Switches Ruijie Reyee de las series ES, NBS y NIS

Manual de implementación

Versión del documento: V1.8
Fecha: 2023.12.26
Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 Ruijie Networks

Todos los derechos reservados en el presente documento y declaración.

Sin el consentimiento previo por escrito de Ruijie Networks, ninguna empresa o individuo puede reproducir, extraer, respaldar, modificar o difundir el contenido del presente documento, de ninguna manera o de ninguna forma, o traducirlo en otros idiomas o utilizarlo, parcial o totalmente, para fines comerciales.



y los demás logotipos de las redes Ruijie son marcas comerciales de Ruijie Networks.

Todas las demás marcas comerciales o marcas registradas que se mencionan en el presente documento pertenecen a sus respectivos dueños.

Exclusión de responsabilidad

Los productos, servicios y funciones adquiridos están sujetos a contratos y términos comerciales, y algunos, o todos los productos, servicios y funciones descritos en el presente documento puede que no se encuentren disponibles para su compra o uso. A excepción del acuerdo en el contrato, Ruijie Networks no hace declaraciones o garantías, explícitas o implícitas, respecto al contenido del presente documento.

El contenido del presente documento está sujeto a cambios en cualquier momento debido a las mejoras en la versión de los productos o por otras razones; Ruijie Networks se reserva el derecho de modificar su contenido sin previo aviso.

El presente documento está diseñado solamente como manual de usuario. Al elaborar este manual, Ruijie Networks ha hecho lo posible por garantizar la exactitud y confiabilidad del contenido; sin embargo, esto no garantiza que el contenido esté libre de errores u omisiones y la información en el presente documento no constituye garantía alguna, explícita o implícita.

Prólogo

Principales usuarios

El presente documento está dirigido a:

- Ingenieros de redes
- Ingenieros de soporte técnico y servicio
- Administradores de redes

Asistencia técnica

- Sitio web oficial de Ruijie Reyee: https://www.ruijienetworks.com/products/reyee

Reglas de uso

1. Símbolos de la interfaz gráfica de usuario (GUI)

Símbolos de la interfaz	Descripción	Ejemplo
Negritas	1. Nombres de los botones 2. Nombres de las ventanas, pestañas, campos y elementos del menú 3. Enlace	1. Haga clic en **Aceptar**. 2. Seleccione **Asistente de Config**. 3. Haga clic en el enlace **Descargar archivo**.
>	Elementos de los menús multinivel	Seleccione **Sistema** > **Hora**.

2. Avisos

Este documento también incluye avisos para indicar puntos importantes durante el procedimiento. A continuación, se describen los significados de estos:

Advertencia

Una alerta que señala reglas o información importante que, de no entenderse o acatarse, puede ocasionar la pérdida de datos o daño en el equipo.

Nota

Una alerta que señala reglas o información esencial que, de no entenderse o acatarse, puede ocasionar fallas o deterioro en el funcionamiento.

Instrucción

Una alerta con información complementaria o adicional que, de no entenderse o acatarse, no tiene mayores consecuencias.

Especificación

Una alerta que respalda la descripción del producto o versión.

3. Instrucción

La intención del presente manual es ayudar a los usuarios a comprender el producto, instalarlo y configurarlo totalmente.

El ejemplo del tipo de puerto puede ser diferente en la situación real. Inicie la configuración de acuerdo con el tipo de puerto compatible con el producto.

La información que se muestra como ejemplo puede incluir contenido de otros productos de la serie (como el modelo o la descripción). Considere solamente la información que se muestra referente al producto.

Los routers e íconos de sus productos en este manual representan los routers comunes y los conmutadores de capa-3 con protocolo de enrutamiento.

Este manual solo ofrece información sobre la configuración (incluidos el modelo, la descripción, el tipo de puertos y la interfaz de software) con fines indicativos. En caso de que exista cualquier discrepancia o incoherencia entre el manual y la versión real, prevalecerá la versión real.

Índice

1 Introducción a los switches Reyee ES200

1.1 Información general de los switches Reyee Serie ES2

Los switches o conmutadores Ruijie Reyee de vigilancia inteligente ofrecen varias opciones de puertos para satisfacer los requerimientos de las redes de vigilancia mediante video de diferentes niveles. Los conmutadores Ruijie Reyee de vigilancia inteligente son compatibles con la PoE de salida, para garantizar que todas las cámaras se enciendan de manera simultánea cuando se conectan al switch de carga máxima. Además, los switches Ruijie Reyee de vigilancia inteligente cuentan con funciones de gestión sencillas y fáciles de usar, mientras que ofrecen la facilidad de conectar y usar la configuración predeterminada de fábrica. Pueden detectar rápidamente fallas en la red de vigilancia, reiniciar el puerto PoE y usar una configuración VLAN, entre otras funciones. También admiten la gestión remota a través de la app o plataforma Ruijie Cloud, para llevar a cabo funciones más sencillas y convenientes de O&M de la red de vigilancia, reduciendo su costo.

1.1.1 Lista de productos

Modelo	Puerto Ethernet 10/100 Base-T con negociación automática	Puerto Ethernet 10/100/1000 Base-T con negociación automática	Puerto SFP 1000Base-X	Puerto para consola
RG-ES205GC-P	N/A	5 (Puertos 1-4 compatibles con PoE+/PoE)	N/A	N/A
RG-ES209GC-P	N/A	9 (Puertos 1-8 compatibles con PoE+/PoE)	N/A	N/A
RG-ES218GC-P	N/A	16 (compatibilidad con PoE+/PoE)	2	N/A
RG-ES226GC-P	N/A	24 (PoE+/PoE)	2	N/A

Modelo	Puerto Ethernet 10/100 Base-T con negociación automática	Puerto Ethernet 10/100/1000 Base-T con negociación automática	Puerto SFP 1000Base-X	Puerto para consola
RG-ES224GC	N/A	24	N/A	N/A
RG-ES216GC	N/A	16	N/A	N/A
RG-ES106D-P V2	6	N/A	N/A	N/A
RG-ES126S-LP V2	24	1	1 puerto combinado	N/A
RG-ES126S-P V2	24	1	1 puerto combinado	N/A

Los puertos SPF no son compatibles con 100Base-FX y anteriores.

1000Base-T es compatible con 1000Base-TX y 10Base-T en el enlace descendente.

1.1.2 Indicador LED

LED	Estado	Significado
LED de estado del sistema	Sin luz	El conmutador no está recibiendo energía.
	Verde parpadeante	La energía PoE excede la energía total del dispositivo (370 W). El dispositivo alimentado (PD) que acaba de conectar no enciende debido a la falta de energía. La función de conmutación se encuentra operando.
	Verde fijo	El conmutador está funcionando.
Indicador LED de estado de PoE del puerto RJ45	Sin luz	PoE no está habilitado.
	Verde fijo	PoE está habilitado. El puerto está operando.
	Verde parpadeante	Sobrecarga de PoE.
Indicador LED de estado del puerto RJ-45, a una velocidad de 1000 Mbps	Sin luz	El puerto no está conectado.
	Verde fijo	El puerto está conectado a una velocidad de 10/100/1000 Mbps.
	Verde parpadeante	El puerto está recibiendo o transmitiendo datos a una velocidad de 10/100/1000 Mbps.
	Sin luz	El puerto no está conectado.

Indicador LED de estado del puerto SFP	Verde fijo	El puerto está conectado a una velocidad de 1000 Mbps.
	Verde parpadeante	El puerto está recibiendo o transmitiendo datos a una velocidad de 1000 Mbps.

1.1.3 Botón

Botón	Descripción
Botón LED de cambio del modo de puerto	Cuando se gira el botón a la posición izquierda (Modo 1) el LED indica el estado de funcionamiento del puerto. Cuando el LED muestra una luz verde fija, significa que se estableció el enlace. Cuando el LED muestra una luz verde parpadeante, significa que se están transmitiendo o recibiendo datos. Cuando se gira el botón a la posición derecha (Modo 2), el LED indica el estado PoE de los puertos. Cuando el LED muestra una luz verde fija, los puertos compatibles con PoE están suministrando energía. Cuando el LED muestra una luz verde parpadeante, hay sobrecarga de energía de los puertos.
Botón de restablecimiento del sistema	El conmutador se reinicia al presionar el botón de restablecimiento por menos de 2 segundos. El conmutador restablece la configuración predeterminada de fábrica al presionar el botón de restablecimiento por más de 5 segundos (hasta que el LED de estado parpadee).

1.2 Switch Reyee NBS Serie

Los conmutadores de la serie Reyee RG-NBS3100 disponibles se adaptan a las aplicaciones de pequeñas y medianas empresas (PyMes) y cuentan con diferentes niveles de acceso para sus redes. Cuentan con asignación de VLAN y funciones de seguridad avanzadas, como las Listas de Control de Acceso (ACL). El modelo con extensión -P permite el PoE de salida y puede proporcionar energía PoE, en diferentes situaciones, para AP inalámbricos, cámaras digitales y otros dispositivos.

Los conmutadores de la serie RG-NBS3200 de Reyee son conmutadores Ethernet capa 2 de próxima generación y brindan un alto desempeño, sólida seguridad y servicio multifuncional integrado. Adoptan un diseño arquitectónico de hardware eficiente, con especificaciones de entrada más largas y una experiencia de operación más práctica. La serie RG-NBS3200 brinda una conexión gigabit flexible de enlace ascendente a puertos 10GE. Toda la serie de conmutadores cuenta con cuatro puertos ópticos 10GE fijos con una capacidad de enlace ascendente de alto desempeño.

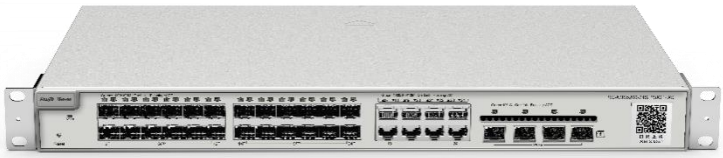
Los conmutadores de la serie Ruijie RG-NBS5100&5200 son conmutadores Ethernet capa 3 de próxima generación, alto desempeño, seguridad y servicio multifuncional. Mediante la adopción de un diseño arquitectónico de hardware eficiente, esta serie de conmutadores cuenta con una tabla de direcciones MAC más amplia y una experiencia de operación más práctica. La serie RG-NBS5100 brinda una conexión gigabit y un enlace ascendente, mientras que la serie RG-NBS5200 brinda una conexión gigabit y un enlace ascendente

a puertos 10G. Todos los conmutadores de la serie cuentan con cuatro puertos ópticos 10GE fijos con una capacidad de enlace ascendente de alto desempeño.

Los conmutadores de la serie RG-NBS5100&5200 brindan una calidad de servicio QoS integral de principio a fin, además de una configuración flexible y de gran seguridad para redes pequeñas y medianas. La serie RG-NBS5100&5200 es rentable, además de satisfacer las necesidades de las redes empresariales sobre alta velocidad, seguridad e inteligencia.

El modelo RG-NBS6002 es un switch de red de tipo caja intercambiable de 1U desarrollado de manera independiente por Ruijie Networks. Cuenta con dos ranuras para tarjetas de línea para cuatro tipos de tarjetas de línea y dos ranuras para módulos de fuente de alimentación para proporcionar una fuente de alimentación redundante 1+1. En la siguiente tabla se describen los componentes del switch RG-NBS6002.

Los switches de la serie RG-NBS7000 son switches de última generación creados de manera independiente por Ruijie Networks. Existen dos modelos de este switch disponibles: el RG-NBS7003 y el RG-NBS7006. RG-NBS7003: Cualquier tarjeta de línea puede funcionar como motor supervisor en la ranura 1 (esta ranura debe estar ocupada). Cuenta con tres ranuras para tarjetas de línea. RG-NBS7006: cuenta con dos ranuras para motores supervisores y seis ranuras para tarjetas de línea.



1.2.1 Lista de productos

Modelo	10/100/1000 Puerto Ethernet Base-T	Puerto SFP 1000Base-X Puerto	Puerto SFP+ 10GE	Puerto para consola	Fuente de alimentación
RG-NBS3100-24GT4SFP	24	4	N/A	N/A	Individual
RG-NBS3100-24GT4SFP-P	24 (compatibilidad con PoE+)	4	N/A	N/A	Individual
RG-NBS3100-8GT2SFP	8	2	N/A	N/A	Adaptador de corriente
RG-NBS3100-8GT2SFP-P	8 (compatibilidad con PoE+)	2	N/A	N/A	Individual
RG-NBS3200-24GT4XS	24	N/A	4	N/A	Individual

RG-NBS3200-24SFP/8GT4XS	8 (combo)	24	4	N/A	Individual
RG-NBS3200-24GT4XS-P	24 (compatibilidad con PoE+)	N/A	4	N/A	Individual
RG-NBS3200-48GT4XS	48	N/A	4	N/A	Individual
RG-NBS3200-48GT4XS-P	48 (compatibilidad con PoE+)	N/A	4	N/A	Individual
RG-NBS5100-24GT4SFP	24	4	N/A	N/A	Individual
RG-NBS5100-48GT4SFP	48	4	N/A	N/A	Individual
RG-NBS5200-24GT4XS	24	N/A	4	N/A	Individual
RG-NBS5200-24SFP/8GT4XS	8 (combo)	24	4	N/A	Individual
RG-NBS5200-48GT4XS	48	N/A	4	N/A	Individual
RG-NBS3100-48GT4SFP-P	48	4	N/A	N/A	Única
RG-NBS5100-24GT4SFP-P	24	4	N/A	N/A	Única
RG-NBS5200-24GT4XS-P	24	N/A	4	N/A	Única
RG-NBS5200-48GT4XS-UP	48	N/A	4	N/A	Única
RG-NBS6002 Dos ranuras para módulos de servicio	N/A	N/A	N/A	N/A	2, admite alimentación redundante 1+1
M6000-24GT2XS	24	N/A	2	N/A	N/A
M6000-24SFP2XS	N/A	24	2	N/A	N/A
M6000-16GT8SFP2XS	16	8	2	N/A	N/A
M6000-16SFP8GT2XS	8	16	2	N/A	N/A

RG-NBS7003 Tres ranuras para tarjetas de línea Cualquier tarjeta de línea puede funcionar como motor supervisor en la ranura 1 (esta ranura debe estar ocupada).	N/A	N/A	N/A	No dispone de consola pero cuenta con un puerto de gestión	2, alimentación redundante 1+1
RG-NBS7006 Dos ranuras para motores supervisores y seis ranuras para tarjetas de línea **Motor supervisor** M7006-CM	N/A	N/A	N/A	N/A	4, admite alimentación redundante 1+1 y 2+2
M7006-CM El motor supervisor del switch RG-NBS7006	N/A	N/A	N/A	Puerto de gestión de 10/100 Mbps	N/A
M7000-16XS-EA	N/A	N/A	16	N/A	N/A
M7000-24GT24SFP2XS-EA	24	24	2	N/A	N/A
M7000-48GT2XS-EA	48	N/A	2	N/A	N/A
M7000-24GT2XS-EA	24	N/A	2	N/A	N/A
M7000-48SFP2XS-EA	N/A	48	2	N/A	N/A
M7000-24SFP2XS-EA	N/A	24	2	N/A	N/A
M7000-8XS-EA	N/A	N/A	8	N/A	N/A

Los puertos SFP no son compatibles con 100Base-FX y anteriores.

1000Base-T es compatible con 100Base-TX, 10Base-T y anteriores.

El puerto combo cuenta con un puerto SFP 1000Base-X y un puerto Ethernet 10/100/1000Base-T. Esto significa que solo uno de los puertos está disponible a la vez.

Tarjetas de línea para la serie 7K	Puerto Ethernet 10/100/1000 Base-T	Puerto SFP 1000 Base-X	Puerto SFP+ de 10 G
M7000-16XS-EA	-	-	16
M7000-24GT24SFP2XS-EA	24	24	2
M7000-48GT2XS-EA	48	-	2
M7000-48SFP2XS-EA	-	48	2
M7000-24SFP2XS-EA	-	24	2
M7000-8XS-EA	-	-	8

El modelo RG-NBS6002 es un switch de red de tipo caja intercambiable de 1U desarrollado de manera independiente por Ruijie Networks. Cuenta con dos ranuras para tarjetas de línea para cuatro tipos de tarjetas de línea y dos ranuras para módulos de fuente de alimentación para proporcionar una fuente de alimentación redundante 1+1. En la siguiente tabla se describen los componentes del switch RG-NBS6002.

Los switches de la serie RG-NBS7000 son switches de última generación creados de manera independiente por Ruijie Networks. Existen dos modelos de este switch disponibles: el RG-NBS7003 y el RG-NBS7006. RG-NBS7003: Cualquier tarjeta de línea puede funcionar como motor supervisor en la ranura 1 (esta ranura debe estar ocupada). Cuenta con tres ranuras para tarjetas de línea. RG-NBS7006: cuenta con dos ranuras para motores supervisores y seis ranuras para tarjetas de línea.

1.2.2 Indicador LED

LED	Estado	Significado
LED de estado del sistema	Sin luz	El conmutador no está recibiendo energía.
	Verde parpadeante (0.5 Hz)	El conmutador está funcionando, pero se está generando una alarma de insuficiencia de energía PoE.
	Verde parpadeante (10 Hz)	El conmutador se está actualizando o inicializando.
	Verde fijo	El conmutador está conectado a Ruijie Cloud.
Indicador LED de estado del puerto Ethernet 10/100/1000Base-T	Sin luz	El puerto no está conectado.
	Verde fijo	El puerto está conectado a una velocidad de 10/100/1000 Mbps.
	Verde parpadeante	El puerto está recibiendo o transmitiendo datos a una velocidad de 10/100/1000 Mbps.

Indicador LED de estado de PoE del puerto RJ45	Sin luz	PoE no está habilitado.
	Verde fijo	PoE está habilitado. El puerto está operando.
	Verde parpadeante	El puerto tiene una falla por sobrecarga de PoE.
Indicador LED de estado del puerto SFP	Sin luz	El puerto no está conectado.
	Verde fijo	El puerto está conectado.
	Verde parpadeante	El puerto está recibiendo o transmitiendo datos.
Indicador LED de estado del puerto SFP+	Sin luz	El puerto no está conectado.
	Verde fijo	El puerto está conectado.
	Verde parpadeante	El puerto está recibiendo o transmitiendo datos.

1.2.3 Botón

Botón	Descripción
Botón de cambio de modo PoE	Presione el botón de cambio de modo PoE por más de 3 segundos para cambiar del modo de PoE al modo de velocidad del puerto.
Botón de restablecimiento	El conmutador se reinicia al presionar el botón de restablecimiento por menos de 2 segundos. El conmutador restablece la configuración predeterminada de fábrica al presionar el botón de restablecimiento por más de 5 segundos (hasta que el LED de estado parpadee).

1.3 Switch de la serie Reyee NIS

1.3.1 Lista de productos

Modelo	Puerto Ethernet 10/100/1000 BASE-T con negociación automática	Puerto SFP 1000 BASE-X	Puerto para consola	Puerto SFP+ de 10 GE	Fuente de alimentación
RG-NIS3100-8GT4SFP-HP	8	4	N/A	N/A	Redundancia 1+1
RG-NIS3100-8GT2SFP-HP	8	2	N/A	N/A	Redundancia 1+1
RG-NIS3100-4GT2SFP-HP	4	2	N/A	N/A	Redundancia 1+1

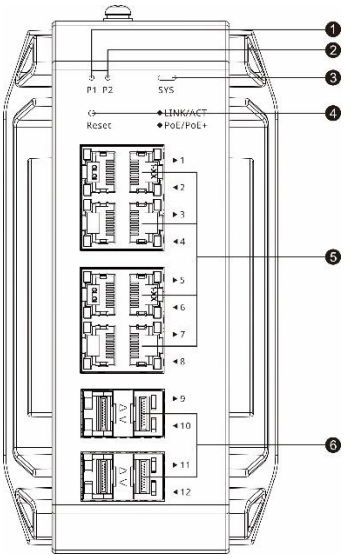
Nota

Los puertos 1000 BASE-T son retrocompatibles con los puertos 100 BASE-T y 10 BASE-T.

1.3.2 Indicador LED

1. Panel frontal

Figura 1-1 Panel frontal del RG-NIS3100-8GT4SFP-HP



1. Indicador LED de estado de la alimentación P1
2. Indicador LED de estado de la alimentación P2
3. Indicador LED de estado del sistema
4. Botón de restablecimiento
5. Puertos Ethernet 10/100/1000 BASE-T con negociación automática
6. Puertos SFP GE

Botón de restablecimiento: mantenga pulsado el botón durante menos de 2 segundos para reiniciar el dispositivo. Mantenga pulsado el botón durante más de 5 segundos hasta que el indicador LED de estado del sistema comience a parpadear para restaurar la configuración de fábrica y reiniciar el sistema.

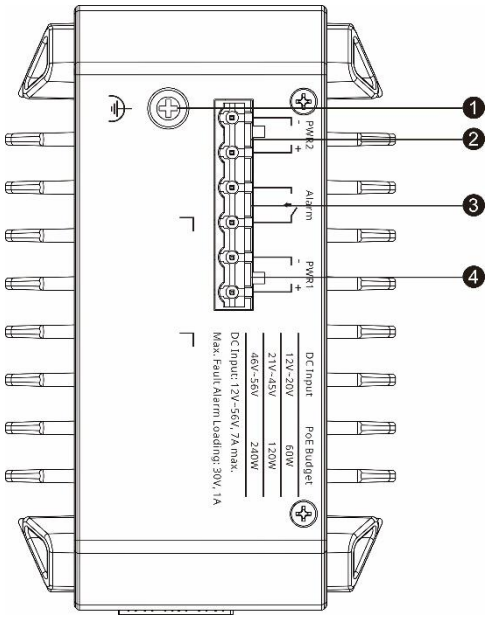
2. Indicadores LED

Indicador LED	Etiqueta serigrafiada	Estado	Descripción
Indicador LED de estado del sistema	SYS	Apagado	El switch no está encendido.
		Parpadeo rápido en verde (8-10 Hz)	El switch se está iniciando.
		Verde fijo	El switch funciona correctamente.
		Parpadeo lento en verde (0,5 Hz)	El switch no está conectado a la nube.

		Parpadeo en verde (2 Hz)	El switch se está restaurando a la configuración de fábrica y se apagará o se está actualizando.
		Parpadeo en verde en distintos momentos (ciclo: 1 s encendido y 1 s apagado, 0,25 s encendido y 0,25 s apagado, 0,25 s encendido y 0,25 s apagado, 0,25 s encendido y 1,75 s apagado)	El programa principal se ha perdido o dañado, o determinadas funciones presentan un comportamiento anómalo.
Indicadores LED de los puertos eléctricos y los puertos ópticos	LINK/ACT	Apagado	El puerto no está funcionando.
		Verde fijo	El puerto está funcionando.
		Parpadeo en verde	El puerto está funcionando y está recibiendo o enviado datos.
	PoE/PoE+	Apagado	La fuente de alimentación PoE se encuentra apagada.
		Amarillo fijo	La fuente de alimentación PoE se encuentra encendida.
Indicadores LED de estado de la alimentación	P1	Apagado	La fuente de alimentación PWR1 se encuentra apagada.
		Encendido fijo	La fuente de alimentación PWR1 se encuentra encendida.
	P2	Apagado	La fuente de alimentación PWR2 se encuentra apagada.
		Encendido fijo	La fuente de alimentación PWR2 se encuentra encendida.

3. Panel superior

Figura 1-2 Panel superior del NIS3100-8GT4SFP-HP



1. Perno de conexión a tierra 3. Puerto de alarma	2. Conector de alimentación de CC de la fuente de alimentación PWR2 4. Conector de alimentación de CC de la fuente de alimentación PWR1

4. Panel trasero

El switch admite dos modos de instalación: el montaje en carril DIN y el montaje en pared.

Figura 1-3 Panel trasero para el montaje en carril DIN

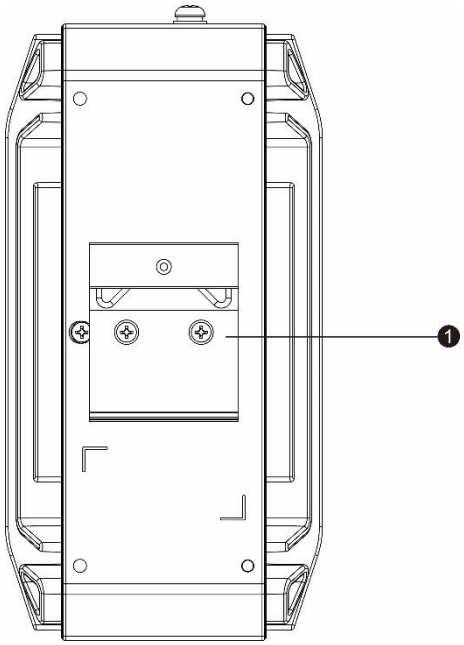
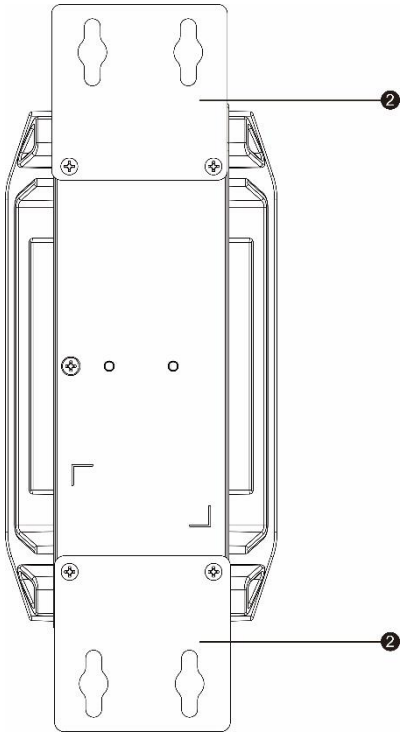


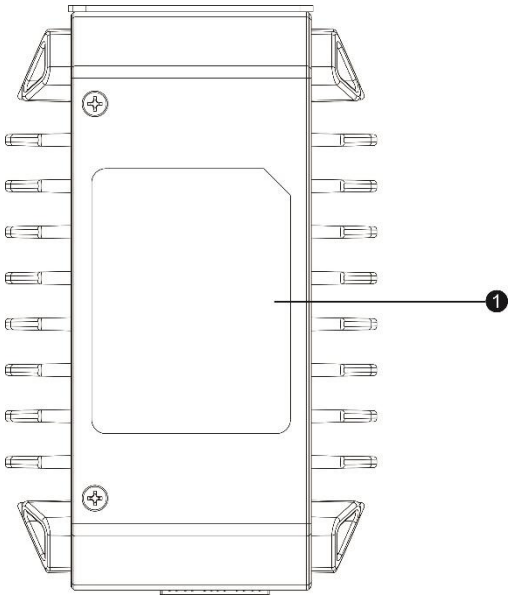
Figura 1-4 Panel trasero para el montaje en pared



1. Abrazadera para carril DIN	2. Orificios de montaje

1.3.3 Panel inferior

Figura 1-5 Panel inferior del NIS3100-8GT4SFP-HP



1. Placa de identificación

1.3.4 Refrigeración

El RG-NIS3100-8GT4SFP-HP cuenta con un sistema de refrigeración natural para garantizar su correcto funcionamiento en determinados entornos. Para garantizar su correcta ventilación, deje un espacio libre mínimo de 100 mm alrededor del dispositivo.

2 Administración de los dispositivos

2.1 Inicio de sesión

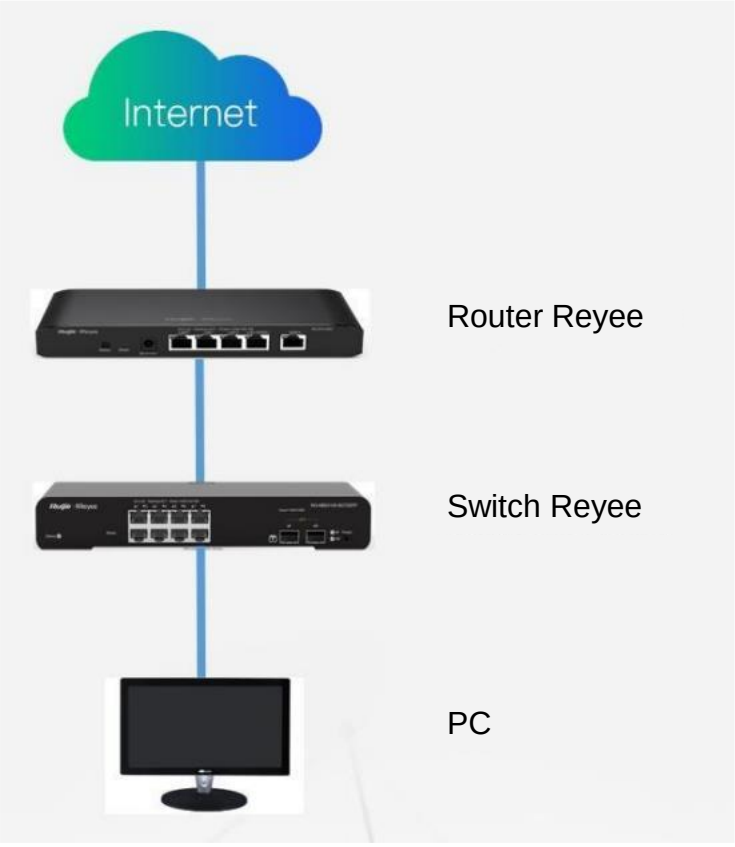
La Eweb es un sistema de gestión de red basado en la web que se utiliza para administrar o configurar dispositivos. Se puede acceder a la Eweb mediante un navegador como Google Chrome. Para gestionar dispositivos mediante la web, es necesario contar con un servidor web y un cliente web. El servidor web, integrado en un dispositivo, se utiliza para recibir y procesar solicitudes del cliente, así como para devolver los resultados del procesamiento al cliente web. El cliente web generalmente se refiere a un navegador, como Google Chrome, IE o Firefox.

Los conmutadores gestionados de Reyee pueden gestionarse a través de la interfaz web y de forma remota, por medio de la aplicación o la plataforma Ruijie Cloud, con acceso gratuito ilimitado. Se puede visualizar el estado de la red, modificar la configuración y resolver fallas fácilmente.

2.1.1 Ejemplo de configuración

Topología de la red

En la siguiente imagen, se muestra cómo acceder al sistema de gestión Eweb de un conmutador de acceso o agregación a través del navegador de la PC para administrar o configurar el dispositivo.

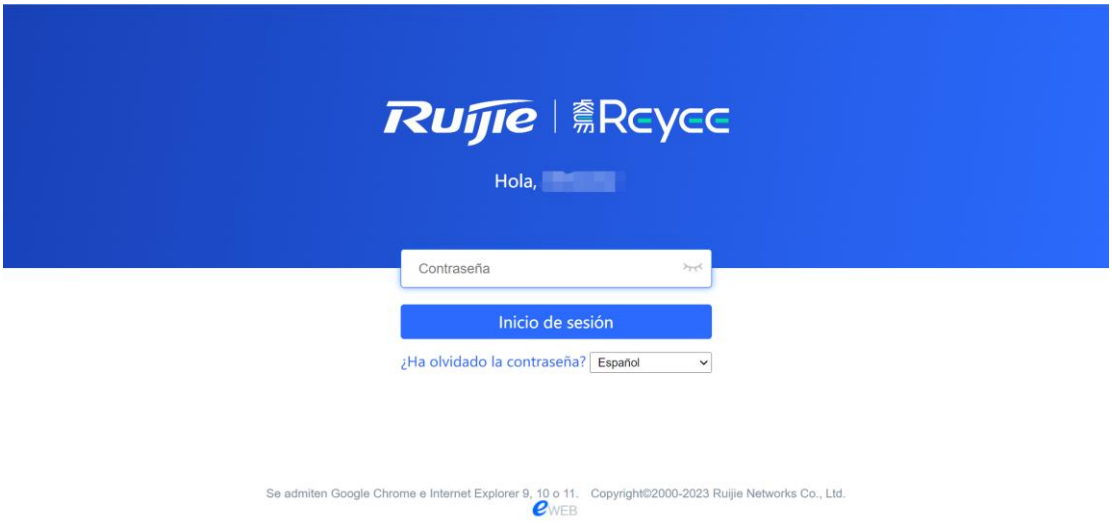


Configure automáticamente la asignación de la dirección IP en la PC.

Visite http://192.168.110.1 a través de Google Chrome.

Ingrese la contraseña en la página de acceso y haga clic en **Inicio de sesión**.

La contraseña predeterminada es **admin**.



Para los dispositivos Reyee EG, utilice 192.168.110.1 o 10.44.77.254 para acceder al dispositivo.

Para los conmutadores Reyee, utilice 10.44.77.200 para acceder al dispositivo.

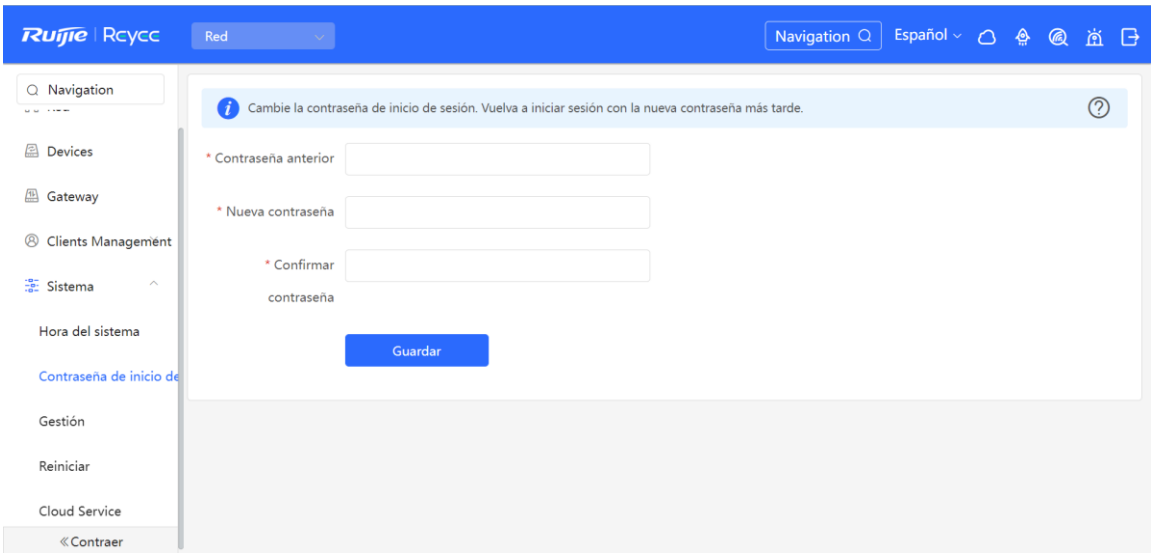
Para los AP Reyee, utilice 192.168.120.1 o 10.44.77.254 para acceder al dispositivo.

Para la serie de puentes inalámbricos EST, utilice 10.44.77.254 para acceder al dispositivo.

La contraseña de acceso predeterminada para todos los dispositivos Reyee es **admin**.

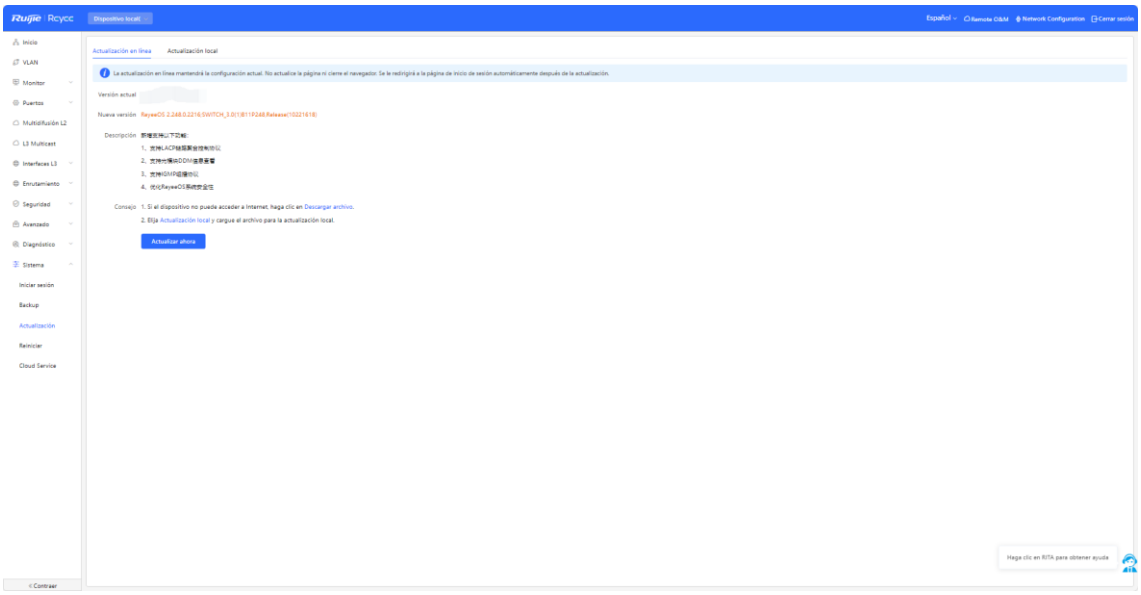
Visite https://10.44.77.253 para ingresar al dispositivo maestro de la red Reyee.

2.2 Configuración de la contraseña



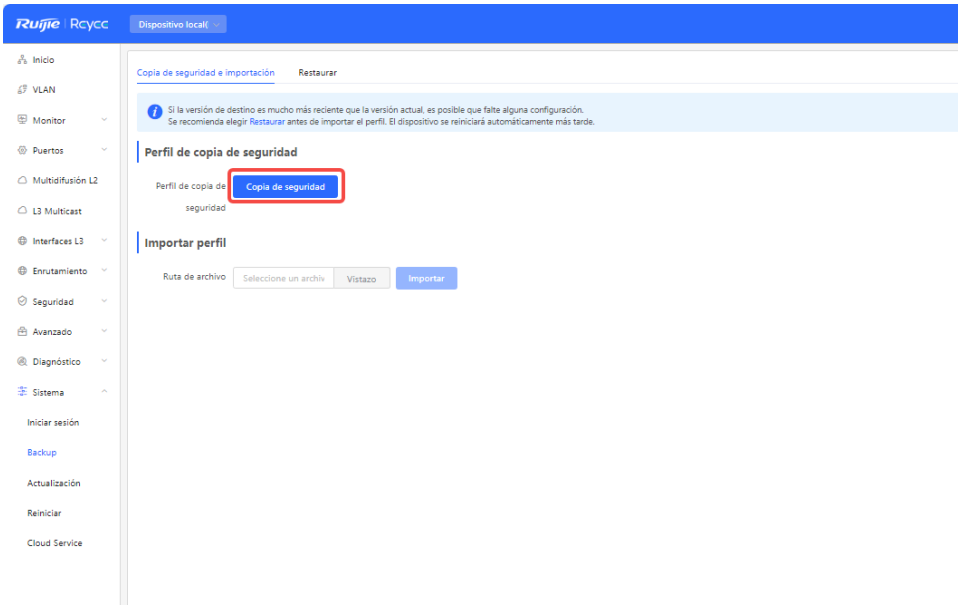
2.3 Actualización del dispositivo

Inicie sesión en el sistema eWeb del dispositivo y seleccione **Dispositivo local > Sistema > Actualización**.

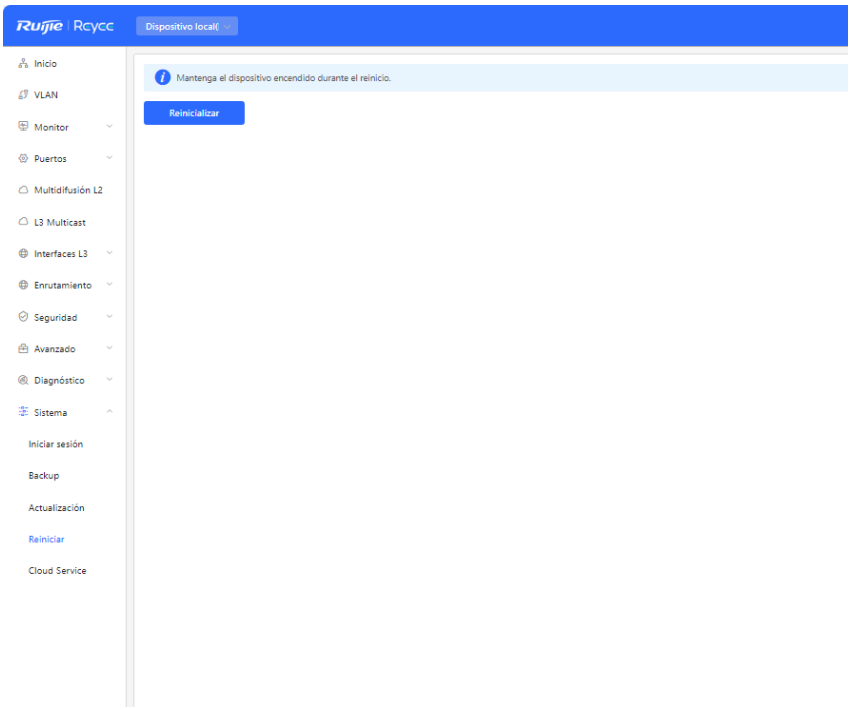


2.4 Respaldo o restablecimiento de la configuración

Inicie sesión en el sistema eWeb del dispositivo y seleccione **Dispositivo local > Sistema > Backup**.

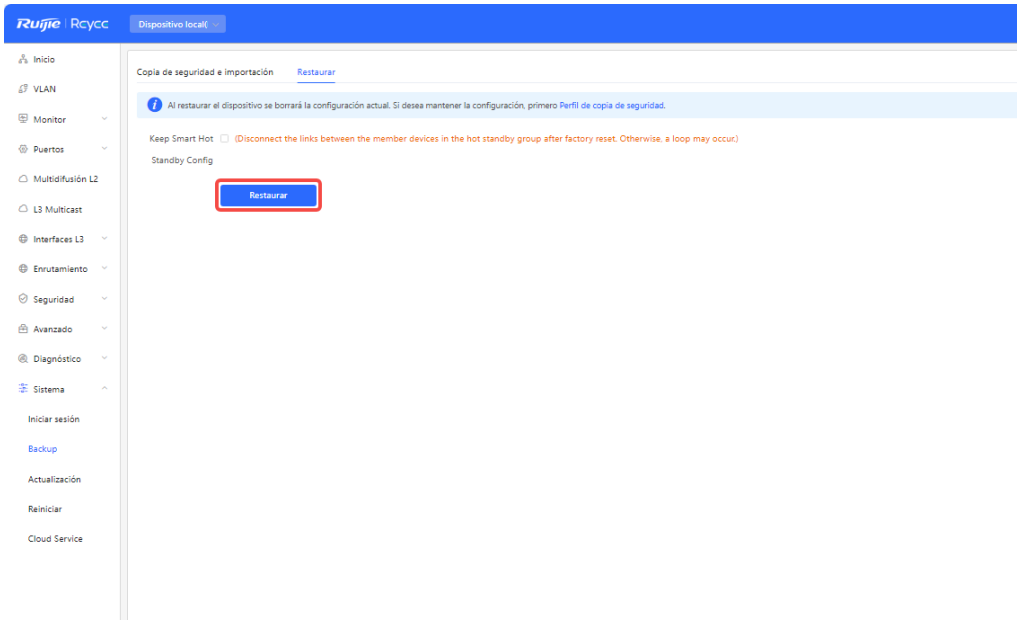


Inicie sesión en el sistema eWeb del dispositivo y haga clic en **Dispositivo local > Sistema > Reiniciar**. A continuación, puede reiniciar sus dispositivos.



2.5 Restablecimiento de la configuración predeterminada

Acceda a la Eweb para restablecer todos los dispositivos conectados a la red.



3 Primeros pasos

3.1 Preparación para la instalación

3.1.1 Recomendaciones de seguridad

Para evitar cualquier daño personal o al equipo, preste atención a estas recomendaciones de seguridad antes de instalar cada dispositivo. Las siguientes recomendaciones de seguridad no cubren todos los peligros posibles.

1. Instalación

- Mantenga la carcasa limpia y libre de cualquier tipo de polvo.
- No deje dispositivos en zonas de paso.
- No utilice ropa holgada ni accesorios que puedan engancharse o enredarse en algún dispositivo durante la instalación y mantenimiento.

2. Traslado

- No mueva los dispositivos frecuentemente.
- Si mueve los dispositivos, mantenga el equilibrio y evite daños en las piernas, los pies y la espalda.

Antes de mover los dispositivos, apague todas las fuentes de alimentación y desmantele los módulos de alimentación.

3. Electricidad

- Respete las regulaciones y especificaciones locales cuando realice actividades con el sistema eléctrico. Los operadores deben estar debidamente calificados.
- Antes de instalar el dispositivo, revise cuidadosamente cualquier peligro potencial alrededor, como la conexión a tierra de la fuente de alimentación o la humedad en el suelo o piso.
- Antes de instalar el dispositivo, localice el interruptor de emergencia de la fuente de alimentación de la habitación. En caso de accidente, primero desconecte la fuente de alimentación.
- En lo posible, evite mantener solo el conmutador encendido.
- Asegúrese de realizar todas las comprobaciones pertinentes antes de desconectar la fuente de alimentación.

No coloque el equipo en un lugar húmedo. No permita que ningún líquido entre en la carcasa.

4. Prevención de daños por descarga de electricidad estática

Para prevenir el daño por electricidad estática, preste atención a los siguientes puntos:

- Coloque adecuadamente a tierra los tornillos de conexión a tierra en el panel trasero del dispositivo; utilice una toma de corriente monofásica de tres hilos y un cable de tierra para protección eléctrica (PE) como toma de corriente de AC.
- Evite que entre el polvo.

Asegúrese de contar con las condiciones de humedad adecuadas.

5. Láser

Algunos dispositivos admiten diferentes modelos de módulos ópticos que son productos láser Clase I de venta en el mercado. El uso incorrecto de los módulos ópticos puede ocasionar daños. Por lo tanto, preste atención a los siguientes puntos cuando los utilice:

- Cuando un transceptor de fibra se encuentre funcionando, asegúrese de que el puerto se haya conectado a una fibra óptica o tenga una cubierta antipolvo, para evitar que ingrese el polvo y el riesgo de quemaduras.

Cuando el módulo óptico esté funcionando, no jale el cable de fibra o vea directamente dentro del transceptor. El transceptor emite una luz láser que puede dañar sus ojos.

3.1.2 Requisitos del sitio de instalación

El sitio de instalación debe cumplir con los siguientes requisitos, para garantizar el funcionamiento normal y una vida útil y prolongada de los conmutadores Reyee.

1. Ventilación

Para instalar el dispositivo, deje al menos 10 cm de distancia a ambos lados y en la parte trasera del plano del gabinete, a la altura de las ranuras de ventilación, para garantizar una buena ventilación. Después de conectar los cables, agrúpelos o colóquelos en el rack para evitar que bloqueen las entradas de aire. Se recomienda limpiar el dispositivo regularmente. En especial, evite que el polvo tape la pantalla de malla situada en la parte trasera del gabinete.

2. Temperatura y humedad

Para garantizar el buen funcionamiento y prolongar la vida útil del router, mantenga las condiciones de temperatura y humedad adecuadas en la sala de equipos.

Si la temperatura y humedad en la sala de equipos no cumple con los requisitos por un plazo prolongado, el router podría dañarse.

Los entornos con una humedad elevada pueden provocar que el material aislante presente un mal aislamiento o incluso que se produzca una fuga de corriente eléctrica. En ocasiones, los materiales pueden sufrir cambios en su desempeño mecánico y las piezas metálicas pueden oxidarse.

En un entorno con baja humedad, las cintas aislantes pueden secarse y encogerse. La electricidad estática puede producirse fácilmente y poner en peligro los circuitos en el dispositivo.

En un entorno de alta temperatura, el router puede sufrir un daño más serio. Puede reducir su desempeño de manera significativa y pueden ocurrir diversas fallas en el hardware.

3. Limpieza

El polvo es una amenaza severa para el funcionamiento del router. El polvo de interiores que cae sobre el equipo puede entrar a través de la electricidad estática, lo que ocasiona un mal contacto de la junta metálica. Esta adherencia electrostática puede producirse con mayor facilidad cuando la humedad relativa es baja. Esto afecta el ciclo de vida de la AP y provoca fallas de comunicación.

4. Conexión a tierra

Un buen sistema de puesta a tierra es la base para la estabilidad y seguridad del funcionamiento del dispositivo, ya que evitará que sea golpeado por rayos y generará resistencia a las interferencias. Revise

con atención las condiciones de la conexión a tierra en el sitio de instalación, según las especificaciones, y lleve a cabo el procedimiento como corresponda.

- Conexión a tierra contra rayos

  El sistema de protección contra rayos de una instalación es un sistema independiente que consiste en un pararrayos y un conector al sistema de puesta a tierra que, por lo general, comparte la referencia de potencia y el cable de tierra. La conexión a tierra contra descargas de rayos se instala en la ubicación.

- Conexión a tierra de compatibilidad electromagnética (EMC)

  La conexión a tierra que se requiere para el diseño EMC incluye un cable de tierra blindado, un filtro de toma a tierra, supresores de ruido e interferencia y una referencia de nivel. Todo lo anterior constituye los requisitos necesarios para la conexión a tierra. La resistencia de los cables de tierra debe ser menor a 1 Ω.

5. Interferencia electromagnética o EMI

La interferencia electromagnética (EMI), tanto del exterior, como del interior del dispositivo o del sistema de aplicación, afecta el sistema en lo relativo a la conductividad, como el acoplamiento capacitivo, el acoplamiento inductivo y la radiación electromagnética.

Existen dos tipos de interferencia: la interferencia radiada y la interferencia conducida, en función del tipo de ruta de transmisión.

Cuando la energía, generalmente de radiofrecuencia, de un componente llega a un componente sensible a través del espacio, la energía se conoce como interferencia radiada. La fuente de interferencia puede ser parte del sistema interferido o de una unidad aislada eléctricamente. La interferencia conducida es el resultado de la conexión de un cable electromagnético o de señal entre la fuente y el componente sensible, cuyo cable conduce la interferencia de una unidad a otra. La interferencia conducida generalmente afecta la fuente de alimentación del dispositivo, pero puede controlarse a través de un filtro. Las interferencias radiadas pueden afectar a cualquier trayectoria de la señal del dispositivo, por lo que son difíciles de evitar.

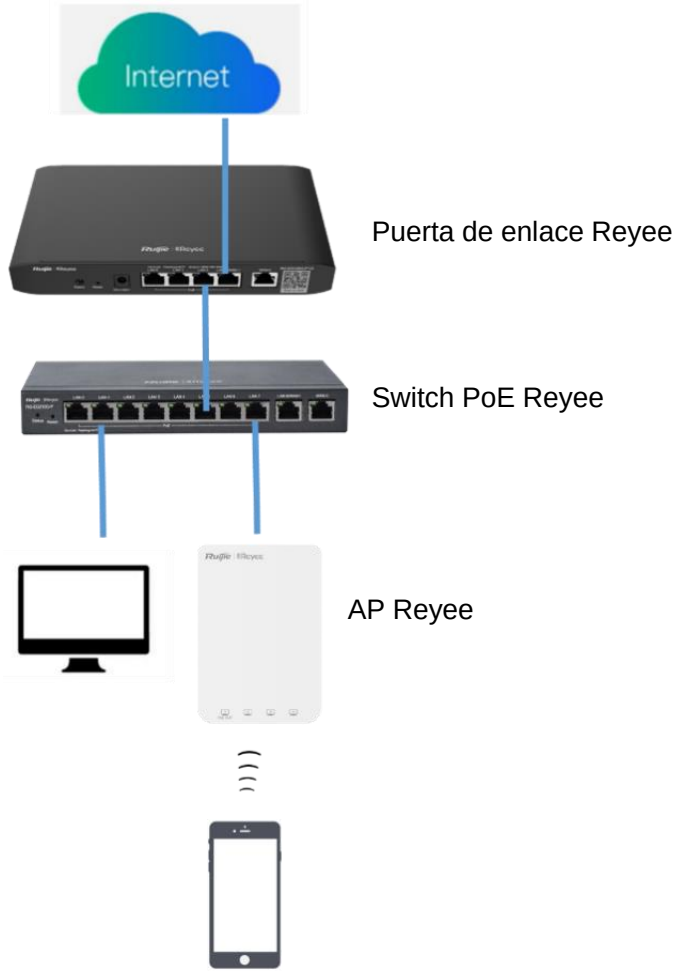
- Para el sistema de fuente de alimentación de TN AC, debe usarse la toma de corriente monofásica de tres núcleos con conductores a tierra protectores (PE) para filtrar de manera eficaz las interferencias de la red eléctrica mediante los circuitos de filtrado.
- No utilice el dispositivo de conexión a tierra para un dispositivo eléctrico o un dispositivo de conexión a tierra contra rayos. Además, el dispositivo de conexión a tierra del aparato debe instalarse lejos del dispositivo de conexión a tierra del aparato eléctrico y del dispositivo de conexión a tierra contra rayos.
- Mantenga el dispositivo lejos del transmisor de radio de alta potencia, la estación transmisora de radar y el dispositivo de alta frecuencia y corriente.
- Tome las medidas necesarias de protección contra la electricidad estática.

Coloque los cables de la interfaz en la sala de equipos. Se prohíbe la instalación de cables en exteriores con el fin de evitar daños en las interfaces de señal de los dispositivos causados por la sobretensión o la sobrecorriente por rayos.

3.1.3 Planificación de la red

El servidor DHCP cuenta con dos grupos de direcciones en la puerta de enlace de salida:

- 192.168.110.0/24 en VLAN 1 para dispositivos de esta red
- 192.168.10.0/24 en VLAN 10 para los clientes de esta red



Los siguientes puertos se utilizan para gestionar la plataforma Ruijie Cloud. Para conectar los dispositivos en Ruijie Cloud, asegúrese de que estos puertos se encuentren disponibles y que la red permita el flujo de datos.

Domain name (Cloud-as)	DST.IP	Domain name (Cloud-eu，Cloud-me)	DST.IP	DST.TCP	DST.UDP
Device Online Related:		Device Online Related:			
devicereg.ruijienetworks.com	35.197.150.240	devicereg.ruijienetworks.com	35.190.10.141	80,443	
ryrc.ruijienetworks.com	35.197.150.240	ryrc.ruijienetworks.com	35.234.108.108	80,443	
stunrc.ruijienetworks.com	35.197.150.240	stunrc.ruijienetworks.com	35.234.108.108		34,783,479
stunsvr-as.ruijienetworks.com	34.126.80.150	stunsvr-eu.ruijienetworks.com	35.246.237.78		34,783,479
stunb-as.ruijienetworks.com	34.126.80.150	cwmpsvr-eu.ruijienetworks.com	34.159.112.239		34,783,479
stunc-as.ruijienetworks.com	34.87.169.209	cwmpcp-eu.ruijienetworks.com	34.120.73.71		34,783,479
cwmpsvr-as.ruijienetworks.com	35.197.136.171	cwmpb-eu.ruijienetworks.com	34.159.112.239	80, 443	
cwmpcp-as.ruijienetworks.com	34.160.143.162				
cwmpb-as.ruijienetworks.com	35.197.136.171				
Log Upload:		Log Upload:			
34.87.93.12	34.87.93.12	cloudlog-eu.ruijienetworks.com	35.246.247.49	80,443	
Advanced Service:		Advanced Service:			
firmware.ruijienetworks.com	34.87.32.36	firmware.ruijienetworks.com	34.89.153.55	80,443	
cloudweb.ruijienetworks.com	34.87.32.36	cloudweb.ruijienetworks.com	34.89.153.55	80,443	
fastonline.ruijienetworks.com	34.87.32.36	fastonline.ruijienetworks.com	34.89.153.55	80,443	
cloudapi.ruijienetworks.com	35.197.150.240	cloudapi.ruijienetworks.com	35.234.108.108	80,443	
cdn.ruijienetworks.com	35.201.94.110	cdn.ruijienetworks.com	35.190.93.193	80,443	
ES Series Switch		ES Series Switch			
iotrc.ruijienetworks.com	34.87.101.31	iotrc.ruijienetworks.com	34.107.106.56		7683
iotsvr-as.ruijienetworks.com	35.247.161.22	iotsvr-eu.ruijienetworks.com	35.242.228.40		5683
iotlog-as.ruijienetworks.com	35.240.167.168	iotlog-eu.ruijienetworks.com	35.198.144.180		6683
iotdl-as.ruijienetworks.com	34.87.141.45	iotdl-eu.ruijienetworks.com	35.234.118.145		8683
MQTT Devices with P206 version		MQTT Devices with P206 version			
ryrcmq.ruijienetworks.com	34.120.84.165	ryrcmq.ruijienetworks.com	34.149.186.87	25857	
ehrrcmq.ruijienetworks.com	34.120.84.165	ehrrcmq.ruijienetworks.com	34.149.186.87	25857	
mqclt001-as.rj.link	34.160.191.165	mqclt001-eu.rj.link	34.120.138.185	25857	

3.2 Instalación rápida

3.2.1 Instalación rápida a través de Ruijie Cloud APP

La siguiente topología de red incluye la puerta de enlace Reyee, el switch PoE Reyee y el punto de acceso remoto (RAP) Reyee.

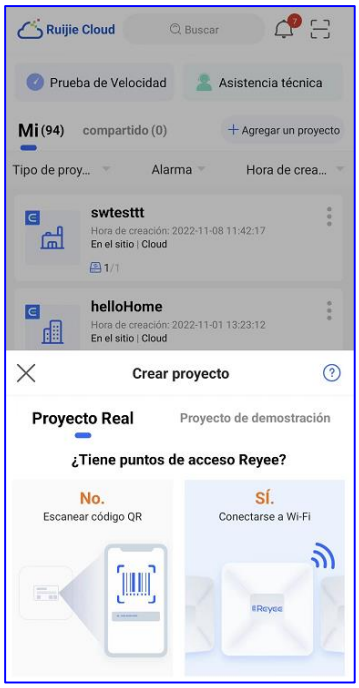
Puerta de enlace Reyee

Switch PoE Reyee

AP Reyee

1. Crear un proyecto.

Abra Ruijie Cloud App, haga clic en **Crear Proyecto** y seleccione **Conectarse a Wi-Fi**.

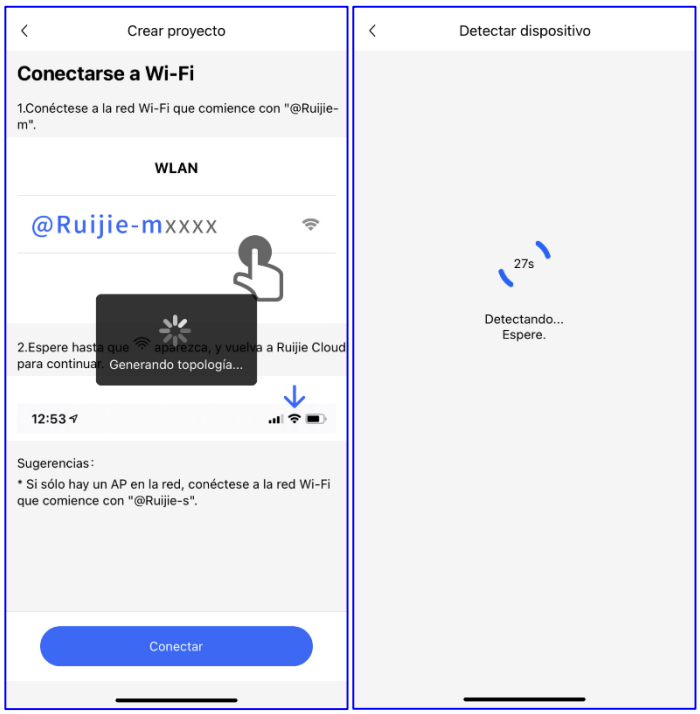


Después de dar clic en **Sí**, Ruijie Cloud App le pedirá conectarse al SSID **@Ruijie-mxxxx**.

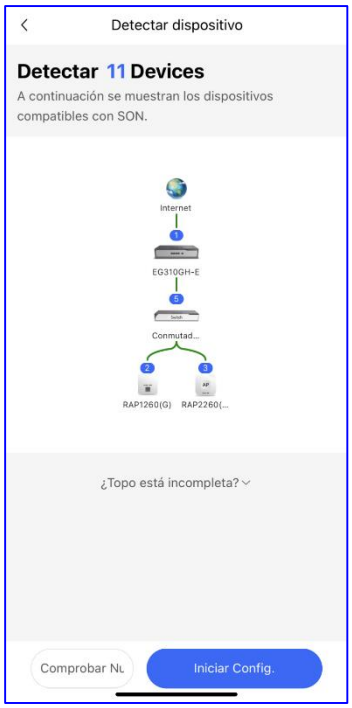
Confirme que **@Ruijie-m*xxxx*** se haya generado después de que la autoorganización de la red se haya completado exitosamente, y que **@Ruijie-s*xxxx*** se haya generado en un dispositivo independiente. ***xxxx*** deben ser los últimos cuatro dígitos de la dirección MAC de un dispositivo.

Conéctese al SSID **@Ruijie-mxxxx** en su teléfono celular.

Después de conectarse al SSID **@Ruijie-mxxxx**, Cloud App generará la topología para detectar todos los dispositivos en la red SON.

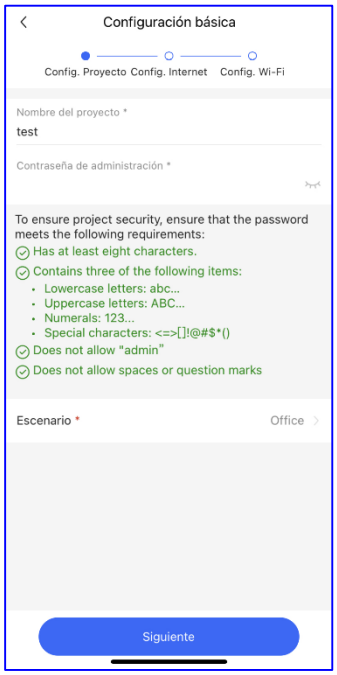


Después de que haya detectado los dispositivos, Cloud App mostrará los dispositivos y la topología. Haga clic en **Iniciar Config.** para establecer la configuración básica de este proyecto.

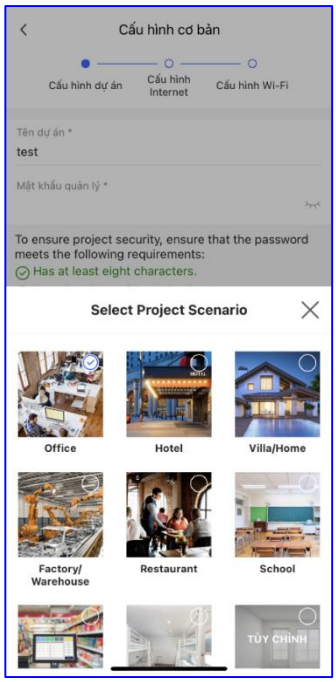


2. Configurar el proyecto.

Ingrese el **Nombre del Proyecto** y la **Contraseña de administración**.

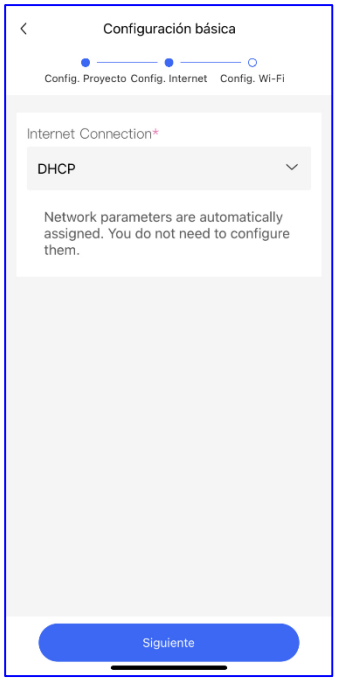


Después, seleccione el escenario del proyecto, según lo requiera.



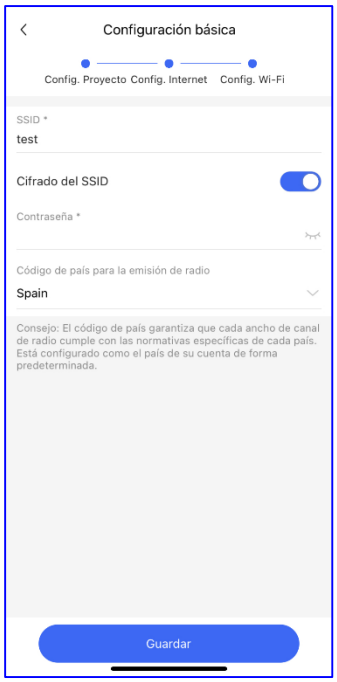
3. Configurar el Internet.

Para la configuración de WAN, seleccione **PPPoE**, **DHCP** o **IP estática**.

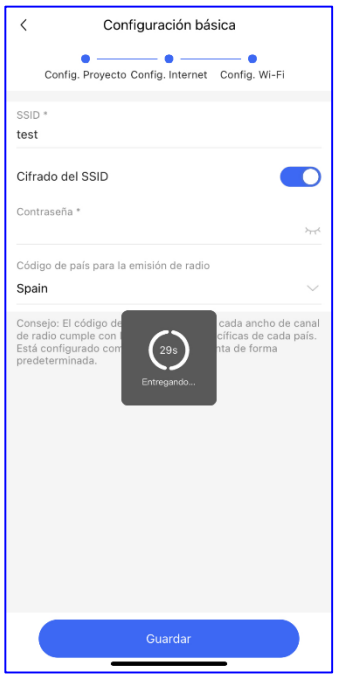


4. Configurar el SSID.

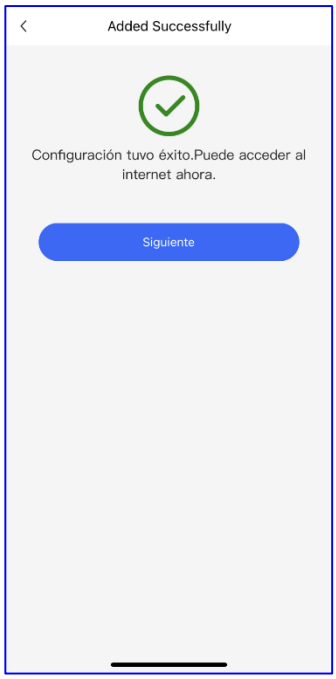
Para configurar el SSID, ingrese el nombre del SSID y habilite la opción Abrir para configurar sin código de seguridad o establezca una contraseña para este SSID. Seleccione el código del país.



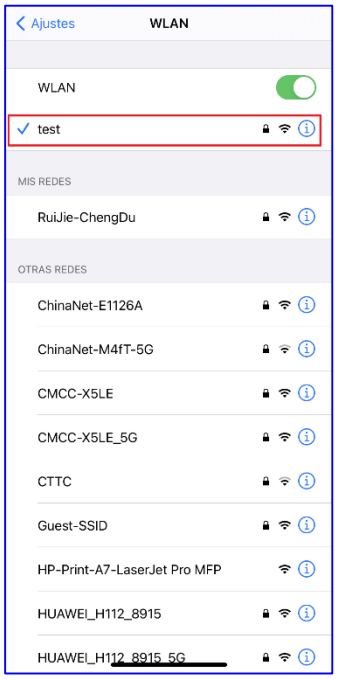
La configuración se sincronizará con la red.



Después de 3 segundos, Ruijie Cloud App indicará que la configuración se completó exitosamente.

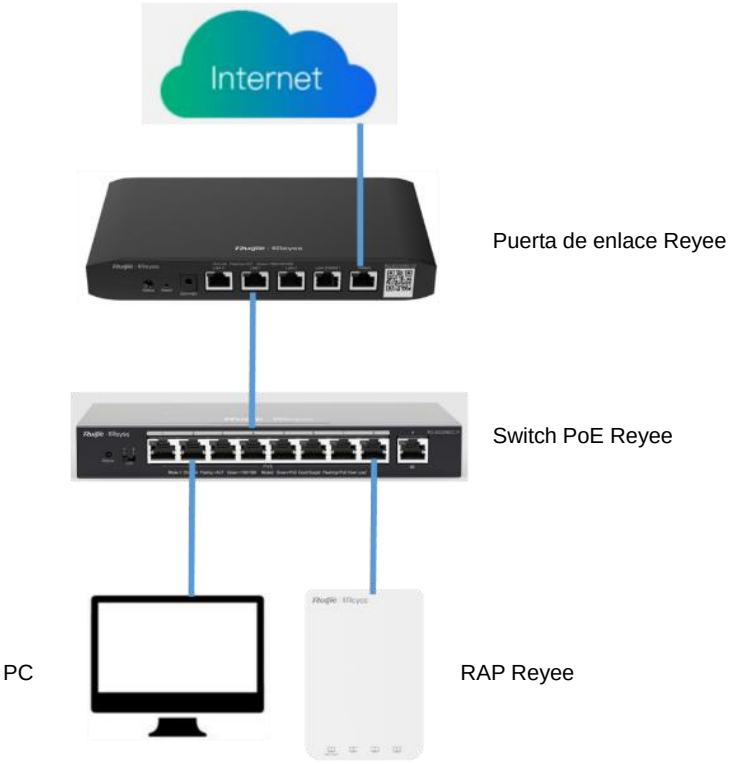


Ahora ya puede conectarse al SSID creado para administrar toda la red en Cloud App.

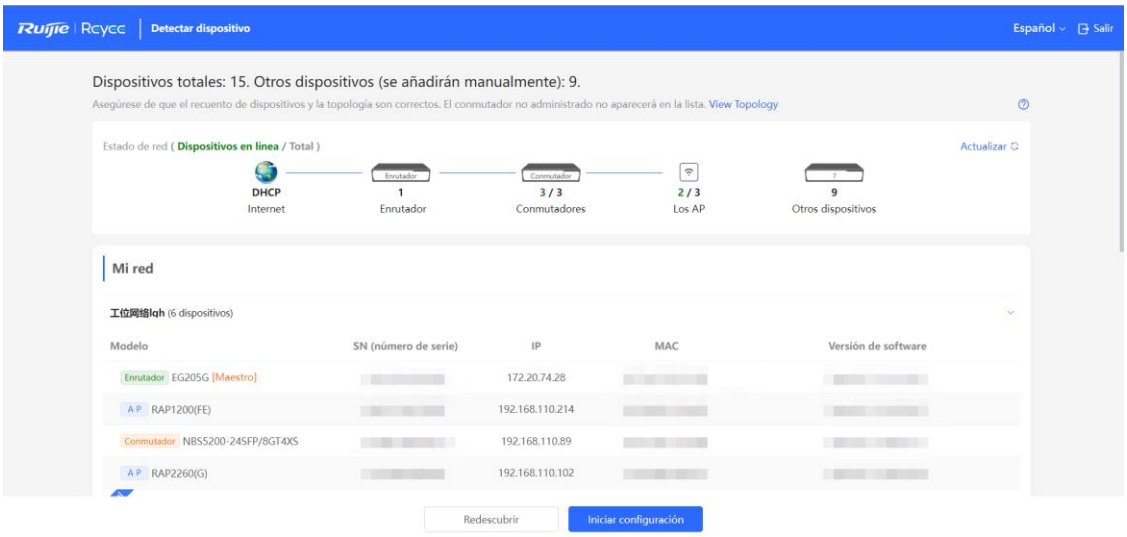


3.2.2 Instalación rápida a través de la Eweb Reyee

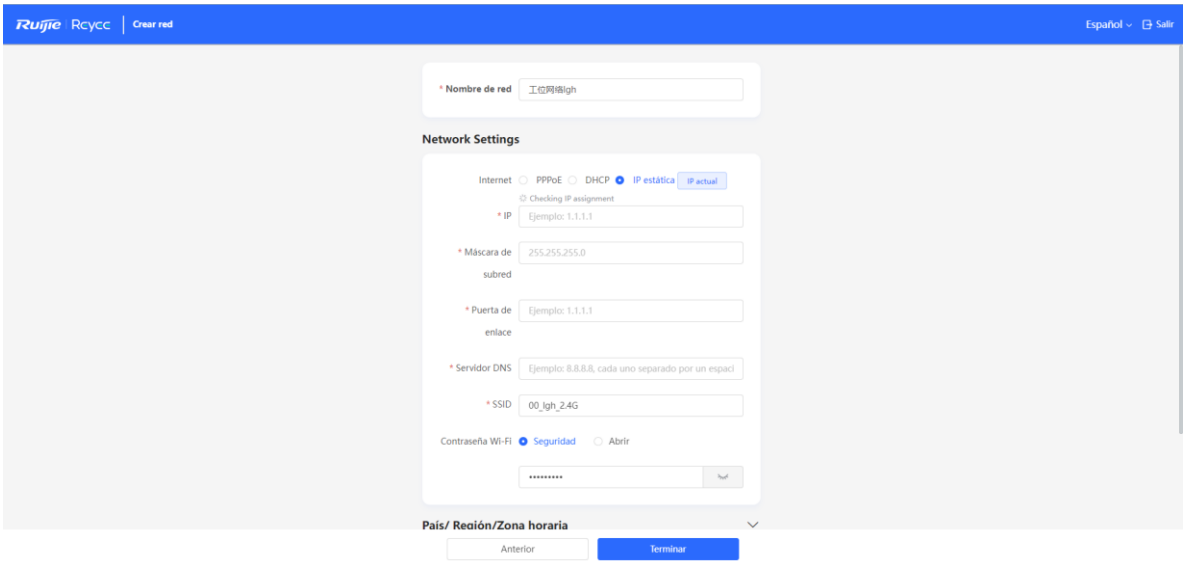
La siguiente topología de red incluye la puerta de enlace Reyee, el switch PoE Reyee y el punto de acceso remoto (RAP) Reyee.

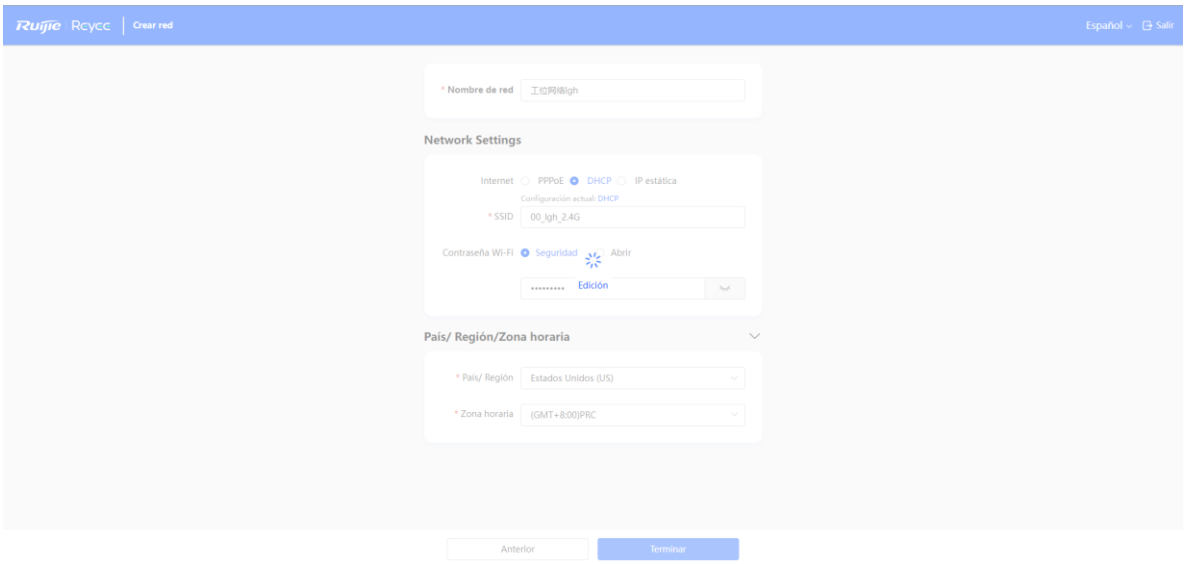


Conecte la PC a un switch PoE y configure la dirección IP estática 192.168.110.x; luego, ingrese 192.168.110.1 en la barra de dirección del navegador para iniciar sesión en la Eweb de EG. Todos los dispositivos de la red se mostrarán en la Eweb. Haga clic en **Iniciar configuración** para un inicio rápido de la red.

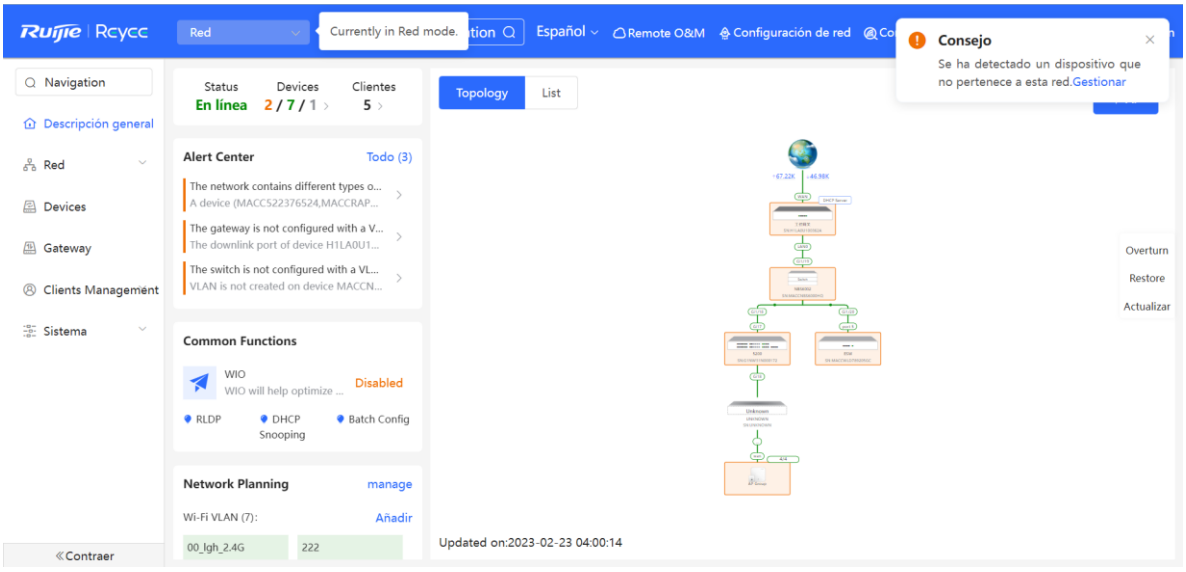


Para realizar la configuración rápida de esta red, ingrese el nombre de red, configure el modo de acceso a Internet de la red e ingrese la contraseña del SSID, o habilite la opción Abrir para no crear una contraseña. Después, seleccione el código de país o región y haga clic en **Crear red y Terminar**. La configuración se aplicará y se activará.





Cuando la configuración se aplique y se active, podrá acceder a la sección **Descripción general** para administrar la SON de los dispositivos Reyee.



4 Configuración de los switches de la serie Reyee ES

4.1 Información del puerto de gestión

4.1.1 Barra de estado del puerto

La barra de estado del puerto se encuentra en la parte superior de la página web y muestra el identificador o ID del puerto, su atributo (ascendente/descendente) y el estado de la conexión. Haga clic en **Collapse** para ocultar la barra de estado del puerto.

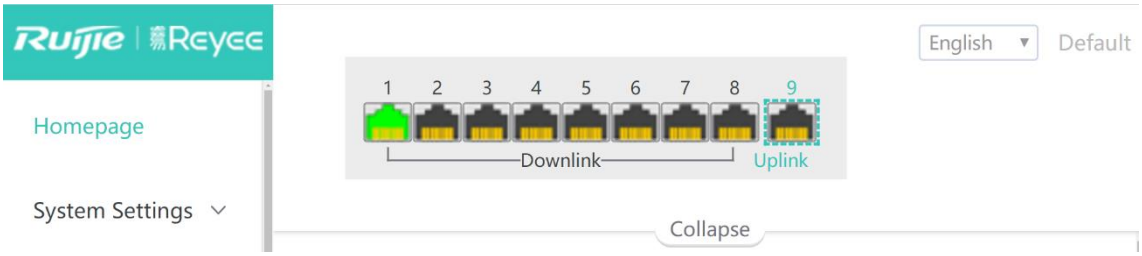
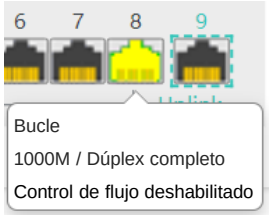
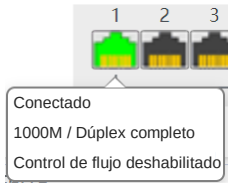
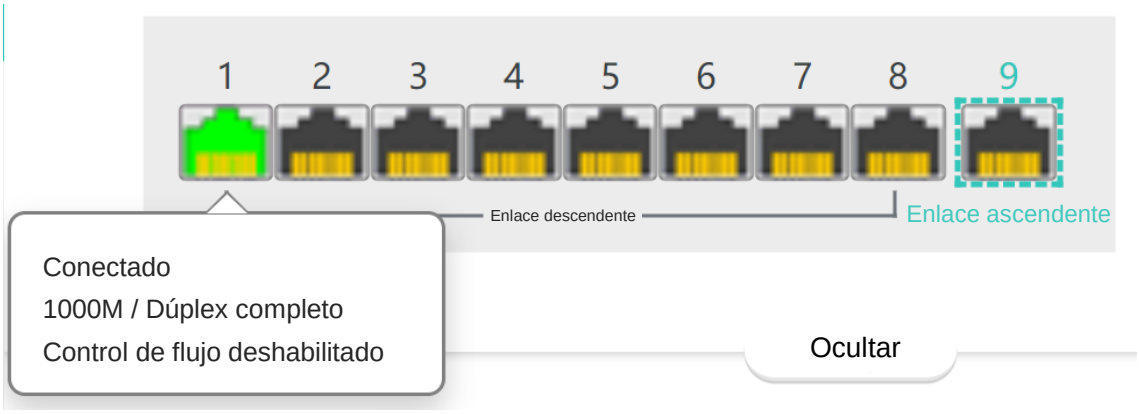


Tabla 4-1

Ícono del puerto	Descripción
	Si el ícono del puerto es de forma cuadrada, indica que es un puerto óptico.
	Si el ícono del puerto es de la forma de un conector RJ-45, indica que es un puerto eléctrico.
	Si el color del ícono del puerto es negro, indica que el puerto está desconectado.
	Si el color del ícono del puerto es gris, indica que el puerto está deshabilitado y que no puede recibir o transmitir paquetes de datos.
	Si el color del ícono del puerto es amarillo, indica que existe un bucle.

	Si el color del ícono del puerto es verde, indica que el puerto está trabajando normalmente.
	El número en la parte superior del ícono del puerto es el ID utilizado para identificar el puerto del dispositivo. El ID del puerto se utiliza para especificar el puerto a configurar.
	Los puertos del dispositivo se clasifican en puertos de enlace ascendente o de enlace descendente. El puerto de enlace ascendente se utiliza para conectar a dispositivos de red de flujo ascendente y a la red central. El puerto de enlace descendente se utiliza para conectarse a las terminales. Cuando la función de aislamiento de puerto está habilitada, los puertos de enlace descendente del dispositivo están aislados unos de otros y solo pueden establecer comunicación a través de los puertos de enlace ascendente. Para obtener más información, consulte el capítulo 4.4 Aislamiento de puertos

Los diferentes colores y formas de los íconos de cada puerto representan distintos estados del puerto. Tabla 4-1 lista de íconos del puerto. Mueva el cursor sobre el ícono del puerto. El estado del puerto se mostrará, incluyendo su estado de conexión, la velocidad del puerto, el modo dúplex y el estado del control de flujo.



4.1.2 Información general del puerto

Seleccione **Página de inicio**.

La página de inicio muestra la información general del puerto, incluyendo su estado, velocidad de recepción/transmisión (velocidad Rx/Tx), estado de aislamiento y estado de detección de un bucle. Además, admite consultas hechas por el dispositivo de enlace descendente.

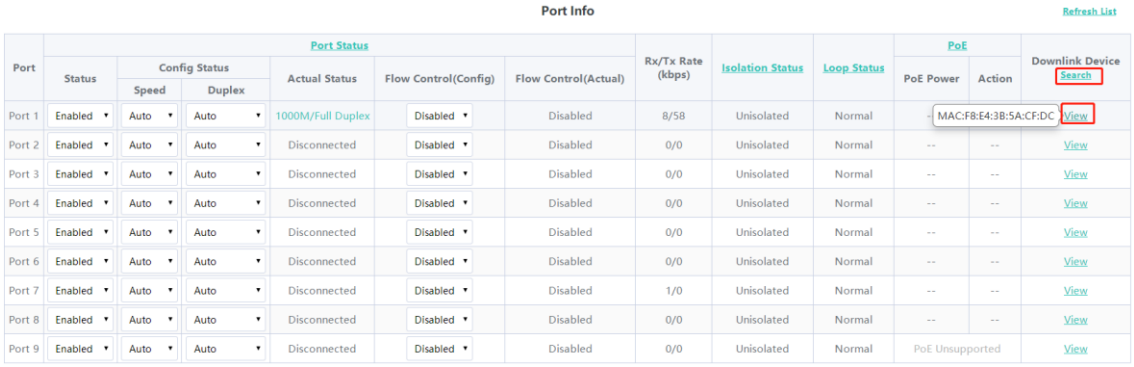
Haga clic en **Port Status** para configurar los atributos básicos del puerto. Para obtener más información, consulte el capítulo 4.2 Configuración y visualización de los atributos de puertos

Haga clic en **Isolation Status** para configurar la función de aislamiento del puerto, para que los puertos de enlace descendente del dispositivo queden aislados unos de otros. Para obtener más información, consulte el capítulo 4.4 Aislamiento de puertos

Haga clic en **Loop Status** para habilitar la función de protección contra bucles. Cuando se detecte un bucle, el puerto donde este ocurra se apagará automáticamente. Para obtener más información, consulte el capítulo 6.3 Protección contra bucles

Haga clic en **Search** en la columna **Downlink Device** para buscar el dispositivo de enlace descendente del puerto elegido. Luego, haga clic en **View** para ver la dirección MAC del dispositivo de enlace descendente.

Haga clic en **Refresh List** para actualizar y obtener la información más reciente de los puertos.



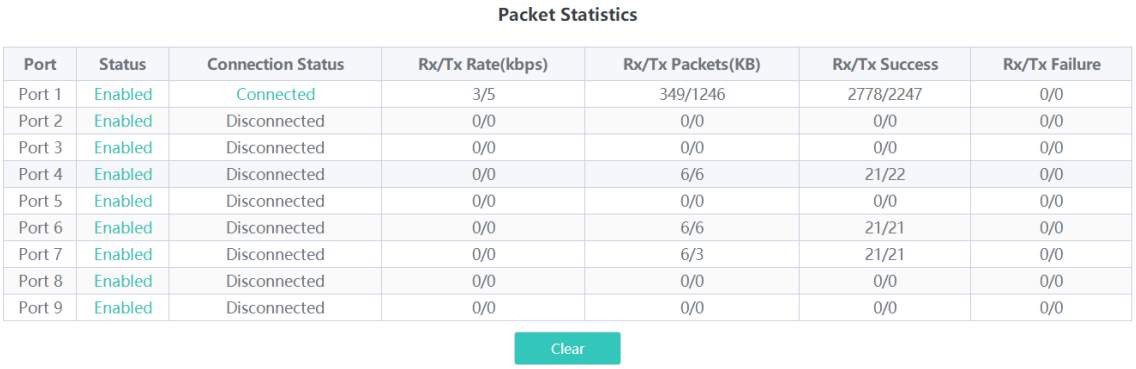
Port	Status	Speed	Duplex	Actual Status	Flow Control(Config)	Flow Control(Actual)	Rx/Tx Rate (kbps)	Isolation Status	Loop Status	PoE Power	Action	Downlink Device
Port 1	Enabled	Auto	Auto	1000M/Full Duplex	Disabled	Disabled	8/58	Unisolated	Normal	--	--	View
Port 2	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 3	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 4	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 5	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 6	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 7	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	1/0	Unisolated	Normal	--	--	View
Port 8	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 9	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	PoE Unsupported		View

4.1.3 Estadísticas de los paquetes de puertos

Seleccione **Monitoreo** > **Packet Statistics**.

La página **Packet Statistics** muestra el estado del puerto y de la conexión, la velocidad de Rx/Tx (kbps), los paquetes Rx/Tx (KB) y el éxito o fallas en Rx/Tx.

Haga clic en **Clear** para borrar las estadísticas de los paquetes que actualmente están en todos los puertos y restablecerlas.



Port	Status	Connection Status	Rx/Tx Rate(kbps)	Rx/Tx Packets(KB)	Rx/Tx Success	Rx/Tx Failure
Port 1	Enabled	Connected	3/5	349/1246	2778/2247	0/0
Port 2	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 3	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 4	Enabled	Disconnected	0/0	6/6	21/22	0/0
Port 5	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 6	Enabled	Disconnected	0/0	6/6	21/21	0/0
Port 7	Enabled	Disconnected	0/0	6/3	21/21	0/0
Port 8	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 9	Enabled	Disconnected	0/0	0/0	0/0	0/0

4.2 Configuración y visualización de los atributos de puertos

SeleccioneConfiguración del switch > Configuración del puerto.

4.2.1 Configuración de puertos

Es posible configurar por lotes los atributos básicos de los puertos Ethernet.

Haga clic en **Select** en la columna **Port** para que se muestren las opciones de todos los puertos de los dispositivos. Seleccione los puertos que desea configurar, el estado, la velocidad, el modo dúplex y el control de flujo; después haga clic en **Save**.

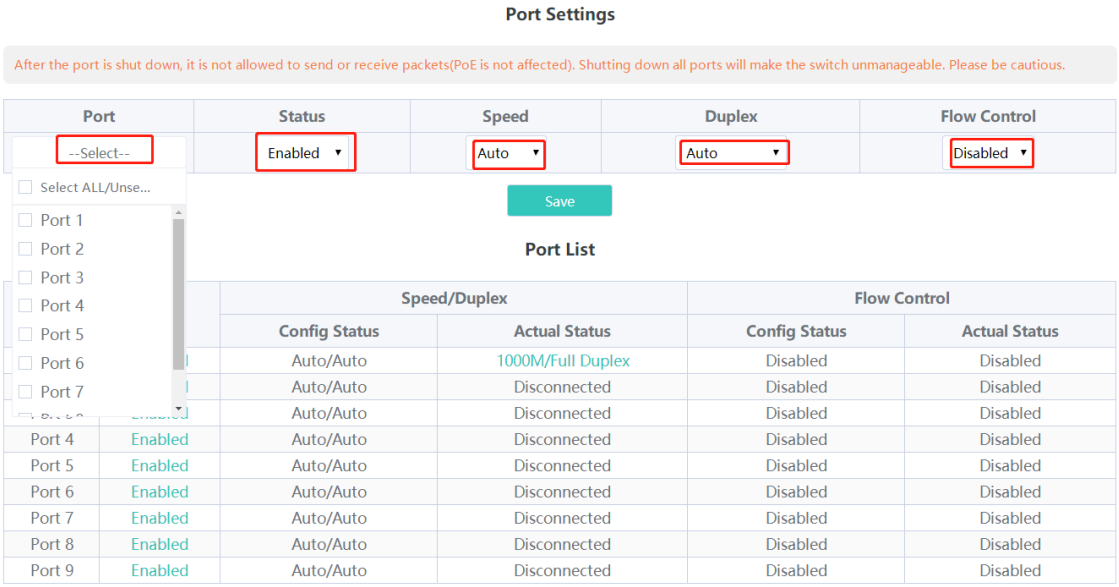


Tabla 4-2 Parámetros básicos de la configuración de puertos

Parámetro	Descripción	Valor predeterminado
Puerto	Seleccione los puertos a configurar.	NA
Estado	Cuando el puerto está deshabilitado, no puede recibir o transmitir paquetes (no afecta a PoE)	Habilitado
Velocidad	Configure la velocidad de operación del puerto físico Ethernet. Cuando la velocidad está en **Auto**, el puerto local y el remoto trabajan en modo negociación automática. La velocidad negociada debe encontrarse dentro de la capacidad del puerto.	Automático
Dúplex	● Dúplex completo: el puerto puede recibir paquetes al mismo tiempo que envía otros. ● Semidúplex: el puerto puede recibir o enviar paquetes, pero no al mismo tiempo. ● Negociación automática: el puerto local y el remoto pueden trabajar en modo negociación automática.	Automático
Control de flujo	La función de control de flujo habilita al puerto para procesar las tramas de control de flujo recibidas y enviar tramas de control de flujo cuando hay una congestión en la red.	Deshabilitado

Precaución

Apagar todos los puertos puede ocasionar una falla en la gestión del conmutador. Por lo tanto, actúe con prudencia al realizar esta acción.

4.2.2 Estado del puerto

Se puede visualizar el estado de la configuración de los atributos del puerto y revisar si los valores están activos, incluyendo la velocidad del puerto, el modo dúplex y el estado del control de flujo.

Port List

Port	Status	Speed/Duplex		Flow Control	
		Config Status	Actual Status	Config Status	Actual Status
Port 1	Enabled	Auto/Auto	1000M/Full Duplex	Disabled	Disabled
Port 2	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 3	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 4	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 5	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 6	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 7	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 8	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 9	Enabled	Auto/Auto	Disconnected	Disabled	Disabled

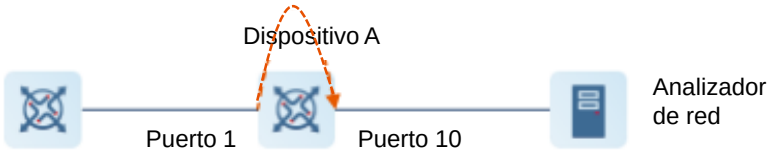
4.3 Duplicación de puertos

4.3.1 Descripción general

En las situaciones de monitoreo de redes y resolución de problemas, se debe analizar el tráfico de datos en nodos de red o puertos de dispositivos que sean sospechosos. Cuando se habilita la función de duplicación de puertos, los paquetes recibidos del puerto de origen y transmitidos a este se duplican en el puerto duplicado (en adelante, puerto de destino). Los paquetes en el puerto de destino se pueden monitorear y analizar a través del analizador de la red, sin afectar el envío de datos del dispositivo que se está monitoreando.

En la Figura 4-1, al configurar la duplicación de puertos en el Dispositivo A, los paquetes en el Puerto 1 se duplican en el Puerto 10. Aunque el analizador de red no se encuentre conectado directamente al Puerto 1, este puede recibir todos los paquetes del Puerto 1 y monitorear el tráfico de datos de dicho puerto.

Figura 4-1 Conexión de la duplicación de puertos en la red



4.3.2 Pasos para la configuración

Seleccione **Configuración del switch** > **Port Mirroring**.

Seleccione puerto de origen, dirección de monitoreo y puerto de destino, y haga clic en **Save**. El dispositivo permite la configuración de un solo puerto de destino.

Para borrar la configuración de duplicación de puertos, haga clic en **Delete**.

Precaución

- Es posible seleccionar varios puertos de origen, pero solo debe haber un puerto de destino. Ninguno de los puertos de origen puede contener al puerto de destino.
- En los conmutadores RG-ES205C-P, RG-ES205GC-P, RG-ES209C-P y RG-ES209GC-P, el puerto de destino solo admite la recepción de paquetes y no puede transmitir datos a los conmutadores.

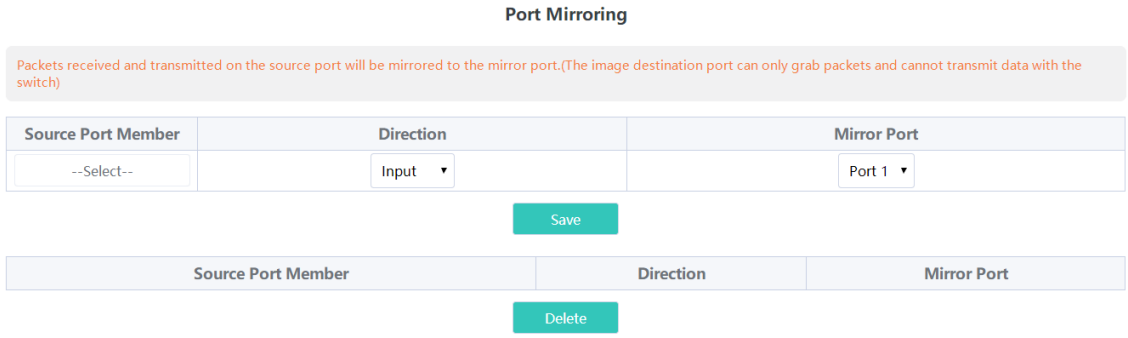


Tabla 4-3 Parámetros de la duplicación de puertos

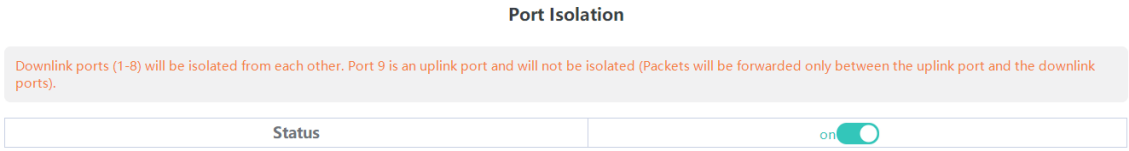
Parámetro	Descripción
Puerto miembro de origen	El puerto de origen también se conoce como puerto monitoreado. Los paquetes del puerto de origen se duplicarán en el puerto de destino para llevar a cabo un análisis de la red o para la resolución de problemas. Se pueden seleccionar varios puertos de origen. Los paquetes de estos puertos se duplicarán en el puerto de destino.
Dirección	La dirección del tráfico de datos monitoreado en el puerto de origen: ● Dos direcciones (entrada y salida): todos los paquetes en el puerto de origen, incluyendo los recibidos y transmitidos, se duplicarán en el puerto de destino. ● Entrada: los paquetes recibidos por el puerto de origen se duplicarán en el puerto de destino. ● Salida: los paquetes transmitidos por el puerto de origen se duplicarán en el puerto de destino.
Puerto de destino	El puerto de destino o duplicado también se conoce como puerto de monitoreo. El puerto de destino se encuentra conectado al dispositivo de monitoreo y transmite paquetes del puerto de origen al dispositivo de monitoreo.

4.4 Aislamiento de puertos

Seleccione **Configuración del switch** > **Port Isolation.**

El aislamiento de puertos se utiliza para aislar paquetes de Capa 2. Cuando la función de aislamiento de puertos está habilitada, los puertos de enlace descendente están aislados unos de otros y solo pueden establecer comunicación a través de los puertos de enlace ascendente.

Esta función está deshabilitada por defecto. Cambie el interruptor a **On** para habilitarla.



Precaución

Los números de puertos de enlace ascendente o descendente y los identificadores de los puertos de diferentes dispositivos varían.

4.5 Límite de velocidad basado en puertos

Seleccione **Configuración de QoS** > **Port Rate**.

Es posible configurar reglas de limitación de la velocidad de entrada y salida de los paquetes en los puertos. Por defecto, no existe una velocidad límite en los puertos.

Seleccione el puerto a configurar, el tipo y el estado del límite de velocidad, e ingrese la velocidad límite. Haga clic en **Save** para guardar la configuración. La configuración se mostrará como corresponde en la tabla **Port Rate**, justo debajo del botón **Save**.

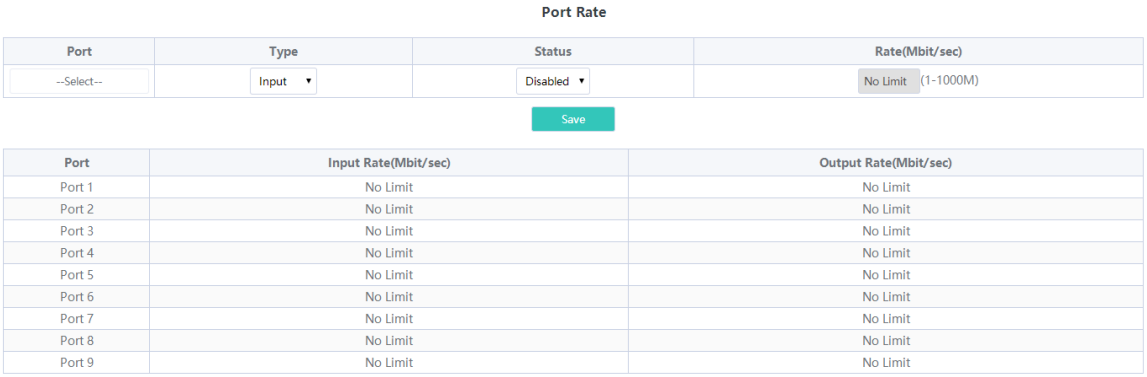


Tabla 4-4 Parámetros de la velocidad límite

Parámetro	Descripción	Valor predeterminado
Puerto	Si lo desea, puede seleccionar varios puertos en lote para configurar la velocidad límite.	N/A
Tipo	Dirección del tráfico de datos con velocidad límite: ● Entrada y salida: velocidad límite de los paquetes reenviados por el puerto, incluyendo los recibidos y transmitidos. ● Entrada: velocidad límite para los paquetes recibidos por el puerto. ● Salida: velocidad límite para los paquetes transmitidos por el puerto.	N/A

Estado	Determina si desea habilitar o deshabilitar la velocidad límite.	Deshabilitado
Velocidad (Mbps)	Velocidad máxima en la que los paquetes son reenviados al puerto.	Sin límite

Nota

- El rango del límite de velocidad para los puertos de RG-ES205C-Ph es de 1 Mbps a 100 Mbps.
- La velocidad máxima compatible con los puertos 1 al 8 en el RG-ES209C-P es de 100 Mbps. Si la velocidad configurada excede los 100 Mbps, la velocidad efectiva seguirá siendo de 100 Mbps. El rango de velocidad límite para el puerto 9 es de 1 Mbps a 1000 Mbps.
- El rango de velocidad límite para los puertos en RG-ES226GC-P, RG-ES218GC-P, RG-ES205GC-P, RG-ES209GC-P, RG-FS303AB, RG-FS306-P, RG-FS306-D es de 1 Mbps a 1000 Mbps.

4.6 Dirección IP de gestión

Seleccione **Configuración del sistema** > **IP Settings**.

Es posible configurar la dirección IP de gestión del dispositivo. Al acceder a la dirección IP de gestión, puede configurar y administrar el dispositivo.

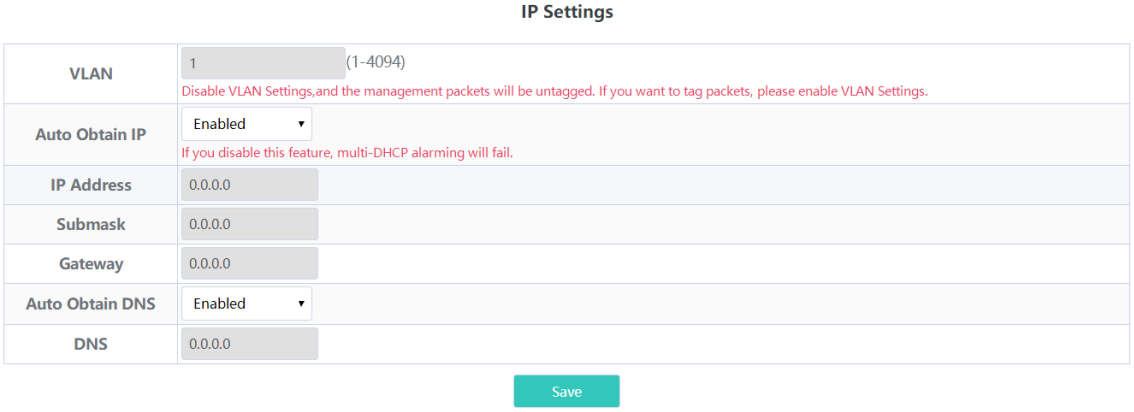
Hay dos modos de Internet disponibles:

- Dirección IP dinámica: habilite **Auto Obtain IP** para usar la dirección IP asignada de manera dinámica por el servidor DHCP ascendente.
- Dirección IP estática: deshabilite **Auto Obtain IP** para utilizar la dirección IP fija configurada manualmente.

Habilite **Auto Obtain IP**. El dispositivo obtendrá automáticamente los parámetros del servidor DHCP. Puede seleccionar la función de obtener una dirección DNS automáticamente del servidor DHCP. Si **Auto Obtain DNS** está deshabilitado, configure una dirección DNS manualmente.

Después de deshabilitar **Auto Obtain IP**, configure manualmente la dirección IP, la máscara de subred, la puerta de enlace de la dirección IP y la dirección DNS. Haga clic en **Save** para guardar la configuración.

VLAN se utiliza para administrar las etiquetas VLAN de los paquetes de gestión. Deshabilite la configuración de VLAN. Los paquetes de gestión no estarán etiquetados y la configuración de la VLAN de gestión no será compatible. Por defecto, la VLAN de gestión del dispositivo es VLAN 1.



Nota

- Deshabilite la configuración de VLAN. Los paquetes de gestión no se etiquetarán. Si desea etiquetar los paquetes, habilite la configuración de VLAN. Para obtener más información, consulte el capítulo 5.2.1 Configuración global de la VLAN
- La VLAN de gestión debe seleccionarse de entre las VLAN existentes. Para crear una VLAN estática, consulte el capítulo 5.2.2 Configuración de las VLAN estáticas
- Le recomendamos vincular la VLAN de gestión configurada a un puerto de enlace ascendente. De otro modo, es posible que no pueda acceder al sistema de gestión de la web. Para obtener más información, consulte el capítulo 5.2.3 Configuración de puertos VLAN
- Si deshabilita **Auto Obtain IP**, la alarma de conflicto con el servidor DHCP se desactivará. Para obtener más información acerca de la alarma de conflicto con el servidor DHCP, consulte el capítulo 9.2 Alerta de conflictos del servidor DHCP

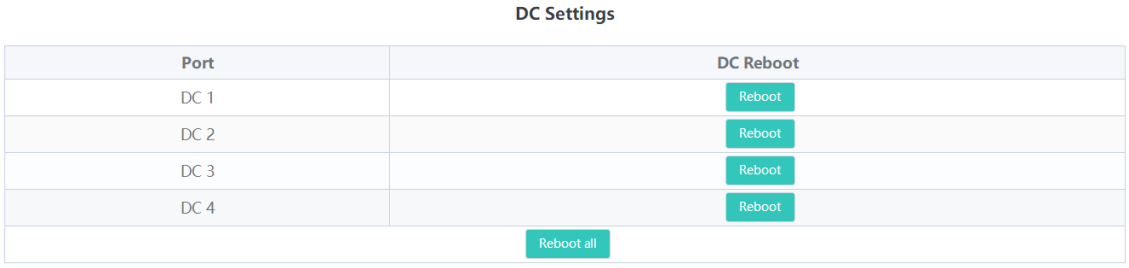
4.7 Reinicio de un dispositivo conectado a un puerto DC

Precaución

Solamente el RG-FS306-D admite esta función.

Seleccione **DC Settings**.

Elija el dispositivo conectado al puerto DC que desea restablecer y haga clic en **Reboot** para reiniciar el dispositivo. Haga clic en **Reboot all** para restablecer los dispositivos conectados a todos los puertos DC del conmutador.



5 Configuración de los conmutadores de la serie ES

5.1 Gestión de direcciones MAC

5.1.1 Descripción general

La tabla de direcciones MAC registra los mapeos desde las direcciones MAC y los puertos a las VLAN.

El dispositivo consulta la tabla de direcciones MAC con base en la dirección MAC de destino de un paquete recibido. Si el dispositivo encuentra una entrada que es consistente con la dirección MAC de destino en el paquete, este lo reenvía a través del puerto especificado por la entrada en modo unidifusión. Si el dispositivo no encuentra dicha entrada, reenvía el paquete a través de todos los puertos, excepto el de recepción, en modo difusión.

Los tipos de entrada de dirección MAC se clasifican en:

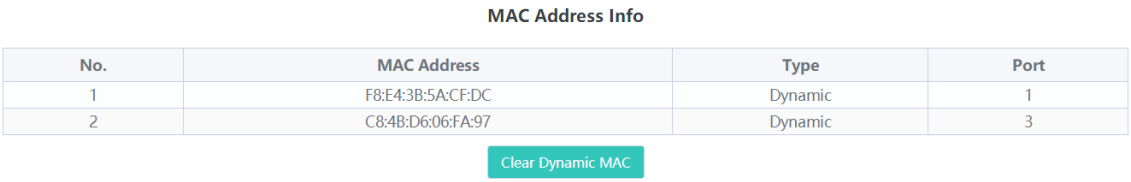
- Entradas de direcciones MAC estáticas: las entradas de direcciones MAC estáticas se configuran manualmente. Los paquetes cuya dirección MAC de destino coincida con una de dichas entradas se reenvían a través del puerto correspondiente.
- Entradas de direcciones MAC dinámicas: el dispositivo aprende de manera dinámica las entradas de direcciones MAC dinámicas. Estas se generan automáticamente por el dispositivo.

5.1.2 Visualización de la tabla de direcciones MAC

Seleccione **Configuración del switch** > **MAC Address Info**.

Esta página muestra la dirección MAC del dispositivo, incluyendo la dirección MAC estática configurada manualmente y la dirección MAC dinámica aprendida automáticamente por el dispositivo.

Haga clic en **Clear Dynamic MAC** para borrar la dirección MAC dinámica aprendida por el dispositivo. El dispositivo aprenderá nuevamente la dirección MAC y generará una tabla de direcciones MAC.



Nota

- Si deshabilita la VLAN, el dispositivo reenviará los paquetes únicamente a la dirección MAC de destino. El identificador de la VLAN o VLAN ID no se muestra en la tabla de direcciones MAC.
- Se muestran hasta 100 direcciones MAC.

5.1.3 Búsqueda de direcciones MAC

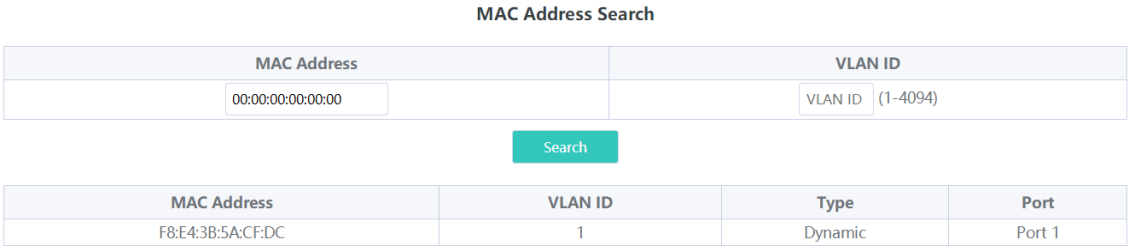
Seleccione **Configuración del switch** > **Buscar MAC**.

Es posible buscar entradas de direcciones MAC de acuerdo con la dirección MAC y la VLAN ID.

Precaución

Si se deshabilita la VLAN, la VLAN ID no se registrará en la tabla de direcciones MAC. Las entradas de direcciones MAC solo se pueden encontrar con base en direcciones MAC.

Ingrese la dirección MAC y la VLAN ID; posteriormente, haga clic en **Search**. Las entradas de direcciones MAC que coincidan con el criterio de búsqueda se mostrarán en la tabla, justo debajo del botón **Search**. Además, se pueden ingresar caracteres parciales de una dirección MAC para hacer una búsqueda difusa.



5.1.4 Configuración de direcciones MAC estáticas

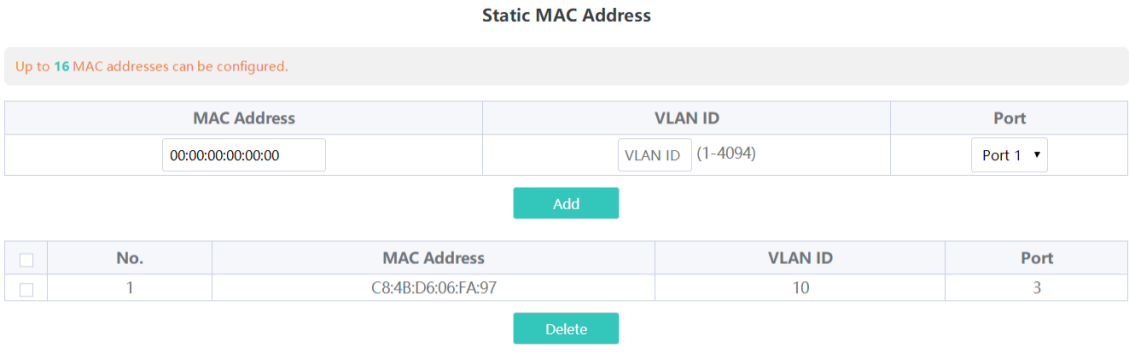
Seleccione **Configuración del switch** > **Dirección MAC estática**.

Al configurar una dirección MAC estática, se puede vincular manualmente la dirección MAC de un dispositivo de red de enlace descendente a uno de los puertos del conmutador. Cuando el dispositivo recibe un paquete destinado a la dirección MAC estática de una VLAN, el dispositivo reenvía el paquete al puerto especificado.

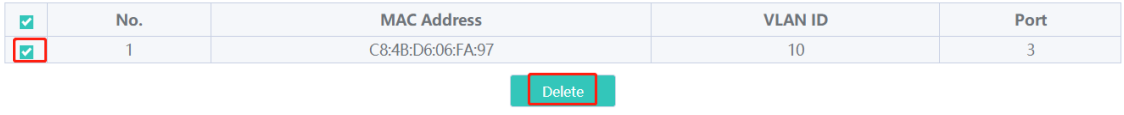
Precaución

Si se deshabilita la VLAN, la VLAN ID no se registrará en la tabla de direcciones MAC. No se puede configurar una VLAN a la dirección MAC estática a la que pertenece.

Ingrese una dirección MAC, especifique la VLAN ID y seleccione el puerto de transmisión. Luego, haga clic en **Add** para añadir una dirección MAC estática. Las entradas de direcciones MAC se actualizarán como corresponde en la tabla de direcciones MAC.



Si desea borrar una dirección MAC estática, seleccione la entrada que desea borrar en la tabla y haga clic en **Delete**.



5.2 Configuración de la VLAN

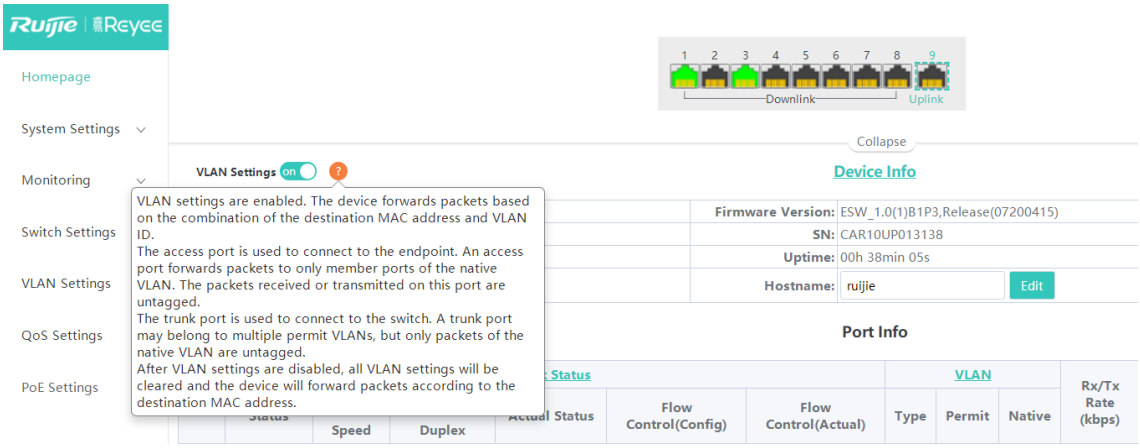
5.2.1 Configuración global de la VLAN

Seleccione **Homepage** > **Device Info**.

La página muestra el estado de la configuración de la VLAN. Utilice el interruptor **on-off** para habilitar o deshabilitar la configuración de la VLAN.

Cuando se deshabilita la VLAN, el dispositivo funciona como un conmutador no configurado. El dispositivo envía paquetes de acuerdo con la dirección MAC destino y la VLAN ID de los paquetes enviados permanece sin modificaciones durante el proceso.

Cuando se habilita la VLAN, el dispositivo funciona como un conmutador configurado. El dispositivo envía los paquetes de acuerdo con la dirección MAC y la VLAN ID. El tipo de puerto se puede configurar como enlace de acceso o troncal, dependiendo de si los paquetes cuentan con una etiqueta VLAN. Además, todos los puertos del dispositivo se inicializarán como puertos de acceso.



5.2.2 Configuración de las VLAN estáticas

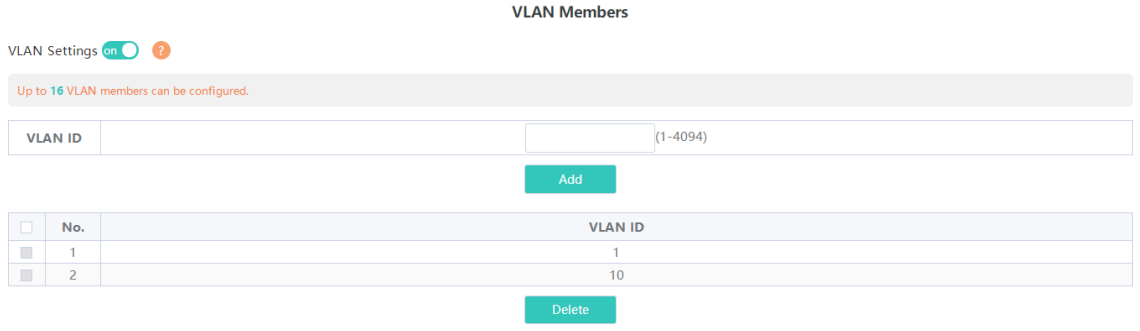
Precaución

Las VLAN estáticas pueden crearse solamente cuando la configuración global de la VLAN está habilitada. Para obtener más información, consulte el capítulo 5.2.1 Configuración global de la VLAN

Seleccione **VLAN Settings** > **VLAN Members**.

Ingrese la VLAN ID y haga clic en **Add** para crear una VLAN estática.

La tabla de VLAN contiene las VLAN existentes. Seleccione las VLAN que desea borrar y haga clic en **Delete**. Las VLAN seleccionadas se eliminarán. La VLAN 1 no se puede borrar.



Nota

- El rango de las VLAN ID es de 1 a 4094. La VLAN 1 es la VLAN predeterminada.
- La VLAN predeterminada (VLAN 1), la VLAN de gestión, la VLAN nativa, la VLAN de autorización y la VLAN de acceso no se pueden eliminar.

5.2.3 Configuración de puertos VLAN

Precaución

Se puede configurar el puerto VLAN solo cuando la configuración global de la VLAN está habilitada. Para obtener más información, consulte el capítulo 5.2.1 Configuración global de la VLAN

Seleccione **VLAN Settings** > **VLAN Settings**.

Configure el modo de puerto y los miembros VLAN de un puerto. Sabrá cuáles son las VLAN permitidas en el puerto y si los paquetes reenviados por ese puerto contienen etiquetas.

Nota

Se sugiere crear miembros VLAN (consulte el capítulo 5.2.2 Configuración de las VLAN estáticas) antes de configurar un puerto que se base en VLAN. Haga clic en **VLAN Members** para acceder a la página de **VLAN Members** donde podrá añadir miembros VLAN.

Seleccione el puerto que desea configurar y el modo de puerto. Si elige el modo acceso, seleccione **Access VLAN** para el puerto y haga clic en **Save**. Si elige el modo troncal, seleccione **Native VLAN** para el puerto, ingrese el rango de VLAN ID permitido por el puerto y haga clic en **Save**.

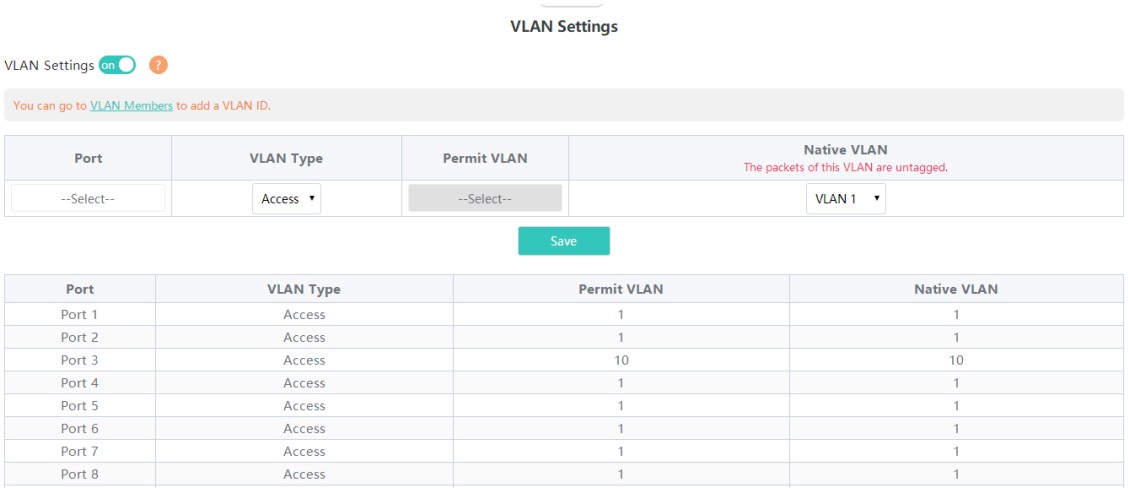


Tabla 5-1 Modos de puertos

Modo de puerto	Descripción

Acceso	Un puerto de acceso solamente puede pertenecer a una VLAN y permitir tramas únicamente de dicha VLAN para que pasen a través de ella. Esta VLAN se conoce como VLAN de acceso. Las tramas de los puertos de acceso no llevan una etiqueta VLAN. Cuando el puerto de acceso recibe una trama sin etiqueta de un dispositivo remoto, el dispositivo local determina que proviene de una VLAN de acceso y añade la VLAN ID de acceso a la trama. Los puertos de acceso están conectados a una terminal.
Troncal	Un puerto troncal es compatible con una VLAN nativa y varias VLAN de autorización. Las tramas de la VLAN nativa reenviadas por el puerto troncal no llevan etiquetas, mientras que las de la VLAN de autorización sí. Los puertos troncales están conectados a conmutadores. Se puede configurar un rango de VLAN de autorización para limitar las tramas de VLAN que pueden reenviarse. Asegúrese que los puertos troncales en los dos extremos del enlace se encuentren configurados en la misma VLAN nativa.

Nota

La configuración inadecuada de las VLAN en un puerto (especialmente en los de enlace ascendente) puede ocasionar fallas para iniciar sesión en el sistema de gestión de la web. Tenga precaución al configurar al VLAN.

6 Funciones de seguridad

6.1 Inspección DHCP

6.1.1 Descripción general

La función de inspección del Protocolo de Configuración Dinámica de Host (DHCP), o DHCP Snooping, permite que el conmutador evite que los clientes obtengan las direcciones IP de un servidor DHCP no autorizado. Al habilitar esta función, el conmutador almacena parámetros, tales como las direcciones IP y MAC en los paquetes DHCP que se intercambian entre clientes y servidores, para prevenir cualquier ataque del DHCP.

