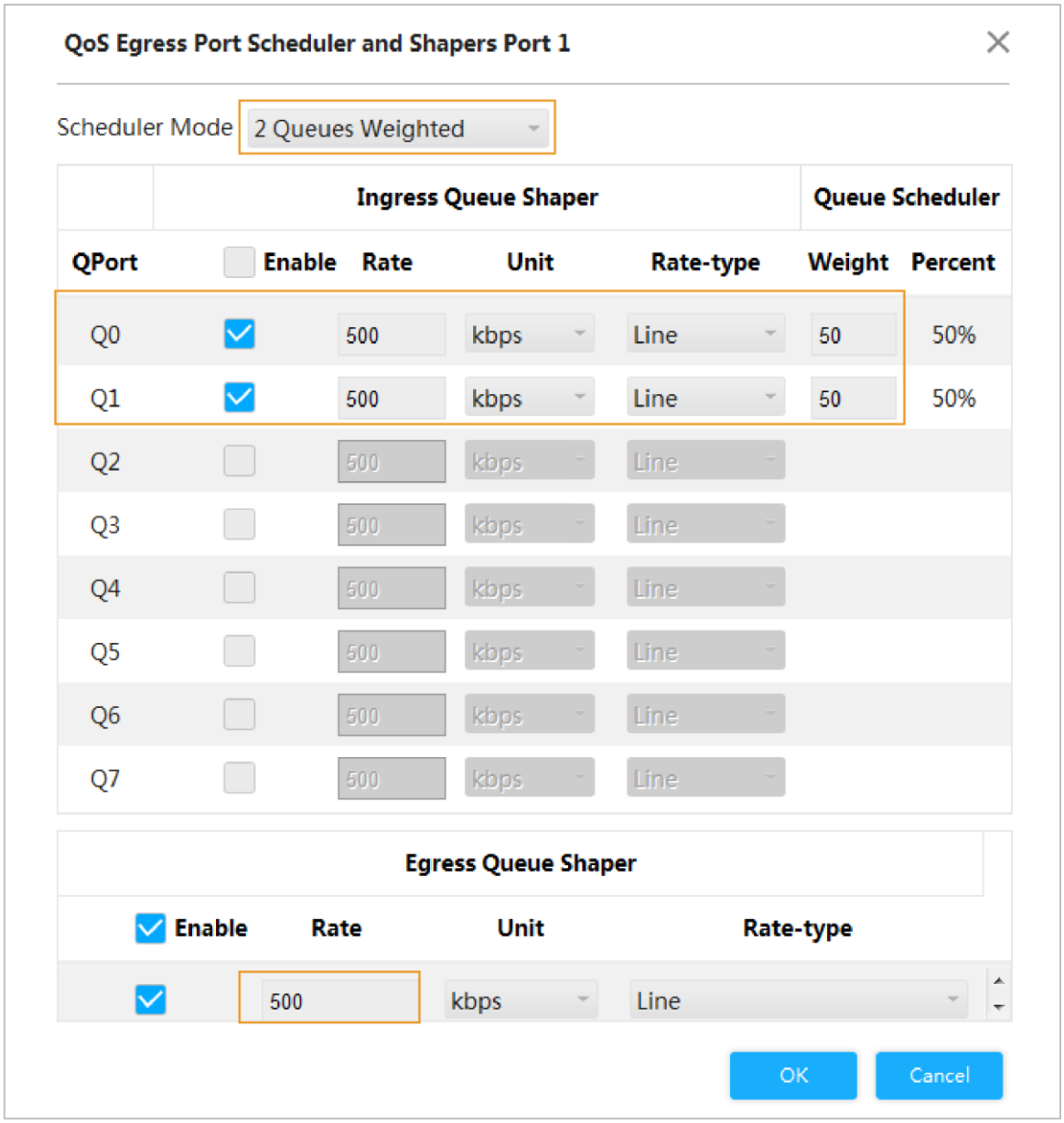
2) En **Formador de cola de entrada,** selecciona el **Velocidad** de **Q0** y **Q1** ser 500 kbps, y

Tipo de cambio para ser Line. En **Formador de cola de salida,** selecciona el **Velocidad** ser 500 kbps, y **Tipo de cambio** ser - estar **Línea.**

3)

Cuando se produce una congestión y la velocidad de los dos puertos es de 400 kbps, la velocidad que pasa por el puerto de salida es de 250 kbps.

Figura 3-56 Programadores de puertos



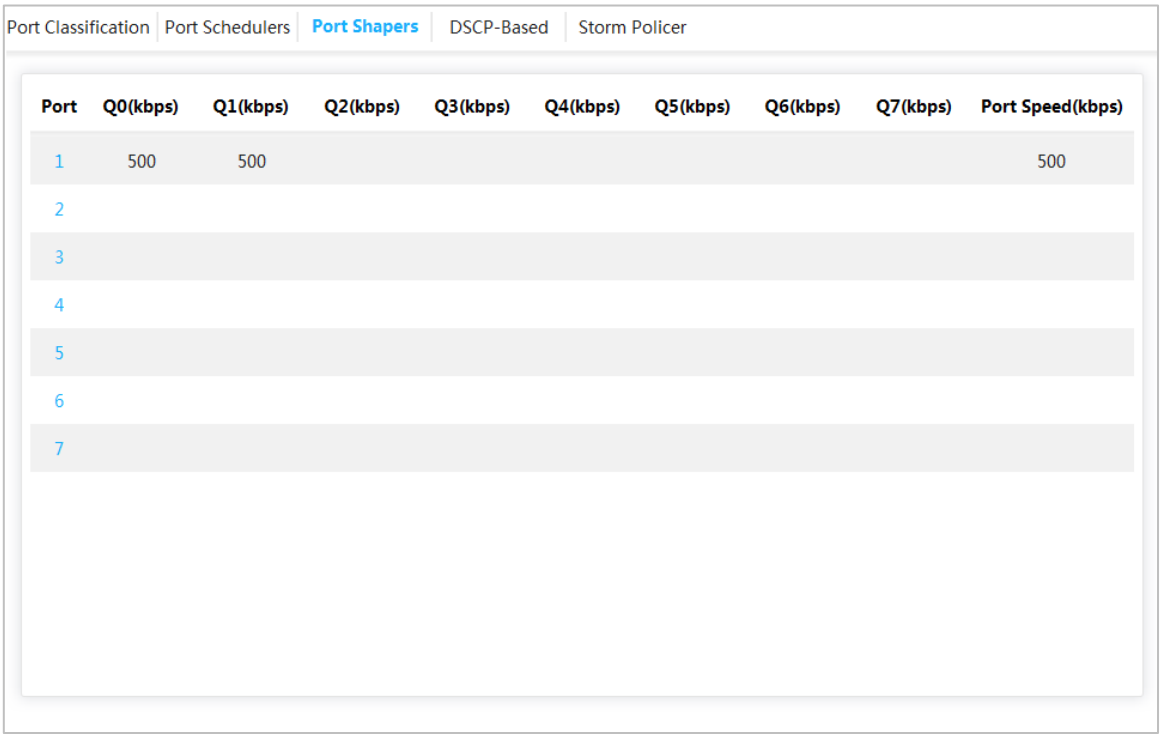
Paso 4 Haga clic en **OKAY.**

3.2.6.3 Modeladores de puertos

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

Seleccione **Avanzado> Rara vez usado> QoS> Port Shapers.** los **Formadores de puertos** se muestra la interfaz. Vea la Figura 3-57.

