Routers serie Ruijie Reyee RG-EG

Manual de implementación

Versión del documento: V1.2
Fecha: 02 de agosto de 2023

Copyright

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
- Sitio web de asistencia técnica: https://www.ruijienetworks.com/support
- Portal de casos: https://caseportal.ruijienetworks.com
- Comunidad: https://community.ruijienetworks.com
- Correo electrónico de asistencia técnica: service_rj@ruijienetworks.com

Reglas de uso

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

Símbolos de la interfaz	Descripción	Ejemplo
Negritas	1. Nombre de los botones 2. Nombre de las ventanas, pestañas, campos y elementos del menú 3. Enlace	1. Haga clic en **OK**. 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 del procedimiento. A continuación, se describen los significados de los mismos.

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.

Precaución

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

Nota

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. Nota

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

- No obstante, el ejemplo del tipo de puerto puede ser diferente a 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.

Índice

1 Presentación del producto

El router de la serie Reyee RG-EG es un router administrado en la nube y está diseñado para villas y casas, restaurantes, oficinas pequeñas y hoteles. Es asequible, pequeño y fácil de usar, con un ancho de banda de 500–600 Mbps, que admite hasta 200 clientes.

Los routers de la serie Reyee RG-EG proporcionan redes líderes en la industria con funciones de detección automática para routers, conmutadores y dispositivos inalámbricos.

Los routers de la serie Reyee RG-EG pueden realizar configuraciones de VLAN por puerto para lograr el aislamiento de puertos, e integrar controles de flujo inteligentes para lograr una planeación de red completa y hacer diagnósticos de redes locales y remotas.

1.1 Modelos

Los routers de la serie RG-EG cuentan con cinco modelos.

Modelo	10/100/1000 Puerto Ethernet Base-T	Número máximo de clientes concurrentes	Ancho de banda recomendado	Capacidad de gestión
RG-EG105G-P	5 (compatibilidad con PoE)	100	Ancho de banda asimétrico de 500 Mbps (control de flujo deshabilitado) Ancho de banda asimétrico de 300 Mbps (control de flujo habilitado)	Modo AC: 300 Modo router: 32
RG-EG105G-P V2	5 (compatibilidad con PoE)	100	Ancho de banda asimétrico de 500 Mbps (control de flujo deshabilitado) Ancho de banda asimétrico de 600 Mbps (control de flujo habilitado)	Modo AC: 300 Modo router: 32

Modelo	10/100/1000 Puerto Ethernet Base-T	Número máximo de clientes concurrentes	Ancho de banda recomendado	Capacidad de gestión
RG-EG105G	5	100	Ancho de banda asimétrico de 500 Mbps (control de flujo deshabilitado) Ancho de banda asimétrico de 300 Mbps (control de flujo habilitado)	Modo AC: 300 Modo router: 32
RG-EG105G V2	5	100	Ancho de banda asimétrico de 600 Mbps (control de flujo deshabilitado) Ancho de banda asimétrico de 500 Mbps (control de flujo habilitado)	Modo AC: 300 Modo router: 32
RG-EG105GW	5	100 (número recomendado de terminales inalámbricas: 60)	Ancho de banda asimétrico de 500 Mbps (control de flujo deshabilitado) Ancho de banda asimétrico de 300 Mbps (control de flujo habilitado)	Modo router: 32
RG-EG210G-E	10	200	Ancho de banda asimétrica de 1 Gbps (control de flujo deshabilitado) Ancho de banda asimétrica de 1 Gbps (control de flujo habilitado)	Modo AC: 500 Modo router: 150

Modelo	10/100/1000 Puerto Ethernet Base-T	Número máximo de clientes concurrentes	Ancho de banda recomendado	Capacidad de gestión
RG-EG210G-P	10 (compatibilidad con PoE)	200	Ancho de banda asimétrico de 600 Mbps (control de flujo deshabilitado) Ancho de banda asimétrico de 500 Mbps (control de flujo habilitado)	Modo AC: 500 Modo router: 150
RG-105GW(T)	5	100	600 Mbps (1500 bytes, NAT + auditoría de flujos) 400 Mbps (1500 bytes, NAT + autenticación, identificación de la aplicación, auditoría y control de flujos)	No. de dispositivos gestionables (AP + switches NBS, modo router, incluyendo este dispositivo): 32 No. de dispositivos gestionables (AP + switches NBS, modo repetidor cableado, incluyendo este dispositivo): N/A No. de dispositivos gestionables (AP + switches NBS, modo repetidor cableado, incluyendo este dispositivo): 32 No. de dispositivos gestionables (switches ES): 128

1.2 Indicadores LED

Indicador LED	Estado	Descripción
SYS	Parpadeo	Parpadeo rápido (a 8 Hz): el router se está iniciando. Parpadeo lento (a 0.5 Hz): no se localiza la red. Un parpadeo largo seguido de tres parpadeos cortos (a 0.8 Hz): el router está fallando. Dos parpadeos consecutivos (a 0.8 Hz): ● El router se está restaurando a la configuración de fábrica. ● El router está actualizando el software. Nota: en este caso, no apague el router.
	Encendido fijo	El router está funcionando adecuadamente.
	Sin luz	El router no está encendido.
Puerto	Parpadeo	El puerto está conectado y está enviando y recibiendo tráfico.
	Encendido fijo	El puerto está conectado y no está enviando ni recibiendo tráfico.
	Sin luz	No se detectó ningún enlace para este puerto.
Red de malla	Sin luz	● El emparejamiento de malla no se ha implementado. ● El retransmisor inalámbrico no se ha configurado.
	Parpadeo alternado	Emparejamiento de malla en proceso.
	Tres barras encendidas	● La intensidad de la señal de la red de malla es alta. ● La intensidad de la señal del retransmisor inalámbrico es alta.
	Dos barras encendidas	● La intensidad de la señal de la red de malla es media. ● La intensidad de la señal del retransmisor inalámbrico es media.
	Una barra encendida	● La intensidad de la señal de la red de malla es baja. ● La intensidad de la señal del retransmisor inalámbrico es baja.

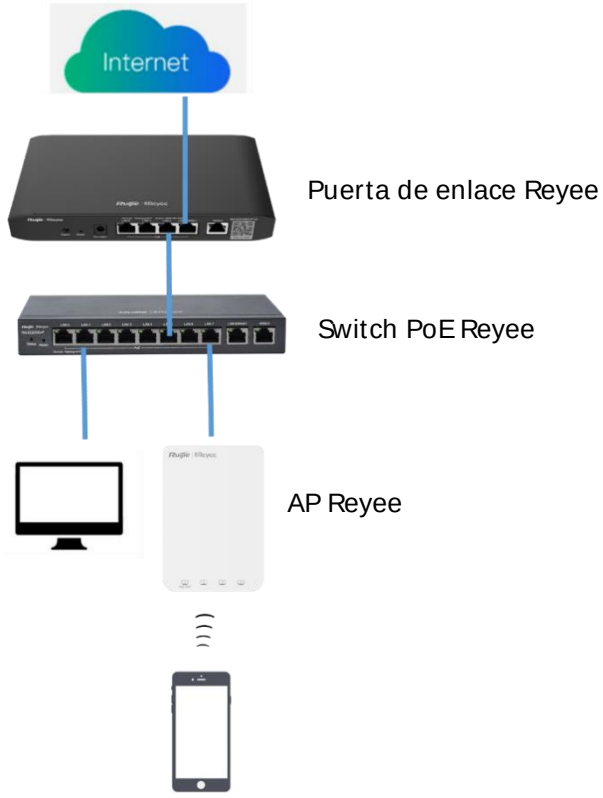
1.3 Botón

Botón	Descripción
Restablecimiento	Presione el botón **Restablecimiento** por menos de 2 segundos para reiniciar el dispositivo. Presione el botón **Restablecimiento** por más de 5 segundos para restablecer la configuración de fábrica. (Suelte el botón cuando el indicador LED de estado del sistema emita una luz intermitente). La dirección IP de gestión predeterminada es http://192.168.110.1.
Botón de la red de malla	Presione el botón **Malla** por menos de 2 segundos para realizar la vinculación con la red de malla.

2 Primeros pasos

2.1 Planeación de red

La siguiente imagen muestra una topología típica de un router Reyee.



El servidor DHCP cuenta con dos grupos de direcciones en el router Reyee: La dirección 192.168.110.0/24 en VLAN 1 es para los dispositivos de esta red y la 192.168.10.0/24 en VLAN 10 es para los clientes de esta red.

Los siguientes puertos se utilizan para gestionar la plataforma Ruijie Cloud. Para que los dispositivos se puedan conectar en línea a través de esta plataforma, asegúrese de que dichos 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	

2.2 Instalación del router

2.2.1 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 sin polvo.
   - No coloque los dispositivos en zonas de paso.
   - No utilice ropa holgada ni accesorios que puedan engancharse o enredarse en algún dispositivo durante la instalación y el mantenimiento.
2. **Traslado**
   - Evite mover 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 algún procedimiento que involucre 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 dejar sin supervisión 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 la 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 inadecuado 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.

2.2.2 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 routers Reyee EG.

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 una vida útil y prolongada del router, mantenga la temperatura y humedad adecuadas en la sala de equipos.

Si la temperatura y la humedad de la sala de equipos no cumplen 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. En ocasiones, los materiales pueden sufrir cambios mecánicos 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, ocasionando el 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 del AP y ocasiona 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 una resistencia a la interferencia. 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 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 CA TN 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 de 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 de los rayos.

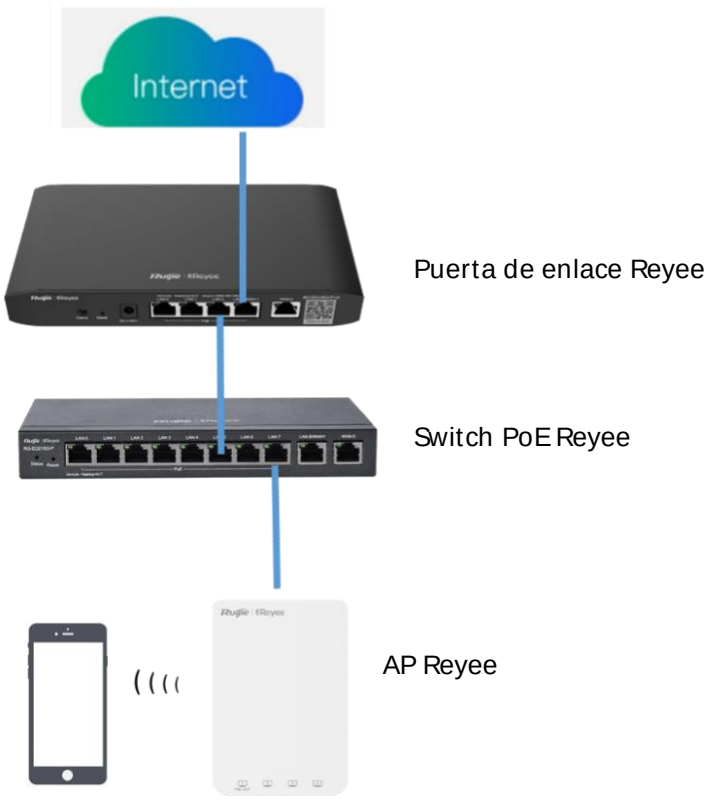
2.2.3 Pasos para la instalación

Para más detalles acerca de los pasos para la instalación, consulte la *Guía de referencia e instalación del hardware.*

2.3 Instalación rápida

2.3.1 Instalación rápida a través de Ruijie Cloud App

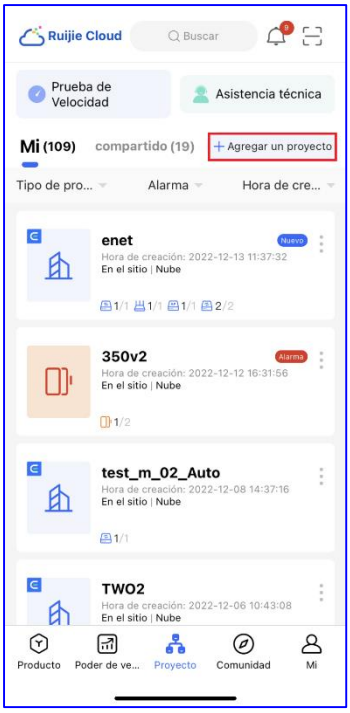
El router Reyee se utiliza frecuentemente con el switch PoE Reyee y un punto de acceso remoto (RAP) Reyee.



Conecte los dispositivos a través de Ruijie Cloud App para su configuración y mantenimiento vía remota.

(1) Cree un proyecto.

a Abra Ruijie Cloud App, haga clic en **Agregar un proyecto** y seleccione **Conectarse a Wi-Fi**.



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

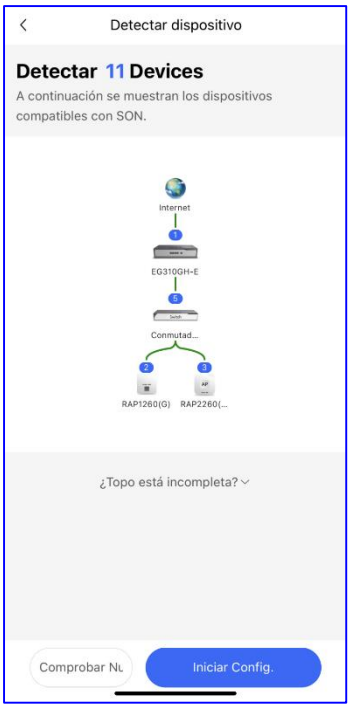
Nota

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.

c Haga clic en **Conectar** y acceda al SSID **@Ruijie-mxxxx**.

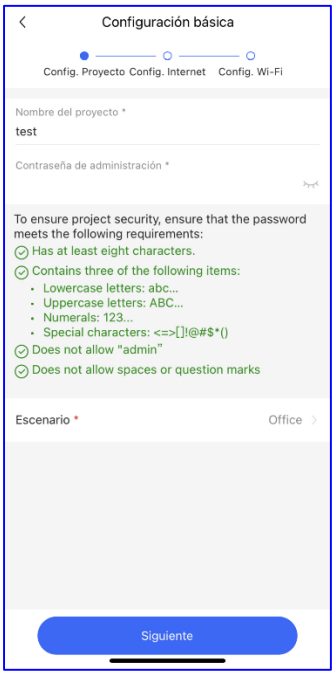
d Después de conectarse al SSID **@Ruijie-mxxxx**, Cloud App generará la topología para detectar todos los dispositivos en la red SON.

e Después de que haya detectado los dispositivos, Cloud App los mostrará junto con la topología.



(2) Haga clic en **Iniciar Config.** para realizar la configuración básica de este proyecto.

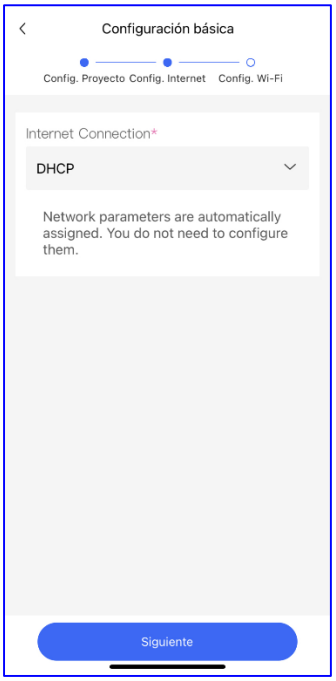
a Configure el **Nombre del proyecto** y la **Contraseña de administración**.



b Después, seleccione el escenario de este proyecto según lo requiera.

(3) Configure el Internet.

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



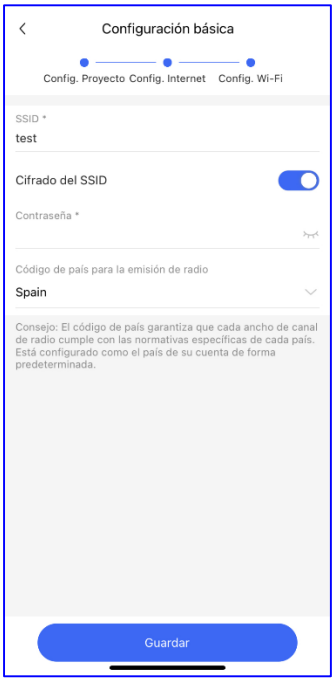
(4) Configure el SSID.

a Ingrese el nombre del SSID.

b Configure la red como abierta para permitir que los clientes tengan acceso al SSID.

c Configure la contraseña de este SSID.

d Seleccione el código del país.



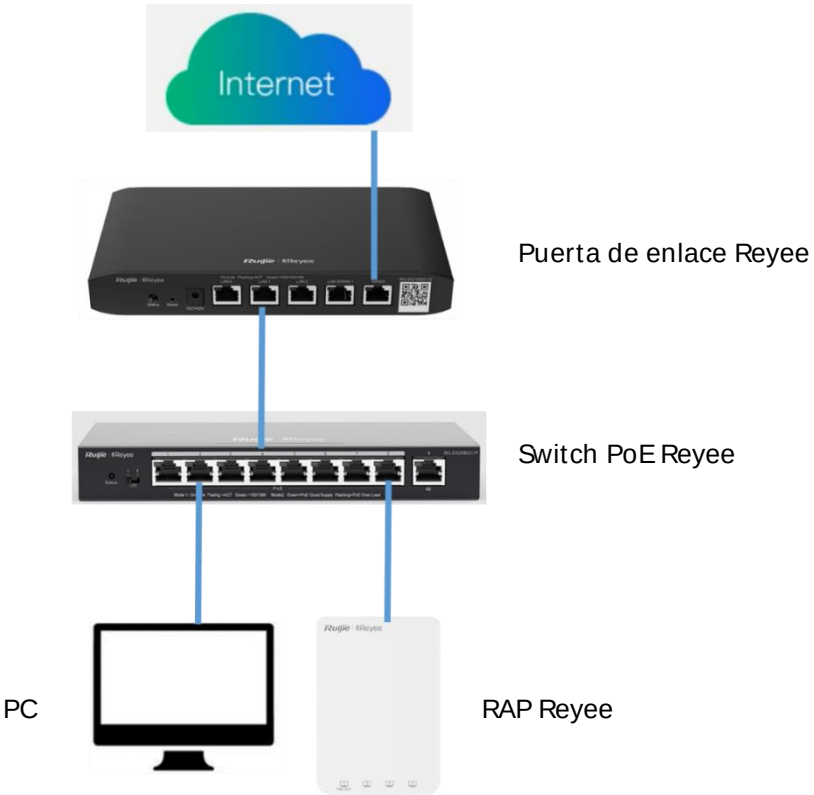
e La configuración se sincronizará con la red.

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

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

2.3.2 Instalación rápida a través de la Reyee Eweb

El router Reyee se utiliza frecuentemente con el switch PoE Reyee y un punto de acceso remoto (RAP) Reyee.

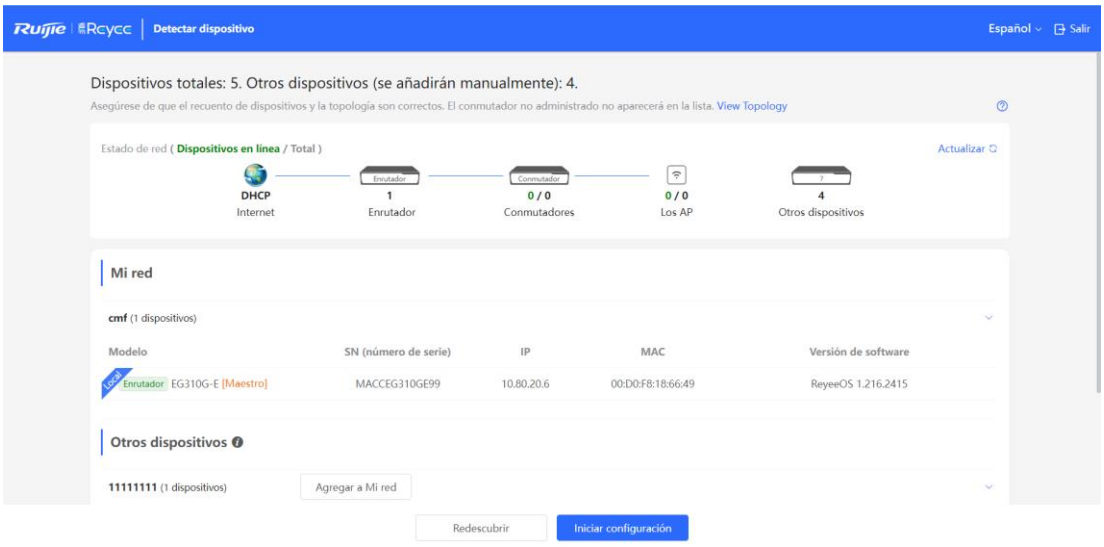


Puede utilizar un sistema de administración web para configurar y dar mantenimiento al router Reyee.

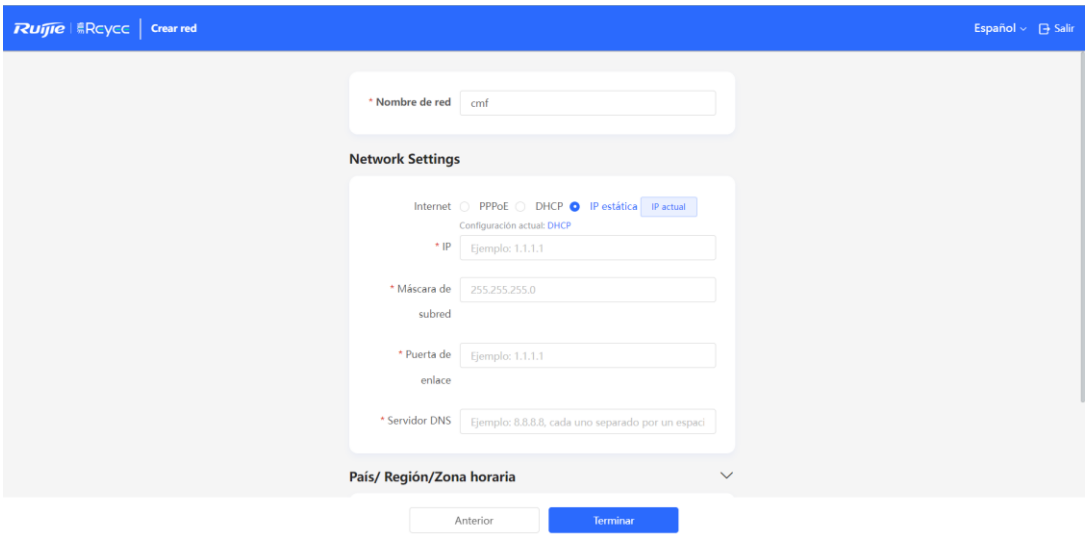
(1) Conecte una PC a un switch PoE, configure la dirección IP de la PC en la dirección IP estática 192.168.110.x.

(2) Ingrese 192.168.110.1 en la barra de dirección para que el navegador inicie sesión en la Eweb del EG.

Todos los dispositivos de la red se mostrarán en la Eweb.



(3) Haga clic en **Iniciar configuración** para un inicio rápido de la red.

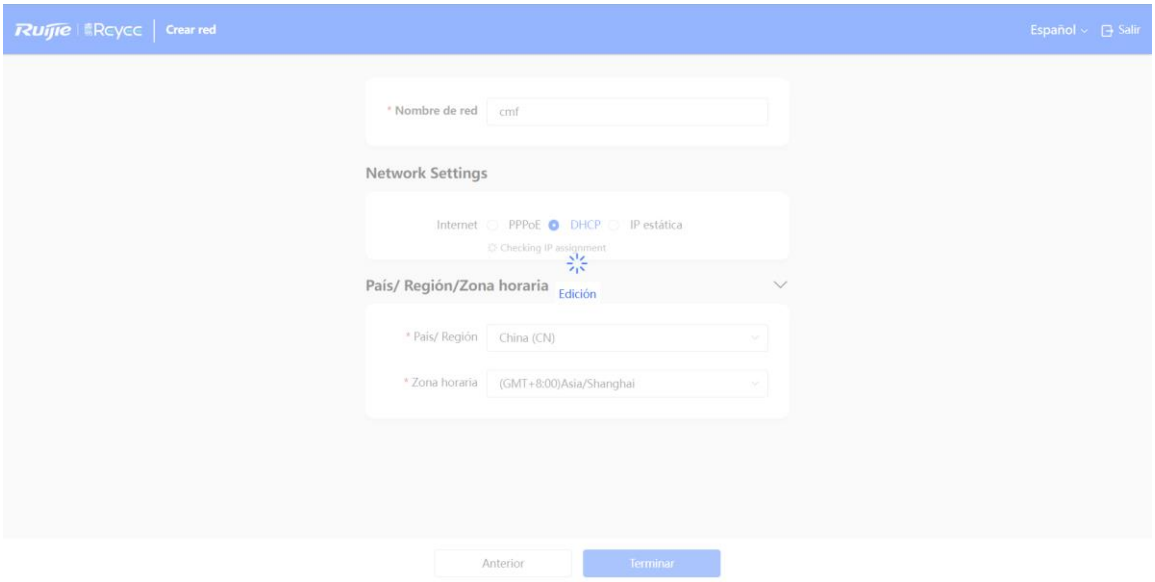


a Ingrese el nombre de la red y configure el modo de acceso a Internet de esta.

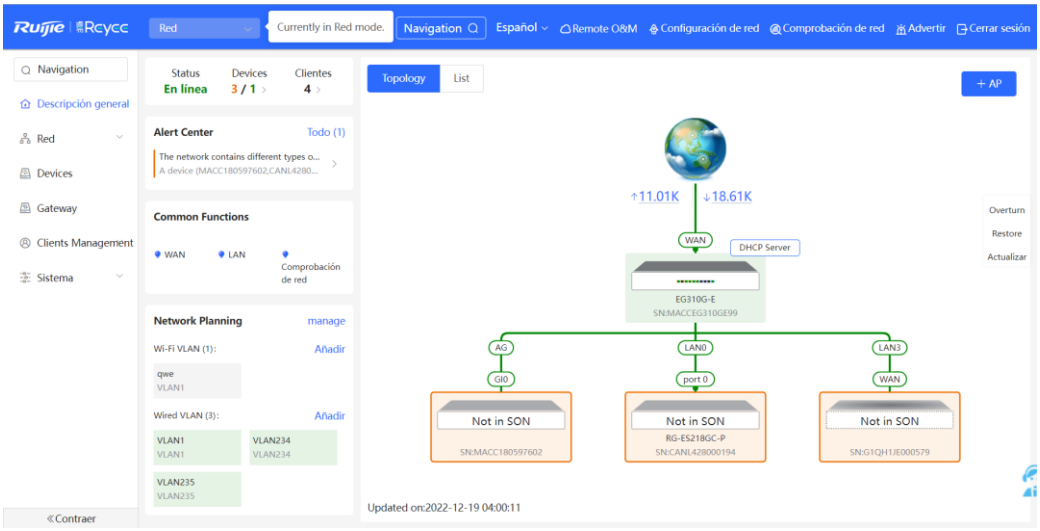
b Ingrese la contraseña del SSID o configúrelo como abierto.

c Seleccione el país o región donde se encuentra.

(4) Haga clic en **Terminar**. La configuración se aplicará y se activará.



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



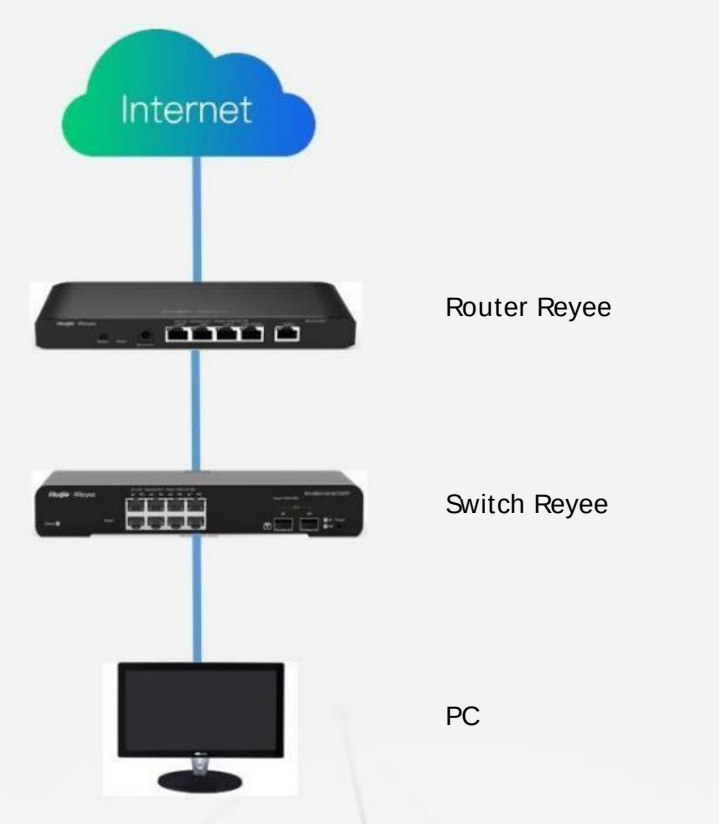
3 Administración del dispositivo

3.1 Inicio de sesión

La Eweb es una red de gestión basada en la web y se utiliza para administrar o configurar dispositivos. Se puede acceder a la Eweb mediante un navegador como Google Chrome. La gestión basada en la web involucra un servidor web y un cliente web. El servidor web, integrado en un dispositivo, se utiliza para recibir y procesar las solicitudes del cliente y para devolver los resultados del procesamiento al cliente web. El cliente web se refiere generalmente a un navegador, como Google Chrome, IE o Firefox.

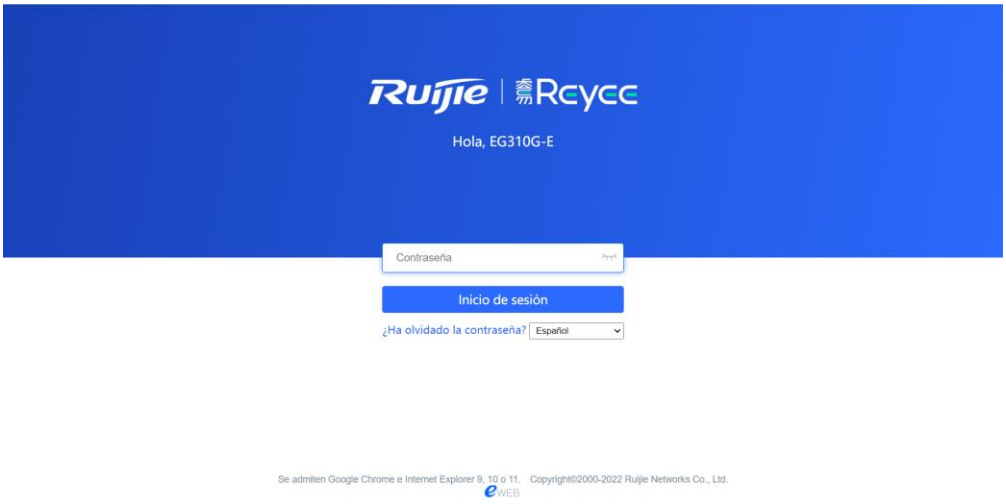
Los routers Reyee admiten tanto la gestión de la interfaz web como la gestión remota a través de la aplicación y la plataforma Ruijie Cloud, con acceso gratuito ilimitado. En ellas puede visualizar el estado de la red, modificar su configuración y resolver fallas fácilmente.

Se puede acceder al sistema de gestión Eweb de un conmutador de acceso o de agregación a través del navegador de la PC para administrar o configurar el dispositivo.



1. Configure el modo asignación de IP en la PC para obtener la dirección IP automáticamente.
2. Visite http://192.168.110.1 a través de Google Chrome.
3. Ingrese la contraseña en la página de inicio y haga clic en **Inicio de sesión**.

   La contraseña predeterminada es **admin**.



Para el dispositivo Reyee EG, utilice 192.168.110.1 o 10.44.77.254 para tener acceso a él.

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

Visite https://10.44.77.253 para iniciar sesión en el dispositivo maestro de la red Reyee.

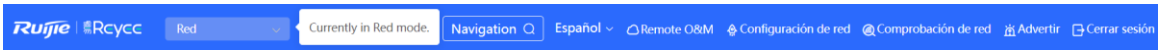
3.2 Cambiar de una página de administración a otra

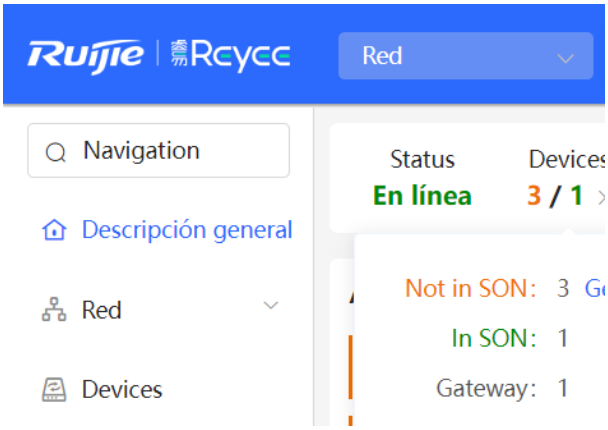
Cuando deshabilita la función de descubrimiento de red de autoorganización, la página web se encuentra en modo Dispositivo local. (La función de descubrimiento de red de autoorganización se habilita al momento de la entrega. Para obtener información más detallada, consulte la sección 3.1 Cambiar el modo de trabajo).

Después de habilitar la función de descubrimiento de red de autoorganización, puede cambiar de la página web de la red a la del dispositivo local. Haga clic en el modo de gestión actual en la barra de navegación y seleccione el modo deseado de la lista desplegable.

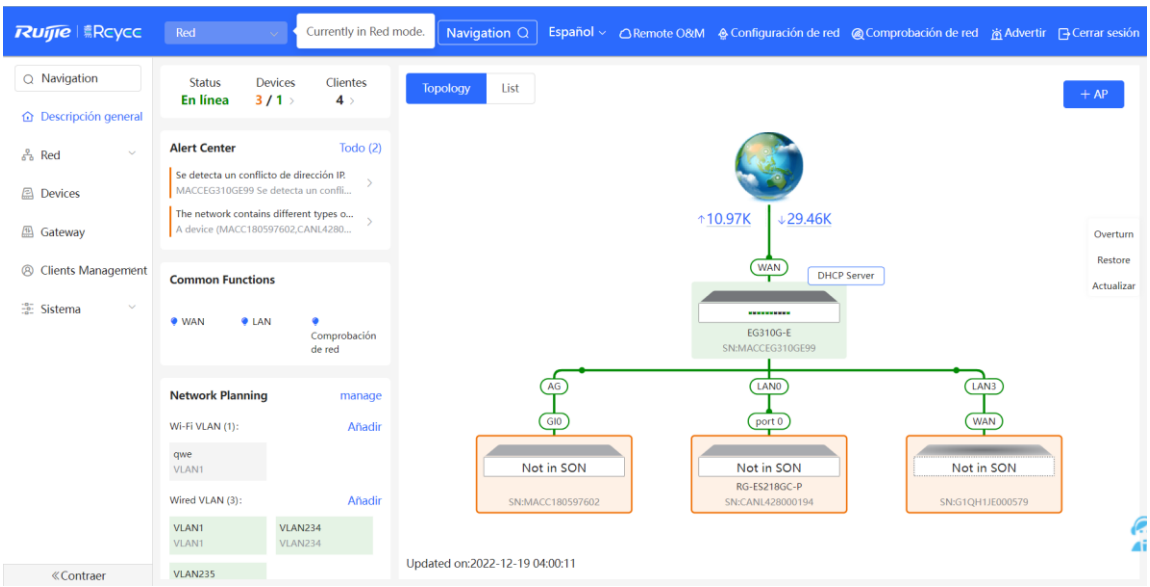
Modo Red: visualice la información de gestión de todos los dispositivos en la red para configurarlos desde una perspectiva en conjunto.

Modo Dispositivo local: configure el dispositivo en el que inició sesión.

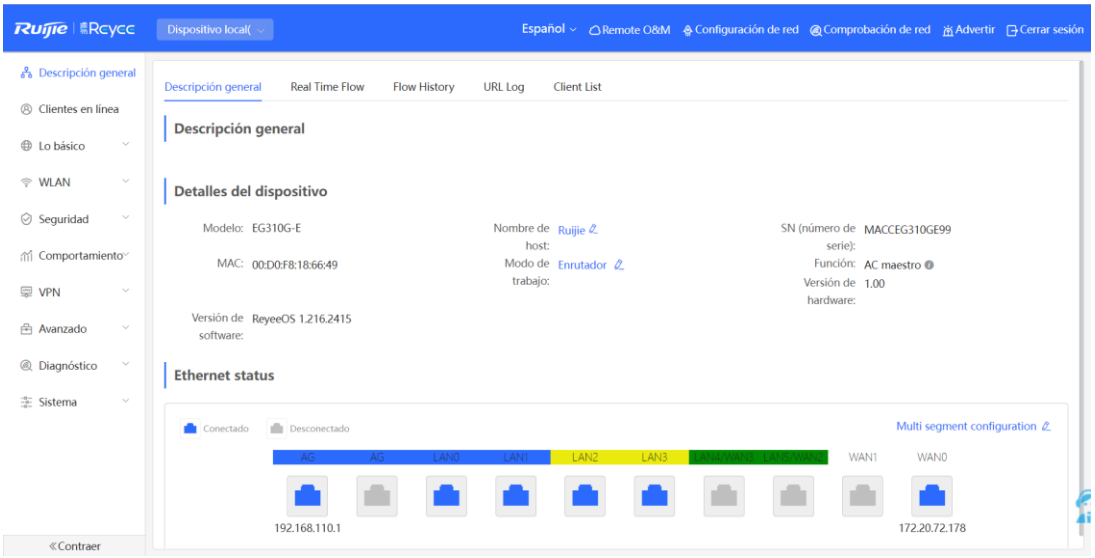




Página de la red:



Página del dispositivo local:



3.3 Configuración de la contraseña

Cambie la contraseña de manera regular para garantizar la seguridad de la cuenta.

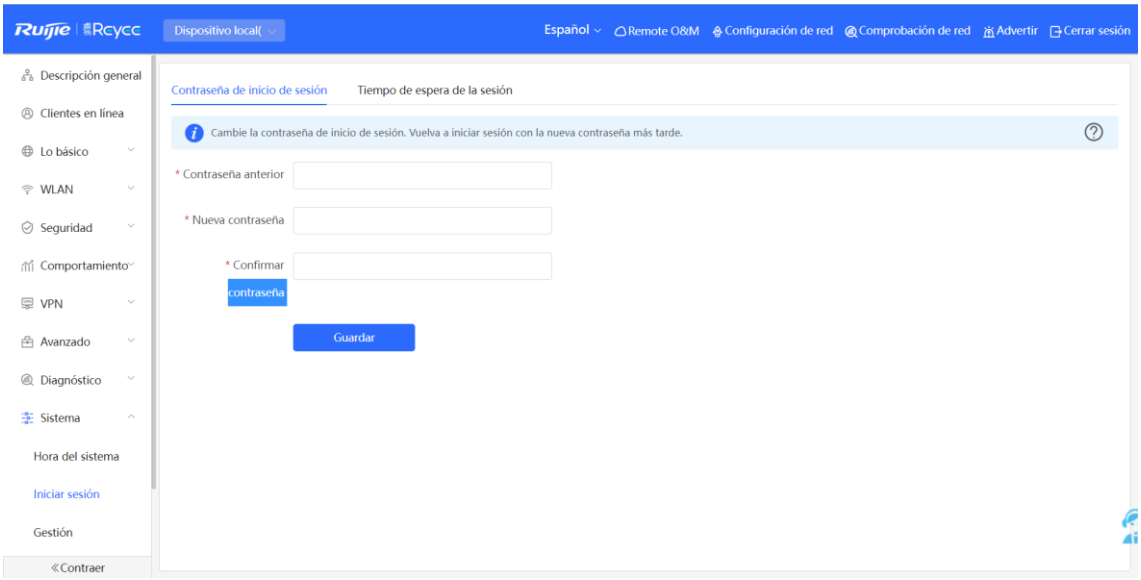
(1) Inicie sesión en el sistema de gestión web usando la dirección IP predeterminada.

(2) Cambie al modo **Dispositivo local**.

(3) Seleccione **Sistema** > **Iniciar sesión** > **Contraseña de inicio de sesión**.

(4) Ingrese la contraseña anterior y la contraseña nueva.

(5) Haga clic en **Guardar**.



Después de guardar la configuración, utilice la nueva contraseña para iniciar sesión.

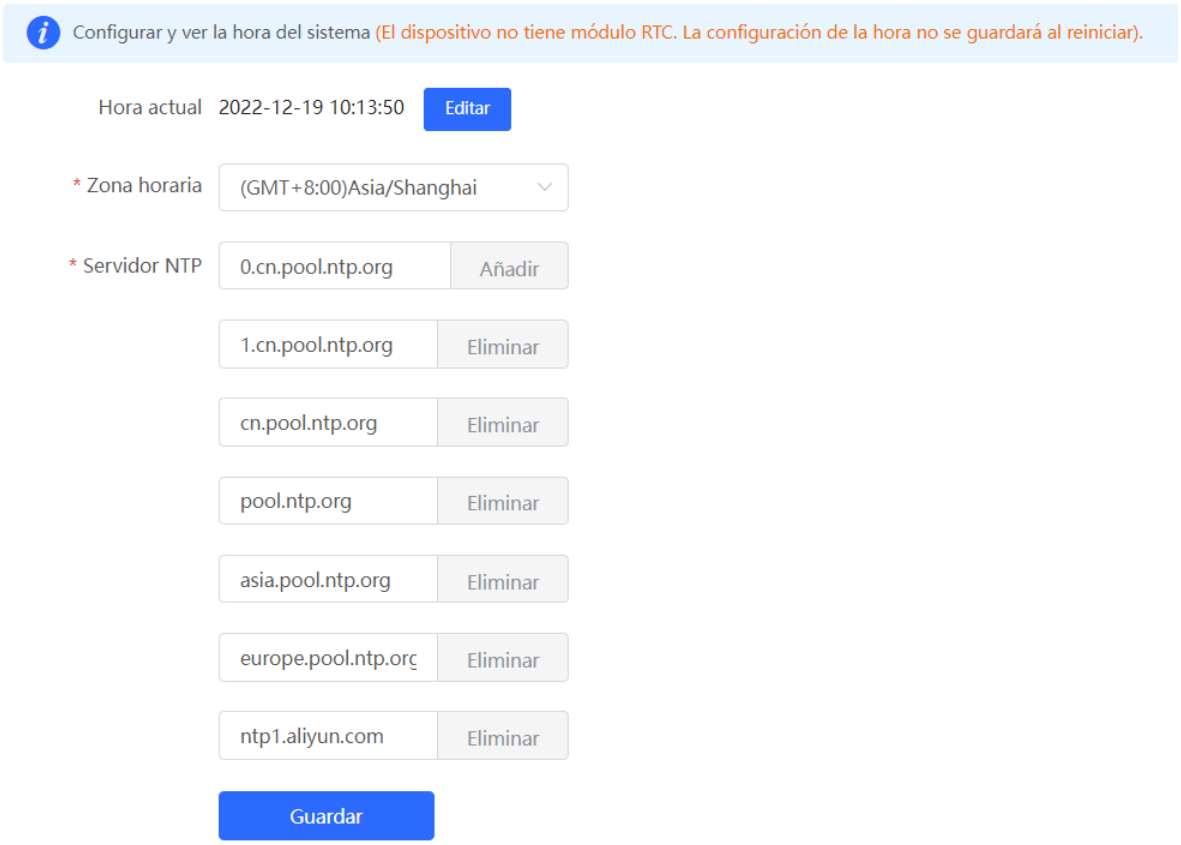
Precaución

En el modo de red SON, la contraseña de inicio de sesión de todos los dispositivos en la red se cambiará de manera sincronizada.

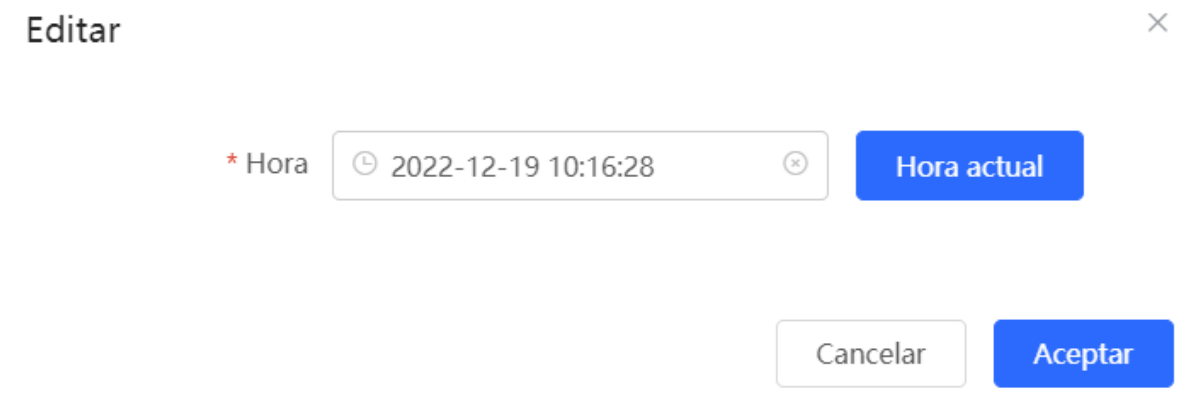
3.4 Configuración de la hora del sistema

Seleccione **Sistema** > **Hora del sistema**.

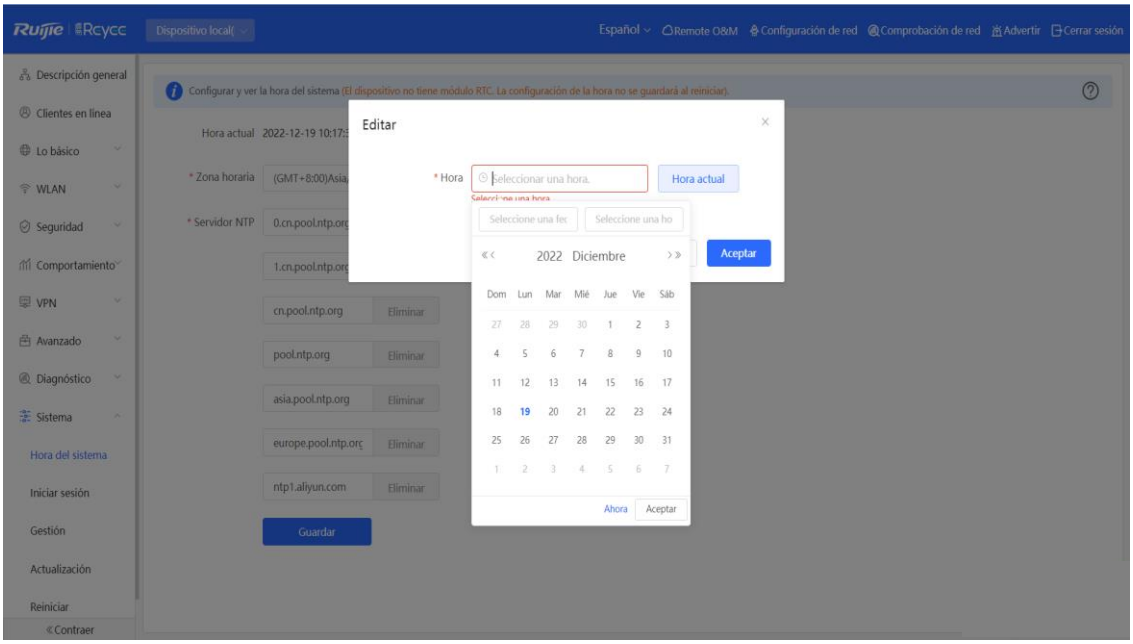
Puede visualizar la hora actual del sistema. Si la hora es incorrecta, compruebe y seleccione la zona horaria local. Si la zona horaria es correcta, pero la hora sigue siendo incorrecta, haga clic en **Editar** para configurar la hora manualmente. Además, el dispositivo admite los servidores de Protocolo de hora de red (NTP). Por defecto, varios servidores actúan como respaldo entre ellos. Se puede añadir o eliminar el servidor local, según se requiera.

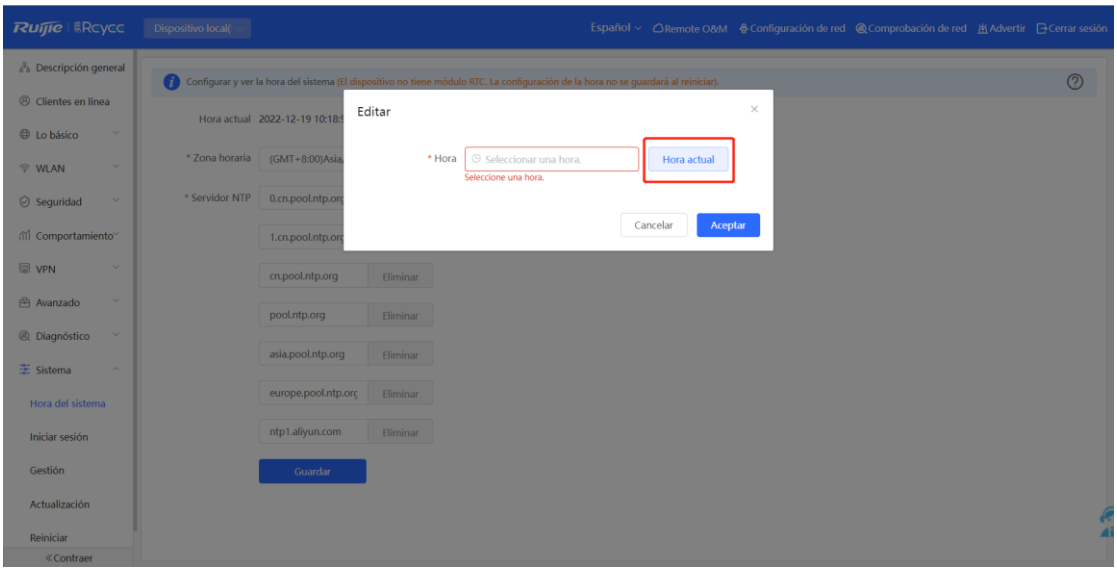


Seleccione **Hora actual** > **Editar** > **Hora actual**. La hora actual del sistema aparecerá automáticamente en el campo correspondiente.

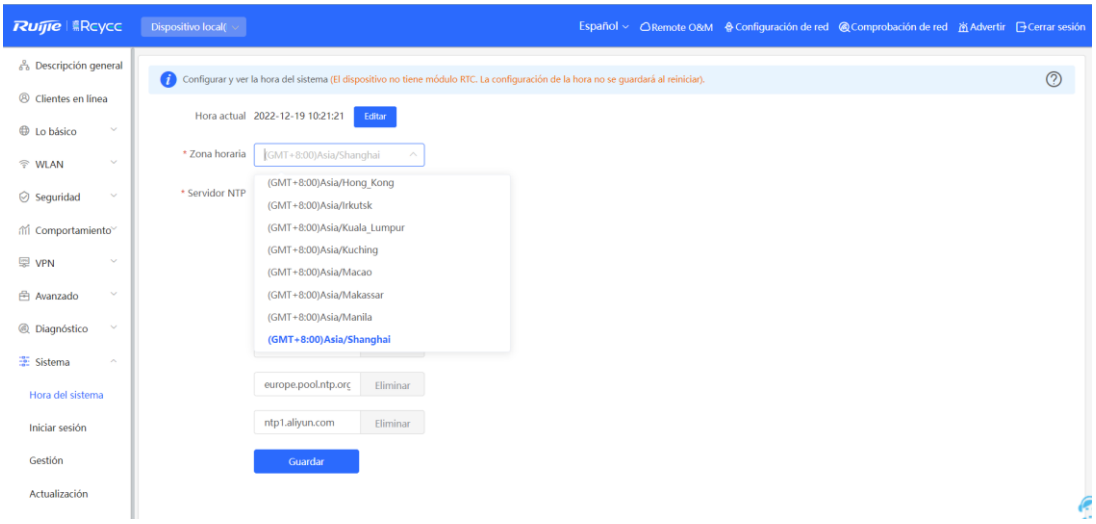


- Edite manualmente la hora actual del sistema o haga clic en **Hora actual** para sincronizarla automáticamente.

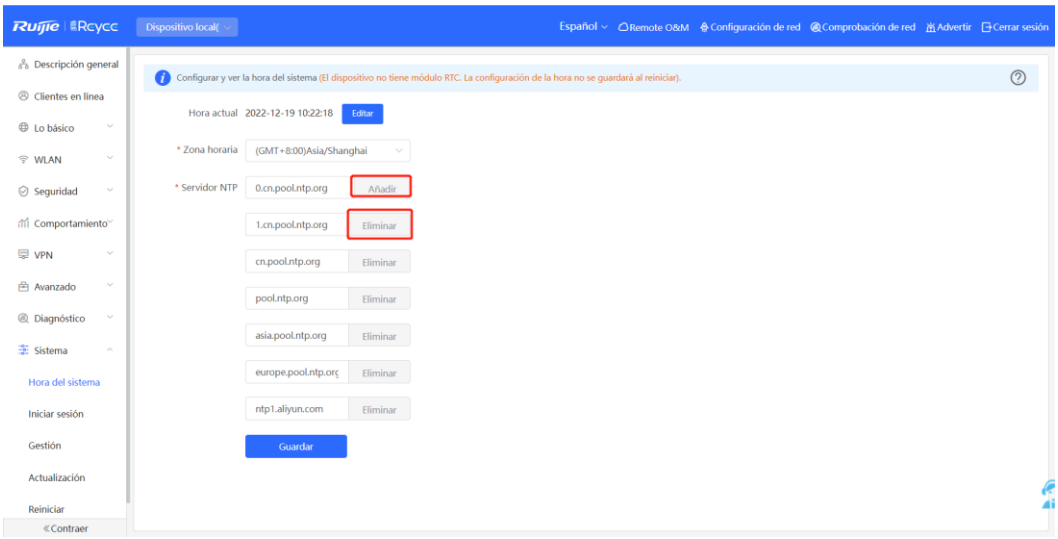




- Seleccione manualmente uno de los valores de la lista desplegable de **Zona horaria**.



- Añada o elimine el servidor NTP.



3.5 Configuración de una actualización

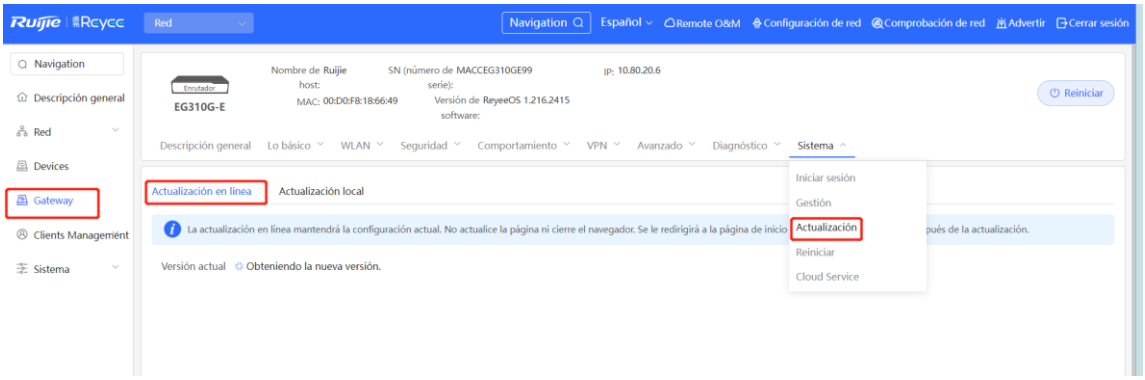
Para usar nuevas funciones, actualice el router con la versión más reciente. Hay dos métodos para actualizar los routers: en línea y local.

3.5.1 Actualización en línea

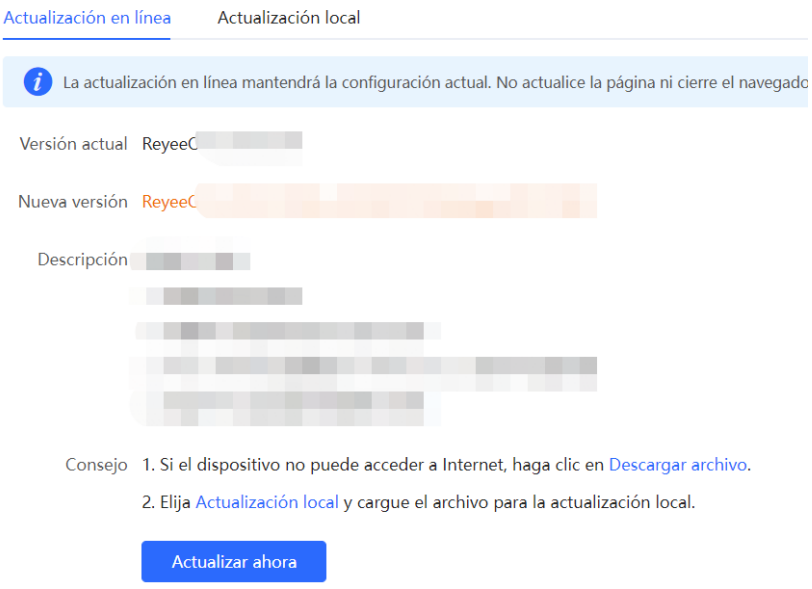
El router que está conectado a Internet se puede actualizar en línea.

Inicie sesión en la Eweb del dispositivo.

(1) Seleccione **Gateway** > **Sistema** > **Actualización** > **Actualización en línea**.



- Si aparece un mensaje indicando que la versión actual es la más reciente, no es necesario actualizar el router.
- Si hay una nueva versión disponible, haga clic en **Actualizar ahora** para actualizar el router. Este procedimiento no afecta la configuración actual, pero el router se reiniciará después de actualizarse exitosamente. No actualice la página o cierre el navegador durante la actualización. Después de la actualización, aparecerá automáticamente la página de inicio de sesión.



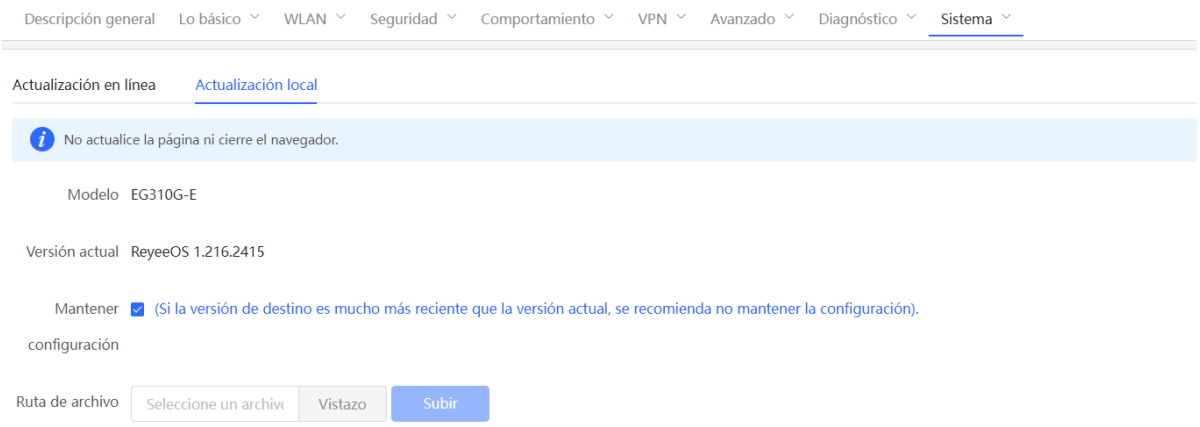
3.5.2 Actualización local

Actualice el router cargando un paquete de actualización en forma local.

Confirme la versión que desea y descargue el paquete de actualización del sitio web oficial.

(1) Inicie sesión en la Eweb del dispositivo.

(2) Seleccione **Gateway** > **Sistema** > **Actualización** > **Actualización local**.

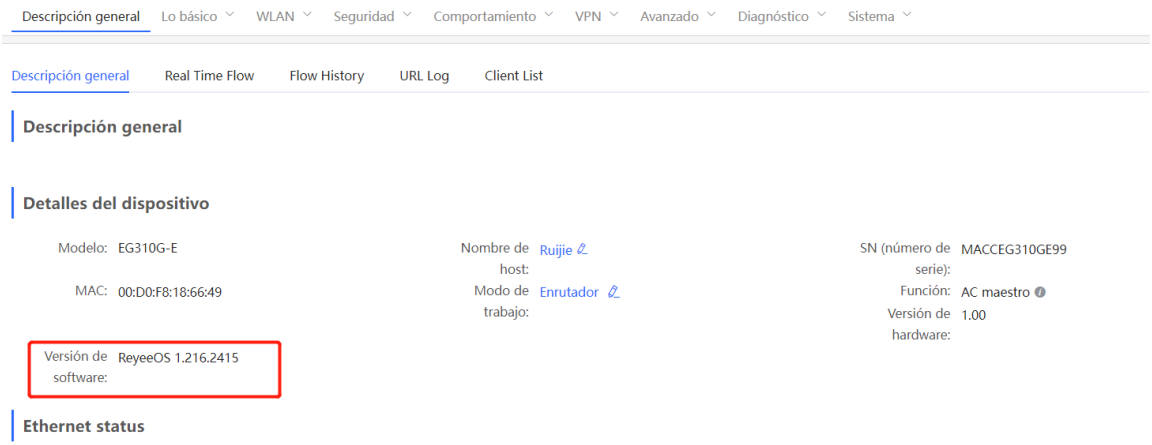


(3) Haga clic en **Vistazo**, seleccione el paquete de actualización en una PC local y haga clic en **Subir** para cargar el archivo.

(4) Cuando haya cargado el archivo exitosamente, el sistema mostrará la información del paquete de actualización y le preguntará si desea llevarla a cabo. Haga clic en **Aceptar** para iniciar la actualización.

(5) Cuando la actualización se haya completado, seleccione **Gateway** > **Descripción general**, y revise si la versión actual coincide con la versión deseada en la ventana **Detalles del dispositivo**.

- Si la versión es consistente, la actualización fue exitosa.
- Si la versión no es consistente, la actualización falló. Vuelva a intentarlo más tarde o póngase en contacto con RITA.

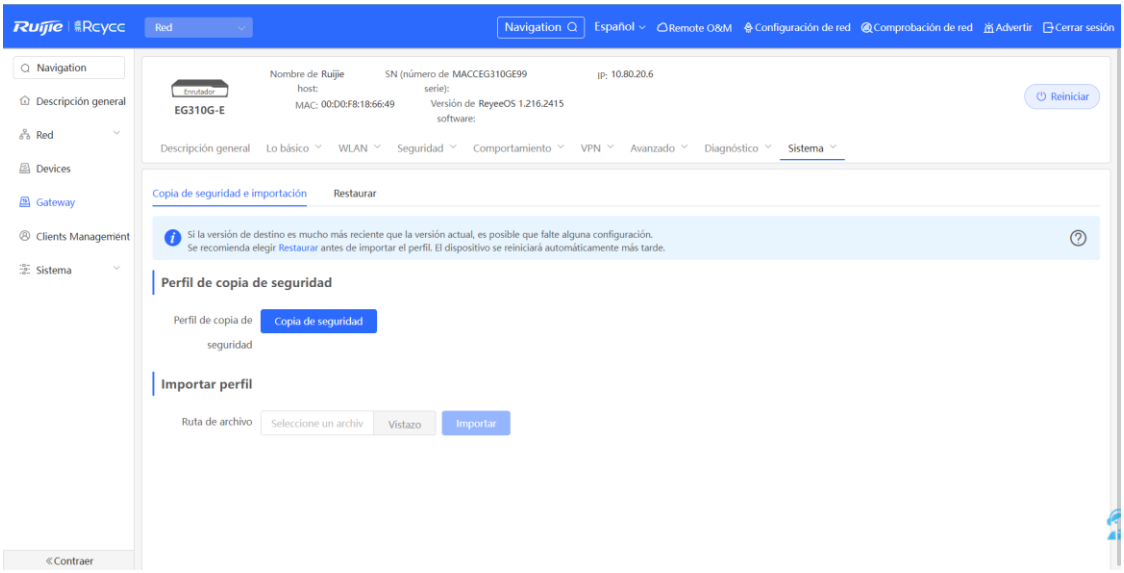


3.6 Respaldo o restablecimiento de la configuración

Respalde la configuración para restablecerla rápidamente en caso de alguna falla.

(1) Inicie sesión en la Eweb del router.

(2) Seleccione **Gateway** > **Sistema** > **Gestión**.



(3) Haga clic en **Copia de seguridad** para descargar localmente el archivo de la configuración.

(4) Para restablecer la configuración, haga clic en **Vistazo**, seleccione el archivo de respaldo en la PC local y haga clic en **Importar** para importar el archivo de configuración. El router se reiniciará.

Si la versión que eligió es mucho más reciente que la actual, es posible que falten algunas configuraciones.

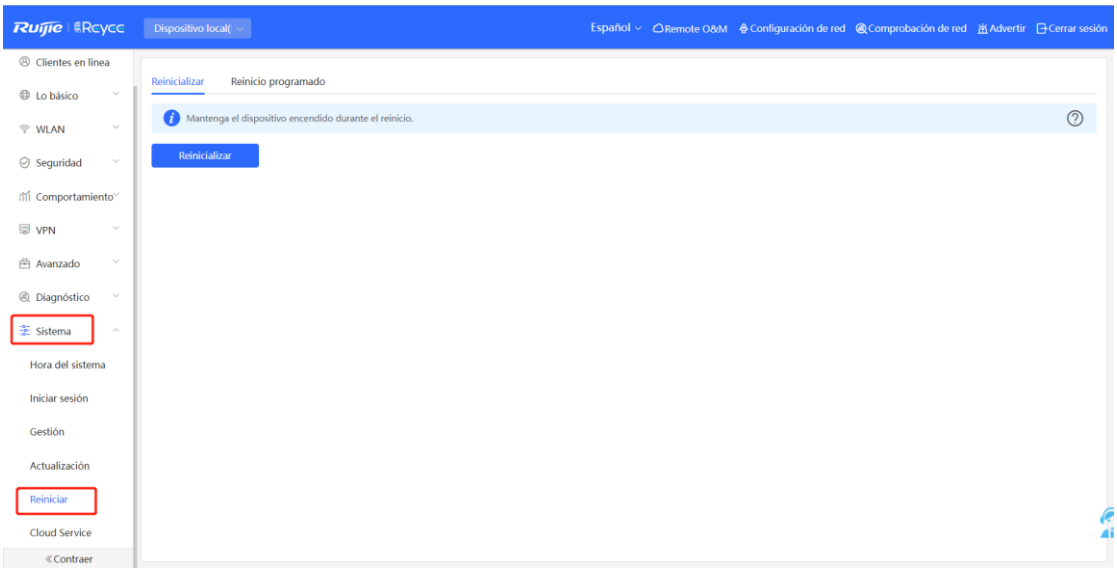
Se recomienda restablecer los valores antes de importar la configuración. Si restablece el router, este se reiniciará automáticamente.

3.7 Configuración del reinicio

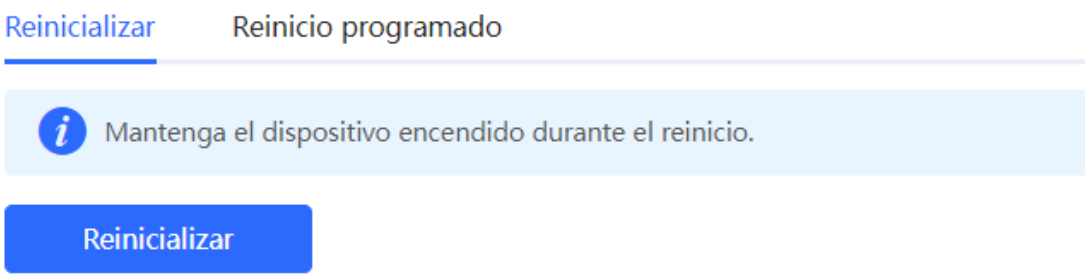
3.7.1 Reinicio del dispositivo actual

- Cambie al modo **Dispositivo local**.

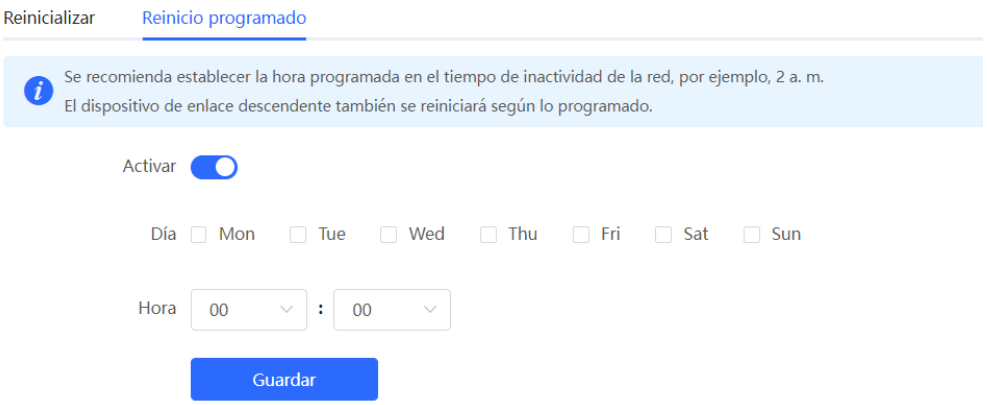
Seleccione **Sistema** > **Reiniciar**.



Haga clic en **Reinicializar**. El dispositivo se reiniciará inmediatamente. No actualice o cierre la página durante la actualización. Después de que el dispositivo se haya reiniciado, se abrirá la página de inicio de sesión.

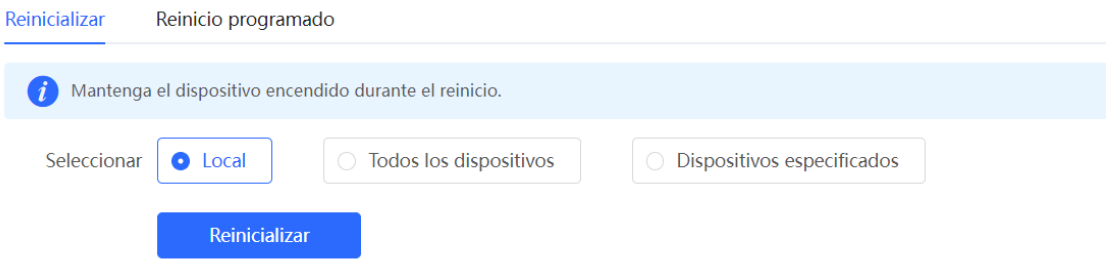


Haga clic en **Reinicio programado**. Habilite la función y seleccione el tiempo de reinicio programado. El dispositivo se reiniciará de acuerdo con la fecha y hora programadas.



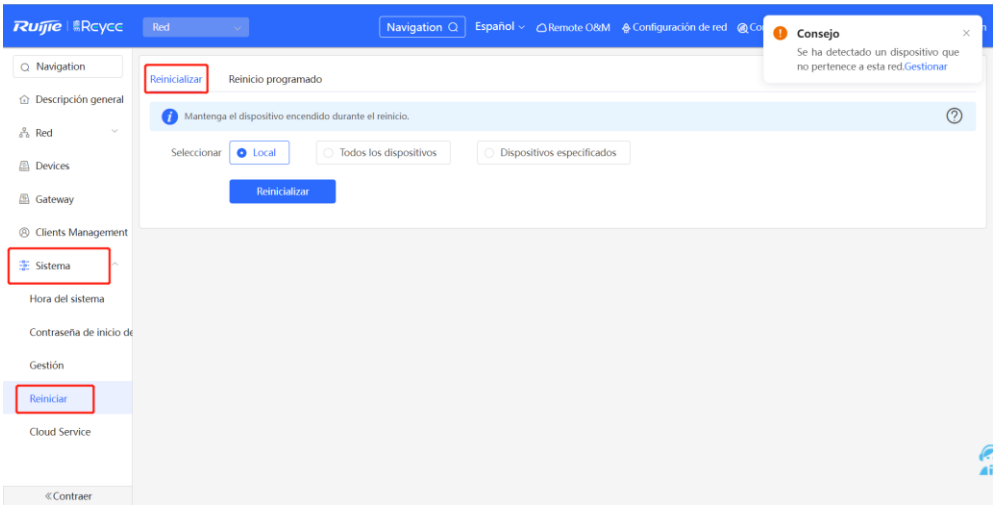
- Cambie al modo **Red**.

Seleccione **Sistema** > **Reiniciar** > **Reinicializar**. Seleccione **Local** para reiniciar el dispositivo actual.

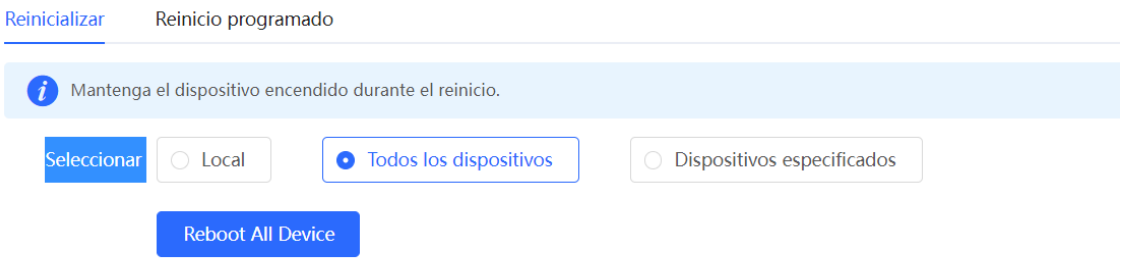


3.7.2 Reiniciar todos los dispositivos en la red

Cambie al modo **Red**. Seleccione **Sistema** > **Reiniciar** > **Reinicializar**.



Seleccione **Todos los dispositivos** y haga clic en **Reboot All Device** para reiniciar todos los dispositivos de la red.



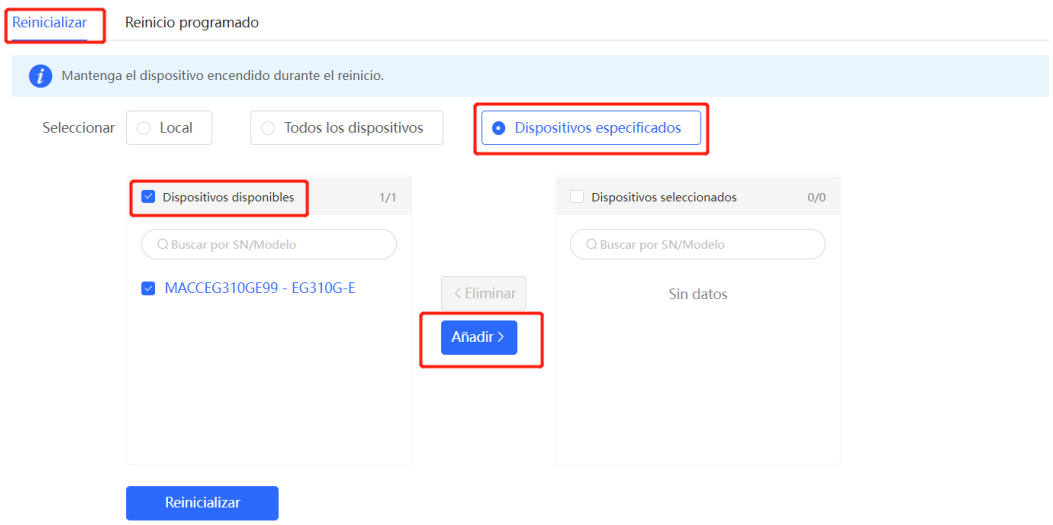
Precaución

El procedimiento toma tiempo y afecta toda la red. Por lo tanto, se recomienda que realice esta operación con precaución.

3.7.3 Reiniciar dispositivos especificados

Cambie al modo **Red**. Seleccione **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 que se encuentren en la lista de **Dispositivos seleccionados** se reiniciarán.



3.7.4 Configuración del reinicio programado

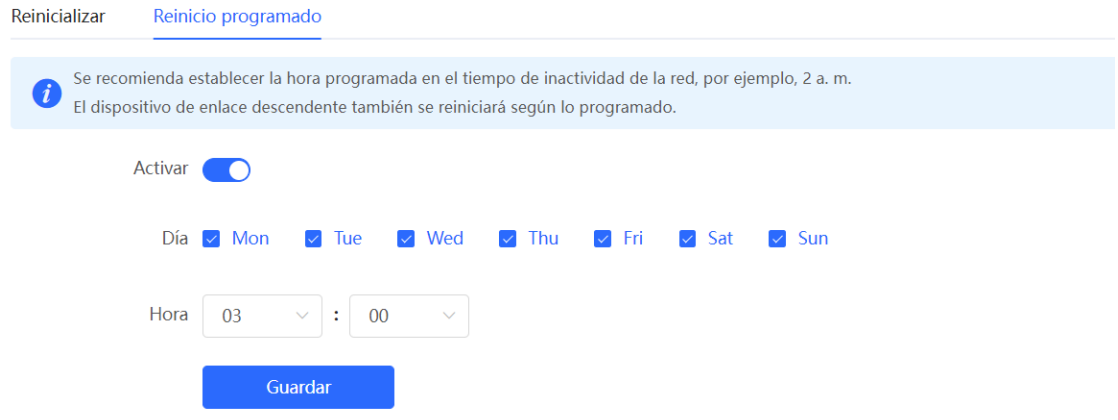
Confirme que la hora del sistema sea correcta para evitar interrupciones en la red ocasionadas por el reinicio del dispositivo en una hora incorrecta. Para información más detallada acerca de cómo configurar la hora del sistema, consulte la sección Configuración de la hora del sistema.

Seleccione **Sistema** > **Reiniciar** > **Reinicio programado**.

Establezca el interruptor en **Activar** y seleccione la fecha y hora del reinicio programado semanalmente. Haga clic en **Guardar**. Cuando la hora coincida con la hora de reinicio programada, el dispositivo se reiniciará. Se recomienda establecer la hora del reinicio programado en horas de inactividad.

Precaución

Este procedimiento afecta a toda la red. Por lo tanto, se recomienda que realice esta operación con precaución.