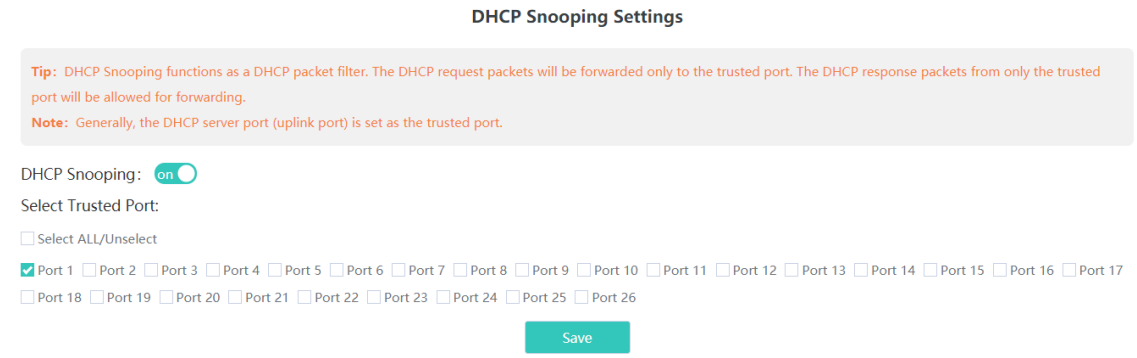
6.1.2 Pasos para la configuración

Seleccione **Configuración del switch** > **DHCP Snooping Settings**.

Mueva el interruptor a **on** para habilitar la función de inspección DHCP, seleccione los puertos de confianza y luego, haga clic en **Save**. Cuando se habilita la función de inspección DHCP, los paquetes de petición de los clientes DHCP se reenvían únicamente a puertos de confianza. Con respecto a los paquetes de respuesta de los servidores DHCP, solo aquellos provenientes de puertos de confianza se reenvían.

Nota

El puerto de enlace ascendente conectado al servidor DHCP se configura como el puerto de confianza.



6.2 Control de tormentas

6.2.1 Descripción general

Cuando una red de área local (LAN) tiene difusión, multidifusión o unidifusión desconocida de flujos de datos en exceso, la velocidad de la red disminuye y se pueden generar tiempos de espera para la transmisión de los paquetes. A esta situación se le conoce como tormenta LAN, que puede ser ocasionada por errores en la ejecución de los protocolos de topología o la inadecuada configuración de una red.

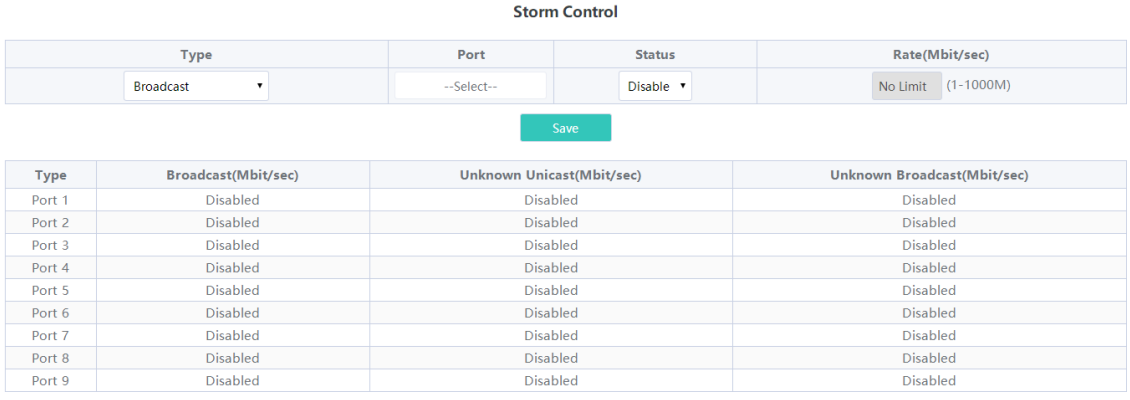
El control de tormentas puede configurarse separadamente para difusión, multidifusión y unidifusión desconocida de flujos de datos. Cuando la velocidad de difusión, multidifusión o unidifusión desconocida de flujos de datos que recibe un dispositivo excede el rango especificado, este transmite solamente los paquetes de un rango específico y descarta los que están fuera de este rango hasta que la velocidad vuelva a estar dentro del rango. Esto previene que un desbordamiento de datos ingrese a la LAN y ocasione una tormenta.

6.2.2 Pasos para la configuración

Seleccione **Configuración de la QoS** > **Storm Control**.

Seleccione el tipo de control de tormentas, el puerto y el estado; defina la velocidad límite y haga clic en **Save**.

El tipo de control de tormentas y la velocidad correspondiente se muestran en la tabla justo debajo del botón **Save**. Cuando la función de control de tormentas está deshabilitada, el flujo de datos de difusión, multidifusión y unidifusión desconocida no cuenta con un límite de velocidad. El estado correspondiente se muestra como **Disabled**. Cuando el control de tormentas está habilitado, se muestran los límites de velocidad correspondientes.



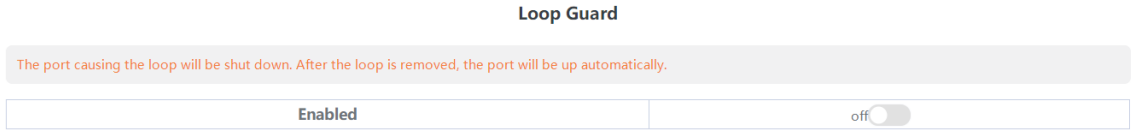
Nota

- La velocidad límite para los puertos del switch RG-ES205C-P es de 1 Mbps a 100 Mbps.
- La velocidad máxima admitida por los puertos 1 al 8 en el RG-ES209C-P es de 100 Mbps. Si la velocidad configurada excede los 100 Mbps, la velocidad efectiva seguirá siendo de 100 Mbps. La velocidad límite para el puerto 9 es de 1 Mbps a 1000 Mbps.
- La velocidad límite para los puertos en los modelos RG-ES226GC-P, RG-ES218GC-P, RG-ES205GC-P, RG-ES209GC-P, RG-FS303AB, RG-FS306-P y RG-FS306-D es de 1 Mbps a 1000 Mbps.

6.3 Protección contra bucles

Seleccione **Monitoreo** > **Loop Guard**.

Cuando la función de protección contra bucles se encuentra habilitada, el puerto donde ocurra un bucle se apagará automáticamente. Después de que se haya eliminado el bucle, el puerto volverá a encenderse automáticamente. Por defecto, la función de protección contra bucles está deshabilitada.



7 Configuración del PoE

Precaución

Solo los dispositivos RG-ES226GC-P, RG-ES218GC-P, RG-ES209GC-P, RG-ES209C-P, RG-ES205GC-P, RG-ES205C-P y RG-FS306-P admiten la función de PoE.

Seleccione **Configuración del PoE**.

El dispositivo admite la fuente de alimentación a través de PoE. Visualice y configure el estado de la potencia.

Estado del dispositivo: en la pantalla se muestra la potencia total, la utilizada, la restante y el estado de trabajo del sistema PoE.

PoE Info

Total Power	Used	Remaining	Work Status
120w	0w	120w	Normal

Estado del puerto: en la pantalla se muestra el voltaje, la corriente, la potencia de salida y el estado de la potencia de los puertos del dispositivo. Se puede habilitar o deshabilitar la función PoE cambiando el interruptor **on-off**. Cuando la función PoE se encuentre deshabilitada, el puerto no podrá suministrar energía a dispositivos externos.

Si un PD falla, encienda nuevamente el puerto conectado a este para reiniciarlo.

PoE Settings

PoE Status When off, PoE will not work on this port	Port	Power(W)	Current(mA)	Voltage(V)	Power Status	Action
on	Port 1	0	0	0	Powered Off	--
on	Port 2	0	0	0	Powered Off	--
on	Port 3	0	0	0	Powered Off	--
on	Port 4	0	0	0	Powered Off	--
on	Port 5	0	0	0	Powered Off	--
on	Port 6	0	0	0	Powered Off	--
on	Port 7	0	0	0	Powered Off	--
on	Port 8	0	0	0	Powered Off	--
Port 9 Unsupported						

Nota

Los puertos ópticos en RG-ES226GC-P, RG-ES218GC-P y RG-FS306-P no admiten la función PoE.

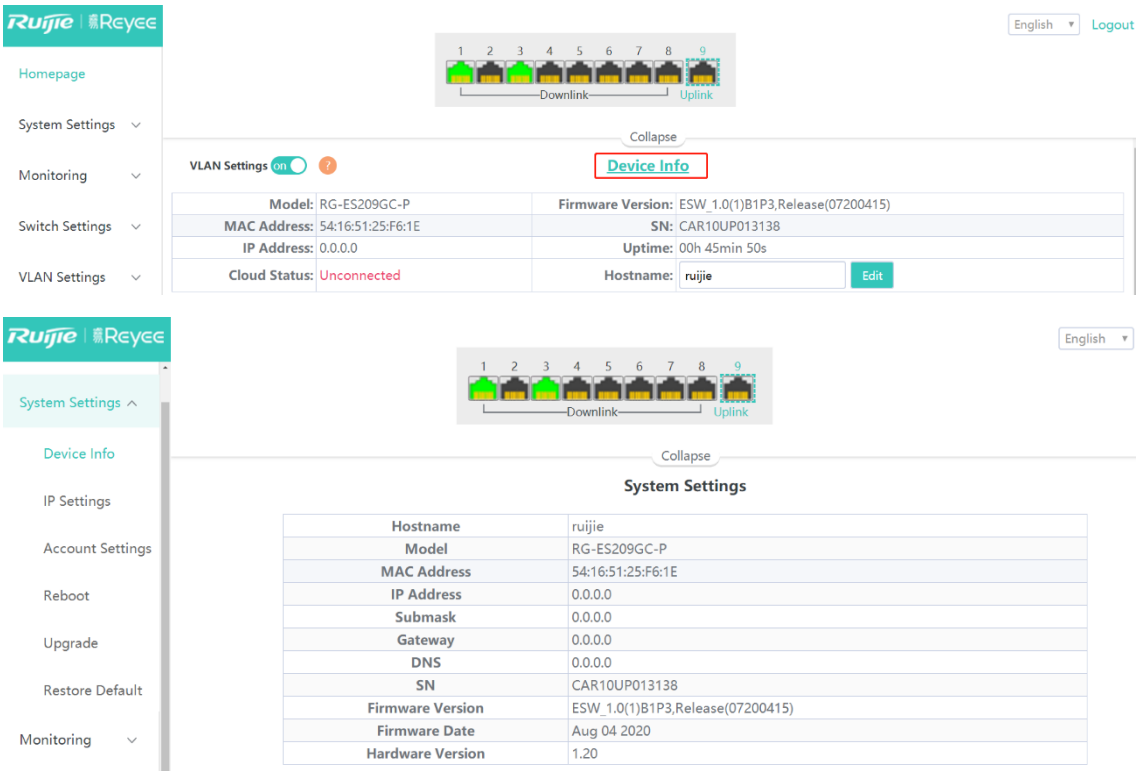
8 Configuración del sistema

8.1 Información del dispositivo de gestión

8.1.1 Visualización de la información del dispositivo

Seleccione **Homepage** > **Device Info**.

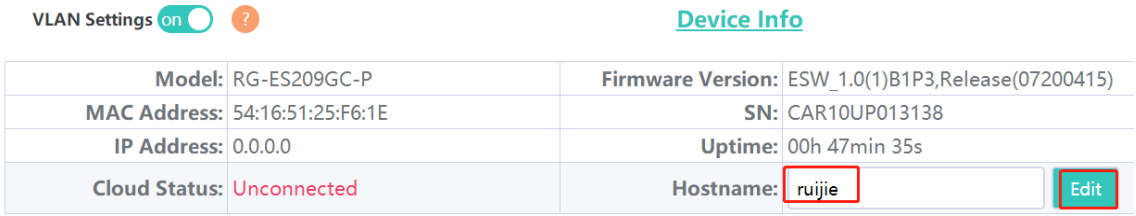
En la página de inicio se mostrará la información del dispositivo, incluyendo el nombre de host, el modelo del dispositivo, el número de serie, la versión de firmware, la dirección IP, la dirección MAC, el estado de la nube y el tiempo de actividad. Haga clic en **Device Info** para acceder a la página **Device Info** (**System Settings** > **Device Info**) y visualizar información más detallada del dispositivo.



8.1.2 Edición del nombre de host

Seleccione **Homepage** > **Device Info**.

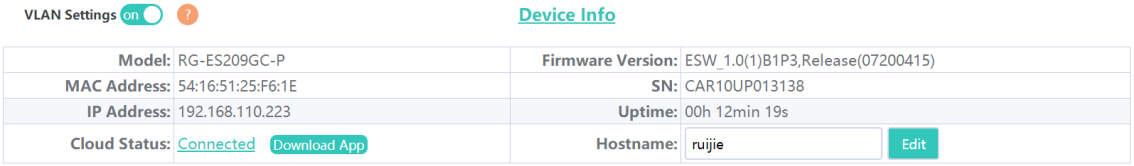
Ingrese el nombre de host y haga clic en **Edit** para cambiarlo y distinguir diferentes dispositivos.



8.1.3 Administración de la nube

Seleccione **Página de inicio** > **Device Info**.

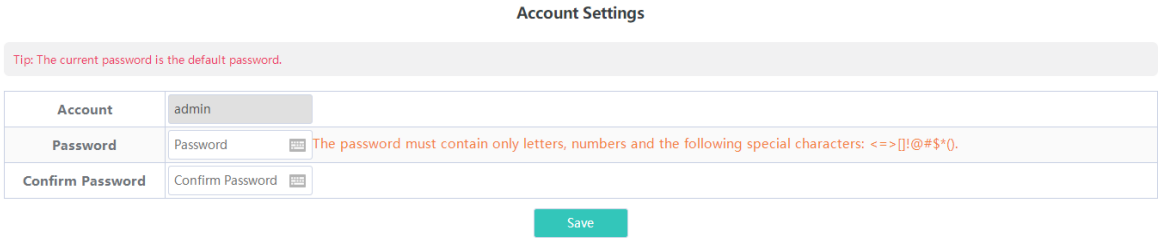
En **Cloud Status** se muestra si el dispositivo está conectado a la nube. Después de vincular el dispositivo a una cuenta de gestión de la nube, el valor **Cloud Status** es **Connected**. Ahora puede administrar el dispositivo de forma remota a través de la página web de Ruijie Cloud o de la aplicación. Haga clic en **Connected** para acceder a la página de inicio de Ruijie Cloud (https://cloud-as.ruijienetworks.com). Haga clic en **Download App** para descargar Ruijie Cloud App.



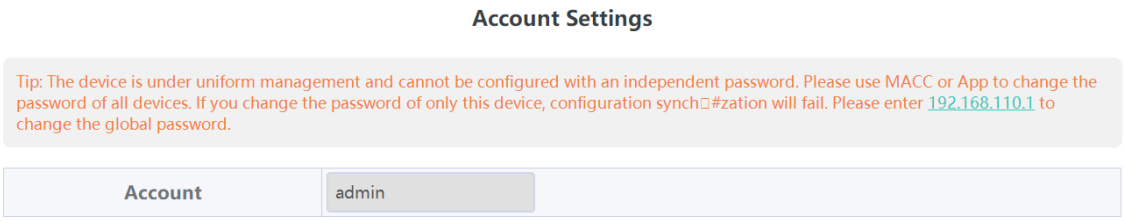
8.2 Configuración de la contraseña

Cuando la contraseña del dispositivo es la predeterminada, este solicita que se restablezca al iniciar sesión en el sistema de gestión Eweb. Haga clic en **Sí** para acceder a la página **Account Settings** (o seleccione **Configuración del sistema** > **Account Settings** para ingresar igualmente).

Establezca una nueva contraseña, de acuerdo con la sugerencia, y haga clic en **Save** para guardar la configuración.



El dispositivo que se administra de manera uniforme no puede configurarse con una contraseña independiente. Es necesario que siga la sugerencia para iniciar sesión en el dispositivo maestro y configurar una contraseña global.



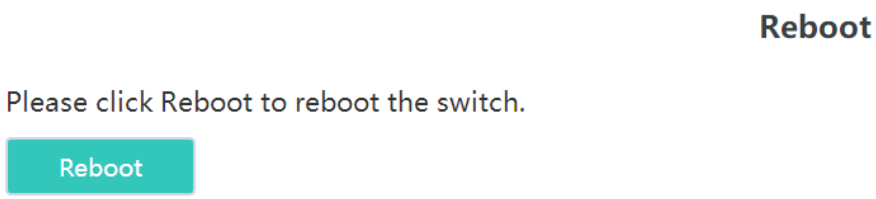
Precaución

- Al iniciar sesión en el sistema de gestión Eweb, primero establezca la contraseña de gestión del dispositivo antes de configurar otras funciones.
- Recuerde la contraseña para administrar el dispositivo (el usuario y la contraseña por defecto son **admin/admin**). Tendrá que volver a iniciar sesión después de cambiar la contraseña.
- Si el dispositivo se administra de manera uniforme, utilice el control de acceso o MACC, o la aplicación para cambiar la contraseña del conjunto de la red. El cambio de contraseña del dispositivo puede ocasionar una falla en este al sincronizar la configuración del conjunto de la red.

8.3 Restablecimiento del dispositivo

Seleccione **Configuración del sistema** > **Reboot**.

Haga clic en **Reboot** para restablecer el conmutador.



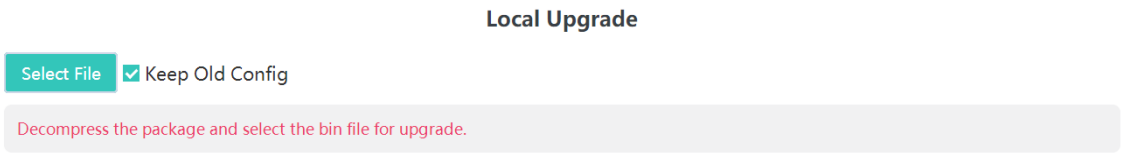
8.4 Actualización del sistema

8.4.1 Actualización local

Seleccione **Configuración del sistema** > **Actualización**.

Haga clic en **Select File** para elegir el paquete de actualización de los archivos locales (el paquete de actualización es un archivo BIN. Si es un archivo con terminación tar.gz, descomprima el paquete y elija el archivo BIN para la actualización).

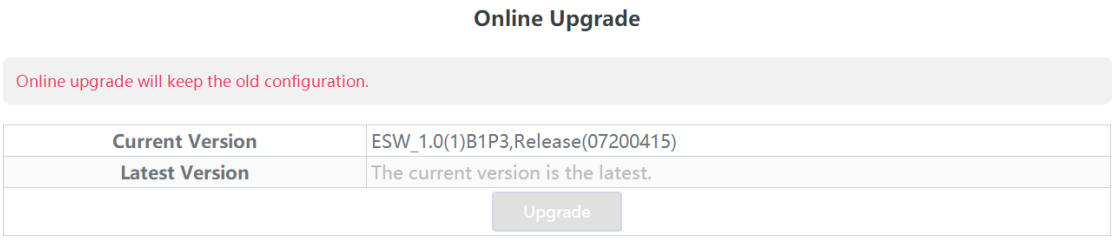
Por defecto, la opción **Keep Old Config** está seleccionada; esta indica que la configuración actual se guardará después de actualizar el dispositivo. Si existe una gran diferencia entre la versión actual y la actualización, no se recomienda usar la función **Keep Old Config**.



8.4.2 Actualización en línea

Seleccione **Configuración del sistema** > **Actualización**.

Cuando hay una nueva versión en la nube, el número de la versión más reciente se mostrará en esta página y el botón **Upgrade** estará disponible. El dispositivo descargará de la nube el paquete de instalación de la versión recomendada y se actualizará a la versión más reciente. Si se decide hacer la actualización en línea, la configuración previa se guardará por defecto.



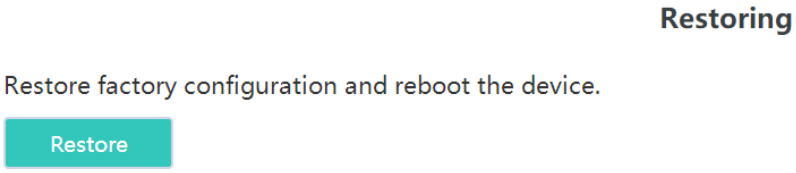
Nota

El tiempo que toma hacer actualizaciones en línea depende de la velocidad actual de la red.

8.5 Restauración de la configuración de fábrica

Seleccione **Configuración del sistema** > **Restauración de fábrica**.

Haga clic en **Restore** para restablecer la configuración predeterminada y reiniciar el dispositivo.



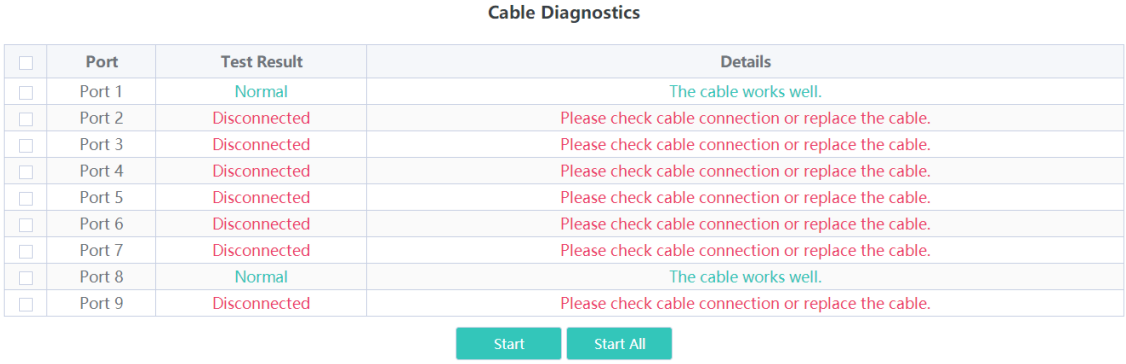
9 Monitoreo

9.1 Diagnóstico de cables

Seleccione **Monitoreo** > **Cable Diagnostics**.

El diagnóstico de cables se utiliza para revisar el estado de los cables Ethernet. Por ejemplo, puede verificar si los cables tienen un corto circuito o si están desconectados.

Seleccione los puertos que desea detectar y luego haga clic en **Start** para iniciar el diagnóstico de cables. El resultado de la prueba se mostrará como corresponde. Haga clic en **Start All** para llevar a cabo el diagnóstico de cables de todos los puertos en un solo clic.



Precaución

Si elige un puerto de enlace ascendente para hacer un diagnóstico, esto puede generar que la red se desconecte de forma intermitente. Por lo tanto, actúe con prudencia al realizar esta acción.

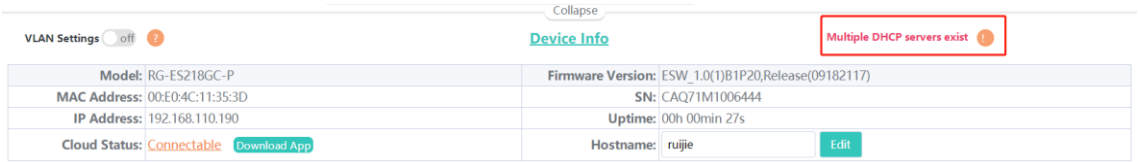
9.2 Alerta de conflictos del servidor DHCP

Precaución

- Solo los dispositivos RG-ES226GC-P, RG-ES218GC-P, RG-ES224GC y RG-ES216GC son compatibles con la alerta de conflictos del servidor DHCP.
- La alerta de conflictos del servidor DHCP no es efectiva cuando la dirección IP del dispositivo no se obtiene de forma dinámica. Para configurar adecuadamente una dirección IP, consulte el capítulo 4.6 Dirección IP de gestión

Seleccione **Página de inicio**.

Cuando existen múltiples servidores DHCP en una LAN, el sistema enviará una alama de conflicto. En la columna **Device Info** se mostrará un mensaje de alerta.



Mueva el cursor sobre para visualizar los detalles de la alerta, incluyendo la VLAN donde está ocurriendo el conflicto, el puerto, la dirección IP del servidor DHCP y la dirección MAC.

9.3 Visualización de la información del conmutador

Seleccione **Monitoreo** > **Switches**.

Si el conmutador se administra de manera uniforme, algunas de las funciones no podrán configurarse de forma independiente (como la contraseña). Para facilitar la configuración, en esta página se mostrará la información del dispositivo maestro en la VLAN. Haga clic en **IP Address** en el dispositivo maestro para acceder a la página del **Dispositivo maestro** y realizar la configuración global.

Primary Device

The current device has been managed by the master device. Please click the IP address to manage the master device.

IP Address	SN	Model
192.168.110.1	H1RP4HH076624	EG105GW-E

El dispositivo automáticamente encontrará otros conmutadores en la misma VLAN de gestión. La información acerca de estos conmutadores se mostrará en **Switch List**.

La primera fila en **Switch List** muestra información sobre el dispositivo actual, y las filas siguientes muestran la información de otros dispositivos. Haga clic en **IP Address** en un dispositivo para acceder a su sistema de gestión Eweb (se requiere iniciar sesión).

Switch List

Up to 16 switches of the same management VLAN can be discovered.

No.	IP Address	SN	Hostname	Model
1	192.168.110.209(Local)	CARL542000171	ruijie	RG-ES205C-P
2	192.168.110.39	MACCLLES226GC	ruijie	RG-ES226GC-P
3	192.168.110.102	CAQB1AW047292	ruijie	New Model

Nota

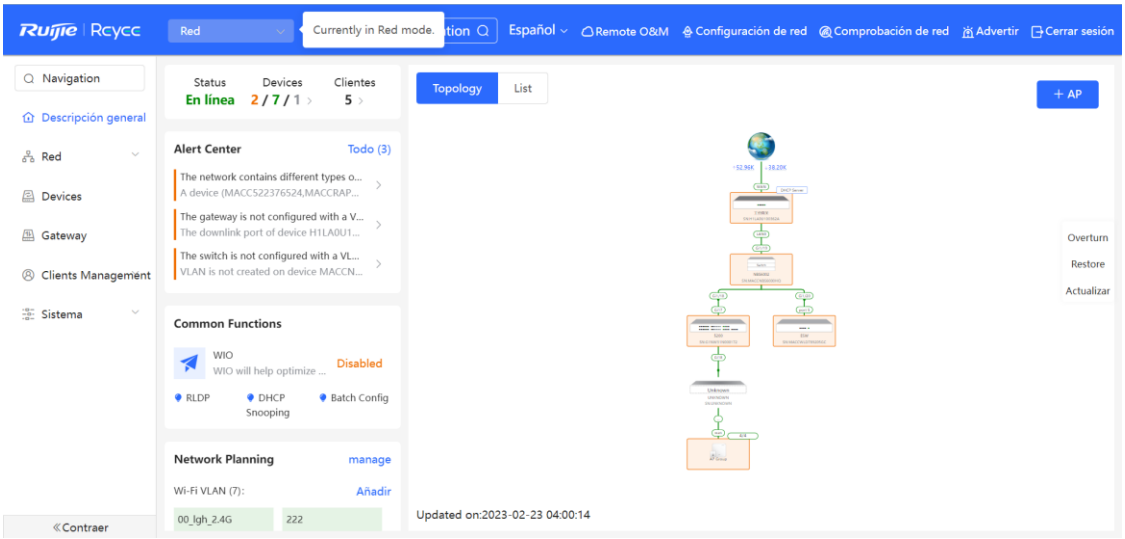
El número de switches que pueden encontrarse varía según el modelo del producto:

- Los modelos RG-ES226GC-P, RG-ES218GC-P y RG-FS303-AB pueden encontrar 32 switches.
- Los RG-ES205C-P, RG-ES205GC-P, RG-ES209C-P, RG-ES209GC-P, RG-FS306-P y RG-FS306-D pueden encontrar 16 switches.

10 Gestión de redes de los switches de las series NBS y NIS

10.1 Información general de la red

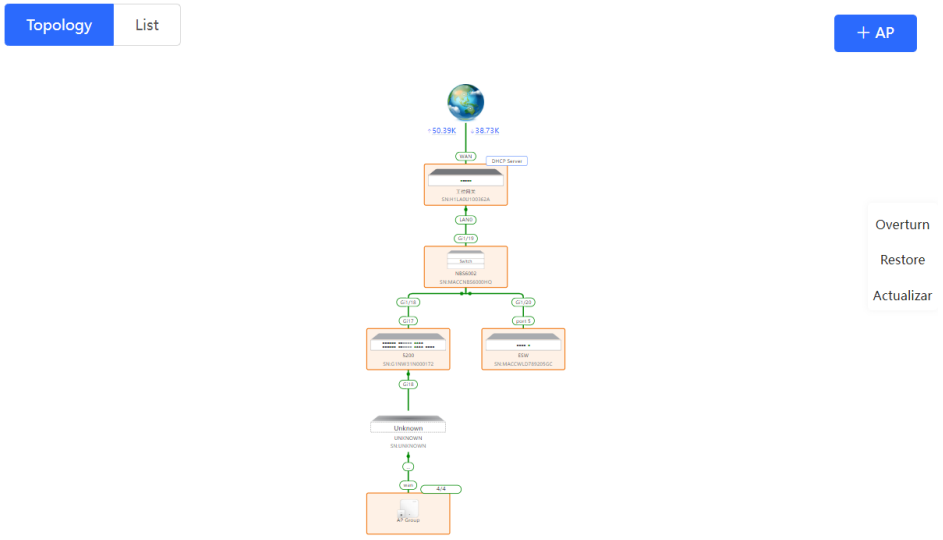
En modo red, la página **Descripción general** muestra la topología de la red actual, el tráfico en tiempo real de los enlaces ascendentes y descendentes, el estado de conexión de la red y el número de usuarios. Además, proporciona atajos para configurar la red y los dispositivos. El estado de red de toda la red se puede supervisar y administrar en esta página.



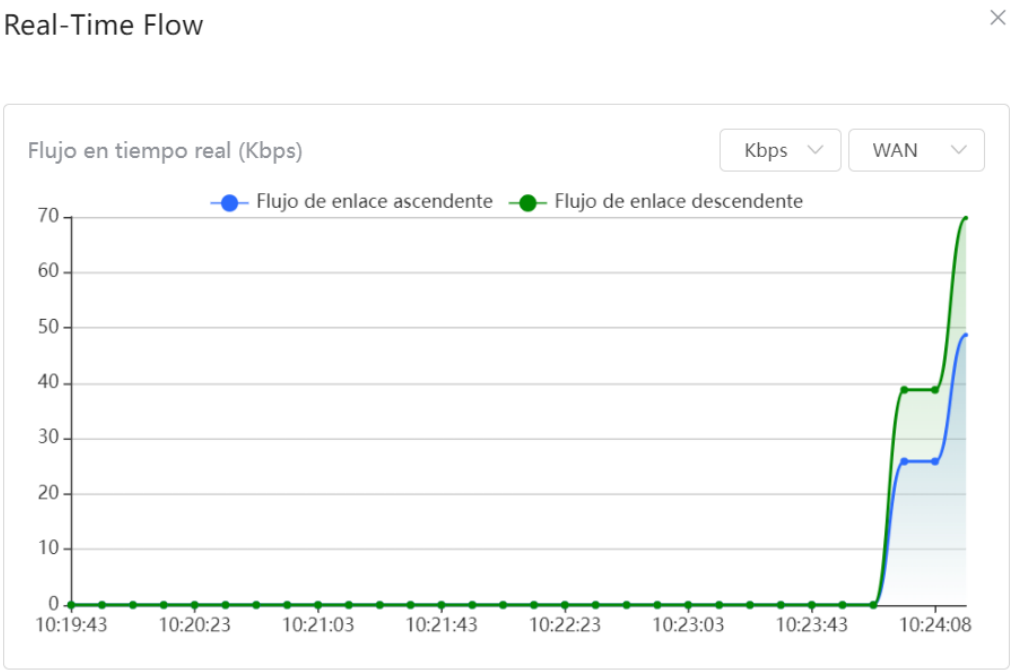
10.2 Visualización de la información de red

Seleccione **Red** > **Descripción general**.

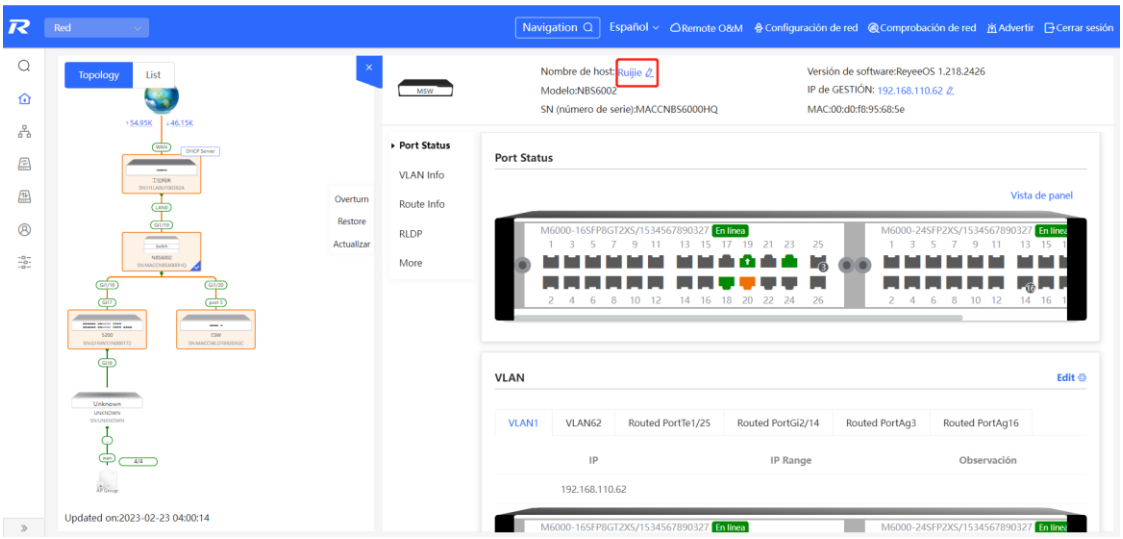
La topología de la red cuenta con información sobre los dispositivos en línea, el número de puertos conectados, los SN de los dispositivos y el tráfico en tiempo real de enlaces ascendentes y descendentes.



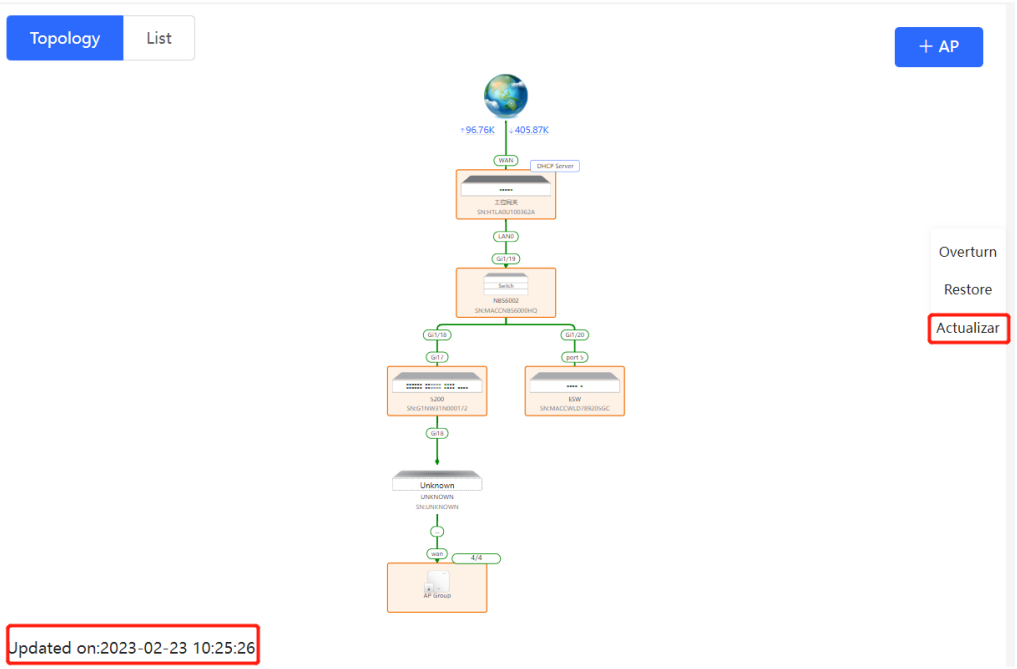
- Haga clic en el elemento de tráfico de datos para visualizar su información en tiempo real.



- Haga clic en uno de los dispositivos en la topología para visualizar su estado operativo y configuración, y establezca las funciones del dispositivo. Por defecto, el modelo del producto se utiliza como nombre del dispositivo. Haga clic en  para modificar el nombre del dispositivo y que mediante su descripción pueda distinguirlos.



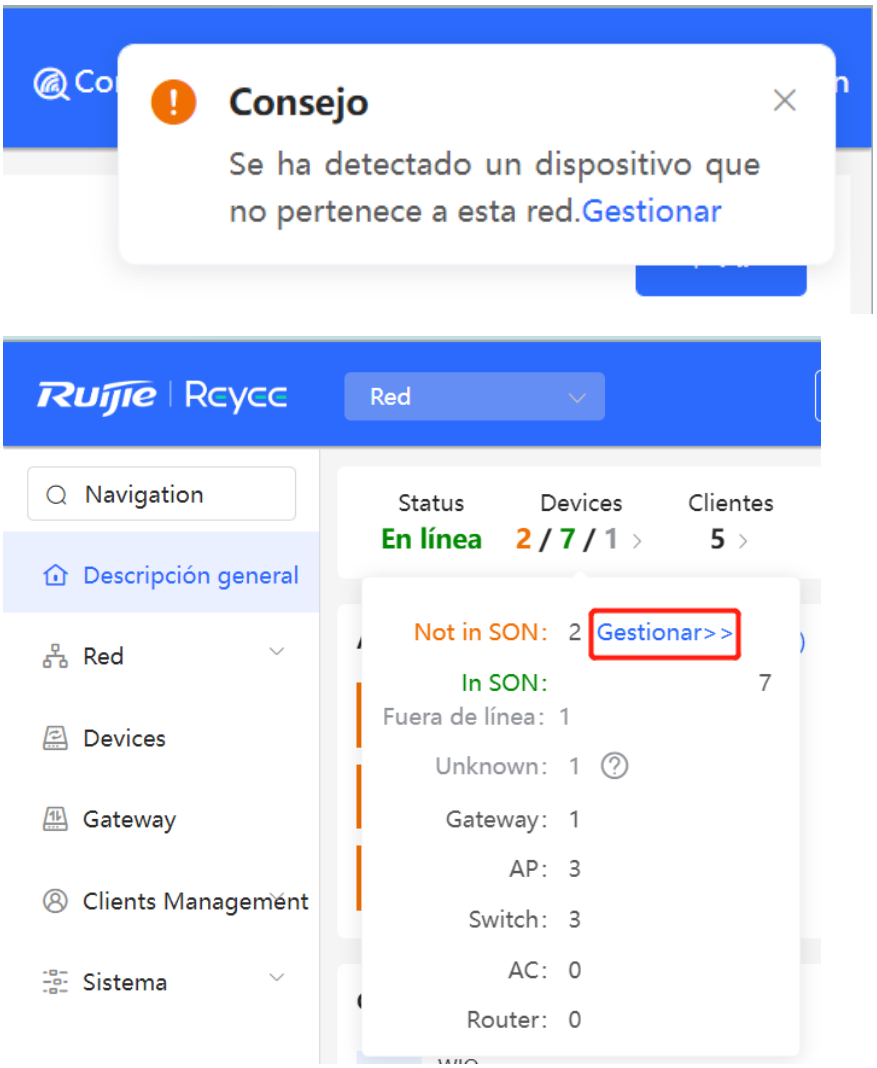
- El tiempo de actualización se muestra en la esquina inferior derecha de la topología. Haga clic en **Actualizar** para actualizarla. Considere que toma tiempo actualizar los datos de la topología.



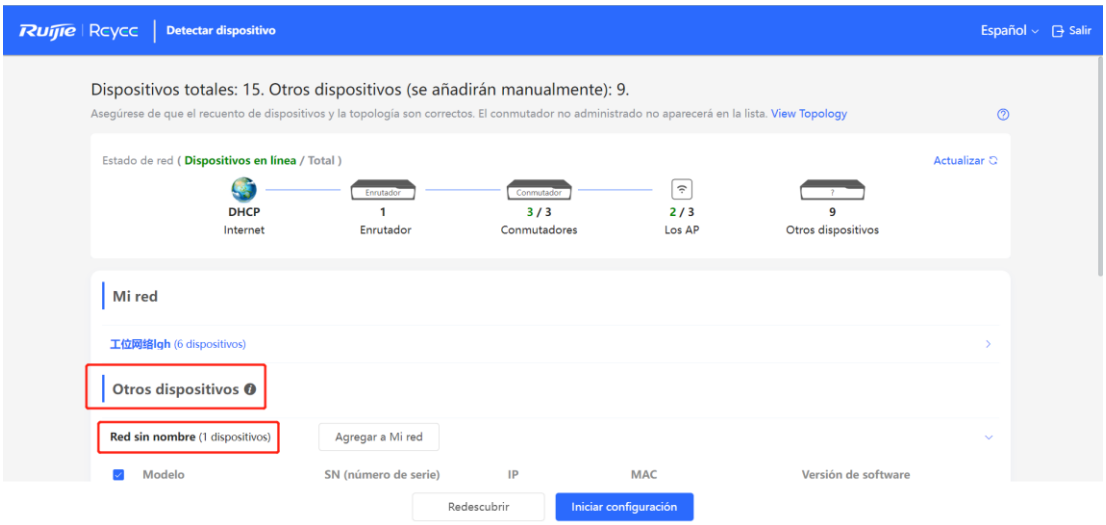
10.3 Añadir dispositivos conectados

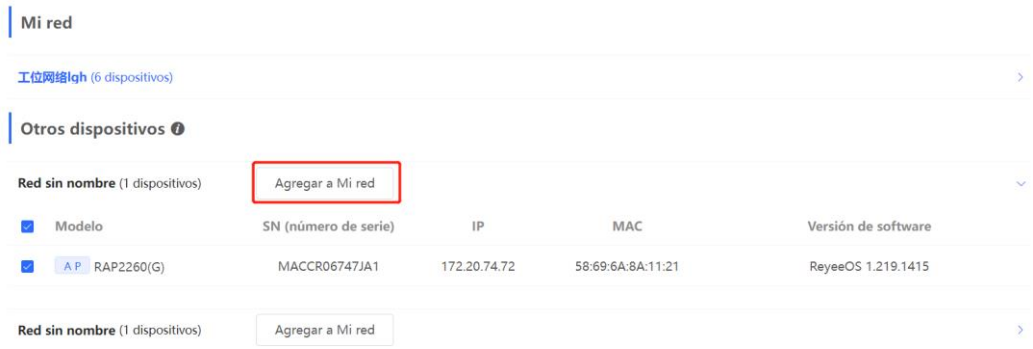
10.3.1 Conexión cableada

(1) Cuando un nuevo dispositivo se conecta a un dispositivo existente en la red, el sistema muestra el siguiente mensaje: “Se ha detectado un dispositivo que no pertenece a esta red” y también muestra el número de esos dispositivos en color naranja debajo de **Devices** en la esquina superior izquierda de la página **Descripción general**. Haga clic en **Gestionar** para añadir un dispositivo a la red actual.



(2) Cuando el sistema cambie a la página **Lista de dispositivos**, haga clic en **Otros dispositivos**. En **Otros dispositivos**, elija el dispositivo que añadirá a la red y haga clic en **Agregar a Mi red**.





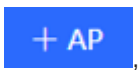
(3) No es necesario ingresar la contraseña si el dispositivo por añadir está recién entregado. Si el dispositivo ya tiene una contraseña, introdúzcala en el apartado correspondiente. Si la contraseña es incorrecta no podrá añadir el dispositivo.

10.3.2 AP Mesh

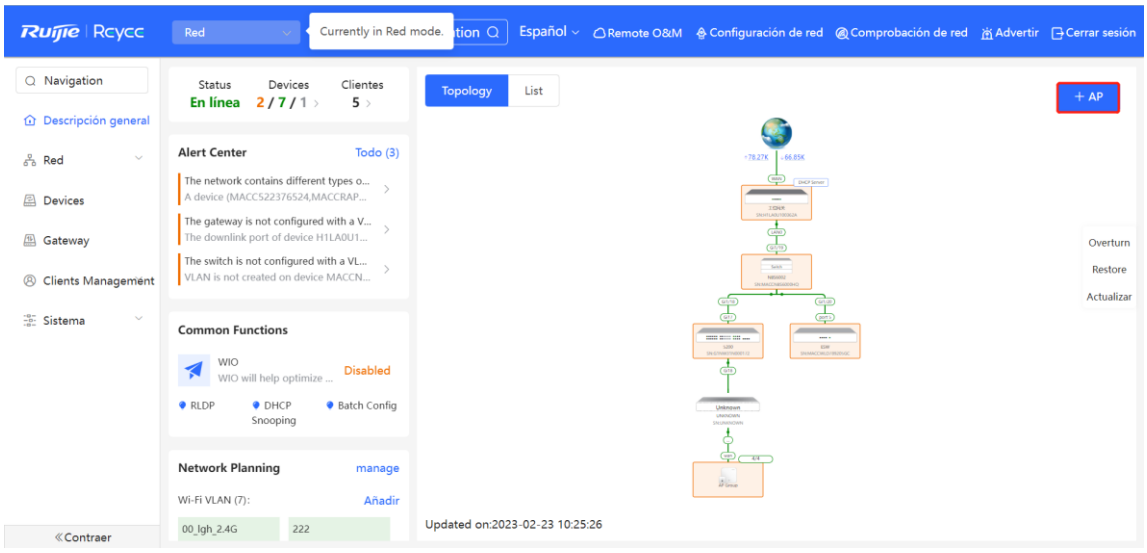
Si el punto de acceso o AP admite la función Reyee mesh, no es necesario conectar los cables después de encender el AP. El AP se puede añadir a la red actual en modo Reyee mesh, establecer una red mesh con otros dispositivos inalámbricos y sincronizar automáticamente la configuración del Wi-Fi.

Precaución

La función Reyee mesh debe estar habilitada en la red en vivo para que pueda buscar un AP. (Para más información, consulte 21.9 Habilitar la función Reyee Mesh.) En este caso, el AP debe encenderse cerca. Es posible que la búsqueda del AP falle si se encuentra alejado o hay obstáculos bloqueando la señal.

(1) Coloque el nuevo AP encendido cerca de un AP existente, donde el nuevo AP pueda recibir la señal de Wi-Fi del AP existente. Inicie sesión en un dispositivo de la red. En la página **Descripción general**, haga clic en 

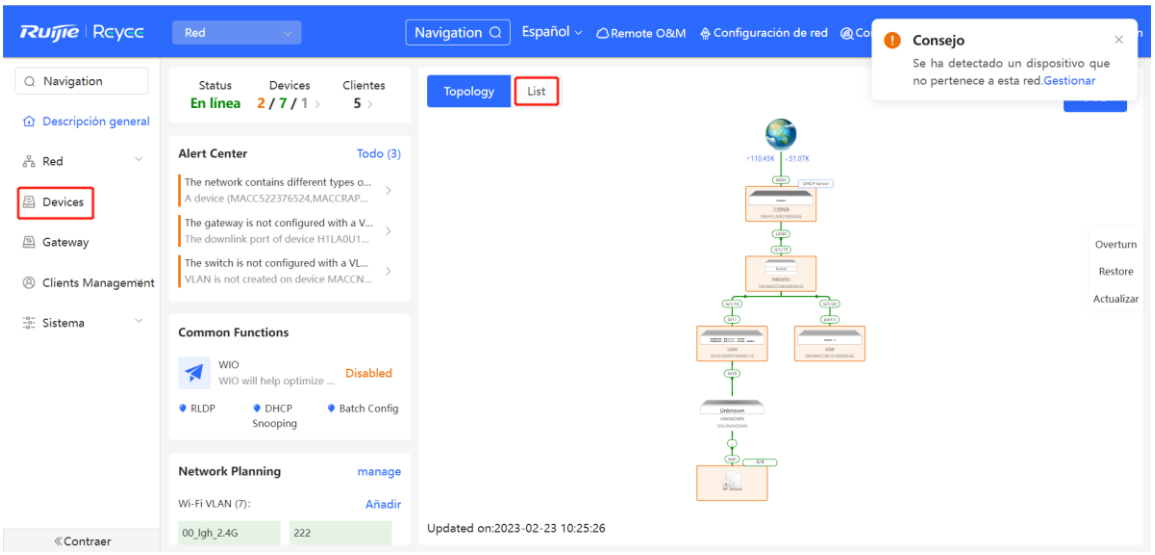
, en la esquina superior derecha de la topología, para escanear los AP cercanos que no pertenezcan a la red actual y que no estén conectados a un cable de red.

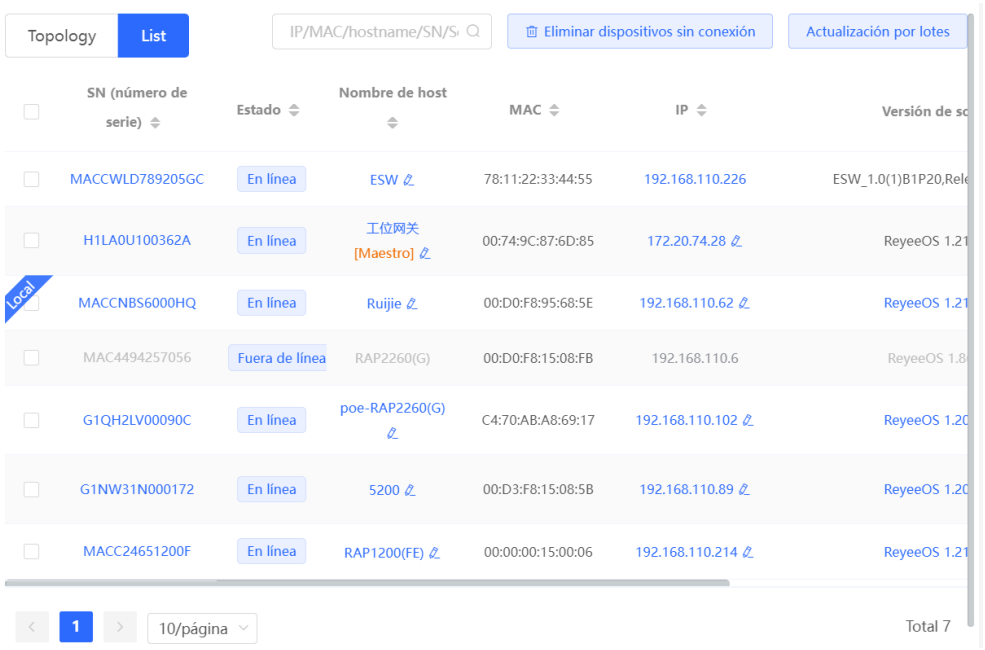


(2) Seleccione el AP objetivo para añadirlo a la red actual. No es necesario ingresar la contraseña si el dispositivo que añadirá es nuevo. Si el dispositivo ya tiene una contraseña, introduzca la contraseña de gestión del dispositivo.

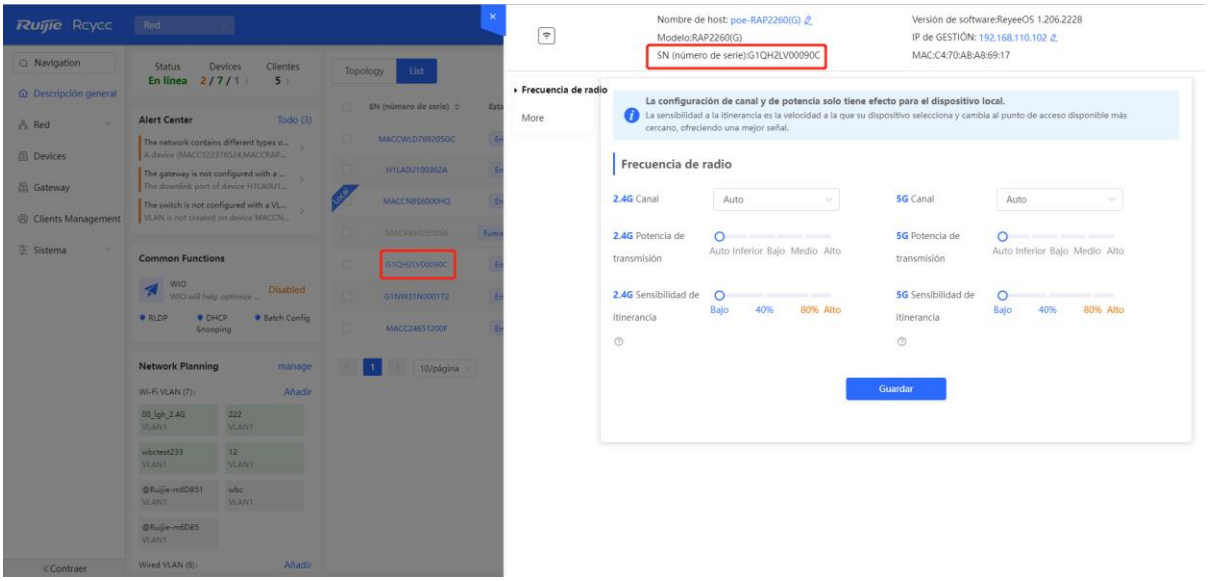
10.4 Administración de los dispositivos conectados

En la página **Descripción general**, haga clic en **List**, en la esquina superior izquierda de la topología, o haga clic en **Devices**, en la barra de menú, para cambiar a la lista de dispositivos. Ahora puede ver toda la información del dispositivo en la red activa. Solo debe iniciar sesión en uno de los dispositivos de la red para configurar y administrar el conjunto de dispositivos en ella.

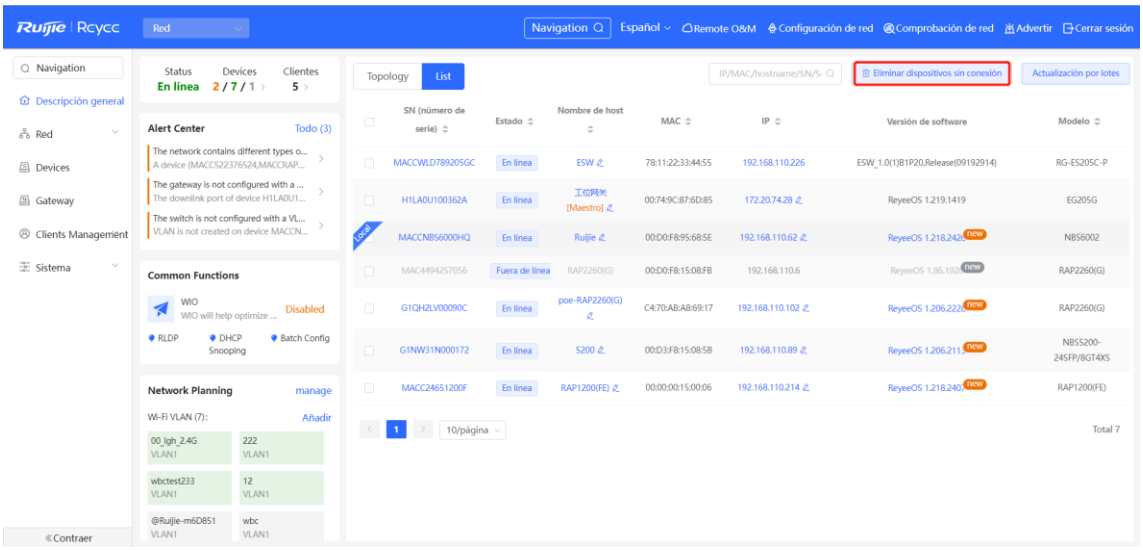




- Para configurar un dispositivo específico de forma separada, haga clic en el **SN** del dispositivo.

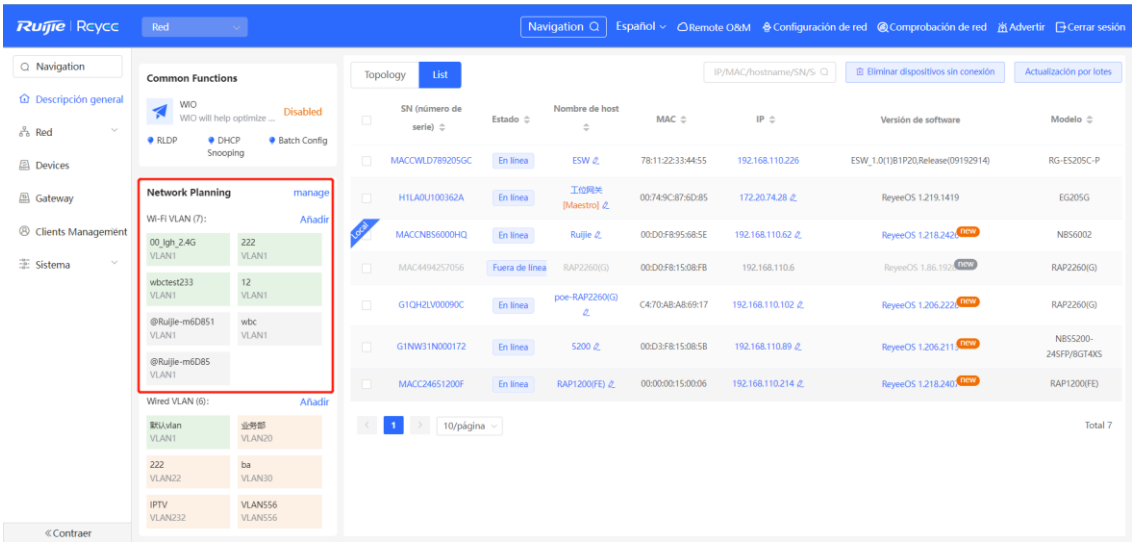


- Revise los dispositivos que se encuentran sin conexión y haga clic en **Eliminar dispositivos sin conexión** para quitarlos de la lista y de la topología de red.



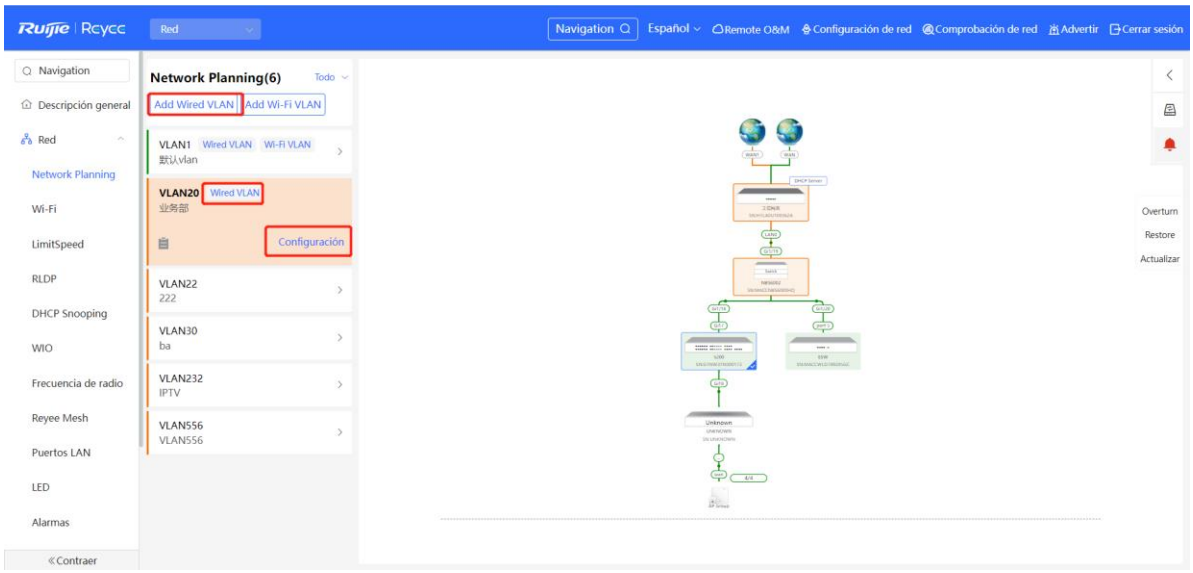
10.5 Configuración de la red de servicio

Las configuraciones de la red alámbrica e inalámbrica pertenecientes a la red actual se muestran en el lado inferior izquierdo de la página **Descripción general**. Haga clic en **manage** para cambiar a la página de la configuración de la red de servicio (o seleccione **Red** > **Network Planning**).

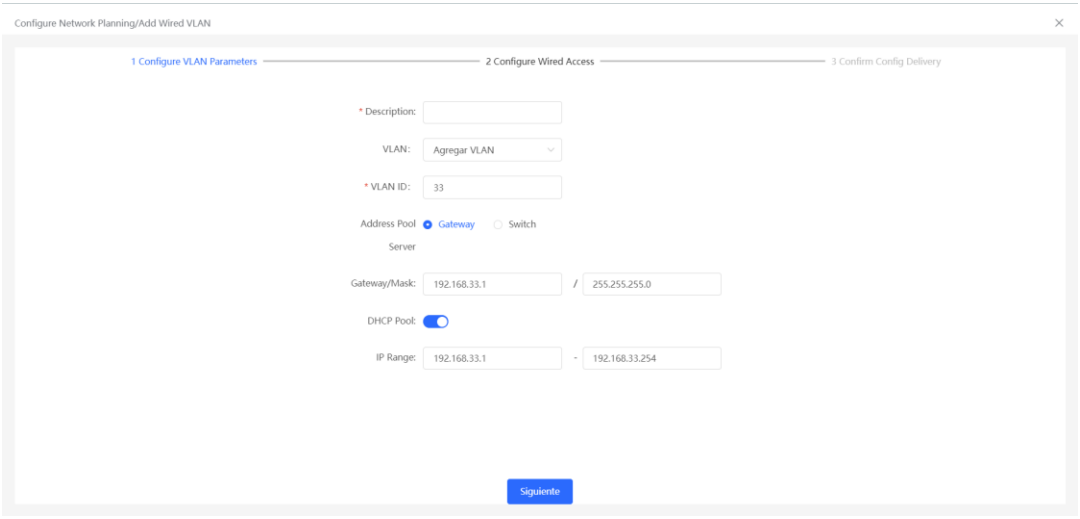


10.5.1 Configuración de la red alámbrica

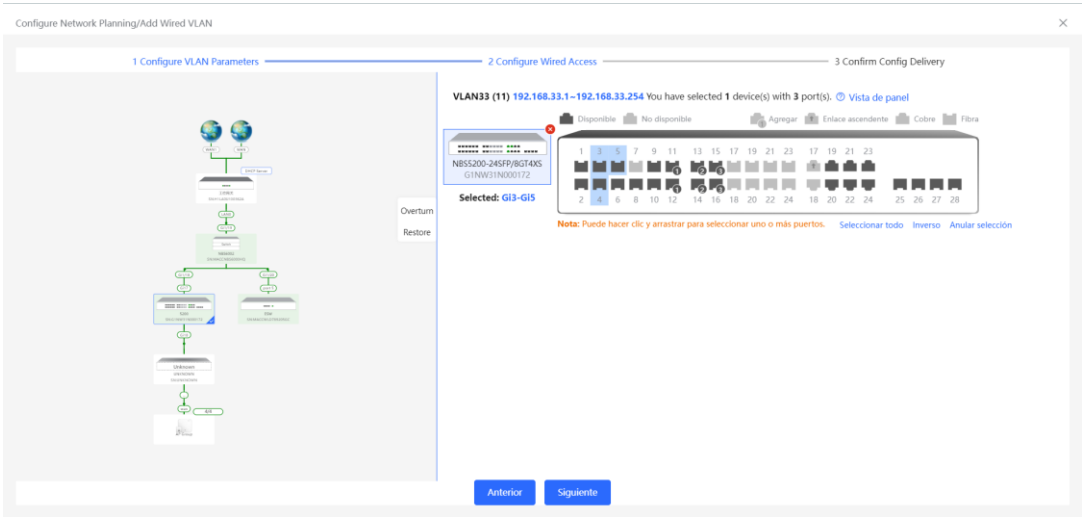
(1) Haga clic en **Add Wired VLAN** para añadir la configuración de la red alámbrica o seleccionar una VLAN cableada existente y haga clic en **Configuración** para modificarla.



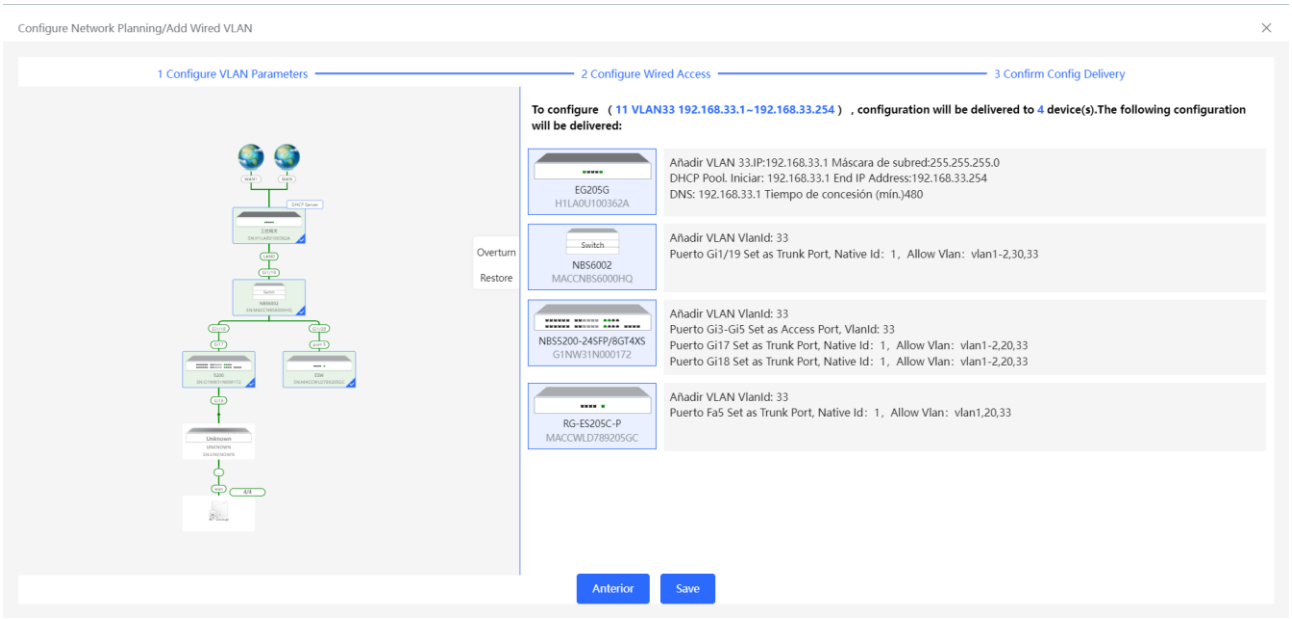
(2) Configure una VLAN cableada, especifique el servidor del grupo de direcciones para los clientes de acceso en la VLAN, y determine si debe crear un nuevo grupo de direcciones DHCP. Es posible seleccionar un switch o una puerta de enlace como el servidor de grupo de direcciones. Después de configurar los parámetros de servicio, haga clic en **Siguiente**.



(3) Seleccione el switch que desee configurar en la topología, seleccione los puertos del switch que se añadirán a la VLAN y haga clic en **Siguiente**.

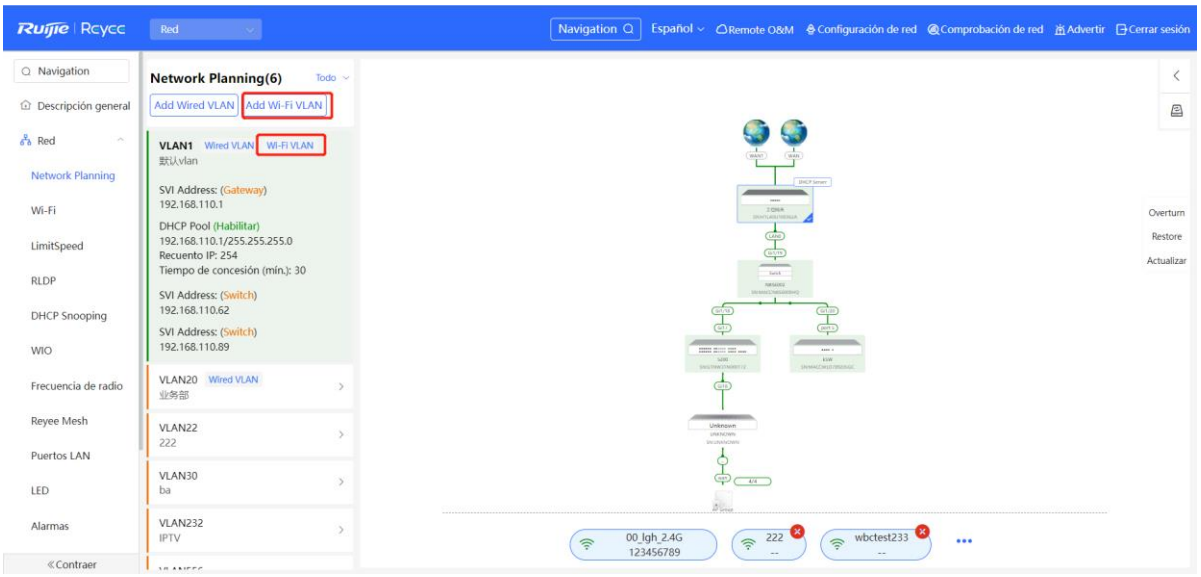


(4) Confirme que los elementos de la configuración que requiere sean correctos y luego haga clic en **Save**. Espere a que la configuración se haga efectiva.

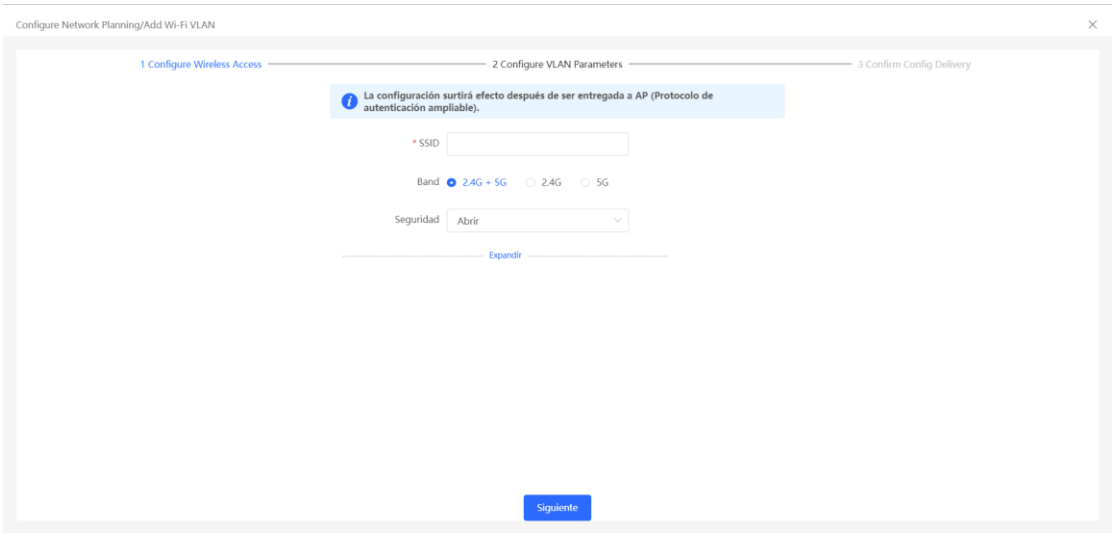


10.5.2 Configuración de la red inalámbrica

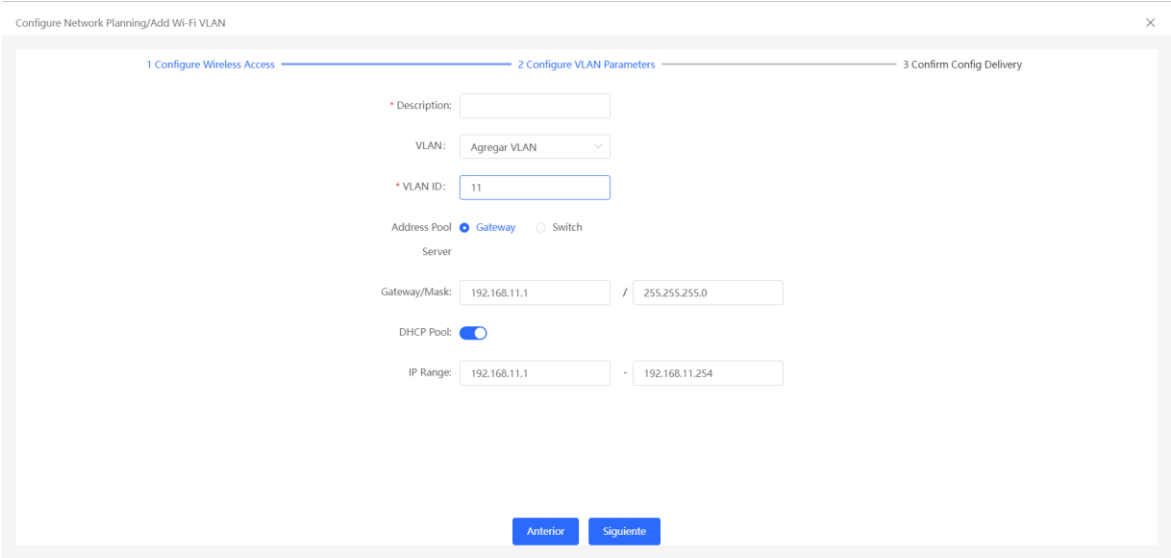
(1) Haga clic en **Add Wi-Fi VLAN** para añadir la configuración de la red inalámbrica, o seleccionar una VLAN de Wi-Fi existente, y haga clic en **Configuración** para modificarla.



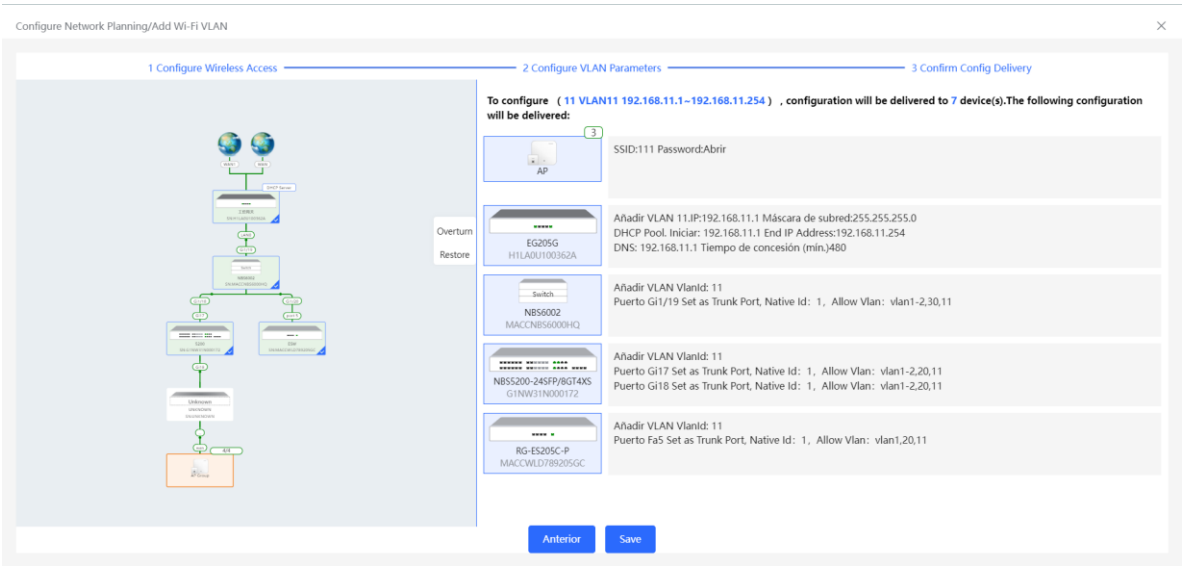
(2) Establezca el nombre y la contraseña de Wi-Fi, y la banda de frecuencia. Haga clic en **Siguiente**.



(3) Configure una VLAN para acceso inalámbrico, especifique el servidor del grupo de direcciones para los clientes de acceso en la VLAN, y determine si debe crear un nuevo grupo de direcciones DHCP. Es posible seleccionar un switch o una puerta de enlace como el servidor de grupo de direcciones. Después de configurar los parámetros de servicio, haga clic en **Siguiente**.



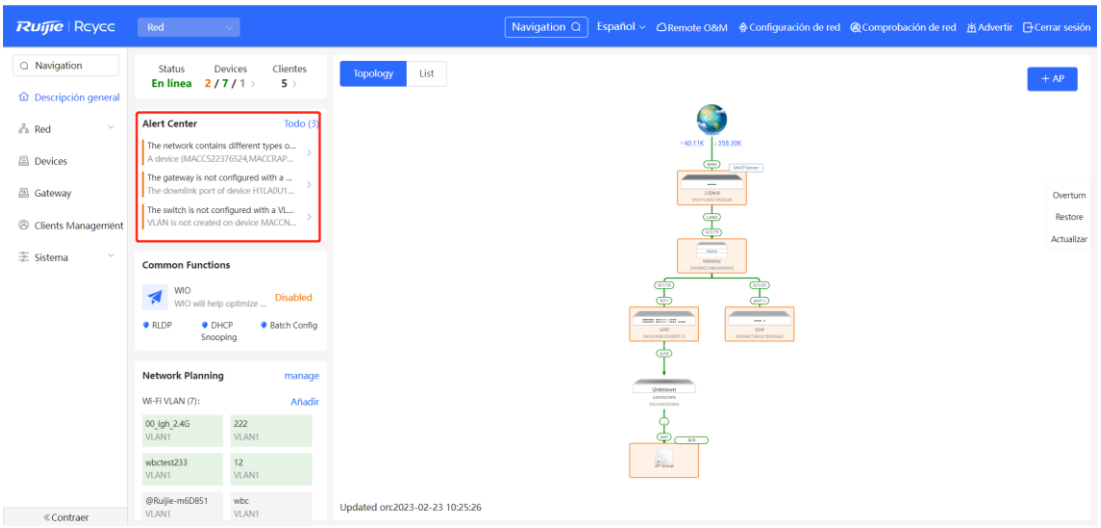
(4) Confirme que los elementos de la configuración que requiere sean correctos y luego, haga clic en **Save**. Espere a que la configuración se haga efectiva.

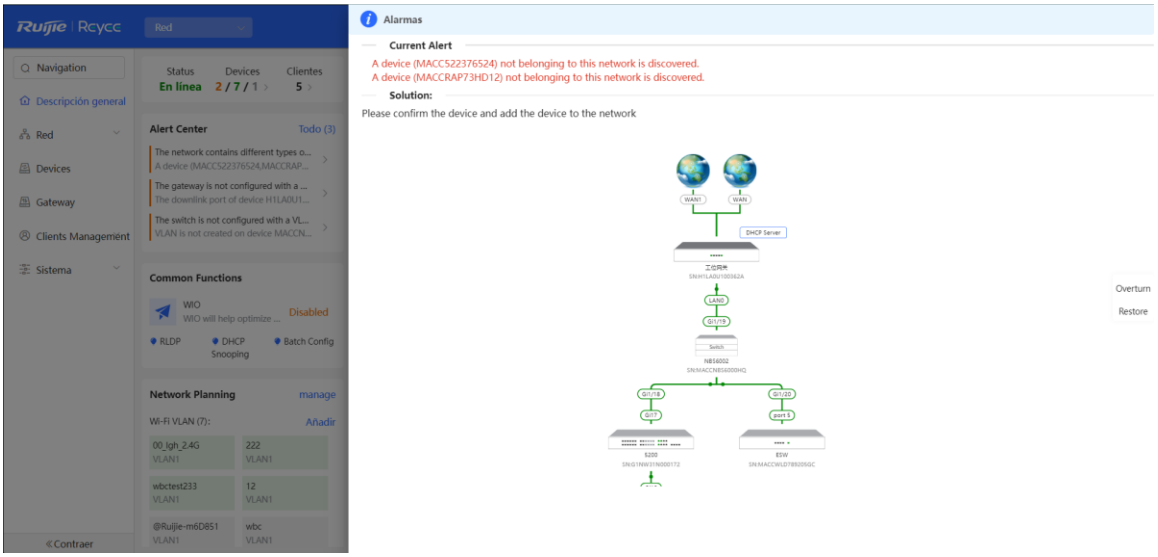


10.6 Procesamiento de alarmas

Seleccione **Red** > **Descripción general**.

Si existe una excepción en la red, en la página **Descripción general** se mostrará una alerta relativa a esta excepción y su solución correspondiente. Haga clic en **Alert Center** para visualizar el dispositivo con fallas, los detalles del problema y su solución. Resuelva y aborde el problema de acuerdo con la solución correspondiente.

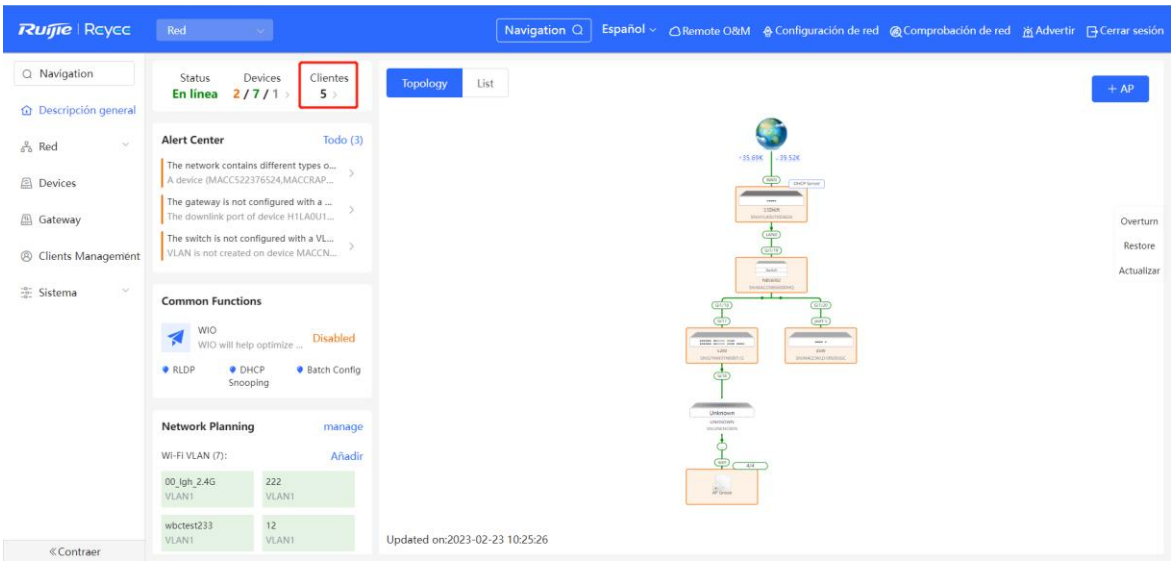




10.7 Visualización de los clientes en línea

El apartado **Clientes** que se muestra en la esquina superior izquierda de la página **Descripción general**, muestra el total de clientes que se encuentran en línea en la red activa. Si mueve el cursor al número de clientes, se mostrará el número de ellos con acceso cableado y los de acceso inalámbrico en las bandas de 2.4 GHz y 5 GHz.

Haga clic para cambiar a la página de clientes en línea (o seleccione **Clientes** > **Clientes en línea**).



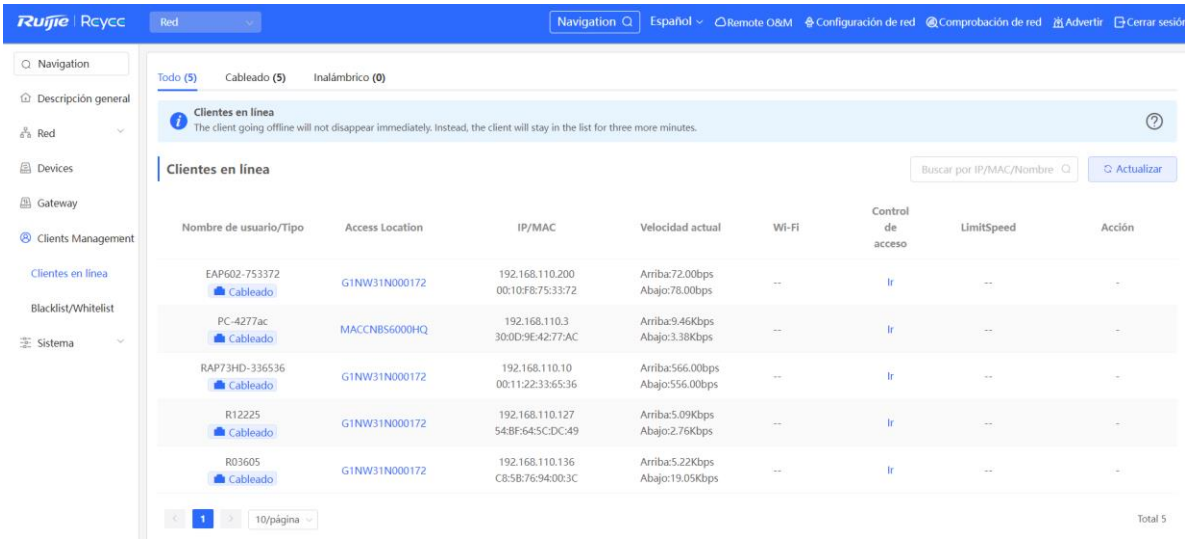


Tabla 10-1 Descripción de la información de los clientes en línea

Campo	Descripción
Nombre de usuario/Tipo	Nombre y tipo de acceso del cliente. El tipo de acceso puede ser cableado o inalámbrico.
Ubicación de acceso	SN del dispositivo conectado a un cliente. Haga clic en él para visualizar el puerto de acceso durante la conexión cableada.
IP/MAC	Dirección IP y dirección MAC del cliente.
Velocidad de la corriente	Velocidades de transmisión de datos de los enlaces ascendentes y descendentes del cliente.
Wi-Fi	Información de la red inalámbrica asociada a los clientes conectados, incluyendo el

Campo	Descripción
	canal, la intensidad de la señal, el tiempo en línea y la velocidad de negociación.

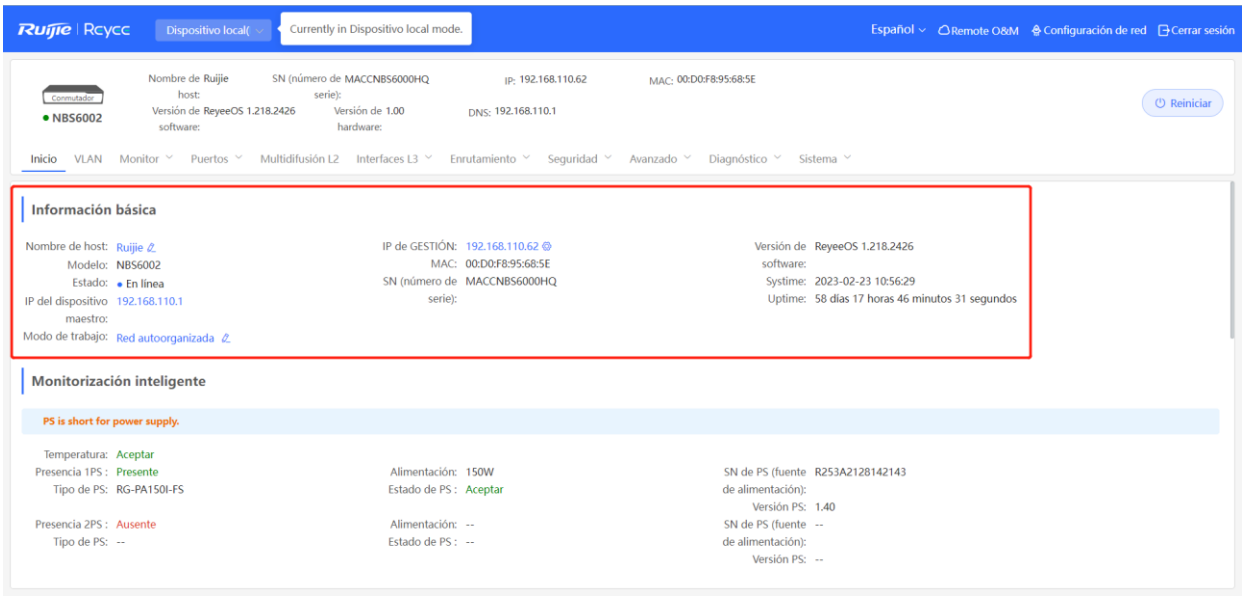
11 Gestión básica de los switches de las series NBS y NIS

11.1 Descripción general

11.1.1 Información básica sobre el dispositivo

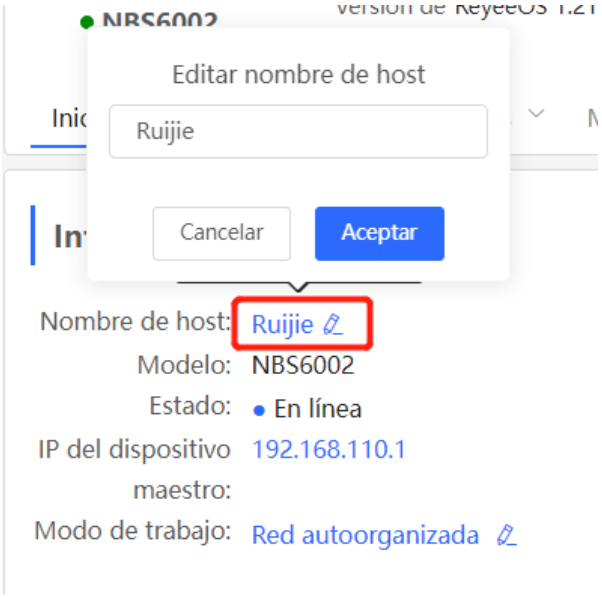
Seleccione **Dispositivo local** > **Inicio** > **Información básica**.

La información básica incluye el nombre del dispositivo, el modelo del dispositivo, el número de serie, la versión de software, la IP de gestión, la dirección MAC, el estado de la red, la hora del sistema, el modo de trabajo, el estado de la fuente de alimentación, etc.



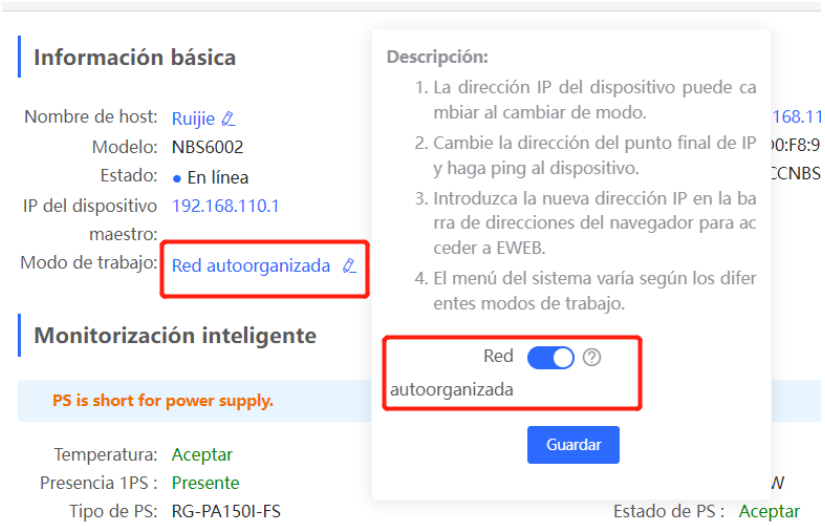
1. Configurar el nombre del dispositivo

Haga clic en nombre del dispositivo para modificarlo y distinguirlo de otros dispositivos.



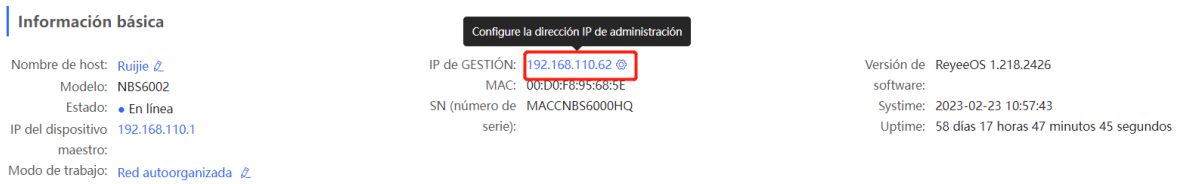
2. Cambiar el modo de trabajo

Haga clic en el modo de trabajo actual para cambiarlo.



3. Configurar la dirección IP de administración

Haga clic en la dirección IP de gestión para cambiar a la página de configuración de esta. Para más información, consulte 12.6 Configuración de la dirección IP de gestión



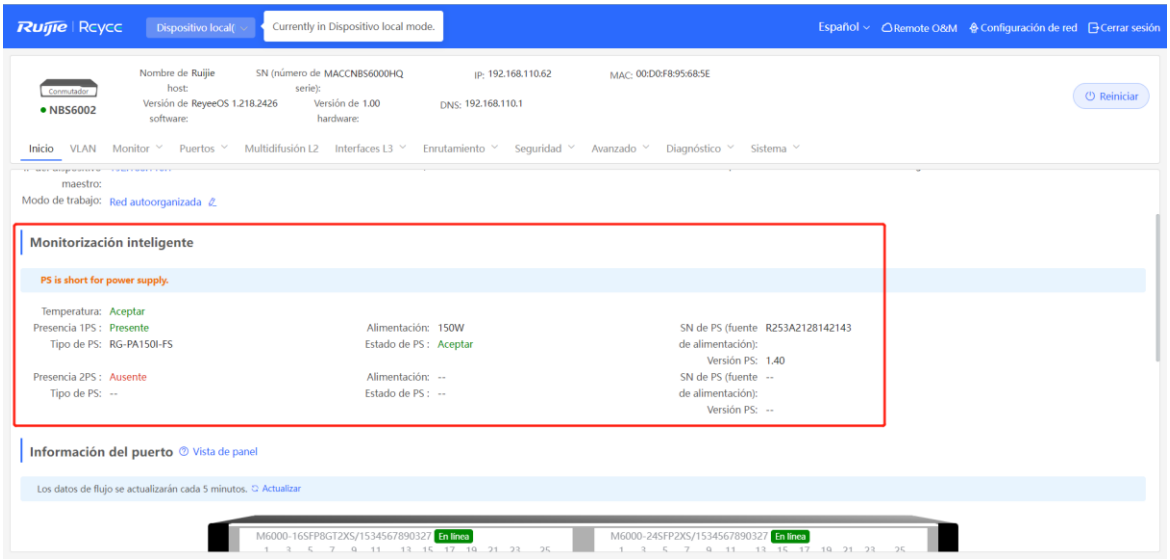
11.1.2 Información sobre el monitoreo del hardware

Precaución

Solo las series RG-NBS6002, RG-NBS7003 y RG-NBS7006 pueden mostrar este tipo de información.

Seleccione **Dispositivo local** > **Inicio** > **Monitorización inteligente**.

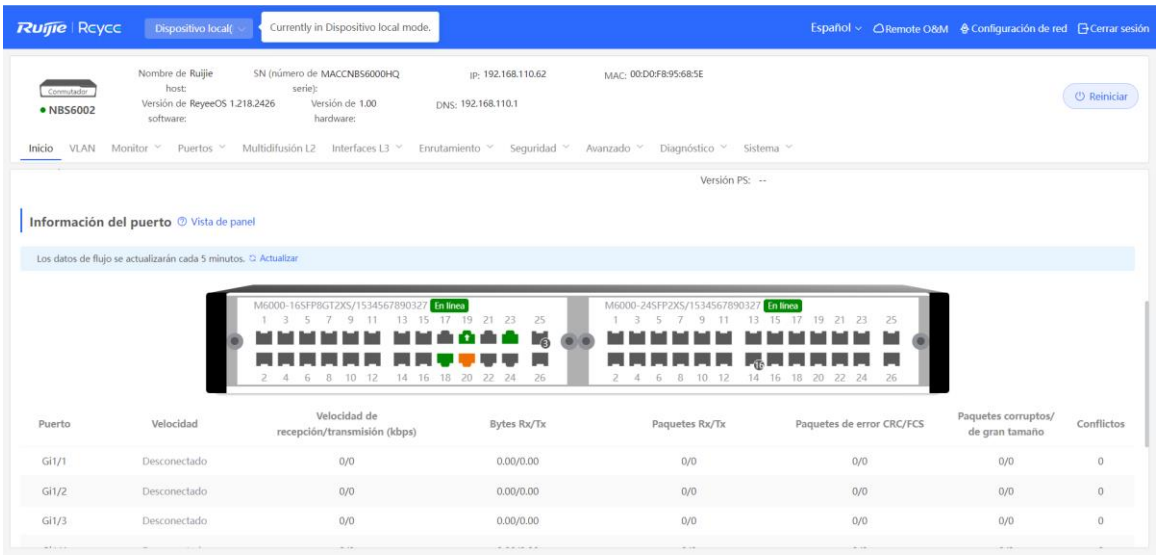
Se muestra el estado de trabajo actual del hardware del dispositivo, como la temperatura y el estado de la fuente de alimentación.

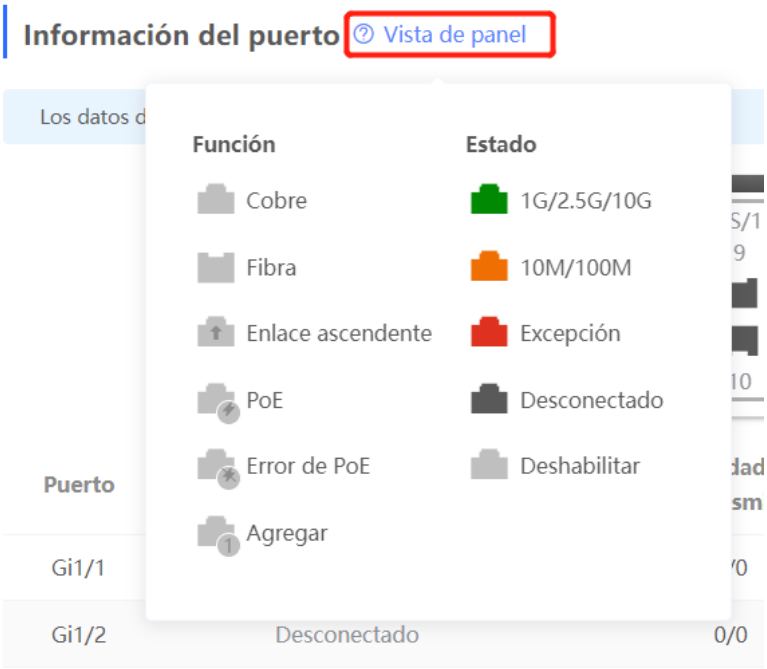


11.1.3 Información del puerto

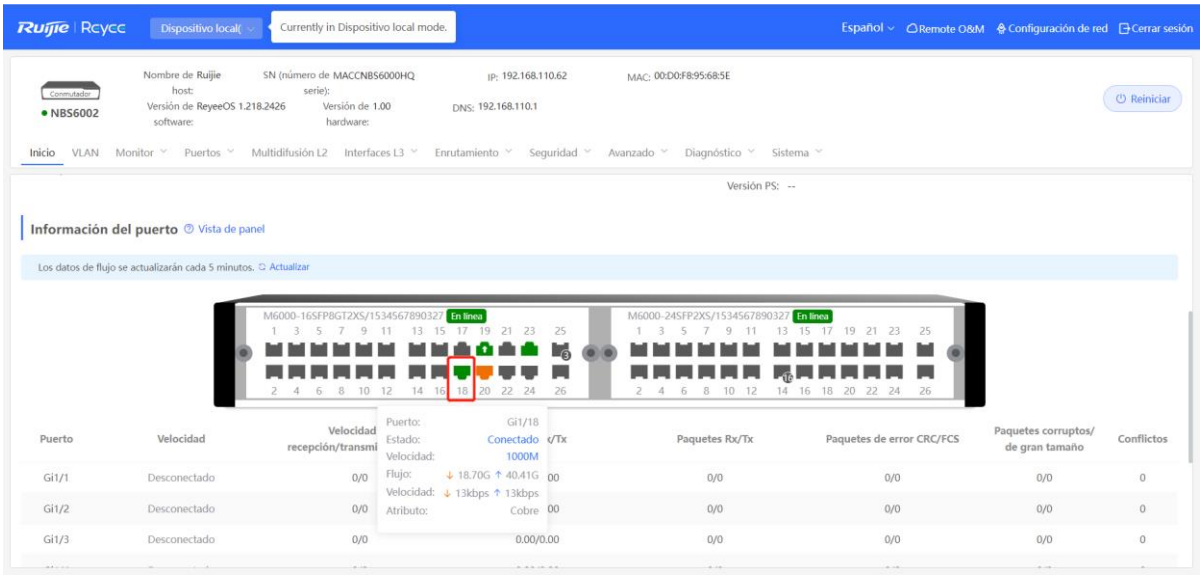
Seleccione **Dispositivo local** > **Inicio** > **Información del puerto**.

- La página de información del puerto muestra los detalles de todos los puertos en el conmutador. Haga clic en **Vista de panel** para visualizar las funciones de los puertos y los estados correspondientes a los íconos del puerto, de acuerdo con su color y forma.

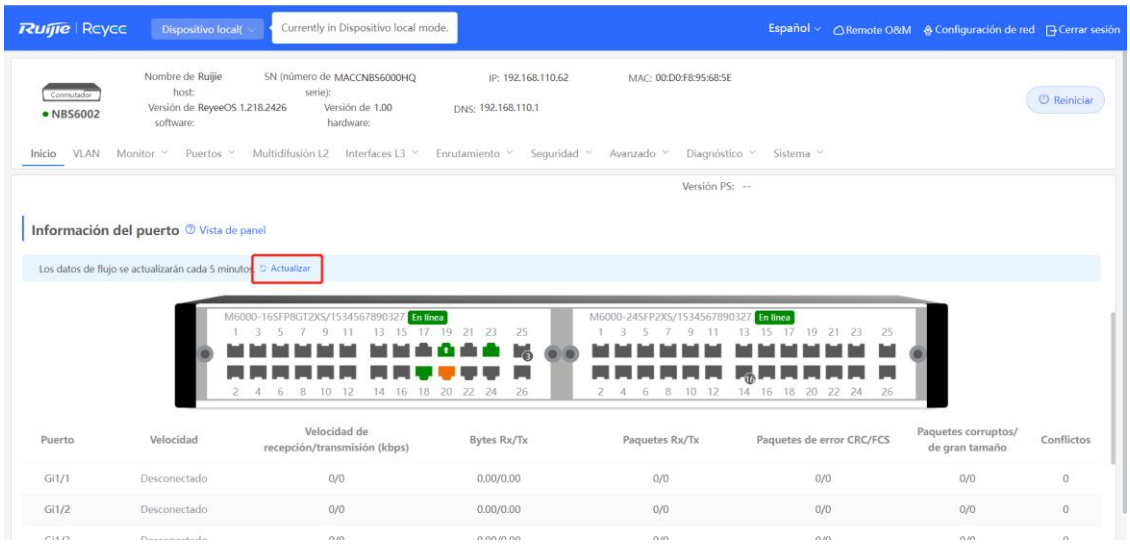




- Mueva el cursor al ícono del puerto (por ejemplo, Gi14) en el panel del puerto. Se mostrará más información acerca del puerto, como el identificador de puerto, su estado y velocidad, el tráfico de enlace ascendente y descendente, la velocidad de transmisión y su atributo óptico o eléctrico.



- El tráfico de datos de actualiza automáticamente cada 5 minutos. Haga clic en **Actualizar**, sobre el panel del puerto, para obtener la información más reciente del tráfico del puerto y su estado de forma simultánea.



11.2 Estadísticas de flujo del puerto

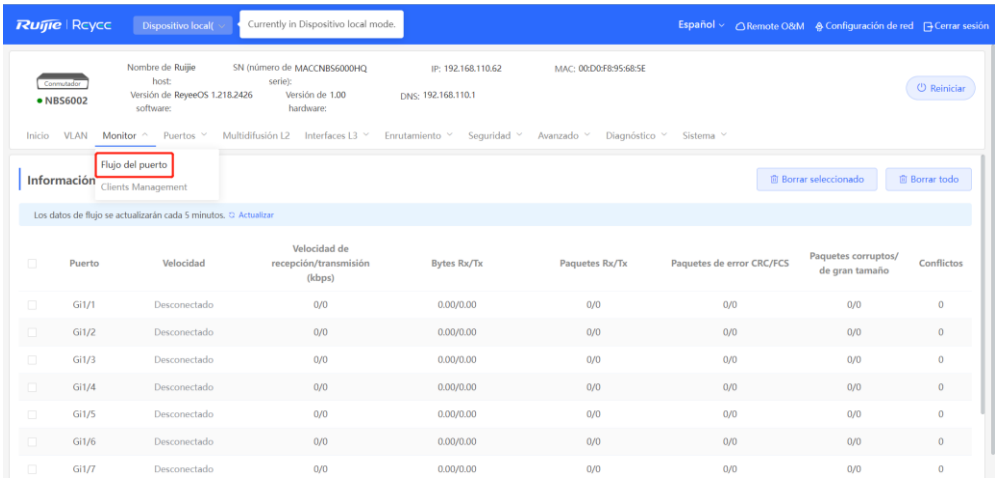
Seleccione **Dispositivo local** > **Monitor** > **Flujo del puerto**.

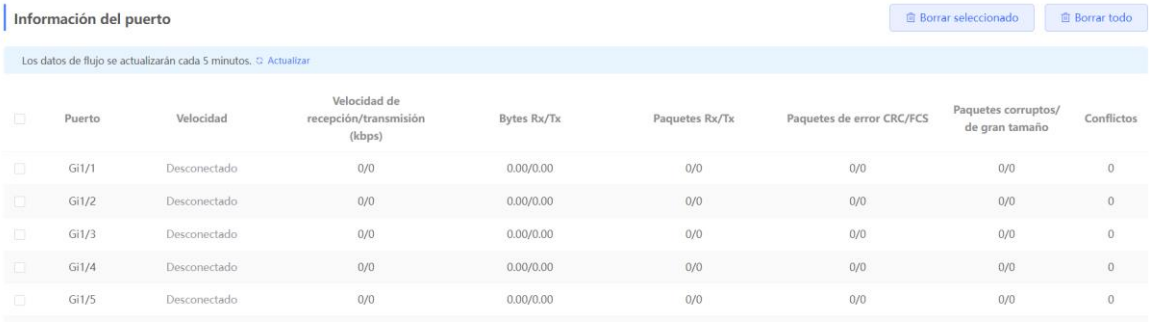
Se mostrará las estadísticas de tráfico, como la velocidad del puerto del dispositivo, el número de paquetes enviados y recibidos, y el número de paquetes con errores. La velocidad del puerto se actualiza cada 5 segundos. Otras estadísticas del tráfico se actualizan cada 5 minutos.

Seleccione el puerto y haga clic en **Borrar seleccionado** o en **Borrar todo** para eliminar las estadísticas, tales como el tráfico del puerto actual, para que comience a reunir la información nuevamente.

Nota

Los puertos agregados se pueden configurar. El tráfico de un puerto agregado es la suma del tráfico de todos los puertos miembros.





11.3 Gestión de direcciones MAC

11.3.1 Descripción general

La tabla de direcciones MAC registra los mapeos de las direcciones MAC y los puertos a las VLAN.

El dispositivo consulta la tabla de direcciones MAC con base en la dirección MAC de destino de un paquete recibido. Si el dispositivo encuentra una entrada consistente con la dirección MAC de destino en el paquete, este lo reenvía a través de la interfaz correspondiente a la entrada en modo unidifusión. Si el dispositivo no encuentra dicha entrada, reenvía el paquete a través de todas las interfaces, excepto la de recepción, en modo difusión.

Los tipos de entrada de dirección MAC se clasifican en:

- Entradas de direcciones MAC estáticas: se configuran manualmente. Los paquetes cuya dirección MAC de destino coincida con una de dichas entradas se reenvían a través de la interfaz correspondiente. Este tipo de entradas no envejece.
- Entradas de direcciones MAC dinámicas: se generan de manera dinámica por el conmutador. Los paquetes cuya dirección MAC de destino coincida con una de dichas entradas se reenvían a través de la interfaz correspondiente. Este tipo de entradas envejecen.
- Entradas de direcciones MAC filtradas: se configuran manualmente. Los paquetes cuya dirección MAC de origen o destino coincida con una de dichas entradas se descartan. Este tipo de entradas no envejece.

Nota

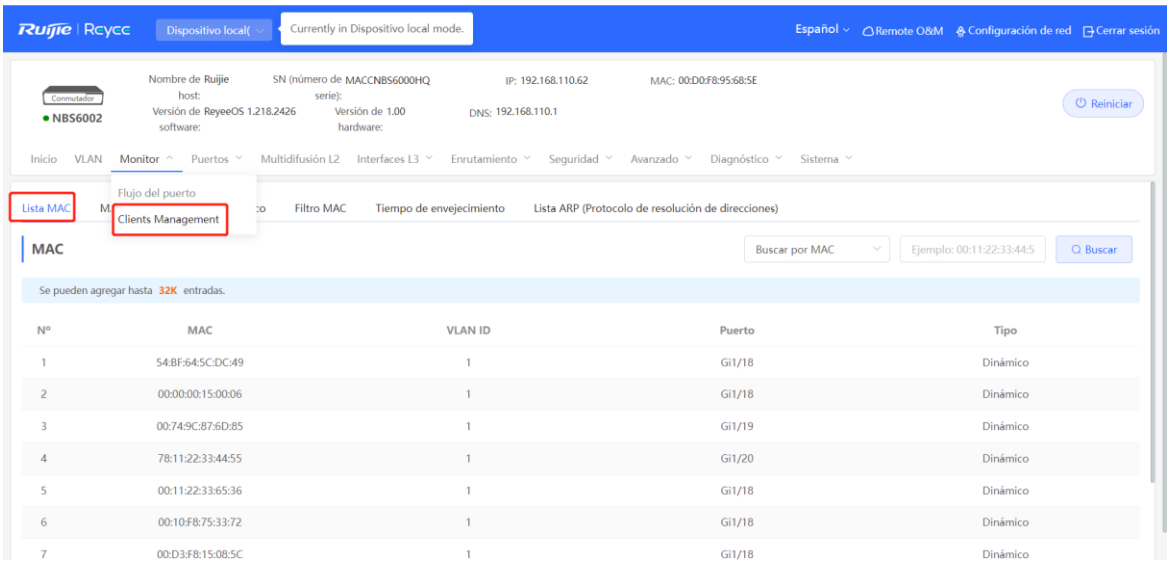
Esta sección describe la gestión de las entradas de direcciones MAC estáticas, dinámicas y filtradas, sin incluir las de multidifusión.

11.3.2 Visualización de la tabla de direcciones MAC

Seleccione **Dispositivo local** > **Monitor** > **Clients Management** > **Lista MAC**.

Esta sección muestra la información de la dirección MAC del dispositivo, incluyendo la dirección MAC estática configurada manualmente, la dirección MAC filtrada y la dirección MAC dinámica aprendida automáticamente por el dispositivo.

Consulta de entradas de direcciones MAC dinámicas: las entradas de direcciones MAC pueden consultarse con base en la dirección MAC, la VLAN ID o el número del puerto. Seleccione el tipo de búsqueda, ingrese la cadena de caracteres y haga clic en **Buscar**. La entradas MAC que coinciden con el criterio de búsqueda se muestran en la lista. También son compatibles con la búsqueda difusa.



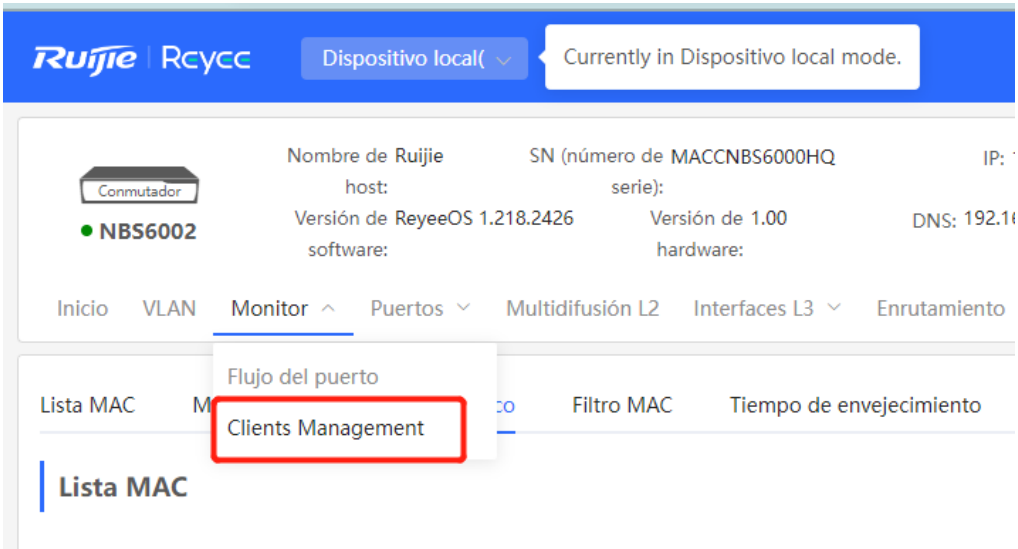
Nota

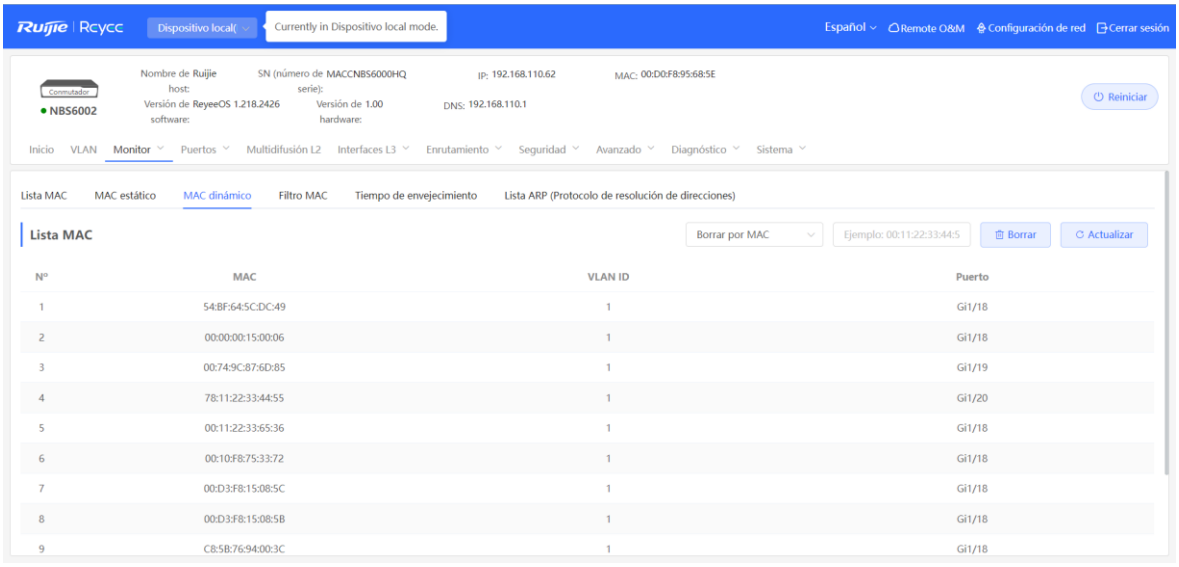
La capacidad de entrada de una dirección MAC depende del producto. Por ejemplo, la capacidad de la entrada de una dirección MAC en el dispositivo del ejemplo anterior es de 32K.

11.3.3 Visualización de las direcciones MAC dinámicas

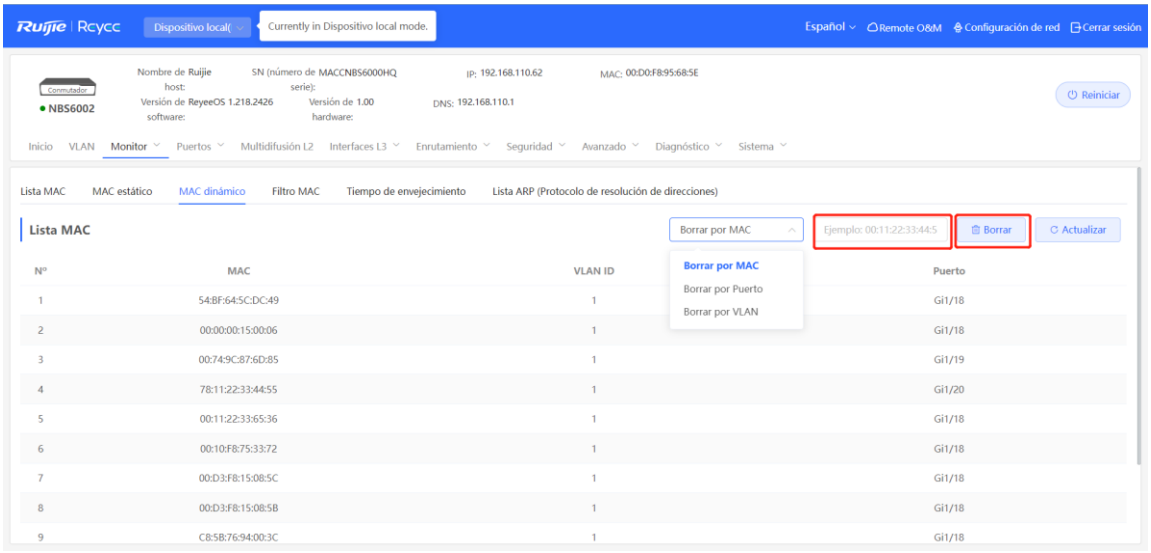
Seleccione **Dispositivo local** > **Monitor** > **Clients Management** > **MAC dinámico**.

Después de recibir un paquete, el dispositivo generará automáticamente entradas de direcciones MAC dinámicas con base en su dirección MAC de origen. Esta página muestra las entradas de direcciones MAC dinámicas aprendidas por el dispositivo. Haga clic en **Actualizar** para obtener las entradas de direcciones MAC dinámicas más recientes.



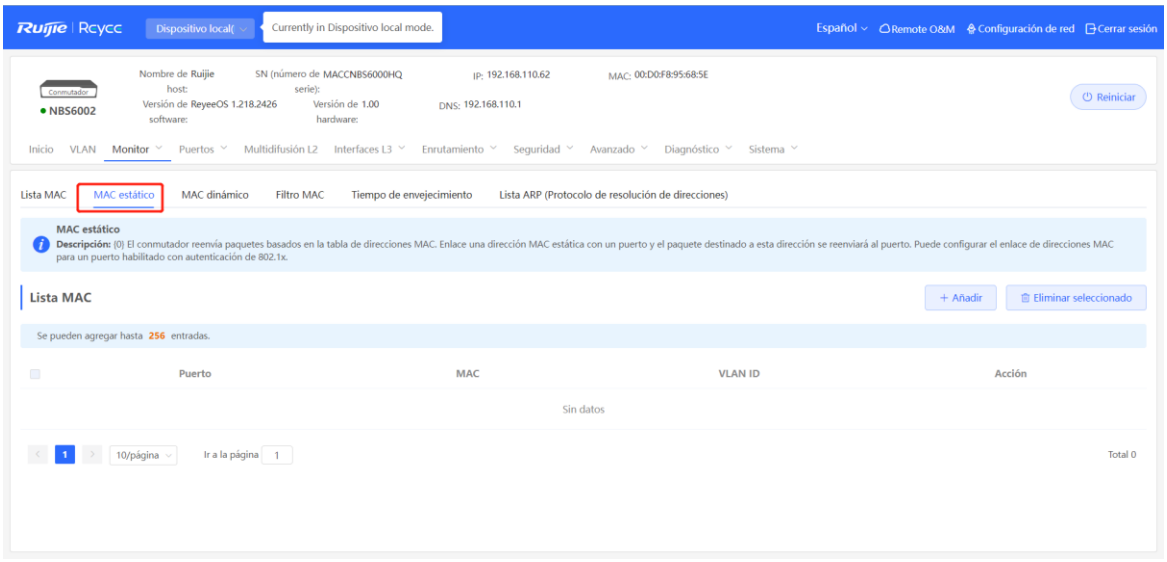


Seleccione el modo de eliminación (**Borrar por MAC**, **Borrar por Puerto** o **Borrar por VLAN**), ingrese la cadena de caracteres que coincida con la entrada de la dirección MAC dinámica y haga clic en **Borrar**. El dispositivo borrará las entradas de las direcciones MAC que coincidan con el criterio de búsqueda.



11.3.4 Configuración del enlace de direcciones MAC estáticas

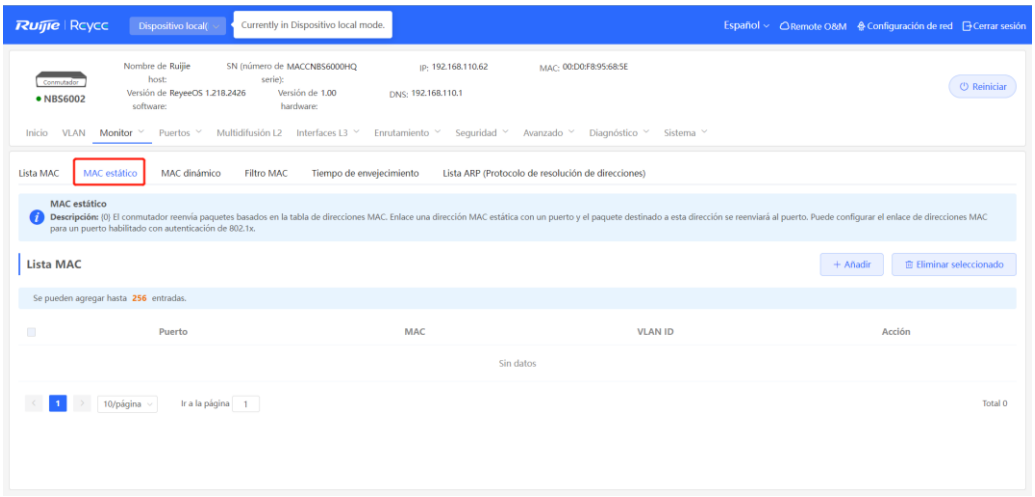
El conmutador reenvía datos con base en la tabla de direcciones MAC. Se puede vincular manualmente la dirección MAC de un dispositivo de red de enlace descendente a una interfaz del conmutador en una entrada de dirección MAC estática. Cuando el dispositivo recibe un paquete destinado a esta dirección MAC estática de una VLAN, el conmutador reenvía el paquete a la interfaz especificada. Por ejemplo, cuando la autenticación 802.1x se habilita en la interfaz, se puede configurar el enlace de la dirección MAC estática sin autenticación.

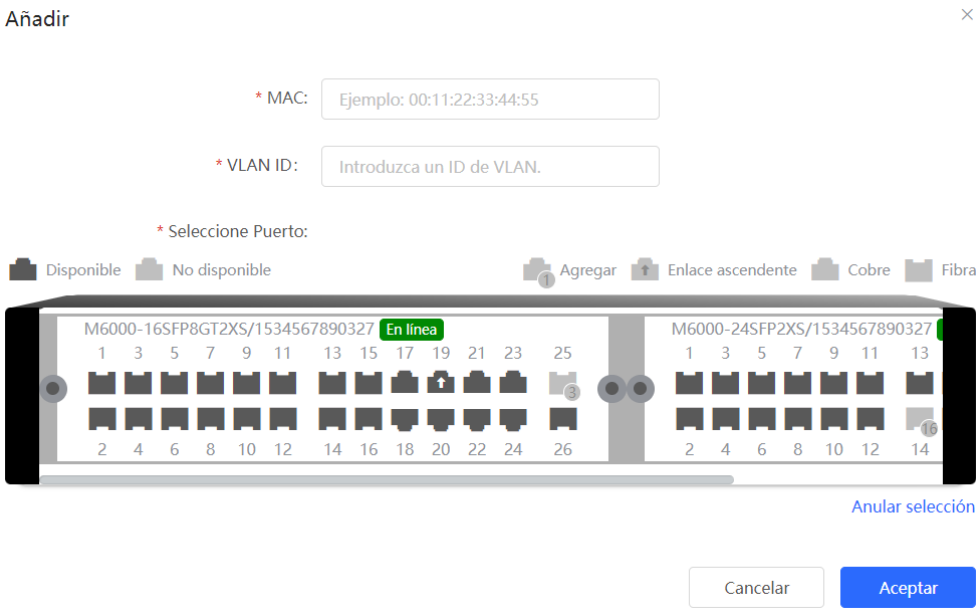


1. Añadir entradas de direcciones MAC estáticas

Seleccione **Dispositivo local** > **Monitor** > **Clients Management** > **MAC estático**.