Figura 3-57 Modeladores de puertos



3.2.6.4 Basado en DSCP

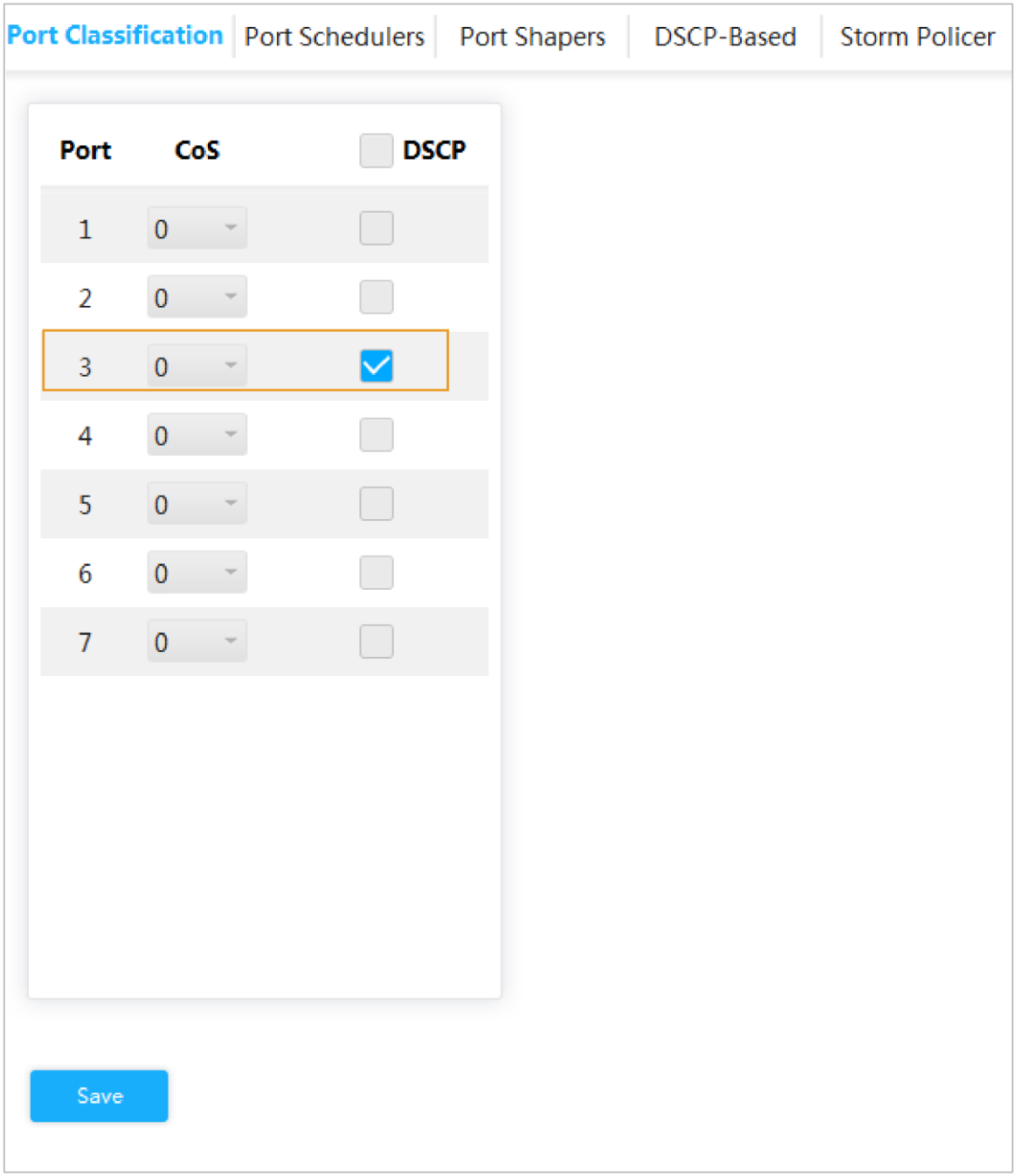
Asegúrese de haber habilitado DSCP antes de configurar la función DSCP.

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

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

Paso 2 Habilite DSCP en el puerto DSCP. Suponga que el puerto 3 es el puerto de salida, consulte la Figura 3-58.

Figura 3-58 Clasificación de puertos



Paso 3 Hacer clic **Salvar.**

Paso 4 Seleccione **Avanzado> Rara vez usado> QoS> Basado en DSCP.**

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

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

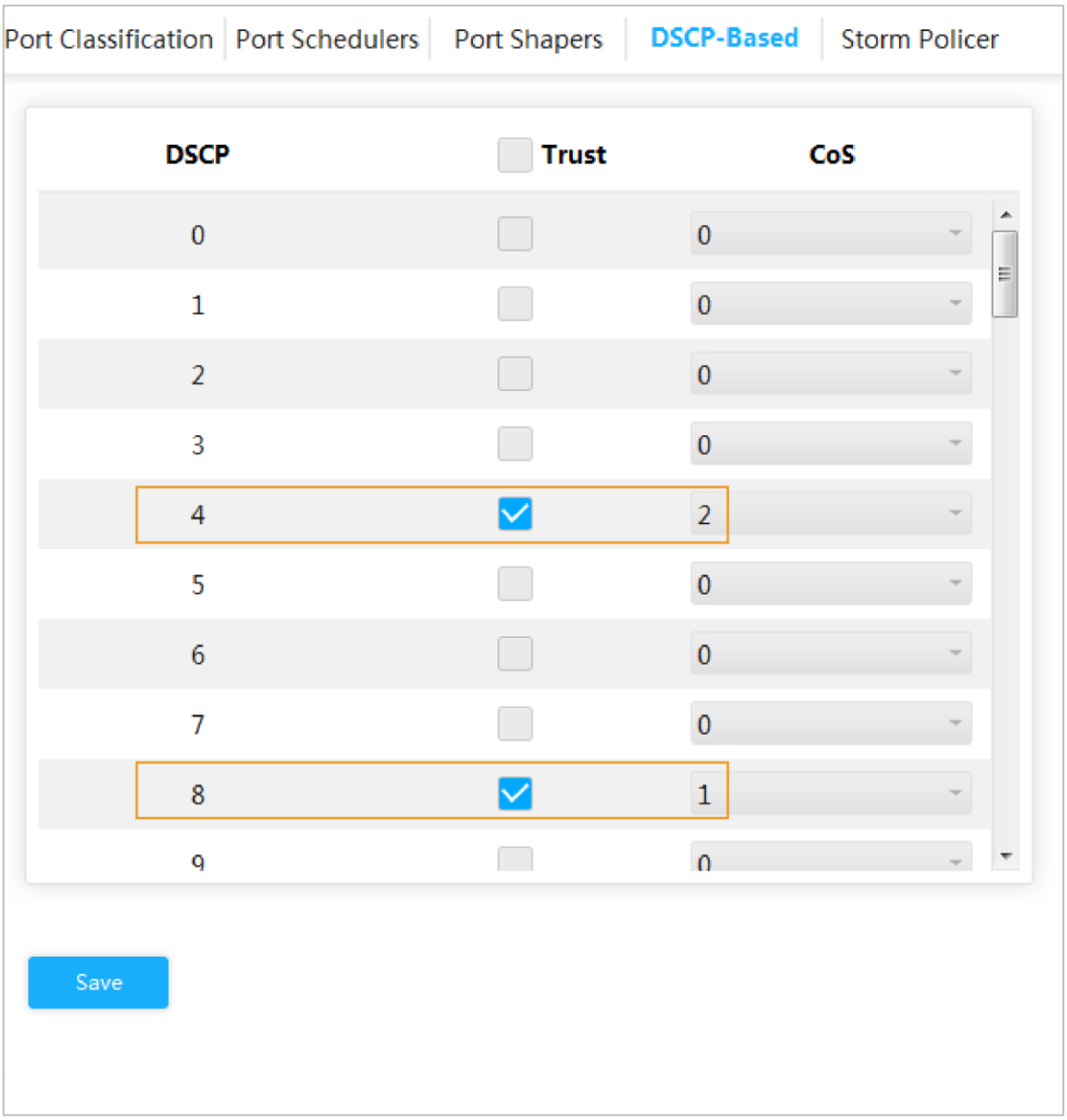
1) Cuando DSCP son 4 y 8, seleccione **Confiar** para habilitar la función. Vea la Figura 3-59.

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 de puerto correspondiente pasará primero por el puerto de salida.

Figura 3-59 Basado en DSCP



Paso 6 Haga clic en **Salvar.**

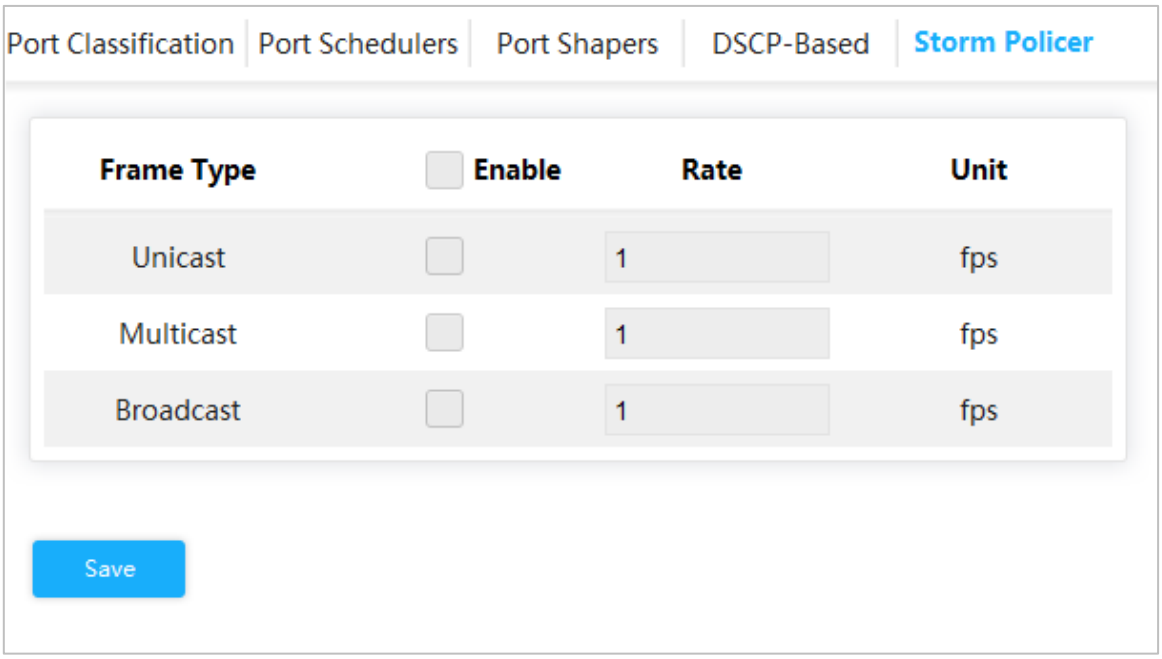
3.2.6.5 Policía de tormentas

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

Paso 1 Seleccione **Avanzado> Rara vez usado> QoS> Storm Policer.**

los **Policía de tormentas** se muestra la interfaz. Vea la Figura 3-60.