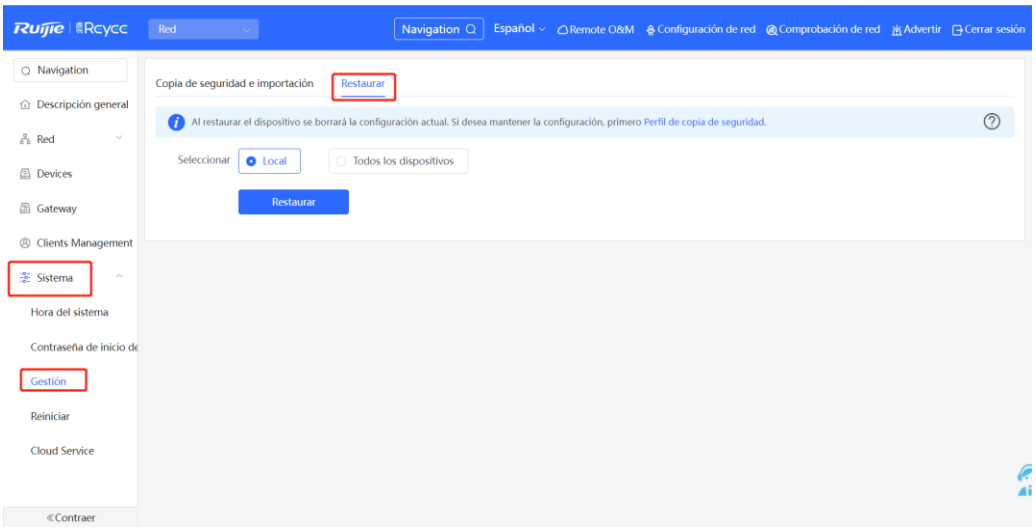
3.8 Restauración de la configuración de fábrica

Restablezca la configuración de fábrica y la contraseña por defecto.

El procedimiento borra toda la configuración actual. Se recomienda respaldar la configuración antes de restablecer los valores de fábrica.

(1) Inicie sesión en la Eweb del dispositivo.

(2) Seleccione **Sistema** > **Gestión** > **Restaurar**.



(3) Seleccione el dispositivo objetivo.

- **Local**: seleccione **Local**. Solo se restablecerá el dispositivo local.
- **Todos los dispositivos**: seleccione **Todos los dispositivos**. Todos los dispositivos de la red se restablecerán.

(4) Haga clic en **Restaurar** para restablecer todos los dispositivos seleccionados con la configuración de fábrica.

4 Configuración común

4.1 Configuración de acceso a la red

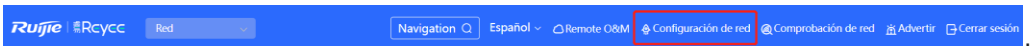
Configure la red para conectar el router a Internet rápidamente.

Hay tres modos disponibles para acceder a Internet:

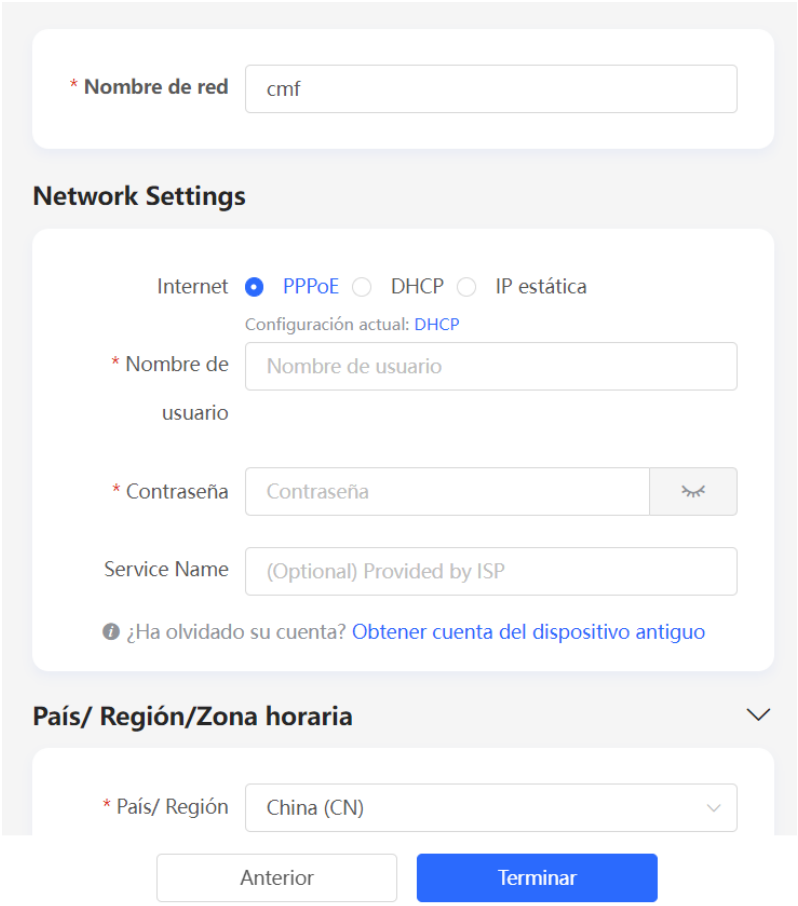
- PPPoE
- DHCP
- Dirección IP estática

4.1.1 Configuración del PPPoE a través del puerto WAN

(1) Haga clic en **Configuración de red** para acceder a la página.



Configure **Internet** en **PPPoE**, en la ventana de **Network Settings**.

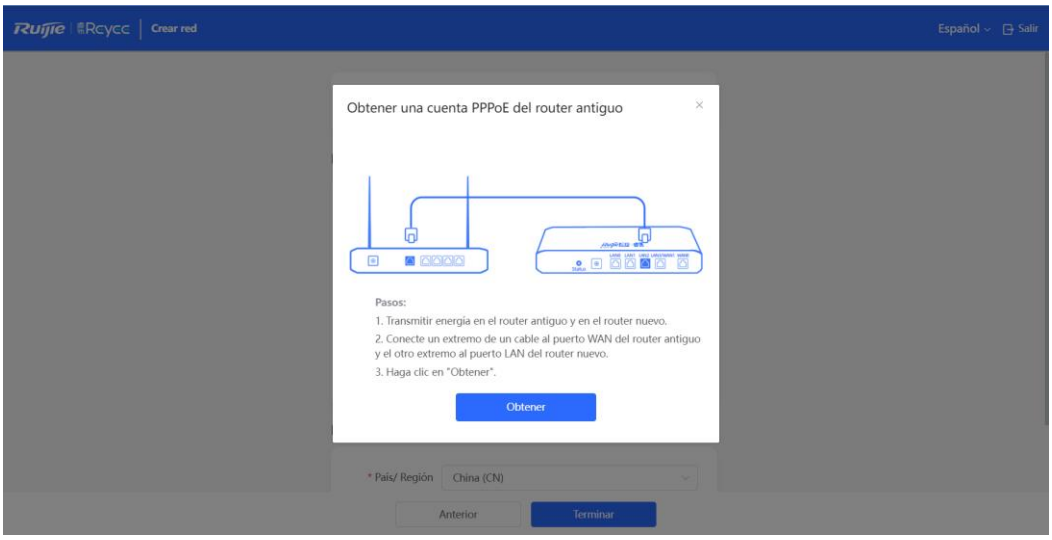


(2) Ingrese el **Nombre de usuario** y **Contraseña** que le haya proporcionado un ISP. El parámetro **Service Name** es opcional.

(3) Si olvida la contraseña que le proporcionó el ISP, haga clic en **Obtener cuenta del dispositivo antiguo.**

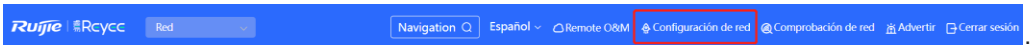
(4) Haga clic en **Terminar**. El router inicia la conexión con el Internet.

(5) Cuando el router se haya conectado, puede gestionarlo desde Ruijie Cloud o la Eweb.

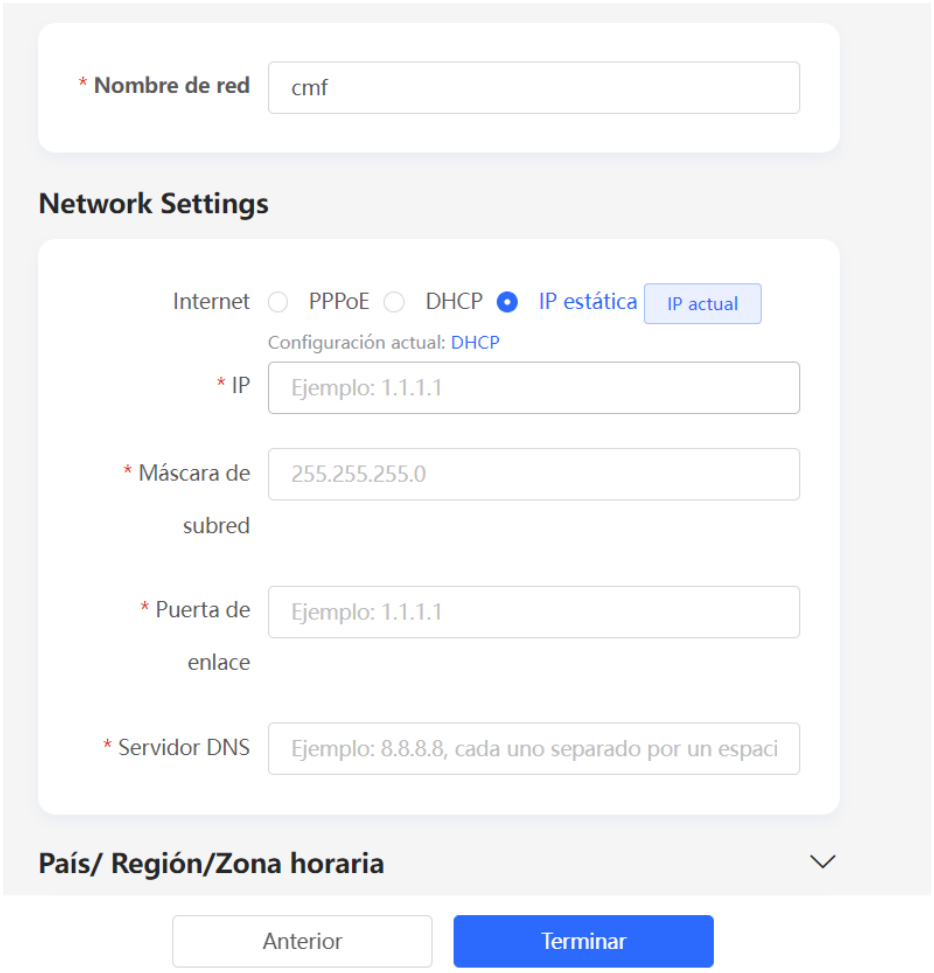


4.1.2 Configuración de una dirección IP estática a través de un puerto WAN

(1) Haga clic en **Configuración de red** para acceder a la página.



(2) Configure **Internet** en **IP estática**, en la ventana de **Network Settings**.



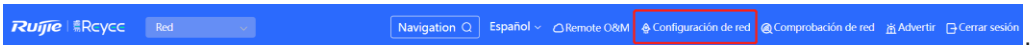
(3) Configure los parámetros de dirección IP, máscara de subred, puerta de enlace de la dirección IP y dirección de servidor DNS.

(4) Haga clic en **Terminar**. El router inicia la conexión con el Internet.

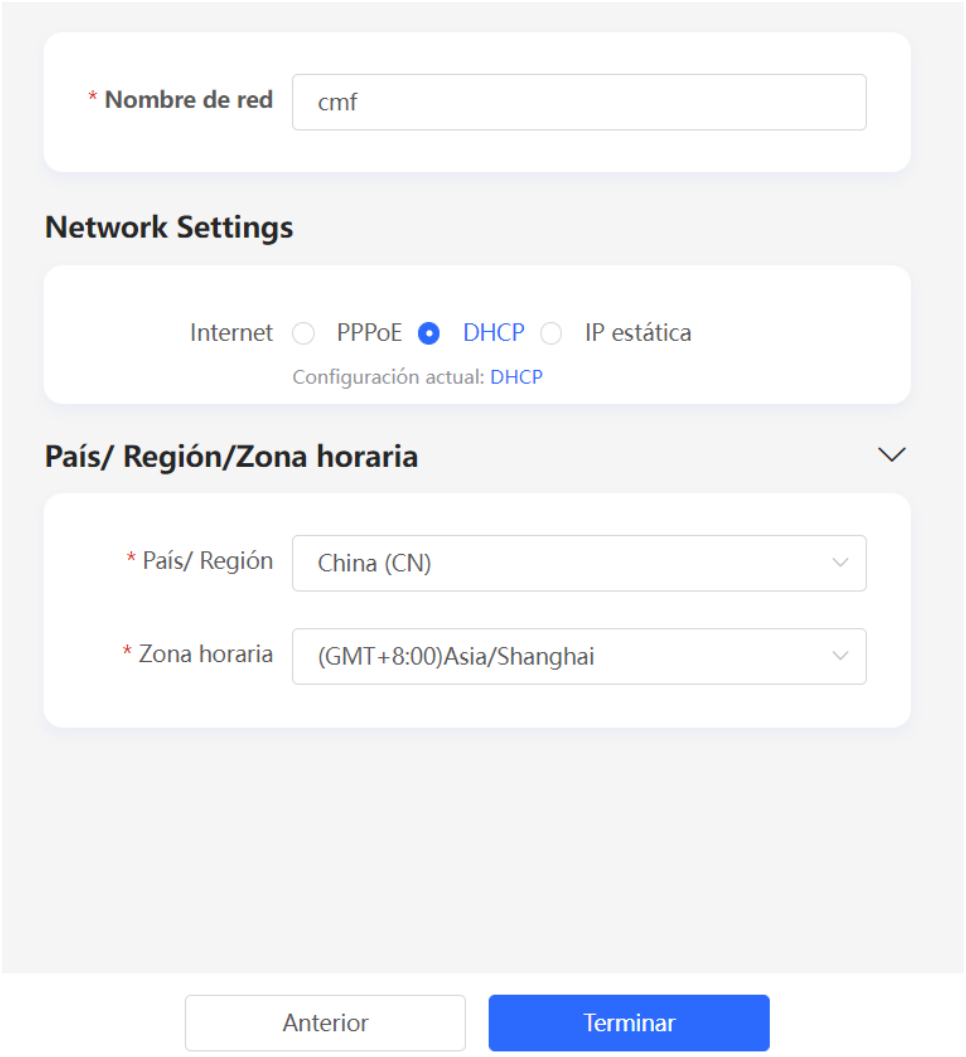
(5) Cuando el router se haya conectado, puede gestionarlo desde Ruijie Cloud o la Eweb.

4.1.3 Configuración de la DHCP a través de un puerto WAN

(1) Haga clic en **Configuración de red** para acceder a la página.



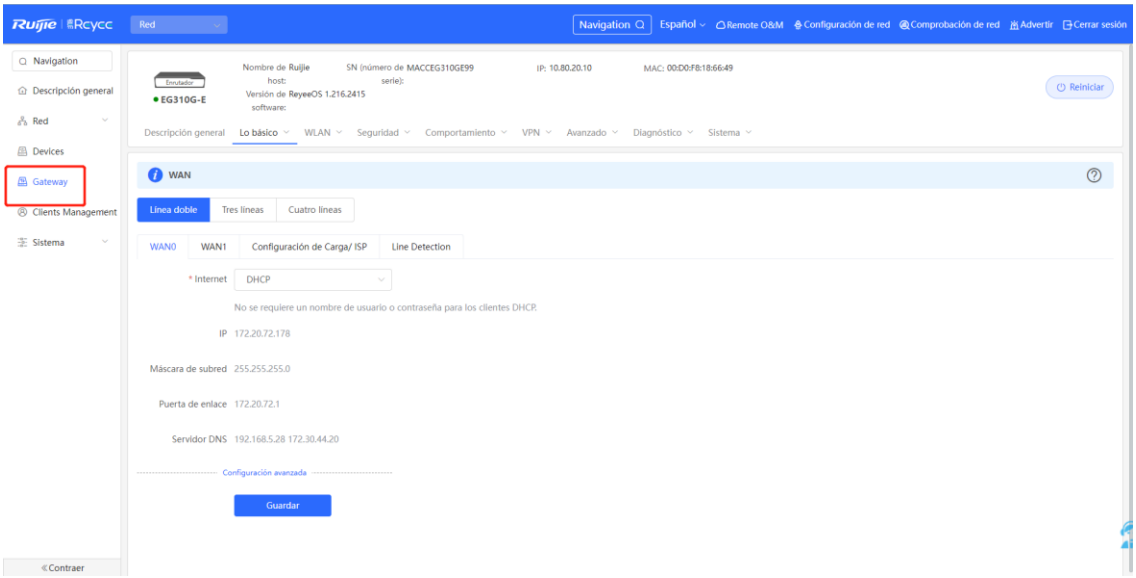
(2) Configure **Internet** en **DHCP**, en la ventana de **Network Settings**.



(3) Haga clic en **Terminar**. El router inicia la conexión con el Internet.

Cuando el router se haya conectado, puede gestionarlo desde Ruijie Cloud o la Eweb. La WAN se puede configurar a través de la siguiente página.

Seleccione **Gateway** > **Lo básico** > **WAN**.



4.2 Gestión de un AP

Nota

- Para administrar un punto de acceso o AP de enlace descendente, habilite la función de descubrimiento de red de autoorganización (SON) (consulte la sección 4.2.1 Cambiar el modo de trabajo). Por defecto, la configuración inalámbrica se sincroniza en todos los dispositivos de la red. Puede configurar grupos para limitar el alcance del dispositivo bajo gestión inalámbrica. Para más información, consulte la sección 4.2.2 Configuración de Grupos de AP.
- A excepción de los routers RG-EG105GW y RG-105GW(T), los demás routers Reyee no envían señales de Wi-Fi. La configuración inalámbrica requiere estar disponible para que los AP de enlace descendente se hagan efectivos.

4.2.1 Cambiar el modo de trabajo

1. Modo de trabajo

- Modo Enrutador

El dispositivo admite funciones de enrutamiento como el reenvío mediante enrutamiento, la traducción de direcciones de red (NAT) y la gestión de comportamiento. Puede asignar direcciones a dispositivos descendentes, reenviar datos de red con base en las rutas y llevar a cabo procedimientos de NAT.

En modo Enrutador, el dispositivo puede acceder a la red a través del Protocolo de marcación punto a punto sobre Ethernet (PPPoE), de una dirección IP dinámica y de una dirección IP estática. También puede conectarse directamente a un cable de red de fibra óptica al hogar (FTTH) o a un dispositivo de enlace ascendente para proporcionar el acceso a la red y administrar los dispositivos de enlace descendente.

- Modo AC

El dispositivo solo admite reenvíos de Capa 2. No proporciona funciones de enrutamiento ni de servidor de Protocolo de Configuración Dinámica de Host (DHCP). Por defecto, el puerto WAN obtiene una dirección IP a través del DHCP. El modo AC se utiliza en escenarios donde la red trabaja de manera normal. En este

modo, el dispositivo actúa como controlador de gestión o AC para acceder a la red en modo bypass y administrar los AP.

2. Descubrimiento SON

Cuando se configura un modo de trabajo, se puede habilitar la función de descubrimiento SON. Por defecto, esta función está habilitada.

Cuando se habilita, el dispositivo se puede descubrir en una red y descubrir otros dispositivos en ella. Los dispositivos se interconectan entre ellos con base en su estado y sincronizan la configuración global. Se puede iniciar sesión en la página de gestión de la web de cualquier dispositivo en la red para revisar su información. Si esta función se habilita, los clientes pueden mantener y administrar su red actual de manera más eficiente. Se recomienda mantenerla habilitada.

Si la función de descubrimiento SON se deshabilita, el dispositivo no será descubierto en la red y funcionará de modo independiente. Después de iniciar sesión en la página web, se puede configurar y administrar solamente el dispositivo actual al que se accedió. Si solo se configura un dispositivo o no es necesario sincronizarlo con la configuración global, se puede deshabilitar la función de descubrimiento SON.

Nota

En modo AC, por defecto, la función de descubrimiento SON se encuentra habilitada.

Si la función se habilita, la función de autoorganización se puede visualizar en la página **Detalles del dispositivo**.

Los menús de la página web varían dependiendo si la función está habilitada o no. Para más información, consulte la sección 3.2 Presentación del producto.

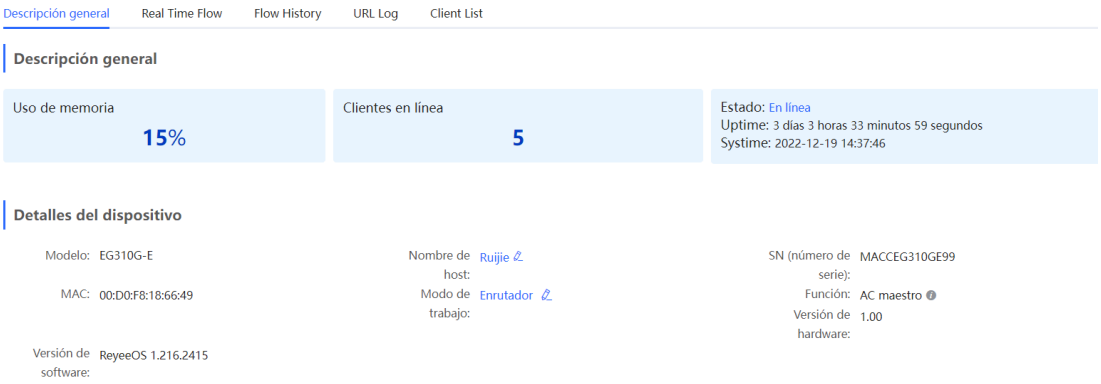
3. Pasos para la configuración

Cambie al modo **Dispositivo local**. Seleccione **Descripción general > Detalles del dispositivo**.

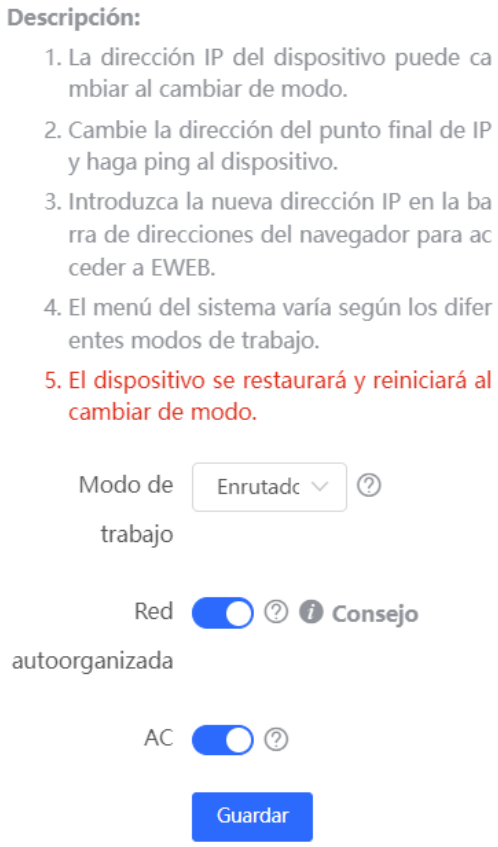
Haga clic en **Modo de trabajo** para editar el modo.

Precaución

Después de que cambie el modo de trabajo, el dispositivo restablecerá la configuración predeterminada de fábrica y se reiniciará. Proceda con precaución al realizar este cambio.



Función AC: si el dispositivo trabaja en modo enrutador y la función de descubrimiento SON está habilitada, puede habilitase o no la función AC. Si habilita la función AC, el dispositivo en modo enrutador admite la función AC virtual y puede administrar dispositivos de enlace descendente. Si deshabilita la función AC, restablezca el dispositivo en modo AC o SON para poder administrar dispositivos de enlace descendente.



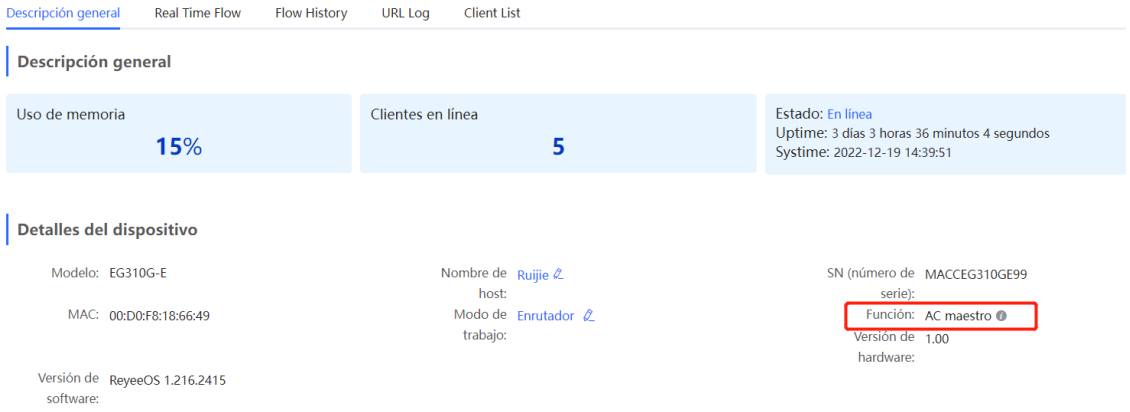
4. Visualización de la función de autoorganización

Seleccione **Dispositivo local > Descripción general > Detalles del dispositivo**.

Si la función de descubrimiento SON se habilita, se puede visualizar la función de autoorganización en la página Detalles del dispositivo.

AP/AC maestro: el dispositivo actúa como un AC para administrar dispositivos de enlace descendente.

AP/dispositivo esclavo: el dispositivo se conecta al AC en modo autoorganización y es administrado por el AC. Los AP esclavos se administran de manera uniforme por el dispositivo maestro AP o AC. Algunas configuraciones de la red inalámbrica no se pueden modificar de forma separada en modo local y deben ser suministradas por dicho dispositivo maestro.



4.2.2 Configuración de Grupos de AP

1. Descripción general

Después de habilitar la función de descubrimiento SON, el dispositivo actúa como AP o AC maestro para hacer configuraciones en lote y administrar los AP de enlace descendente por grupos. Antes de configurar los AP, asígnelos a diferentes grupos.

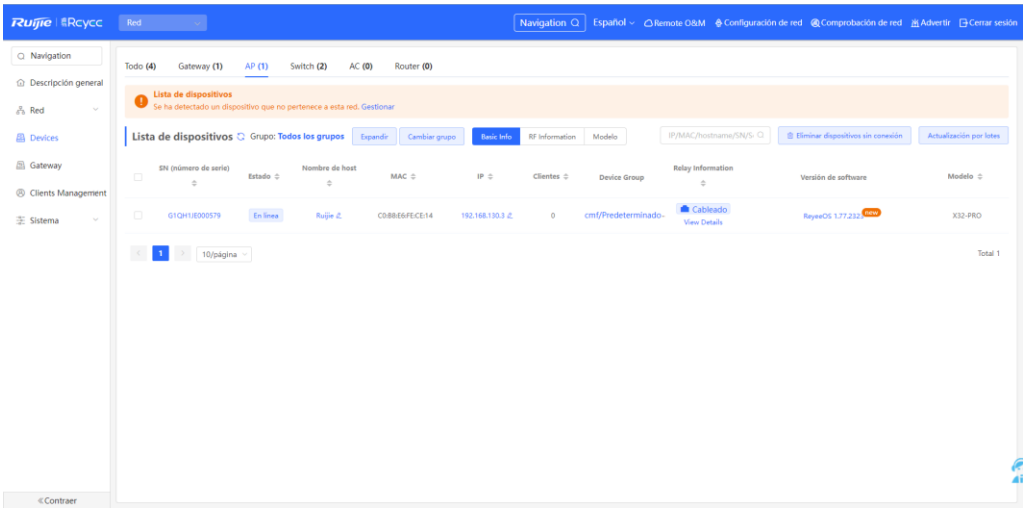
Nota

Si especifica grupos al configurar la red inalámbrica, esta se hace efectiva en los dispositivos inalámbricos de los grupos especificados.

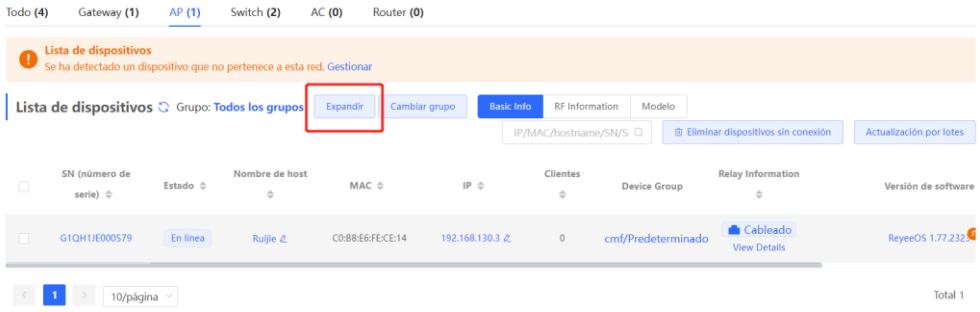
2. Pasos para la configuración

Cambie al modo **Red**. Seleccione **Devices** > **AP**.

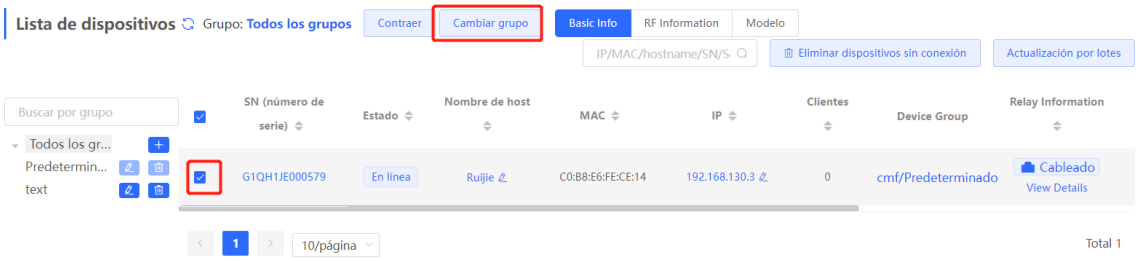
(1) Visualice la información de todos los AP en la red actual, incluyendo la información básica, la información de la RF y el modelo. Haga clic en el SN de un AP para configurarlo de manera separada.

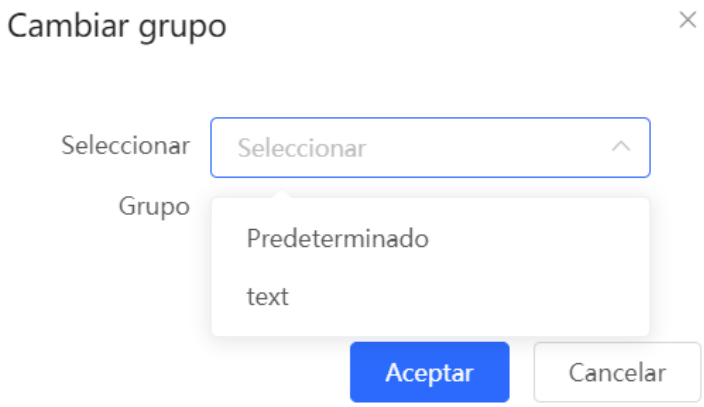


(2) Haga clic en **Expandir**. En el lado izquierdo de la lista se muestra la información de todos los grupos actuales. Haga clic en  para crear un grupo. Puede crear un máximo de ocho grupos. Seleccione el grupo objetivo y haga clic en  para modificar su nombre o en  para borrarlo. El nombre predeterminado del grupo no se puede modificar ni borrar.



(3) Haga clic en el nombre de un grupo del lado izquierdo para visualizar todos los dispositivos en él. Cada dispositivo puede pertenecer únicamente a un solo grupo. Por defecto, todos los dispositivos 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 movido el dispositivo al grupo especificado, este usará la configuración del nuevo grupo. Haga clic en **Eliminar dispositivos sin conexión** para eliminar de la lista aquellos dispositivos que se encuentren sin conexión.





4.2.3 Configuración Wi-Fi

Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Configuración Wi-Fi**.

Ingrese el SSID y la contraseña de Wi-Fi, seleccione la banda de frecuencia que usa la señal y haga clic en **Guardar**.

Haga clic en **Expandir** para configurar los parámetros de Wi-Fi.

Precaución

Modificar la configuración ocasionará el restablecimiento de la configuración inalámbrica, haciendo que los clientes se desconecten de su sesión. Se recomienda que realice esta operación con precaución.

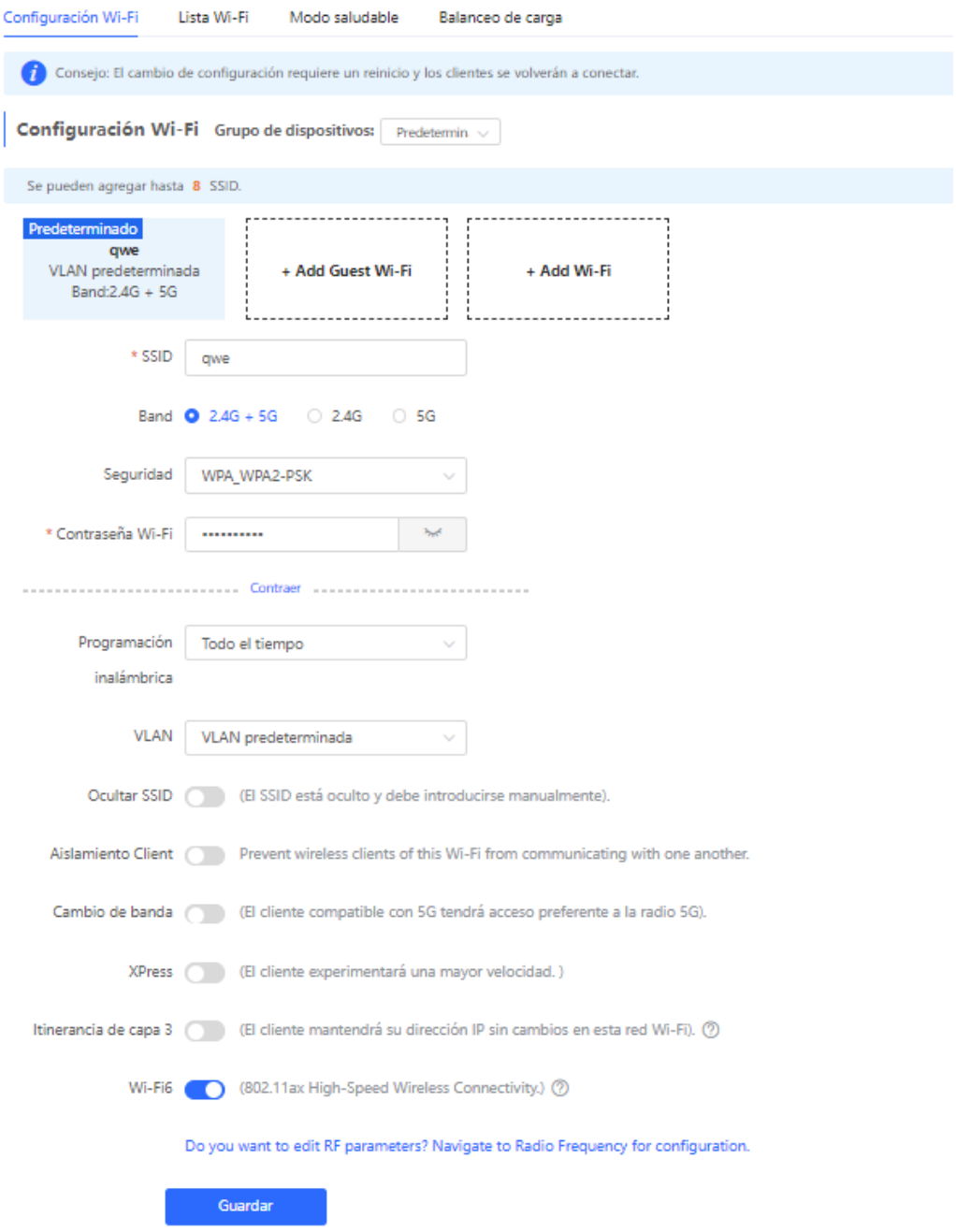


Tabla 4- 1 Configuración de la red inalámbrica

Parámetro	Descripción
SSID	Ingrese el nombre que se muestra cuando un cliente inalámbrico busca una red inalámbrica.
Codificación del SSID	Si el SSID no contiene caracteres chinos, este elemento permanecerá oculto. Si contiene caracteres chinos, este elemento se mostrará. Seleccione UTF-8 o GBK.

Parámetro	Descripción
Banda	Configure la banda que usa la señal de Wi-Fi. Las opciones son 2.4 GHz y 5 GHz. La banda 5 GHz proporciona en la red una velocidad de transmisión más rápida y con menos interferencia que la banda de 2.4 GHz, pero es inferior a esta en términos del rango de cobertura de la señal y el desempeño al pasar entre paredes. Seleccione la banda adecuada según lo requiera. El valor predeterminado es **2.4G+ 5G**, lo que indica que el dispositivo proporciona señales para ambas bandas.
Seguridad	Seleccione un modo de encriptación para conexiones de red inalámbricas. 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 (recomendado): la WPA2-PSK o WPA-PSK se utiliza para encriptación.
Contraseña Wi-Fi	Especifique la contraseña para la interconexión con la red inalámbrica. La contraseña debe estar formada por una cadena de 8 a 16 caracteres.
Programación inalámbrica	Especifica el periodo durante el que se encuentra habilitado el Wi-Fi. Cuando se configura este parámetro, los usuarios solo se pueden conectar a Wi-Fi durante ese lapso.
VLAN	Configure la VLAN a la que pertenece la señal de Wi-Fi. Puede seleccionar una VLAN de entre las disponibles, o haga clic en **Agregar VLAN** y vaya a la página de **Configuración de LAN** para añadir una VLAN.
Ocultar SSID	Habilitar la función de ocultar SSID puede prevenir el acceso de usuarios no autorizados al Wi-Fi, lo que mejora la seguridad. Sin embargo, los teléfonos móviles o las computadoras no podrán encontrar el nombre del SSID si esta función está habilitada. Ingrese manualmente el nombre y contraseña correctos para conectarse a Wi-Fi. Registre el SSID actual antes de habilitar esta función.
Aislamiento Client	Si habilita esta función de aislamiento, los clientes asociados al Wi-Fi son aislados unos de otros y los usuarios conectados al mismo AP (en el mismo segmento de red) no pueden tener acceso entre ellos. Esto mejora la seguridad.

Parámetro	Descripción
Cambio de banda	El cambio de banda permite que los clientes con compatibilidad 5G seleccionen, preferentemente, la red Wi-Fi de 5 GHz. Esta función se puede habilitar solamente cuando el parámetro **Banda** se configura en **2.4G+ 5G**.
XPress	Cuando la función XPress se habilita, el dispositivo envía paquetes de juego preferentemente, proporcionando una red inalámbrica más estable para jugar.
Itinerancia de Capa 3	La itinerancia de red autoorganizada o roaming de Capa 3 permite que los clientes conserven sus direcciones IP cuando son asociados con el mismo Wi-Fi. Esta función mejora la experiencia de roaming de los usuarios en el escenario de una VLAN cruzada.
Wi-Fi6	El Wi-Fi6 ofrece a los usuarios de conexión inalámbrica una velocidad de acceso a la red más rápida y una experiencia optimizada. Esta función es válida solamente para AP y routers aptos para 802.11ax. Los clientes también deben ser compatibles con 802.11ax para experimentar un acceso a la red de gran velocidad habilitada por el Wi-Fi 6. Si los clientes no son compatibles con Wi-Fi 6, deshabilite esta función.

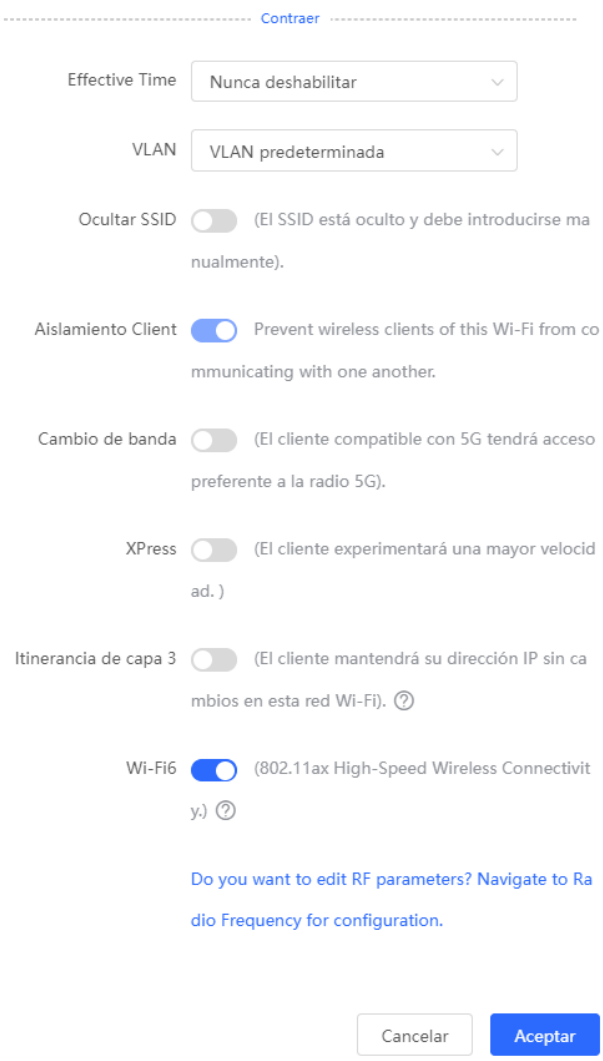
4.2.4 Configuración del Wi-Fi de invitados

Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Configuración Wi-Fi** > **Añadir Wi-Fi de invitados**.

El Wi-Fi de invitados es una red inalámbrica para invitados y, por defecto, se encuentra deshabilitada. La función de aislamiento de clientes está habilitada por defecto para la red Wi-Fi de invitados y no puede deshabilitarse. En este caso, los clientes asociados con dicha red están mutuamente aislados y solo pueden acceder a Internet a través de Wi-Fi. Esto mejora la seguridad del acceso a la red. Es posible configurar una programación inalámbrica para la red de invitados. Cuando la programación específica haya vencido, la red no se podrá localizar.

Habilite la red Wi-Fi de invitados y configure el SSID y la contraseña. Haga clic en **Expandir** para configurar la programación inalámbrica del Wi-Fi de invitados y sus parámetros. Para más información, consulte la sección4.2.3 Configuración Wi-Fi. Haga clic en **Aceptar**. Los invitados pueden acceder a Internet a través del Wi-Fi, después de ingresar el SSID y la contraseña.

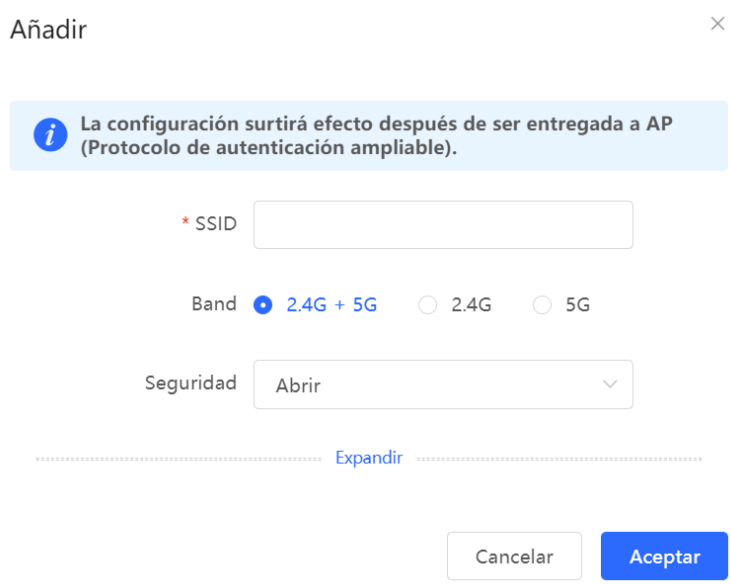

* SSID
@Ruijie-guest-6649
Band
2.4G + 5G
2.4G
5G
Seguridad
Abrir
Expandir
Cancelar
Aceptar


Contraer
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 one 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).
Wi-Fi6
(802.11ax High-Speed Wireless Connectivity.)
Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.
Cancelar
Aceptar

4.2.5 Añadir más redes Wi-Fi

Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Lista Wi-Fi** y elija el grupo de dispositivos al que desea añadirle más redes Wi-Fi.

Haga clic en **Add Wi-Fi**, ingrese el SSID y la contraseña, y luego presione **Aceptar** para crear una red Wi-Fi. Haga clic en **Expandir** si desea configurar más parámetros del Wi-Fi. Para más información, consulte la **sección** 4.2.3 Configuración Wi-Fi. Después de añadir una red Wi-Fi, los clientes podrán encontrarla y consultar su información en la lista Wi-Fi.

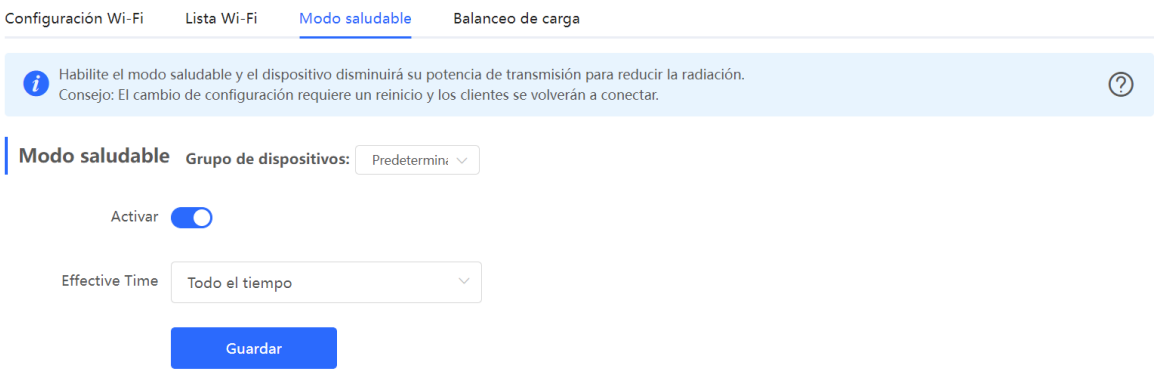


4.2.6 Modo saludable

Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Modo saludable**.

Habilite el modo saludable y seleccione la programación inalámbrica para dicho modo.

Al habilitar el modo saludable, la potencia de transmisión de la radiofrecuencia (RF) y el rango de cobertura de Wi-Fi del dispositivo inalámbrico se reducen durante la programación. Esto puede ocasionar señales débiles y el congelamiento de la red. Se recomienda deshabilitar este modo o configurar la programación inalámbrica para un periodo de inactividad.



4.2.7 Configuración de la RF

Cambie al modo **Red**. Seleccione **Red > Frecuencia de radio**.

El dispositivo puede detectar el entorno inalámbrico circundante al encenderlo y seleccionar la configuración apropiada. Sin embargo, no es posible evitar que la red se congele debido a los cambios en el entorno. Lo que se puede hacer es analizar el entorno inalámbrico de los AP y routers y seleccionar manualmente los parámetros apropiados.

Precaución

Modificar la configuración ocasionará el restablecimiento de la configuración inalámbrica, haciendo que los clientes se desconecten de su sesión. Se recomienda que realice esta operación con precaución.

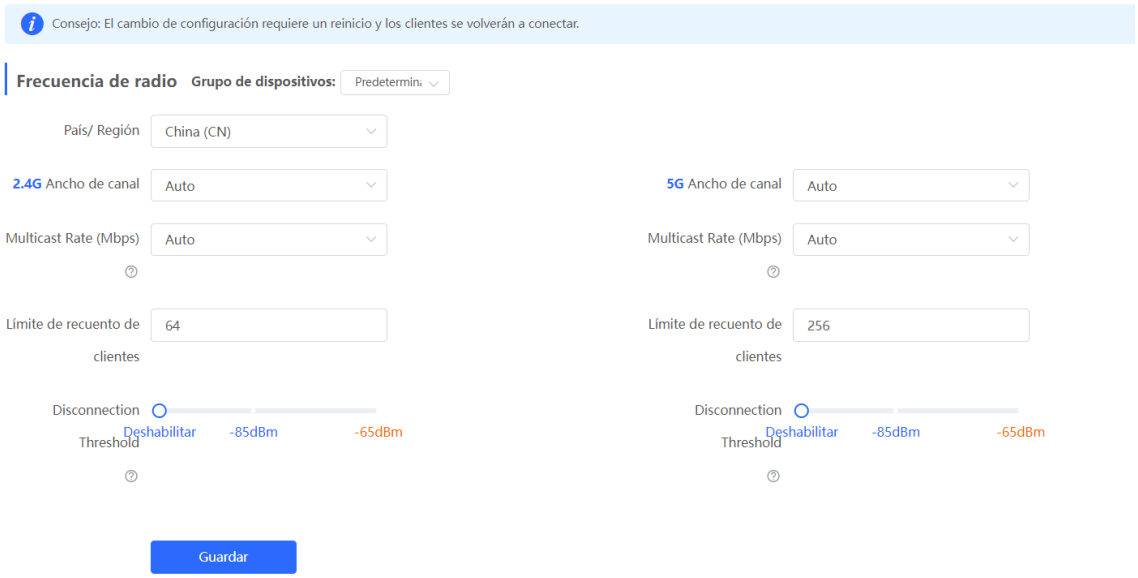


Tabla 4- 2 Configuración de la RF

Parámetro	Descripción
País/Región	Los canales de Wi-Fi estipulados por cada país pueden ser diferentes. Para garantizar que los clientes encuentren las señales de Wi-Fi, seleccione el país o región donde está localizado el dispositivo.
2.4G/5G Ancho de canal	Un ancho de banda menor indica una red más estable, mientras que uno mayor indica menos interferencia. En caso de una interferencia grave, seleccione un ancho de banda menor para evitar que la red se congele en algún punto. El ancho de canal de 2.4 GHz es compatible con los anchos de banda de 20 MHz y 40 MHz. El ancho de canal 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 se selecciona automáticamente con base en el entorno.
Límite de recuento de clientes	Si un gran número de usuarios están conectados a un AP o un router, el desempeño de la red inalámbrica de estos puede degradarse, afectando su experiencia de acceso a Internet. Cuando este parámetro se configura, y el número de usuarios de acceso permitido alcanza el valor especificado, el AP o el router rechazan el acceso a nuevos usuarios. Si los clientes requieren mayor ancho de banda, este parámetro se puede ajustar en un valor menor. Se recomienda mantener los ajustes de fábrica, a menos que se especifique lo contrario.
Límite de desconexión	Cuando hay varias 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 inalámbrica del usuario final es menor al límite de desconexión, la conexión Wi-Fi se pierde. En este caso, el cliente debe seleccionar una señal inalámbrica más cercana. Si el límite de desconexión es alto, aumentará la posibilidad de desconexión. Para garantizar un acceso normal a Internet, se recomienda configurar este parámetro en **Deshabilitar** o en un valor menor a -75 dBm.

Nota

- Los canales inalámbricos disponibles dependen del código del país o región. Seleccione el código con base en donde se encuentre su dispositivo.
- El canal, la potencia de transmisión y la sensibilidad del roaming no pueden configurarse de manera global. Por lo tanto, deberá configurarlos de manera separada en cada dispositivo.

4.2.8 Configuración de una lista negra o una lista blanca de Wi-Fi

1. Descripción general

Las listas negras o listas blancas se pueden configurar de manera global o con base en el SSID. Y la coincidencia puede ser exacta con las direcciones MAC o con base en el OUI.

Lista negra de Wi-Fi: los clientes en esta lista de Wi-Fi no tienen acceso a Internet. Aquellos que no se encuentren en la lista tienen libre acceso a Internet.

Lista blanca de Wi-Fi: solo los clientes en esta lista de Wi-Fi tienen acceso a Internet. Aquellos que no se encuentren en la lista no tienen acceso a Internet.

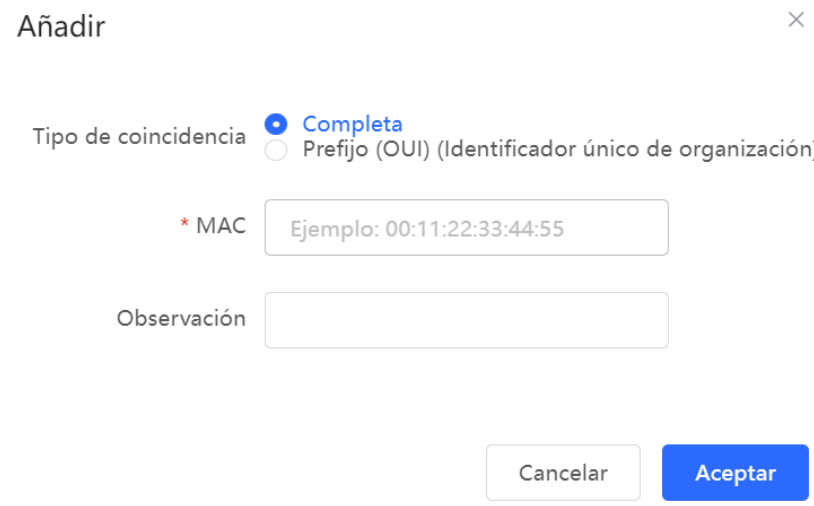
Precaución

Si la lista blanca se encuentra vacía, no surte ningún efecto. En este caso, todos los clientes tienen acceso a Internet.

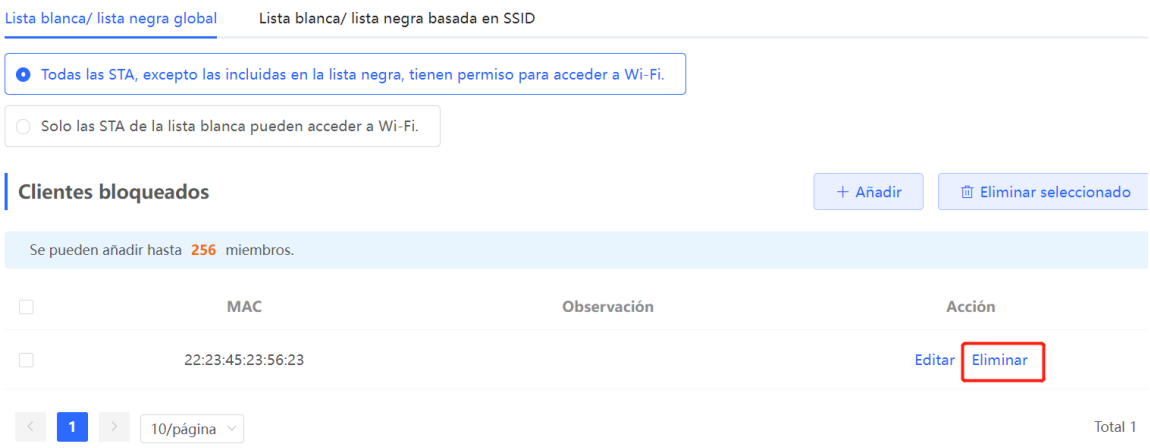
2. Configuración de una lista negra o una lista blanca global

Cambie al modo **Red**. Seleccione **Gestión de clientes** > **Lista blanca/lista negra** > **Lista blanca/lista negra global**.

Seleccione el modo lista negra o lista blanca y haga clic en **Añadir** para incluir a un cliente en la lista que requiera. En el cuadro de **Añadir**, ingrese la dirección MAC, alguna observación sobre el cliente objetivo y haga clic en **Aceptar**. Si un cliente ya está asociado con el router, su dirección MAC aparecerá automáticamente. Haga clic en la dirección MAC para ingresarla de forma automática. A todos los clientes de la lista negra se les forzará a desconectarse y no podrán acceder a la red Wi-Fi. La configuración de las listas globales, blanca y negra, se aplicará en todas las redes Wi-Fi del router.



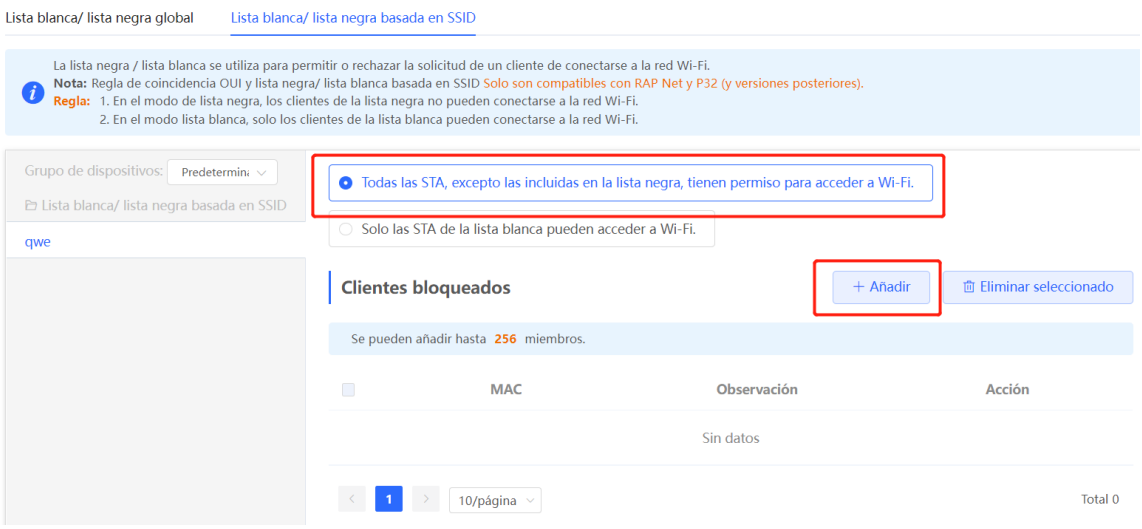
Si se borra un cliente de la lista negra, el cliente podrá conectarse a la red Wi-Fi. Si se borra un cliente de la lista blanca, se le forzará a desconectarse y no podrá acceder al Wi-Fi.



3. Configuración de una lista negra o una lista blanca basada en SSID

Cambie al modo **Red**. Seleccione **Gestión de clientes > Lista blanca/lista negra > Lista blanca/lista negra basada en SSID**.

Seleccione la red Wi-Fi objetivo de la columna izquierda, el modo lista blanca o lista negra, y haga clic en Añadir para configurar a un cliente en la lista que requiera. La lista negra o lista blanca basada en el SSID restringirá el acceso del cliente a la red Wi-Fi especificada.



4.2.9 Configuración del balanceo de carga de un AP

1. Descripción general

La función de balanceo de carga de un AP se utiliza para mantener la estabilidad de carga de los AP en la red inalámbrica. Cuando los AP que no cuentan con un balanceo de carga se añaden a un grupo con balanceo de carga, los clientes se asociarán automáticamente con los AP de carga ligera. El balanceo de carga del AP admite dos modos:

- **Balanceo de carga del cliente**: la carga se equilibra de acuerdo con el número de clientes asociados. Cuando hay un gran número de clientes asociados a un AP, y la diferencia con el número de clientes del AP con la carga más ligera ha alcanzado el valor especificado, el cliente solo podrá asociarse con otro de los AP en el grupo.
- **Balanceo de carga del tráfico**: la carga se equilibra de acuerdo con el tráfico de los AP. Cuando el tráfico en un AP es pesado y la diferencia con el tráfico del AP con la carga más ligera ha alcanzado el valor especificado, el cliente solo podrá asociarse con otro de los AP en el grupo.

Ejemplo: añada AP1 y AP2 a un grupo y seleccione el balanceo de carga del cliente. Configure tanto el número límite de clientes como la diferencia límite en 3. Si AP1 está asociado con cinco clientes y AP2 con dos clientes, se activa la función de balanceo de carga. Se denegarán los intentos de nuevos clientes para asociarse a AP1, por lo que solo se podrán asociar a AP2.

Cuando la solicitud de un cliente es denegada por un AP y falla en su intento de asociarse con otro AP en el grupo, el cliente continuará intentando asociarse con este AP. Si el número de clientes intentando asociarse alcanza el valor especificado, el AP permitirá al cliente asociarse, garantizando su acceso a Internet de manera normal.

2. Configuración del balanceo de carga del cliente

Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Balanceo de carga**.

Haga clic en **Añadir**. En el cuadro de diálogo que aparece, en **Tipo** elija la opción **Balanceo de carga del cliente** y configure **Nombre de grupo**, **Miembros** y **Regla**.

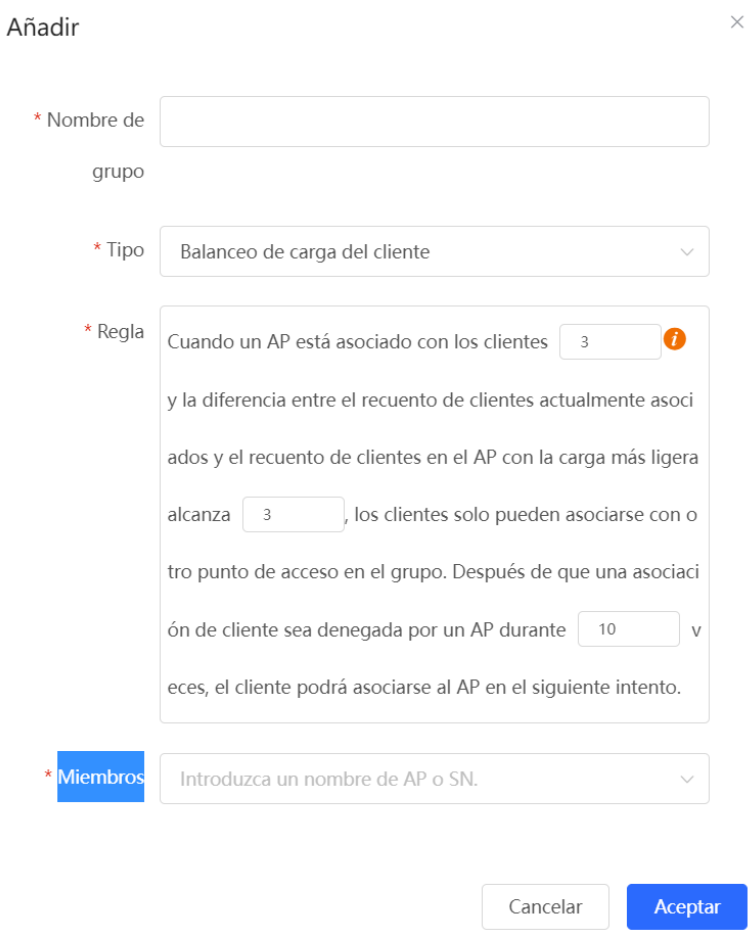


Tabla 4- 3 Configuración del balanceo de carga del cliente

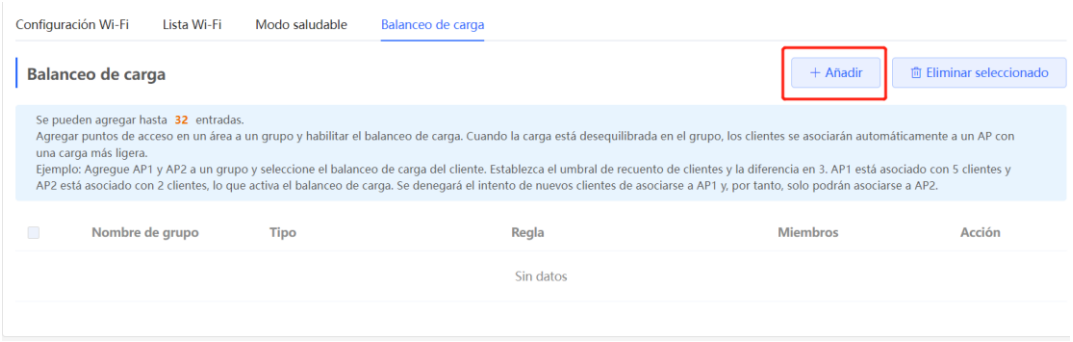
Parámetro	Descripción
Nombre de grupo	Ingrese el nombre del grupo del AP con balanceo de carga.
Tipo	Seleccione el balanceo de carga del cliente.

Parámetro	Descripción
Regla	Configure una regla detallada acerca del balanceo de carga, incluyendo el número máximo de clientes permitidos para asociarse con un AP, la diferencia entre el número de clientes actualmente asociados y el de clientes asociados con el AP de la carga más ligera, y el número de intentos para tener acceso al AP con carga completa. Por defecto, cuando un AP se asocia con tres clientes y la diferencia entre el número de clientes actualmente asociados y el de clientes asociados con el AP con la carga más ligera llega a 3, los clientes solo pueden asociarse con otro de los AP en el grupo. Después de que un AP haya denegado la solicitud de asociación de un cliente 10 veces, el cliente podrá asociarse con el AP en el siguiente intento.
Miembros	Especifique los AP para añadir al grupo con balanceo de carga del AP.

3. Configuración del balanceo de carga del tráfico

Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Balanceo de carga**.

Haga clic en **Añadir**. En el cuadro de diálogo que aparece, en **Tipo** elija la opción **Balanceo de carga del tráfico**, y configure **Nombre de grupo**, **Miembros** y **Regla**.



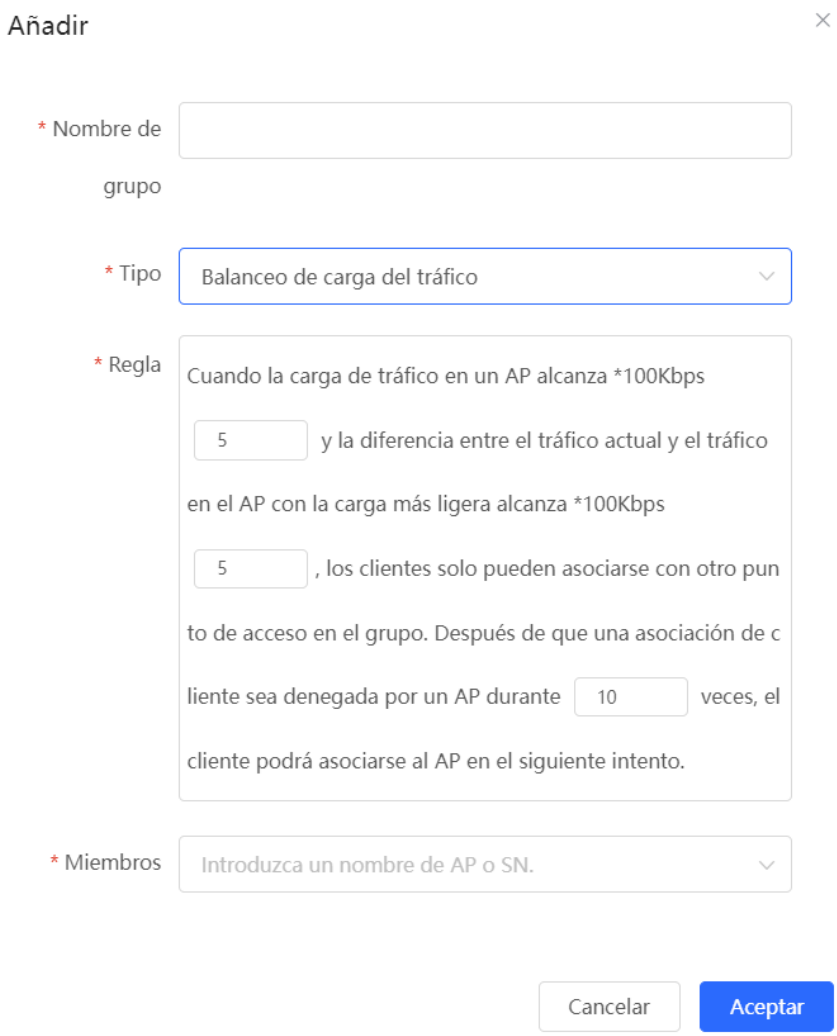


Tabla 4- 4 Configuración del balanceo de carga del tráfico

Parámetro	Descripción
Nombre de grupo	Ingrese el nombre del grupo del AP con balanceo de carga.
Tipo	Seleccione **Balanceo de carga del tráfico**.
Regla	Configure una regla detallada acerca del balanceo de carga, incluyendo el tráfico máximo permitido en un AP, la diferencia entre el tráfico actual y el del AP con la carga más ligera, y el número de intentos para tener acceso al AP con carga completa. Por defecto, cuando la carga de tráfico en un AP llega a 500 Kbps y la diferencia entre el tráfico actual y el del AP con la carga más ligera llega a 500 Kbps, los clientes solo pueden asociarse con otro de los AP en el grupo. Después de que un AP haya denegado la solicitud de asociación de un cliente 10 veces, el cliente podrá asociarse con el AP en el siguiente intento.

Parámetro	Descripción
Miembros	Especifique los AP para añadir al grupo con balanceo de carga del AP.

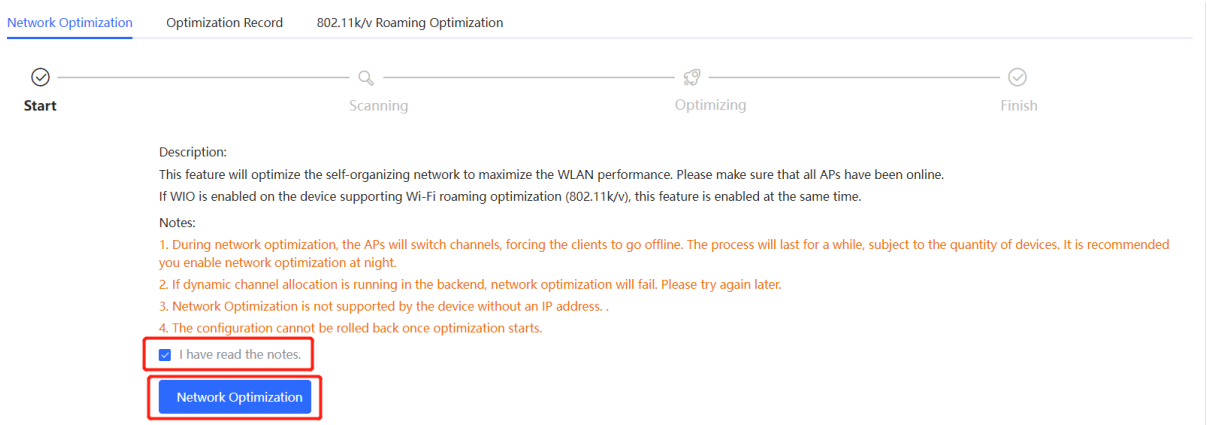
4.2.10 Optimización de la red inalámbrica en un solo clic

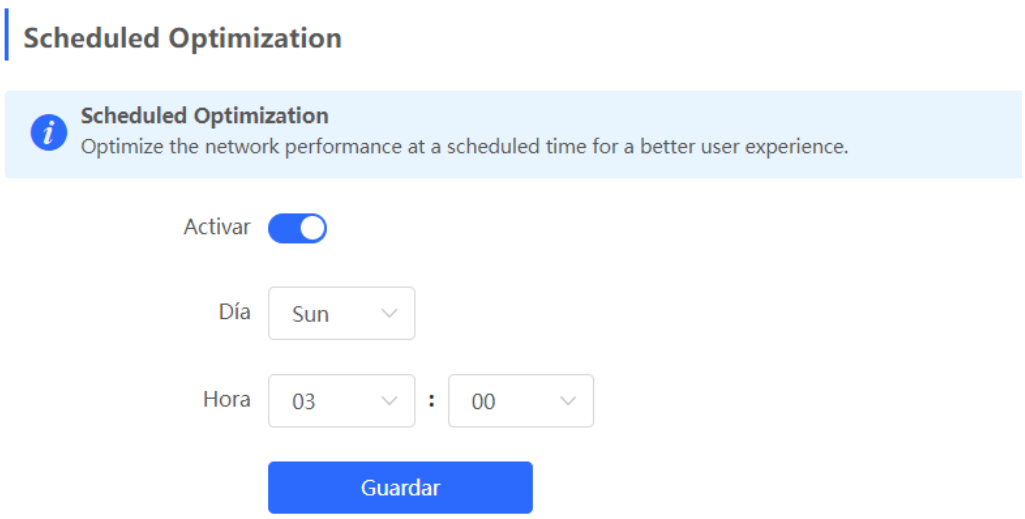
Cambie al modo **Red**. Seleccione **Red > WIO**.

En la pestaña **Network Optimization**, seleccione **I have read the notes**, y haga clic en **Network Optimization** para llevar a cabo la optimización automática de la red inalámbrica en su propio ambiente. Se puede configurar una optimización programada para optimizar la red en una hora específica. Se recomienda configurar la optimización programada durante la noche o en un periodo de inactividad.

Precaución

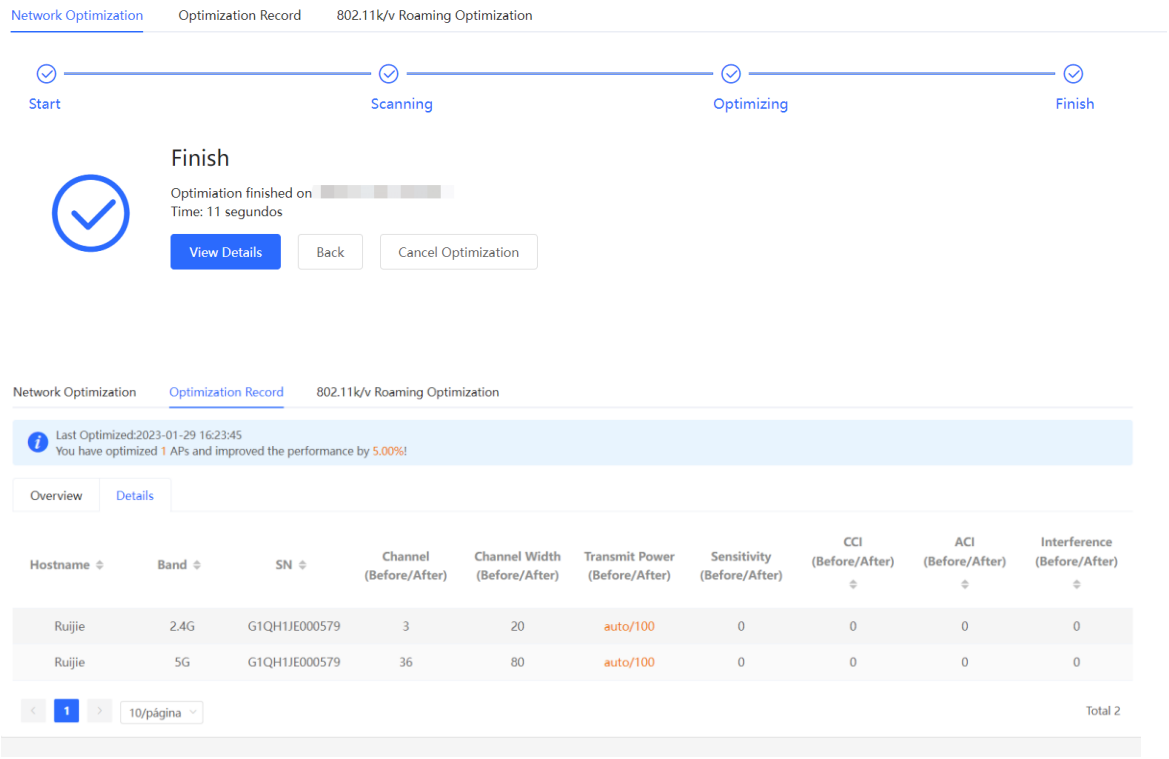
Es posible que se desconecte a los clientes durante la optimización; además, considere que no es posible revertir la configuración una vez iniciada. Se recomienda que realice esta operación con precaución.





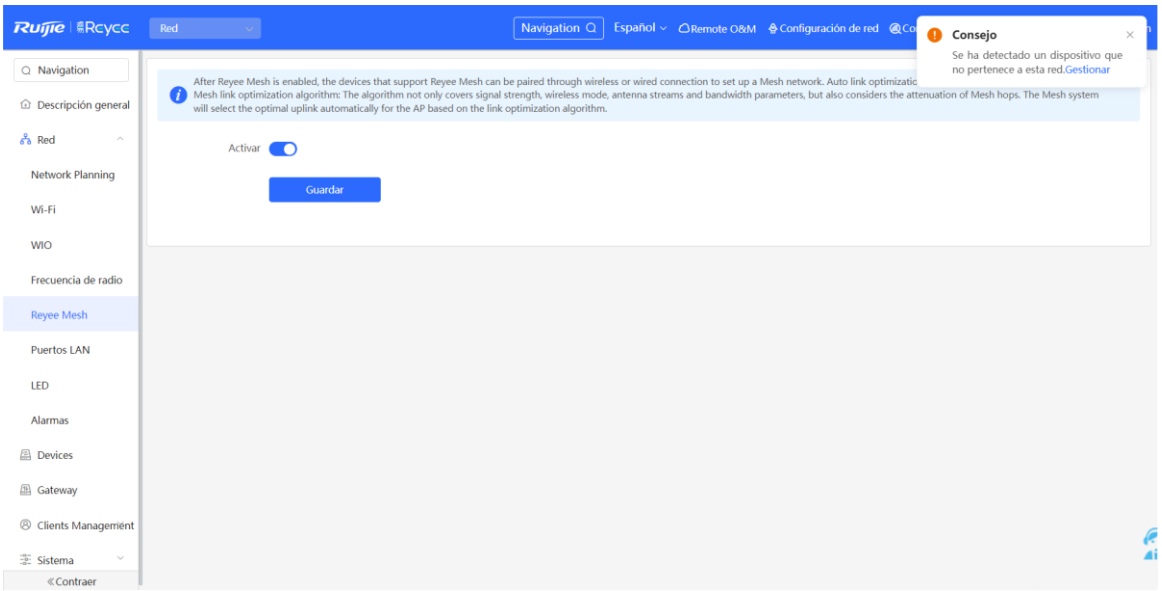
Después de iniciada la optimización, espere hasta que se complete. Una vez completada, haga clic en **Cancel Optimization** para restablecer los parámetros optimizados de la RF a los valores predeterminados.

Haga clic en **View Details** o en la pestaña **Optimization Record** para visualizar los detalles registrados de la más reciente optimización.



4.2.11 Habilitar la red Reyee Mesh

Cambie al modo **Red**. Seleccione **Red** > **Reyee Mesh**.



Después de que haya habilitado Reyee Mesh, se puede configurar una red de malla a través del emparejamiento de malla de los dispositivos que compatibles con Reyee Mesh. Presione el botón **Mesh** en el dispositivo para descubrir automáticamente un nuevo dispositivo para el emparejamiento de malla o inicie sesión en la página de gestión para seleccionarlo. Por defecto, Reyee Mesh se habilita en dispositivos con firmware ReyeeOS 1.86 o más reciente.

Siga los siguientes pasos para configurar una red de malla:

(1) Conecte el primer router a la red y configúrelo como dispositivo primario.

(2) Coloque el segundo router a 2 m del primero. Prenda el primer router.

(3) El indicador LED de estado del sistema del segundo router parpadeará por 2 o 3 minutos. Cuando el indicador LED de estado del sistema esté en encendido fijo, significa que el segundo router está prendido.

(4) Presione el botón **MESH** del primer router para realizar el emparejamiento de malla automáticamente.

Los LED de MESH en ambos routers estarán parpadeando por alrededor de 2 minutos. Cuando los LED de MESH dejen de parpadear y se queden en blanco fijo, el emparejamiento estará completo.

(5) Coloque el segundo router donde desee tener cobertura Wi-Fi y luego préndalo.

Espere de 3 a 5 minutos hasta que el LED de MESH muestre una luz fija. La red de malla se encuentra configurada y ahora puede acceder a Internet al conectarse a la nueva red Wi-Fi.