Haga clic en **Añadir**, ingrese la dirección MAC y la VLAN ID, seleccione el puerto al que se reenviará el paquete y haga clic en **Aceptar**. Después de añadir la entrada de la dirección MAC correctamente, la tabla de direcciones MAC se actualizará.



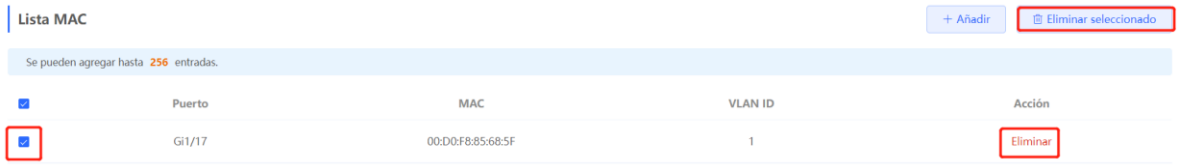


2. Eliminación de las entradas de direcciones MAC estáticas

Seleccione **Dispositivo local** > **Monitor** > **Clients Management** > **MAC estático**.

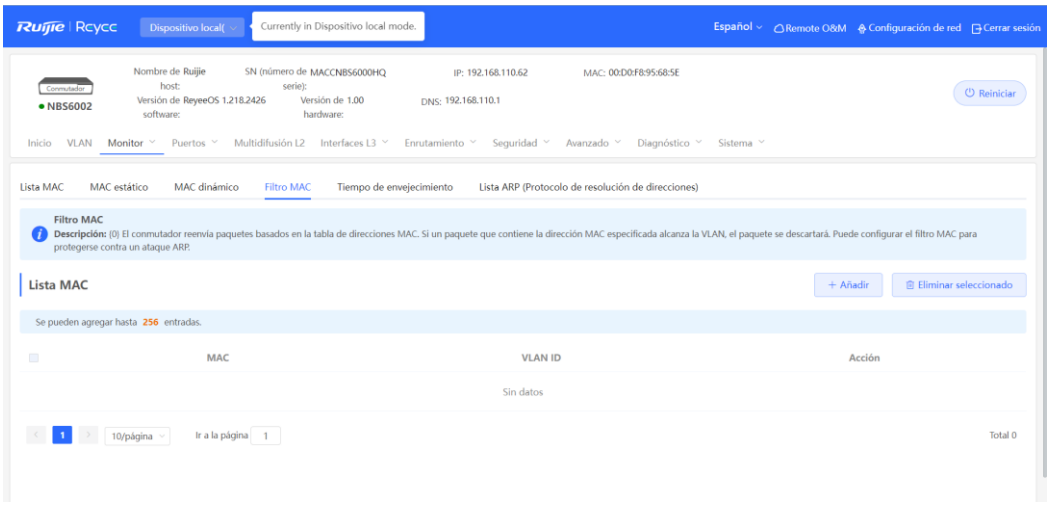
Eliminación por lotes: en **Lista MAC**, seleccione las entradas de las direcciones MAC a eliminar y haga clic en **Eliminar seleccionado**. En el cuadro de diálogo que aparece, haga clic en **Aceptar**.

Eliminación individual: en **Lista MAC**, busque la entrada a eliminar y haga clic en el botón **Borrar** de la última columna llamada **Acción**. En el cuadro de diálogo que aparece, haga clic en **Aceptar**.



11.3.5 Configuración del filtro de direcciones MAC

Para evitar que un host envíe o reciba paquetes en situaciones específicas, se puede añadir la dirección MAC del host a una entrada de dirección MAC filtrada. Cuando la entrada quede configurada, los paquetes cuya dirección MAC de origen o destino coincida con la entrada de la dirección MAC filtrada se descartarán directamente. Por ejemplo, si un usuario comienza a llevar a cabo ataques ARP, la dirección MAC del usuario se puede configurar como una dirección a ser filtrada para prevenirlos.



1. Añadir filtro de direcciones MAC

Seleccione **Dispositivo local** > **Monitor** > **Clients Management** > **Filtro MAC**.

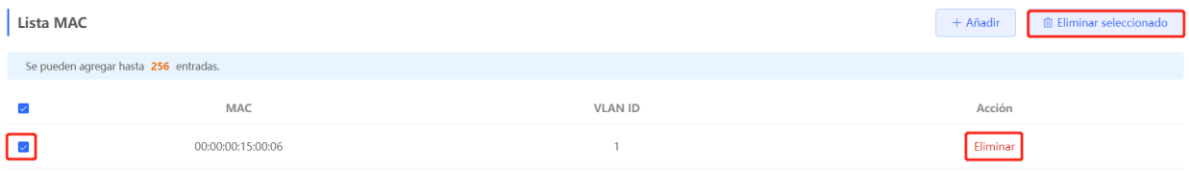
Haga clic en **Añadir**. En el cuadro de diálogo que aparece, ingrese la dirección MAC y la VILAN ID, y luego haga clic en **Aceptar**.

2. Eliminación de las entradas de direcciones MAC

Seleccione **Dispositivo local** > **Monitor** > **Clients Management** > **Filtro MAC**.

Eliminación por lotes: en **Lista MAC**, seleccione las entradas de las direcciones MAC a eliminar y haga clic en **Eliminar seleccionado**. En el cuadro de diálogo que aparece, haga clic en **Aceptar**.

Eliminación individual: en **Lista MAC**, busque la entrada a eliminar y haga clic en el botón **Eliminar** de la última columna llamada **Acción**. En el cuadro de diálogo que aparece, haga clic en **Aceptar**.



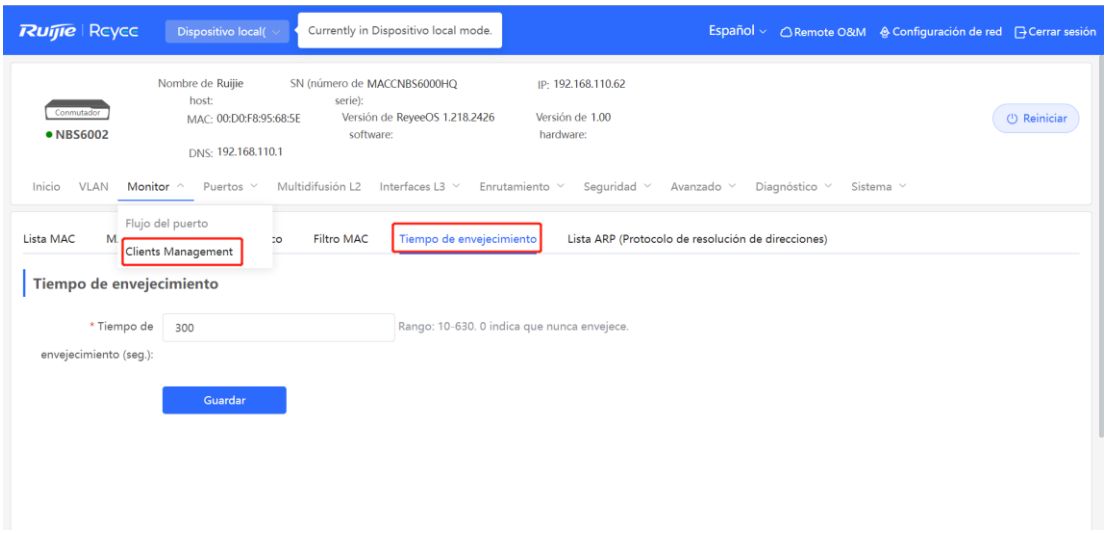
11.3.6 Configuración del tiempo de envejecimiento de la dirección MAC

El tiempo de envejecimiento de las entradas de direcciones MAC dinámicas que el dispositivo aprende, se puede configurar. Las entradas de direcciones MAC estáticas y las entradas filtradas no envejecen.

El dispositivo borra las entradas de direcciones MAC dinámicas no usadas, con base en el tiempo de envejecimiento, para optimizar sus recursos de entrada. Si el tiempo de envejecimiento es muy largo, puede ocasionar que las entradas inútiles no sean borradas a tiempo. Sin embargo, un tiempo de envejecimiento corto puede llevar a la eliminación de entradas válidas y un aprendizaje recurrente de direcciones MAC por parte del dispositivo, lo que incrementa la frecuencia de los paquetes de difusión. Por lo tanto, se recomienda configurar el tiempo de envejecimiento adecuado de las entradas de direcciones MAC, según se requiera, para ahorrar recursos en el dispositivo sin afectar la estabilidad de la red.

Seleccione **Dispositivo local** > **Monitor** > **Clients Management** > **Tiempo de envejecimiento**.

Ingrese un tiempo de envejecimiento válido y haga clic en **Guardar**. El rango de tiempo de envejecimiento es de 10 a 630 segundos. El valor 0 indica que las entradas de las direcciones MAC no envejecen.



11.4 Visualización de la información del ARP

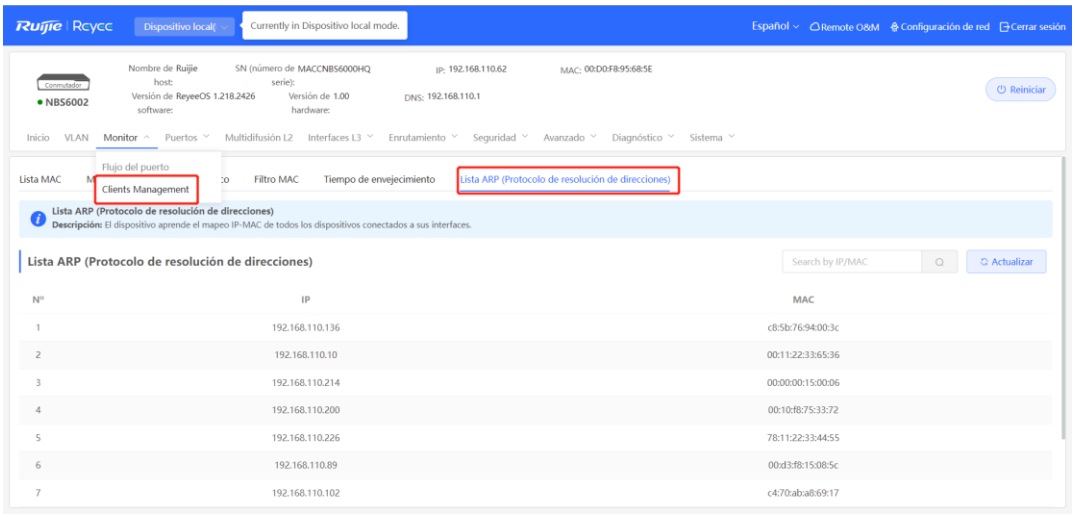
Seleccione **Dispositivo local** > **Monitor** > **Clients Management** > **Lista ARP**.

El Protocolo de Resolución de Direcciones (ARP) se utiliza para establecer una correspondencia entre direcciones IP y direcciones MAC. El ARP habilita a un conmutador para que obtenga la dirección MAC asociada con la dirección IP y almacene el mapeo entre las direcciones IP y las MAC en su memoria caché.

El conmutador aprende la dirección IP y la dirección MAC en los dispositivos de la red conectada a sus interfaces y genera las entradas ARP correspondientes. La página **Lista ARP** despliega las entradas ARP aprendidas por el conmutador. En la sección **Lista ARP**, se pueden buscar entradas ARP específicas por dirección IP o MAC. Haga clic en **Actualizar** para obtener las entradas ARP más recientes.

Nota

Para más información acerca del ARP, consulte 16.2 Configuración de la ruta estática IPv6



11.5 Lista de dispositivos cercanos IPv6

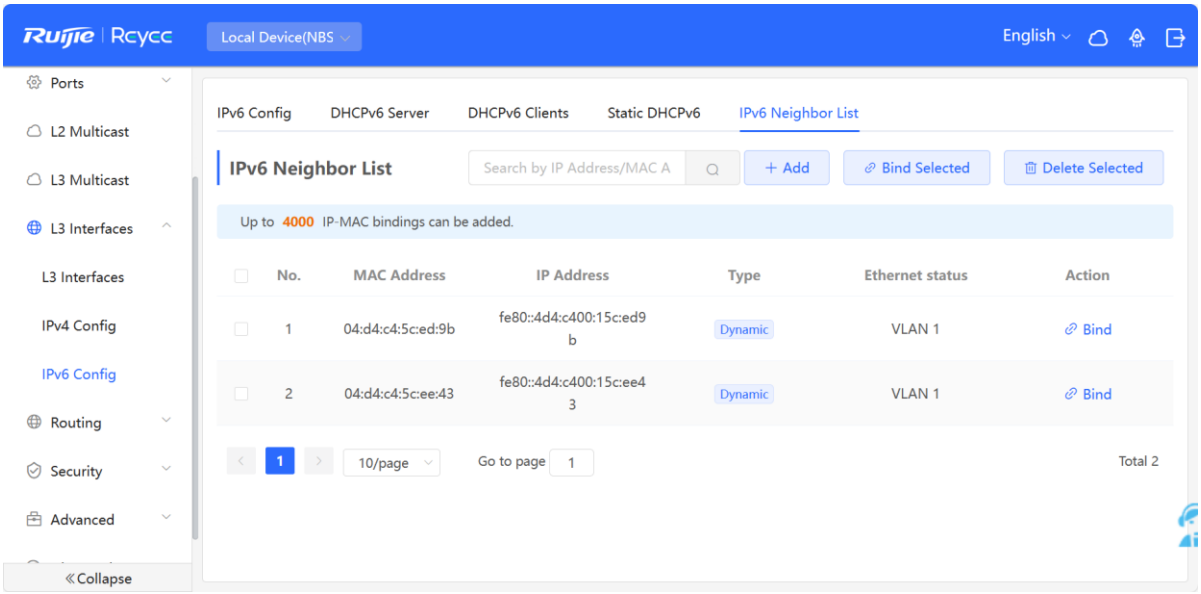
En el sistema del protocolo IPv6, el protocolo de detección de dispositivos cercanos (NDP) constituye un protocolo fundamental esencial. El NDP sustituye a los protocolos de detección de routers basados en el ICMP y el ARP que se utilizan en el protocolo IPv4 y admite distintas funciones como la resolución de direcciones, el seguimiento del estado de los dispositivos cercanos, la detección de direcciones duplicadas, la detección de routers y el redireccionamiento.

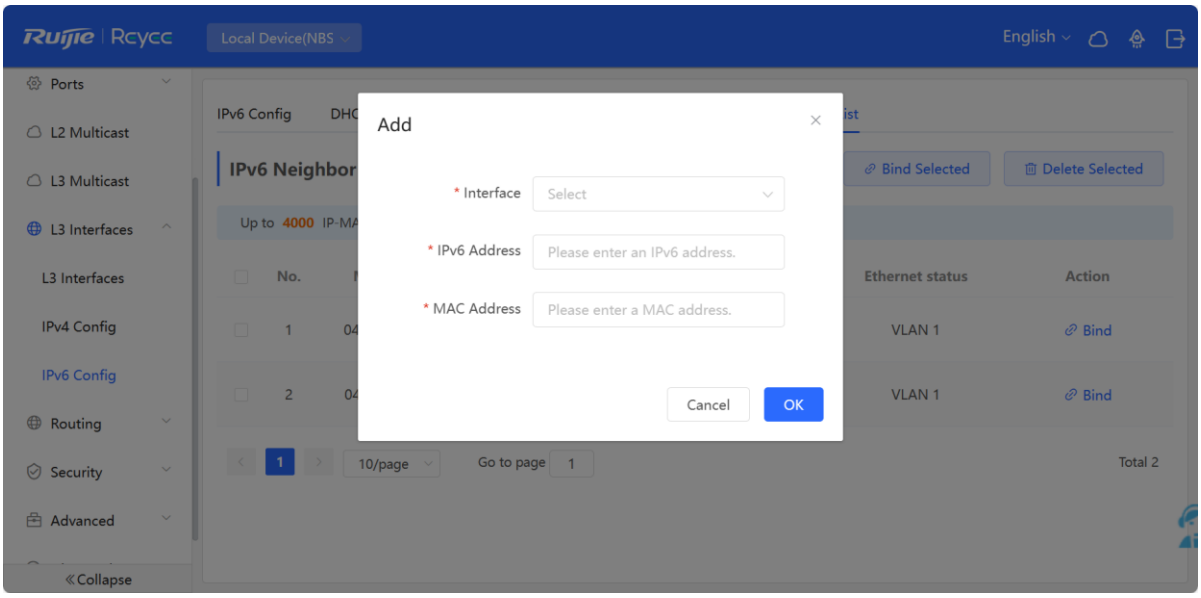
Seleccione **Local Device** > **L3 Interfaces** > **IPv6 Config** > **IPv6 Neighbor List**.

Haga clic en **Add** para añadir manualmente la interfaz, la dirección IPv6 y la dirección MAC del dispositivo cercano.

Haga clic en **Bind Selected** para vincular las direcciones IPv6 y MAC de la lista y evitar que se produzcan ataques de ND.

Si lo desea, puede editar, eliminar, eliminar por lotes y buscar un dispositivo cercano por su dirección IP o MAC.





11.6 VLAN

11.6.1 Información general de VLAN

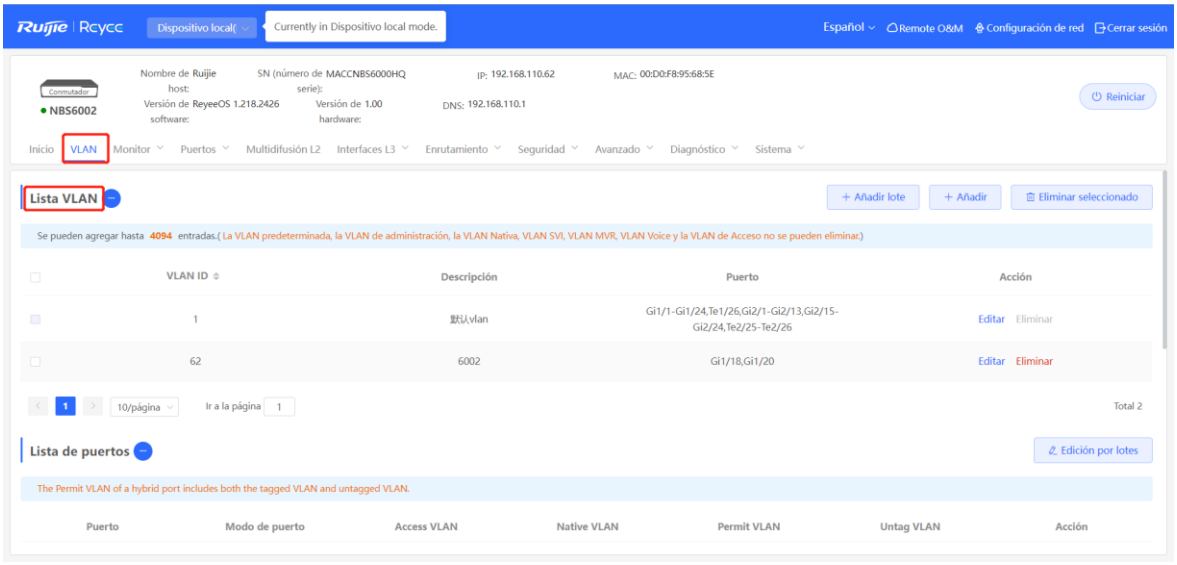
Una red de área local virtual (VLAN) es una red lógica creada en una red física. Una VLAN tiene las mismas propiedades que una red física normal, excepto que la VLAN no está limitada a su ubicación física. Cada VLAN cuenta con un dominio de difusión independiente. El aislamiento de las diferentes VLAN es de Capa 2. Las tramas de unidifusión, difusión y multidifusión de Capa 2 se reenvían y difunden dentro de una VLAN y no se transmitirán a otras VLAN.

Cuando un puerto se define como miembro de una VLAN, todos los clientes conectados a ese puerto pertenecen a la VLAN. Una red admite múltiples VLAN. Las VLAN pueden implementar una comunicación de Capa 3 entre ellas a través de dispositivos o interfaces de Capa 3.

11.6.2 Creación de una VLAN

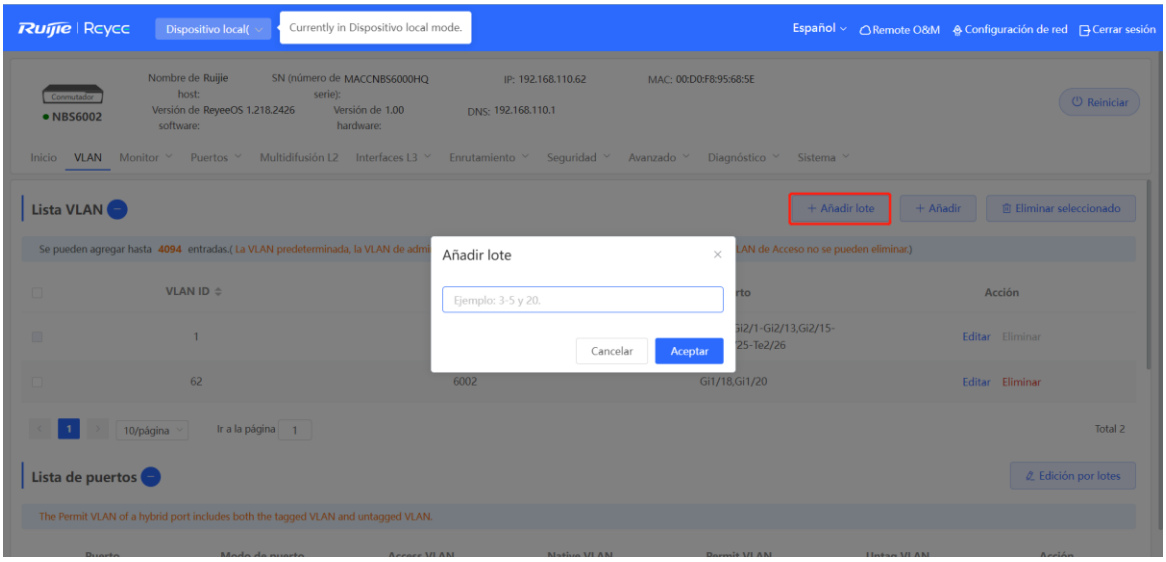
Seleccione **Dispositivo local** > **VLAN** > **Lista VLAN**.

La lista de VLAN contiene toda la información existente acerca de estas. Se puede modificar o borrar la VLAN existente o crear una.

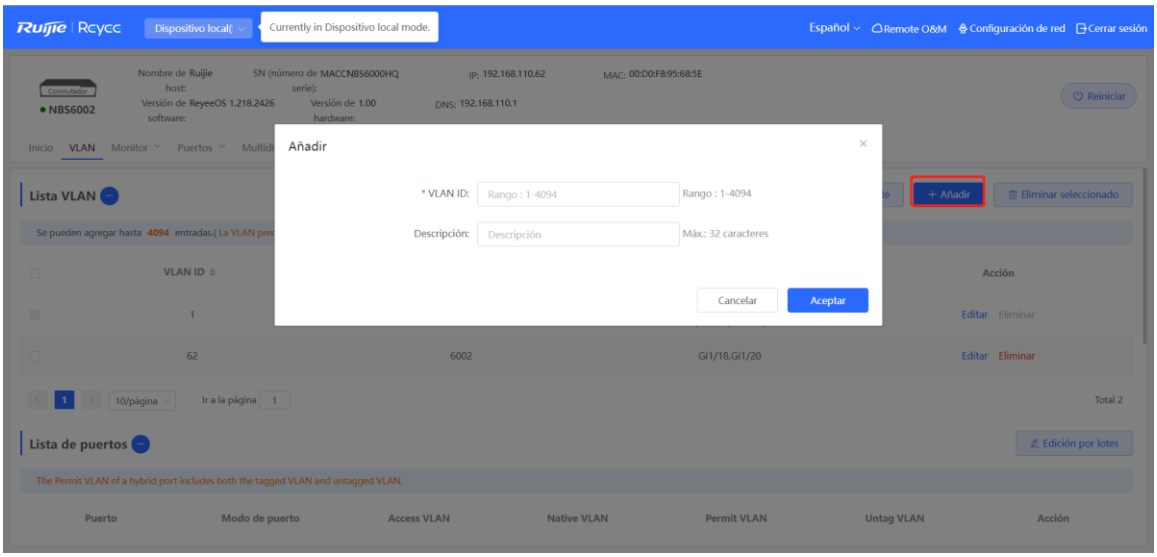


1. Añadir una VLAN

Creación por lotes: haga clic en **Añadir lote**. En el cuadro de diálogo que aparece, ingrese el rango de VLAN ID y haga clic en **Aceptar**. Las VLAN añadidas se mostrarán en la **Lista VLAN**. Los rangos de VLAN ID están separados por comas (,).



Creación individual: haga clic en **Añadir**. Ingrese la VLAN ID y la descripción de la VLAN, y haga clic en **Aceptar**. La VLAN añadida se mostrará en la **Lista VLAN**

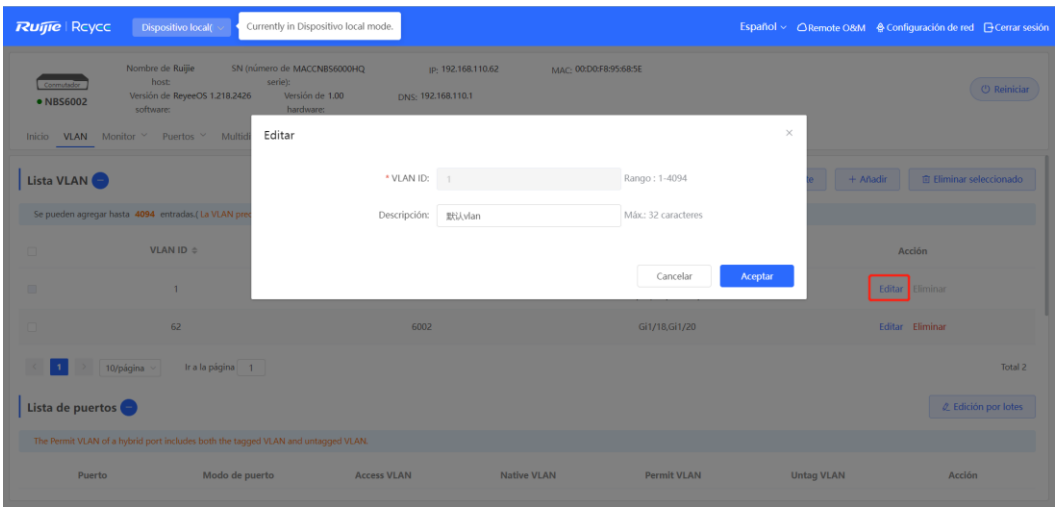


Nota

- El rango de las VLAN ID es de 1 a 4094.
- Se pueden separar varias VLAN para añadirlas a los lotes mediante comas (,) y separar las VLAN ID de principio a fin de un rango de VLAN con un guion (-).
- Si no se configura ninguna descripción cuando la VLAN se añada, el sistema automáticamente crea una descripción de esta en el formato especificado; por ejemplo, VLAN000XX. Las descripciones de las diferentes VLAN deben ser únicas.
- Si el dispositivo es compatible con funciones de Capa 3, las VLAN, los puertos enrutados y los puertos agregados de Capa 3 compartirán los mismos recursos de hardware limitados. Si un recurso no es suficiente, se mostrará un mensaje indicando el origen de la insuficiencia para las VLAN.

2. Modificación de la descripción de la VLAN

En **Lista VLAN**, haga clic en el botón **Editar** de la última columna **Acción** para modificar la descripción de una VLAN en específico.



3. Eliminación de una VLAN

Eliminación por lotes: en **Lista VLAN**, seleccione las entradas de las direcciones VLAN a eliminar y haga clic en **Eliminar seleccionado**.

Eliminación individual: en **Lista VLAN**, haga clic en el botón **Eliminar** de la última columna **Acción** para eliminar una **VLAN** en específico.

Nota

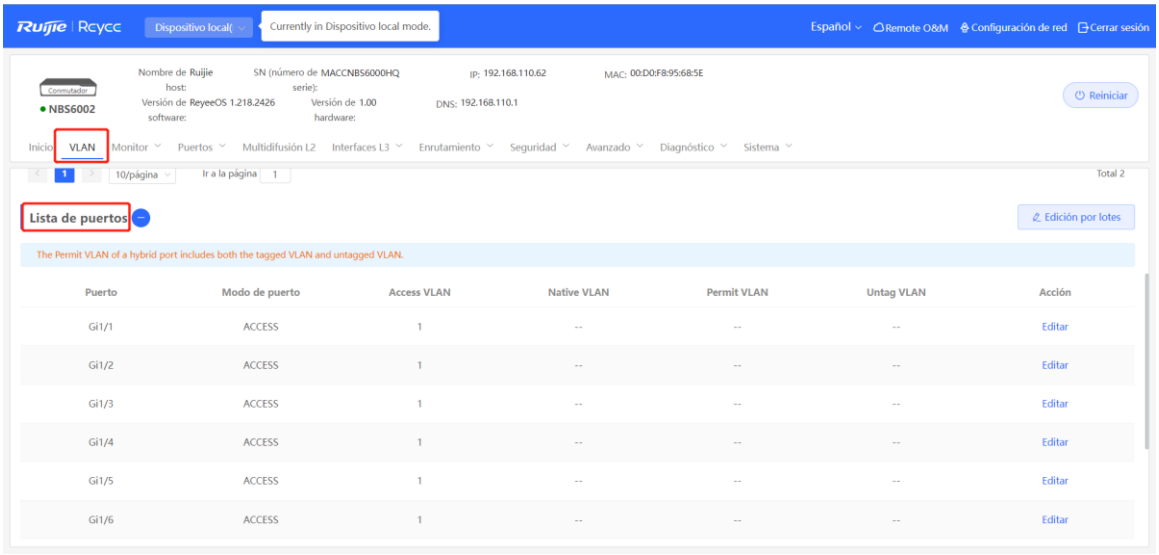
La VLAN predeterminada (VLAN 1), la VLAN de gestión, la VLAN nativa y la VLAN de acceso no se pueden eliminar. Para estas VLAN, el botón **Eliminar** está inhabilitado.

11.6.3 Configuración de un puerto VLAN

1. Descripción general

Seleccione **Dispositivo local** > **VLAN** > **Lista de puertos**.

En la sección **Lista de puertos**, se muestra la asignación de la VLAN del puerto actual. Para crear múltiples VLAN en la página de **Lista VLAN**, (consulte 11.6.2 Creación de una VLAN) y después configure el puerto con base en ellas.



Se puede configurar el modo de puerto y los miembros VLAN de este para determinar si se le permite a las VLAN pasar a través este, y si los paquetes a reenviar por el puerto cuentan con el campo de etiqueta.

Tabla 11-1 Descripción del modo de puerto

Modo de puerto	Función
Puerto de acceso	Un puerto de acceso solamente puede pertenecer a una VLAN y únicamente permite que las tramas de esta VLAN pasen a través de él. Esta VLAN se conoce como VLAN de acceso. La VLAN de acceso tiene atributos, tanto de VLAN nativa como de VLAN permitida. Las tramas enviadas desde el puerto de acceso no llevan etiqueta. Cuando el puerto de acceso recibe una trama sin etiqueta de un dispositivo remoto, el dispositivo local determina que proviene de una VLAN de acceso y añade la VLAN ID de acceso a la trama.
Puerto troncal	Un puerto troncal admite una VLAN nativa y varias VLAN permitidas. Las tramas reenviadas por el puerto troncal de una VLAN nativa no llevan etiquetas, mientras que las reenviadas de una VLAN permitida, sí llevan. Por defecto, un puerto troncal pertenece a todas las VLAN del dispositivo y puede reenviar las tramas de todas ellas. Se puede configurar un rango de VLAN permitida para limitar las tramas que se pueden reenviar. Asegúrese de que los puertos troncales en los dos extremos del enlace se encuentren configurados con la misma VLAN nativa.
Puerto híbrido	Los puertos híbridos admiten una VLAN nativa y varias VLAN permitidas. Las redes VLAN permitidas se dividen en VLAN con etiqueta y VLAN sin etiqueta. Las tramas que reenvía el puerto híbrido desde una VLAN con etiqueta llevan etiquetas y las tramas que reenvía el puerto híbrido desde una VLAN sin etiqueta no llevan etiquetas. Las tramas que reenvía el puerto híbrido desde una VLAN nativa no deben llevar etiquetas, por lo que esta solo puede pertenecer a la lista de VLAN sin etiqueta.

Nota

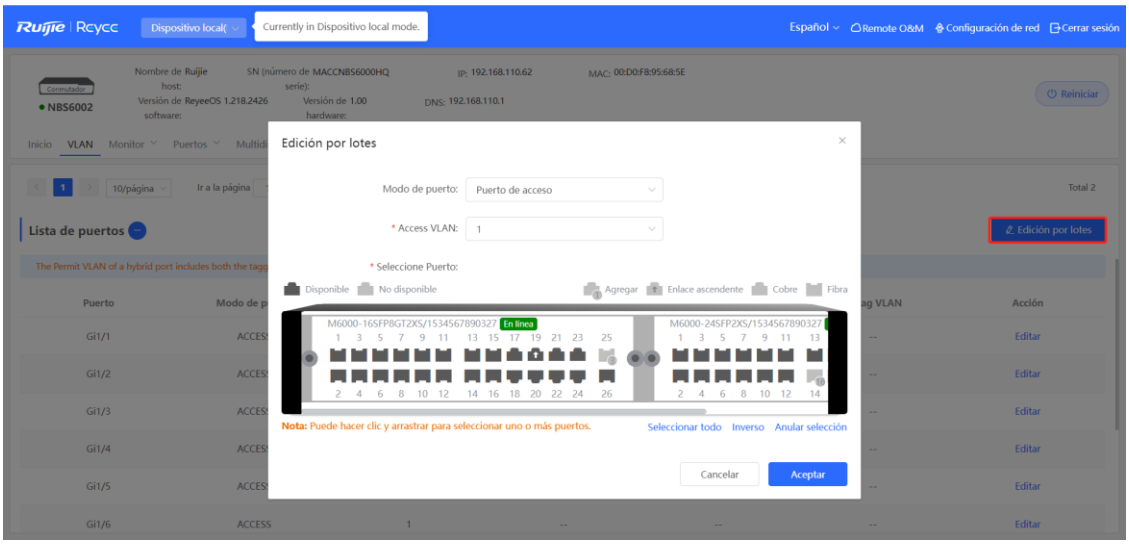
El que un producto admita el modo híbrido, depende de su versión.

2. Procedimiento

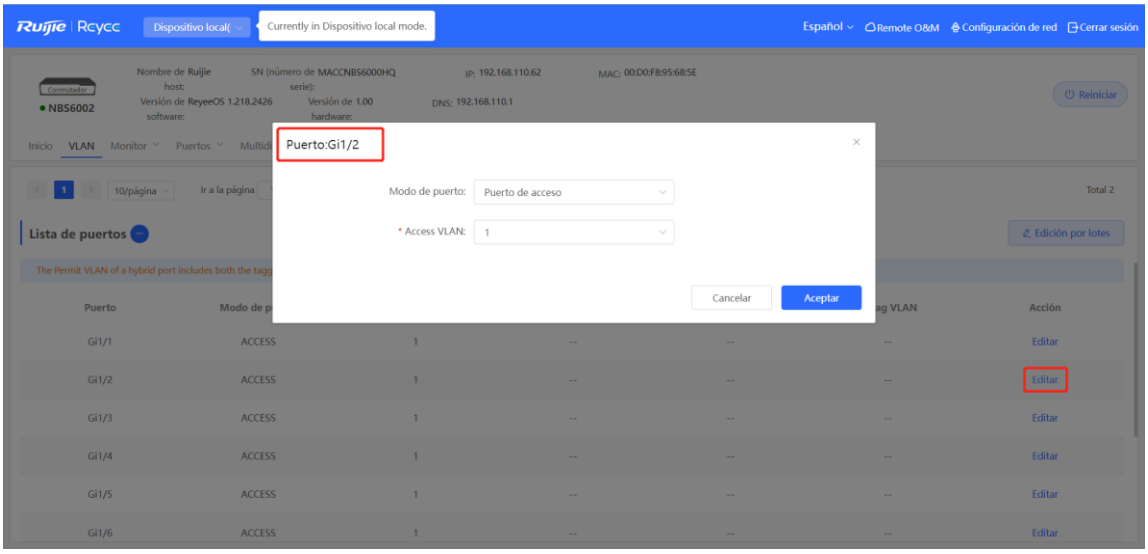
Seleccione **Dispositivo local** > **VLAN** > **Lista de puertos**.

Configure las VLAN del puerto por lotes: haga clic en **Editar por lotes**, seleccione el puerto que desee configurar en el panel de puertos y seleccione el modo de puerto. Si el modo de puerto es Puerto de acceso, deberá seleccionar la opción VLAN de acceso; si el modo de puerto es Puerto troncal, deberá seleccionar la opción VLAN nativa e introducir el rango de ID de VLAN permitidas; si el modo de puerto es Puerto híbrido, deberá seleccionar la opción VLAN nativa e introducir el rango de VLAN permitidas y el rango de VLAN sin etiqueta. Haga clic en **Aceptar** para finalizar la configuración por lotes. En el modo híbrido, las VLAN

permitidas incluyen VLAN con etiqueta y VLAN sin etiqueta. El rango de VLAN sin etiqueta debe incluir la VLAN nativa.



En **Lista de puertos**, haga clic en el botón **Editar** del puerto especificado de la última columna **Acción**, configúrelo junto con la VLAN correspondiente y haga clic en **Aceptar**.



Nota

- Los rangos de la VLAN ID van de 1 a 4094, donde la VLAN 1 es la predeterminada y no puede ser eliminada.
- Cuando los recursos de hardware no son suficientes, el sistema muestra un mensaje de falla en la creación de una VLAN.
- La configuración inadecuada de las VLAN en un puerto (especialmente en los de enlace ascendente) puede ocasionar fallas para iniciar sesión en el sistema de gestión Eweb. Por lo tanto, sea precavido cuando configure las VLAN.

11.6.4 Configuración de conmutadores en lote

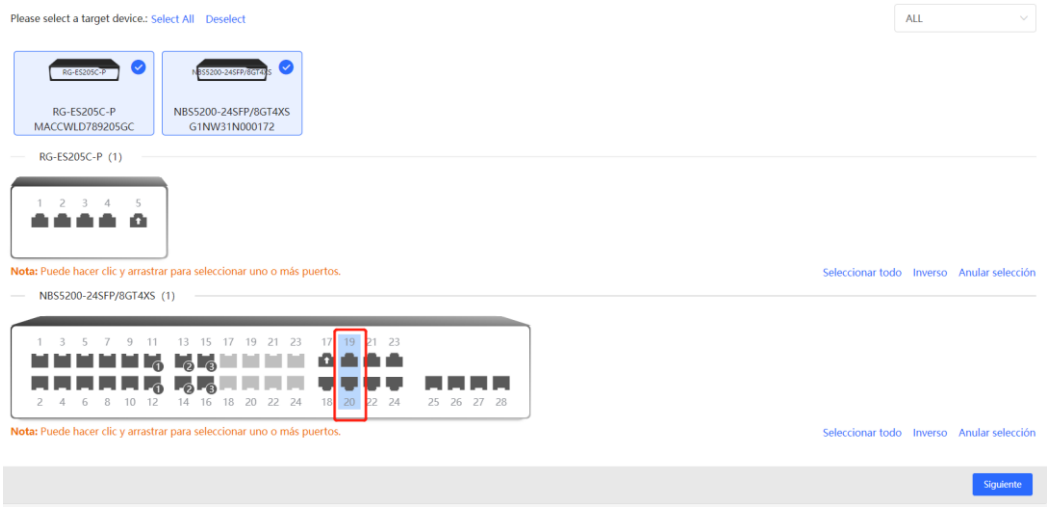
1. Descripción general

Se pueden crear VLAN en lote, configurar los atributos del puerto y designar las VLAN del puerto a los conmutadores en una red.

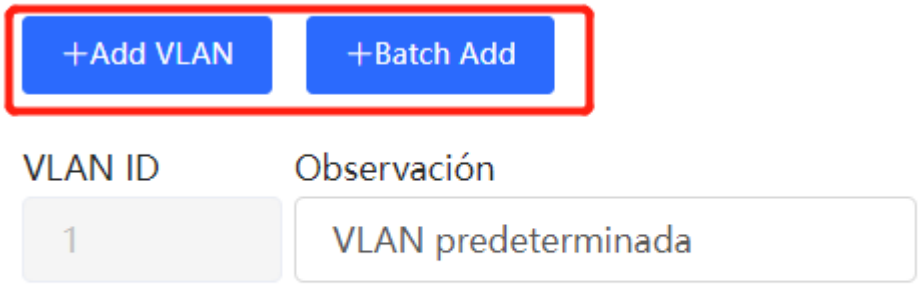
2. Procedimiento

Seleccione **Red** > **Red** > **Batch Config**.

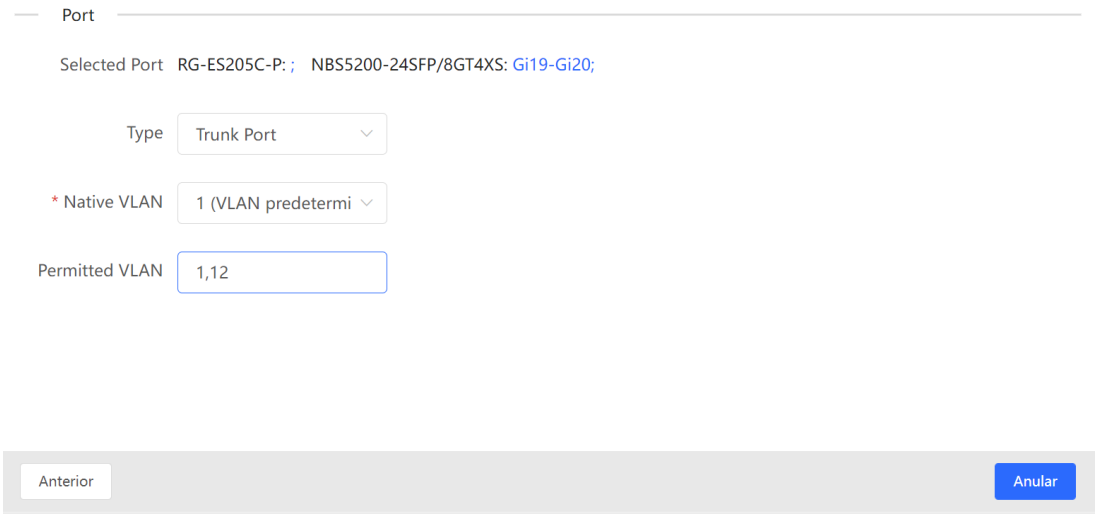
(1) Esta página despliega todos los conmutadores de una red activa. Seleccione los conmutadores a configurar y los puertos deseados en el esquema de puertos del dispositivo que aparece abajo. Si hay muchos dispositivos en la red activa, seleccione el modelo del producto de la lista que se despliega para filtrarlos. Después de seleccionar los dispositivos y puertos, haga clic en **Siguiente**.



(2) Haga clic en **Add VLAN** para crear una VLAN para los dispositivos seleccionados en lote. Si desea crear varias VLAN, haga clic en **Batch Add** y defina el rango de VLAN ID, como 3-5, 100. Después de configurar las VLAN, haga clic en **Siguiente**.

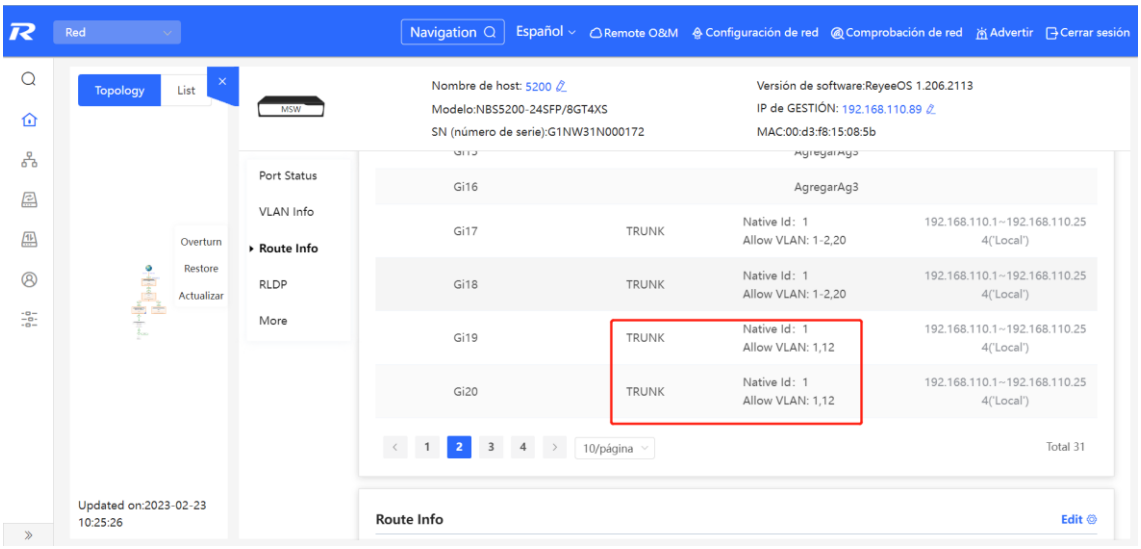


(3) Configure los atributos del puerto para aquellos seleccionados en el paso 1 en un lote. Seleccione un tipo de puerto. Si en **Type** selecciona **Puerto de acceso**, configure **VLAN ID**. Si en **Type** selecciona **Trunk Port**, configure **Native VLAN** y **Permitted VLAN**. Después de configurar los atributos del puerto, haga clic en **Puenteo** para enviar las configuraciones del lote a los dispositivos objetivo.



11.6.5 Verificación de la configuración

Revise la información de la VLAN y el puerto acerca de los conmutadores para saber si las configuraciones del lote se entregaron correctamente.



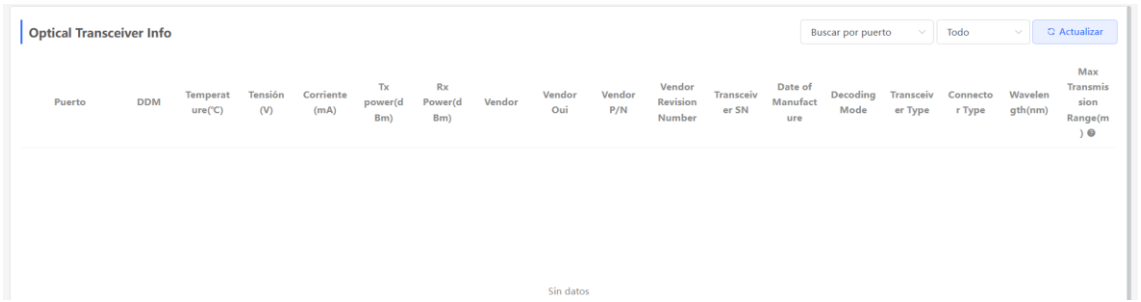
11.7 Visualización de la información de un transceptor óptico

Seleccione **Dispositivo local** > **Supervisión** > **Optical Transceiver Info**.

En la página **Optical Transceiver Info** se muestra la información básica de un transceptor óptico, incluido el puerto al que está conectado, la función DDM, la temperatura, la tensión, la corriente, la potencia Tx (Tx Power), la potencia Rx local (Rx Power), etc.

Puede consultar la información de un transceptor óptico introduciendo el puerto al que se encuentra conectado en el cuadro de búsqueda.

Los datos que se muestran en esta página se actualizan de forma automática cada 5 segundos. Si lo desea, también puede hacer clic en **Actualizar** para actualizar la información del transceptor óptico.



12 Gestión de puertos de los switches de las series NBS y NIS

12.1 Descripción general

El módulo de administración de puertos permite realizar una configuración básica de estos, agregar puertos, gestionar la función de duplicación de puertos (SPAN), limitar la velocidad de los puertos y configurar su dirección IP de gestión.

Tabla 12-1 Descripción de los tipos de puertos

Tipo de puerto	Descripción	Observaciones
Puerto del switch	El puerto de un switch o conmutador consiste en un puerto físico independiente en el dispositivo, que proporciona solamente funciones de conmutación de Capa 2. Los puertos de un conmutador se utilizan para administrar los puertos físicos y sus funciones de protocolo de Capa 2 asociadas.	
Puerto agregado de Capa 2	Una interfaz vincula varios miembros físicos para formar un enlace lógico. Para la conmutación de Capa 2, el puerto agregado es un puerto de switch de alto ancho de banda. Este proporciona los anchos de banda de múltiples puertos miembros para aumentar el ancho de banda del enlace. Además, para las tramas enviadas a través de un puerto agregado de Capa 2, el equilibrio de carga se realiza en los puertos miembros de Capa 2 de este puerto. Si el enlace miembro del puerto agregado falla, este puerto de Capa 2 automáticamente transfiere el tráfico del enlace al de otros enlaces miembros disponibles, mejorando la confiabilidad de la conexión.	
SVI	Una interfaz virtual de switch (SVI) funciona como la interfaz de administración de un conmutador, a través de la cual este se puede gestionar. También se puede crear una SVI como interfaz de puerta de enlace, que equivale a la interfaz virtual de una VLAN, y puede usarse para el enrutamiento entre VLAN en dispositivos de Capa 3.	Para su configuración, consulte 15.1 Configuración de una interfaz de Capa 3

Tipo de puerto	Descripción	Observaciones
Puerto enrutado	En dispositivos de Capa 3, se puede configurar un puerto físico independiente como puerto enrutado y usarlo como interfaz de puerta de enlace para la conmutación de Capa 3. Los puertos enrutados no cuentan con funciones de conmutación de Capa 2, por lo que no se asocian con las VLAN. Solo funcionan como interfaces de acceso.	Para su configuración, consulte 15.1 Configuración de una interfaz de Capa 3
Puerto agregado de Capa 3	Un puerto agregado de Capa 3 es un grupo de puertos agregados lógicos, compuestos de varios puertos miembros físicos, que es similar al puerto agregado de Capa 2. Los puertos por agregar deben ser de Capa 3 y del mismo tipo. Un puerto agregado sirve como interfaz de puerta de enlace para la conmutación de Capa 3. Varios enlaces físicos en el mismo grupo agregado se considera un enlace lógico. Varios enlaces físicos se combinan en un enlace lógico, aumentando su ancho de banda. Las tramas que se envían a través de puertos agregados de Capa 3 tienen un equilibrio de carga entre los puertos miembros. Si el enlace miembro del puerto agregado falla, este puerto de Capa 3 automáticamente transfiere el tráfico del enlace al de otros enlaces miembros, mejorando la confiabilidad de la conexión. Los puertos agregados de Capa 3 no admiten la conmutación de Capa 2.	Para su configuración, consulte 15.1 Configuración de una interfaz de Capa 3

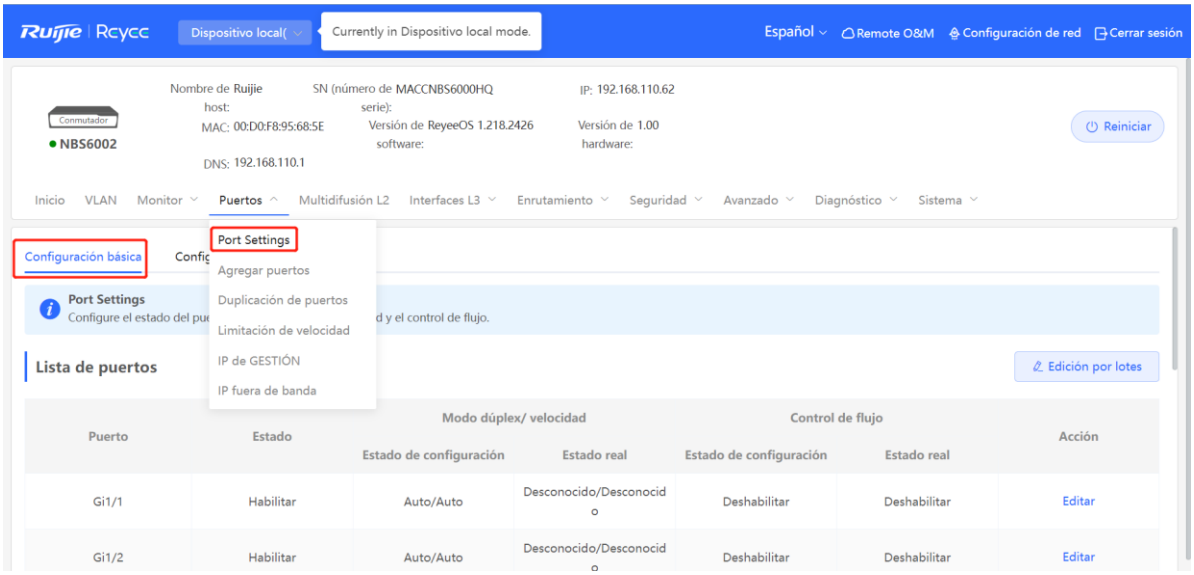
12.2 Configuración del puerto

La configuración del puerto incluye sus atributos comunes. Se puede ajustar la velocidad del puerto y configurar el estado de la interfaz, el modo dúplex, el modo de control de flujo, el conmutador Ethernet de bajo consumo, el tipo medio del puerto y la MTU.

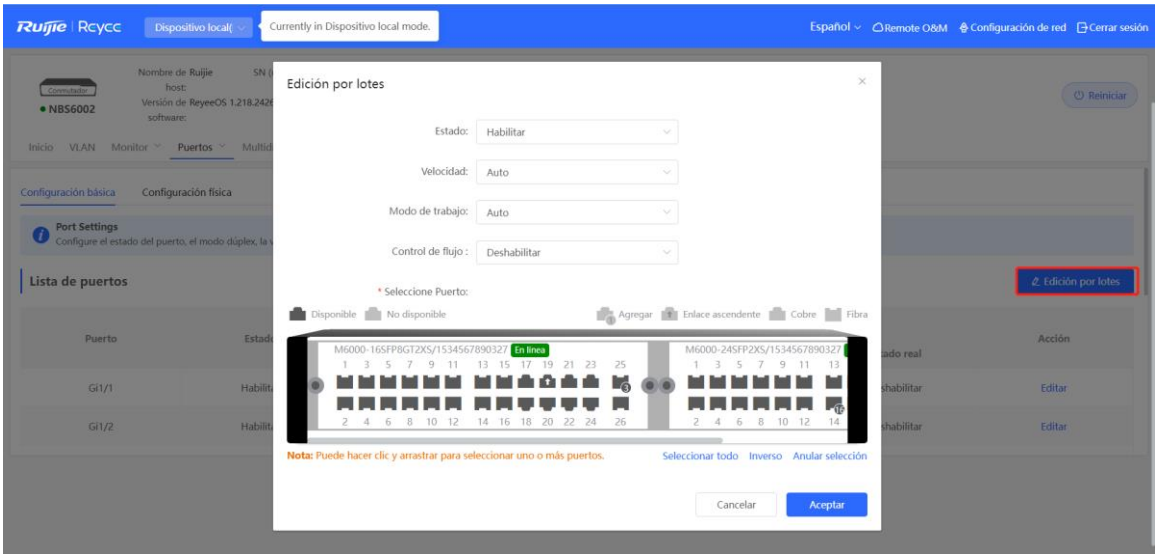
12.2.1 Configuración básica del puerto

Seleccione **Dispositivo local** > **Puertos** > **Port Settings** > **Configuración básica**.

En la página de **Configuración básica** se puede configurar el estado del puerto, la velocidad, el modo dúplex y el modo de control de flujo. Esta página muestra el estado actual de cada puerto.



Configuración por lotes: haga clic en **Edición por lotes** y seleccione el puerto a configurar. En el cuadro de diálogo que aparece, seleccione el estado del puerto, su velocidad, el modo de trabajo y el control de flujo; y haga clic en **Aceptar** para aceptar la configuración. Para la configuración por lotes, solo puede configurar los atributos comunes que admiten los puertos seleccionados.



Configuración individual: en **Lista de puertos**, seleccione la entrada del puerto y haga clic en **Editar** en la última columna **Acción**. En el cuadro de diálogo que aparece, seleccione el estado del puerto, su velocidad, el modo de trabajo y el control de flujo; después, haga clic en **Aceptar** para completar la configuración.

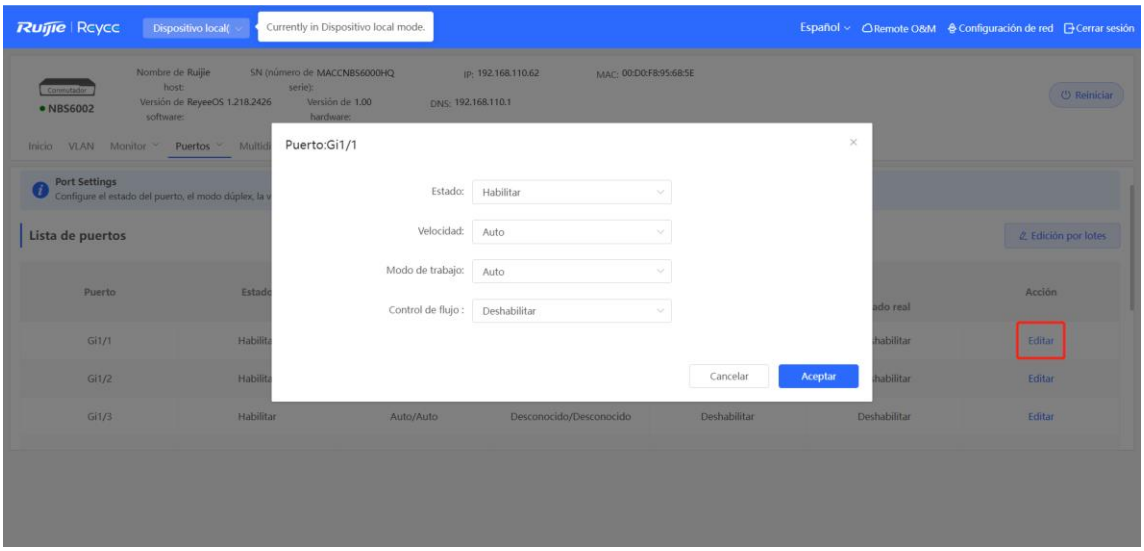


Tabla 12-2 Descripción de los parámetros básicos para la configuración de puertos

Parámetro	Descripción	Valor predeterminado
Estado	Si un puerto está deshabilitado, no podrá recibir o enviar tramas, y la función de procesamiento de datos correspondiente se perderá, pero la función de fuente de datos de alimentación PoE no se verá afectada.	Habilitado
Velocidad	Velocidad a la que trabaja la interfaz física de Ethernet. **Auto** significa que la velocidad del puerto está determinada a través de la negociación automática entre los dispositivos locales y remotos.	Automático
Modo de trabajo	● Dúplex completo: el puerto puede recibir paquetes al mismo tiempo que envía otros. ● Semidúplex: el puerto puede recibir o enviar paquetes, pero no al mismo tiempo. ● Auto: el modo dúplex del puerto se determina a través de la negociación automática entre los dispositivos locales y remotos.	Automático
Control de flujo	Si el control de flujo está habilitado, el puerto procesará las tramas de control de flujo recibidas y las enviará cuando ocurra una congestión en el puerto.	Deshabilitado

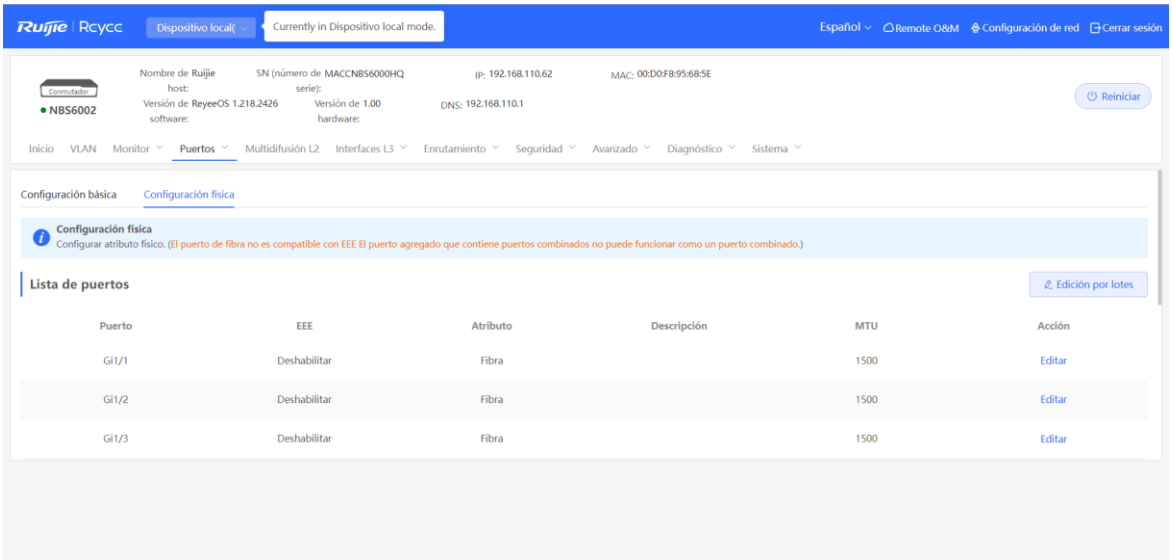
Nota

La velocidad de un puerto GE se puede establecer en **1000M**, **100M**, o **auto**. La velocidad de un puerto 10G se puede establecer en **10G**, **1000M**, o **auto**.

12.2.2 Configuración física

Seleccione **Dispositivo local** > **Puertos** > **Port Settings** > **Configuración física**.

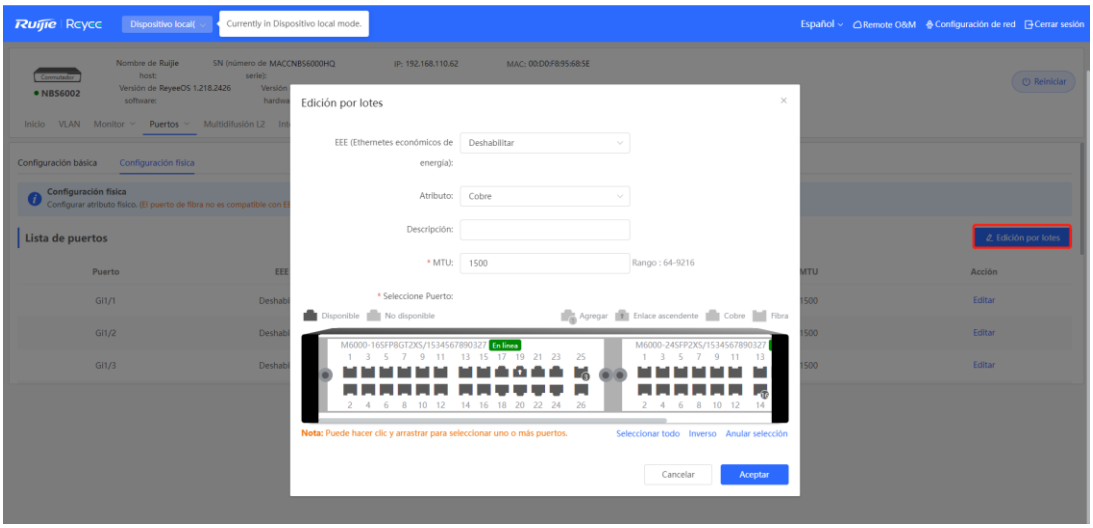
En esta página puede habilitar la función Ethernet de bajo consumo (EEE) y establecer el tipo de medio y la MTU de los puertos.



Configuración por lotes: haga clic en **Edición por lotes**. En el cuadro de diálogo que aparece, seleccione el puerto a configurar, la función EEE y la MTU, ingrese la descripción del puerto y haga clic en **Aceptar**.

Nota

Los puertos eléctricos y ópticos no pueden configurarse de manera simultánea durante la configuración en lote.



Configuración individual: haga clic en el botón **Editar**, en la columna **Acción** de la lista. En el cuadro de diálogo que aparece, configure la función EEE y el modo de puerto, ingrese la descripción del puerto y haga clic en **Aceptar**.

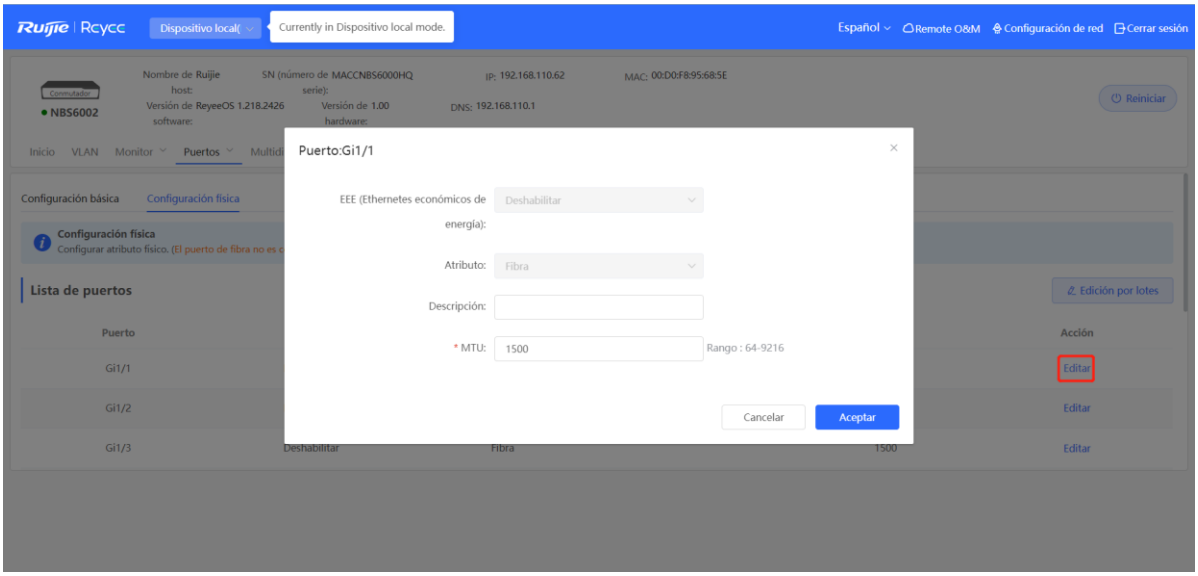


Tabla 12-3 Descripción de los parámetros básicos para la configuración física

Parámetro	Descripción	Valor predeterminado
EEE	Es la abreviatura de Ethernetes económicos de energía, que se basa en el protocolo estándar IEEE 802.3az. EEE ahorra energía al configurar la interfaz en modo ahorro de energía por inactividad del sistema (LPI), cuando la conexión de Ethernet está inactiva. Valor: Habilitado/Deshabilitado	Deshabilitado
Atributo	Determine si el puerto es eléctrico u óptico. Solo los puertos combos admiten el cambio de modo.	Según los atributos del puerto
Descripción	Se puede añadir una descripción para etiquetar las funciones del puerto.	NA
MTU	La Unidad de Transmisión Máxima (MTU) se utiliza para notificar al extremo remoto sobre el tamaño máximo aceptable de la unidad de servicio de datos. Indica el tamaño de la carga útil aceptable del remitente. La MTU de un puerto se puede configurar para limitar la longitud de una trama que puede recibirse o reenviarse a través de este.	1500

Nota

- Cada puerto admite diferentes atributos y elementos de configuración.
- Solo los puertos combos admiten el cambio de modo del puerto.
- Los puertos ópticos no son compatibles con el parámetro EEE.

12.3 Puertos agregados

12.3.1 Información general de puertos agregados

Un puerto agregado es un enlace lógico formado por varios enlaces físicos vinculados. Se utiliza para ampliar el ancho de banda del enlace, lo que mejora la confiabilidad de la conexión.

El puerto agregado admite equilibrios de carga; esto es, distribuye de manera equitativa el tráfico entre los enlaces miembros. El puerto agregado también implementa el respaldo de los enlaces. Cuando el enlace miembro del puerto agregado se desconecta, el sistema automáticamente distribuye su tráfico entre los enlaces miembros disponibles. Los paquetes de difusión o multidifusión recibidos por el enlace miembro del puerto agregado no se reenvían a otros enlaces miembros.

- Si una interfaz independiente que conecta dos dispositivos admite un máximo de velocidad de 1000 Mbps (asuma que las interfaces de ambos dispositivos admiten esa velocidad), cuando el tráfico del servicio en un enlace exceda los 1000 Mbps, el tráfico excedente será descartado. La agregación de enlaces puede resolver este problema. Por ejemplo, utilice *n* cables de red para conectar dos dispositivos y vincule las interfaces. De este modo, las interfaces están lógicamente vinculadas para admitir un tráfico máximo de 1000 Mbps multiplicado por *n*.
- Si dos dispositivos están conectados por un solo cable, cuando el enlace entre las dos interfaces se desconecte, los servicios que lleve a cabo este enlace se verán interrumpidos. Después de que se vinculen varias interfaces, mientras haya un enlace disponible, los servicios que lleven a cabo no se interrumpirán.

12.3.2 Conceptos básicos

1. Dirección del puerto agregado estático

En el modo de puerto agregado estático, añada manualmente una interfaz física a un puerto agregado. El puerto agregado estático se puede implementar fácilmente. Es posible agregar varios enlaces físicos ejecutando los comandos para añadir interfaces físicas a un puerto agregado. Una vez que una interfaz miembro se añade al puerto agregado, esta puede mandar y recibir datos, y equilibrar el tráfico en este puerto.

2. Agregación dinámica

El modo agregación dinámica se crea para puertos WAN de puertas de enlace de la serie RG-MR. El ancho de banda máximo de un puerto WAN de una puerta de enlace MR admite 2000 Mbps. Cuando el puerto de intranet quede conectado al conmutador, un solo puerto puede admitir únicamente un ancho de banda máximo de 1000 Mbps. Para evitar el desperdicio de ancho de banda de un enlace descendente, incremente el máximo de ancho de banda del puerto entre la puerta de enlace MR y el conmutador. La agregación dinámica puede encargarse de esta situación.

Al conectar dos puertos miembros de agregación fijos en la puerta de enlace MR a dos puertos cualquiera en el conmutador, los dos puertos del conmutador podrán ser agregados automáticamente a través del intercambio de paquetes. Al puerto agregado generado automáticamente de esta manera en el conmutador se le llama agregación dinámica de puertos, y los dos puertos correspondientes son puertos miembros del puerto agregado.

Nota

Los puertos de agregación dinámica se pueden eliminar después de que el dispositivo los haya generado automáticamente, pero los puertos miembros no se pueden modificar.

3. Equilibrio de la carga

Con base en las características de los paquetes, como la dirección MAC de origen y destino, la dirección IP de origen y destino, el ID del puerto de origen L4 y destino L4, recibidos por una de las interfaces de recepción, un puerto agregado puede diferenciar los flujos de los paquetes, de acuerdo con uno o varios algoritmos combinados. El puerto agregado manda el mismo flujo de paquetes a través del mismo enlace miembro y distribuye de manera equitativa los flujos entre los enlaces miembros. Por ejemplo, en el modo de equilibrio de carga que se basa en las direcciones MAC de origen, los paquetes se distribuyen entre los diferentes enlaces miembros de un puerto agregado con base en sus direcciones MAC. Los paquetes de diferentes direcciones MAC de origen se distribuyen entre los diferentes enlaces miembros y los paquetes con la misma dirección MAC de origen se reenvían por ese mismo enlace.

Los puertos agregados admiten los modos de equilibrio de carga en los siguientes elementos:

- Dirección MAC de origen o destino
- Direcciones MAC de origen y destino
- Dirección IP de origen o destino
- Direcciones IP de origen y destino
- Puerto de origen
- Puerto de origen o destino L4
- Puertos de origen y destino L4

12.3.3 Configuración de puertos agregados

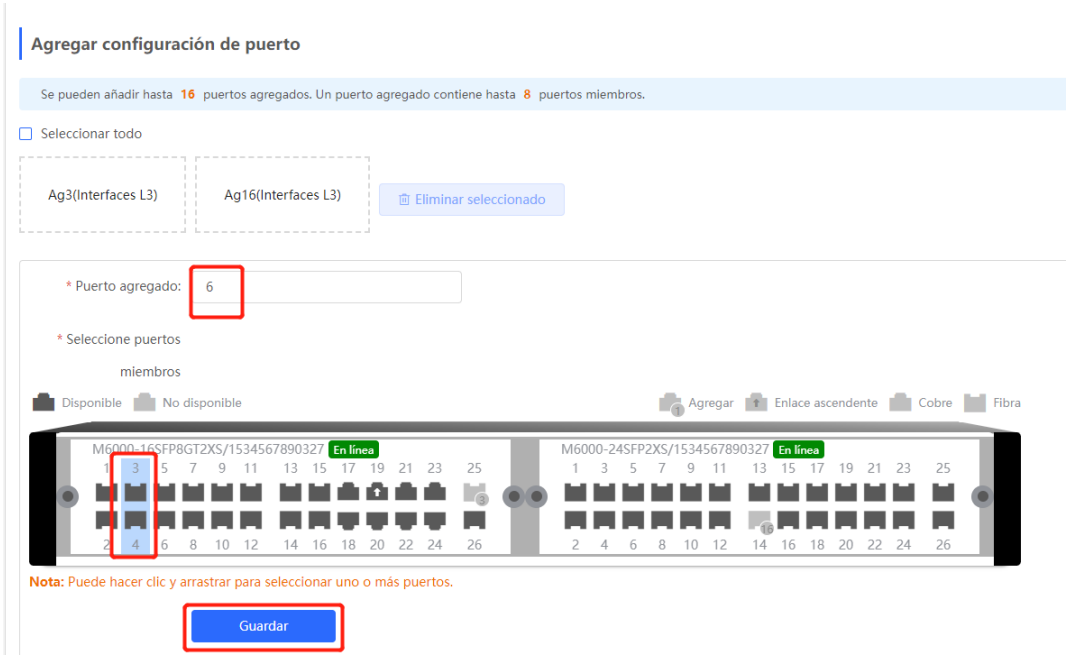
Seleccione **Dispositivo local** > **Puertos** > **Puertos agregados** > **Configuración de puertos agregados**.

1. Añadir puertos agregados estáticos

Ingrese un ID de puerto agregado, seleccione los puertos miembros (los puertos que se han añadido a un puerto agregado no pueden seleccionarse) y haga clic en **Guardar**. El panel del puerto muestra que se añadió correctamente el puerto agregado.

Nota

- Un puerto agregado contiene máximo ocho puertos miembros.
- Los atributos de los puertos agregados deben ser los mismos, y los puertos eléctricos y ópticos no pueden ser agregados.

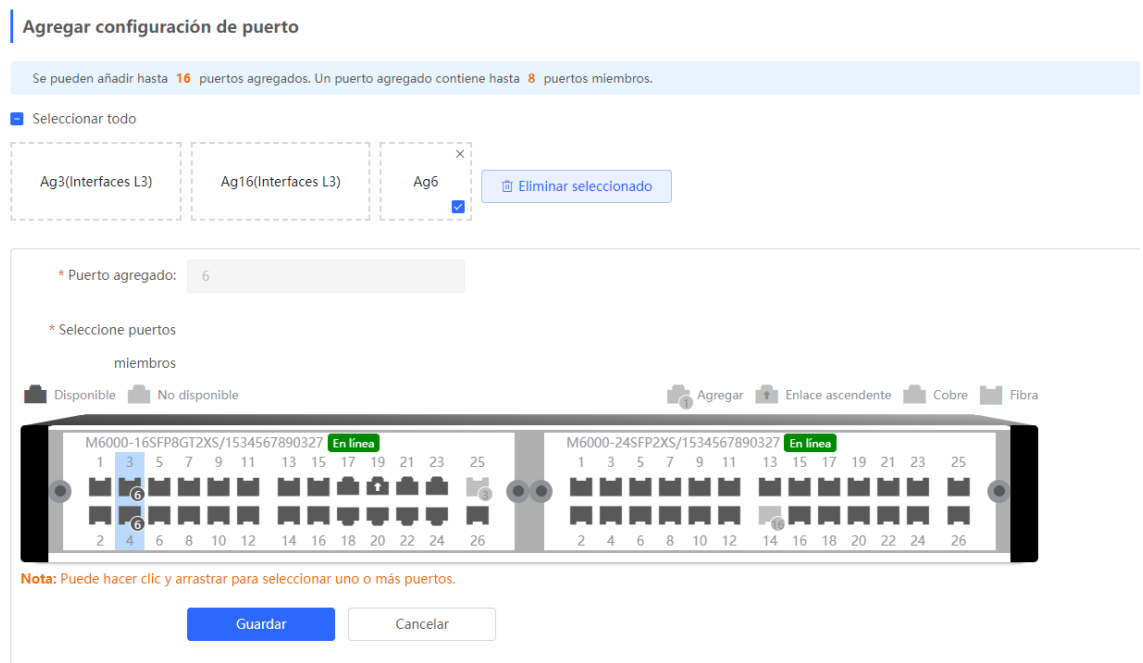


2. Modificación de los puertos miembros de un puerto agregado estático

Haga clic en el puerto agregado estático añadido. Los puertos miembros del puerto agregado se mostrarán como seleccionados. Haga clic en un puerto para quitar la selección, o seleccione otros puertos para unirlos al puerto agregado actual. Haga clic en **Guardar** para modificar los puertos miembros del puerto agregado.

Nota

Los puertos miembros de puertos de agregación dinámica no se pueden modificar.

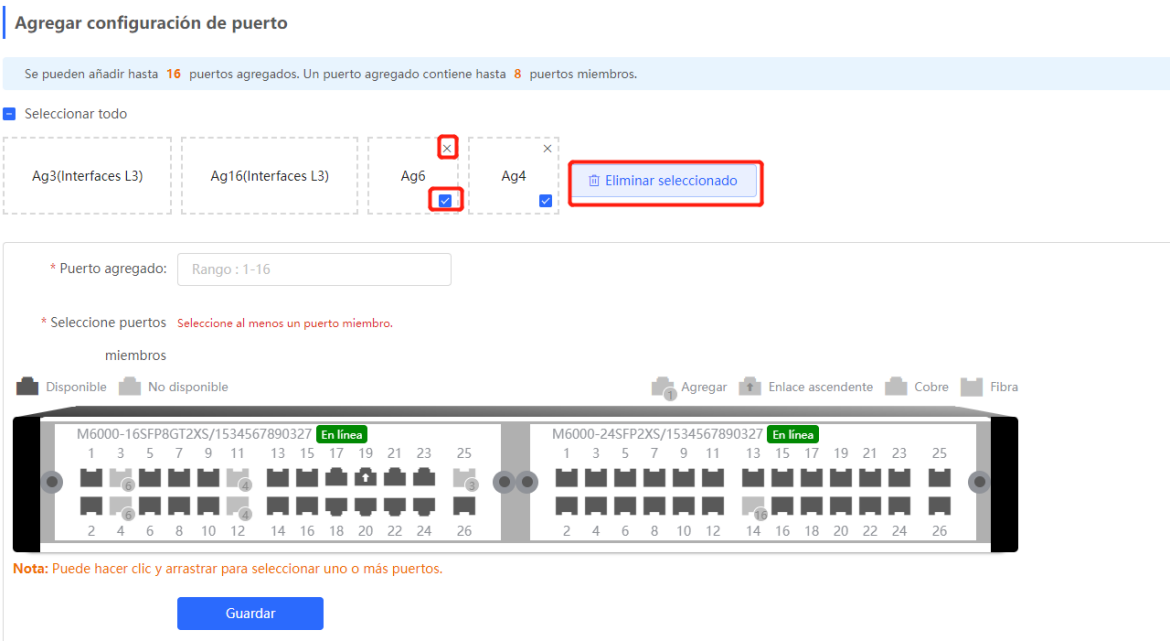


3. Eliminación de puertos agregados

Mueva el cursor sobre el ícono del puerto agregado y haga clic en ✕, o seleccione el puerto agregado que desea borrar y haga clic en **Eliminar seleccionado** para eliminarlo. Los puertos eliminados estarán disponibles en el panel de puertos y pueden usarse para formar un nuevo puerto agregado.

Precaución

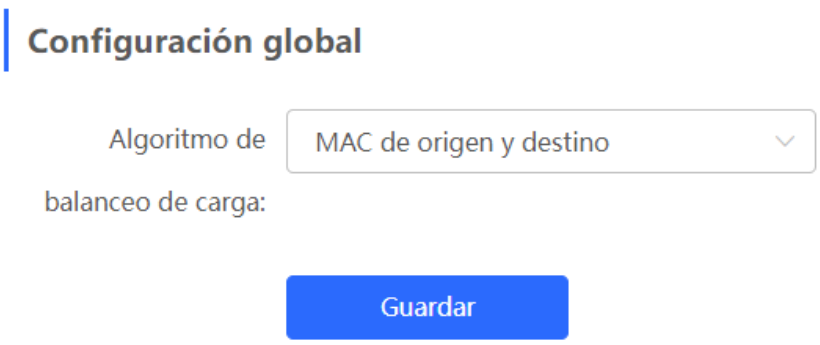
Cuando un puerto agregado se elimina, sus puertos miembros quedan deshabilitados y se restablece su configuración predeterminada.



12.3.4 Configuración de un modo de equilibrio de carga

Seleccione **Dispositivo local** > **Puertos** > **Puerto agregado** > **Configuración global**.

Seleccione **Algoritmo de balanceo de carga** y haga clic en **Guardar**. El conmutador distribuye los paquetes entrantes entre los enlaces miembros usando el algoritmo de equilibrio de carga especificado. El flujo de los paquetes con atributos consistentes se transmite por un enlace miembro, mientras que los flujos de paquetes diferentes se distribuyen equitativamente entre diferentes enlaces.



12.4 Duplicación de puertos

12.4.1 Descripción general

La función de duplicación de puertos (SPAN) copia los paquetes de un puerto especificado a otro que está conectado a un dispositivo de monitoreo de red. Cuando se configura un puerto duplicado o puerto espejo, los paquetes del puerto origen se copiarán y enviarán al puerto de destino; generalmente, el analizador de paquetes está conectado al puerto de destino para analizar el estado de los paquetes del puerto de origen, con el fin de monitorear todos los paquetes entrantes y salientes del puerto origen.

En la Figura 12-1, al configurar el puerto duplicado en el Dispositivo A, el conmutador copia los paquetes del Puerto 1 al Puerto 10. Aunque el analizador de red conectado al Puerto 10 no está conectado directamente al Puerto 1, puede recibir todos los paquetes a través del Puerto 1. Al hacer esto, los flujos de datos transmitidos por el Puerto 1 pueden ser monitoreados.

Figura 12-1 Duplicación de puertos

La SPAN logra el análisis del tráfico de datos de nodos o puertos de dispositivos sospechosos en la red sin afectar el reenvío de datos del dispositivo monitoreado. Se utiliza principalmente en situaciones de monitoreo de la red y de solución de problemas.

12.4.2 Procedimiento

Seleccione **Dispositivo local** > **Puertos** > **Duplicación de puertos**.

Haga clic en **Editar**, seleccione el puerto de origen, el puerto de destino, la dirección del monitoreo y determine si se recibirán paquetes de otros puertos, excepto del puerto duplicado; luego haga clic en **Aceptar**. Se puede configurar un máximo de cuatro entradas SPAN.

Para eliminar la configuración de duplicación de puertos, haga clic en **Eliminar** en la fila correspondiente en la última columna de **Acción**.

Precaución

- Se pueden seleccionar varios puertos de origen para monitorear el tráfico, pero solo un puerto de destino. Además, los puertos de origen para el monitoreo de tráfico no pueden contener el puerto de destino.
- Un puerto agregado no puede usarse como puerto de destino.
- Se puede configurar un máximo de cuatro entradas SPAN. La SPAN no puede configurarse para puertos que se han utilizado para SPAN.

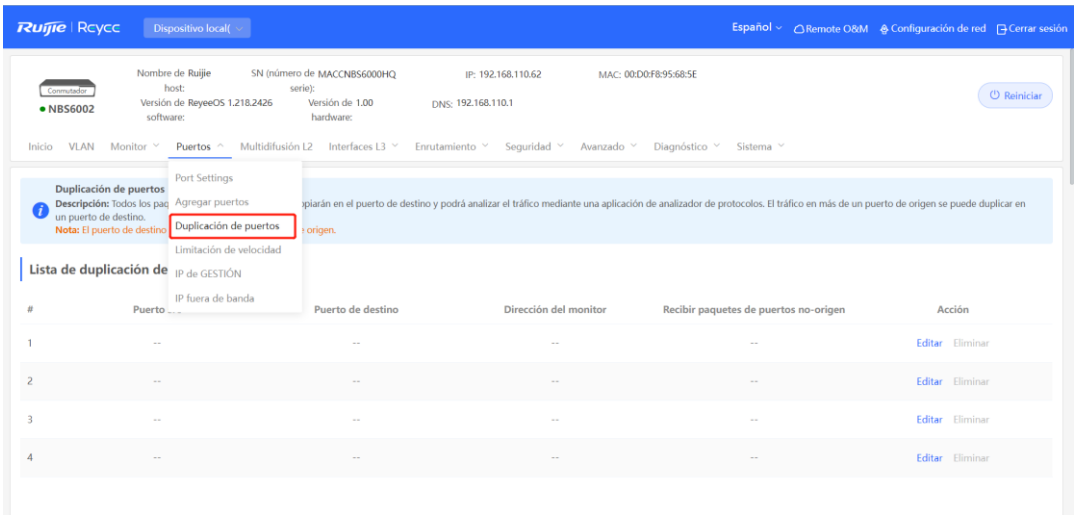


Tabla 12-4 Descripción de los parámetros de la duplicación de puertos

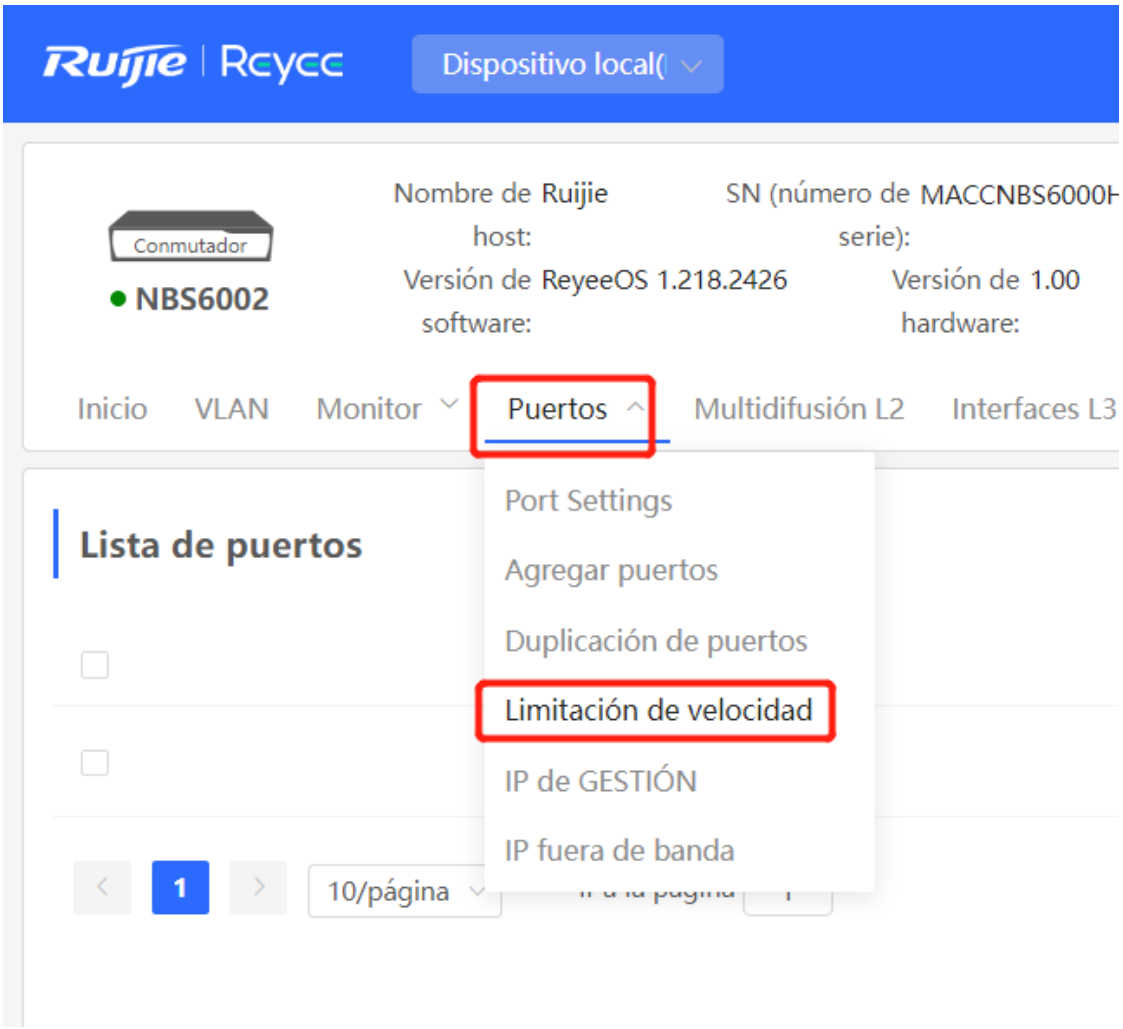
Parámetro	Descripción	Valor predeterminado
Puerto de origen	El puerto de origen también se conoce como puerto monitoreado. Los flujos de datos en el puerto de origen se monitorean para el análisis de la red o la resolución de problemas. Se pueden seleccionar varios puertos de origen y duplicarlos en un puerto de destino.	N/A
Puerto de destino	El puerto de destino también se conoce como puerto de monitoreo; esto es, el puerto conectado al dispositivo de monitoreo. Este reenvía los paquetes recibidos del puerto de origen al dispositivo de monitoreo.	N/A

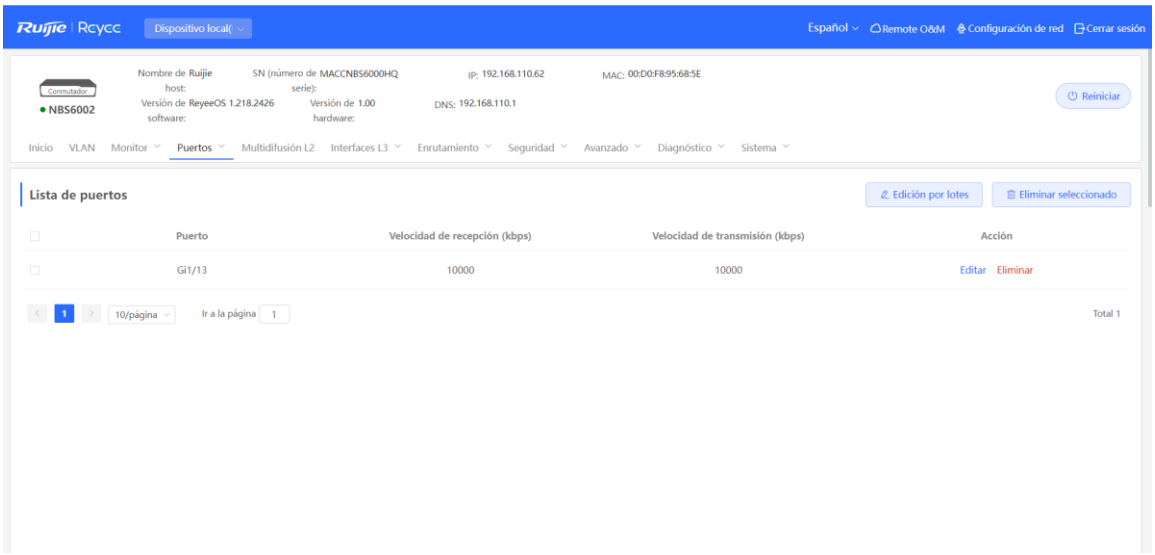
Parámetro	Descripción	Valor predeterminado
Dirección del monitoreo	Tipos de paquetes (dirección del flujo de datos) a ser monitoreados por un puerto de origen. ● Ambos: indica todos los paquetes que pasen a través del puerto, incluyendo los entrantes y salientes. ● Entrantes: indica todos los paquetes recibidos por el puerto de origen y copiados al puerto de destino. ● Salientes: indica todos los paquetes transmitidos por el puerto de origen y copiados al puerto de destino.	Ambos
Recepción de paquetes de puertos de no-origen	Aplica al puerto de destino e indica si un puerto de destino reenvía otros paquetes mientras realiza el monitoreo. ● Habilitado: cuando el conmutador los paquetes del puerto de origen, los paquetes de otros puertos, excepto los del puerto de origen, se reenvían normalmente. ● Deshabilitado: solo los paquetes del puerto de origen son monitoreados.	Habilitado

12.5 Limitación de velocidad

Seleccione **Dispositivo local** > **Puertos** > **Limitación de velocidad**.

El módulo de **Limitación de velocidad** le permite configurar límites respecto al tráfico de los puertos, incluyendo límites de velocidad de transmisión y de recepción de los puertos.





1. Parámetros de velocidad límite

Haga clic en **Edición por lotes**. En el cuadro de diálogo que aparece, seleccione los puertos e ingrese los límites de velocidad, y haga clic en **Aceptar**. Como mínimo, debe configurar la velocidad de recepción y de

transmisión. Cuando la configuración se complete, el límite de velocidad se mostrará en las reglas de velocidad límite de la lista de puertos.

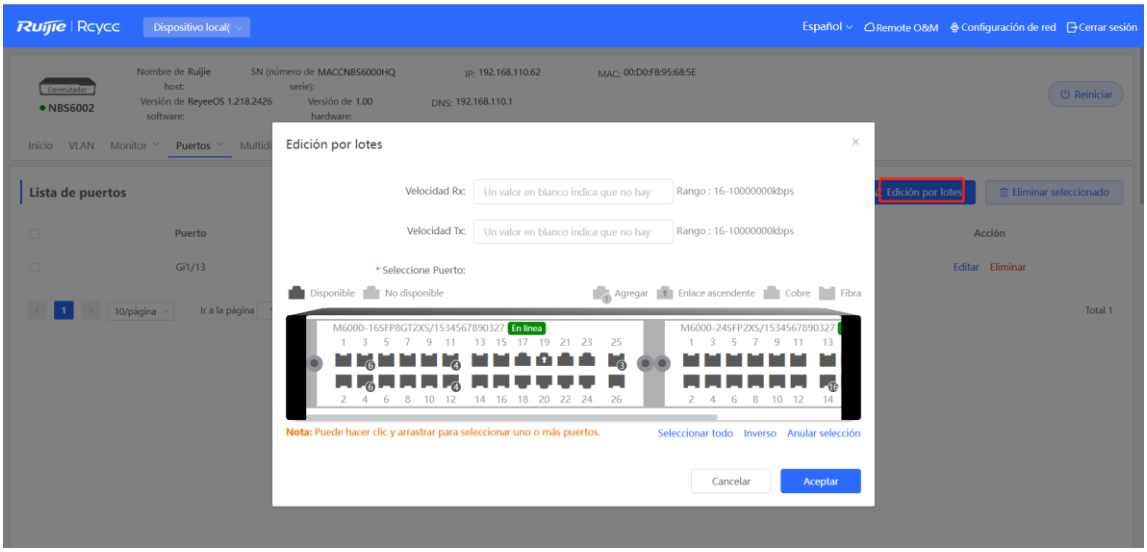
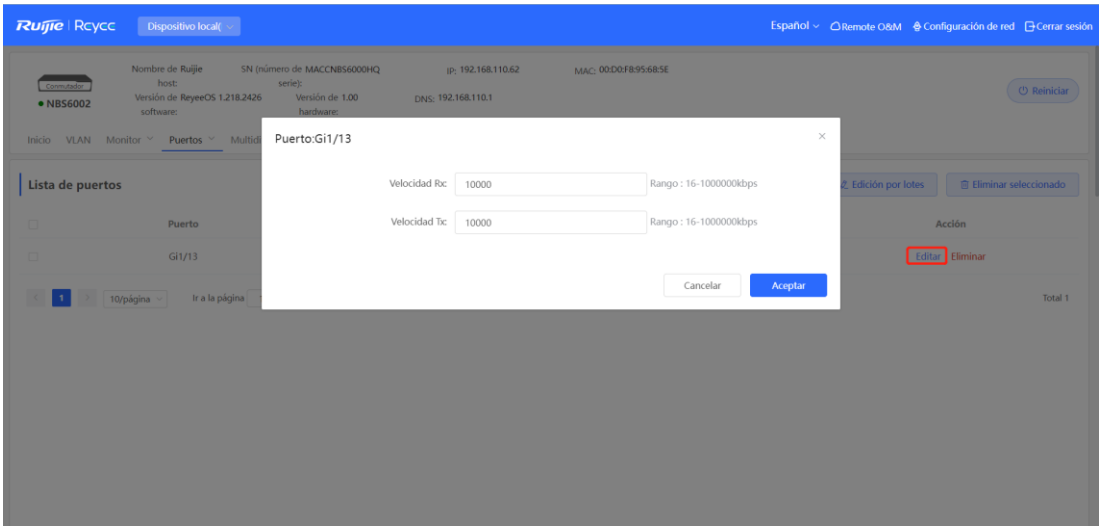


Tabla 12-5 Descripción de los parámetros de la velocidad límite

Parámetro	Descripción	Valor predeterminado
Velocidad Rx	Velocidad máxima en la que los paquetes son enviados de un puerto al conmutador, en kbit/s.	Sin límite
Velocidad Tx	Velocidad máxima en la que los paquetes son enviados de un conmutador al puerto, en kbit/s.	Sin límite

2. Modificación de los límites de velocidad de un solo puerto

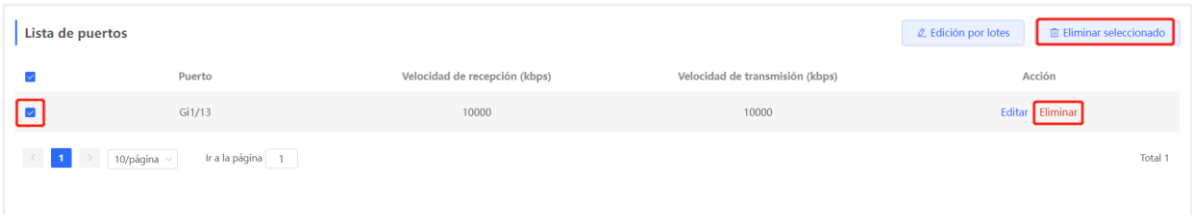
En la lista de puertos para la que se ha configurado el límite de velocidad, haga clic en **Editar** en el puerto correspondiente, establezca las velocidades de recepción y transmisión en el cuadro de diálogo que aparece y haga clic en **Aceptar**.



3. Eliminación de los límites de velocidad

Configuración por lotes: seleccione múltiples registros en **Lista de puertos**, haga clic en **Eliminar seleccionado**, y presione **Aceptar** en el cuadro de diálogo que aparezca.

Configuración individual: en **Lista de puertos**, haga clic en **Eliminar** en el puerto correspondiente, y presione **Aceptar** en el cuadro de diálogo que aparezca.



Nota

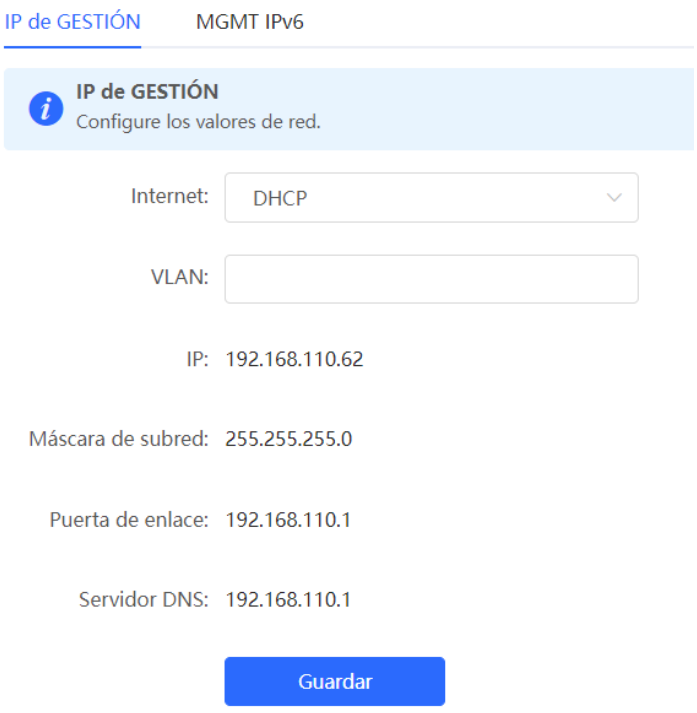
- Cuando configure los límites de velocidad de un puerto, configure al menos la velocidad de recepción y de transmisión.
- Cuando no se establecen límites de recepción y de transmisión, el puerto no tiene límites de velocidad.

12.6 Configuración de la dirección IP de gestión

12.6.1 Configuración de las direcciones IPv4 de gestión

Seleccione **Dispositivo local** > **Puertos** > **IP de GESTIÓN**.

La página **IP de GESTIÓN** le permite configurar la dirección IP de gestión del dispositivo. Se puede configurar y administrar el dispositivo ingresando a la dirección IP de gestión.



El dispositivo se puede conectar de dos modos:

- **DHCP**: utiliza una dirección IP temporal asignada de manera dinámica por el servidor DHCP ascendente para el acceso a Internet.
- **IP estática**: utiliza una dirección IP estática configurada manualmente por los usuarios para el acceso a la Internet.

Si selecciona **DHCP**, el dispositivo obtiene parámetros del servidor DHCP. Si se selecciona **IP estática** tendrá que incluir la VLAN de gestión, la dirección IP, la máscara de subred, la dirección IP de puerta de enlace predeterminada y la dirección del servidor DNS. Haga clic en **Guardar** para que la configuración se active.

Nota

- Si el recuadro de la VLAN de gestión está vacío o no se especifica, la VLAN 1 se activará por defecto.
- La VLAN de gestión debe seleccionarse de entre las VLAN existentes. Si no se crea una VLAN, consulte la lista de VLAN para añadir una de ellas (para más información, consulte 11.6.2 Creación de una VLAN11.6.2).
- Le recomendamos vincular la VLAN de gestión configurada a un puerto de enlace ascendente. De otro modo, es posible que no pueda acceder al sistema de gestión Eweb.

12.6.2 Configuración de las direcciones IPv6 de gestión

Configure la dirección IPv6 que se haya utilizado para iniciar sesión en la página de gestión del dispositivo.

Seleccione **Dispositivo local** > **Puertos** > **MGMT IPv6**.

Configure la dirección IPv6 de gestión para que pueda iniciar sesión en la página de gestión del dispositivo a través de la dirección IPv6 del dispositivo.

El dispositivo admite los siguientes tipos de conexión a Internet:

- **Nulo**: la función IPv6 se encuentra desactivada en el puerto actual.
- **DHCP**: el dispositivo obtiene una dirección IPv6 de forma dinámica del dispositivo ascendente.
- **IP estática**: debe configurar manualmente la dirección IPv6, la longitud, la dirección de la gateway y el servidor DNS.

Haga clic en **Guardar**.

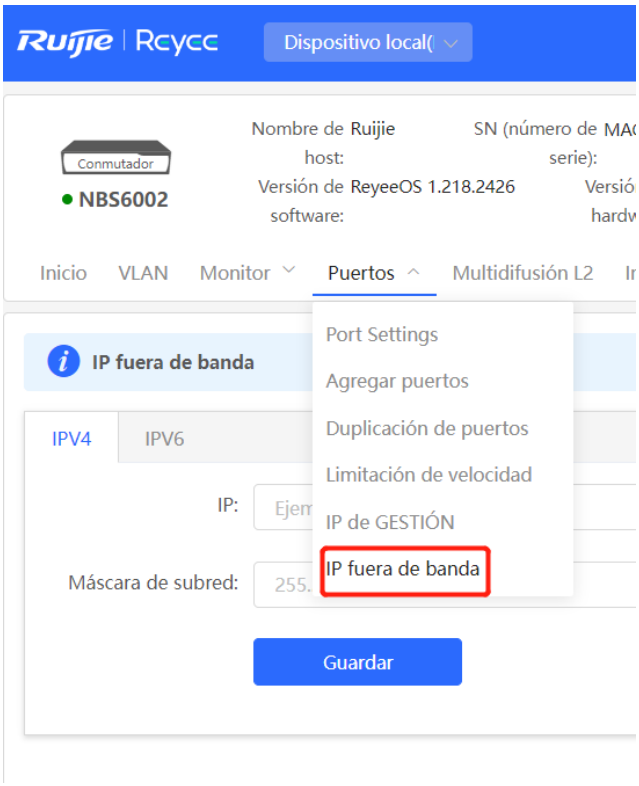
12.7 Configuración de la dirección IP fuera de banda

Precaución

Solamente las series RG-NBS6002, RG-NBS7003 y RG-NBS7006 admiten esta función.

Seleccione **Dispositivo Local** > **Puertos** > **IP fuera de banda**.

Establezca la dirección IP de la interfaz de gestión del conmutador modular.



Nota

No se ha configurado ninguna dirección IP para la administración del puerto por defecto. Actualmente, solo la dirección IP estática puede configurarse para administrar el puerto, pero no es compatible con el DHCP.

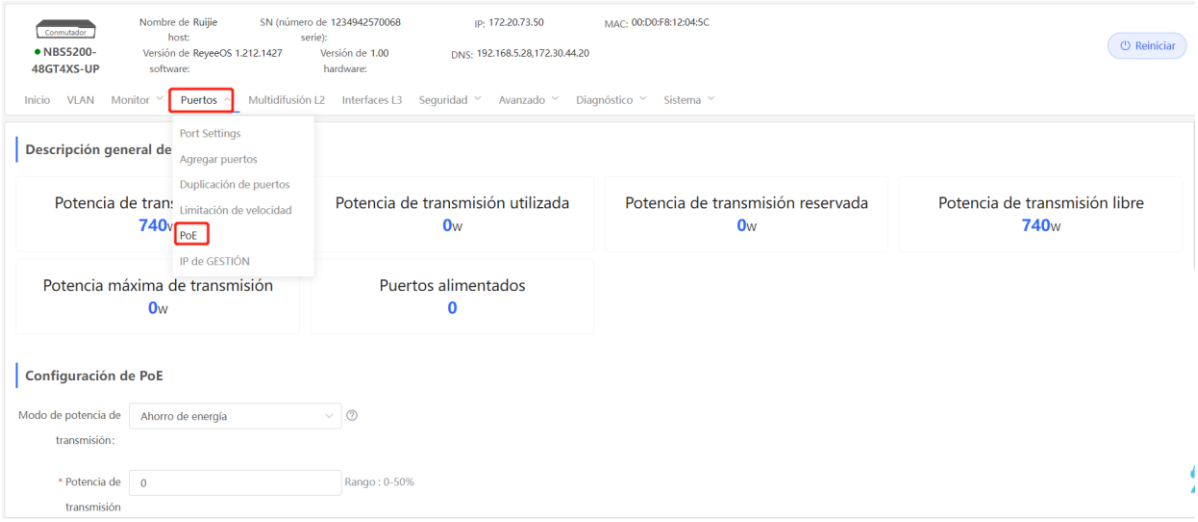
12.8 Configuración de PoE

Precaución

Solo los conmutadores PoE (modelos de dispositivo marcados con **-P**) admiten esta función.

Seleccione **Dispositivo local** > **Puertos** > **PoE**.

El dispositivo suministra potencia a través de los puertos a los dispositivos alimentados por PoE. Revise la fuente de alimentación actual, configure el sistema y vea las directivas del puerto de suministro de potencia respectivamente para lograr una distribución de potencia flexible.



12.8.1 Visualización de la información global de la alimentación PoE

Seleccione **Dispositivo local** > **Puertos** > **PoE** > **Descripción general de PoE**.

En la página **Descripción general de PoE** se muestra la información global de la alimentación PoE, incluida la potencia total, la potencia utilizada, la potencia reservada, la potencia libre, la potencia pico y los puertos alimentados.

12.8.2 Configuración global de PoE

Seleccione **Dispositivo local** > **Puertos** > **PoE** > **Configuración de PoE**.

El **Modo de potencia de transmisión** se refiere a la forma en que el dispositivo asigna la potencia a un PD conectado. Los valores son **Auto** o **Ahorro de energía**.

En modo **Auto**, el sistema asigna la potencia con base en las clases de PD detectados en los puertos. El dispositivo asigna la potencia a los PD de Clase 0 a 4 con base en un valor fijo:

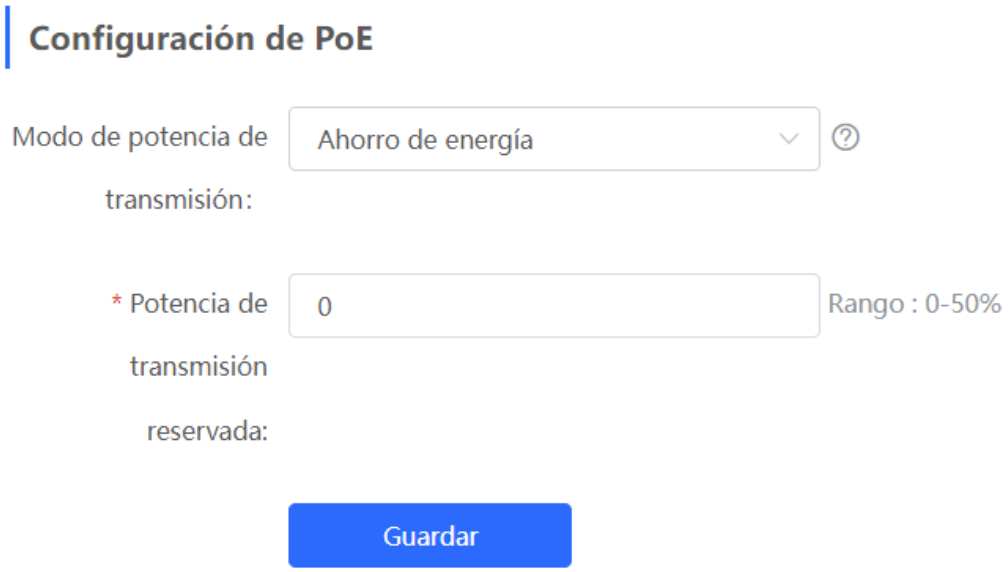
- Clase 0: 15.4 W
- Clase 1: 4 W
- Clase 2: 7 W

- Clase 3: 15.4 W
- Clase 4 Tipo 1: 15.4 W
- Clase 4 Tipo 2: 30 W

En este modo, si el puerto está conectado a un dispositivo de Clase 3 y el consumo de potencia es de 11 W solamente, el dispositivo PoE asignará la potencia al puerto con base en la potencia de 15.4 W.

En el modo **Ahorro de energía**, el dispositivo PoE ajusta dinámicamente la potencia asignada con base en el consumo real de los PD. Cuando la potencia está totalmente cargada, el consumo real de potencia del PD puede fluctuar. En este caso, la fuente de alimentación del puerto puede fluctuar en consecuencia. Para prevenir este problema, se puede configurar la **Potencia de transmisión reservada**. La potencia reservada en realidad no se utilizará para garantizar que la potencia total consumida por el sistema actual no exceda el límite del dispositivo PoE. La potencia reservada se expresa como un porcentaje total de potencia PoE Los rangos de valor van de 0 a 50.

Vigilancia de la PoE: la opción **Vigilancia de la PoE** permite supervisar el estado de los dispositivos alimentados (PD) que se encuentran conectados. Cuando el dispositivo alimentado (PD) no responde o deja de funcionar correctamente, la función Vigilancia de la PoE reinicia la función PoE del puerto de forma automática para restablecer el funcionamiento del PD.



12.8.3 Configuración de la fuente de alimentación de los puertos

Seleccione **Dispositivo local** > **Puertos** > **PoE**.> **Lista de puertos**.

Haga clic en **Editar** en el puerto correspondiente o en **Edición por lotes** para configurar la función de fuente de alimentación PoE del puerto.

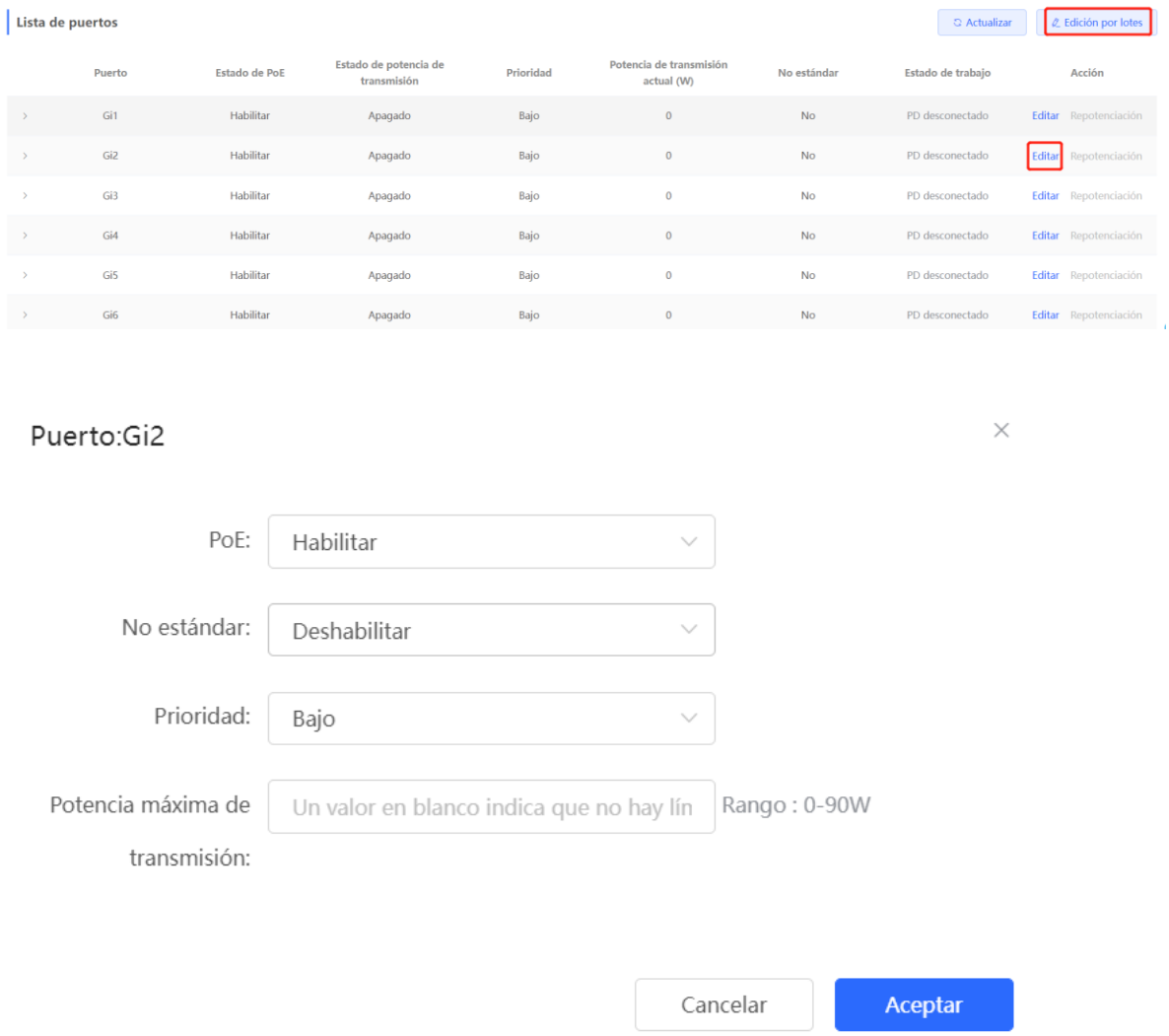


Tabla 12-6 Descripción de los parámetros para la configuración de la fuente de alimentación de los puertos

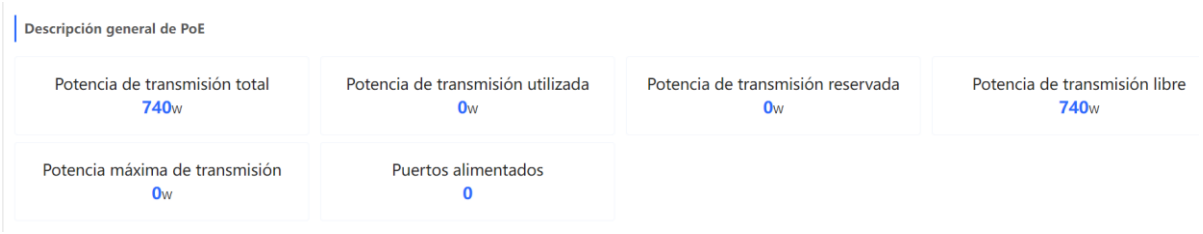
Parámetro	Descripción	Valor predeterminado
PoE	Determine si se habilita la función de fuente de alimentación en los puertos.	Habilitado
No estándar	Por defecto, el dispositivo solamente suministra potencia a los PD que cumplen con el estándar IEEE 802.3af y 802.3at. En la práctica, puede que algunos PD no cumplan con los estándares. Cuando el modo no estándar se habilita, el puerto del dispositivo puede suministrar potencia a algunos PD no estándar.	Deshabilitado

Parámetro	Descripción	Valor predeterminado
Prioridad	La prioridad de la fuente de alimentación del puerto se clasifica en tres niveles: **Alto**, **Medio** y **Bajo**. En los modos **Auto** y **Ahorro de energía**, los puertos con alta prioridad se encienden primero. Cuando la potencia PoE del sistema del dispositivo no es suficiente, los puertos con menor prioridad se apagan primero. Los puertos con la misma prioridad se ordenan de acuerdo con su número. Un puerto con menor número indica una prioridad mayor.	Bajo
Potencia máxima de transmisión	El rango de potencia máxima que un puerto puede transmitir es de 0 a 30, en watts (W). Un valor en blanco indica que no tiene límite.	Sin límite

12.8.4 Visualización de la información global de PoE

Seleccione **Dispositivo local** > **Puertos** > **PoE**.> **Descripción general de PoE**.

La página **Descripción general de PoE** muestra la información de la fuente de alimentación global de la función PoE, incluyendo la potencia total del sistema, la utilizada, la reservada, la restante disponible, el pico máximo de potencia y el número de puertos alimentados en ese momento.



12.8.5 Visualización de la información del puerto PoE

Seleccione **Dispositivo local** > **Puertos** > **PoE**.> **Lista de puertos**.

La página de **Lista de puertos** muestra la configuración PoE y el estado de cada puerto. Haga clic en para ampliar la información detallada.

Cuando el PD conectado al puerto se debe reiniciar (por ejemplo, cuando el AP conectado al puerto es anormal), se puede hacer clic en **Repotenciación** para apagar el puerto y luego encenderlo para restablecer el dispositivo conectado al puerto de alimentación.

Tabla 12-7 Descripción de la información de la fuente de alimentación de los puertos

Campo	Descripción
Puerto	ID del puerto del dispositivo.
Estado de PoE	Determine si desea habilitar la función de PoE en los puertos.
Estado de potencia de transmisión	Determine si actualmente el puerto suministra energía a los PD.
Prioridad	La prioridad de la fuente de alimentación del puerto se clasifica en tres niveles: **Alto**, **Medio** y **Bajo**.
Potencia de transmisión actual	Potencia de salida de la corriente del puerto, en watts (W).
No estándar	Determine si el modo de compatibilidad no estándar está habilitado.
Estado de trabajo	Estado de trabajo de los puertos PoE.
Corriente	Corriente actual del puerto, en miliamperios (mA).
Voltaje	Voltaje actual del puerto, en voltios (V).
Potencia de transmisión promedio	Potencia promedio de corriente del puerto; concretamente, el promedio de muestreo de la potencia de la corriente después de encender el puerto, en watts (W).
Potencia máxima de transmisión	Potencia de salida máxima del puerto, en watts (W).
Potencia de transmisión a solicitud del PD	Potencia solicitada por el PD al equipo proveedor de alimentación eléctrica (PSE), en watts (W).
Potencia de transmisión asignada por el PSE	Potencia asignada a un PD por el PSE, en watts (W).

Campo	Descripción
Tipo de PD	Información del tipo de PD obtenido mediante el LLDP. El valor es **Tipo 1** o **Tipo 2**.
Clase de PD	Nivel de PD conectado al puerto, que es de Clase 0-4, con base en los estándares IEEE 802.3af/802.3at.

13 Multidifusión de capa 2 de los switches de las series NBS y NIS

13.1 Descripción general de la multidifusión

Los métodos de transmisión del IP se clasifican en unidifusión, multidifusión y difusión. En el modo de multidifusión IP, un paquete IP se envía de un origen y se reenvía a un grupo específico de receptores. En comparación con la unidifusión y la difusión, la multidifusión IP ahorra en ancho de banda y reduce las cargas de la red. Por lo tanto, la multidifusión IP se aplica a los servicios de la red en tiempo real, como el Internet, la TV, la educación a distancia, las transmisiones en vivo y las conferencias multimedia.

13.2 Configuración global de la multidifusión

Seleccione **Dispositivo local** > **Multidifusión L2** > **Configuración global**.

La **Configuración global** le permite especificar la versión de IGMP, si se habilita la supresión de mensajes de informes, y el comportamiento del procesamiento de paquetes de multidifusión desconocidos.