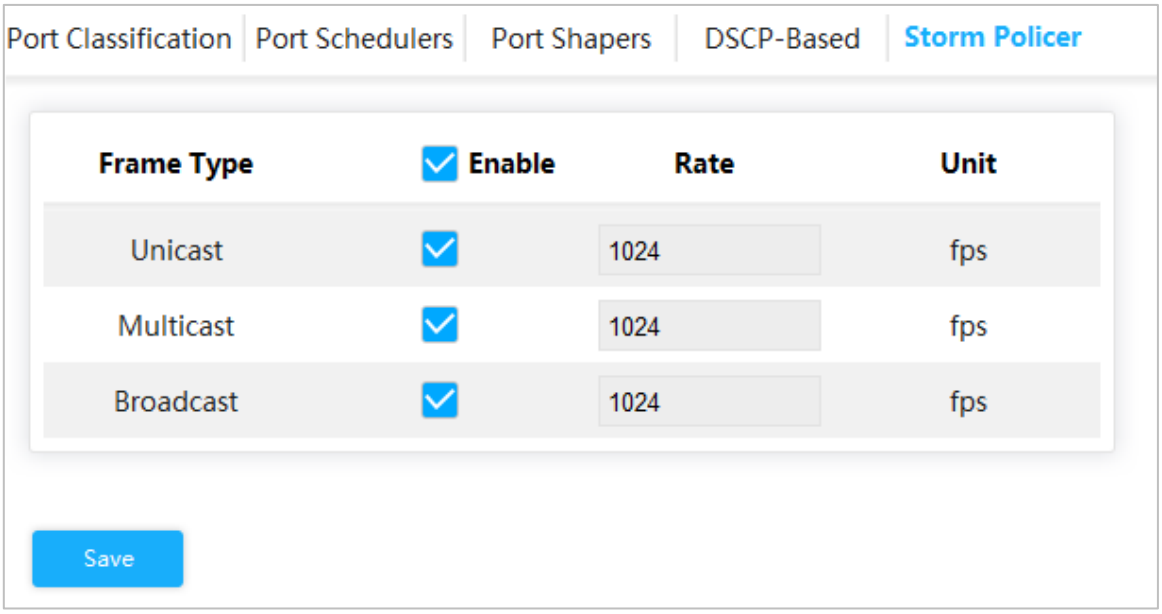
Figura 3-60 Vigilante de tormentas



Paso 2 El puerto puede recibir una velocidad de hasta 1024 fps. Vea la Figura 3-61.

- En **Unicast,** Selecciona el **Habilitar** e ingrese 1024 en **Velocidad.** Significa que el puerto puede recibir una velocidad de hasta 1024 fps de paquete de unidifusión.
- En **Multidifusión,** Selecciona el **Habilitar** e ingrese 1024 en **Velocidad.** Significa que el puerto puede recibir una velocidad de hasta 1024 fps de paquete de multidifusión.
- En **Transmitir,** Selecciona el **Habilitar** e ingrese 1024 en **Velocidad.** Significa que el puerto puede recibir una velocidad de hasta 1024 fps de paquete de transmisión.

Figura 3-61 Configuración del regulador de tormentas



Paso 3 Haga clic en **Salvar.**

3.2.7 SNMP

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

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

La red SNMP proporciona dos elementos, NMS y Agente.

- NMS (Sistema de administración de red) es el administrador de la red SNMP y proporciona una interfaz amigable hombre-máquina para ayudar al administrador de la red a terminar la mayor parte del trabajo de administración de la red.

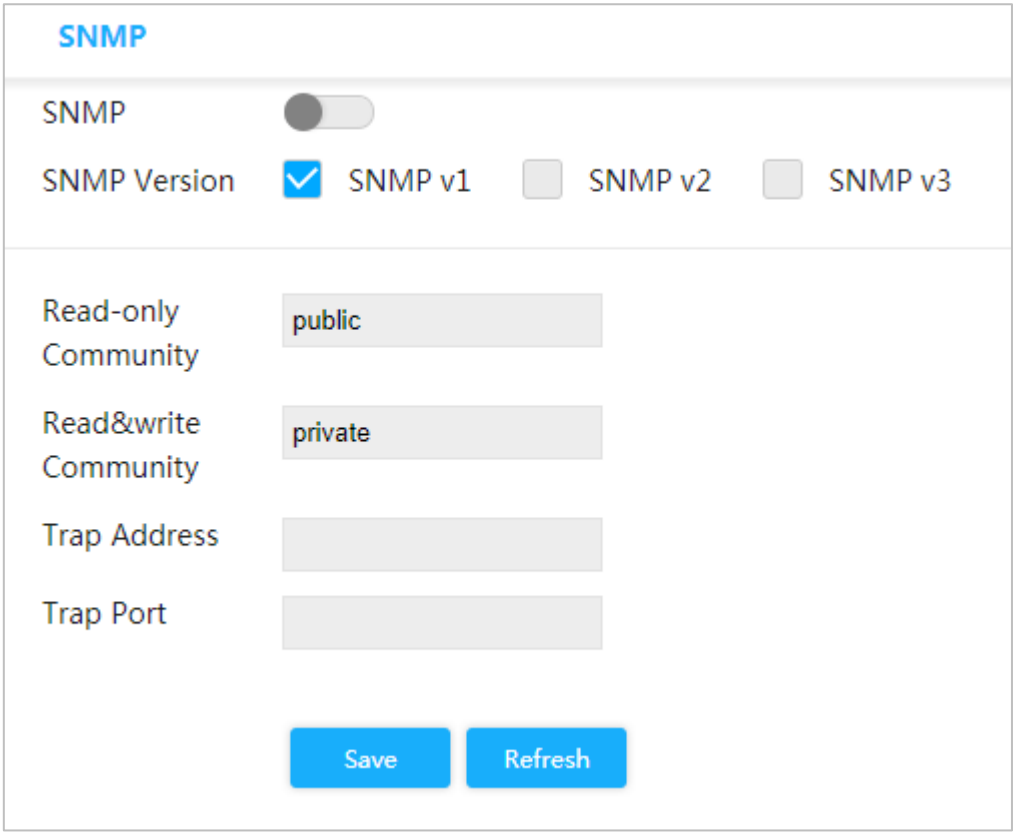
- El agente es el rol administrado en la red SNMP y recibe y maneja el paquete de solicitud de NMS. En algunas circunstancias de emergencia, por ejemplo, si cambia el estado del puerto, el Agente puede enviar un paquete de alarma a NMS de forma proactiva.

3.2.7.1 Habilitación de la función SNMP

Paso 1 Seleccione **Avanzado> Rara vez usado> SNMP.**

los **SNMP** se muestra la interfaz. Vea la Figura 3-62.

Figura 3-62 SNMP



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

Cada agente SNMP v3 tiene un ID de motor como su 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.**