Nota

- Asegúrese de que el nuevo router se encuentre cerca del router primario y que haya pocos obstáculos entre ellos.
- Si desea añadir tres o más routers a la red de malla, repita los pasos 2 a 4. Puede añadir ocho dispositivos en un grupo en cualquier momento.

4.2.12 Configuración de un puerto LAN de un AP de enlace descendente.

Precaución

La configuración se aplica solo en los AP de enlace descendente con un puerto LAN cableado.

Cambie al modo **Red**. Seleccione **Red** > **Puertos LAN**.

En la ventana de **Configuración predeterminada**, ingrese la VLAN ID y haga clic en **Guardar** para configurar la VLAN a la cual pertenece el puerto LAN del AP. Si el campo de VLAN ID está vacío, el puerto LAN y el puerto WAN pertenecen a la misma VLAN.

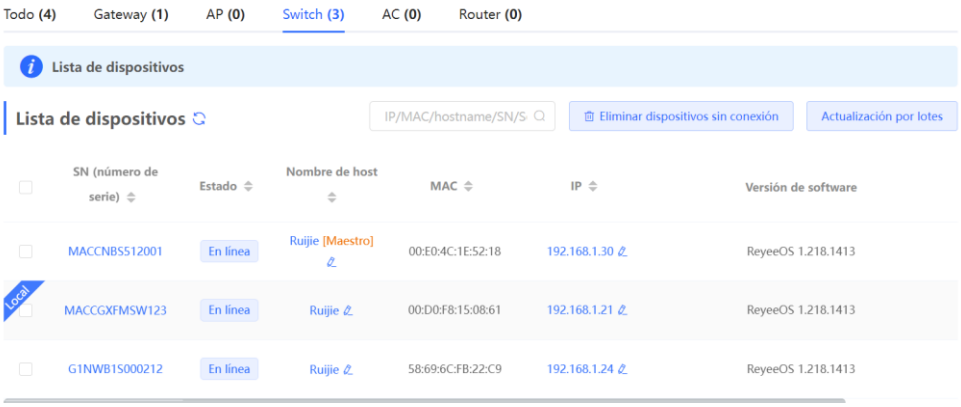
Haga clic en **Añadir** para agregar el puerto cableado del AP. Ingrese una VLAN ID y seleccione un AP.

En modo SON, la configuración del puerto cableado de AP aplica a todos los AP con puertos LAN cableados en la red actual. La configuración aplicada para los AP en **Configuración del puerto LAN** surte efecto de manera preferente.

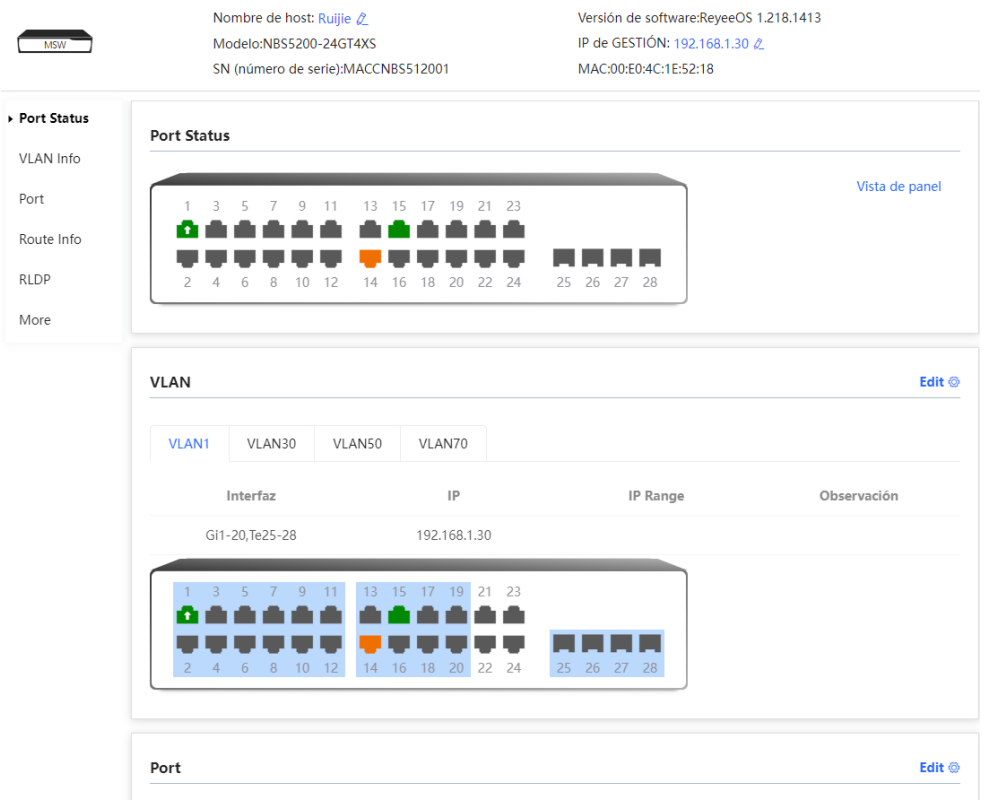
En el caso de los AP, si no se especifica ningún valor en **Configuración del puerto LAN**, se aplicará la configuración predeterminada para los puertos cableados del AP.

4.3 Configuración del switch

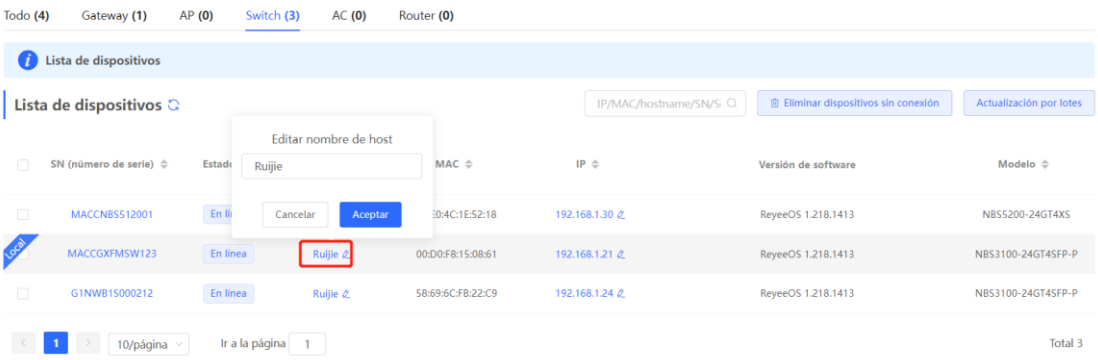
La **Lista de dispositivos** incluye todos los conmutadores administrados por el router. La información incluye el nombre de host del conmutador, la dirección IP, la dirección MAC, el estado, el modelo, la versión del software y el SN. Se pueden revisar las categorías del AP haciendo clic en .



- **Gestionar**: abra la página de configuración detallada del conmutador.



- **Editar nombre de host**: modifique el nombre del host del conmutador.

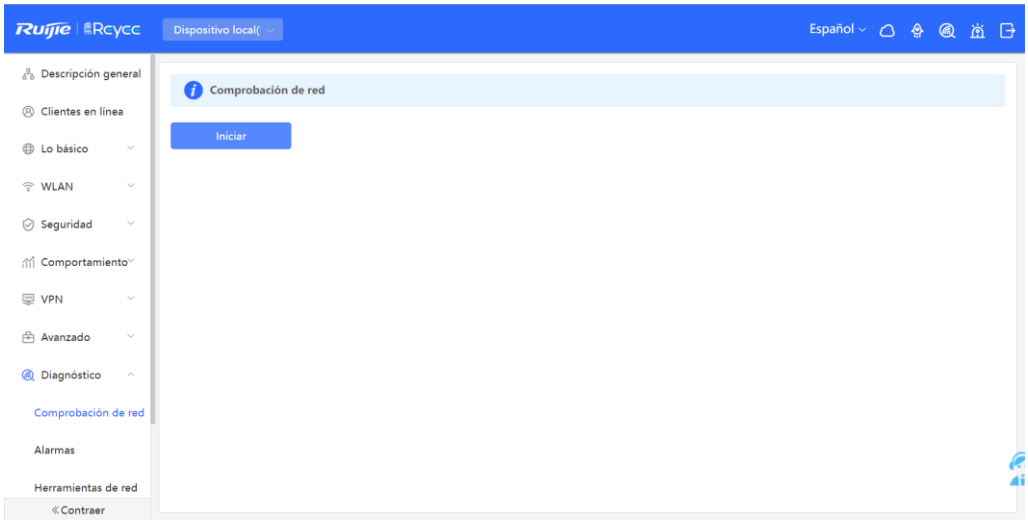


4.4 Diagnóstico

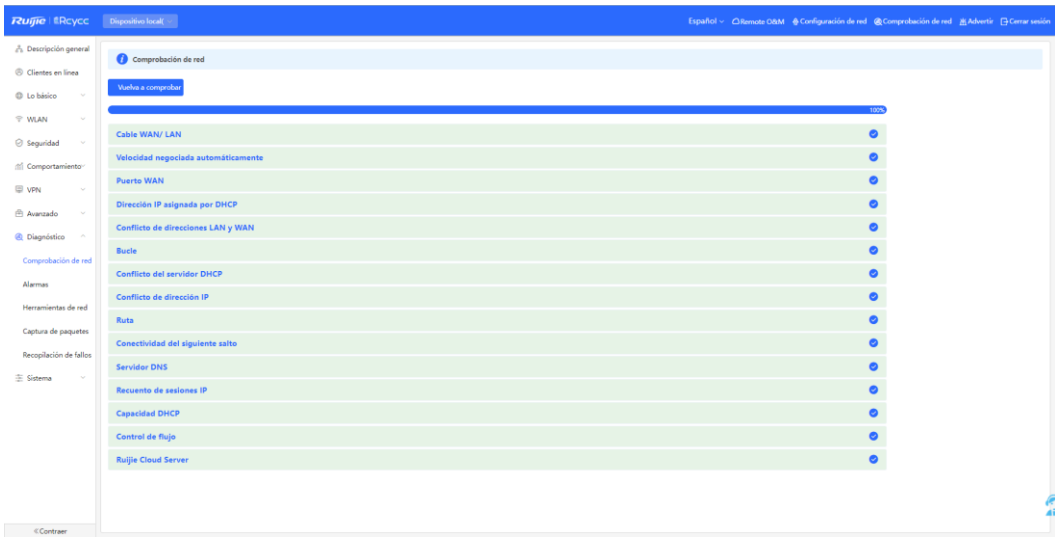
4.4.1 Revisión de la red

En esta página puede analizar su red y resolver cualquier problema que presente.

(1) Cambie al modo **Dispositivo local**. Seleccione **Diagnóstico > Comprobación de red**. Haga clic en **Iniciar** y luego en **Aceptar** en el cuadro de diálogo para comenzar a analizar el estado de la red.



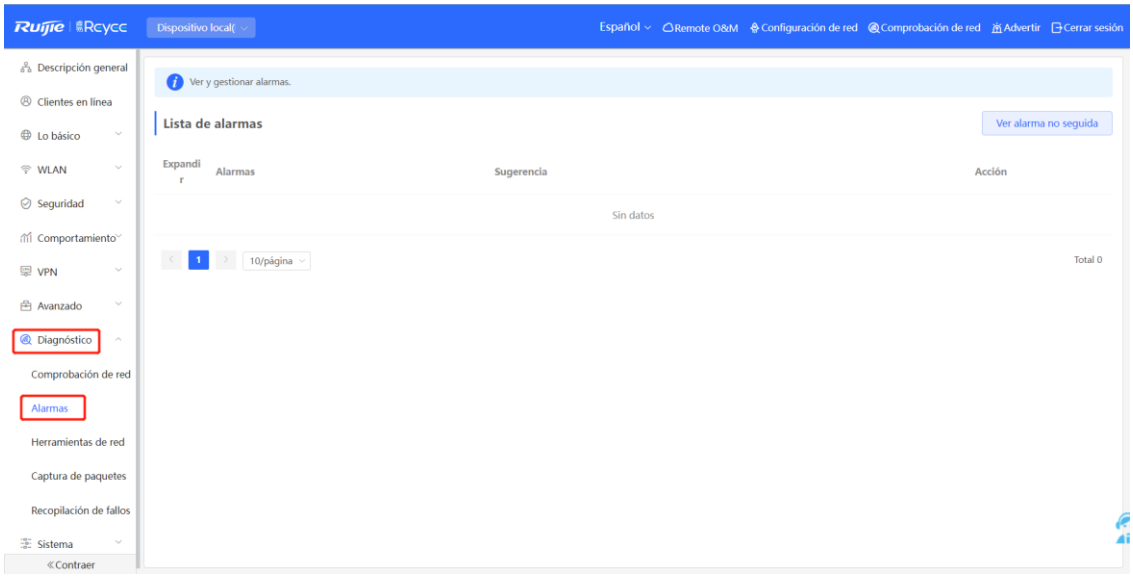
(2) Los resultados se mostrarán después de que la revisión termine.



4.4.2 Alarmas

La página de **Alarmas** le permite consultarlas y administrarlas.

(1) Cambie al modo **Dispositivo local**. Seleccione **Diagnóstico** > **Alarmas**.

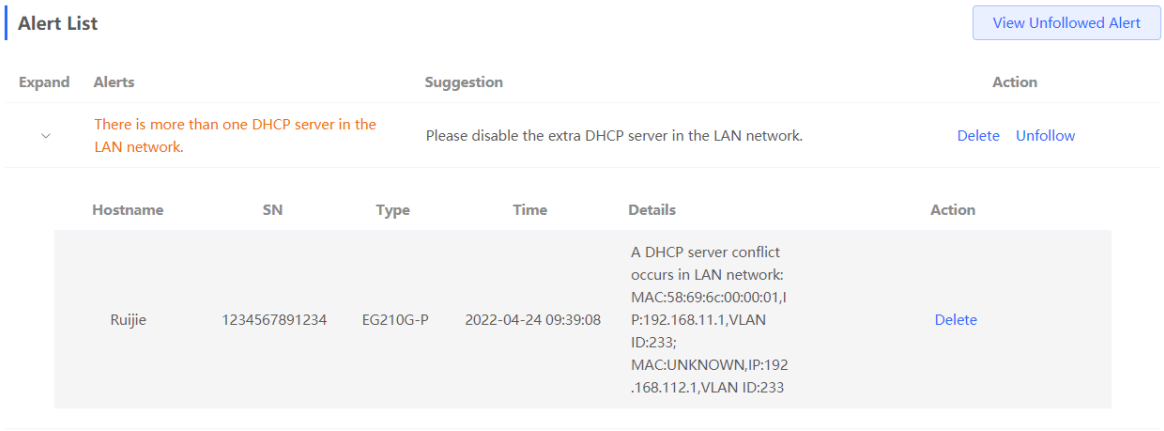


(2) La página de **Lista de alarmas** muestra los posibles problemas en el ambiente de la red y del dispositivo.

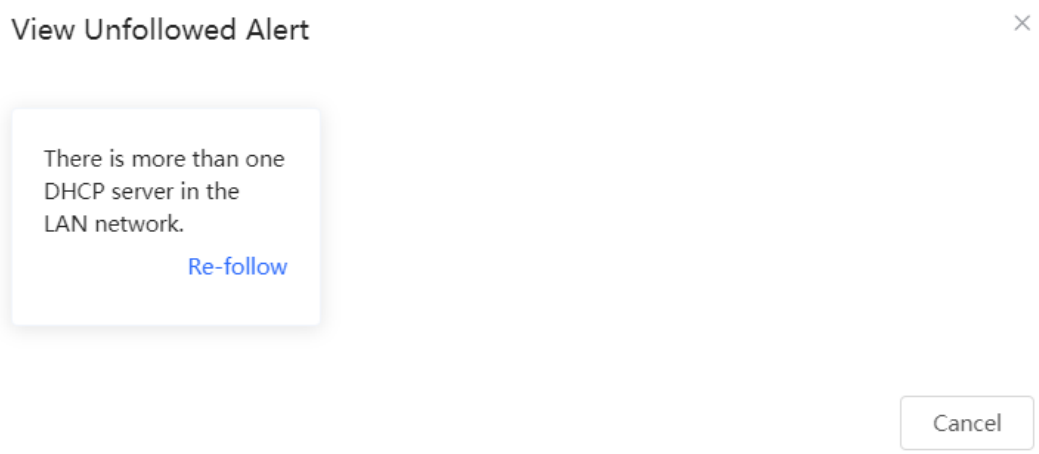
Todos los tipos de alarmas se encuentran activados de forma predeterminada. En la columna de **Action**, haga clic en **Unfollow** para dejar de recibir este tipo de alertas.

Precaución

Después de dejar de seguir un tipo de alerta en específico, no podrá descubrir ni procesar todas las alertas de este tipo a tiempo. Por lo tanto, se recomienda que realice esta operación con precaución.

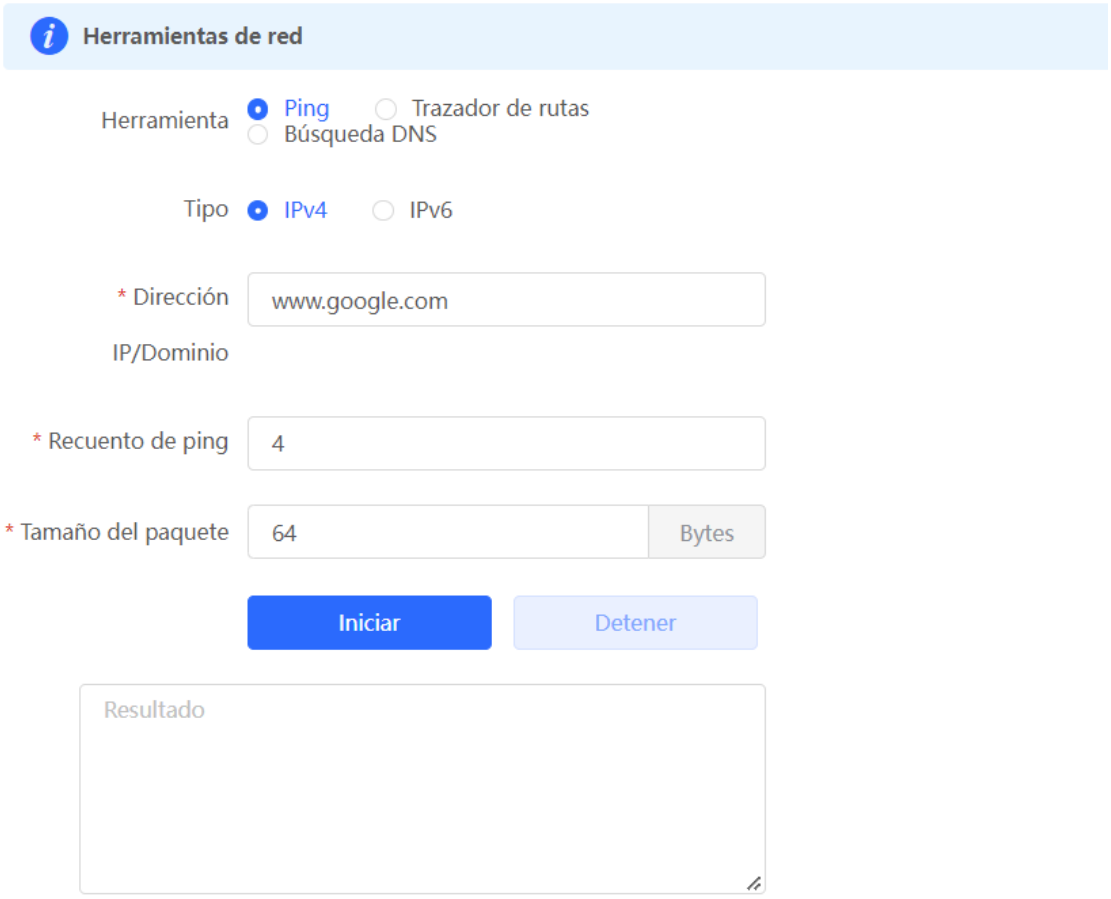


(3) Haga clic en **View Unfollowed Alert** para ver la alerta no seguida. En la ventana que aparece, puede seguir la alerta nuevamente.



4.4.3 Herramientas de red

Cambie al modo **Dispositivo local**. Seleccione **Diagnóstico** > **Herramientas de red**.

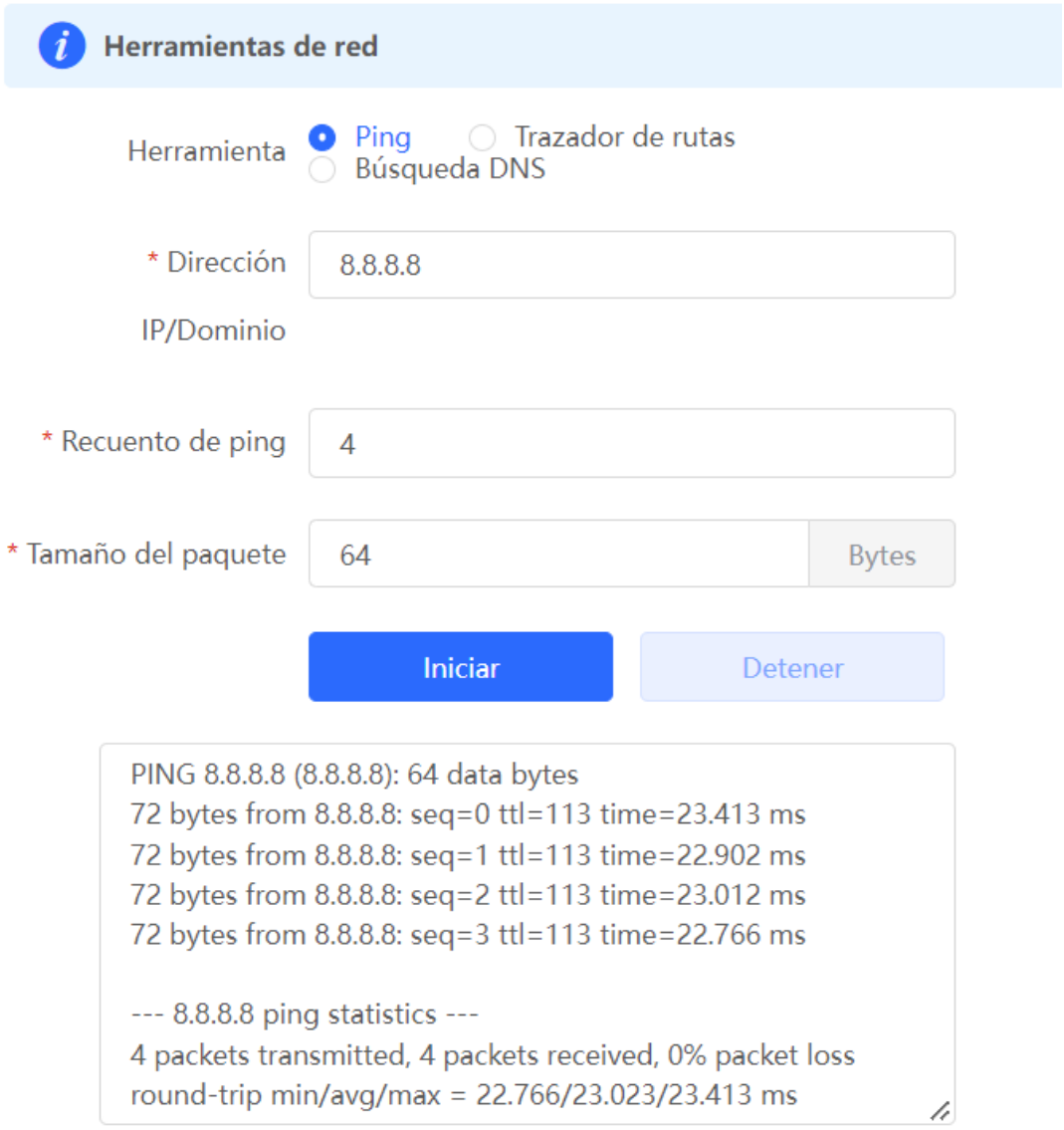


Seleccione un método de diagnóstico, ingrese una dirección IP o URL y haga clic en **Iniciar**.

- El método ping se utiliza para probar la conectividad entre el dispositivo probado y la dirección o el URL especificados. Si el procedimiento del ping falla, la dirección IP o el URL fallan en hacer ping desde el dispositivo.
- El método trazador de rutas se utiliza para rastrear las rutas de la red a la dirección IP o el URL especificados.
- El método búsqueda DNS se utiliza para revisar la dirección del servidor DNS para el análisis del URL.

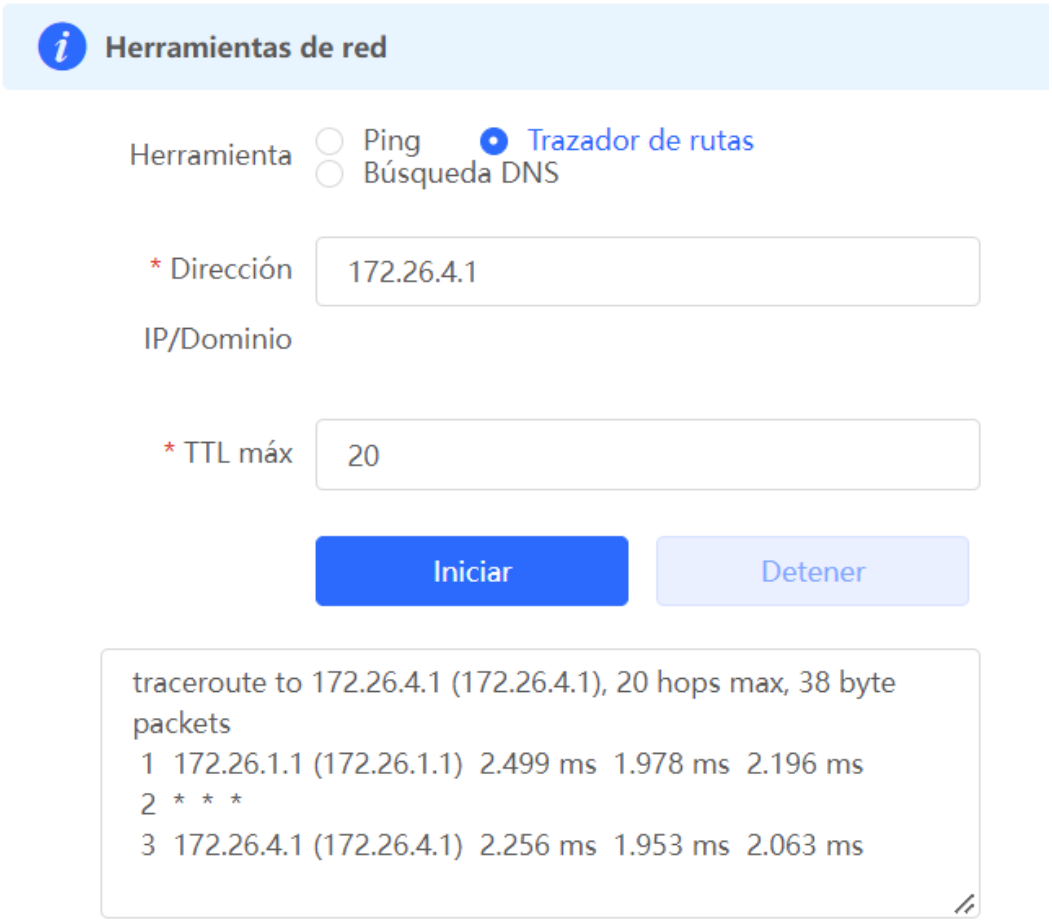
1. Herramienta de ping

Configure la **Dirección IP/Dominio,** el **Recuento de ping** y el **Tamaño del paquete** en esta página y haga clic en **Iniciar**. El resultado del ping se mostrará.



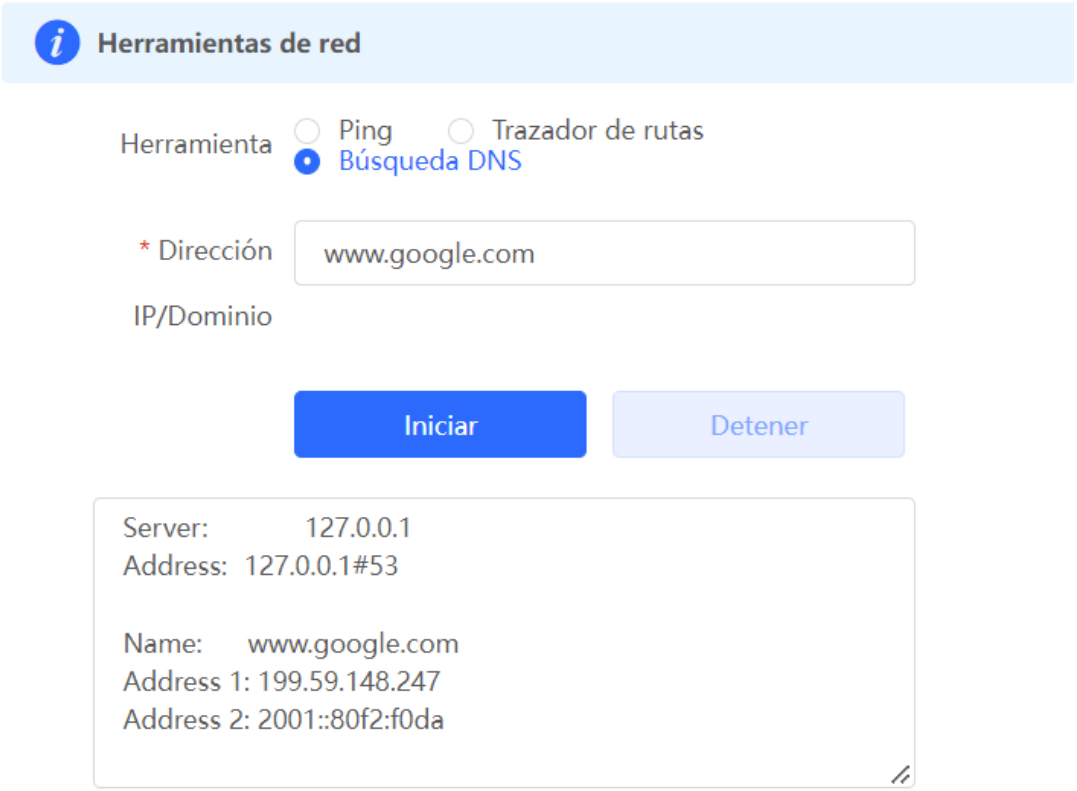
2. Herramienta de trazador de rutas

Configure en esta página la **Dirección IP/Dominio**, el **TTL máx** y haga clic en **Iniciar**. El resultado del trazador de rutas se mostrará.



3. Herramienta de búsqueda DNS

Esta herramienta se utiliza para averiguar el nombre del dominio en una dirección IP.



4.4.4 Captura de paquetes

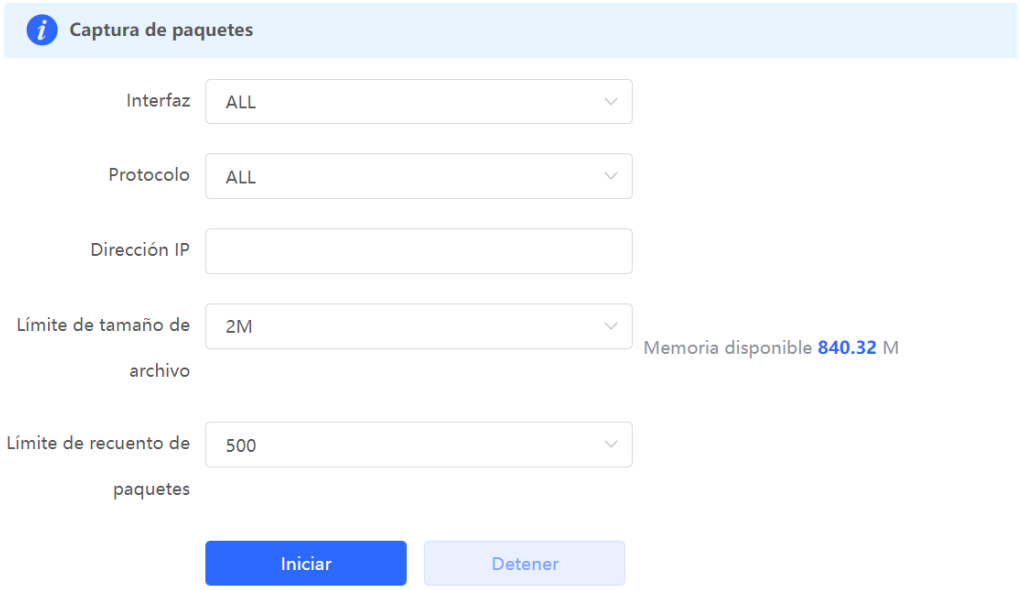
Cambie al modo **Dispositivo local**. Seleccione **Dispositivo local** > **Captura de paquetes**.

Si el dispositivo falla y se requiere identificar el problema, se puede analizar el resultado de la captura de paquetes para localizarlo y rectificarlo.

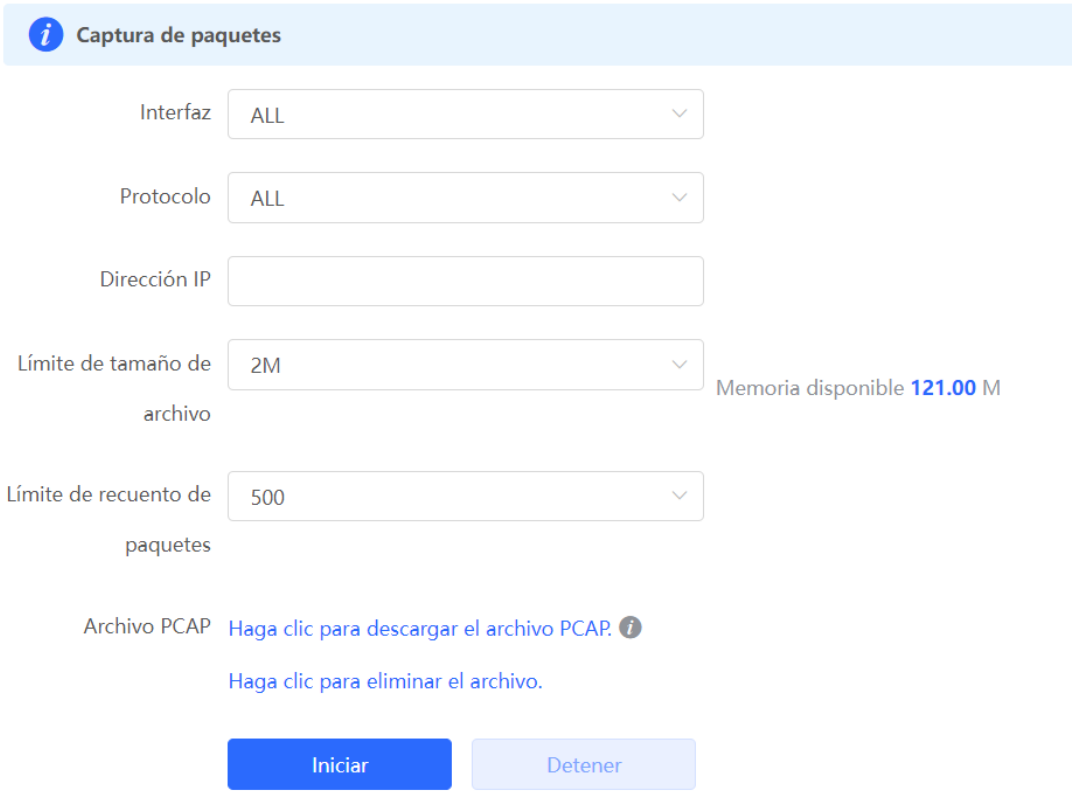
Configure una interfaz y un protocolo, y especifique la dirección IP del host para capturar el contenido de los paquetes de datos. Seleccione el límite del tamaño del archivo y del recuento de paquetes para determinar las condiciones para detener automáticamente la captura de paquetes. Si el tamaño del archivo o el número de paquetes alcanza el límite especificado, la captura de paquetes se detendrá y se generará un enlace de descarga de un diagnóstico de paquetes. Haga clic en **Iniciar** para ejecutar el comando de captura de paquetes.

Precaución

El procedimiento de captura de paquetes puede ocupar muchos recursos del sistema, ocasionando que la red se congele. Por lo tanto, se recomienda que realice esta operación con precaución.



La captura de paquetes puede detenerse en cualquier momento. Posteriormente, se genera un enlace de descarga. Haga clic en este enlace para guardar localmente el resultado de la captura de paquetes en formato PCAP. Utilice cualquier software como Wireshark para ver y analizar el resultado.



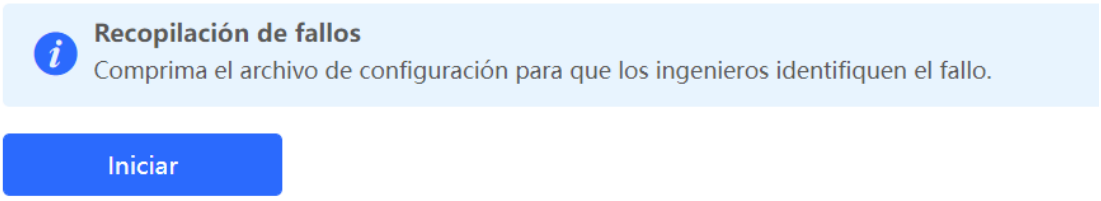
- **Interfaz:** capture los paquetes que están pasando por la interfaz seleccionada.
- **Protocolo:** capture los paquetes del protocolo seleccionado.

- **Dirección IP:** capture los paquetes de la dirección IP seleccionada.
- **Límite de tamaño de archivo:** establezca el límite del tamaño de un paquete.
- **Límite de recuento de paquetes:** establezca el límite de recuento de paquetes. Cuando el número de paquetes llegue al límite, la captura de paquetes se detendrá y se generará un enlace de descarga.

4.4.5 Recopilación de fallos

Cambie al modo **Dispositivo local**. Seleccione **Diagnóstico local** > **Recopilación de fallos**.

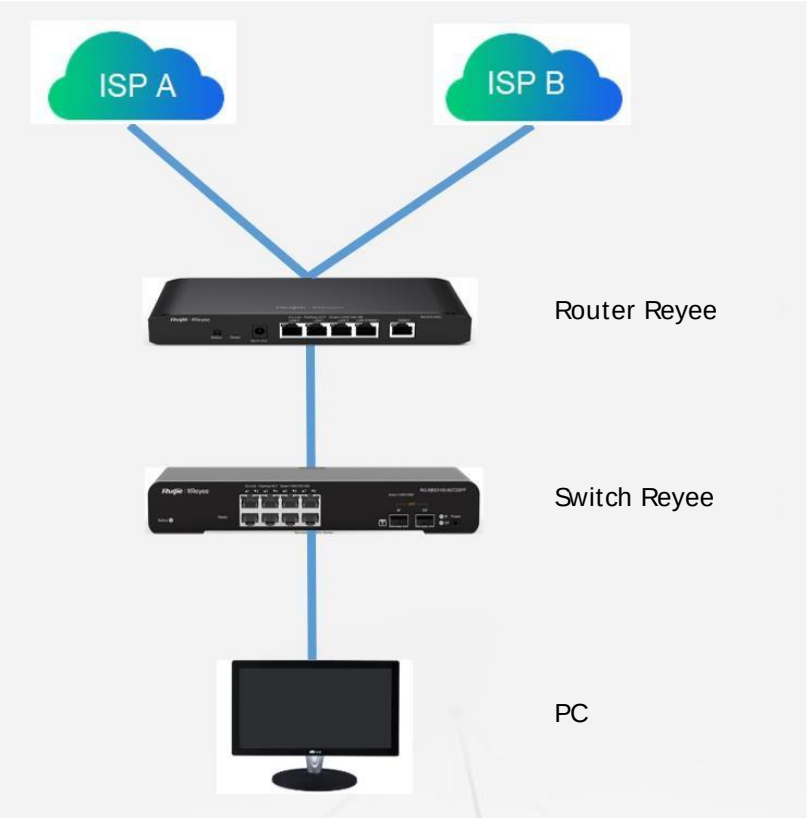
Cuando el dispositivo falla, se debe recopilar la información correspondiente. Haga clic en **Iniciar**. Los archivos de configuración del dispositivo se guardarán en un archivo comprimido. Descargue de manera local el archivo comprimido y entréguelo al personal de I y D para que localicen la falla.



Comprima el archivo de configuración para que los ingenieros identifiquen los errores.

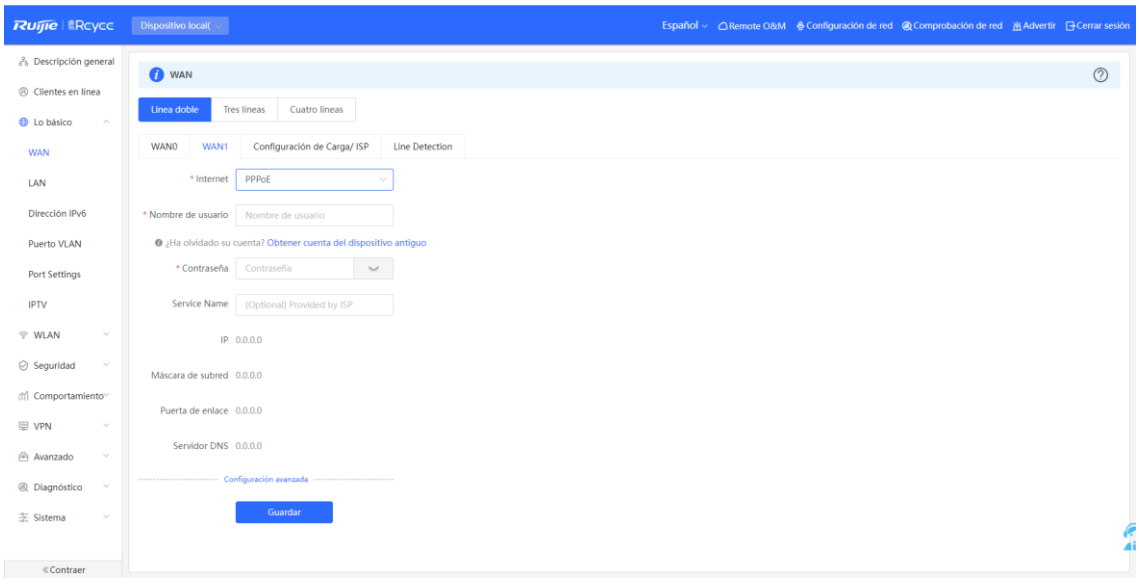
4.5 Equilibrio de carga de la WAN

Si hay más de un puerto WAN, parte del tráfico se enruta a través de la ruta del ISP, y el tráfico restante se administrará de acuerdo con el modo de carga.



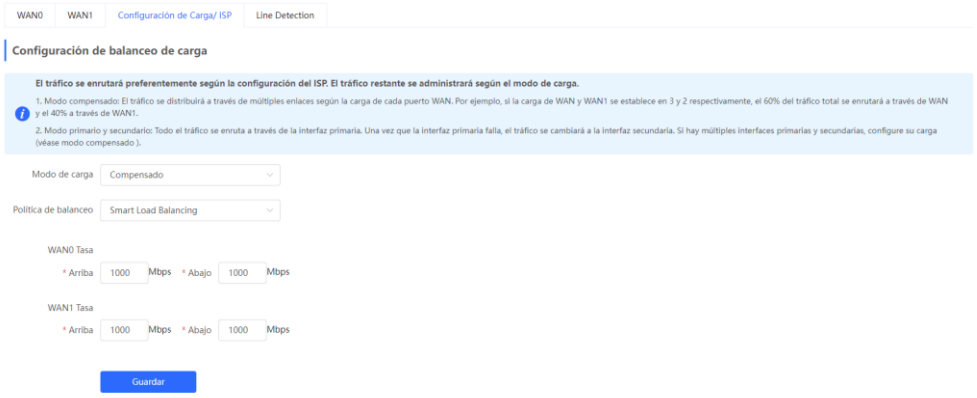
Prepare dos cables de enlace ascendente para tener acceso a Internet antes de la configuración.

(1) Cambie al modo **Dispositivo local**. Seleccione **Lo básico** > **WAN**.



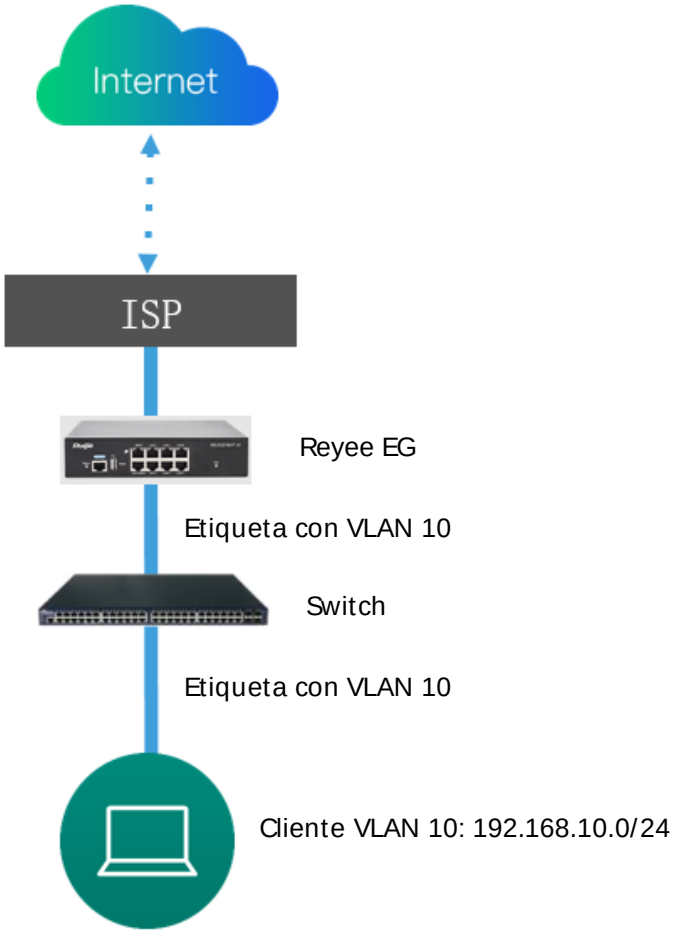
(2) Configure **WAN** según corresponda.

(3) Seleccione **Configuración de Carga/ ISP** y configure el modo de carga y el peso de la interfaz.

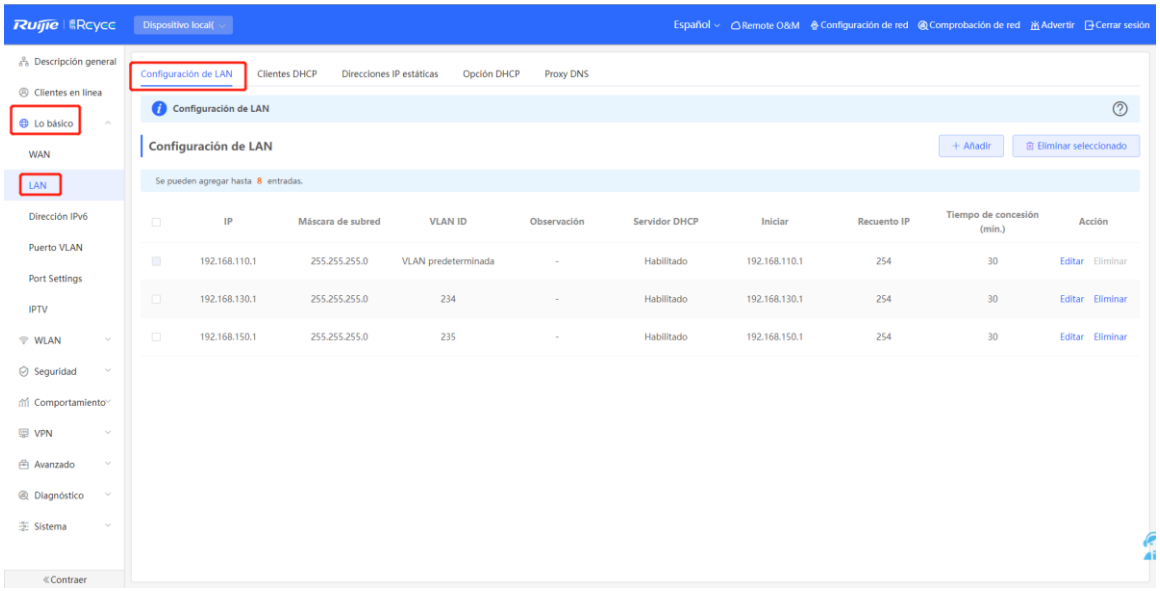


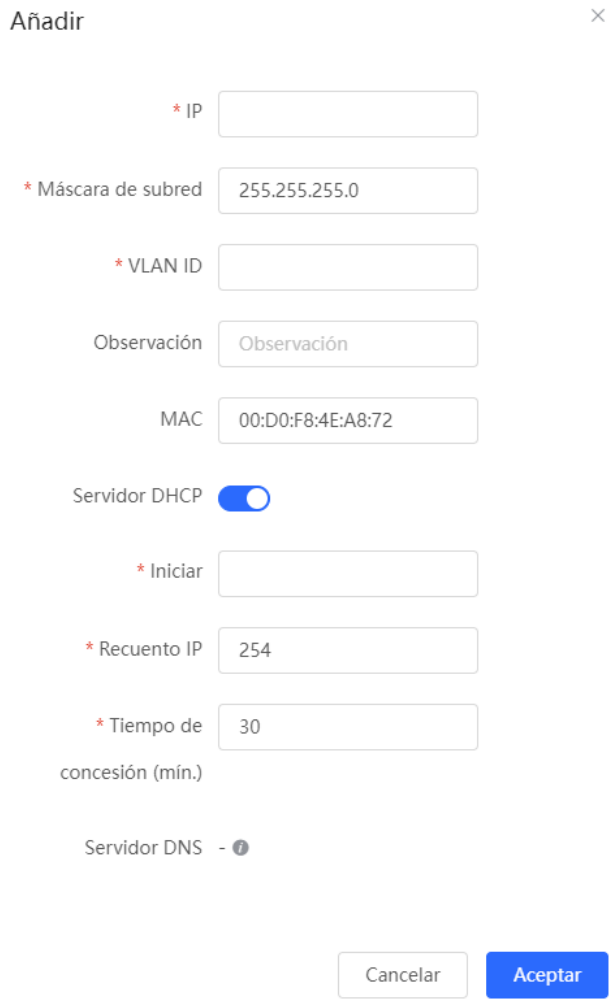
- **Compensado:** el tráfico se distribuirá a través de múltiples enlaces, según la carga de cada puerto WAN. Por ejemplo, si el valor de **WAN** y **WAN1** se configura en 3 y 2, respectivamente, el 60 % del tráfico total se enrutará a **WAN** y el 40 % a **WAN1**.
- **Primario y secundario:** todo el tráfico se enrutará a través de la interfaz primaria. Si se produce un error en la interfaz primaria, el tráfico cambiará a la interfaz secundaria. Si hay múltiples interfaces primarias y secundarias, configure sus valores.

4.6 Puerto VLAN



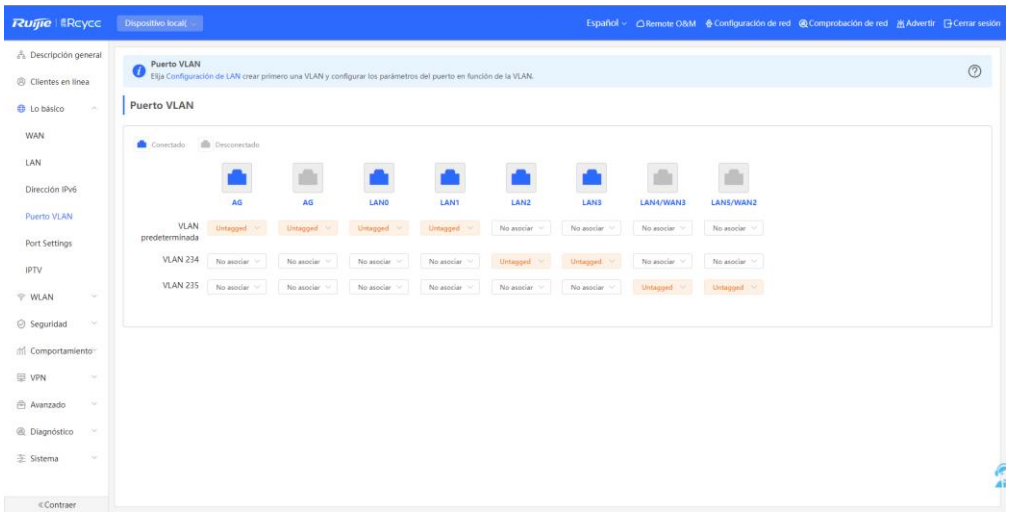
(1) Cambie al modo **Dispositivo local**. Seleccione **Lo básico** > **LAN** para crear primero una VLAN.





Cuando la LAN haya sido configurada exitosamente, se mostrará en **Configuración de LAN**.

(2) Seleccione **Lo básico** > **Puerto VLAN para etiquetar la VLAN**. Por defecto, el modo etiquetado se utiliza para las VLAN.

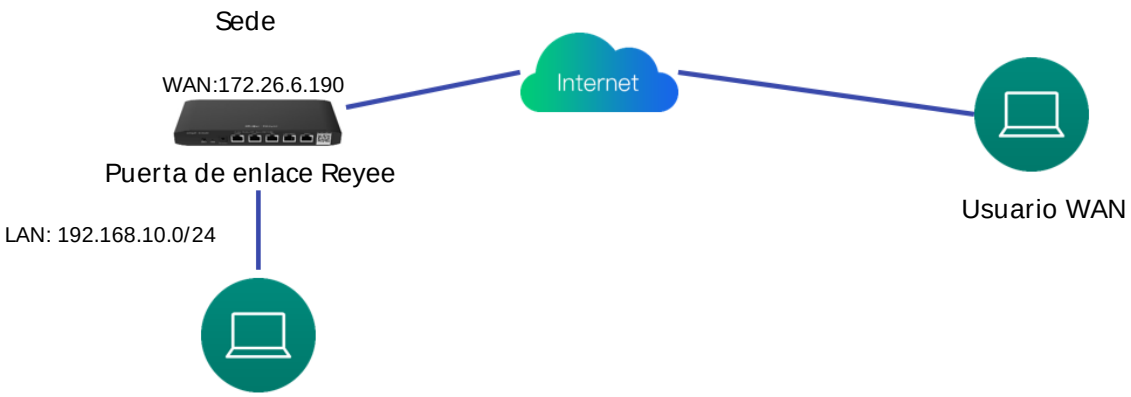


- **NO ETIQUETADO:** si el tráfico de VLAN 10 se configura en el puerto 2 como **NO ETIQUETADO**, esta será la VLAN nativa del puerto. Los paquetes de VLAN 10 se reenvían a través del puerto 2 sin su etiqueta correspondiente y se consideran pertenecientes a VLAN 10.
- En cada puerto se puede configurar una sola VLAN con tráfico no etiquetado.
- La VLAN nativa del puerto 1 es la predeterminada y no puede modificarse.
- **ETIQUETADO:** si el tráfico de VLAN 10 y el de VLAN 20 se configuran como **ETIQUETADO** en el puerto 2, los paquetes de ambas se reenviarán a través de este.
- **No asociar:** si el tráfico de VLAN 10 y el de VLAN 20 se configuran como **No asociar** en el puerto 2, este no recibirá ni transmitirá los paquetes de ninguna de ellas.

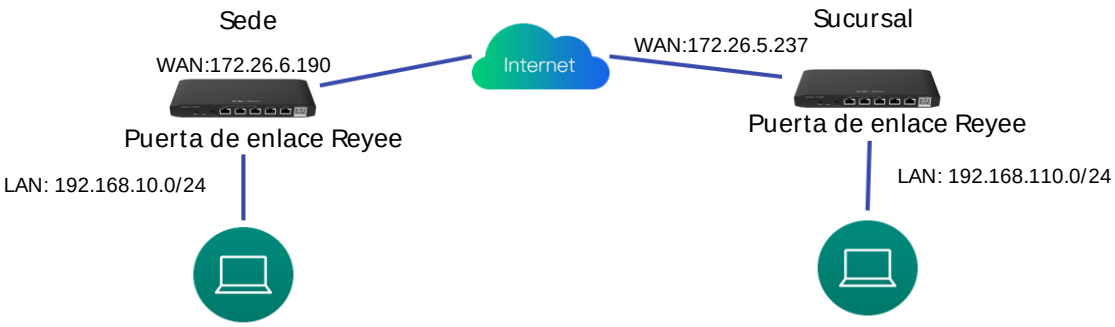
4.7 VPN

Escenario de aplicación

- Escenario de cliente a sitio



- Escenario de sitio a sitio



4.7.1 VPN PPTP

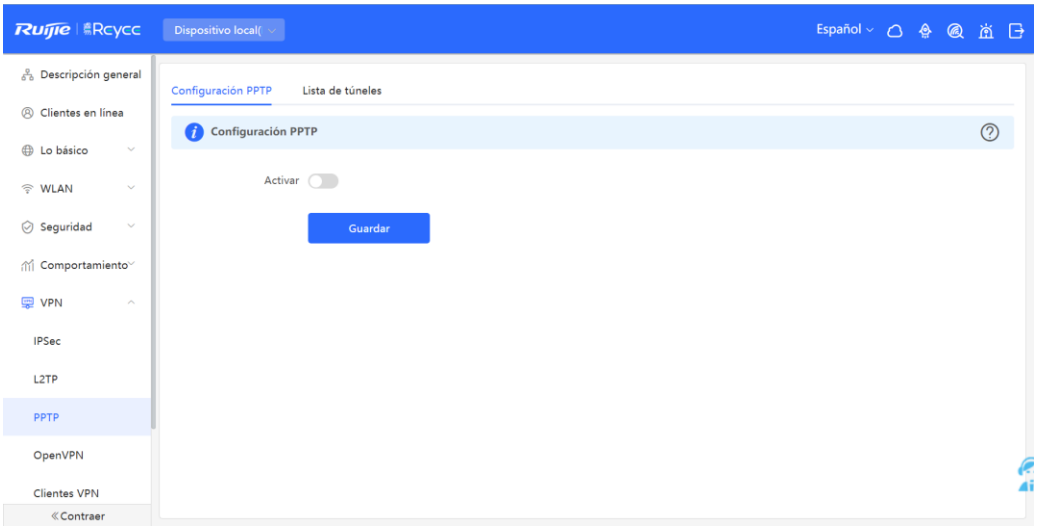
La VPN PPTP se utiliza generalmente en escenarios donde se requiere conectar a un cliente con un sitio y un sitio con otro sitio. Por ejemplo, los clientes trabajan desde casa y requieren acceder a los servidores de la empresa mediante túneles de VPN PPTP; una empresa cuenta con tres sucursales que están distribuidas en tres lugares diferentes y cada una necesita establecer un túnel con las otras a través de un router.

1. Configuración para un escenario de cliente a sitio

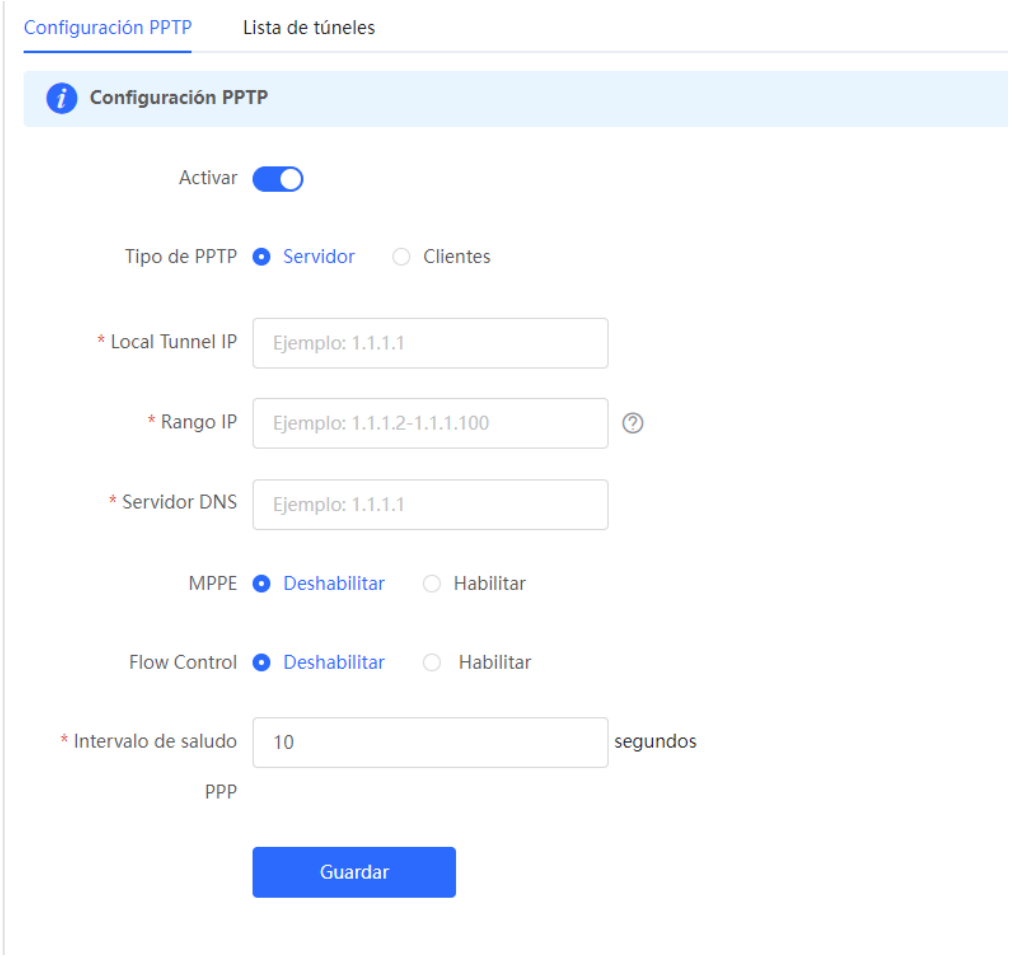
(1) Lado de la sede:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

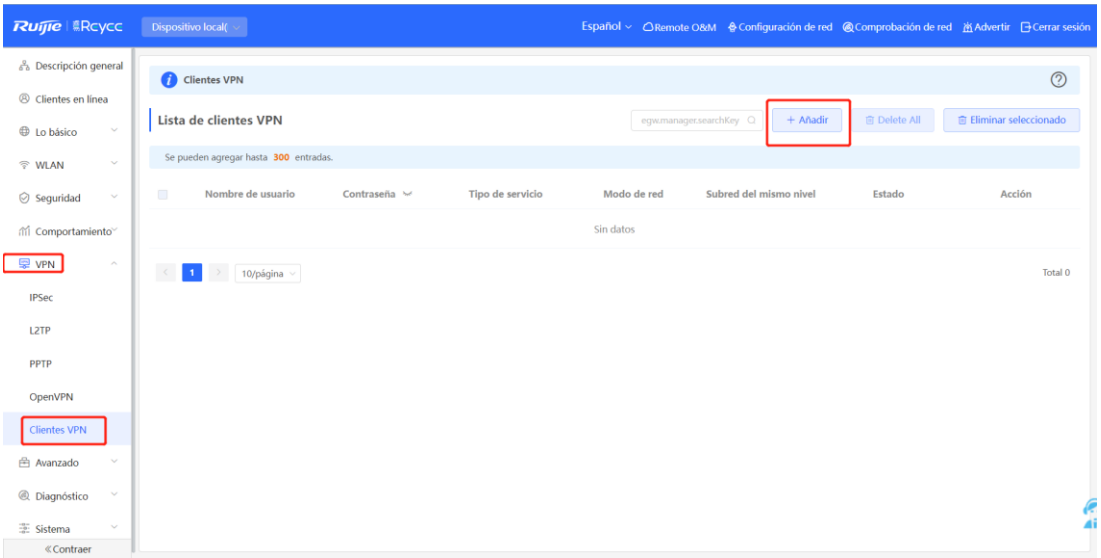
b Cambie al modo **Dispositivo local**. Seleccione **VPN** > **PPTP** y active PPTP.

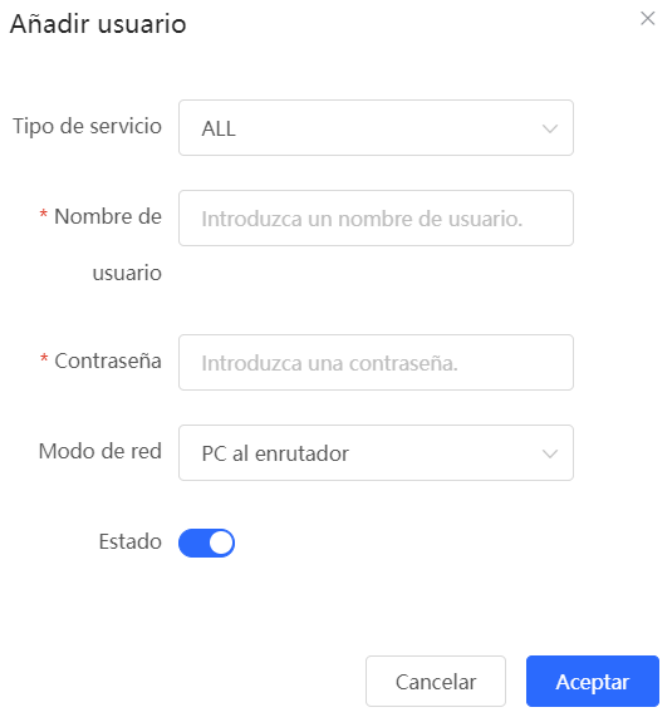


c Lleve a cabo la configuración de PPTP y haga clic en **Guardar**.



d Seleccione **VPN > Clientes VPN** y configure los clientes VPN.



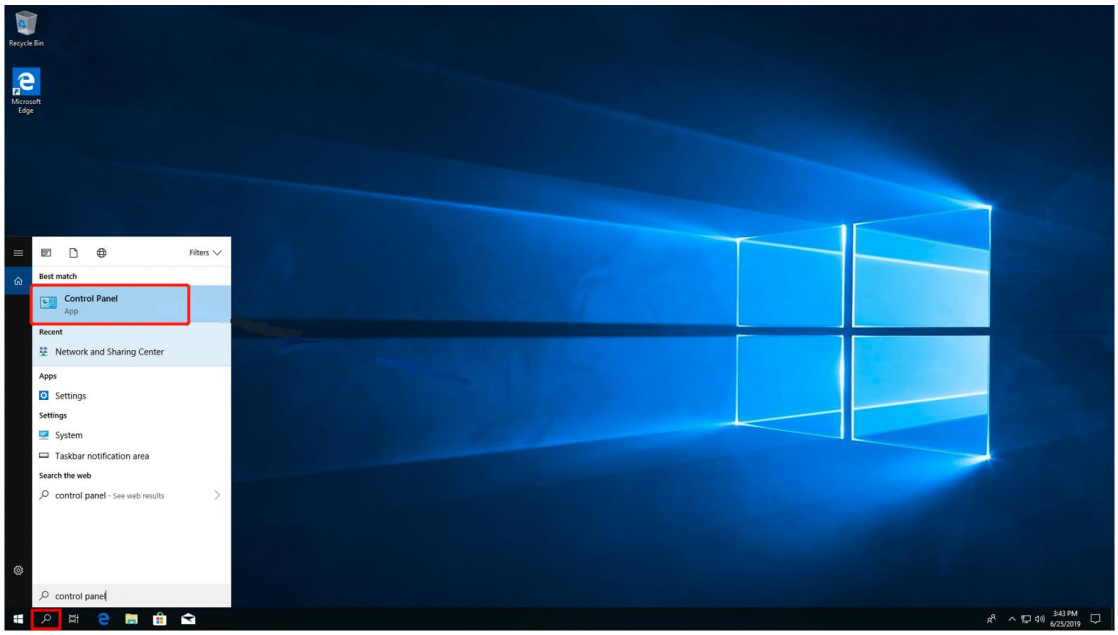


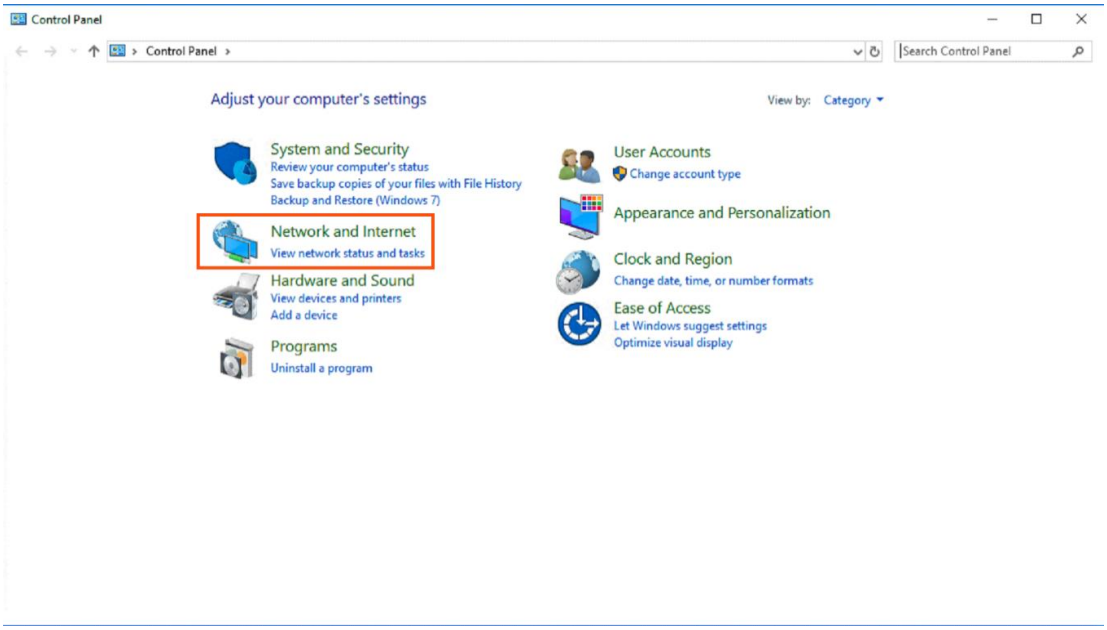
Nota

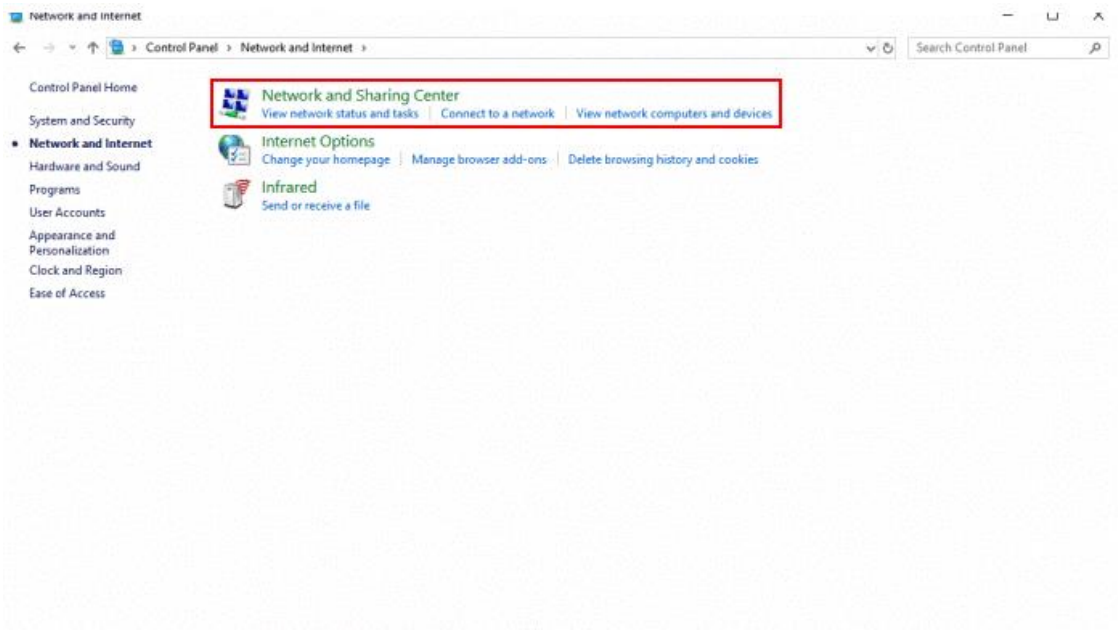
- **Tipo de servicio**: seleccione **PPTP**.
- **Modo de red**: seleccione **Enrutador a Enrutador**:
- **Subred del mismo nivel:** complete el segmento de la red interna de la sucursal. El valor y el segmento de la red interna de la sede no pueden superponerse.

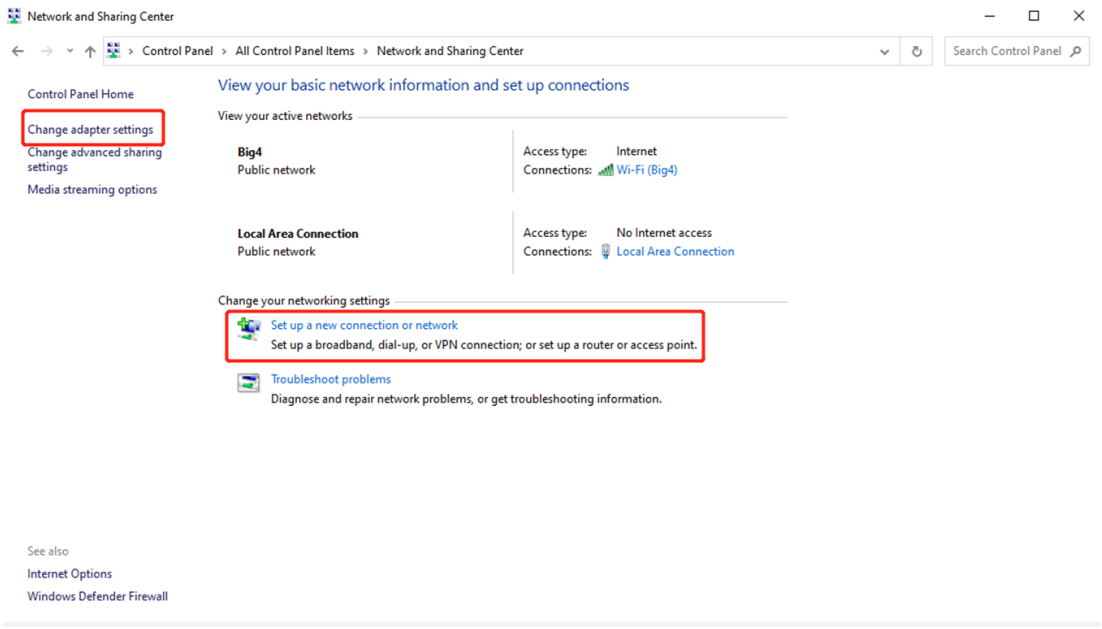
(2) Lado del cliente (se utiliza Windows 10 como ejemplo):

a Seleccione **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

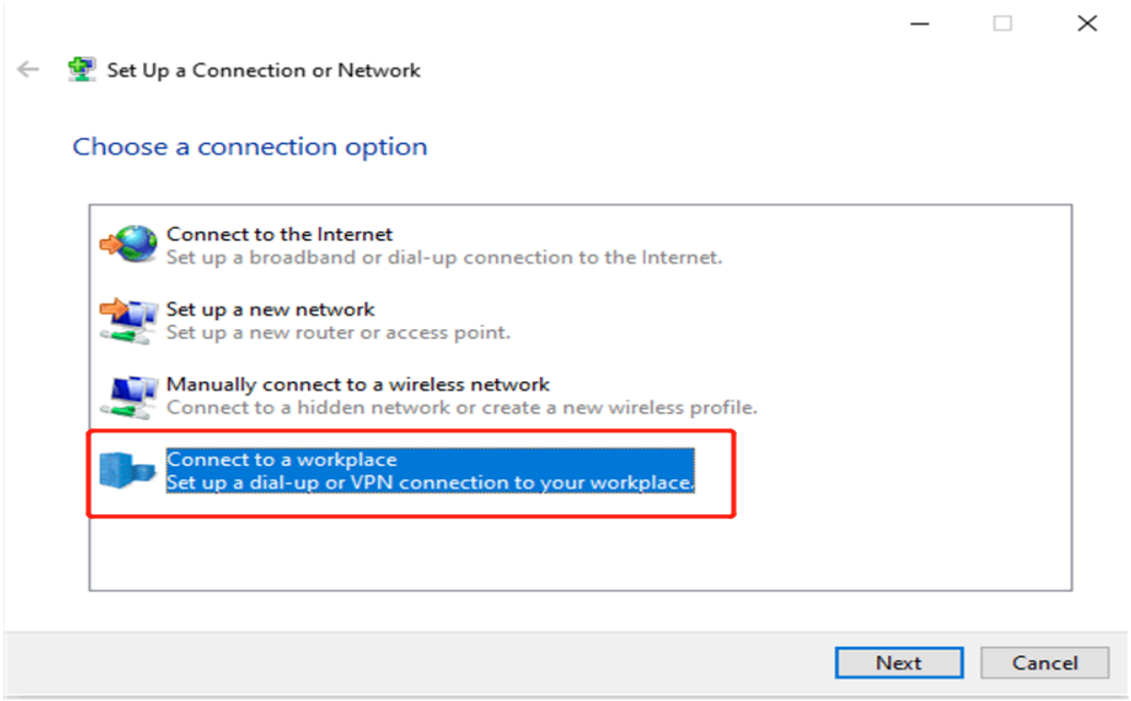


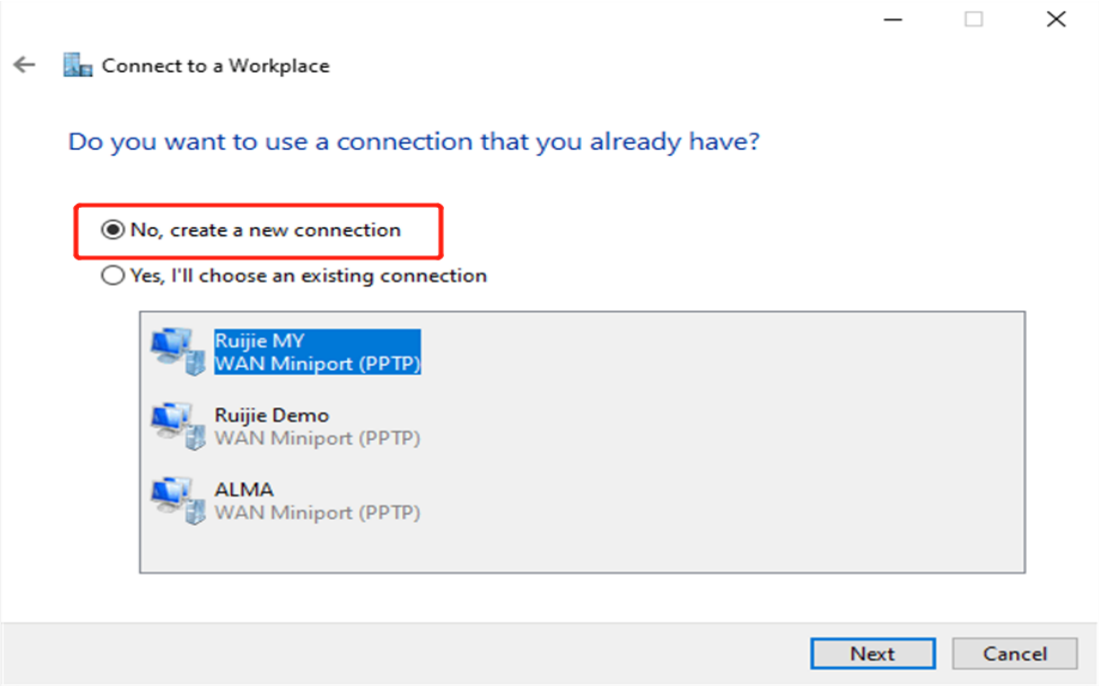

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

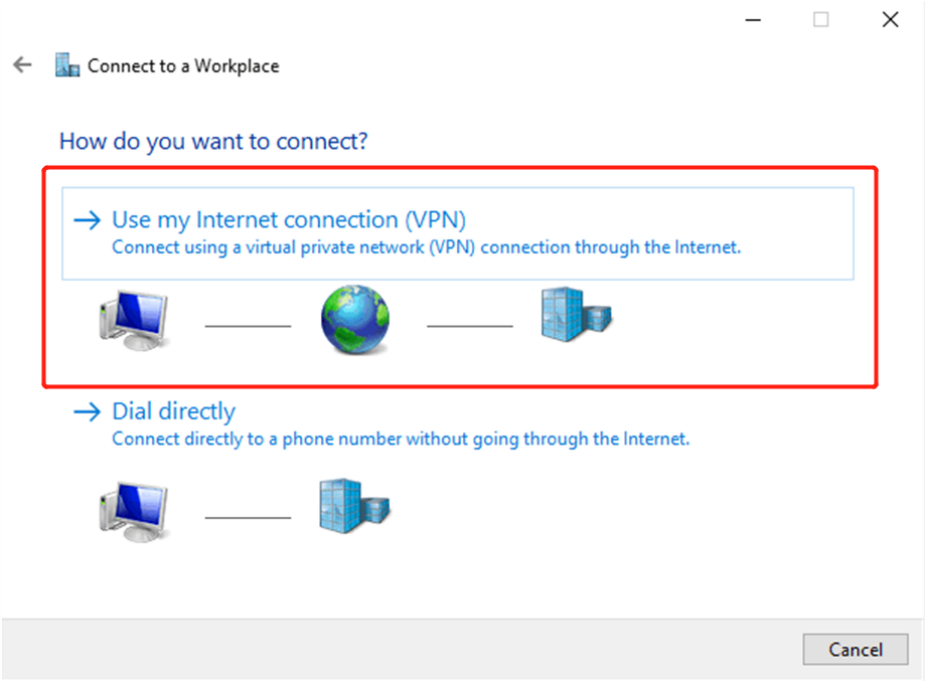

Network and Internet
Control Panel › Network and Internet ›
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Network and Sharing Center
View network status and tasks | Connect to a network | View network computers and devices
Internet Options
Change your homepage | Manage browser add-ons | Delete browsing history and cookies
Infrared
Send or receive a file

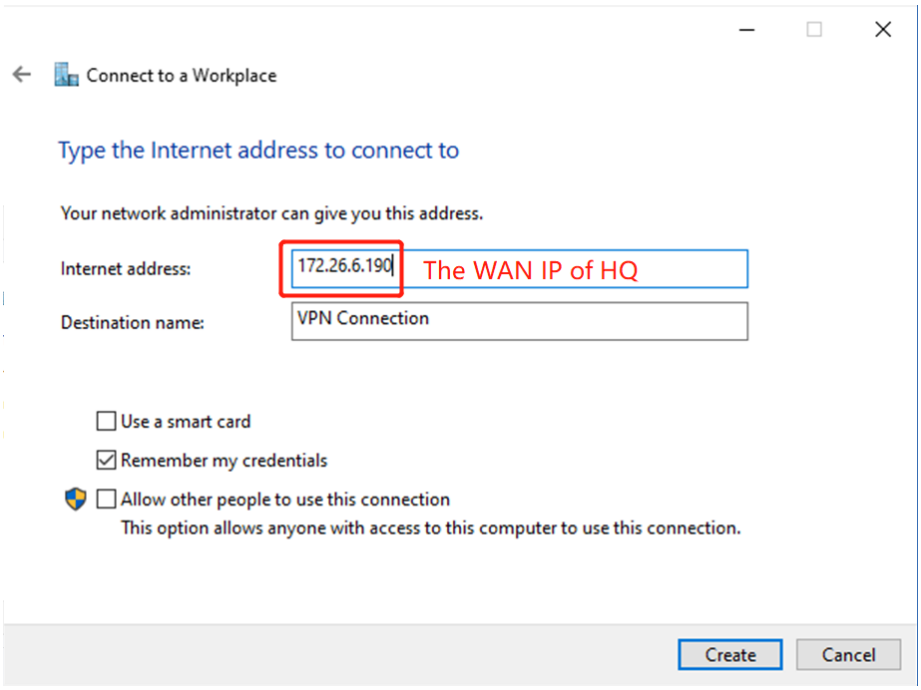


b Configure una conexión VPN.