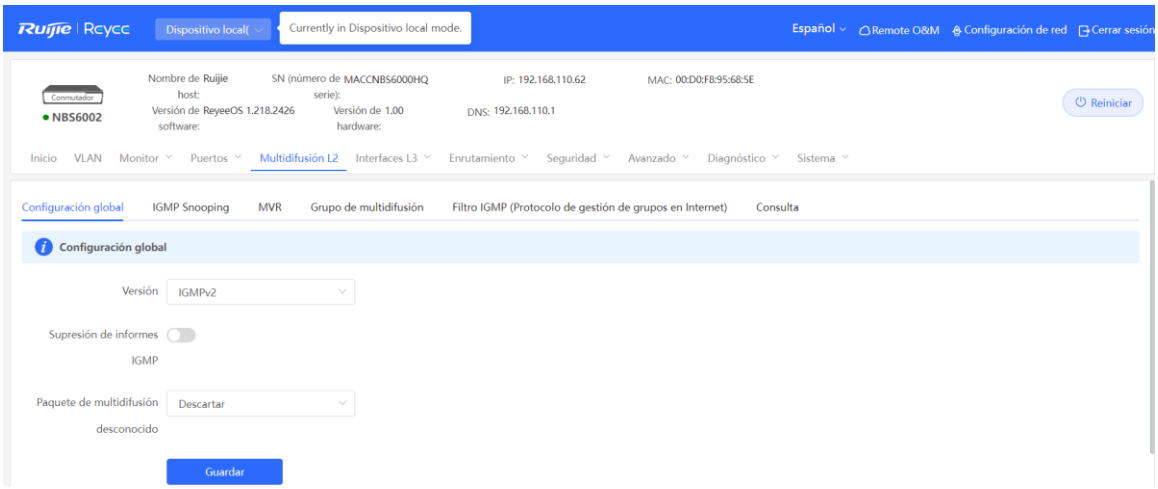


Tabla 13-1 Descripción de los parámetros para la configuración global de la multidifusión

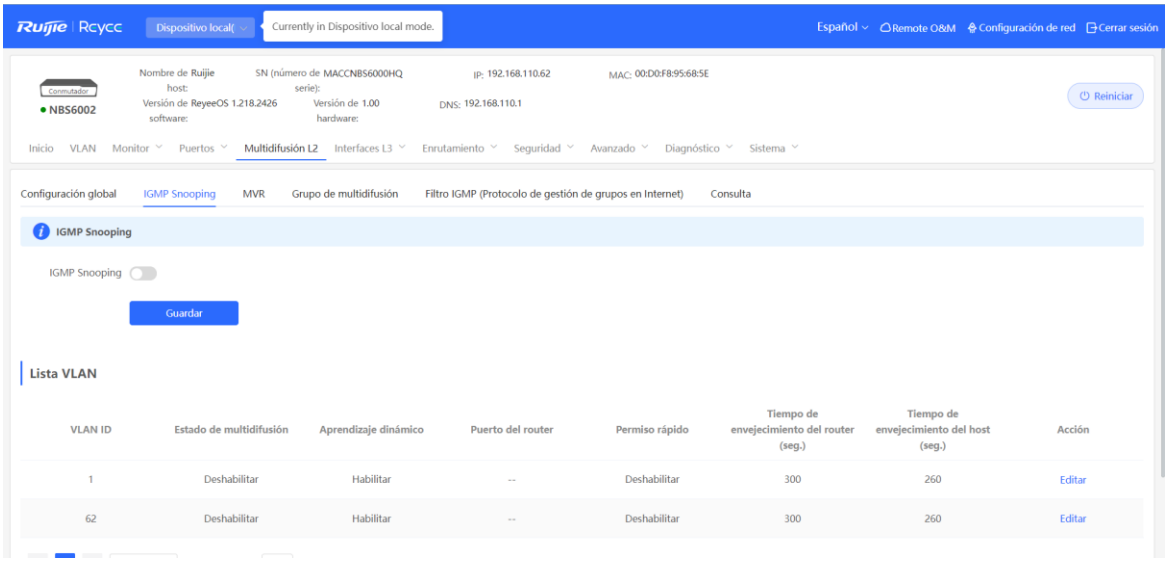
Parámetro	Descripción	Valor predeterminado
Versión	El Protocolo de gestión de grupos en Internet (IGMP) es un protocolo TCP/IP que administra los miembros de un grupo de multidifusión IPv4 y se ejecuta en dispositivos y hosts de multidifusión que residen en el stub de la red de multidifusión, creando y manteniendo la membresía del grupo de multidifusión entre los hosts y los dispositivos de multidifusión. Hay tres versiones de IGMP: IGMPv1, IGMPv2 e IGMPv3. Este parámetro se utiliza para configurar la versión más alta de paquetes IGMP que pueden procesarse en la multidifusión de Capa 2 y puede configurarse en IGMPv2 o IGMPv3.	IGMPv2
Supresión de informes IGMP	Esta función reduce el número de paquetes en la red, ahorra el ancho de banda de esta, y garantiza el desempeño del dispositivo de multidifusión IGMP. El conmutador reenvía solamente un mensaje de Informe al router de multidifusión si varios clientes de enlace descendente, conectados a este de manera simultánea, envían el mensaje de Informe para solicitar el mismo grupo de multidifusión.	Deshabilitado
Paquete de multidifusión desconocido	Cuando las funciones de multidifusión global y VLAN se habilitan, el método de procesamiento para recibir paquetes de multidifusión desconocidos puede configurarse en **Descartar** o **Desbordar**.	Descartar

13.3 IGMP Snooping

13.3.1 Descripción general

El IGMP Snooping o inspección IGMP es un mecanismo de inspección de multidifusión IP que se ejecuta en una VLAN para gestionar y controlar el tráfico de multidifusión IP dentro de la misma VLAN. Implementa una multidifusión de Capa 2.

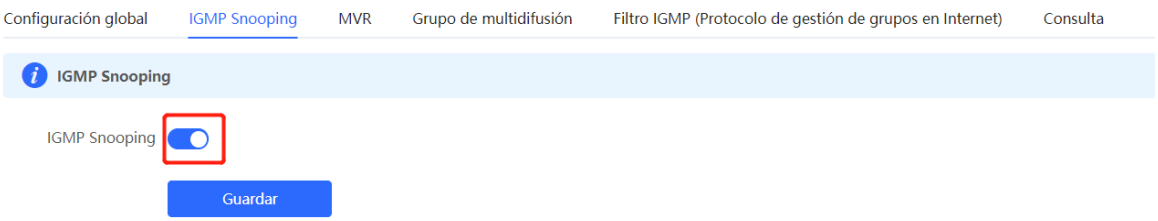
En la mayoría de los casos, los paquetes de multidifusión requieren pasar por conmutadores de Capa 2, especialmente en algunas redes de área local (LAN). Cuando el dispositivo de conmutación de Capa 2 no ejecuta el IGMP Snooping, los paquetes de multidifusión IP se difunden en la VLAN. Cuando el dispositivo de conmutación de Capa 2 ejecuta el IGMP Snooping, el dispositivo de Capa 2 puede escuchar los paquetes IGMP de un host de usuario y del dispositivo ascendente habilitado para PIM. De esta forma, se establece una entrada de multidifusión de Capa 2 y los paquetes de multidifusión IP se envían solamente a los receptores miembros del grupo, evitando que los datos de la multidifusión se difundan en la red de Capa 2.



13.3.2 Habilitar el IGMP Snooping global

Seleccione **Dispositivo local** > **Multidifusión L2** > **IGMP Snooping**.

Habilite **IGMP Snooping** y haga clic en **Guardar**.



13.3.3 Configuración de los parámetros del procesamiento de paquetes IGMP

Al controlar el procesamiento de los paquetes del protocolo, un dispositivo de multidifusión de Capa 2 puede establecer entradas estáticas o dinámicas para los reenvíos de multidifusión. Además, el dispositivo puede ajustar los parámetros para actualizar las entradas dinámicas para los reenvíos de multidifusión y la membresía del IGMP Snooping rápidamente.

Seleccione **Dispositivo local** > **Multidifusión** > **IGMP Snooping**.

El IGMP Snooping se implementa con base en las VLAN. Por lo tanto, a cada VLAN le corresponde una entrada de IGMP Snooping Hay tantas entradas IGMP Snooping como VLAN en el dispositivo.

Haga clic en **Editar** en la entrada de la VLAN. En el cuadro de diálogo que aparece, habilite o deshabilite el estado de multidifusión de la VLAN, el aprendizaje dinámico, el permiso rápido y el puerto del router; establezca el tiempo de envejecimiento y haga clic en **Aceptar**.

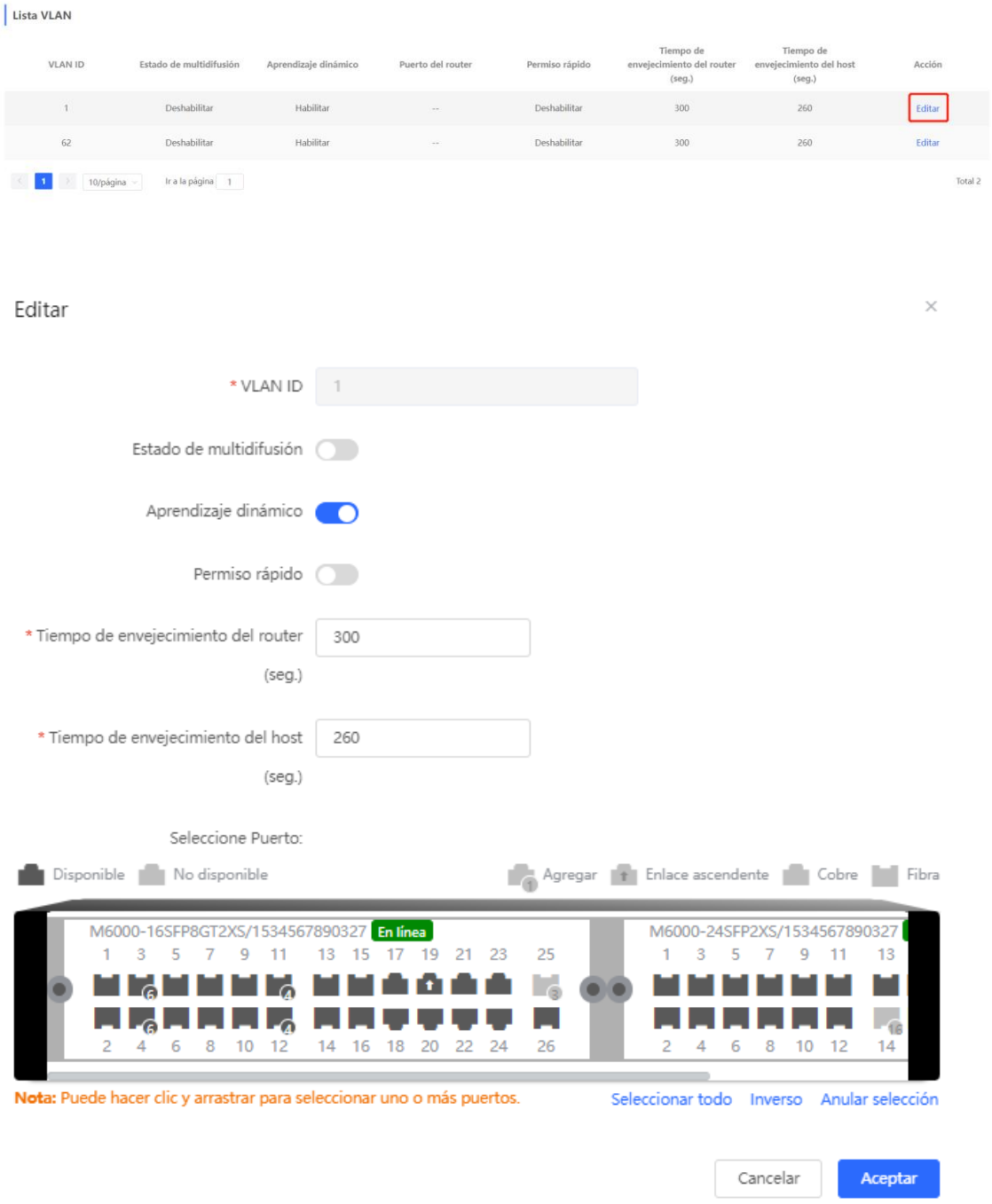


Tabla 13-2 Descripción de los parámetros para la configuración de la VLAN del IGMP Snooping

Parámetro	Descripción	Valor predeterminado
Estado de multidifusión	Determine si se habilita o deshabilita la función de VLAN de multidifusión. La función de multidifusión de la VLAN se hace efectiva únicamente cuando tanto el IGMP Snooping global como la VLAN de multidifusión están habilitados.	Deshabilitado

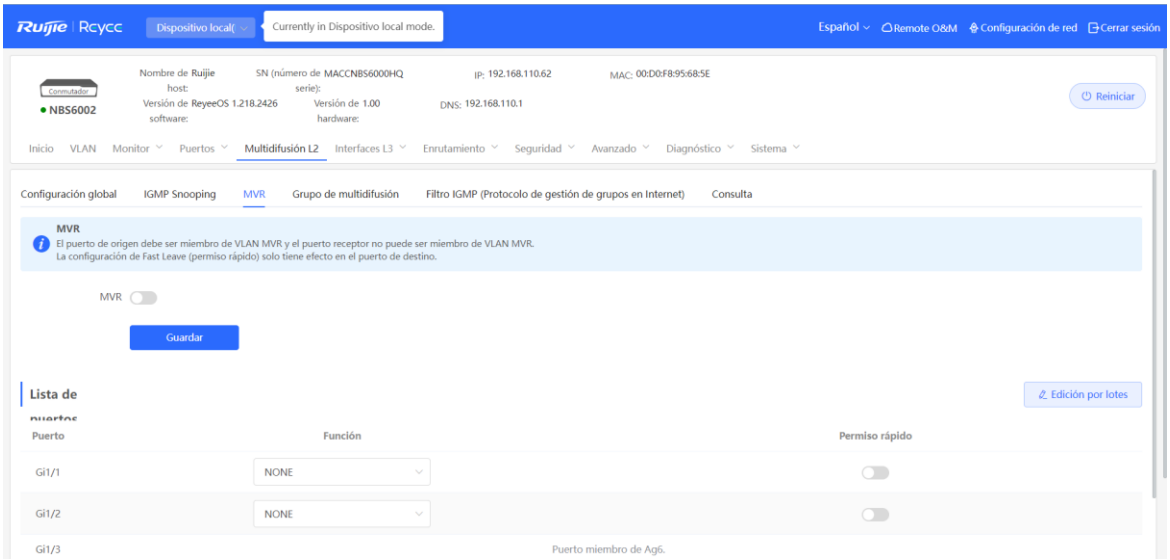
Parámetro	Descripción	Valor predeterminado
Aprendizaje dinámico	El dispositivo que ejecuta el IGMP Snooping identifica los puertos en la VLAN como puertos del router o puertos miembros. El puerto del router está localizado en el dispositivo de multidifusión de Capa 2 que está conectado al dispositivo de multidifusión de Capa 3; y el puerto miembro es el que está conectado al dispositivo de multidifusión de Capa 2. Al escuchar los paquetes IGMP, el dispositivo de multidifusión de Capa 2 puede descubrir y mantener automáticamente puertos de router dinámicos de multidifusión.	Habilitado
Puerto del router	La lista de puertos del router de multidifusión incluyen puertos enrutados dinámicamente aprendidos (si la función de aprendizaje dinámico está habilitada) y puertos enrutados configurados estáticamente.	NA
Permiso rápido	Al habilitar la función de permiso rápido, cuando el puerto reciba mensajes de Permiso, inmediatamente borrará el puerto del grupo de multidifusión sin esperar el tiempo de envejecimiento. Cuando el dispositivo reciba mensajes de Consulta y paquetes de datos de multidifusión del grupo específico correspondiente, el dispositivo no los seguirá reenviando al puerto. Esta función aplica cuando un host está conectado a un puerto del dispositivo y está habilitado en el conmutador de acceso directamente conectado a una terminal.	Deshabilitado
Tiempo de envejecimiento del router (seg.)	El dispositivo graba los puertos del dispositivo ascendente recibidos en la lista de puertos del router y borra el puerto donde no se han recibido datos cuando alcanza su tiempo de envejecimiento. En una red inestable, el puerto del router se borrará después de alcanzar su tiempo de envejecimiento, interrumpiendo las funciones de multidifusión. En este caso, se puede establecer un tiempo de envejecimiento más largo. El rango de tiempo de envejecimiento va de 30 a 3600, en segundos.	300 segundos

Parámetro	Descripción	Valor predeterminado
Tiempo de envejecimiento del host (seg.)	El dispositivo graba los puertos del host ascendentes recibidos en la lista de puertos del router y borra el puerto donde no se han recibido datos cuando alcanza su tiempo de envejecimiento. En una red inestable, el puerto del router se borrará después de alcanzar su tiempo de envejecimiento, interrumpiendo las funciones de multidifusión. En este caso, se puede establecer un tiempo de envejecimiento más largo. Es el tiempo de envejecimiento dinámicamente aprendido de los puertos miembros de un grupo de difusión, en segundos.	260 segundos
Seleccione Puerto	En el cuadro de diálogo que aparece, seleccione un puerto y configúrelo como el puerto del router estático. El puerto no envejecerá.	NA

13.4 Configuración del MVR

13.4.1 Descripción general

La función IGMP Snooping habilita un dispositivo para reenviar tráfico de multidifusión en la misma VLAN únicamente. Si el tráfico de multidifusión necesita enviarse a VLAN diferentes, el puerto de origen de multidifusión debe enviar el tráfico a diferentes VLAN. El registro de VLAN de multidifusión (MVR) permite ahorrar en el ancho de banda ascendente y reducir la carga de las fuentes de multidifusión. El MVR puede copiar el tráfico de multidifusión recibido de una VLAN MVR a la VLAN que pertenece el usuario, y reenviar el tráfico.



13.4.2 Configuración de los parámetros globales del MVR

Seleccione **Dispositivo local** > **Multidifusión L2** > **MVR**.

Habilite el MVR, seleccione la VLAN MVR, configure el grupo de multidifusión compatible con la VLAN y haga clic en **Guardar**. Se pueden especificar varios grupos de multidifusión ingresando las IP de multidifusión inicial y final.

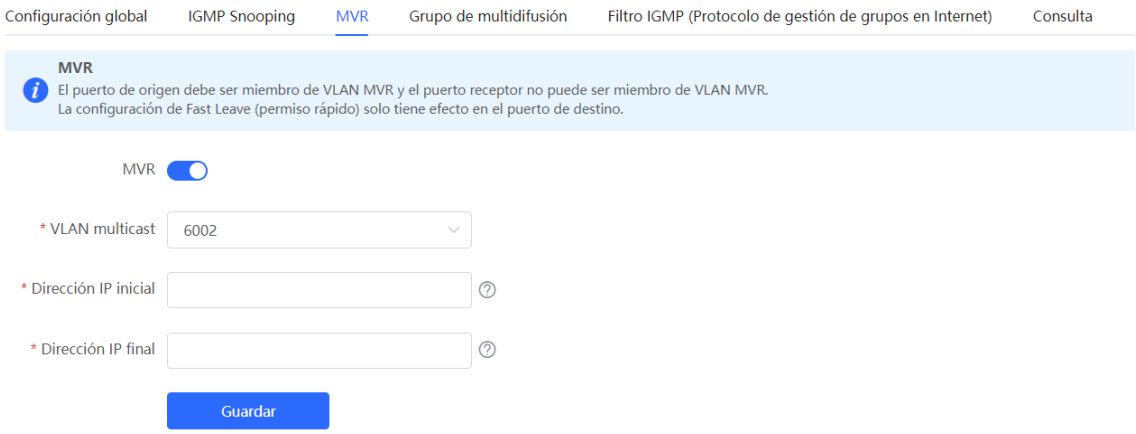


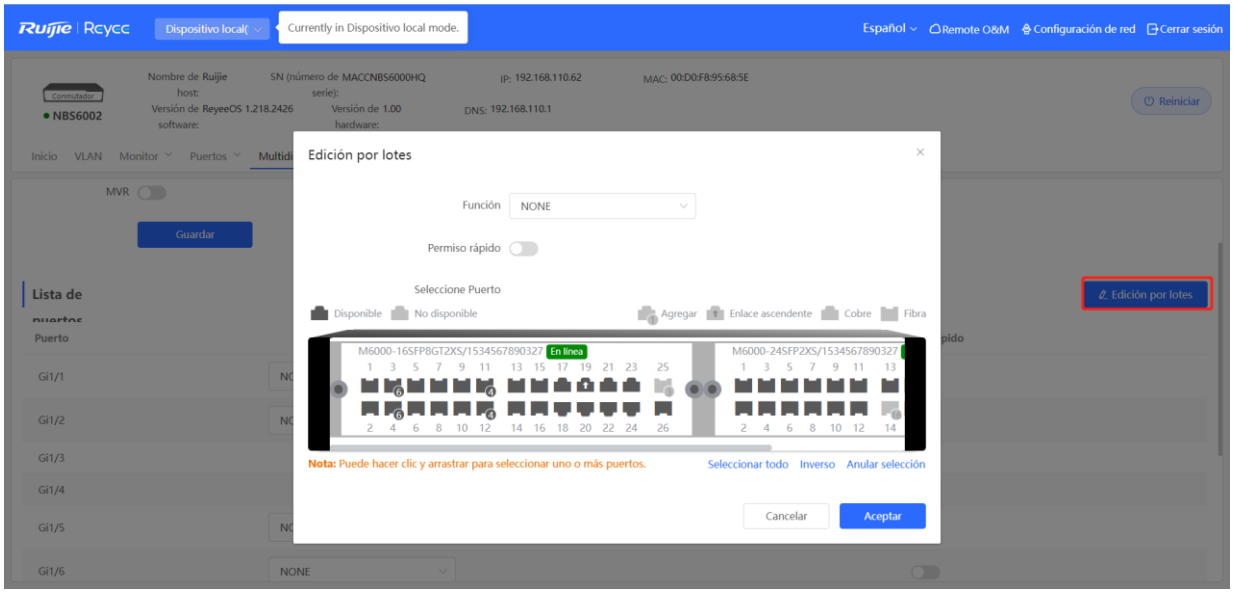
Tabla 13-3 Descripción de los parámetros para la configuración global del MVR

Parámetro	Descripción	Valor predeterminado
MVR	Habilitar o deshabilitar globalmente el MVR	Deshabilitado
VLAN de multidifusión	VLAN de una fuente de multidifusión.	1
Dirección IP inicial	Dirección IP inicial de multidifusión aprendida o configurada de un grupo de multidifusión MVR.	N/A
Dirección IP final	Dirección IP final de multidifusión aprendida o configurada de un grupo de multidifusión MVR.	N/A

13.4.3 Configuración de los puertos MVR

Seleccione **Dispositivo local** > **Multidifusión L2** > **MVR**.

Configuración por lotes: haga clic en **Edición por lotes**, seleccione la función del puerto y el puerto a configurar, elija si habilitar o no la función del permiso rápido en el puerto, y haga clic en **Aceptar**.



Configuración individual: haga clic en la lista desplegable para seleccionar el tipo de función del MVR del puerto. Haga clic en la columna **Permiso rápido** para configurar la función.

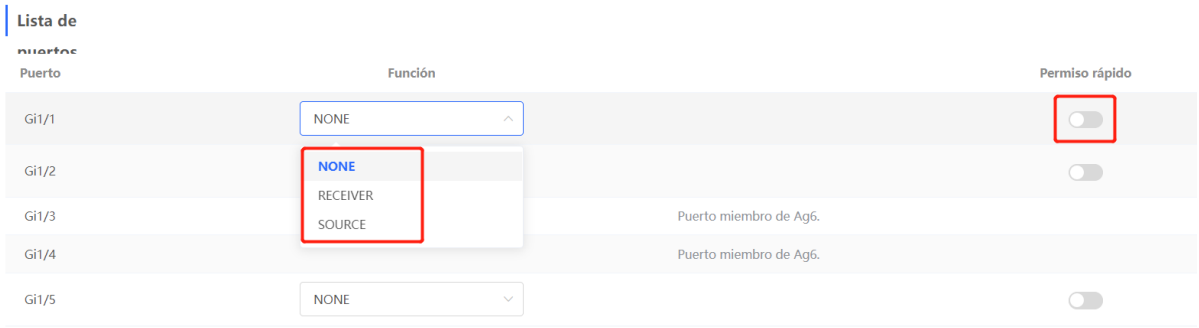


Tabla 13-4 Descripción de los parámetros para la configuración del MVR de los puertos

Parámetro	Descripción	Valor predeterminado
Función	**NONE**: la función MVR está deshabilitada. **SOURCE**: puerto de origen que recibe las transmisiones de datos de multidifusión. **RECEIVER**: puerto receptor conectado al cliente.	**NONE**
Permiso rápido	Configure la función de permiso rápido para el puerto. Con la función de permiso rápido habilitada, si el puerto recibe mensajes de permiso, el puerto se borra directamente del grupo de multidifusión.	**Deshabilitado**

Nota

- Si se configura un puerto origen o un puerto receptor, el puerto origen debe pertenecer a la VLAN MVR y el puerto receptor no debe pertenecer a esta.
- La función de permiso rápido es efectiva solamente en el puerto receptor.

13.5 Configuración de un grupo de multidifusión

Seleccione **Dispositivo local** > **Multidifusión L2** > **Grupo de multidifusión**.

Un grupo de multidifusión se compone de los puertos de destino a los que se enviarán los paquetes de multidifusión. Los paquetes de multidifusión se envían a todos los puertos del grupo de multidifusión.

Visualice la **Lista de multidifusión** en la página actual. Puede hacer consultas sobre entradas del grupo de multidifusión en la barra de búsqueda, en la esquina superior derecha, con base en la VLAN ID o las direcciones de multidifusión.

Haga clic en **Añadir** para crear un grupo de multidifusión.

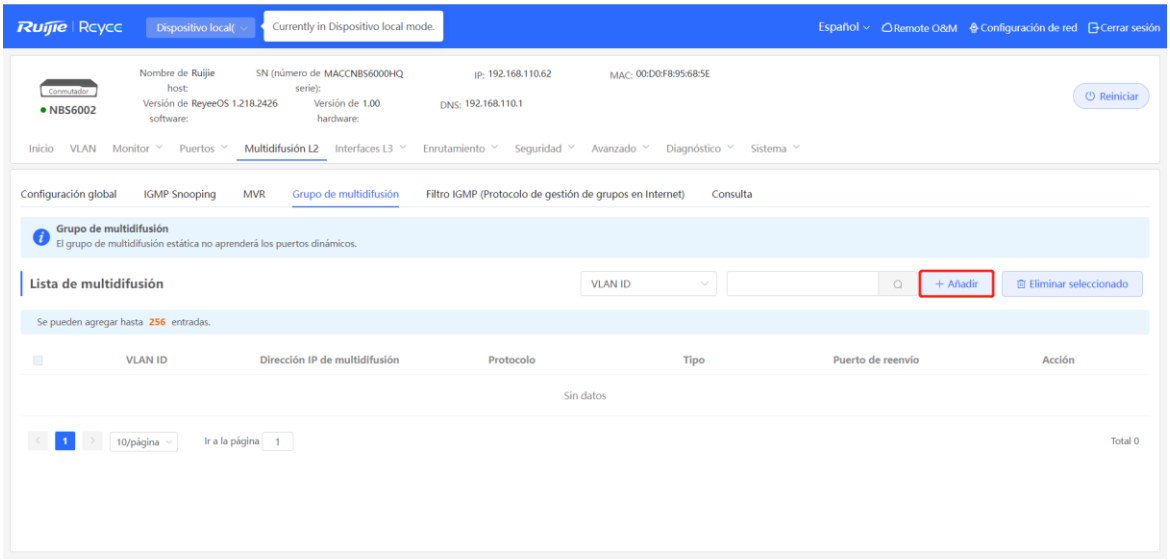


Tabla 13-5 Descripción de los parámetros para la configuración del grupo de multidifusión

Parámetro	Descripción	Valor predeterminado
VLAN ID	VLAN a la que pertenece el tráfico de multidifusión recibido.	N/A
Dirección IP de multidifusión	Dirección IP de multidifusión bajo pedido.	N/A
Protocolo	Si la VLAN ID es de multidifusión y la dirección de multidifusión está dentro del rango de la dirección IP de multidifusión MVR, se utiliza MVR. En cualquier otro caso, se utiliza IGMP Snooping.	N/A
Tipo	Los modos para generar grupos de multidifusión pueden ser estáticamente configurados o dinámicamente aprendidos. En situaciones normales, un puerto puede unirse al grupo de multidifusión solo después de que este reciba un mensaje de Informe de IGMP en modo multidifusión (modo dinámicamente aprendido). Si un puerto es añadido manualmente a un grupo, este puede ser estáticamente añadido e intercambiar información del grupo de multidifusión con el router PIM sin intercambiar paquetes con IGMP.	N/A
Puerto de reenvío	Lista de puertos que reenvían tráfico de multidifusión.	N/A

Nota

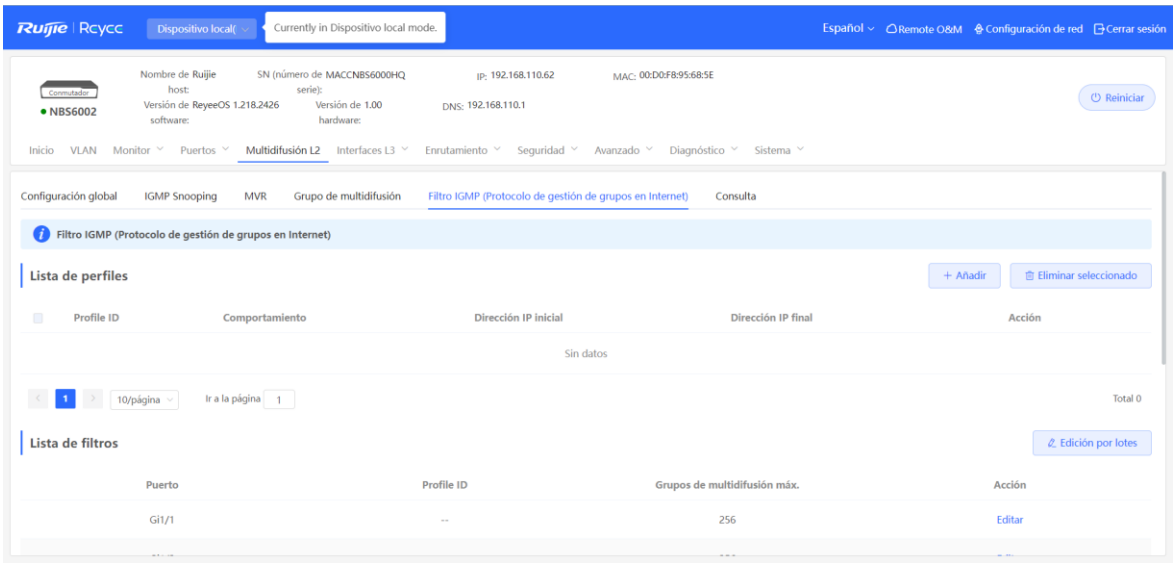
Los grupos de multidifusión estáticos no pueden aprender puertos de reenvío dinámicos.

13.6 Configuración del filtro de un puerto

Seleccione **Dispositivo local** > **Multidifusión L2** > **Filtro IGMP**.

Generalmente, los puertos activos en un dispositivo pueden unirse a cualquier grupo de multidifusión. Se puede utilizar un filtro de puerto para configurar un rango de grupos de multidifusión que permita o niegue el acceso del usuario. El alcance del servicio de multidifusión para usuarios se puede personalizar, para garantizar el interés de los operadores y prevenir el tráfico de multidifusión no válido.

Para configurar el filtro de un puerto, configure un perfil y un rango para la dirección de grupo del puerto.



13.6.1 Configuración de un perfil

Seleccione **Dispositivo local** > **Multidifusión L2** > **Filtro IGMP > Lista de perfiles**.

Haga clic en **Añadir** para crear un **Perfil**. El perfil se utiliza para definir un rango de grupos de multidifusión que permita o niegue el acceso del usuario; además, es referencia para otras funciones.

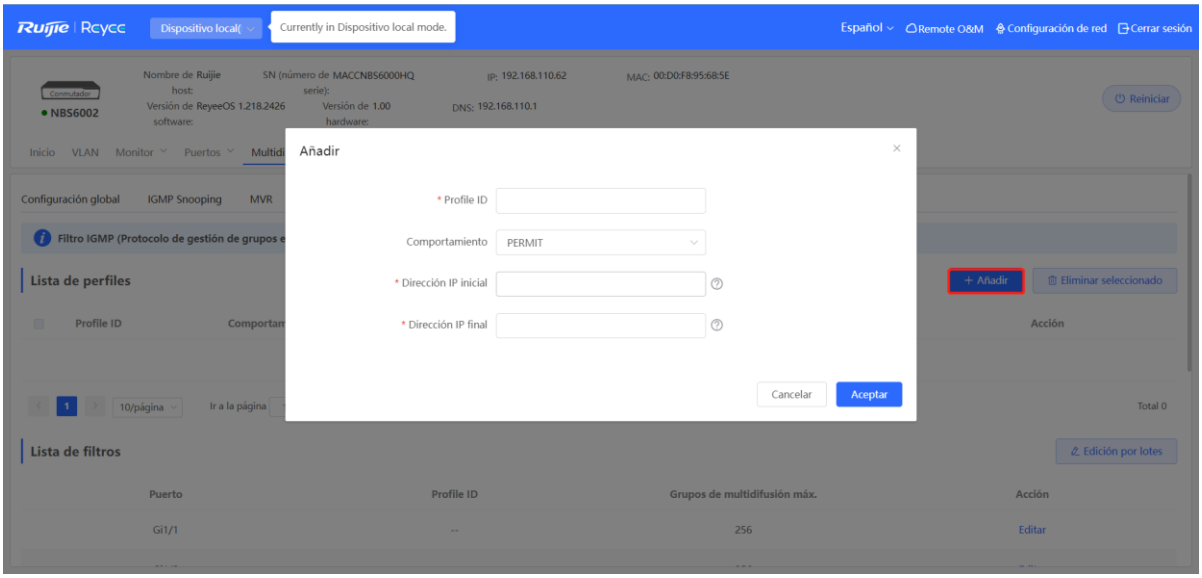


Tabla 13-6 Descripción de los parámetros para la configuración de perfiles

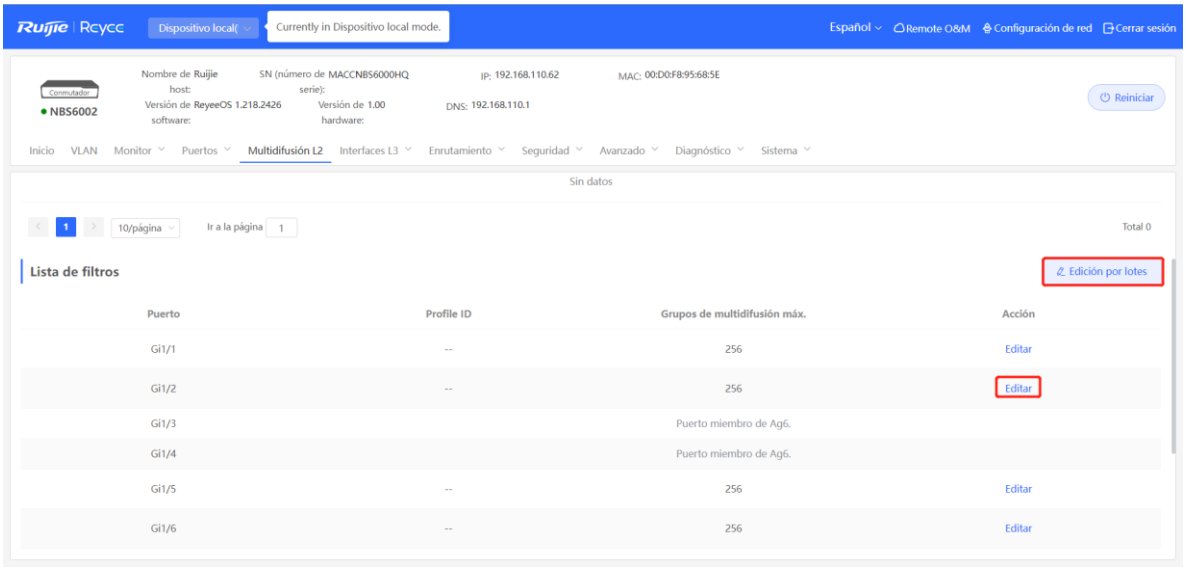
Parámetro	Descripción	Valor predeterminado
ID del perfil	Identificador del perfil.	NA
Comportamiento	DENEGAR: prohíbe las direcciones IP de multidifusión en un rango específico. PERMITIR: autoriza las direcciones IP de multidifusión solicitadas en un rango específico.	NA
Dirección IP inicial	Dirección IP de multidifusión de inicio dentro del rango de direcciones del grupo de multidifusión.	NA
Dirección IP final	Dirección IP final de multidifusión dentro del rango de direcciones del grupo de multidifusión.	NA

13.6.2 Configuración de un rango de grupos de multidifusión para un perfil

Seleccione **Dispositivo local** > **Multidifusión L2** > **Filtro IGMP > Lista de filtros**.

El filtro del puerto puede hacer referencia a un perfil para definir el rango de direcciones del grupo de multidifusión permitidas o rechazadas.

Haga clic en **Edición por lotes** o en **Editar** de un puerto en particular. En el cuadro de diálogo que aparece, seleccione ID del perfil e ingrese el número máximo de grupos de difusión permitidos por el puerto; haga clic en **Aceptar**.



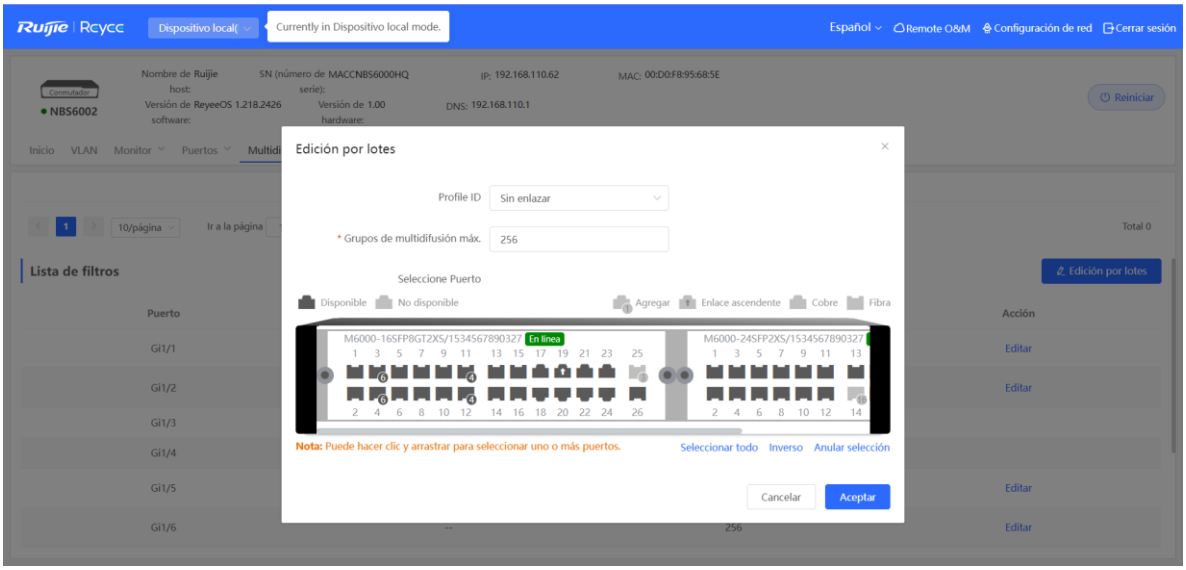


Tabla 13-7 Descripción de los parámetros para la configuración un filtro de puerto

Parámetro	Descripción	Valor predeterminado
ID del perfil	Es el perfil que se hace efectivo en el puerto. Si no se configura, este no se vincula al puerto.	NA

Parámetro	Descripción	Valor predeterminado
Grupos de multidifusión máx.	Número máximo de grupos de multidifusión a los que un puerto puede unirse. Si se solicita tráfico pesado de multidifusión en paralelo, el dispositivo de multidifusión puede sufrir daños graves. Por lo tanto, configure el número máximo de grupos de multidifusión permitidos para que el puerto pueda garantizar el ancho de banda.	256

13.7 Configuración de un consultante IGMP

13.7.1 Descripción general

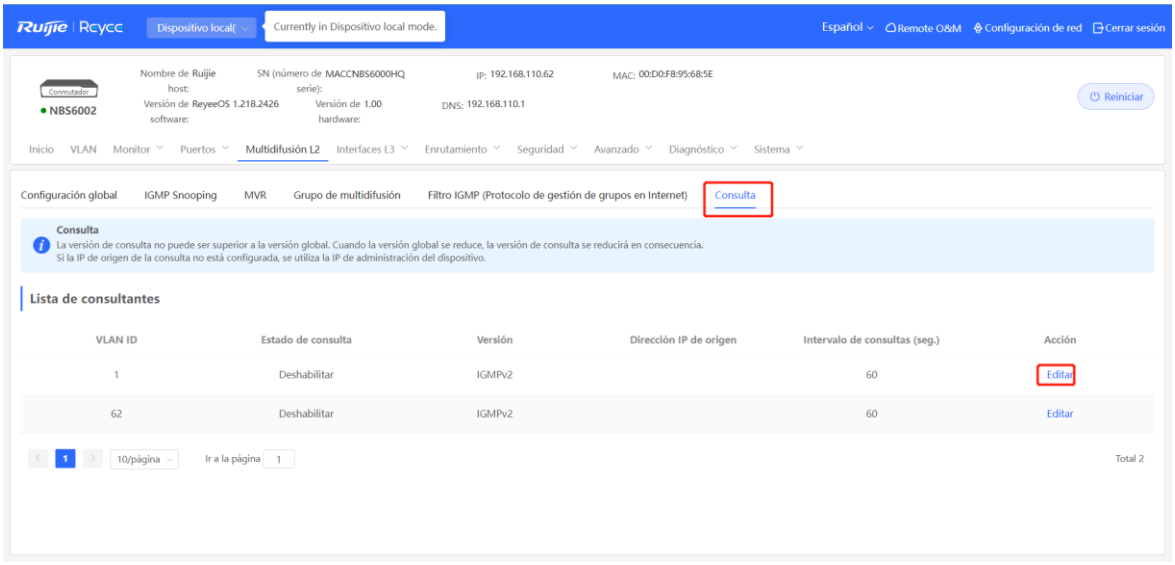
En una red de multidifusión de tres capas, el dispositivo de multidifusión de Capa 3 funciona como el consultante y ejecuta el IGMP para mantener la membresía del grupo. Los dispositivos de multidifusión de Capa 2 solo requieren escuchar a los paquetes IGMP para establecer y mantener las entradas de reenvío e implementar la multidifusión de Capa 2. Cuando una fuente de difusión y un host de usuario están en la misma red de Capa 2, la función de consulta no aparece disponible porque dicho dispositivo de Capa 2 no admite IGMP. Para resolver el problema, configure la función de consultante IGMP Snooping en el dispositivo de Capa 2, para que este mande los paquetes de consulta IGMP a los hosts de usuario, de parte del dispositivo de multidifusión de Capa 3, y escuche y preserve los paquetes de Informe IGMP respondidos por los hosts de usuarios para establecer entradas de reenvío de multidifusión de Capa 2.

13.7.2 Procedimiento

Seleccione **Dispositivo local** > **Multidifusión L2** > **Consulta**.

Configure un consultante por cada VLAN. El número de consultantes es el mismo que el de los dispositivos VLAN.

En **Lista de consultantes**, haga clic en el botón **Editar**, en la columna **Acción**. En el cuadro de diálogo que aparece, seleccione si desea habilitar un consultante, defina la versión de este y la dirección IP de origen, así como el intervalo de consultas del paquete, y haga clic en **Aceptar**.



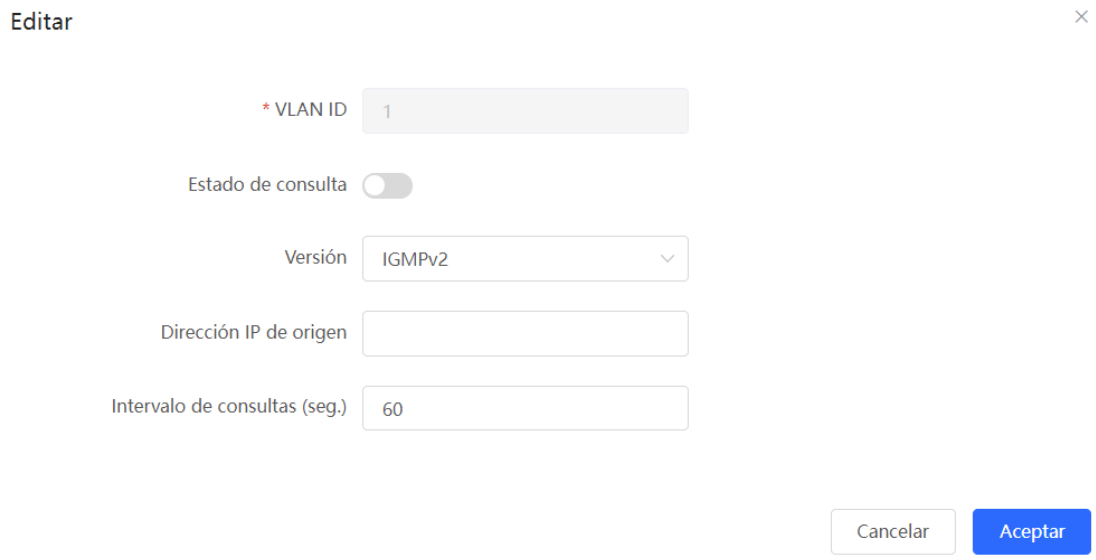


Tabla 13-8 Descripción de los parámetros para la configuración de consultantes

Parámetro	Descripción	Valor predeterminado
Estado de consulta	Habilite o deshabilite la función de consultante VLAN.	Deshabilitado
Versión	Versión del protocolo IGMP de paquetes de consulta enviados por el consultante. Se puede configurar en IGMPv2 o IGMPv3.	IGMPv2
Dirección IP de origen	Dirección IP de origen transportada en paquetes de consulta enviados por el consultante.	NA

Parámetro	Descripción	Valor predeterminado
Intervalo de consultas (seg.)	Intervalo de transmisión del paquete. El rango de tiempo de envejecimiento va de 30 a 18000, en segundos.	60 segundos

Nota

- La versión de consultante no puede ser posterior a la versión global de IGMP. Si se utiliza una versión anterior de IGMP global, se necesita una versión anterior de consultante en consecuencia.
- Si no se configura una dirección IP de origen para el consultante, la dirección IP de gestión del dispositivo se usará como la dirección IP de origen del consultante.

14 Multidifusión de capa 3 de los switches de las series NBS y NIS

14.1 Descripción general

La multidifusión de capa 3 (L3 Multicast) es un método de comunicación que utiliza el direccionamiento multidifusión en la capa de red para enviar datos. La multidifusión permite que el emisor envíe paquetes a un grupo de receptores al mismo tiempo, lo que reduce el consumo de ancho de banda de la red y disminuye su carga. Este tipo de multidifusión se utiliza ampliamente en aplicaciones como las videoconferencias, los medios de retransmisión y la VoIP, entre otras.

En la multidifusión de capa 3, cada dirección de grupo de multidifusión corresponde a un grupo de multidifusión concreto y los miembros de un grupo de multidifusión comparten la misma dirección de grupo de multidifusión. El emisor envía paquetes de datos a la dirección de grupo de multidifusión y los routers de la red reenvían los paquetes a todos los miembros del grupo de multidifusión en función de la dirección de grupo de multidifusión y los protocolos de enrutamiento que se utilicen.

14.2 Tabla de enrutamiento multidifusión

Seleccione **Dispositivo local** > **L3 Multicast** > **Multicast Routing Table**.

En la página **Multicast Routing Table** se muestra la información de la tabla de enrutamiento multidifusión de capa 3, incluida la dirección IP de origen, la dirección de grupo de multidifusión, la interfaz de entrada, la interfaz de salida y el tiempo de vida (TTL). Puede buscar la información de enrutamiento basándose en la dirección IP de origen o en la dirección de grupo de multidifusión. Si lo desea, puede hacer clic en **Actualizar** para ver la información actualizada de la tabla de enrutamiento multidifusión.

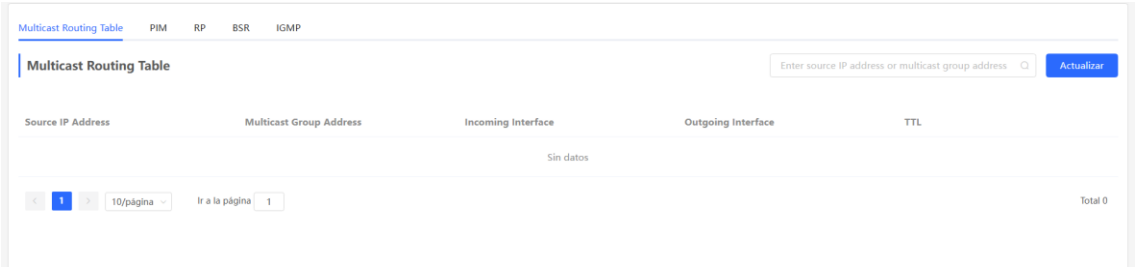


Tabla 14-1 Descripción de los parámetros de la tabla de enrutamiento multidifusión (Mulicast Routing Table)

Parámetro	Descripción	Valor predeterminado
Source IP Address	Dirección IP del dispositivo de origen que envía el paquete de multidifusión.	N/A
Multicast Group Address	Dirección IP especial que identifica a un grupo de multidifusión. En la tabla de enrutamiento, la dirección de grupo de multidifusión es la dirección IP del grupo de multidifusión de destino.	N/A

Parámetro	Descripción	Valor predeterminado
Incoming Interface	Interfaz que recibe los paquetes de multidifusión.	N/A
Outgoing Interface	Cuando el router recibe un paquete de multidifusión, lo reenvía a la interfaz de salida correspondiente en función del valor del campo Outgoing Interface (interfaz de salida) de la tabla de enrutamiento.	N/A
TTL	El valor TTL es el tiempo durante el cual una entrada de la tabla de enrutamiento continúa siendo válida. Una vez que transcurre este tiempo, se considera que la entrada de la tabla de enrutamiento ha caducado y deja de utilizarse.	N/A

14.3 Configuración del protocolo PIM

14.3.1 Descripción general

La multidifusión independiente del protocolo (PIM) es un protocolo de enrutamiento multidifusión intradominio independiente del protocolo. Este protocolo permite utilizar la comunicación multidifusión por medio del uso de distintos protocolos de enrutamiento unidifusión, incluidos, entre otros, el enrutamiento estático, el RIP y el OSPF. A través del uso del protocolo PIM, los routers pueden intercambiar información del enrutamiento multidifusión, lo que permite establecer y mantener árboles multidifusión y, de este modo, entregar los paquetes de datos de multidifusión de forma eficiente desde la fuente a los receptores dentro del grupo de multidifusión.

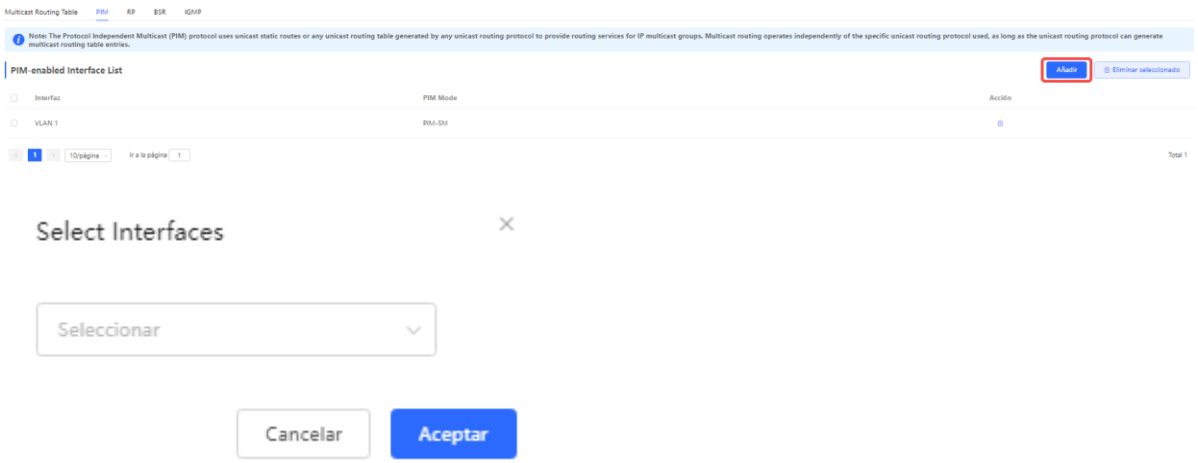
El protocolo PIM se encuentra disponible en dos modos ampliamente utilizados:

- El modo denso PIM (PIM-DM)
  Este modo puede utilizarse en redes de pequeña escala o en escenarios con tráfico de multidifusión denso. En el modo PIM-DM, los paquetes de multidifusión se envían por todas las rutas disponibles, lo que se traduce en un mayor ancho de banda de la red y un mayor consumo de recursos.
- El modo disperso (PIM-SM)
  Este modo puede utilizarse en redes de gran escala o escenarios con tráfico de multidifusión disperso. En el modo PIM-SM, los routers solo reenvían los paquetes de multidifusión por las rutas necesarias, lo que reduce de forma eficaz el uso del ancho de banda de la red.

14.3.2 Habilitación del protocolo PIM

Seleccione **Dispositivo local** > **L3 Multicast** > **PIM** > **PIM-enabled Interface List**.

Haga clic en **Añadir**. Aparece una ventana emergente. En la ventana emergente, seleccione la interfaz en la que desee habilitar el PIM y haga clic en **Aceptar**. El reenvío de paquetes de multidifusión puede utilizarse en la interfaz que seleccione. El modo PIM que se muestra de forma predeterminada es el modo PIM-SM.



14.3.3 Visualización de la tabla de dispositivos cercanos del PIM

En el protocolo PIM, los routers detectan los routers cercanos y establecen relaciones de proximidad mediante el intercambio de mensajes Hello. Una vez que se establece una relación de proximidad entre dos routers compatibles con el PIM, estos pueden intercambiar información de multidifusión, incluida las adhesiones a grupos de multidifusión y los estados de los reenvíos de multidifusión. Al actualizar y mantener la tabla de dispositivos cercanos del PIM de forma continua, los routers compatibles con el PIM pueden reenviar y procesar los paquetes de multidifusión de forma eficaz basándose en la información de los dispositivos cercanos, lo que permite lograr una comunicación multidifusión eficaz.

Seleccione **Dispositivo local** > **L3 Multicast** > **PIM** > **PIM Neighbor Table**.

En la página **PIM Neighbor Table** se muestra información de los dispositivos cercanos del PIM como la interfaz, el dispositivo cercano del PIM, el TTL y el tiempo de caducidad. Puede buscar información de la tabla de dispositivos cercanos del PIM introduciendo la interfaz o el dispositivo cercano del PIM en el cuadro de búsqueda. Si lo desea, puede hacer clic en **Actualizar** para ver la información actualizada de la tabla de dispositivos cercanos del PIM.

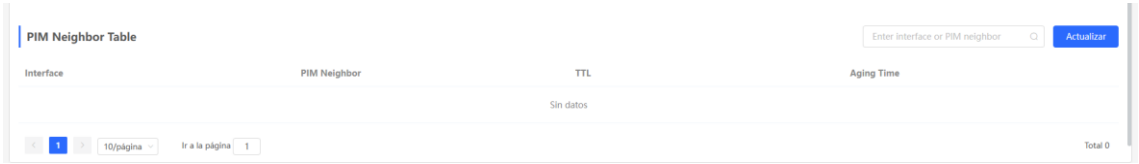


Tabla 14-2 Descripción de los parámetros de la tabla de dispositivos cercanos del PIM

Parámetro	Descripción	Valor predeterminado
Interface	Interfaz que conecta el router cercano al router local.	N/A
PIM Neighbor	Dirección IP del router cercano.	N/A

Parámetro	Descripción	Valor predeterminado
TTL	El valor TTL indica el tiempo durante el cual los mensajes Hello que envían los routers cercanos continúan siendo válidos. Si el router local no recibe ningún mensaje Hello nuevo de un dispositivo dentro del tiempo del TTL, este considerará que el router cercano se encuentra inactivo o ha caducado.	N/A
Aging Time	Si un router cercano se vuelve inactivo o deja de enviar mensajes Hello, la entrada correspondiente de la tabla de dispositivos cercanos del PIM se eliminará una vez que haya transcurrido el tiempo de caducidad que se haya indicado.	105 segundos

14.4 Configuración del RP

14.4.1 Descripción general

El punto de encuentro (RP) constituye un concepto fundamental del protocolo PIM. En la comunicación multidifusión, cuando un emisor envía un paquete de datos de multidifusión, este debe identificar un punto específico como punto de encuentro desde el que los distintos receptores puedan recibir el paquete de multidifusión. El RP es el router del punto de encuentro en el árbol de multidifusión. Los RP pueden configurarse manualmente o elegirse de forma dinámica a través del mecanismo BSR (router de arranque).

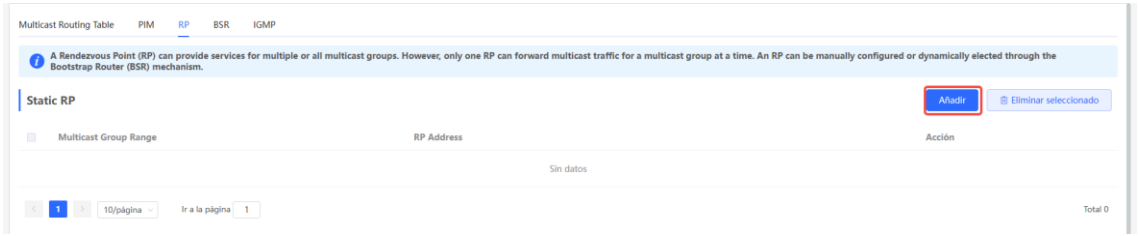
Nota

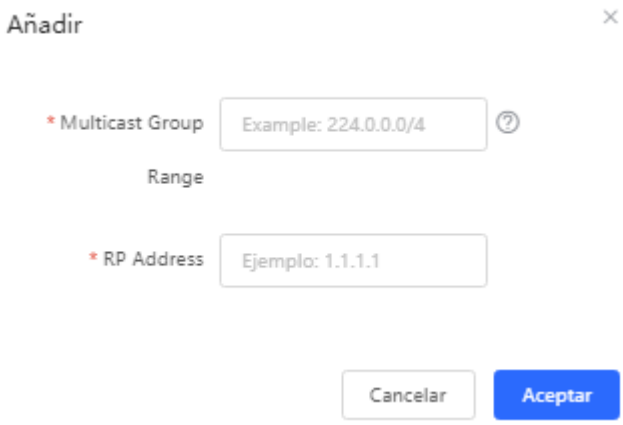
Un RP puede proporcionar servicios a varios o a todos los grupos de multidifusión. Sin embargo, solo un RP puede reenviar tráfico de multidifusión para un grupo de multidifusión a la vez.

14.4.2 Configuración de un RP estático

Seleccione **Dispositivo local** > **L3 Multicast** > **RP** > **Static RP**.

Haga clic en **Añadir**. En la ventana emergente que se muestra, introduzca el rango de grupos de multidifusión cubierto por el RP y la dirección del RP y, a continuación, haga clic en **Aceptar**.





14.4.3 Configuración de un RP candidato

En las redes basadas en el protocolo PIM, el RP candidato se refiere a un router que cumple los requisitos para convertirse en RP. Puede configurar distintos routers compatibles con el PIM en el dominio del PIM como RP candidatos para que se elija un RP adecuado. Este proceso permite mejorar la eficacia y la fiabilidad de la comunicación multidifusión.

Seleccione **Dispositivo local** > **L3 Multicast** > **RP** > **Candidate RP**.

Active la opción **Local routing device as candidate RP:** para establecer el dispositivo local como el RP candidato. Introduzca la prioridad, el intervalo de anuncio, la dirección IP de origen y el grupo de multidifusión seleccionado. A continuación, haga clic en **Guardar**.

Tabla 14-3 Descripción de los parámetros de configuración del RP candidato

Parámetro	Descripción	Valor predeterminado
Priority	La prioridad determina qué RP candidato se convertirá en el RP durante el proceso de elección. Puede seleccionar un valor para la prioridad entre 0 y 255, siendo el valor menor el que indica una mayor prioridad. De este modo, cuanto mayor es la prioridad de un RP candidato, más posibilidades tiene de ser elegido como el RP.	192
Advertisement Interval	Un RP candidato anuncia su presencia y su disponibilidad enviando mensajes PIM. El intervalo de anuncio determina la frecuencia con la que un RP candidato envía estos mensajes. Si se acorta el intervalo de anuncio, puede notificarse a otros routers la presencia de un RP candidato con mayor rapidez, aunque también se incrementa la carga de la red.	60 segundos
Source IP Address	La dirección IP de origen de los mensajes PIM que envía el RP candidato, que pueden ser una interfaz o una dirección IP.	N/A
Designated multicast group	Los mensajes PIM que envía el RP candidato deben contener una dirección de grupo de multidifusión comprendida entre 224.0.0.0/4 y 239.255.255.255/32. Los RP candidatos suelen enviar varios mensajes, donde cada uno de ellos indica una dirección de grupo de multidifusión diferente, para notificar a otros routers que pueden convertirse en el RP de estos grupos de multidifusión. Puede hacer clic en **Añadir** para configurar varias direcciones de grupo de multidifusión.	N/A

14.5 Configuración del BSR

14.5.1 Descripción general

En el modo PIM-SM, el RP debe configurarse manualmente, lo cual supone una tarea tediosa para las redes de gran escala. El mecanismo BSR (router de arranque) permite seleccionar de forma automática el RP, lo que simplifica el proceso de configuración del RP. El BSR actúa como el eje central de la gestión del dominio PIM-SM y es responsable de recopilar y anunciar la información del RP dentro del dominio. El BSR es elegido por los BSR candidatos.

Nota

Un dominio PIM-SM solo puede tener un BSR, aunque puede tener distintos BSR candidatos.

14.5.2 Configuración del BSR

Seleccione **Dispositivo local** > **L3 Multicast** > **BSR** > **Local Routing Device as Candidate BSR**.

Active la opción **Local routing device as candidate BSR:** para que el dispositivo local se convierta en el BSR candidato. Introduzca la prioridad y la dirección IP de origen. A continuación, haga clic en **Guardar**.

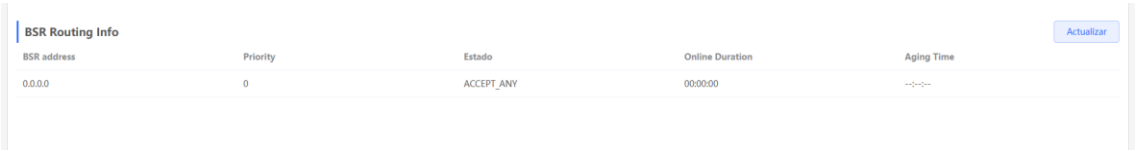
Tabla 14-4 Descripción de los parámetros de configuración del BSR candidato

Parámetro	Descripción	Valor predeterminado
Priority	Los BSR candidatos con mayor prioridad tienen más posibilidades de ser elegidos como el BSR. Puede seleccionar un valor para la prioridad entre 0 y 255, siendo el valor menor el que indica una mayor prioridad.	192
Source IP Address	La dirección IP de origen de los mensajes PIM que envía el BSR candidato, que pueden ser una interfaz o una dirección IP.	N/A

14.5.3 Visualización de la información de enrutamiento del BSR

Seleccione **Dispositivo local** > **L3 Multicast** > **BSR** > **BSR Routing Info**.

En la página **BSR Routing Info** se muestra la información de enrutamiento del BSR, incluida la dirección del BSR, la prioridad, el estado, el tiempo de conexión y el tiempo de caducidad. Si lo desea, puede hacer clic en **Actualizar** para ver la información actualizada del enrutamiento del BSR.



14.6 Configuración del IGMP

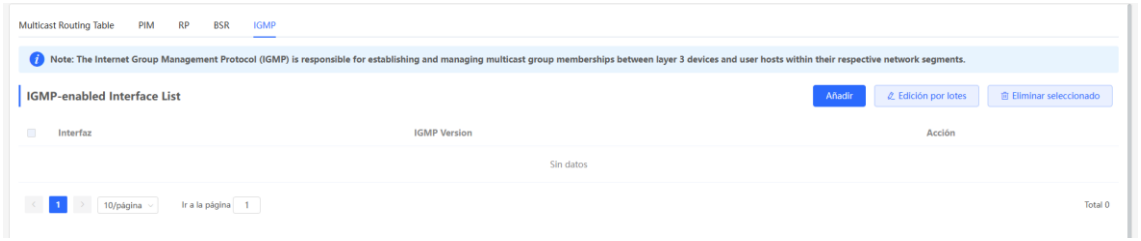
14.6.1 Descripción general

El protocolo de gestión de grupos de Internet (IGMP) se utiliza para permitir la comunicación multidifusión en redes IPv4. El IGMP se ocupa de gestionar la adhesión a los grupos de multidifusión, así como de facilitar la comunicación entre los hosts y los routers de multidifusión. Con el protocolo IGMP, los hosts pueden unirse o abandonar un grupo de multidifusión determinado y anunciar su adhesión a los routers de multidifusión. Los routers de multidifusión utilizan el IGMP para determinar qué hosts son miembros de un grupo de multidifusión, lo que permite reenviar el tráfico de multidifusión de manera eficaz.

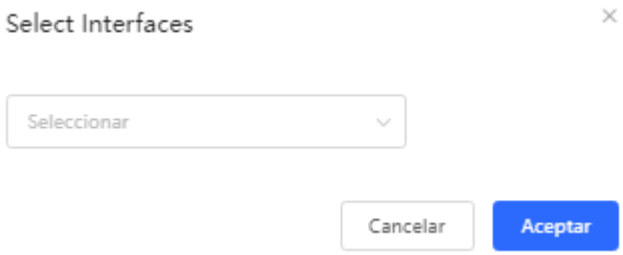
14.6.2 Habilitación del protocolo IGMP

Seleccione **Dispositivo local** > **L3 Multicast** > **IGMP** > **IGMP-enabled Interface List**.

En la página **IGMP-enabled Interface List** se muestra información básica de las interfaces compatibles con el IGMP, incluida la interfaz y la versión del IGMP.

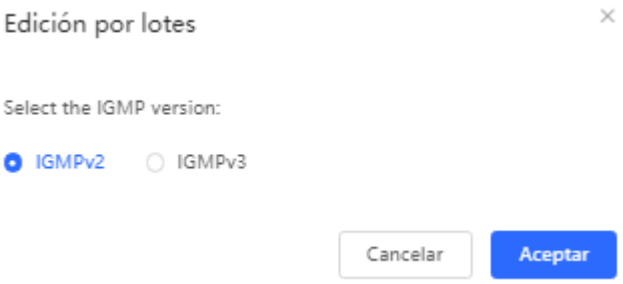


Añadir: haga clic en **Añadir**. Aparece la venta emergente **Select Interfaces**. En la ventana emergente, seleccione la interfaz en la que desee habilitar el IGMP. A continuación, haga clic en **Aceptar**. El IGMP se habilita en la VLAN correspondiente.



Edición por lotes: seleccione las interfaces y haga clic en **Edición por lotes**. En la ventana emergente que se muestra, seleccione la versión del IGMP y, a continuación, haga clic en **Aceptar**.

El IGMPv3 ofrece una funcionalidad y una flexibilidad mejoradas en comparación con el IGMPv2. Esta versión admite más funciones de gestión de grupos de multidifusión, proporciona un control más preciso sobre los métodos de adhesión y consulta, además de introducir mecanismos de seguridad. Gracias a estas mejoras, el IGMPv3 puede utilizarse en escenarios que requieren un mayor nivel de gestión y seguridad de la multidifusión.



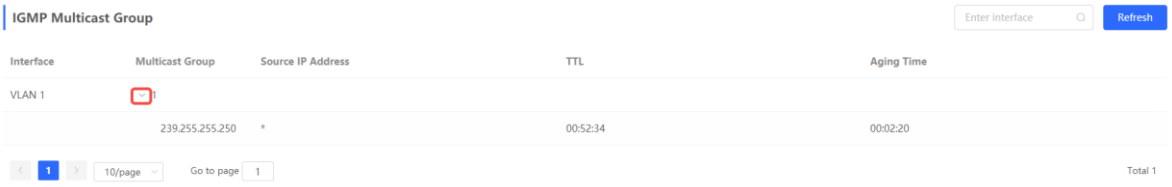
Eliminación por lotes: seleccione las interfaces y haga clic en **Eliminación por lotes**. El IGMP se deshabilita en las interfaces que haya seleccionado.

14.6.3 Visualización de los grupos de multidifusión del IGMP

Seleccione **Dispositivo local** > **L3 Multicast** > **IGMP** > **IGMP Multicast Group**.

En la página **IGMP Multicast Group** se muestra información sobre los grupos de multidifusión del IGMP, incluido el número de grupos de multidifusión, las direcciones IP de origen, el TTL y el tiempo de caducidad. Puede hacer clic para ampliar un grupo de multidifusión para ver las direcciones IP detalladas asociadas al grupo de multidifusión en esa interfaz.

Además, puede buscar información de grupos de multidifusión del IGMP introduciendo la interfaz en el cuadro de búsqueda. Si lo desea, puede hacer clic en **Refresh** para ver la información actualizada de un grupo de multidifusión del IGMP.



15 Gestión de las interfaces L3 de los switches de las series NBS y NIS

Precaución

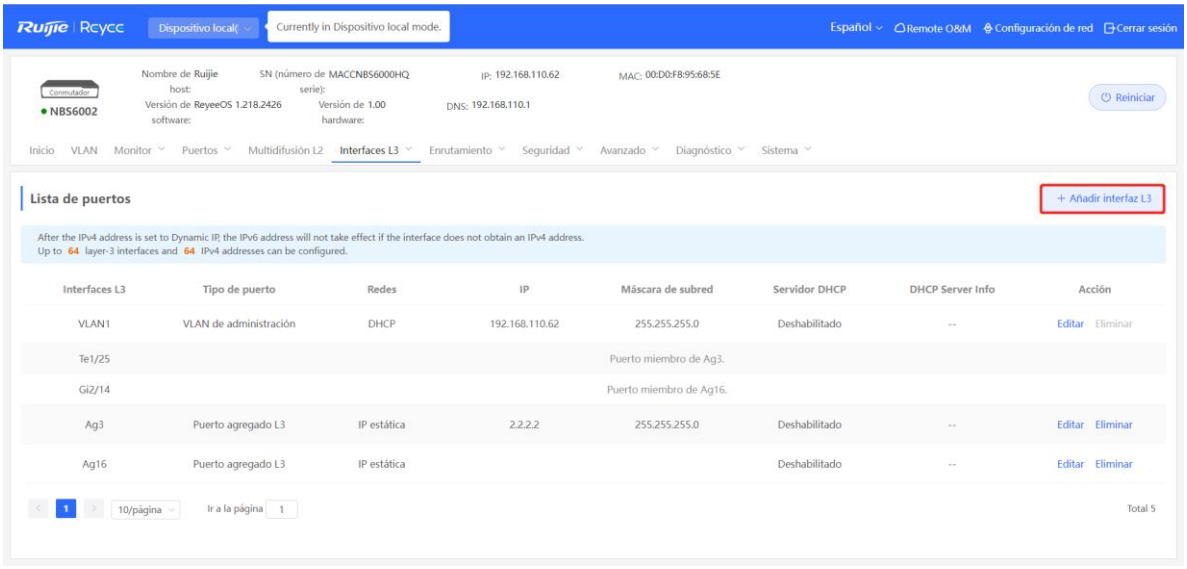
Esta sección aplica únicamente para los conmutadores de la serie NBS que son compatibles con las funciones de Capa 3. Los conmutadores como los de las series RG-NBS3100 y RG-NBS3200, las cuales no admiten funciones de Capa 3, no son compatibles con las funciones mencionadas en esta sección.

15.1 Configuración de una interfaz de Capa 3

Seleccione **Dispositivo local** > **Interfaces L3** > **Interfaces L3**.

La lista de puertos muestra diferentes tipos de interfaces de Capa 3 en el dispositivo, incluyendo interfaces virtuales o SVI, puertos enrutados y puertos agregados de Capa 3.

Haga clic en **Añadir interfaz L3** para configurar una nueva interfaz de Capa 3.



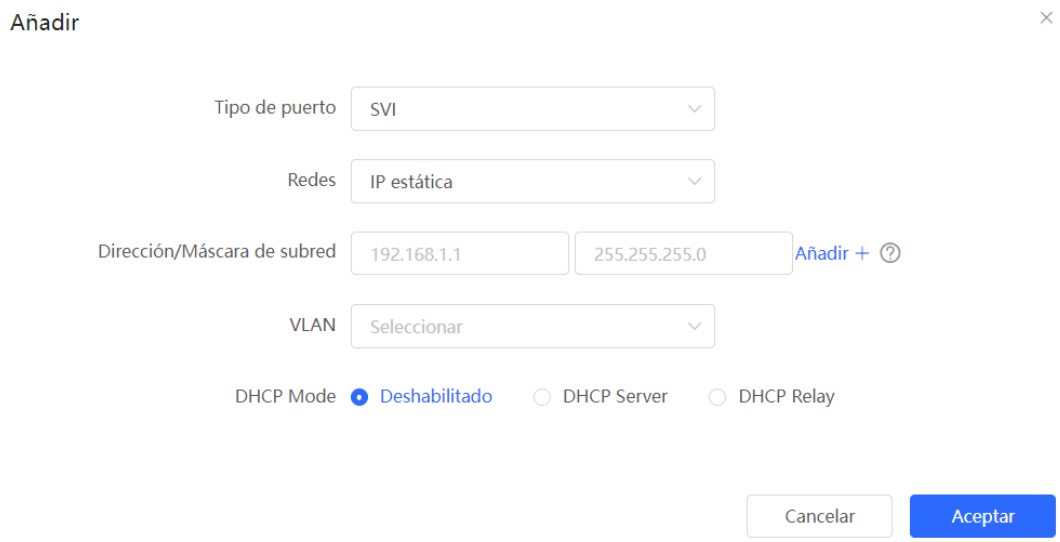


Tabla 15-1 Descripción de los parámetros para la configuración de interfaces de Capa 3

Parámetro	Descripción
Tipo de puerto	Tipo de interfaz de Capa 3 creada. Puede ser una SVI, un puerto enrutado o un puerto agregado de Capa 3. Para información más detallada, consulte la Tabla 4-1.
Redes	Un puerto obtiene una dirección IP a través del DHCP o en modo estático.
VLAN	VLAN a la cual pertenece una SVI.
Dirección/Máscara de subred	Cuando la **Red** está configurada en **IP estática**, se necesita ingresar la dirección IP y la máscara de subred.
Seleccione un puerto	Seleccione el puerto del dispositivo a configurar.
Añadir	Agregar un ID de puerto. Por ejemplo, añada un Ag1 cuando el puerto agregado de Capa 3 sea creado.
Modo DHCP	Determine si se habilita el servicio DHCP en la interfaz de Capa 3. **Deshabilitado**: el servicio DHCP está deshabilitado. No se puede asignar ninguna dirección IP a los clientes conectados a la interfaz. **DHCP Server**: el dispositivo funciona como el servidor DHCP para asignar direcciones IP a los dispositivos de enlace descendente conectados a la interfaz. Establezca la dirección IP inicial de un grupo de direcciones, el número de direcciones IP que pueden ser asignadas y la dirección de la concesión. Para más información, consulte 15.3.1 Habilitación de los servicios DHCP **DHCP Relay**: el dispositivo sirve como un agente DHCP de retransmisión, obtiene las direcciones IP de un servidor externo y asigna direcciones IP a dispositivos de enlace descendente. La dirección IP de la interfaz y la del servidor DHCP se deben configurar. La dirección IP de la interfaz debe estar en el mismo

Parámetro	Descripción
	segmento de red que el del grupo de direcciones del servidor DHCP.
Dirección IP excluida (Rango)	Cuando el dispositivo funciona como el servidor DHCP, establezca la dirección IP en el grupo de direcciones que no son para asignar.

Nota

- La VLAN 1 es la SVI predeterminada del dispositivo. Esta no se puede modificar o borrar.
- La VLAN de gestión solo aparece en la página de **Interfaces L3**, pero no se puede modificar. Para modificarla, seleccione **Puertos** > **IP de GESTIÓN**. Para más información, consulte 12.6 Dirección IP de gestión.
- Las funciones de retransmisión DHCP y del servidor DHCP de una interfaz de Capa 3 no pueden configurarse simultáneamente.
- Los puertos miembros de la interfaz de Capa 3 deben ser puertos enrutados.

15.2 Configuración de la dirección IPv6 para la interfaz L3

El IPv6 es un conjunto de protocolos estándar para la capa de red de Internet que resuelve los siguientes problemas del protocolo IPv4:

- El agotamiento de direcciones:

El NAT debe habilitarse en la gateway para convertir varias direcciones de red privadas en una dirección de red pública. Como consecuencia, se produce un retraso adicional causado por la traducción de direcciones y puede interrumpir la conexión entre los dispositivos de dentro y fuera de la gateway. Además, se debe añadir un mapeador para permitir el acceso a los dispositivos de la Intranet desde Internet.

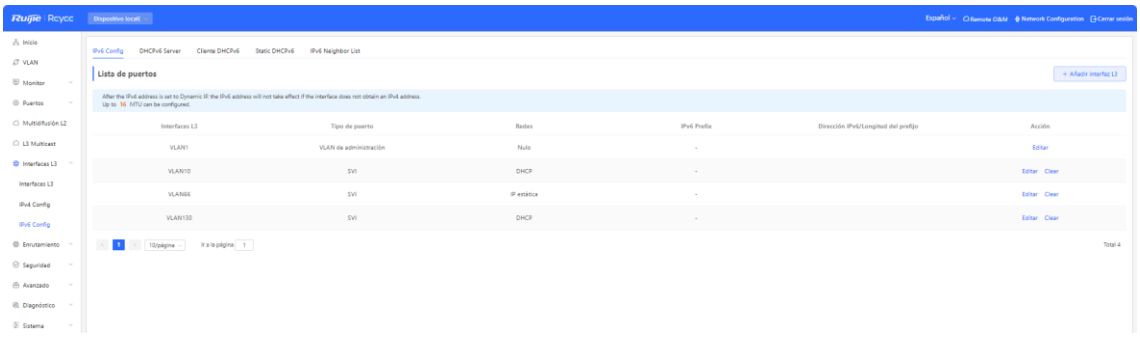
- El diseño defectuoso:

Las direcciones IP no pueden formarse a través del mapeo de la topología de la red, por lo que se necesita una tabla de enrutamiento a gran escala.

- La falta de autenticación y confidencialidad integradas:

El protocolo IPv4 no requiere encriptado. Resulta difícil rastrear la fuente tras la traducción de las direcciones. Debido a que el número de direcciones de un segmento de red es limitado, los atacantes pueden escanear fácilmente todos los hosts de la LAN. El protocolo IPv6 integra IPSec de forma predeterminada, por lo que permite establecer conexiones de extremo a extremo sin necesidad de traducir las direcciones y rastrear la fuente con facilidad. IPv6 cuenta con un gran espacio de direcciones. Las direcciones con prefijo de 64 bits admiten 64 bits de host, lo que aumenta la dificultad y el coste de la búsqueda evitando así que se produzcan ataques.

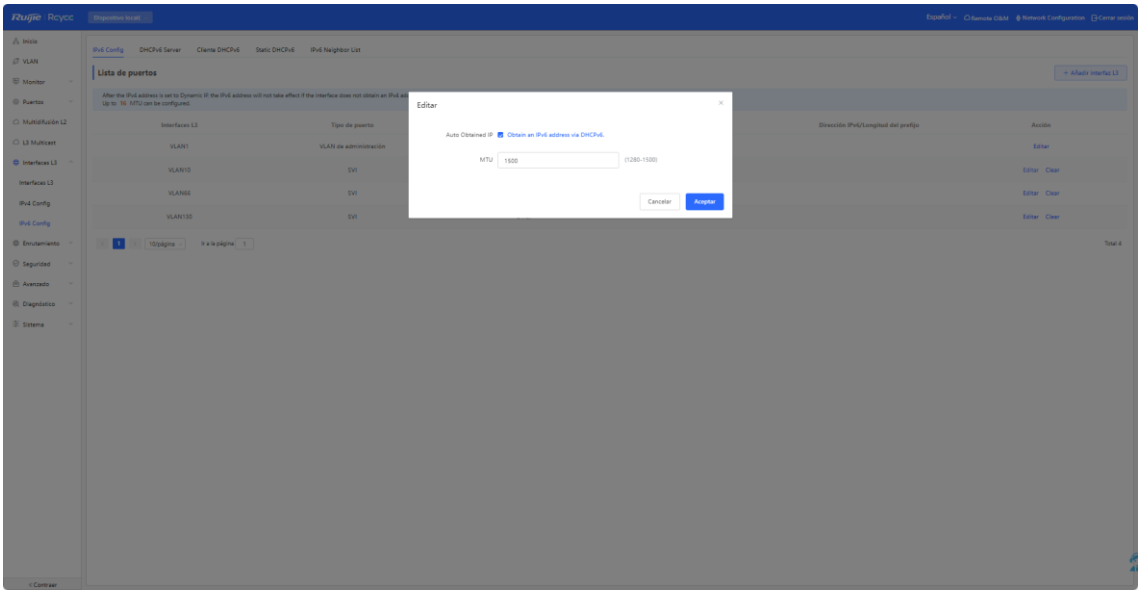
Seleccione **Dispositivo local** > **Interfaces L3** > **IPv6 Config**.



Precaución

- Añada primero una interfaz L3 IPv4. A continuación, seleccione la interfaz en la página de configuración de interfaces L3 IPv6 y haga clic en **Editar**.
- Si la dirección IPv4 de una interfaz está configurada como **DHCP** y no se obtiene ninguna dirección IPv4, la dirección IPv6 de esta interfaz no se aplicará.

- En caso de que haya disponible un servidor DHCPv6 ascendente, seleccione la opción **Auto Obtained IP** e introduzca la MTU. El valor predeterminado de la MTU es **1500**. Se recomienda mantener el valor predeterminado. A continuación, haga clic en **Aceptar**.



- Si no hay disponible ningún servidor DHCPv6 ascendente para asignar la dirección IP, configure la información de IPv6 de la siguiente manera:

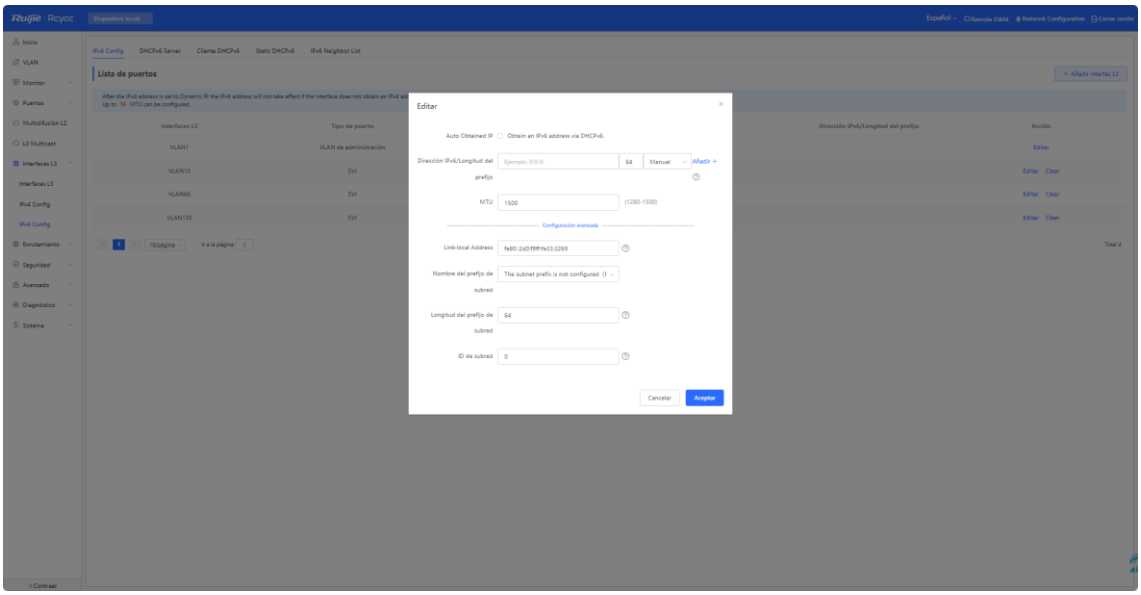


Tabla 15-2 Parámetros de configuración de las direcciones IPv6 de la interfaz L3

Parámetro	Descripción
Obtain an IPv6 address via DHCPv6	Si no hay ningún servidor DHCPv6 ascendente disponible, no seleccione la opción Obtain an IPv6 address via DHCPv6. En su lugar, añada la dirección IPv6 de forma manual.
Dirección IPv6/Longitud del prefijo	Configure la dirección IPv6 y la longitud del prefijo. Puede hacer clic en **Añadir** para configurar varias direcciones IPv6. Si la dirección IP primaria se encuentra vacía, la dirección IP secundaria que configure no será válida. Para configurarla manualmente, puede seleccionar una longitud del prefijo entre 1 y 128. Para configurarla de forma automática, puede seleccionar una longitud del prefijo entre 1 y 64. Si la longitud del prefijo IPv6 de la interfaz L3 se encuentra entre 48 y 64, puede asignarse esta dirección.
MTU	Configure la MTU. El valor predeterminado de la MTU es 1500.
Configuración avanzada	Haga clic en Configuración avanzada para configurar las opciones Link-local address, Nombre del prefijo de subred, Longitud del prefijo de subred e ID de subred.
Link-local Address	Es la dirección local de enlace que se utiliza para numerar los hosts en un único enlace de red. Los 10 primeros bits de la dirección de enlace en notación binaria deben ser «1111111010».
Nombre del prefijo de subred	Identifica un enlace determinado (subred).

Parámetro	Descripción
Longitud del prefijo de subred	Indica la longitud (en bits) del prefijo de subred de la dirección. Puede seleccionar un valor entre 48 y 64 (la longitud del prefijo de subred debe ser mayor que la longitud del prefijo asignado por el servidor).
ID de subred	Configure el ID de subred de la interfaz en notación hexadecimal. El número de ID de subred disponible es (2N - 1), donde N es igual a (longitud del prefijo de subred de la interfaz - longitud del prefijo asignado por el servidor).

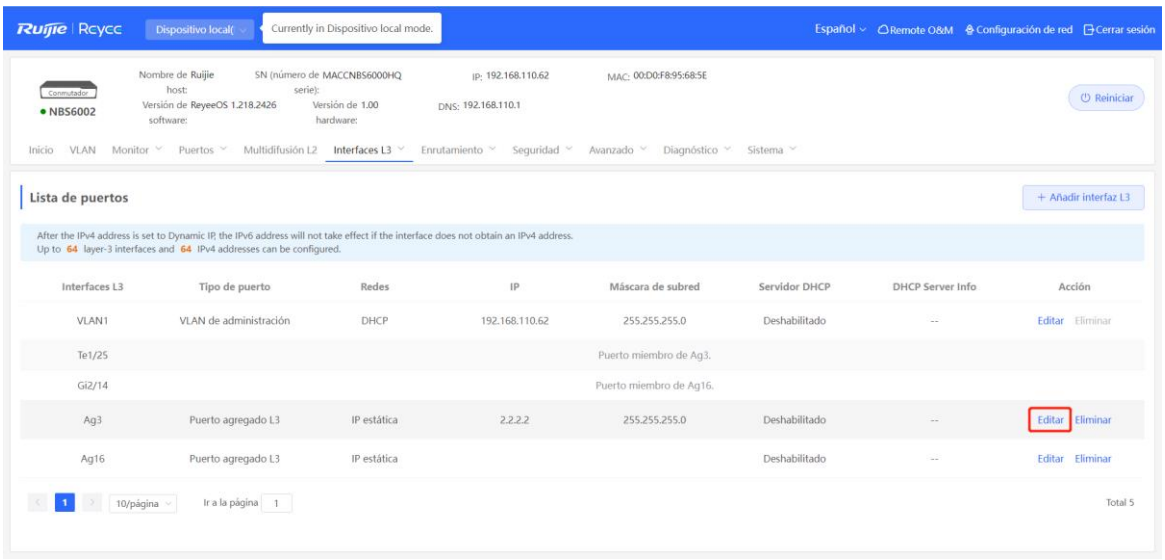
15.3 Configuración del servicio DHCP

Cuando la función de servidor DHCP quede habilitada en la interfaz de Capa 3, el dispositivo puede asignar direcciones de IP a dispositivos de enlace descendente conectados a la interfaz de Capa 3.

15.3.1 Habilitación de los servicios DHCP

Seleccione **Dispositivo local** > **Interfaces L3** > **Interfaces L3**.

Haga clic en **Editar**, en el puerto designado, o en **Añadir Interfaz L3** para añadir una interfaz de Capa 3. Seleccione el modo DHCP para la asignación local e ingrese la dirección IP inicial del grupo de direcciones, el número de direcciones IP asignadas, el rango de direcciones IP excluidas y el tiempo de concesión de la dirección.



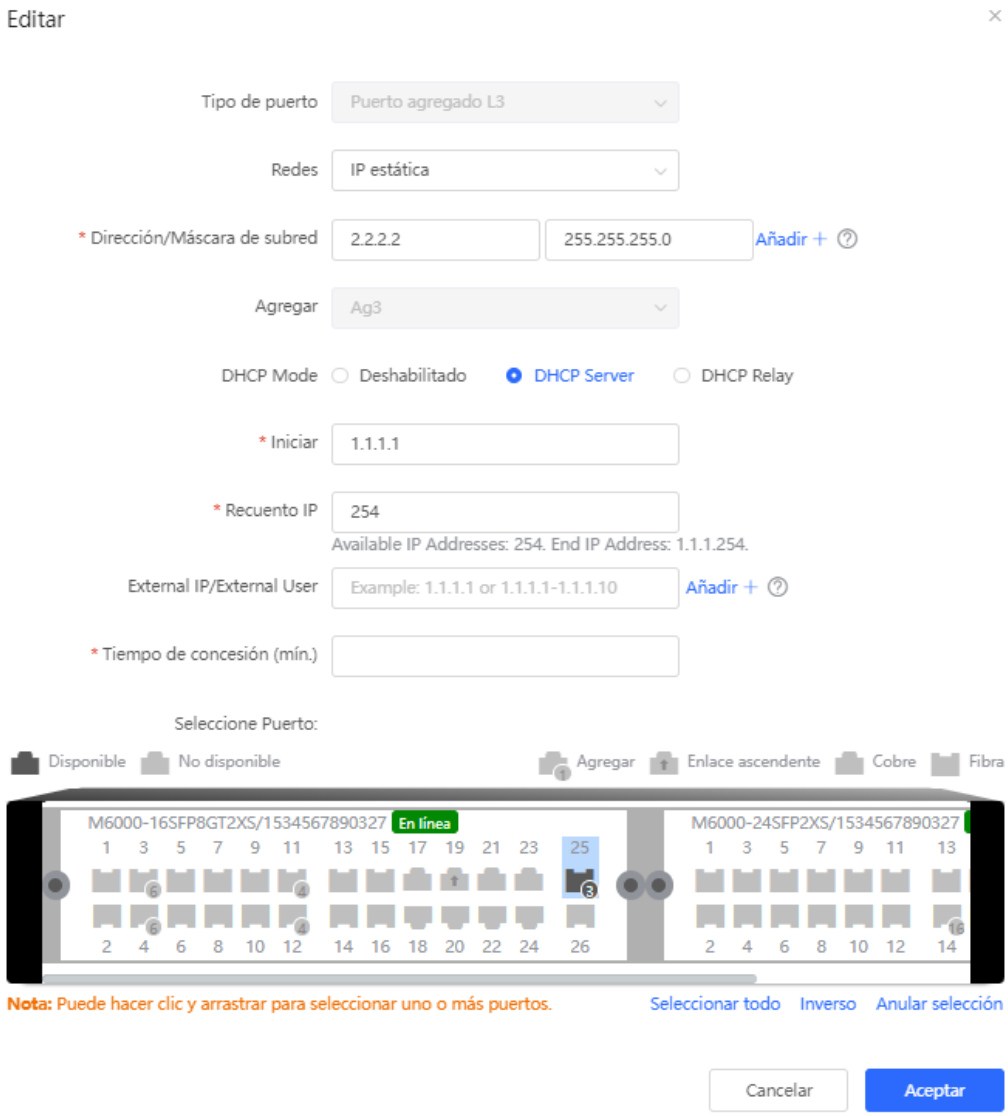


Tabla 15-3 Descripción de los parámetros para la configuración del servidor DHCP

Parámetro	Descripción
Modo DHCP	DHCP se utiliza para la asignación de direcciones IP.
Iniciar	El servidor DHCP asigna la dirección IP de inicio automáticamente, la cual es la dirección IP de inicio de su grupo de direcciones. El cliente obtiene una dirección IP del grupo de direcciones. Si se utilizan todas las direcciones del grupo de direcciones, no se podrá obtener ninguna otra dirección IP de este.
Recuento IP	Número de direcciones IP en el grupo de direcciones.
Dirección IP excluida (Rango)	Direcciones IP en el grupo de direcciones que no se usan para asignar. Se puede determinar una sola dirección IP o segmento de red IP y añadir hasta 20 segmentos de direcciones.

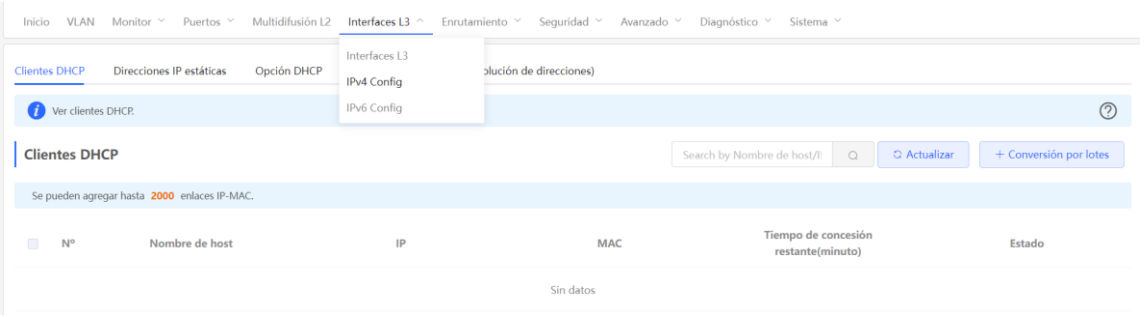
Parámetro	Descripción
Tiempo de concesión (mín.)	Dirección concesionada, en minutos. Cuando un cliente de enlace descendente se conecta, la dirección IP concesionada se renueva automáticamente. Si la dirección IP concesionada no se renueva debido a la desconexión del cliente o por la inestabilidad de la red, esta se reclamará una vez que el tiempo de concesión termine. Cuando la conexión del cliente de enlace descendente se restablezca, este puede solicitar una dirección IP nuevamente.

15.3.2 Revisión del cliente DHCP

Seleccione **Dispositivo local** > **Interfaces L3** > **IPv4 Config** > **Clientes DHCP**.

Se pueden revisar las direcciones automáticamente asignadas a clientes de enlaces descendentes después de que la interfaz de Capa 3 sea habilitada con el DHCP. Encuentre información del cliente con base en la dirección MAC, la dirección IP o el nombre de usuario.

Encuentre el cliente objetivo y haga clic en el botón **Convertir en IP estática**, en la columna de **Estado**, o seleccione los clientes que desee convertir y haga clic en **Conversión por lotes**. La dirección dinámica se enlaza con la dirección MAC del cliente y este enlace se añade a la lista de asignación de direcciones estáticas, para que el host pueda obtener una dirección IP vinculada para cada conexión. Para información más detallada acerca de cómo visualizar la lista de asignación de direcciones estáticas, consulte 15.3.3 Configuración de la asignación de direcciones IP estáticas

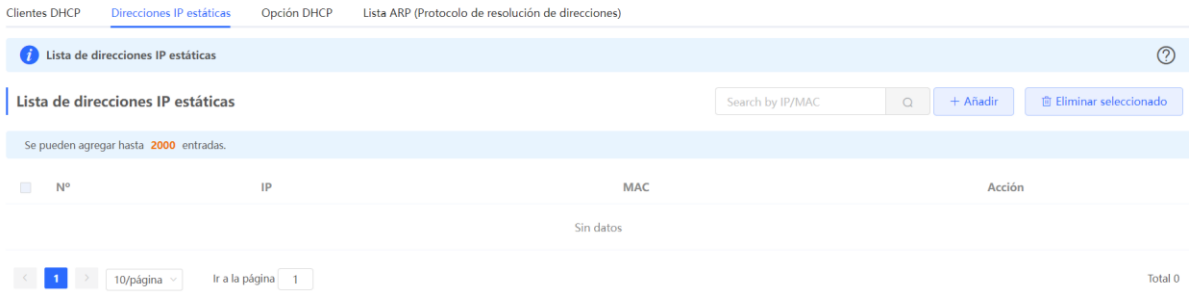


15.3.3 Configuración de la asignación de direcciones IP estáticas

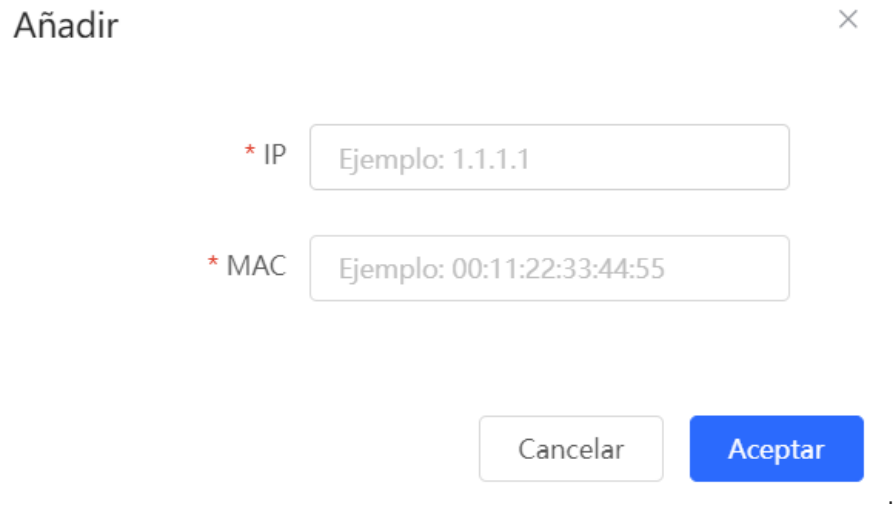
Seleccione **Dispositivo local** > **Interfaces L3** > **IPv4 Config** > **Direcciones IP estáticas**.

Ahora se muestran las entradas de clientes que se convirtieron en entradas de direcciones estáticas en la lista de clientes y las añadidas manualmente. Se puede hacer una búsqueda de entradas por dirección IP asignada o por la dirección MAC del dispositivo, en el cuadro que está en la esquina superior derecha de la pantalla.

Entradas que son



Haga clic en **Añadir**. En el cuadro de diálogo que aparece de direcciones IP estáticas enlazadas, ingrese la dirección MAC y la dirección IP del cliente a vincular, y haga clic en **Aceptar**. Después de vincular una dirección IP estática, esta aparecerá cada vez que el cliente de enlace descendente correspondiente se conecte a la red.



Para borrar una dirección estática, seleccione la entrada estática a borrar en la **Lista de Direcciones IP estáticas** y haga clic en **Eliminar seleccionado**, o haga clic en **Borrar**, en la última columna **Acción**, en la entrada correspondiente.

15.3.4 Opciones para configurar el servidor DHCP

Seleccione **Dispositivo local** > **Interfaces L3** > **IPv4 Config** > **Opción DHCP**.

La configuración disponible para dispositivos descendentes es opcional y es efectiva a nivel global cuando la interfaz de Capa 3 es el servidor DHCP.

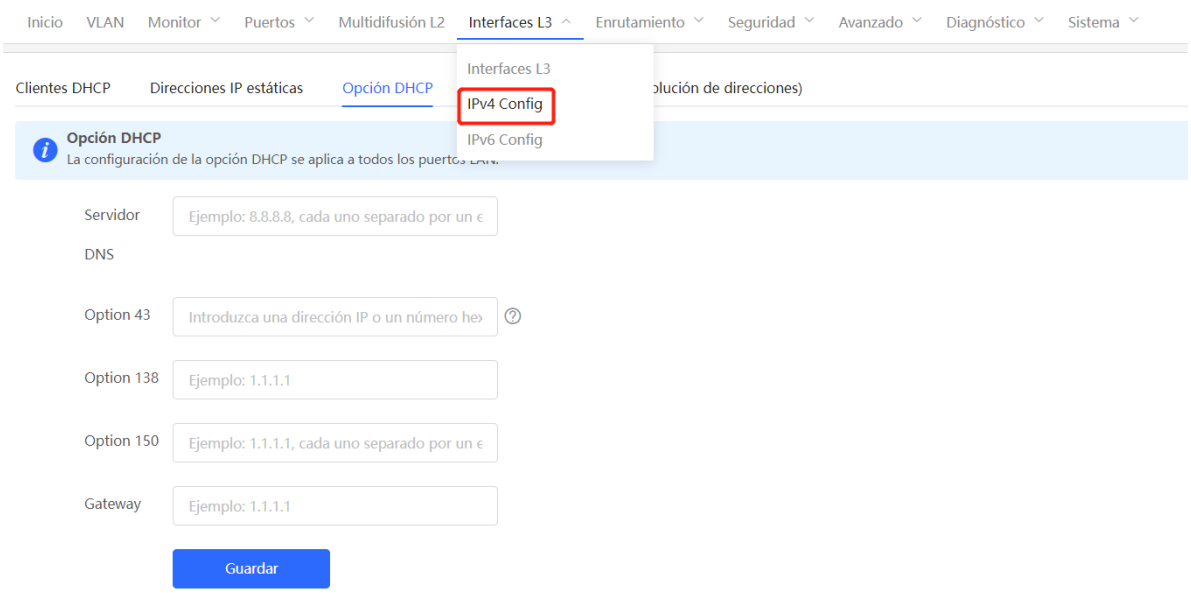


Tabla 15-4 Descripción de los parámetros para la configuración de la opción del servidor DHCP

Parámetro	Descripción
Servidor DNS	Dirección del servidor DNS proporcionada por un proveedor de servicios de Internet o ISP. Se pueden ingresar varias direcciones IP y separarlas por espacios.
Opción 43	Cuando el controlador de acceso (AC) y el AP no están en la misma LAN, el AP no puede encontrar el AC en modo multidifusión después de haberle sido asignada una dirección IP del servidor DHCP. Para habilitar que el AP descubra el AC, configure la Opción 43 de los paquetes de Respuesta de DHCP en el servidor DHCP.
Opción 138	Ingrese la dirección IP del AC. Cuando el AC y el AP no están en la misma LAN, configure la Opción 138 (similar a la Opción 43), para habilitar que el AP obtenga la dirección IPv4 del AC.
Opción 150	Ingrese la dirección IP del servidor TFTP. Ingrese la dirección IP del servidor TFTP, la cual se especifica en la dirección del servidor TFTP asignado al cliente. Se pueden ingresar varias direcciones IP y separarlas por espacios.
Gateway	Indica la dirección de la gateway predeterminada que los dispositivos cliente utilizan para acceder a redes que se encuentran fuera de su subred local, que suele ser la dirección IP de un router u otro dispositivo de red que se conecta a otras redes o a Internet.

Nota

Las opciones de DHCP son opcionales cuando el dispositivo funciona como servidor DHCP de Capa 3. La configuración será efectiva a nivel global y no requiere ser configurada por defecto. Si no se especifica una

dirección del servidor DNS, la dirección DNS asignada a un puerto de enlace descendente actuará como la puerta de enlace de la dirección IP por defecto.

15.4 Configuración del servidor DHCPv6

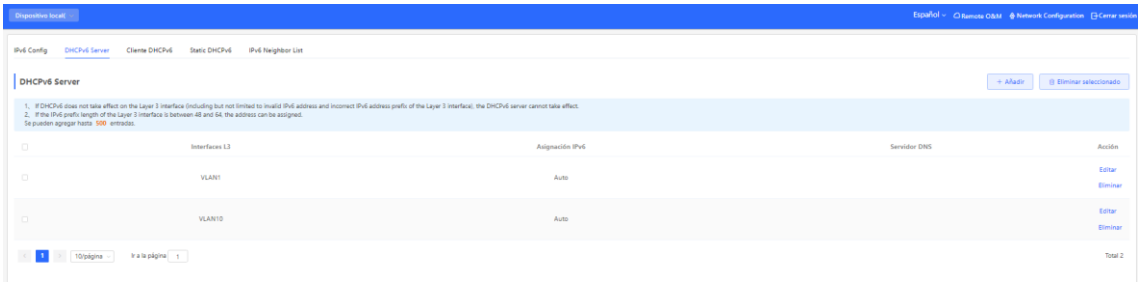
El protocolo de configuración dinámica de hosts para IPv6 (DHCPv6) es un protocolo que permite al servidor DHCP enviar información de configuración (como la dirección de red IPv6) a los nodos IPv6.

Comparado con otros métodos de asignación de direcciones IPv6 (como la configuración manual y la configuración automática de direcciones sin estado), el protocolo DHCPv6 proporciona las funciones de asignación de direcciones, delegación de prefijos (PD) y asignación de parámetros de configuración.

- El DHCPv6 es a la vez un protocolo de configuración automática de direcciones con estado y un protocolo de configuración de direcciones sin estado. Además, admite la adición y reutilización flexible de las direcciones de red y puede registrar las direcciones asignadas, mejorando así la gestión de la red.
- La función de asignación de parámetros de configuración del DHCPv6 puede resolver el problema derivado de la imposibilidad de obtener parámetros con el protocolo de configuración automática de direcciones sin estado y proporcionar al host información de configuración como la dirección del servidor DNS y el nombre de dominio.

Seleccione **Dispositivo local** > **Interfaces L3** > **IPv6 Config**.

(1) Haga clic en **Añadir**, seleccione una interfaz L3 y un método de asignación de direcciones IP e introduzca el plazo de concesión de la dirección y la dirección del servidor DNS. El tiempo de concesión de la dirección son 30 minutos de forma predeterminada. Se recomienda mantener el valor predeterminado. A continuación, haga clic en **Aceptar**.



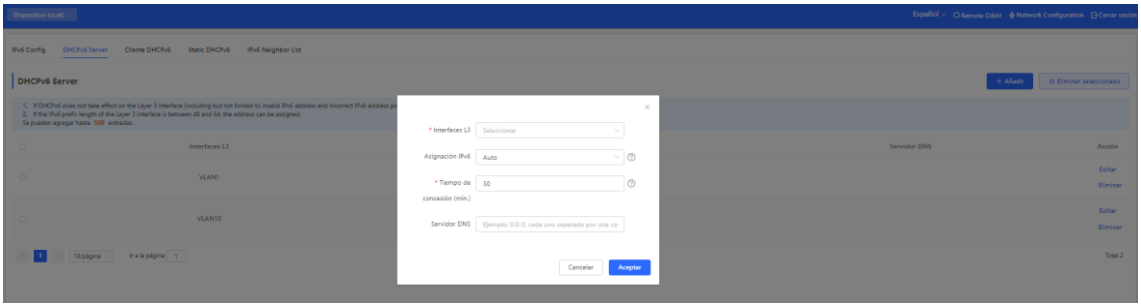


Tabla 15-5 Parámetros de configuración de las direcciones IPv6 de la interfaz L3

Parámetro	Descripción
Interfaces L3	Permite seleccionar la interfaz L3 para la que debe añadirse el servidor DHCPv6.
Asignación IPv6	Si este parámetro se establece en Auto, se utilizarán tanto el protocolo DHCPv6 como el mecanismo SLAAC para asignar direcciones IPv6.
Tiempo de concesión (min)	El valor predeterminado son 30 minutos. Puede seleccionar un valor entre 30 y 2880 minutos. Cuando el dispositivo permanece conectado y la red funciona con normalidad, este parámetro se actualiza periódicamente (se restablece al valor 0).
Servidor DNS	Permite introducir la dirección del servidor DNS.

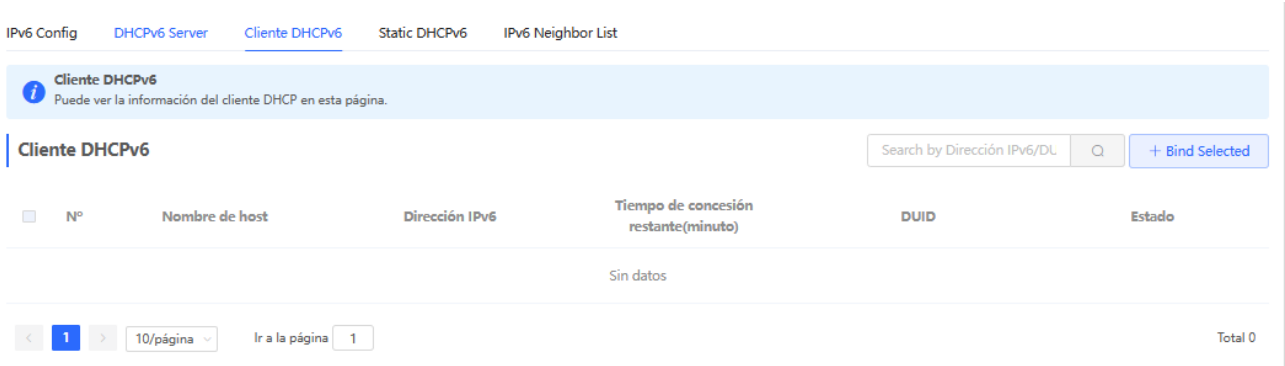
15.4.2 Visualización de clientes DHCPv6

Seleccione **Dispositivo local** > **Interfaces L3** > **IPv6 Config**. > **Cliente DHCPv6**.

Consulte la información del cliente que obtiene la dirección IPv6 del dispositivo, incluido el nombre del host, la dirección IPv6, el plazo de concesión restante, el identificador único del DHCPv6 (DUID) y el estado. Haga clic en + Bind Selected para vincular las direcciones IP y los hosts por lotes para que las direcciones IP que obtengan los hosts del switch no cambien.

Nota

Cada servidor o cliente solo tiene un DUID para identificarlo.

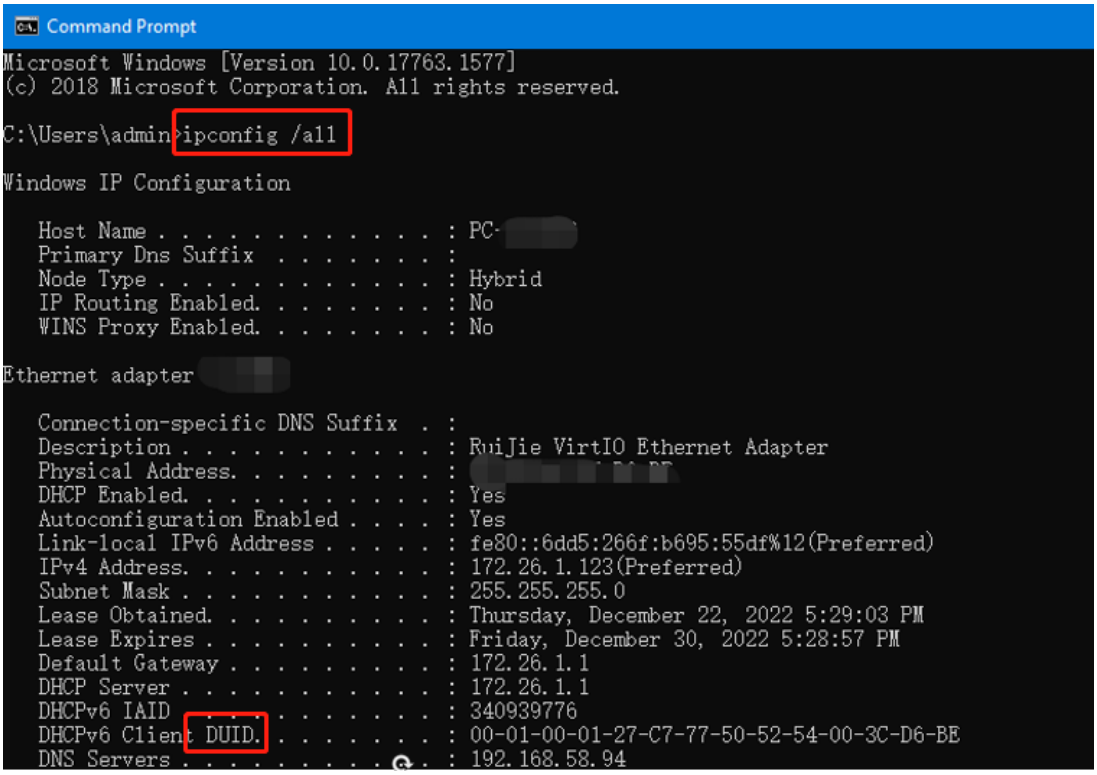


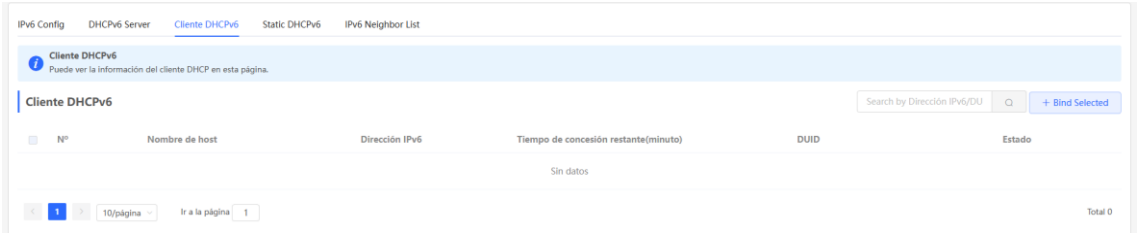
15.4.3 Configuración de la dirección DHCPv6 estática

Configure la dirección IPv6 vinculada de forma estática al DUID de un cliente para que este pueda obtener en cada momento la dirección indicada.

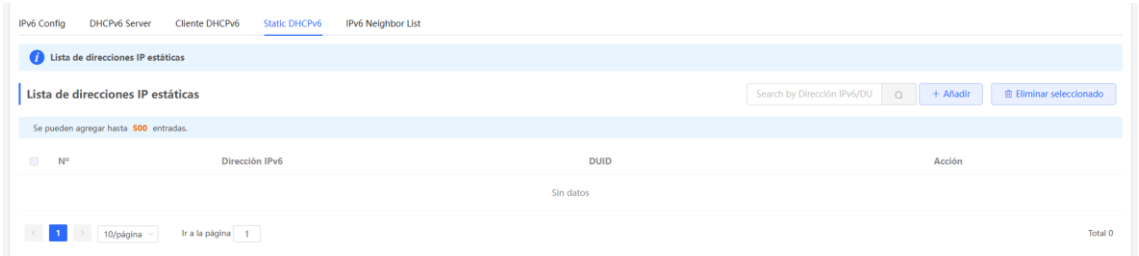
Seleccione **Dispositivo local** > **Interfaces L3** > **IPv6 Config** > **Static DHCPv6**.

Haga clic en **Añadir** e introduzca la dirección IPv6 y el DUID. Se recomienda vincular la dirección IPv6 y el DUID de la lista de clientes. Si lo desea, puede ejecutar el comando **ipconfig /all** en el símbolo del sistema de Windows para ver el DUID.





Puede ver la información de los clientes DHCPv6 en esta página.



15.5 Configuración de la lista de dispositivos cercanos del IPv6

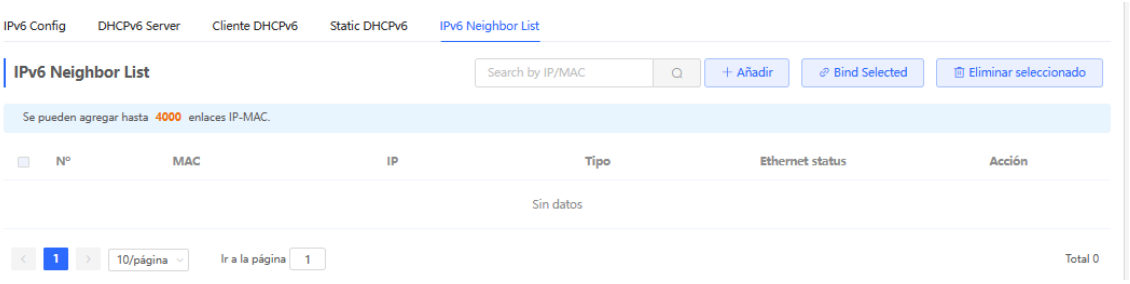
En el IPv6, el protocolo de detección de dispositivos cercanos (NDP) es un protocolo básico importante. El NDP sustituye a los protocolos de detección de routers basados en el ICMP y el ARP del IPv4 y admite las siguientes funciones: resolución de direcciones, seguimiento del estado de los dispositivos cercanos, detección de direcciones duplicadas, detección de routers y redireccionamiento.

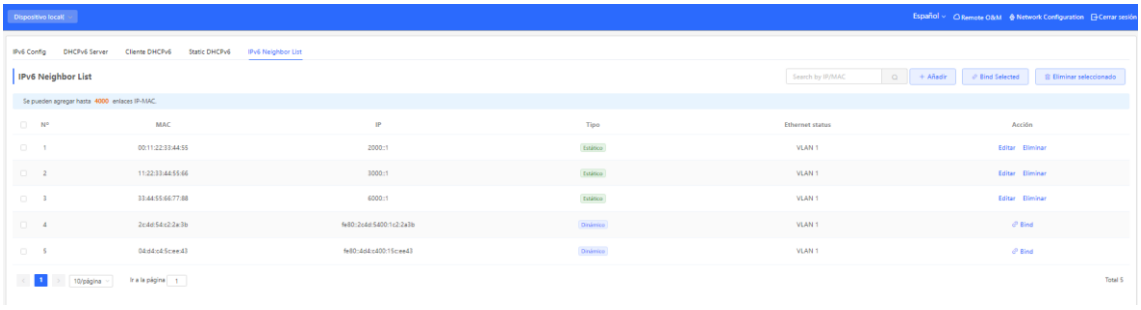
Seleccione **Dispositivo local** > **Interfaces L3** > **IPv6 Config** > **IPv6 Neighbor List**.

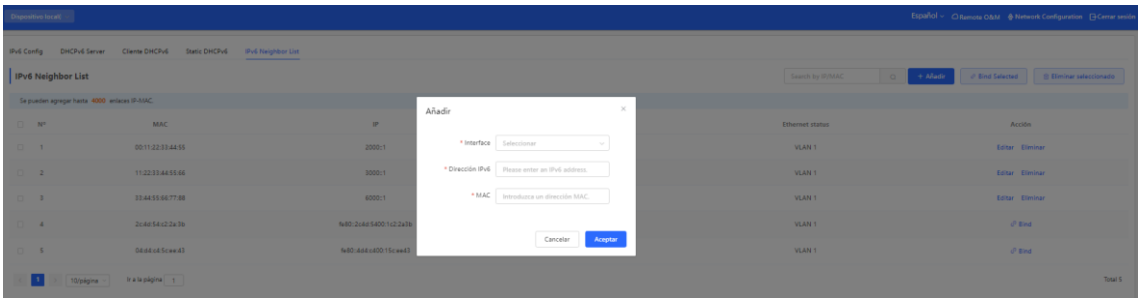
Haga clic en **Añadir** y añada manualmente la interfaz, la dirección IPv6 y la dirección MAC del dispositivo cercano.

Haga clic en **Bind Selected** para vincular la dirección IPv6 y la dirección MAC de la lista y evitar que se produzcan ataques de ND.

Si lo desea, también puede modificar, eliminar, eliminar por lotes y buscar dispositivos cercanos (por la dirección IP o MAC).





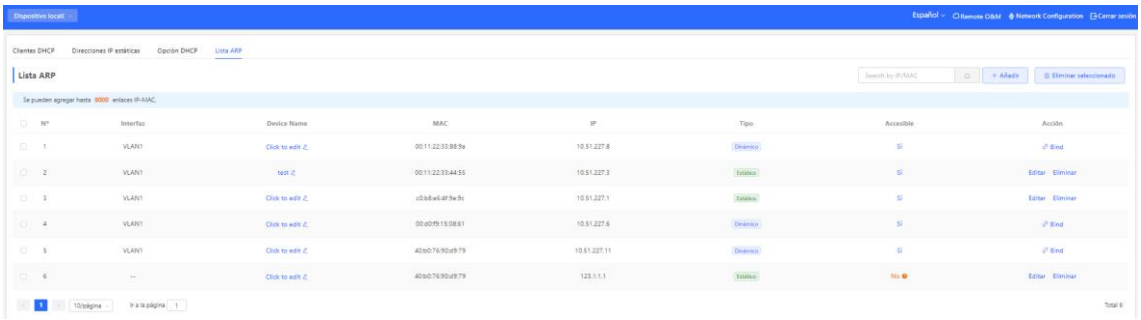


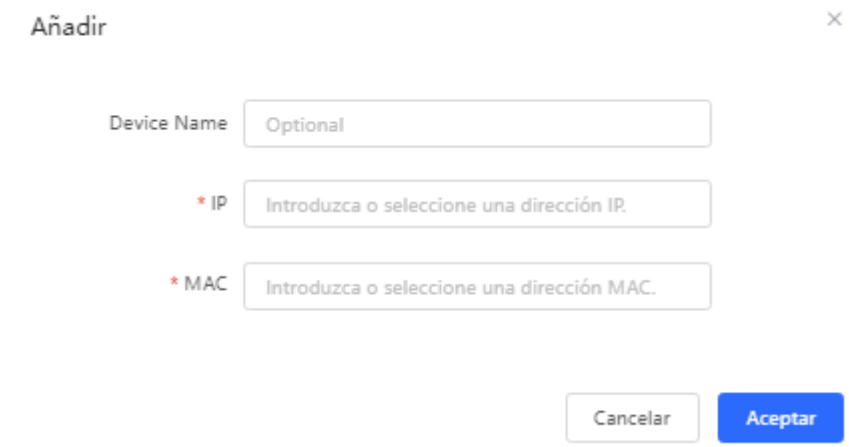
15.6 Configuración de una entrada de ARP estática

Seleccione **Dispositivo local** > **Interfaces L3** > **IPv4 Config** > **ARP List**.

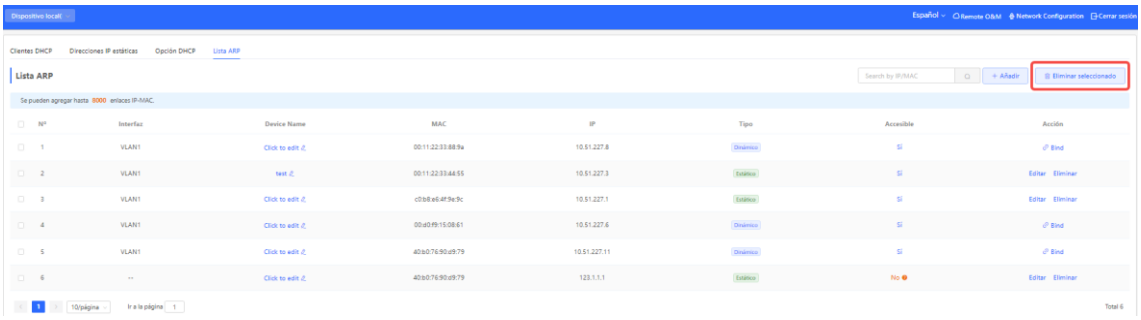
El dispositivo aprende la dirección IP y la dirección MAC de los dispositivos de la red conectados a sus interfaces y genera las entradas del protocolo de resolución de direcciones (ARP) correspondientes. Se puede configurar el mapeo ARP o especificar manualmente el mapeo de IP-MAC para evitar que los dispositivos aprendan entradas ARP incorrectas y para mejorar la seguridad de la red.

- Para enlazar una entrada ARP dinámica a una estática, seleccione la entrada del mapeo ARP, dinámicamente obtenida en **ARP List,** y haga clic en **Bind** para completar el enlace.
- Para configurar una entrada de ARP estática manualmente, haga clic en **Add**, ingrese la dirección IP y la dirección MAC a vincular, y haga clic en **OK**.





Para eliminar el enlace entre una dirección IP estática y una dirección MAC, haga clic en **Delete** en la columna **Action**.



16 Configuración de rutas de los switches de las series NBS y NIS

Precaución

El contenido que se describe en este capítulo solo es aplicable a los switches de la serie NBS con funciones de capa 3. Los switches de las series RG-NIS, RG-NBS3100 y RG-NBS3200 no son compatibles con las funciones que se describen en este apartado.