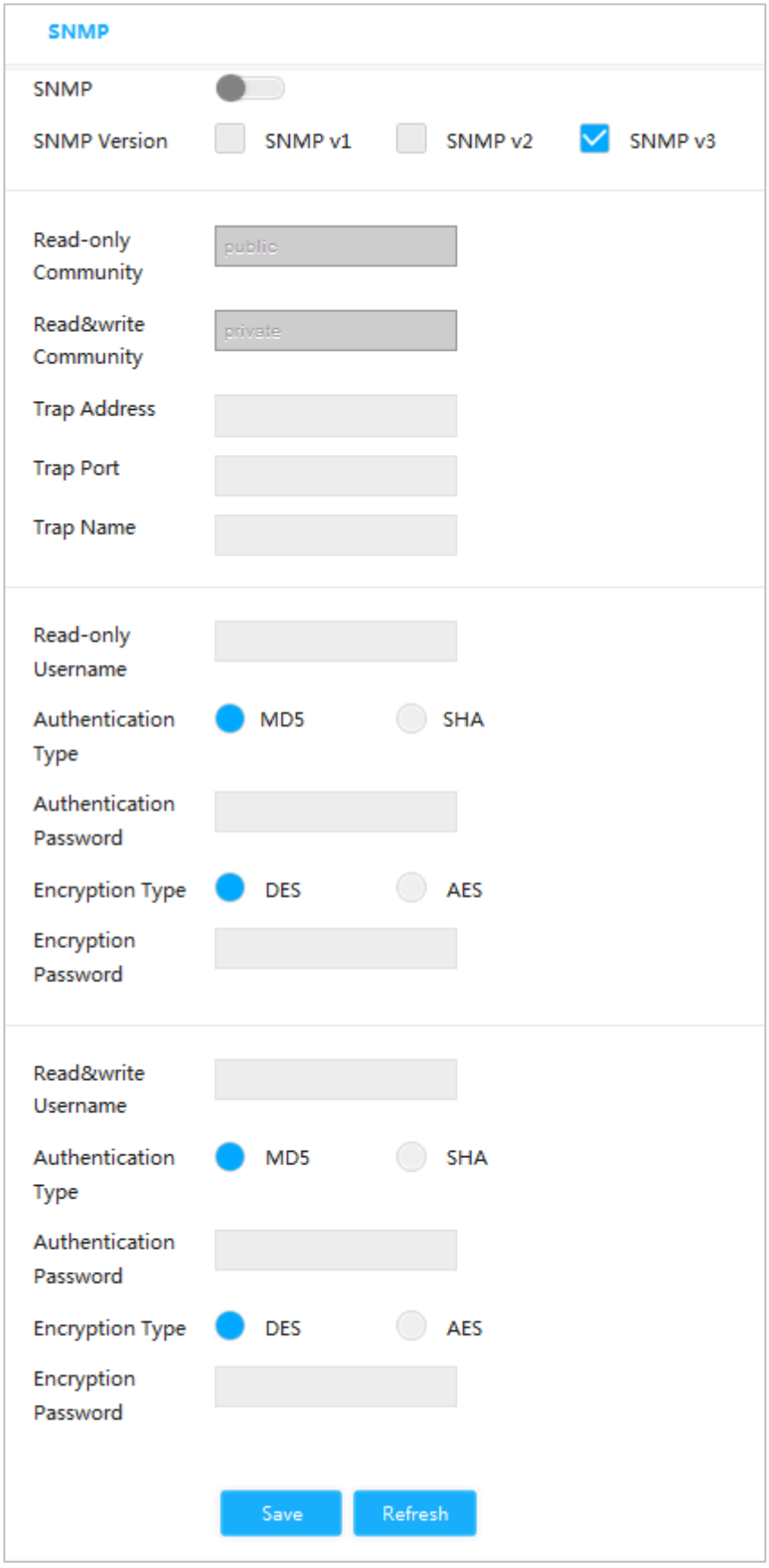
Paso 2 Configure la comunidad de solo lectura, la comunidad de lectura y escritura, la dirección de captura y el puerto de captura.

Paso 3 Haga clic en **Salvar.**

3.2.7.3 Configuración de SNMP v3

Paso 1 Seleccione SNMP v3 en **Versión SNMP.** Vea la Figura 3-63.

Figura 3-63 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 tipo y contraseña de cifrado.

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

Paso 5 Haga clic en **Salvar.**

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 la dirección IP para la estación de trabajo y asegurarse de que la dirección IP para cada estación de trabajo sea diferente. El servidor DHCP simplifica la tarea de gestión de la red que antes debería realizarse manualmente.

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

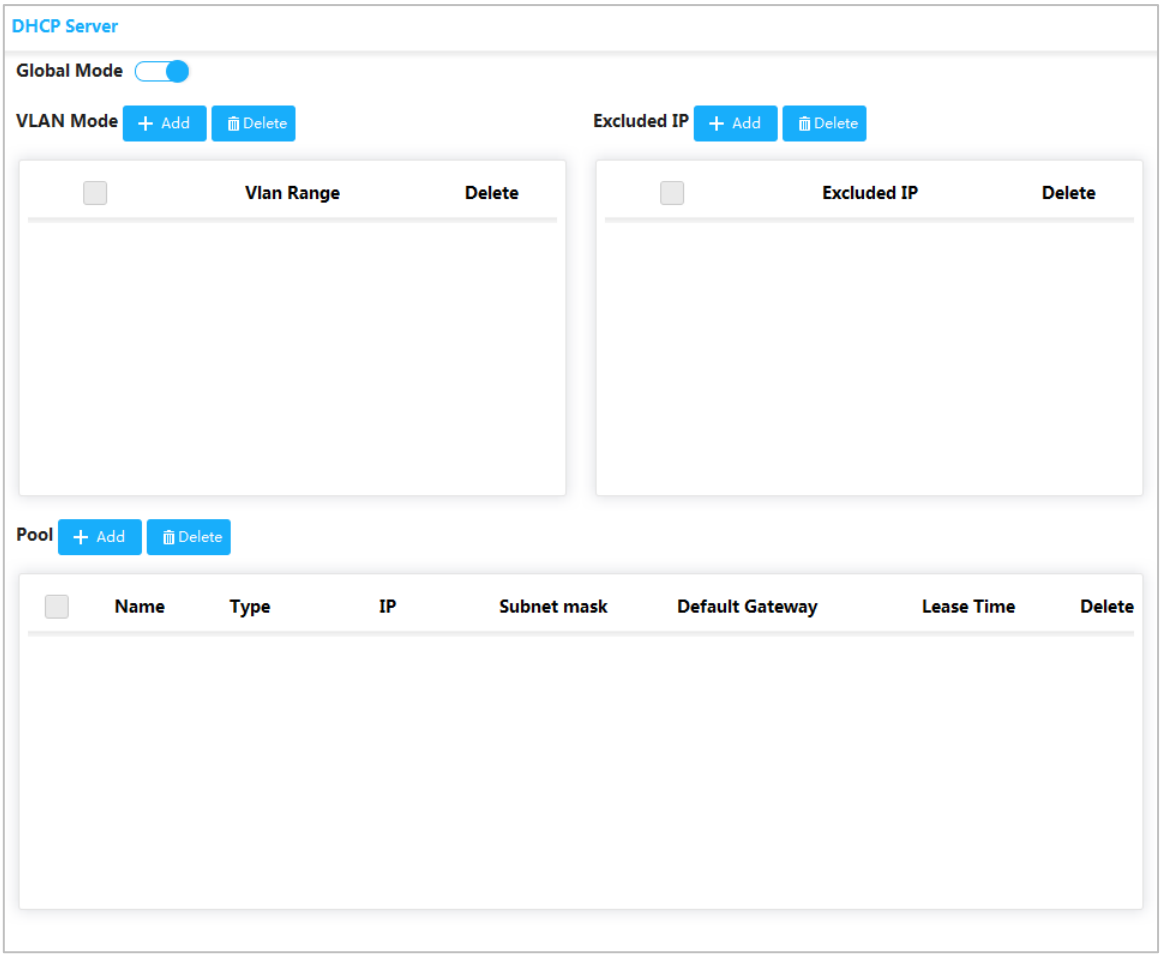
- La escala de la red es grande. La carga de trabajo es demasiado pesada si se configura manualmente y la administración centralizada de la red será difícil.
- La cantidad de PC es mayor que la cantidad de direcciones IP en la red y es imposible asignar una dirección IP estática para cada PC. Por ejemplo, la cantidad de usuarios que pueden acceder a la red al mismo tiempo está limitada por el ISP y el usuario necesita adquirir la dirección IP de forma dinámica.
- Solo una pequeña cantidad de PC necesitan 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 Seleccione **Avanzado> Rara vez usado> DHCP> Servidor DHCP.**

los **servidor DHCP** se muestra la interfaz. Vea la Figura 3-64.

Figura 3-64 Servidor DHCP



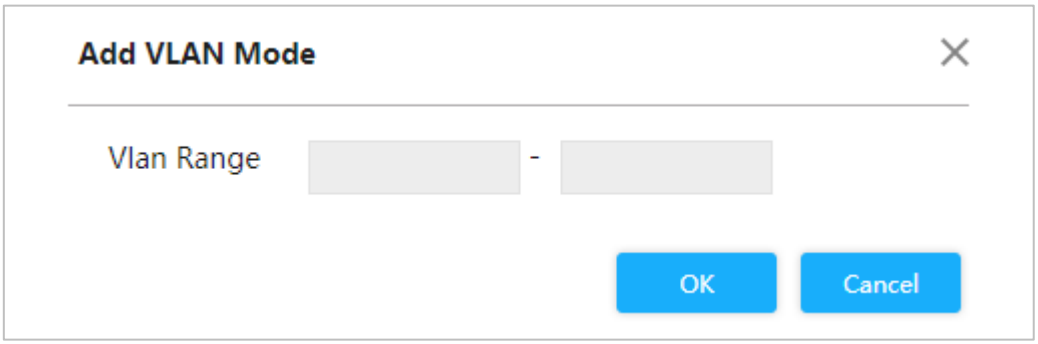
Paso 2 Haga clic en en **Modo global,** para habilitar la función del servidor DHCP.

Paso 3 Configure el modo DHCP.

Primero agregue la interfaz VLAN. Consulte "3.1.1.2 IP y ruta".

1) Haga clic en Agregar en modo VLAN. los **Agregar modo VLAN** se muestra la interfaz. Vea la Figura 3-65.