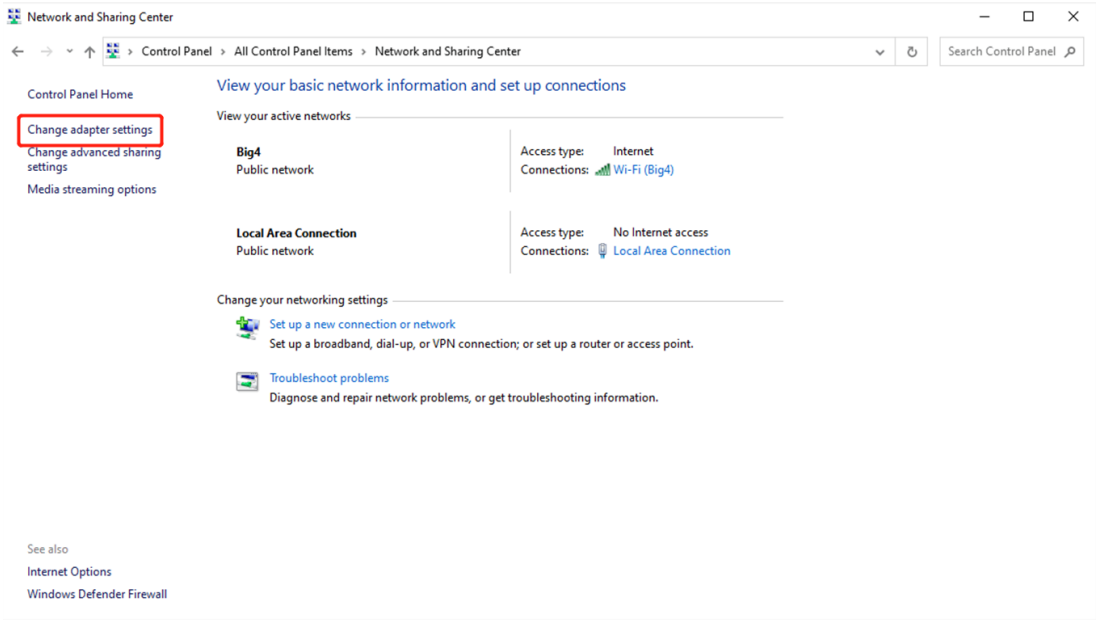


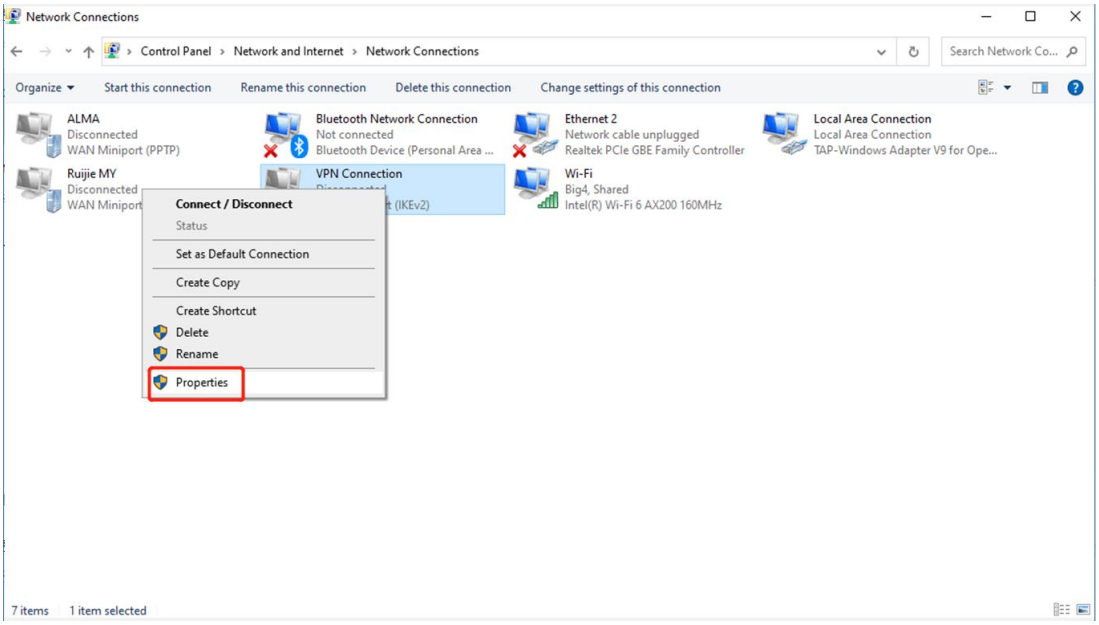

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

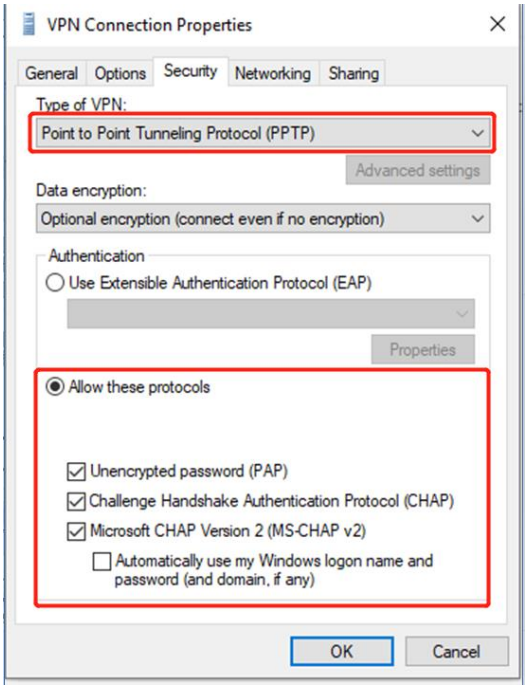

Connect to a Workplace
How do you want to connect?
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
Cancel



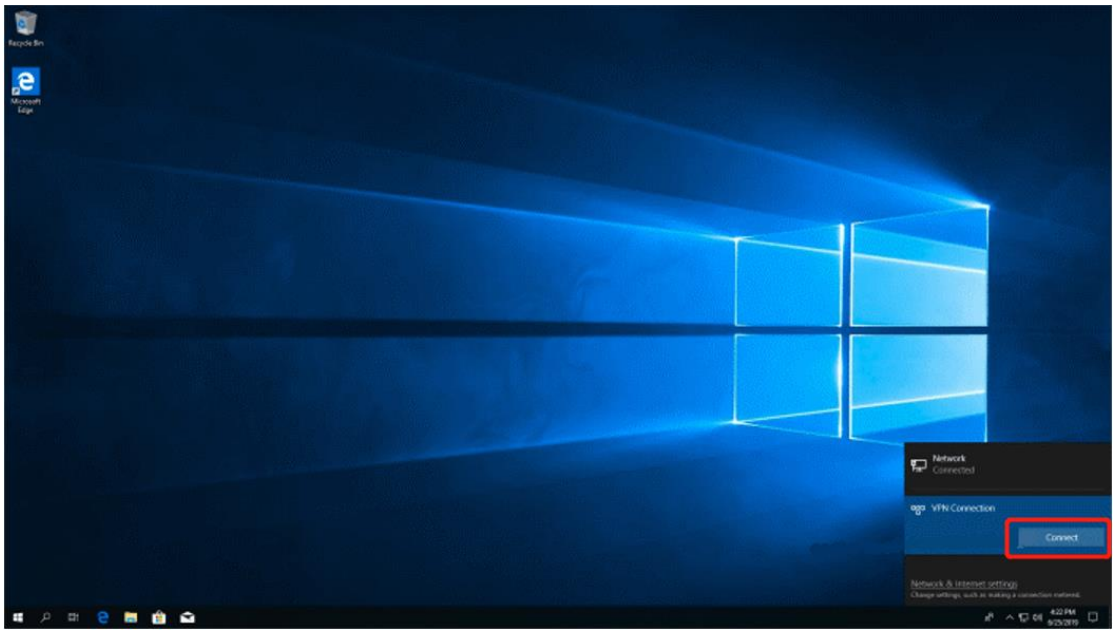
c Cambie la configuración del adaptador.

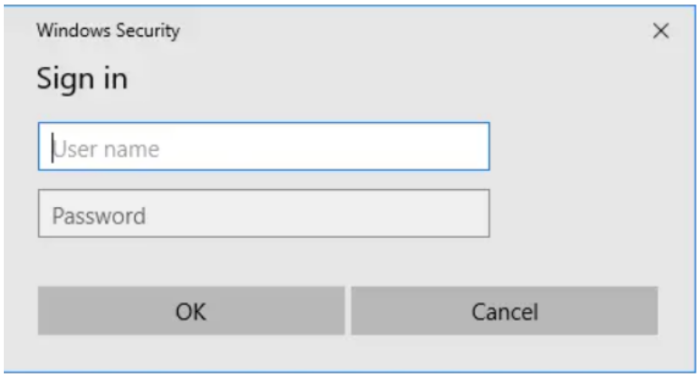


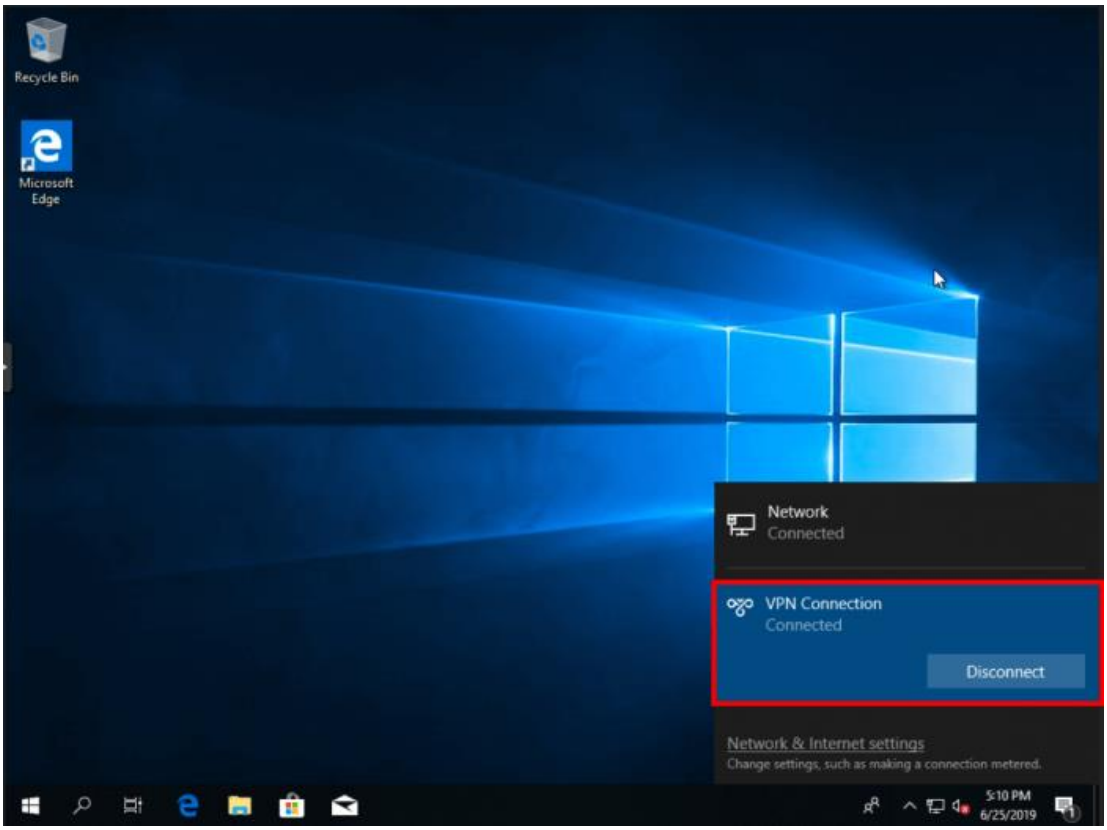




d Verifique el estado de la conexión VPN.


Network
Connected
VPN Connection
Connect
Network & Internet settings


Windows Security
Sign in
User name
Password
OK
Cancel



e Si su PC no cuenta con acceso a los dispositivos internos (192.168.10.0/24) de la sede después de configurar la conexión VPN, añada la siguiente ruta estática en su PC. La dirección IP 192.168.100.2 es la que la PC obtiene de la sede. De este modo, la PC tendrá acceso a los dispositivos internos de la sede.

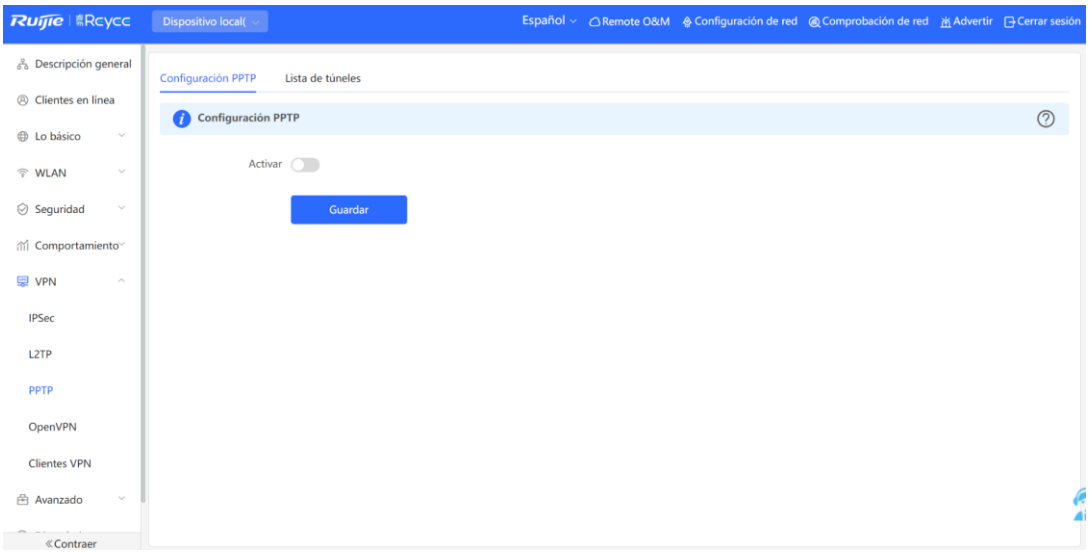
```
C:\Users\Daisy>route add 192.168.168.10.0 mask 255.255.255.0 192.168.100.2
```

2. Configuración para un escenario de sitio a sitio

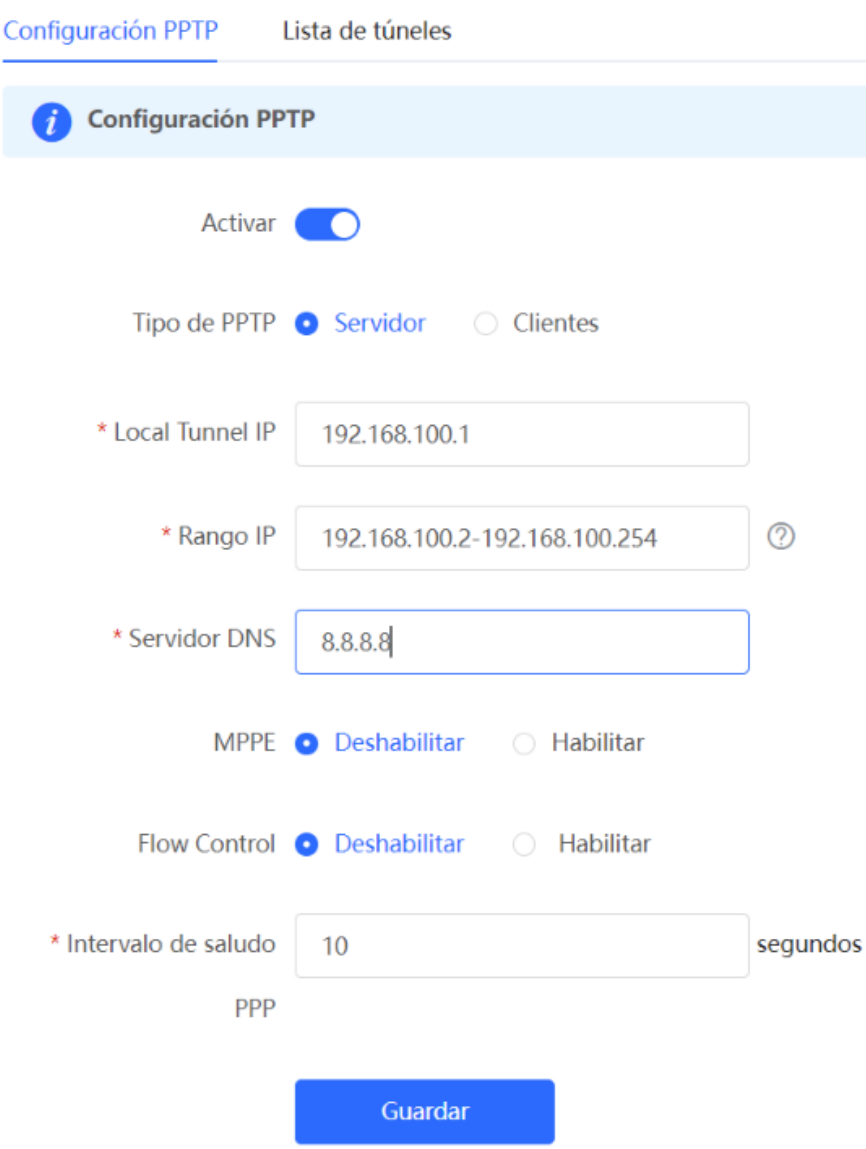
(1) Lado de la sede:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

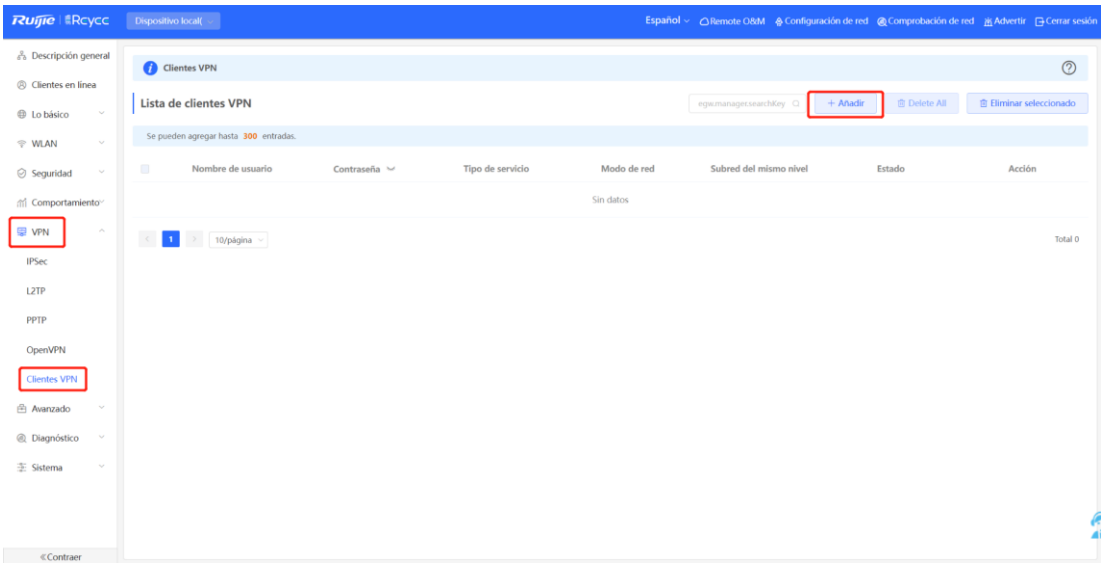
b Cambie al modo **Dispositivo local**. Seleccione **VPN** > **PPTP**.

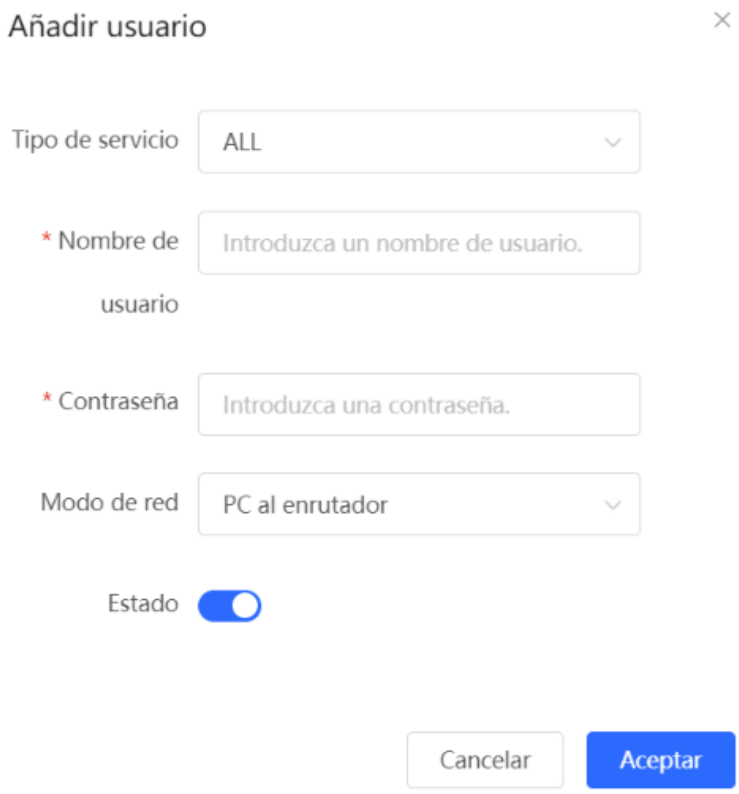


c Active el PPTP; en **Tipo de PPTP**, seleccione **Servidor** y configure el PPTP; finalmente, haga clic en **Guardar**.



d Seleccione **VPN > Clientes VPN** para configurar la VPN de los clientes.





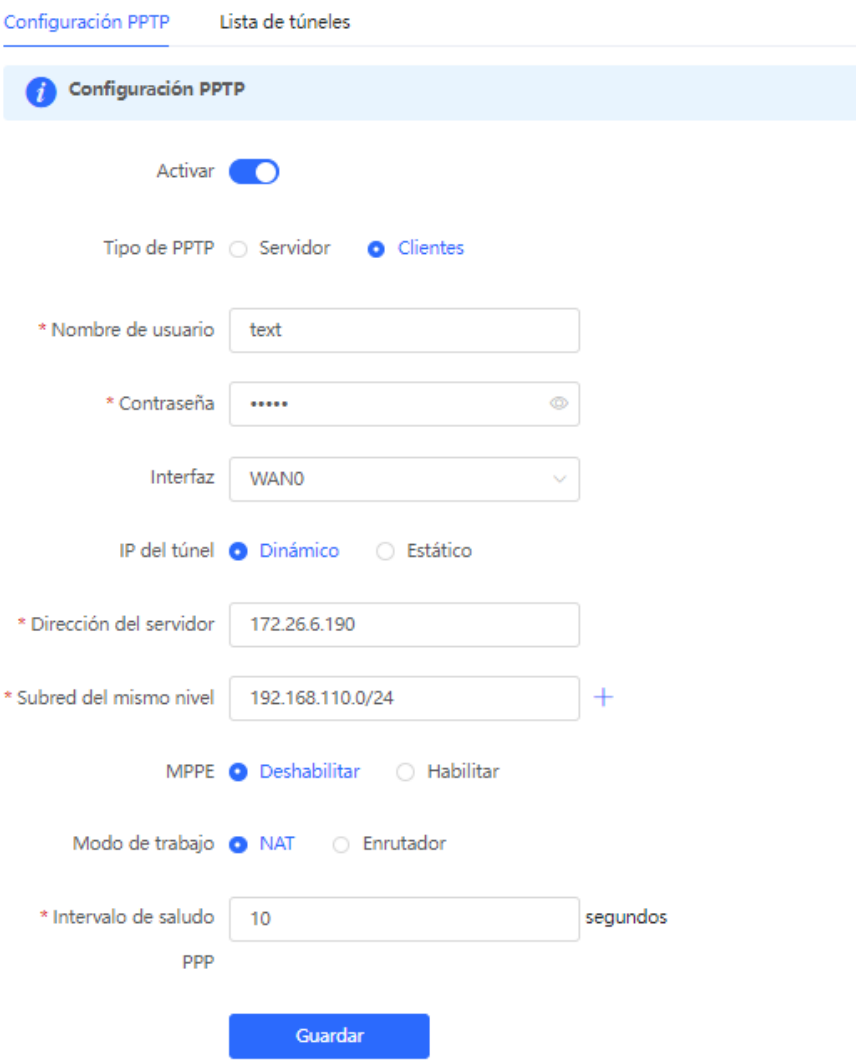
Precaución

El valor de **Subred del mismo nivel** es el rango de dirección IP local de su sucursal.

(2) Lado de la sucursal:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

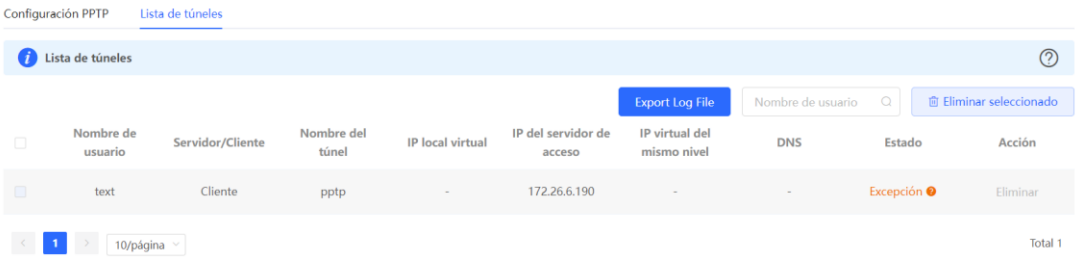
b Cambie al modo **Dispositivo local**. Seleccione **VPN > PPTP**, active **PPTP**, y en **Tipo de PPTP**, seleccione **Clientes**.



Precaución

- **Tipo de PPTP**: seleccione Clientes.
- **Nombre de usuario** y **Contraseña**: complete con los mismos datos que agregó en la sede.
- **IP del túnel**: seleccione la dirección en el rango de dirección IP del grupo de direcciones definidas por la sede. Si selecciona **Dinámico**, la dirección IP del grupo de direcciones se asigna de manera aleatoria. Si selecciona **Estático**, cualquier dirección IP del grupo de direcciones se puede ingresar sin ningún problema.
- **Dirección del servidor**: complete con la dirección del puerto WAN de la sede. Se requiere la dirección IP de una red pública. Aquí, la dirección de una red privada se utiliza solo como referencia.
- **Subred del mismo nivel:** complete con el segmento de red interna de la sede. El valor y el segmento de red interna de la sucursal no pueden superponerse.
- **Modo de trabajo**: especifique si la sede puede tener acceso a la intranet de la sucursal. De ser así, seleccione **Enrutador**. De lo contrario, seleccione **NAT**.

c Revise el estado de la conexión VPN.



4.7.2 VPN L2TP

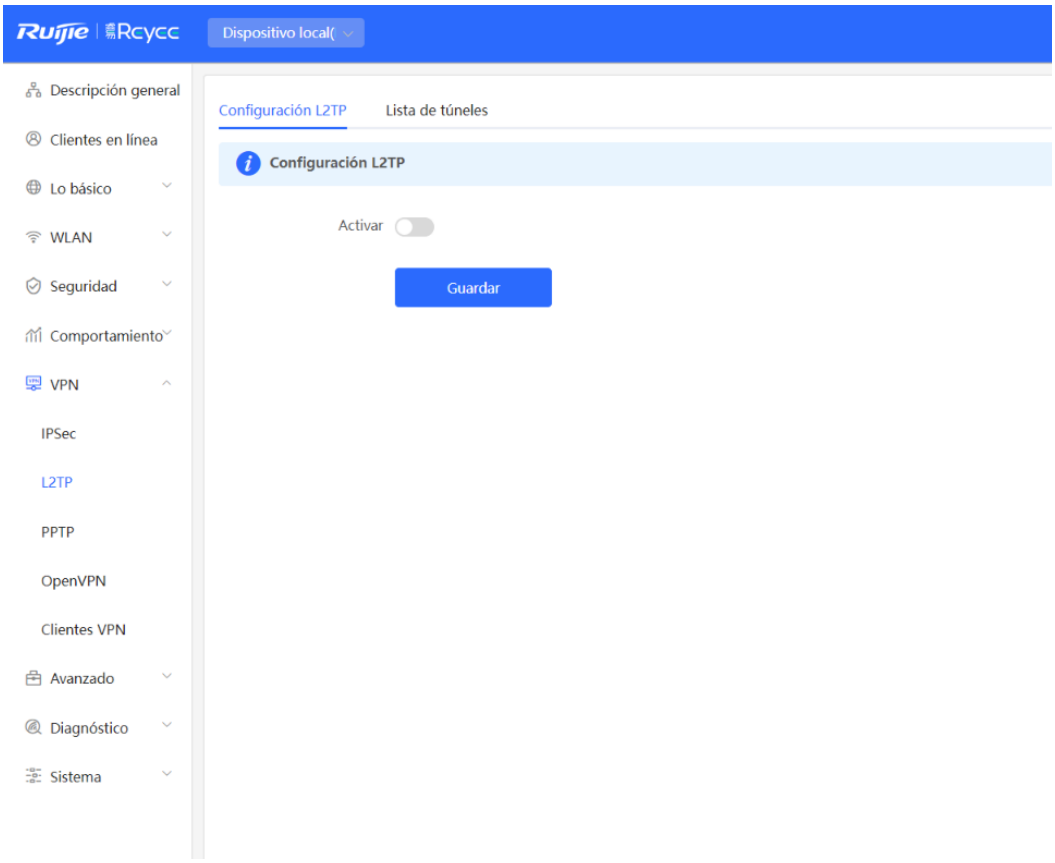
La VPN L2TP se utiliza generalmente en escenarios donde se requiere conectar un cliente con un sitio y un sitio con otro sitio. Por ejemplo, los clientes trabajan desde casa y requieren acceder a los servidores de la empresa mediante túneles de VPN L2TP; una empresa cuenta con tres sucursales que están distribuidas en tres lugares diferentes de la Internet y cada una de ellas necesita establecer un túnel con las otras a través de un router.

1. Configuración para un escenario de cliente a sitio

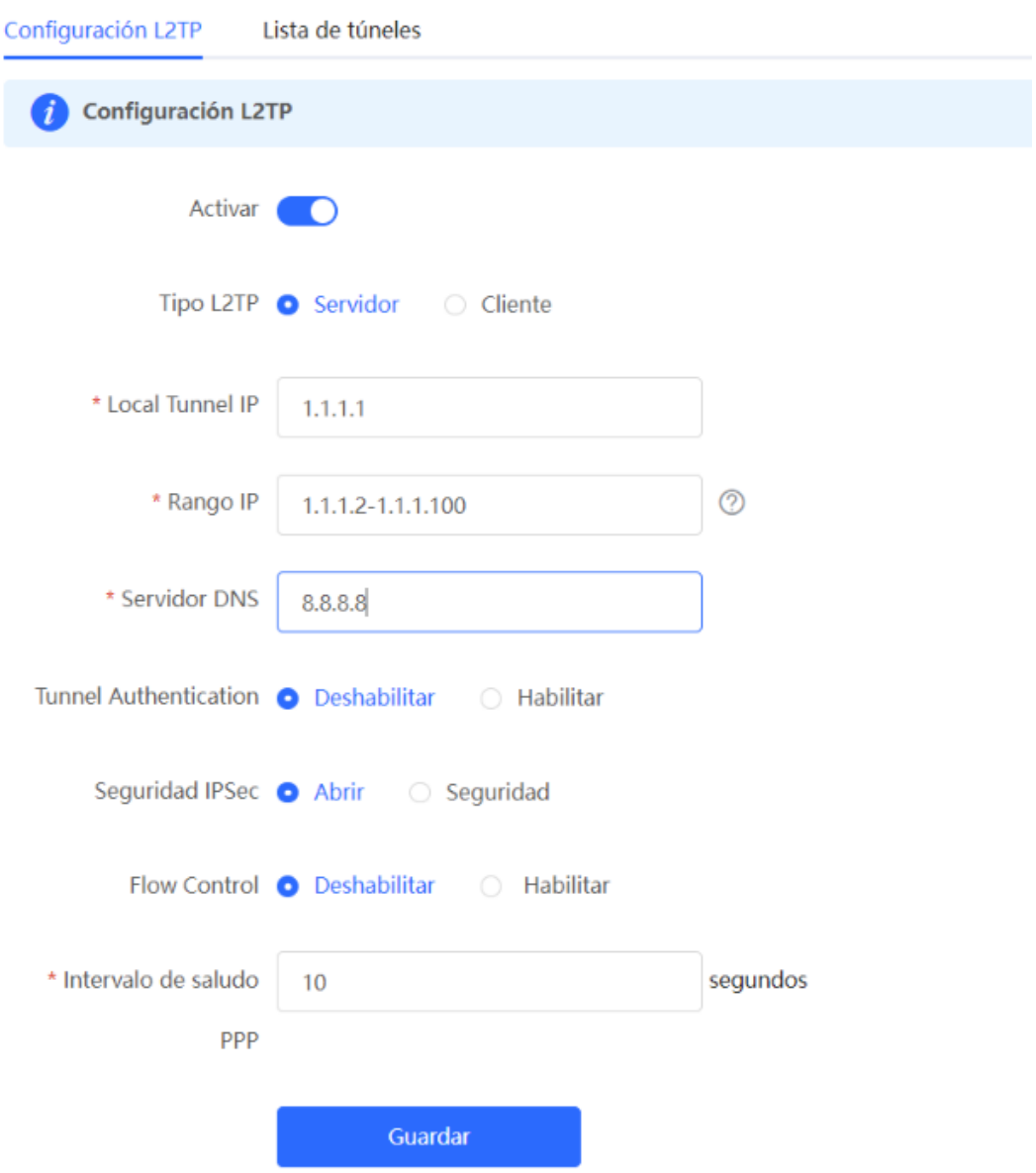
(1) Lado de la sede:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

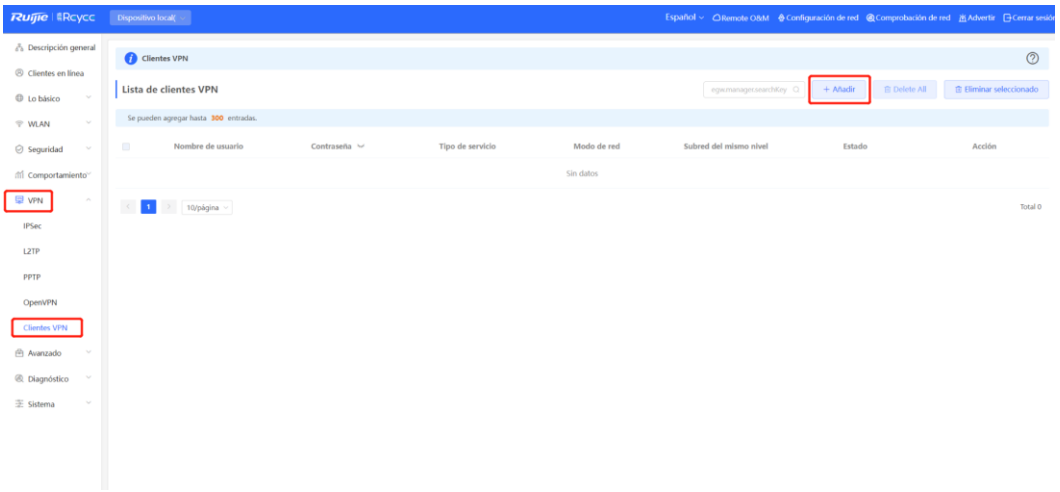
b Cambie al modo **Dispositivo local**. Seleccione **VPN** > **L2TP**.

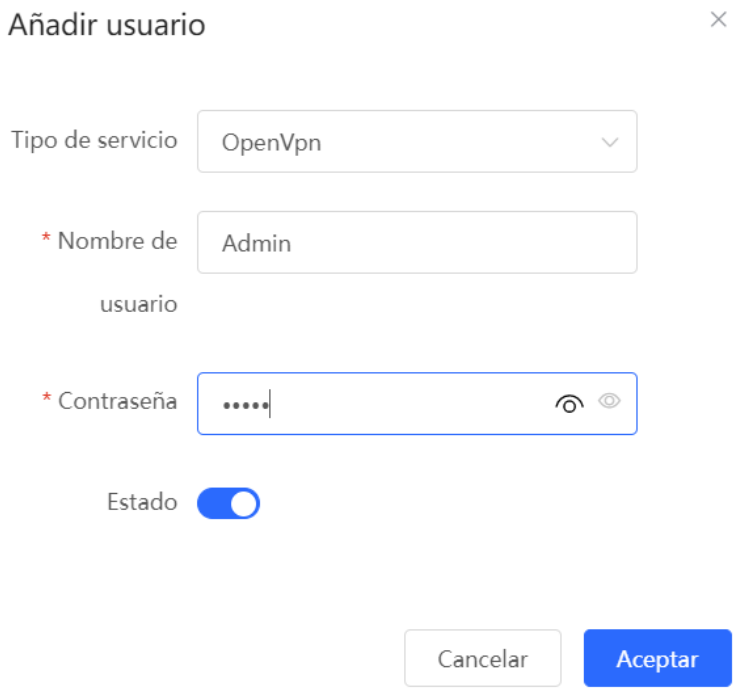


c Active L2TP, lleve a cabo su configuración y haga clic en **Guardar**.



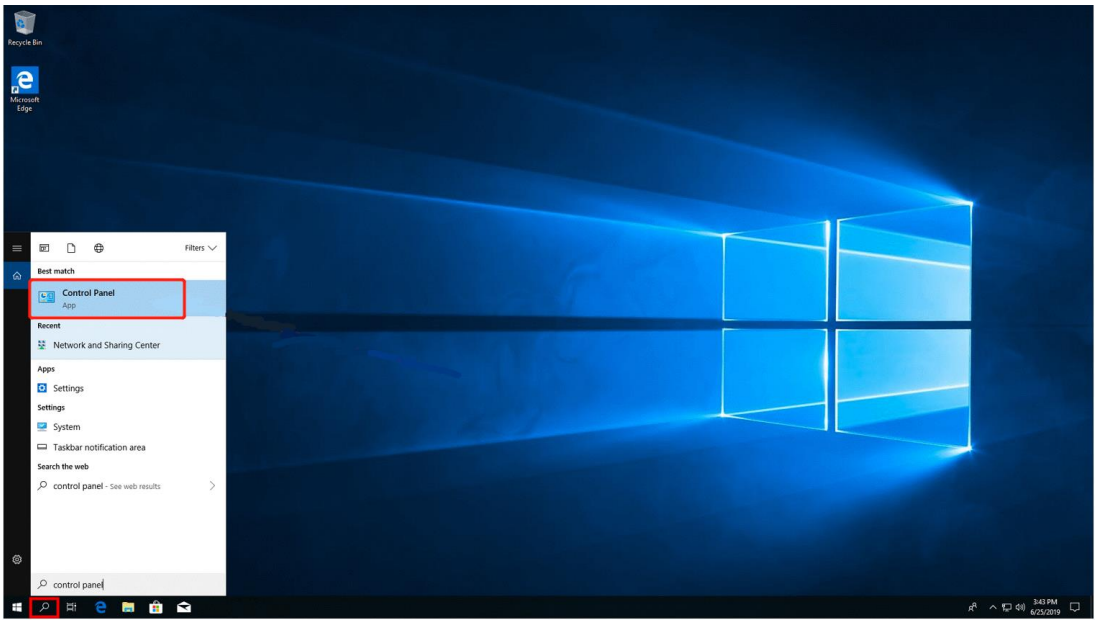
d Seleccione **Dispositivo local > VPN > Clientes VPN** para configurar los clientes VPN.

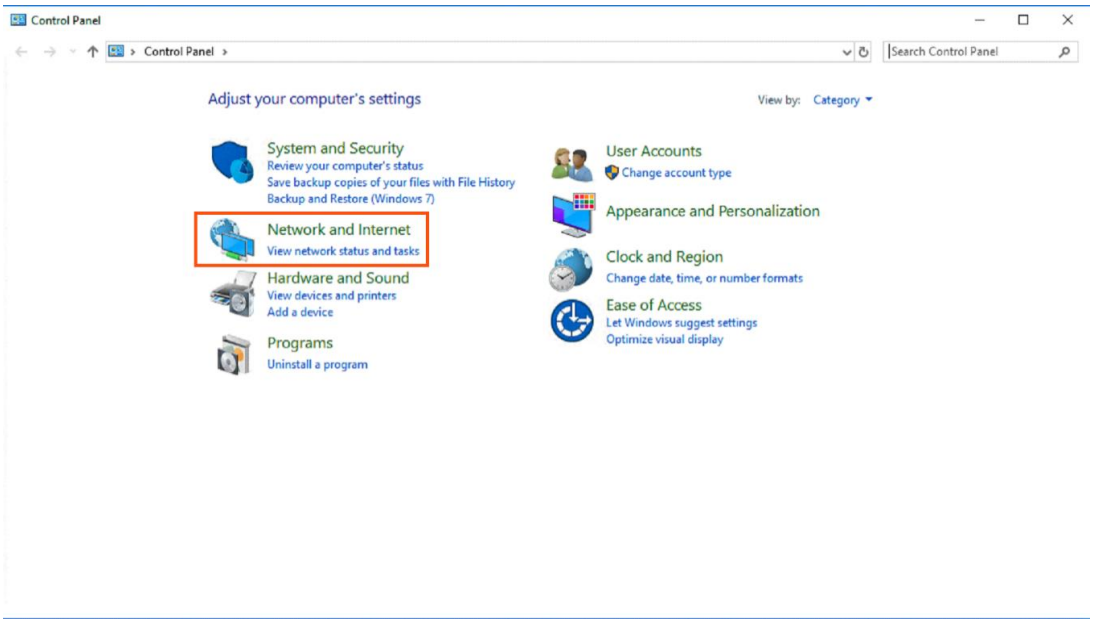


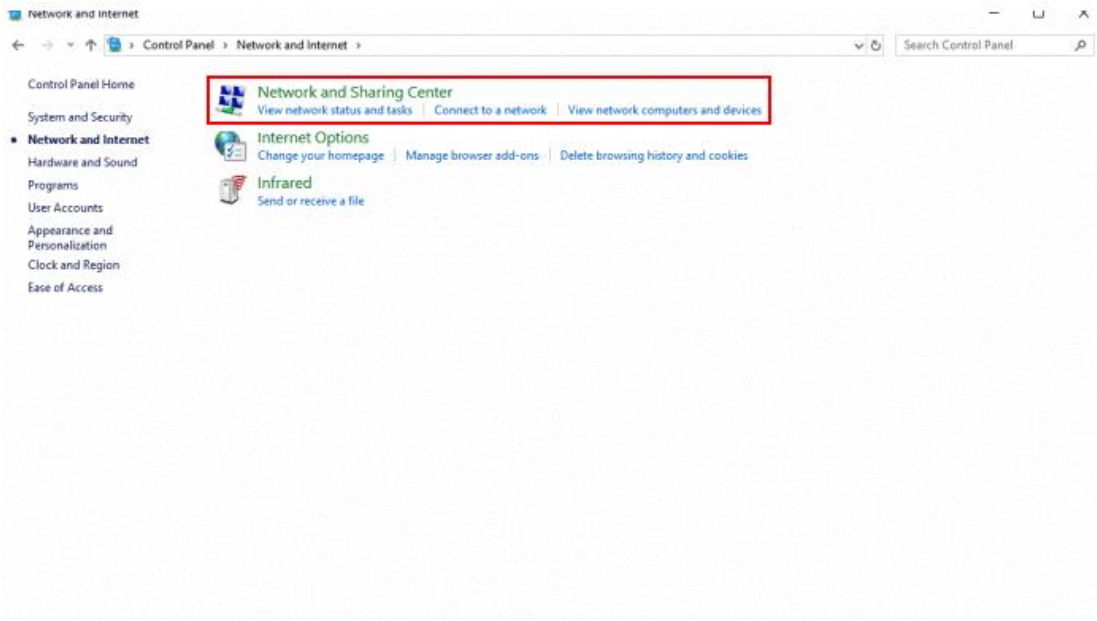


(2) Lado del cliente (se utiliza Windows 10 como ejemplo):

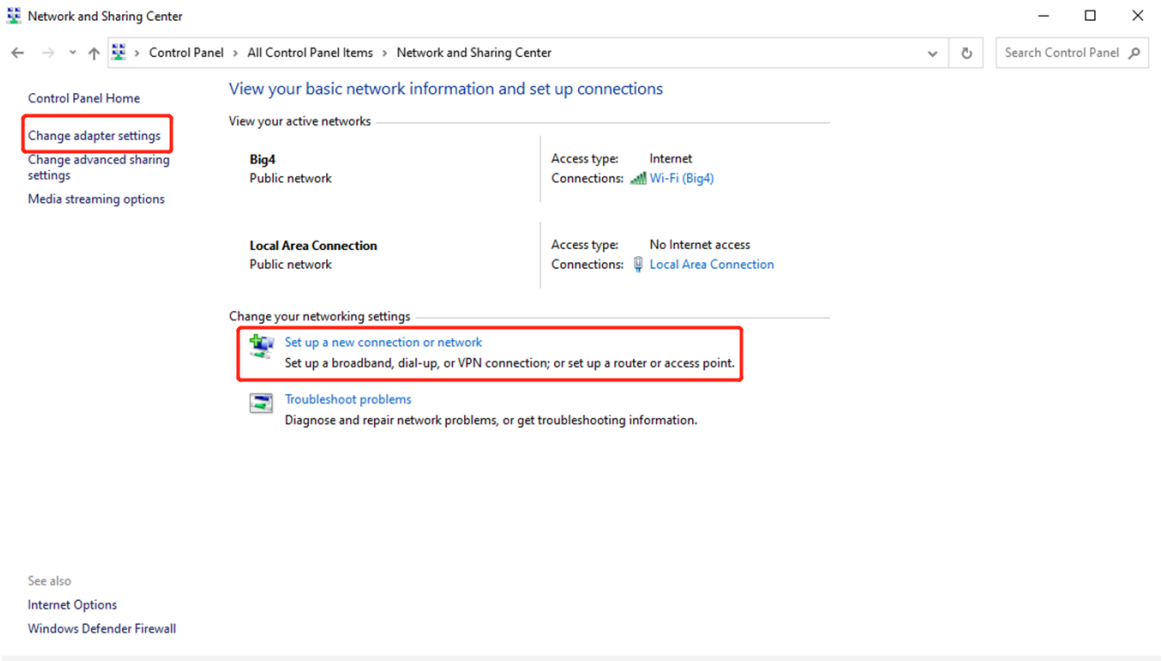
a Seleccione **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

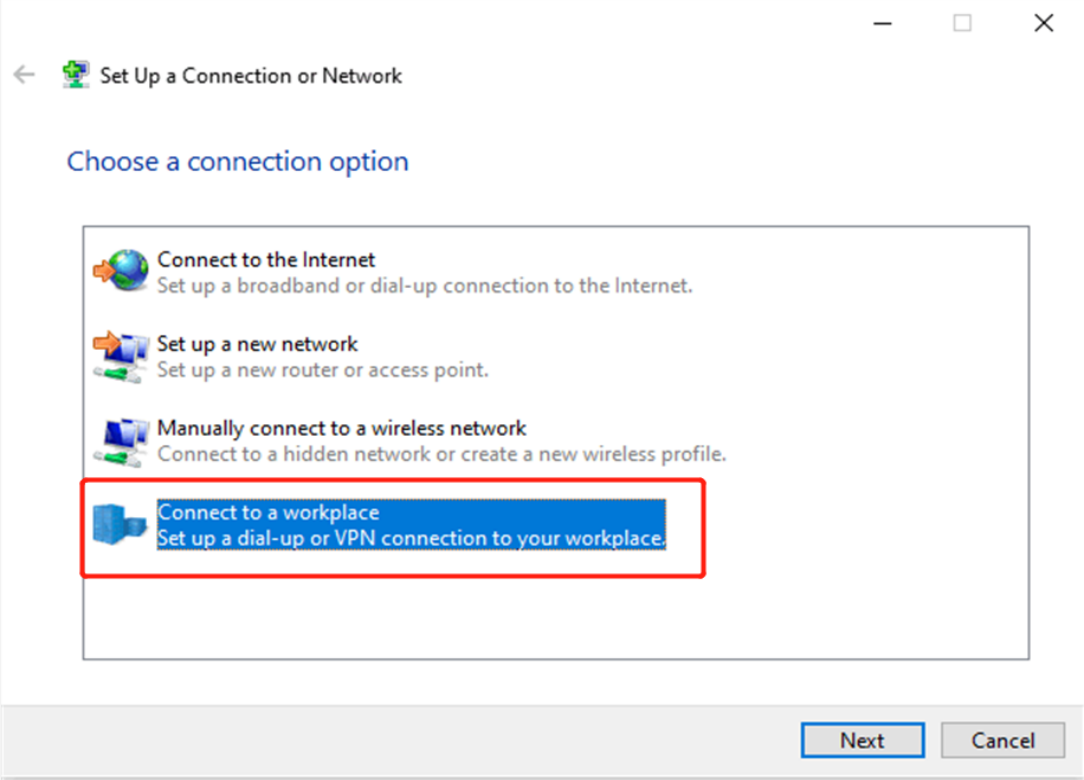

Recycle Bin
Microsoft Edge
Filters
Best match
Control Panel
App
Recent
Network and Sharing Center
Apps
Settings
Settings
System
Taskbar notification area
Search the web
control panel - See web results
control panel

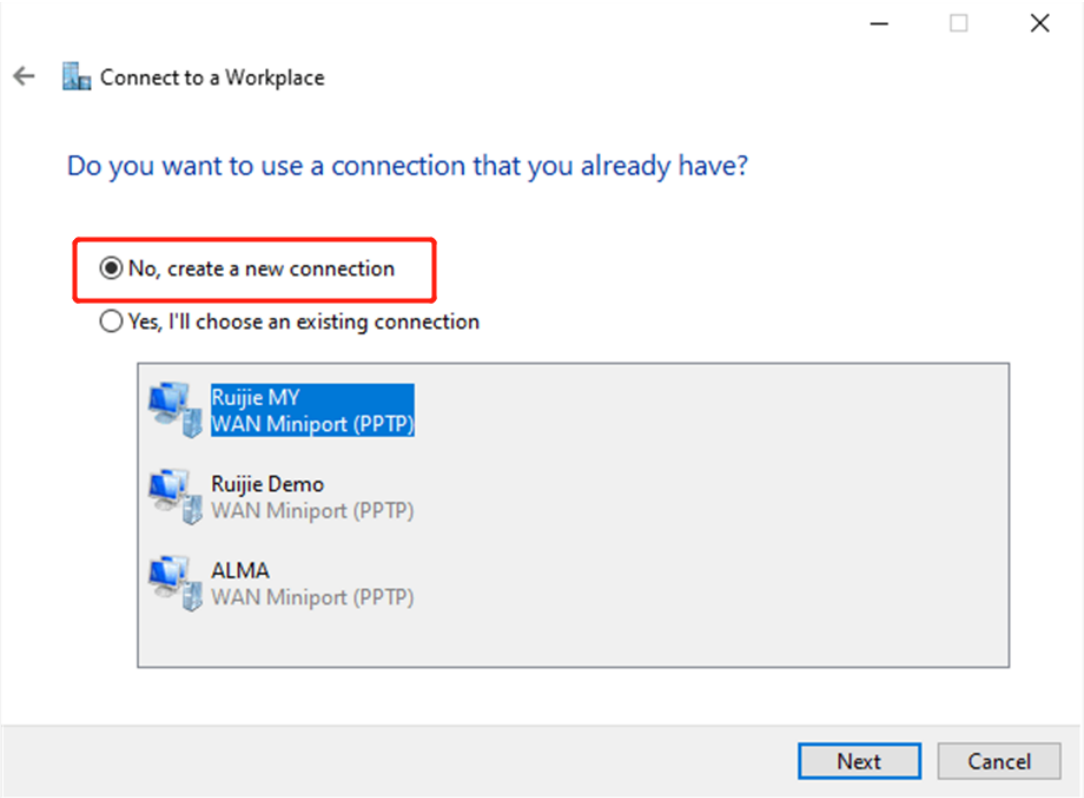

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

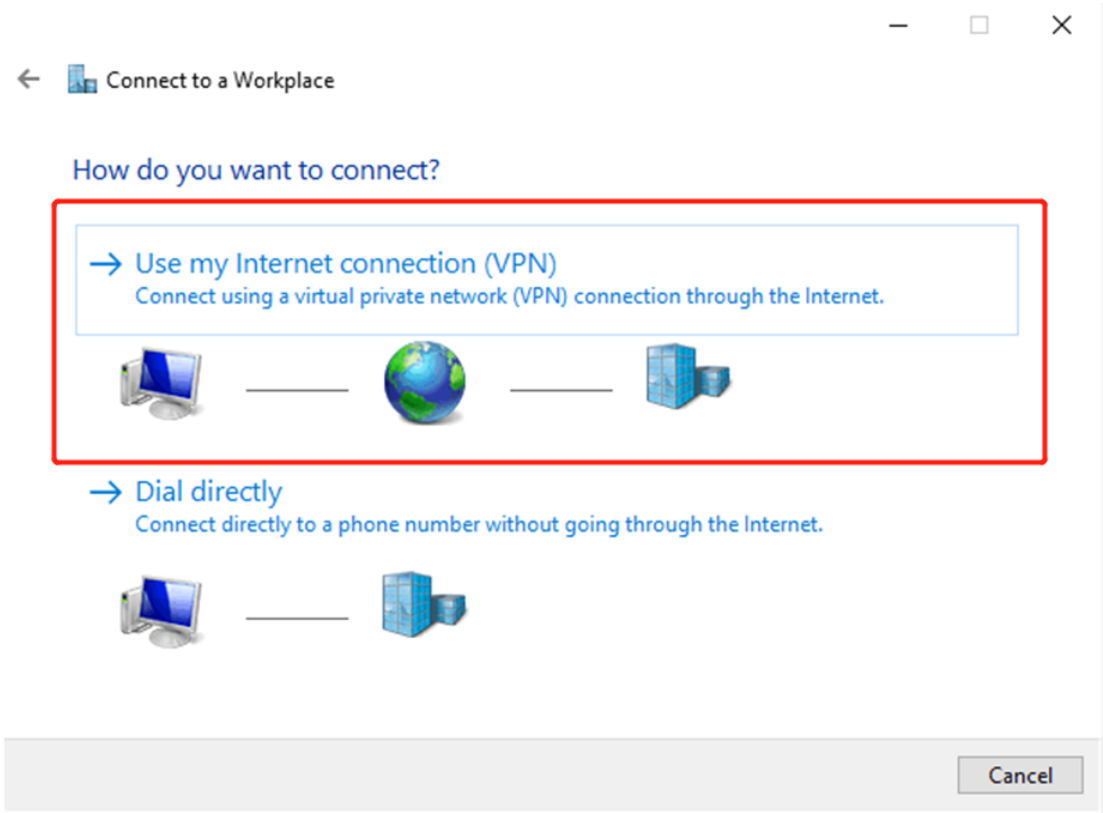


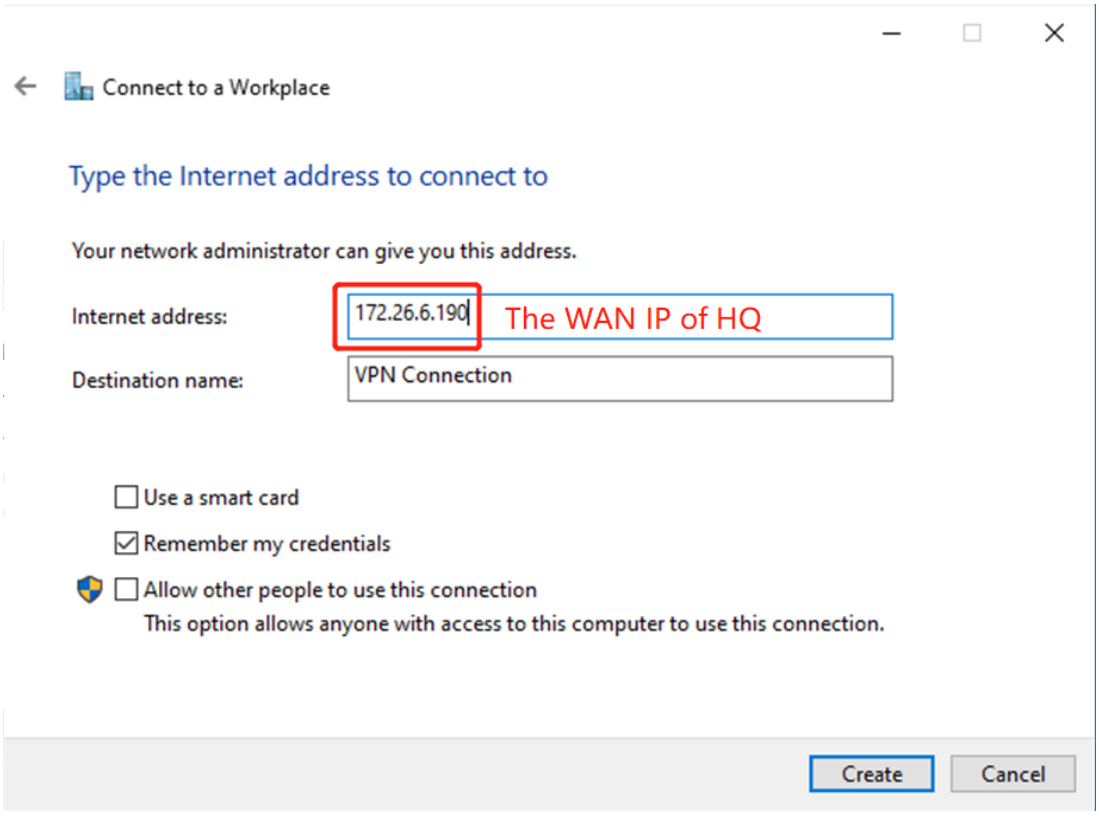
b Configure una conexión VPN.



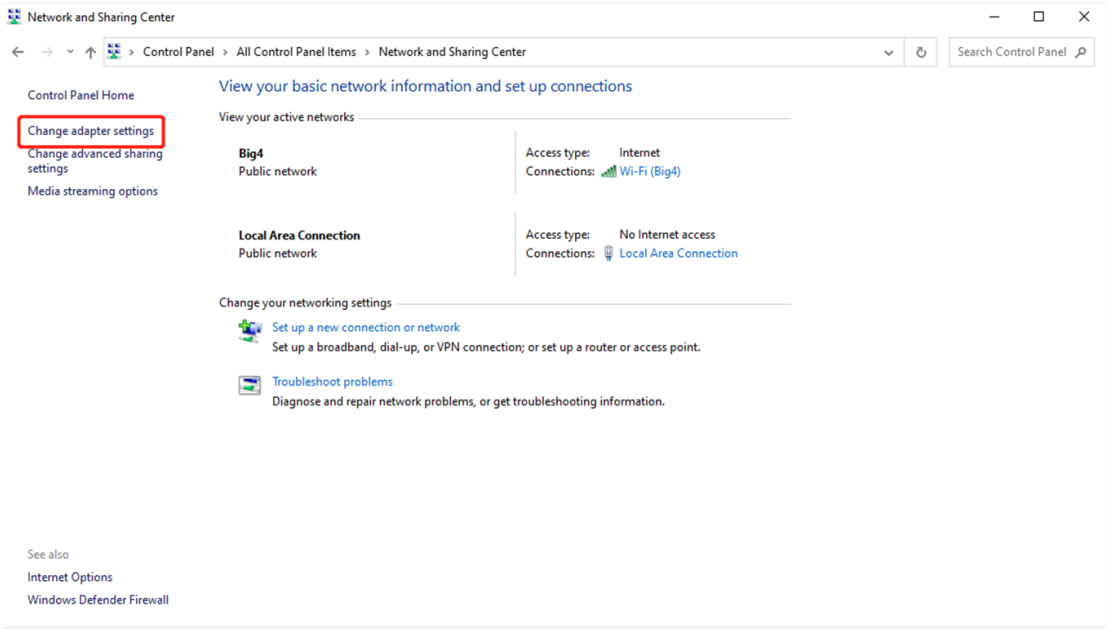

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel

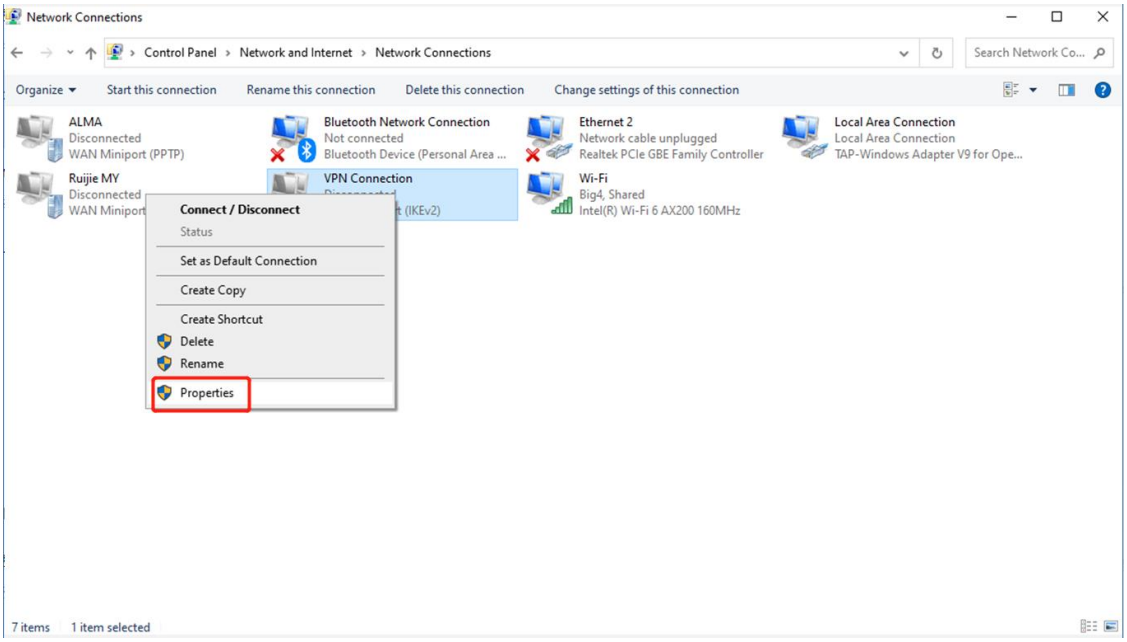

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

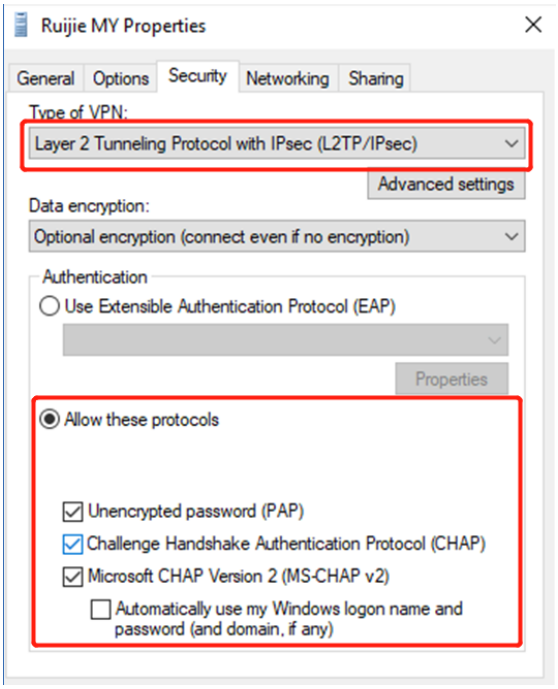

Connect to a Workplace
How do you want to connect?
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
Cancel


Connect to a Workplace
Type the Internet address to connect to
Your network administrator can give you this address.
Internet address:
172.26.6.190
The WAN IP of HQ
Destination name:
VPN Connection
Use a smart card
Remember my credentials
Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.
Create
Cancel

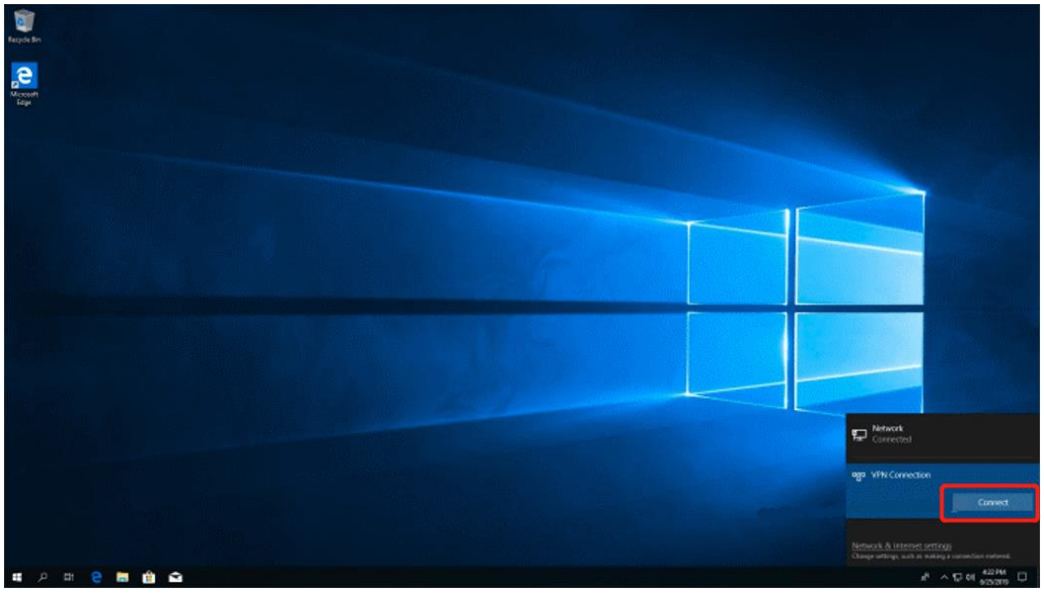
c Cambie la configuración del adaptador.

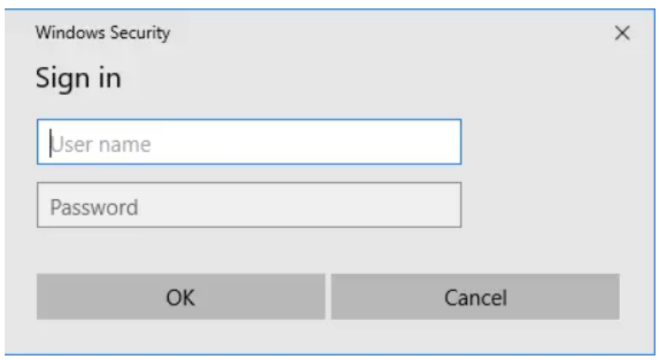


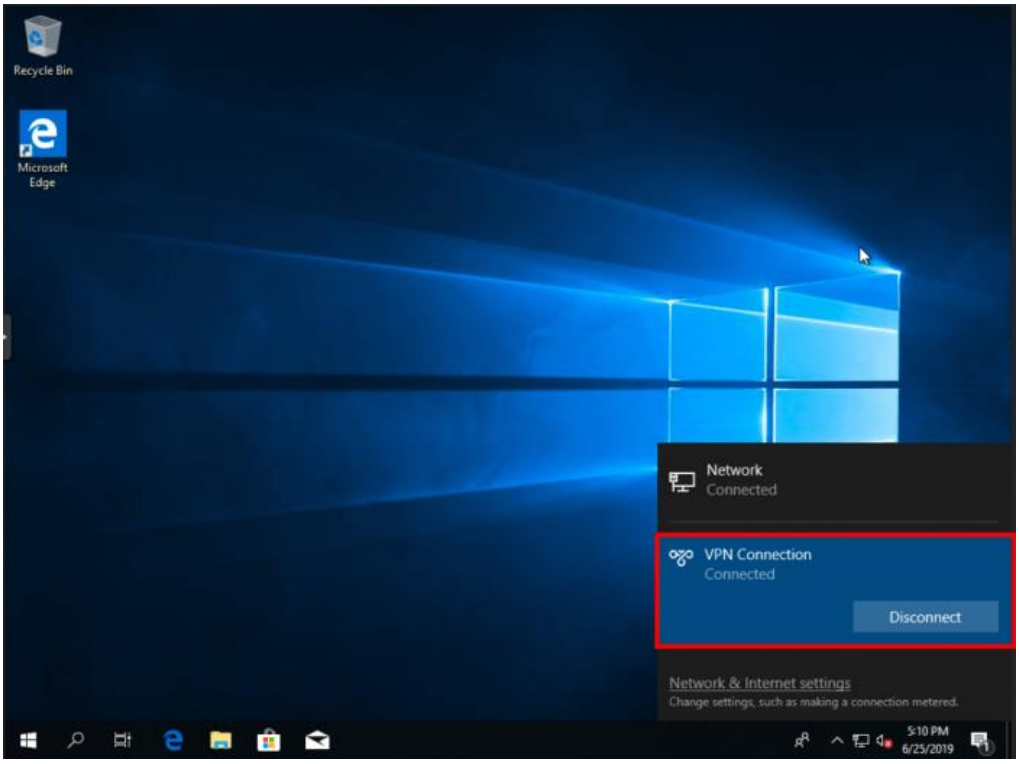




d Revise el estado de la conexión de la VPN.







e Si su PC no cuenta con acceso a los dispositivos internos (192.168.10.0/24) de la sede después de configurar la conexión VPN, añada la siguiente ruta estática en su PC. La dirección IP 192.168.100.2 es la que la PC obtiene de la sede. De este modo, la PC tendrá acceso a los dispositivos internos de la sede.