16.1 Configuración de rutas estáticas

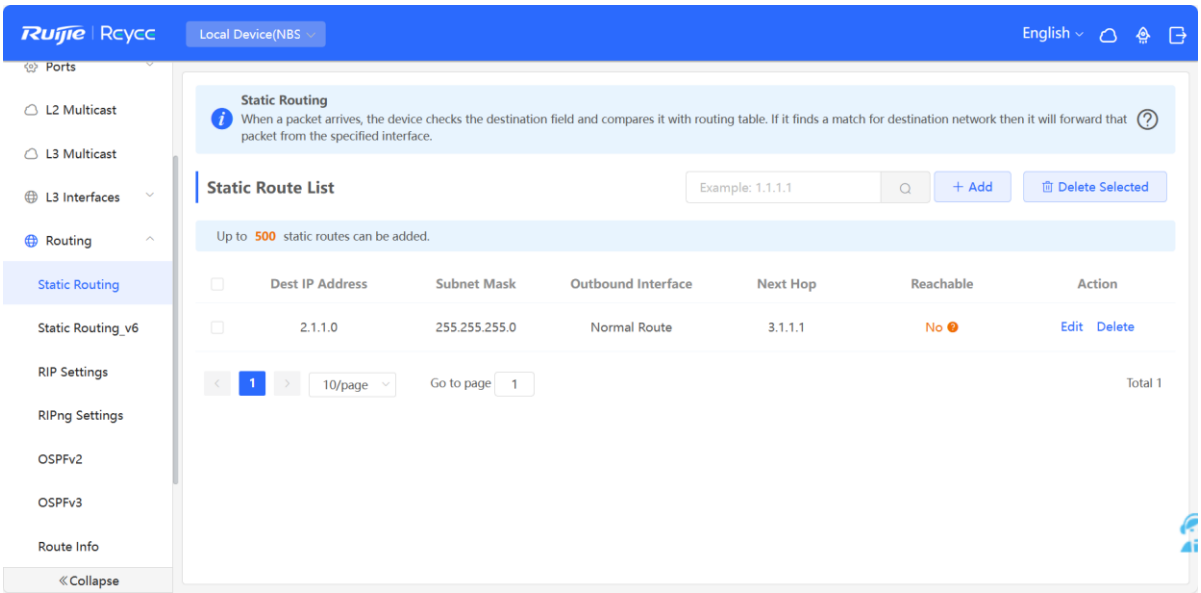
Seleccione **Local device** > **Routing** > **Static Routing**.

Las rutas estáticas las configura el usuario de forma manual. Cuando un paquete de datos coincide con una ruta estática, este se redirecciona basándose en el modo de redirección que se haya seleccionado.

Precaución

Las rutas estáticas no se adaptan de forma automática a los cambios que se producen en la topología de la red. Cuando la topología de la red cambie, deberá configurar las rutas estáticas de nuevo.

Haga clic en **Add**. En el cuadro de diálogo que se muestra, introduzca la dirección IP de destino, la máscara de subred, la interfaz de salida y la dirección IP del siguiente salto para crear una ruta estática.



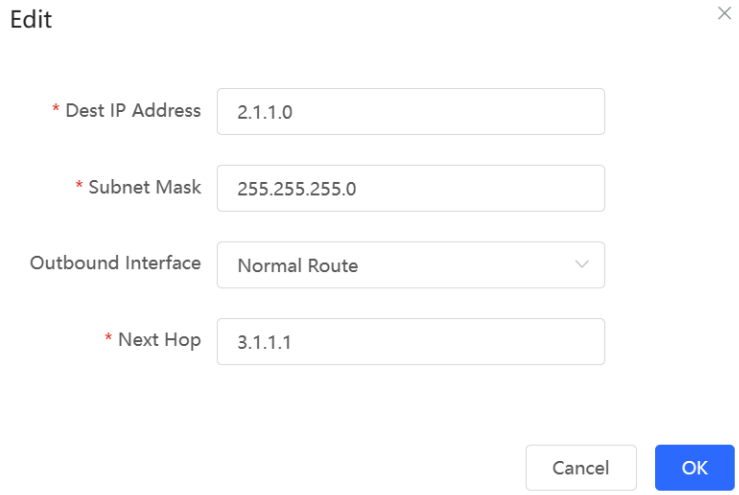
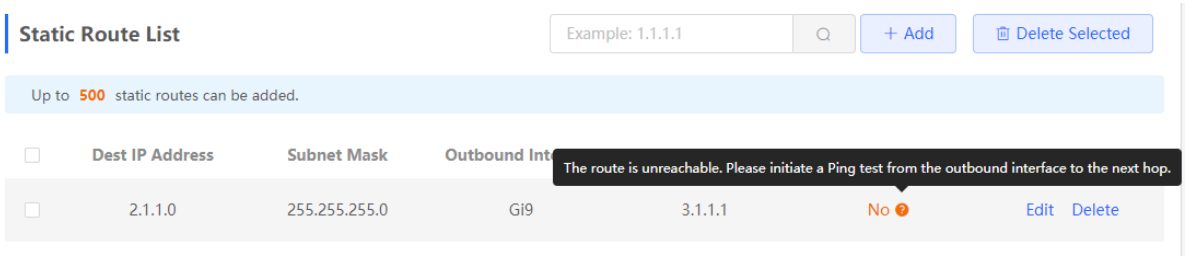


Tabla 16-1 Descripción de los parámetros de configuración de las rutas estáticas

Parámetro	Descripción
Dest IP Address	Permite indicar la red de destino a la que desee que se envíe el paquete de datos. El dispositivo establece el paquete de datos en función de la dirección de destino y la máscara de subred.
Subnet Mask	Permite indicar la máscara de subred de la red de destino. El dispositivo establece el paquete de datos en función de la dirección de destino y la máscara de subred.
Outbound Interface	Permite indicar la interfaz que redireccionará el paquete de datos.
Next Hop	Permite indicar la dirección IP del siguiente salto de la ruta para el paquete de datos.

Tras crear una ruta estática, puede encontrar la configuración de la ruta correspondiente y el estado de la capacidad de acceso a la misma en la lista de rutas estáticas. El parámetro **Reachable** indica si se puede acceder al siguiente salto, lo que le permitirá determinar si la ruta podrá aplicarse. Si el valor es **No**, compruebe si la interfaz de salida de la ruta actual puede hacer ping a la dirección del siguiente salto.



Para eliminar o modificar una ruta estática, en la página **Static Route List**, puede hacer clic en **Delete** o **Edit** en la última columna **Action** o seleccionar la entrada de ruta estática que desea eliminar y hacer clic en **Delete Selected** para eliminar varias entradas de rutas estáticas.

16.2 Configuración de la ruta estática IPv6

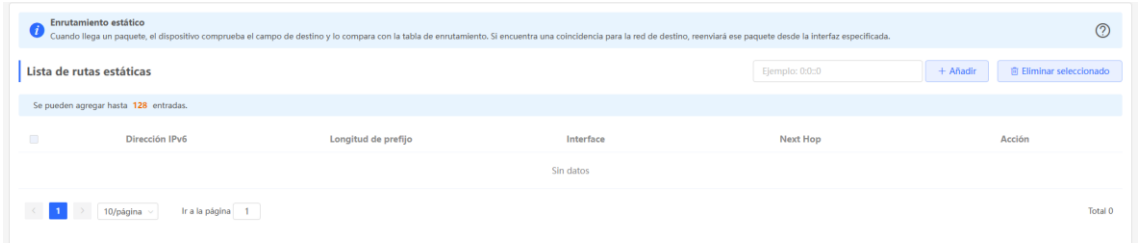
Seleccione **Dispositivo local** > **Enrutamiento** > **Enrutamiento estático**.

La ruta estática IPv6 debe configurarse de forma manual. Cuando el paquete coincide con la ruta estática, este se redirecciona basándose en el método de redirección que se haya seleccionado.

Precaución

La ruta estática no se adapta de forma automática a los cambios que se producen en la topología de la red. Cuando la topología de la red cambie, deberá volver a configurar la ruta estática de forma manual.

Haga clic en **Añadir** e introduzca la dirección IPv6 de destino, la longitud, la interfaz de salida y la dirección IP del siguiente salto para crear una ruta estática.



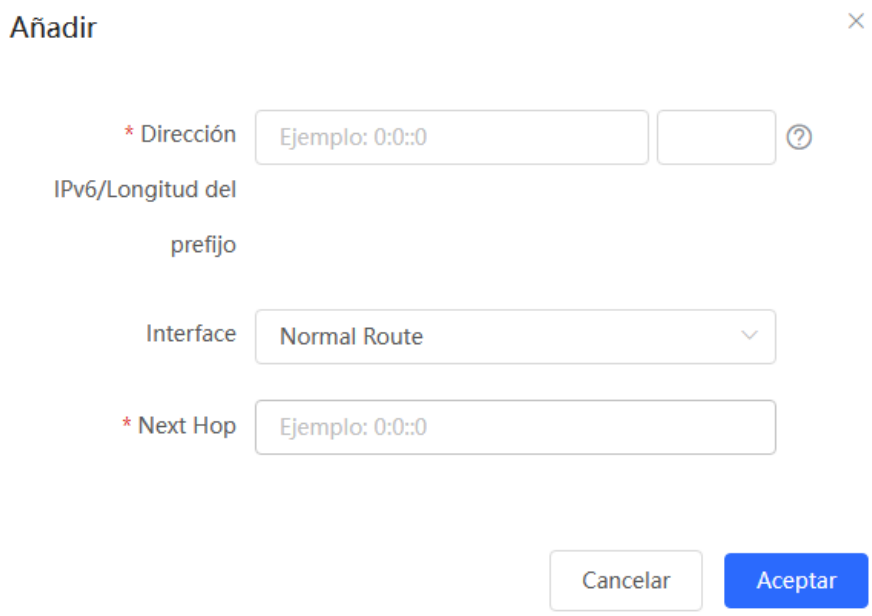


Tabla 16-2 Parámetros de configuración de la ruta estática IPv6

Parámetro	Descripción
Dirección IPv6/Longitud del prefijo	Red de destino del paquete. La dirección de destino del paquete se establece en función de la dirección IPv6 y la longitud del prefijo.
Interface	Interfaz que reenvía el paquete.
Next Hop	Dirección IP del siguiente nodo de enrutamiento al que se envía el paquete.

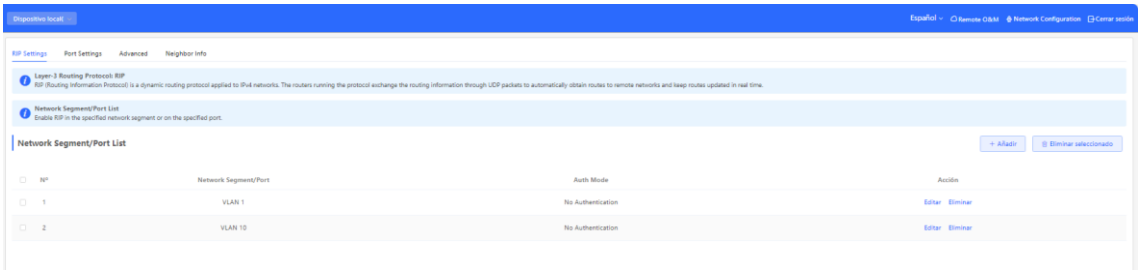
16.3 Configuración del RIP

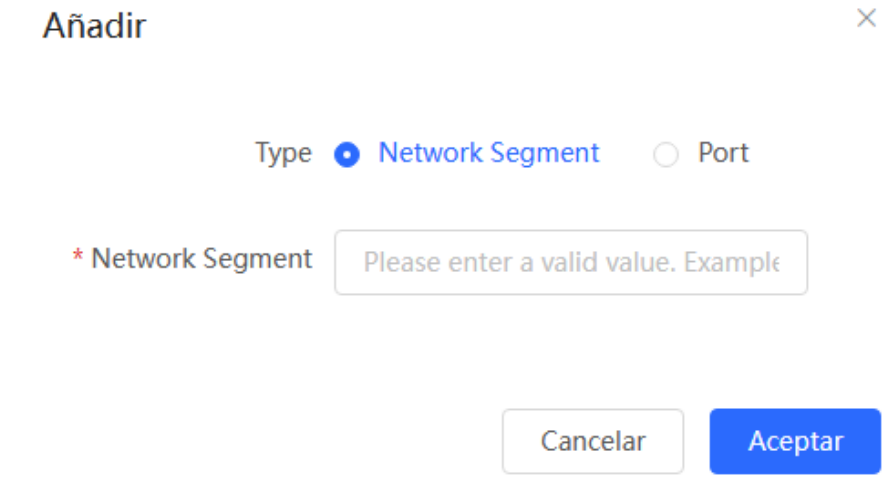
El protocolo de información de enrutamiento (RIP) se puede utilizar en redes de pequeño y mediano tamaño y es un protocolo de enrutamiento dinámico fácil de configurar. El RIP mide la distancia de la red en función del número de saltos y selecciona una ruta en función de la distancia. Este protocolo utiliza el puerto UDP 520 para intercambiar la información de enrutamiento.

16.3.1 Configuración de las funciones básicas del RIP

Seleccione **Dispositivo local** > **Enrutamiento** > **RIP Settings**.

Haga clic en **Añadir** y configure el segmento de red y la interfaz.


Dispositivo local
Español
Remote O&M
Network Configuration
Cerrar sesión
RIP Settings
Port Settings
Advanced
Neighbor Info
Layer-3 Routing Protocol: RIP
RIP (Routing Information Protocol) is a dynamic routing protocol applied to IPv4 networks. The routers running the protocol exchange the routing information through UDP packets to automatically obtain routes to remote networks and keep routes updated in real time.
Network Segment/Port List
Enable RIP in the specified network segment or on the specified port.
Network Segment/Port List
+ Añadir
Eliminar seleccionado
Nº
Network Segment/Port
Auth Mode
Acción
1
VLAN 1
No Authentication
Editar
Eliminar
2
VLAN 10
No Authentication
Editar
Eliminar


Añadir
Type
Network Segment
Port
* Network Segment
Please enter a valid value. Example
Cancelar
Aceptar

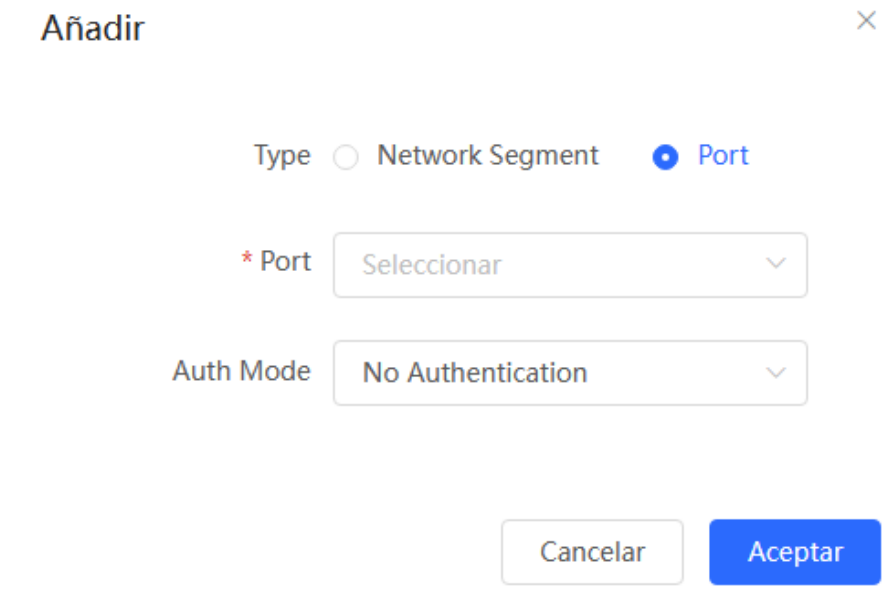

Añadir
Type
Network Segment
Port
* Port
Seleccionar
Auth Mode
No Authentication
Cancelar
Aceptar

Tabla 16-3 Parámetros de configuración del RIP

Parámetro	Descripción
Type	**Network Segment**: permite habilitar la opción RIP en el segmento de red que haya indicado. Las direcciones IP de este segmento de red se añaden a la tabla de enrutamiento del RIP. El dispositivo y sus dispositivos cercanos compatibles con el protocolo RIP obtienen la tabla de enrutamiento el uno del otro. **Port**: permite habilitar la opción RIP en el puerto que haya indicado. Todas las direcciones IP de este puerto se añaden a la tabla de enrutamiento del RIP. El dispositivo y sus dispositivos cercanos compatibles con el protocolo RIP obtienen la tabla de enrutamiento el uno del otro.
Network Segment	Permite introducir el segmento de red, por ejemplo, **10.1.0.0/24**, cuando la opción **Type** se establece en **Network Segment**. El RIP se habilitará en todas las interfaces del dispositivo que abarque este segmento de red.
Port	Permite seleccionar una interfaz VLAN o un puerto físico cuando la opción **Type** se establece en **Port**.
Auth Mode	**No Authentication**: los paquetes del protocolo no se autentican. **Encrypted Text**: los paquetes del protocolo se autentican y la clave de autenticación se envía junto con los paquetes del protocolo en forma de texto encriptado. **Plain Text**: los paquetes del protocolo se autentican y la clave de autenticación se envía junto con los paquetes del protocolo en forma de texto plano.

Auth Key	Permite introducir la clave de autenticación para autenticar los paquetes del protocolo cuando la opción **Auth Mode** se establece en **Encrypted Text** o **Plain Text**.

16.3.2 Configuración del puerto RIP

Seleccione **Dispositivo local** > **Enrutamiento** > **RIP Settings** > **Port Settings**.

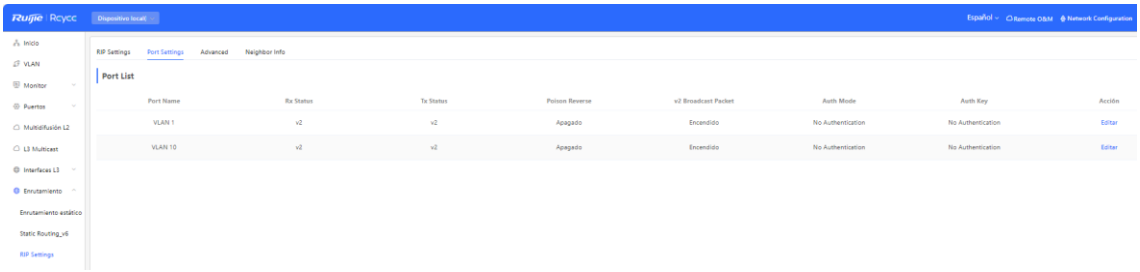


Tabla 16-4 Configuración de los parámetros de la lista de puertos

Parámetro	Descripción
Port Name	Nombre del puerto en el que se encuentra habilitado el RIP.
Rx Status	Versión del RIP de los paquetes que se están recibiendo en este momento.
Tx Status	Versión del RIP de los paquetes que se están enviando en este momento.
Poison Reverse	Una vez que el puerto detecta la ruta, la opción de sobrecarga de rutas se establece en **16** (lo que indica que no se puede acceder a la ruta) y esta se devuelve al dispositivo cercano desde el puerto original para evitar que se produzca un bucle.

v2 Broadcast Packet	Cuando un dispositivo cercano no admite la multidifusión, pueden enviarse paquetes de difusión. Se aconseja deshabilitar los paquetes de difusión del RIPv2 para mejorar el rendimiento de la red.
Auth Mode	**No Authentication**: los paquetes del protocolo no se autentican. **Encrypted Text**: los paquetes del protocolo se autentican y la clave de autenticación se envía junto con los paquetes del protocolo en forma de texto encriptado. **Plain Text**: los paquetes del protocolo se autentican y la clave de autenticación se envía junto con los paquetes del protocolo en forma de texto plano.
Auth Key	Permite introducir la clave de autenticación para autenticar los paquetes del protocolo cuando la opción **Auth Mode** se establece en **Encrypted Text** o **Plain Text**.
Acción	Haga clic en **Editar** para modificar la configuración del RIP del puerto.

16.3.3 Configuración de la configuración global del RIP

Seleccione **Dispositivo local** > **Enrutamiento** > **RIP Settings** > **Advanced**, haga clic en **Edit Config** y configure los parámetros de la configuración global del RIP.

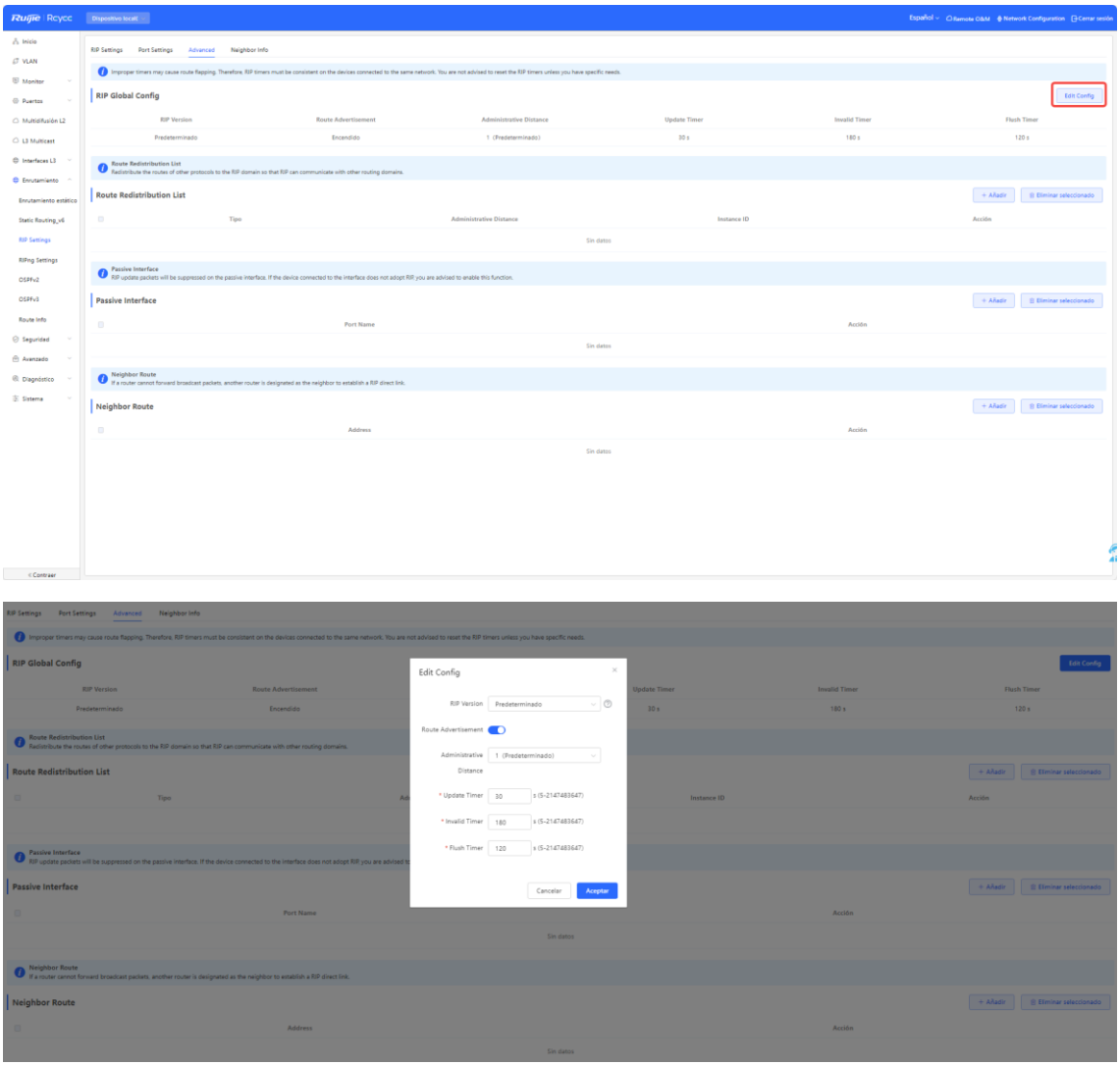


Tabla 16-5 Parámetros de la configuración global del RIP

Parámetro	Descripción
RIP Version	Predeterminado: seleccione la opción RIPv2 para enviar y RIPv1/v2 para recibir paquetes. **V1**: seleccione la opción RIPv1 para enviar y recibir paquetes. **V2**: seleccione la opción RIPv2 para enviar y recibir paquetes.

Parámetro	Descripción
Route Advertisement	Tras habilitar la opción Anuncio de la ruta (Route Advertisement), el dispositivo actual genera una ruta de forma predeterminada y la envía al dispositivo cercano.
Administrative Distance	Redistribuye rutas de otros protocolos al dominio del RIP para que este interactúe con los demás dominios de enrutamiento.
Update Timer	Ciclo de actualización del RIP. La información del enrutamiento se actualiza cada 30 segundos de forma predeterminada.
Invalid Timer	Si no se recibe ninguna actualización antes de que una ruta deje de ser válida, se considera que no se puede acceder a la ruta. El valor predeterminado es 180 segundos.
Flush Timer	Si no se recibe ninguna actualización antes de que transcurra el tiempo del temporizador de purga de una ruta no válida, la ruta se elimina completamente de la tabla de enrutamiento del RIP. El valor predeterminado es 120 segundos.

16.3.4 Configuración de la lista de redistribución de rutas del RIP

Redistribuye rutas de otros protocolos al dominio del RIP para que este interactúe con los demás dominios de enrutamiento.

Seleccione **Dispositivo local** > **Enrutamiento** > **RIP Settings** > **Advanced**, haga clic en **Añadir** y seleccione el tipo y la distancia administrativa (administrative distance).

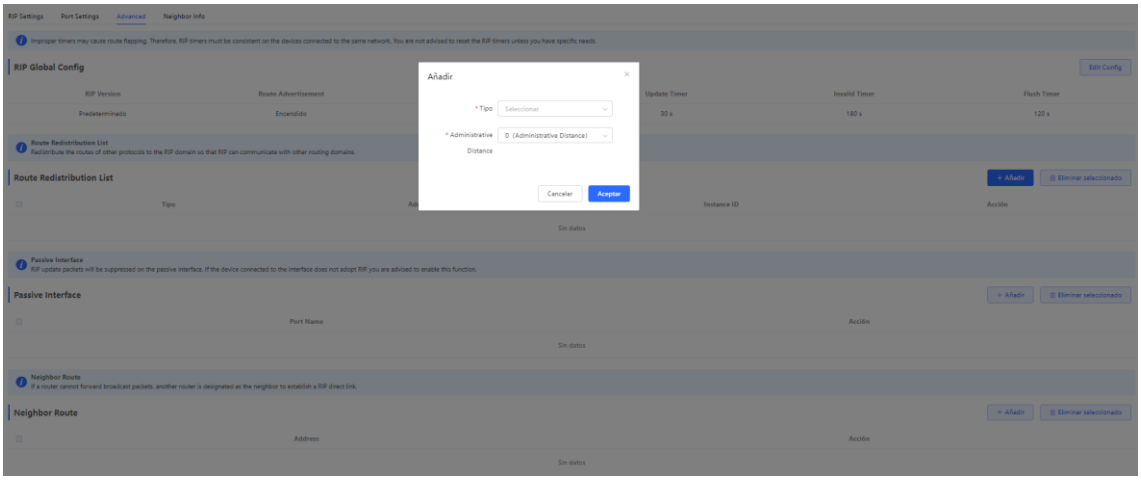
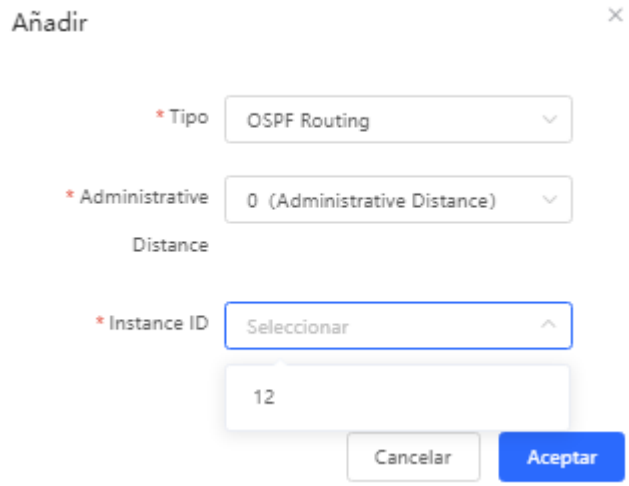


Tabla 16-6 Parámetros de redistribución de rutas del RIP

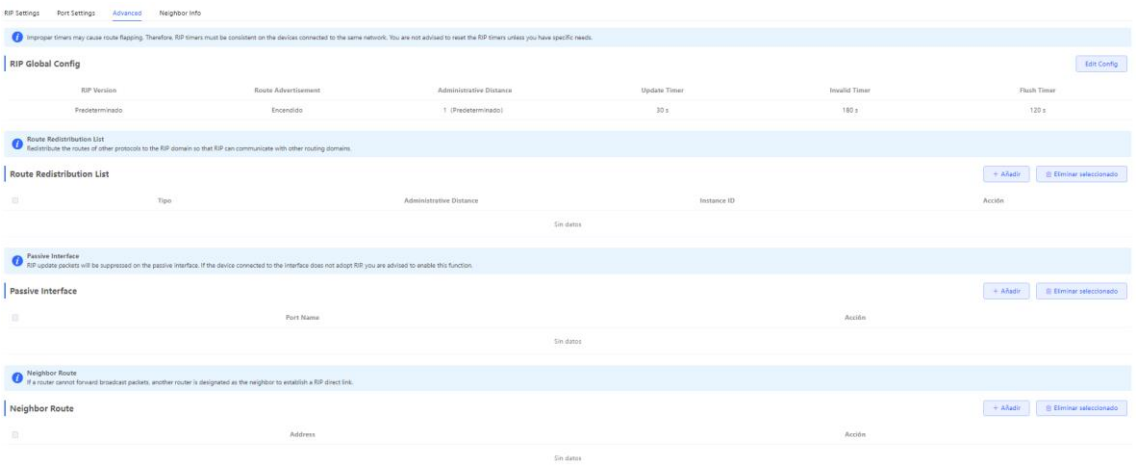
Parámetro	Descripción
Tipo	Direct Routing OSPF Routing Static Routing
Administrative Distance	Cuanto menor es la distancia administrativa, mayor es la prioridad. El valor predeterminado es **0**. Puede seleccionar un valor entre 0 y 16.
Instance ID	Seleccione el ID de instancia del OSPF que deba redistribuirse. El protocolo OSPFv2 debe habilitarse en el dispositivo local.

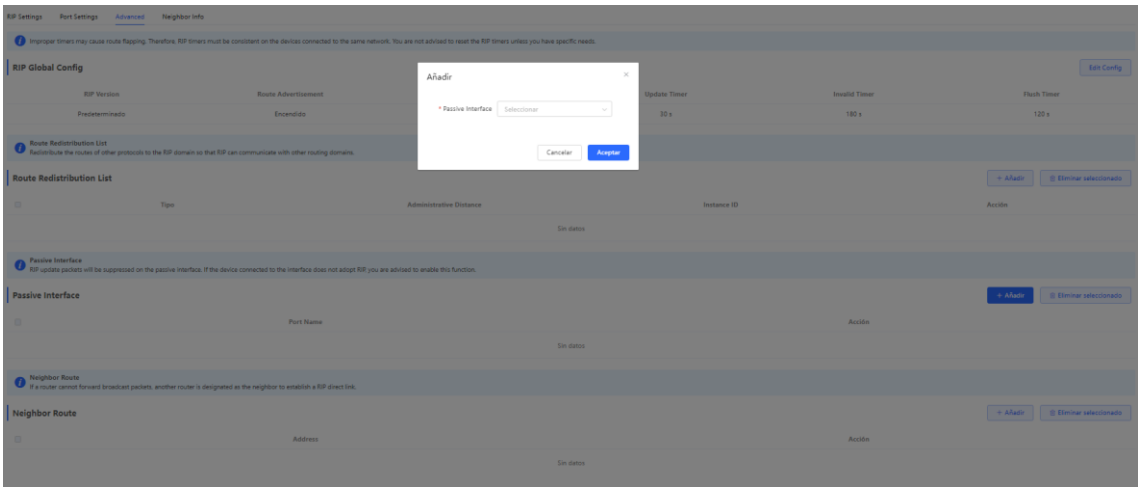


16.3.5 Configuración de una interfaz pasiva

Si una interfaz se configura como interfaz pasiva, esta suprimirá los paquetes de actualización del RIP. Si el dispositivo homólogo conectado no utiliza el RIP, le recomendamos que habilite la interfaz pasiva.

Seleccione **Dispositivo local** > **Enrutamiento** > **RIP Settings** > **Advanced**, haga clic en **Añadir** y seleccione una interfaz pasiva.

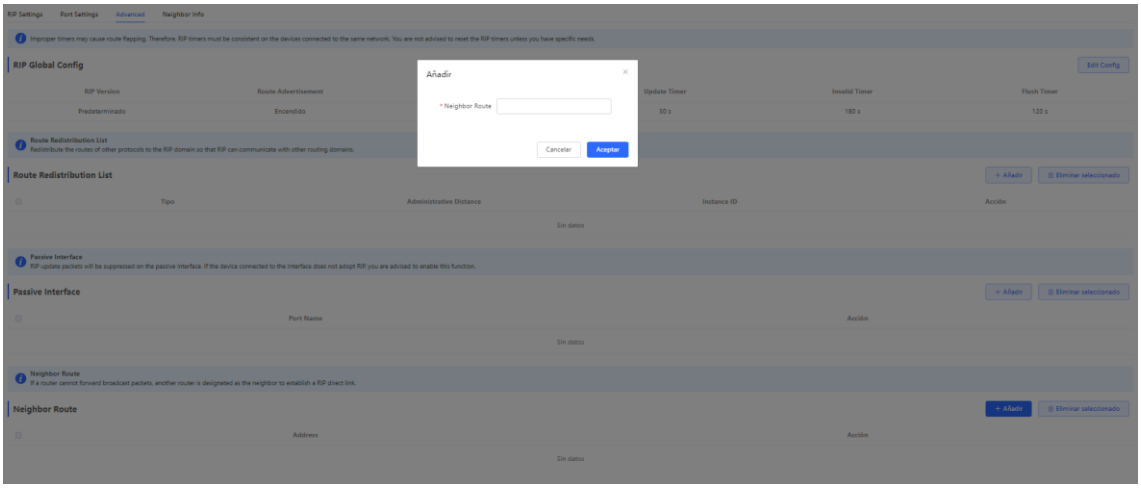


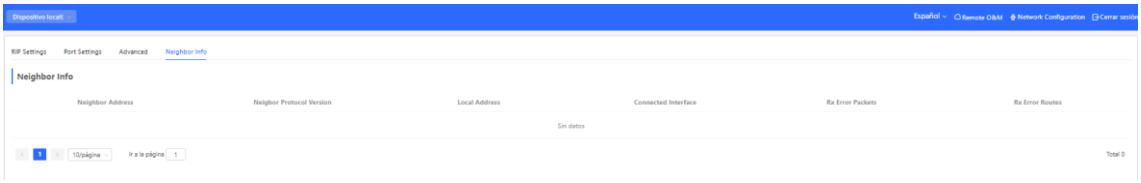


16.3.6 Configuración de una ruta cercana

Cuando el router no puede procesar paquetes de difusión, puede designarse otro router como router cercano para establecer un enlace directo del RIP.

Seleccione **Dispositivo local** > **Enrutamiento** > **RIP Settings** > **Advanced**, haga clic en **Añadir** e introduzca la dirección IP del router cercano.





16.4 Configuración del RIPng

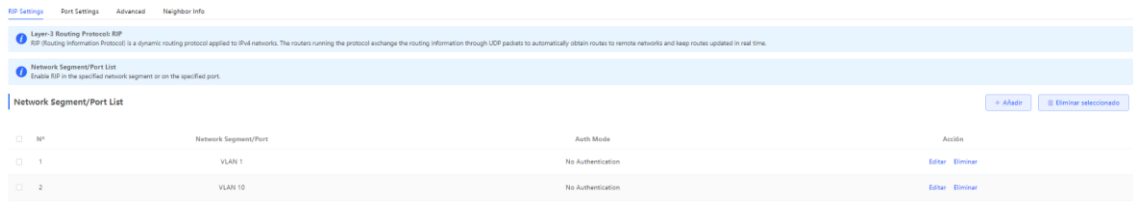
16.4.1 Configuración de las funciones básicas del RIPng

El protocolo de información de enrutamiento de última generación (RIPng) proporciona la función de enrutamiento para redes IPv6.

Este protocolo utiliza el puerto UDP 512 para intercambiar la información de enrutamiento.

Seleccione **Dispositivo local** > **Enrutamiento** > **RIPng Settings**.

Haga clic en **Añadir**, establezca la opción **Type** en **Network Segment** o **Port** e indique el segmento de red o el puerto según corresponda.

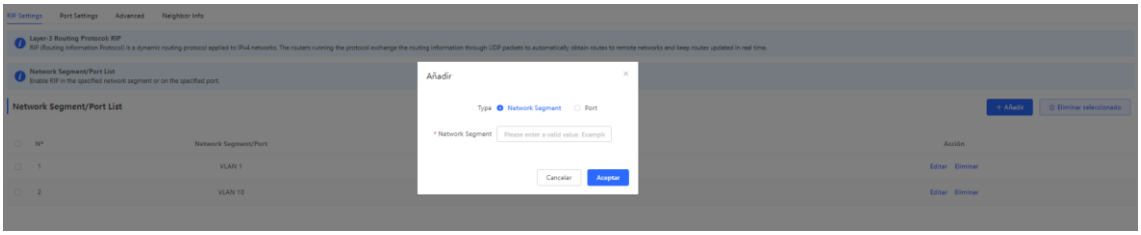


rip.protong

El protocolo de información de enrutamiento de última generación (RIPng) es un protocolo de enrutamiento de unidifusión que se utiliza en las redes IPv6.

Network Segment/Port List

Habilite el RIPng en el segmento de red o en el puerto que haya indicado.



Si la longitud de la dirección se encuentra entre 48 y 64, la dirección se utilizará como prefijo.

O bien, habilite el RIPng en el puerto que indique:

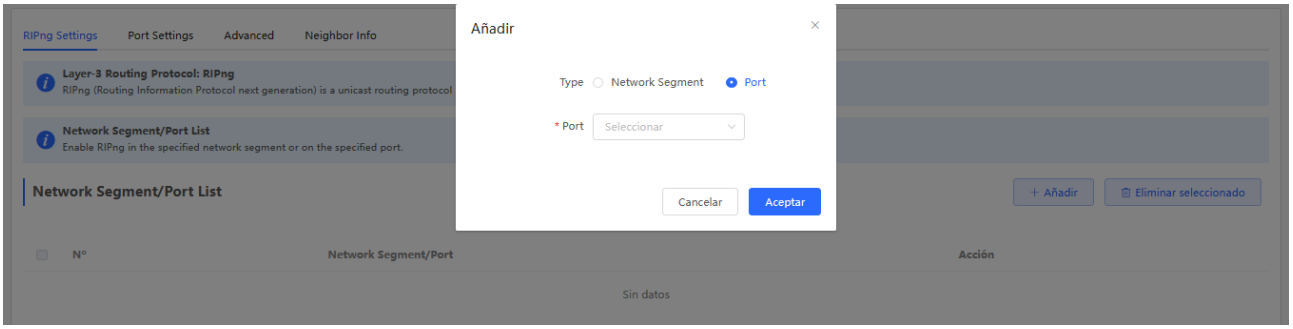


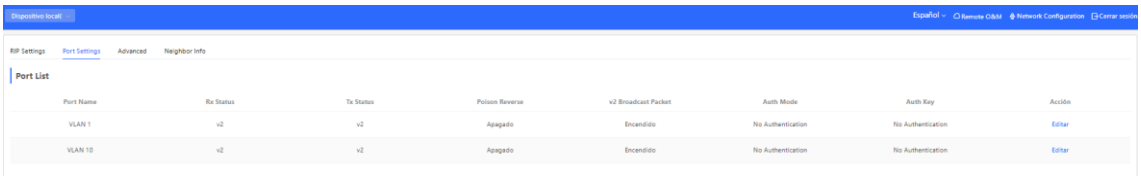
Tabla 16-7 Parámetros de configuración del RIPng

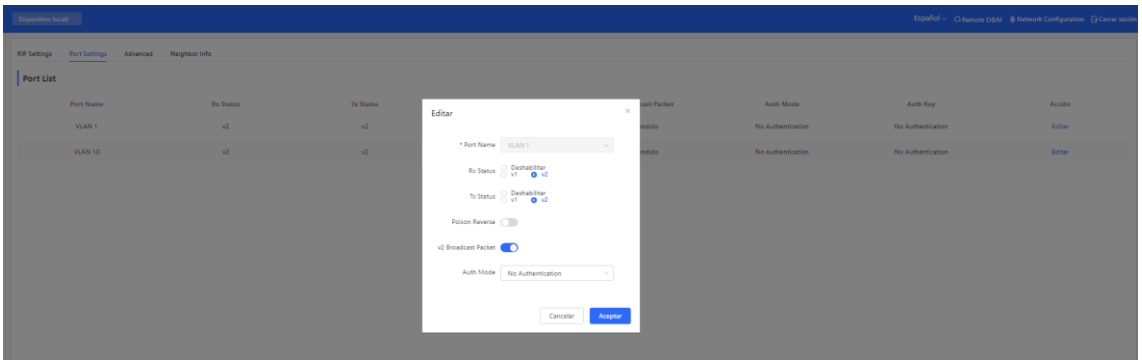
Parámetro	Descripción
Type	**Network Segment**: permite habilitar la opción RIP en el segmento de red que haya indicado. Las direcciones IP de este segmento de red se añaden a la tabla de enrutamiento del RIP y el dispositivo y sus dispositivos cercanos compatibles con el RIP obtienen la tabla de enrutamiento el uno del otro. **Port**: permite habilitar la opción RIP en el puerto que haya indicado. Todas las direcciones IP de este puerto se añaden a la tabla de enrutamiento del RIP y el dispositivo y sus dispositivos cercanos compatibles con el RIP obtienen la tabla de enrutamiento el uno del otro.
Network Segment	Permite introducir la dirección IPv6 y la longitud del prefijo cuando la opción **Type** se establece en **Network Segment**. El RIPng se habilitará en todas las interfaces del dispositivo que abarque este segmento de red.
Port	Permite seleccionar una interfaz VLAN o un puerto físico cuando la opción **Type** se establece en **Port**.

16.4.2 Configuración del puerto RIPng

RIPng Poison Reverse: una vez que el puerto detecta la ruta, la opción de sobrecarga de rutas se establece en **16** (lo que indica que no se puede acceder a la ruta) y esta se devuelve al dispositivo cercano desde el puerto original para evitar que se produzca un bucle.

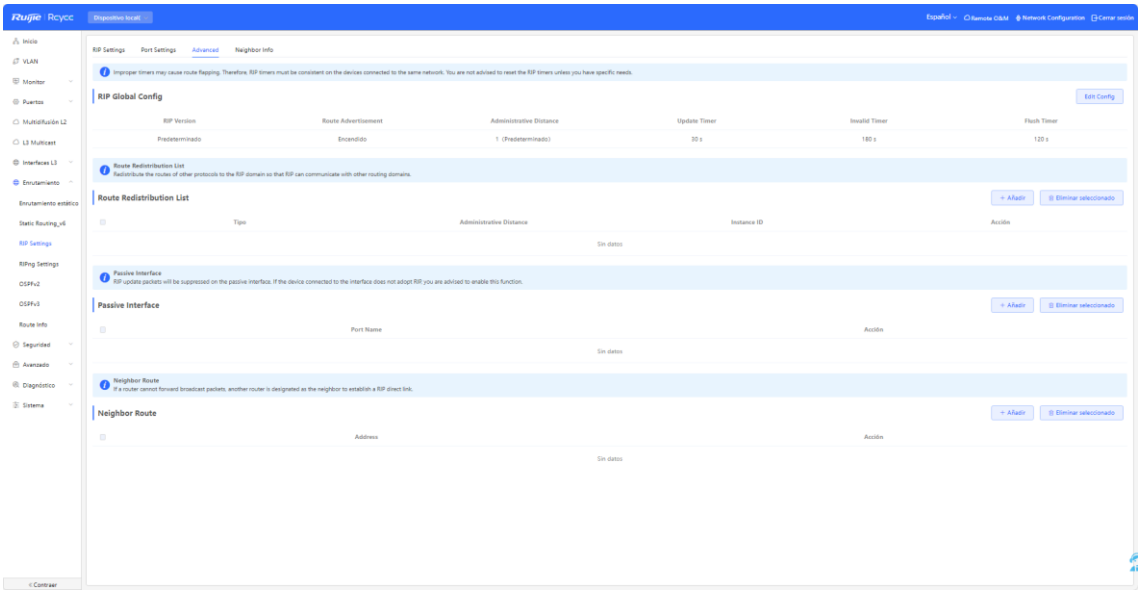
Seleccione **Dispositivo local** > **Enrutamiento** > **RIPng Settings** > **Port Settings**, haga clic en Editar y habilite la opción **Poison Reverse**.





16.4.3 Configuración de la configuración global del RIPng

Seleccione **Dispositivo local** > **Enrutamiento** > **RIPng Settings** > **Advanced** y haga clic en **Edit Config**.



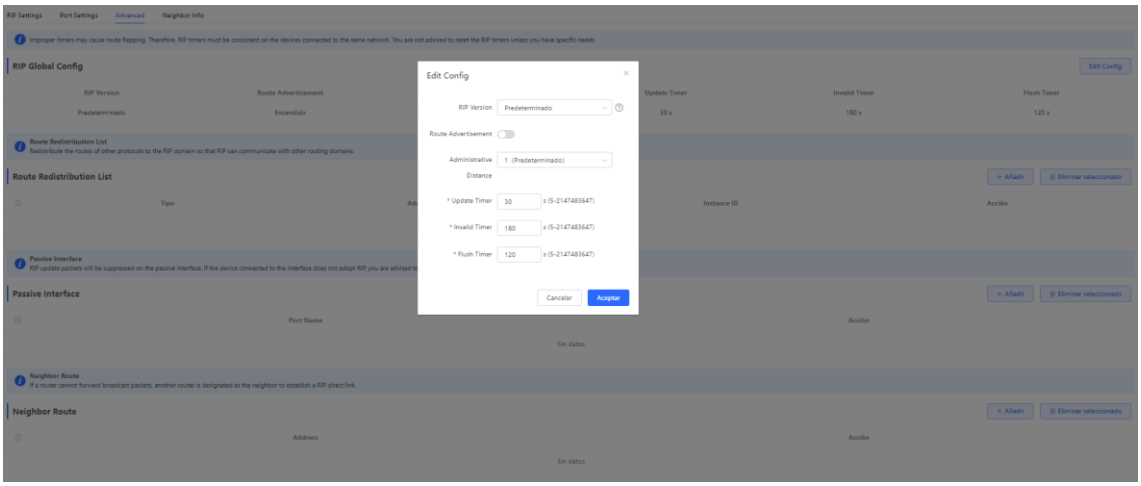


Tabla 16-8 Parámetros de la configuración global del RIPng

Parámetro	Descripción
Route Advertisement	Tras habilitar la opción Anuncio de la ruta (Route Advertisement), el dispositivo actual genera una ruta de forma predeterminada y la envía al dispositivo cercano.
Administrative Distance	Redistribuye rutas de otros protocolos al dominio del RIP para que este interactúe con los demás dominios de enrutamiento.
Update Timer	Ciclo de actualización del RIP. La información del enrutamiento se actualiza cada 30 segundos de forma predeterminada.
Invalid Timer	Si no se recibe ninguna actualización antes de que una ruta deje de ser válida, se considera que no se puede acceder a la ruta. El valor predeterminado es 180 segundos.
Flush Timer	Si no se recibe ninguna actualización antes de que transcurra el tiempo del temporizador de purga de una ruta no válida, la ruta se elimina completamente de la tabla de enrutamiento del RIP. El valor predeterminado es 120 segundos.

16.4.4 Configuración de la lista de redistribución de rutas del RIPng

Redistribuye rutas de otros protocolos al dominio del RIPng para que interactúe con los demás dominios de enrutamiento.

Seleccione **Dispositivo local** > **Enrutamiento** > **RIPng Settings** > **Advanced** y haga clic en **Añadir**.

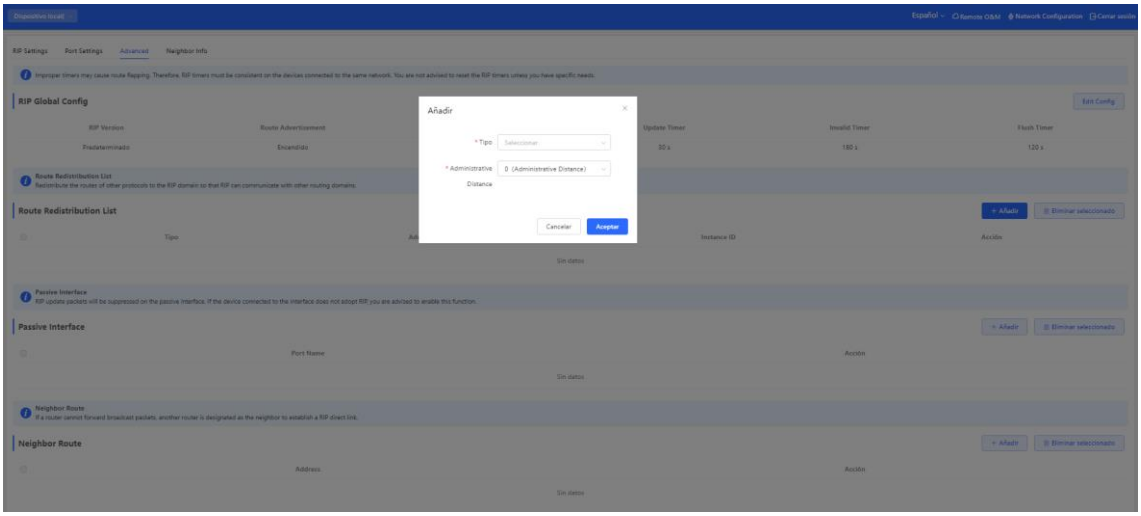


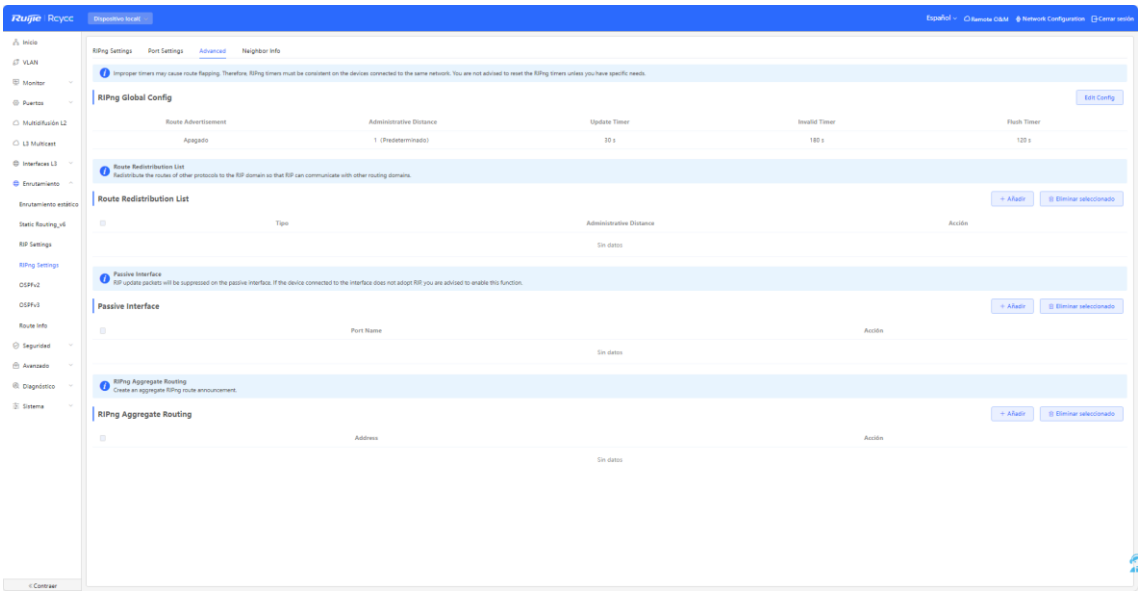
Tabla 16-9 Parámetros de redistribución de rutas del RIP

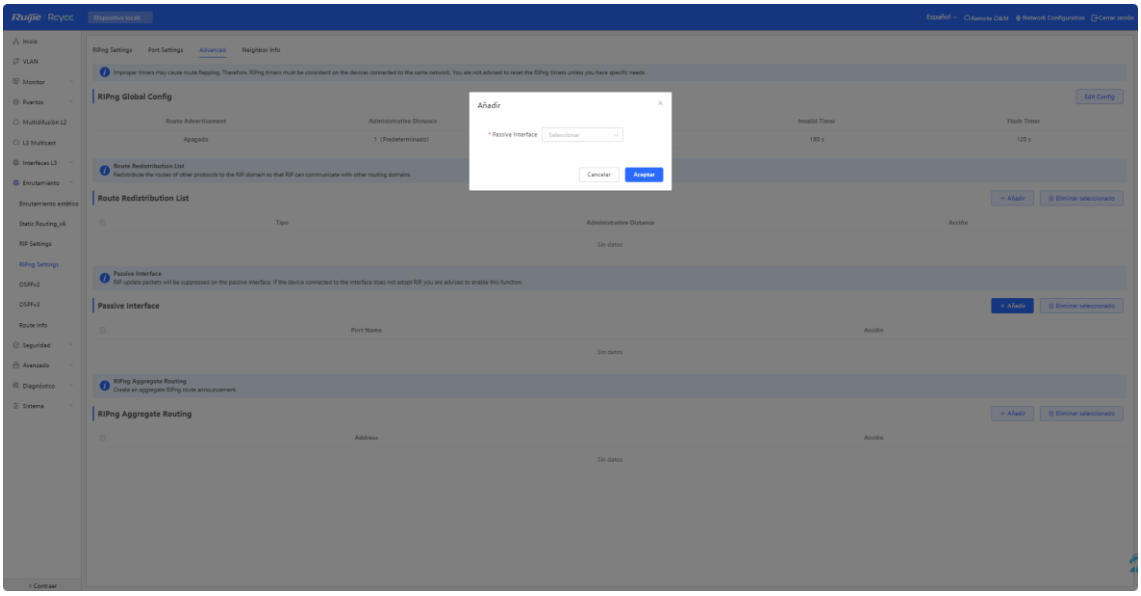
Parámetro	Descripción
Tipo	Enrutamiento directo Enrutamiento del OSPF Enrutamiento estático
Administrative Distance	Rango de valores: 0-16. El valor predeterminado es **0**.

16.4.5 Configuración de la interfaz pasiva del RIPng

Si una interfaz se configura como interfaz pasiva, esta suprimirá los paquetes de actualización del RIPng. Si el dispositivo homólogo conectado no utiliza el RIP, le recomendamos que habilite la interfaz pasiva.

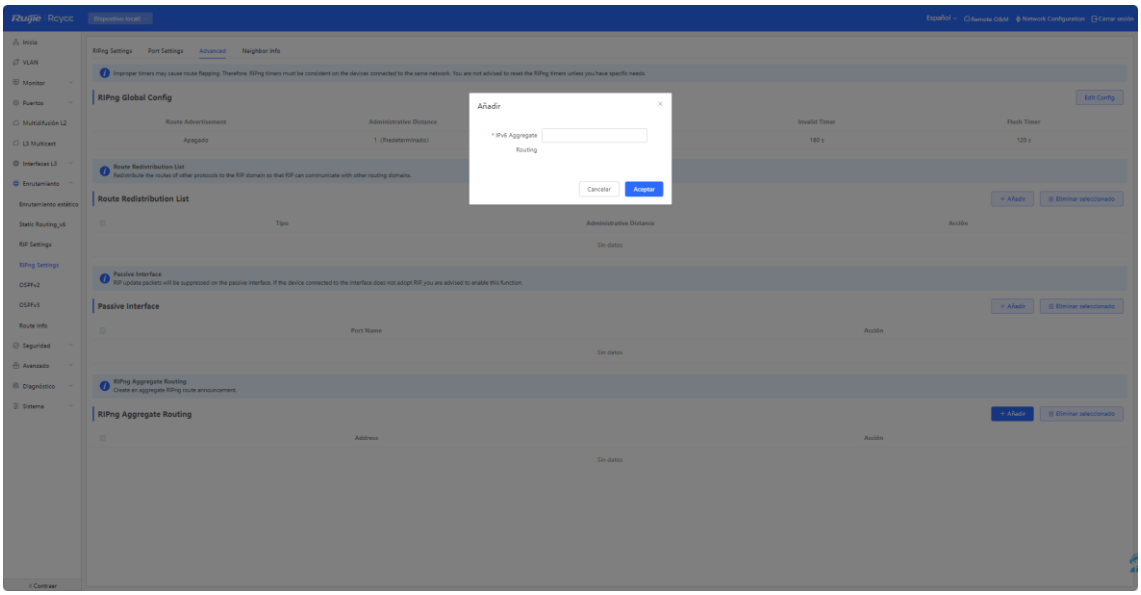
Seleccione **Dispositivo local** > **Enrutamiento** > **RIPng Settings** > **Advanced**, haga clic en **Añadir** e introduzca la dirección IP del router cercano.





16.4.6 Configuración de la ruta agregada IPv6

Seleccione **Dispositivo local** > **Enrutamiento** > **RIP Settings** > **Advanced**, haga clic en **Añadir** e introduzca la dirección IPv6 y la longitud del prefijo (rango de valores: 0-128).



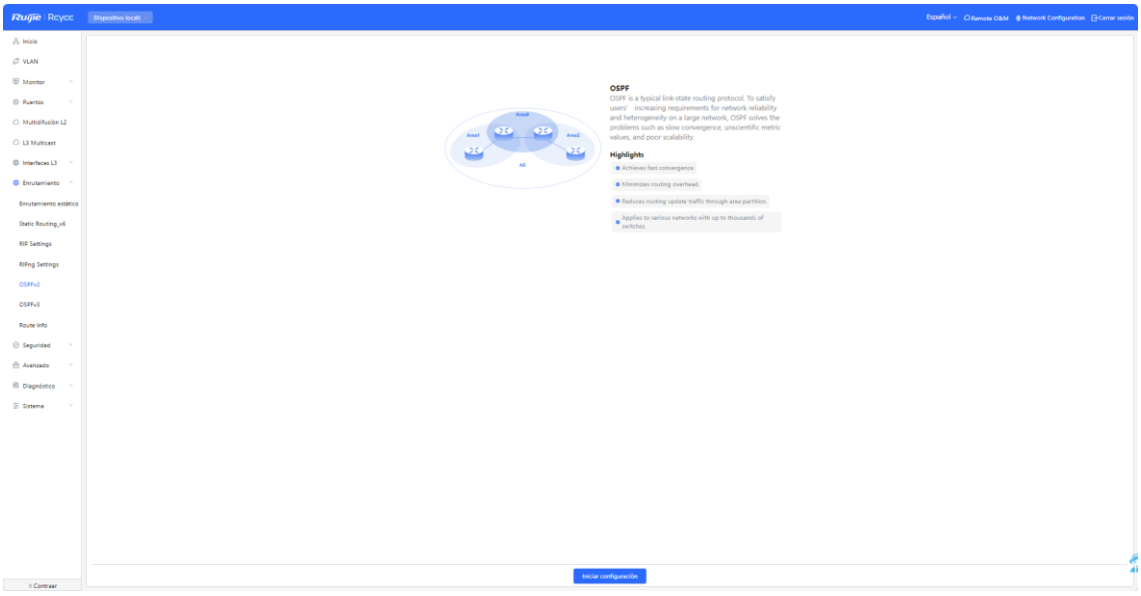
16.5 OSPFv2

El protocolo OSPF (abrir primero la ruta más corta) puede utilizarse en redes de gran escala. El IPv4 utiliza el protocolo OSPFv2 y el IPv6 utiliza el OSPFv3.

El OSPF es un protocolo de enrutamiento de estado de enlace típico que puede resolver los problemas de actualización lenta de rutas, medición imprecisa y mala escalabilidad en redes de gran tamaño. El uso de este protocolo es adecuado para redes de diversos tamaños e incluso para una red con hasta miles de dispositivos.

16.5.1 Configuración de los parámetros básicos del protocolo OSPFv2

Seleccione **Dispositivo local** > **Enrutamiento** > **OSPFv2**, haga clic en **Iniciar configuración** y, a continuación, configure una instancia y una interfaz respectivamente.



(1) Configure una instancia.

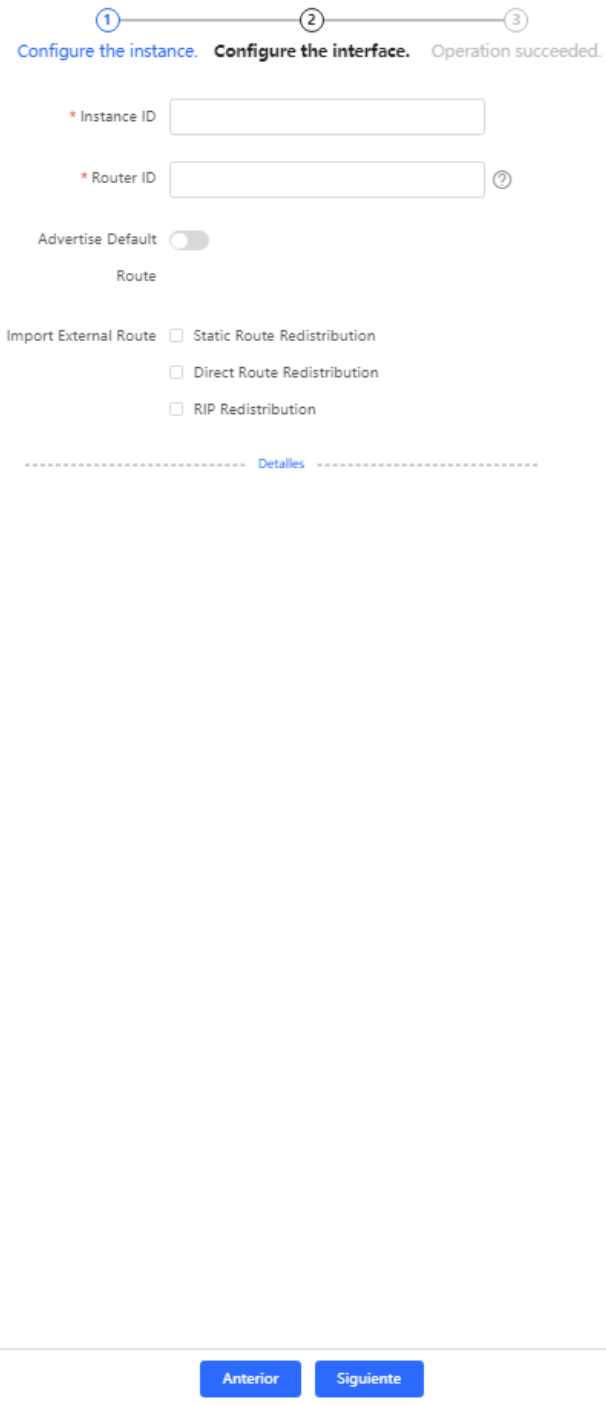


Tabla 16-10 Parámetros de configuración de las instancias

Parámetro	Descripción
Instance ID	Cree una instancia del OSPF basándose en el tipo de servicio. La instancia solo se aplica a nivel local y no afecta al intercambio de paquetes con otros dispositivos.
Router ID	Permite identificar un router en un dominio OSPF. **Precaución** Los ID de router que se encuentran en el mismo dominio debe ser únicos. Si se utiliza la misma configuración, esto podría provocar que se produzcan errores a la hora de detectar dispositivos cercanos.
Advertise Default Route	Genera una ruta predeterminada y la envía al dispositivo cercano. Tras habilitar esta función, debe introducir la métrica y seleccionar un tipo. La métrica predeterminada es **1**. Tipo 1: las métricas que se muestran en los diferentes routers varían. Tipo 2: las métricas que se muestran en todos los routers son las mismas.

Parámetro	Descripción
Import External Route	Redistribuye rutas de otros protocolos al dominio del OSPF para que interactúe con los demás dominios de enrutamiento. Si selecciona **Static Route Redistribution**, debe introducir el valor, que es **20** de forma predeterminada. Si selecciona **Direct Route Redistribution**, debe introducir el valor, que es **20** de forma predeterminada. Si selecciona **RIP Redistribution**, debe introducir el valor, que es **20** de forma predeterminada.
Detalles	Permite ampliar la configuración detallada.

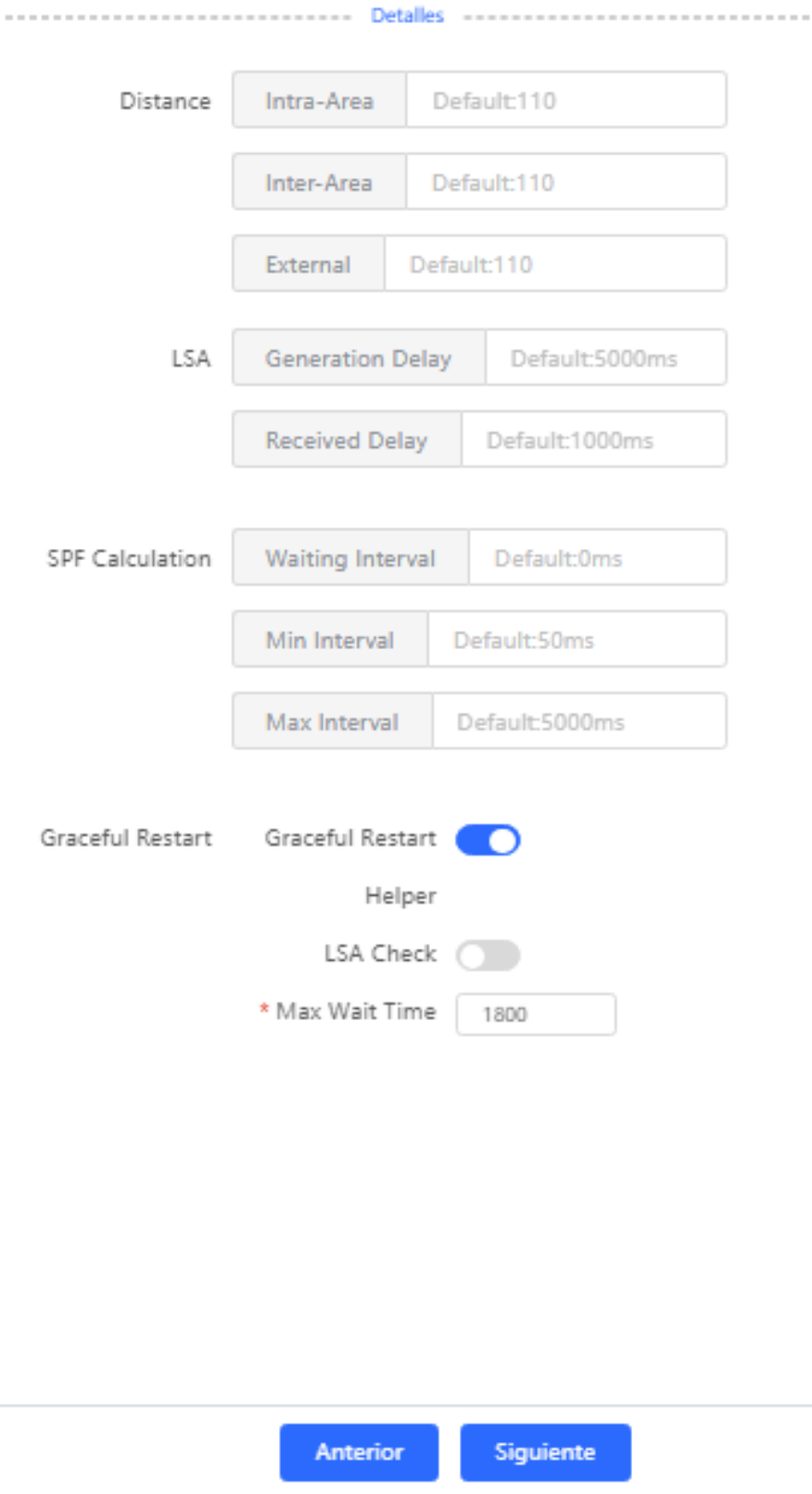

Detalles
Distance
Intra-Area
Default:110
Inter-Area
Default:110
External
Default:110
LSA
Generation Delay
Default:5000ms
Received Delay
Default:1000ms
SPF Calculation
Waiting Interval
Default:0ms
Min Interval
Default:50ms
Max Interval
Default:5000ms
Graceful Restart
Graceful Restart
Helper
LSA Check
* Max Wait Time
1800
Anterior
Siguiente

Tabla 16-11 Parámetros de la configuración detallada de instancias

Parámetro	Descripción
Distancia	Se utiliza para seleccionar el protocolo. De forma predeterminada, las distancias intraárea (intra-area), interárea (inter-area) y externa (external) son **110**.
LSA	Los cambios frecuentes en la red y la fluctuación de rutas pueden ocupar demasiado ancho de banda de red y recursos del dispositivo. Los retardos de la generación y la recepción del LSA se indican en el OSPF de forma predeterminada. El valor predeterminado son 1000 ms.
SPF Calculation	Cuando se produce un cambio en la base de datos de estado de enlace (LSDB), el OSPF vuelve a calcular la ruta más corta y establece el intervalo para evitar que los cambios frecuentes en la red ocupen un gran número de recursos. **Waiting Interval**: cuando el estado cambia, el temporizador se activa. El retraso se calcula por primera vez al finalizar el tiempo del temporizador. El valor predeterminado son 0 ms. **Min Interval**: a medida que aumenta el número de cambios, el tiempo de cada intervalo aumenta en función del algoritmo y el valor por defecto son 50 ms. **Max Interval**: cuando el intervalo calculado alcanza el intervalo máximo, el intervalo posterior siempre es igual al intervalo máximo. Si el tiempo transcurrido desde que se ha realizado el último cálculo supera el intervalo máximo y la LSDB no se actualiza, el temporizador se desactiva.

Parámetro	Descripción
Graceful Restart	El reinicio de gracia (GR) puede evitar la fluctuación de rutas que se produce debido a la interrupción del tráfico y a la conmutación de la placa activa/standby, garantizando así la estabilidad de los servicios clave. **Graceful Restart Helper**: la función Graceful Restart Helper se habilita al encender el switch. **LSA Check**: los paquetes del LSA fuera del dominio se comprueban al encender el switch. **Max Wait Time**: el tiempo comienza una vez que el dispositivo recibe el paquete del GR del dispositivo homólogo. Si el dispositivo homólogo no realiza el GR dentro del **Max Wait Time**, el dispositivo sale del modo GR Helper. El valor predeterminado es 1800 segundos.

(2) **Configure una interfaz.**

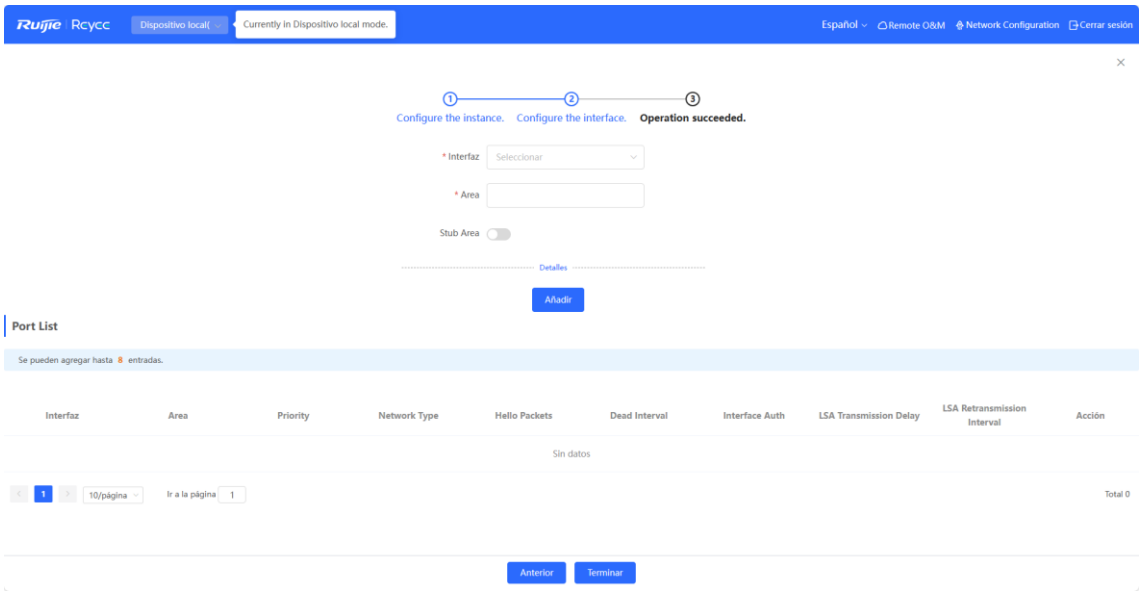


Tabla 16-12 Parámetros de configuración de una interfaz

Parámetro	Descripción
Interfaz	Seleccione la interfaz L3 compatible con el OSPF.
Area	Configure el ID de zona. Rango de valores: 0-4294967295
Stub Area	Si la opción **Stub Area** se encuentra habilitada, debe configurar el tipo de zona y el aislamiento de rutas entre zonas. Stub area: los routers situados en el borde de la zona no anuncian rutas fuera de la zona, por lo que la tabla de enrutamiento de la zona es pequeña. Not-So-Stubby Area (NSSA): permite importar algunas rutas externas. Inter-area route isolation: tras habilitar esta función, las rutas entre zonas no se importan a esta zona.
Detalles	Permite ampliar la configuración detallada.

(3)

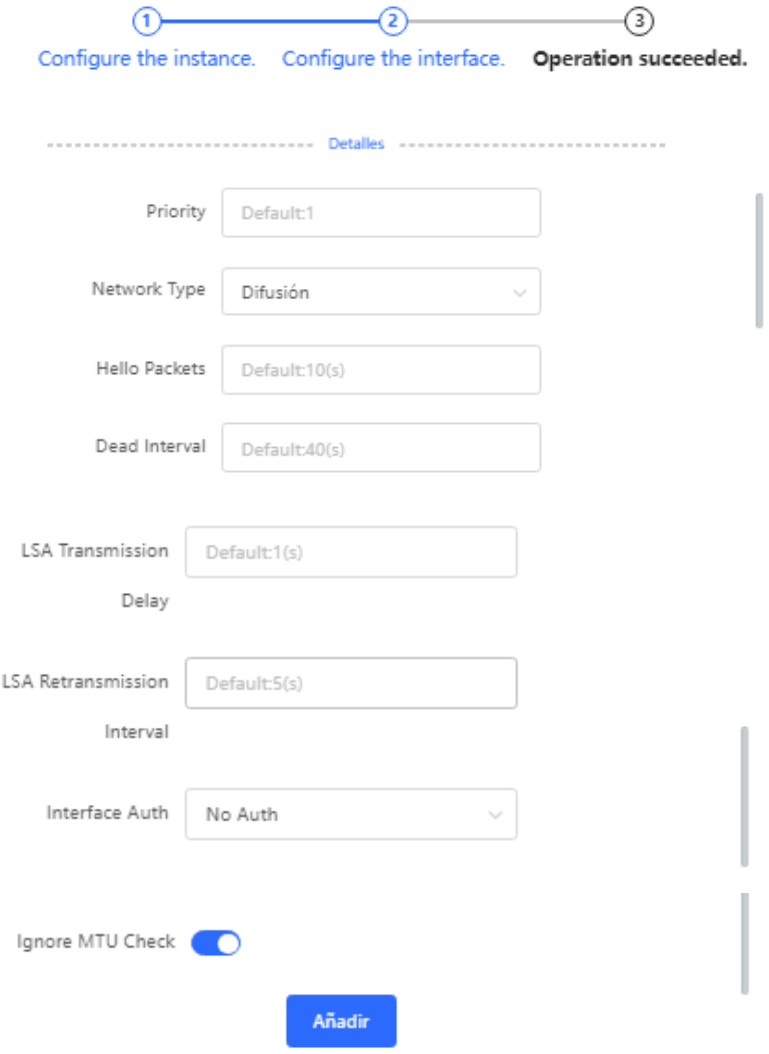


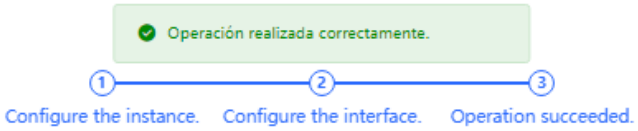
Tabla 16-13 Parámetros de la configuración detallada de una interfaz

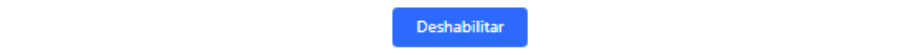
Parámetro	Descripción
Priority	El valor es 1 de forma predeterminada.
Network Type	Difusión Unidifusión Multidifusión Acceso múltiple sin difusión

Parámetro	Descripción
Hello Packets	Intervalo para la transmisión periódica, que se utiliza para detectar y mantener la relación de dispositivos cercanos del OSPF. El valor predeterminado es 10 segundos.
Dead Interval	Tiempo tras el cual el dispositivo cercano deja de ser válido. El valor predeterminado es 40 segundos.
LSA Transmission Delay	Retardo de la transmisión del LSA de la interfaz. El valor predeterminado es 1 segundo.
LSA Retransmission Interval	Tiempo tras el cual se retransmite el LSA después de que este se pierda. El valor predeterminado es 5 segundos.
Interface Auth	**No Auth**: los paquetes del protocolo no se autentican. Es el valor predeterminado. **Plain Text**: los paquetes del protocolo se autentican y la clave de autenticación se envía junto con los paquetes del protocolo en forma de texto plano. **MD5**: los paquetes del protocolo se autentican y la clave de autenticación se encripta mediante el algoritmo MD5. A continuación, esta se envía junto con los paquetes del protocolo.
Ignore MTU Check	Se encuentra habilitada de forma predeterminada.

(2) Realice la configuración.

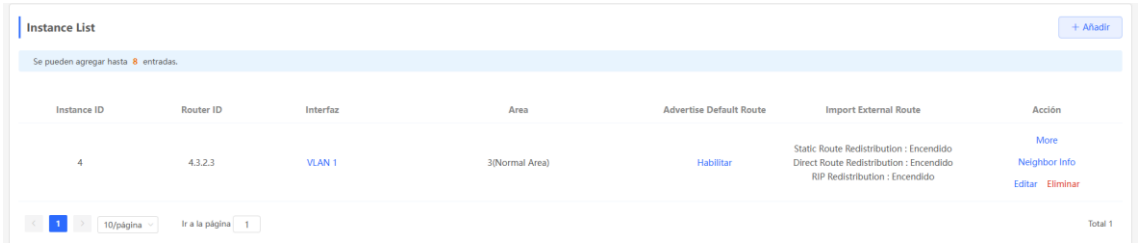
Tras realizar la configuración, puede seleccionar **Dispositivo local** > **Enrutamiento** > **OSPFv2** y ver la lista de instancias.

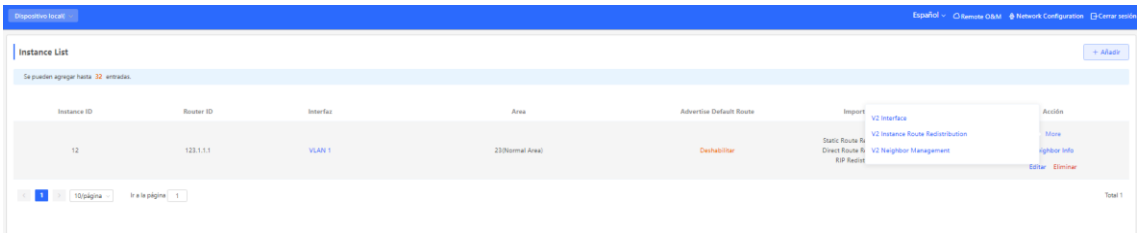


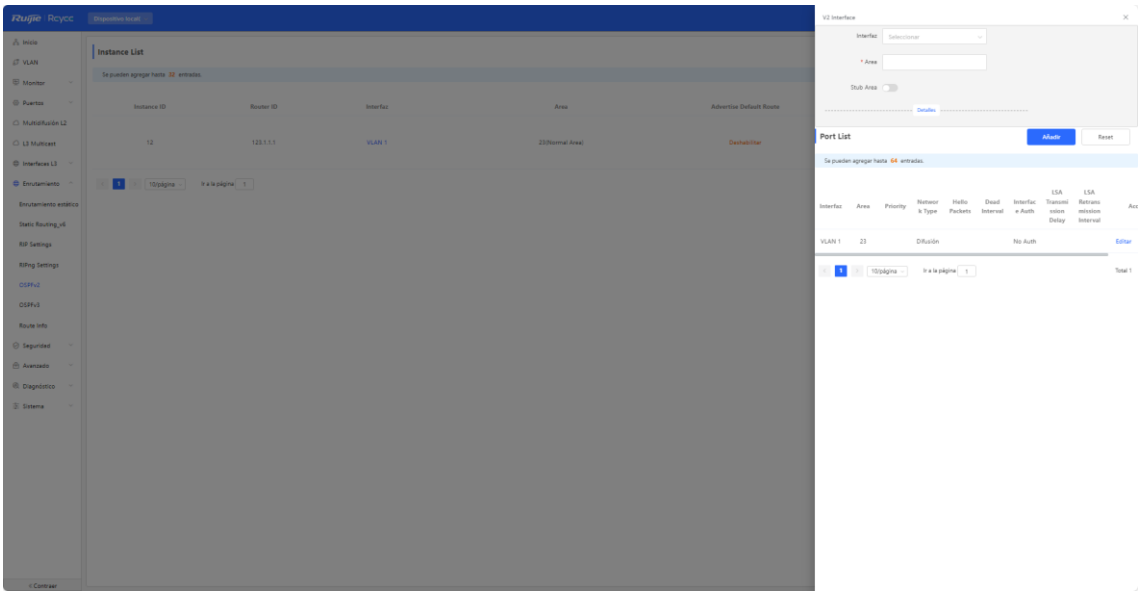


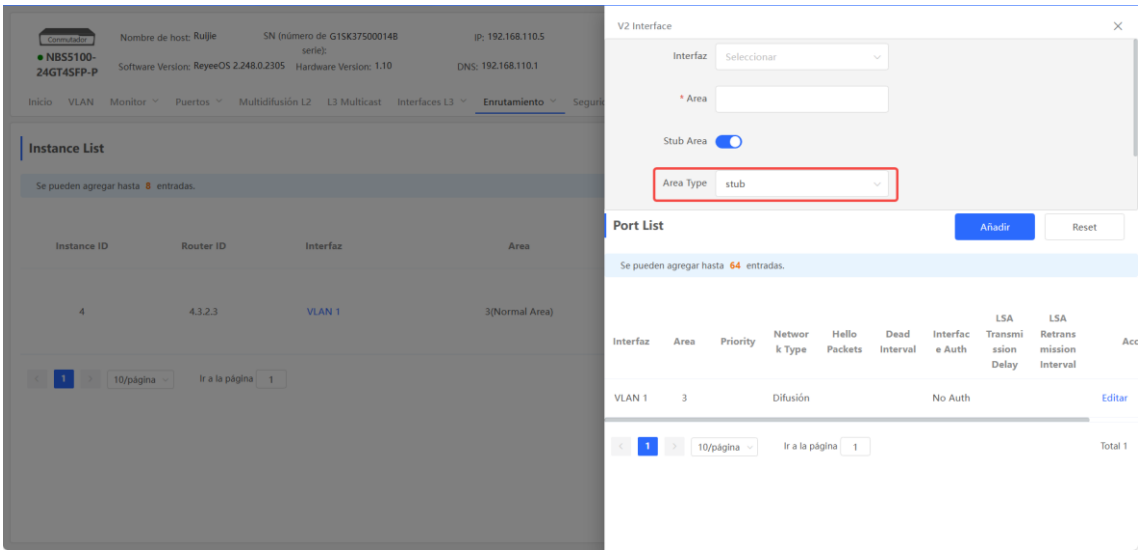
16.5.2 Adición de una interfaz OSPFv2

Seleccione **Dispositivo local** > **Enrutamiento** > **OSPFv2**, haga clic en **More** en la columna **Acción** y seleccione **V2 Interface**.


Instance List
+ Añadir
Se pueden agregar hasta 8 entradas.
Instance ID
Router ID
Interfaz
Area
Advertise Default Route
Import External Route
Acción
4
4.3.2.3
VLAN 1
3(Normal Area)
Habilitar
Static Route Redistribution : Encendido
Direct Route Redistribution : Encendido
RIP Redistribution : Encendido
More
Neighbor Info
Editar
Eliminar
10/página
Ir a la página
1
Total 1

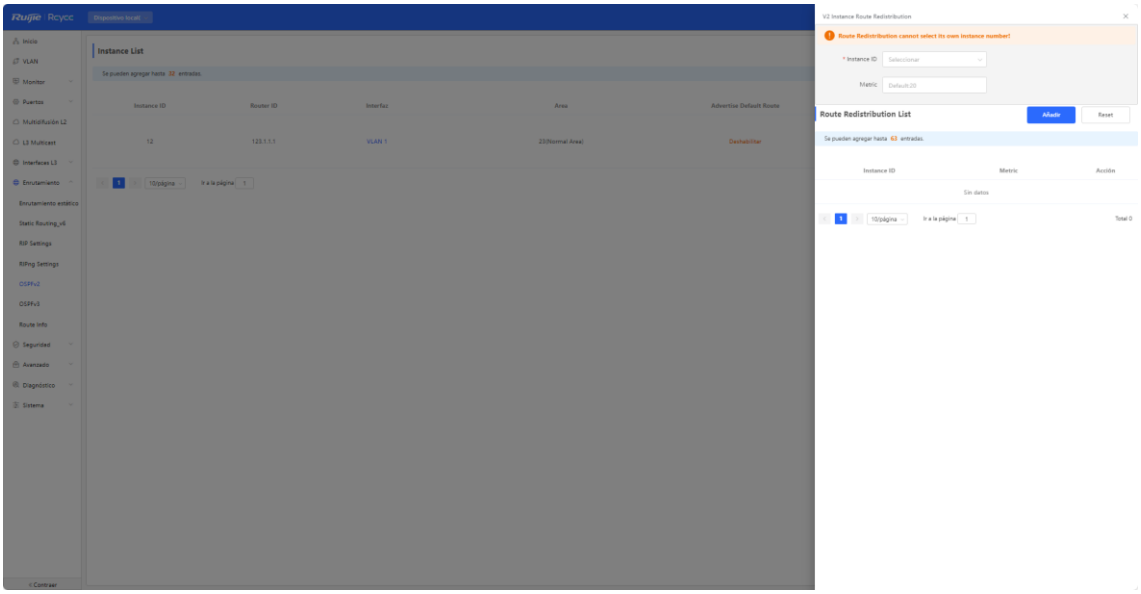

Instance List
+ Añadir
V2 Interface
V2 Instance Route Redistribution
V2 Neighbor Management
Editar
Eliminar
Total 1


Instance List
V2 Interface
Port List
Añadir
Reset


Nombre de host: Ruijie
SN (número de serie): G1SK37500148
IP: 192.168.110.5
NBS5100-24GT4SFP-P
Software Version: ReyeeOS 2.248.0.2305
Hardware Version: 1.10
DNS: 192.168.110.1
Inicio
VLAN
Monitor
Puertos
Multidifusión L2
L3 Multicast
Interfaces L3
Enrutamiento
Instance List
Se pueden agregar hasta 8 entradas.
Instance ID
Router ID
Interfaz
Area
4
4.3.2.3
VLAN 1
3(Normal Area)
10/página
Ir a la página
1
V2 Interface
Interfaz
Seleccionar
* Area
Stub Area
Area Type
stub
Port List
Añadir
Reset
Se pueden agregar hasta 64 entradas.
Interfaz
Area
Priority
Network Type
Hello Packets
Dead Interval
Interface Auth
LSA Transmission Delay
LSA Retransmission Interval
VLAN 1
3
Difusión
No Auth
Editar
10/página
Ir a la página
1
Total 1

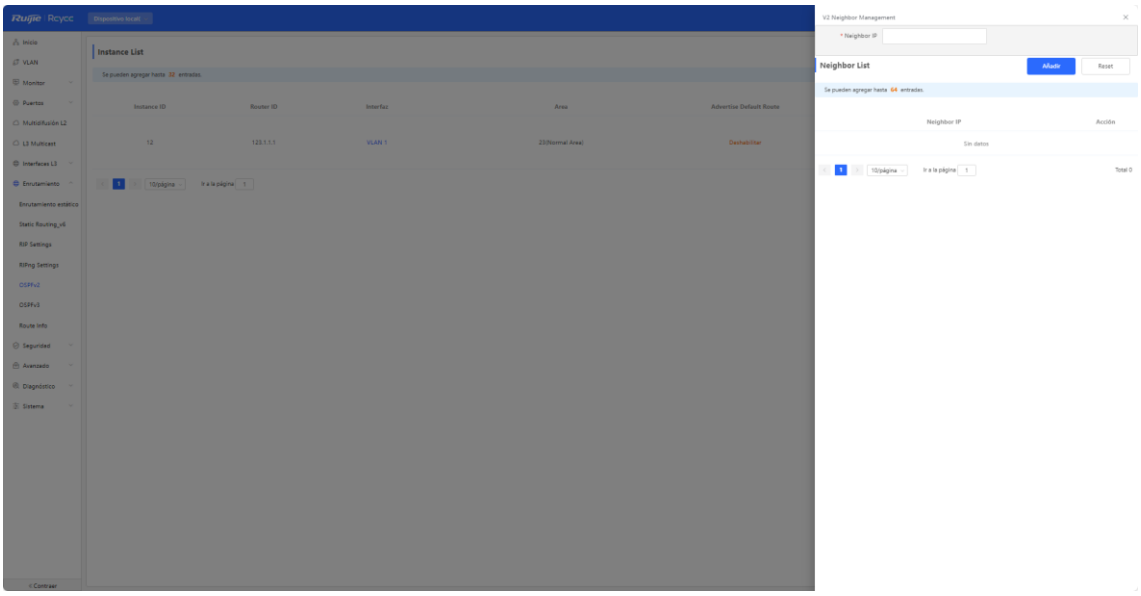
16.5.3 Redistribución de rutas de instancias del OSPFv2

Seleccione **Dispositivo local** > **Enrutamiento** > **OSPFv2**, haga clic en **More** en la columna **Acción** y seleccione **V2 Instance Route Redistribution**.



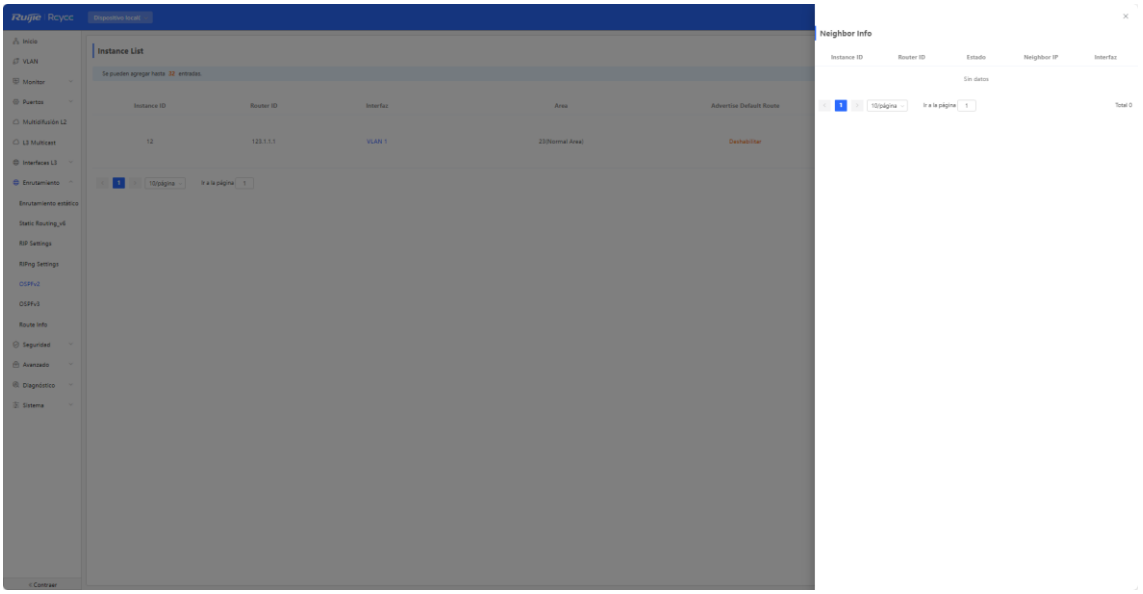
16.5.4 Gestión de dispositivos cercanos del OSPFv2

Seleccione **Dispositivo local** > **Enrutamiento** > **OSPFv2**, haga clic en **More** en la columna **Acción** y seleccione **V2 Neighbor Management**.



16.5.5 Visualización de la información de los dispositivos cercanos del OSPFv2

Seleccione **Dispositivo local** > **Enrutamiento** > **OSPFv2** y haga clic en **Neighbor Info** en la columna **Acción**.



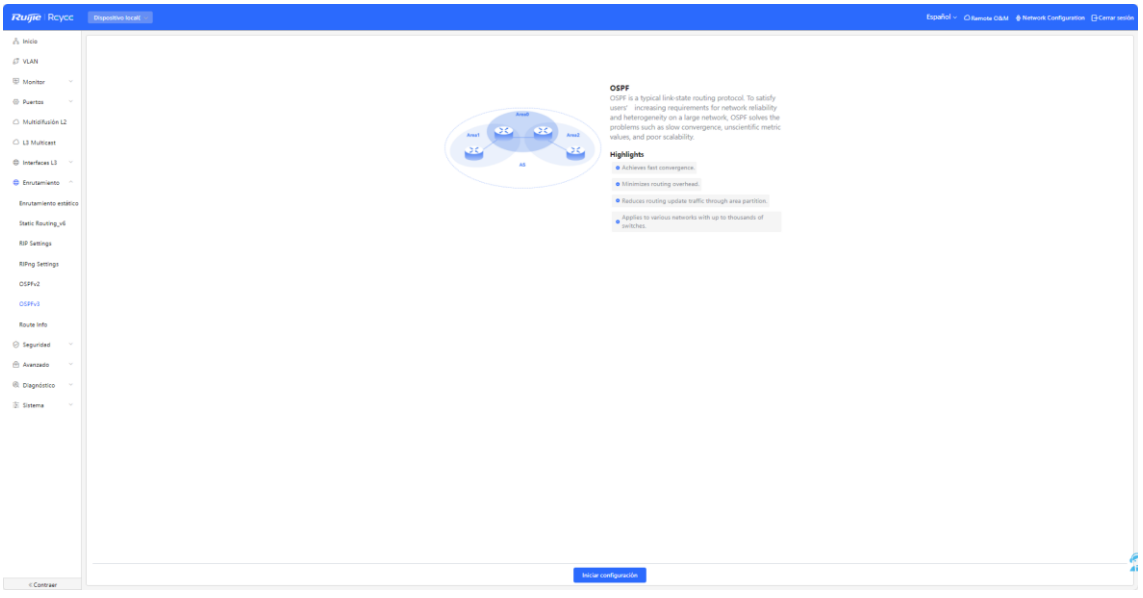
16.6 OSPFv3

El protocolo OSPF (abrir primero la ruta más corta) puede utilizarse en redes de gran escala. El IPv4 utiliza el protocolo OSPFv2 y el IPv6 utiliza el OSPFv3.

16.6.1 Configuración de los parámetros básicos del protocolo OSPFv3

Seleccione **Dispositivo local** > **Enrutamiento** > **OSPFv3**, haga clic en **Iniciar configuración** y, a continuación, configure una instancia y una interfaz respectivamente.

1. **Configure una instancia.**



OSPF

El OSPF es un protocolo de enrutamiento de estado de enlace típico. Para responder a las crecientes necesidades de los usuarios respecto a la fiabilidad y la heterogeneidad de la red en las redes de gran tamaño, el OSPF resuelve problemas como la convergencia lenta, los valores de las métricas imprecisos y la mala escalabilidad.

Características destacadas

Logra una convergencia rápida.

Minimiza la sobrecarga del enrutamiento.

Reduce el tráfico de actualización del enrutamiento a través de la partición de las zonas.

Puede aplicarse a distintas redes con hasta miles de switches.

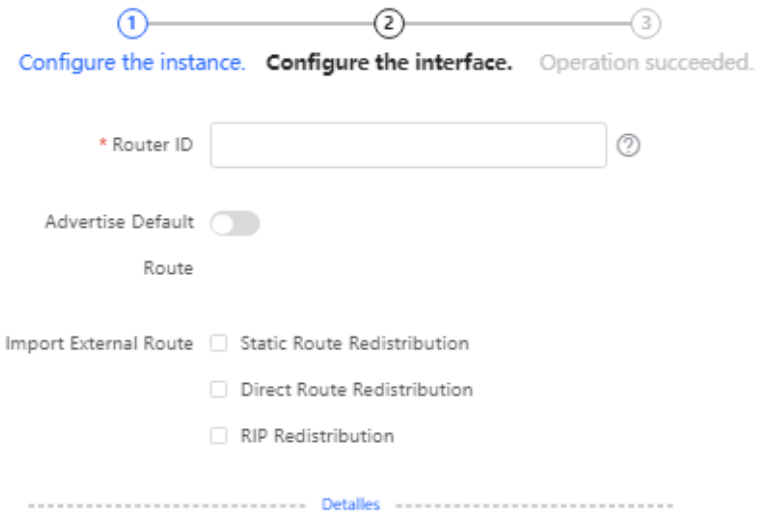

1
2
3
Configure the instance.
Configure the interface.
Operation succeeded.
* Router ID
Advertise Default Route
Import External Route
Static Route Redistribution
Direct Route Redistribution
RIP Redistribution
Detalles
Anterior
Siguiente

Tabla 16-14 Parámetros de configuración de las instancias

Parámetro	Descripción
Instance ID	Cree una instancia del OSPF basándose en el tipo de servicio. La instancia solo se aplica a nivel local y no afecta al intercambio de paquetes con otros dispositivos.
Router ID	Permite identificar un router en un dominio OSPF. **Precaución** Los ID de router que se encuentran en el mismo dominio debe ser únicos. Si se utiliza la misma configuración, esto podría provocar que se produzcan errores a la hora de detectar dispositivos cercanos.
Advertise Default Route	Genera una ruta predeterminada y la envía al dispositivo cercano. Tras habilitar esta función, debe introducir la métrica y seleccionar un tipo. La métrica predeterminada es **1**. Type 1: las métricas que se muestran en los diferentes routers varían. Type 2: las métricas que se muestran en todos los routers son las mismas.

Parámetro	Descripción
Import External Route	Redistribuye rutas de otros protocolos al dominio del OSPF para que interactúe con los demás dominios de enrutamiento. Si selecciona **Static Route Redistribution**, debe introducir el valor, que es **20** de forma predeterminada. Si selecciona **Direct Route Redistribution**, debe introducir el valor, que es **20** de forma predeterminada. Si selecciona **RIP Redistribution**, debe introducir el valor, que es **20** de forma predeterminada.
Detalles	Permite ampliar la configuración detallada.

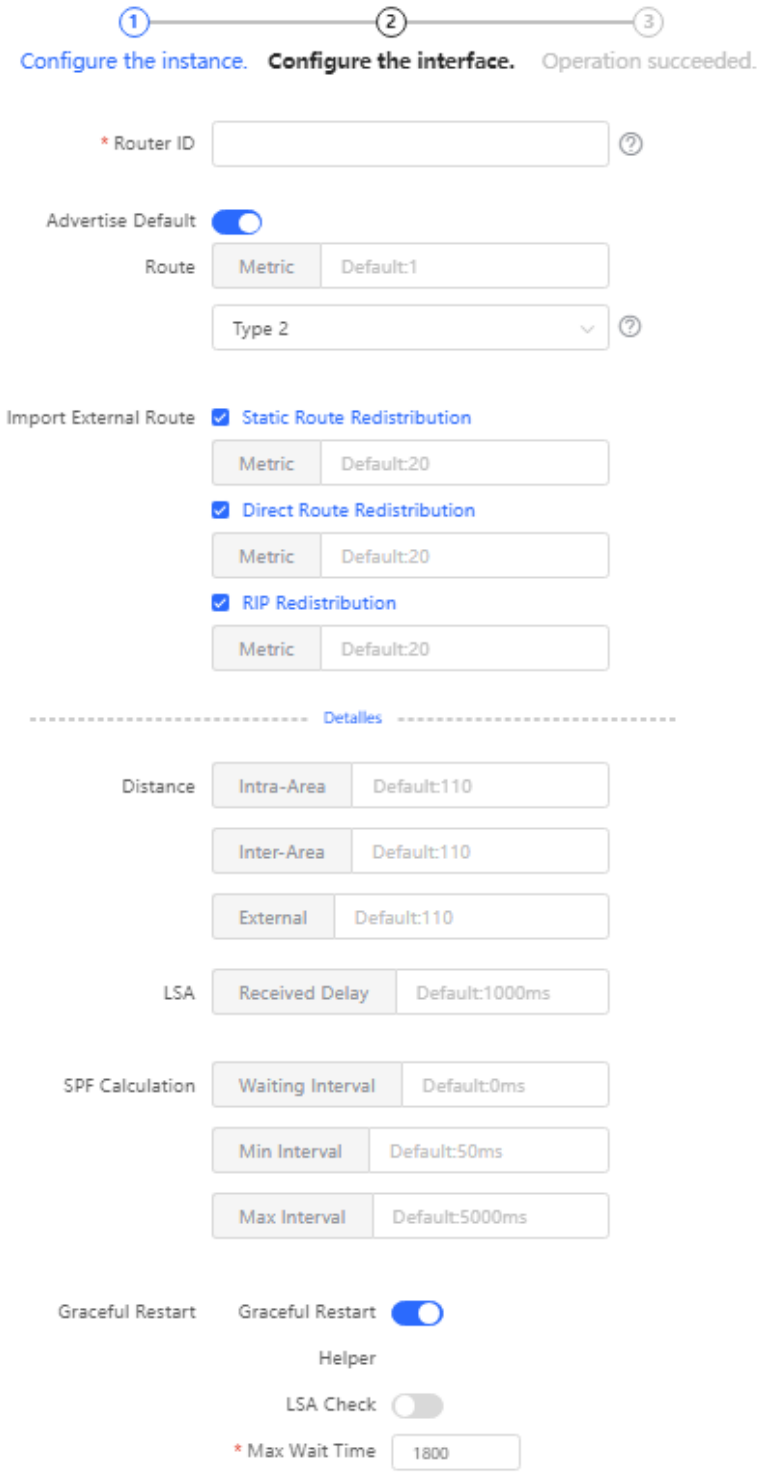

1
2
3
Configure the instance.
Configure the interface.
Operation succeeded.
* Router ID
Advertise Default Route
Metric
Default:1
Type 2
Import External Route
Static Route Redistribution
Metric
Default:20
Direct Route Redistribution
Metric
Default:20
RIP Redistribution
Metric
Default:20
Detalles
Distance
Intra-Area
Default:110
Inter-Area
Default:110
External
Default:110
LSA
Received Delay
Default:1000ms
SPF Calculation
Waiting Interval
Default:0ms
Min Interval
Default:50ms
Max Interval
Default:5000ms
Graceful Restart
Graceful Restart
Helper
LSA Check
* Max Wait Time
1800
Anterior
Siguiente

Tabla 16-15 Parámetros de la configuración detallada de instancias

Parámetro	Descripción
Distance	Se utiliza para seleccionar el protocolo. De forma predeterminada, las distancias intraárea (intra-area), interárea (inter-area) y externa (external) son **110**.
LSA	Los cambios frecuentes en la red y la fluctuación de rutas pueden ocupar demasiado ancho de banda de red y recursos del dispositivo. Los retardos de la generación y la recepción del LSA se indican en el OSPF de forma predeterminada. El valor predeterminado son 1000 ms.
SPF Calculation	Cuando se produce un cambio en la base de datos de estado de enlace (LSDB), el OSPF vuelve a calcular la ruta más corta y establece el intervalo para evitar que los cambios frecuentes en la red ocupen un gran número de recursos. **Waiting Interval**: cuando el estado cambia, el temporizador se activa. El retraso se calcula por primera vez al finalizar el tiempo del temporizador. El valor predeterminado son 0 ms. **Min Interval**: a medida que aumenta el número de cambios, el tiempo de cada intervalo aumenta en función del algoritmo y el valor por defecto son 50 ms. **Max Interval**: cuando el intervalo calculado alcanza el intervalo máximo, el intervalo posterior siempre es igual al intervalo máximo. Si el tiempo transcurrido desde que se ha realizado el último cálculo supera el intervalo máximo y la LSDB no se actualiza, el temporizador se desactiva.

Parámetro	Descripción
Graceful Restart	El reinicio de gracia (GR) puede evitar la fluctuación de rutas que se produce debido a la interrupción del tráfico y a la conmutación de la placa activa/standby, garantizando así la estabilidad de los servicios clave. **Graceful Restart Helper**: la función Graceful Restart Helper se habilita al encender el switch. **LSA Check**: los paquetes del LSA fuera del dominio se comprueban al encender el switch. **Max Wait Time**: el tiempo comienza una vez que el dispositivo recibe el paquete del GR del dispositivo homólogo. Si el dispositivo homólogo no realiza el GR dentro del **Max Wait Time**, el dispositivo sale del modo GR Helper. El valor predeterminado es 1800 segundos.

2. Configure una interfaz.

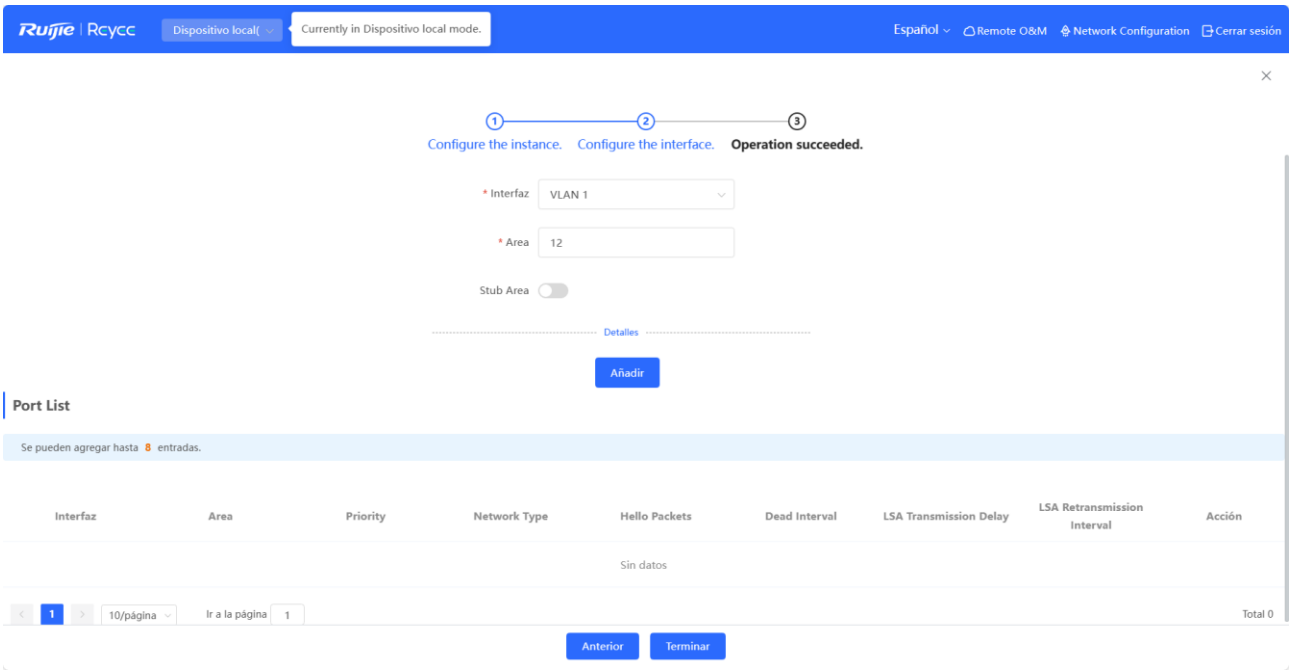
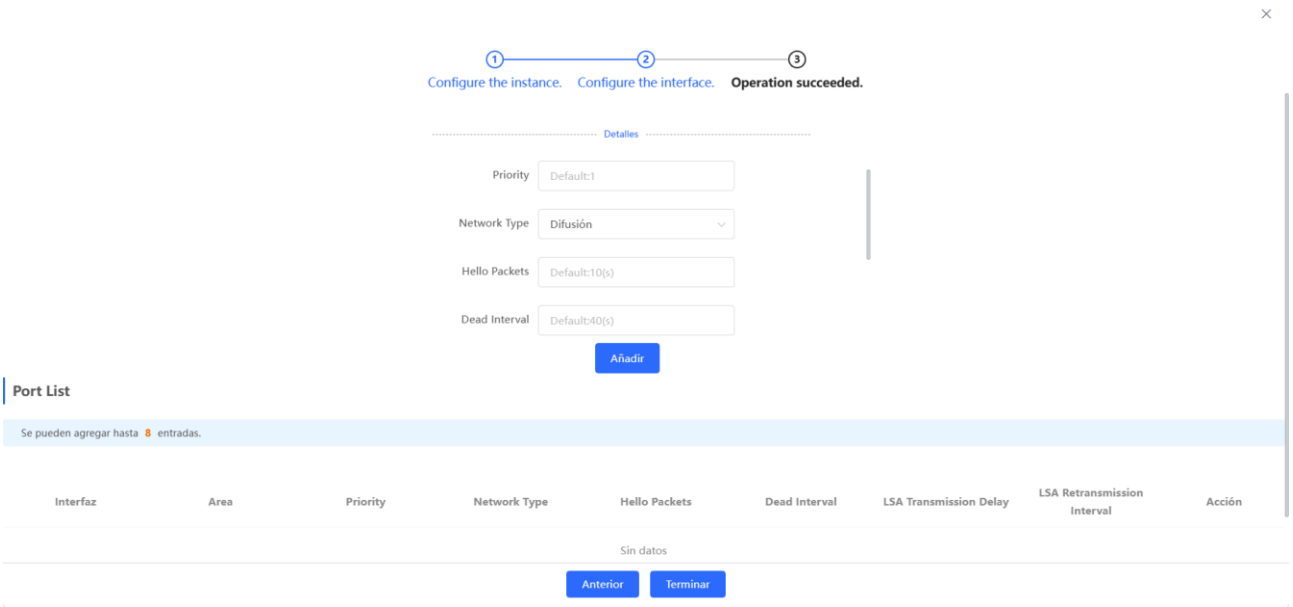


Tabla 16-16 Parámetros de configuración de una interfaz

Parámetro	Descripción
Interfaz	Seleccione la interfaz L3 compatible con el OSPF.
Area	Configure el ID de zona. Rango de valores: 0-4294967295
Stub Area	Si la opción **Stub Area** se encuentra habilitada, debe configurar el tipo de zona y el aislamiento de rutas entre zonas. Stub area: los routers situados en el borde de la zona no anuncian rutas fuera de la zona, por lo que la tabla de enrutamiento de la zona es pequeña. Not-So-Stubby Area (NSSA): permite importar algunas rutas externas.
Detalles	Permite ampliar la configuración detallada.



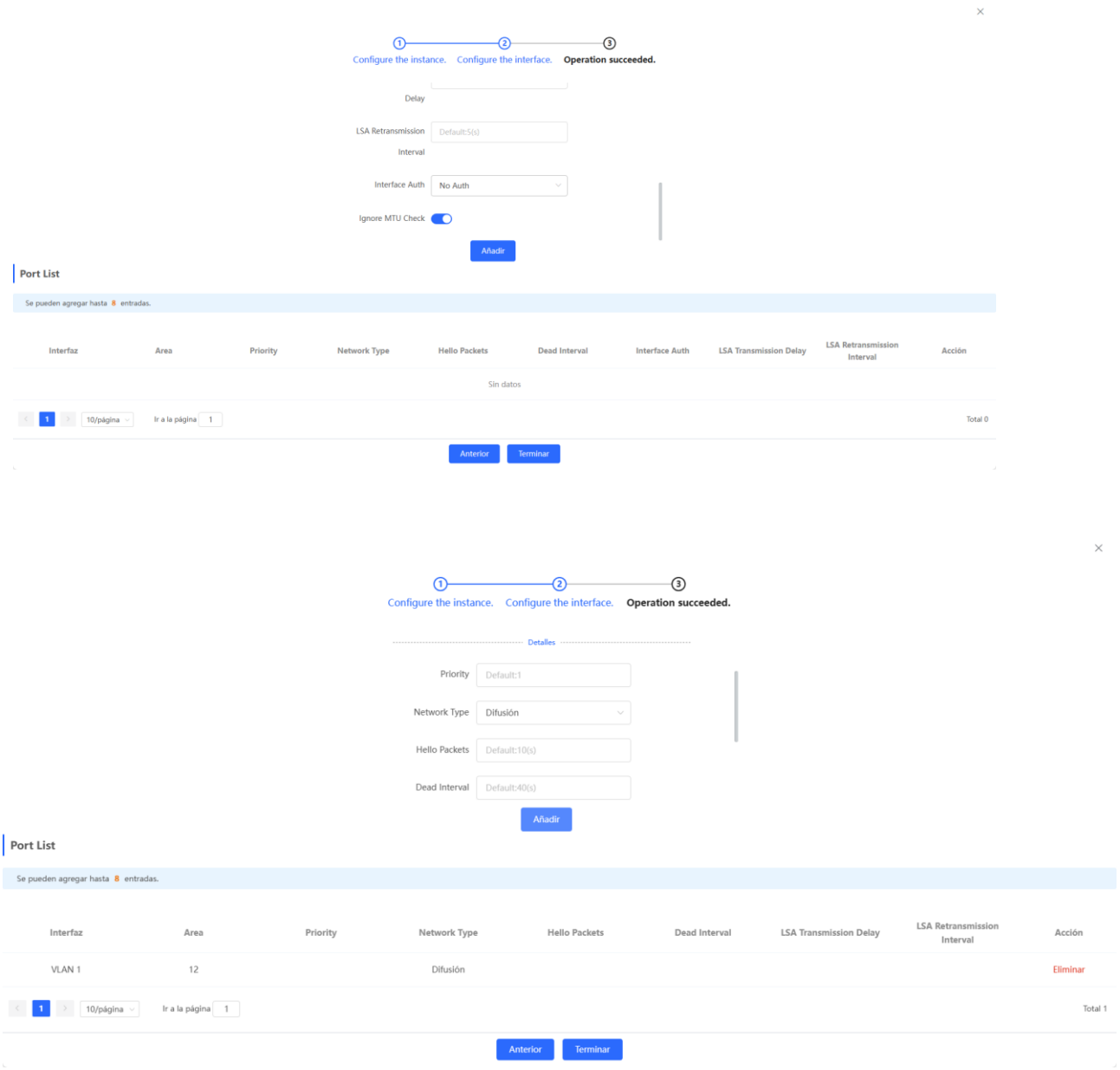
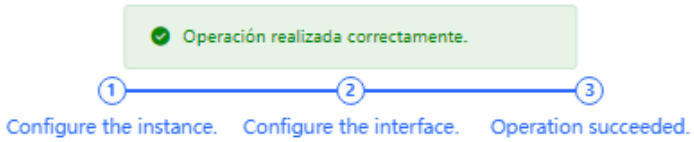


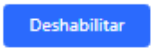
Tabla 16-17 Parámetros de la configuración detallada de una interfaz

Parámetro	Descripción
Priority	El valor es 1 de forma predeterminada.

Parámetro	Descripción
Network Type	Difusión Unidifusión Multidifusión Acceso múltiple sin difusión
Hello Packets	Intervalo para la transmisión periódica, que se utiliza para detectar y mantener la relación de dispositivos cercanos del OSPF. El valor predeterminado es 10 segundos.
Dead Interval	Tiempo tras el cual el dispositivo cercano deja de ser válido. El valor predeterminado es 40 segundos.
LSA Transmission Delay	Retardo de la transmisión del LSA de la interfaz. El valor predeterminado es 1 segundo.
LSA Retransmission Interval	Tiempo tras el cual se retransmite el LSA después de que este se pierda. El valor predeterminado es 5 segundos.
Interface Auth	**No Auth**: los paquetes del protocolo no se autentican. Es el valor predeterminado. **Plain Text**: los paquetes del protocolo se autentican y la clave de autenticación se envía junto con los paquetes del protocolo en forma de texto plano. **MD5**: los paquetes del protocolo se autentican y la clave de autenticación se encripta mediante el algoritmo MD5. A continuación, esta se envía junto con los paquetes del protocolo.
Ignore MTU Check	Se encuentra habilitado de forma predeterminada.

3. Realice la configuración.

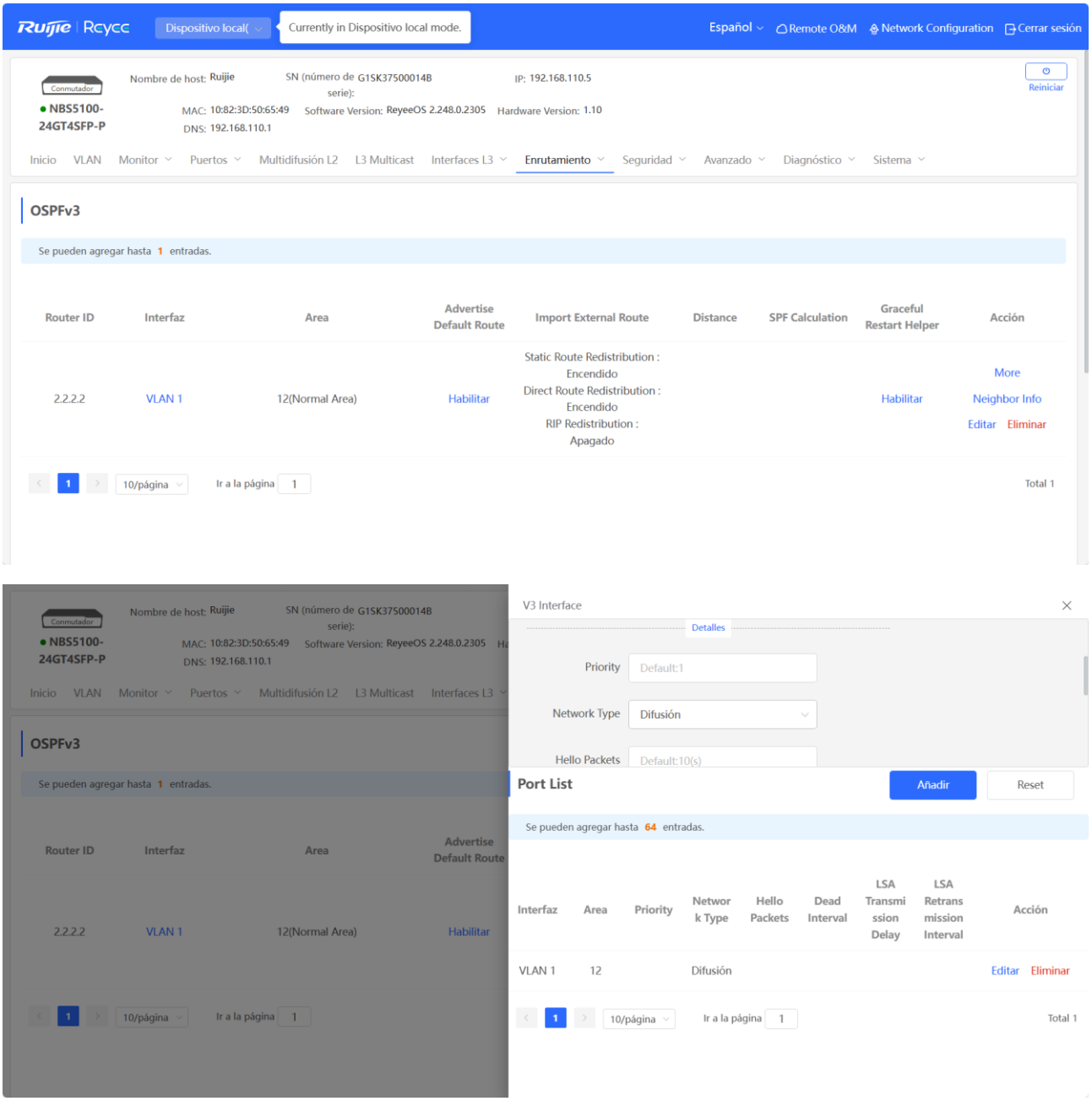


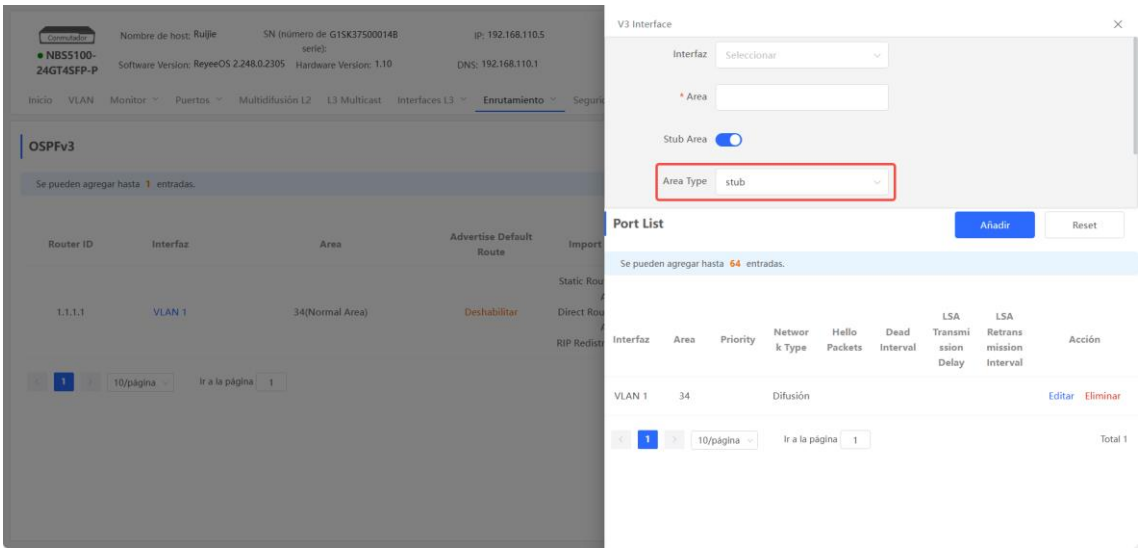


Tras realizar la configuración, puede seleccionar **Dispositivo local** > **Enrutamiento** > **OSPFv3** y ver la lista de instancias.

16.6.2 Adición de una interfaz OSPFv3

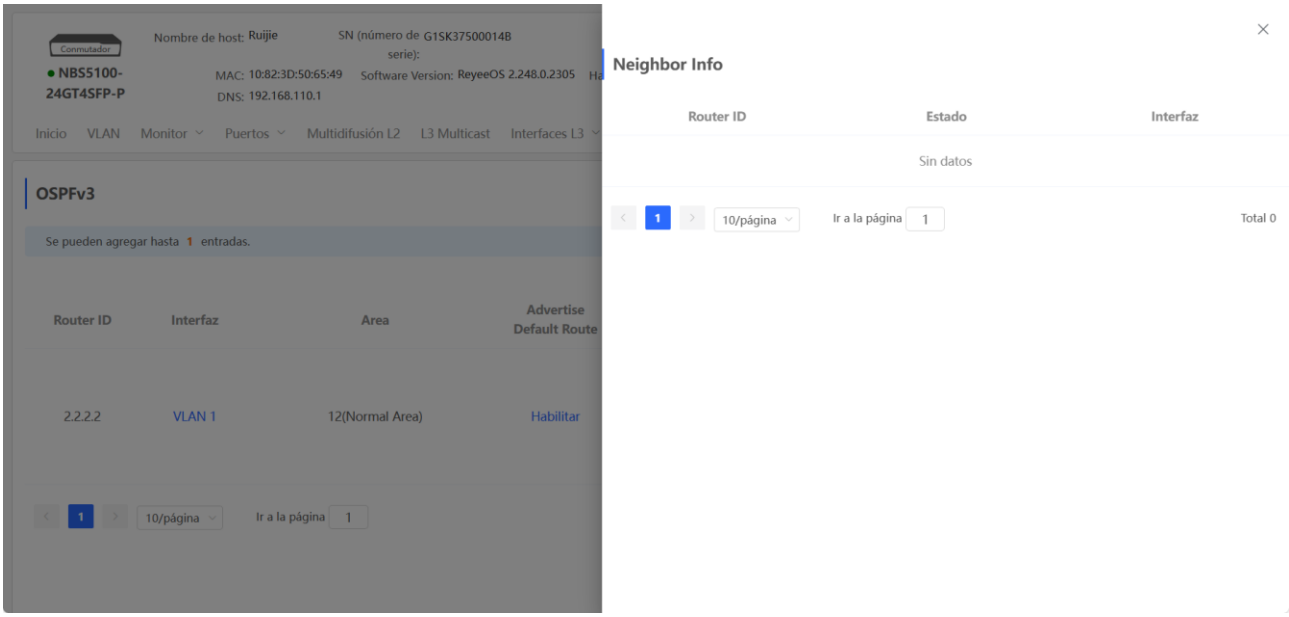
Seleccione **Dispositivo local** > **Enrutamiento** > **OSPFv3**, haga clic en **More** en la columna **Acción** y seleccione **V3 Interface**.