Figura 3-65 Agregar modo VLAN



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

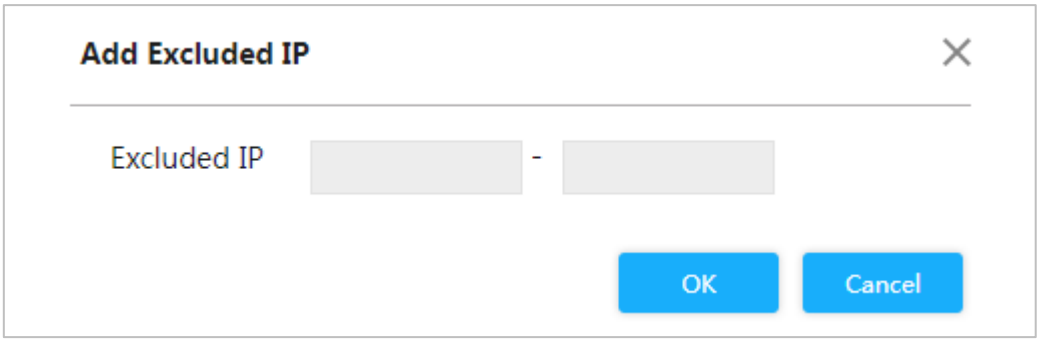
3) Haga clic en **OKAY.**

Paso 4 Configure el segmento de red de la IP excluida.

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

1) Haga clic en Agregar en IP excluida. los **Agregar IP excluida** se muestra la interfaz. Vea la Figura 3-66.

Figura 3-66 Agregar IP excluida



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

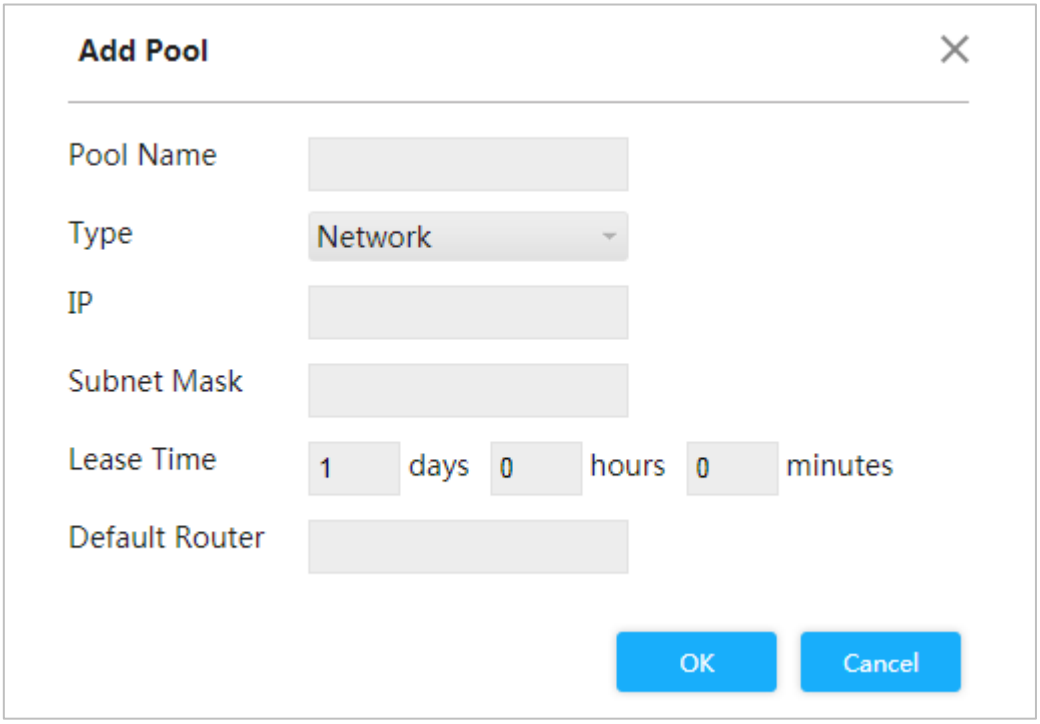
3) Haga clic en **OKAY.**

Paso 5 Agregue el grupo de direcciones DHCP.

1) Haga clic en **Añadir** en **Piscina.**

los **Agregar grupo** se muestra la interfaz. Vea la Figura 3-67.

Figura 3-67 Agregar grupo



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

Tabla 3-7 Parámetros de la piscina

Parámetro	Descripción
Nombre de la piscina	Nombre del grupo de direcciones DHCP, como vlan2_test. Dos
Tipo	tipos: **Red** y **Anfitrión.** • Red: el segmento de red de una IP. Anfitrión: una IP • específica
IP	La dirección IP del host o la red. La máscara de subred del host o la red.
Máscara de subred	Ingrese el tiempo de arrendamiento del grupo de direcciones. Configure la
Tiempo de arrendamiento	puerta de enlace predeterminada del grupo de direcciones.
Puerta	

3) Haga clic en **OKAY.**

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 principales capacidades, 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 entregarlo a su vecino. El vecino mantendrá la información recibida en forma de MIB estándar (Management Information Base), de modo que la administración de la red pueda consultar y juzgar el estado de comunicación del enlace.

LLDP

Paso 1 Seleccione **Avanzado> Rara vez usado> LLDP.**

los **LLDP** se muestra la interfaz. Vea la Figura 3-68.

Figura 3-68 LLDP

Paso 2 Configure el modo LLDP.

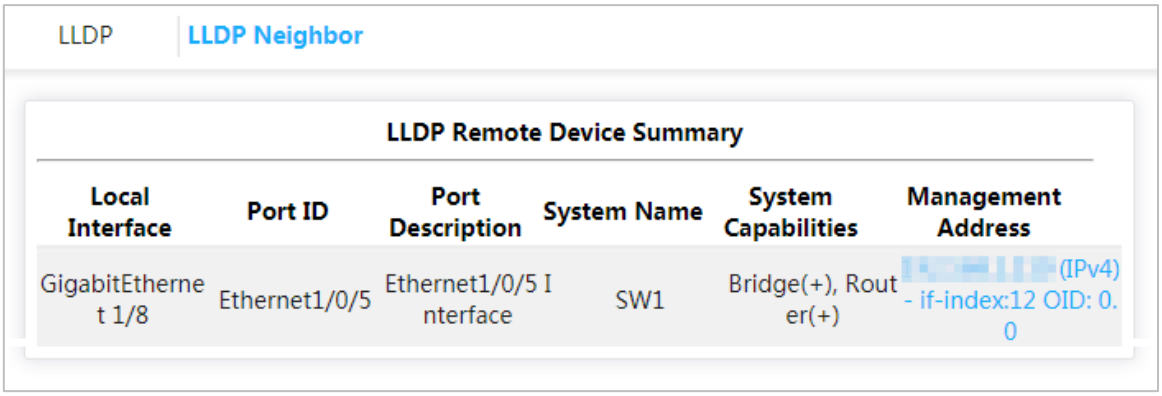
- Seleccione **Habilitar:** Ambos envían y reciben paquetes LLDP. Seleccione **Inhabilitar:**
- No envíe ni reciba paquetes LLDP. Seleccione **Rx activado** l **y:** Reciba solo paquetes
- LLDP. Seleccione **Tx solamente:** Solo envíe paquetes LLDP.
-

Paso 3 Haga clic en **Salvar.**

Ver la información de vecinos LLDP.

Seleccione **Avanzado> Rara vez usado> LLDP> Vecino LLDP.** los **Vecino LLDP** se muestra la interfaz. Vea la Figura 3-69.