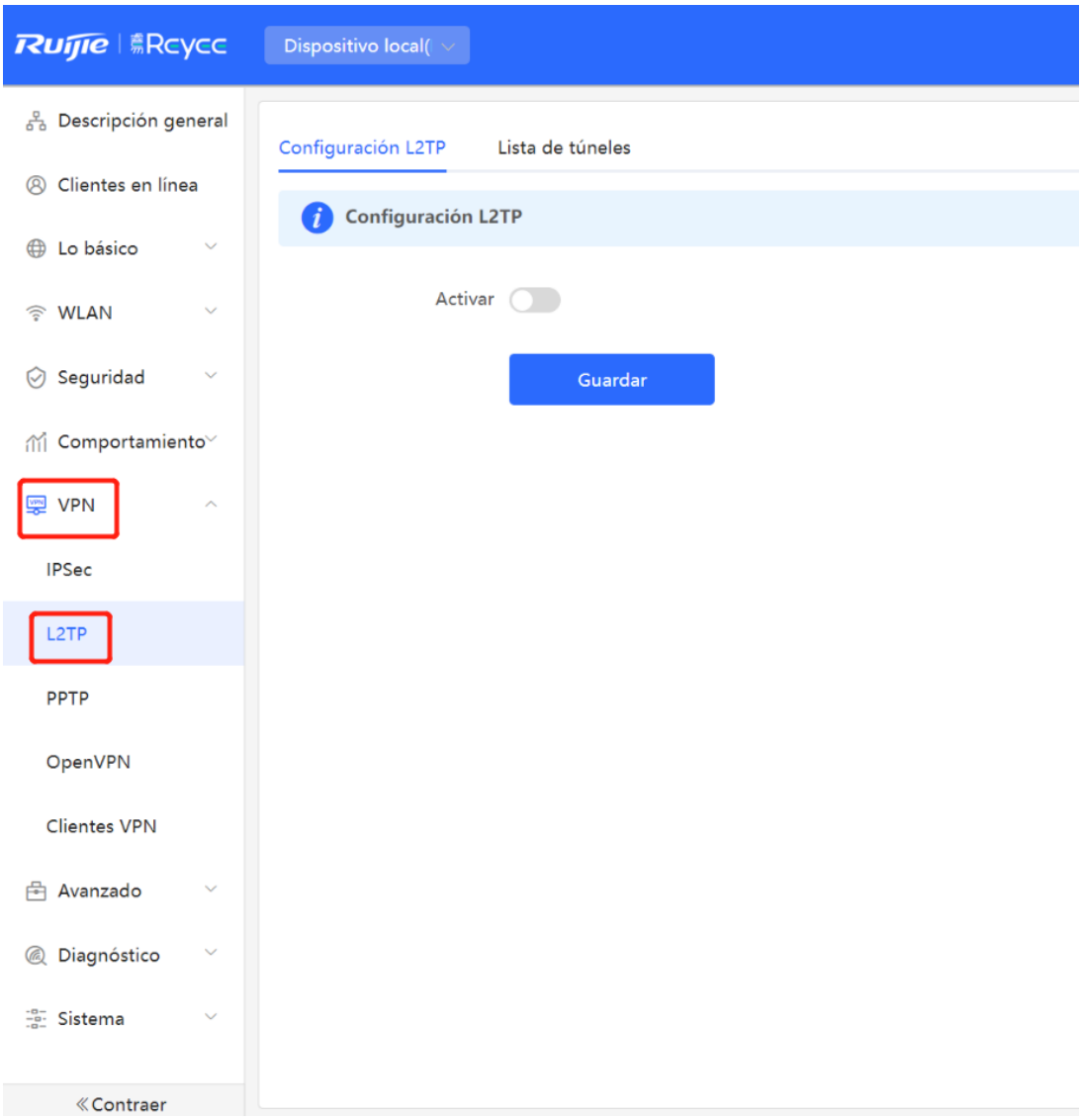
```
C:\Users\Daisy>route add 192.168.168.10.0 mask 255.255.255.0 192.168.100.2
```

2. Configuración para un escenario de sitio a sitio

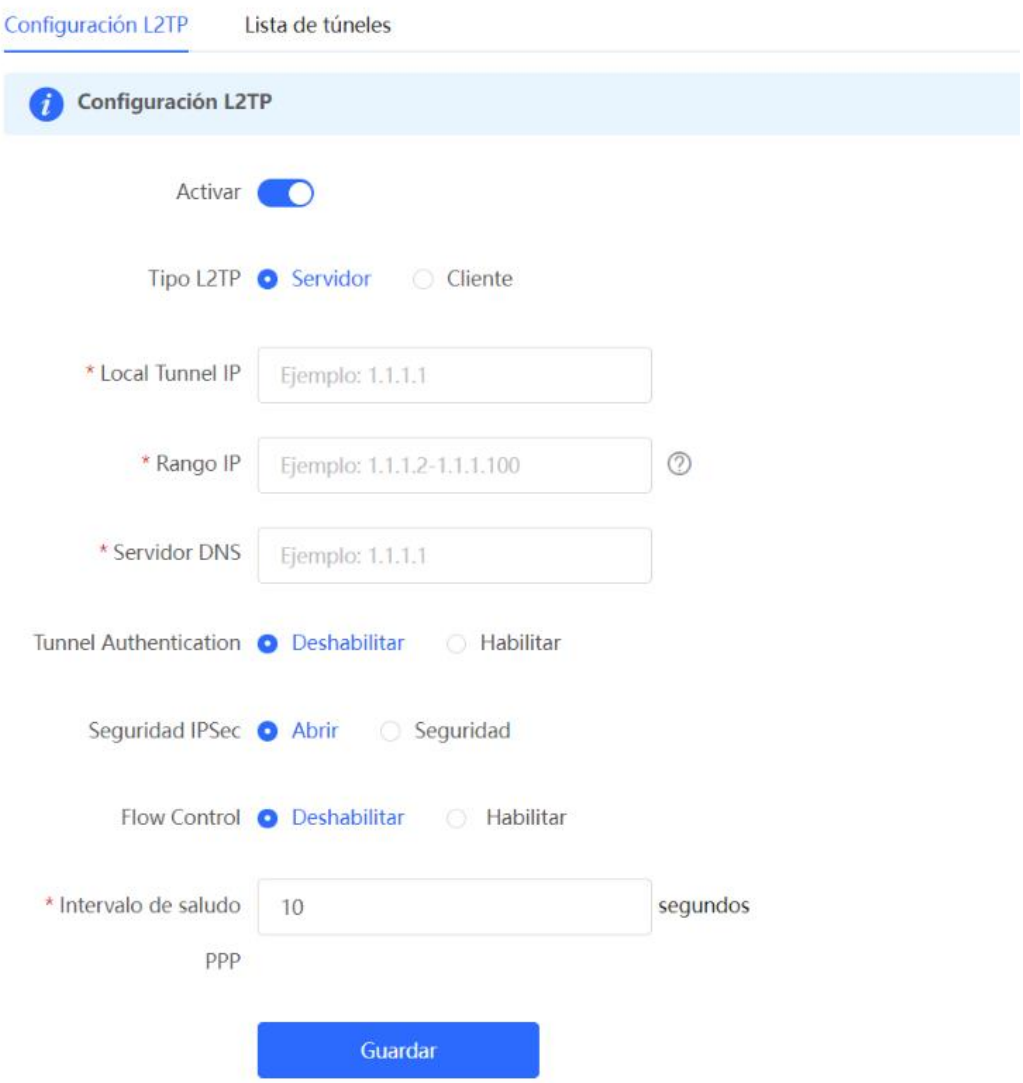
(1) Lado de la sede:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

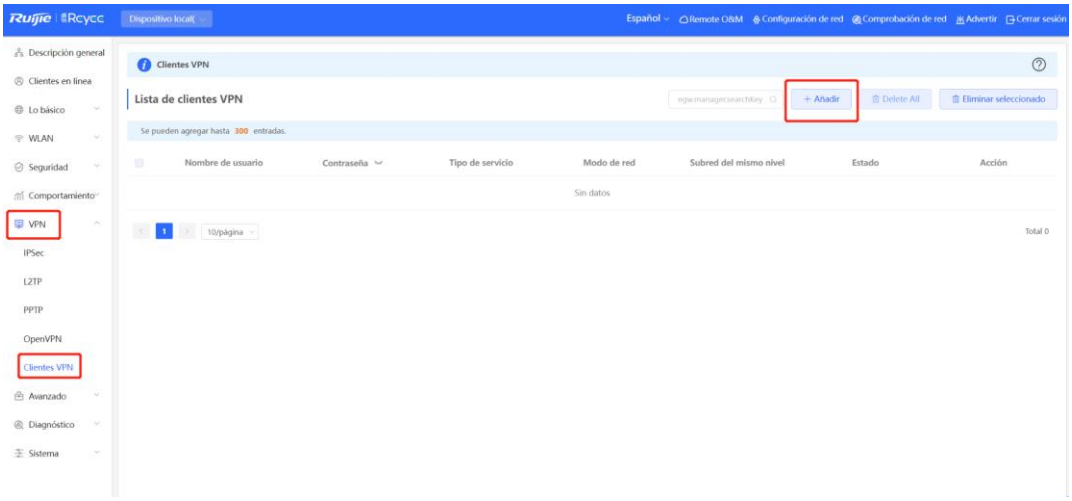
b Cambie al modo **Dispositivo local**. Seleccione **VPN** > **L2TP**.

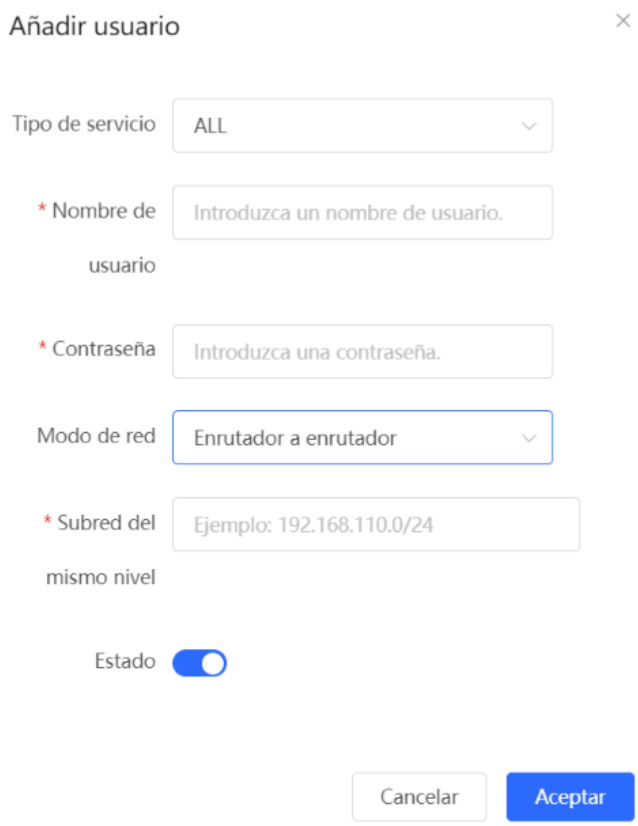


c Active L2TP, en **Tipo de L2TP** seleccione la opción **Servidor**, configure la L2TP, y haga clic en **Guardar**.



d Seleccione **VPN > Clientes VPN** y configure los clientes VPN.





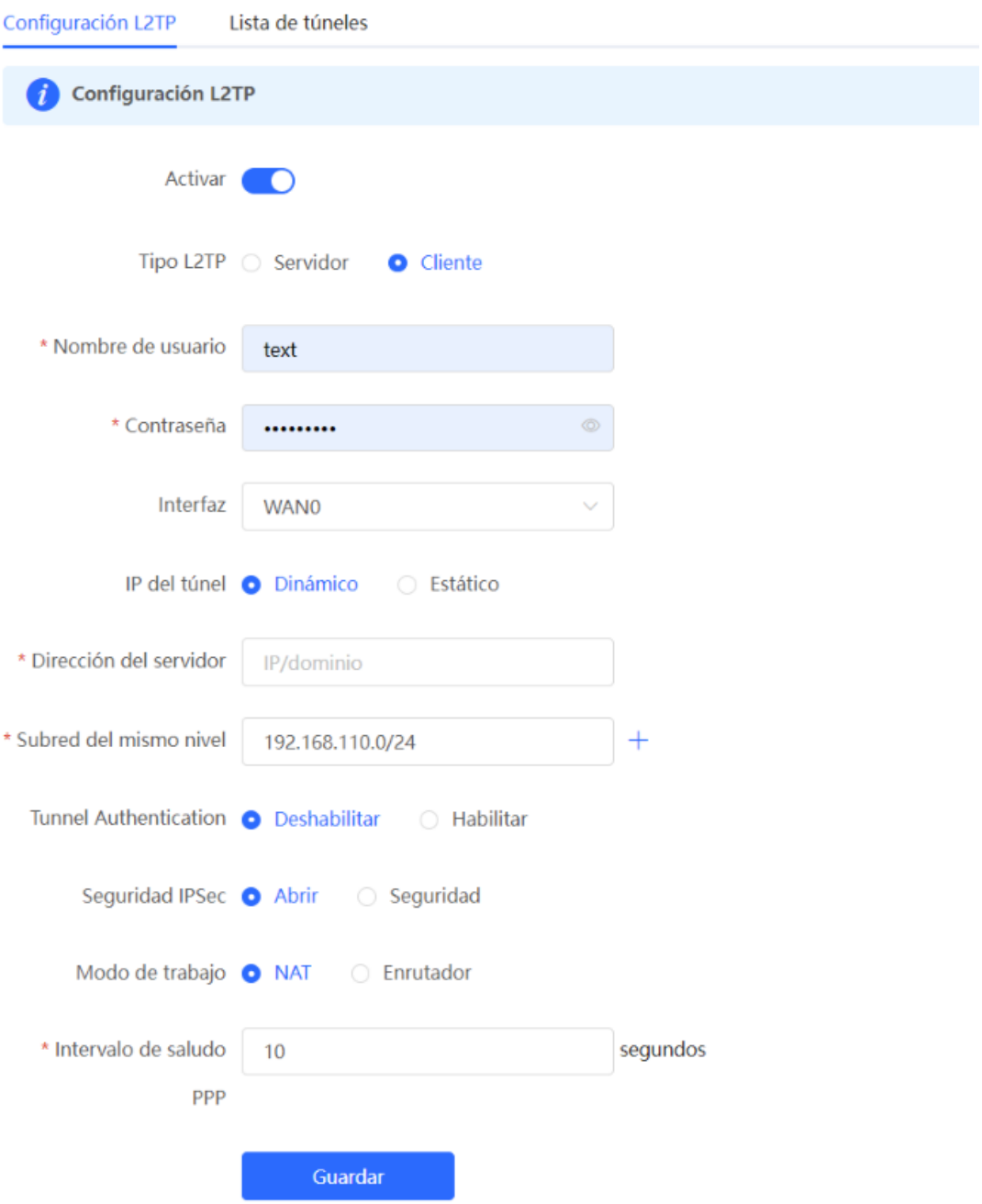
Precaución

El valor de **Subred del mismo nivel** es el rango de dirección IP local de su sucursal.

(2) Lado de la sucursal:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

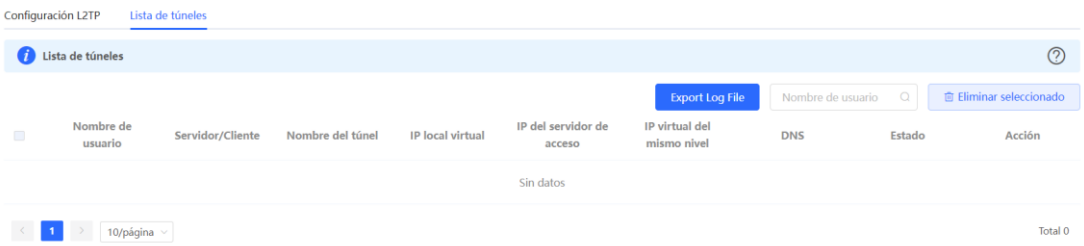
b Cambie al modo **Dispositivo local**. Seleccione **VPN > L2TP**, active **L2TP**, y establezca **Tipo L2TP** como **Cliente**.



Precaución

- **NAT**: NAT se usa en los paquetes L2TP entrantes (la dirección IP de la fuente se reemplaza con el IP local virtual).
- **Enrutador**: solamente se enrutan los paquetes L2TP entrantes.

c Revise el estado de la conexión de la VPN.



4.7.3 VPN IPsec

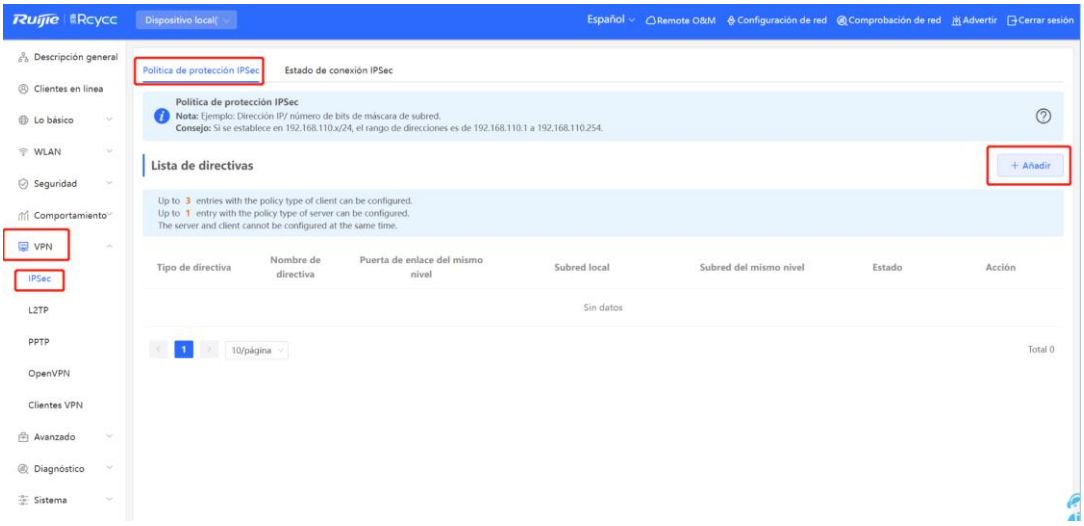
La VPN IPsec se utiliza para escenarios de un sitio a otro. Por ejemplo, tres sucursales de una empresa están distribuidas en tres lugares diferentes de Internet; cada sucursal utiliza un router para establecer túneles entre ellas; los datos que viajan entre las Intranets (varias PC) de la empresa están conectados de forma segura por medio de los túneles de la VPN IPsec establecidos en estos routers.

La VPN IPsec solo se utiliza para escenarios de un sitio a otro.

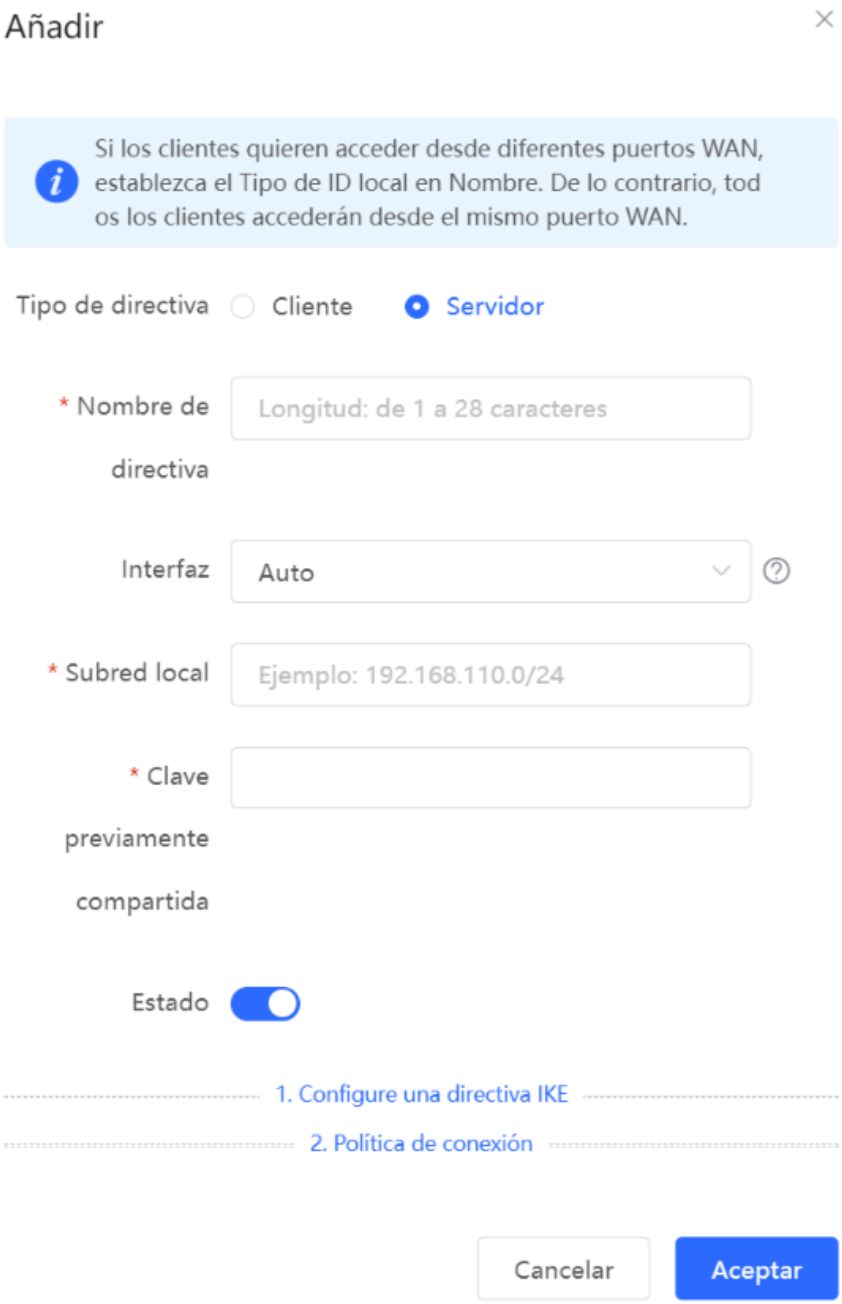
(1) Lado de la sede:

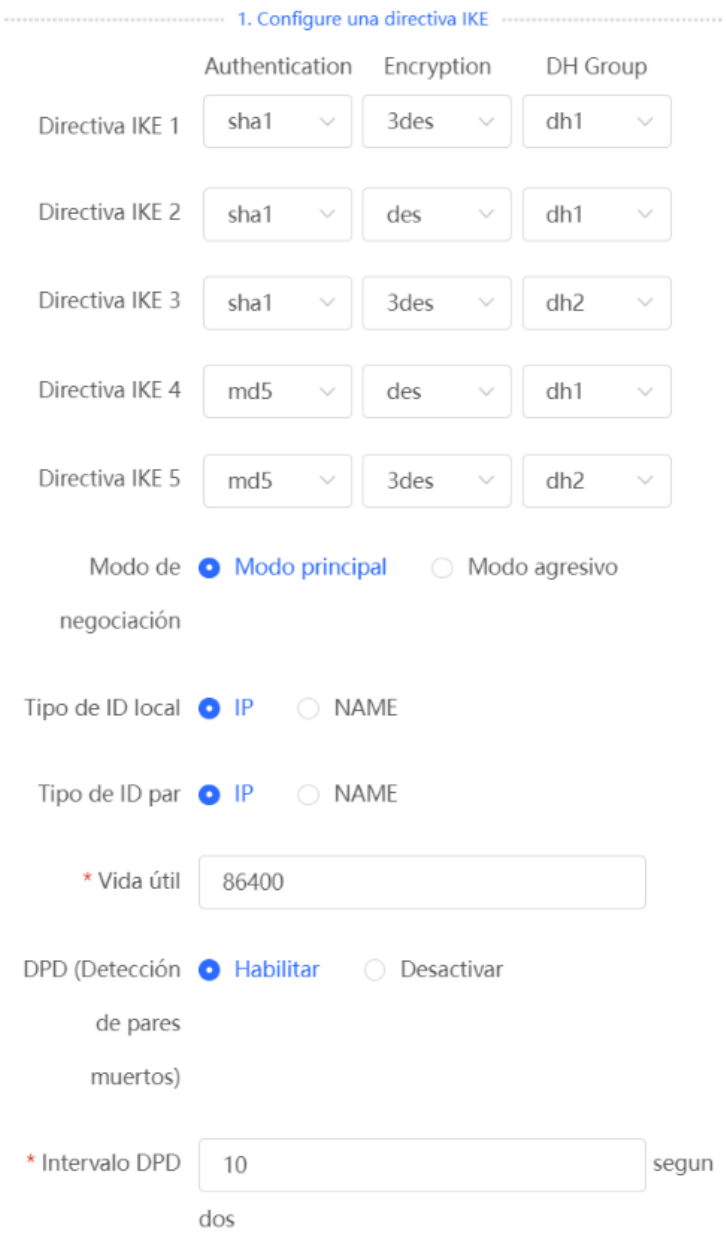
a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

b Cambie al modo **Dispositivo local**. Seleccione **VPN** > **IPSec** > **Política de protección IPSec**.



c Configure una directiva de seguridad VPN IPsec.

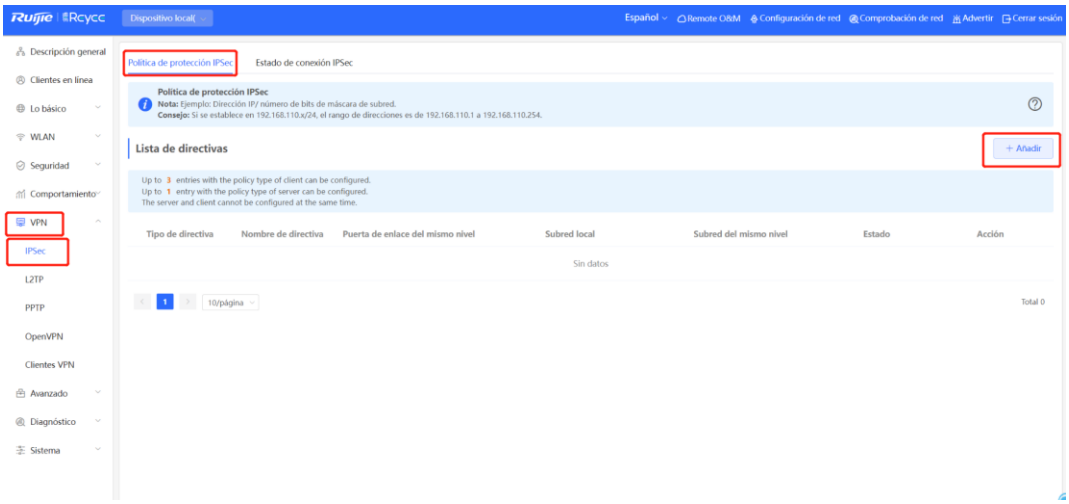

Añadir
Si los clientes quieren acceder desde diferentes puertos WAN, establezca el Tipo de ID local en Nombre. De lo contrario, tod os los clientes accederán desde el mismo puerto WAN.
Tipo de directiva
Cliente
Servidor
* Nombre de directiva
Longitud: de 1 a 28 caracteres
Interfaz
Auto
* Subred local
Ejemplo: 192.168.110.0/24
* Clave previamente compartida
Estado
1. Configure una directiva IKE
2. Política de conexión
Cancelar
Aceptar


1. Configure una directiva IKE
Authentication
Encryption
DH Group
Directiva IKE 1
sha1
3des
dh1
Directiva IKE 2
sha1
des
dh1
Directiva IKE 3
sha1
3des
dh2
Directiva IKE 4
md5
des
dh1
Directiva IKE 5
md5
3des
dh2
Modo de negociación
Modo principal
Modo agresivo
Tipo de ID local
IP
NAME
Tipo de ID par
IP
NAME
* Vida útil
86400
DPD (Detección de pares muertos)
Habilitar
Desactivar
* Intervalo DPD
10
segundos

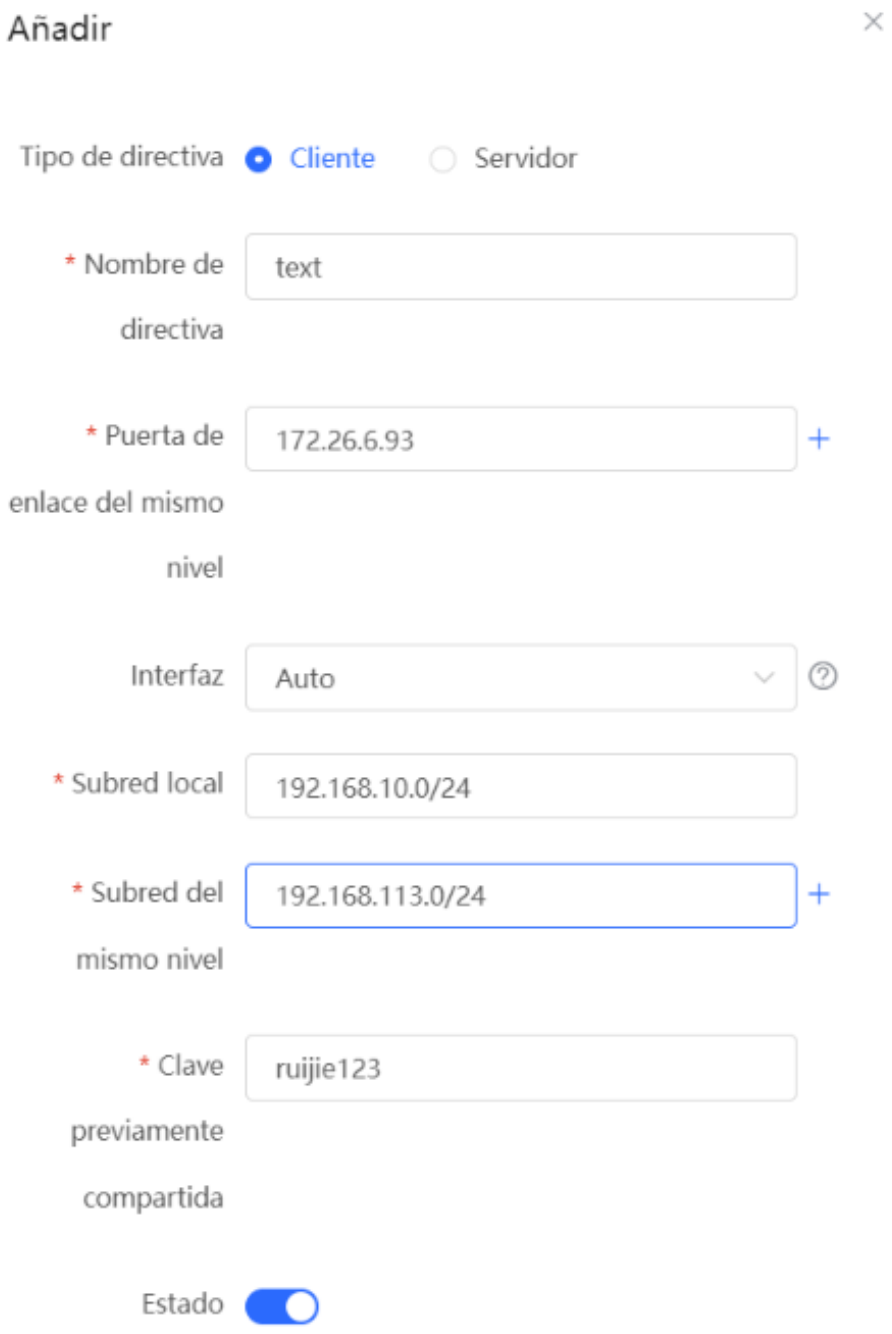
(2) Lado de la sucursal:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

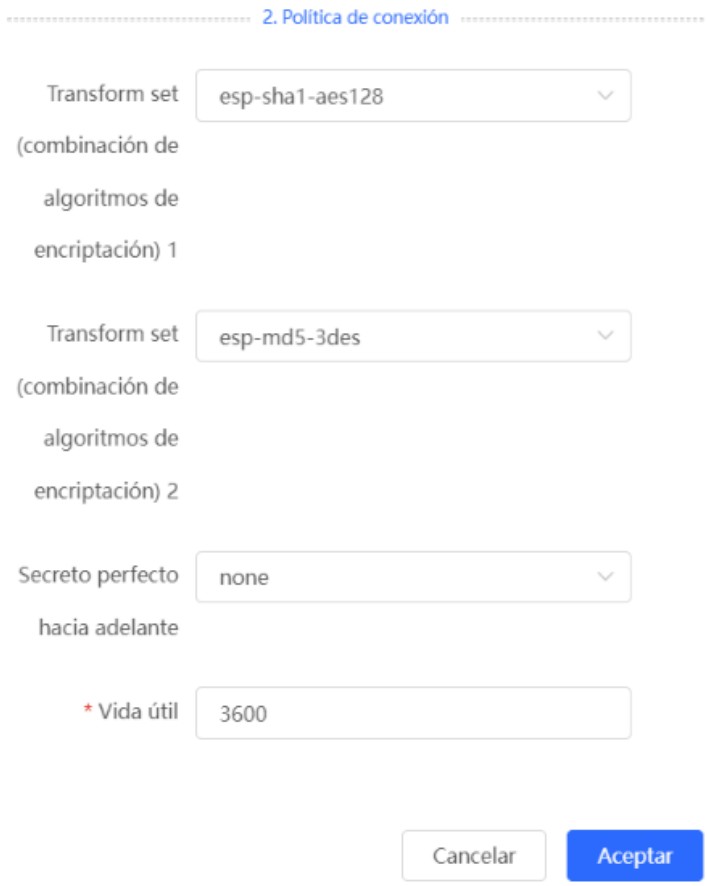
b Cambie al modo **Dispositivo local**. Seleccione **VPN** > **IPSec** > **Política de protección IPSec**.



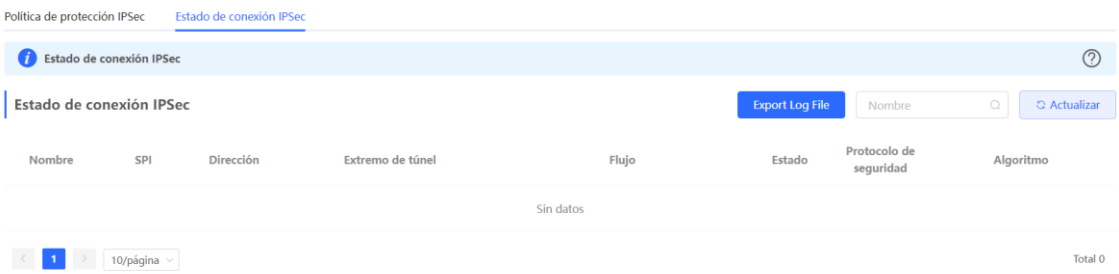
c Configure una directiva VPN IPsec. Asegúrese de que la directiva IKE y la directiva de conexión sean las mismas en ambos lados.


Añadir
Tipo de directiva
Cliente
Servidor
* Nombre de directiva
text
* Puerta de enlace del mismo nivel
172.26.6.93
Interfaz
Auto
* Subred local
192.168.10.0/24
* Subred del mismo nivel
192.168.113.0/24
* Clave previamente compartida
ruijie123
Estado


1. Configure una directiva IKE
Authentication
Encryption
DH Group
Directiva IKE 1
sha1
3des
dh1
Directiva IKE 2
sha1
des
dh1
Directiva IKE 3
sha1
3des
dh2
Directiva IKE 4
md5
des
dh1
Directiva IKE 5
md5
3des
dh2
Modo de negociación
Modo principal
Modo agresivo
Tipo de ID local
IP
NAME
Tipo de ID par
IP
NAME
* Vida útil
86400
DPD (Detección de pares muertos)
Habilitar
Desactivar
* Intervalo DPD
10
segundos



d Revise el estado de la conexión de IPsec.



Precaución

Si el EG de la sede no cuenta con una dirección IP pública configurada para otros dispositivos externos, se debe configurar un mapeo de puertos en ellos; y en **Tipo de ID local**, seleccionar **NAME** en los dispositivos de la sede y de las sucursales.

4.7.4 L2TP sobre VPN IPsec

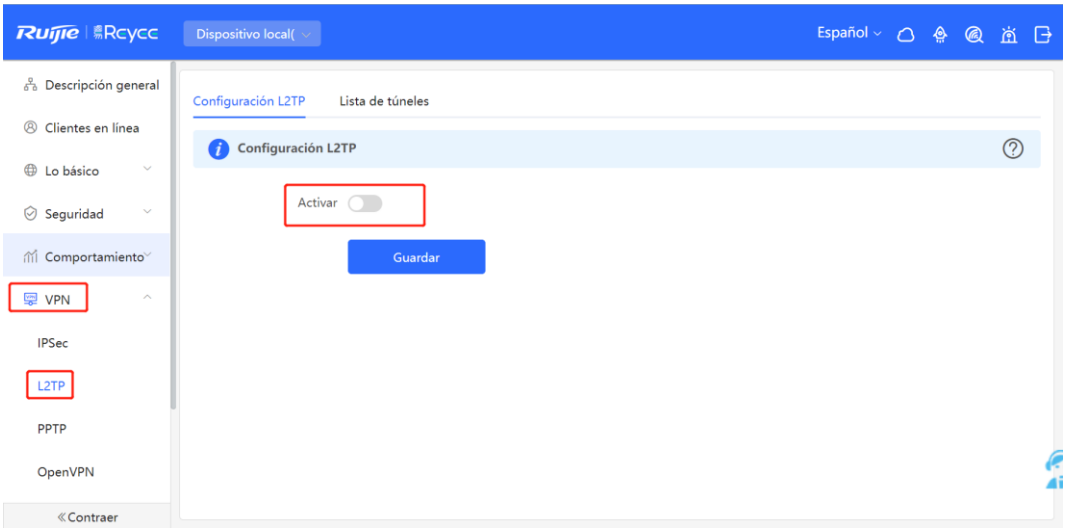
El L2TP sobre la VPN IPsec se utiliza generalmente en escenarios donde se requiere conectar un sitio con otro y un cliente con un sitio. Por ejemplo, tres sucursales de una empresa están distribuidas en tres lugares

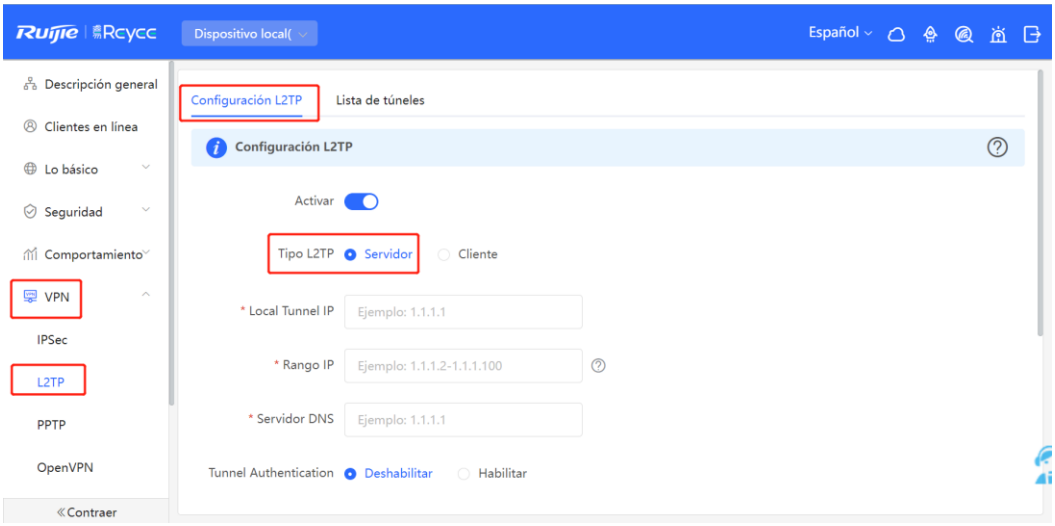
diferentes de Internet; cada sucursal utiliza un router para establecer túneles entre ellas, y los datos que viajan entre las Intranets (varias PC) de la empresa están conectados de forma segura por medio de los túneles de L2TP sobre VPN IPsec, establecidos por estos routers; el personal que trabaja desde casa cuenta con acceso a los datos de la empresa a través de los túneles de L2TP sobre VPN IPsec.

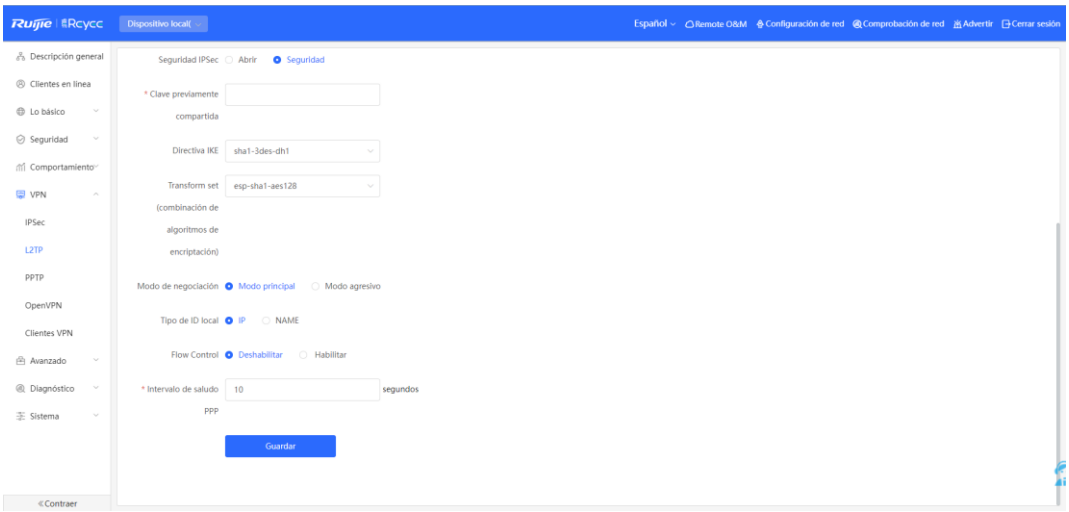
(1) Lado de la sede:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

b Cambie al modo **Dispositivo local**. Seleccione **VPN > L2TP > Configuración L2TP** y configure **Seguridad IPSec**.



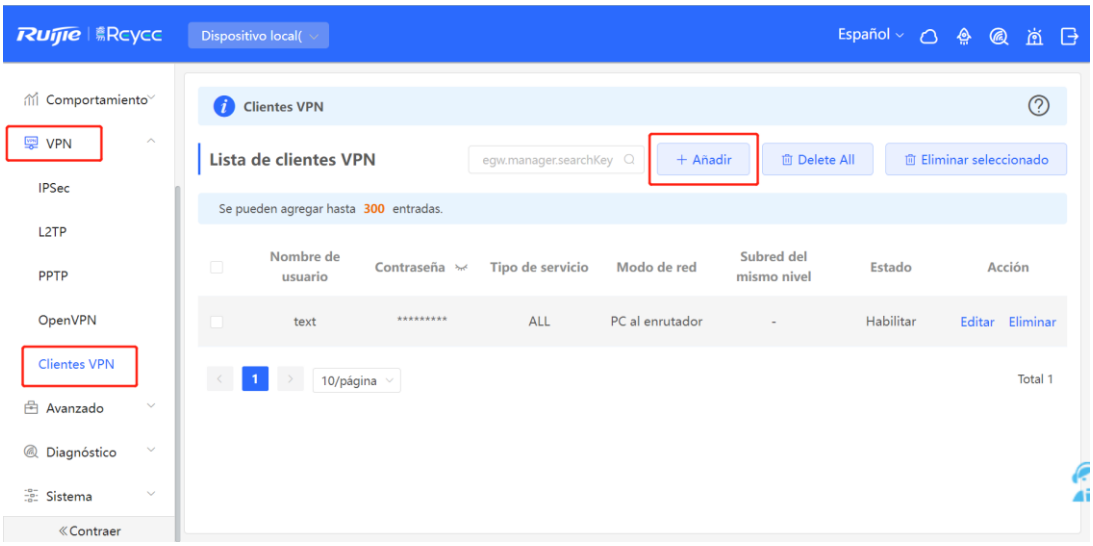


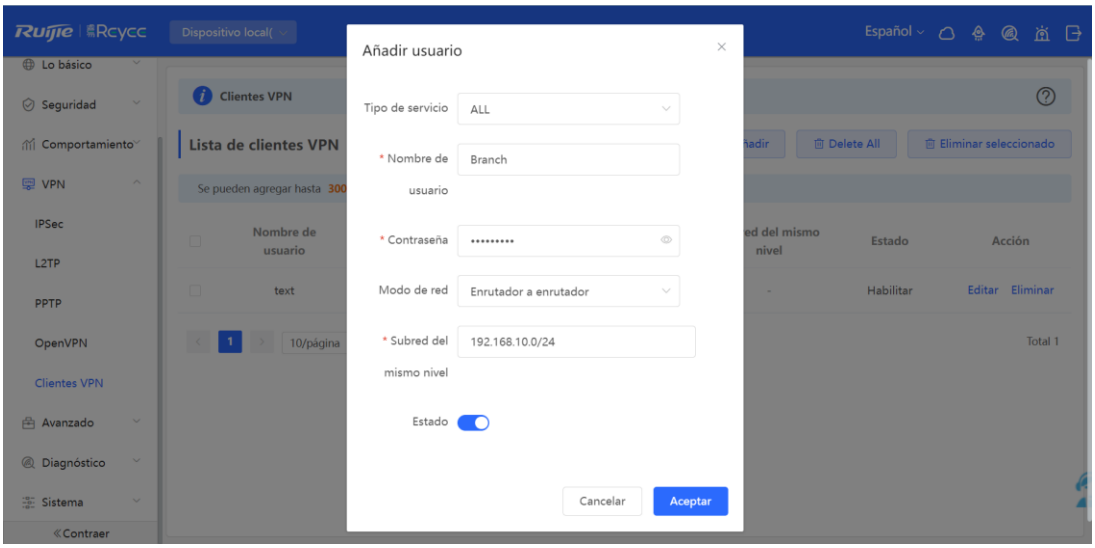


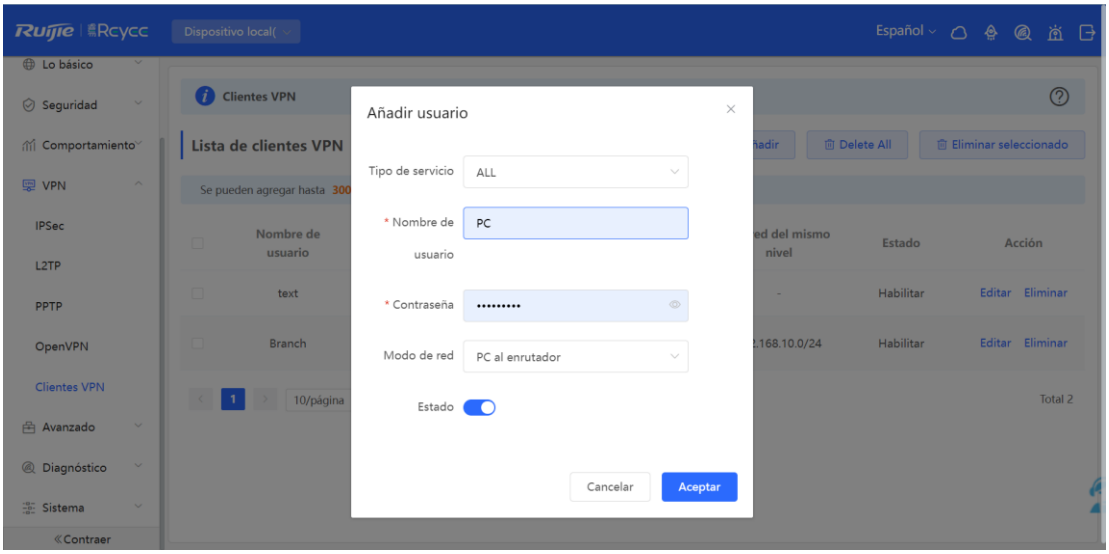
Precaución

- **Intervalo de saludo PPP**: indica el intervalo para enviar mensajes de saludo PPP sobre la conexión IPsec.
- **Seguridad IPSec**: indica si se utiliza IPsec.
- **Clave previamente compartida**: indica que se requiere la clave previamente compartida para el encriptado de IPsec.
- **Tipo de ID local**: cuando el puerto WAN de la sede esté configurado con la dirección IP pública, seleccione **IP**. Cuando el puerto WAN de la sede esté configurado con la dirección IP privada, seleccione **NAME** y configure la DMZ en el dispositivo externo.

c Configure la VPN de los clientes para el EG y la PC de la sucursal.







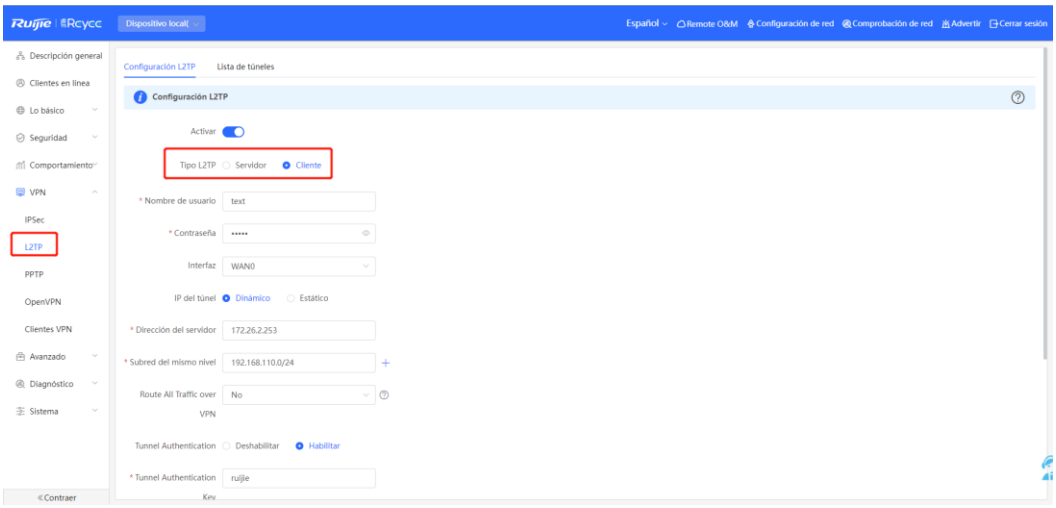
Precaución

- **PC al enrutador**: se establece una conexión entre una PC y una terminal.
- **Enrutador a enrutador**: se configura una conexión directa, no compartida y segura entre dos terminales.

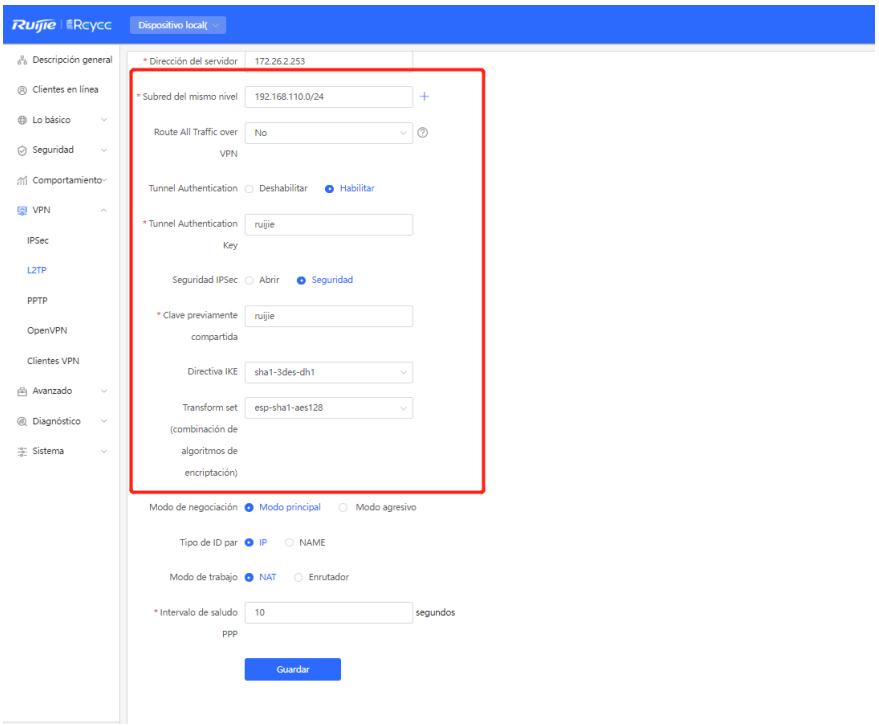
(2) Lado de la sucursal:

a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

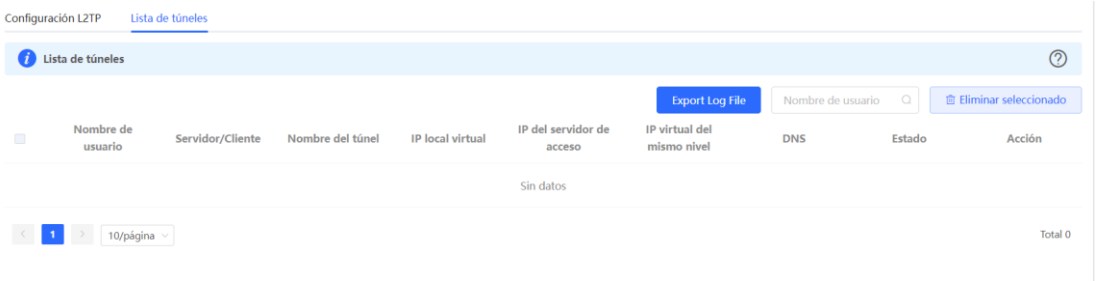
b Cambie al modo **Dispositivo local**, seleccione **VPN > L2TP** y habilite **Autenticación IPSec**.



c Configure una seguridad IPsec y confirme que los valores de **Clave previamente compartida**, **Directiva IKE** y **Transform set (combinación de algoritmos de encriptación)** sean los mismos en ambos lados.

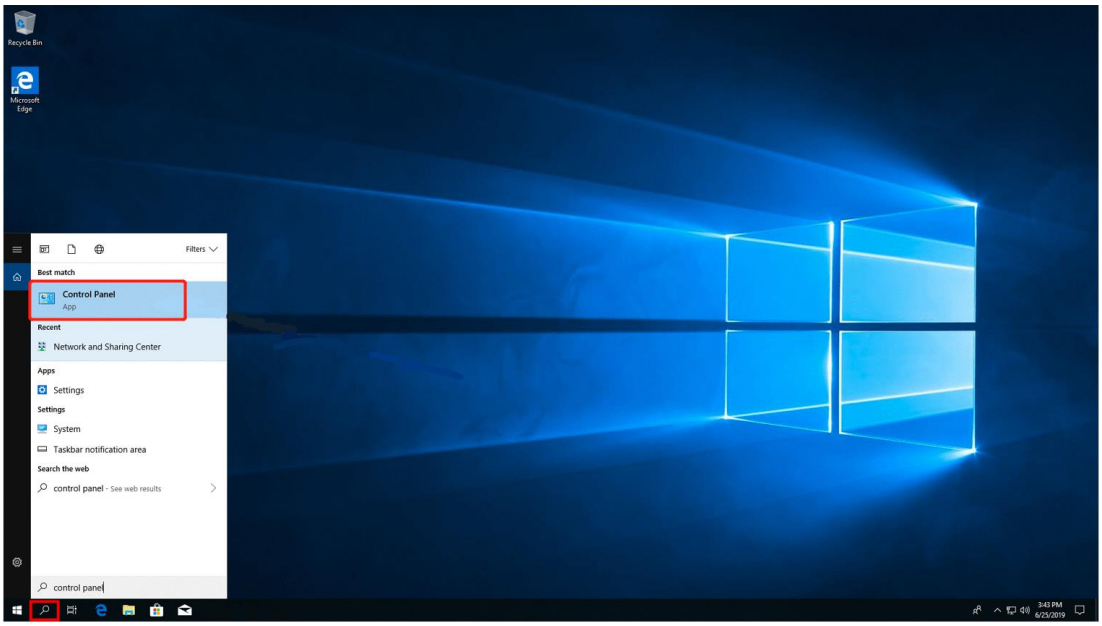


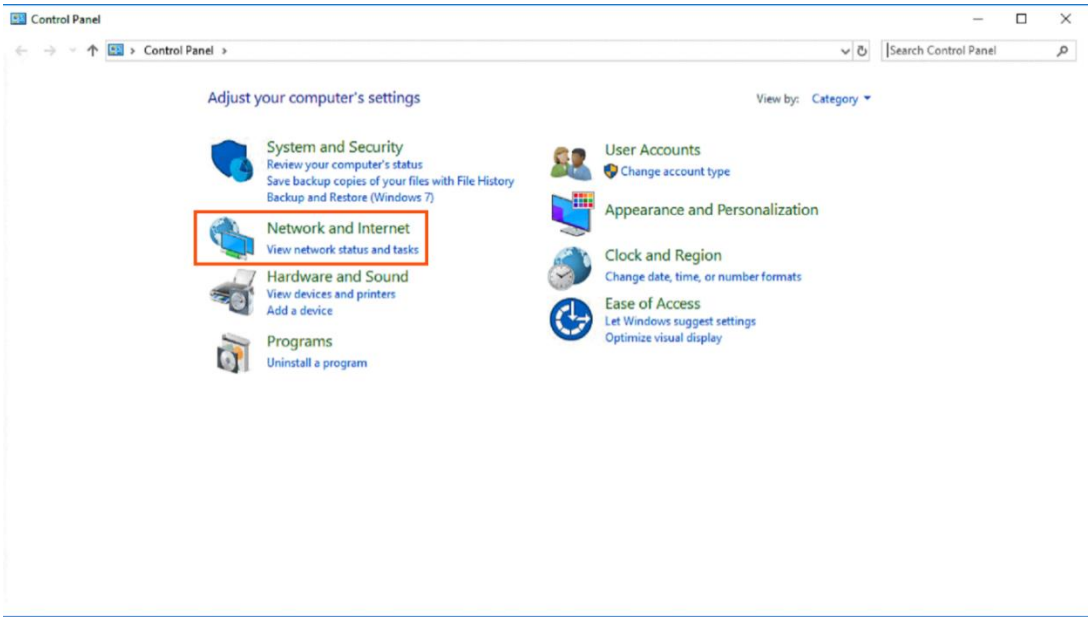
d Revise el estado de la conexión de L2TP sobre IPsec.

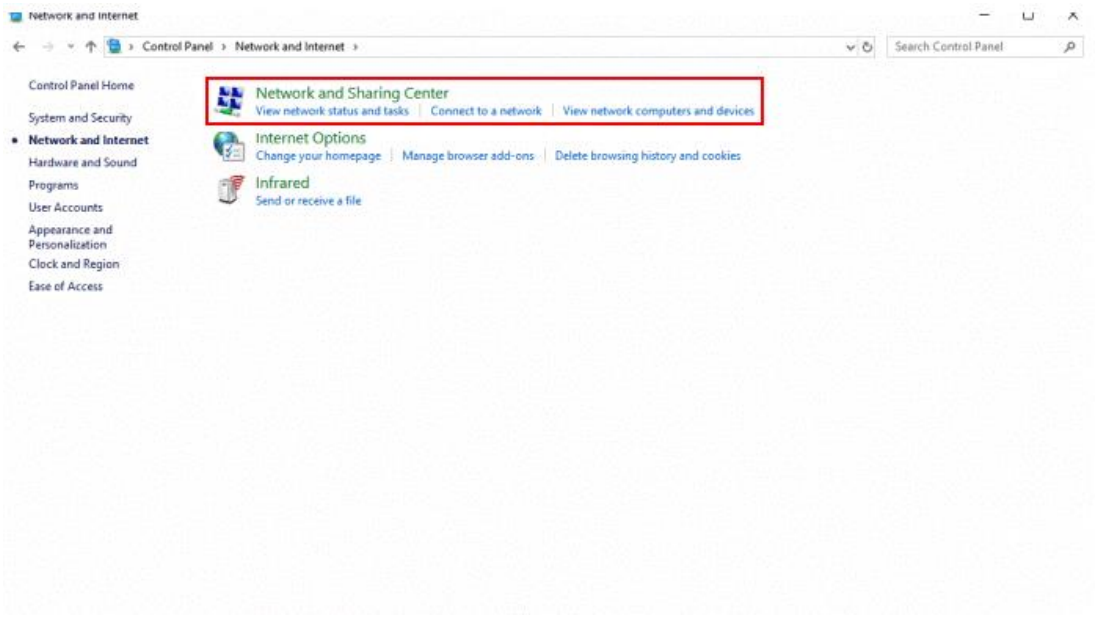


(3) Lado del cliente (se utiliza Windows 10 como ejemplo):

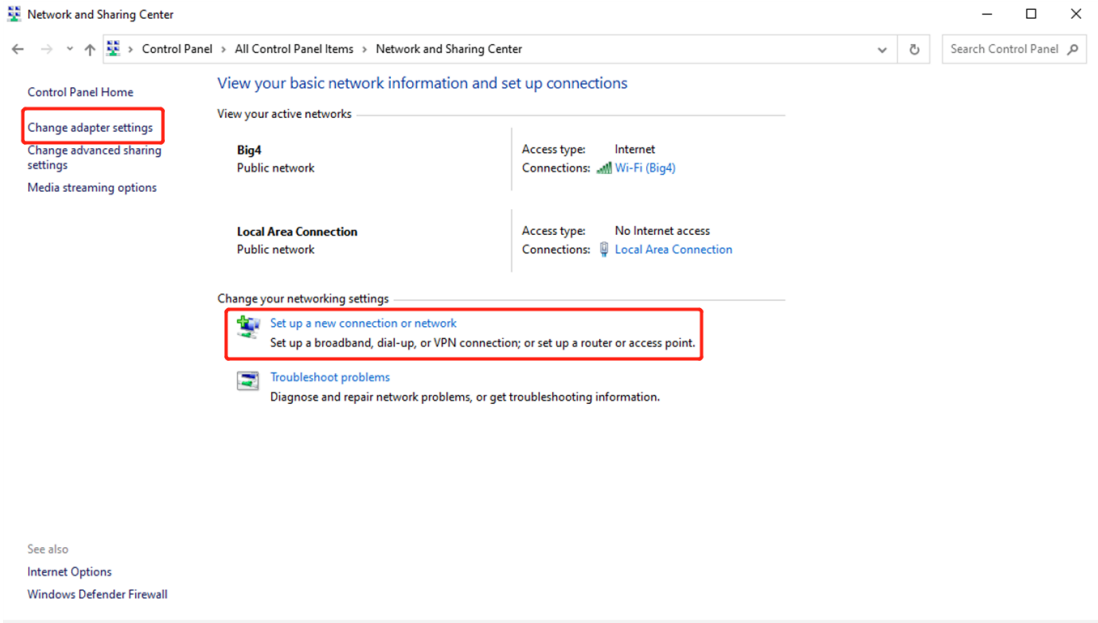
a Seleccione **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

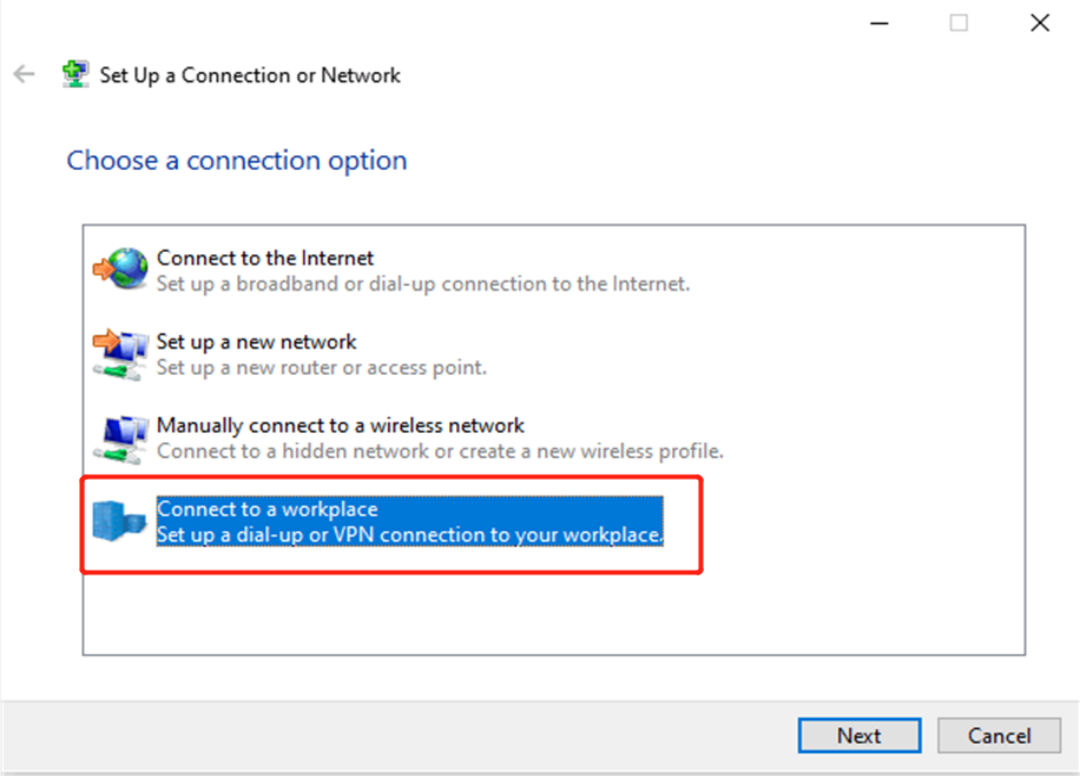


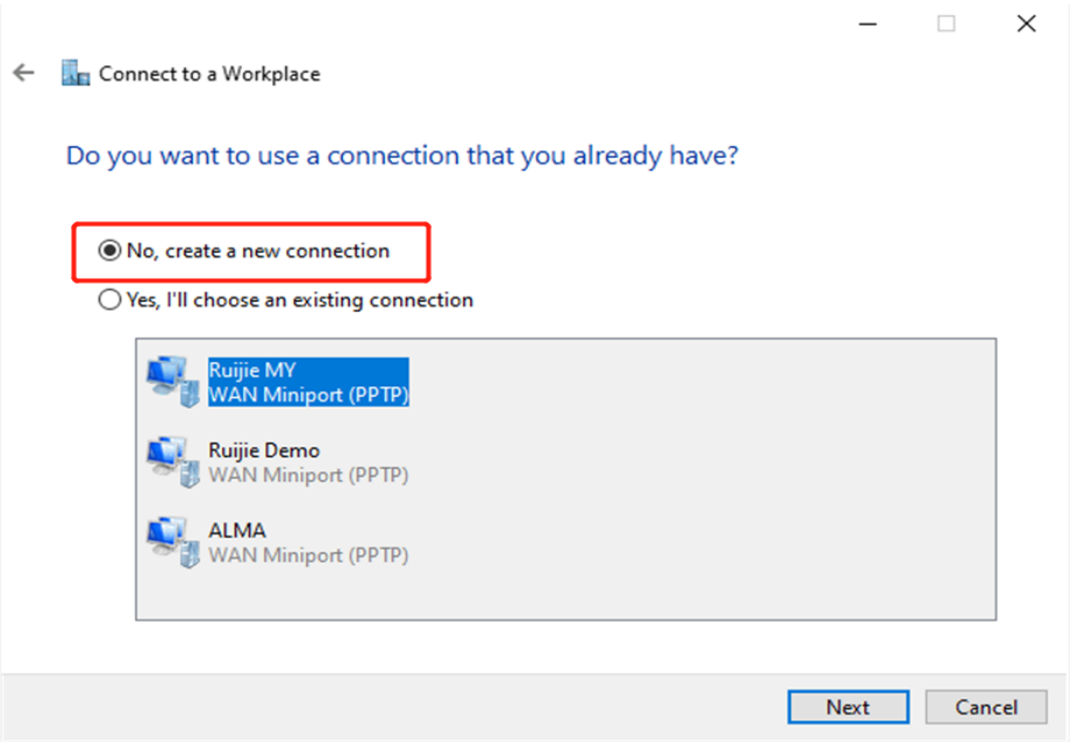


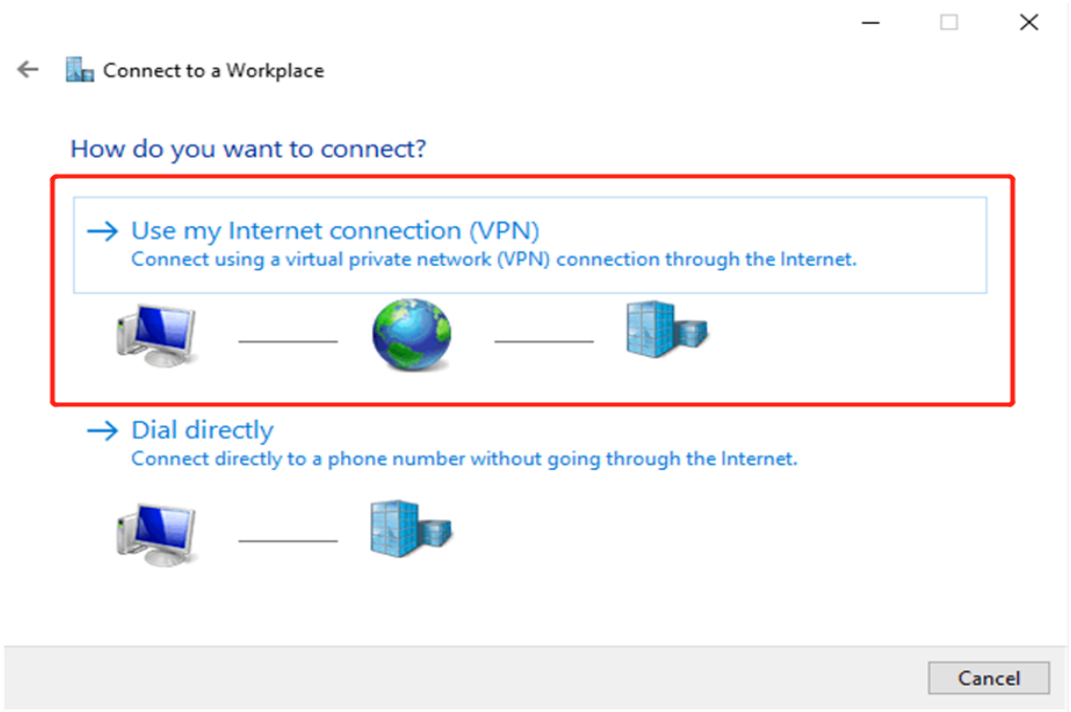


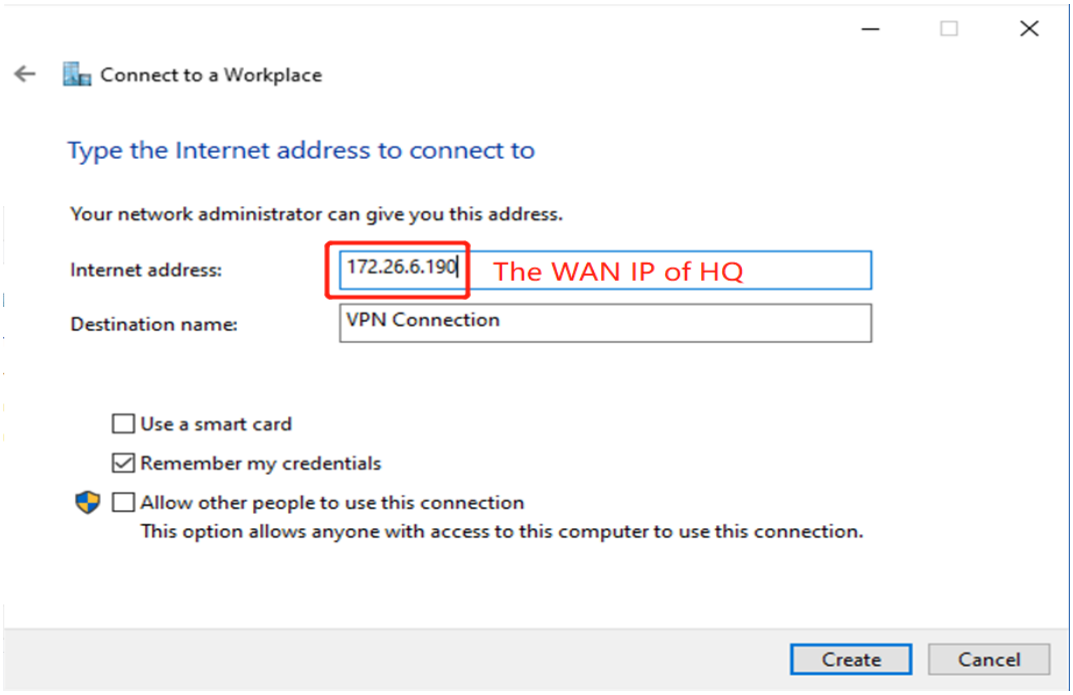
b Configure una conexión VPN.



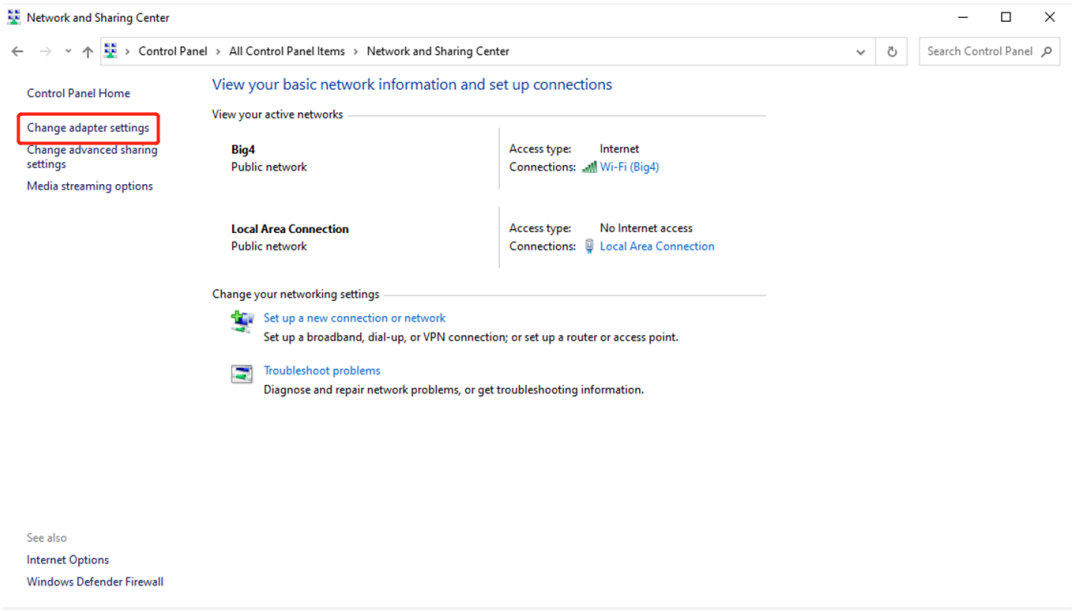

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel

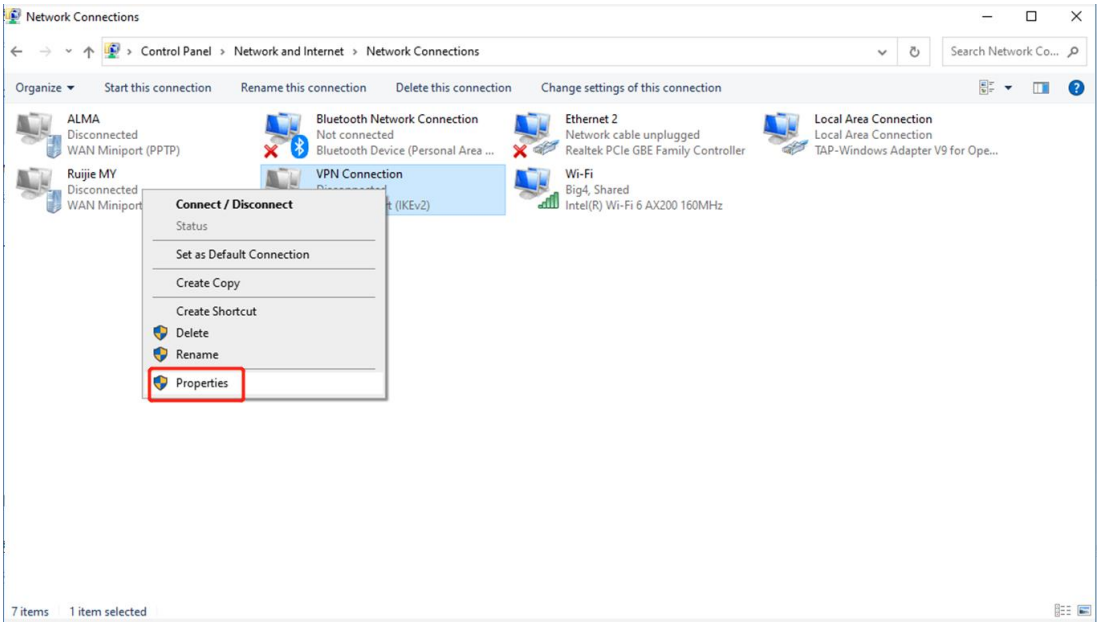

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

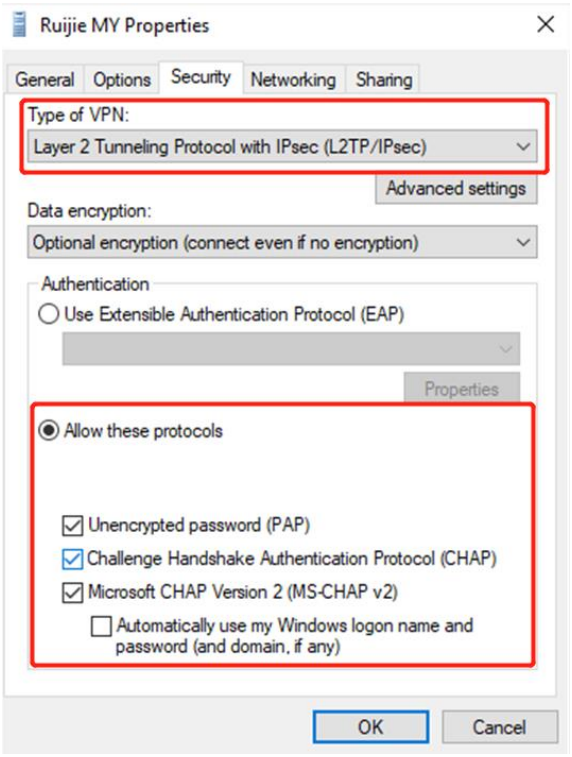




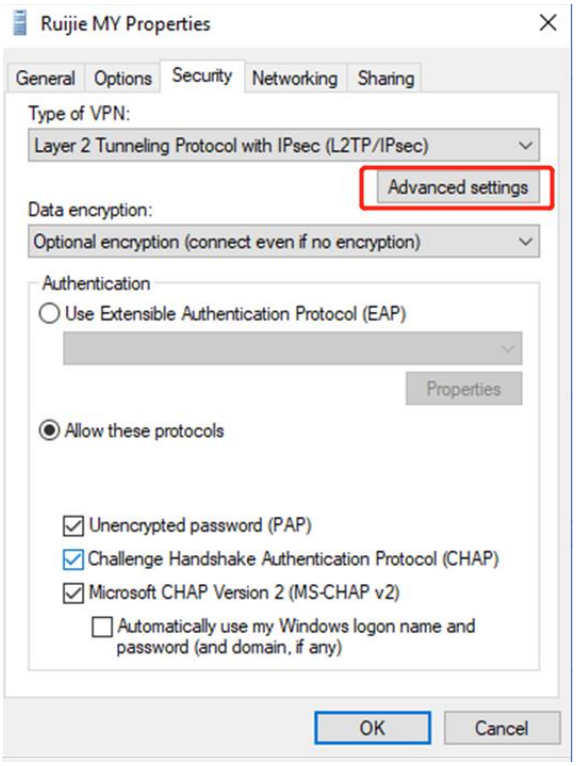
c Cambie la configuración del adaptador.