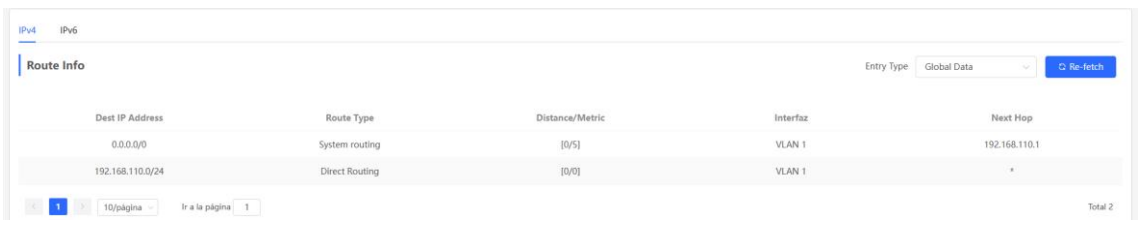


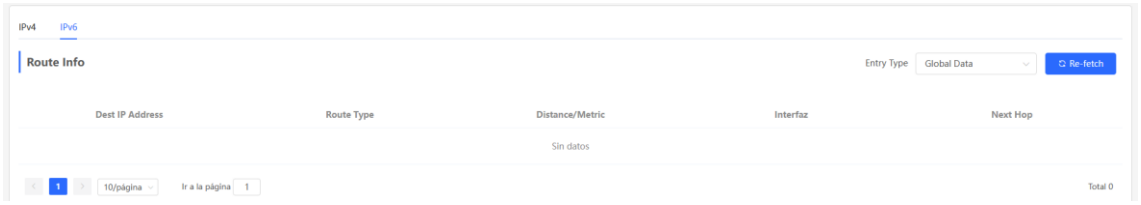
16.6.3 Visualización de la información de los dispositivos cercanos del OSPFv3

Seleccione **Dispositivo local** > **Enrutamiento** > **OSPFv3** y haga clic en **Neighbor Info** en la columna **Acción**.



16.7 Información de la tabla de enrutamiento




IPv4
IPv6
Route Info
Entry Type
Global Data
Re-fetch
Dest IP Address
Route Type
Distance/Metric
Interfaz
Next Hop
Sin datos
1
10/página
Ir a la página
1
Total 0

17 Seguridad de los switches de las series NBS y NIS

17.1 Inspección DHCP

17.1.1 Descripción general

La función de inspección del Protocolo de Configuración Dinámica de Host (DHCP), o DHCP Snooping, permite que el conmutador evite que los clientes obtengan las direcciones IP de un servidor DHCP no autorizado. Al habilitar esta función, el conmutador almacena parámetros, tales como las direcciones IP y MAC en los paquetes DHCP que se intercambian entre clientes y servidores, para prevenir cualquier ataque del DHCP. Las entradas de los datos de usuarios generadas en el conmutador, habilitadas con inspección DHCP, se pueden usar para las aplicaciones de seguridad, como la protección de origen IP.

17.1.2 Configuración de un dispositivo independiente

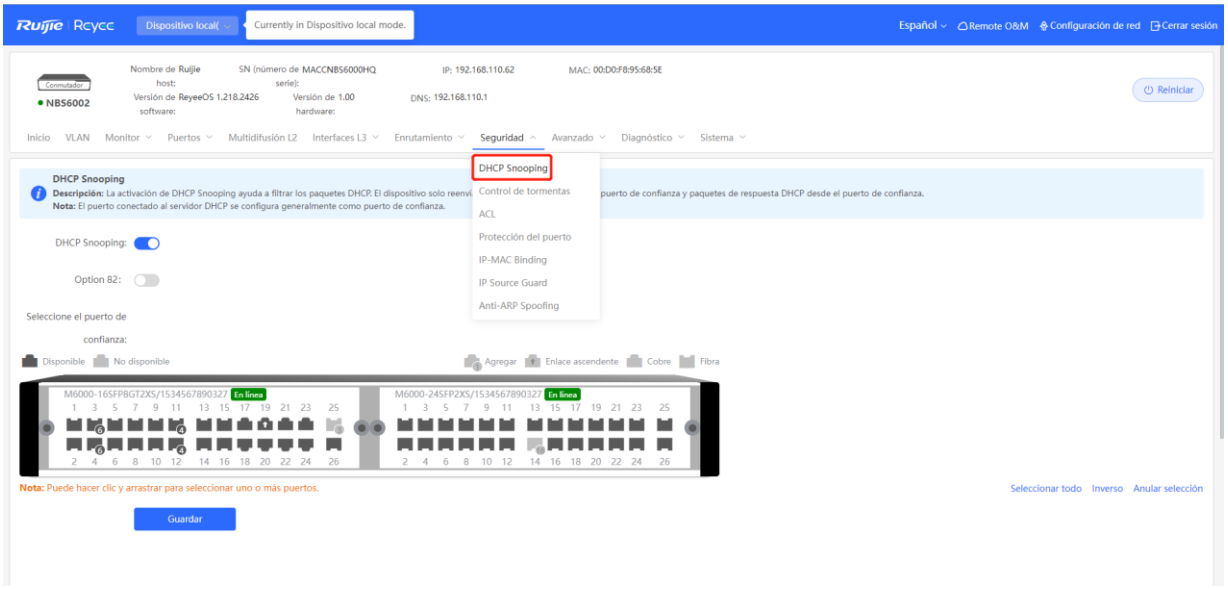
Seleccione **Dispositivo local** > **Seguridad** > **DHCP Snooping**.

Habilite la función de inspección DHCP, seleccione el puerto a configurar como el puerto de confianza en el panel del puerto y haga clic en **Guardar**. Después de habilitar la inspección DHCP, los paquetes de petición de los clientes del DHCP son reenviados únicamente a puertos de confianza; para los paquetes de respuesta de los servidores DHCP, solo aquellos provenientes de los puertos de confianza son reenviados.

Nota

Generalmente, el puerto de enlace ascendente conectado al servidor DHCP se configura como el puerto de confianza.

El elemento Opción 82 se utiliza para mejorar la seguridad del servidor DHCP y optimizar la póliza de asignación de direcciones IP. El paquete de petición del DHCP llevará a Opción 82 cuando esta sea habilitada.

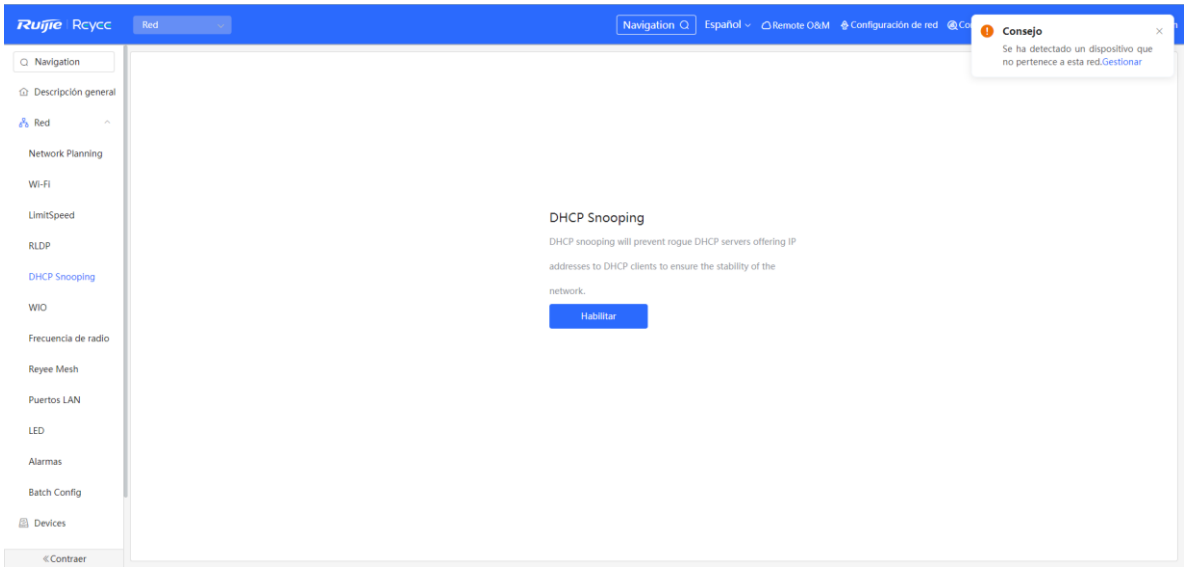


17.1.3 Configuración grupal de conmutadores de la red

Seleccione **Red** > **DHCP Snooping**.

Habilitar la función de inspección DHCP en conmutadores de la red, garantiza que los usuarios obtengan los parámetros de configuración de la red de ese servidor DHCP en específico. Esto evita que las terminales en línea de una red obtengan direcciones IP asignadas por routers privados y garantizan la estabilidad de esta.

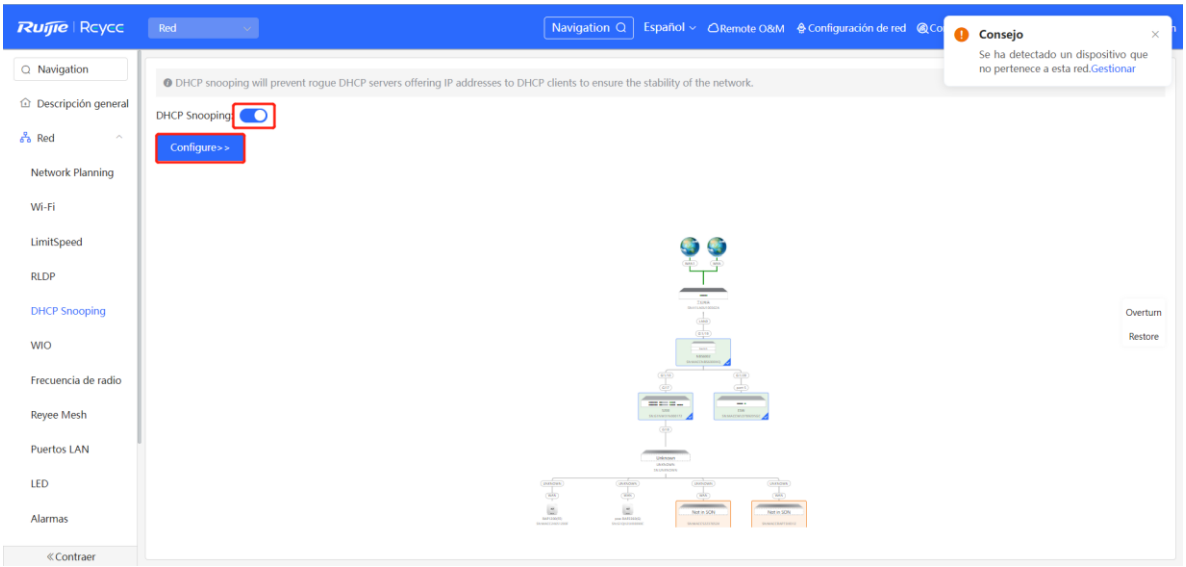
(1) Haga clic en **Habilitar** para acceder a la página de **DHCP Snooping Config.**



(2) En la topología de la red se puede seleccionar el acceso a los conmutadores donde se desea habilitar la inspección DHCP, ya sea en modo recomendado o personalizado. Si se selecciona el modo recomendado, todos los conmutadores de la red se seleccionan automáticamente. Si se selecciona el modo personalizado, se pueden

seleccionar manualmente los conmutadores deseados. Haga clic en **Deliver Config**. La inspección DHCP está habilitada en los conmutadores seleccionados.

(3) En la topología, seleccione el conmutador de acceso en el cual se debe habilitar la inspección DHCP. Si se selecciona **Recommended**, todos los conmutadores de la red se seleccionan automáticamente. Si se selecciona **Custom**, se pueden seleccionar manualmente los conmutadores deseados. Haga clic en **Deliver Config** para habilitar la inspección DHCP en los conmutadores seleccionados.



17.2 Control de tormentas

17.2.1 Descripción general

Cuando una red de área local (LAN) tiene difusión, multidifusión o unidifusión desconocida de flujos de datos en exceso, la velocidad de la red disminuye y se pueden generar tiempos de espera para la transmisión de los paquetes. A esta situación se le conoce como tormenta LAN, que puede ser ocasionada por errores en la ejecución de los protocolos de topología o la inadecuada configuración de una red.

El control de tormentas puede configurarse separadamente para los flujos de difusión, multidifusión y unidifusión desconocida de datos. Cuando la velocidad de los flujos de difusión, multidifusión desconocida o unidifusión desconocida de datos que recibe un dispositivo excede el rango especificado, este transmite solamente los paquetes de un rango específico y descarta los que están fuera de este rango hasta que la velocidad vuelva a estar dentro del rango. Esto previene que un desbordamiento de datos ingrese a la LAN y ocasione una tormenta.

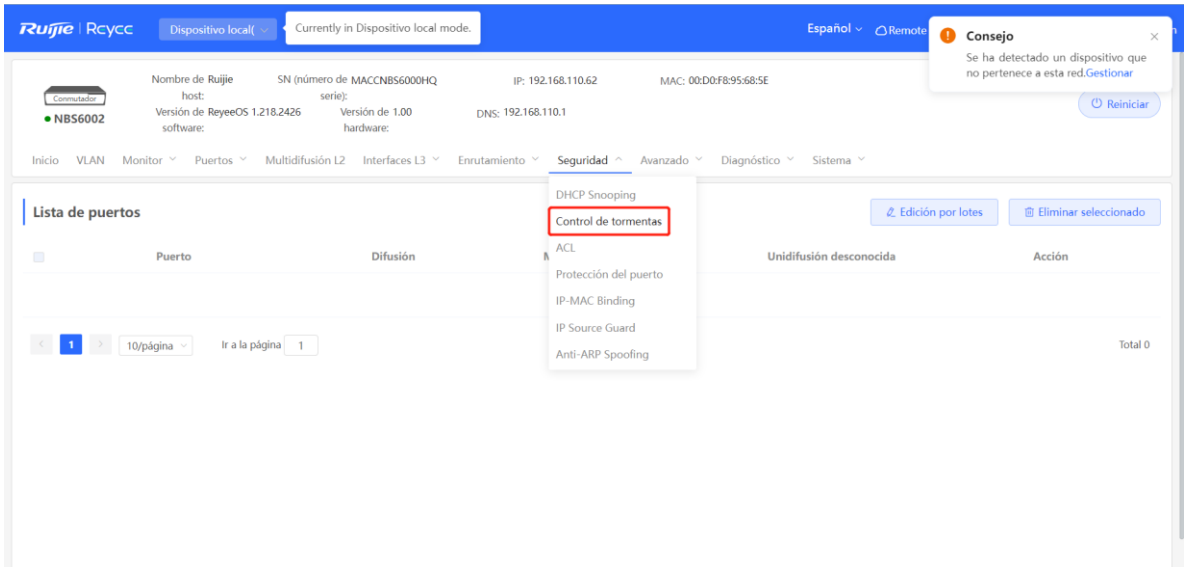
17.2.2 Procedimiento

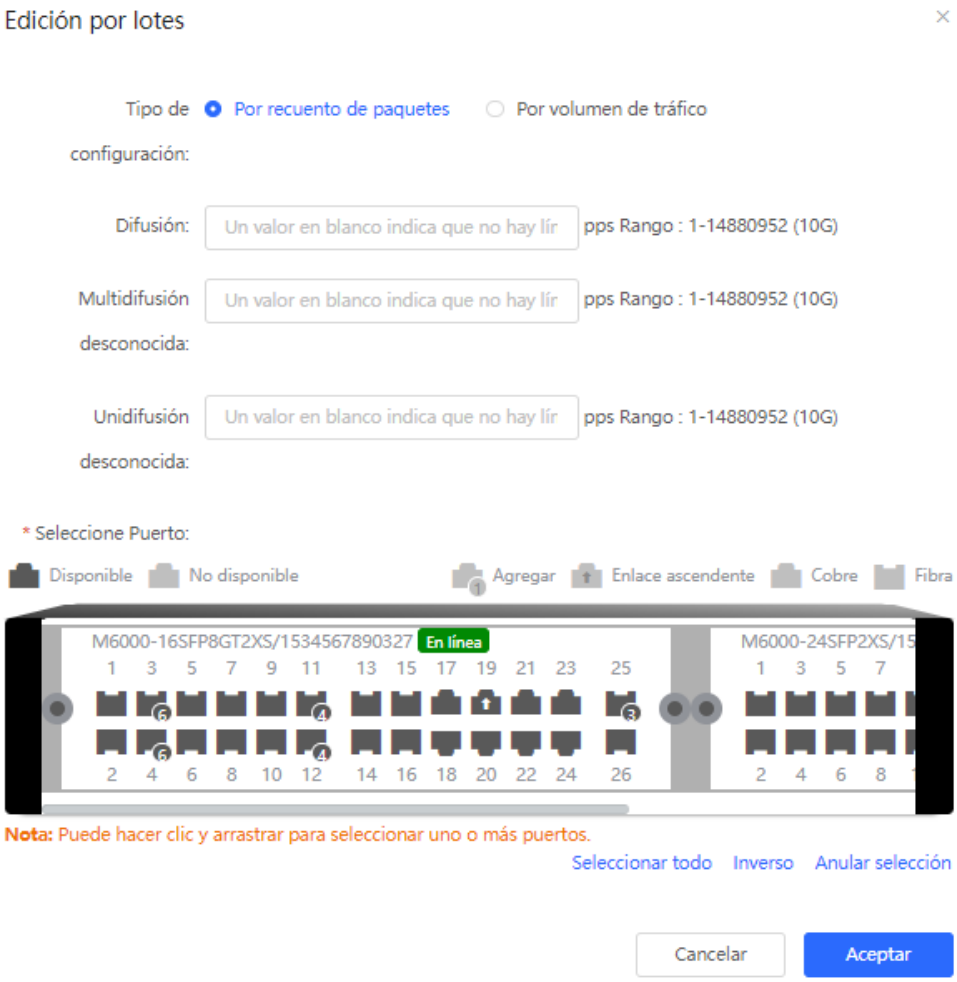
Seleccione **Dispositivo local** > **Seguridad** > **Control de tormentas**.

Haga clic en **Edición por lotes**. En el cuadro de diálogo que aparece, seleccione los tipos y puertos de configuración, establezca los límites de velocidad de los paquetes de difusión, de multidifusión desconocida y de unidifusión desconocida, y haga clic en **Aceptar**. Para modificar o borrar las reglas de límite de velocidad después de completar la configuración, haga clic en **Editar** o **Eliminar** en la columna **Acción**.

Hay dos modos de configuración:

- El control de tormentas con base en paquetes por segundo: si la velocidad de los flujos de datos recibidos a través del puerto del dispositivo excede el límite configurado, los flujos de datos en exceso se descartan hasta que la velocidad vuelva a estar dentro del rango establecido.
- El control de tormentas con base en kilobytes por segundo: si la velocidad de los flujos de datos recibidos a través del puerto del dispositivo excede el límite configurado, los flujos de datos en exceso se descartan hasta que la velocidad vuelva a estar dentro del rango establecido.





17.3 ACL

17.3.1 Descripción general

Una lista de control de acceso (ACL) se considera comúnmente un filtro de paquetes. La ACL define una serie de reglas para permitir o denegar accesos y las aplica a las interfaces del dispositivo para controlar los paquetes enviados y recibidos por estas, con el fin de aumentar la seguridad del dispositivo de la red.

Las ACL se pueden añadir con base en direcciones MAC o IP y vincularlas a las interfaces.

17.3.2 Creación de reglas para una ACL

Seleccione **Dispositivo local** > **Seguridad** > **ACL** > **Lista ACL (lista de control de acceso)**.

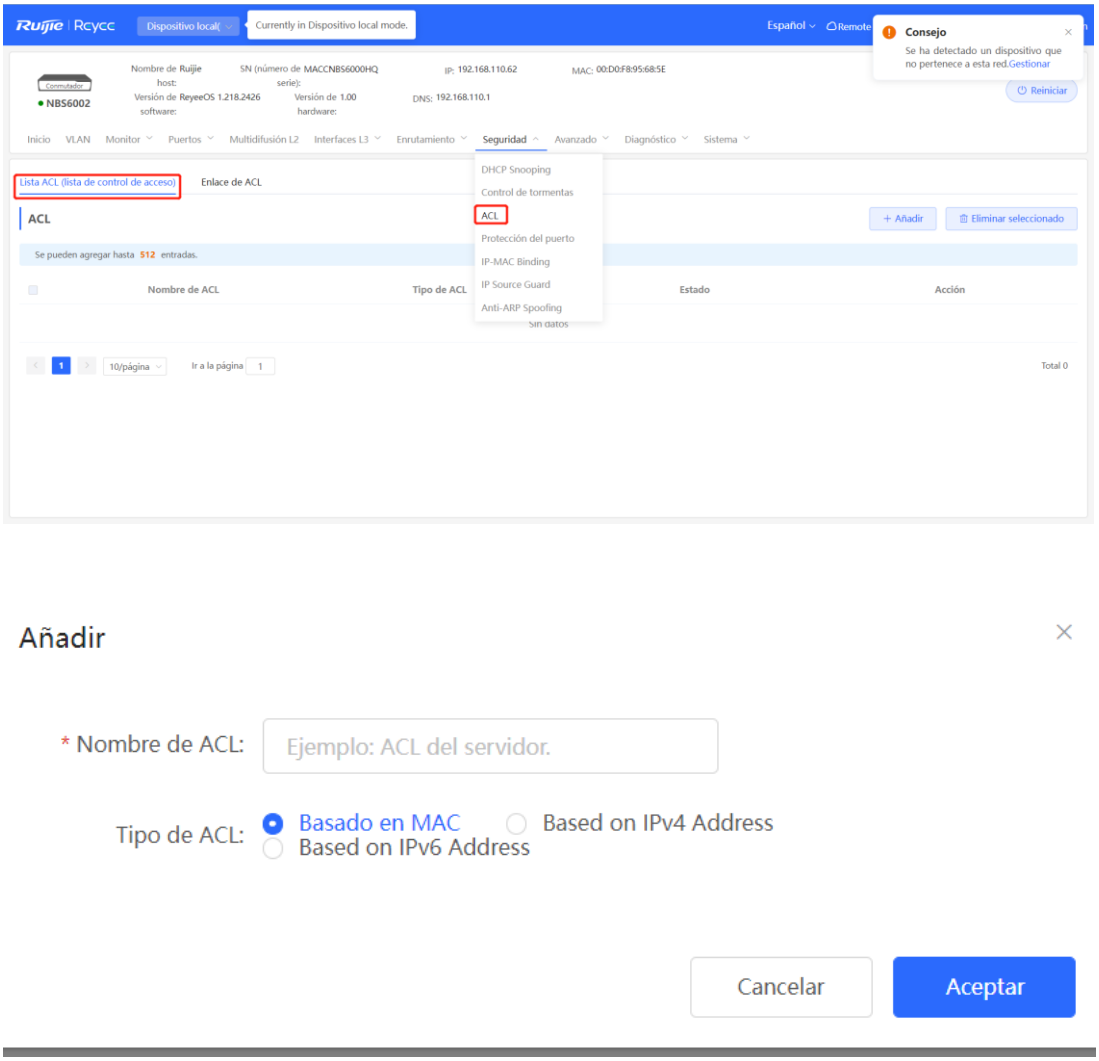
(1) Haga clic en **Añadir** para establecer el tipo y el nombre de ACL y haga clic en **Aceptar**.

Con base en las direcciones MAC: para controlar el ingreso y salida de paquetes de Capa 2 en el puerto, niegue o permita el acceso a estos paquetes específicos destinados a una red.

Con base en las direcciones IP: para controlar el ingreso y salida de paquetes en un puerto, niegue o permita el acceso de paquetes específicos destinados a una red.

- Control de acceso basado en la dirección MAC: regula el flujo de paquetes de capa 2 que entran y salen de los puertos, permitiendo o denegando determinados paquetes en función de sus direcciones de capa 2.

- Control de acceso basado en IPv4: regula el flujo de paquetes IPv4 que entran y salen de los puertos, permitiendo o denegando determinados paquetes en función de sus direcciones IPv4.
- Control de acceso basado en IPv6: regula el flujo de paquetes IPv4 que entran y salen de los puertos, permitiendo o denegando determinados paquetes en función de sus direcciones IPv4.



(2) Haga clic en **Detalles**, en la columna **Acción** de la ACL, configure las reglas de filtrado en la columna que aparece y haga clic en **Guardar**. Se pueden añadir varias reglas.

Las reglas incluyen dos acciones: **Permitir** y **Bloquear**. La secuencia de una regla en una ACL determina la prioridad de la coincidencia con la regla en la ACL. Al procesar paquetes, el dispositivo de la red encuentra la coincidencia de los paquetes con las entradas de control de acceso o ACE, con base en los números de secuencia de la regla. Haga clic en **Mover** en la lista de reglas para ajustar el orden de coincidencia.

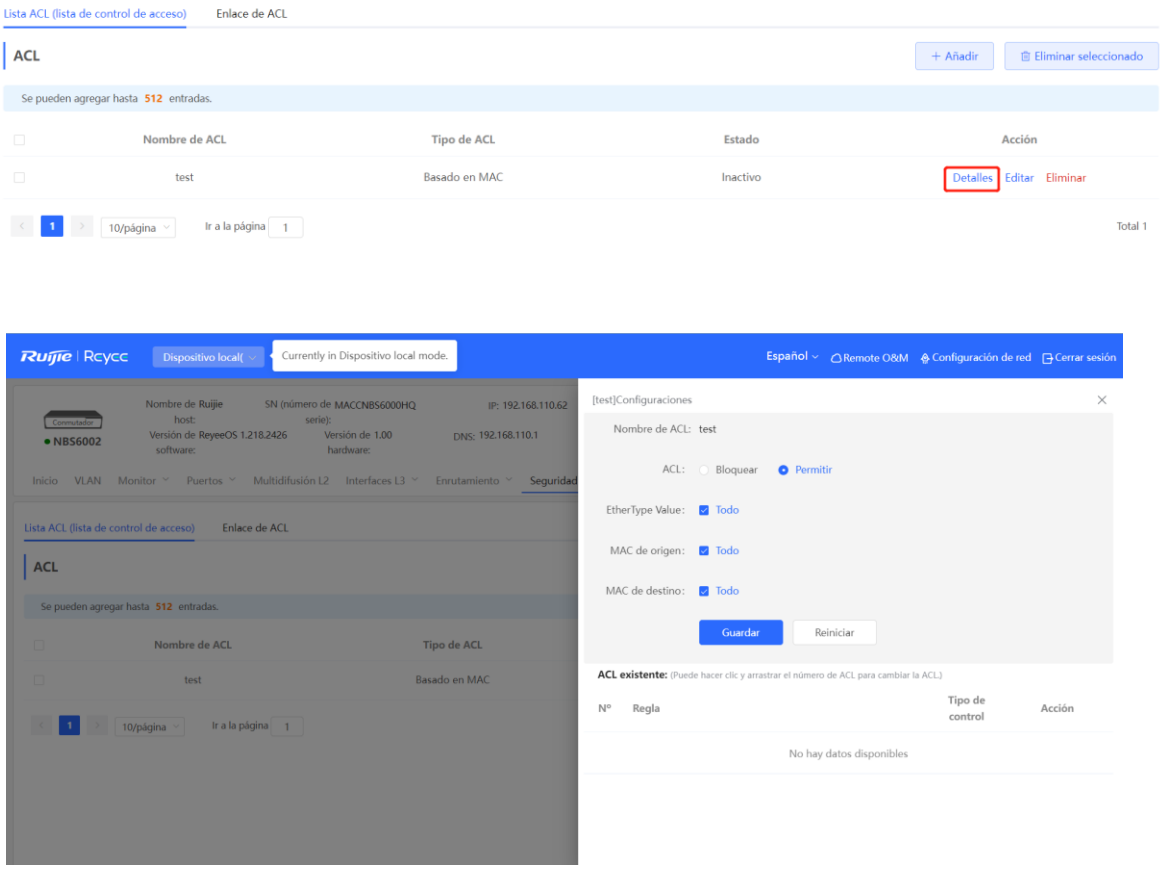


Tabla 17-1 Descripción de los parámetros para la configuración de la regla ACL

Parámetro	Descripción
ACL	Acción en una ACL: Bloquear: si los paquetes coinciden con esta regla, se les niega el acceso. Permitir: si los paquetes coinciden con esta regla, se les permite el acceso.
Número de protocolo IP	Coincidencia con el número de protocolo IP. Los rangos de valor van de 0 a 255. **Todo** indica que los paquetes de todos los protocolos IP coinciden.Aplicable al control de acceso basado en IPv4 y al control de acceso basado en IPv6.
Dirección IP de origen	Coincidencia con la dirección IP de origen de los paquetes. Seleccione **Todo** para que todas las direcciones IP de origen coincidan.Aplicable al control de acceso basado en IPv4 y al control de acceso basado en IPv6.
Dirección IP de destino	Coincidencia con la dirección IP de destino de los paquetes. Seleccione **Todo** para que todas las direcciones IP de destino coincidan.Aplicable al control de acceso basado en IPv4 y al control de acceso basado en IPv6.

Parámetro	Descripción
Valor EtherType	Coincidencia con el tipo de protocolo Ethernet. Los rangos de valor van de 0x600 a 0xFFFF. Seleccione **Todo** para que todos los números de los tipos de protocolo coincidan. Aplicable al control de acceso basado en la dirección MAC.
MAC de origen	Coincidencia con la dirección MAC del host de origen. Seleccione **Todo** para que todas las direcciones MAC de origen coincidan. Aplicable al control de acceso basado en la dirección MAC.
MAC de destino	Coincidencia con la dirección MAC del host de destino. Seleccione **Todo** para que todas las direcciones MAC de destino coincidan. Aplicable al control de acceso basado en la dirección MAC.

Nota

- Los nombres de las ACL son únicos. Solo puede modificar el nombre de una ACL creada.
- La ACL aplicada a un puerto no puede editarse o eliminarse. Para editar una ACL, primero debe desvincularla del puerto.
- La regla de ACL predeterminada que niega todos los paquetes está localizada al final de una ACL.

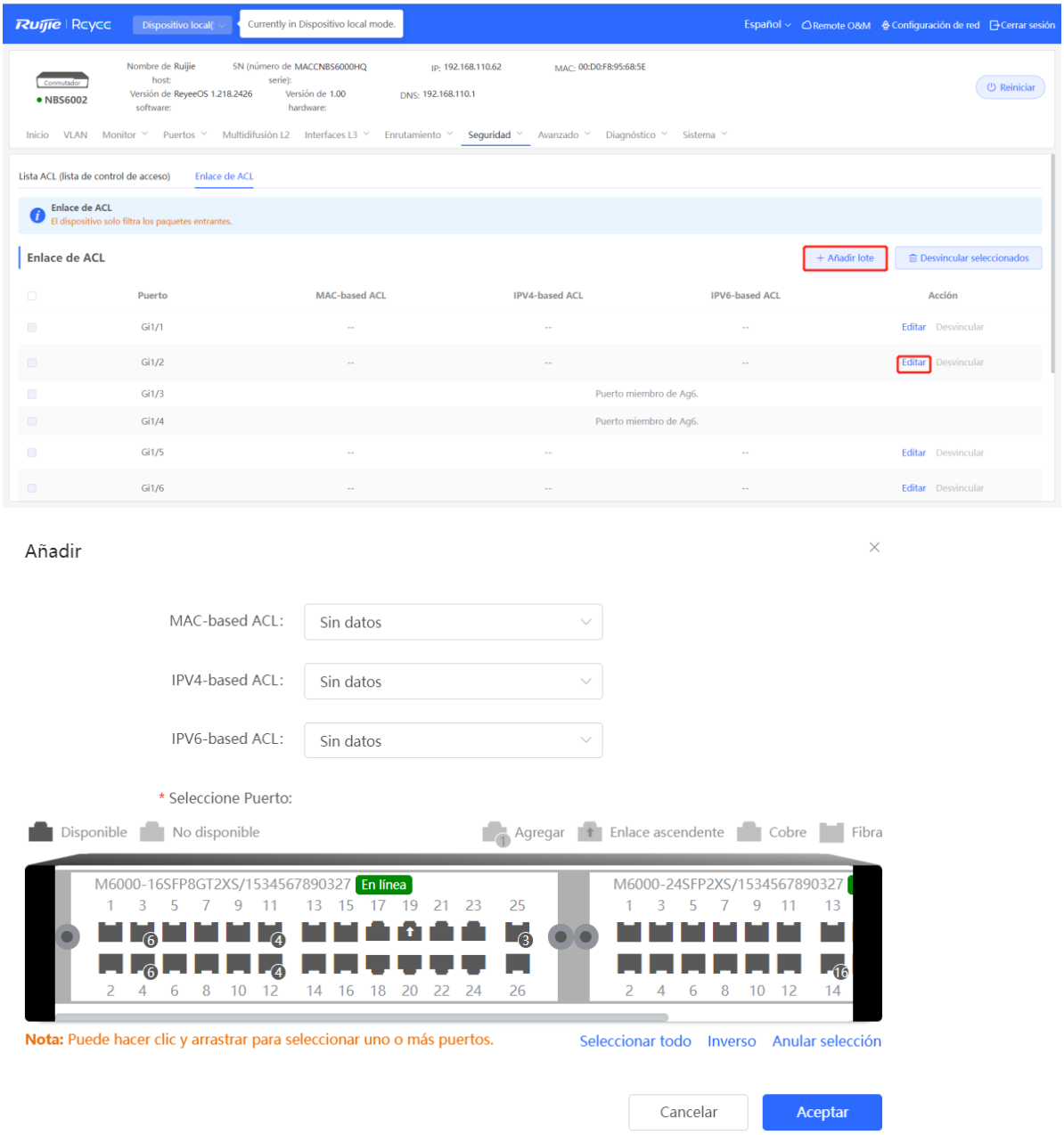
17.3.3 Aplicación de las reglas de una ACL

Seleccione **Dispositivo local** > **Seguridad** > **ACL** > **Lista ACL**.

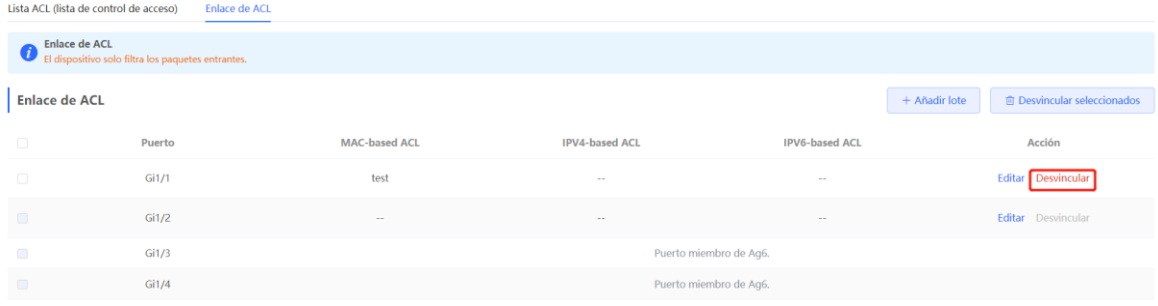
Haga clic en **Añadir por lotes** o **Editar por lotes** en la columna **Acción**, seleccione la ACL que desee para los puertos y haga clic en **Aceptar**.

Nota

Las ACL pueden aplicarse a los puertos solamente en la dirección entrante; es decir, filtra los paquetes entrantes.



Después de aplicar una ACL a un puerto, se puede hacer clic en **Desvincular**, en la columna **Acción**, o localizar el puerto y hacer clic en **Desvincular seleccionados** eliminar la vinculación de ACL con el puerto.

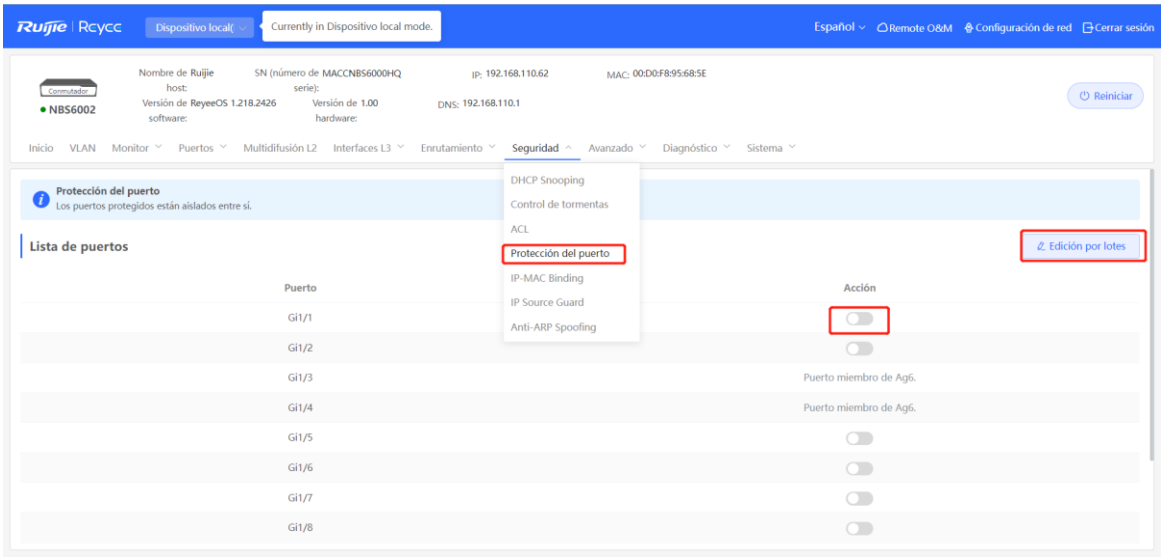


17.4 Protección del puerto

Seleccione **Dispositivo local** > **Seguridad** > **Protección del puerto**.

En algunas situaciones, se debe deshabilitar la comunicación entre algunos puertos del dispositivo. Es posible configurar algunos puertos como puertos protegidos. Los puertos en los que se habilita la función de protección de puerto (puertos protegidos) no se pueden comunicar entre ellos, los usuarios de diferentes puertos están aislados en la Capa 2. Los puertos protegidos pueden comunicarse con puertos no protegidos.

La protección de puertos se encuentra deshabilitada por defecto; esta se puede habilitar para varios puertos haciendo clic en la protección por lotes. Haga clic en **Edición por lotes** para habilitar la protección, seleccione los puertos que desea incluir y haga clic en **Aceptar**.



17.5 Enlace IP-MAC

17.5.1 Descripción general

Después de configurar el enlace IP-MAC en un puerto para mejorar la seguridad, el dispositivo revisa que las direcciones IP de origen y las MAC de origen de los paquetes IP sean las configuradas para el dispositivo, filtra los paquetes IP que no coincidan con el enlace y controla estrictamente la validez de las fuentes de entrada.

17.5.2 Procedimiento

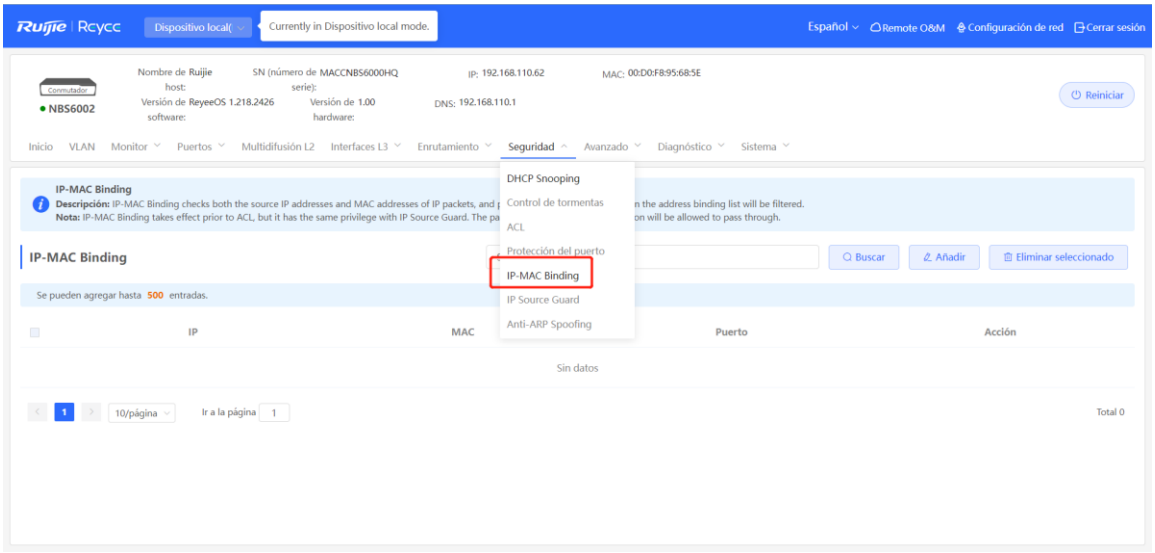
Seleccione **Dispositivo local** > **Seguridad** > **IP-MAC Binding**.

1. Añadir una entrada de enlace IP-MAC

Haga clic en **Añadir**, seleccione el puerto deseado, ingrese la dirección IP y la dirección MAC por vincular y haga clic en **Aceptar**. Debe ingresar al menos una dirección IP y una dirección MAC. Para modificar el enlace, haga clic en **Editar** en la columna **Acción**.

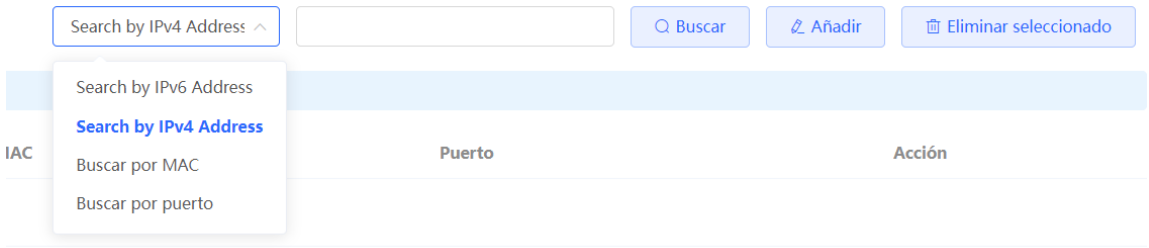
Precaución

El enlace IP-MAC tiene prioridad sobre la ACL y es equivalente a la protección de origen IP. El paquete que coincida con cualquier entrada de enlace tendrá permitido pasar.



2. Búsqueda de entradas de enlace

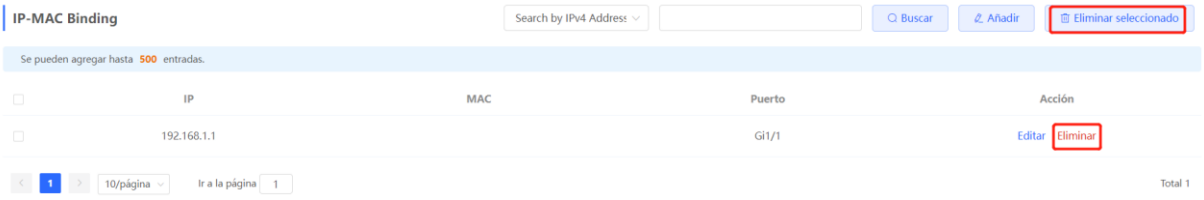
Se pueden hacer consultas de entradas de los enlaces con base en las direcciones IP, las direcciones MAC o los puertos en la barra de búsqueda localizada en la esquina superior derecha. Seleccione el tipo de búsqueda, ingrese la cadena de caracteres y haga clic en **Buscar**. Las entradas que coinciden con el criterio de búsqueda se muestran en la lista.



3. Eliminación de una entrada de enlace IP-MAC

Eliminación por lotes: en **IP-MAC Binding,** seleccione una entrada a eliminar y haga clic en **Eliminar seleccionado**. En el cuadro de diálogo que aparece, haga clic en **Aceptar**.

Eliminación individual: haga clic en el botón **Eliminar** en la última columna **Acción** de la lista. En el cuadro de diálogo que aparece, haga clic en **Aceptar**.



17.6 Protección de origen IP

17.6.1 Descripción general

Cuando la función de protección de origen IP quede habilitada, el dispositivo revisa los paquetes IP de los puertos que no son de confianza. Se puede configurar el dispositivo para revisar solamente los campos IP o IP+MAC con el fin de filtrar los paquetes IP que no coincidan con la lista de enlaces. Esto evita que los usuarios configuren direcciones IP privadas y que se falsifiquen paquetes IP.

Precaución

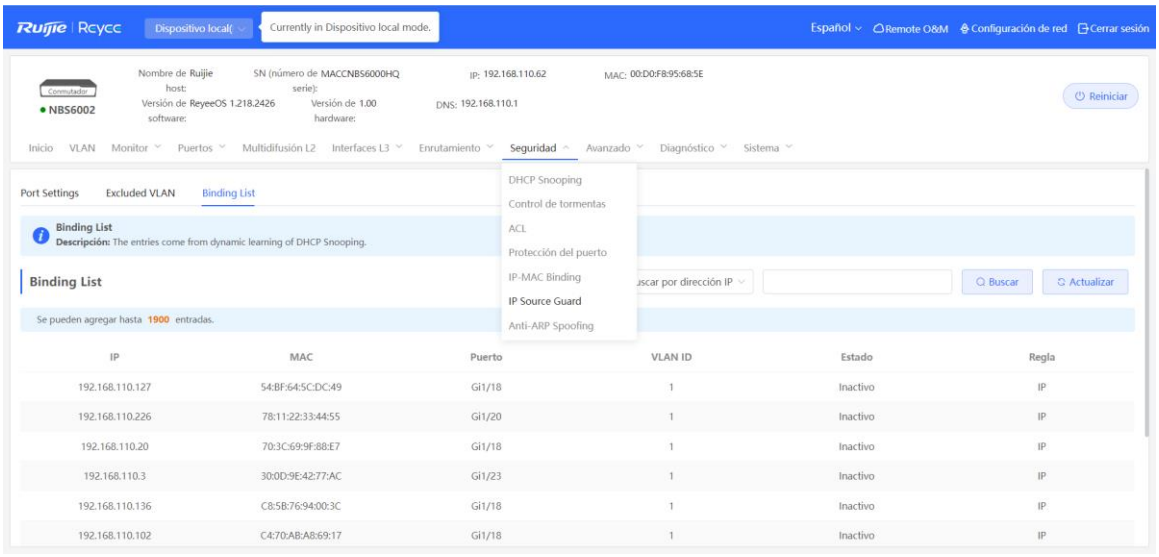
La protección de origen IP debe habilitarse con inspección DHCP. De otro modo, el reenvío de paquetes IP puede resultar afectado. Para configurar la inspección DHCP, consulte 17.1 Inspección DHCP

17.6.2 Revisión de la lista de enlaces

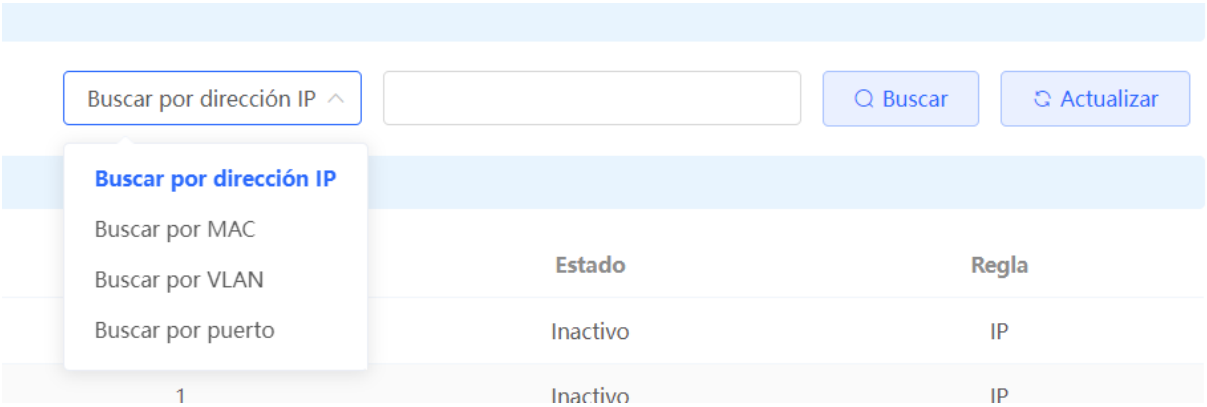
Seleccione **Dispositivo local** > **Seguridad** > **IP Source Guard** > **Binding List**.

La lista de enlaces es la base de la protección de origen IP. La información en **Binding List** proviene de los resultados de aprendizaje dinámico de la base de datos de los enlaces de inspección DHCP. Cuando se habilita la protección de origen IP, los datos de la base de datos de enlaces de inspección DHCP se sincronizan con la lista de enlaces de la protección de origen IP. En este caso, los paquetes IP se filtran estrictamente a través de la protección de origen IP en los dispositivos con inspección DHCP habilitada.

Haga clic en **Actualizar** para obtener los datos más recientes en **Binding List.**



Se pueden hacer consultas de entradas de enlaces con base en las direcciones IP, las direcciones MAC, las VLAN o los puertos en la barra de búsqueda localizada en la esquina superior derecha. Haga clic en la lista desplegable para seleccionar el tipo de búsqueda, ingrese la cadena de caracteres para la búsqueda y haga clic en **Buscar**.



17.6.3 Habilitar la protección de origen IP en un puerto

Seleccione **Dispositivo local** > **Seguridad** > **IP Source Guard** > **Basic settings**.

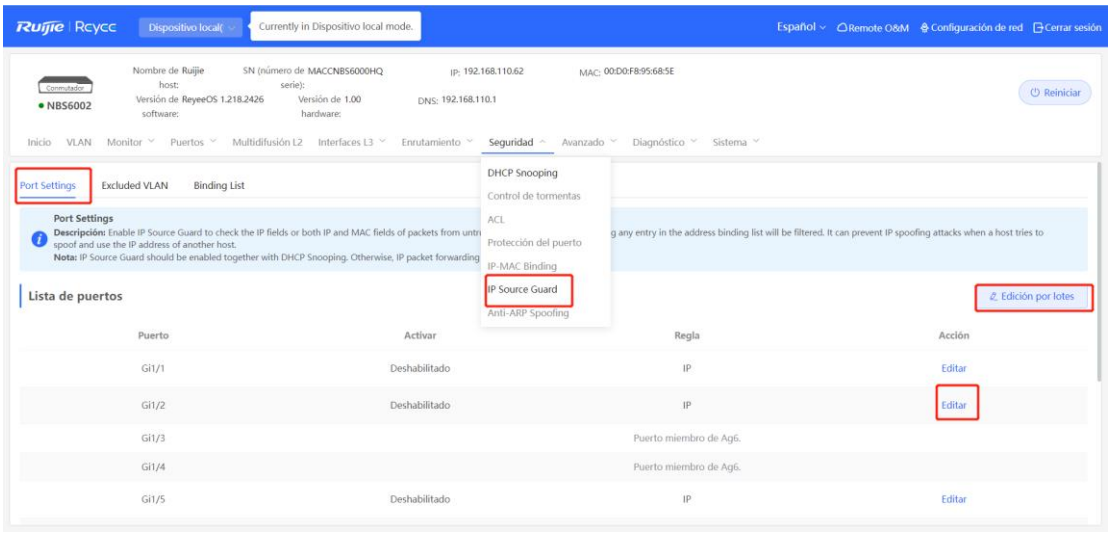
En **Lista de puertos**, haga clic en el botón **Editar**, en la última columna **Acción**. Seleccione **Habilitado** y la regla de coincidencia, y haga clic en **Aceptar**.

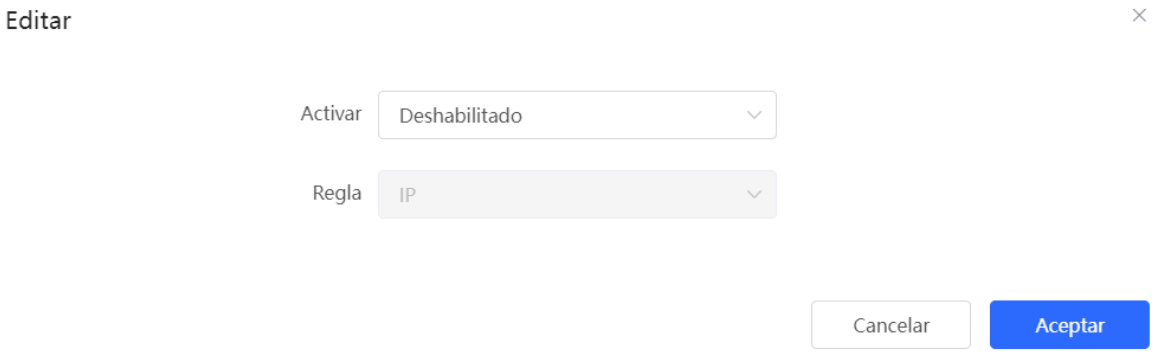
Hay dos reglas de coincidencia:

- Dirección IP: las direcciones IP de origen de todos los paquetes IP que pasan a través del puerto, se revisan. Los paquetes pueden pasar a través del puerto solamente cuando las direcciones IP de origen de estos coincidan con aquellas en la lista de enlaces.
- Dirección IP y dirección MAC: las direcciones IP de origen y las direcciones MAC de los paquetes IP que pasan a través del puerto, se revisan. Los paquetes pueden pasar a través del puerto solamente cuando, tanto las direcciones IP como las direcciones MAC de origen L2 y las direcciones IP de origen L3 de estos coincidan con una entrada en la lista de enlaces.

Precaución

- La protección de origen IP no puede habilitarse en un puerto de confianza donde esté habilitada la función de inspección DHCP.
- La protección de origen IP puede habilitarse solamente en una interfaz de Capa 2.





17.6.4 Configuración de la exclusión de direcciones VLAN

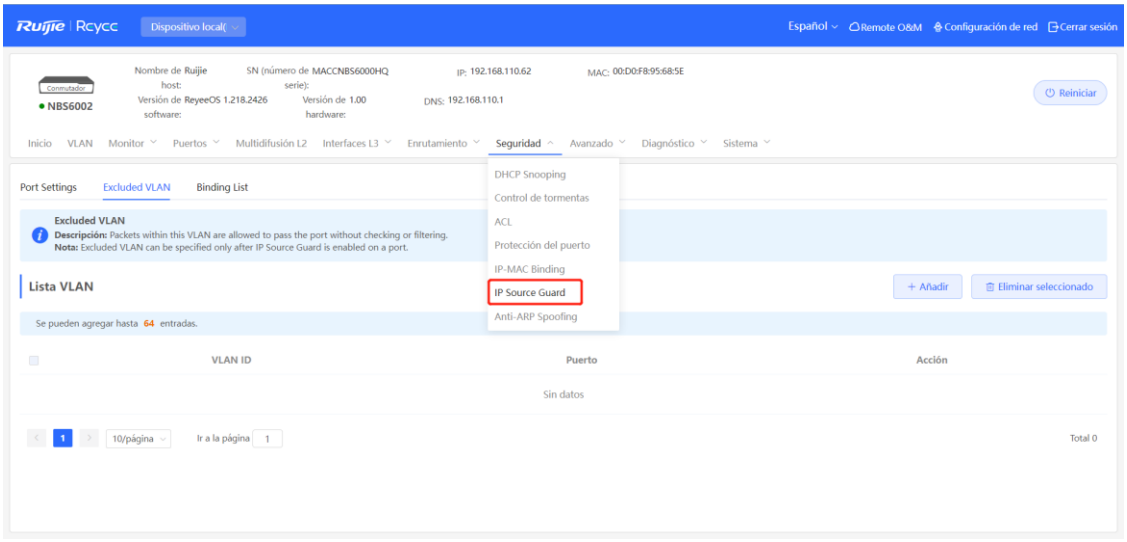
Seleccione **Dispositivo local** > **Seguridad** > **IP Source Guard** > **Excluded VLAN**.

Cuando la protección de origen IP se habilita en una interfaz, por defecto se hace efectiva para todas las VLAN en ella. Se pueden especificar VLAN excluidas, en las que los paquetes IP no se revisan ni filtran; es decir, dichos paquetes IP no están bajo el control de la protección de origen IP.

Haga clic en **Editar**, ingrese la VLAN ID a excluir y el puerto deseado, y haga clic en **Aceptar**.

Precaución

Las VLAN excluidas de un puerto se pueden especificar solo después de habilitar la función de protección de origen IP en este. Las VLAN excluidas se eliminarán automáticamente cuando la protección de origen IP se deshabilite en el puerto.



17.7 Configuración de la autenticación 802.1x

17.7.1 Introducción sobre el funcionamiento

El IEEE802.1x (control de acceso a la red basado en los puertos) es un estándar de control de acceso a la red basado en los puertos que proporciona servicios de acceso seguro para las redes LAN.

El IEEE 802 LAN, siempre que los usuarios puedan conectarse a los dispositivos de red, les permite acceder directamente a los recursos de la red sin necesidad de autenticarse ni autorizarse. Por este motivo, este comportamiento sin control conlleva riesgos de seguridad para la red. El protocolo IEEE 802.1x se propuso para resolver el problema de seguridad de las redes LAN 802.

El 802.1x admite la autenticación, la autorización y la contabilidad, tres aplicaciones de seguridad a las que se conoce como AAA.

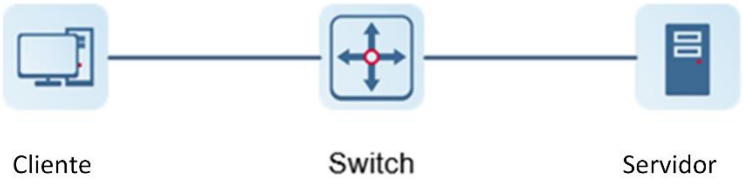
- Autenticación (Authentication): se utiliza para determinar si los usuarios pueden obtener derechos de acceso y restringir a los usuarios ilegales.
- Autorización (Authorization): determina qué servicios pueden utilizar los usuarios autorizados y controla los

derechos de los usuarios legítimos.

- Contabilidad (Accounting): registra el uso de los recursos de la red por parte de los usuarios y sirve de base para el cobro.

El 802.1x puede utilizarse en redes que controlan el acceso de los usuarios para implantar los servicios de autenticación y autorización para los usuarios con acceso.

Asimismo, el sistema 802.1x se basa en una estructura típica Cliente/Servidor, que incluye tres entidades: el cliente, el dispositivo de acceso y el servidor de autenticación. En la siguiente figura se muestra el diagrama de una arquitectura típica.



- El cliente suele ser un dispositivo terminal de usuario y el usuario puede iniciar la autenticación 802.1X iniciando el software cliente. El cliente debe ser compatible con el protocolo de autenticación extensible sobre redes LAN (EAPoL).
- Access point o dispositivo de switching compatible con el protocolo 802.1x. Proporciona un puerto para que el cliente acceda a la LAN. El puerto puede ser un puerto físico o un puerto lógico.
- El servidor de autenticación se utiliza para llevar a cabo la autenticación, la autorización y la contabilidad de los usuarios y suele ser un servidor RADIUS.

Nota

Los dispositivos de switching RG- NBS solo admiten la función de autenticación.

17.7.2 Configuración del 802.1x

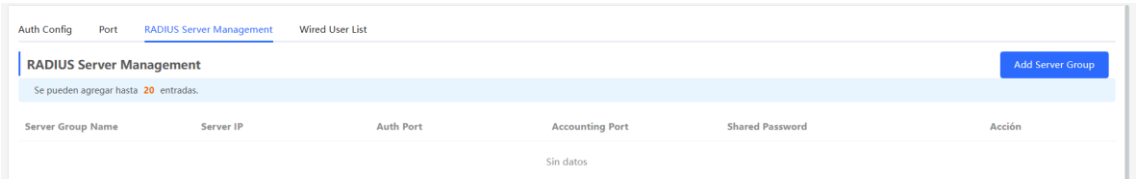
1. Configuración de un servidor RADIUS

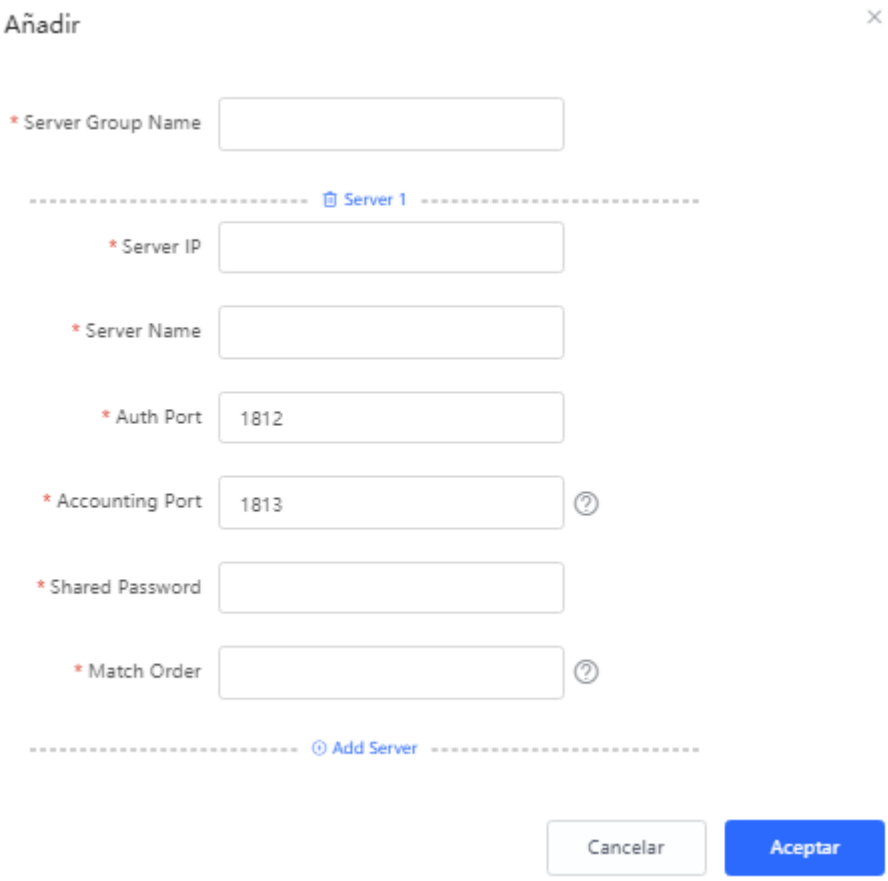
Seleccione **Dispositivo local** > **Seguridad** > **802.1x Authentication** > **RADIUS Server Management**.

Antes de realizar la configuración, confirme que:

- El servidor Radius se ha instalado y configurado íntegramente como se indica a continuación.
  - Se requiere el nombre de usuario y la contraseña para el inicio de sesión de los clientes.
  - El firewall se encuentra desactivado, ya que, de lo contrario, el mensaje de autenticación podría ser interceptado, lo que provocaría un fallo en la autenticación.
  - El servidor Radius cuenta con una IP de confianza.
- Existe conexión de red entre el dispositivo de autenticación y el servidor Radius.
- Se han obtenido las direcciones IP del servidor Radius y el dispositivo de autenticación.

(1) Haga clic en **Add Server Group** para añadir un grupo de servidores.





Parámetro	Descripción
Server Group Name	El nombre del grupo de servidores. Si lo desea, puede añadir varios servidores a un grupo de servidores. Si el servidor con mayor prioridad no responde, el sistema cambia a otros servidores en el orden correspondiente. **Nota** Para utilizar esta función es necesario que la función de detección de servidores se encuentre habilitada.
Server IP	La dirección del servidor Radius.
Auth Port	El número de puerto que se utiliza para acceder a la autenticación de usuarios en el servidor Radius.
Accounting Port	El número de puerto que se utiliza para acceder al proceso de contabilidad en el servidor Radius.

Parámetro	Descripción
Shared Password	La clave compartida del servidor Radius.
Match Order	El sistema permite añadir hasta 5 servidores Radius. Cuanto mayor sea el valor del orden de coincidencia, mayor será la prioridad.

(2) Configure la configuración global del servidor y haga clic en **Guardar**.

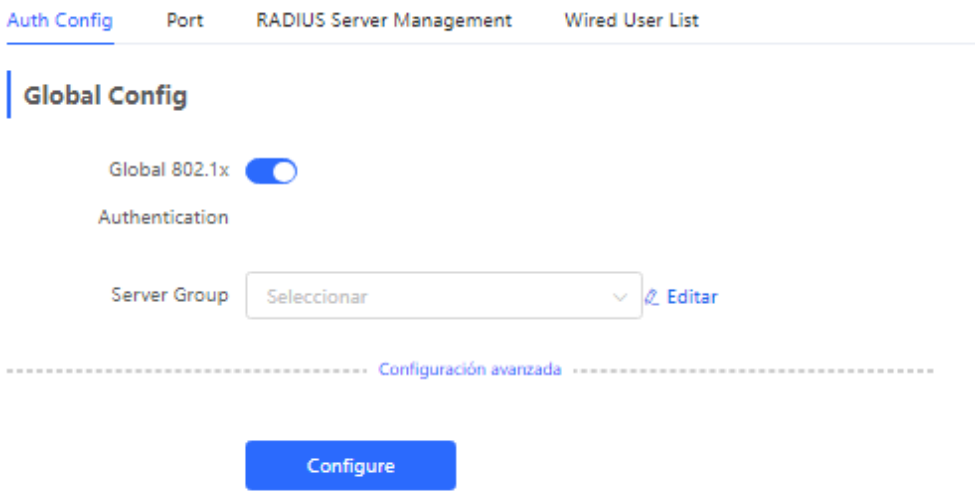
Parámetro	Descripción
Packet Retransmission Interval	Permite configurar el intervalo para que el dispositivo envíe paquetes de solicitud antes de confirmar que no hay respuesta del servidor RADIUS.
Packet Retransmission Count	Permite configurar el número de veces que el dispositivo envía paquetes de solicitud antes de confirmar que no hay respuesta del servidor RADIUS.
Server Detection	Si esta función se encuentra habilitada, deberá configurar los campos «Server Detection Period», «Server Detection Times» y «Server Detection Username». Esta función se utiliza para determinar el estado del servidor para decidir si deben habilitarse funciones como la función de escape.

Parámetro	Descripción
MAC Address Format	Permite configurar el formato de la dirección MAC del atributo RADIUS n.º 31 (Calling-Stationg-ID). A continuación se muestran los formatos admitidos: El formato hexadecimal separado por puntos, como 00d0.f8aa.bbcc. El formato IETF, como 00-D0-F8-AA-BB-CC. Sin formato (valor predeterminado), como 00d0f8aabbcc.

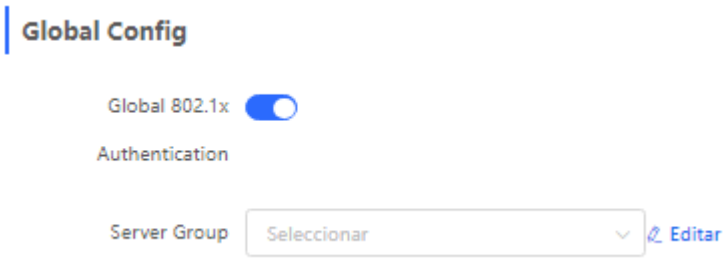
2. Configuración de la configuración global de la autenticación 802.1x

Seleccione **Dispositivo local** > **Seguridad** > **802.1x Authentication** > **Auth Config.**.

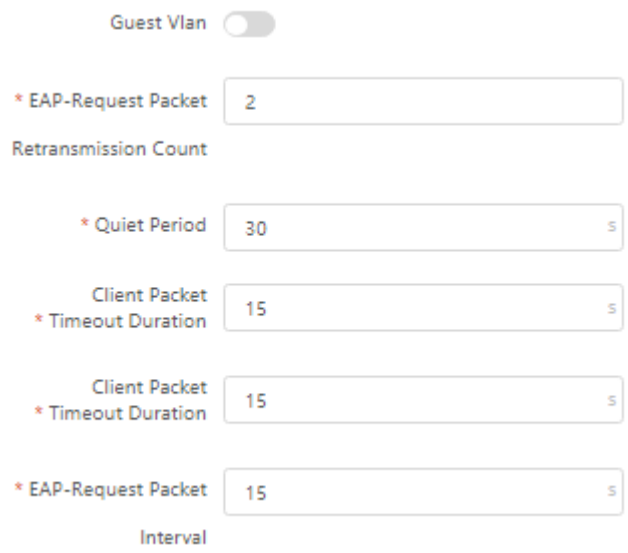
(1) Haga clic en el botón **Global 802.1x**. El sistema le pedirá que confirme si desea habilitarlo, haga clic en **Configure**.



(2) Seleccione el grupo de servidores.



(3) Haga clic en Configuración avanzada para configurar parámetros como la VLAN de invitados.



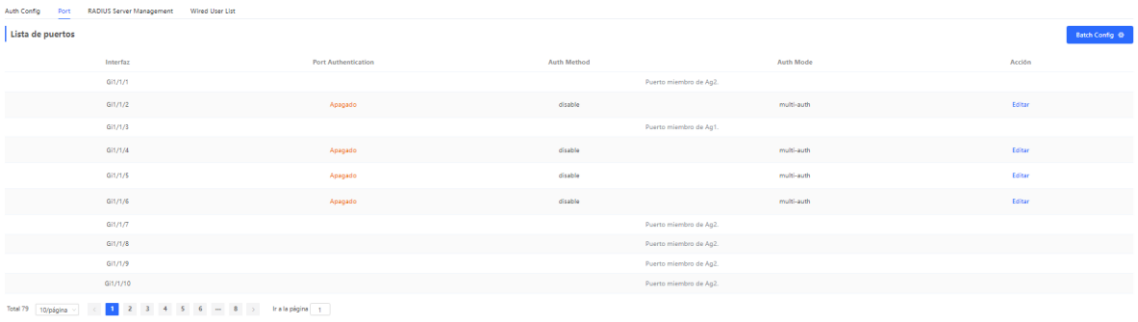
Parámetro	Descripción
Server Escape	Si el servidor se desconecta, todos los usuarios podrán acceder a Internet.
Re-authentication	Obliga a los clientes a que vuelvan a autentificarse cada determinados intervalos de tiempo para garantizar la seguridad de la red.
Guest VLAN	Proporciona una VLAN a los clientes no autenticados para restringir su acceso.
EAP-Request Packet Retransmission Count	Permite establecer el número de veces que se retransmitirá el mensaje de solicitud EAP cuando no se reciba respuesta. Rango de valores: 1 a 10 veces.
Quiet Period	Durante el proceso de autenticación es el tiempo de inactividad entre el que el cliente y el servidor no intercambian mensajes de autenticación. Rango de valores: 0-65535 segundos.
Client Packet Timeout Duration	El tiempo límite para que el servidor espere la respuesta del cliente. Se considera que se ha producido un fallo de autenticación cuando se sobrepasa este tiempo. Rango de valores: 1-65535 segundos.

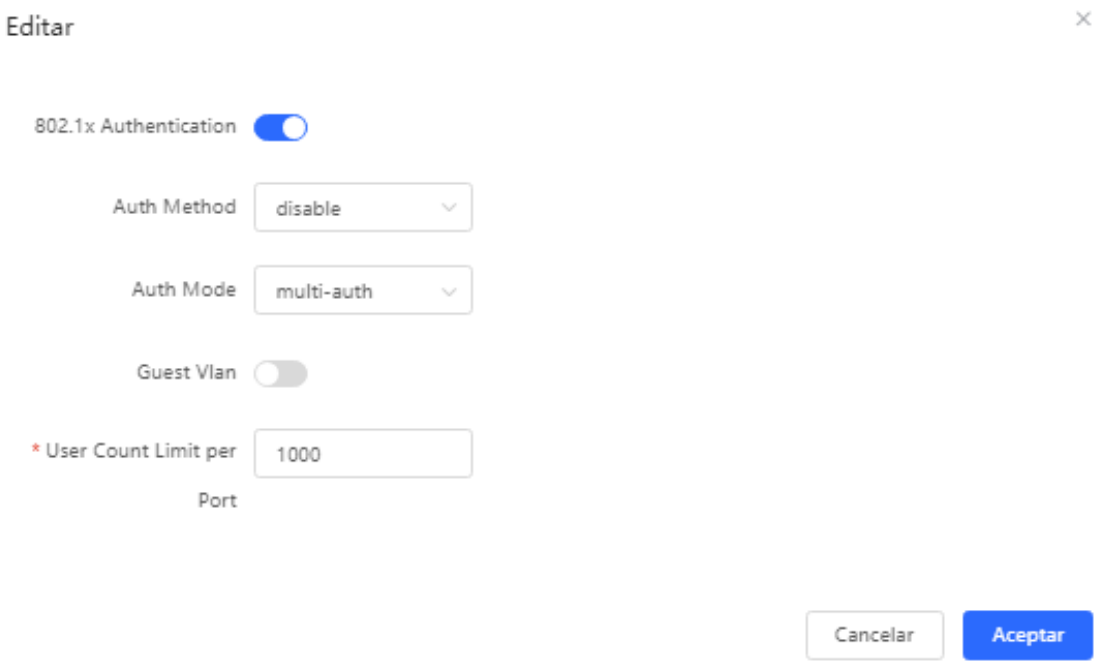
Parámetro	Descripción
Client Packet Timeout Duration	El límite de tiempo para que el cliente espere la respuesta del servidor. Se considera que se ha producido un fallo de autenticación cuando se sobrepasa este tiempo. Rango de valores: 1-65535 segundos.
EAP-Request Packet Interval	Permite establecer el intervalo de tiempo entre el envío de mensajes de solicitud EAP para controlar la velocidad del proceso de autenticación. Rango de valores: 1-65535 segundos.

3. Configuración de la interfaz válida

Seleccione **Dispositivo local** > **Seguridad** > **802.1x Authentication** > **Port**.

(1) Haga clic en Configuración de la interfaz, en Modificar o en Batch Config. tras configurar una única interfaz y edite los parámetros de autenticación de la interfaz.





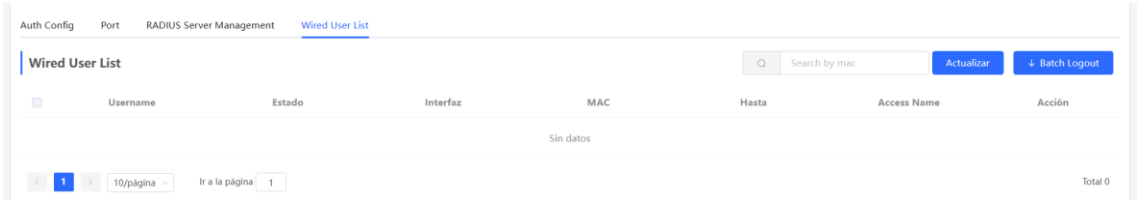
Parámetro	Descripción
802.1x Authentication	Cuando se habilita, la interfaz seleccionada activa la autenticación 8.02.1x.
Auth Method	disable: desactiva el método de autenticación, que produce el mismo efecto que desactivar el switch con autenticación 802.1x. force-auth: autenticación obligatoria, el cliente puede acceder directamente a Internet sin contraseña. force-unauth: forzar la no autenticación, el cliente no puede autenticarse y no puede acceder a Internet. auto: autenticación automática, el dispositivo debe autenticarse y puede acceder a Internet tras realizar la autenticación. Se recomienda seleccionar el método de autenticación automática.

Parámetro	Descripción
Auth Mode	multi-auth: admite varios dispositivos que utilicen el mismo puerto para la autenticación, aunque cada dispositivo debe autenticarse de forma independiente. multi-host: varios dispositivos pueden compartir el mismo puerto. Mientras un usuario realice la autenticación, los siguientes podrán acceder a Internet. single-host: cada puerto solo permite que se autentique un dispositivo, que puede acceder a Internet una vez que haya realizado la autenticación correctamente.
Guest Vlan	Cuando se habilita, los dispositivos que no consiguen la autenticación se asignan de forma dinámica a la VLAN de invitados que se haya indicado. Aviso Debe crear primero un ID de VLAN y aplicarlo a la interfaz. A continuación, en Gestión de la seguridad > Autenticación 802.1x > Configuración avanzada en la configuración de la autenticación, habilite la opción VLAN de invitados e introduzca el ID.
User Count Limit per Port	Permite limitar el número de usuarios de la interfaz. Descripción de la diferencia entre productos El rango de valores de los switches de la serie NBS3100 es 1-256, mientras que el de otros switches es 1-1000.

17.7.3 Visualización de la lista de usuarios de autenticación conectados mediante una conexión por cable

Cuando la función 8.02.1x se configura en toda la red y un terminal se autentica y se conecta a la red, puede ver la lista de usuarios autenticados.

Seleccione **Dispositivo local** > **Gestión de la seguridad** > **Autenticación 802.1x** para obtener información concreta de los usuarios.



Haga clic en **Actualizar** para obtener la información más reciente de la lista de usuarios.

Si desea desconectar a un determinado usuario de la red, puede seleccionarlo y hacer clic en **Desconectar** en la columna **Acción**. Si lo desea, también puede seleccionar varios usuarios y hacer clic en **Batch logout**.

17.8 Antisuplantación de ARP

17.8.1 Descripción general

La antisuplantación o *anti-spoofing* de ARP se utiliza para revisar si la dirección IP de origen de un paquete ARP que pasa a través de un puerto de acceso está configurada en la dirección IP de la puerta de enlace. De ser así, el paquete se descartará para evitar que los hosts reciban paquetes de respuesta de ARP incorrectos. De no ser así, el paquete no será procesado. De este modo, solo el dispositivo ascendente puede enviar paquetes ARP y los paquetes de respuesta ARP falsos enviados por otros clientes serán filtrados y eliminados.

17.8.2 Procedimiento

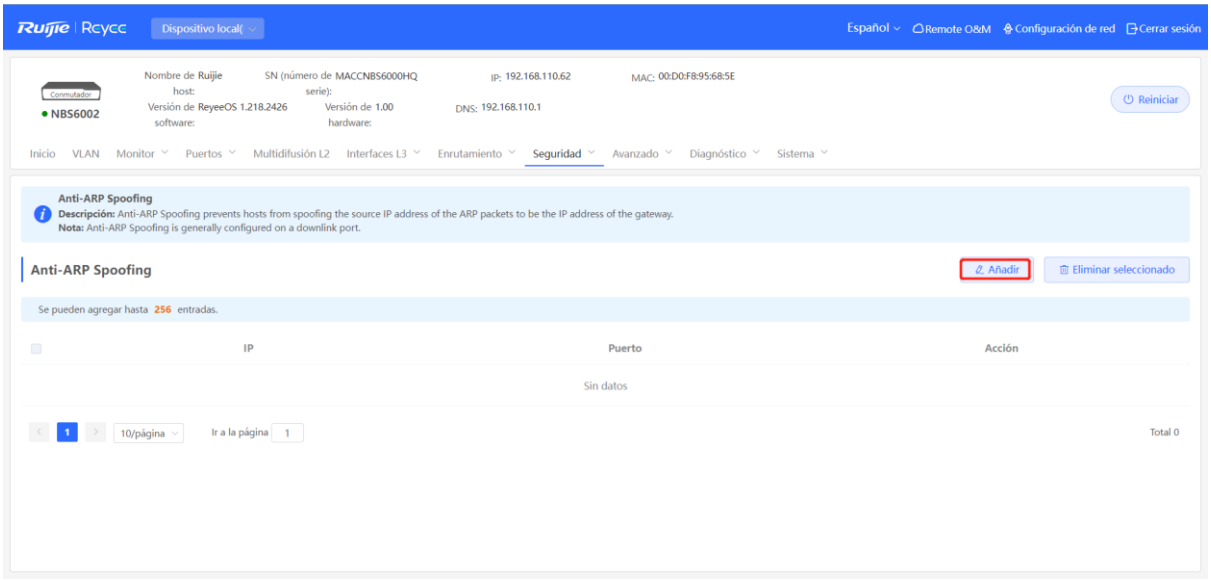
Seleccione **Dispositivo local** > **Seguridad** > **Anti-ARP Spoofing**.

1. Habilitar la antisuplantación de ARP

Haga clic en **Añadir**, seleccione el puerto deseado e ingrese la dirección IP de la puerta de enlace; después, haga clic en **Aceptar**.

Nota

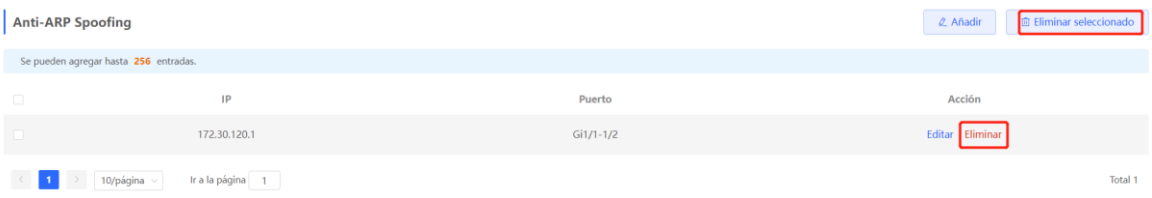
Generalmente, la función de antisuplantación de ARP se habilita en los puertos de enlace descendente del dispositivo.



2. Deshabilitar la antisuplantación de ARP

Configuración por lotes: seleccione una entrada a eliminar y en la lista haga clic en **Eliminar seleccionado**.

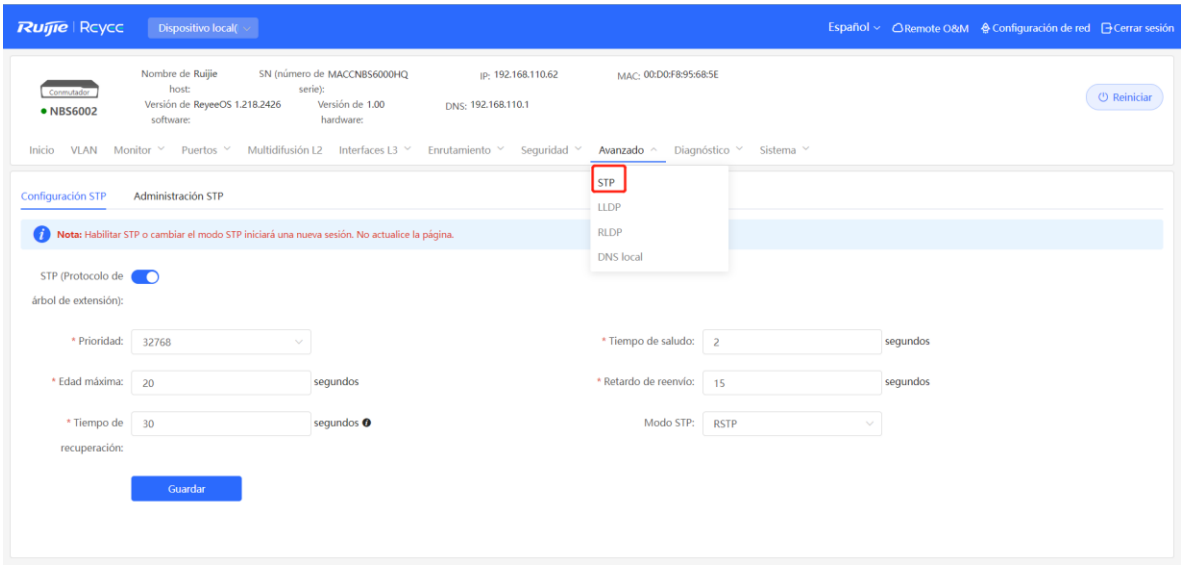
Configuración individual: en la entrada correspondiente, haga clic en el botón **Eliminar** de la última columna **Acción**.



18 Configuración avanzada de los switches de las series NBS y NIS

18.1 STP

El Protocolo de árbol de extensión (STP) es un protocolo de administración de Capa 2 que elimina los bucles de Capa 2 al bloquear selectivamente los enlaces redundantes en la red. También proporciona la función de respaldo de enlaces.

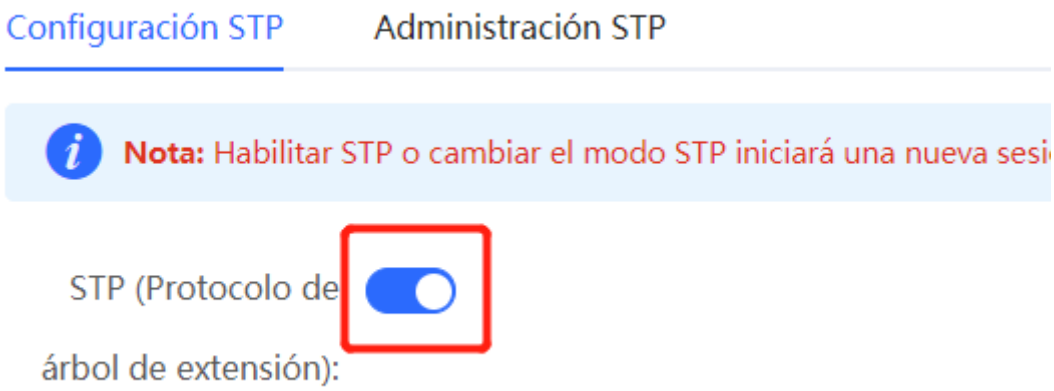


18.1.1 Configuración global del STP

Seleccione **Dispositivo local** > **Avanzado** > **STP** > **Configuración STP**.

(1) Habilite la función STP y haga clic en **Aceptar** en el cuadro de diálogo que aparece. Por defecto, la función STP está deshabilitada.

> **Precaución**
>
> Habilitar o cambiar el modo STP iniciará una nueva sesión. No actualice la página durante la configuración.



(2) Configure los parámetros globales de STP y haga clic en **Guardar**.

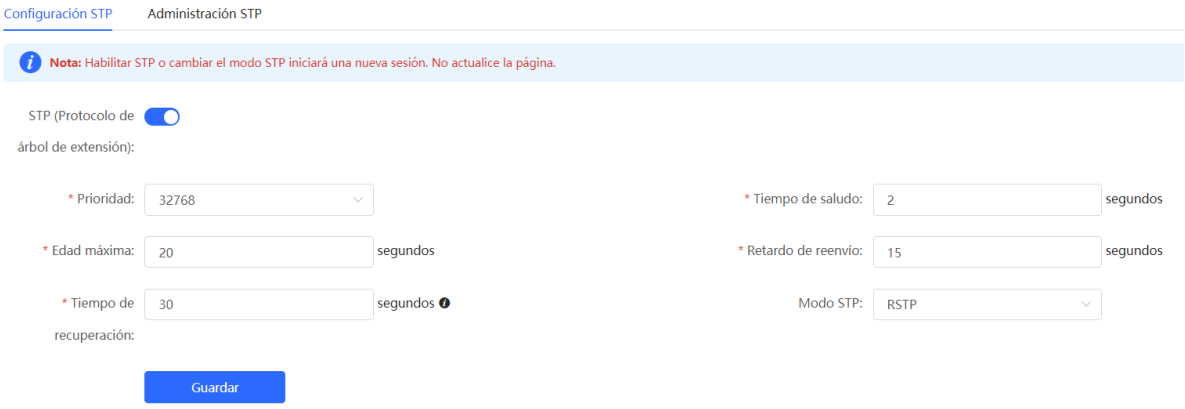


Tabla 18-1 Descripción de los parámetros para la configuración global del STP

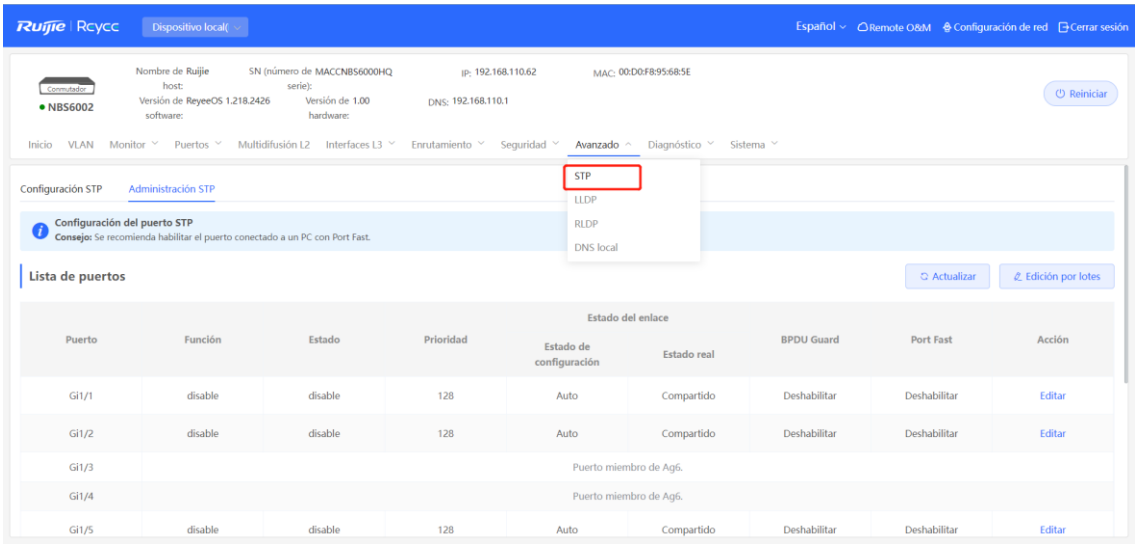
Parámetro	Descripción	Valor predeterminado
STP	Determine si se habilita STP. Se hace efectivo a nivel global. Los atributos de STP pueden configurarse solamente después de que se habilite el STP.	Deshabilitado
Prioridad	Prioridad de puente. El dispositivo compara primero la prioridad de puente durante la selección del puente raíz. Un valor menor indica una prioridad mayor.	32768
Edad máxima	Tiempo máximo de caducidad de las BPDU. Los paquetes que han vencido son descartados. Si un puente no raíz no recibe la BPDU del puente raíz antes de que el tiempo de envejecimiento expire, el puente raíz o el enlace a este se considera fallido.	20 segundos

Parámetro	Descripción	Valor predeterminado
Tiempo de recuperación	El tiempo de recuperación de la red cuando hay enlaces redundantes en esta.	30 segundos
Tiempo de saludo	Intervalo del envío entre dos BPDU adyacentes.	2 segundos
Retardo de reenvío	Intervalo en el que el estado del puerto cambia; esto es, intervalo para que el puerto cambie de estado de escucha a estado de aprendizaje, o de aprendizaje a envío.	15 segundos
Modo STP	Modo de trabajo del STP. El dispositivo admite STP y el Protocolo de árbol de extensión rápida (RSTP).	RSTP

18.1.2 Implementación de STP en un puerto

Seleccione **Dispositivo local** > **Avanzado** > **STP** > **Administración STP**.

Configure las propiedades STP para un puerto. Haga clic en **Editar por lotes** para seleccionar los puertos y configurar los parámetros STP; o haga clic en **Editar** en la columna de **Acción**, en **Lista de puertos**, para configurar los puertos designados.



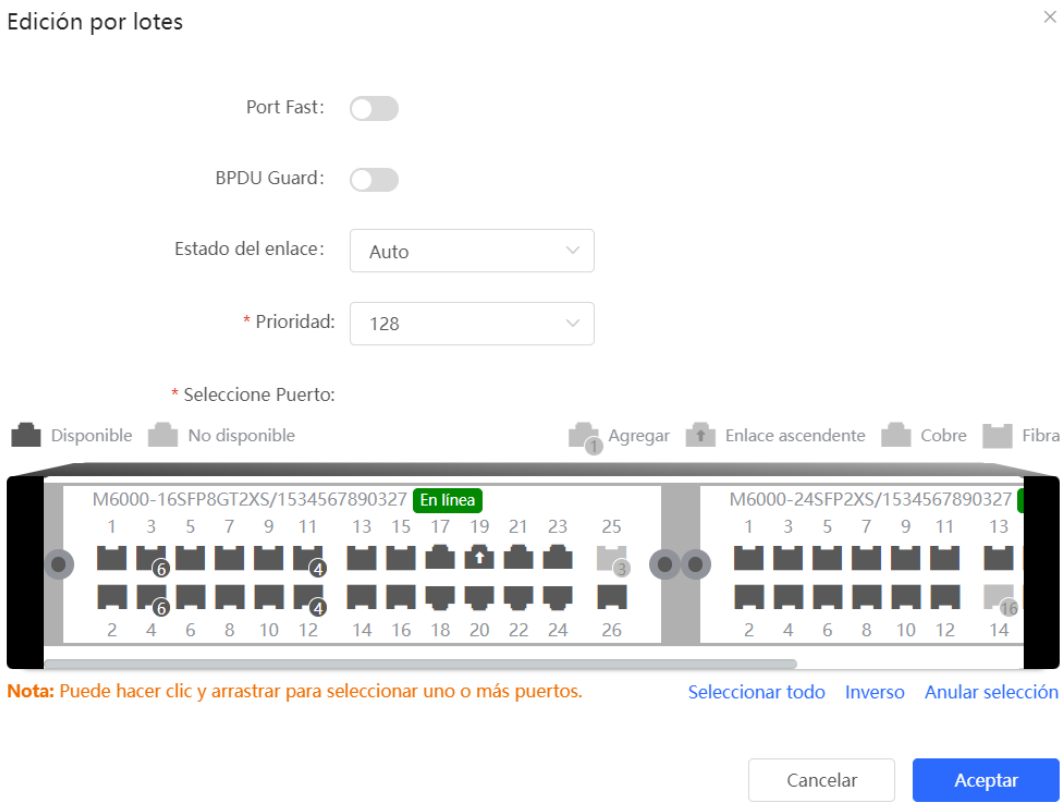


Tabla 18-2 Descripción de los parámetros para la configuración del STP de los puertos

Parámetro	Descripción	Valor predeterminado
Función	● Raíz: indica el puerto más cercano a la raíz. ● Alternativo: indica el puerto de respaldo de un puerto raíz. Cuando un puerto raíz falla, el puerto alternativo se vuelve el puerto raíz inmediatamente. ● Designado (puerto designado): indica el puerto que conecta el puente raíz o un puente ascendente a un dispositivo descendente. ● Deshabilitado (puerto bloqueado): indica el puerto en estado bloqueado en el árbol de extensión.	NA

Parámetro	Descripción	Valor predeterminado
Estado	● Deshabilitado: el puerto se apaga manualmente o, debido a una falla, no participa en el árbol de extensión y no reenvía datos, y puede hacer la transición al estado bloqueado después de ser habilitado. ● Bloqueado: un puerto en estado bloqueado no puede reenviar paquetes de datos o aprender direcciones, pero puede enviar y recibir BPDU de configuración y enviarlas al CPU. ● Escucha: si el puerto puede convertirse en el puerto raíz o designado, este entrará en un estado de escucha. Un puerto en estado de escucha no reenvía datos o aprende direcciones, pero puede recibir y enviar BPDU de configuración. ● Aprendizaje: un puerto en estado de aprendizaje no puede reenviar datos, pero comienza a aprender direcciones y puede recibir, procesar y enviar BPDU de configuración. ● De reenvío: una vez que el puerto entra en este estado, puede reenviar cualquier tipo de datos, aprender direcciones, y recibir, procesar y enviar BPDU de configuración.	NA
Prioridad	La prioridad del puerto se usa para elegir su función y el puerto de mayor prioridad se selecciona preferentemente para entrar en estado de reenvío.	128
Estado del enlace Estado de la configuración	El tipo de enlace puede ser **Compartido**, **Extremo a Extremo** o **Auto**. En modo **Auto**, el tipo de interfaz se determina con base en el modo dúplex. Para puertos dúplex completos, el tipo de interfaz es **Extremo a Extremo**; para los puertos semidúplex, la interfaz es **Compartida**.	Automático
Estado del enlace Estado real	El tipo de enlace real puede ser **Compartido** o **Extremo a Extremo**.	NA
Protección BPDU	Determine si se habilita la función de protección BPDU. Cuando la función quede habilitada, si se habilita PortFast en un puerto, o el puerto es automáticamente identificado como un puerto extremo conectado a una terminal, el puerto que recibe las BPDU se deshabilitará y entrará en estado Error-deshabilitado. En este caso, un usuario no autorizado puede añadir un dispositivo de red a la red, dando como resultado un cambio en su topología.	Deshabilitado
PortFast	Determine si se habilita la función PortFast. Después de que se habilita PortFast en un puerto, este no puede recibir o enviar BPDU. En este caso, el host conectado directamente al puerto no puede recibir BPDU. Si un puerto donde se ha habilitado PortFast sale de dicho estado automáticamente cuando recibe las BPDU, la función de filtro BPDU se deshabilita automáticamente. Generalmente, el puerto conectado a la PC es habilitado con PortFast.	Deshabilitado

Nota

- Se sugiere usar PortFast en el puerto conectado a la PC.
- Un puerto cambia al estado de reenvío después de que el STP es habilitado por más de 30 segundos. Por lo tanto, puede ocurrir una desconexión temporal y los paquetes no se pueden reenviar.

18.2 LLDP

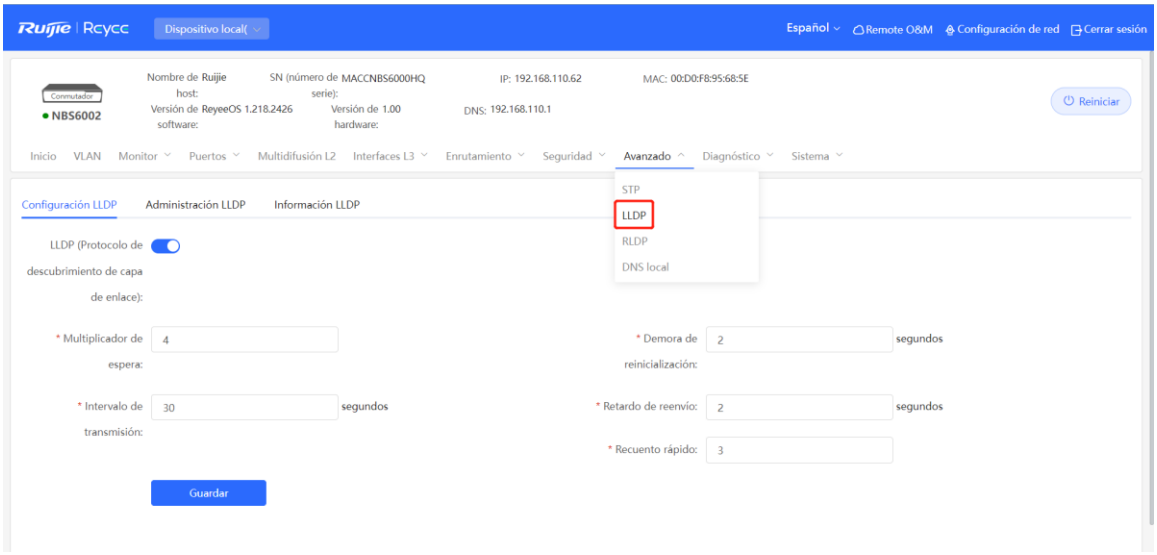
18.2.1 Descripción general

El Protocolo de descubrimiento de capa de vínculo (LLDP) está definido por el estándar IEEE 802.1AB. El LLDP puede descubrir dispositivos y detectar cambios en la topología. Con el LLDP, el sistema de gestión Eweb puede aprender el estado de conexión topológica; por ejemplo, los puertos de un dispositivo conectados a otros dispositivos, velocidades de los puertos a ambos extremos del enlace y coincidencia del modo dúplex. Un administrador puede localizar y resolver fallas rápidamente con base en la información anterior.

18.2.2 Configuración global del LLDP

Seleccione **Dispositivo local** > **Avanzado** > **LLDP** > **Configuración LLDP**.

(1) Habilite la función LLDP y haga clic en **Guardar** en el cuadro que aparece. Por defecto, la función STP está habilitada. Cuando el LLDP se encuentre habilitado, ignore este paso.



(2) Configure los parámetros globales del LLDP y haga clic en **Guardar**.

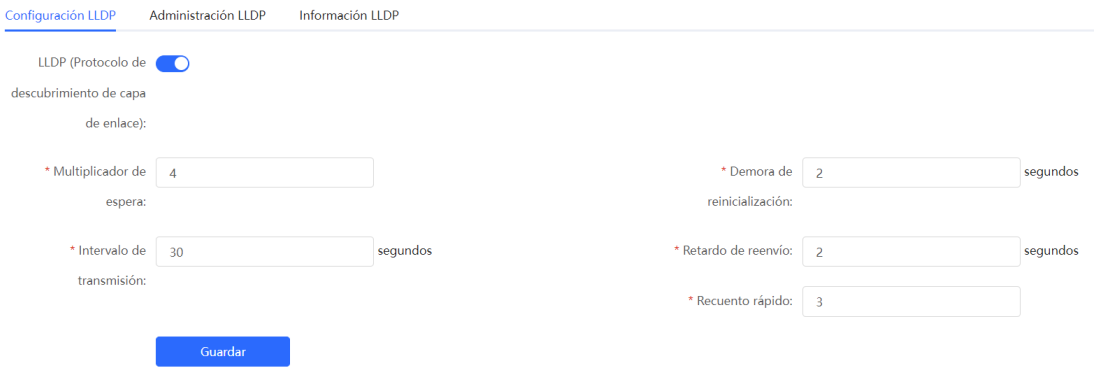


Tabla 18-3 Descripción de los parámetros para la configuración global del LLDP

Parámetro	Descripción	Valor predeterminado
LLDP	Determine si la función LLDP está habilitada.	Habilitado
Multiplicador de espera	Multiplicador TTL del LLDP. En los LLDPDU, el TTL TLV indica el TTL de información local de un dispositivo vecino. El valor de TTL TLV se calcula usando la siguiente fórmula: TTL TLV = multiplicador TTL x intervalo de transmisión LLDPDU + 1 El valor de TTL TLV se puede modificar configurando el multiplicador TTL y el intervalo de transmisión LLDPDU.	4
Intervalo de transmisión	Intervalo de transmisión LDPDU, en segundos. El valor de TTL TLV se calcula usando la siguiente fórmula: TTL TLV = multiplicador TTL x intervalo de transmisión LLDPDU + 1 El valor de TTL TLV se puede modificar configurando el multiplicador TTL y el intervalo de transmisión LLDPDU.	30 segundos
Recuento rápido	Número de paquetes que se transmiten rápidamente. Cuando se descubre un nuevo vecino o el modo de trabajo del LLDP se cambia, el dispositivo iniciará el mecanismo de transmisión rápida, para que los dispositivos vecinos aprendan la información sobre dicho dispositivo lo antes posible. El mecanismo de transmisión rápida acorta el intervalo de transmisión del LLDPDU a 1 s, manda un determinado número de LLDPDU continuamente, y luego restablece el intervalo normal de transmisión. Se puede configurar el número de LLDPDU que se pueden transmitir rápidamente por el mecanismo de transmisión.	3

Parámetro	Descripción	Valor predeterminado
Demora de reinicialización	La demora de inicialización de puertos, en segundos. Se puede configurar una demora de inicialización para prevenir la frecuente inicialización del estado de la máquina, ocasionado por cambios frecuentes en el modo de trabajo de los puertos.	2 segundos
Retardo de reenvío	Demora en el envío de los LLDPDU, en segundos Cuando la información local del dispositivo cambia, este transmite inmediatamente los LLDPDU a sus vecinos. Se puede configurar una demora de transmisión para evitar la transmisión frecuente de LLDPDU, ocasionada por los frecuentes cambios de la información local. Si se utiliza una pequeña demora, el cambio frecuente de la información local ocasionará la transmisión frecuente de LLDPDU. Si se utiliza una mayor demora, es posible que no se transmita ningún LLDPDU, incluso cuando la información local se cambie. Establezca una demora adecuada de acuerdo con la situación real.	2 segundos

18.2.3 Implementación del LLDP en un puerto

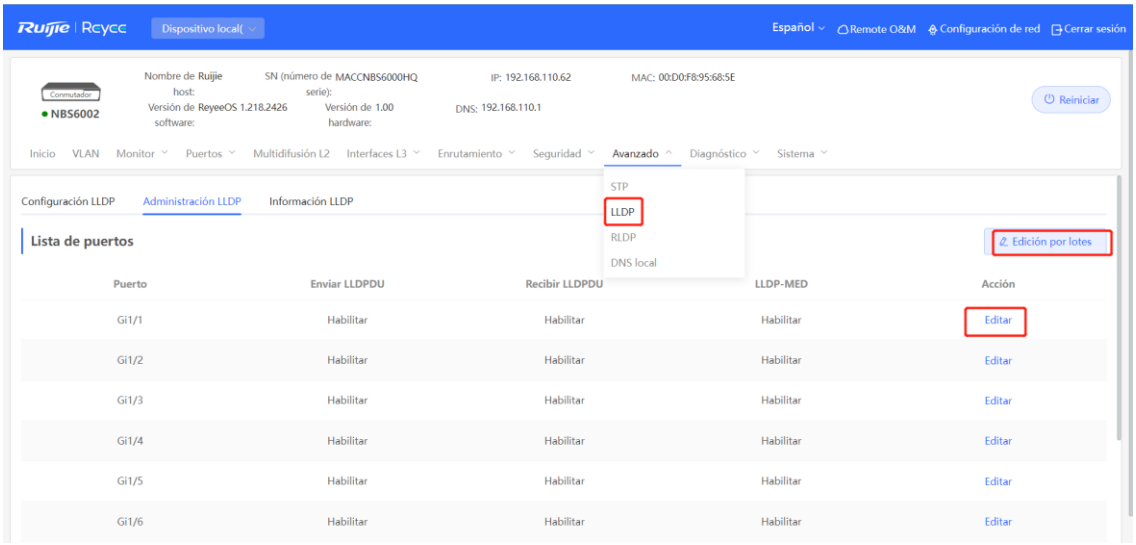
Seleccione **Dispositivo local** > **Avanzado** > **LLDP** > **Administración LLDP**.

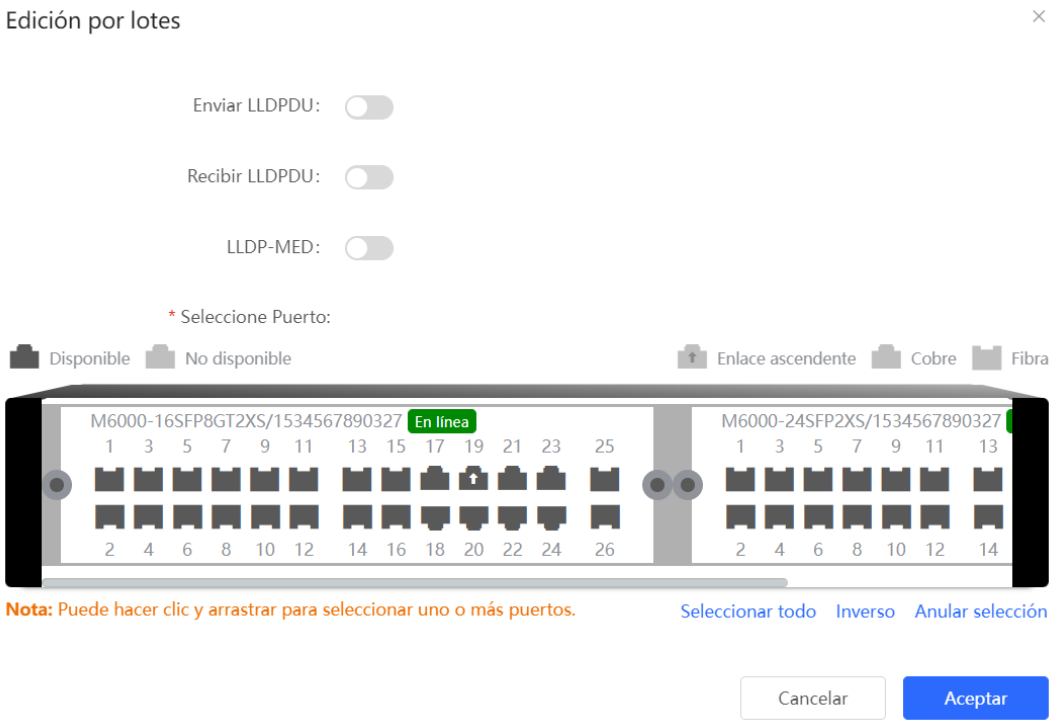
En **Lista de puertos**, haga clic en **Editar** en la columna **Acción**; o haga clic en **Edición por lotes**, seleccione el puerto deseado, configure el modo de trabajo del LLDP en dichos puertos, determine si se habilita **LLDP-MED**, y haga clic en **Aceptar**.

Enviar LLDPDU: después de habilitar **Enviar LLDPDU** en un puerto, este puede enviar LLDPDU.

Recibir LLDPDU: después de habilitar **Recibir LLDPDU** en un puerto, este puede recibir LLDPDU.

LLDP-MED: después de habilitar **LLDP-MED**, el dispositivo puede descubrir dispositivos vecinos cuando su terminal par admita el Protocolo de descubrimiento de capa de vínculo y puntos de conexión de medios (LLDP-MED).



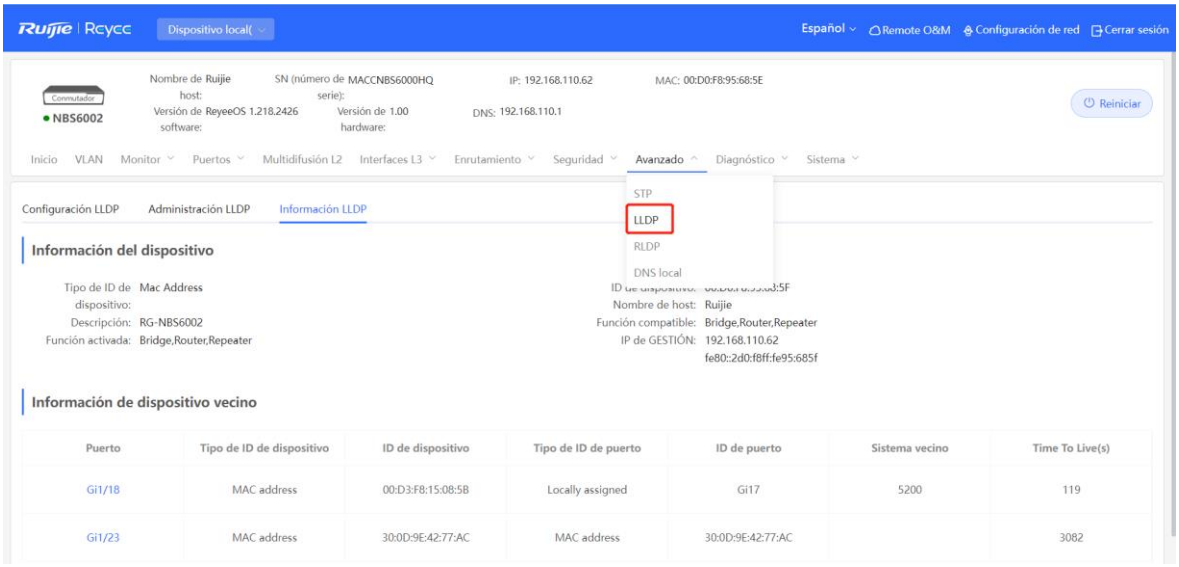


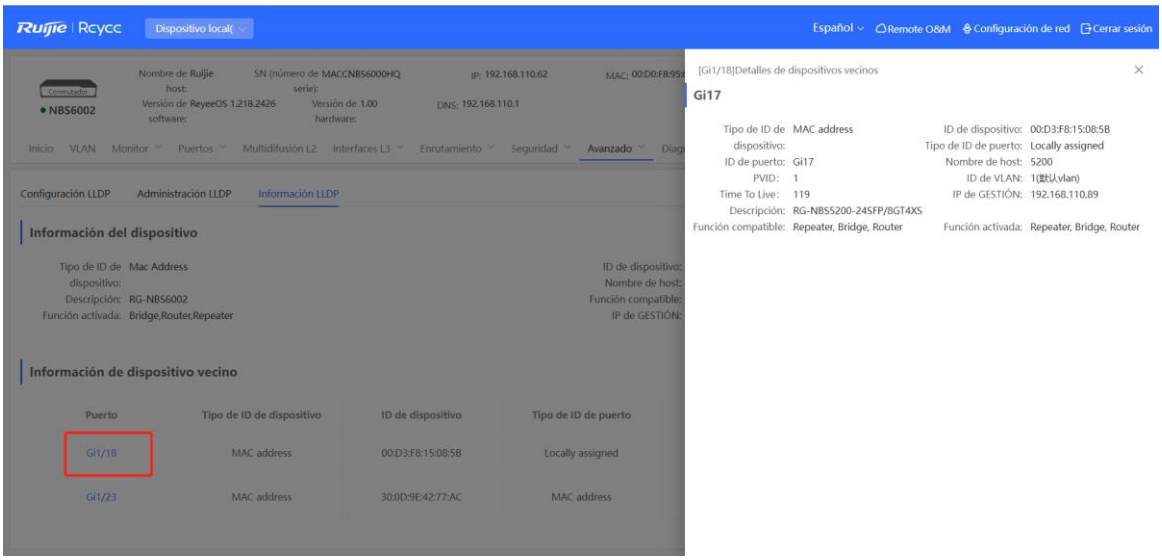
18.2.4 Visualización de la información del LLDP

Seleccione **Dispositivo local** > **Avanzado** > **LLDP** > **Información LLDP**.

La página de **Información LLDP** muestra toda su información, incluyendo aquella del dispositivo local y los dispositivos vecinos de cada puerto. Haga clic en nombre del puerto y despliegue los detalles acerca de los puertos vecinos.

Revise la conexión de la topología a través de la información del LLDP o utilice el LLDP para detectar errores. Por ejemplo, dos conmutadores están directamente conectados en la topología de la red. Cuando un administrador configura la velocidad de los puertos VLAN y el modo dúplex, surgirá un error si las configuraciones no coinciden con aquellas conectadas al puerto vecino.





18.3 RLDP

18.3.1 Descripción general

El Protocolo de detección de enlace rápido (RLDP) es un protocolo de detección de falla de enlace Ethernet que se utiliza para detectar rápidamente fallas en las funciones de enlace unidireccionales, bidireccionales y bucles de enlace descendente. Cuando se encuentra una falla, el RLDP apaga automáticamente los puertos importantes o solicita al administrador que los apague manualmente, de acuerdo con los procedimientos configurados ante fallas, evitando el tráfico incorrecto de reenvío o bucles de Capa 2.

La función RLDP puede habilitarse en conmutadores de acceso de la red por lotes. Por defecto, los puertos de los conmutadores se apagarán automáticamente cuando ocurra un bucle. También se puede configurar si la

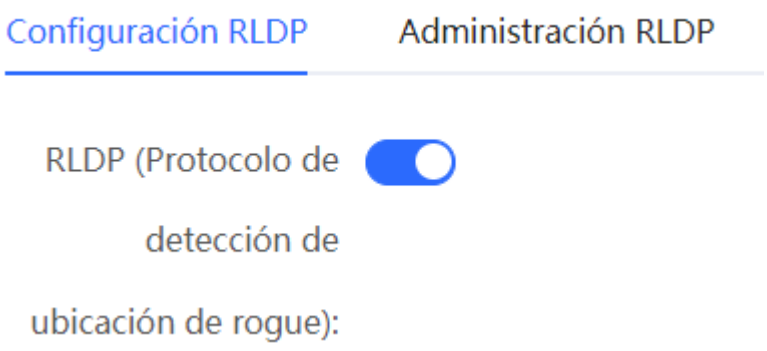
detección de bucles está habilitada en cada puerto de un mismo conmutador y los métodos de manejo después de la detección de una falla de enlace.

18.3.2 Configuración de un dispositivo independiente

1. Configuración global del RLDP

Seleccione **Dispositivo local** > **Avanzado** > **RLDP** > **Configuración RLDP**.

(1) Habilite la función RLDP y haga clic en **Aceptar** en el cuadro de diálogo que aparece. Por defecto, la función RLDP está deshabilitada.



(2) Configure los parámetros globales del RLDP y haga clic en **Guardar**.

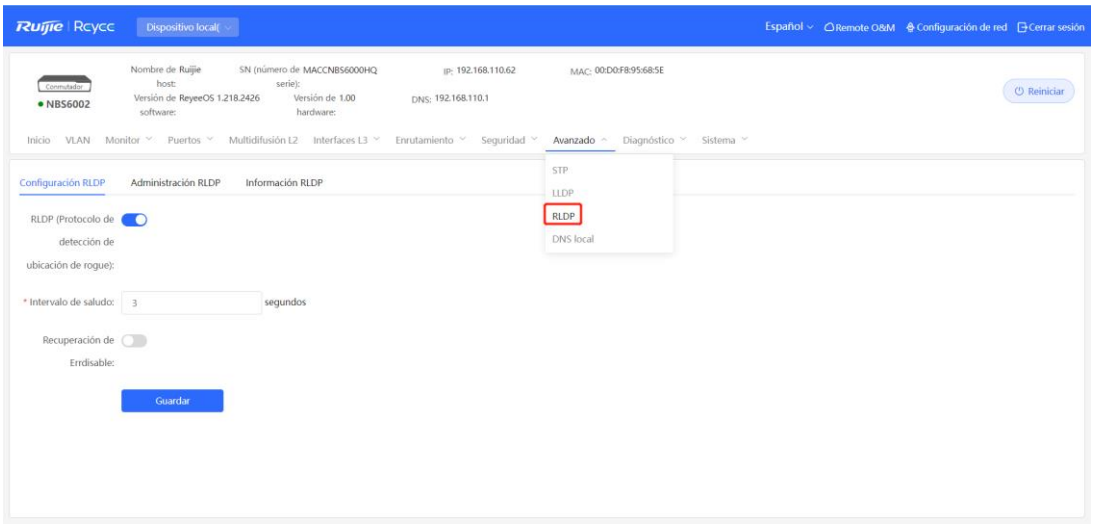


Tabla 18-4 Descripción de los parámetros para la configuración global del RLDP

Parámetro	Descripción	Valor predeterminado
RLDP	Determine si la función RLDP está habilitada.	Deshabilitado
Intervalo de saludo	Intervalo del RLDP para detectar paquetes de envío, en segundos.	3 segundos

Parámetro	Descripción	Valor predeterminado
Recuperación por Errdisable	Al habilitar esta función, el puerto automáticamente recupera el estado de inicialización después de que ocurre un bucle.	Deshabilitado
Intervalo de recuperación por Errdisable	Intervalo en el que todos los puertos con falla se restablecen al estado de inicialización y la detección de enlaces vuelve a comenzar, en segundos.	30 segundos

2. Implementación del RLDP en un puerto

Seleccione **Dispositivo local** > **Avanzado** > **RLDP** > **Administración RLDP**.

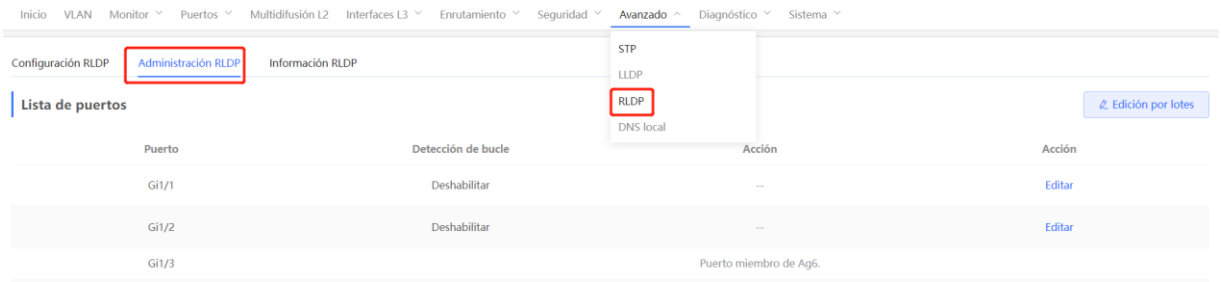
En **Lista de puertos**, haga clic en **Editar** en la columna **Acción**, o haga clic en **Edición por lotes**, seleccione el puerto deseado, configure si desea habilitar la detección de bucles en el puerto y el método de manejo después de la detección de una falla, y haga clic en **Aceptar**.

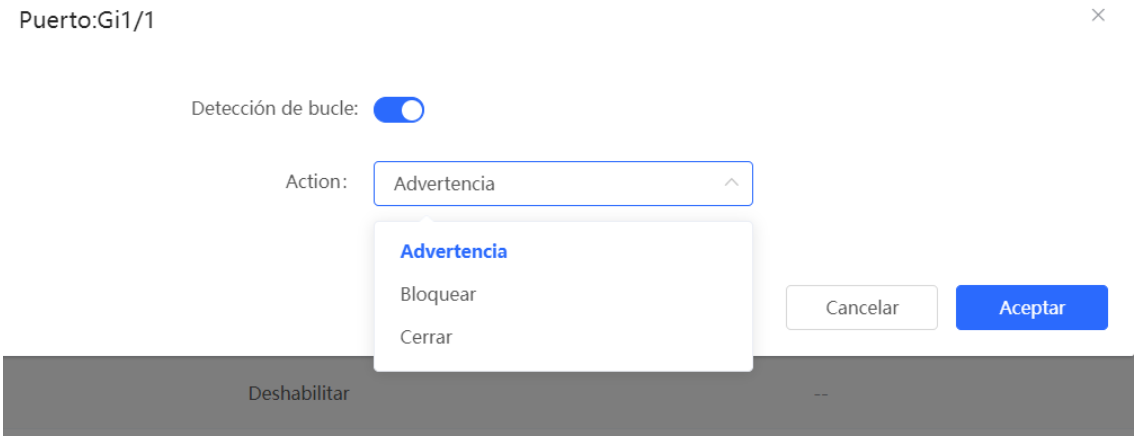
Hay tres métodos para procesar las fallas de los puertos.

- **Advertencia:** únicamente aparece información importante para indicar la falla del puerto y el tipo de esta.
- **Bloquear:** cuando se genera una alarma por una falla, se puede configurar el puerto dañado para que no pueda reenviar los paquetes recibidos.
- **Cerrar:** cuando se genera una alarma por una falla, se puede configurar el puerto para que se cierre.

Precaución

- Cuando la función RLDP se utiliza en un puerto agregado, los valores a configurar en la opción **Acción** solo son **Advertencia** o **Cerrar**.
- Cuando se ejecuta la detección RLDP en un puerto agregado, si los paquetes detectados se reciben en el mismo dispositivo y las VLAN del puerto que envía y recibe los paquetes son diferentes, el dispositivo no reconoce que haya ocurrido un bucle.

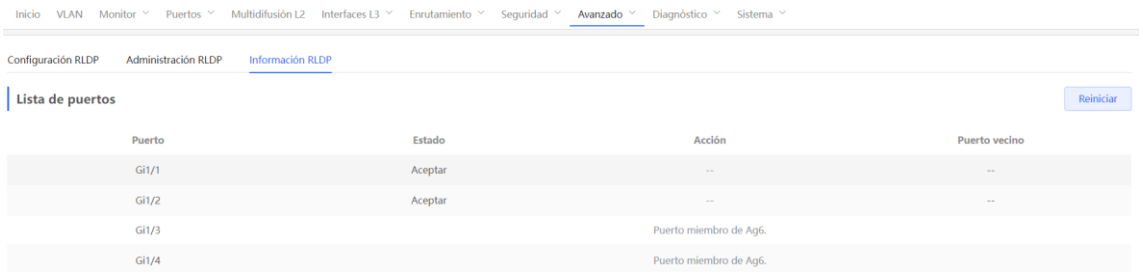




3. Visualización de la información del RLDP

Seleccione **Dispositivo local** > **Avanzado** > **RLDP** > **Información RLDP**.