Figura 3-69 Vecino LLDP

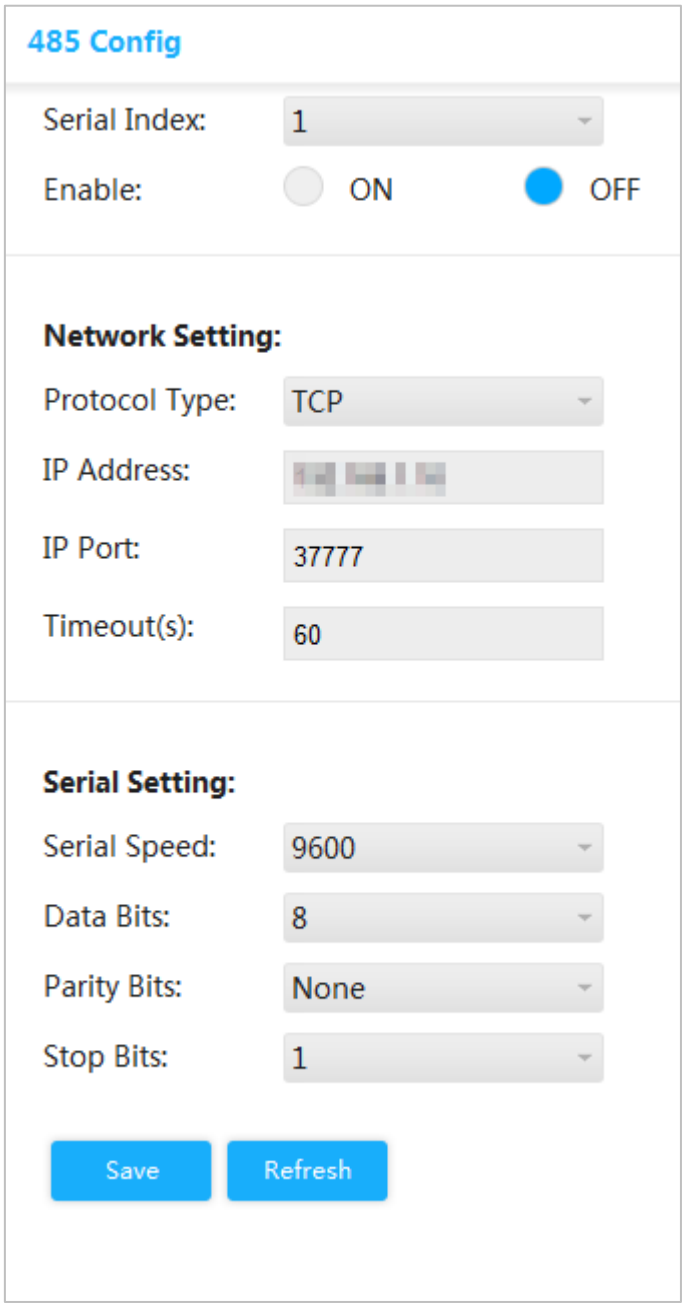


3.2.10 Configuración 485

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

Seleccione **Avanzado> Rara vez usado> 485 Config.** los **485 Config** se muestra la interfaz. Vea la Figura 3-70.

Figura 3-70 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 para el PD externo (Powered Device) de forma remota con par trenzado. La función PoE ayuda a centralizar la fuente de alimentación y facilita la copia de seguridad. El terminal de red ya no necesita la fuente de alimentación externa, y un cable de red es suficiente. Cumple con los estándares de IEEE 802.3af e IEEE 802.3at, adoptando el puerto de alimentación acordado a nivel mundial. Se puede aplicar en teléfono IP, AP (punto de acceso) inalámbrico, cargador de dispositivo portátil, lector de tarjetas, cámara de red, recolección de fechas, etc.

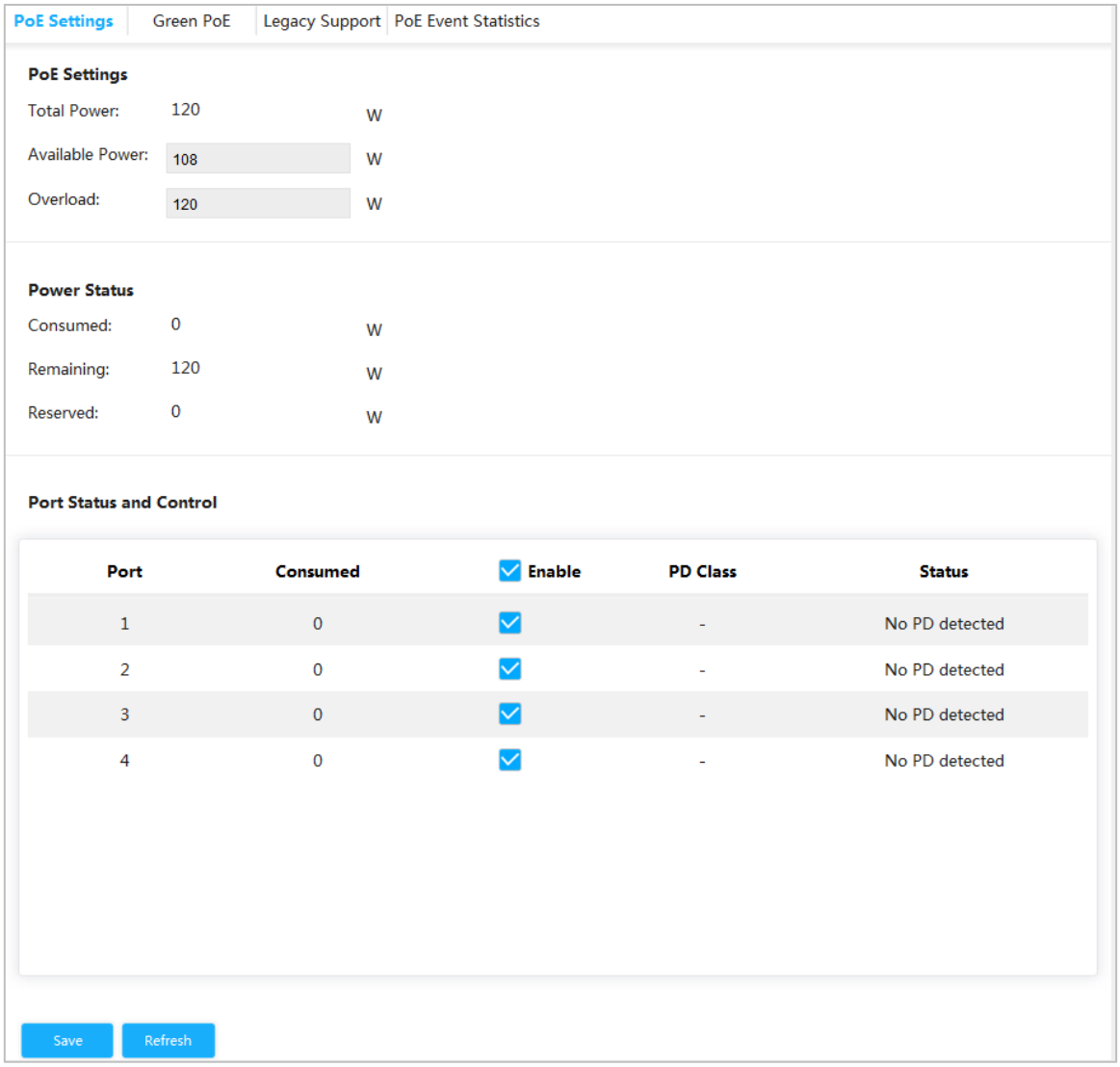
3.2.11.1 Parámetros de PoE

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

Paso 1 Seleccione **Avanzado> Poco usado> PoE> Configuración de PoE.**

los **Configuración de PoE** se muestra la interfaz. Vea la Figura 3-71.

Figura 3-71 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.

Paso 4 En **Estado y control del puerto,** Selecciona el **Habilitar** cuadro para habilitar o deshabilitar PoE del puerto correspondiente.

Paso 5 Hacer clic **Salvar.**

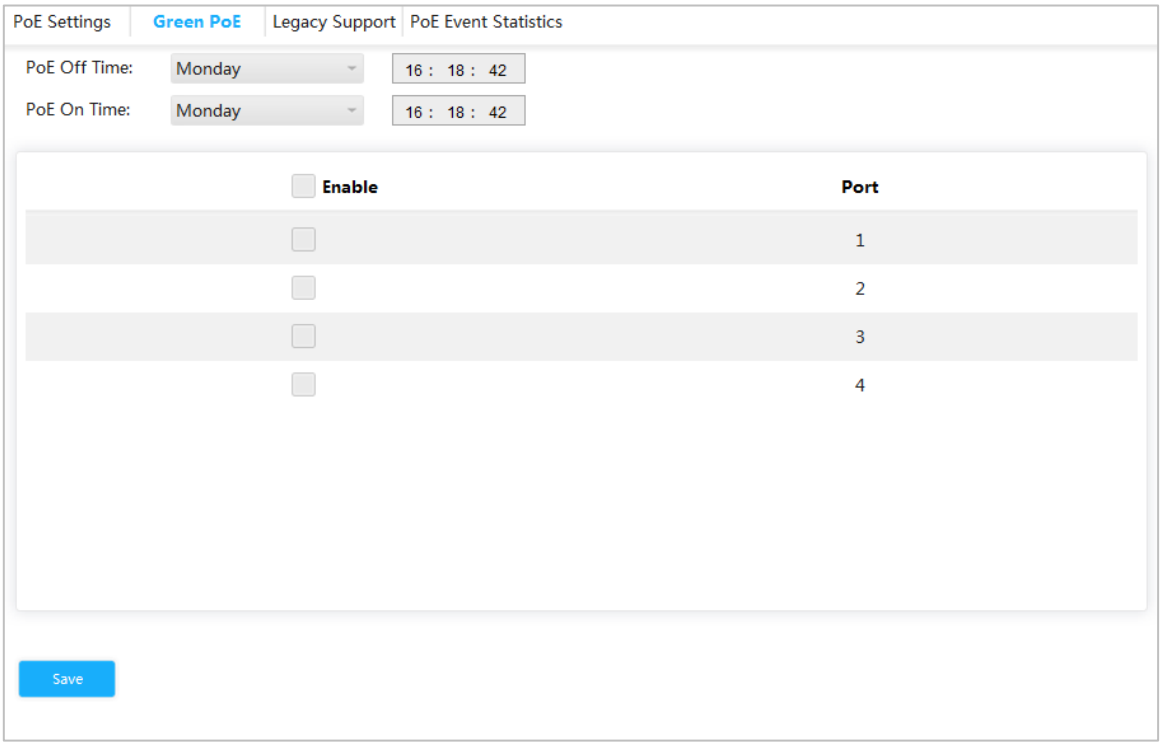
3.2.11.2 PoE verde

Configure el tiempo de apagado de PoE y el tiempo de encendido de PoE.