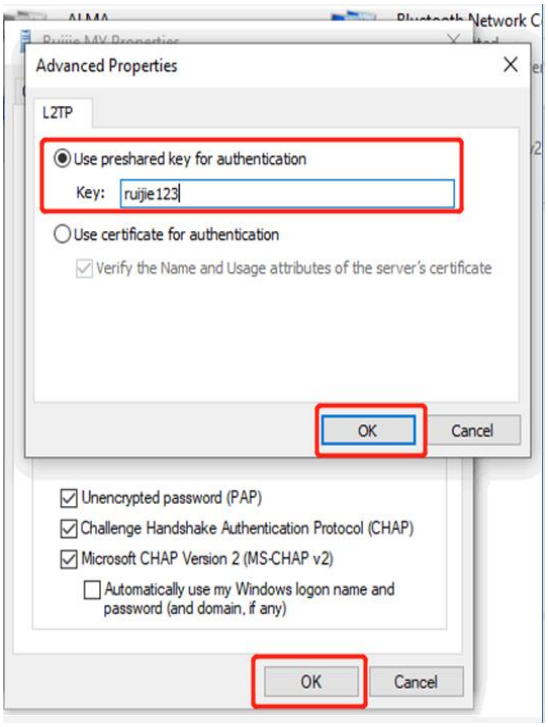

Network and Sharing Center
Control Panel › All Control Panel Items › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
Big4
Public network
Access type: Internet
Connections: Wi-Fi (Big4)
Local Area Connection
Public network
Access type: No Internet access
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Defender Firewall


Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Co...
Organize
Start this connection
Rename this connection
Delete this connection
Change settings of this connection
ALMA
Disconnected
WAN Miniport (PPTP)
Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...
Ethernet 2
Network cable unplugged
Realtek PCIe GBE Family Controller
Local Area Connection
Local Area Connection
TAP-Windows Adapter V9 for Ope...
Ruijie MY
Disconnected
VPN Connection
Wi-Fi
Big4, Shared
Intel(R) Wi-Fi 6 AX200 160MHz
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties
7 items
1 item selected

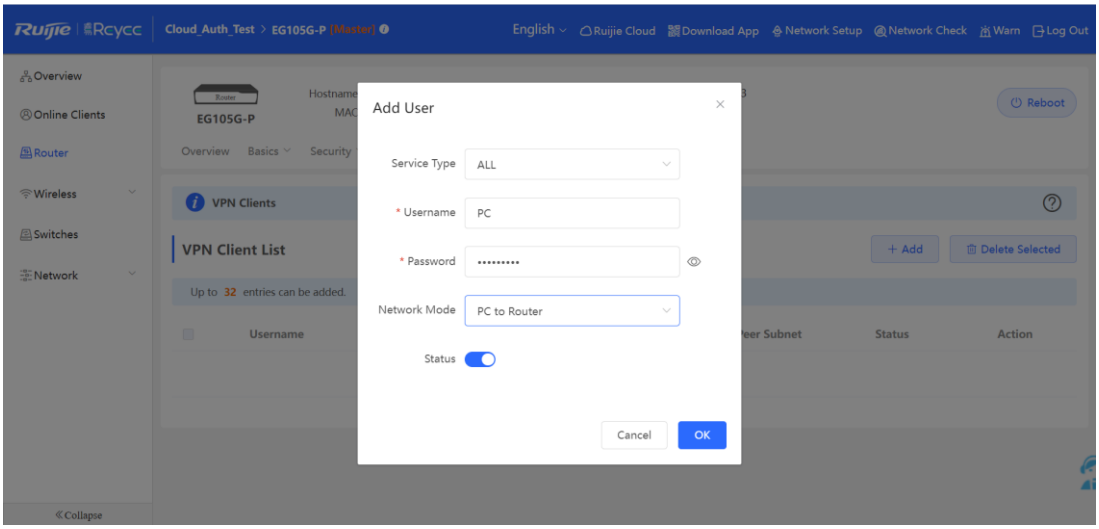


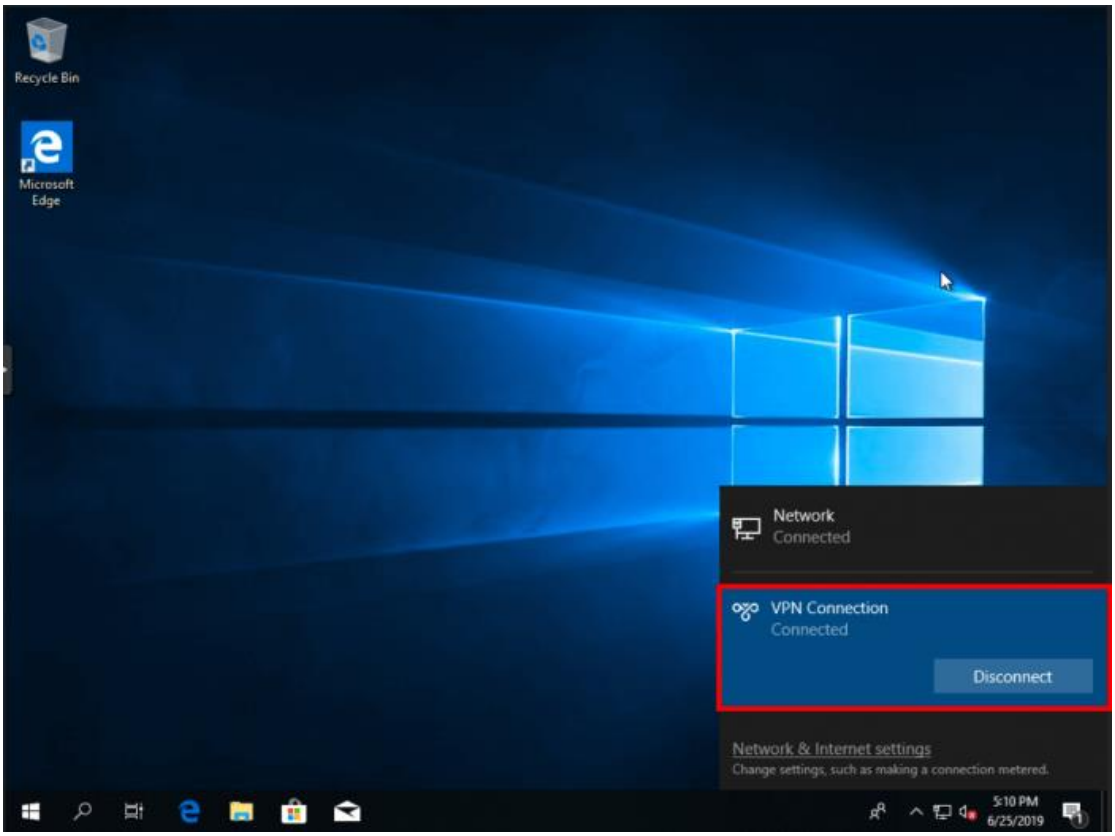
d Haga clic en **Advanced Settings** para configurar la contraseña previamente compartida.





e En **Network Mode**, elija la opción **PC to Router**.





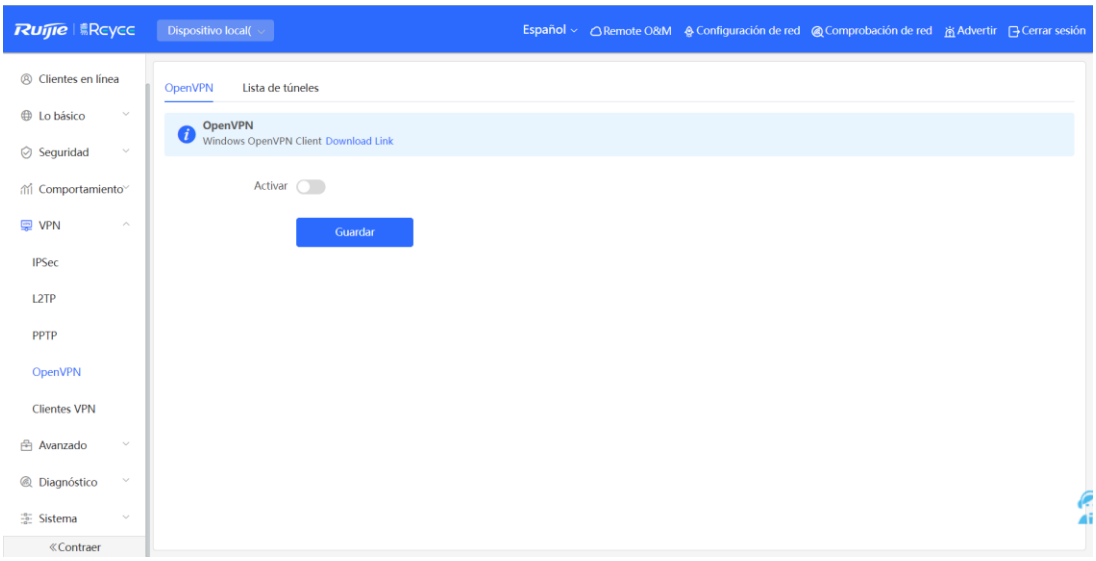
4.7.5 Open VPN

Open VPN se utiliza generalmente en escenarios donde se requiere conectar un sitio con otro sitio y un cliente con un sitio. Es una implementación de VPN de capa de aplicación basada en la biblioteca OpenSSL. En comparación con la VPN tradicional, Open VPN es más sencilla de utilizar. La VPN es un canal o túnel privado virtual que proporciona una transmisión segura de datos entre empresas. Open VPN cuenta con todas las funciones de la VPN SSL, que utiliza tecnología de red segura de Capa 2 y Capa 3, y las del Protocolo de capa de sockets seguros (SSL) o el de Seguridad de la capa de transporte (TLS), ambos estándares de la industria. SSL y TLS son protocolos de seguridad que proporcionan protección e integridad a los datos para las comunicaciones de red. Open VPN admite modos flexibles de autorización de clientes y certificados, nombres de usuario y contraseñas, permitiendo a los usuarios conectarse a esta a través de interfaces virtuales. Open VPN no es una aplicación web basada en proxy o en acceso basado en un navegador.

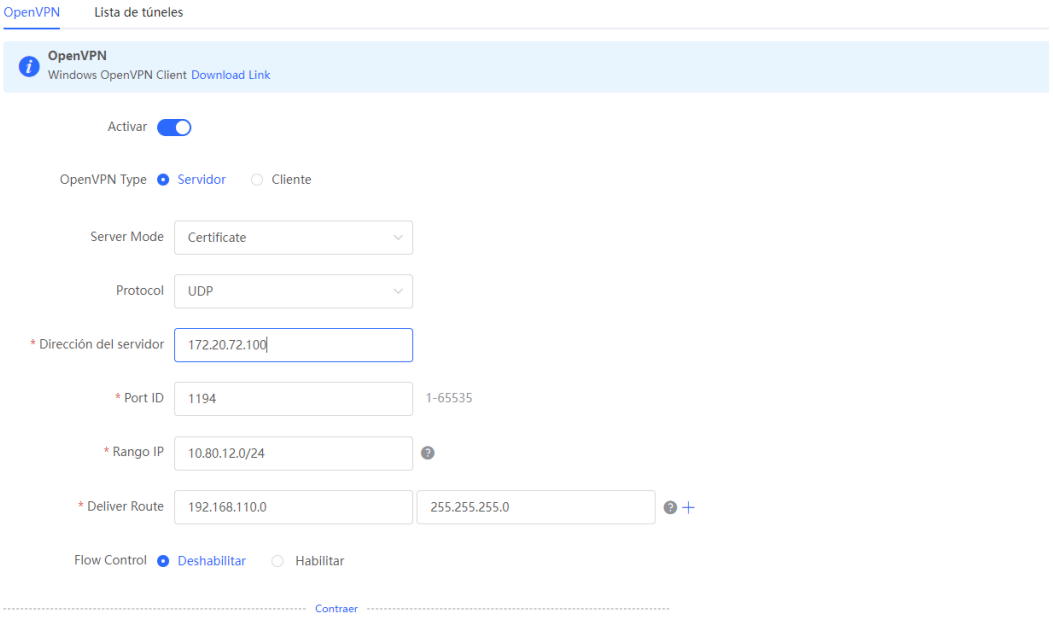
(1) Lado de la sede:

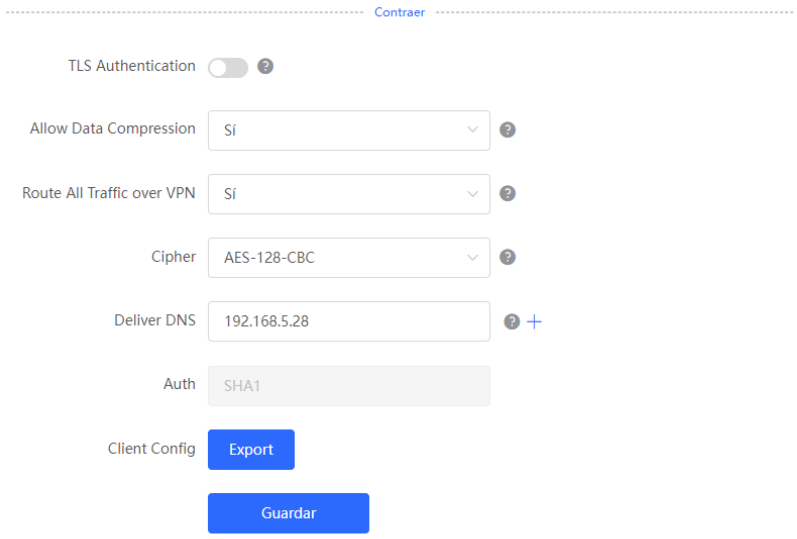
a Inicie sesión en el Reyee EG con la dirección IP predeterminada 192.168.110.1.

b Cambie al modo **Dispositivo local**. Seleccione **VPN** > **OpenVPN**.



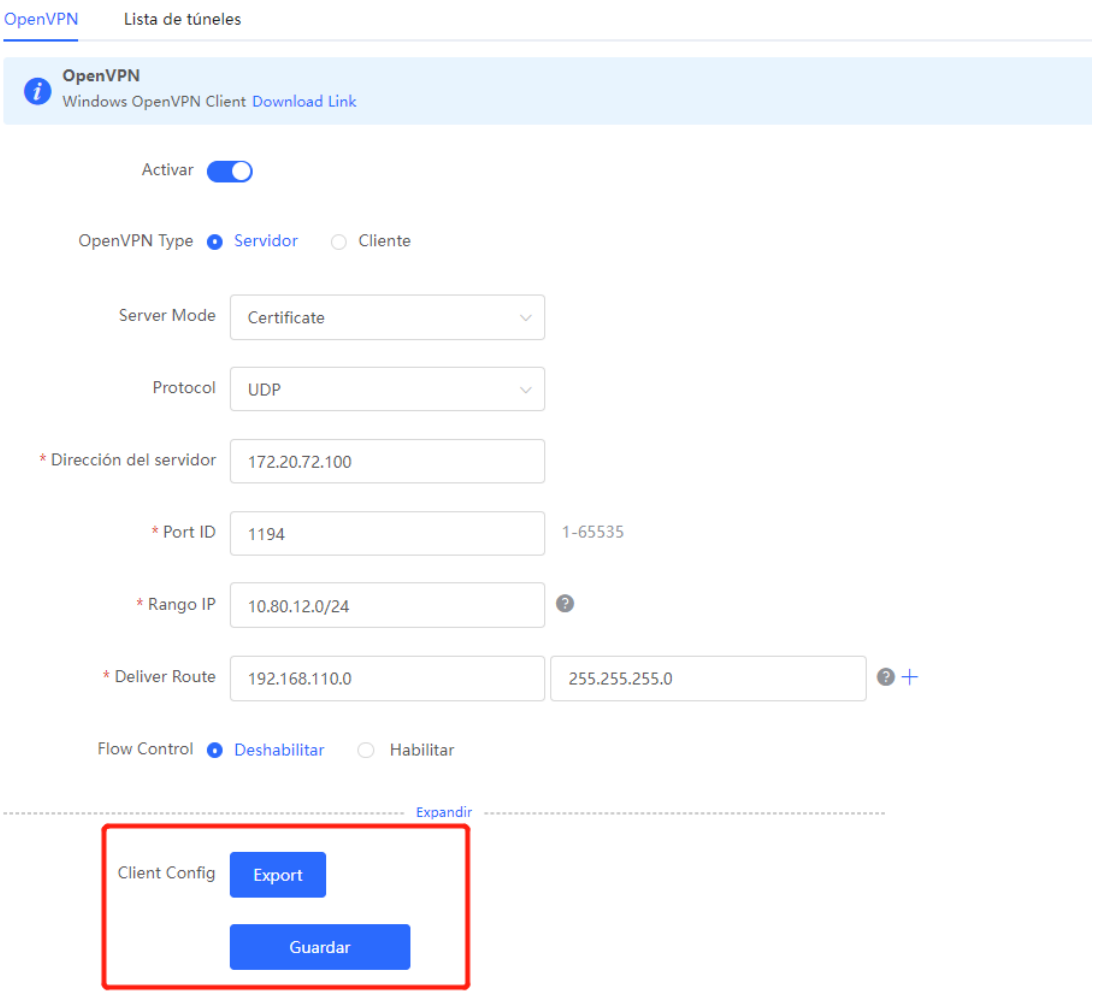
c Habilite **OpenVPN** y configure la información de la VPN.





- **OpenVPN Type**: seleccione **Servidor** o **Cliente**, según lo requiera.
- **Server Mode**: seleccione un modo de autenticación.
  - Cuenta: ingrese la contraseña correcta de la cuenta e importe el archivo del certificado CA en el cliente.
  - Certificado: importe el certificado CA correcto, el certificado del cliente y archivo de la clave privada en el cliente.
  - Cuenta y certificado: debe ingresar la contraseña correcta de la cuenta e importar el certificado CA correcto, el certificado del cliente y archivo de la clave privada en el cliente.
  - **Protocol**: seleccione **TCP** o **UDP**.
- **Dirección del servidor**: ingrese la dirección IP de WAN o el nombre del dominio.
- **Port ID**: utilice el puerto predeterminado 1194.
- **Rango IP**: asigne las direcciones IP en el rango para clientes.
- **Deliver Route**: la ruta del cliente se utiliza cuando este tiene acceso a la Intranet del servidor.
- **Expandir**
- **TLS Authentication:** cada conexión VPN está asegurada por una clave TLS.
- **Allow Data Compression**: por defecto, el valor es **Sí**.
- **Route All Traffic over VPN**: por defecto, el valor es **No**.
- **Cipher**: se puede seleccionar un algoritmo para el encriptado de datos. Por defecto, se utiliza AES-128-CBC.
- **Deliver DNS**: al cliente se le asigna una dirección DNS.
- **Auth**: por defecto, se utiliza SHA1.

d Haga clic en **Guardar** para guardar la configuración y luego en **Export** para exportar la configuración del cliente.



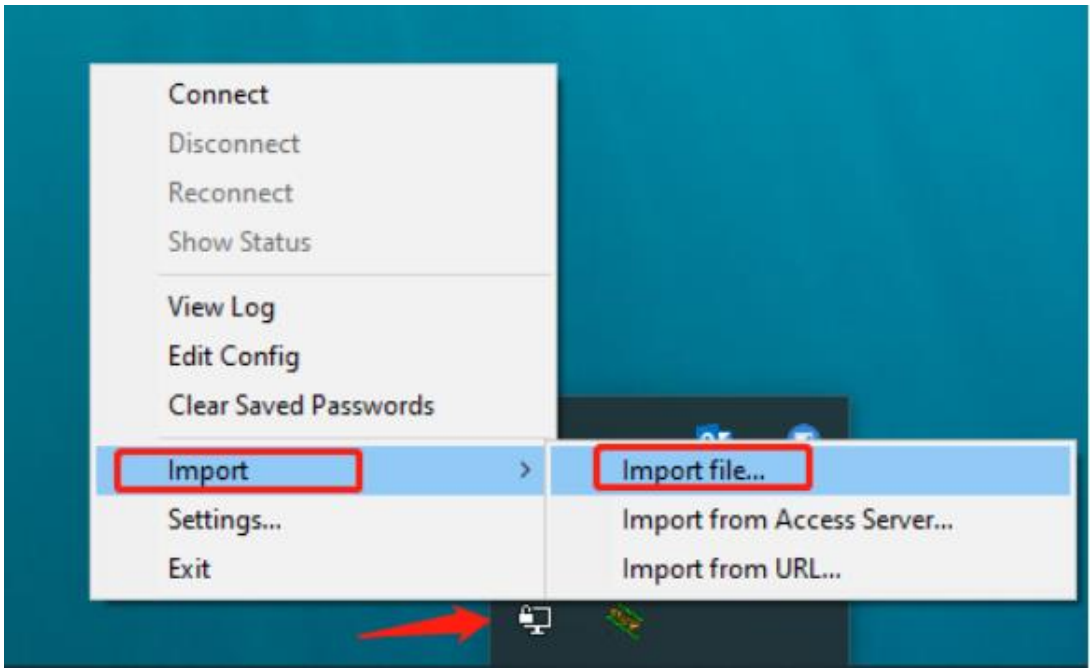
(2) Lado del cliente (se utiliza Windows 10 como ejemplo):

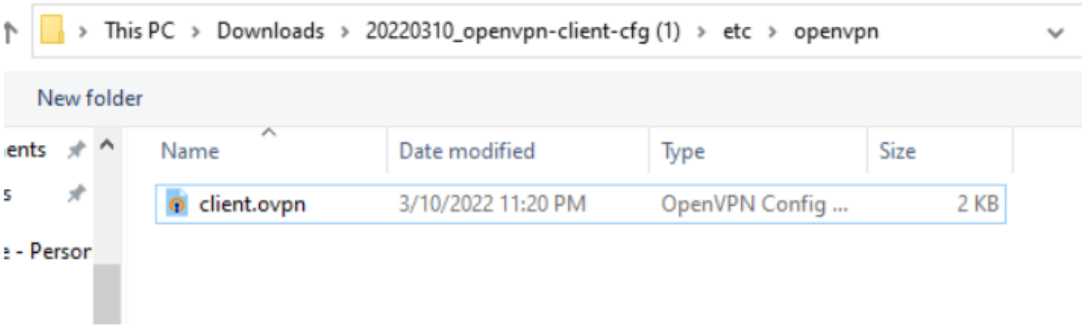
a Descargue e instale la aplicación OpenVPN en su PC.

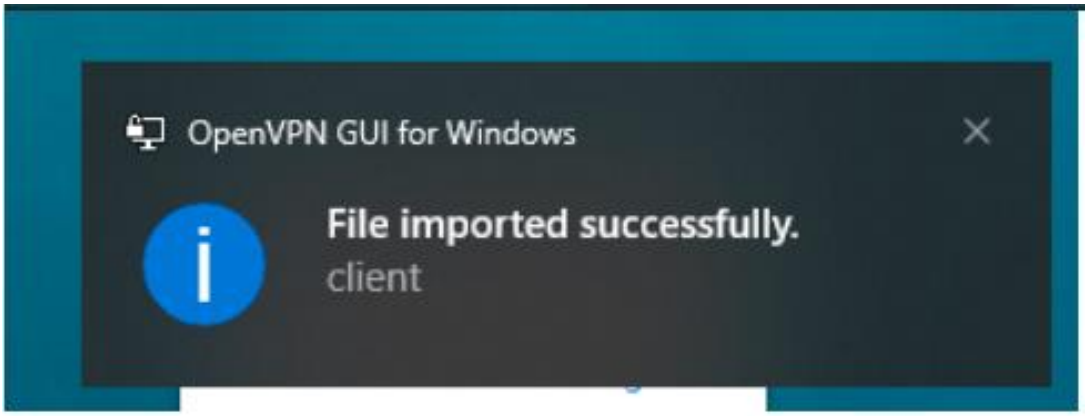
Puede descargar el cliente OpenVPN en https://openvpn.net/community-downloads/. Seleccione una versión apropiada para su PC.

b Importe la configuración de cliente al cliente OpenVPN después de haberlo instalado en su PC.

- Exporte la configuración del cliente en la página web.
- Haga clic derecho en **OpenVPN** y seleccione **Import** > **Import file...** para importar la configuración del cliente en el cliente.

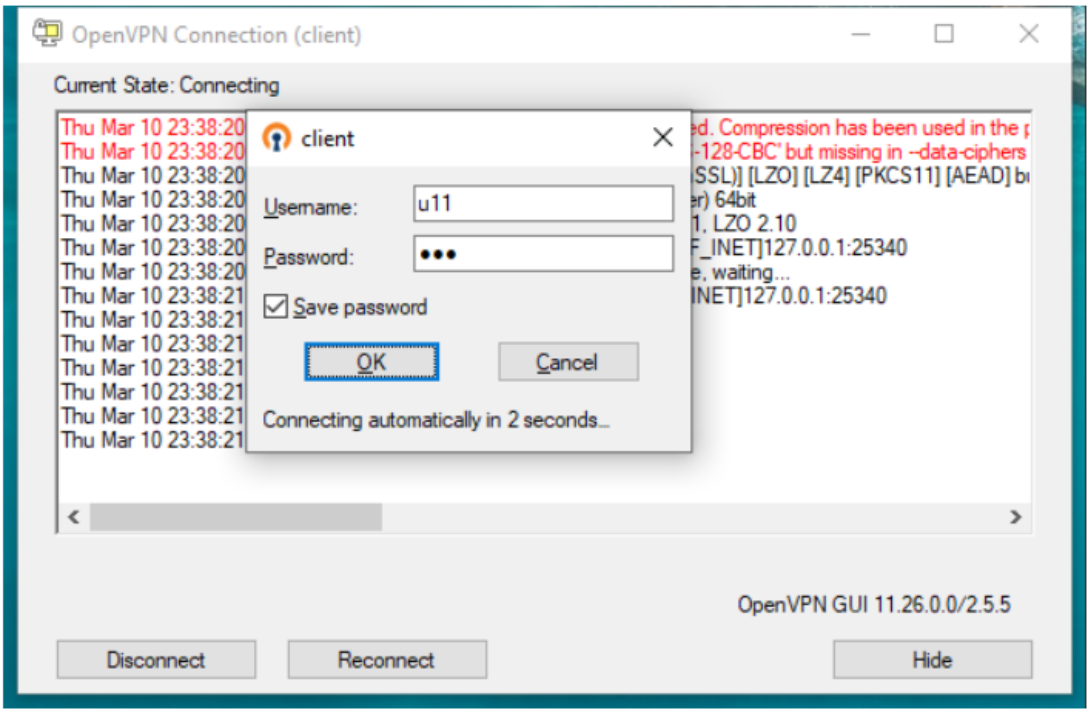


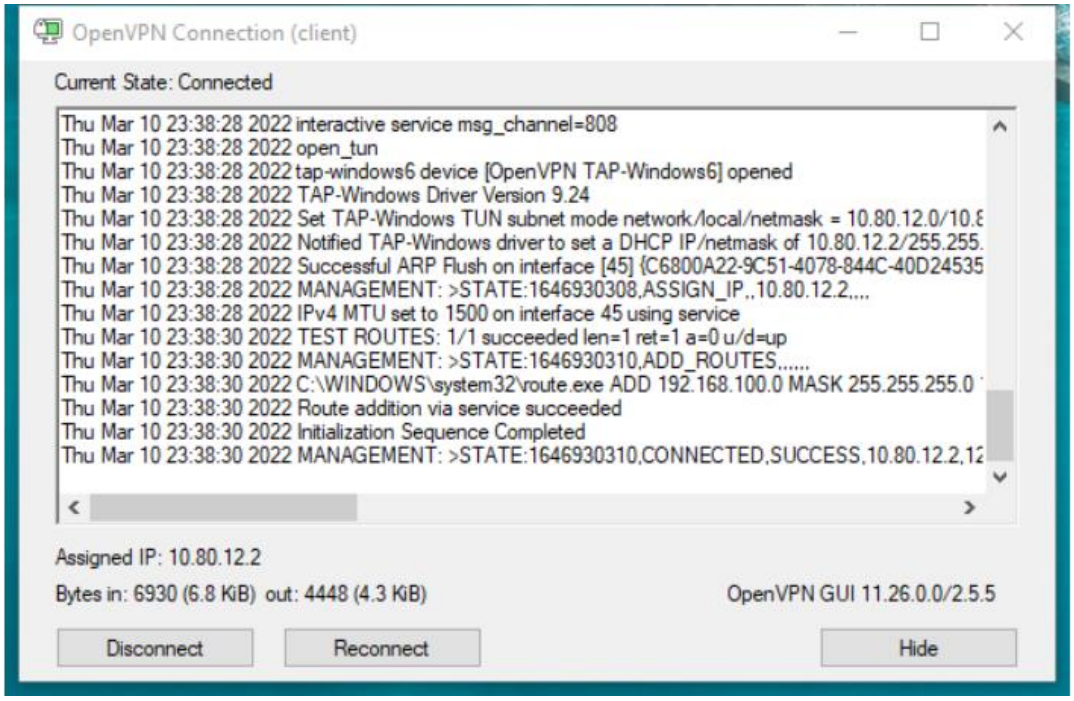




Cuando aparezca el mensaje **"File imported successfully"**, ya puede conectarse a la VPN.

c Haga clic en **OpenVPN** y seleccione **Conectar**. Si utiliza un método de autenticación de cuenta, ingrese su cuenta VPN.





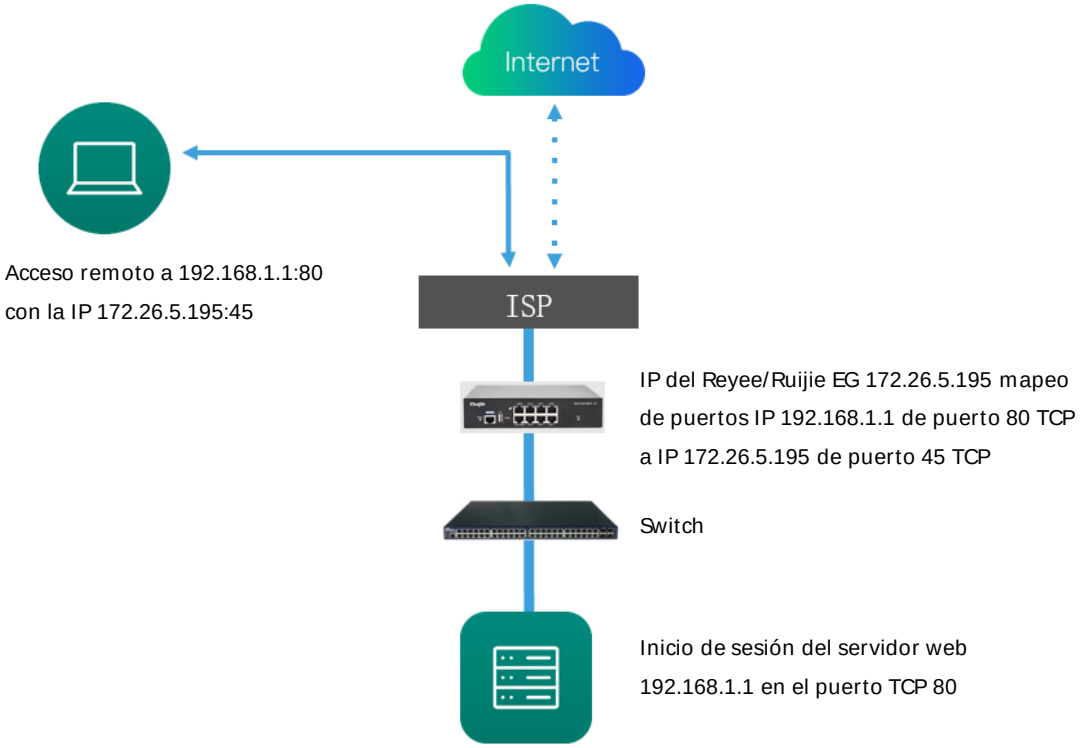
4.8 Mapeo de puertos

El mapeo de puertos se utiliza para asignar la dirección IP del servidor interno y el número de puerto a una dirección IP externa, para que el personal fuera de la red tenga acceso a los servidores internos. La diferencia entre el mapeo de puertos y la DMZ es que la primera solo realiza el mapeo de uno o dos puertos, mientras que la DMZ realiza el de todos los puertos.

- Escenario típico para el mapeo de puertos

  La función de mapeo de puertos establece una relación de redireccionamiento entre la dirección IP y el número de puerto de un puerto WAN con la dirección IP y el número de puerto de un servidor en la LAN, para que todo el tráfico de acceso destinado a un puerto de servicio del puerto WAN se redirija al puerto correspondiente del servidor LAN especificado. Esta función habilita a los usuarios externos a acceder proactivamente al host de servicio de una LAN a través de la dirección IP y el número de puerto de la WAN especificada.

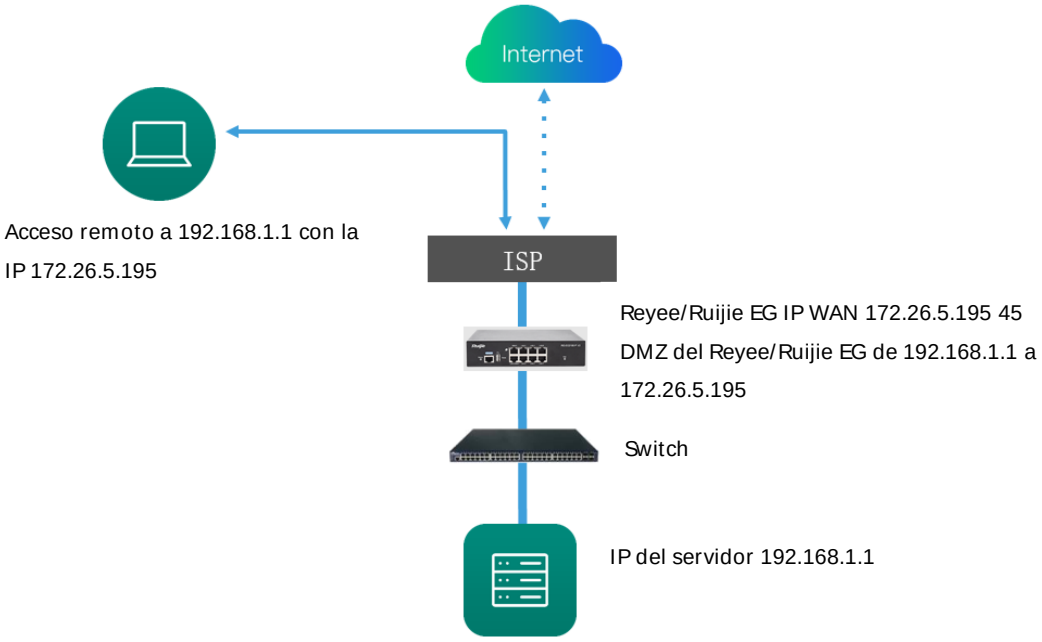
  El mapeo de puertos permite a los usuarios acceder a cámaras y computadoras en las redes de sus hogares cuando están en las empresas o en un viaje de negocios.



- Escenario típico de DMZ

  Cuando un paquete de datos entrante no encuentra ninguna entrada del mapeo de puertos, este se redirige al servidor LAN, de acuerdo con la regla de zona desmilitarizada (DMZ). Todos los paquetes enviados proactivamente del Internet al dispositivo se reenvían al host de la DMZ designada, aprovechando el acceso al servidor LAN de los usuarios externos de la red. La DMZ proporciona acceso al servicio de red externa mientras garantiza la seguridad de los otros hosts en la LAN.

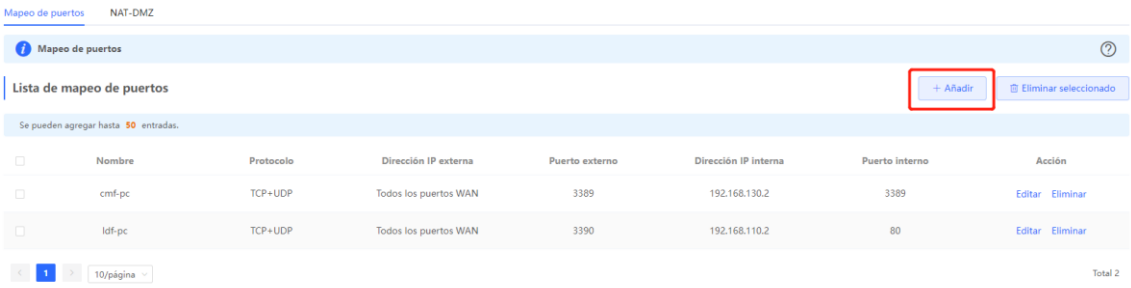
  El mapeo de puertos o la DMZ se utilizan cuando un usuario de la red externa desea acceder al servidor LAN; por ejemplo, contar con acceso a un servidor implementado en la Intranet cuando se encuentra en la empresa o en un viaje de negocios.



4.8.1 Configuración del mapeo de puertos

(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Mapeo de puertos** > **Mapeo de puertos**.

(2) Haga clic en **Añadir**. En el cuadro de diálogo que aparece, ingrese el nombre de la regla, el tipo de servicio y de protocolo, así como el rango del puerto externo, la dirección de IP del servidor interno y el rango del puerto interno. Puede crear un máximo de 50 reglas de mapeo de puertos.



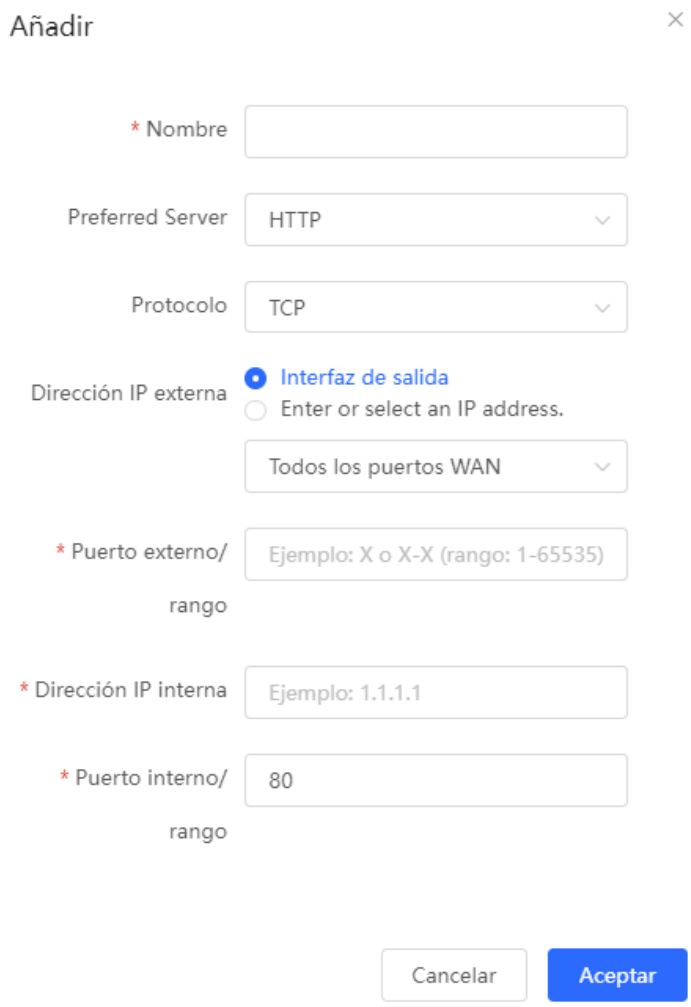


Tabla 4- 5 Configuración del mapeo de puertos

Parámetro	Descripción
Nombre	Ingrese la descripción de una regla de mapeo de puertos, la cual se utiliza para identificarla.
Servidor preferido	Seleccione el tipo de servicio para el mapeo, como HTTP o FTP. El número interno de puertos normalmente usado por el servicio aparece automáticamente. Si no se conoce el tipo de servicio, seleccione **Personalizado**.
Protocolo	Seleccione el tipo de protocolo de la capa de transmisión utilizado por el servicio, como TCP o UDP. El valor **TODOS** indica que la regla aplica para ambos protocolos. Este debe cumplir con la configuración del cliente del servicio.

Parámetro	Descripción
Dirección IP externa	Especifique la dirección del host utilizada para tener acceso a la red externa. **Interfaz de salida:** puede seleccionar **Todos los puertos WAN** o especificar uno solo. **Enter or select an IP address**: seleccione o ingrese la dirección IP del puerto WAN.
Puerto externo/rango	Especifique el número de puerto utilizado para el acceso a Internet. Confirme el número de puerto en el software del cliente, como el software de monitoreo por cámara. Puede ingresar un número o rango de puerto, como 1050-1060. Si ingresa el rango de puerto, el valor de **Puerto interno/rango** debe ser el mismo.
Dirección IP interna	Especifique la dirección IP del servidor interno que será mapeado hacia el puerto WAN; esto es, la dirección IP del dispositivo LAN que proporciona el acceso a Internet, como la dirección IP de una cámara de red.
Puerto interno/rango	Especifique el número de puerto de servicio del servidor interno que será mapeado hacia el puerto WAN; esto es, el número de puerto de la aplicación que proporciona el acceso a Internet, como el puerto 8080 del servicio web. Puede ingresar un número o rango de puerto, como 1050-1060. Si ingresa un rango de puerto, el número de puertos debe ser el mismo que el especificado en **Puerto externo/rango**.

(3) Revise si el dispositivo de la red externa cuenta con acceso a los servicios en el host de destino utilizando la dirección IP y el número de puerto externo.

4.8.2 Configuración de NAT-DMZ

(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Mapeo de puertos** > **Mapeo de puertos** > **NAT-DMZ**.

(2) Haga clic en **Añadir**. Ingrese el nombre de la regla y la dirección IP del servidor interno, seleccione la interfaz a la cual aplica la regla, especifique su estado y haga clic en **Aceptar**. Puede configurar solo una regla DMZ por interfaz de salida.

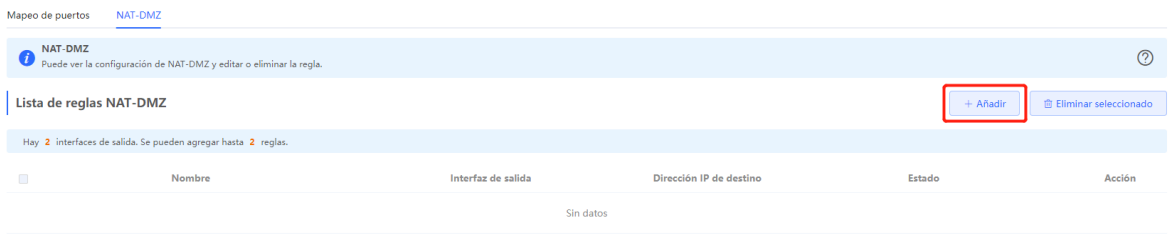


Table 4-6 Configuración de la regla DMZ

Parámetro	Descripción
Nombre	Ingrese la descripción de la regla de mapeo, la cual se utiliza para identificar la regla.
Dirección IP de destino	Especifique la dirección IP del host DMZ al que se redirigen los paquetes; esto es, la dirección IP del servidor interno al que se puede tener acceso desde Internet.
Interfaz de salida	Especifique el puerto WAN en la regla DMZ. Puede configurar solo una regla por puerto WAN.
Estado	Especifique si desea que la regla surta efecto. Esta surte efecto cuando se habilita el parámetro **Estado**.

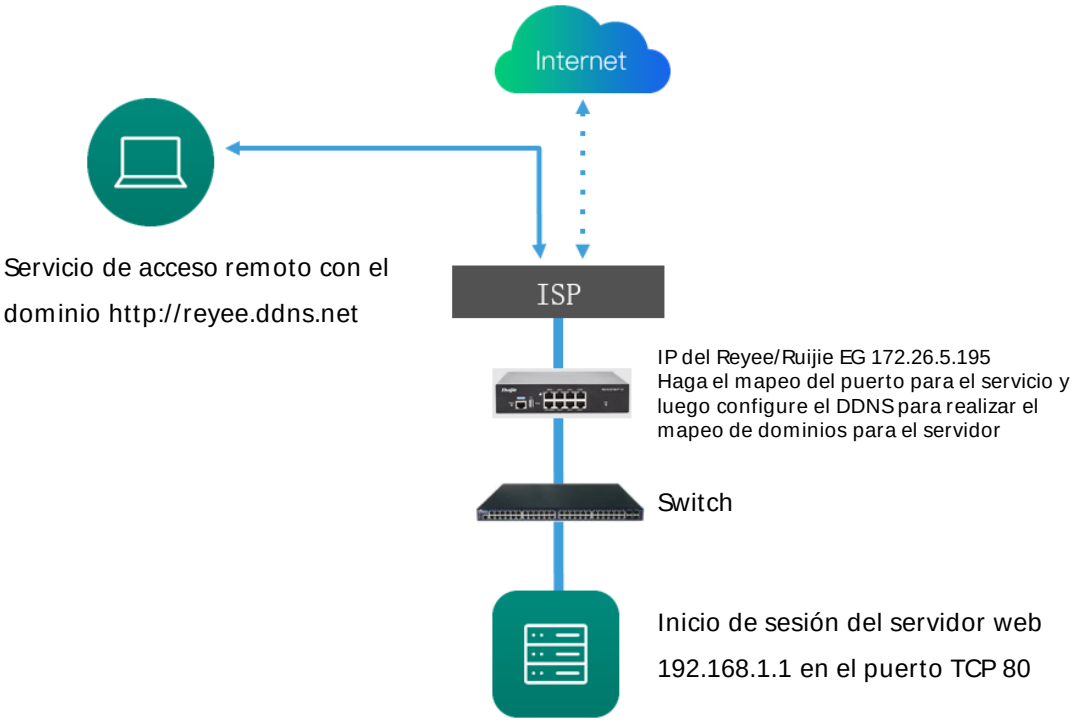
Precaución

Cuando la DMZ y el mapeo de puertos se configuran, este último tiene preferencia.

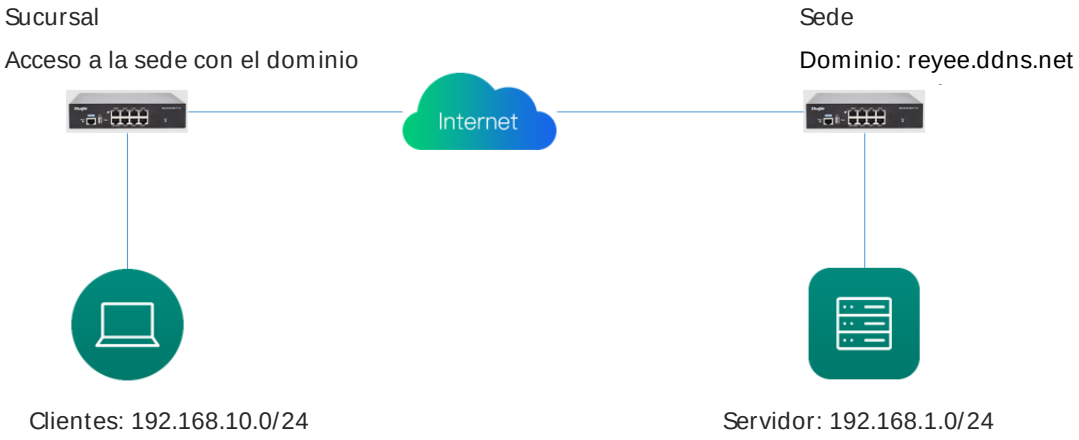
4.9 DNS dinámico

El sistema dinámico de nombres de dominio (DDNS) se utiliza para hacer mapeos de las direcciones IP dinámicas de los usuarios a un nombre de dominio fijo. Cada vez que un usuario se conecta a la red, el programa del cliente transferirá la dirección IP dinámica del host de usuario al programa del servidor ubicado en un host del proveedor de servicio. En ese momento, el programa del servidor es responsable de brindar los servicios DNS y de implementar la resolución dinámica de nombres de dominio.

- Acceso al servidor con el nombre del dominio

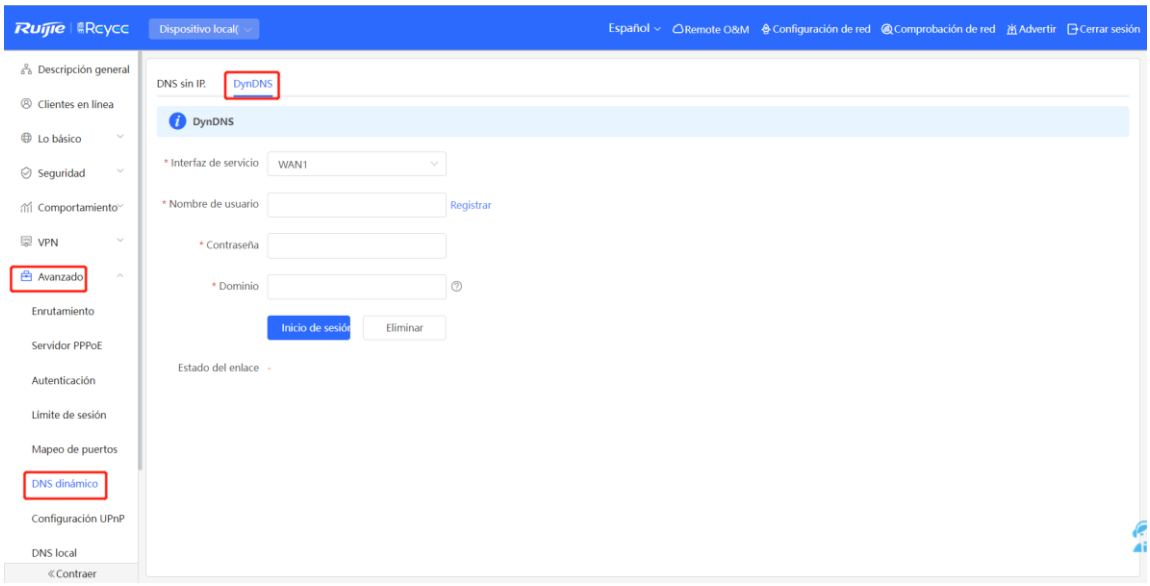


- Conexión VPN con el nombre del dominio



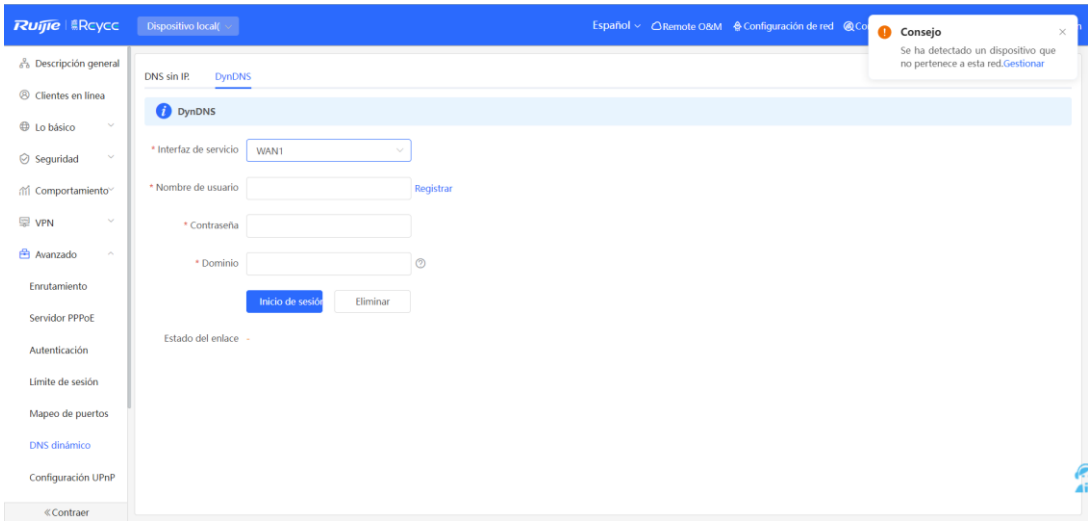
(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado > DNS dinámico**.

Hay tres servidores DDNS que puede elegir para conectarse: Peanut Shell DDNS, NO-IP DNS y DynDNS.



(2) Cuando se utiliza Peanut Shell DDNS, se recomienda usar WeChat o Peanut Shell para escanear el código QR para registrar una cuenta.

(3) Puede usar el valor de **Dominio** para tener acceso al servidor de la intranet o el dispositivo de la sede.



4.10 Autenticación

4.10.1 Escenario de aplicación

A medida que las redes inalámbricas se vuelven populares, el Wi-Fi se ha vuelto uno de los medios de publicidad para los vendedores. Los usuarios se pueden conectar al Wi-Fi, proporcionado por los vendedores, para navegar en Internet después de ver los anuncios o seguir las cuentas oficiales de WeChat. Además, para evitar vulnerabilidades de seguridad, la red inalámbrica de las oficinas generalmente permite que solo los empleados estén asociados con su Wi-Fi; por lo que las identidades de los clientes deben verificarse.

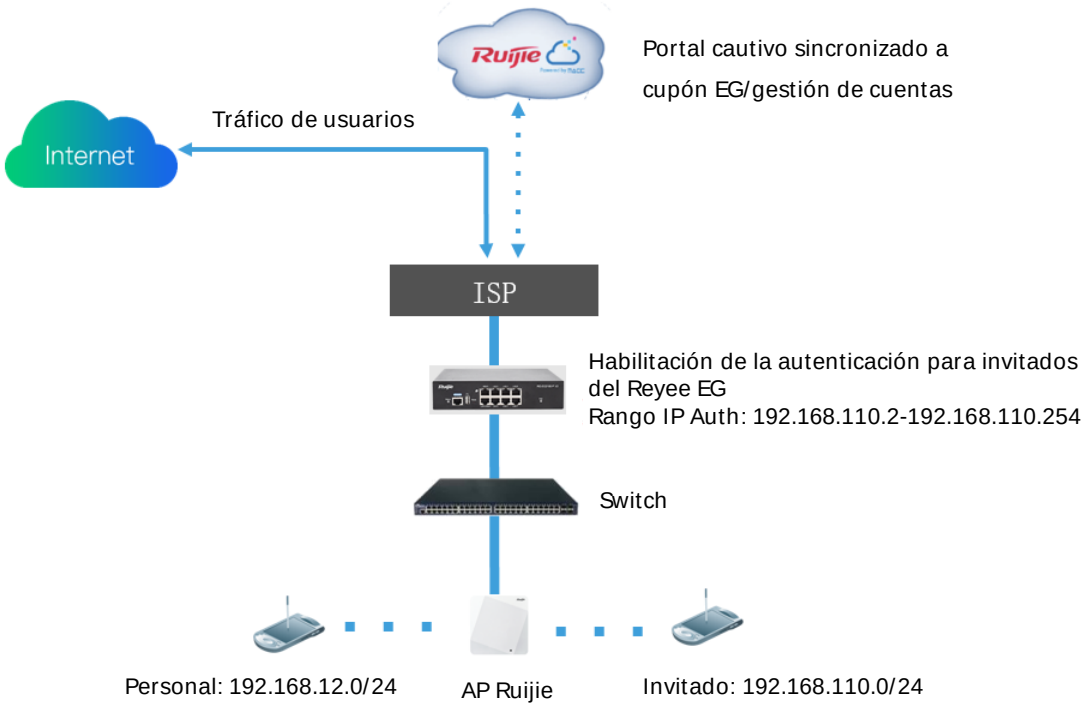
El dispositivo utiliza un portal de autenticación para ejecutar la visualización de la información de los usuarios y su administración. Cuando los usuarios se conectan a la red Wi-Fi, el tráfico no se enruta a Internet. Primero deben pasar por un proceso de identificación en el sitio web del portal de autenticación y solo a aquellos que estén autorizados se les permitirá el uso de los recursos de la red. Los vendedores y empresas pueden personalizar las páginas del portal para la autenticación de identidad y mostrar publicidad.

(1) Antes de habilitar la autenticación de Wi-Fi, asegúrese de que las señales inalámbricas sean estables y que los usuarios puedan conectarse y navegar por Internet de manera normal. El SSID inalámbrico utilizado para la autenticación en una red se debe configurar en **open**. El encriptado puede ocasionar demoras en la interconexión de Wi-Fi durante la autenticación.

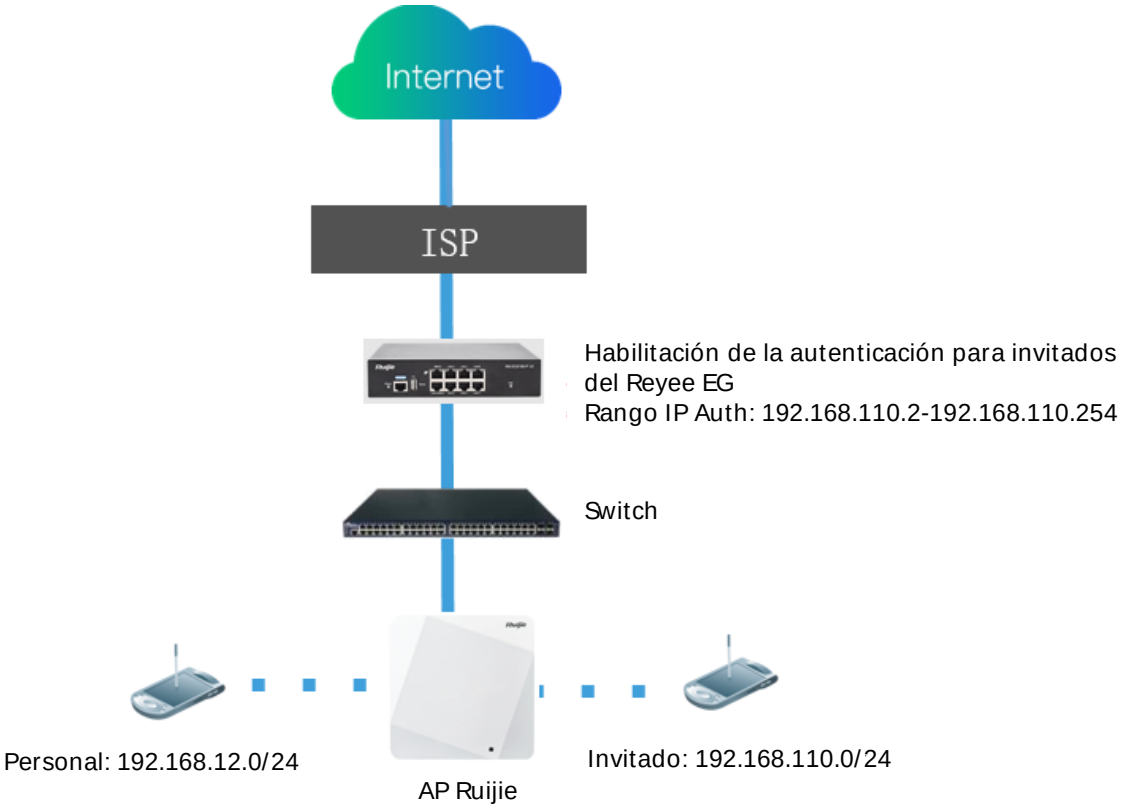
(2) Si la dirección IP del AP de una red se encuentra dentro del alcance de la autenticación, añada el AP como usuario de libre autenticación. En una red de Capa 2, añada la dirección MAC del AP a la lista blanca de direcciones MAC de libre autenticación.

- En una red de Capa 3, añada la dirección IP del AP a la lista blanca de direcciones IP de libre autenticación.

- **Escenario de autenticación en la nube**



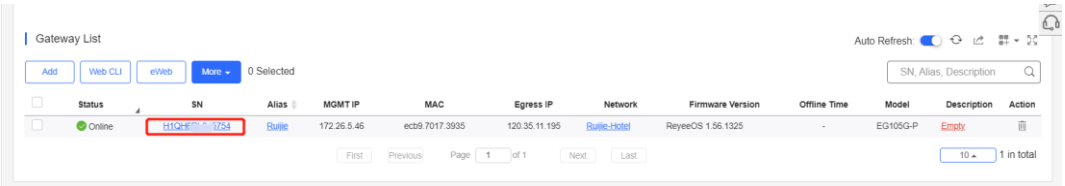
- **Escenario de autenticación de una cuenta local**



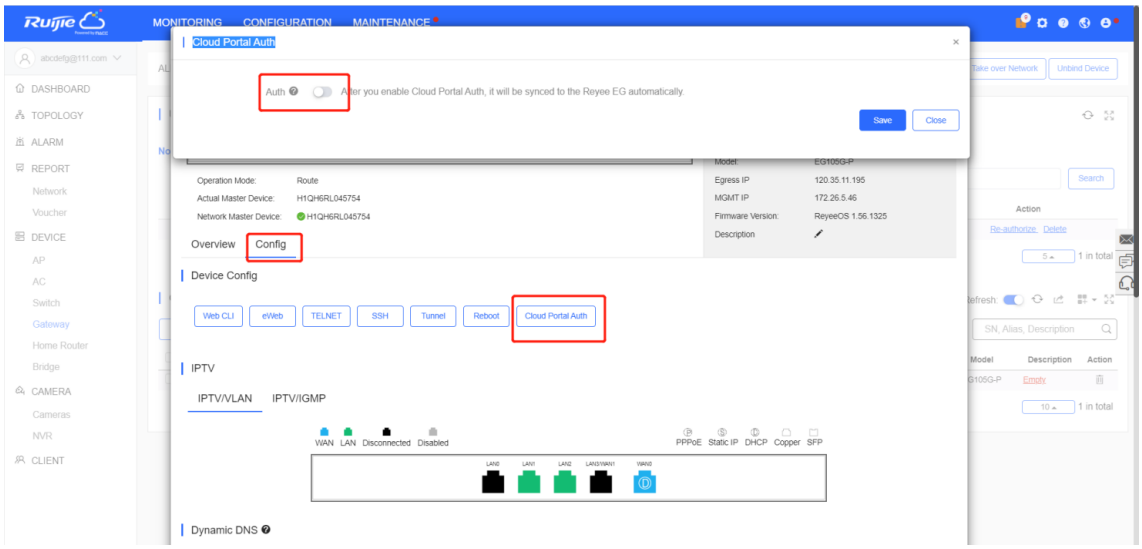
4.10.2 Autenticación de la nube

Los dispositivos Reyee EG admiten la autenticación mediante un portal en la nube, incluyendo los modos de autenticación con un solo clic, cupón, cuenta y SMS (integración con Twilio).

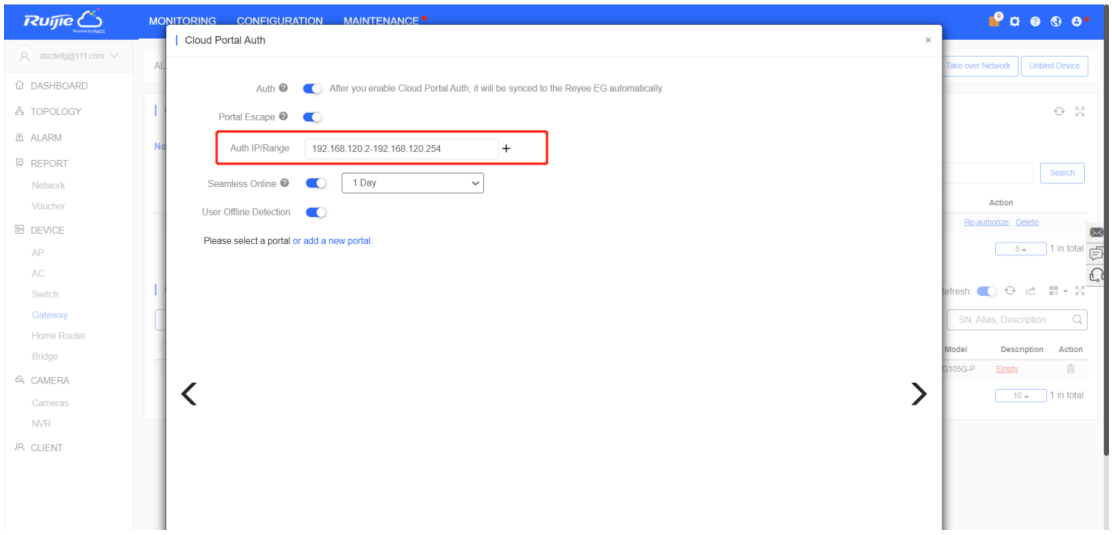
(1) Configure la autenticación de la nube y haga clic en el SN del EG para acceder a su página de detalles.



(2) Seleccione **Config** > **Cloud Portal Auth.**



(3) Ingrese el valor de **Auth IP/Range** para el usuario que requiere autenticarse antes de permitirle el acceso a Internet.

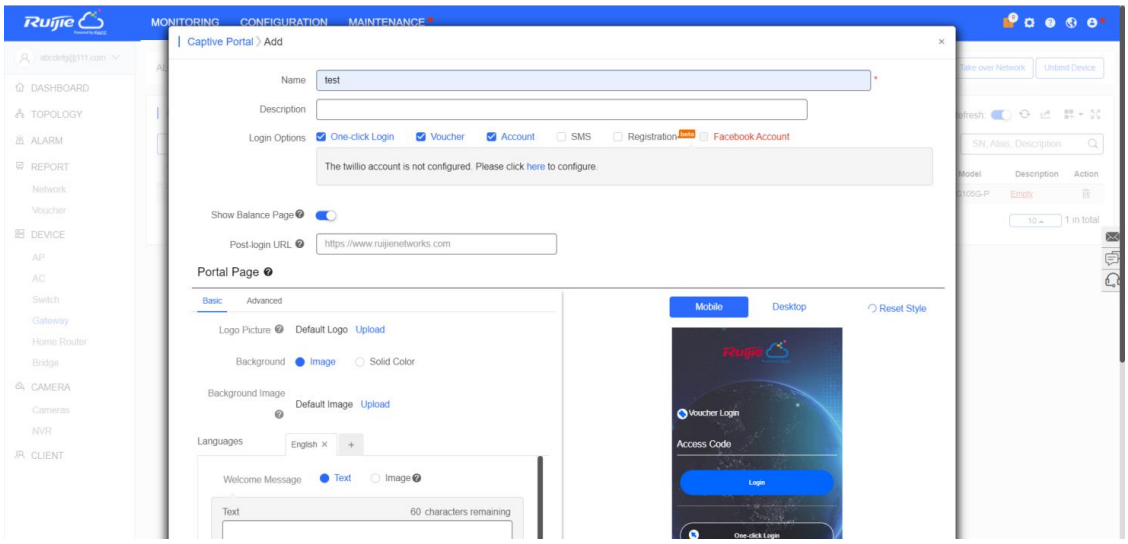


Portal Escape: cuando el servidor de la nube cae, esta función permite que los clientes tengan acceso a Internet directamente, sin autenticación.

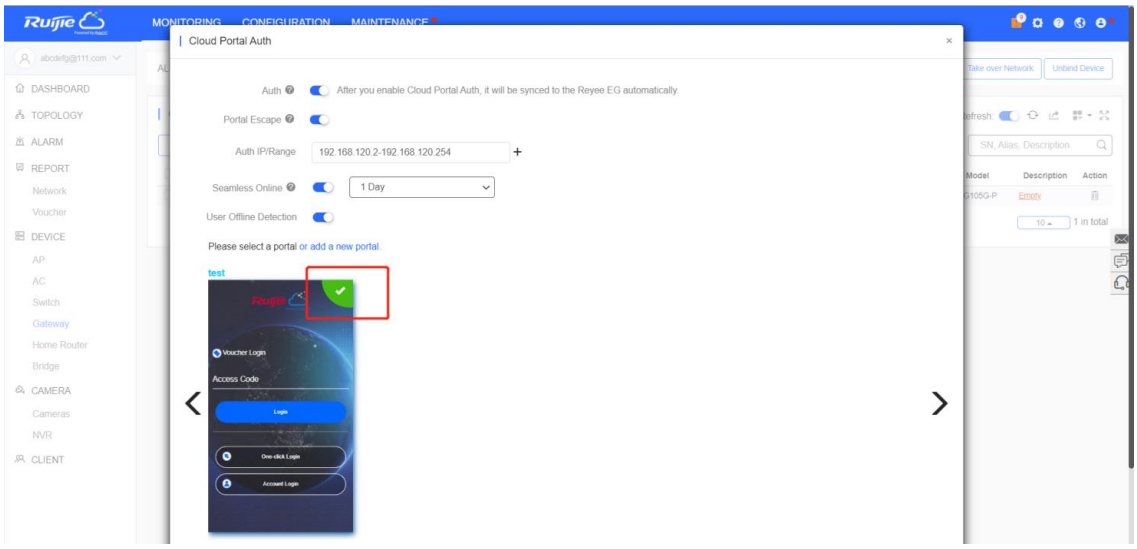
Seamless Online: los usuarios pasan por la autenticación una sola vez. Si desean volver a estar en línea, no requieren pasar por el proceso. Una vez que los usuarios se hayan conectado, no requieren iniciar sesión nuevamente en el periodo especificado. Puede seleccionar **1 Day**, **1 semana**, **1 mes**, o **Siempre**.

User Offline Detection: los usuarios no tendrán acceso a Internet después del plazo especificado.

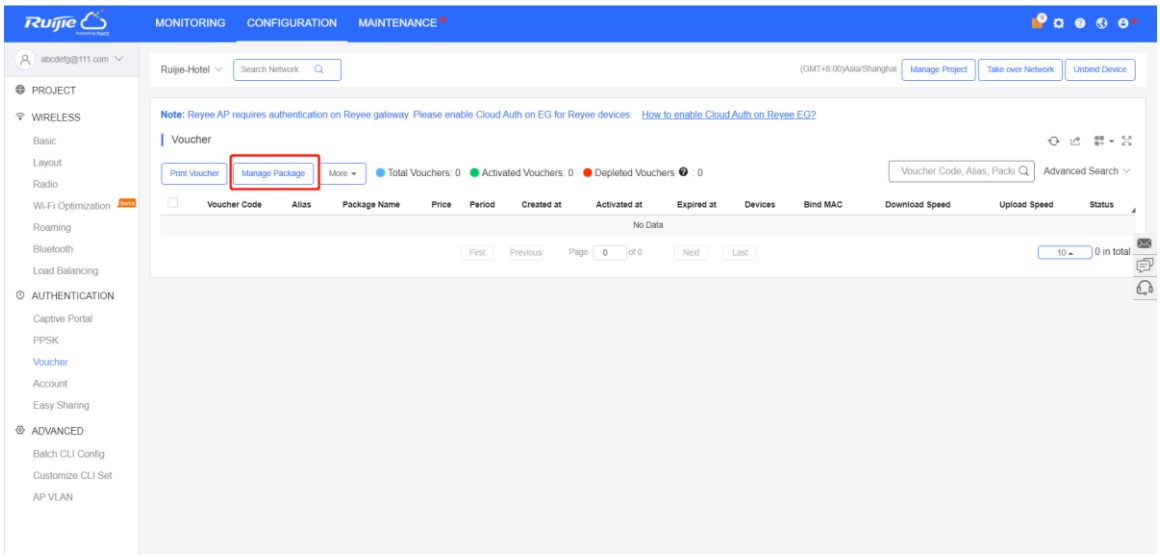
(4) Haga clic en **add a new portal** para añadir una página al portal.



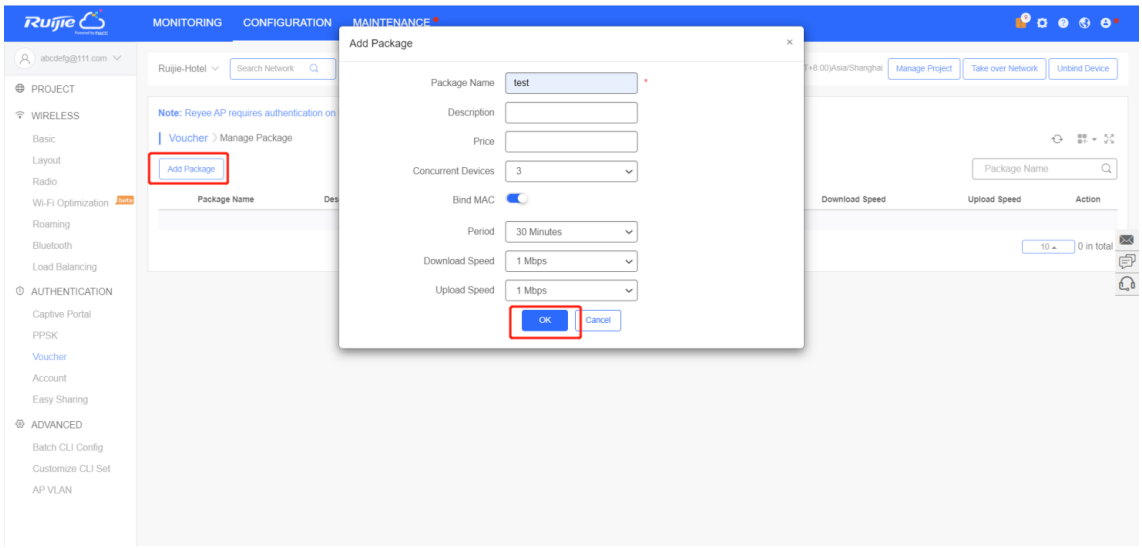
(5) Haga clic en la página del portal para que sea aplicada y luego en **Guardar**.



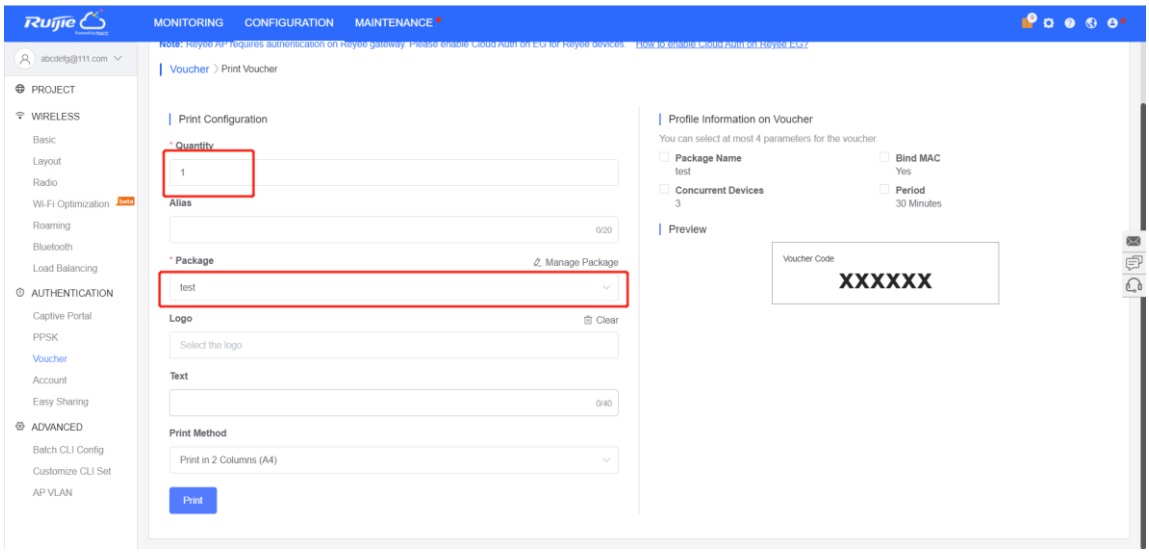
(6) Si utiliza un cupón o una cuenta de autenticación, seleccione **Configuration > Voucher/Account** para añadir un cupón o una cuenta para los clientes. Haga clic en **Manage Package** para añadir un paquete.

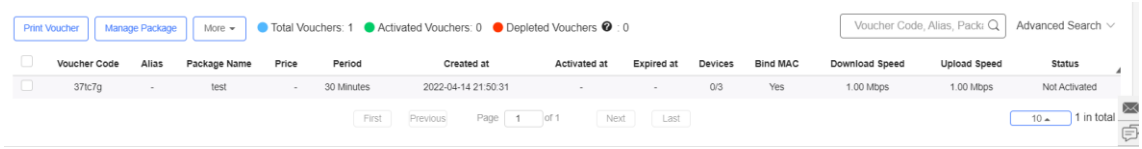


(7) Haga clic en **Add Package** y configure el valor de **Price**, **Concurrent Devices**, **Bind MAC**, **Period**, **Download Speed** y **Upload Speed**.

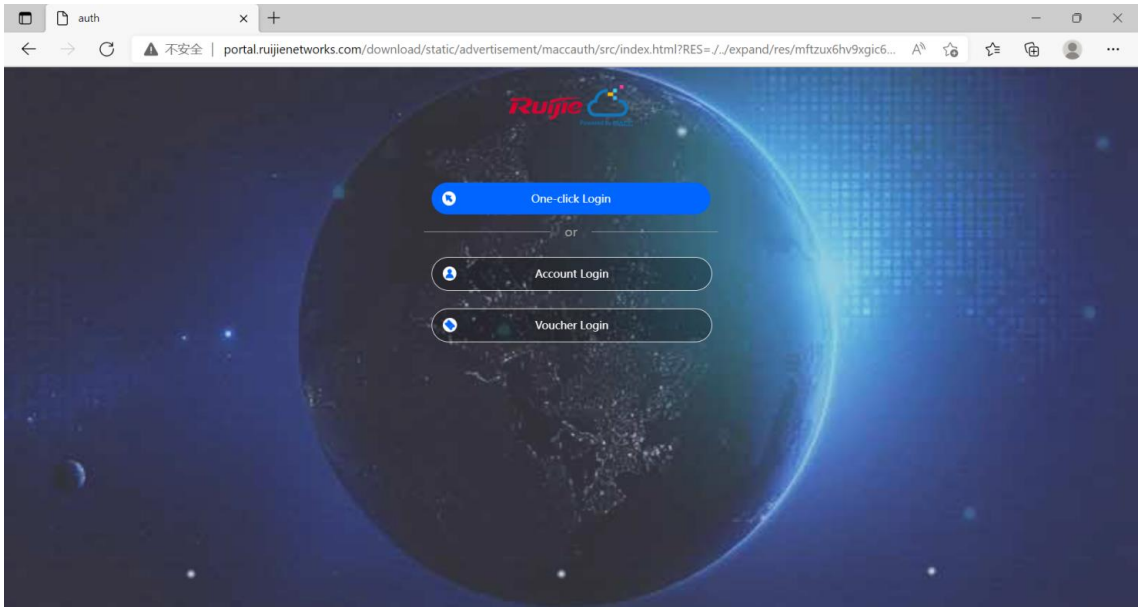


(8) Haga clic en **Print Voucher** para añadir un cupón. Configure el valor de **Quantity** y seleccione el paquete que acaba de añadir. Haga clic en **Print.**





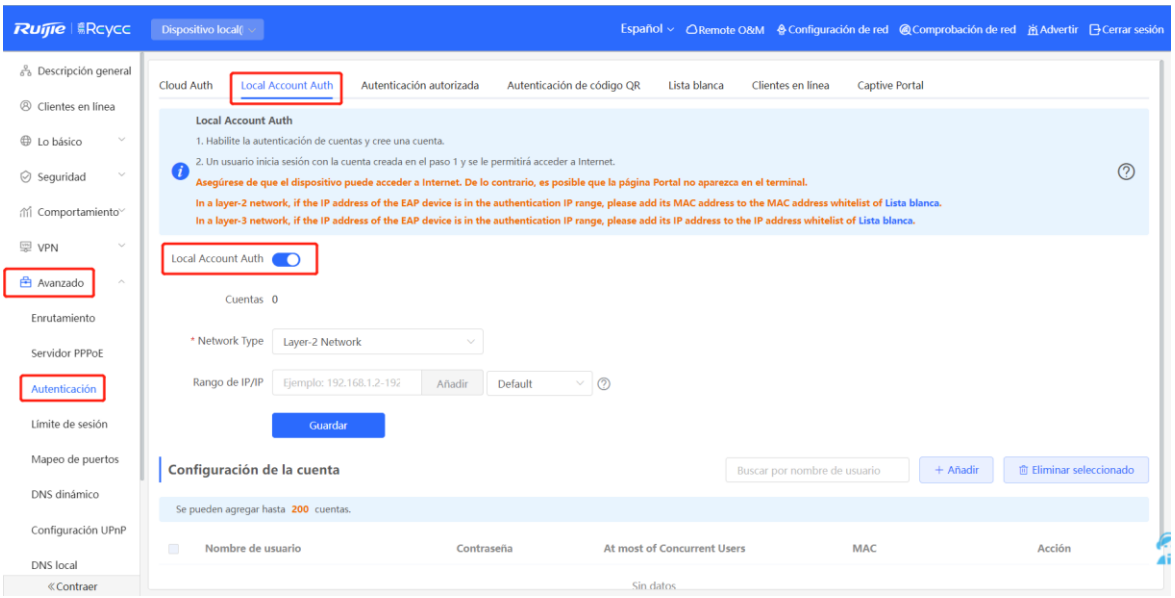
(9) Haga clic en **One-click Login** para iniciar sesión y realizar el proceso de autenticación en la PC.



4.10.3 Autenticación de una cuenta local

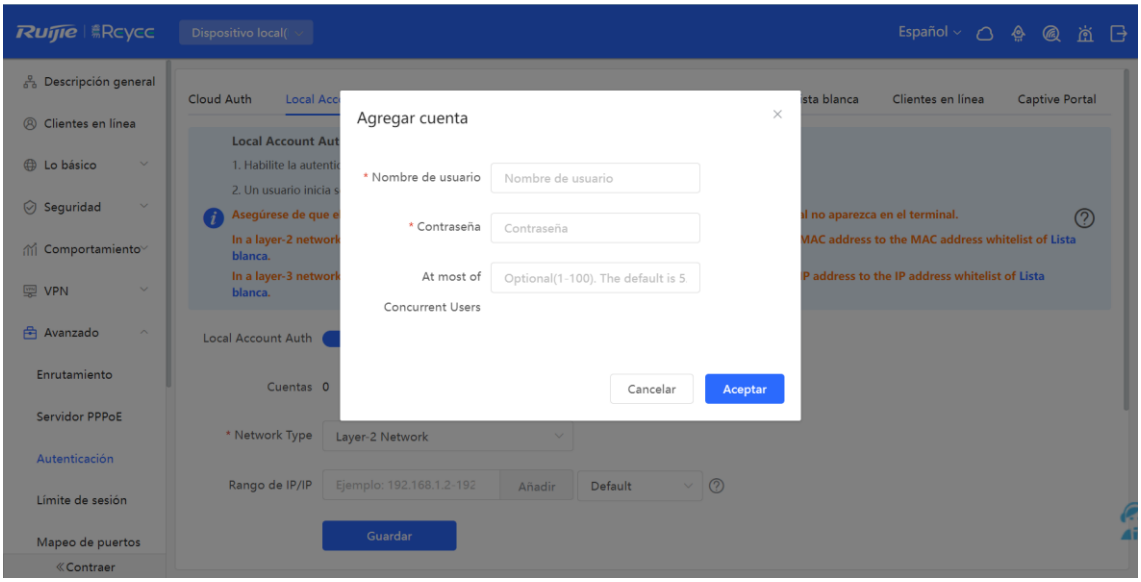
Los dispositivos Reyee EG cuentan con la función de autenticación de cuenta local. Tanto la página como la cuenta del portal se crean localmente.