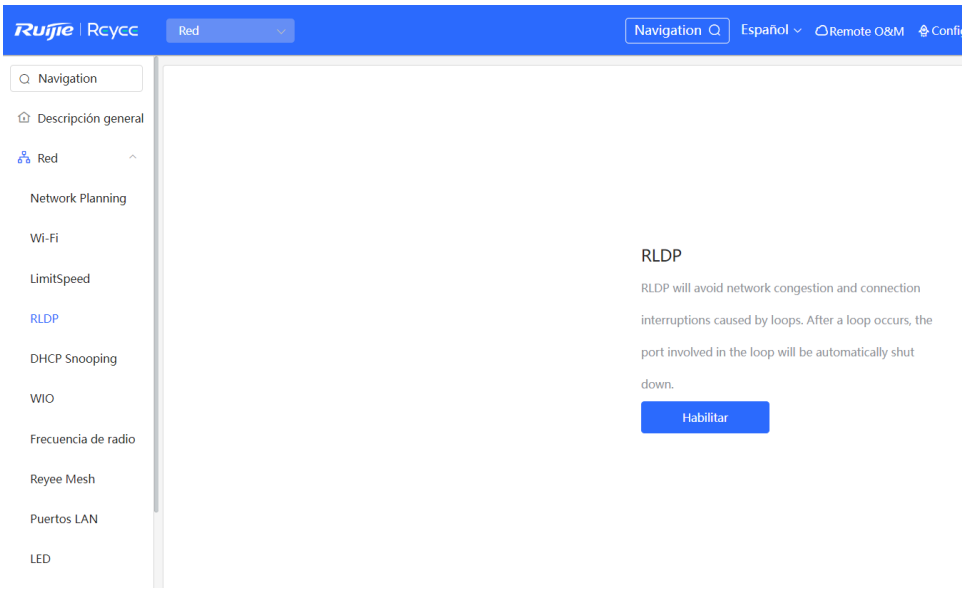
Visualice el estado de la detección, los métodos de manejo ante el resultado y los puertos que conectan con el dispositivo adyacente al dispositivo local. Haga clic en **Reiniciar** para restablecer a estado normal el estado de falla del RLDP que desencadenó un puerto.



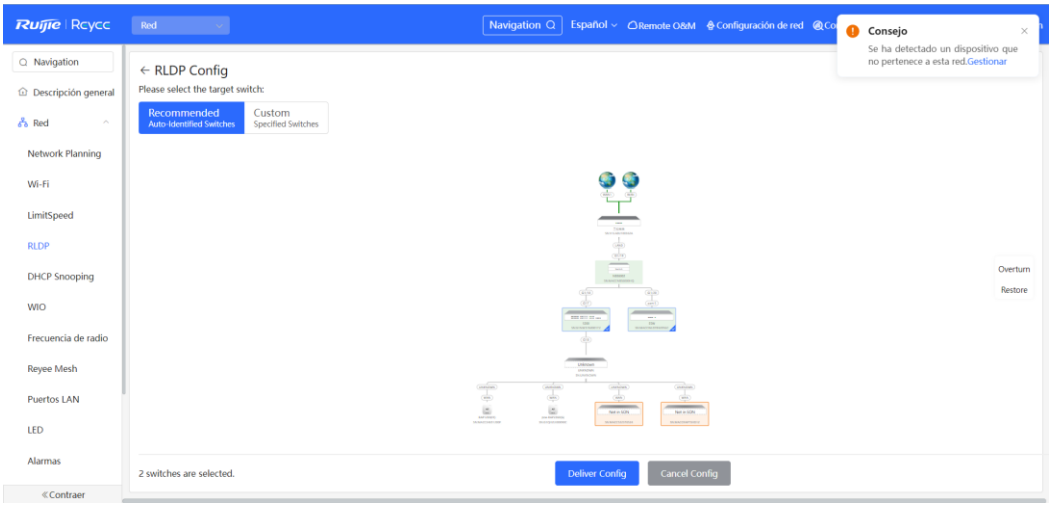
18.3.3 Configuración grupal de conmutadores de la red

Seleccione **Red** > **RLDP**.

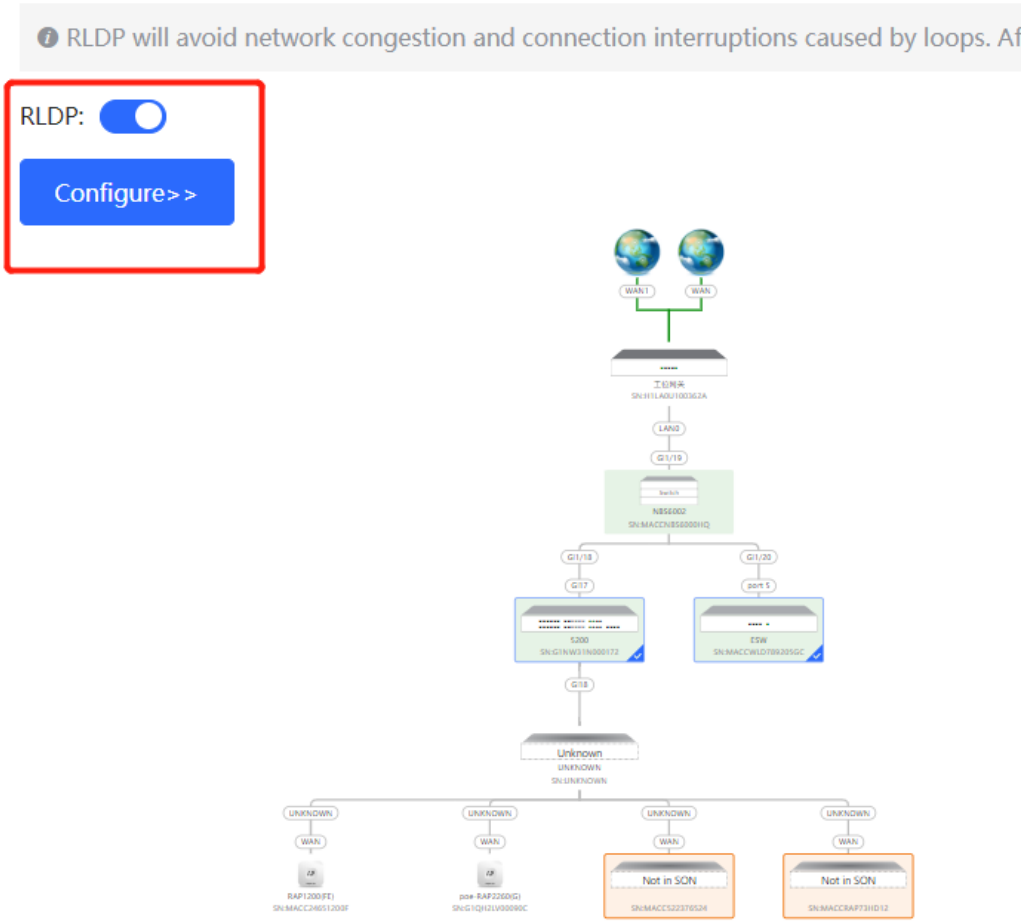
(1) Haga clic en **Habilitar** para acceder a la página **RLDP Config.**



(2) En la topología de la red, se puede seleccionar el acceso a los conmutadores donde se desea habilitar el RLDP, ya sea en modo recomendado o personalizado. Si se selecciona el modo recomendado, todos los conmutadores de acceso en la red se seleccionan automáticamente. Si se selecciona el modo personalizado, se pueden seleccionar manualmente los conmutadores de acceso deseados. Haga clic en **Deliver Config**. El RLDP está habilitado en los conmutadores seleccionados.



(3) Cuando la configuración se encuentre disponible, para modificar el rango efectivo de la función RLDP, haga clic en **Configure** para seleccionar los conmutadores deseados nuevamente en la topología. Deshabilite el RLDP en todos los conmutadores con un solo clic.

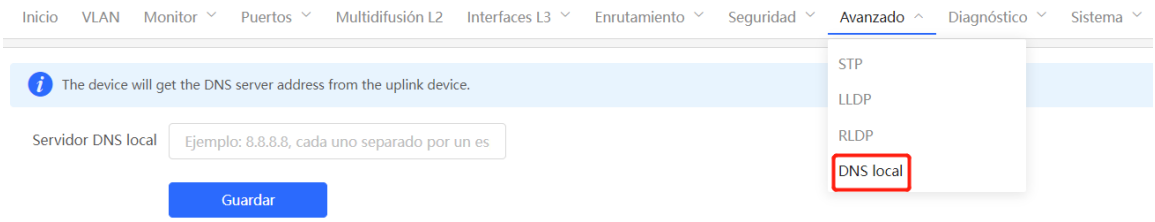


18.4 Configuración del servidor DNS local

El servidor DNS local es opcional. El dispositivo obtiene la dirección del servidor DNS del dispositivo de enlace ascendente conectado por defecto.

Seleccione **Dispositivo local** > **Avanzado** > **DNS local**.

Introduzca la dirección del servidor DNS que utilice el dispositivo local. Si existen varias direcciones, sepárelas con espacios. Haga clic en **Guardar**. Tras configurar el DNS local, el dispositivo utilizará primero el DNS de la dirección IP de gestión para resolver los nombres de dominio. Si el dispositivo no puede analizar los nombres de dominio, deberá utilizar esta dirección DNS en su lugar.



18.5 VLAN de voz

Precaución

La función VLAN de voz es compatible con los conmutadores de las series RG-NBS3100, RG-NBS3200, RG-NBS5100 y RG-NBS5200.

18.5.1 Descripción general

Una VLAN de voz está dedicada al tráfico de voz. Al crear una VLAN de voz y se añadir puertos conectados a dispositivos de voz, se pueden transmitir datos de voz a través de la VLAN de voz y tener una directiva específica de QoS para las transmisiones de voz, con el fin de mejorar la prioridad de la transmisión del tráfico de voz y garantizar la calidad de la llamada.

18.5.2 Configuración global de la VLAN de voz

Seleccione **Dispositivo local** > **Avanzado** > **Voice LAN** > **Configuración global**.

Habilite la función de VLAN de voz, configure los parámetros globales y haga clic en **Guardar**.

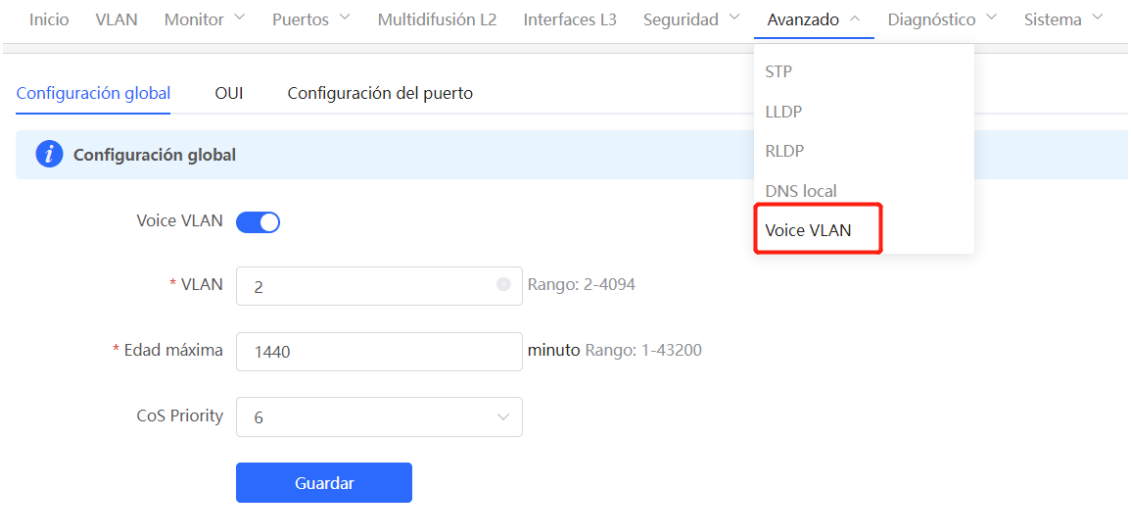


Tabla 18-5 Descripción de los parámetros para la configuración global de la VLAN de voz

Parámetro	Descripción	Valor predeterminado
VLAN de voz	Determine si se habilita la función de VLAN de voz.	Deshabilitado
VLAN	ID de la VLAN de voz	NA
Edad máxima	Tiempo de envejecimiento de la VLAN de voz, en minutos. En modo automático, cuando la dirección MAC en un paquete de voz envejezca, si el puerto no recibe más paquetes de voz dentro del tiempo de envejecimiento, el dispositivo elimina este puerto de la VLAN de voz.	1440 minutos
Prioridad CoS	Prioridad de Capa 2 de los paquetes de transmisión de voz en una VLAN de voz. El rango de valor va de 0 a 7. Un valor mayor indica una prioridad mayor. Se puede modificar la prioridad del tráfico de voz para mejorar la calidad de la llamada.	6

18.5.3 Configuración del OUI de una VLAN de voz

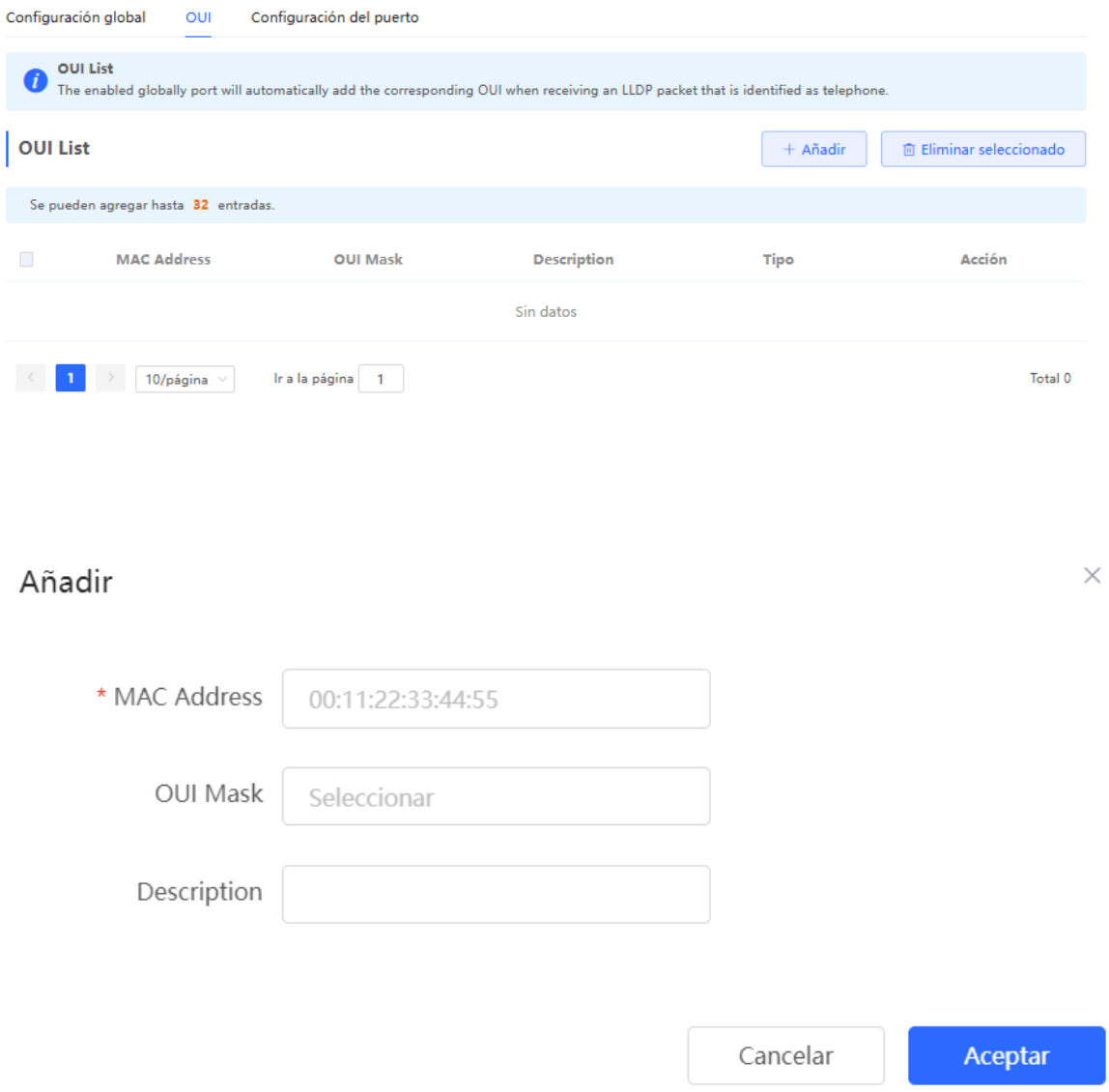
Seleccione **Dispositivo local** > **Avanzado** > **Voice LAN** > **OUI**.

La dirección MAC de origen de un paquete de voz contiene el identificador único organizativo (OUI) del fabricante del dispositivo de voz. Cuando el OUI de la VLAN de voz quede configurado, el dispositivo lo compara con la dirección MAC de origen en un paquete recibido, para identificar los paquetes de datos de voz, y los envía a la VLAN de voz para su transmisión.

Nota

Tras habilitar la función VLAN de voz en un puerto, cuando este recibe paquetes LLDP enviados por teléfonos IP, puede identificar los campos de las funciones del dispositivo en los paquetes e identificar los dispositivos con la función **Teléfono** como dispositivos de voz. **Además, también extrae** la dirección MAC de origen de un paquete del protocolo y la procesa como la dirección MAC del dispositivo de voz. De este modo, la OUI puede añadirse de forma automática.

Haga clic en **Añadir**. En el cuadro de diálogo que aparece, ingrese la dirección MAC y el OUI, y haga clic en **Aceptar**.



18.5.4 Configuración de la función VLAN de voz en un puerto

Seleccione **Dispositivo local** > **Avanzado** > **Voice LAN** > **Configuración del puerto**.

Haga clic en **Editar** en el puerto, o haga clic en **Edición por lotes** en la esquina superior derecha. En el cuadro de diálogo que aparece, seleccione si se habilita la función VLAN de voz en el puerto, configure el modo VLAN de voz a aplicar, especifique si se habilita el modo de seguridad, y haga clic en **Aceptar**.

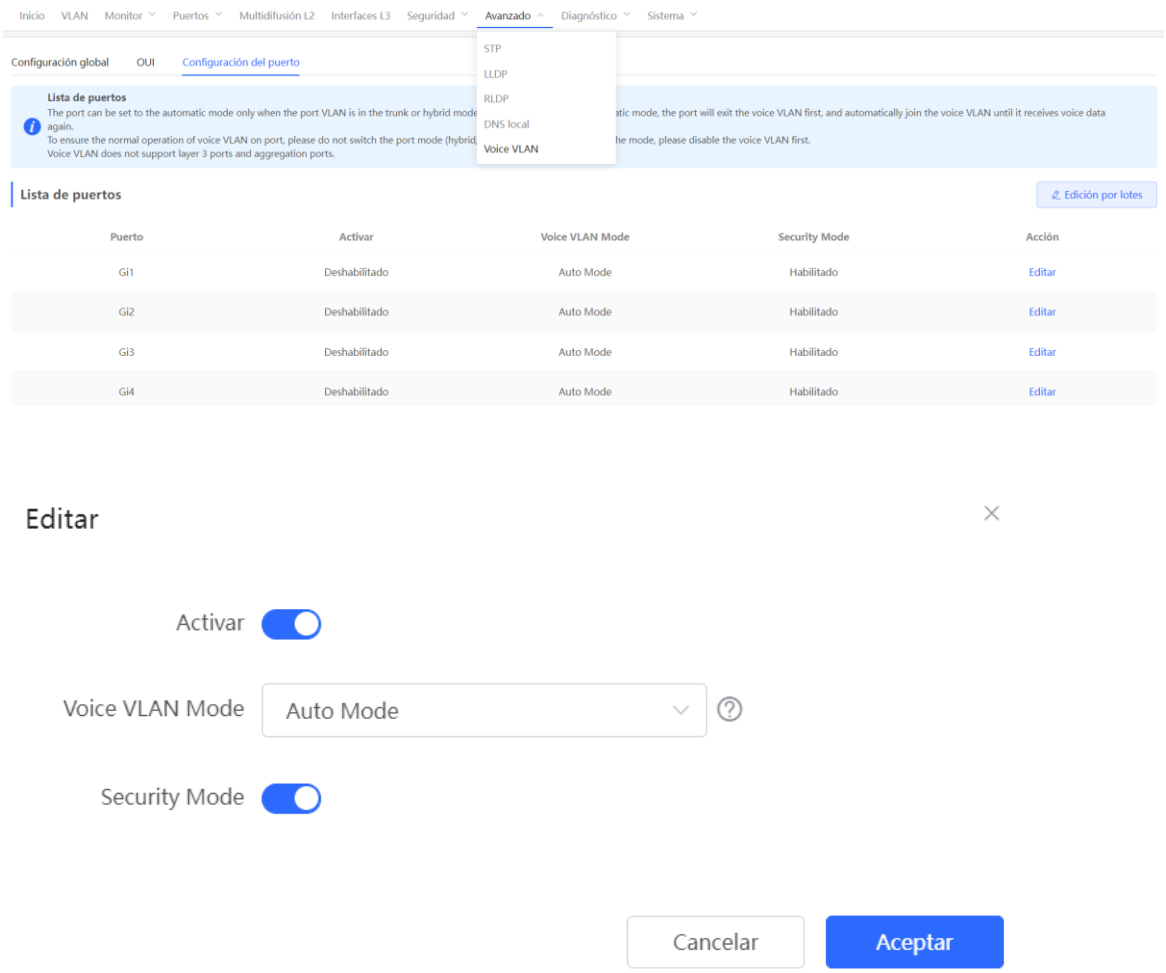


Tabla 18-6 Descripción de los parámetros para la configuración de la VLAN de voz en un puerto

Parámetro	Descripción	Valor predeterminado
VLAN de voz	Con base en las diferentes maneras en las que se puede habilitar la función de VLAN de voz en un puerto, esta puede funcionar en modo auto o manual: ● **Modo automático:** en este modo, el dispositivo revisa si las VLAN de autorización de un puerto contienen a la VLAN de voz, después de habilitar la función VLAN de voz en dicho puerto. De ser así, el dispositivo elimina la VLAN de voz de las VLAN de autorización del puerto hasta que este recibe el paquete de voz conteniendo el OUI especificado. Luego, el dispositivo añade automáticamente la VLAN de voz a las VLAN de autorización del puerto. Si el puerto no recibe un paquete de voz conteniendo el OUI especificado, dentro del tiempo de envejecimiento, el dispositivo elimina la VLAN de voz de las VLAN de autorización del puerto. ● **Modo manual:** si las VLAN de autorización de un puerto contienen la VLAN de voz, los paquetes de voz pueden transmitirse en la VLAN de voz.	Modo automático
Modo de	Cuando el modo de seguridad se habilita, solo se puede transmitir	Habilitado

Parámetro	Descripción	Valor predeterminado
seguridad	tráfico de voz en la VLAN de voz. El dispositivo revisa la dirección MAC de origen en cada paquete. Cuando la dirección MAC de origen en el paquete coincide con el OUI de la VLAN de voz, el paquete puede transmitirse en la VLAN de voz. De otro modo, el dispositivo descarta el paquete. Cuando el modo de seguridad se deshabilita, las direcciones MAC de origen de los paquetes no se revisan y todos los paquetes se pueden transmitir en la VLAN de voz.	

Precaución

- El modo VLAN de voz en el puerto se puede configurar en modo auto solo cuando el puerto se configura como troncal. Cuando la VLAN de voz del puerto funciona en modo auto, este sale de la VLAN de voz primero y se añade automáticamente a esta solo después de recibir datos de voz.
- Cuando la función de VLAN de voz quede habilitada en un puerto, no cambie el modo de Capa 2 (modo troncal o de acceso) del puerto para garantizar su operación normal. Si requiere cambiar el modo de Capa 2 del puerto, primero deshabilite la función VLAN de voz en el puerto.
- No se recomienda la transmisión de datos de servicio ni de voz a través de la VLAN de voz. Para transmitir tanto datos de voz como de servicio en la VLAN de voz, deshabilite la función VLAN de voz en el modo de seguridad.
- La función VLAN de voz no está disponible para puertos de Capa 3 o agregados.

18.6 Configuración de la función Smart Hot Standby (VCS)

La función Smart Hot Standby (espera en caliente inteligente) permite que varios switches actúen como dispositivos con espera en caliente entre sí, garantizando así el reenvío ininterrumpido de datos en caso de que se produzca un fallo en un único punto.

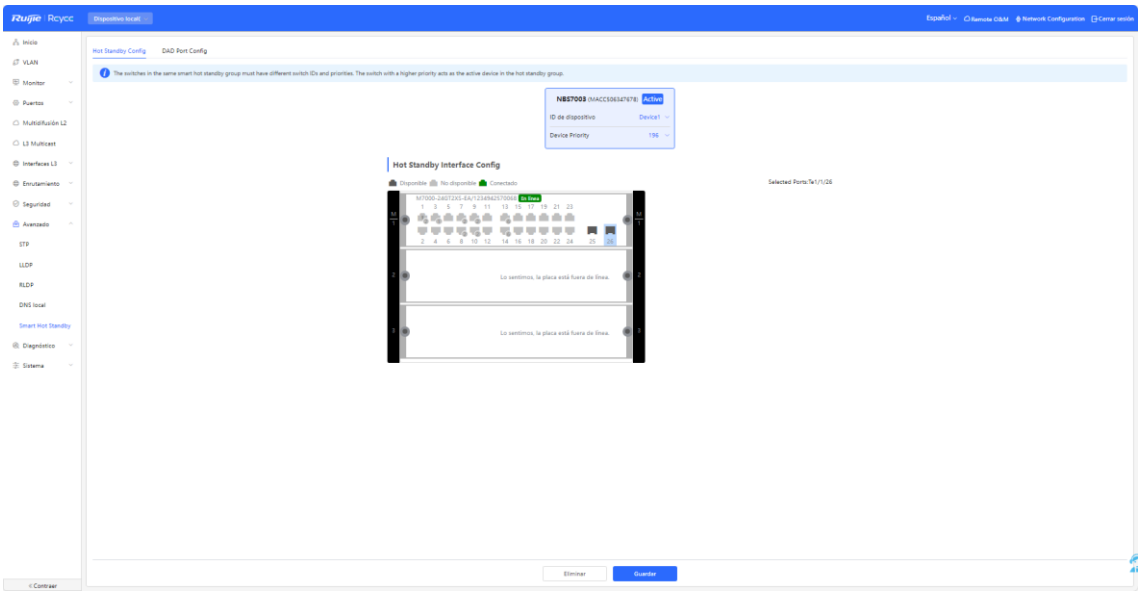
18.6.1 Configuración de la función de espera en caliente

Vea o modifique las interfaces con espera en caliente que haya seleccionado, los ID de dispositivo y las prioridades. El switch cuya prioridad sea mayor se selecciona como switch activo en un grupo con espera en caliente.

Precaución

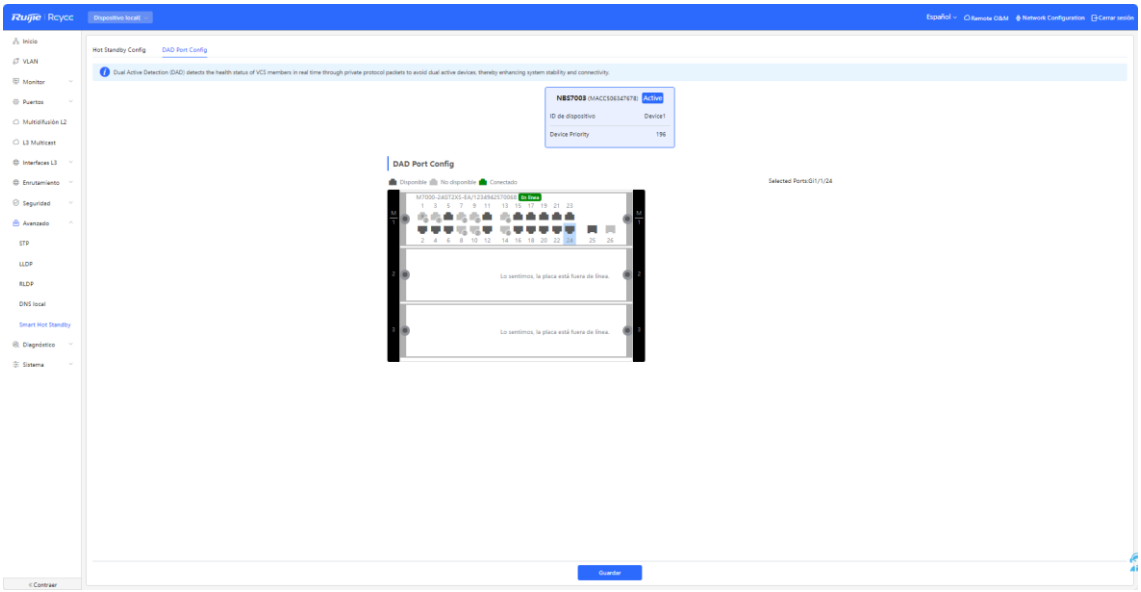
Los dispositivos de los grupos con espera en caliente deben tener configurados un ID de dispositivo y una prioridad únicos.

Seleccione **Dispositivo local** > **Avanzado** > **Smart Hot Standby.**



18.6.2 Configuración de las interfaces DAD

Tras seleccionar las interfaces DAD de los switches activo y en espera, conecte dichas interfaces DAD mediante un cable de red para evitar que se produzcan fallos de red a causa de la duplicación de los dispositivos activos.

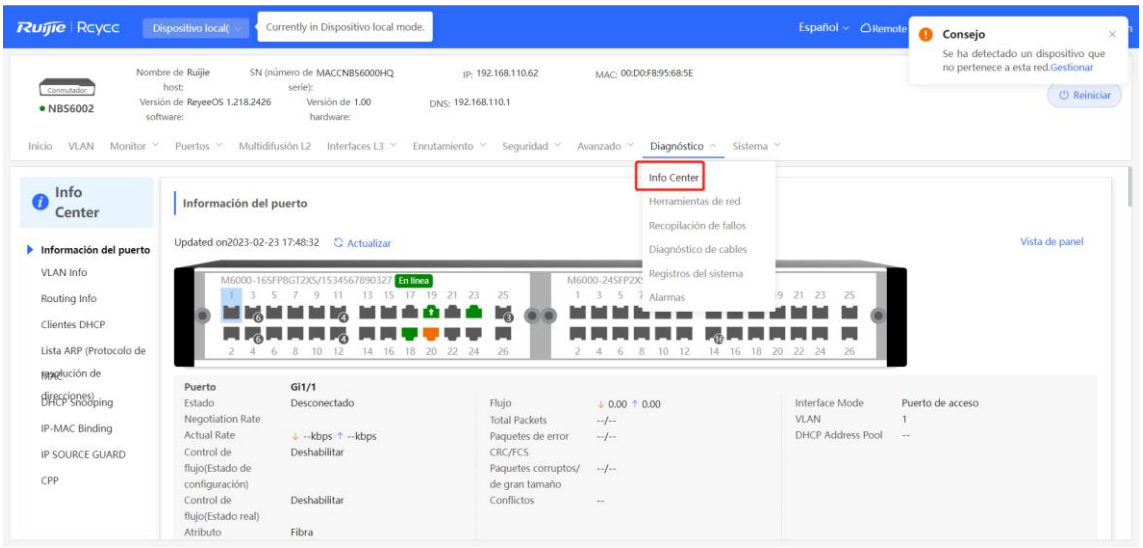


19 Diagnóstico de los switches de las series NBS y NIS

19.1 Centro de información

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center**.

En la sección **Info Center**, se puede visualizar el tráfico del puerto, la información de la VLAN, la información del enrutador, la lista de clientes, la lista ARP, la dirección MAC, la inspección DHCP, el enlace IP-MAC, la protección de origen IP y las estadísticas CPP del dispositivo y sus configuraciones.



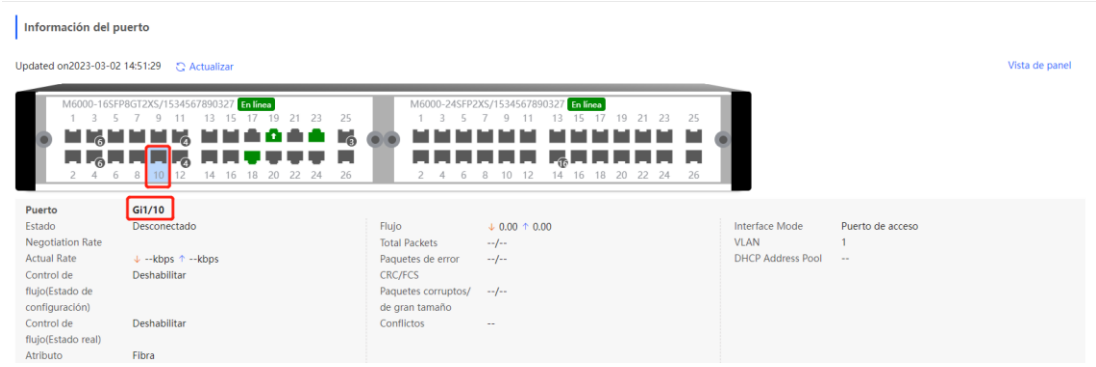
19.1.1 Información del puerto

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center** > **Información del puerto**.

La **Información del puerto** muestra el estado y la configuración del puerto. Haga clic en el ícono del puerto para visualizar su información detallada.

Nota

- Para configurar el control de flujo del puerto o el atributo óptico o eléctrico de un puerto combo, consulte 12.2 Configuración del puerto
- Para configurar el modo Capa 2 del puerto y la VLAN a la que pertenece, consulte 11.6.3 Configuración de un puerto VLAN



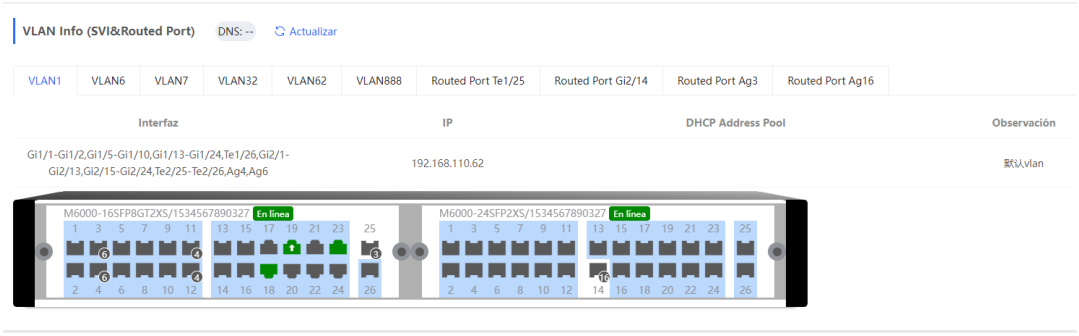
19.1.2 Información de la VLAN

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center** > **VLAN Info**.

La página **VLAN Info** muestra la información del puerto SVI y puerto enrutado, incluyendo la información del puerto incluida en la VLAN, la dirección IP del puerto y si la dirección del pool de DHCP está habilitada.

Nota

- Para configurar la VLAN, consulte 11.6 VLAN
- Para configurar los puertos SVI y los puertos enrutados, consulte 15.1 Configuración de una interfaz de Capa 3



19.1.3 Información del enrutamiento

Precaución

Si el dispositivo no admite funciones de Capa 3 (como los conmutadores de las series RG-NBS3100 y RG-NBS3200), este tipo de información no se mostrará.

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center** > **Routing Info**.

La página **Routing Info** muestra la información de enrutamiento en el dispositivo. Se pueden hacer consultas de entradas de los enrutamientos con base en las direcciones IP en la barra de búsqueda localizado en la esquina superior derecha.

Nota

Para crear enrutamientos estáticos, consulte 0

Configuración del servidor DHCPv6

19.1.4 Clientes DHCP

Precaución

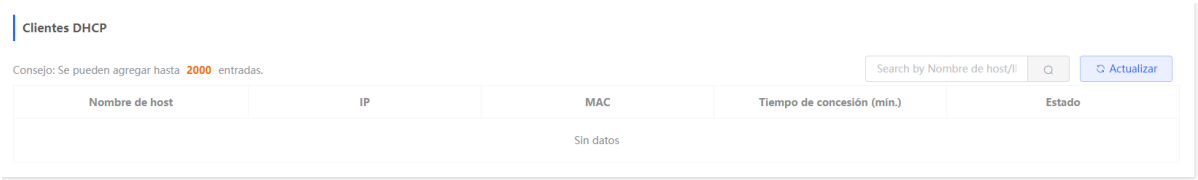
Si el dispositivo no admite funciones de Capa 3 (como los conmutadores de las series RG-NBS3100 y RG-NBS3200), este tipo de información no se mostrará.

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center** > **Clientes DHCP**.

La página **Clientes DHCP** muestra las direcciones IP asignadas a terminales por el dispositivo usado como servidor DHCP.

Nota

Para configurar las funciones del servidor DHCP, consulte 15.2 Configuración de la dirección IPv6 para la interfaz L3.



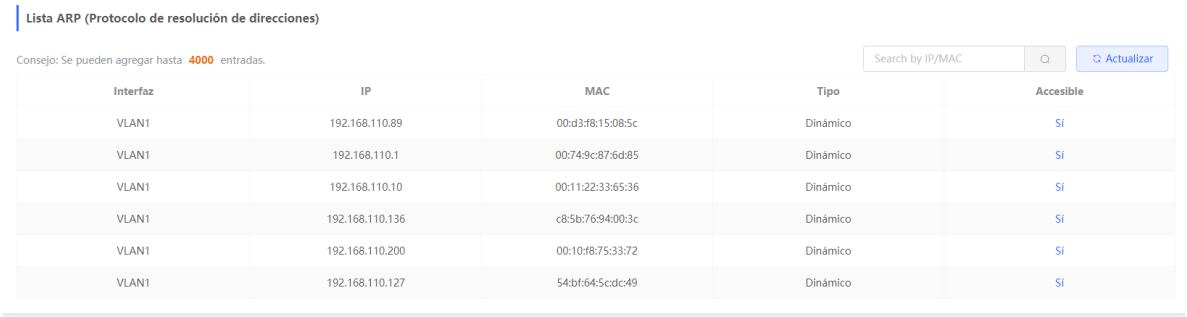
19.1.5 Lista ARP

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center** > **Lista ARP**.

La página **Lista ARP** muestra la información de ARP en el dispositivo, incluyendo las entradas del mapeo ARP dinámicamente aprendidas y estáticamente configuradas.

Nota

Para enlazar las entradas del mapeo ARP o configurarlas manualmente, consulte 6.4.



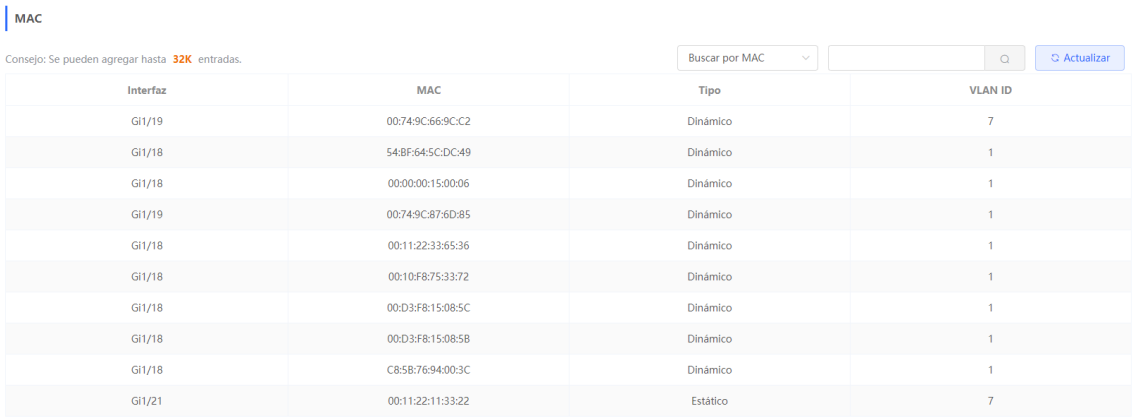
19.1.6 Dirección MAC

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center > MAC**.

La página **MAC** muestra la información de la dirección MAC del dispositivo, incluyendo la dirección MAC estática configurada manualmente, la dirección MAC filtrada y la dirección MAC dinámica automáticamente aprendida por el dispositivo.

Nota

Para configurar las funciones de la dirección MAC, consulte 11.3 Gestión de direcciones MAC



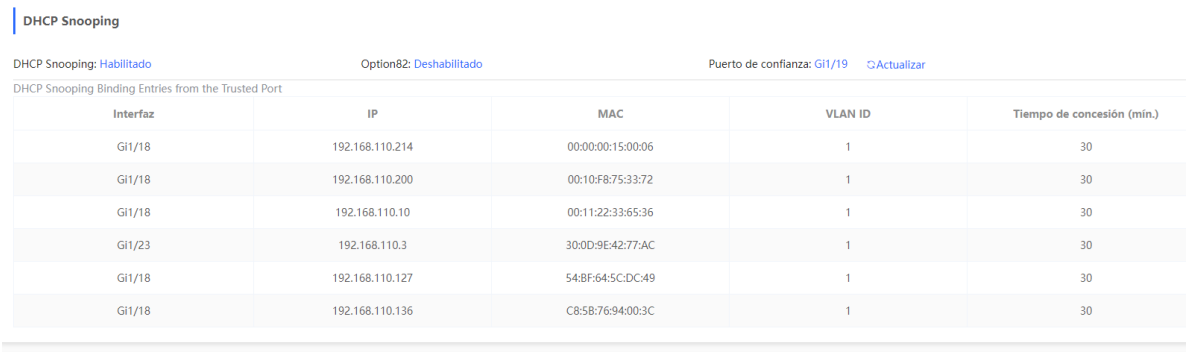
19.1.7 Inspección DHCP

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center** > **DHCP Snooping**.

La página **DHCP Snooping** muestra la configuración actual de la función de inspección DHCP y la información del usuario aprendida dinámicamente por el puerto de confianza.

Nota

Para modificar la configuración de inspección DHCP, consulte 17.1 Inspección DHCP.



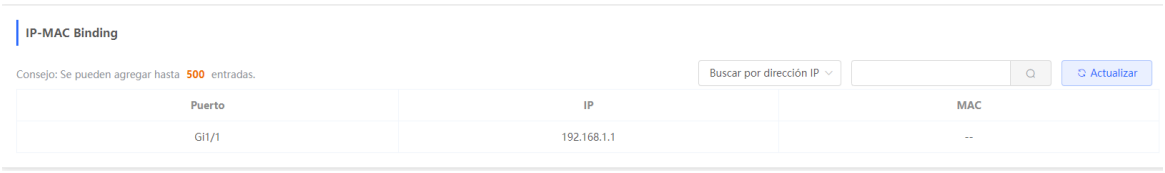
19.1.8 Enlace IP-MAC

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center** > **IP-MAC Binding**.

La página **IP-MAC Binding** muestra las entradas de los enlaces IP-MAC configurados. El dispositivo revisa si las direcciones IP de origen y las MAC de origen de los paquetes IP coinciden con aquellas configuradas en el dispositivo, y filtra las que no coincidan con las entradas de los enlaces.

Nota

Para añadir o modificar los enlaces IP-MAC, consulte 17.5 Enlace IP-MAC



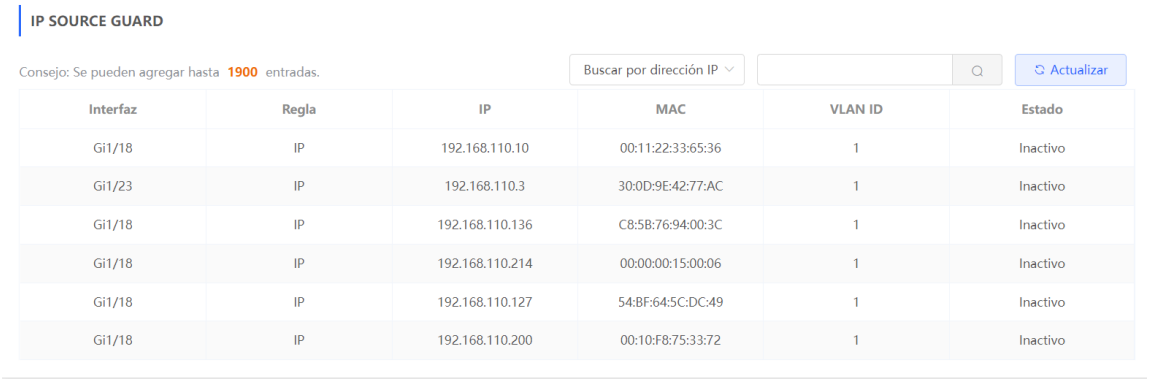
19.1.9 Protección de origen IP

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center** > **IP Source Guard**.

La página de PROTECCIÓN DE ORIGEN IP muestra la lista de enlaces de esta función. La función de protección de origen IP revisará los paquetes IP de los puertos de confianza que no sean DHCP, de acuerdo con la lista, y filtrará aquellos que no se encuentren en ella.

Nota

Para configurar la función de protección de origen IP, consulte 17.6 Protección de origen IP

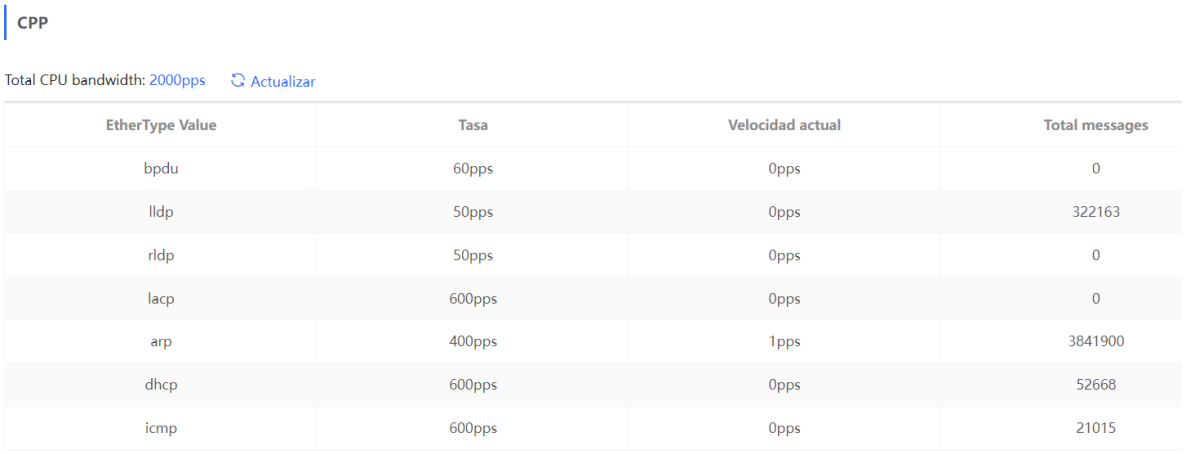


Interfaz	Regla	IP	MAC	VLAN ID	Estado
Gi1/18	IP	192.168.110.10	00:11:22:33:65:36	1	Inactivo
Gi1/23	IP	192.168.110.3	30:0D:9E:42:77:AC	1	Inactivo
Gi1/18	IP	192.168.110.136	C8:5B:76:94:00:3C	1	Inactivo
Gi1/18	IP	192.168.110.214	00:00:00:15:00:06	1	Inactivo
Gi1/18	IP	192.168.110.127	54:BF:64:5C:DC:49	1	Inactivo
Gi1/18	IP	192.168.110.200	00:10:F8:75:33:72	1	Inactivo

19.1.10 Información de la CPP

Seleccione **Dispositivo local** > **Diagnóstico** > **Info Center > CPP**.

La página **CPP** muestra el total actual de ancho de banda del CPU y las estadísticas de diferentes tipos de paquete, incluyendo el ancho de banda, la velocidad actual y el número total de paquetes.



EtherType Value	Tasa	Velocidad actual	Total messages
bpdu	60pps	0pps	0
lldp	50pps	0pps	322163
rldp	50pps	0pps	0
lacp	600pps	0pps	0
arp	400pps	1pps	3841900
dhcp	600pps	0pps	52668
icmp	600pps	0pps	21015

19.2 Herramientas de red

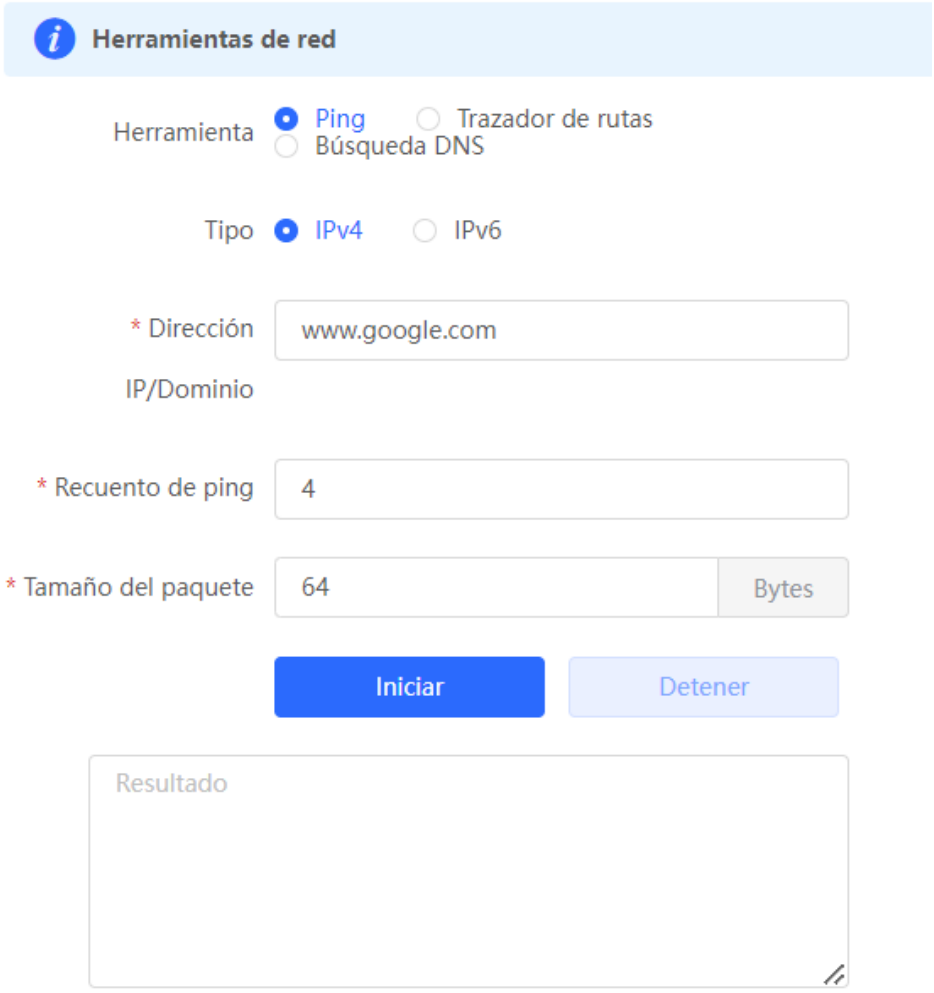
La página de **Herramientas de red** brinda tres herramientas para detectar el estado de la red: **Ping**, **Trazador de rutas** y **Búsqueda DNS**.

19.2.1 Ping

Seleccione **Dispositivo local** > **Diagnóstico** > **Herramientas de red**.

El comando **Ping** se usa para detectar la conectividad de la red.

Seleccione **Ping**, ingrese la dirección IP de destino o dominio, configure el recuento de ping y el tamaño del paquete, y haga clic en **Iniciar** para probar la conectividad de la red entre el dispositivo y la dirección IP o dominio. Si se muestra el mensaje “Ping falló”, la dirección IP o dominio no se localizó.

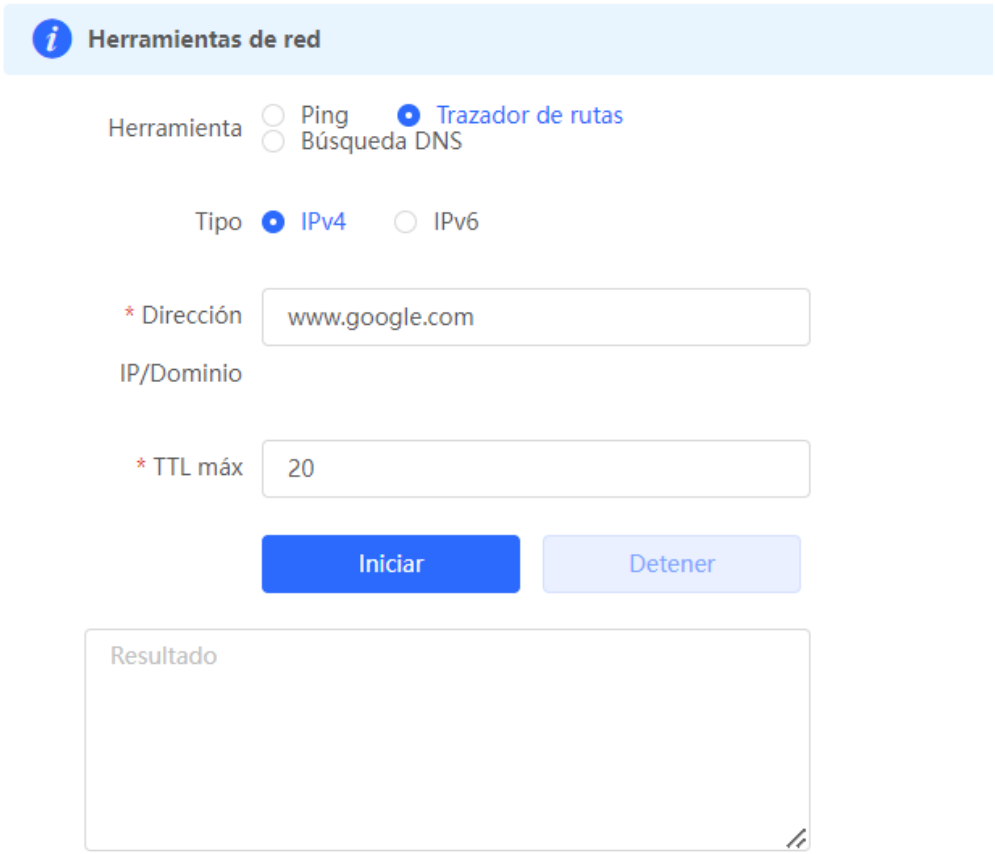


19.2.2 Trazador de rutas

Seleccione **Dispositivo local** > **Diagnóstico** > **Herramientas de red**.

La función **Trazador de rutas** se utiliza para identificar la ruta de la red de un dispositivo a otro. En una red sencilla, los paquetes en la ruta de la red pasan a través de un solo nodo de enrutamiento o de ninguno. En una red compleja, los paquetes pasan a través de docenas de nodos de enrutamiento antes de llegar a su destino. La función Trazador de rutas se puede usar para determinar la ruta de transmisión de paquetes de datos durante la comunicación.

Seleccione **Trazador de rutas**, ingrese la dirección IP de destino o el valor TTL máximo utilizado por el URL y el trazador, y haga clic en **Iniciar**.

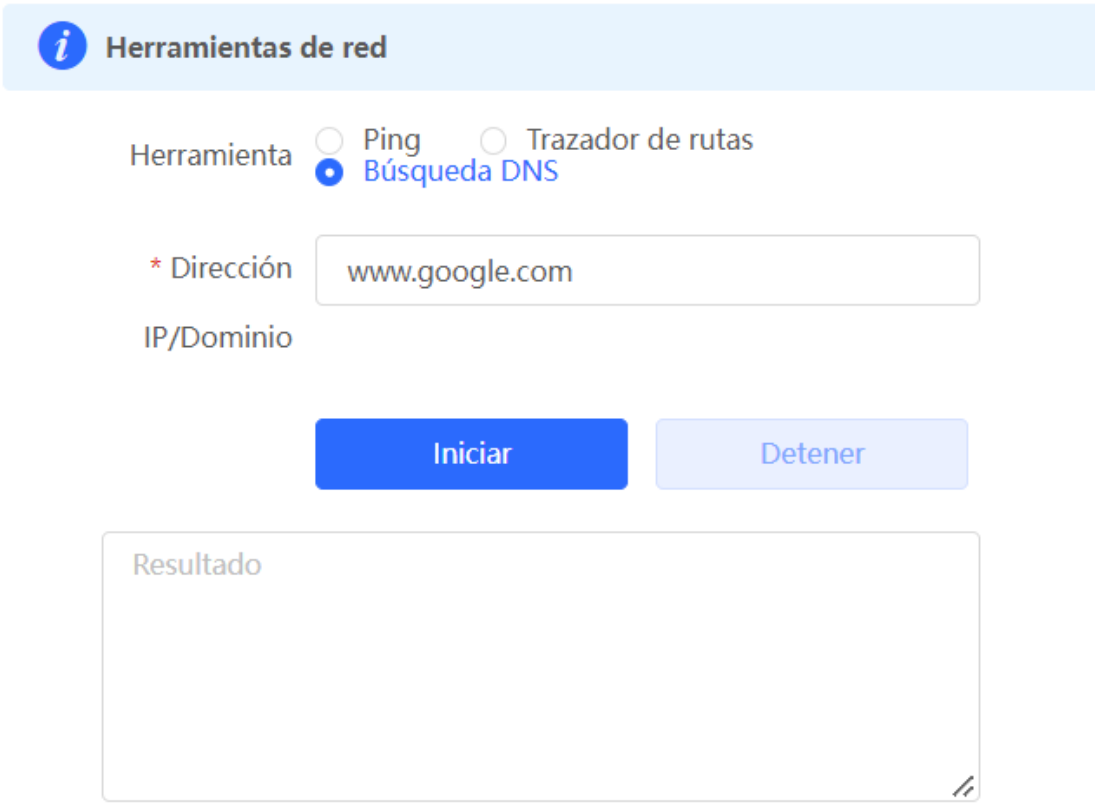


19.2.3 Búsqueda DNS

Seleccione **Dispositivo local** > **Diagnóstico** > **Herramientas de red**.

La búsqueda DNS se utiliza para consultar información del nombre de dominio o para diagnosticar problemas en el servidor DNS. Si el dispositivo puede hacer un ping de la dirección IP de Internet desde su página web, pero el buscador no puede abrirlo, utilice la función de búsqueda DNS para revisar si la resolución del nombre de su dominio es normal.

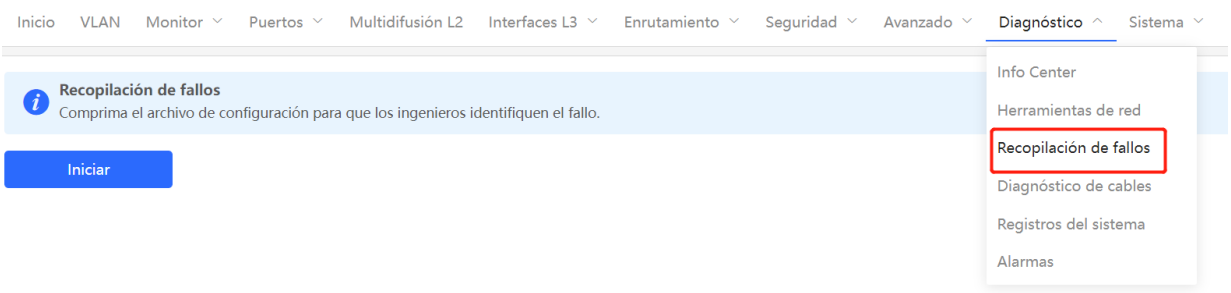
Seleccione **Búsqueda DNS**, ingrese una dirección IP de destino o un URL y haga clic en **Iniciar**.



19.3 Recopilación de fallos

Seleccione **Dispositivo local** > **Diagnóstico** > **Recopilación de fallos**.

Cuando ocurre un fallo en el dispositivo, se puede recopilar información de este con un solo clic. Haga clic en **Iniciar**. Los archivos de configuración del dispositivo se guardarán en un archivo comprimido. Descargue de manera local el archivo comprimido y entréguelo al personal de Investigación y Desarrollo (R&D) para que localicen la falla.

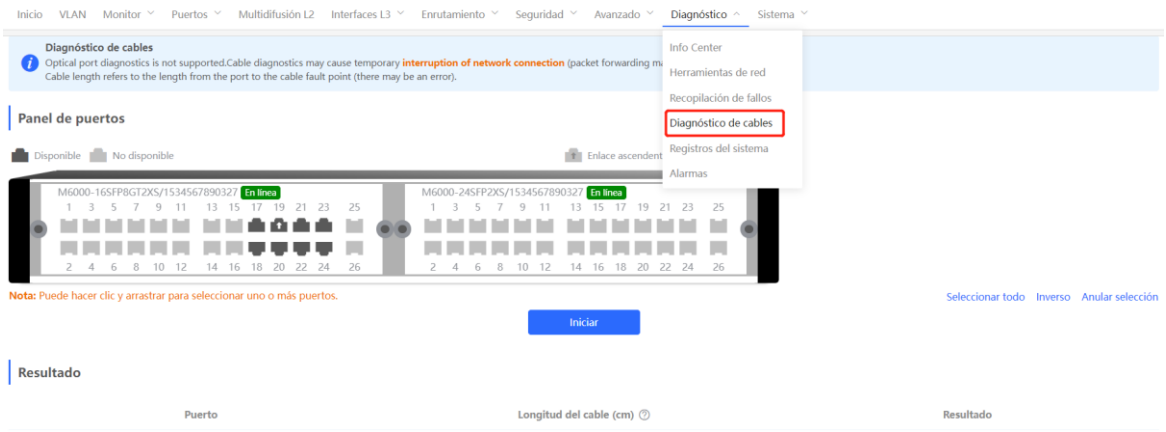


19.4 Diagnóstico de cables

Seleccione **Dispositivo local** > **Diagnóstico** > **Diagnóstico de cables**.

La función de diagnóstico de cables puede detectar la longitud aproximada de un cable conectado a un puerto y si este tiene alguna falla.

Seleccione el puerto a detectar en el panel de puertos y haga clic en **Iniciar**. Los resultados de la prueba se mostrarán abajo.



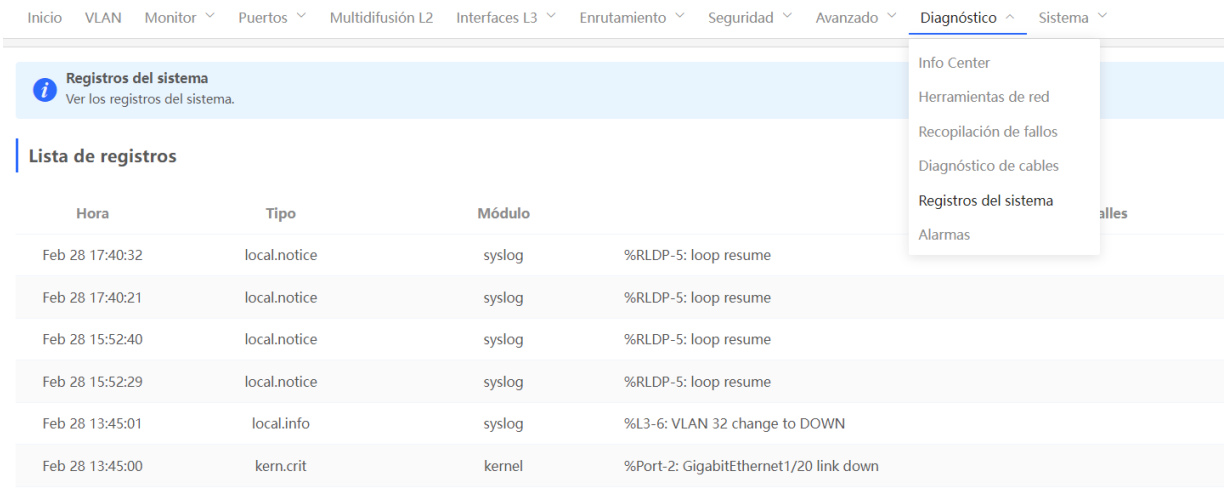
Precaución

- El puerto óptico no admite esta función.
- Si un puerto detectado contiene un puerto de enlace ascendente, es posible que la red se desconecte de manera intermitente. Por lo tanto, actúe con prudencia al realizar esta acción.

19.5 Registros del sistema

Seleccione **Dispositivo local** > **Diagnóstico** > **Registros del sistema**.

Los registros del sistema graban las operaciones del dispositivo, la hora y los módulos. Los registros del sistema se utilizan por un administrador para monitorear el estado de ejecución del sistema y para localizar fallas. Se pueden buscar registros específicos por tipo de falla, el módulo de falla y una palabra clave en la información de la falla.



19.6 Alarmas

Seleccione **Dispositivo local** > **Diagnóstico** > **Alarmas**.

Nota

Seleccione **Red** > **Alarmas** para visualizar la información de las alertas del dispositivo de la red.

La página de **Alarmas** muestra las posibles fallas en el ambiente de la red para facilitar su prevención, así como la localización y resolución de problemas. Se puede visualizar el tiempo en el que ocurre la alerta, el puerto, el impacto y la sugerencia de cómo manejarlo y rectificación de las fallas del dispositivo, de acuerdo con las sugerencias de manejo.

Todos los tipos de alertas se notifican por defecto. Haga clic en **Dejar de seguir** para no continuar recibiendo este tipo de alarmas. El sistema no volverá a mostrarlas. Para habilitar la función de notificación de este tipo de alarmas nuevamente, vuelva a seguir el tipo de alarma que se encuentra en la página **Removed Alert**.

Precaución

Después de dejar de seguir una alarma, el sistema no emite mensajes de alarma para este tipo de fallos. En este caso, las fallas no se pueden manejar a tiempo. Por lo tanto, actúe con prudencia al realizar esta acción.

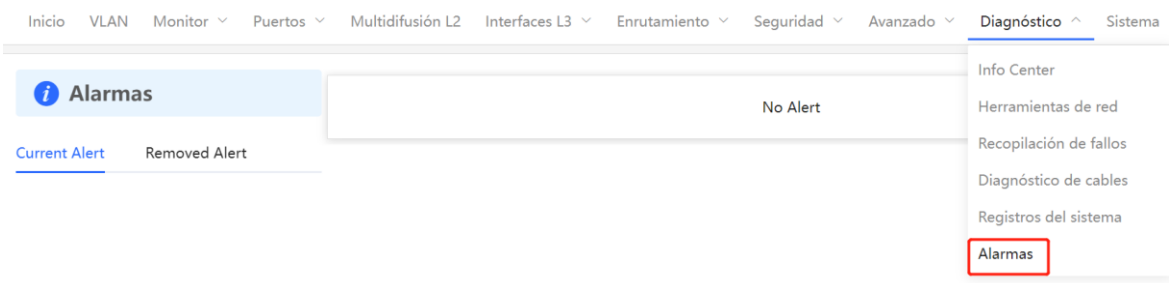


Tabla 19-1 Tipos de alertas y compatibilidad con los productos

Tipo de alerta	Descripción	Observaciones
Las direcciones en el grupo de DHCP deben agotarse.	El dispositivo actúa como servidor DHCP y el número de direcciones asignadas está por alcanzar el número máximo de aquellas que pueden estar en el grupo de direcciones.	Esta función aplica únicamente a los dispositivos que admiten funciones de Capa 3. Los productos como los conmutadores de las series RG-NBS3100 y RG-NBS3200, que no son compatibles con las funciones de Capa 3, no admiten este tipo de alertas.
La dirección IP de un dispositivo local entra en conflicto con otro dispositivo.	La dirección IP de un dispositivo local entra en conflicto con otro cliente de la LAN.	NA

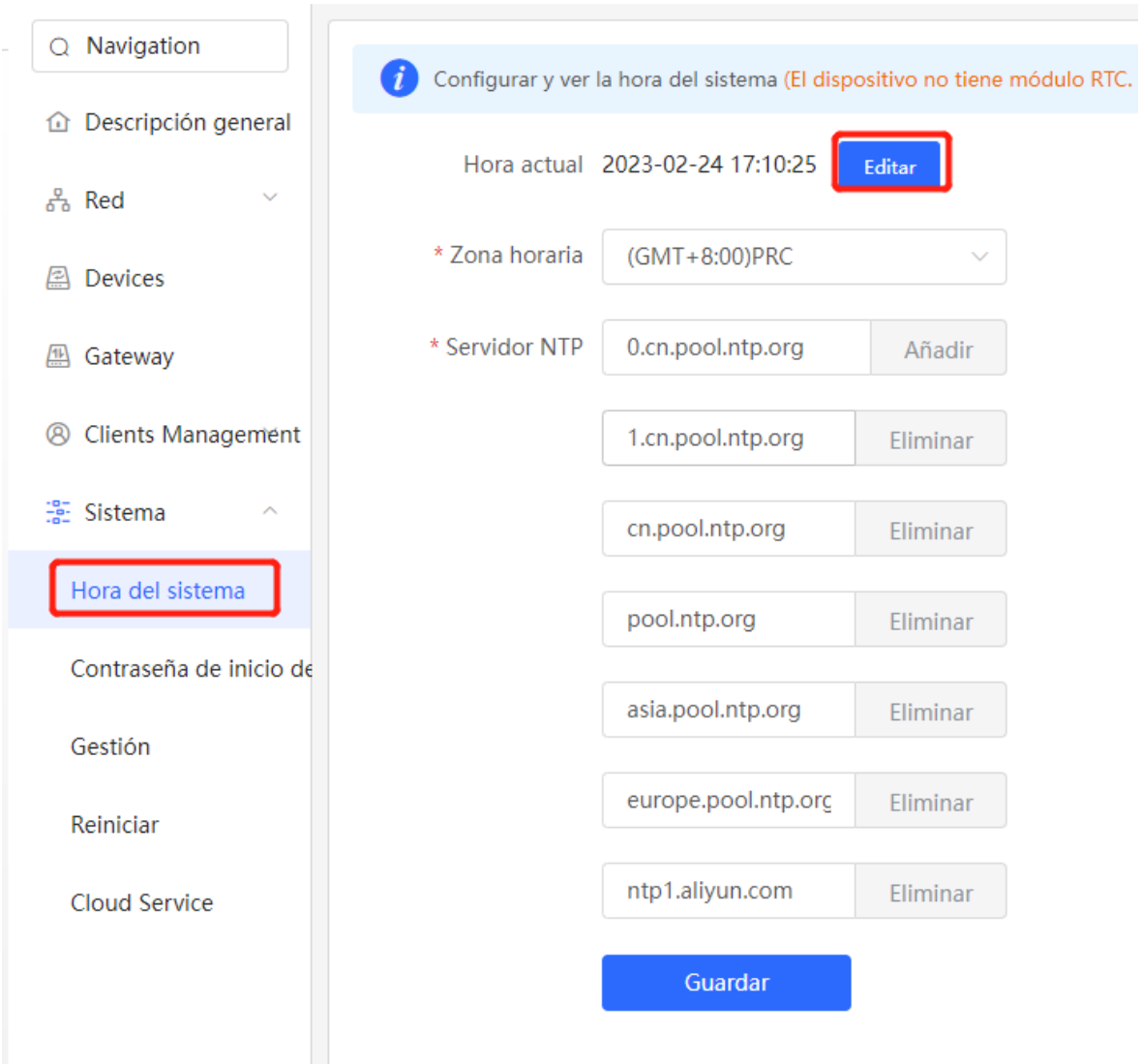
Tipo de alerta	Descripción	Observaciones
Un conflicto de dirección IP ocurre en los dispositivos de enlace descendente conectados al dispositivo.	Entre los dispositivos conectados al dispositivo en la LAN, un conflicto de dirección IP ocurre en uno o más dispositivos.	NA
La tabla de direcciones MAC está llena de entradas.	El número de entradas de direcciones MAC de Capa 2 está por llegar al límite del hardware del dispositivo.	NA
La tabla ARP está llena de entradas ARP.	El número de entradas ARP en la red excede la capacidad ARP del dispositivo.	NA
PoE no se está ejecutando.	La función PoE del dispositivo no está disponible y no puede suministrar alimentación.	Esto aplica únicamente a los conmutadores de la serie NBS que admiten funciones de PoE. (Los modelos de los dispositivos están marcados con "-P").
La potencia total de PoE está sobrecargada.	La potencia total de PoE del dispositivo está sobrecargada y el nuevo PD conectado no puede suministrarle potencia adecuadamente.	Esto aplica únicamente a los conmutadores de la serie NBS que admiten funciones de PoE. (Los modelos de los dispositivos están marcados con "-P").
El dispositivo tiene una alarma de bucle.	Un nuevo bucle ocurre en la LAN.	NA

20 Configuración del sistema de los switches de las series NBS y NIS

20.1 Configuración de la hora del sistema

Seleccione **Networkwide Management > Sistema > Hora del sistema**.

Se puede visualizar la hora actual del sistema. Si la hora es incorrecta, revise y seleccione la zona horaria local. Si la zona horaria es correcta, pero la hora sigue siendo incorrecta, haga clic en **Editar** para establecer la hora manualmente. Además, el dispositivo admite los servidores de Protocolo de hora de red (NTP). Por defecto, varios servidores actúan como respaldo entre ellos. Puede añadir o eliminar el servidor local según lo necesite.



Haga clic en **Hora actual** para modificar la hora. La hora del sistema del dispositivo conectado se pondrá automáticamente.

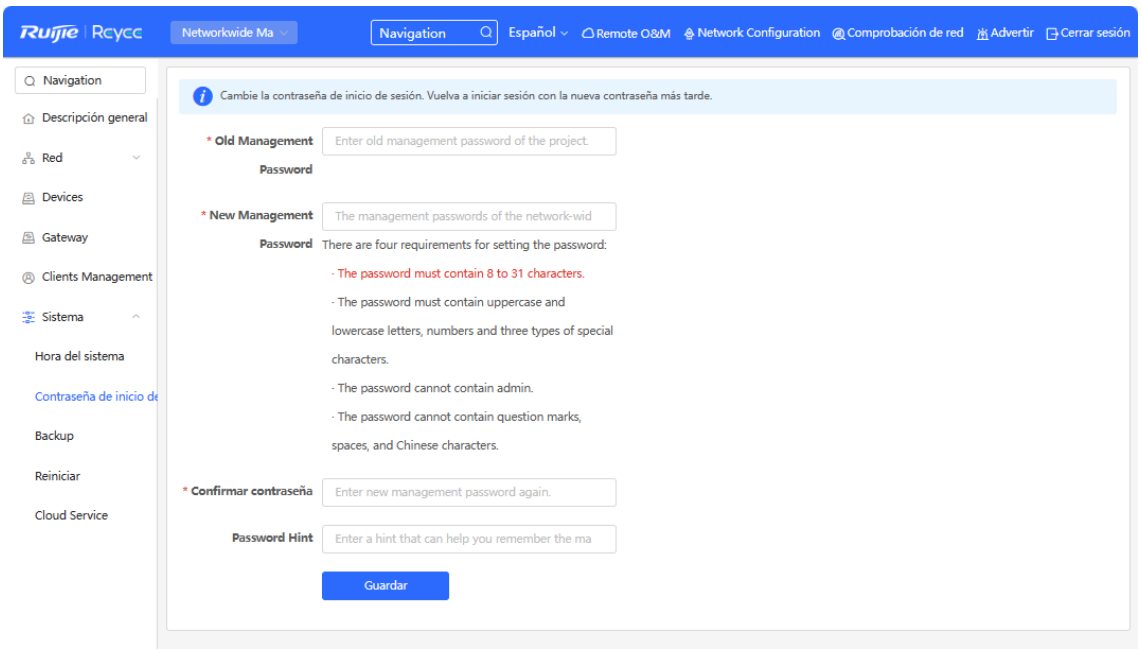
20.2 Configuración de la contraseña de inicio de sesión

Seleccione **Networkwide Management** > **Sistema** > **Contraseña de inicio de sesión**.

Ingrese la contraseña anterior y la contraseña nueva. Cuando haya guardado la configuración, utilice la nueva contraseña para iniciar sesión.

Precaución

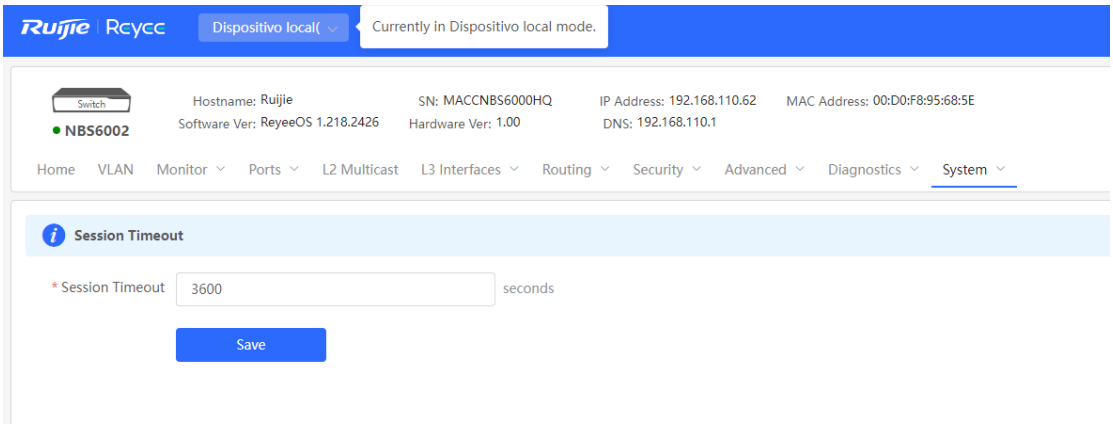
Cuando se habilita la función de descubrimiento de red de autoorganización (SON), la contraseña de inicio de sesión de todos los dispositivos en la red se cambiará de manera sincronizada.



20.3 Configuración del tiempo de duración de una sesión

Seleccione **Dispositivo local > System** > **Login** > **Session Timeout**.

Por defecto, si no cierra una sesión después de iniciarla, el sistema de gestión Eweb le permite continuar teniendo acceso sin autenticación en el buscador actual durante la siguiente hora. Después de transcurrida la hora, el sistema de gestión Eweb actualiza automáticamente la página y debe volver a iniciar sesión para seguir trabajando. El tiempo de duración de la sesión se puede cambiar.



20.4 Configuración del SNMP

20.4.1 Descripción general

El SNMP (protocolo simple de gestión de redes) es un protocolo que se utiliza para gestionar dispositivos de red. Este protocolo se basa en el modelo cliente/servidor y permite supervisar y controlar dispositivos de red de forma remota.

El SNMP consiste en una estación de gestión y agentes. La estación de gestión se comunica con los agentes a través del protocolo SNMP para obtener información como el estado de los dispositivos, información de las configuraciones, datos de rendimiento, etc., a la vez que permite configurar y gestionar los dispositivos.

Además, el SNMP puede utilizarse para gestionar distintos dispositivos de red, como routers, switches, servidores, firewalls, etc. Los usuarios pueden utilizar la interfaz de configuración del SNMP para gestionar usuarios y el software de terceros para supervisar y controlar los dispositivos.

20.4.2 Global Config

1. Descripción general

La opción Global Config (Configuración global) permite habilitar los servicios SNMP y aplicar configuraciones básicas como la versión del protocolo SNMP (v1/v2c/v3), la configuración del puerto local, la configuración de la ubicación del dispositivo y la configuración de la información de contacto.

SNMPv1: v1 es la versión más antigua del SNMP y se caracteriza por su escasa seguridad, ya que solo admite la autenticación simple de las cadenas de comunidad. La versión v1 presenta algunos defectos, como la transmisión en texto plano de las cadenas de comunidad, por lo que es vulnerable a los ataques y de ahí que no se recomiende su uso en las redes modernas.

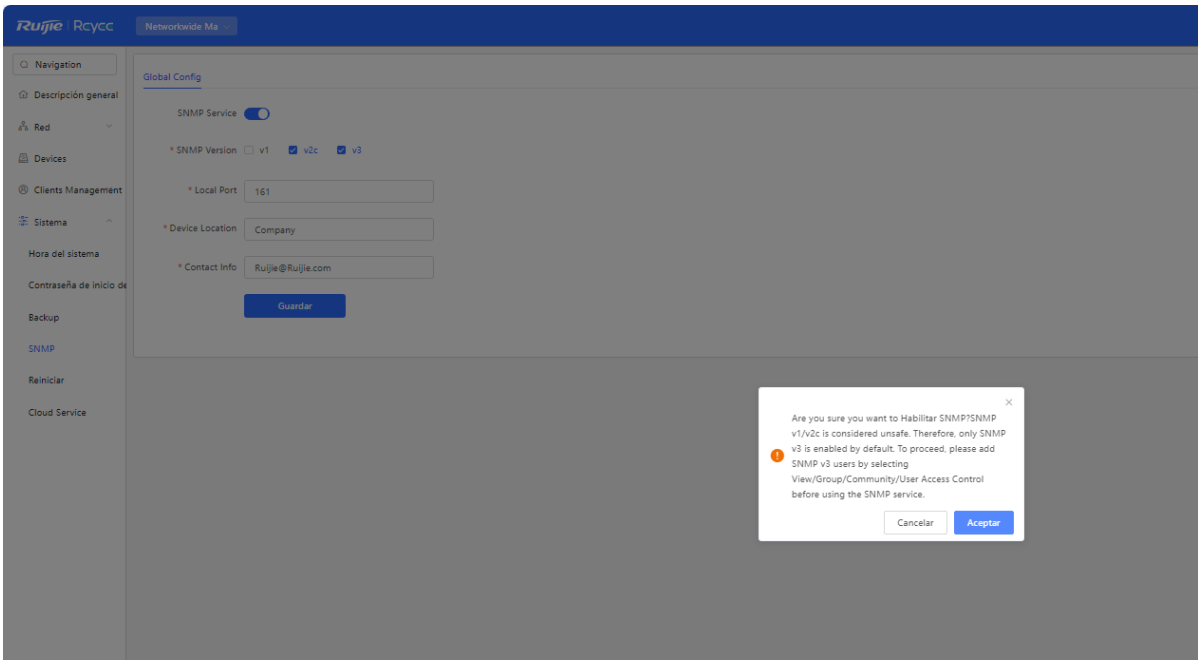
SNMPv2c: la v2c es una versión mejorada con respecto a la v1 que admite una funcionalidad más amplia y tipos de datos más complejos, al mismo tiempo que mejora las medidas de seguridad en comparación con su predecesora. La versión v2c ofrece mejores características de seguridad que la v1 junto con una mayor flexibilidad que permite a los usuarios configurarla según sus necesidades concretas.

SNMPv3: es la última versión del protocolo SNMP e incluye mecanismos de seguridad adicionales como el cifrado de la autenticación de los mensajes en comparación con sus predecesoras, la v1 y la v2, lo que se traduce en mejoras significativas con respecto al control de acceso y las medidas de seguridad generales que utiliza este estándar.

2. Pasos de la configuración:

Networkwide Management > **Sistema** > **SNMP** > **Global Config**

(1) Habilite la opción **SNMP Service**.



Cuando se abre por primera vez, el sistema solicita habilitar el SNMPv3 de forma predeterminada. Haga clic en **Aceptar**.

(1) Establezca los parámetros de la configuración global para el servicio SNMP.

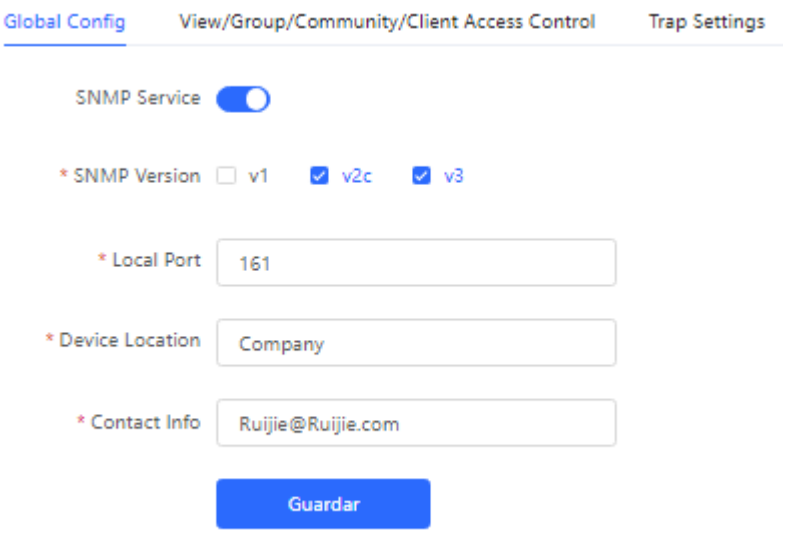


Tabla 20-1 Tabla descriptiva de la opción Configuración global

Parámetro	Parámetro
SNMP Service	Permite habilitar la opción **SNMP Service**.
SNMP Version	El número de versión del protocolo SNMP incluye las versiones: versión v1, versión v2c y versión v3.
Local Port	[1, 65535]
Device Location	No puede contener caracteres chinos, caracteres de ancho completo, signos de interrogación ni espacios. Longitud de caracteres: 1-64.
Contact Info	No puede contener caracteres chinos, caracteres de ancho completo, signos de interrogación ni espacios. Longitud de caracteres: 1-64.

(2) Haga clic en **Guardar**.

Tras habilitar la opción **SNMP Service**, haga clic en **Guardar** para que se apliquen las configuraciones básicas como el número de versión del protocolo SNMP.

20.4.3 View/Group/Group/Client Access Control

1. View/Group/Group/Client Access Control

La MIB (base de información de gestión) puede considerarse una base de datos con distinta información del estado y datos de rendimiento de los dispositivos de red que contiene un gran número de OID (identificadores de objetos), que se utilizan para identificar diferente información del estado y datos de rendimiento de los dispositivos de red en el protocolo SNMP.

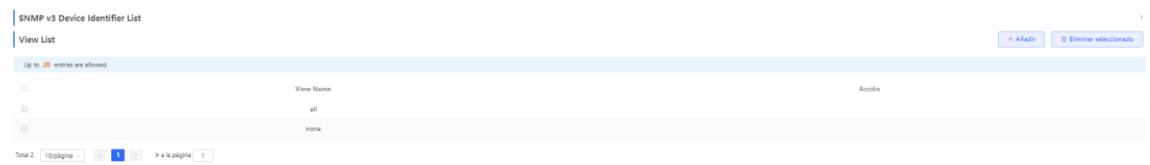
La función de las vistas en el SNMP consiste en limitar el rango de nodos al que pueden acceder los sistemas de gestión en las MIB para mejorar la seguridad y fiabilidad de la gestión de la red. Las vistas constituyen una parte fundamental de la gestión del SNMP que debe configurarse y personalizarse en función de los requisitos específicos de gestión.

Además, las vistas permiten definir distintos subárboles en función de los requisitos al limitar los nodos de las MIB a los que los sistemas de gestión solo pueden acceder dentro de estos subárboles, mientras que los administradores de sistemas no autenticados no pueden acceder a los nodos de las MIB no autorizados para proteger la seguridad de los dispositivos de red. A su vez, las vistas también optimizan la eficacia de la gestión de la red gracias a que mejoran la velocidad de respuesta de los sistemas de gestión.

Pasos de la configuración:

Network-wide Management > Sistema > **SNMP** > **View/Group/Group/Client Access Control** > **View List**

(1) Haga clic en **Añadir** para añadir una vista.



(2) Configure la información básica de la vista.

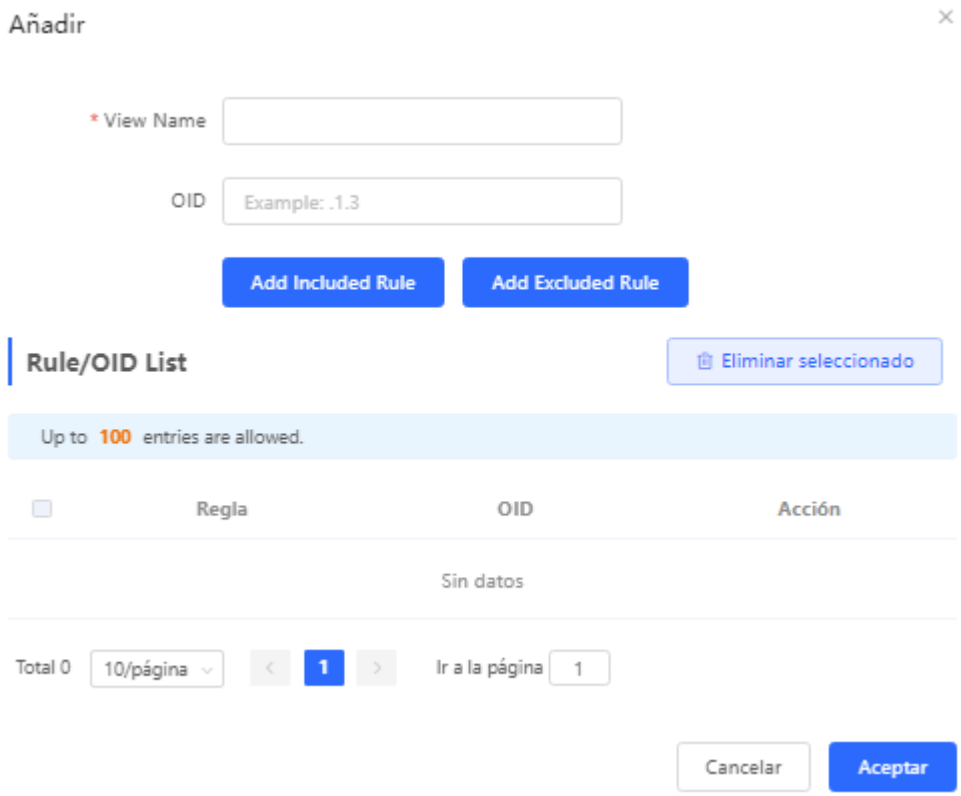


Tabla 20-2 Tabla descriptiva de la información de la configuración de las vistas

Parámetro	Descripción
View Name	El nombre que se utiliza para identificar la vista. La longitud debe ser de 1a 32 caracteres y no puede contener caracteres chinos ni de ancho completo.
OID	Permite el rango de OID incluidos en la vista, que puede ser un único OID o un subárbol de OID.
Add Included Rule o Excluded Rule Add Included Rule Add Excluded Rule	Se divide en reglas de inclusión y reglas de exclusión. Las reglas de inclusión solo permiten el acceso a los OID que se encuentren dentro del rango de OID. Haga clic en **Add Included Rule** para establecer este tipo de vista. Las reglas de exclusión permiten el acceso a todos los OID excepto al rango de OID. Haga clic en **Add Excluded Rule** para establecer este tipo de vista.

Aviso

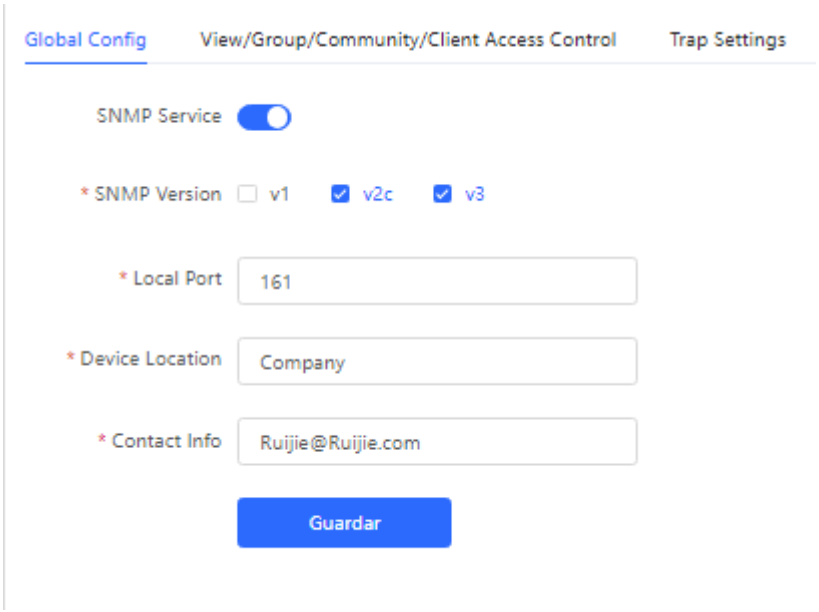
Para la vista que haya creado, añada al menos una regla para el OID. De lo contrario, se mostrará un mensaje de advertencia.

(3) Haga clic en **Aceptar**.

2. Configuración de usuarios v1/v2c

- Introducción

  Cuando la versión del protocolo SNMP se establece en v1/v2c, debe configurar el usuario.



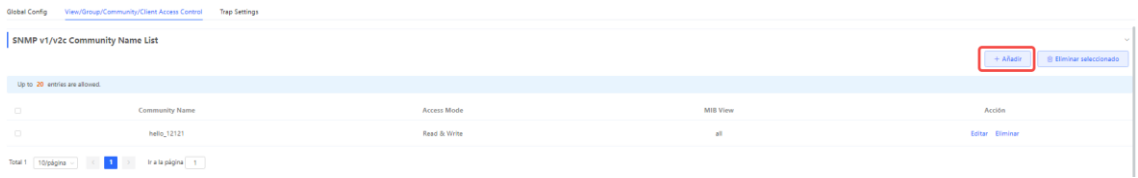
Nota

Seleccione la versión del protocolo SNMP, haga clic en **Guardar** para que se muestren las opciones de configuración correspondientes en la interfaz **View/Group/Group/User Access Control**.

- pasos de la configuración

Seleccione **Networkwide Management** > **Sistema**> **SNMP**> **View/Group/Community/Client Access Control**.

(1) En la página **SNMP v1/v2c Community Name List**, haga clic en **Añadir**.



(2) Cree usuarios v1/v2.

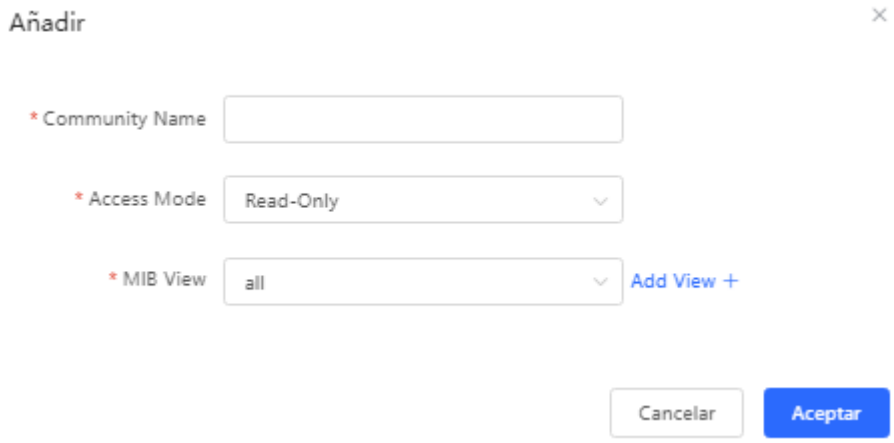


Tabla 20-3 Tabla descriptiva de la información de los usuarios v1/v2

Parámetro	Descripción
Community Name	Debe contener al menos 8 caracteres Debe contener tres tipos de letras mayúsculas, minúsculas, números y caracteres especiales No debe contener admin/público/privado No debe contener signos de interrogación, espacios ni caracteres chinos
Access Mode	Derechos de acceso del nombre de la comunidad (read-only, read-write) Read & Write Read-only
MIB View	Las opciones del cuadro desplegable se aplican a todas las vistas que se hayan configurado (todas las vistas predeterminadas, ninguna).

Aviso
- El nombre de la comunidad no puede repetirse entre usuarios v1/v2c.
- Haga clic en Add View + para añadir una vista.

3. Configuración del grupo v3

- Introducción

El SNMPv3 introduce el concepto de agrupación para mejorar la seguridad y el control de acceso. Un grupo es un conjunto de usuarios del SNMP que comparte la misma política de seguridad y la misma configuración del control de acceso. Mediante el SNMPv3 se pueden configurar varios grupos, cada grupo puede tener su propia política de seguridad y configuración del control de acceso y cada grupo también puede contar con uno o varios usuarios.

- requisitos previos

Cuando la versión del protocolo SNMP se establece en v3, debe configurarse el grupo v3.

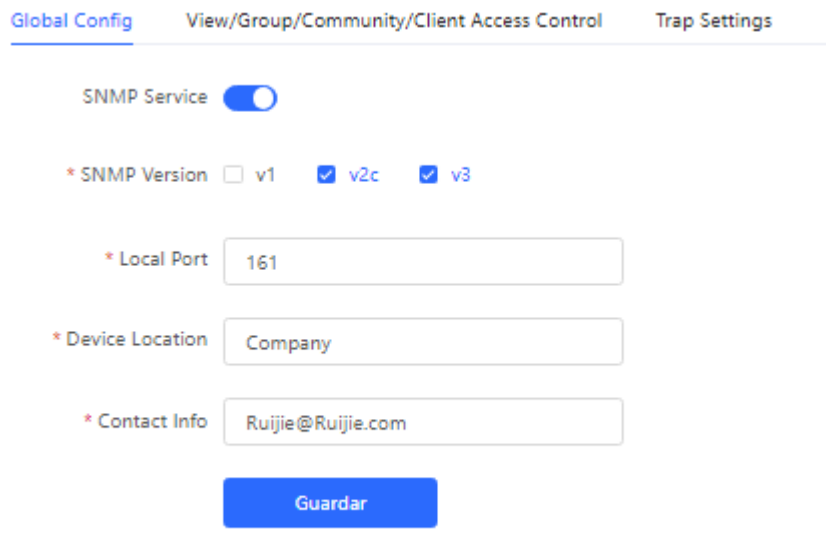
Nota

Seleccione la versión del protocolo SNMP, haga clic en **Guardar** para que se muestren las opciones de configuración correspondientes en la interfaz **View/Group/Group/User Access Control**.

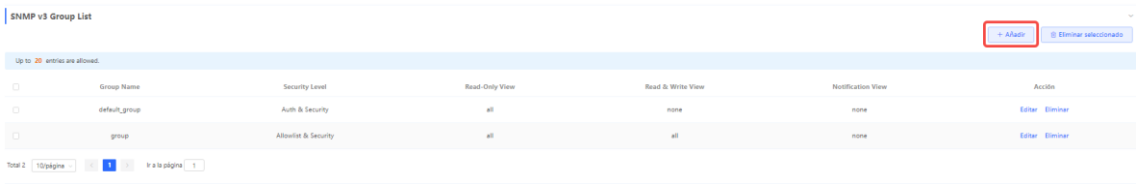
- pasos de la configuración

Network Management > **Setting** > **SNMP** > **View/Group/Group/User Access Control**.

(1) Haga clic en **Añadir** en la página **SNMP v3 Group List** para crear un grupo v3.



(2) Establezca los parámetros correspondientes a los grupos v3.



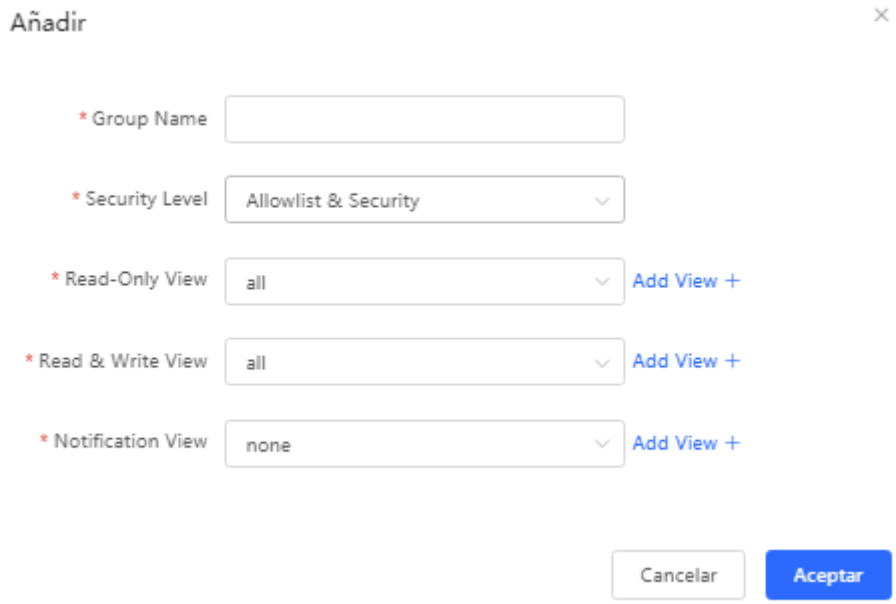


Tabla 20-4 Parámetros de configuración de los grupos v3

Parámetro	Descripción
Group Name	El nombre del grupo de reglas. Puede contener de 1 a 32 caracteres (un caracter chino corresponde a tres caracteres). No puede contener caracteres chinos, caracteres de ancho completo, signos de interrogación ni espacios.
Security Level	El nivel de seguridad mínimo del grupo de reglas (Auth & Security Auth & Open Allowlist & Security authentication with encryption, authentication without encryption, no authentication encryption)
Read-Only View	Las opciones del cuadro desplegable se aplican a todas las vistas que se hayan configurado (todas las vistas predeterminadas, ninguna).
Read & Write View	Las opciones del cuadro desplegable se aplican a todas las vistas que se hayan configurado (todas las vistas predeterminadas, ninguna).
Notification View	Las opciones del cuadro desplegable se aplican a todas las vistas que se hayan configurado (todas las vistas predeterminadas, ninguna).

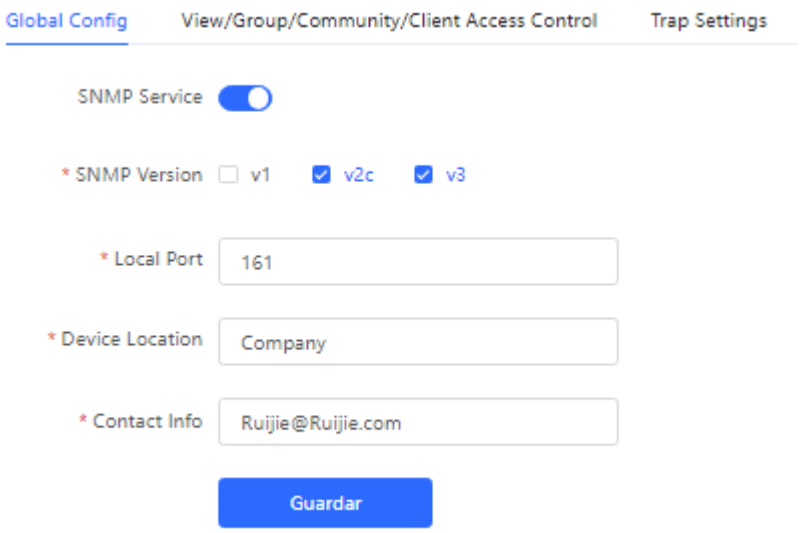
Aviso
- Los grupos limitan el nivel mínimo de seguridad, los permisos de lectura y escritura y el alcance de los usuarios del grupo.
- El nombre del grupo no puede estar repetido. Si necesita añadir una vista, haga clic en **Add View +**.

(3) Haga clic en **Aceptar**.

4. Configuración de usuarios v3

- Introducción
- requisitos previos

Cuando la versión del protocolo SNMP se establece en v3, debe configurarse el grupo v3.



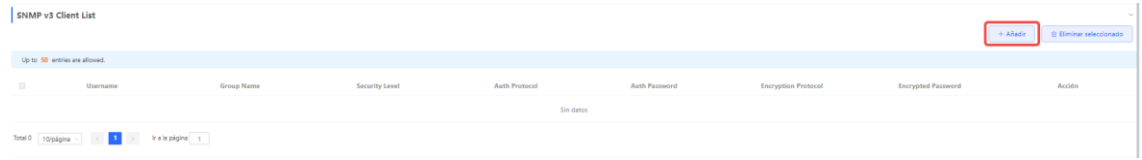
Nota

Seleccione la versión del protocolo SNMP, haga clic en **Guardar** para que se muestren las opciones de configuración correspondientes en la interfaz **View/Group/Group/User Access Control**.

- pasos de la configuración

Network Management > **Setting** > **SNMP** > **View/Group/Group/User Access Control**

(1) En la página **SNMP v3 Client List**, haga clic en **Añadir** para crear un usuario v3.



(2) Establezca los parámetros correspondientes a los usuarios v3.

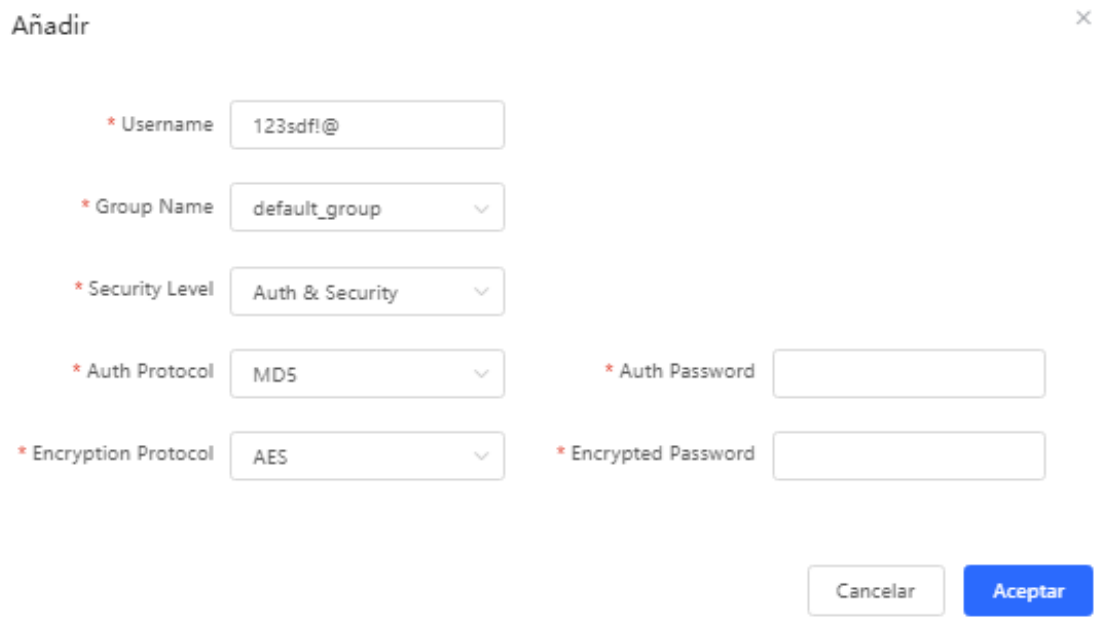


Tabla 20-5 Parámetros de configuración de los usuarios v3

Parámetro	Descripción
Username	Nombre del usuario. Debe contener al menos 8 caracteres Debe contener tres tipos de letras mayúsculas, minúsculas, números y caracteres especiales No debe contener admin/público/privado No debe contener signos de interrogación, espacios ni caracteres chinos
Group Name	El grupo del usuario.
Security Level	Indica el nivel de seguridad del usuario (authentication and encryption, authentication without encryption, no authentication and encryption).
Auth Protocol, Auth Password	Los protocolos de autenticación incluyen: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Auth Password: 8 a 31 caracteres de longitud, no puede contener caracteres chinos, caracteres de ancho completo, signos de interrogación ni espacios y debe contener al menos 3 tipos de letras mayúsculas y minúsculas, números o caracteres especiales. Nota: Debe configurar este parámetro cuando la opción **Security Level** se establezca en **Authentication and encryption** o **Authentication without encryption**.

Parámetro	Descripción
Encryption Protocol, Encrypted Password	Los protocolos de encriptación incluyen: DES/AES/AES192/AES256 Encrypted password: la longitud debe ser de 8~ 31 caracteres y no puede contener caracteres chinos, caracteres de ancho completo, signos de interrogación ni espacios. Formato: debe contener al menos 3 tipos de letras mayúsculas y minúsculas, números o caracteres especiales. Nota: Debe configurar este parámetro cuando la opción **Security Level** se establezca en **Authentication and Encryption**.

Aviso

- El nivel de seguridad del usuario v3 debe ser mayor o igual que el nivel de seguridad de este grupo.
- Existen tres niveles de seguridad. Para la opción **Authentication and Encryption** debe configurar el protocolo de autenticación, la contraseña de autenticación, el protocolo de encriptación y la contraseña de encriptación. Para la opción **Authentication without encryption** solo debe configurar el protocolo de autenticación y el protocolo de encriptación. Para la opción **Without authentication and encryption** no se requiere ninguna configuración.

20.4.4 Ejemplos típicos de la configuración del servicio SNMP

1. Configuración del servicio SNMP versión v2c

- escenarios que pueden utilizarse

El usuario solo debe supervisar la información del dispositivo (no necesita establecerla y emitirla) y utiliza la versión v2c para supervisar la información de los datos de los nodos como 1.3.6.1.2.1.1 a través del software de terceros.

- lista de configuración

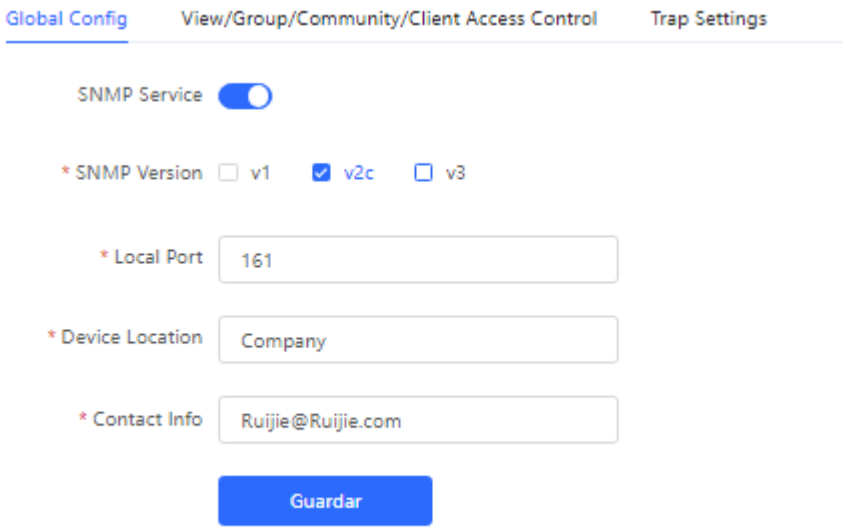
Puede ver los requisitos en la tabla en función del análisis del escenario de uso del usuario:

Tabla 20-6 Formulario de descripción de los requisitos del usuario

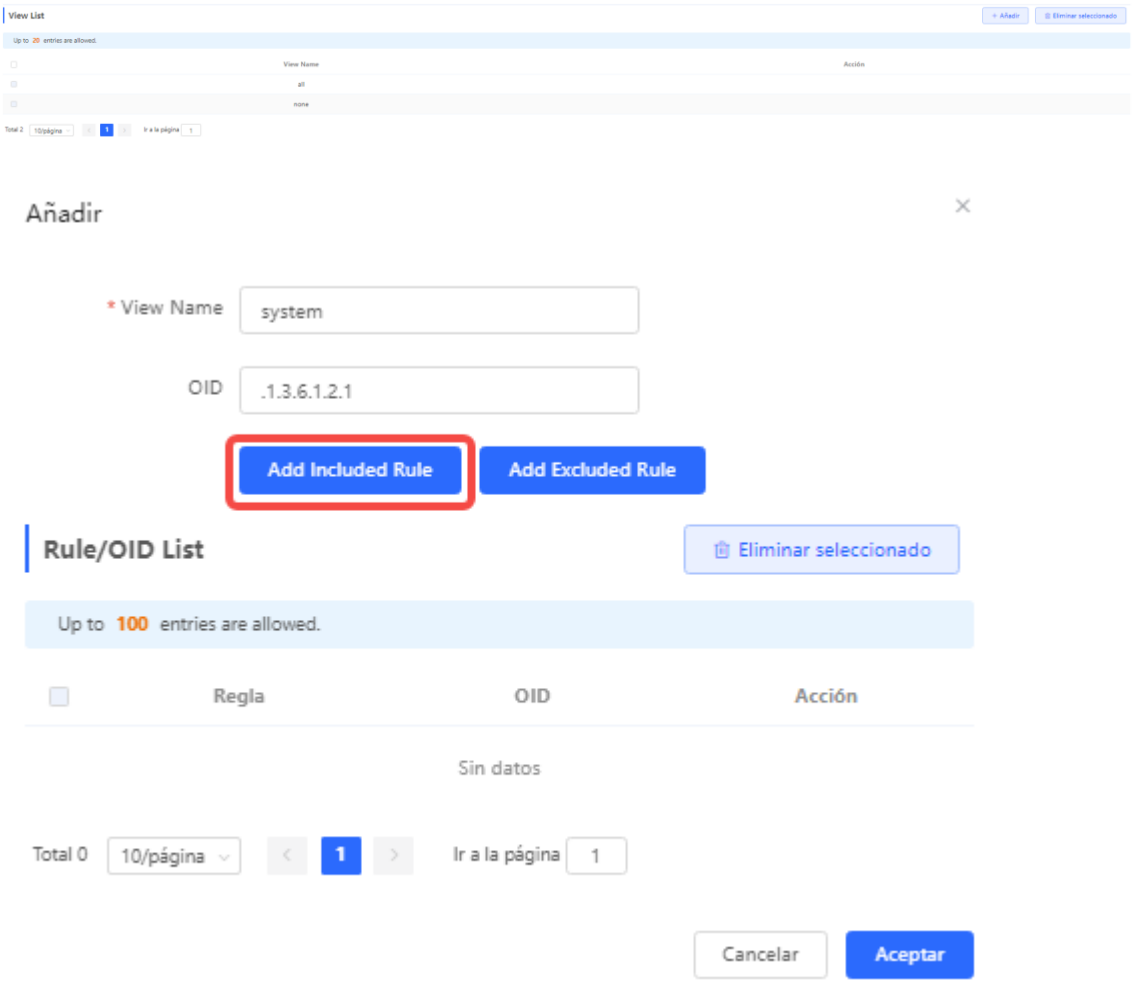
elemento de la descripción	Descripción
Rango de vistas	Regla de inclusión: el OID es el 1.3.6.1.2.1.1 y la vista personalizada se denomina «system».
Número de versión utilizada	La versión v2c. El nombre de la comunidad personalizado es «público» y el número de puerto predeterminado es el 161.
Permisos de lectura y escritura	Permiso de lectura.

- pasos de la configuración

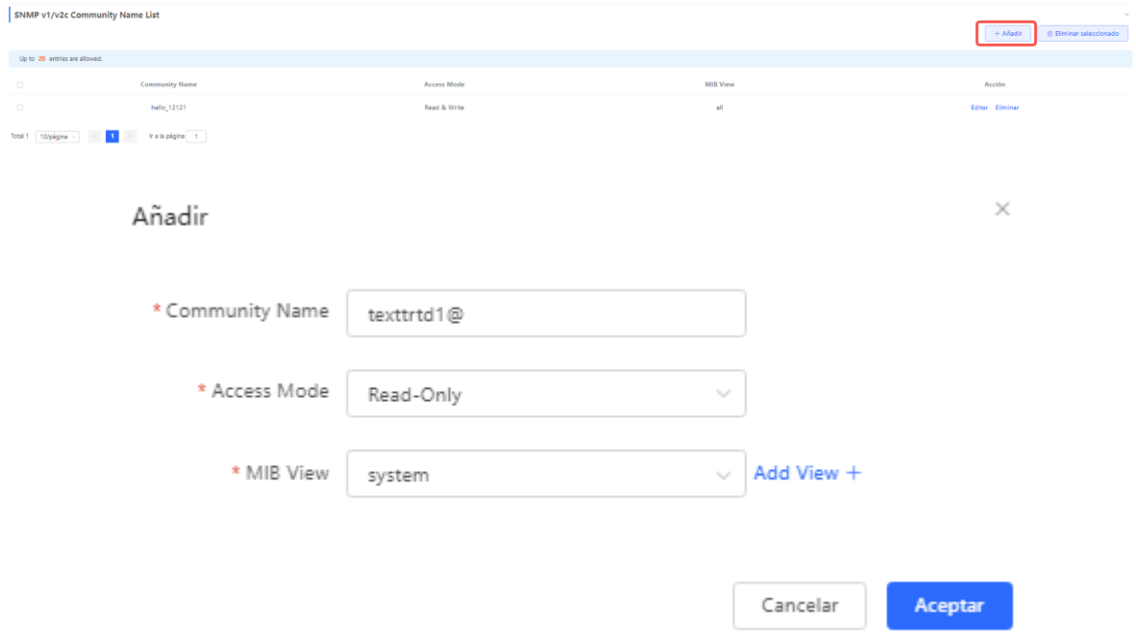
(1) En la interfaz de configuración global, seleccione la versión v2c y deje los demás ajustes tal como aparecen de forma predeterminada. Tras realizar la operación, haga clic en **Guardar**.



(2) En la página **View/Group/Group/User Access Control**, haga clic en **Añadir** en la lista de vistas, introduzca el nombre de la vista y el OID en la ventana emergente, haga clic en **Add included rule** y haga clic en **Aceptar** una vez que se haya realizado la operación.



(3) En la página **View/Group/Group/User Access Control**, haga clic en **Añadir** en la lista de nombres de la comunidad del SNMP v1/v2c, introduzca el nombre de la comunidad, el modo de acceso y la vista en la ventana emergente y haga clic en **Aceptar** tras realizar la operación.



2. Configuración del servicio SNMP versión 3

- escenarios que pueden utilizarse

Los usuarios deben supervisar y controlar los equipos y utilizar la versión v3 del software de terceros para supervisar y enviar datos al nodo público (1.3.6.1.2.1). El nivel de seguridad de la versión v3 utiliza el modo autenticación y encriptación.

- lista de configuración

Puede ver los requisitos en la tabla en función del análisis del escenario de uso del usuario:

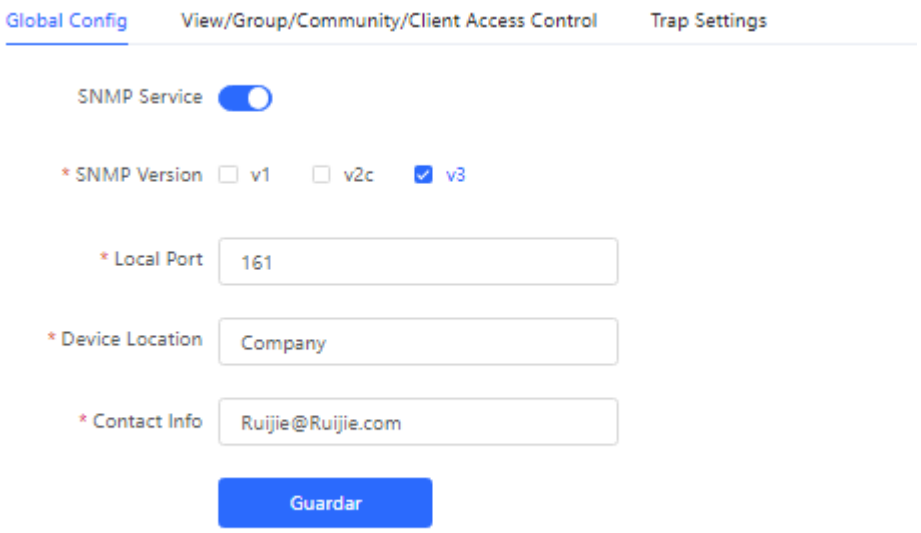
Tabla 20-7 Formulario de descripción de los requisitos del usuario

Parámetro	Descripción
Rango de vistas	Regla de inclusión: el OID es el 1.3.6.1.2.1.1 y la vista personalizada se denomina «public_view».
Configuración del grupo	Group Name: group Security Level Auth & Security En Read-Only View, seleccione «all». En Read & Write View, seleccione «all». En Notification View, seleccione «none».

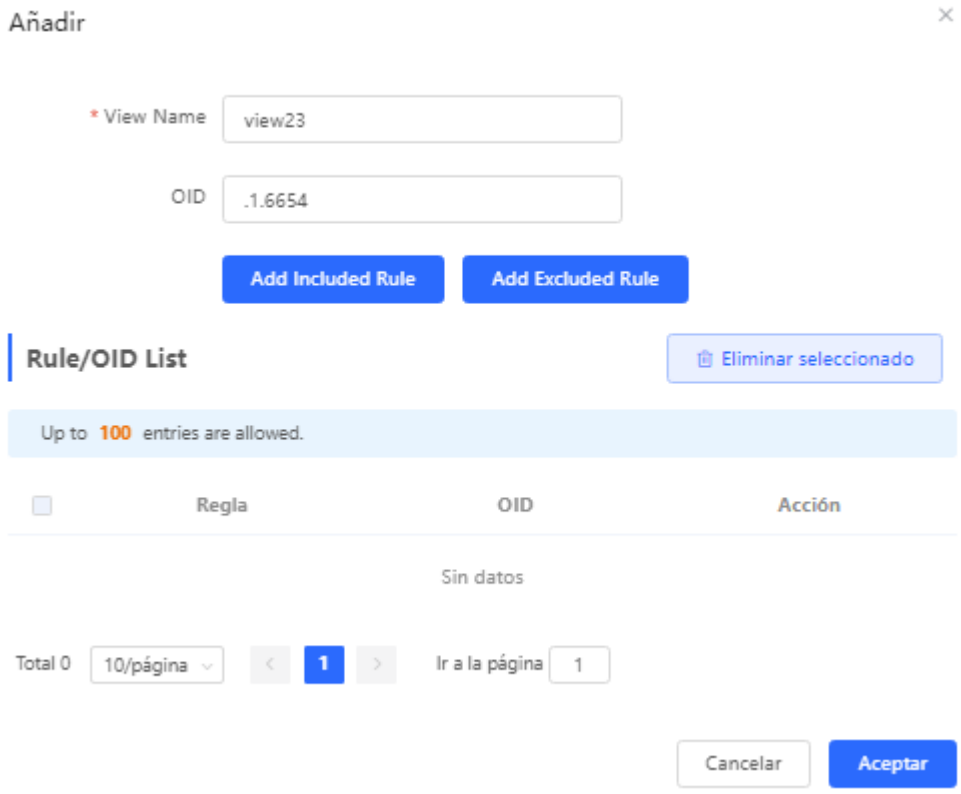
Parámetro	Descripción
Configuración del usuario v3	Username: v3_user Group Name: group Security Level: Auth & Security Auth Protocol/Auth Password: MD5/Ruijie123 Encryption Protocol/Encrypted Password: AES/Ruijie123
Número de versión utilizada	Versión v3, puerto predeterminado 161

- pasos de la configuración

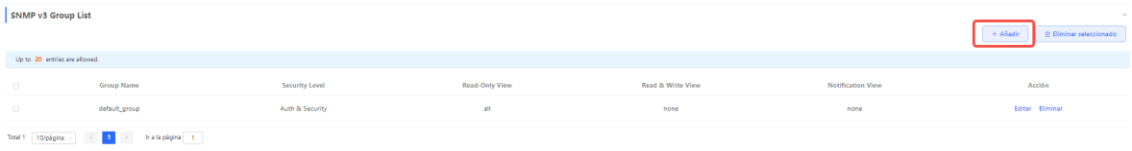
(1) Seleccione la versión v3 en la interfaz de la configuración global, cambie el puerto a 161 y configure el resto de parámetros en los valores predeterminados. Tras realizar la operación, haga clic en **Guardar**.