Paso 1 Seleccione **Avanzado> Rara vez usado> PoE> Green PoE.**

los **PoE verde** se muestra la interfaz. Vea la Figura 3-72.

Figura 3-72 PoE verde



Paso 2 juegos **Tiempo de apagado de PoE.**

Paso 3 Establecer **PoE a tiempo.**

Paso 4 Seleccione el **Habilitar** caja.

Paso 5 Haga clic en **Salvar.**

3.2.11.3 Soporte heredado

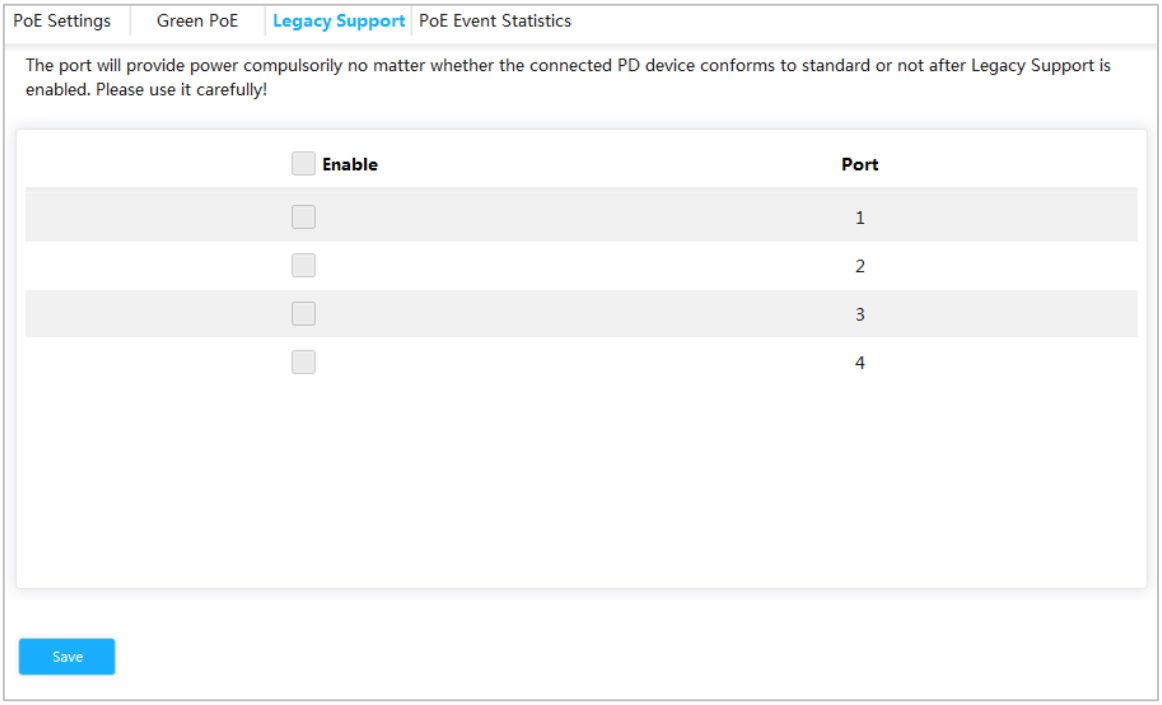
Habilitar **Soporte heredado** en caso de dispositivo alimentado no estándar.

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

Paso 1 Seleccione **Avanzado> Rara vez usado> PoE> Soporte heredado.**

los **Soporte heredado** se muestra la interfaz. Vea la Figura 3-73.

Figura 3-73 Soporte heredado



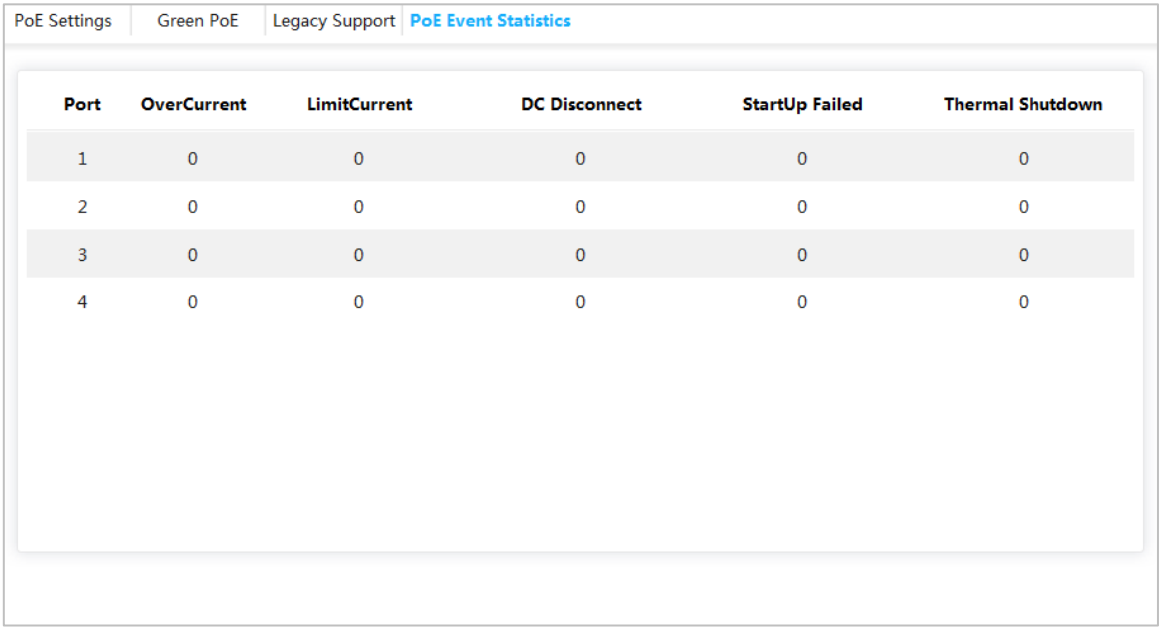
Paso 2 Seleccione el **Habilitar** caja.

Paso 3 Haga clic en **Salvar.**

3.2.11.4 Visualización de estadísticas de eventos de PoE

Seleccione **Avanzado> Rara vez usado> PoE> Estadística de eventos PoE.** los **Estadística de eventos PoE** se muestra la interfaz. Vea la Figura 3-74.

Figura 3-74 Estadística de eventos de PoE



4 Mantenimiento

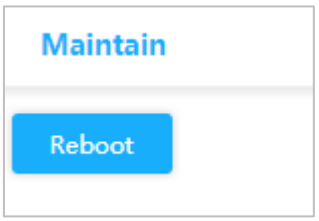
Tomemos como ejemplo el conmutador PoE de 4 puertos. La interfaz de mantenimiento es diferente según los modelos de conmutador. La interfaz real prevalecerá.

4.1 Reinicio del sistema

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

los **Reinicio del sistema** se muestra la interfaz. Vea la Figura 4-1.

Figura 4-1 Reinicio del sistema



Paso 2 Haga clic en **Reiniciar.**

Paso 3 Haga clic en **Confirmar,** y el dispositivo se reinicia.

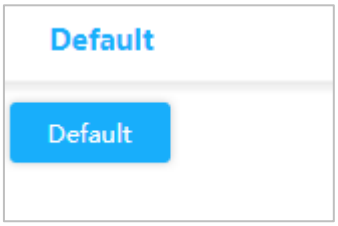
4.2 Restauración de la configuración predeterminada

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

Paso 1 Seleccione **Mantener> Común> Restaurar valores predeterminados.**

los **Defecto** se muestra la interfaz. Vea la Figura 4-2.

Figura 4-2 Restaurar valores predeterminados



Paso 2 Haga clic en **Defecto.**

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

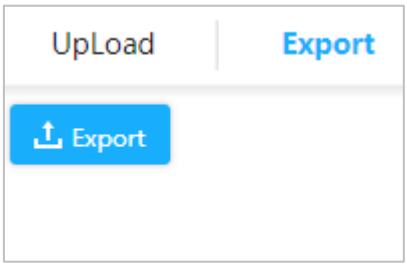
4.3 Gestión de configuración

4.3.1 Exportar archivo de configuración

Paso 1 Seleccione **Mantener> Común> Gestión de configuración> Exportar.**

los **Exportar** se muestra la interfaz. Vea la Figura 4-3.