(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado > Autenticación > Local Account Auth**, habilite la función de autenticación de cuenta local, establezca el valor de **Rango de IP/IP** y haga clic en **Guardar**.



Rango de IP/IP: la dirección IP de un cliente que requiere autenticación. El valor y otras direcciones IP para autenticación no deben superponerse.

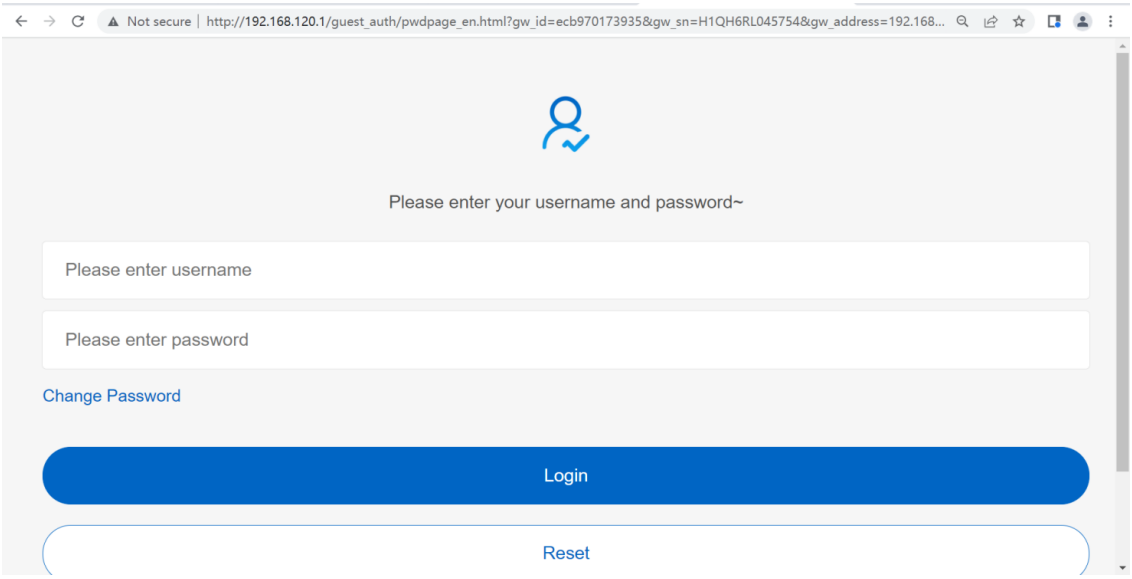
(2) Añada la cuenta que utilizan los clientes. Se pueden agregar como máximo 200 cuentas.



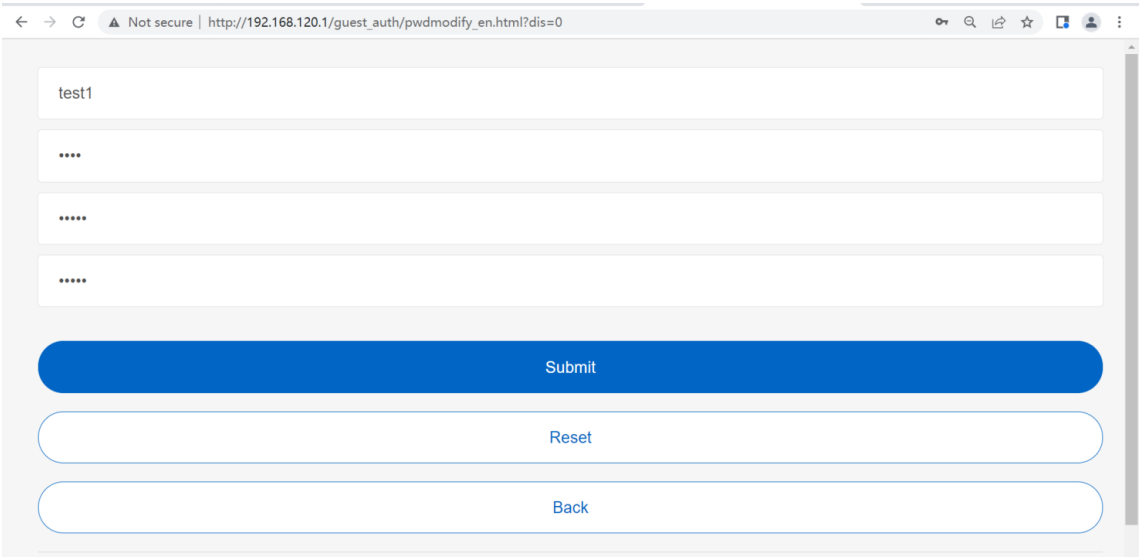
Precaución

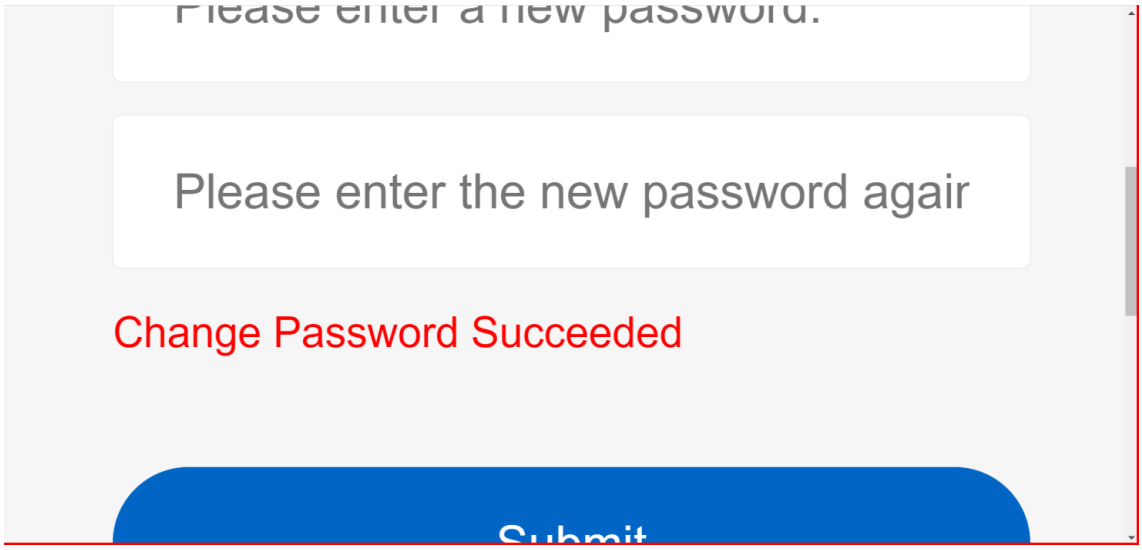
La cuenta puede utilizarse por varios clientes.

(3) Realice el proceso de autenticación en la PC. Normalmente, la página del portal se muestra automáticamente. Si la página no se muestra, ingrese 1.1.1.1 para redirigirse a la página del portal. La página se muestra con base en la configuración del idioma de su navegador.

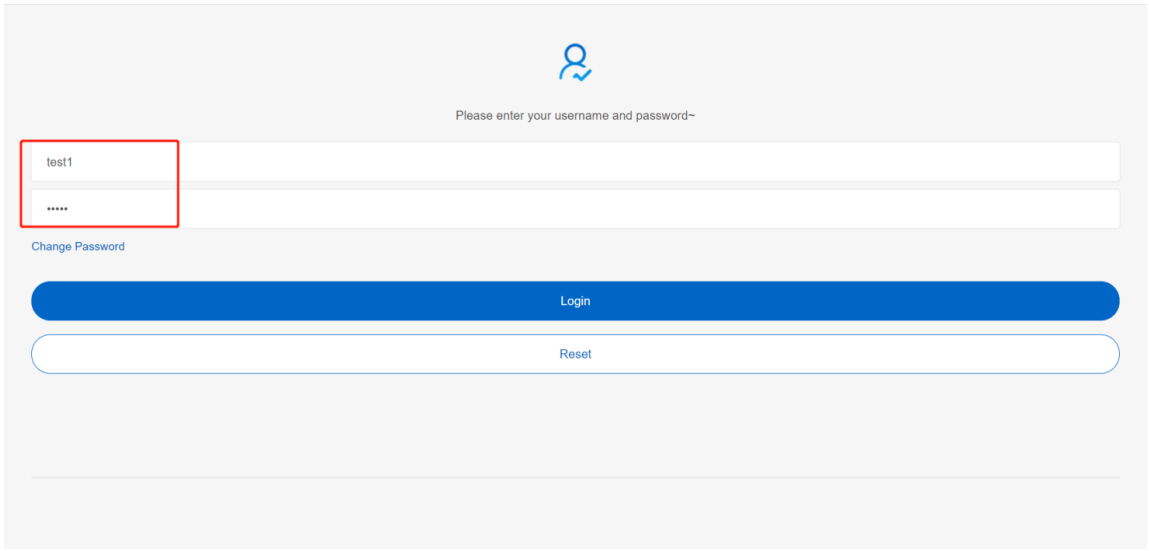


(4) Ingrese **username** y **password**, de acuerdo con la información proporcionada por el gerente. Para cambiar la contraseña, haga clic en **Change Password**.

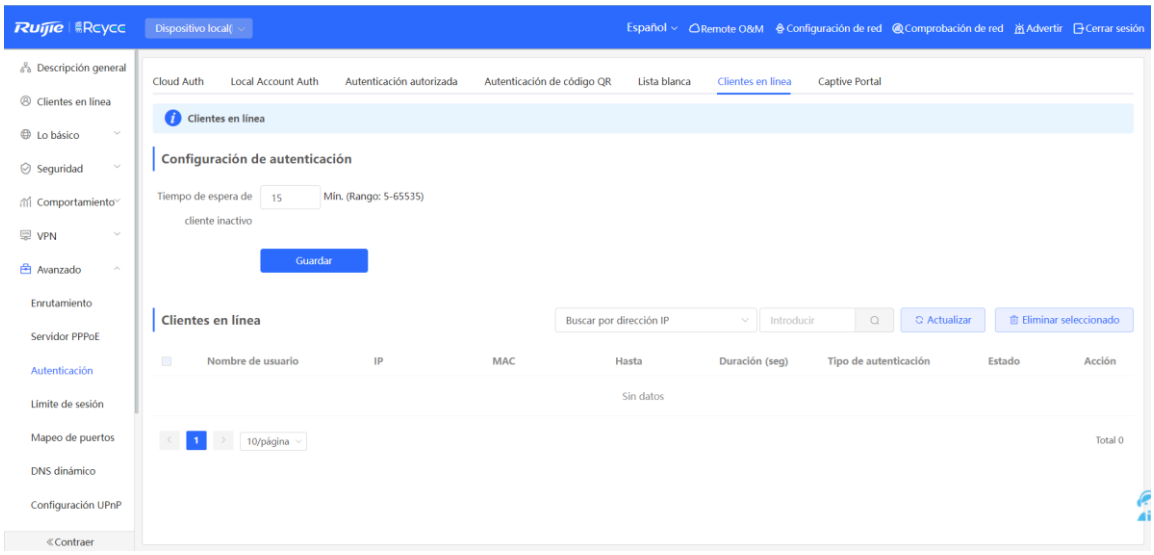




(5) Ingrese el nuevo usuario y contraseña para iniciar sesión. La página aparecerá automáticamente; luego, podrá acceder a Internet.



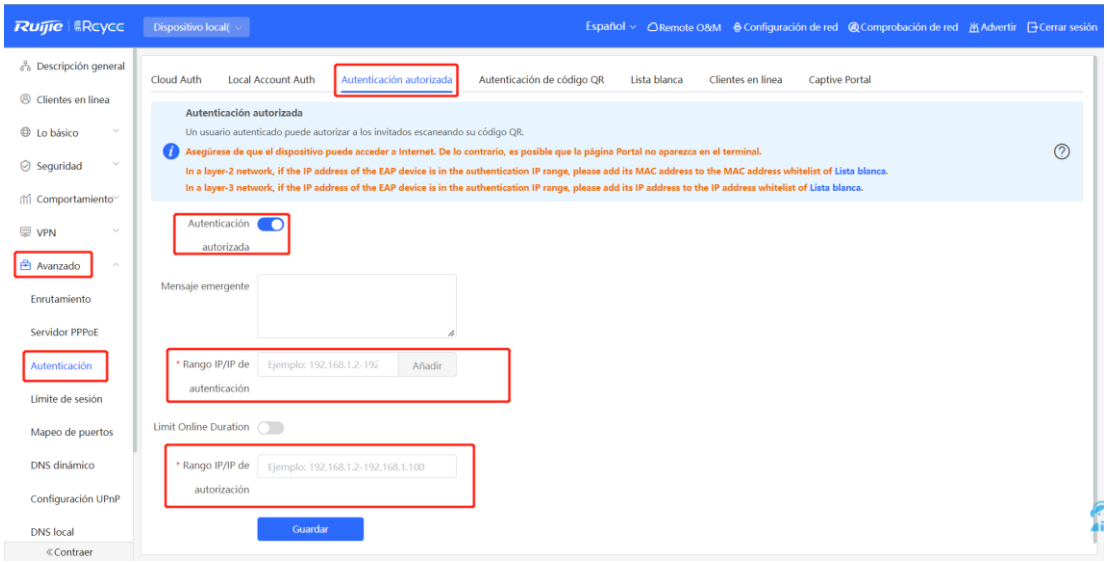
(6) Revise la información en línea en el EG.



4.10.4 Autenticación autorizada

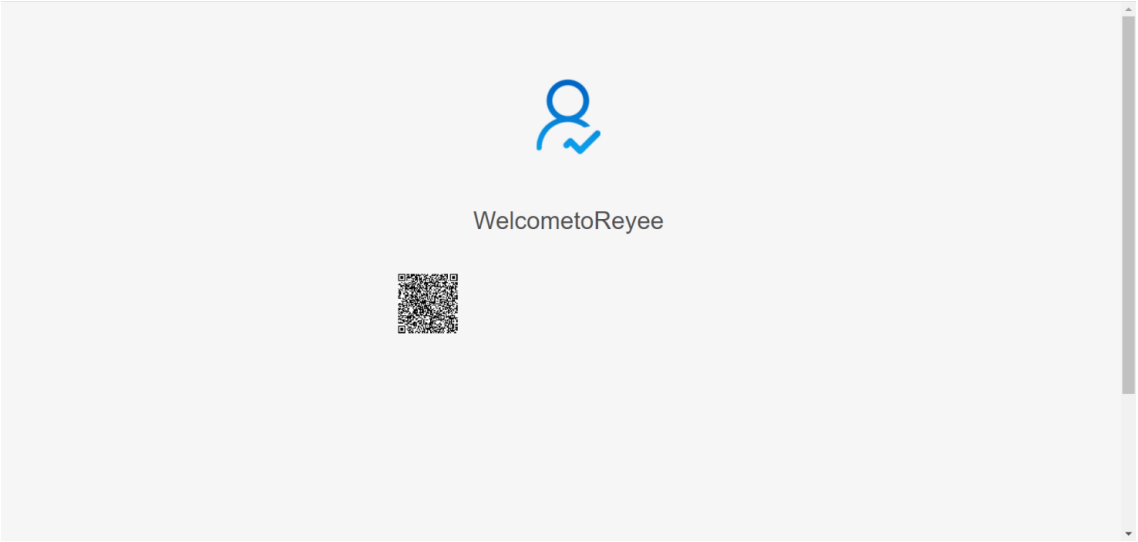
Los dispositivos Reyee EG admiten la función de **Autenticación autorizada**. Cuando esta función se habilita, un usuario autenticado puede autorizar el acceso a invitados por medio de código QR.

(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Autenticación** > **Autenticación autorizada** y habilite **Autenticación autorizada**.

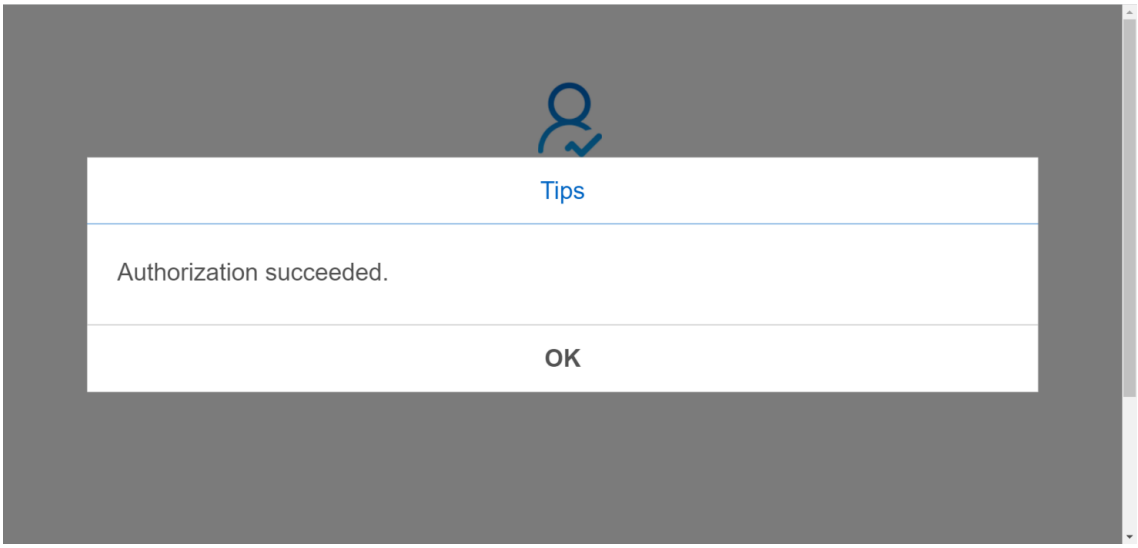


- **Rango IP/IP de autenticación**: indica la dirección IP o rango de direcciones IP de invitados que requieren autenticación.
- **Limit Online Duration**: indica el tiempo que puede permanecer en línea un invitado.
- **Rango IP/IP de autorización**: indica la dirección IP del usuario autenticado.

(2) La siguiente página del portal de autenticación se muestra automáticamente cuando el invitado se conecta a Internet.



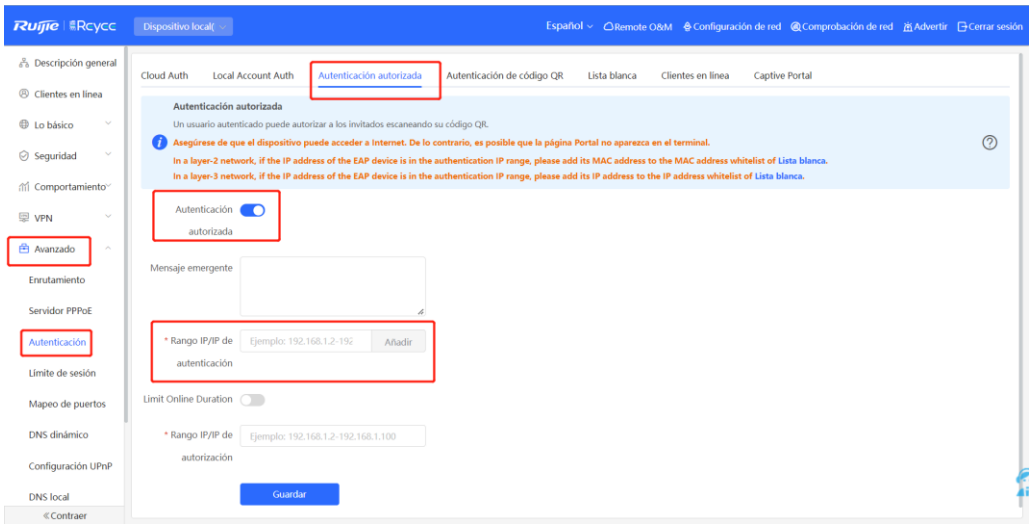
(3) Después de que el cliente autorizado escanea el código QR, el invitado está autorizado para acceder a Internet.



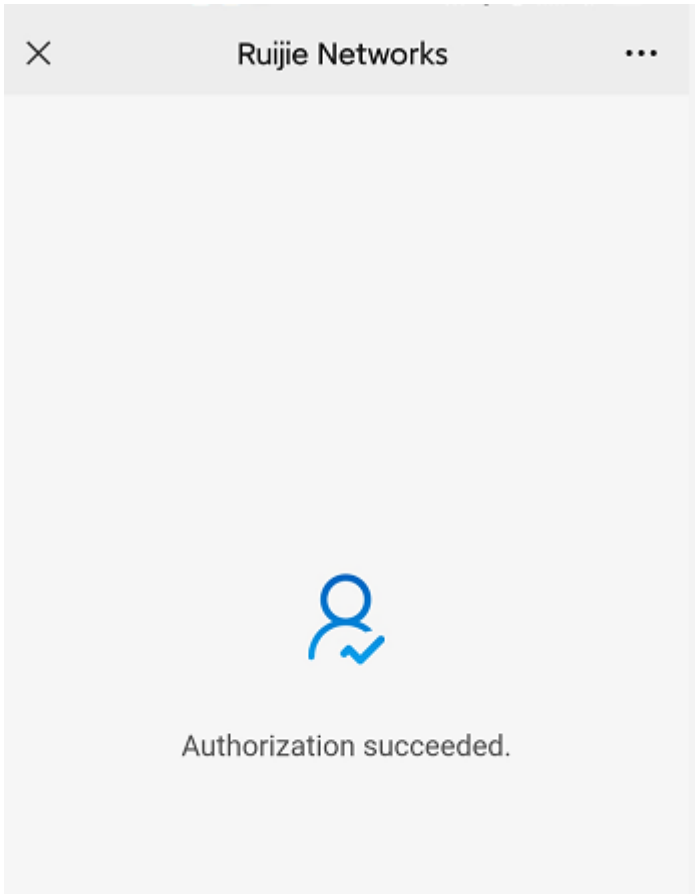
4.10.5 Autenticación a través de código QR

Los dispositivos Reyee EG admiten la autenticación a través de un código QR. Esta función permite que un usuario tenga acceso a Internet cuando escanea el código QR especificado.

(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Autenticación** > **Autenticación de código QR** y habilite **Autenticación de código QR**.



- **Rango IP/IP de autenticación**: indica la dirección IP de un invitado.
- **Limit Online Duration**: indica el tiempo que puede permanecer en línea un invitado.
- **Generador de código QR**: indica el código QR que deben escanear los invitados.

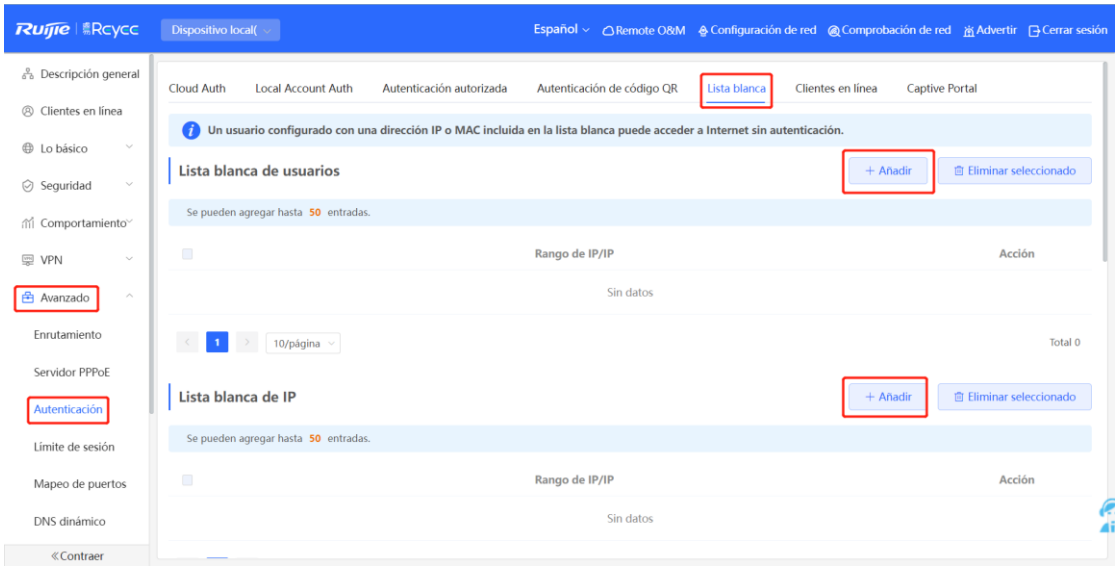


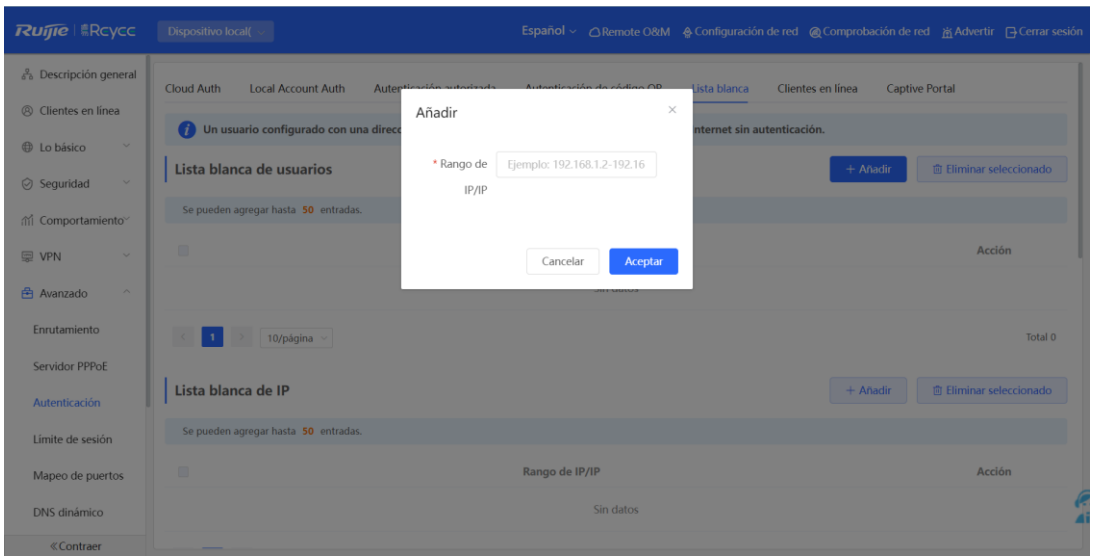
(2) El invitado escanea el código QR y en ese momento tiene acceso a Internet.

4.10.6 Lista blanca

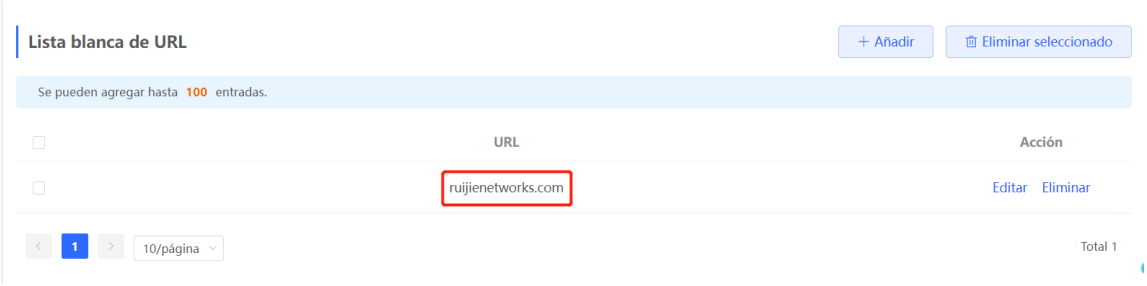
Los usuarios configurados con dirección IP o MAC en la lista blanca tienen acceso a Internet sin la necesidad de autenticación.

(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado > Autenticación > Lista blanca** y añada **Lista blanca de usuarios**, **Lista blanca de IP**, **Lista blanca de URL**, **Lista blanca de MAC** o **Lista negra de MAC**.





- **Lista blanca de usuarios**: indica que los usuarios tienen acceso a Internet sin necesidad de autenticación. Se pueden agregar como máximo 50 entradas.
- **Lista blanca de IP**: indica que los usuarios tienen acceso a la dirección IP externa sin necesidad de autenticación. Se pueden agregar como máximo 50 entradas.
- **Lista blanca de URL**: indica que los usuarios tienen acceso al URL sin necesidad de autenticación. Se pueden agregar como máximo 100 entradas.
- El siguiente URL es el URL predeterminado añadido para la autenticación en la nube.



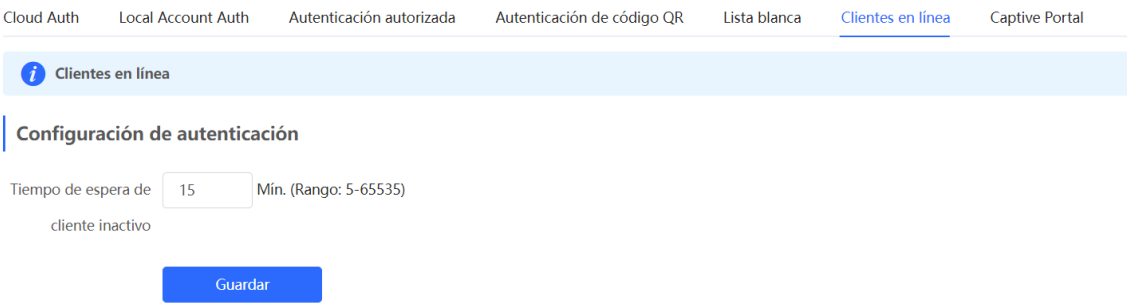
- **Lista blanca de MAC**: indica que los usuarios en la lista blanca de direcciones MAC tienen acceso a Internet sin necesidad de autenticación. Se pueden agregar como máximo 250 cuentas.
- **Lista negra de MAC**: indica que los usuarios en la lista negra de direcciones MAC no tienen acceso a Internet.

4.10.7 Clientes en línea

1. **Configuración del tiempo de espera de cliente inactivo**

   Cambie al modo **Dispositivo local**. Seleccione **Avanzado > Autenticación > Clientes en línea**.

   Puede configurar el tiempo de espera de cliente inactivo. El valor predeterminado es 15 minutos. Si no se detecta ningún tráfico a través del dispositivo de un usuario en línea durante el periodo especificado, este desconectará al usuario. El usuario puede volver a acceder a Internet solo después de autenticarse nuevamente.



   Tiempo de espera de cliente inactivo: el cliente se desconectará después de 15 minutos de inactividad. El rango del valor es de 5 a 65535, en minutos.

2. **Desconexión de un usuario**

   La lista de clientes en línea muestra la información acerca de todos los clientes en línea, incluyendo los de dirección IP, de dirección MAC, la hora de inicio de sesión y el modo de autenticación. Encuentre información del cliente con base en la dirección IP, la dirección MAC o el nombre de usuario. Encuentre al cliente objetivo en la lista de clientes en línea y haga clic en **Eliminar** en la columna **Acción** para borrarlo y finalizar su conexión a Wi-Fi.

4.10.8 Autenticación a través de WeChat

1. Descripción general

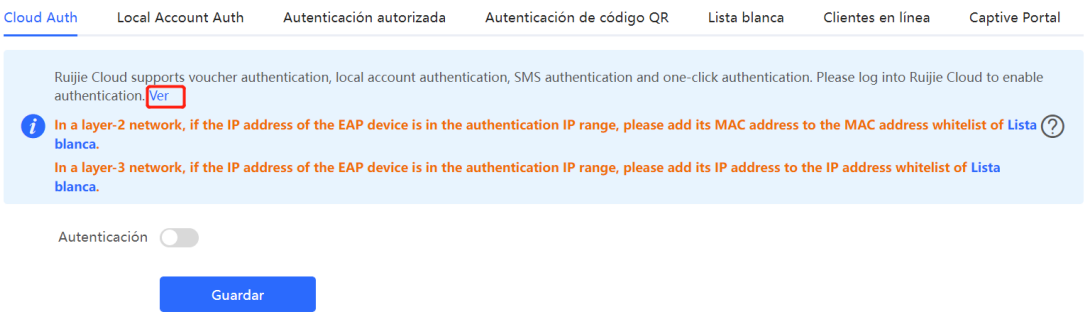
El dispositivo EG se conecta al servidor de autenticación MACC en la nube. Cuando los usuarios de Wi-Fi se conectan, se muestra una página del portal. Los usuarios deben cambiar a WeChat y seguir su cuenta oficial antes de poder tener acceso a Internet. La autenticación a través de WeChat es aplicable en el escenario de centro comercial, donde los vendedores guían a los clientes para seguir sus cuentas oficiales en WeChat mediante la autenticación a través de esta aplicación.

2. Primeros pasos

(1) Conéctese a Wi-Fi a través de WeChat, que es un protocolo de Capa 2. Asegúrese de que el dispositivo de autenticación obtenga las direcciones MAC de los usuarios de conexión inalámbrica.

- La dirección de la puerta de enlace de estos usuarios que requieren autenticación se encuentra en el dispositivo de autenticación.
- Si la dirección de la puerta de enlace no se visualiza en el dispositivo de autenticación, este funciona como servidor DHCP para asignar direcciones IP a los usuarios de conexión inalámbrica y obtener sus direcciones MAC. En este escenario, establezca el valor de **Network Type** en **Red de Capa-3**.

(2) Complete la configuración correspondiente en la plataforma de la cuenta oficial de WeChat y en la de Ruijie Cloud antes de habilitar la autenticación en el dispositivo. Ruijie Cloud admite la autenticación mediante cupón, cuenta local, SMS y con un solo clic. Inicie sesión en Ruijie Cloud para habilitar la función de autenticación.



3. Pasos para la configuración

(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Autenticación** > **Cloud Auth**.

(2) Habilite la autenticación a través de WeChat para tener acceso a Internet.

Habilite la autenticación, configure el **Tipo de servidor** como **Conectar Wi-Fi a través de WeChat**; luego, configure **Network Type**, **Auth Server URL**, **Redireccionamiento IP** y **Escape del cliente**; finalmente, haga clic en **Guardar**.

Tabla 4- 6 Configuración de autenticación a través de WeChat

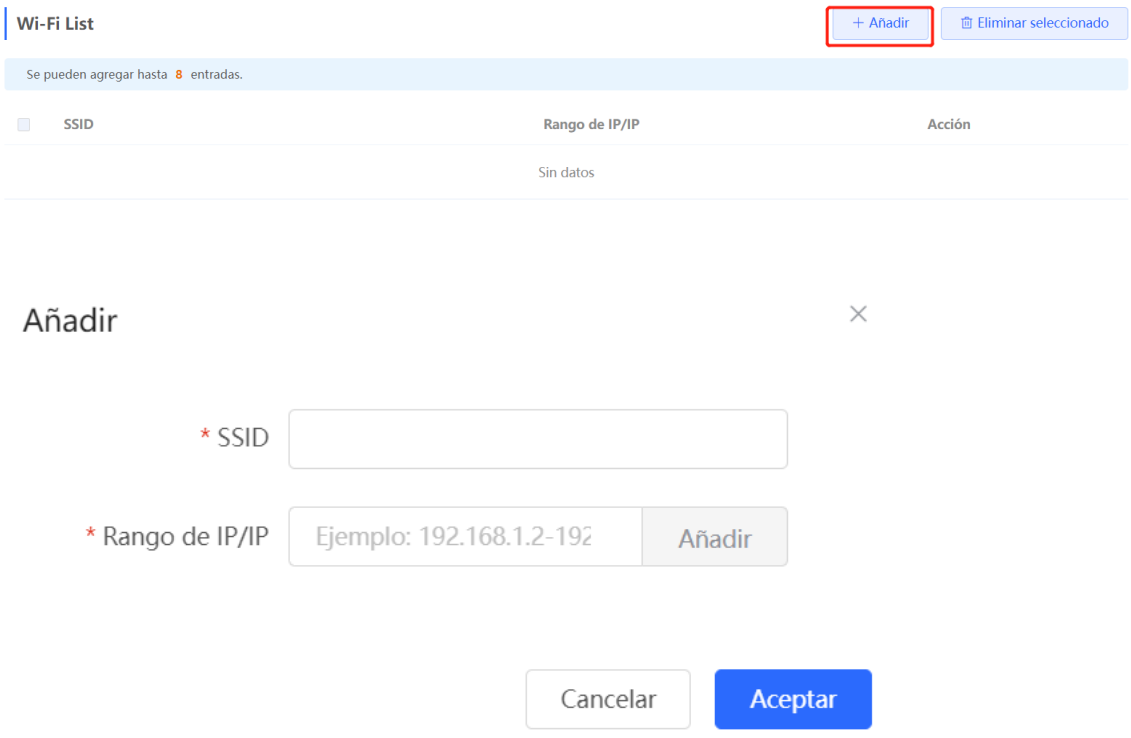
Parámetro	Descripción
Tipo de red	El valor predeterminado es **Layer-2 Network**. Seleccione un tipo de red con base en el ambiente de red actual. La interconexión entre el Wi-Fi y la plataforma WeChat se lleva a cabo en la red de Capa 2. En la red de Capa 3, conecte los dispositivos de enlace descendente al dispositivo de autenticación actual, a través del agente de retransmisión de DHCP, y utilice el grupo de direcciones de DHCP para los segmentos de red ocupados en la autenticación en dicho dispositivo. De este modo, el dispositivo de autenticación obtiene las direcciones MAC de los usuarios de conexión inalámbrica a través de DHCP. En este escenario, configure este parámetro en **Red de Capa-3**.
Tipo de servidor	Seleccione **Conectar Wi-Fi a través de WeChat**.
Auth Server URL	Después de completar la configuración del servidor MACC, este devuelve un URL. El dispositivo envía una solicitud de autenticación a este URL

Parámetro	Descripción
Redireccionamiento IP	El valor corresponde a un menú o una dirección de enlace que se configuró en la cuenta oficial. El valor predeterminado es 118.31.178.137. En la mayoría de los casos, no se requiere cambiar este valor. Cuando un usuario es redirigido a la cuenta oficial de WeChat, requiere visitar esta dirección IP antes de la autenticación posterior.
Escape del cliente	Al habilitar esta función, la función de autenticación en el servidor se deshabilita en caso de que el servidor de autenticación falle, esto es, para que todos los usuarios puedan tener acceso a Internet directamente. Después de arreglar el servidor, la función de autenticación se habilita automáticamente.

(3) Configure el alcance de la autenticación.

Haga clic en **Añadir** en la página actual. En el cuadro de diálogo que aparece, ingrese el SSID y el rango de dirección IP que requiere autenticación y luego, haga clic en **Aceptar**.

Para aquellos clientes (como impresoras, computadoras o algunos usuarios) que no requieren de autenticación, configure el **Rango de IP/IP** como libre de autenticación para que estos clientes tengan acceso directo a Internet.



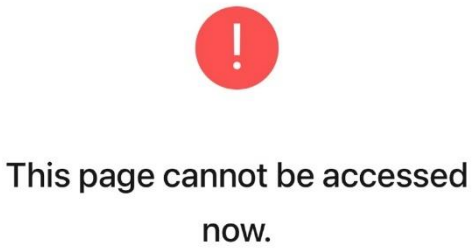
4. Verificación de la configuración

Cuando un teléfono móvil se conecta al Wi-Fi específico, la página de autenticación del portal aparece automáticamente. El usuario visita la página de WeChat, de acuerdo con las instrucciones de la página de

autenticación del portal, sigue su cuenta oficial y hace clic en el menú o enlace de autorespuesta para completar la autenticación. Posteriormente, el usuario puede acceder a Internet de manera normal. Después de completar con éxito la autenticación del usuario, puede ver su información si selecciona **Avanzado** > **Autenticación** > **Clientes en línea**. Para más información, consulte la sección 4.10.7 Clientes en línea.

5. **Resolución de problemas**

   - Cuando un usuario hace clic en el menú o el enlace de autenticación de la cuenta oficial durante la autenticación en WeChat y le aparece el mensaje "**This page cannot be accessed now**", significa que no es posible acceder a la página porque hubo una falla en la autenticación.

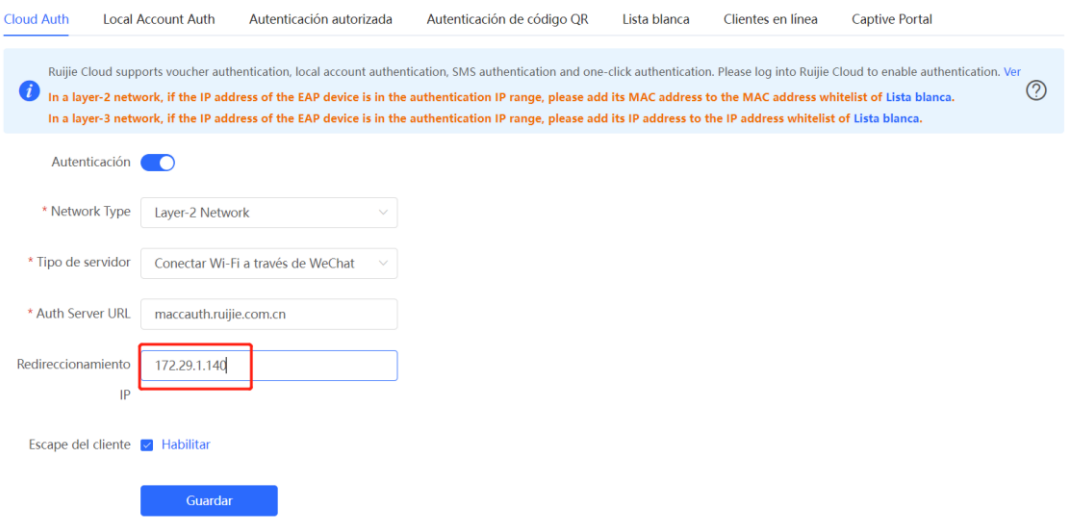


Causa: la dirección de enlace configurada en la entrada de autenticación de la cuenta oficial en la plataforma oficial es considerada no segura por el Centro de Seguridad del cliente de WeChat. Cuando un cliente envía una solicitud a esta dirección, WeChat la bloquea.

Solución: en el menú o enlace de autenticación de la cuenta oficial, cambie la dirección de redirección forzada y la dirección por una dirección IP no utilizada en LAN. Por ejemplo, si el segmento de red 172.29.0.0 en la LAN no se utiliza, configure tanto la dirección IP a la que se redirecciona la cuenta oficial como la dirección del enlace con el segmento 172.29.1.140.

Precaución

Si la dirección IP a la que se redirecciona la cuenta oficial se encuentra en un segmento de red utilizado en la LAN, la autenticación a través de WeChat fallará.



4.10.9 Autenticación a través de WeChat Empresas

1. Descripción general

De manera similar a la autenticación en WeChat, después de conectarse al Wi-Fi, los usuarios deben cambiar a WeChat Empresas y completar la autenticación en el espacio de trabajo correspondiente antes de que puedan tener acceso a Internet. La autenticación en WeChat Empresas se puede utilizar para administrar el acceso a Internet de empleados e invitados en el ámbito empresarial.

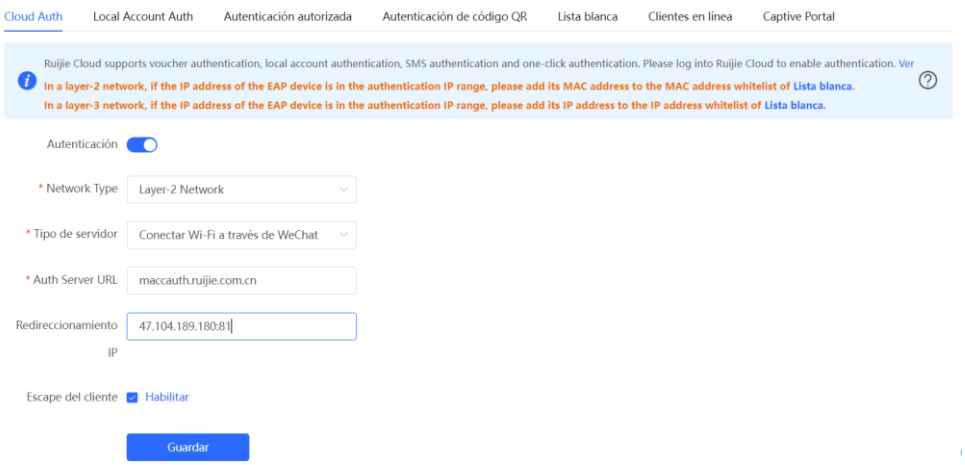
2. Primeros pasos

El procedimiento es el mismo que el de la sección 4.10.8 Autenticación a través de WeChat. Antes de habilitar la autenticación para empresas a través de WeChat, complete las configuraciones principales en su consola y en la plataforma de Ruijie Cloud.

3. Pasos para la configuración

Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Autenticación** > **Cloud Auth**.

Los pasos para la configuración son similares a los de la autenticación en WeChat. La principal diferencia es que la dirección IP para la redirección de la cuenta oficial en el WeChat para empresas debe configurarse en el segmento 47.104.189.180:81. Para más información, consulte la sección 4.10.8 Autenticación a través de WeChat.



Autenticación de empleados

Asegúrese de que los empleados se hayan unido a la organización de WeChat de la empresa. Cuando un empleado conecta un teléfono móvil al Wi-Fi, automáticamente se le redirecciona a WeChat Empresas para realizar la autenticación. Después de abrir WeChat Empresas, el empleado debe ingresar al menú del **Espacio de trabajo** desde la aplicación y hacer clic en la aplicación de autenticación creada por el administrador para obtener un permiso de acceso a Internet. Cuando termina la autenticación, se muestra un mensaje de que se completó exitosamente y el empleado tiene acceso a Internet de forma normal.

En algunos teléfonos móviles, la aplicación de WeChat Empresas no puede iniciar en la página del portal de autenticación debido a una baja compatibilidad. En este caso, los usuarios pueden abrir manualmente WeChat Empresas y continuar el procedimiento.

Autenticación de invitados

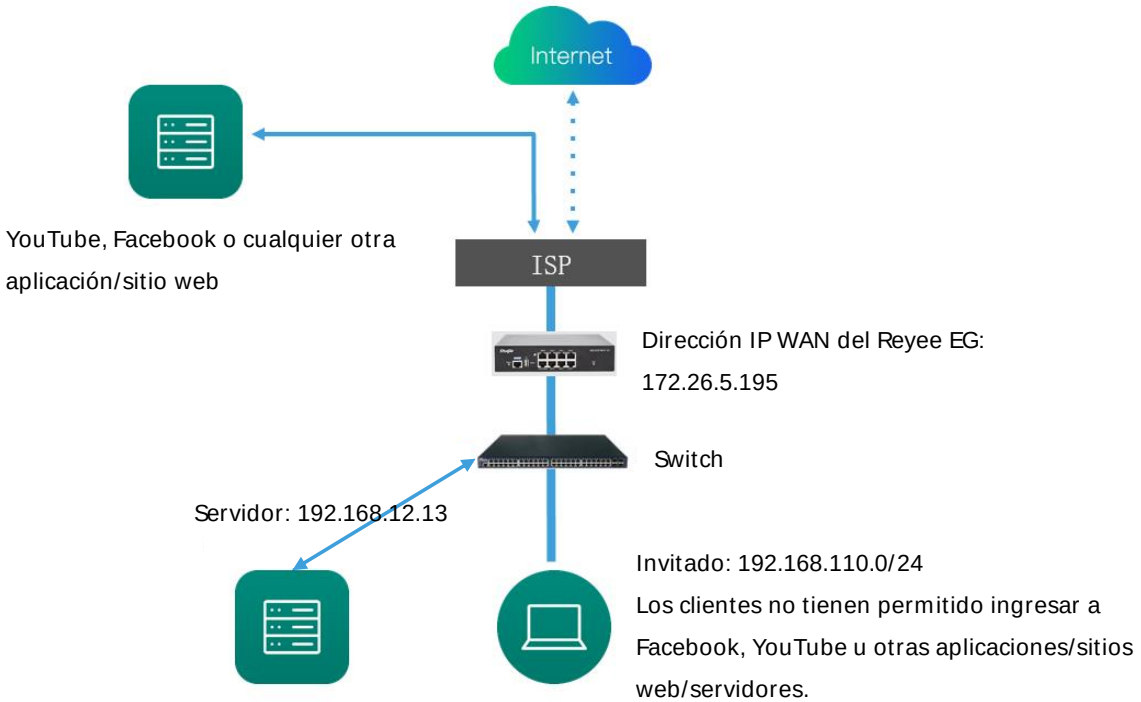
Cuando haya un invitado de visita en una empresa, el empleado puede autorizar su conexión a la red Wi-Fi de la empresa. Cuando el invitado se conecte al Wi-Fi para invitados, aparecerá el código QR para la autenticación. En ese momento, el empleado ya autenticado debe escanear el código QR utilizando WeChat Empresas en su teléfono móvil e ingresar el nombre del invitado. En ese momento, el invitado puede pasar la autenticación y tener acceso a Internet de manera normal.

Para configurar la autenticación de invitados, se necesita configurar al menos dos SSID de Wi-Fi y los segmentos de red correspondientes en la lista de Wi-Fi; estos son utilizados para la conexión de empleados e invitados, respectivamente.

4.11 Comportamiento

4.11.1 Escenario de aplicación

La gestión del comportamiento en línea tiene como objetivo bloquear o prohibir comportamientos específicos durante el acceso a Internet de los usuarios LAN. Esta se clasifica en cinco categorías: control de la aplicación, filtrado de sitios web, gestión de QQ, control de flujo y control de acceso. El rango de efectividad de cada directiva de administración del comportamiento está controlado de manera flexible por la dirección IP del cliente especificado y su tiempo de efectividad.



4.11.2 Control de aplicaciones

El objetivo del control de aplicaciones o apps es controlar el rango de aplicaciones específicas a las que tienen acceso los usuarios. Por defecto, los usuarios pueden ingresar a cualquier aplicación. Cuando se configura una directiva de control de aplicaciones, los usuarios en la red actual no pueden tener acceso a las aplicaciones prohibidas. Esta prohibición se puede basar en un grupo específico de usuarios y un rango de tiempo. Por ejemplo, no está permitido que los empleados ingresen a software de entretenimiento o juegos en la red de la oficina durante las horas de trabajo, con el fin de mejorar la seguridad de la red.

1. Configuración del control de aplicaciones

(1) Cambie al modo **Dispositivo local**. Seleccione **Comportamiento** > **Control de aplicaciones**.

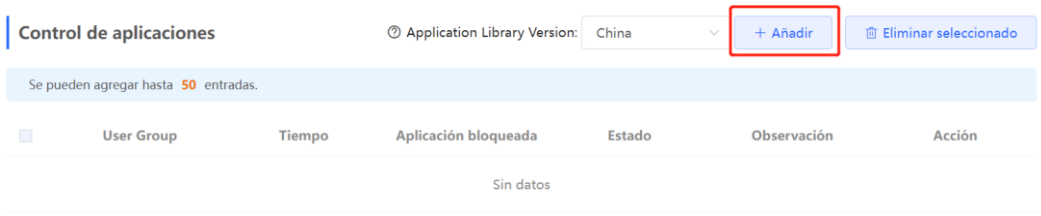
(2) Cambie la biblioteca de aplicaciones.

Las listas de aplicaciones varían dependiendo de la región. Están disponibles tanto la versión china como la versión internacional de la librería de aplicaciones. Seleccione la versión con base en la región.

Haga clic en **Application Library Version** para seleccionarla y luego en **Aceptar**. La versión cambia después de algunos minutos.

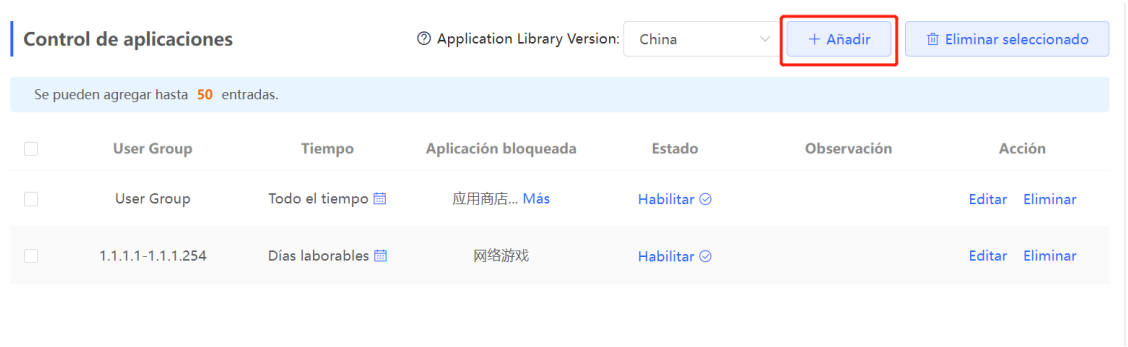
Precaución

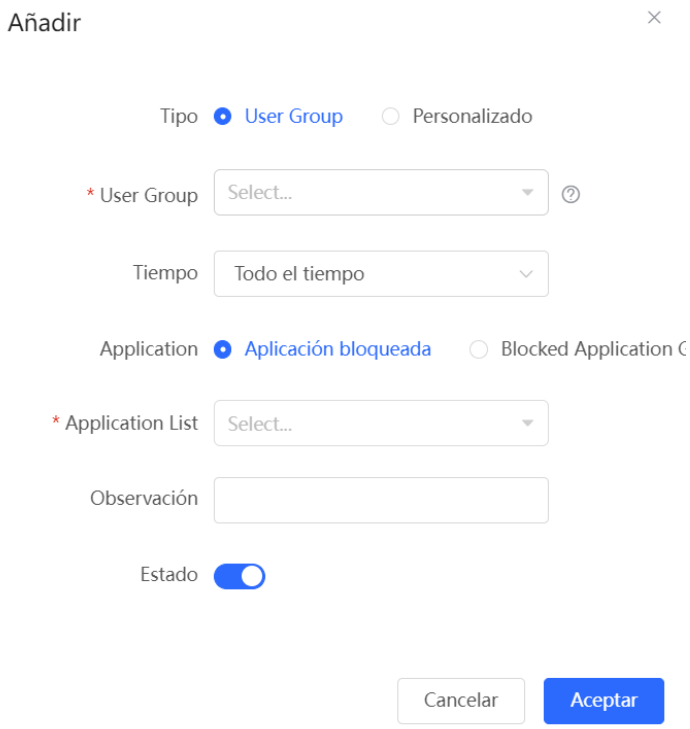
- Cambiar la versión de la biblioteca de aplicaciones tarda aproximadamente un minuto. Por favor, espere.
- Si cambia la biblioteca de aplicaciones, es posible que la antigua directiva aplicada para el control de aplicaciones deje de funcionar. Proceda con precaución al realizar este cambio.



(3) Configure el control de aplicaciones.

Haga clic en **Añadir** para crear una directiva de control de aplicaciones.





Parámetro	Descripción
Tipo	• **User Group**: la directiva es aplicable para los usuarios dentro del grupo de usuarios especificado. Seleccione el grupo de usuarios objetivo. • **Personalizado**: la directiva es aplicable para los usuarios dentro del rango de dirección IP especificado. Ingrese manualmente el rango de la dirección IP gestionada.
Grupo de usuarios	Desde la lista de grupos de usuarios, seleccione a los usuarios administrados por la directiva. Si selecciona a todos los miembros de un grupo de usuarios, la directiva será efectiva para todos ellos y válida para nuevos miembros.
Grupo de direcciones IP	Si el rango de direcciones IP está restringido por la directiva de control de aplicaciones y el tipo de directiva se configura en **Personalizado**, ingrese manualmente el rango.
Tiempo	Especifique el rango de tiempo que estará bajo el control de aplicaciones. En el rango de tiempo especificado, los clientes administrados no podrán tener acceso a aquellas aplicaciones seleccionadas en la lista de aplicaciones prohibidas. Se puede elegir un rango de tiempo de la lista desplegable o seleccionar **Personalizado** y añadir manualmente un rango en específico.
Aplicación bloqueada	Especifique las aplicaciones o grupo de aplicaciones que se bloquearán.

Parámetro	Descripción
Observación	Ingrese la descripción de la directiva.
Estado	Especifique si se habilita la directiva de control de aplicaciones.

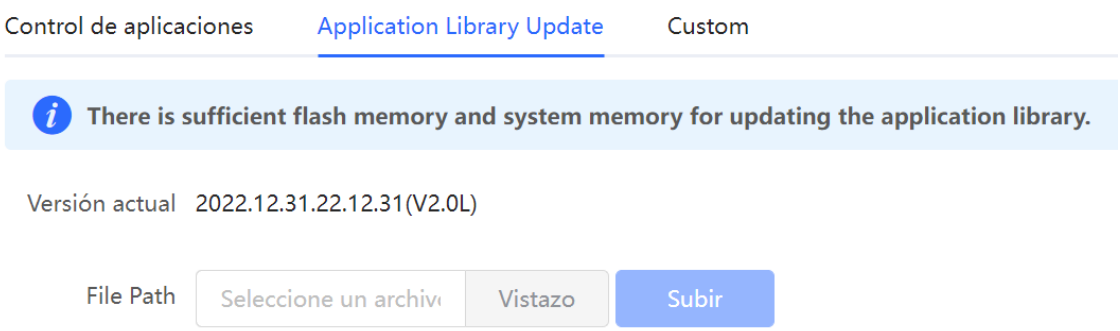
2. Actualización de la biblioteca de aplicaciones

La función de control de aplicaciones depende de la biblioteca de aplicaciones, y la biblioteca de aplicaciones se actualiza con la versión de la aplicación. De ser posible, actualice la biblioteca de aplicaciones a su versión más reciente en la página **Application Library Update**.

(1) Cambie al modo **Dispositivo local**. Seleccione **Comportamiento > Control de aplicaciones > Application Library Update**.

Precaución

- La actualización de la versión de la biblioteca de aplicaciones toma alrededor de 1 minuto para hacerse efectiva. No corte la energía durante la actualización. Puede visualizar la versión actual en la página de la biblioteca de aplicaciones.
- Realice procedimientos subsecuentes basados en la información de la memoria mostrada en la página. Si la memoria resulta insuficiente, se recomienda reiniciar el dispositivo y luego actualizar la biblioteca de aplicaciones.
- Después de la actualización, la directiva original del control de aplicaciones podría dejar de funcionar. Por lo tanto, se recomienda que realice esta operación con precaución.



(2) Haga clic en **Vistazo**. Seleccione un archivo de actualización de la biblioteca de aplicaciones.

(3) Haga clic en **Subir** para cargar el archivo de actualización.

(4) Haga clic en **Aceptar**. Espere a que el sistema complete automáticamente la actualización.

3. Configuración de aplicaciones personalizadas

Con base en el tráfico de paquetes de ciertos sitios web o las aplicaciones que el dispositivo obtenga, los usuarios pueden analizar y extraer información de 5 elementos (protocolo, dirección IP de origen, puerto de

origen, dirección IP de destino y puerto de destino) de los paquetes. Se pueden definir aplicaciones que no estén en la lista predeterminada.

Cuando haya configurado exitosamente las aplicaciones de forma personalizada, configure las directivas en la página de control de aplicaciones para bloquear el acceso de los usuarios a dichas aplicaciones en la red actual.

(1) Cambie al modo **Dispositivo local**. Seleccione **Comportamiento** > **Control de aplicaciones** > **Custom**.

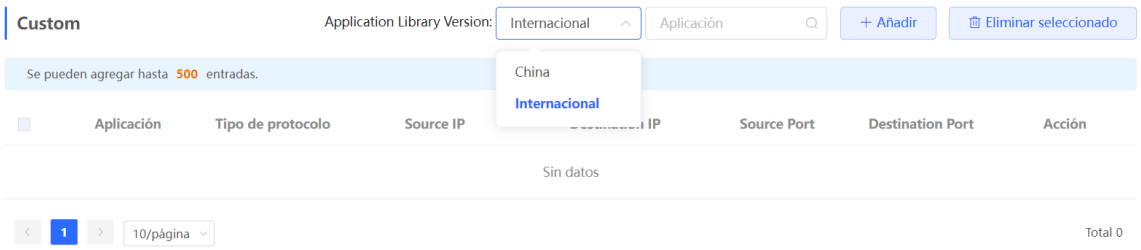
(2) Cambie la biblioteca de aplicaciones.

La lista de aplicaciones varía dependiendo de la región. Están disponibles tanto la versión china como la versión internacional de la librería de aplicaciones. Seleccione la versión con base en la región actual.

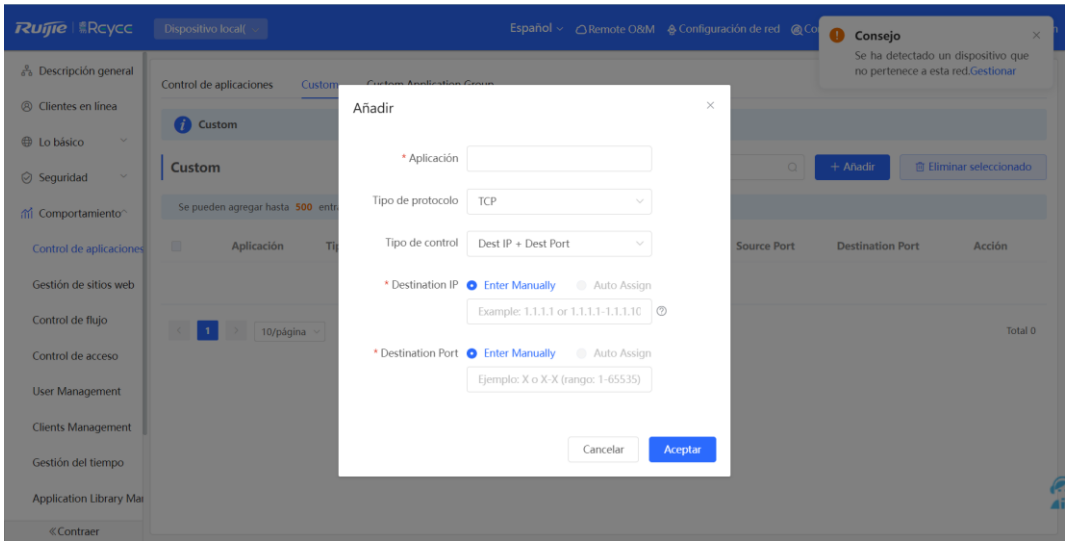
Haga clic en **Application Library Version** y luego seleccione una versión. En el cuadro de diálogo que aparece, haga clic en **Aceptar**. Espere a que el sistema complete el cambio.

Precaución

- La actualización de la versión de la biblioteca toma alrededor de 1 minuto para hacerse efectiva.
- Después de la actualización, la directiva original del control de aplicaciones podría dejar de funcionar. Por lo tanto, se recomienda que realice esta operación con precaución.



(3) Haga clic en **Añadir**. Ingrese la información acerca de una aplicación personalizada.



Parámetro	Descripción
Aplicación	Configure el nombre de la aplicación o app (el nombre debe ser único en la lista de aplicaciones).
Tipo de protocolo	Seleccione el tipo de protocolo con base en el de los paquetes que se obtuvieron. Se puede configurar en TCP, UDP o IP.
Tipo de control	Seleccione el tipo de regla con base en la información extraída de los 5 elementos de los paquetes. Se puede configurar en: **Src IP + Src Port** **Dest IP + Dest Port** **Src IP + Dest IP**
IP de origen/destino	Ingrese la dirección IP de origen/destino.
Puerto de origen/destino	Ingrese el número de puerto de origen/destino.

Nota

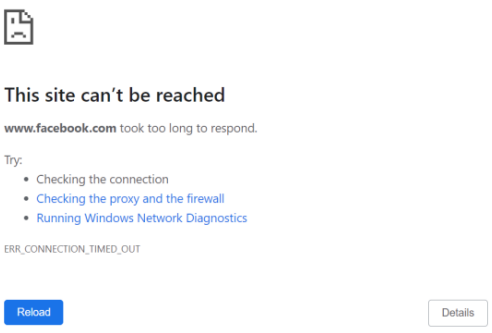
- Si **Tipo de control** se configura en **Src IP + Src Port**, configure la dirección IP de origen y el puerto de origen.
- Si **Tipo de control** se configura en **Dest IP + Dest Port**, configure la dirección IP de destino y el puerto de destino.
- Si **Tipo de control** se configura en **Src IP + Dest IP**, configure la dirección IP de origen y de destino. La dirección IP de origen también puede ser **Auto Assign**.

(4) Haga clic en **Aceptar**.

4. Verifique la configuración

Añada una directiva para bloquear el acceso a Facebook y YouTube de acuerdo con 1. Configuración del control de aplicaciones.

Intente ingresar a Facebook en una PC de invitado y confirme que no le permite el acceso.



4.11.3 Administración de sitios web

La administración de sitios web consiste en agruparlos y filtrarlos. Agrupar los sitios web se refiere a clasificar sus URL. Los grupos existentes se pueden modificar o también se pueden crear otros. Filtrar los sitios web se refiere a controlar el acceso a grupos de sitios web existentes para prohibir a los usuarios el acceso a grupos en específico. El filtrado se puede aplicar con base en un grupo específico de usuarios y un rango de tiempo. Por ejemplo, no está permitido que los empleados ingresen a software de entretenimiento o juegos en la red de la oficina durante las jornadas laborales, con el fin de mejorar la seguridad de la red.

(1) Cambie al modo **Dispositivo local**. Seleccione **Comportamiento > Gestión de sitios web**.

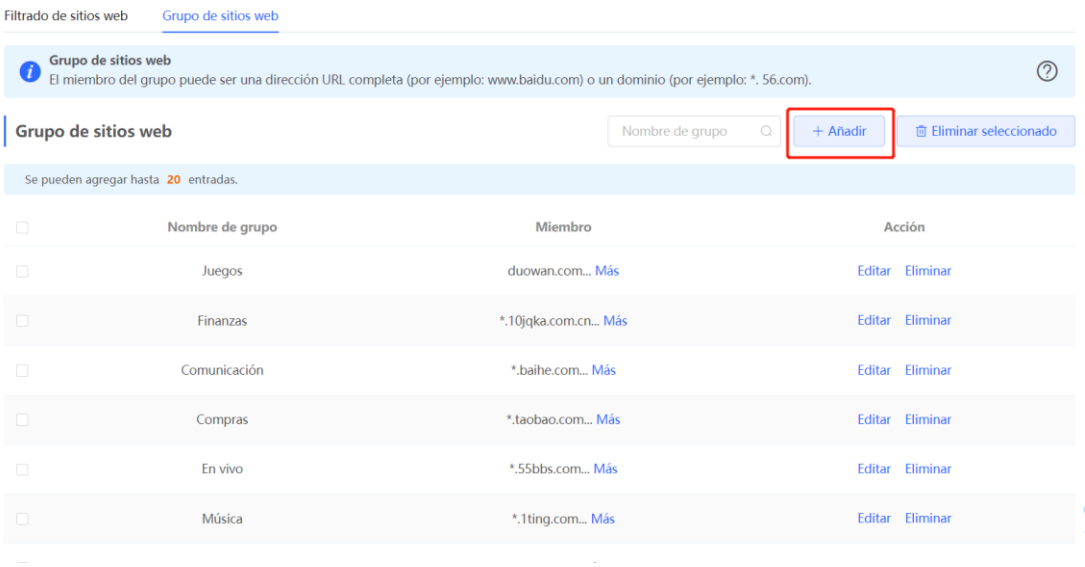
(2) Configure los grupos de sitios web.

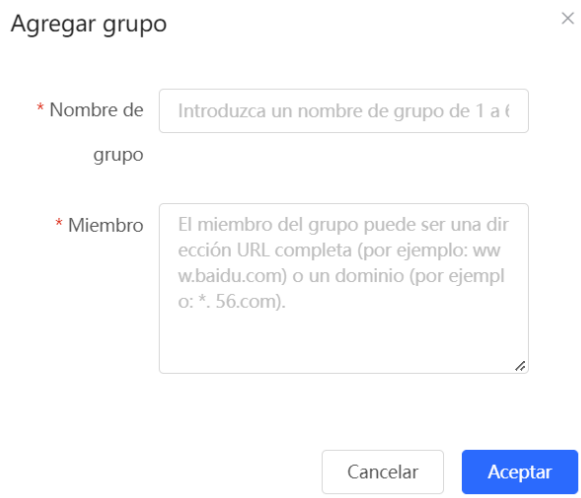
a Haga clic en la pestaña **Grupo de sitios web**. En la página que aparece, visualizará en la lista todos los grupos de sitios web creados. Encuentre el grupo objetivo y haga clic en **Más** en la columna **Miembro** para visualizar todos los URL de los sitios web en el grupo. Encuentre el grupo objetivo y haga clic en **Editar** en la columna **Acción** para modificar los URL de los sitios web miembros. Encuentre el grupo objetivo y haga clic en **Eliminar** en la columna **Acción** para borrarlo.

b Haga clic en **Añadir** para crear un nuevo grupo.

Precaución

Si la regla de filtrado en un grupo de sitios web es referenciada, el grupo no podrá borrarse de la lista. Para borrarlo, modifique la configuración de filtrado de sitios web para quitar la referencia relacionada primero.





Parámetro	Descripción
Nombre de grupo	Configure un nombre único para un grupo de sitios web. El nombre debe estar formado por una cadena de 1 a 64 caracteres.
Miembro	Especifique los miembros en el grupo de sitios web. Puede ingresar varios sitios web por lote. Cada miembro del grupo puede ser un URL completo (como www.baidu.com) o una palabra clave (nombre del dominio con un comodín en el frente, como *.baidu.com). El comodín solo puede aparecer al principio del URL y no puede estar en medio o al final del nombre del dominio.

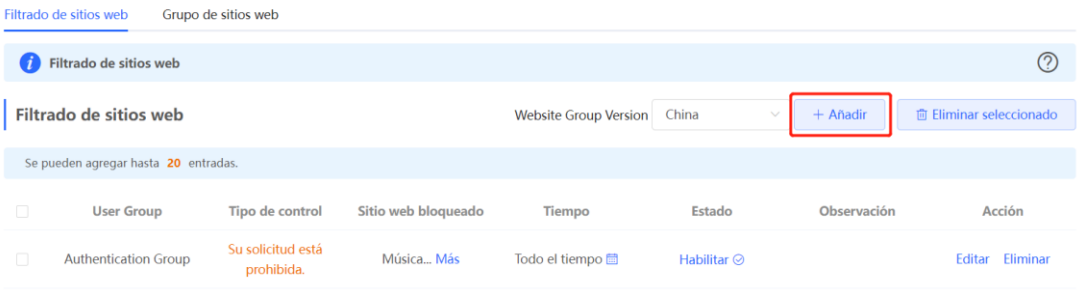
(3) Configure el filtrado de sitios web.

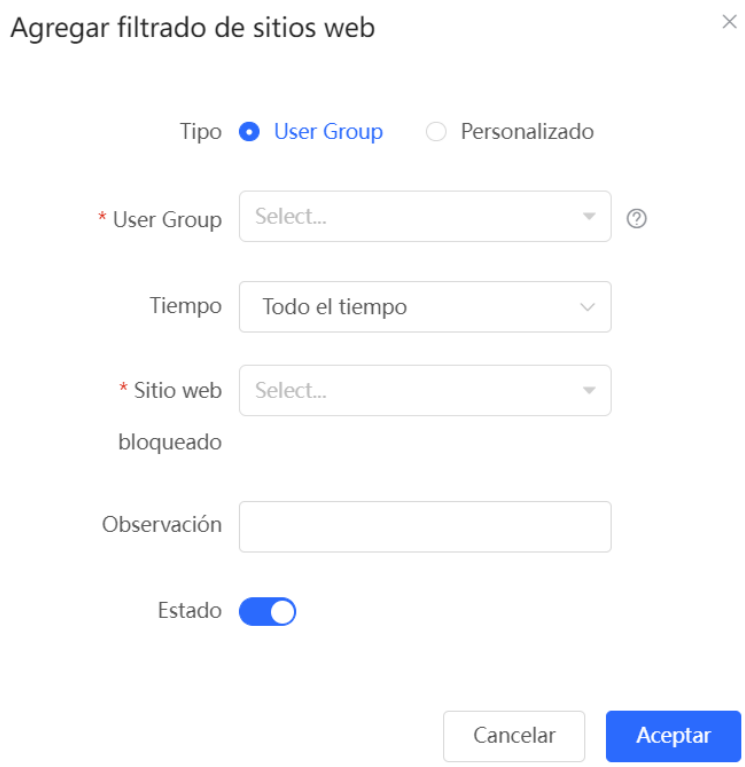
Cambie al modo **Red**.

a Seleccione **Gateway > Comportamiento > Gestión de sitios web > Filtrado de sitios web**.

b Haga clic en la pestaña de **Filtrado de sitios web**. En la página que aparece, todas las reglas de filtrado de sitios web se muestran en la lista. Haga clic en **Editar** para modificar la información de una regla y en **Eliminar** para borrar alguna en específico.

c Haga clic en **Añadir** para crear una regla de filtrado de sitios web.



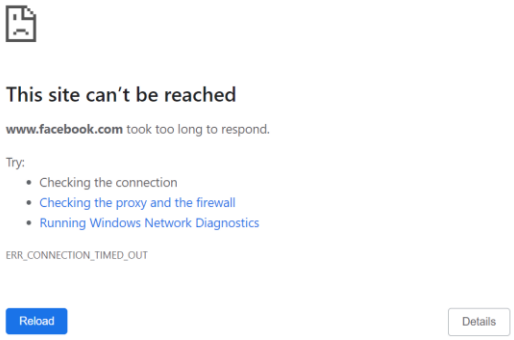


Parámetro	Descripción
Tipo	● **User Group**: la directiva es aplicable para los usuarios dentro del grupo de usuarios especificado. Seleccione un grupo de usuarios objetivo. ● **Personalizado**: la directiva es aplicable para los usuarios dentro del rango de dirección IP especificado. Ingrese manualmente el rango de la dirección IP gestionada.
Grupo de usuarios	Desde la lista de grupos de usuarios, seleccione a los usuarios administrados por la directiva. Si selecciona a todos los miembros de un grupo de usuarios, la directiva será efectiva para todos ellos y válida para nuevos miembros.
Grupo de direcciones IP	Si el rango de direcciones IP está restringido por la directiva de control de aplicaciones y el tipo de directiva se configura en **Personalizado**, ingrese manualmente el rango.
Tiempo	Especifique el rango de tiempo en el que estará bajo el control del filtrado de sitios web. En el rango de tiempo especificado, los clientes administrados no podrán tener acceso a los sitios web prohibidos. Se puede elegir un rango de tiempo de la lista desplegable o seleccionar **Personalizado** y añadir manualmente un rango en específico.
Sitio web bloqueado	Configure el tipo de sitios web que deben ser bloqueados. Puede elegir un grupo existente. Después de seleccionar un grupo, los usuarios no podrán

Parámetro	Descripción
	acceder a los sitios web que se encuentran en este grupo.
Observación	Ingrese la descripción de la regla.
Estado	Especifique si se habilita la regla de filtrado de sitios web.

d Haga clic en **Aceptar**.

(4) Intente ingresar a Facebook en una PC de invitado. Podrá confirmar que el acceso está restringido.



4.11.4 Control de acceso

El control de acceso permite que el dispositivo empareje los paquetes de datos que pasan a través de él con base en reglas específicas y que permita o descarte paquetes de datos durante el rango de tiempo especificado. Esta función controla si se permite que los usuarios LAN tengan acceso a Internet o si se bloquea un flujo de datos específico. El dispositivo encuentra las coincidencias de los paquetes con base en la dirección MAC o IP.

(1) Cambie al modo **Dispositivo local**. Seleccione **Comportamiento** > **Control de acceso**.

La lista de reglas de control de acceso muestra las reglas creadas. Haga clic en **Añadir** para añadir una regla de control de acceso.

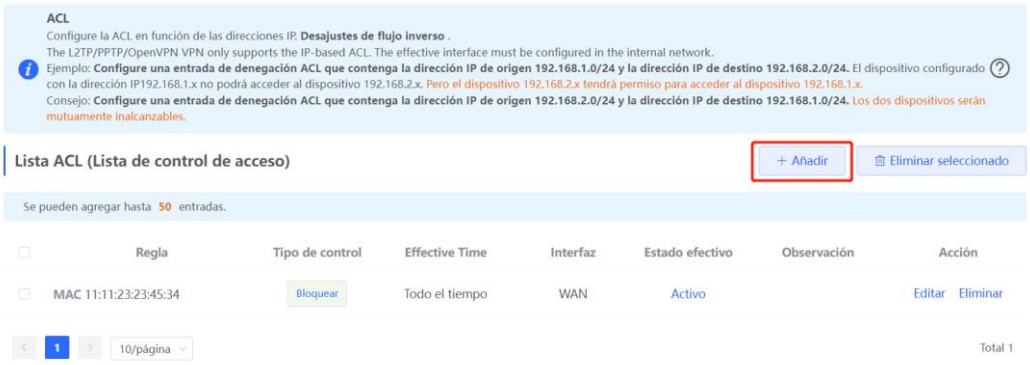


Tabla 4- 9 Información sobre las reglas de control de acceso

Parámetro	Descripción
Estado efectivo	Indique si una regla se hace efectiva. Si se muestra **Inactivo**, el tiempo actual del sistema puede no estar en el rango de tiempo efectivo. Mueva el cursor a  para visualizar los detalles de la causa.
Orden de coincidencia	En la Lista ACL se muestran todas las reglas de control de acceso creadas, con la más reciente clasificada en primer lugar. El dispositivo busca coincidencias con las reglas de acuerdo con su clasificación en la lista. La secuencia de coincidencia de la regla se puede ajustar manualmente haciendo clic en o en la lista.
Acción	La regla se puede editar o eliminar.

(2) Configure una regla ACL con base en una dirección MAC.

Las reglas ACL basadas en direcciones MAC habilitan al dispositivo para que encuentre las coincidencias de los paquetes de datos con base en la dirección MAC de origen y se utilizan generalmente para controlar el acceso a Internet de los usuarios en línea o de clientes específicos.

En el parámetro **Basado en**, configure **MAC**, ingrese la dirección MAC del cliente y seleccione un tipo de regla, configure el rango de tiempo efectivo y haga clic en **Aceptar**.

Nota

Por defecto, las reglas ACL basadas en direcciones MAC son válidas en puertos WAN.