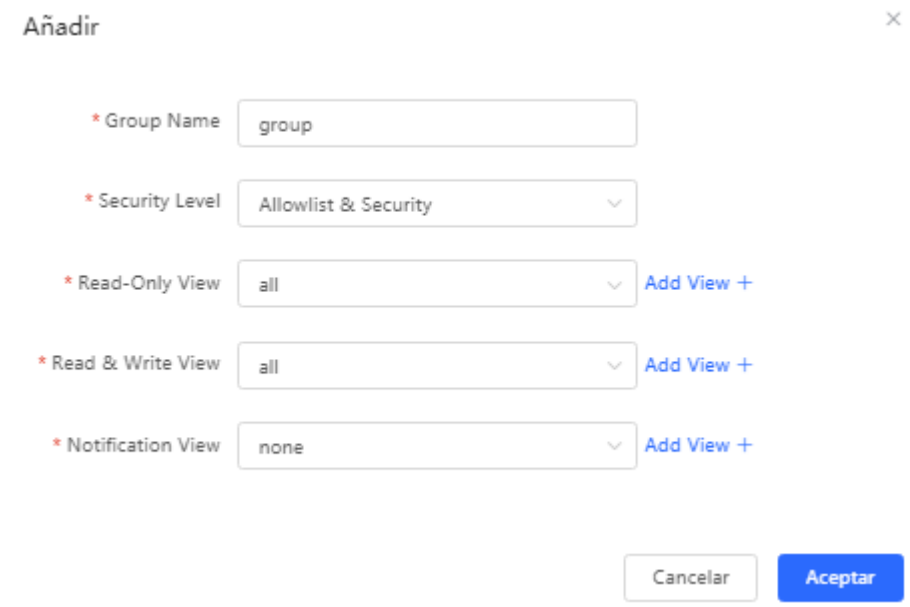


(2) En la página **View/Group/Group/User Access Control**, haga clic en **Añadir** en la lista de vistas, introduzca el nombre de la vista y el OID en la ventana emergente, haga clic en **Add included rule** y haga clic en **Aceptar** una vez que se haya realizado la operación.

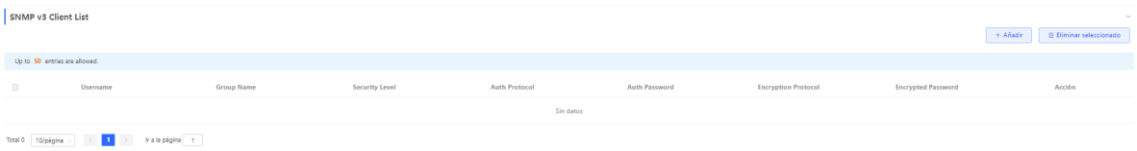


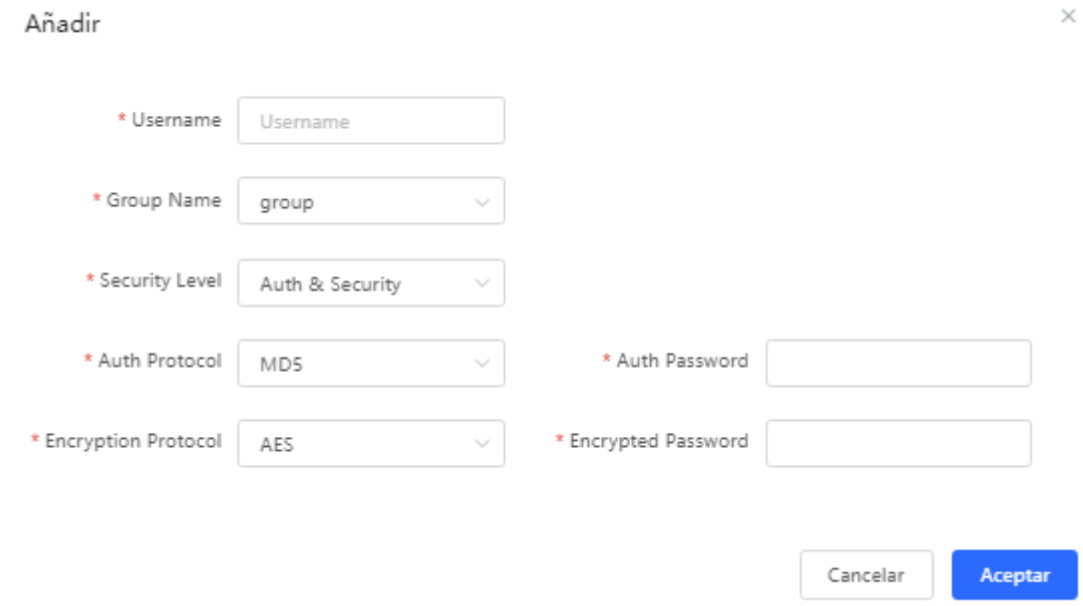
(3) Haga clic en **Añadir** en la lista **SNMP v3 Group List**, introduzca el nombre del grupo y el nivel de seguridad en la ventana emergente (el usuario tiene permisos de lectura y escritura), seleccione la opción «public _view» para la vista de lectura y la vista de lectura y escritura y establezca la vista de notificaciones en «none». Tras realizar la operación, haga clic en **Aceptar**.





(4) Haga clic en **Añadir** en la lista **SNMP v3 Client List**, introduzca el nombre de usuario y el nombre de grupo en la ventana emergente (el nivel de seguridad del usuario es el modo **Auth & Security**), introduzca el protocolo de autenticación (Auth Protocol), la contraseña de autenticación (Auth Password), el protocolo de encriptación (Encryption Protocol) y la contraseña de encriptación (Encrypted Password) correspondientes y haga clic en **Aceptar**.





20.4.5 Configuración del servicio de trampas

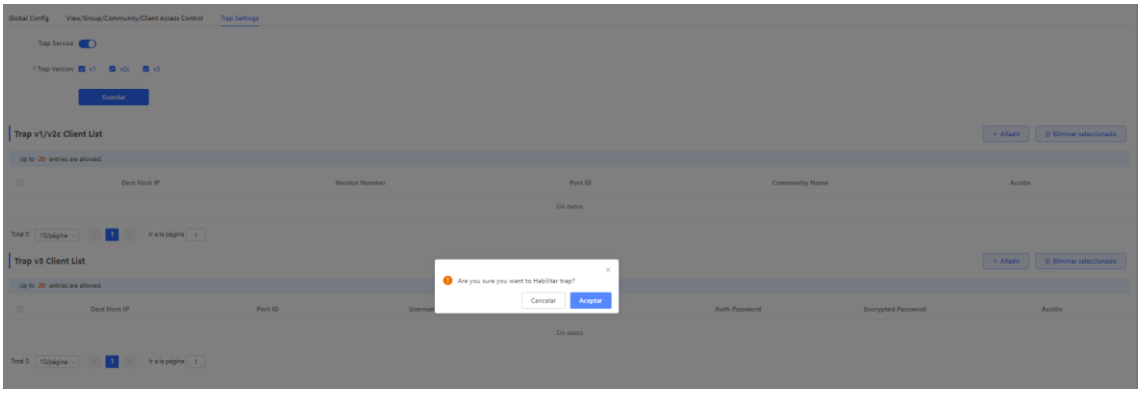
Las trampas son un mecanismo de notificación del protocolo SNMP (protocolo simple de gestión de redes), que se emplea para informar del estado y los eventos de los dispositivos de red a los administradores, incluidos los informes de estado de los dispositivos, los informes de fallos, los informes de rendimiento, los informes de configuración y la gestión de la seguridad. Esta función permite supervisar la red en tiempo real y diagnosticar fallos para ayudar a los administradores a encontrar y resolver a tiempo los problemas de la red.

1. Configuración de las trampas

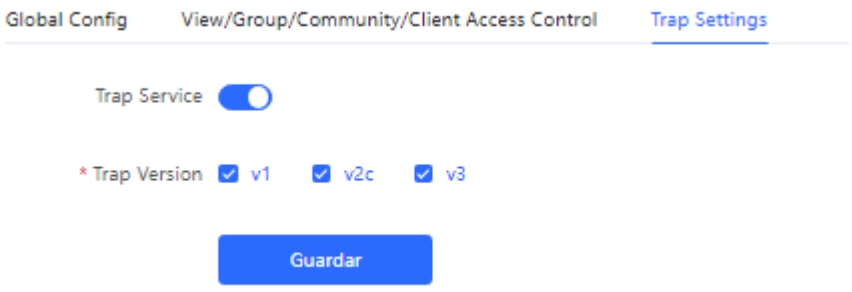
Habilite el servicio de trampas y seleccione la versión actual del protocolo de trampas, entre las que se incluyen las versiones v1, v2c y v3.

Network Management > **Setting** > **SNMP** > **Trap Settings**

(1) Habilite la opción **Trap Service**.



Cuando se habilita por primera vez, el sistema muestra un mensaje de aviso. Haga clic en **Aceptar**.



(2) Establezca la versión de las trampas.

El número de versión del protocolo de trampas incluye las versiones v1, v2c y v3.

(3) Haga clic en **Aceptar**.

Tras habilitar el servicio de trampas, haga clic en **Guardar** para que se aplique la configuración del número de versión del protocolo de trampas.

2. Configuración de usuarios de trampas v1/v2c

- Introducción

Las trampas son un mecanismo de notificación que se utiliza para enviar una alerta a los administradores cuando se producen eventos o fallos importantes en un dispositivo o servicio. Las versiones v1/v2c son dos versiones del protocolo SNMP que se utilizan para gestionar y supervisar la red.

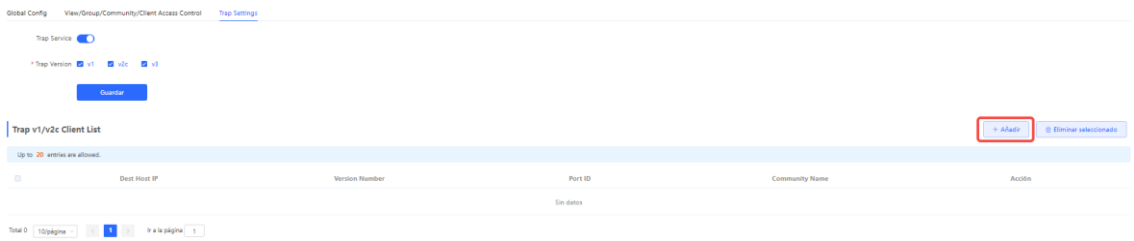
La v1 es la primera versión del protocolo SNMP, que admite funciones básicas de notificación de alarmas, mientras que la v2c es la segunda versión del protocolo SNMP, que admite más opciones de notificación de alarmas y una seguridad más avanzada.

El uso de las versiones v1/v2c del servicio de trampas permite al administrador conocer los problemas de la red a tiempo y adoptar las medidas correspondientes.

- requisitos previos
  Cuando la versión del servicio de trampas se selecciona en v1 o v2c, se debe crear un usuario de trampas v1/v2c.
- funcionamiento de la configuración

Network Management > **Setting** > **SNMP** > **Trap Settings**

(1) Haga clic en **Añadir** en la página **SNMP v1/v2c Client List** para crear un usuario de trampas v1/v2c.



(2) Establezca los parámetros correspondientes a los usuarios de trampas v1/v2c.

configuración

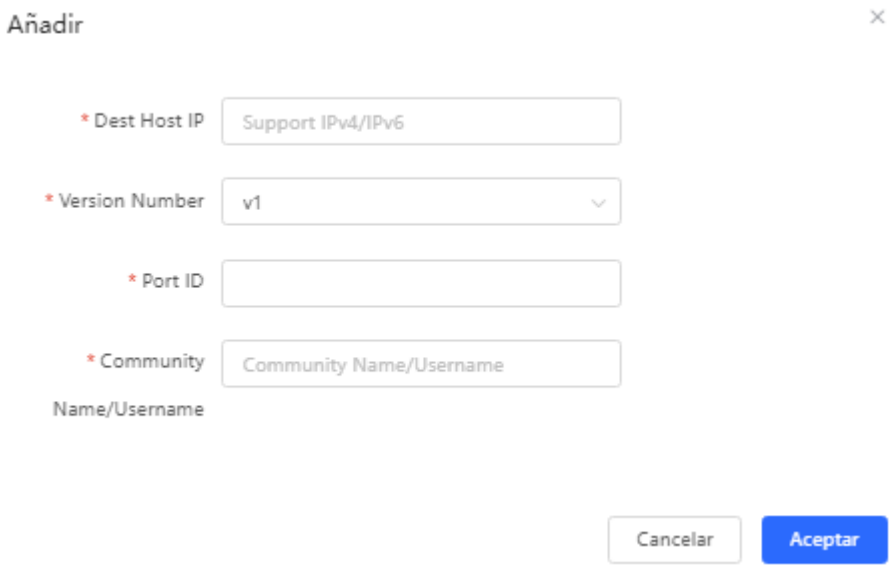


Tabla 20-8 Tabla descriptiva de la información de los usuarios de trampas v1/v2

Parámetro	Descripción
Dest Host IP	La IP del dispositivo homólogo del servicio de trampas (admite direcciones IPv4 e IPv6).
Version Number	El número de versión del servicio de trampas, incluidas las versiones v1|v2c.
Port ID	El puerto del dispositivo homólogo del servicio de trampas [1, 65535].
Community name/Username	El nombre de la comunidad del usuario del servicio de trampas Debe contener al menos 8 caracteres Debe contener tres tipos de letras mayúsculas, minúsculas, números y caracteres especiales No debe contener admin/público/privado No debe contener signos de interrogación, espacios ni caracteres chinos

Aviso
- La dirección IP de los usuarios del servicio de trampas v1/v2c/v3 no puede estar repetida.
- Los nombres de los usuarios del servicio de trampas v1/v2c no pueden estar repetidos.

(3) Haga clic en **Aceptar**.

3. Configuración de usuarios del servicio de trampas v3

- Introducción

El servicio de trampas v3 es un mecanismo de gestión de redes basado en el protocolo SNMP que se utiliza para enviar notificaciones de alarma al personal de gestión. A diferencia de las versiones anteriores, la v3 proporciona opciones de configuración más seguras y flexibles, incluyendo la autenticación y la encriptación.

La versión v3 puede personalizarse para elegir las condiciones y los métodos de envío de las alertas, así como el destinatario de las alertas y la forma de recibir las notificaciones. Esto permite a los administradores conocer el estado de los dispositivos de la red con mayor precisión y adoptar las medidas oportunas para garantizar la seguridad y fiabilidad de la red.

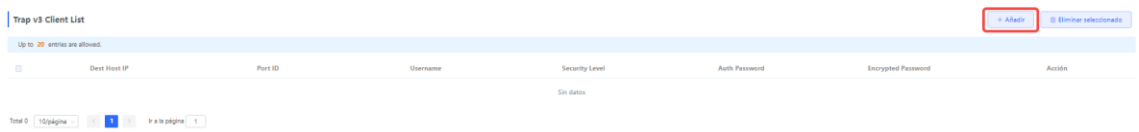
- requisitos previos

Cuando se selecciona v3 como la versión del servicio de trampas, se debe crear un usuario de trampas v3.

- pasos de la configuración

Network Management > **Setting** > **SNMP** > **Trap Settings**

(1) Haga clic en **Añadir** en la página **SNMP v3 Client List** para crear un usuario de trampas v3.



(2) Establezca los parámetros correspondientes a los usuarios de trampas v3.

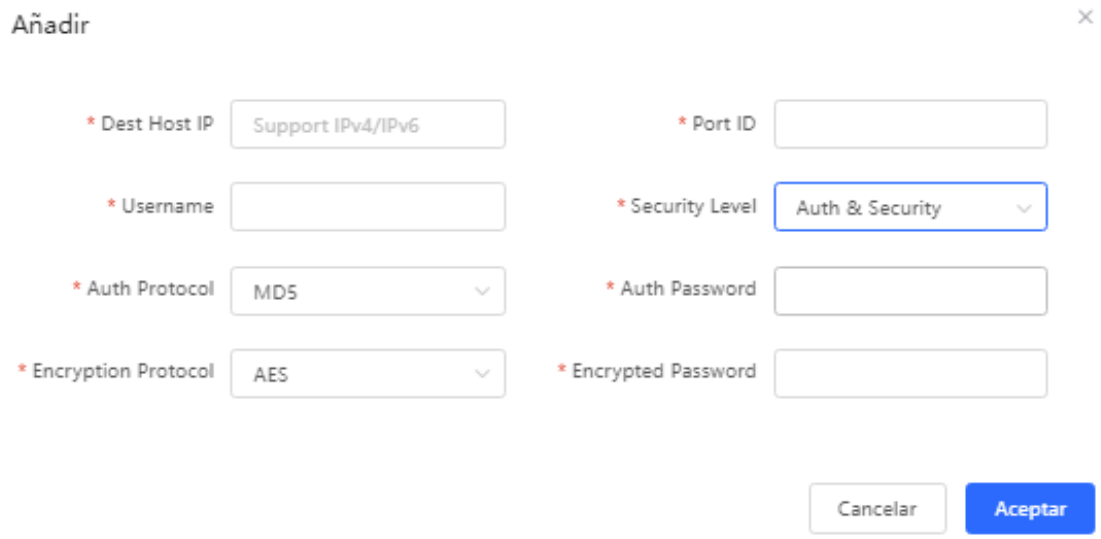


Tabla 20-9 Tabla descriptiva de la información de los usuarios v3

Parámetro	Descripción
Dest Host IP	La IP del dispositivo homólogo del servicio de trampas (admite direcciones IPv4 e IPv6).
Port ID	El puerto del dispositivo homólogo del servicio de trampas [1, 65535].
Username	El nombre de usuario del usuario de trampas v3. Debe contener al menos 8 caracteres Debe contener tres tipos de letras mayúsculas, minúsculas, números y caracteres especiales No debe contener admin/público/privado No debe contener signos de interrogación, espacios ni caracteres chinos
Security Level	Nivel de seguridad del usuario del servicio de trampas, incluyendo tres niveles de autenticación y encriptación, autenticación y encriptación, y autenticación y sin encriptación.
Auth Protocol, Auth Password	Los protocolos de autenticación incluyen: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Auth Password: 8 a 31 caracteres de longitud, no puede contener caracteres chinos, caracteres de ancho completo, signos de interrogación ni espacios y debe contener al menos 3 tipos de letras mayúsculas y minúsculas, números o caracteres especiales. Nota: Debe configurar este parámetro cuando la opción **Security Level** se establezca en **Authentication and encryption** o **Authentication without encryption**.

Parámetro	Descripción
Encryption Protocol, Encrypted Password	Los protocolos de encriptación incluyen: DES/AES/AES192/AES256 Encrypted password: la longitud debe ser de 8~ 31 caracteres y no puede contener caracteres chinos, caracteres de ancho completo, signos de interrogación ni espacios. Formato: debe contener al menos 3 tipos de letras mayúsculas y minúsculas, números o caracteres especiales. Nota: Debe configurar este parámetro cuando la opción **Security Level** se establezca en **Authentication and Encryption**.

Aviso
La dirección IP de los usuarios del servicio de trampas v1/v2c/v3 no puede estar repetida.

20.4.6 Ejemplos típicos de configuración del servicio de trampas

1. Configuración del servicio de trampas versión v2c

- escenarios que pueden utilizarse

Cuando el usuario está supervisando el dispositivo, si este sufre una interrupción repentina o una anomalía, el software de supervisión de terceros no puede detectar y tratar a tiempo la situación anómala, por lo que debe configurar el dispositivo con la IP de destino 192.168.110.85 y el número de puerto 166 para que el dispositivo envíe una trampa de la versión v2c en caso de que se produzca una excepción.

- lista de configuración

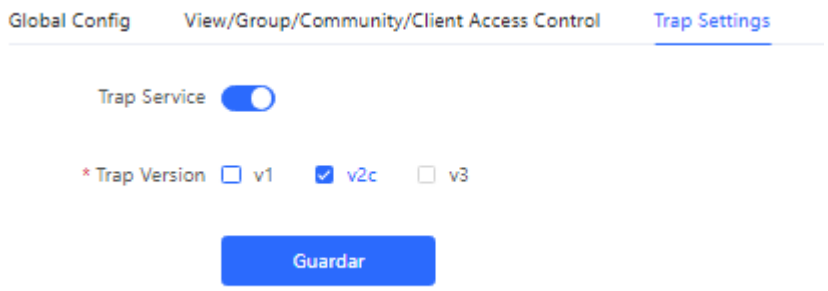
Puede ver los requisitos en la tabla en función del análisis del escenario de uso del usuario:

Tabla 20-10 Formulario de descripción de los requisitos del usuario

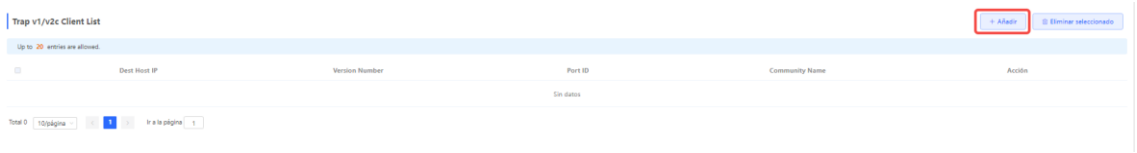
elemento de la descripción	Descripción
Dest Host IP	La IP del host de destino es «192.168.110.85» y el número de puerto es «166».
Version Number	Seleccione la versión v2
Community Name/Username	Trap_public

- pasos de la configuración

(1) Seleccione la versión v2c en la interfaz de configuración de las trampas y haga clic en **Guardar**.



(1) Haga clic en **Añadir** en la lista **Trap v1/v2c Client List**.



(2) Introduzca la IP del host de destino, el número de versión, el número de puerto, el nombre de usuario, así como la demás información y haga clic en **Aceptar** una vez que finalice la configuración.

2. Configuración del servicio de trampas versión V3

- escenarios que pueden utilizarse

Cuando el usuario está supervisando el dispositivo, si este sufre una interrupción repentina o una anomalía, el software de supervisión de terceros no puede detectar y tratar a tiempo la situación anómala, por lo que debe configurar el dispositivo con la IP de destino 192.168.110.87 y el número de puerto 167 para que el dispositivo utilice la versión v3 más segura para enviar trampas.

- lista de configuración

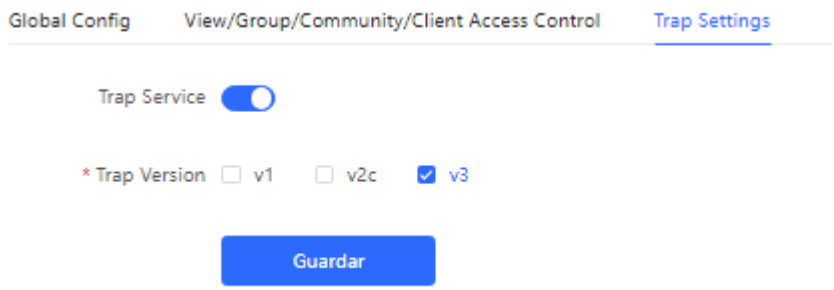
Puede ver los requisitos en la tabla en función del análisis del escenario de uso del usuario:

Tabla 20-11 Formulario de descripción de los requisitos del usuario

elemento de la descripción	Descripción
Dest Host IP	La IP del host de destino es «192.168.110.87» y el número de puerto es «167».
Version Number	Seleccione la versión v3, el nombre de usuario es «trapv3_public».
Auth Protocol/Encryption Protocol Encryption Protocol/Encryption Cypher	Auth Protocol/Auth Password: MD5/Ruijie123 Encryption Protocol/Encrypted Password: AES/Ruijie123

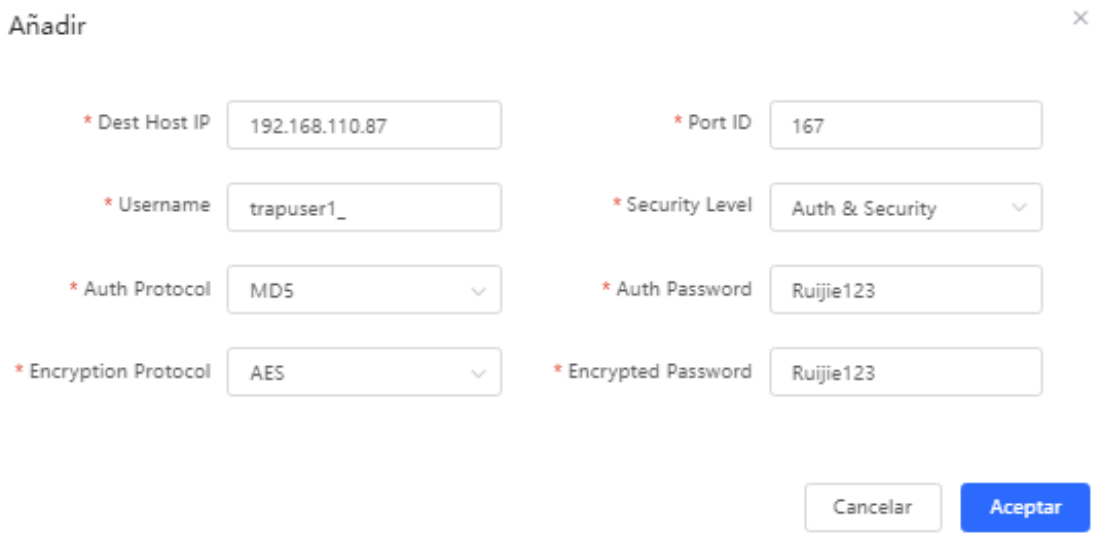
- pasos de la configuración

(1) Seleccione la versión v3 en la interfaz de configuración de las trampas y haga clic en **Guardar**.



(1) Haga clic en **Añadir** en la lista **Trap v3 Client List**.

(2) Introduzca la IP del host de destino, el número de puerto, el nombre de usuario, así como la demás información y haga clic en **Aceptar** una vez que finalice la configuración.

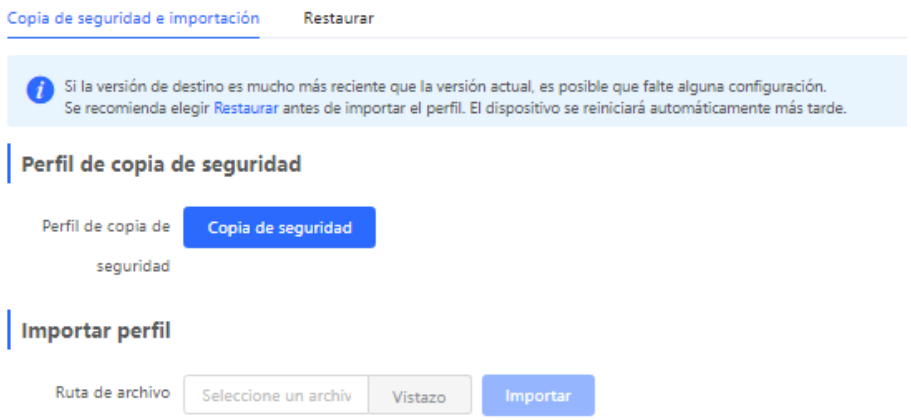


20.5 Configuración de respaldo e importación

Seleccione **Dispositivo local** > **Sistema** > **Backup** > **Copia de seguridad e importación**.

Configuración de respaldo: haga clic en **Backup** para generar la configuración de respaldo y descargarla de manera local.

Configuración de importación: haga clic en **Browse**, seleccione el archivo de la configuración de respaldo de manera local y haga clic en **Import** para usar la configuración especificada por el archivo en el dispositivo. Después de que la configuración se haya importado, el dispositivo se reiniciará.

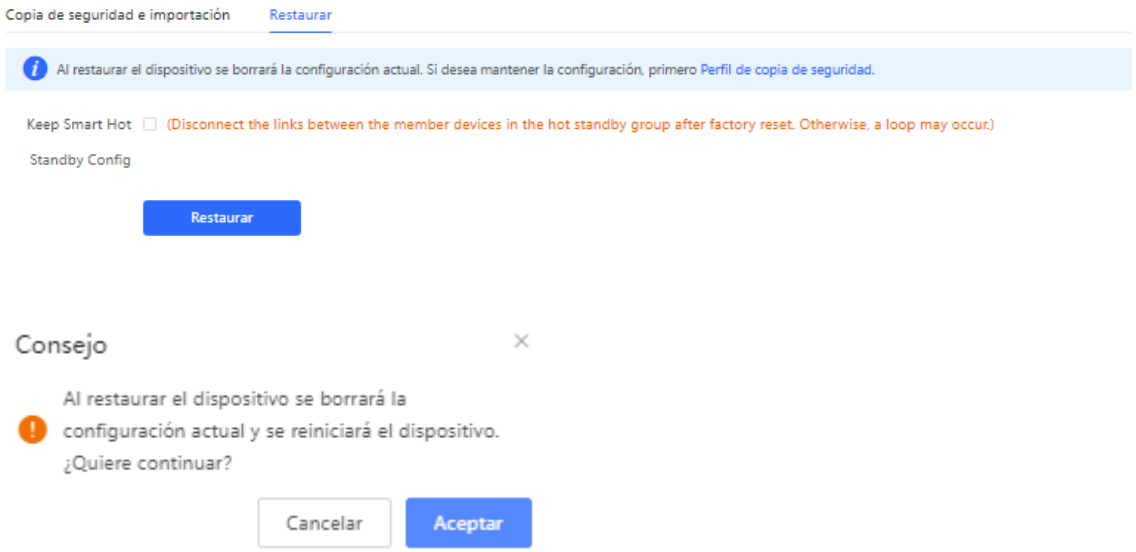


20.6 Restablecimiento

20.6.1 Restablecimiento del dispositivo

Seleccione **Dispositivo local > System** > **Backup** > **Reset**.

Haga clic en **Reset** y luego en **OK** para restablecer la configuración de fábrica.



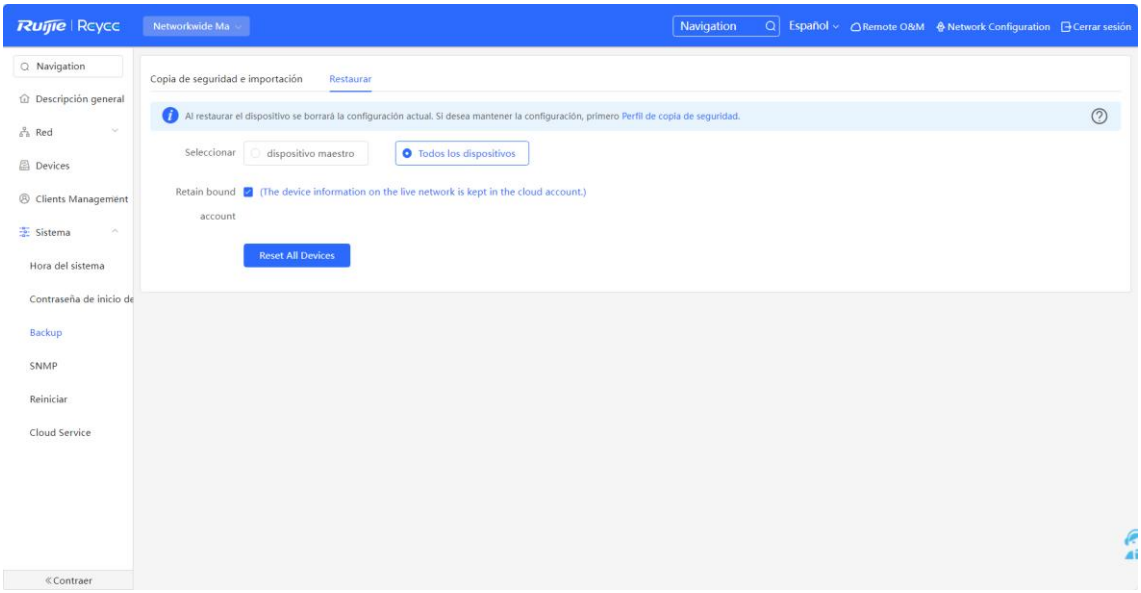
Precaución

Si restablece el dispositivo, se borrarán todos los ajustes actuales y el dispositivo se reiniciará. Si en el sistema actual existe una configuración que considere útil, esta se puede exportar (consulte 20.4 Configuración del SNMP) antes de que restablezca la configuración de fábrica. Por lo tanto, actúe con prudencia al realizar esta acción.

20.6.2 Restablecimiento de los dispositivos en la red

Seleccione **Network Management** > **Sistema** > **Backup** > **Restaurar**.

Seleccione **Todos los dispositivos** y decida si desea **Desvincular la cuenta**; después, haga clic en **Reset all devices**. Todos los dispositivos de la red se restablecerán con la configuración de fábrica.



Precaución

Si restablece la red, se borrarán todos los ajustes actuales de todos los dispositivos en ella y se reiniciarán. Por lo tanto, actúe con prudencia al realizar esta acción.

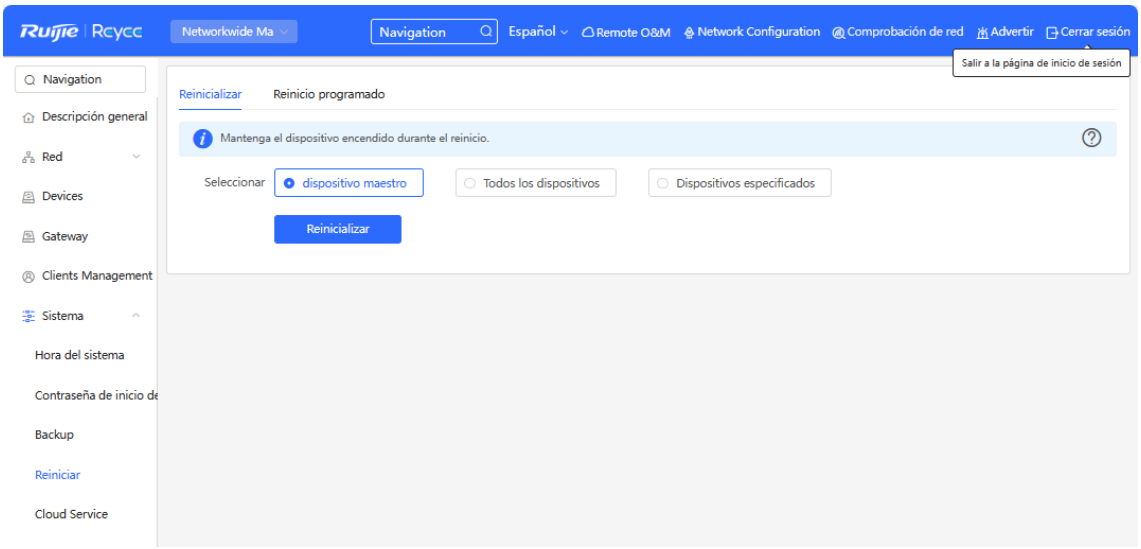
20.7 Reinicio del dispositivo

20.7.1 Reinicio del dispositivo

Seleccione **Modo autoorganización** > **Network Management** > **Sistema** > **Reiniciar** > > **Reiniciar**

Seleccione **Modo independiente** > **Sistema** > **Reinicializar**.

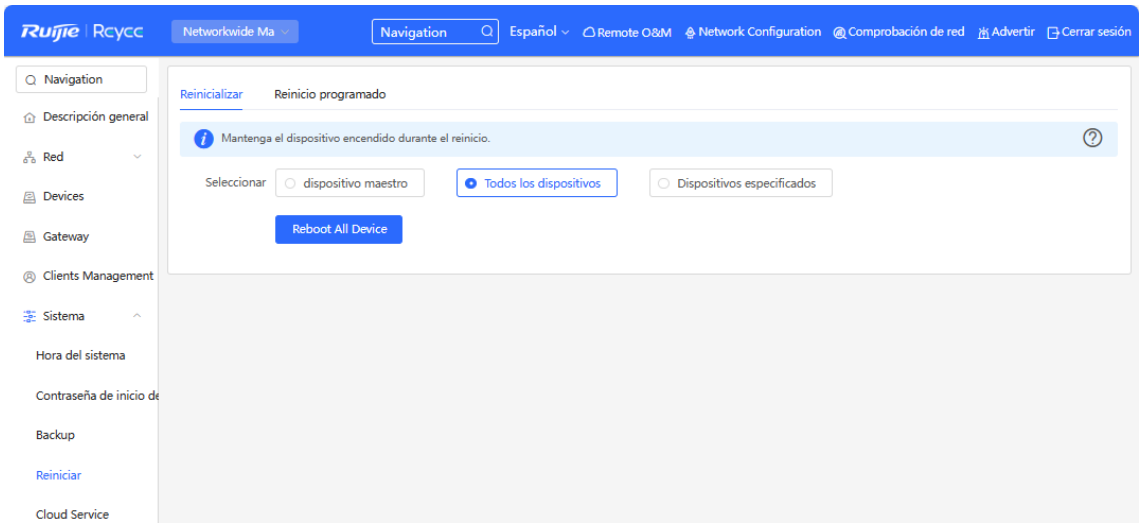
Seleccione **Local** y haga clic en **Todos los dispositivos**. El dispositivo se reiniciará. No actualice la página o cierre el navegador durante el reinicio. Cuando el dispositivo se haya reiniciado correctamente y el servicio web se encuentre disponible, este cambia automáticamente a la página de inicio de sesión.



20.7.2 Reinicio de los dispositivos en la red

Seleccione **Network Management > Sistema** > **Reiniciar** > **Reinicializar**.

Seleccione **Todos los dispositivos** y haga clic en **Reboot All Device** para reinicializar todos los dispositivos de la red.



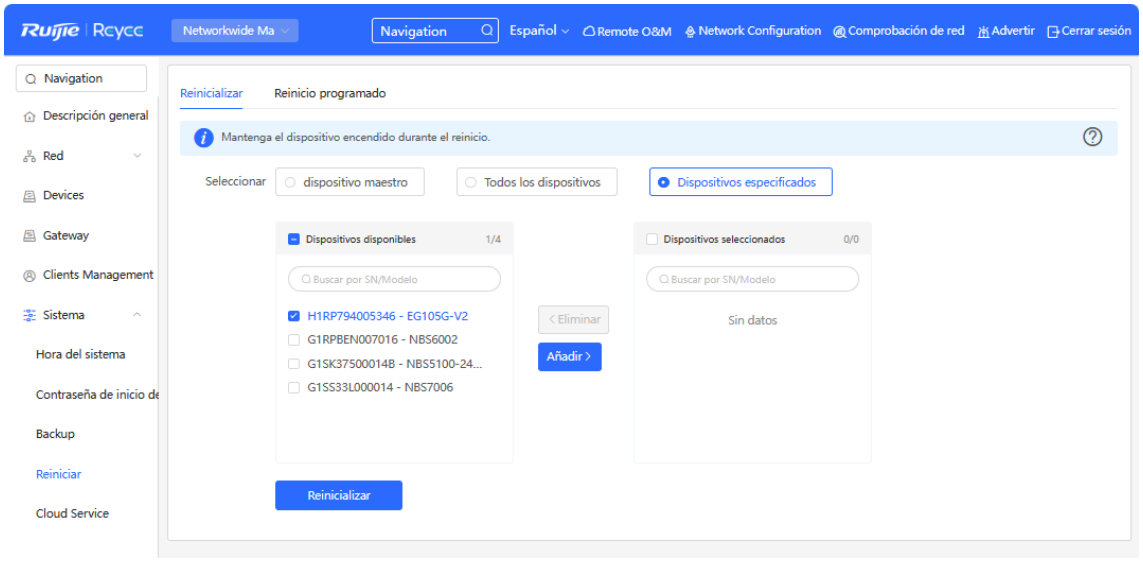
Precaución

Toma tiempo que la red se reinicie. El funcionamiento de la red afectará a toda la red. Por lo tanto, sea precavido al realizar esta acción.

20.7.3 Reinicialización de dispositivos específicos en la red

Seleccione **Networkwide Management** > **Sistema** > **Reiniciar** > **Reinicializar**.

Haga clic en **Dispositivos especificados**, seleccione los dispositivos deseados de la lista de **Dispositivos disponibles** y haga clic en **Añadir** para añadirlos a la lista de **Dispositivos seleccionados** que se encuentra del lado derecho. Haga clic en **Reinicializar**. Los dispositivos especificados en la lista de **Dispositivos seleccionados** se restablecerán.



20.8 Configuración de reinicio programado

Confirme que la hora del sistema sea correcta. Para información más detallada acerca de cómo configurar la hora del sistema, consulte 20.1 Configuración de la hora del sistema

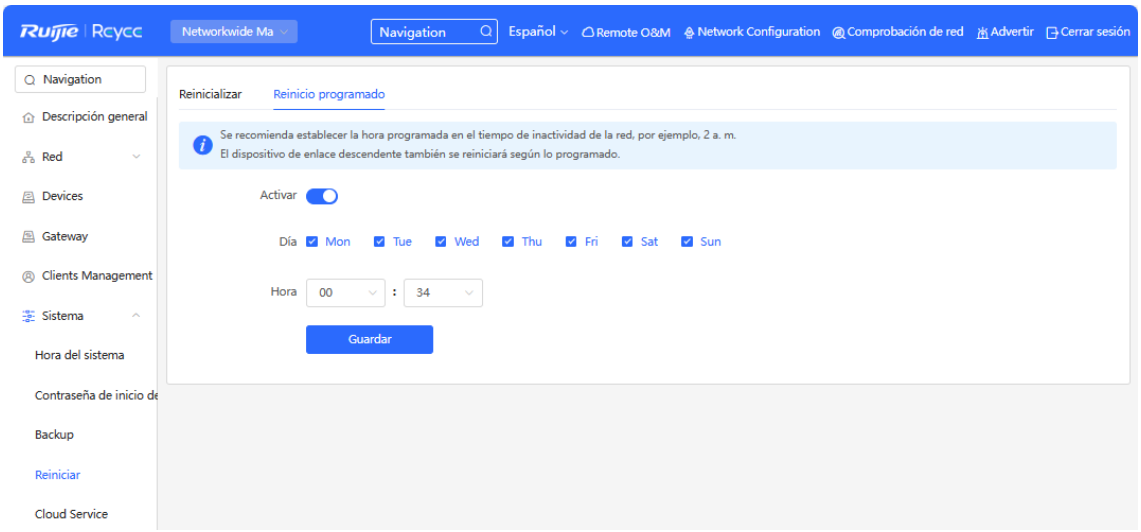
Seleccione **Modo autoorganización** > **Networkwide Management >** > **Sistema** > **Reiniciar >** > **Reinicio programado**.

Seleccione **Modo independiente** > **Sistema** >**Reiniciar** > **Reinicio programado**.

Haga clic en **Activar** y seleccione la fecha y hora de reinicio programado semanalmente. Haga clic en **Guardar**. Cuando la hora del sistema coincida con la hora de reinicio programada, el dispositivo se reiniciará.

Precaución

Cuando se haya habilitado un reinicio programado, todos los dispositivos de la red se reiniciarán a la hora programada. Por lo tanto, sea precavido al realizar esta acción.



20.9 Actualización

Precaución

- Se sugiere respaldar la configuración antes de actualizar el software.
- La actualización de la versión reiniciará el dispositivo. No actualice o cierre el navegador durante la actualización.

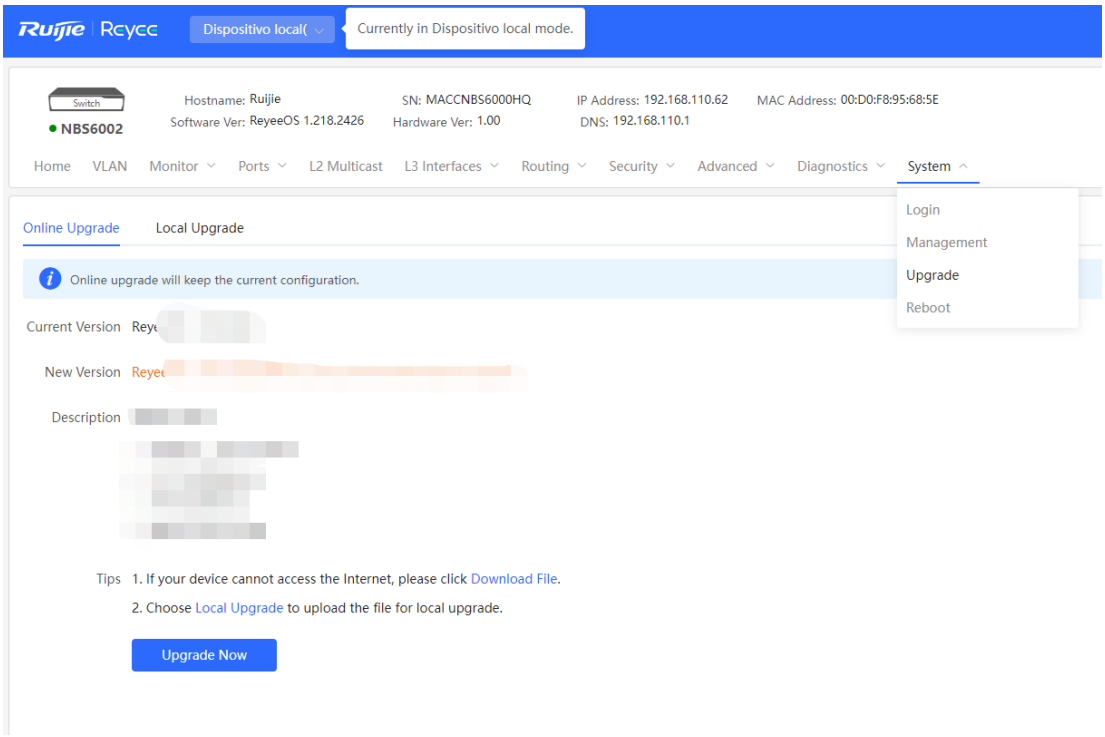
20.9.1 Actualización en línea

Seleccione **Dispositivo local > System** > **Upgrade** > **Online Upgrade**.

La presente página muestra la versión actual del sistema y le permite detectar si se encuentra disponible una versión más reciente. Si hay una nueva versión disponible, haga clic en **Upgrade now** para hacer la actualización en línea. Si el ambiente de la red no es compatible con la actualización en línea, haga clic en **Download File** para descargar el paquete de instalación de la actualización de manera local y luego realice la actualización localmente.

Nota

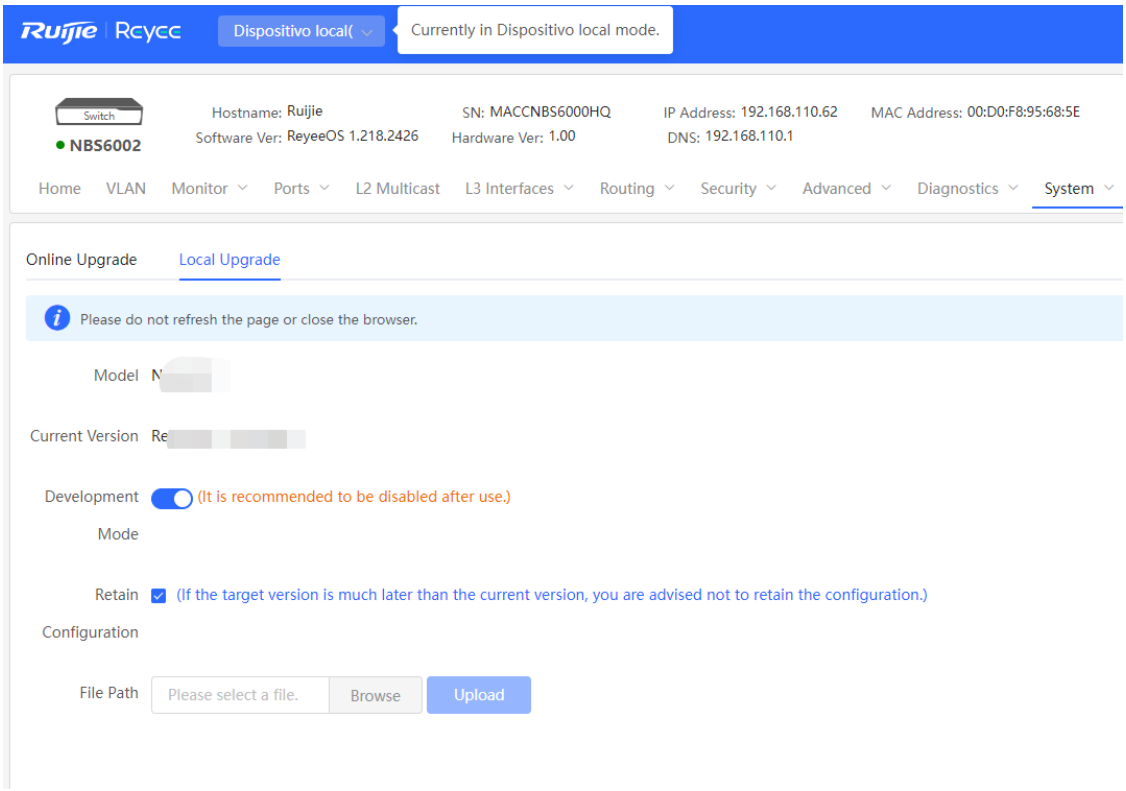
- La actualización en línea conservará la configuración actual.
- No actualice o cierre el navegador durante la actualización. Después de que se haya completado la actualización, se abrirá la página de inicio de sesión automáticamente.



20.9.2 Actualización local

Seleccione **Dispositivo local > System** > **Upgrade** > **Local Upgrade**.

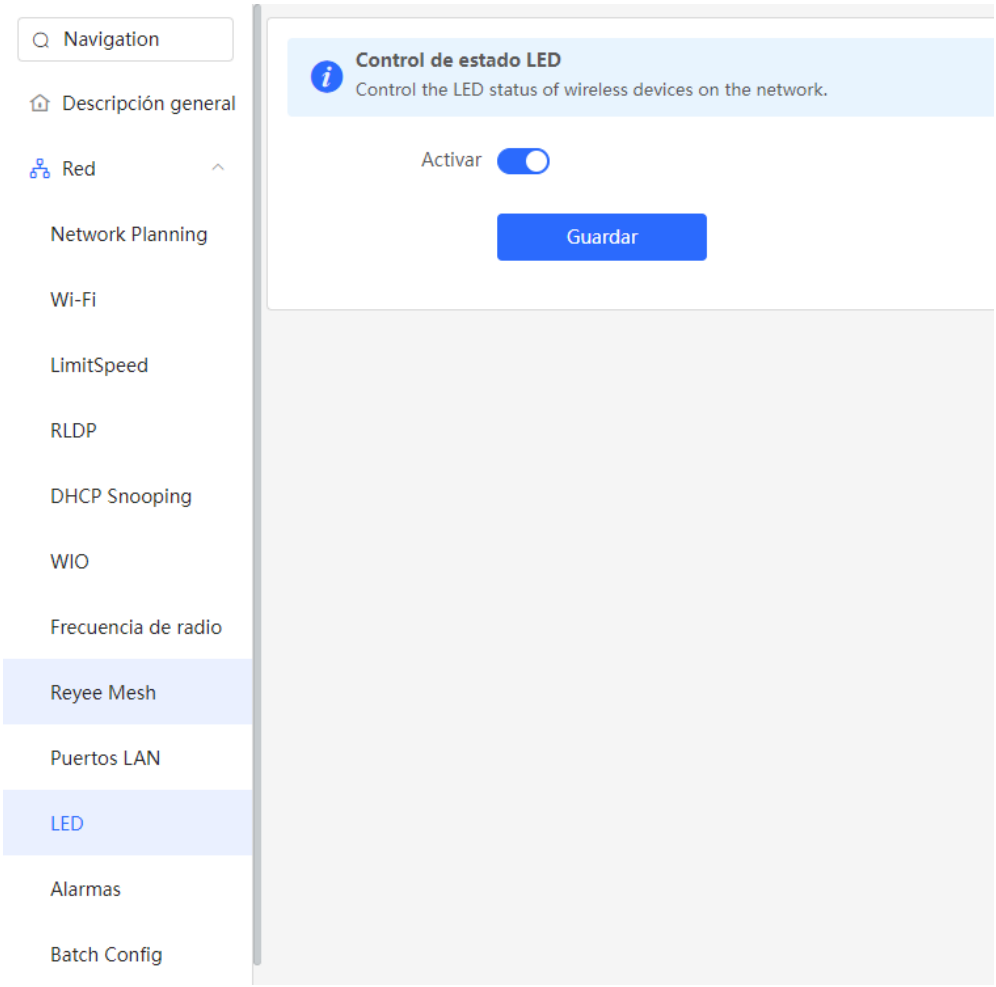
La página **Local Upgrade** muestra el modelo del dispositivo y la versión actual del software. Se puede elegir entre conservar la actualización de la configuración o no. Haga clic en **Browse** para seleccionar el paquete de instalación del software local y luego en **Upload** para cargar el paquete y llevar a cabo la actualización local.



20.10 LED

Seleccione **Networkwide Management** > **Red** > **LED**.

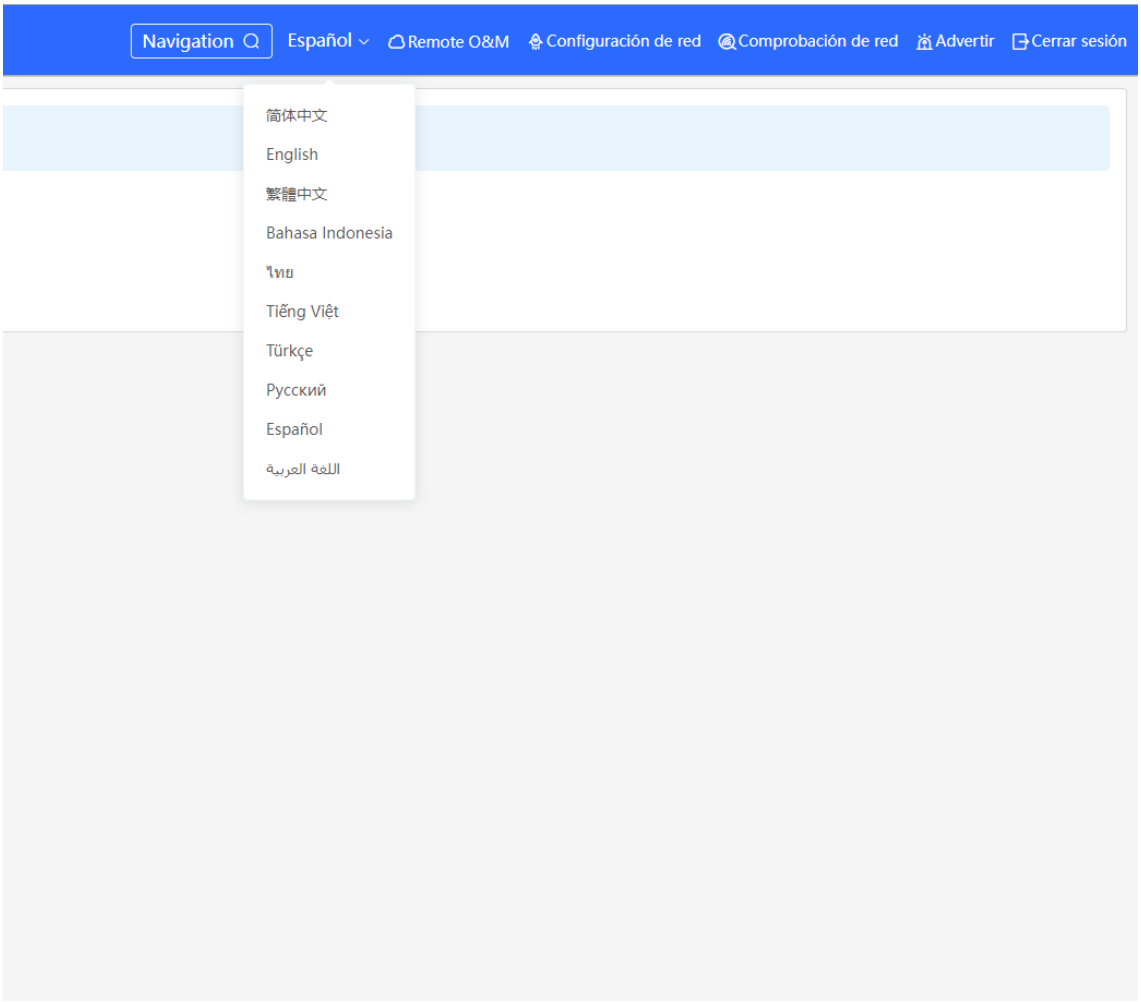
Haga clic en el botón de control de estado LED del AP de enlace descendente. Haga clic en **Guardar** para completar la configuración y hacerla efectiva.



20.11 Cambio de idioma del sistema

Haga clic en English , en la esquina superior derecha de la página web.

Haga clic en el idioma requerido para cambiar el idioma del sistema.


Navigation
Español
Remote O&M
Configuración de red
Comprobación de red
Advertir
Cerrar sesión
简体中文
English
繁體中文
Bahasa Indonesia
ไทย
Tiếng Việt
Türkçe
Русский
Español
اللغة العربية

21 Configuración de las redes wifi de los switches de las series NBS y NIS

Nota

- Para administrar otros dispositivos en SON, habilite la función de descubrimiento de SON. Consulte Cambiar el modo de trabajo. Por defecto, la configuración inalámbrica se sincroniza en todos los dispositivos inalámbricos de la red. Se pueden configurar grupos para limitar el alcance del dispositivo bajo la gestión inalámbrica. Para más información, consulte 21.1 Configuración de grupos de AP
- El dispositivo no admite la transmisión de una señal de Wi-Fi inalámbrica, y la configuración inalámbrica debe sincronizarse en los dispositivos inalámbricos de la red para que sea efectiva.

21.1 Configuración de grupos de AP

21.1.1 Descripción general

Cuando la función de descubrimiento de SON se haya habilitado, el dispositivo actúa como AP o AC maestro para llevar a cabo la configuración por lotes y poder administrar los AP de enlace descendente por grupo. Antes de configurar los AP, asígnelos a diferentes grupos.

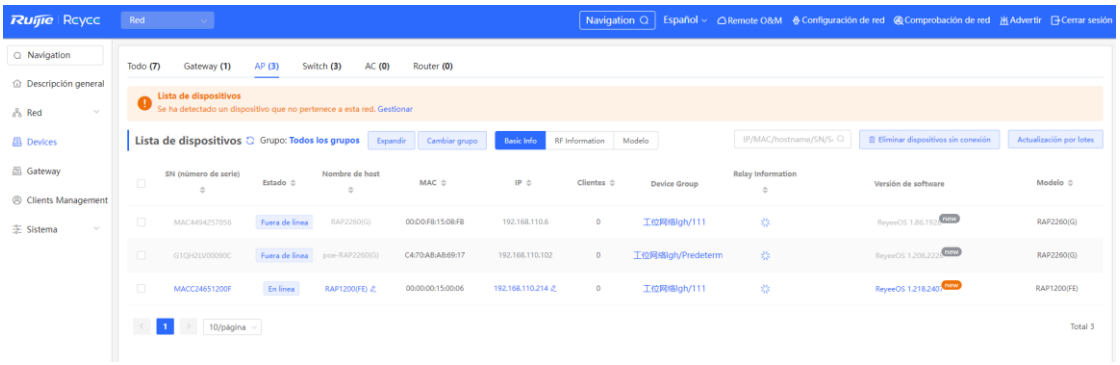
Nota

Si especifica grupos al configurar la red inalámbrica, la configuración será efectiva en los dispositivos inalámbricos de los grupos especificados.

21.1.2 Procedimiento

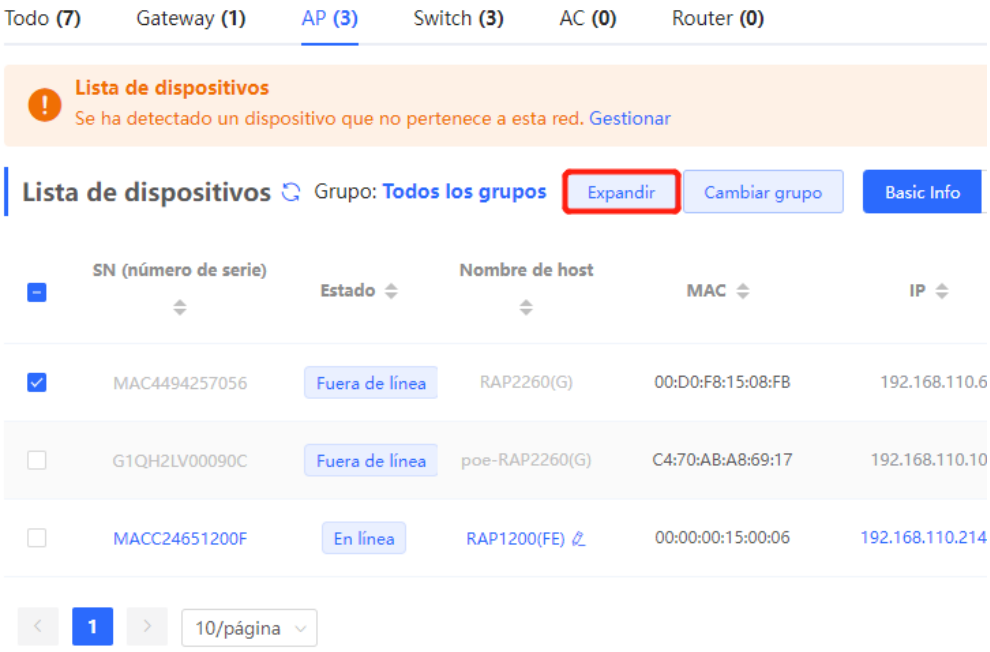
Seleccione **Red** > **Devices** > **AP**.

(1) Consulte la información de todos los AP en la red, incluyendo la información básica, la información de la RF y el modelo. Haga clic en el SN de un AP para configurar el AP de manera separada.



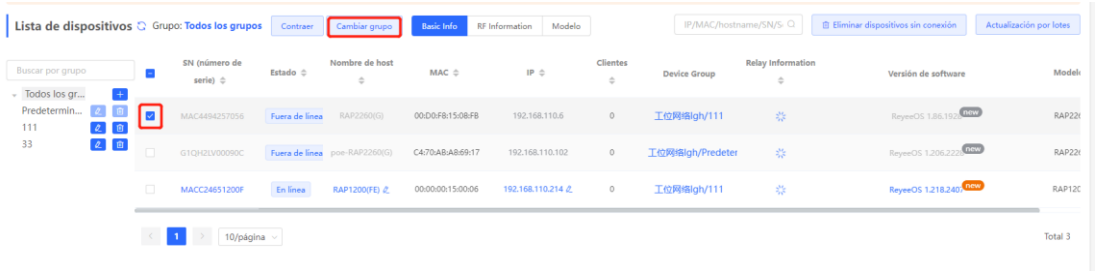
(2) Haga clic en **Expandir**. Del lado izquierdo de la lista, se muestra la información de todos los grupos actuales. Haga clic en  para crear un grupo. Puede crear un máximo de ocho grupos. Seleccione el grupo objetivo

y haga clic en para modificar el nombre del grupo o en para borrarlo. El nombre del grupo predeterminado no se puede modificar ni borrar.



(3) Haga clic en el nombre de un grupo del lado izquierdo. Se muestran todos los AP del grupo. Un AP solo puede pertenecer a un solo grupo. Por defecto, todos los AP pertenecen al grupo predeterminado. Seleccione un registro en la lista de dispositivos y haga clic en **Cambiar grupo** para migrar el dispositivo

seleccionado a un grupo específico. Cuando haya trasladado el dispositivo a un grupo específico, este usará la configuración del nuevo grupo. Haga clic en **Eliminar dispositivos sin conexión** para eliminar los dispositivos sin conexión de la lista.



21.2 Configuración Wi-Fi

Seleccione **Red** > **Red** > **Wi-Fi** > **Configuración Wi-Fi**.

Ingrese el nombre de la red Wi-Fi y la contraseña, seleccione la banda de frecuencia utilizada por la señal Wi-Fi y haga clic en **Guardar**.

Haga clic en **Configuración avanzada** para configurar otros parámetros de Wi-Fi.

Precaución

La modificación ocasionará el reinicio de la configuración inalámbrica, dando como resultado que los clientes conectados salgan de la sesión. Por lo tanto, actúe con prudencia al realizar esta acción.

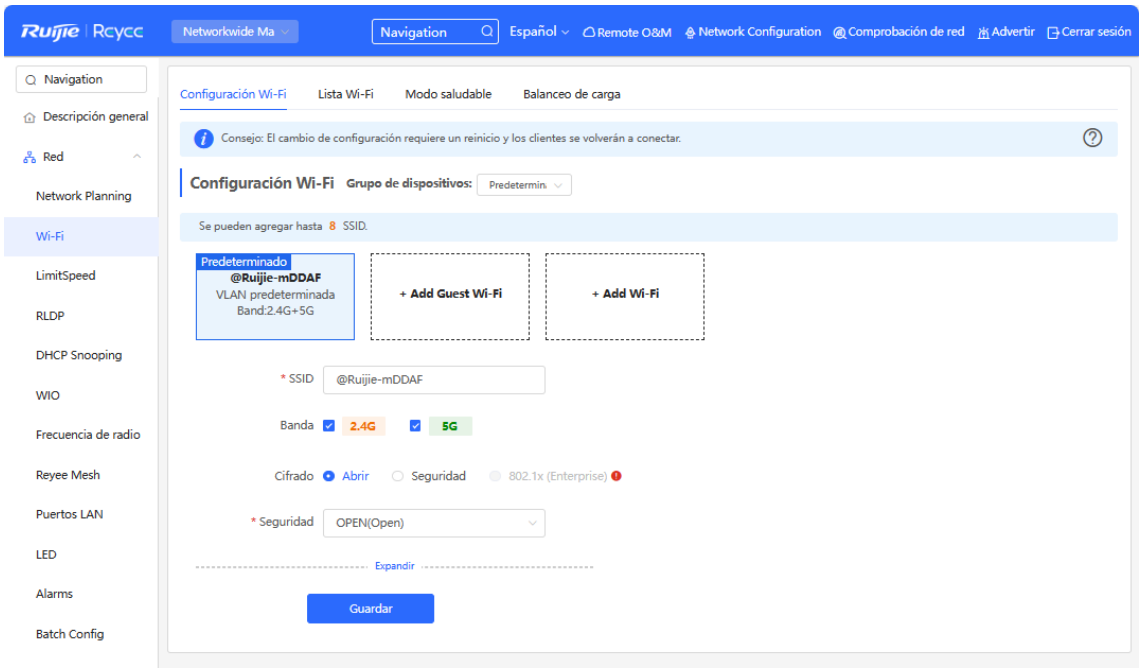

Ruijie | Reyee
Networkwide Ma
Navigation
Español
Remote O&M
Network Configuration
Comprobación de red
Advertir
Cerrar sesión
Navigation
Descripción general
Red
Network Planning
Wi-Fi
LimitSpeed
RLDP
DHCP Snooping
WIO
Frecuencia de radio
Reyee Mesh
Puertos LAN
LED
Alarms
Batch Config
Configuración Wi-Fi
Lista Wi-Fi
Modo saludable
Balanceo de carga
Consejo: El cambio de configuración requiere un reinicio y los clientes se volverán a conectar.
Configuración Wi-Fi
Grupo de dispositivos:
Predetermin
Se pueden agregar hasta 8 SSID.
Predeterminado
@Ruijie-mDDAF
VLAN predeterminada
Band:2.4G+5G
+ Add Guest Wi-Fi
+ Add Wi-Fi
* SSID
@Ruijie-mDDAF
Banda
2.4G
5G
Cifrado
Abrir
Seguridad
802.1x (Enterprise)
* Seguridad
OPEN(Open)
Expandir
Guardar

Tabla 21-1 Configuración de la red inalámbrica

Parámetro	Descripción
SSID	Ingrese el nombre que se muestra cuando un cliente inalámbrico busca una red inalámbrica.
Codificación	Si el SSID no contiene caracteres chinos, este elemento permanecerá oculto. Si el SSID

Parámetro	Descripción
del Identificador de Servicio o SSID	contiene caracteres chinos, este elemento se mostrará. Puede seleccionar UTF-8 o GBK.
Banda	Configure la banda utilizada por las señales de Wi-Fi. Las opciones son 2.4 GHz y 5 GHz. La banda 5 GHz proporciona una velocidad de transmisión de red más rápida y con menos interferencia que la banda de 2.4 GHz, pero es inferior a esta en términos de rango de cobertura de señal y desempeño al pasar entre paredes. Seleccione la banda adecuada, según requiera. El valor predeterminado es **2.4G + 5G**, lo que indica que el dispositivo proporciona señales para ambas bandas de 2.4 GHz y de 5 GHz.
Seguridad	Seleccione un modo encriptado para la conexión inalámbrica de la red. Las opciones son las siguientes: ● **Abierta**: el dispositivo puede asociarse con la red Wi-Fi sin una contraseña. ● **WPA-PSK/WPA2-PSK**: la red Wi-Fi de Acceso Protegido (WPA) o WPA2 se utiliza para encriptación. ● **WPA_WPA2-PSK** (recomendada): la WPA2-PSK o WPA-PSK se utiliza para encriptación.
Contraseña de Wi-Fi	Especifique la contraseña para conectarse a la red inalámbrica. La contraseña es una cadena de 8 a 16 caracteres.
Wi-Fi Standard	Hace referencia a la versión del protocolo de comunicación inalámbrica, como Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac), Wi-Fi 6 (802.11ax), que determina la velocidad, la frecuencia, así como otras características de las conexiones inalámbricas.
Programación inalámbrica	Especifica el periodo durante el cual el Wi-Fi se encuentra habilitado. Después de que haya establecido este parámetro, los usuarios no pueden conectarse al Wi-Fi en ningún otro momento.
VLAN	Configure la VLAN a la que pertenece la señal de Wi-Fi.
Ocultar SSID.	Habilitar la función de ocultar SSID puede prevenir el acceso de usuarios no autorizados a la red Wi-Fi, lo que mejora la seguridad. Sin embargo, los teléfonos móviles o las computadores no pueden encontrar el nombre de Wi-Fi cuando esta función está habilitada. Se debe ingresar manualmente el nombre y contraseña correctos para conectarse al Wi-Fi. Registre el nombre actual de Wi-Fi antes de habilitar esta función.
Aislamiento del cliente	Cuando haya habilitado este parámetro, los clientes asociados al Wi-Fi son aislados unos de otros, y los usuarios conectados al mismo AP (en el mismo segmento de la red) no pueden tener acceso entre ellos. Esto mejora la seguridad.
Cambio de banda	Cuando esta función se habilita, los clientes 5G seleccionan el Wi-Fi 5G de manera preferencial. Esta función se puede habilitar solamente cuando la opción **Band** se configure en **2.4G + 5G**.
XPress	Cuando esta función se habilita, el dispositivo envía paquetes de juego preferentemente,

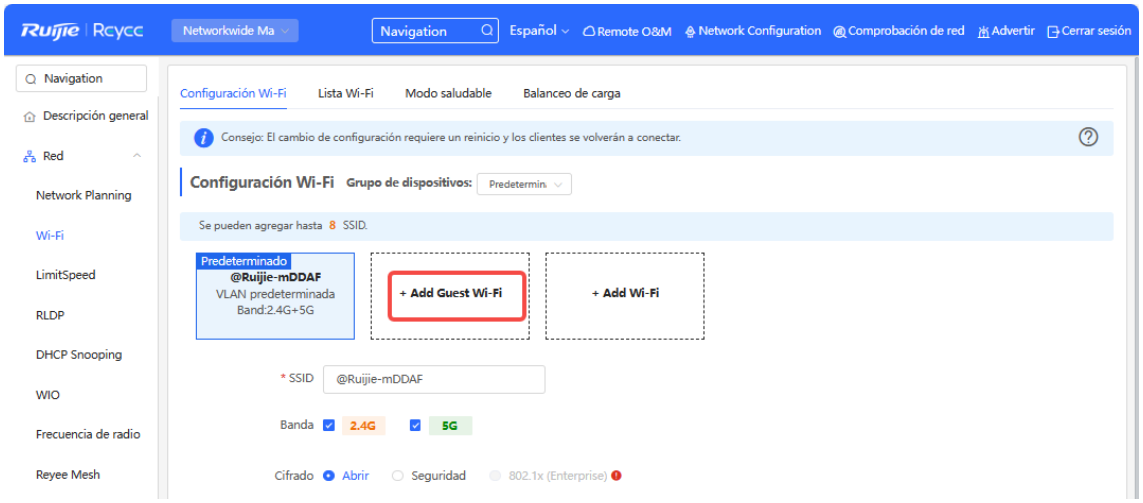
Parámetro	Descripción
	proporcionando una red inalámbrica más estable para jugar.
Itinerancia de Capa -3	Cuando esta función se habilita, los clientes mantendrán sus direcciones IP sin cambios al asociarse con la red misma Wi-Fi. Esta función mejora la experiencia de itinerancia de red autoorganizada de los usuarios en la situación de una VLAN cruzada.
Wi-Fi6	Cuando esta función se habilita, los usuarios inalámbricos tienen una velocidad de acceso a la red más rápida y una experiencia optimizada. Esta función es válida solamente en AP y routers compatibles con 802.11ax. Los clientes deben ser también compatibles con 802.11ax para experimentar un acceso a la red de gran velocidad por medio de Wi-Fi 6. Si los clientes no son compatibles con Wi-Fi 6, deshabilite esta función.
LimitSpeed	Indica la velocidad máxima de transmisión de los datos que se permite a un dispositivo o un usuario en la red wifi y que suele establecerse para poder gestionar la asignación del ancho de banda o garantizar un uso justo entre los dispositivos conectados.

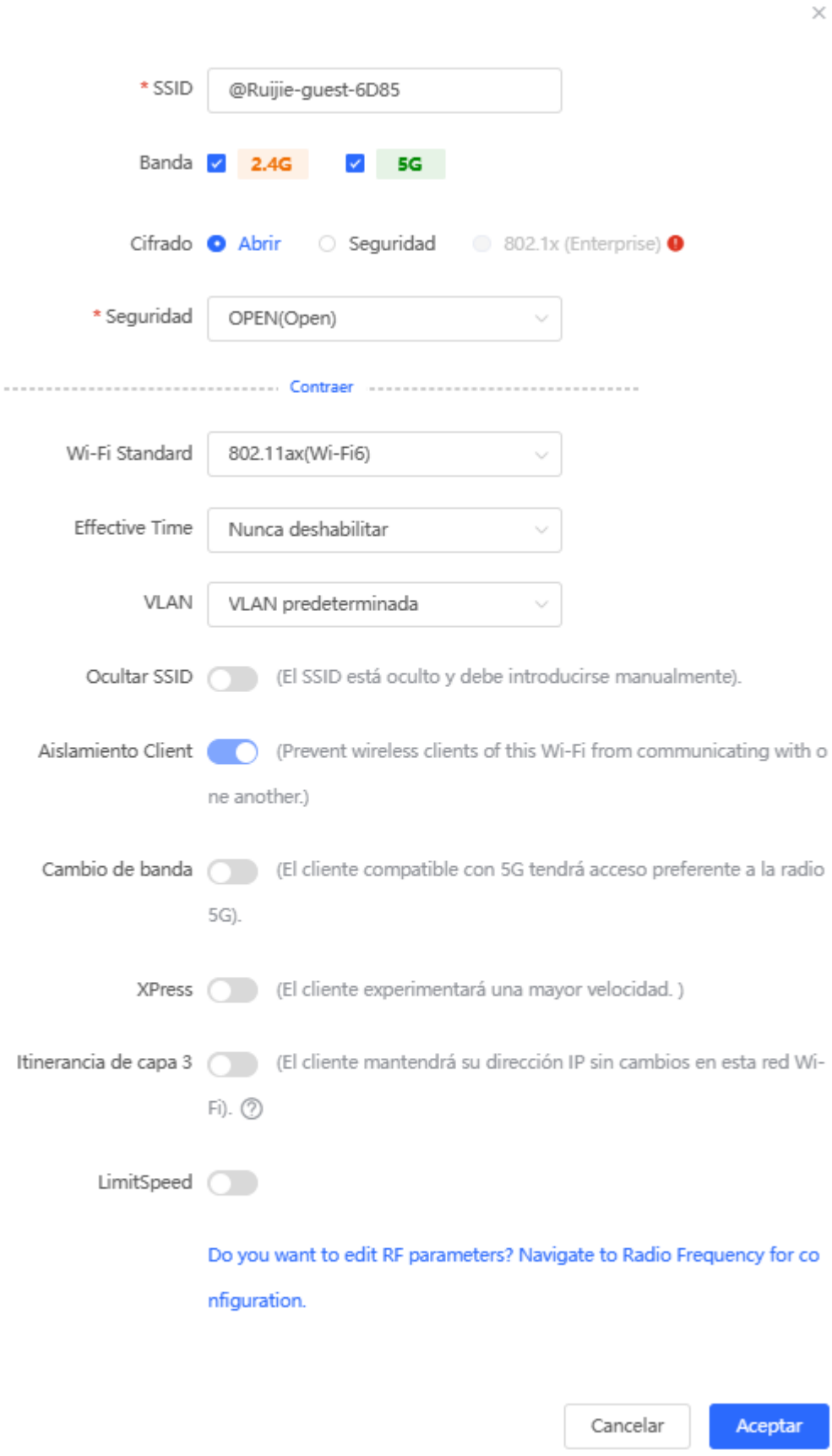
21.3 Configuración de Wi-Fi de invitados

Seleccione **Red** > **Red** > **Wi-Fi** > **Guest Wi-Fi**.

El Wi-Fi de invitados es una red inalámbrica para invitados y, por defecto, se encuentra deshabilitada. La función **Aislamiento Client** está habilitada por defecto para la red Wi-Fi de invitados y no puede deshabilitarse. En este caso, los usuarios asociados con el Wi-Fi de invitados están mutuamente aislados y solo pueden acceder a Internet a través de Wi-Fi. Esto mejora la seguridad del acceso a la red. Se puede configurar una programación inalámbrica para la red de invitados. Cuando la programación especificada haya vencido, la red de invitados no se podrá localizar.

Habilite la red Wi-Fi de invitados y configure el nombre y contraseña. Haga clic en **Expandir** para configurar la programación inalámbrica del Wi-Fi de invitados y cualquiera de sus parámetros. (Para más información, consulte 21.2 Configuración Wi-Fi.) Haga clic en **Guardar**. Los invitados pueden acceder a Internet a través del Wi-Fi, después de ingresar el nombre y contraseña.

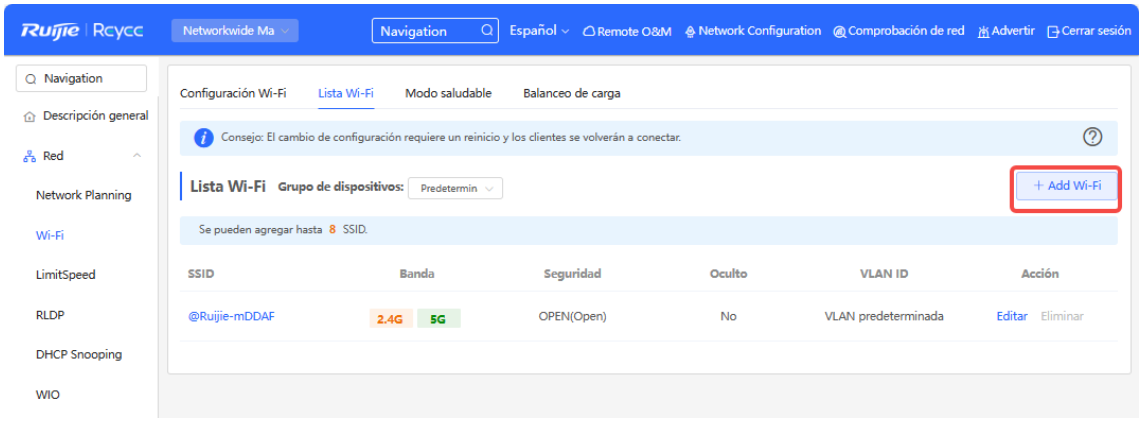



* SSID
@Ruijie-guest-6D85
Banda
2.4G
5G
Cifrado
Abrir
Seguridad
802.1x (Enterprise)
* Seguridad
OPEN(Open)
Contraer
Wi-Fi Standard
802.11ax(Wi-Fi6)
Effective Time
Nunca deshabilitar
VLAN
VLAN predeterminada
Ocultar SSID
(El SSID está oculto y debe introducirse manualmente).
Aislamiento Client
(Prevent wireless clients of this Wi-Fi from communicating with o ne another.)
Cambio de banda
(El cliente compatible con 5G tendrá acceso preferente a la radio 5G).
XPress
(El cliente experimentará una mayor velocidad.)
Itinerancia de capa 3
(El cliente mantendrá su dirección IP sin cambios en esta red Wi-Fi).
LimitSpeed
Do you want to edit RF parameters? Navigate to Radio Frequency for co nfiguration.
Cancelar
Aceptar

21.4 Añadir una red Wi-Fi

Seleccione **Red** > **Red** > **Wi-Fi** > **Lista Wi-Fi**.

Haga clic en **Add Wi-Fi**, ingrese el nombre y la contraseña y haga clic en **Aceptar** para crear una red Wi-Fi. Haga clic en **Expandir** para configurar otros parámetros de Wi-Fi. Para información más detallada, consulte 21.2 Configuración Wi-Fi. Después de que la red Wi-Fi se haya añadido, los clientes podrán encontrarla y su información se mostrará en la lista Wi-Fi

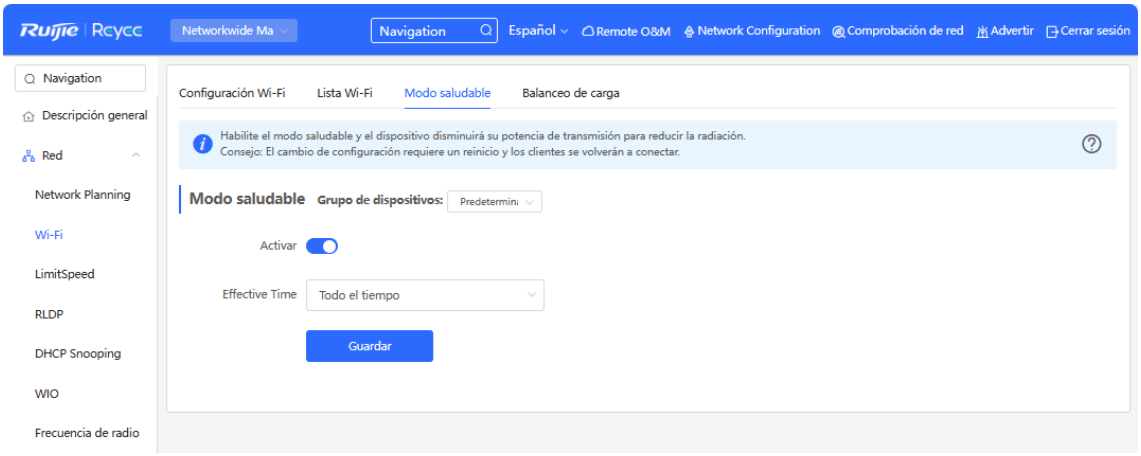


21.5 Modo saludable

Seleccione **Red** > **Red** > **Wi-Fi** > **Modo saludable**.

Habilite el modo saludable y seleccione la programación inalámbrica para dicho modo.

Cuando el modo saludable quede habilitado, la potencia de transmisión de la RF y el rango de cobertura de Wi-Fi del dispositivo inalámbrico se reducirán en la programación. Esto puede resultar en señales débiles y congelamiento de la red. Se sugiere deshabilitar el modo saludable o configurar la programación inalámbrica para el periodo de inactividad.



21.6 Configuración de la frecuencia de radio

Seleccione **Red** > **Red** > **Frecuencia de radio**.

El dispositivo inalámbrico puede detectar el entorno inalámbrico circundante al encenderlo y seleccionar la configuración adecuada. Sin embargo, no se puede evitar que la red se congele debido a los cambios del entorno inalámbrico. Lo que se puede hacer es analizar el entorno inalámbrico de los AP y routers y seleccionar manualmente los parámetros adecuados.

Precaución

La modificación ocasionará el reinicio de la configuración inalámbrica y esto provocará que los clientes conectados salgan de su sesión. Por lo tanto, actúe con prudencia al realizar esta acción.

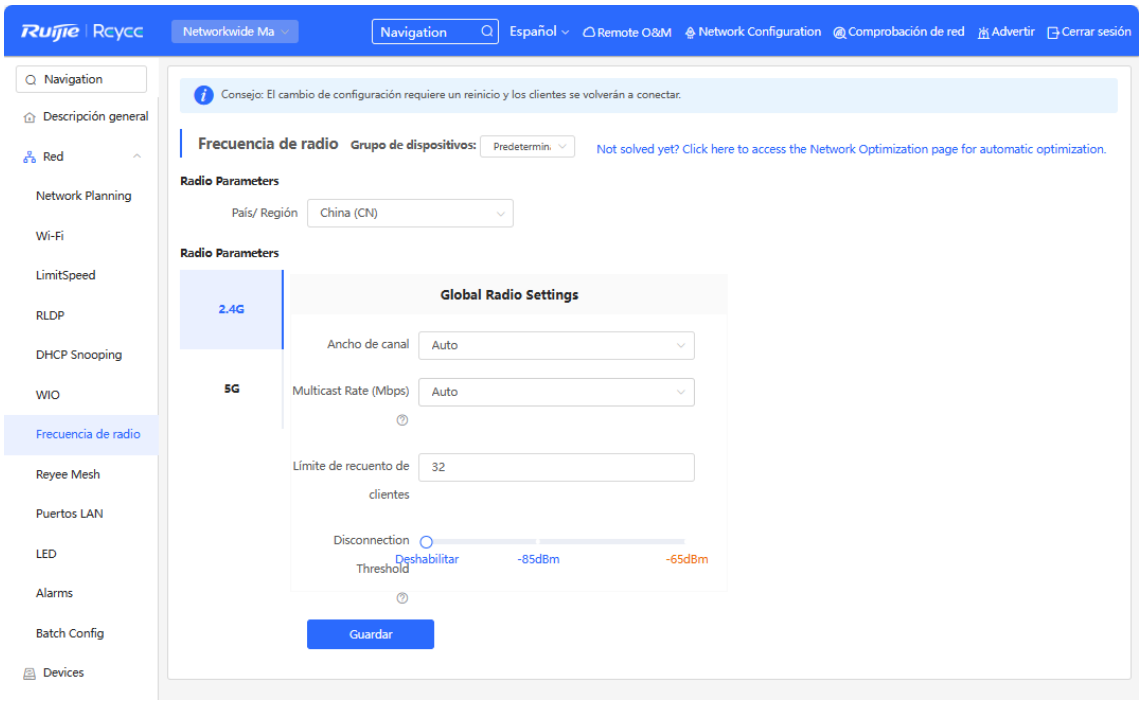


Tabla 21-2 Configuración de la RF

Parámetro	Descripción
País/Región	Los canales de Wi-Fi estipulados por cada país pueden ser diferentes. Para garantizar que los clientes encuentren la señal de Wi-Fi, seleccione el país o región donde está localizado el dispositivo.
Ancho de canal 2.4G/5G	Un ancho de banda menor indica una red más estable y un mayor ancho de banda indica mayor facilidad de interferencia. En caso de una interferencia severa, seleccione un ancho de banda bajo para evitar que la red se congele en algún punto. La banda de 2.4 GHz es compatible con los anchos de banda de 20 MHz y 40 MHz. La banda de 5 GHz es compatible con los anchos de banda de 20 MHz, 40 MHz y 80 MHz. Por defecto, el valor es **Auto**, que indica que el ancho de banda está seleccionado automáticamente con base en el entorno.
Límite de recuento de clientes	Si un gran número de usuarios acceden al AP o al router, el desempeño de la red inalámbrica de estos puede degradarse y, como consecuencia, la experiencia de acceso a Internet de los usuarios se verá afectada. Cuando el número de usuarios de acceso alcance el valor especificado, no podrán acceder nuevos usuarios. Si los clientes requieren mayor ancho de banda, este parámetro se puede ajustar a un valor menor. Se recomienda mantener los ajustes de fábrica, a menos que se especifique lo contrario.

Parámetro	Descripción
Umbral de desconexión	Cuando hay muchas señales de Wi-Fi disponibles, se puede configurar este parámetro para optimizar la calidad de la señal inalámbrica. Cuando un cliente se encuentra alejado del dispositivo inalámbrico y la fuerza de la señal del usuario final es menor que el límite de desconexión, la conexión Wi-Fi se corta. En este caso, el cliente debe seleccionar una señal inalámbrica más cercana. Si el límite de desconexión es alto, el cliente es más propenso a desconectarse. Para garantizar que el cliente cuente con un acceso normal a Internet, se recomienda configurar este parámetro en **Deshabilitar** o en un valor menor a -75 dBm.

Nota

- Los canales inalámbricos que se deben seleccionar están determinados por el código de país. Seleccione el código de país con base en el país o región de su dispositivo.
- El canal, la potencia de transmisión y la sensibilidad de la itinerancia de red autoorganizada no pueden configurarse de manera global, sino separada en cada dispositivo.

21.7 Configuración de una lista blanca/lista negra para la red wifi

21.7.1 Descripción general

Puede configurar la lista blanca/lista negra global o basada en el SSID. La dirección MAC admite tanto una correspondencia total como una correspondencia con la OUI.

Lista negra de la red wifi: los clientes de la lista negra de la red wifi no pueden acceder a Internet. Los clientes que no se añaden a la lista negra de la red wifi pueden acceder a Internet libremente.

Lista blanca de la red wifi: solo los clientes de la lista blanca de la red wifi pueden acceder a Internet. Los clientes que no se añaden a la lista blanca de la red wifi no pueden acceder a Internet.

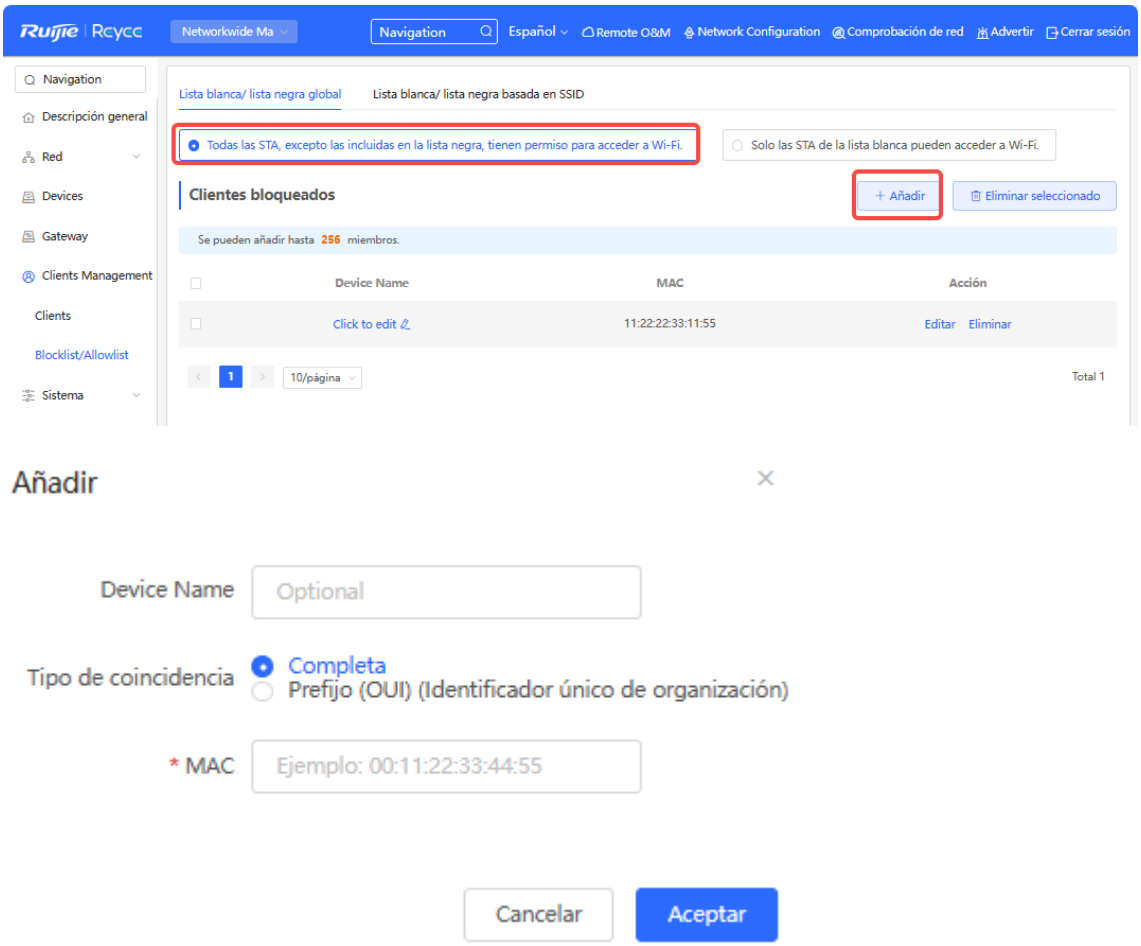
Precaución

Si la lista blanca se encuentra vacía, esta no se aplicará, por lo que todos los clientes podrán acceder a Internet.

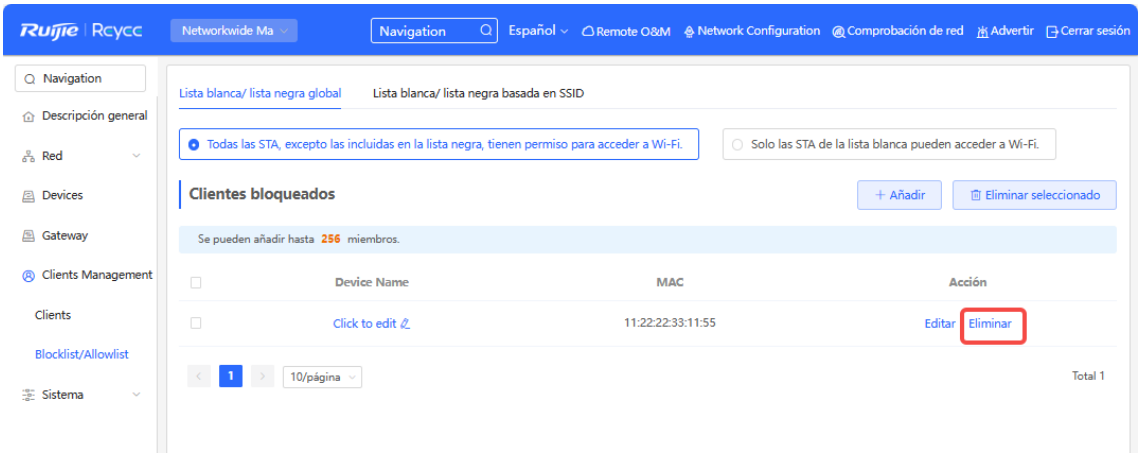
21.7.2 Configuración de una Lista blanca/negra global

Seleccione **Clients Management** > **Blocklist/Allowlist** > **Global Lista blanca/negra global**.

Seleccione el modo de lista blanca o lista negra y haga clic en **Añadir** para configurar un cliente de lista blanca o lista negra. En la ventana **Añadir**, introduzca la dirección MAC y las observaciones del cliente que desee y haga clic en **Aceptar**. Si ya hay un cliente asociado al access point, su dirección MAC aparecerá de forma automática. Haga clic directamente en la dirección MAC para que se introduzca de forma automática. Se forzará la desconexión de todos los clientes de la lista negra y no se les permitirá acceder a la red wifi. La configuración de la lista blanca y la lista negra global se aplicará a todas las redes wifi del access point.



Si hace clic en **Eliminar** en el modo de lista negra, el cliente correspondiente podrá volver a conectarse a la red wifi. Si hace clic en **Eliminar** en el modo de lista blanca y esta no se encuentra no está vacía tras la eliminación, el cliente correspondiente se desconectará y se le permitirá conectarse a la red wifi.



21.7.3 Configuración de la lista blanca/lista negra basada en SSID

Seleccione **Clients** > **Blocklist/Allowlist** > **Lista blanca/lista negra basada en SSID**.

Seleccione la red que desee de la columna de la izquierda, seleccione el modo de lista blanca o lista negra y haga clic en **Añadir** para configurar un cliente de lista blanca o lista negra. La lista negra/lista blanca basada en SSID restringe el acceso de los clientes a la red wifi que haya seleccionado.

21.8 Optimización inalámbrica con un solo clic

Precaución

- La función WIO solo es compatible en con el modo de red autoorganizada.
- Es posible que el cliente se muestre desconectado durante el proceso de optimización. Tenga en cuenta que la configuración no se puede deshacer una vez que se inicia la optimización. Por lo tanto, se recomienda que realice esta operación con precaución.

21.8.1 Optimización de la red

Seleccione **Networkwide Management > Red** > **WIO** > **Network Optimization**.

(1) Seleccione el modo de optimización (Optimization). A continuación haga clic en **OK** para optimizar la red inalámbrica.

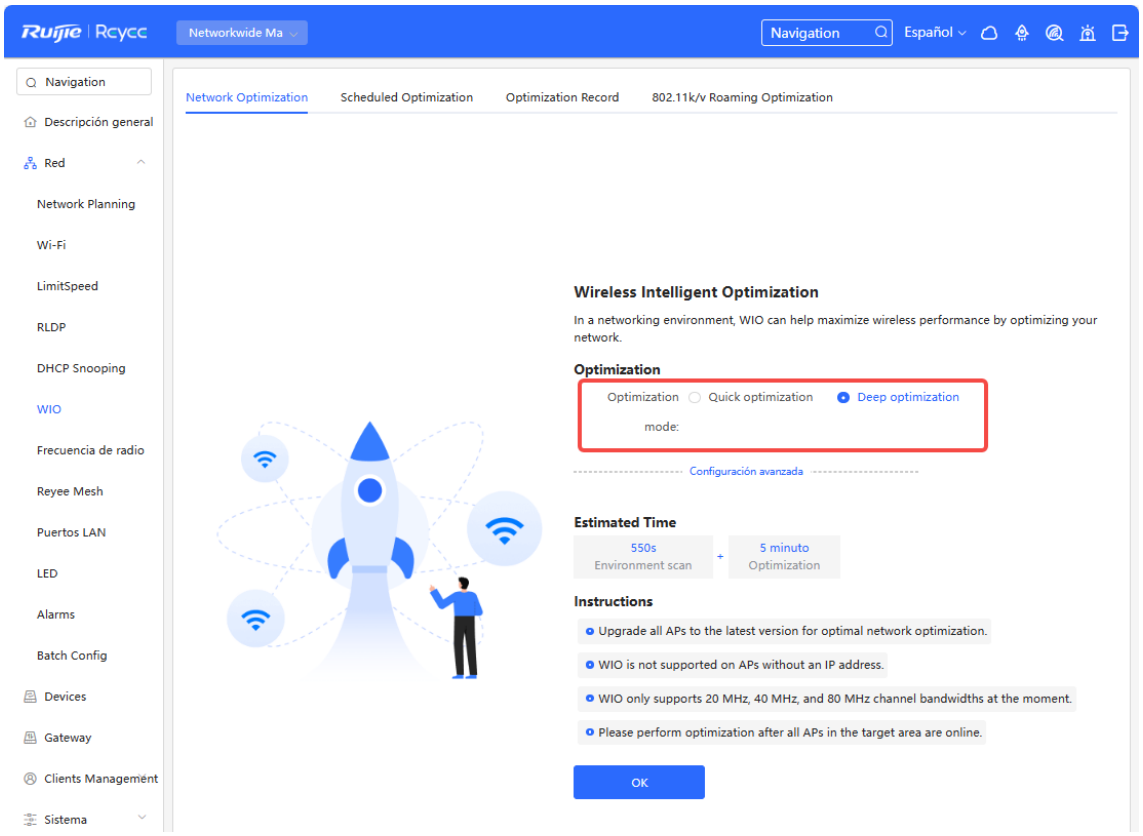
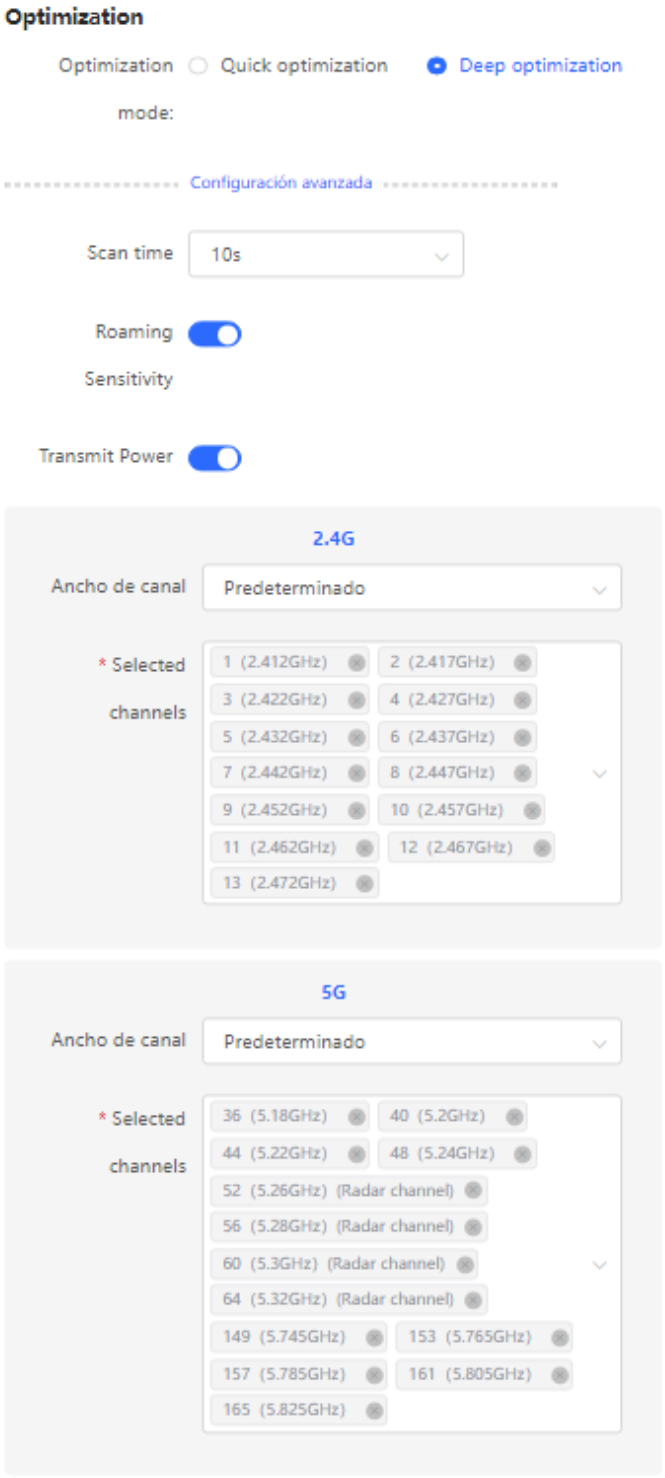


Tabla 21-3 Descripción del modo de optimización

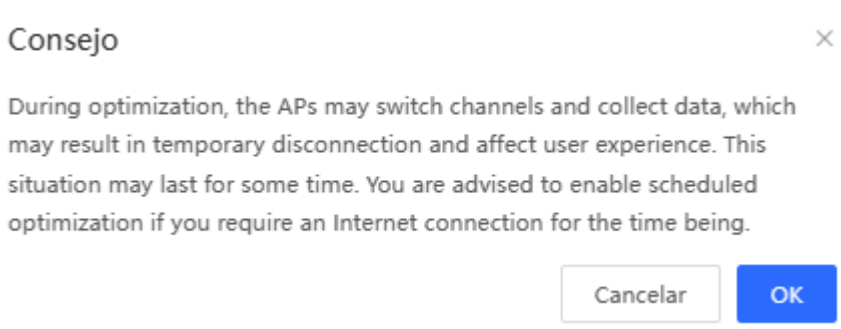
Parámetro	Descripción
Quick optimization	En este modo no se tienen en cuenta las interferencias externas ni el ancho de banda. La optimización rápida se realiza para optimizar el canal, la potencia y la potencia de las tramas de gestión.

Parámetro	Descripción
Deep optimization	En este modo se tienen en cuenta las interferencias externas y el ancho de banda. La optimización detallada se realiza para optimizar el canal, la potencia y la potencia de las tramas de gestión. Haga clic para ampliar la Configuración avanzada y configurar el tiempo de búsqueda, el ancho de banda del canal y los canales. ● Scan time: indica el tiempo de búsqueda de canales durante la optimización. ● Roaming Sensitivity: la sensibilidad de la itinerancia puede optimizarse en función del entorno real para garantizar una itinerancia rápida de los dispositivos inalámbricos. ● Transmit Power aumentar la potencia de transmisión mejora tanto la intensidad como la cobertura de la señal inalámbrica, aunque también puede provocar interferencias en las redes inalámbricas cercanas. Cuando se habilita esta función, el access point ajusta la potencia de transmisión de forma automática en función del entorno. ● 2,4 G ○ Ancho de canal: indica el ancho de banda del canal. El sistema calculará el ancho de banda del canal cuando se selecciona la opción Predeterminado. ○ Selected channels: indica los canales que se van a optimizar. ● 5 G ○ Ancho de canal: indica el ancho de banda del canal. El sistema calculará el ancho de banda del canal cuando se selecciona la opción Predeterminado. ○ Selected channels: indica los canales que se van a optimizar.

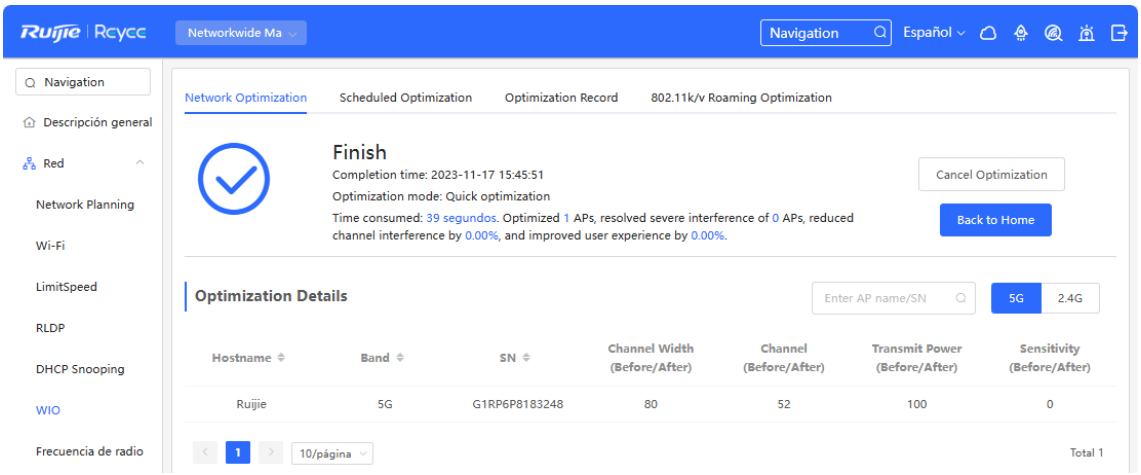
Cuando establezca la opción **Optimization mode** en **Deep optimization**, amplíe la **Configuración avanzada** para establecer el tiempo de búsqueda, el ancho de banda del canal y los canales seleccionados.



(2) Confirme los consejos y haga clic en **OK**.



Una vez que se inicie la optimización, espere pacientemente a que esta finalice. Tras finalizar la optimización, haga clic en **Cancel Optimization** para restaurar los parámetros optimizados de la radiofrecuencia a los valores predeterminados.



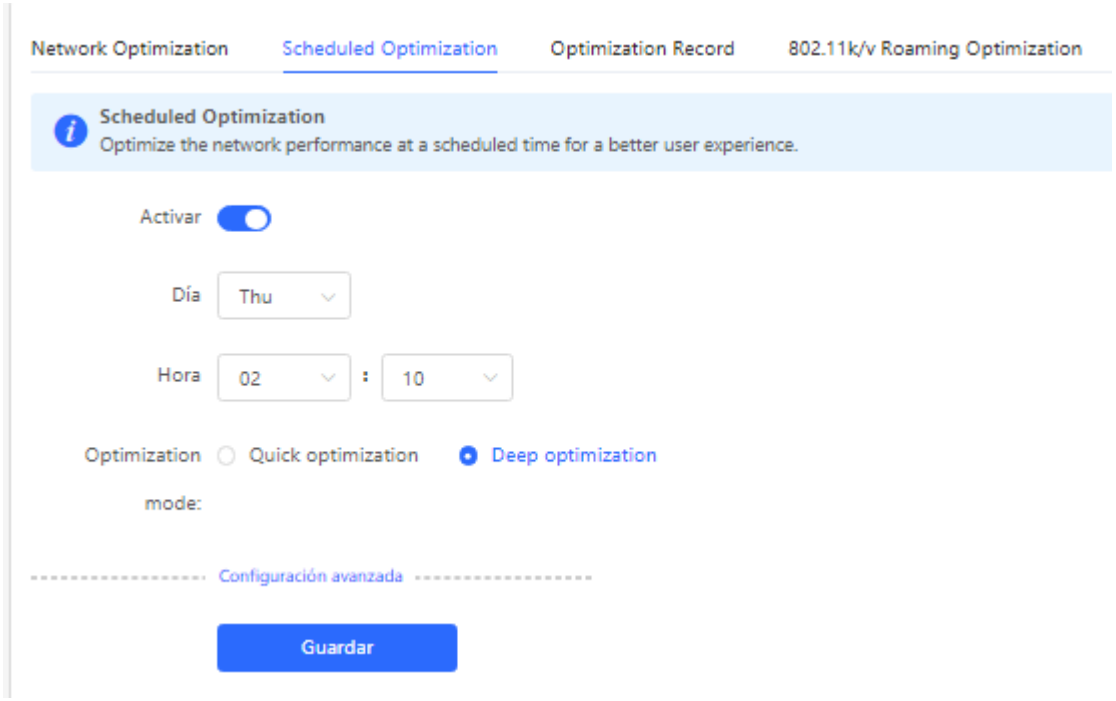
21.8.2 Optimización programada

Puede configurar la optimización programada para optimizar la red en el momento que desee. Se recomienda establecer la hora de la optimización programada al amanecer o durante los periodos de inactividad.

⚠ Precaución

Es posible que los clientes se desconecten durante la optimización y la configuración no se puede deshacer una vez que se inicia la optimización. Realice esta operación con precaución.

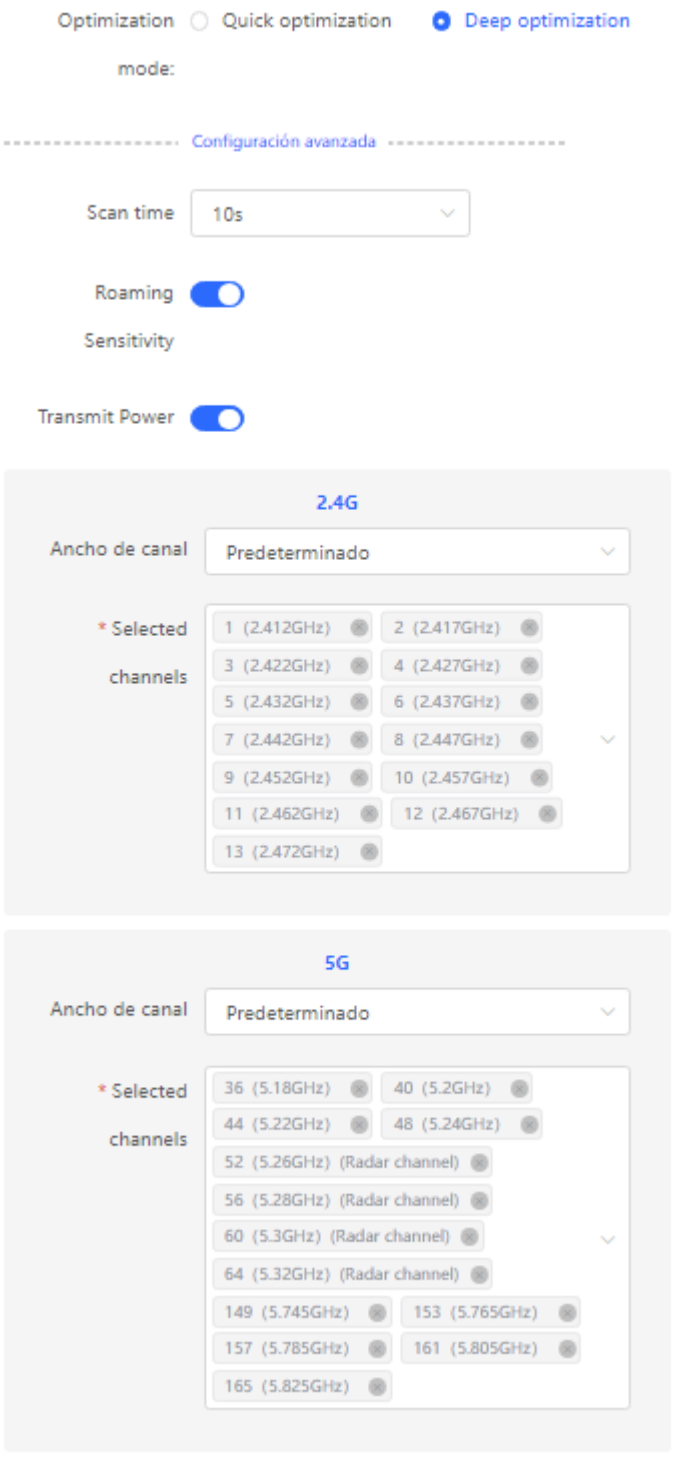
Seleccione **Networkwide Management > Red** > **WIO** > **802.11k/v Roaming Optimization**.



(1) Configure la hora programada.

(2) Seleccione el modo de optimización.

(3) (Opcional) Cuando establezca la opción **Optimization Mode** en **Deep optimization**, amplíe la **Configuración avanzada** para establecer el tiempo de búsqueda, el ancho de banda del canal y los canales seleccionados.



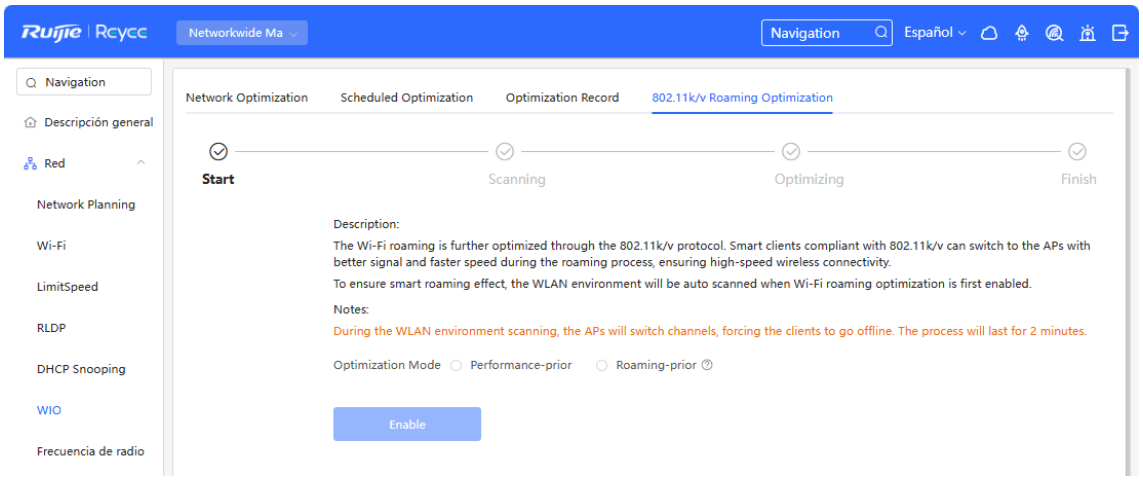
(4) Haga clic en **Guardar**.

21.8.3 Optimización de la itinerancia inalámbrica (802.11k/v)

La itinerancia inalámbrica puede optimizarse aún más mediante el uso del protocolo 802.11k/802.11v. Los puntos de conexión inteligentes compatibles con el estándar IEEE 802.11k/v pueden cambiar su asociación y conectarse a los access points con mejor señal y mayor velocidad, garantizando así una conectividad inalámbrica de alta velocidad.

Para garantizar una alta calidad del servicio de itinerancia inteligente, el entorno de la WLAN se analiza de forma automática cuando la función de optimización de la itinerancia inalámbrica se habilita por primera vez.

Seleccione **Networkwide Management > Red** > **WIO** > **802.11k/v Roaming Optimization**.



Precaución

Es posible que se fuerce la desconexión de los clientes durante la optimización. Tenga cuidado al realizar la operación.

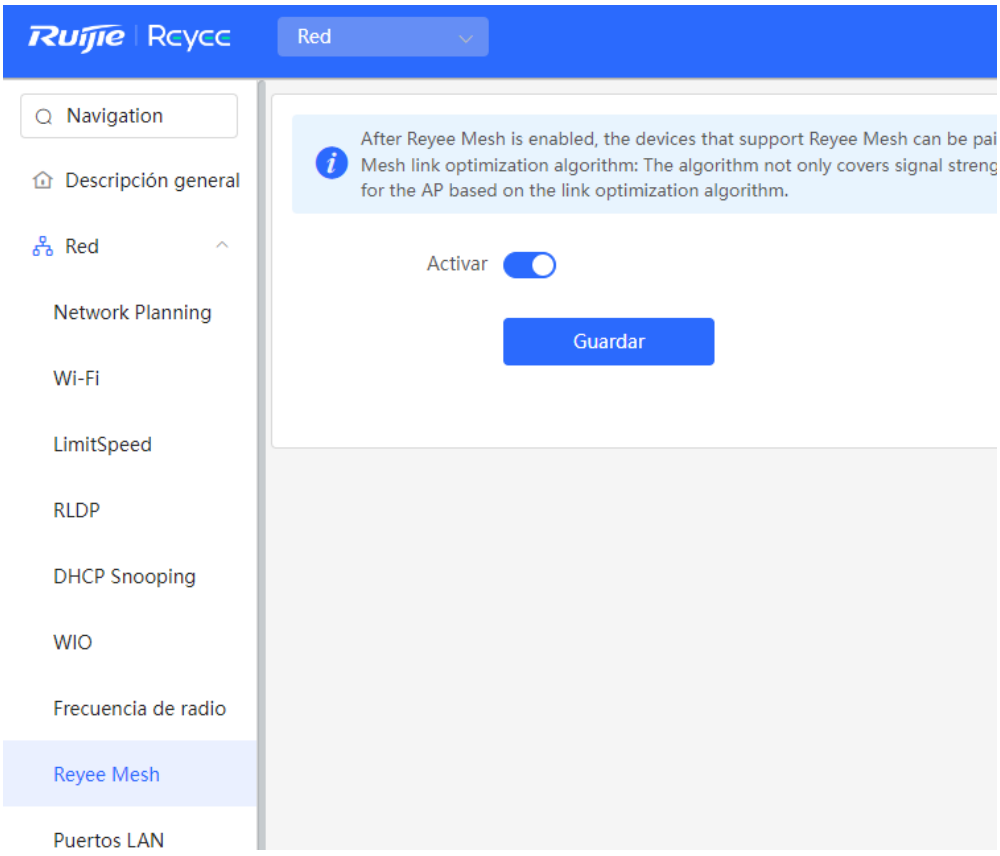
(1)

Haga clic en **Enable** para que se inicie la optimización.

21.9 Habilitar la función Reyee Mesh

Seleccione **Red** > **Red** > **Reyee Mesh**.

Cuando la función Reyee Mesh quede habilitada, los dispositivos que admiten EasyLink pueden emparejarse para formar una red de malla. Los dispositivos pueden buscar automáticamente nuevos routers alrededor de ellos y emparejarse entre ellos a través del botón **Mesh**, o iniciar sesión en la página de gestión para buscar y seleccionar un nuevo router al cual emparejarse.



21.10 Configuración de los puertos AP

Precaución

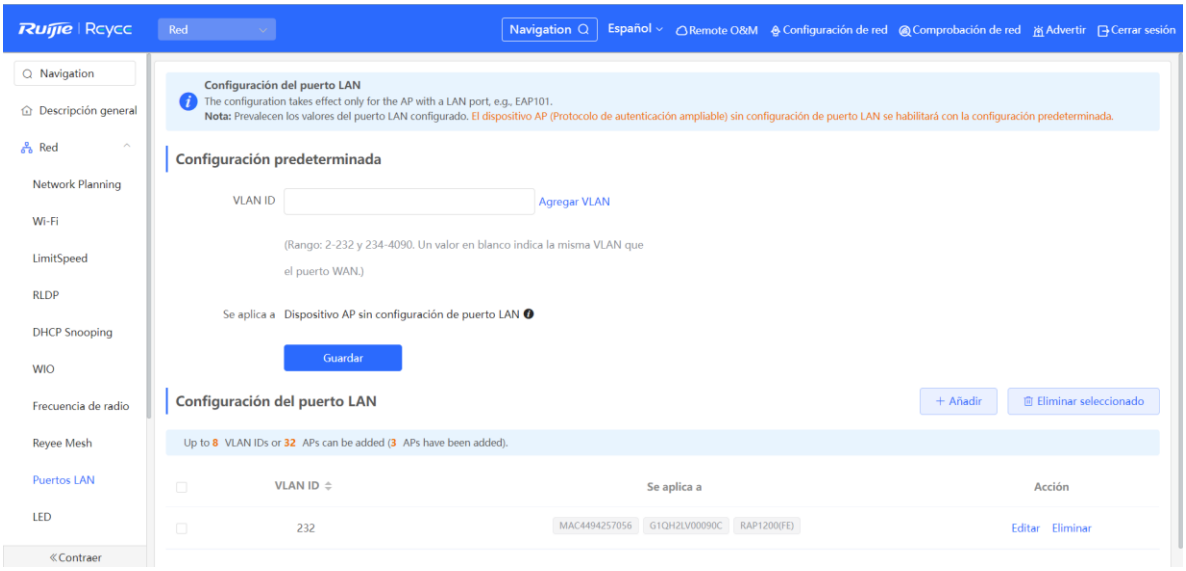
La configuración es válida solo en los AP que proporcionen puertos LAN cableados.

Seleccione **Red** > **Red** > **Puertos LAN**.

Seleccione **Red** > **Red** > **Puertos LAN.**

Ingrese una VLAN ID y haga clic en **Guardar** para configurar la VLAN a la que pertenecen los puertos cableados AP. Si el recuadro de VLAN ID está vacío, los puertos cableados y el puerto WAN pertenecen a la misma VLAN.

En modo SON, la configuración del puerto cableado AP aplica a todos los AP con puertos LAN cableados en la red. La configuración especificada para los AP en **Configuración del puerto LAN** es efectiva de manera preferente. Haga clic en **Añadir** para añadir la configuración del puerto cableado AP. Para los AP, si no se especifica ninguna configuración en **Configuración del puerto LAN**, la configuración predeterminada para puertos cableados AP se hará efectiva.


Ruijie | Rcycc
Red
Navigation
Español
Remote O&M
Configuración de red
Comprobación de red
Advertir
Cerrar sesión
Navigation
Descripción general
Red
Network Planning
Wi-Fi
LimitSpeed
RLDP
DHCP Snooping
WIO
Frecuencia de radio
Reyee Mesh
Puertos LAN
LED
Contraer
Configuración del puerto LAN
The configuration takes effect only for the AP with a LAN port, e.g., EAP101.
Nota: Prevalecen los valores del puerto LAN configurado. El dispositivo AP (Protocolo de autenticación ampliable) sin configuración de puerto LAN se habilitará con la configuración predeterminada.
Configuración predeterminada
VLAN ID
Agregar VLAN
(Rango: 2-232 y 234-4090. Un valor en blanco indica la misma VLAN que el puerto WAN.)
Se aplica a
Dispositivo AP sin configuración de puerto LAN
Guardar
Configuración del puerto LAN
+ Añadir
Eliminar seleccionado
Up to 8 VLAN IDs or 32 APs can be added (3 APs have been added).
VLAN ID
Se aplica a
Acción
232
MAC4494257056
G1QH2LV00090C
RAP1200(FE)
Editar
Eliminar