Figura 4-3 Exportar



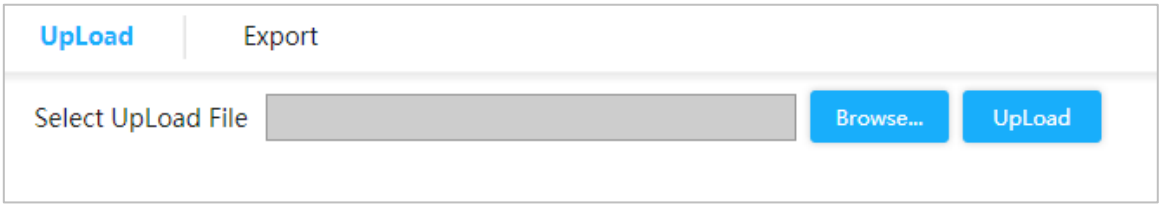
Paso 2 Haga clic en **Exportar.** Exportar archivo de configuración.

4.3.2 Carga del archivo de configuración

Paso 1 Seleccione **Mantener> Común> Gestión de configuración> Cargar.**

los **Subir** se muestra la interfaz. Vea la Figura 4-4.

Figura 4-4 Carga



Paso 2 Haga clic en **Broswe ...,** y seleccione el archivo de configuración para cargar.

Paso 3 Haga clic en **Subir.**

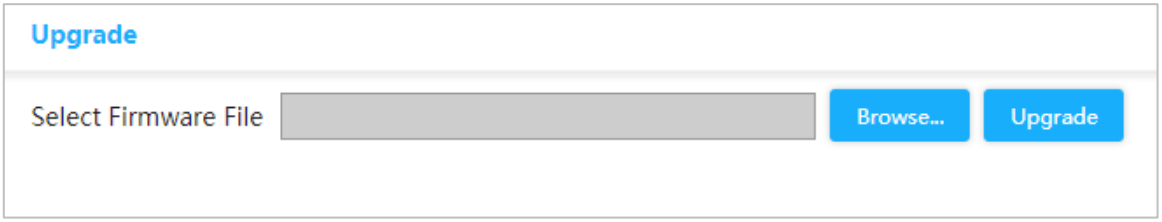
Paso 4 Reinicie el dispositivo y la configuración tendrá efecto.

4.4 Actualización de software

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

los **Actualizar** se muestra la interfaz. Vea la Figura 4-5.

Figura 4-5 Actualización



Paso 2 Haga clic en **Vistazo...,** y seleccione el archivo en formato .mif para cargar.

Paso 3 Haga clic en **Subir.**

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

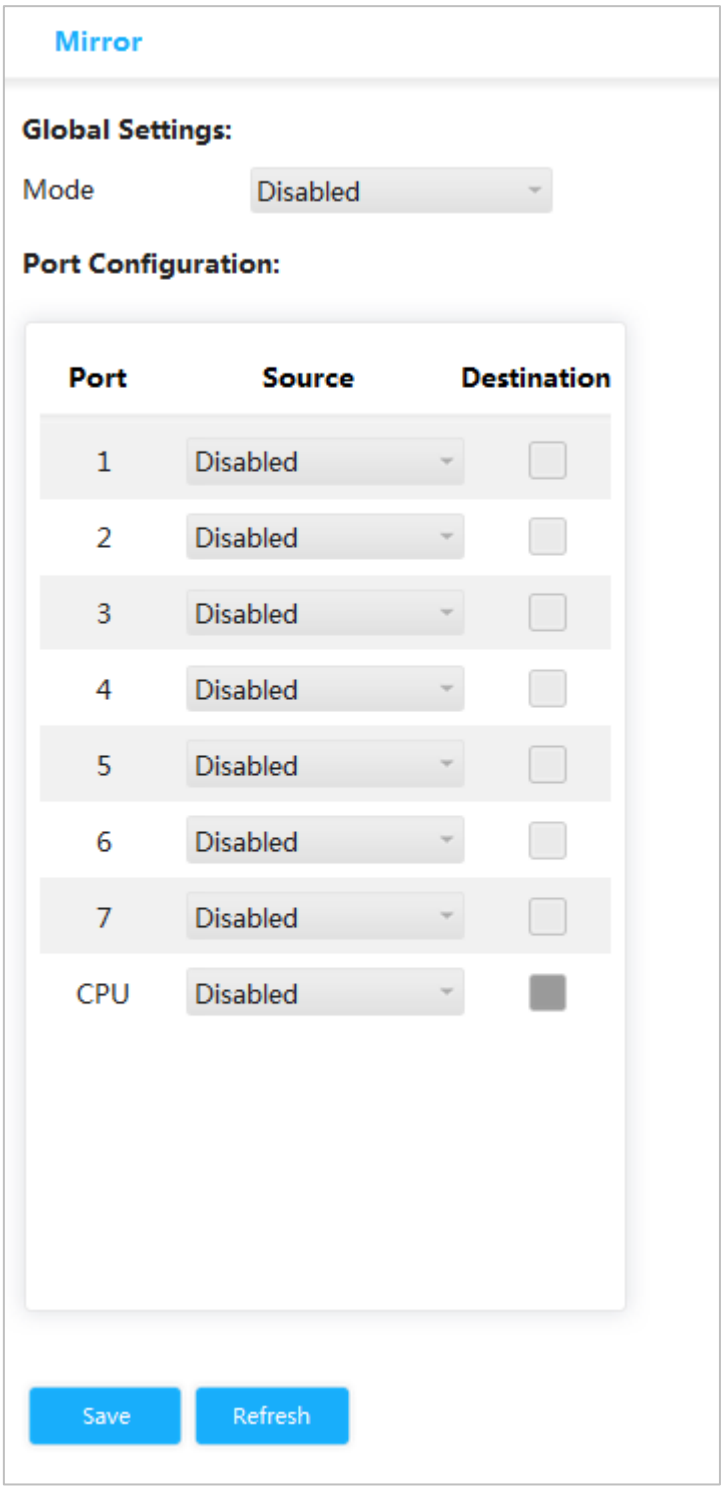
4.5 Reflejo

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

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

los **Espejo** se muestra la interfaz. Vea la Figura 4-6.

Figura 4-6 Espejo



Paso 2 en **Configuración global,** Seleccione **Habilitado** en **Modo** para habilitar la duplicación.

Paso 3 en **Configuración del puerto,** Seleccione **Fuente** o **Destino** según la situación real.

- Seleccione las siguientes cuatro formas para el puerto de origen.
  - Ambos: habilite el puerto como la dirección de origen del espejo.
  - Deshabilitar: 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.

Paso 4 Haga clic en **Salvar.**

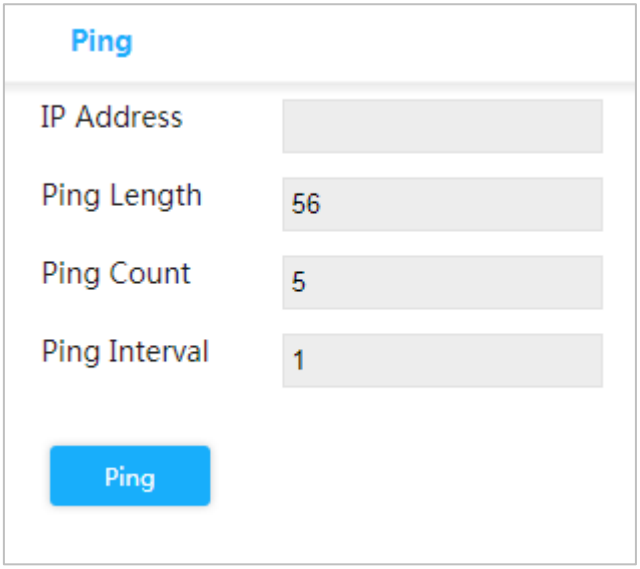
4.6 Ping

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

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

los **Silbido** se muestra la interfaz. Vea la Figura 4-7.

Figura 4-7 Ping



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

Apéndice 1 Recomendaciones de ciberseguridad

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

Acciones obligatorias que deben tomarse 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 contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso; No utilice
- caracteres continuos, como 123, abc, etc .; No utilice caracteres superpuestos, como 111,
- aaa, etc .;

2. Actualice el firmware y el software cliente a tiempo

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

- Le sugerimos que descargue y utilice la última versión del software cliente.

Recomendaciones "Es bueno tener" 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 especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos como daños en el hardware, conexión no autorizada de equipos extraíbles (como un disco flash USB , puerto serie), etc.

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

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

4. Habilitar bloqueo de cuenta

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

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

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

6. **Habilitar HTTPS**

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

7. **Habilitar lista blanca**

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

8. **Enlace de dirección MAC**

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

9. **Asignar cuentas y privilegios de forma razonable**

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

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

    Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir 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 autenticación y de cifrado seguras.
    - SMTP: elija TLS para acceder al servidor de buzones de correo. FTP: elija
    - SFTP y configure contraseñas seguras.
    - Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

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

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

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

12. **Auditoría segura**

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

13. **Registro de red**

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

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

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

    - Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.

- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, 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.

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Dirección: No.1199, Bin'an Road, Binjiang District, Hangzhou, PR China Código postal: 310053

Tel: + 86-571-87688883

Envíe por fax: + 86-571-87688815

Correo electrónico: overseas@dahuatech.com

Sitio web: www.dahuasecurity.com