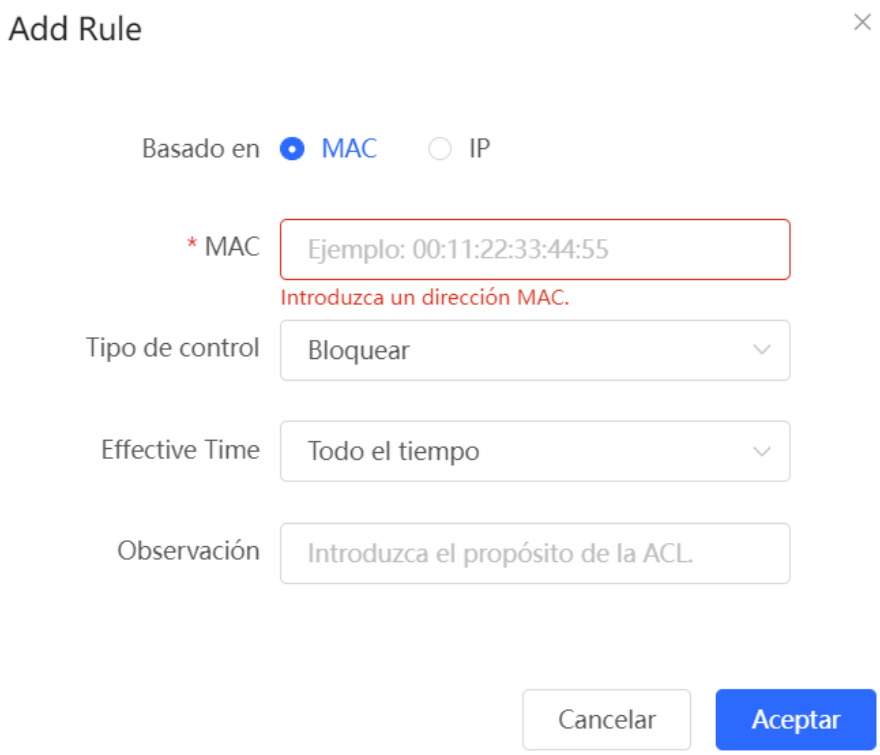


Tabla 4- 10 Configuración de ACL basadas en direcciones MAC

Parámetro	Descripción
MAC	Ingrese la dirección MAC del cliente que debe estar controlada por la regla ACL. Cuando haga clic en el campo de la entrada, se mostrará la información del cliente actual. Haga clic para ingresar automáticamente la dirección MAC correspondiente.
Tipo de control	Especifique el método de procesamiento de las condiciones relativas a la coincidencia de los paquetes de datos. ● Permitir: otorga permiso a los paquetes de datos que coincidan con las condiciones. ● Bloquear: descarta los paquetes de datos que coincidan con las condiciones.
Tiempo efectivo	Se puede elegir un rango de tiempo de la lista desplegable o seleccionar **Personalizado** y añadir manualmente un rango en específico.
Observación	Ingrese la descripción de la regla, la cual se utiliza únicamente para identificarla.

(3) Configure una regla ACL basada en una dirección IP.

Las reglas ACL basadas en direcciones IP permiten que el dispositivo encuentre coincidencias en los flujos de datos con base en la dirección IP de origen, la dirección IP de destino y el número de protocolo.

Configure **Basado en** con el valor **IP**, ingrese la dirección IP y puerto del flujo de datos de origen, así como la dirección IP y puerto del flujo de datos de destino, seleccione el tipo de protocolo y de regla, el rango de tiempo y el puerto efectivos; luego, haga clic en **Aceptar**.

Precaución

Las reglas ACL basadas en direcciones IP se hacen efectivas solamente en una dirección. Por ejemplo, en una regla que define **Bloqueado**, el segmento de la dirección IP de origen es 192.168.1.0/24 y el segmento de la IP de destino es 192.168.2.0/24. Con base en esta regla, el dispositivo en 192.168.1.x no puede acceder al dispositivo en 192.168.2.x, pero el dispositivo en 192.168.2.x sí puede acceder al dispositivo en 192.168.1.x. Para bloquear el acceso bidireccional en este segmento de red, configure otra regla de bloqueo con el segmento 192.168.2.0/24 de la dirección IP de origen y el segmento 192.168.1.0/24 de la dirección IP de destino.

La VPN L2TP y la VPN PPTP solo admiten el control de acceso basado en direcciones IP y los puertos efectivos deben estar en la LAN.

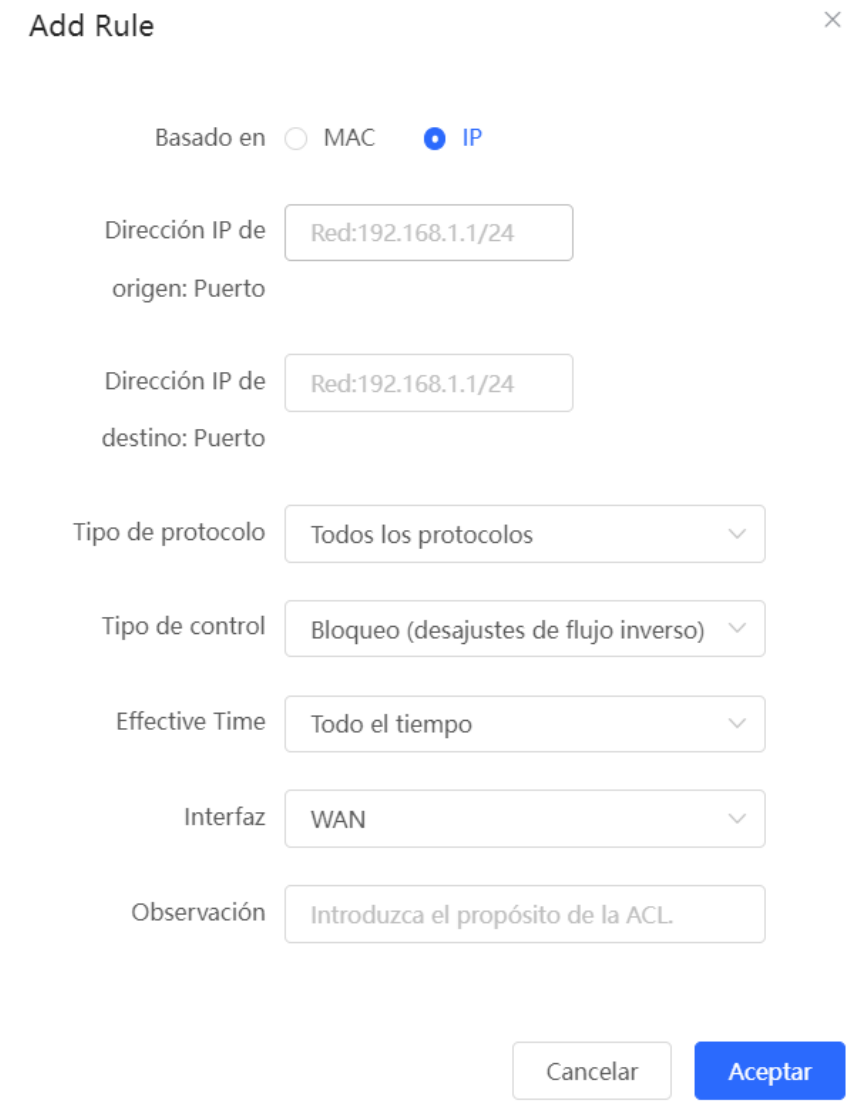


Tabla 4- 11 Configuración de ACL basadas en direcciones IP

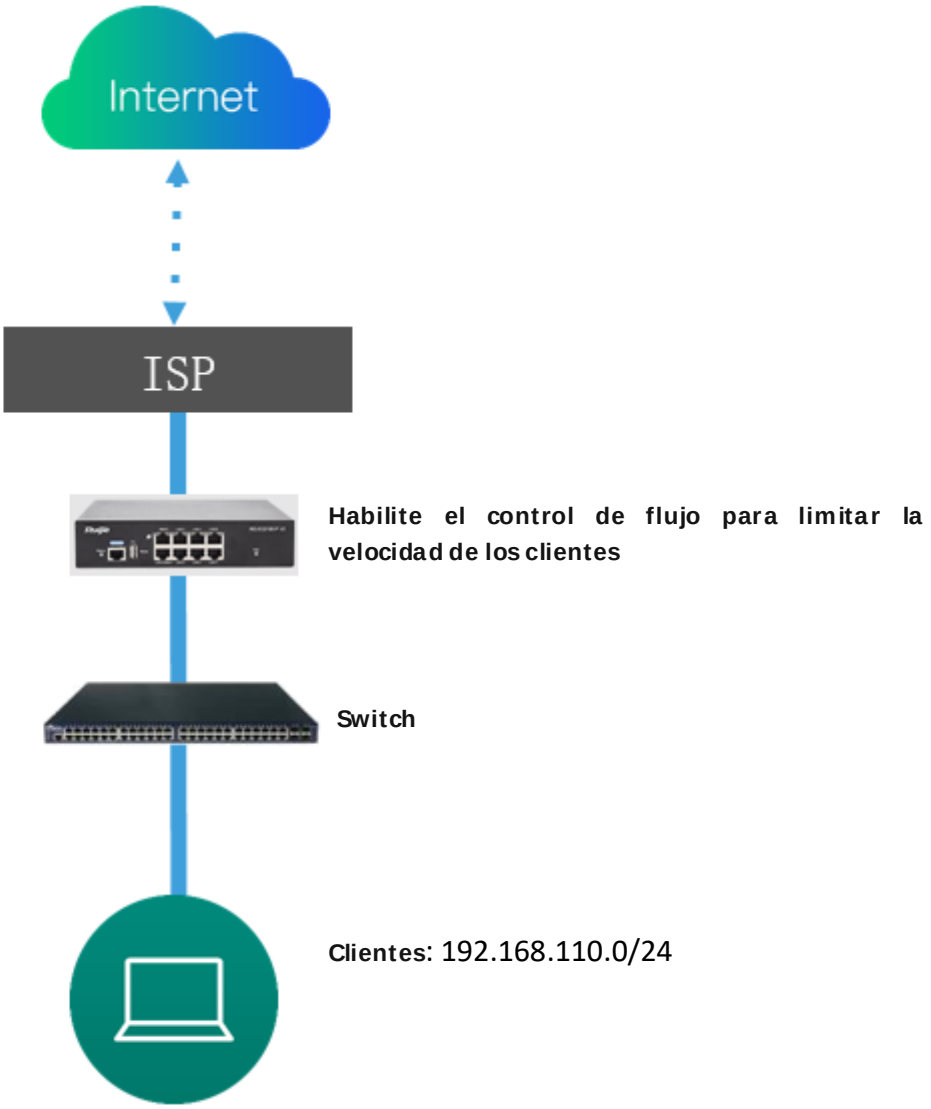
Parámetro	Descripción
Dirección IP de origen: Puerto	Ingrese la dirección IP de origen y el número de puerto para la coincidencia de paquetes de datos. Si este parámetro no se especifica, el dispositivo toma como coincidencia todas las direcciones IP y los números de puerto. La dirección IP de origen puede ser una sola (como 192.168.1.1) o un rango (como 192.168.1.1/24).
Dirección IP de destino: Puerto	Ingrese la dirección IP de destino y el número de puerto para la coincidencia de paquetes de datos. Si este parámetro no se especifica, el dispositivo toma como coincidencia todas las direcciones IP y los números de puerto. La dirección IP de origen puede ser una sola (como 192.168.1.1) o un rango (como 192.168.1.1/24).
Tipo de protocolo	Especifique el tipo de protocolo para la conciencia de paquetes de datos. Las opciones son **TCP**, **UDP** y **ICMP**.
Tipo de control	Especifique el método de procesamiento de las condiciones relativas a la coincidencia de los paquetes de datos. ● Permitir: otorga permiso de paso a los paquetes de datos que coincidan con las condiciones. ● Bloquear: descarta los paquetes de datos que coincidan con las condiciones. Esta regla es válida solamente en una dirección y no bloquea los flujos inversos.
Tiempo efectivo	Se puede elegir un rango de tiempo de la lista desplegable o seleccionar **Personalizado** y añadir manualmente un rango en específico.
Interfaz	Seleccione la interfaz a la cual se aplica la regla. ● LAN: la regla se hace efectiva en un puerto LAN para controlar los paquetes de datos hacia la LAN. ● WAN: la regla se hace efectiva en un puerto WAN para controlar los paquetes de datos recibidos o enviados de Internet.
Observación	Ingrese la descripción de la regla, la cual se utiliza únicamente para identificarla.

4.12 Control de flujo

4.12.1 Escenario de aplicación

El control de flujo habilita al dispositivo para clasificar los flujos con base en reglas y flujos de proceso, utilizando diferentes directivas basadas en sus categorías. El control de flujo puede utilizarse para garantizar

los flujos clave y suprimir los flujos malintencionados. También puede usarse cuando el ancho de banda es insuficiente o los flujos necesitan distribuirse adecuadamente.



4.12.2 Control de flujo inteligente

1. Descripción general

Para limitar el ancho de banda durante el tráfico de los enlaces ascendentes y descendentes de los puertos del dispositivo (como WAN y WAN 1), habilite el control de flujo inteligente. Cuando haya configurado el ancho de banda de la línea para un puerto, el tráfico de los enlaces ascendentes y descendentes del puerto estará limitado dentro del rango especificado. Además, el ancho de banda por usuario debe ajustarse inteligentemente, de acuerdo con el número de usuarios que la compartan, para que sea equitativo.

2. Pasos para la configuración

(1) Cambie al modo **Dispositivo local**. Seleccione **Comportamiento** > **Control de flujo** > **Control de flujo inteligente**.

(2) Mueva el interruptor a la posición **Activar** en la pestaña de **Control de flujo inteligente** y configure el ancho de banda de la línea con base en el actual, asignado por un ISP. Si el dispositivo cuenta con varias líneas, puede configurar el ancho de banda para estos puertos WAN de forma separada.

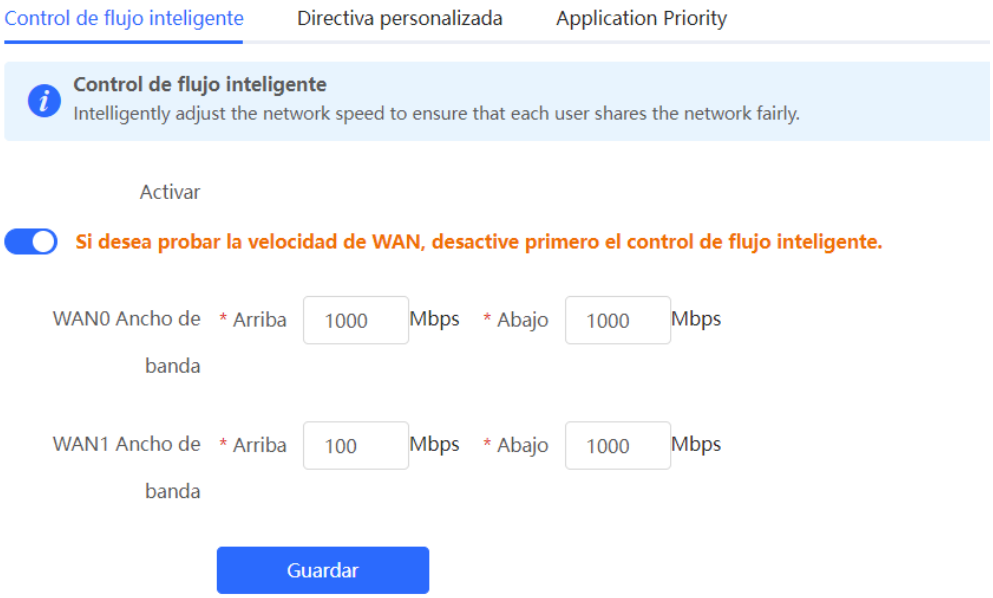


Tabla 4- 7 Configuración del control de flujo inteligente

Parámetro	Descripción
Activar	Especifique si se habilita la función de control de flujo inteligente. Por defecto, se encuentra deshabilitado.
Ancho de banda WAN	Configure los límites de ancho de banda de los enlaces ascendentes y descendentes para los puertos WAN, en Mbps.

(3) Haga clic en **Guardar** para que se aplique la configuración.

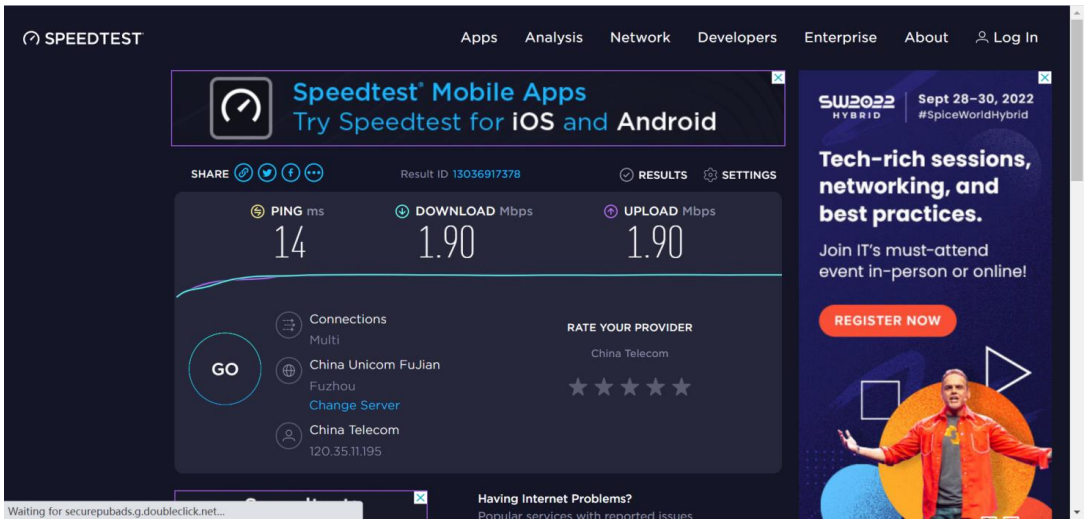
Precaución

Al habilitar el control de flujo, la prueba de velocidad de la red se ve afectada. Para probar la velocidad de la red, deshabilite primero el control de flujo.

Nota

El control de flujo inteligente se puede utilizar para controlar el tráfico de la línea en diferentes modos de la red, incluyendo aquel basado en el ancho de banda, la dirección IP estática y la dirección IP dinámica.

(4) Lleve a cabo la prueba de velocidad. La siguiente imagen muestra que las velocidades de carga y de descarga del invitado se encuentran por debajo de los 2 Mbps.



4.12.3 Directivas personalizadas

1. Descripción general

Las directivas personalizadas se utilizan para restringir el tráfico con direcciones IP específicas con base en el control de flujo inteligente, cumpliendo, de esa manera, con los requerimientos de ancho de banda de usuarios o servidores específicos. Cuando se crea una directiva de control de flujo personalizada, se puede configurar de manera flexible el rango límite del usuario, el de ancho de banda, el del tráfico de aplicaciones y el del modo de velocidad. Una directiva personalizada tiene prioridad sobre la configuración del control de flujo inteligente.

Las directivas personalizadas se clasifican en normales, MACC y VPN con base en el alcance de su aplicación:

- Las normales se utilizan para controlar el tráfico común.
- Las VPN se utilizan para controlar el tráfico a través de VPN.
- Las MACC son directivas de control de flujo configuradas en la nube. La página de gestión web solo muestra las directivas. Las directivas MACC no se pueden modificar en la página de gestión web. Para modificarlas, inicie sesión en MACC.

2. Primeros pasos

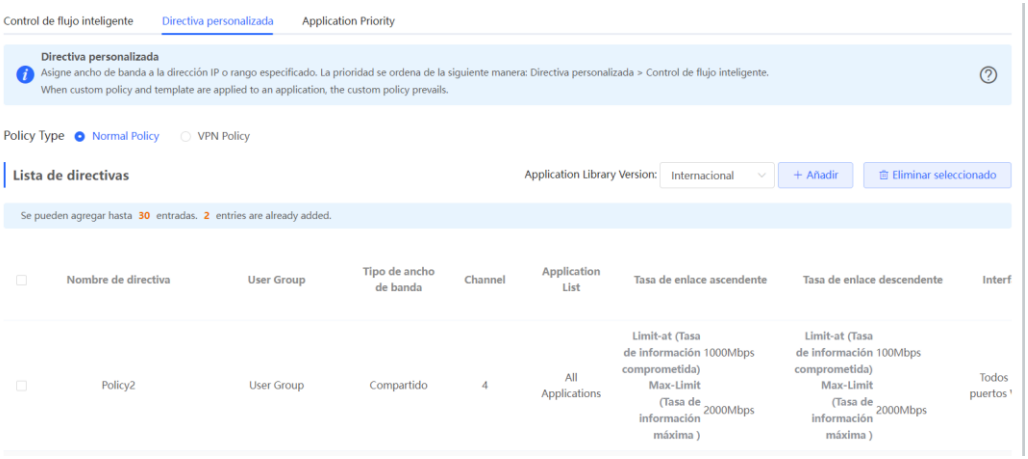
Antes de configurar la directiva personalizada, habilite el control de flujo inteligente. Para más información, consulte la sección 4.12.2 Control de flujo inteligente.

3. Pasos para la configuración

Cambie al modo **Red**.

Seleccione **Gateway > Comportamiento > Control de flujo > Directiva personalizada**.

(1) Configure **Policy type**.



Nota

La opción **Directiva de la nube** se muestra en **Policy Type** solo después de haber configurado la directiva MACC en el MACC.

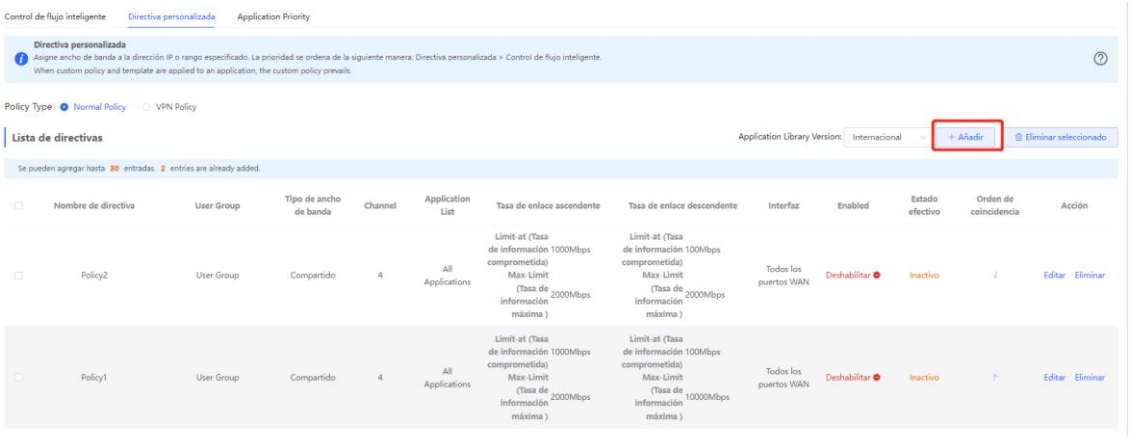
(2) Cambie la biblioteca de aplicaciones.

Las listas de aplicaciones varían dependiendo de la región. Están disponibles tanto la versión china como la versión internacional de la librería de aplicaciones. Seleccione la versión con base en la región.

Haga clic en **Application Library Version** para seleccionarla y luego en **Aceptar**. La versión cambia después de algunos minutos.

Precaución

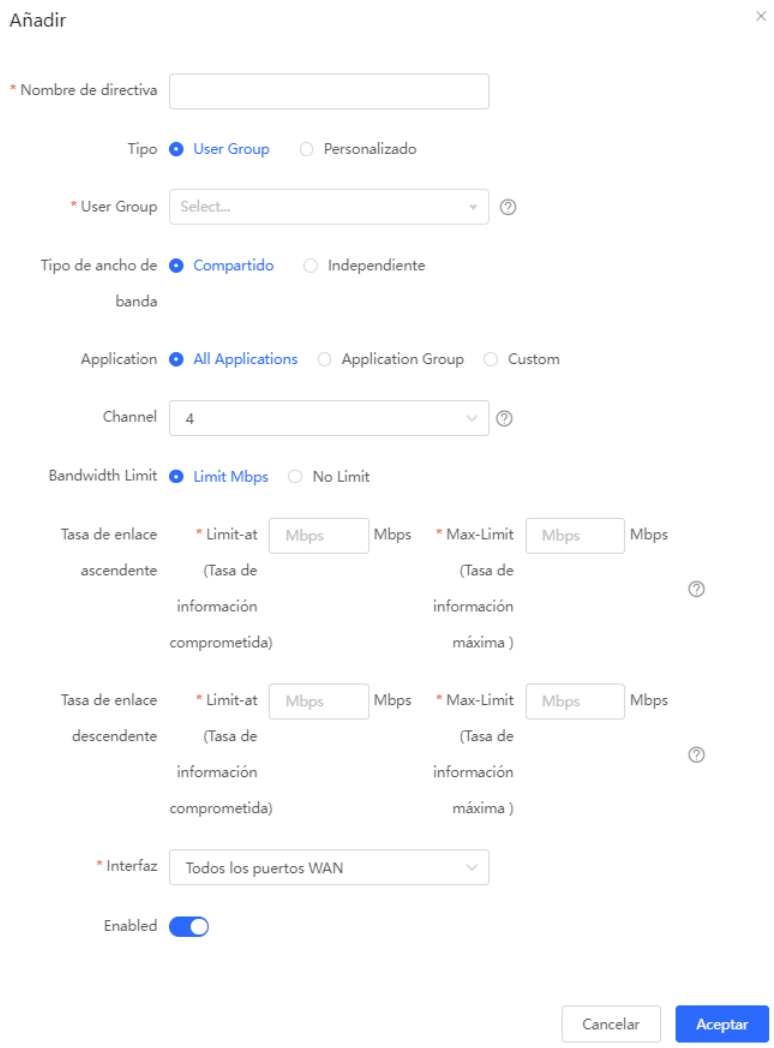
- Cambiar la versión de la biblioteca de aplicaciones tarda aproximadamente un minuto. Por favor, espere.
- Si cambia la biblioteca de aplicaciones, la plantilla de la prioridad de aplicaciones se restablecerá y la directiva de control de aplicaciones anterior podría dejar de funcionar. Proceda con precaución al realizar este cambio.



(1) Configure una directiva personalizada.

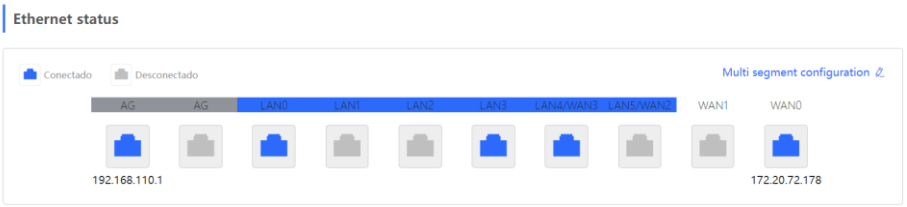
- Configure una directiva normal personalizada.
  a En **Policy Type**, configure **Normal Policy** y haga clic en **Añadir** para crear una directiva de control de flujo normal personalizada.

  Se pueden configurar un máximo de 30 directivas normales personalizadas.



  b Configure los elementos relativos a una directiva normal.

Parámetro	Descripción
Nombre de directiva	El nombre de una directiva solamente identifica una directiva de control de flujo personalizada. No se puede modificar.
Tipo	Tipo de directiva de control de flujo: ● **User Group**: la directiva es aplicable para los usuarios dentro del grupo especificado. Seleccione el grupo de usuarios que se administrará. ● **Personalizado**: la directiva es aplicable para los usuarios dentro del segmento de dirección IP especificado. Ingrese manualmente el rango de dirección IP que se administrará.

Parámetro	Descripción
Grupo de usuarios	Desde la lista del grupo de usuarios, seleccione el usuario que se administrará por la directiva. Si selecciona todos los miembros del grupo, la directiva será efectiva para todo el grupo de usuarios (incluyendo sus nuevos miembros).
Rango IP/IP	Especifique el rango de dirección IP para la directiva de control de flujo que surtirá efecto. Cuando en **Tipo** seleccione **Personalizado**, ingrese manualmente la dirección IP. Puede ingresar una sola dirección IP o un segmento de dirección IP. El rango de dirección IP debe estar dentro del segmento de la LAN. Seleccione **Descripción general** > **Ethernet status** para revisar el segmento de la red del puerto LAN actual. Por ejemplo, en la siguiente imagen se muestra que el segmento de red del puerto LAN es 192.168.110.0/24. 
Tipo de ancho de banda	● **Compartido**: todos los usuarios en un grupo de usuarios (todas las direcciones IP en un rango de direcciones) comparten los anchos de banda configurados de los enlaces ascendentes y descendentes, y el ancho de banda de cada usuario no está limitado. ● **Independiente**: todos los usuarios en un grupo de usuarios (todas las direcciones IP en un rango de direcciones) comparten los anchos de banda configurados de los enlaces ascendentes y descendentes, y es posible limitar el ancho de banda máximo de cada usuario.
Aplicación	Cuando en **Tipo de ancho de banda** se establece la opción **Compartido**, la directiva de control de flujo se puede configurar para que sea efectiva solamente en las aplicaciones especificadas. ● **All Applications**: la directiva de control de flujo es efectiva en todas las aplicaciones de la biblioteca actual. ● **Custom**: la directiva de control de flujo es efectiva solamente en aplicaciones especificadas en la lista. Cuando en **Tipo de ancho de banda** se establece la opción **Independiente**, algunos modelos no admiten la selección de aplicaciones y, por defecto, la directiva de control de flujo aplica en todas las aplicaciones de la biblioteca actual. Para información sobre los modelos, contacte a los ingenieros de soporte técnico.
Lista de aplicaciones	Cuando en **Application** se seleccione la opción **Custom**, se especifican las aplicaciones en las que la directiva será efectiva. El tráfico de las aplicaciones elegidas quedará limitado por la directiva.

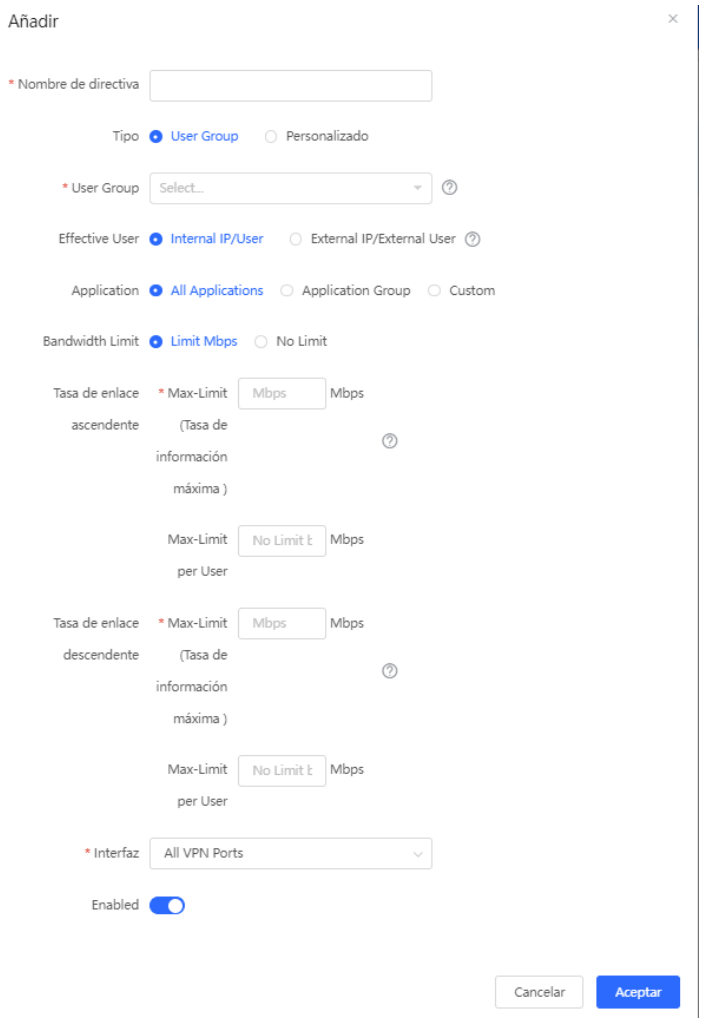
Parámetro	Descripción
Prioridad del canal	Especifica el nivel garantizado de tráfico. Puede seleccionar un valor de 0 a 7. Un valor menor indica una prioridad mayor, y un valor de 0 indica la prioridad máxima. Los valores de prioridad de tráfico diferentes corresponden a grupos de aplicaciones diferentes en una plantilla de aplicaciones. El valor 2 indica el grupo clave, el 4 indica el grupo normal y el 6 indica el grupo de represión. Para la descripción de los grupos de aplicaciones en una plantilla de prioridad, consulte 4.12.4 Prioridad de las aplicaciones.
Límite de ancho de banda	Configure si desea limitar el ancho de banda. ● **Limit Kbps**: para los enlaces ascendentes y descendentes, se pueden configurar límites de ancho de banda, según se requiera. ● **No limit**: cuando el ancho de banda es suficiente, el ancho de banda máximo por utilizar es ilimitado. Cuando el ancho de banda no es suficiente, no se puede garantizar el ancho de banda mínimo.
Ancho de banda de enlace ascendente Velocidad de enlace descendente	Configure la velocidad de transmisión de datos de los enlaces ascendentes y descendentes, en kbps. ● **Tasa de información comprometida**: especifica el ancho de banda mínimo que puede compartirse por todos los usuarios cuando el ancho de banda no es suficiente. ● **Tasa de información máxima**: especifica el ancho de banda máximo total que pueden ocupar todos los usuarios cuando el ancho de banda es suficiente. ● **Tasa de información máxima por Usuario**: especifica el ancho de banda máximo que puede ocupar cada usuario cuando varios lo comparten. Este parámetro es opcional y solamente se puede configurar cuando el **Tipo de ancho de banda** se configura en **Independiente**. Por defecto, la velocidad no se encuentra limitada.
Interfaz	Especifica el puerto WAN en el cual se hará efectiva la directiva. Cuando se configura en **Todos los puertos WAN**, la directiva aplicará a todos los puertos.
Habilitado	Especifique si se habilita la directiva de control de flujo. Si está deshabilitada, la directiva no surtirá efecto.

Precaución

Después de cambiar la versión de la biblioteca de aplicaciones, es posible que deba volver a configurar la lista de aplicaciones.

c Haga clic en **Aceptar**.

- Configure una directiva VPN personalizada.
  a En **Policy Type**, seleccione **VPN Policy** y haga clic en **Añadir** para crear una directiva de control de flujo de VPN personalizada.
  Se puede configurar un máximo de 10 directivas VPN.



b Configuración de los elementos relativos a una directiva VPN.

Parámetro	Descripción
Nombre de directiva	El nombre de una directiva solamente identifica una directiva de control de flujo personalizada. No se puede modificar.
Tipo	Tipo de directiva de control de flujo: ● **User Group**: la directiva es aplicable para los usuarios dentro del grupo especificado. Seleccione el grupo de usuarios que se administrará. ● **Personalizado**: la directiva es aplicable para los usuarios dentro del segmento de dirección IP especificado. Ingrese manualmente el rango de dirección IP que se administrará.
Grupo de usuarios	Desde la lista del grupo de usuarios, seleccione el usuario que se administrará por la directiva. Si selecciona todos los miembros del grupo, la directiva será efectiva para todo el grupo de usuarios (incluyendo sus nuevos miembros).

Parámetro	Descripción
Usuario efectivo	Especifique el tipo de usuarios efectivos: ● **Internal IP/User**: para una puerta de enlace, las direcciones IP de los clientes conectados a ella, son direcciones IP internas. ● **External IP/External User**: para una puerta de enlace, las direcciones IP internas sin conexión a ella son direcciones IP externas, al igual que la dirección IP interna del servidor VPN. Las sugerencias de configuración son las siguientes: ● Si los clientes se configuran para controlar el tráfico de VPN, seleccione **Internal IP/ User** para controlar el tráfico de usuarios de la red interna. Si el servidor VPN se configura para controlar el tráfico de VPN, seleccione **External IP/External User** para controlar el tráfico de usuarios de la red externa. ● Para la VPN del modelo NAT, la dirección IP externa del servidor debe estar en el segmento de dirección IP del grupo de direcciones de VPN. ● Para la VPN en modo router, el segmento de dirección IP debe configurarse en direcciones IP de usuarios restringidos. Para la VPN en modo router, para configurar el control de flujo en direcciones IP internas de clientes, configure direcciones IP internas en las direcciones IP de los objetos del control de flujo.
Aplicación	Cuando el **Tipo de ancho de banda** se configura como **Compartido**, la directiva de control de flujo se puede configurar para que se haga efectiva solamente en aplicaciones especificadas. ● **All Applications**: la directiva de control de flujo es efectiva en todas las aplicaciones de la biblioteca actual. ● **Custom**: la directiva de control de flujo es efectiva solamente en aplicaciones especificadas en la lista. Cuando el **Tipo de ancho de banda** se configura en **Independiente**, algunos modelos no permiten la selección de aplicaciones y, por defecto, la directiva de control de flujo surte efecto en todas las aplicaciones de la biblioteca actual. Para información sobre los modelos, contacte a los ingenieros de soporte técnico.
Lista de aplicaciones	Cuando en **Application** se establece **Custom**, esto indica las aplicaciones en las que se hará efectiva la directiva. El tráfico de las aplicaciones elegidas está limitado por la directiva.
Velocidad máxima de enlace ascendente por usuario Velocidad máxima de enlace descendente por usuario	Configure la velocidad máxima de transmisión de datos de los enlaces ascendentes y descendentes cuando varios usuarios comparten el ancho de banda, en kbps. Este parámetro es opcional y se puede configurar solamente cuando el **Tipo de ancho de banda** se configura en **Independiente**. Por defecto, la velocidad no se encuentra limitada.
Interfaz	Especifica el puerto VPN en el cual se hará efectiva la directiva. Cuando se configura en **All VPN Ports**, la directiva se aplica en todo el tráfico de tipo VPN.

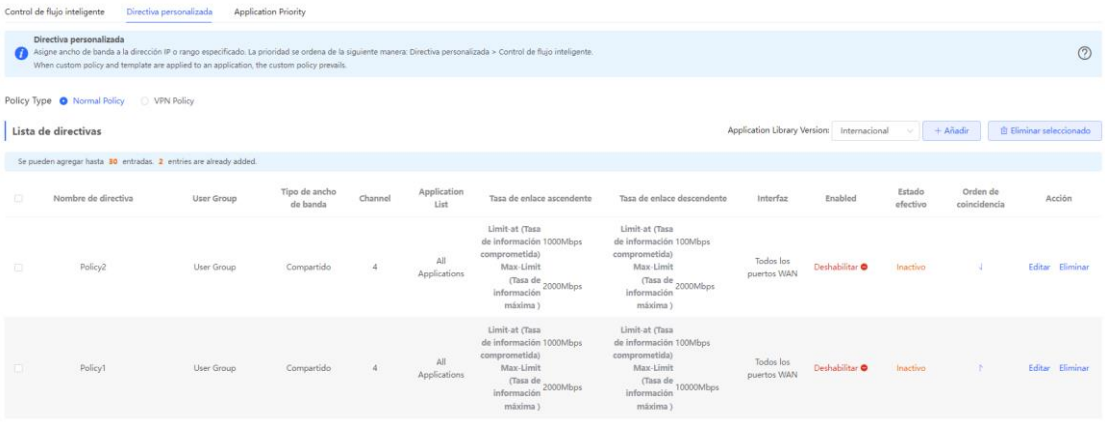
Parámetro	Descripción
Habilitado	Especifique si se habilita la directiva de control de flujo. Si está deshabilitada, la directiva no surtirá efecto.

c Haga clic en **Aceptar**.

(3) Visualización de directivas personalizadas.

Las directivas personalizadas actuales se muestran en la sección de **Lista de directivas**. Las directivas personalizadas se pueden editar o eliminar. Para borrar varias directivas personalizadas en grupo, seleccione las directivas deseadas y haga clic en **Eliminar seleccionado**.

- Lista de directivas normales



- Lista de directivas VPN

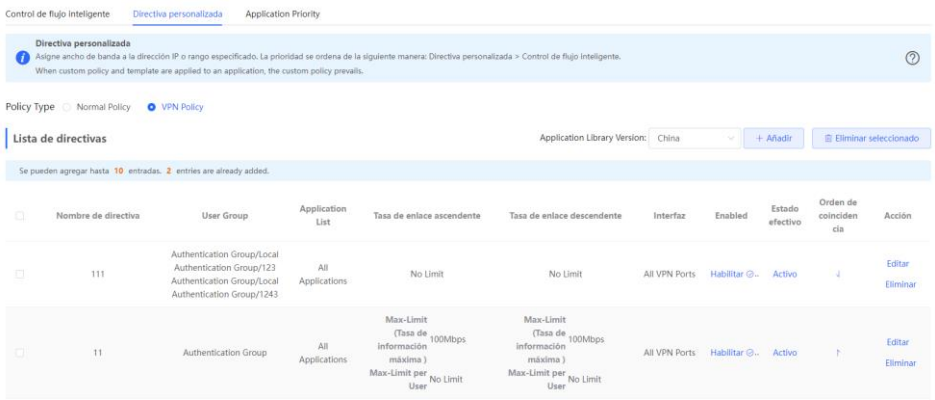


Tabla 4- 8 Información de la lista de directivas

Parámetro	Descripción
Lista de aplicaciones	**Application List** contiene las aplicaciones para las que aplica la directiva. Si **Application Library** coincide con el parámetro **Application** configurado como **Custom** y sustentado por la directiva,  se mostrará en **Application List**. De no ser así, se mostrará  .
Estado (Habilitada)	Determine si la directiva actual se encuentra habilitada. Haga clic para editar su estado. Si **Application Library** coincide con el parámetro **Aplicación** configurado como **Custom** y sustentado por la directiva, **Estado** no se podrá editar directamente. Haga clic en **Editar** en la barra de acción para modificar la directiva o cambie la biblioteca de aplicaciones.
Estado efectivo	Muestra si la directiva es efectiva en el sistema actual. Si el estado se muestra como **Inactivo**, revise si la directiva está habilitada, si el puerto habilitado para la directiva existe y si **Application Library** coincide con el parámetro **Application** para el que es válida la póliza.
Orden de coincidencia	Todas las directivas personalizadas creadas se muestran en la lista de directivas, con la más reciente clasificada en primer lugar. El dispositivo busca coincidencias con las directivas de acuerdo con su clasificación en la lista. La secuencia de coincidencia de la directiva se puede ajustar manualmente haciendo clic en o en la lista.
Acción	Las directivas personalizadas se pueden editar o eliminar.

4.12.4 Prioridad de las aplicaciones

1. Descripción general

Después de habilitar el control de flujo inteligente, se puede configurar la prioridad de las aplicaciones para garantizar el ancho de banda en aquellas con alta prioridad y reducirlo en aquellas con baja prioridad. Se puede predefinir la lista de aplicaciones cuyo ancho de banda debe garantizarse preferentemente, y una lista de aquellas cuyo ancho de banda debe reducirse, según se requiera.

Precaución

Si no existe ninguna aplicación en la lista de directivas personalizadas ni en la de aplicaciones prioritarias, la directiva personalizada surtirá efecto.

2. Primeros pasos

Antes de configurar una aplicación prioritaria, habilite el control de flujo inteligente. Para más información, consulte la sección 4.12.2 Control de flujo inteligente.

- Confirme que la biblioteca de aplicaciones apropiada se haya seleccionado en la página de **Directiva personalizada** (consulte la sección 4.12.3 Directivas personalizadas.

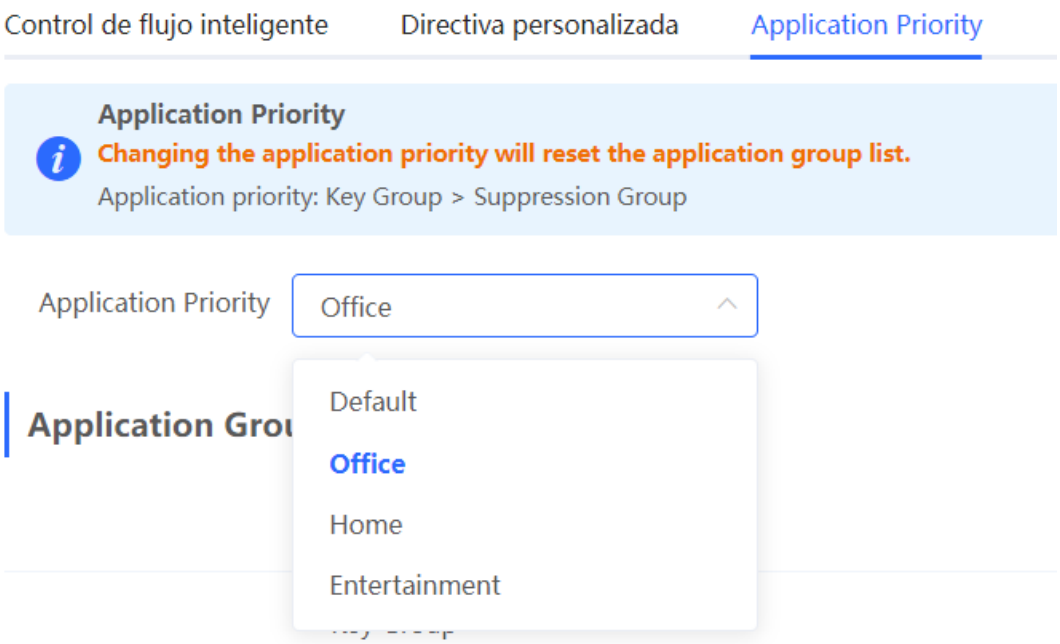
3. Pasos para la configuración

Cambie al modo Dispositivo local. Seleccione **Comportamiento > Control de flujo > Application priority**.

(1) Cree una plantilla de prioridad de aplicación.

Seleccione la plantilla de la lista desplegable en **Application Priority**.

Hay cuatro plantillas de prioridad de aplicación predefinidas para diferentes escenarios. Puede pasar de una a otra para visualizarlas, según lo requiera.



Las plantillas de prioridad de aplicación son las siguientes:

- **Default**: esta plantilla se utiliza durante la inicialización del dispositivo. El ancho de banda del tráfico no se garantiza ni se reduce para ninguna aplicación:
- **Office**: esta plantilla está diseñada para el escenario de oficina, donde el tráfico de las aplicaciones de la red de la empresa se garantiza de forma preferente.
- **Home**: esta plantilla está diseñada para el escenario del hogar, donde el tráfico de las aplicaciones de la red del hogar se garantiza de forma preferente.
- **Entertainment**: esta plantilla está diseñada para el escenario del entretenimiento, donde el tráfico de las aplicaciones de la red de entretenimiento se garantiza de forma preferente.

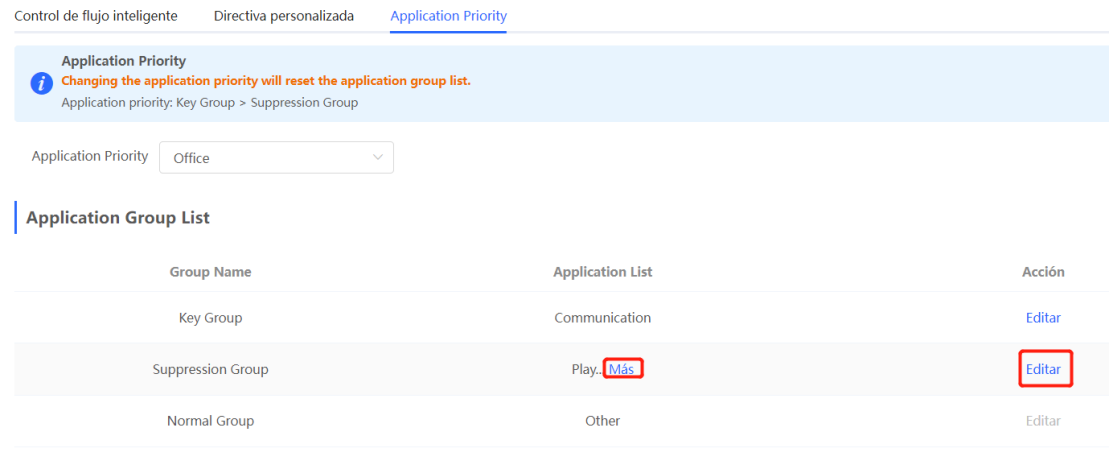
(2) Cree una lista de aplicaciones en grupo.

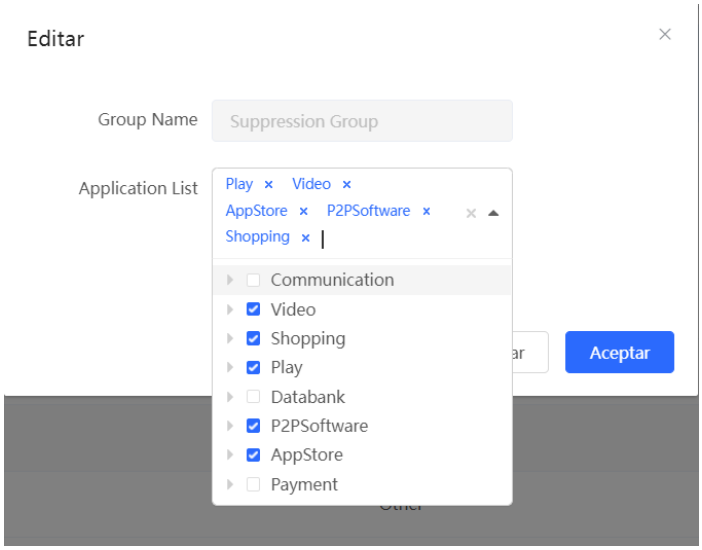
Cada plantilla predeterminada tiene tres grupos de aplicaciones: grupo clave, grupo de bloqueo y grupo normal. La prioridad de las aplicaciones de cada grupo se encuentra en orden descendente:

- **Key Group**: el tráfico de las aplicaciones en la lista de este grupo se garantiza de forma preferente.
- **Suppression Group:** el tráfico de las aplicaciones en la lista de este grupo se reduce para garantizar de forma preferente el de las aplicaciones con mayor prioridad.
- **Normal Group**: todas las aplicaciones en la biblioteca, fuera de las que están en **Key Group** y **Suppression Group** se encuentran incluidas en este grupo. El tráfico de las aplicaciones en este grupo se garantiza después del tráfico de **Key Group**.

Después de que seleccione una plantilla, **Key Group**, **Suppression Group**, **Normal Group** y la lista de aplicaciones para cada grupo se muestran en la plantilla actual. Haga clic en **Más** para visualizar los detalles de cada lista de aplicaciones.

Haga clic en **Editar,** en la columna **Acción**, junto al grupo clave y el bloqueado, para modificar la lista de aplicaciones, permitiendo que el tráfico de estas aplicaciones se garantice o se reduzca.





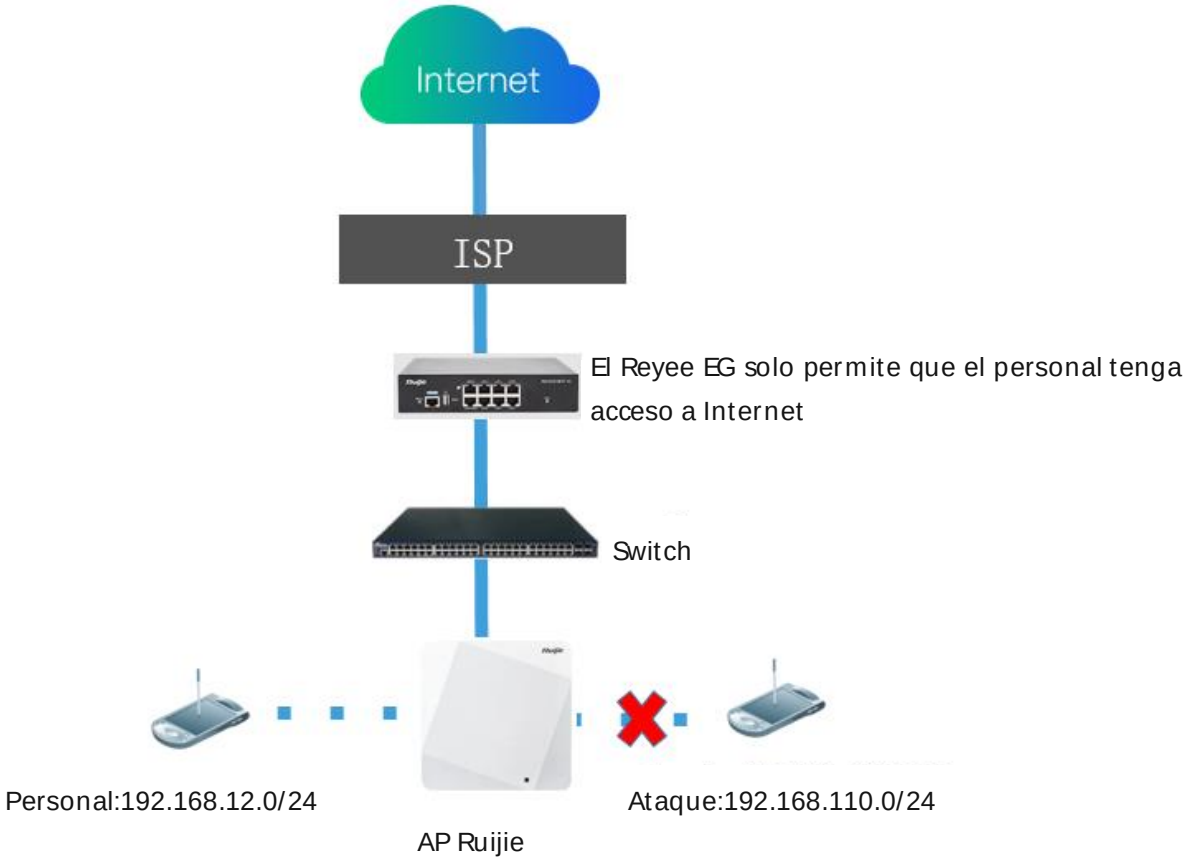
Precaución

- Si cambia la biblioteca de aplicaciones, la lista de aplicaciones también cambiará.

- La lista de aplicaciones se restablecerá después de cambiar la plantilla de prioridad de las aplicaciones.

4.13 Seguridad

4.13.1 Escenario de aplicación



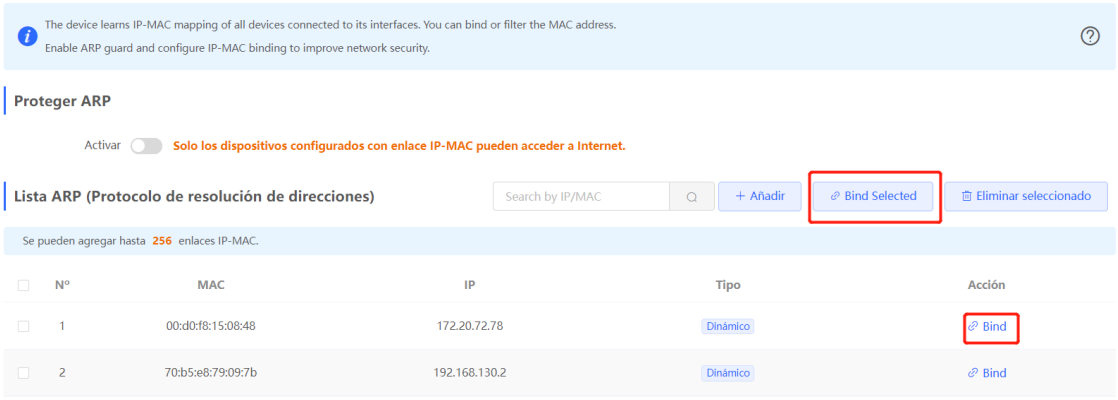
4.13.2 Configuración de la lista ARP y el protector de ARP

El dispositivo aprende las direcciones IP y las direcciones MAC de los dispositivos de red conectados a sus interfaces y genera las entradas del protocolo de resolución de direcciones (ARP) correspondientes. Puede habilitar la función para proteger el ARP y configurar el enlace IP-MAC para restringir el acceso a Internet de los hosts de LAN y mejorar la seguridad de la red.

(1) Cambie al modo **Dispositivo local**. Seleccione **Seguridad** > **Lista ARP**.

(2) Antes de habilitar la protección del ARP, configure el enlace entre las direcciones IP y las direcciones MAC de cualquiera de las siguientes maneras:

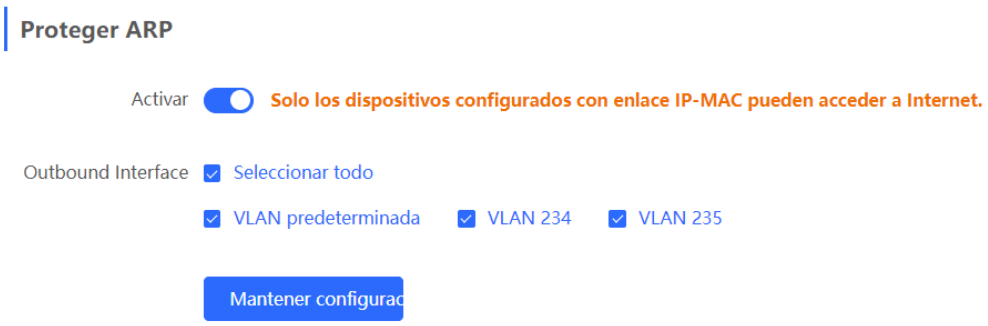
- Seleccione una entrada de ARP dinámico en la lista ARP y haga clic en **Bind**. Se pueden seleccionar varias entradas, para crear vinculaciones al mismo tiempo. Haga clic en **Bind Selected** para completar el procedimiento.



- Haga clic en **Añadir**, seleccione la dirección IP y la dirección MAC que desea vincular y haga clic en **Aceptar**. El cuadro de texto puede desplegar los mapeos de las direcciones existentes en la lista ARP. Haga clic en un mapeo para agregar automáticamente el mapeo de la dirección.

(3) Seleccione **Activar** para habilitar la protección del ARP.

Después de activar la función, solo los hosts de LAN con enlace IP-MAC tendrán acceso a la red externa.



Configure el rango para que la función sea efectiva.

Si selecciona **Seleccionar todo**, la función de protección del ARP será efectiva para todos los clientes en la LAN. Si selecciona un puerto especificado, la función para proteger al ARP se hará efectiva solo para los clientes conectados a dicho puerto.

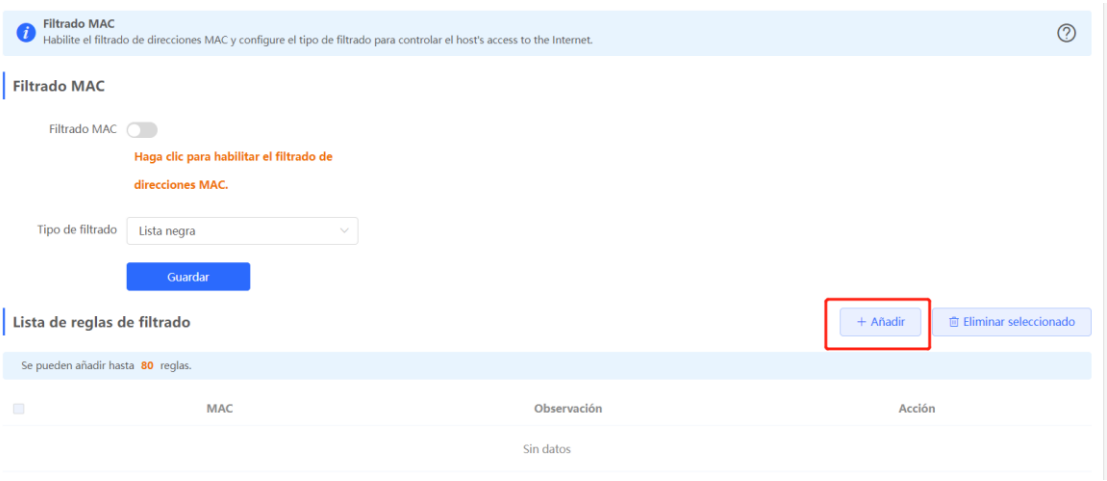
4.13.3 Configuración del filtrado de direcciones MAC

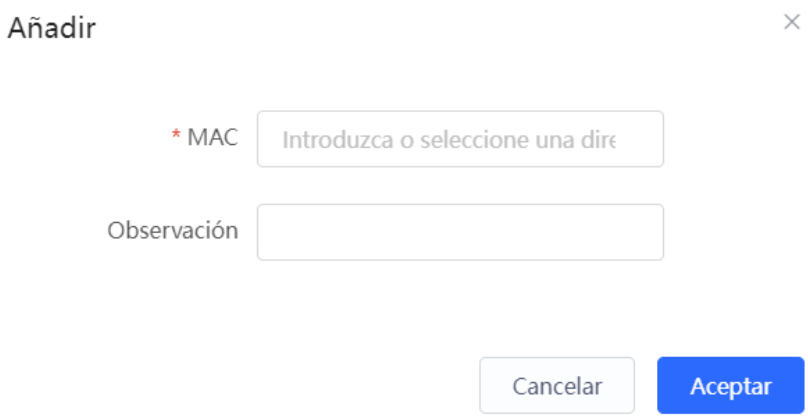
Habilite el filtrado de direcciones MAC y configure una lista blanca o lista negra para controlar de manera efectiva el acceso a Internet por parte de los hosts de una LAN.

- Lista blanca: permite que solo los hosts cuyas direcciones MAC se encuentren en la lista de reglas de filtrado puedan acceder a Internet.
- Lista negra: evita que los hosts cuyas direcciones MAC se encuentren en la lista de reglas de filtrado accedan a Internet.

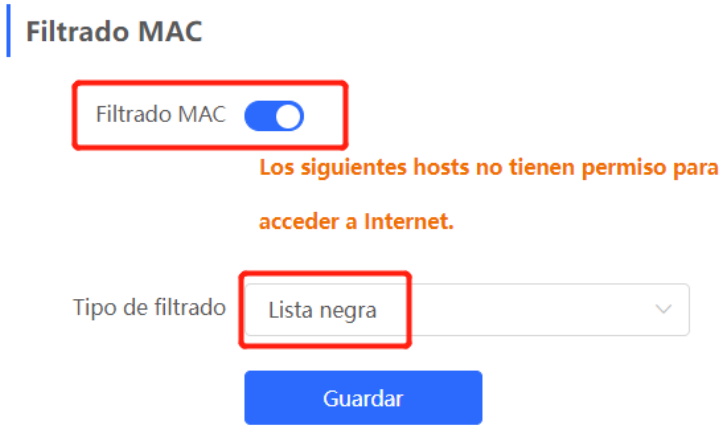
(1) Cambie al modo **Dispositivo local**. Seleccione **Seguridad** > **Filtrado MAC**.

(2) Haga clic en **Añadir**. En el cuadro de diálogo que aparece, ingrese la dirección MAC y observaciones sobre esta. El cuadro de texto puede desplegar los mapeos de las direcciones existentes en la lista ARP. Haga clic en un mapeo para agregar automáticamente la dirección MAC. Haga clic en **Aceptar**. Ha creado una regla de filtrado.





(3) Habilite el filtrado de direcciones MAC, configure el **Tipo de filtrado** y haga clic en **Guardar**.



4.13.4 Configuración de la seguridad del dispositivo

Nota

Esta función solo es compatible con el R202 y versiones posteriores.

1. **Descripción general**

   Prohibit Ping: esta función identifica y descarta directamente los paquetes de ping en el tráfico enviado al dispositivo, con el fin de prohibir el ping. El dispositivo solo puede ser pingueado desde la dirección IP de administrador.

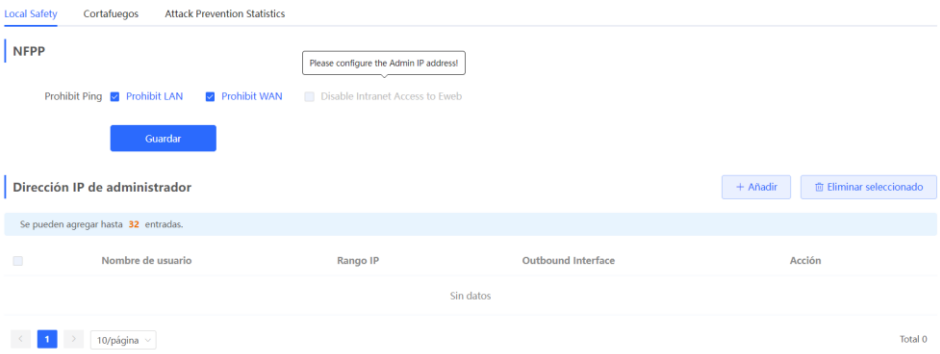
   Dirección IP de administrador: los paquetes enviados desde la dirección IP de administrador tienen permitido el paso.

2. **Habilitar la función de prohibición del ping**

   Cambie al modo **Dispositivo local**. Seleccione **Seguridad** > **Protección local** > **Local Safety.**

   La función de prohibición del ping incluye lo siguiente:

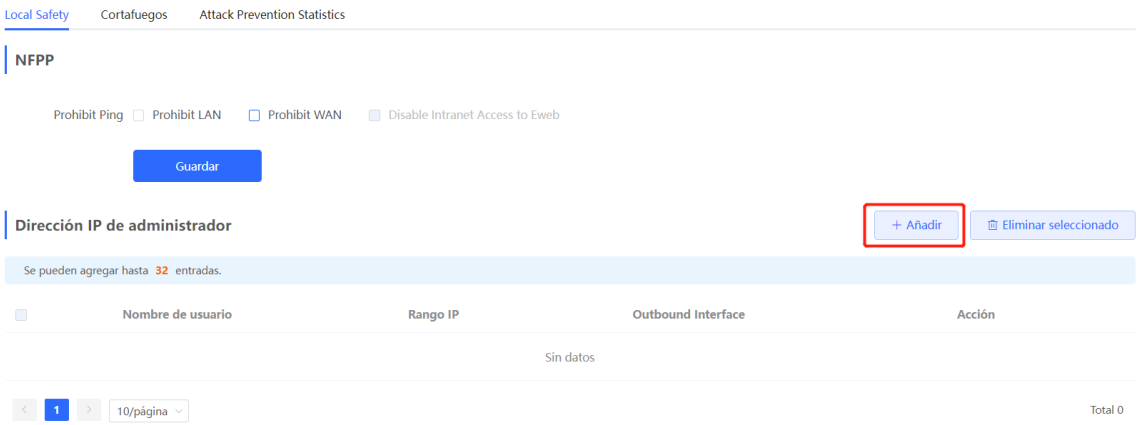
   - Si selecciona **Prohibit LAN**, se descartarán los paquetes de ping enviados por todos los clientes de una LAN al dispositivo.
   - Si selecciona **Prohibit WAN**, se descartarán los paquetes de ping enviados por todos los clientes en las WAN al dispositivo. Los paquetes de ping enviados por un cliente al dispositivo se responderán solo después de que la dirección IP del cliente se encuentre en **Dirección IP de administrador**. Para más detalles de cómo configurar las direcciones IP de administrador, consulte Configuración de una dirección IP de administrador.



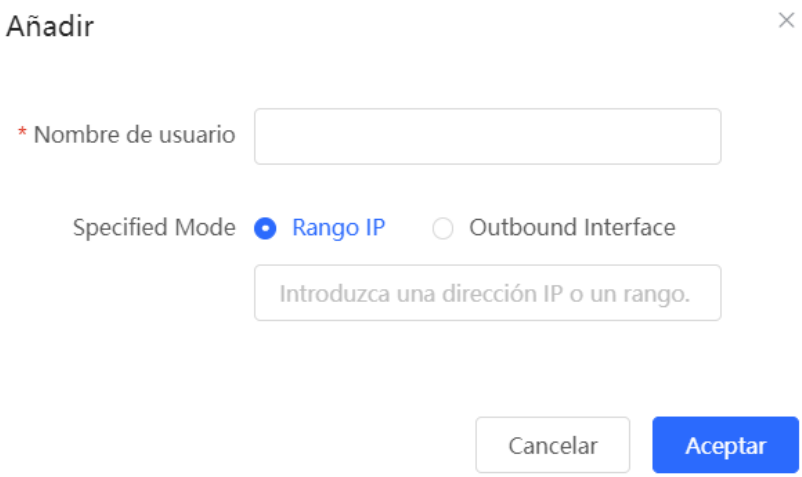
3. Configuración de una dirección IP de administrador

Cambie al modo Dispositivo **local**. **Seleccione Seguridad > Protección local > Local Safety**.

Haga clic en **Añadir**. Ahora puede configurar la información de la dirección IP de administrador.



- Configurar una dirección IP de administrador (basada en una dirección IP)



(1) Configure un nombre para la dirección IP de administrador.

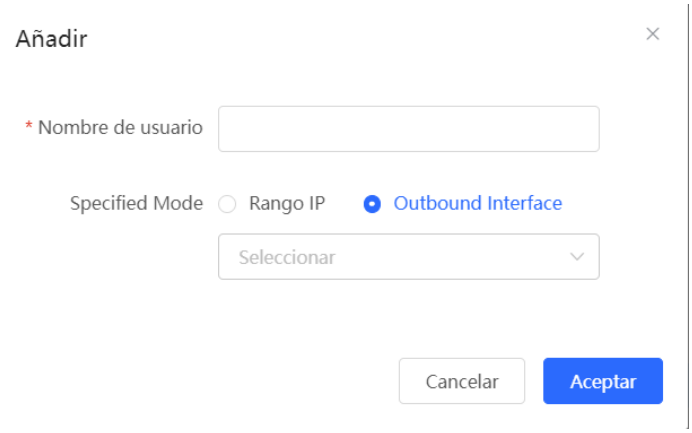
El nombre debe estar formado por una cadena de 1 a 32 caracteres.

(2) Configure en **Specified Mode** el **Rango IP**.

(3) Configure una dirección IP.

Puede ingresar una sola dirección IP o un rango de dirección IP.

- Configurar una dirección IP de administrador (basada en un puerto).



(1) Configure un nombre para la dirección IP de administrador.

El nombre debe estar formado por una cadena de 1 a 32 caracteres.

(2) Configure en **Specified Mode** la opción **Outbound Interface**.

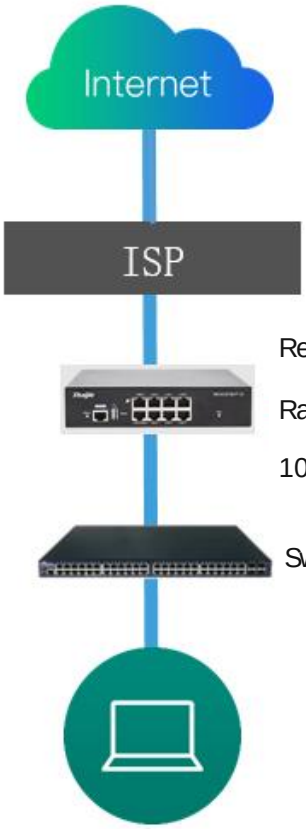
(3) Especifique el puerto.

Puede seleccionar un puerto LAN o un puerto WAN como la interfaz de salida.

4.14 Configuración del servidor PPPoE

4.14.1 Escenario de aplicación

El protocolo punto a punto sobre Ethernet (PPPoE) es un protocolo de túneles de red que encapsulan tramas PPP en tramas Ethernet. Cuando el router actúa como servidor PPPoE, brinda el servicio de acceso a los usuarios LAN y admite la gestión del ancho de banda.



Clientes PPPoE: 10.44.66.100/24

4.14.2 Configuración global

Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Servidor PPPoE** > **Configuración global**.

Elija en **PPPoE Server** la opción **Enable** y configure los parámetros del servidor PPPoE.

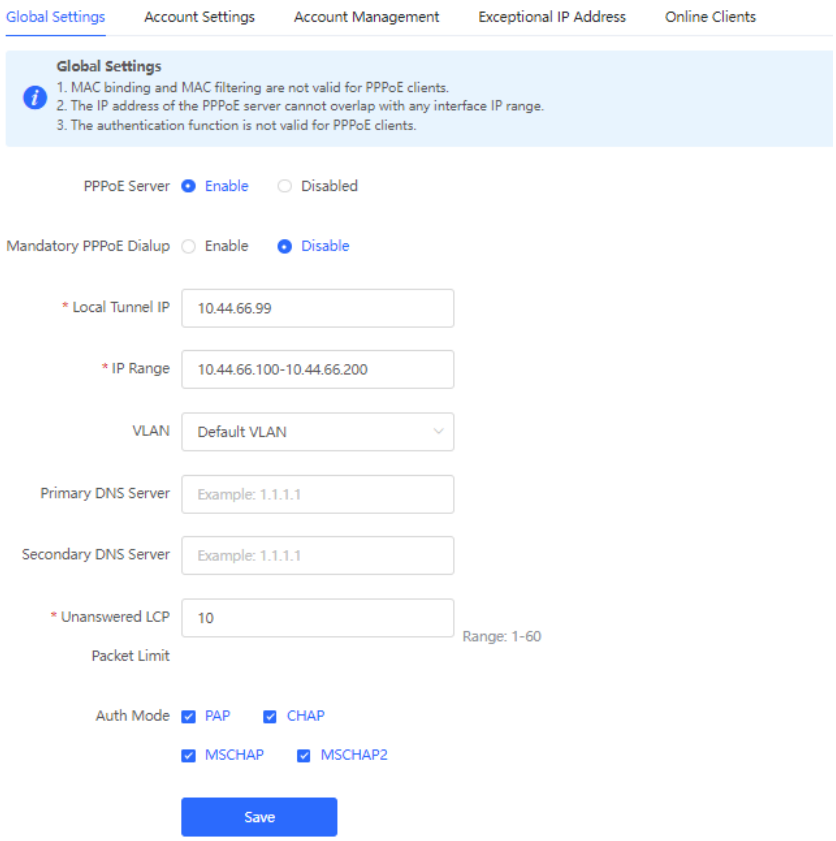


Tabla 4- 7 Configuración del servidor PPPoE

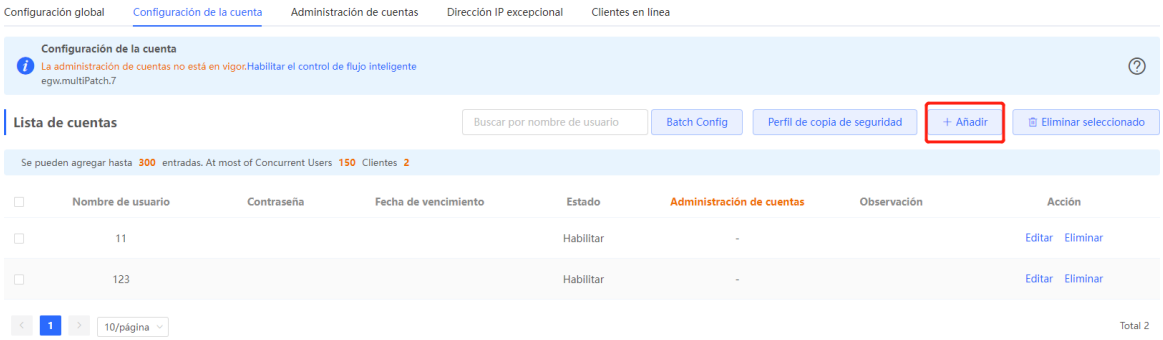
Parámetro	Descripción
Servidor PPPoE	Especifique si se habilita la función de servidor PPPoE.
Conexión por línea conmutada de PPPoE obligatorio	Especifique si los usuarios LAN deben acceder a Internet mediante marcación.
Túnel IP local	Configure la dirección P2P del servidor PPPoE.
Rango IP	Especifique el rango de dirección IP que puede ser asignado por el servidor PPPoE a los usuarios autenticados.
VLAN	Configure el VLAN ID del servidor PPPoE.
Servidor DNS primario/Servidor DNS secundario	Especifique la dirección del servidor DNS disponible para usuarios autenticados.

Parámetro	Descripción
Límite de paquetes LCP sin respuesta	Cuando el número de paquetes LCP sin respuesta en un enlace exceda el valor especificado, el servidor PPPoE automáticamente desconectará dicho enlace.
Modo de autenticación	Seleccione por lo menos un modo de autenticación entre PAP, CHAP, MSCHAP y MSCHAP2.

4.14.3 Configuración de una cuenta de usuario PPPoE

Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Servidor PPPoE** > **Configuración de la cuenta**.

Haga clic en **Añadir** para crear una cuenta de usuario de autenticación PPPoE. Las cuentas creadas se muestran en la sección de **Lista de cuentas**. Encuentre la cuenta objetivo y haga clic en **Editar** para modificar su información. Encuentre la cuenta objetivo y haga clic en **Eliminar** para borrarla.



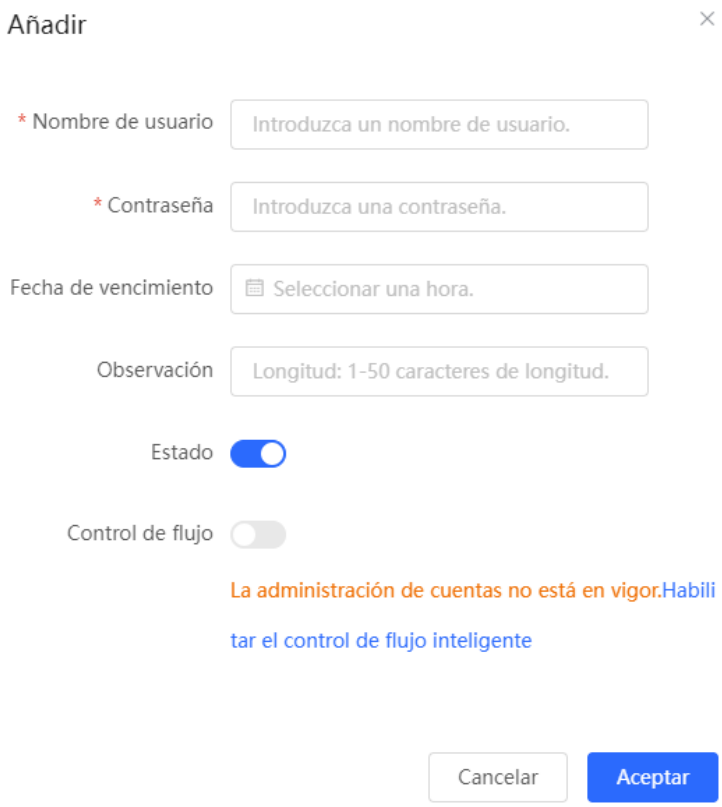


Tabla 4- 8 Configuración de una cuenta de usuario PPPoE

Parámetro	Descripción
Nombre de usuario/Contraseña	Configure el nombre de usuario y la contraseña de la cuenta de autenticación para tener acceso a Internet a través de la marcación PPPoE.
Fecha de vencimiento（Contraseña）	Configure la fecha de vencimiento de la cuenta de autenticación. Cuando la cuenta venza, ya no podrá utilizarse para tener acceso a Internet a través de la autenticación PPPoE.
Observación	Ingrese la descripción de la cuenta.
Estado	Especifique si se habilita esta cuenta de usuario. Si la cuenta se deshabilita, ya no es válida y no se puede usar para tener acceso a Internet a través de la autenticación PPPoE.

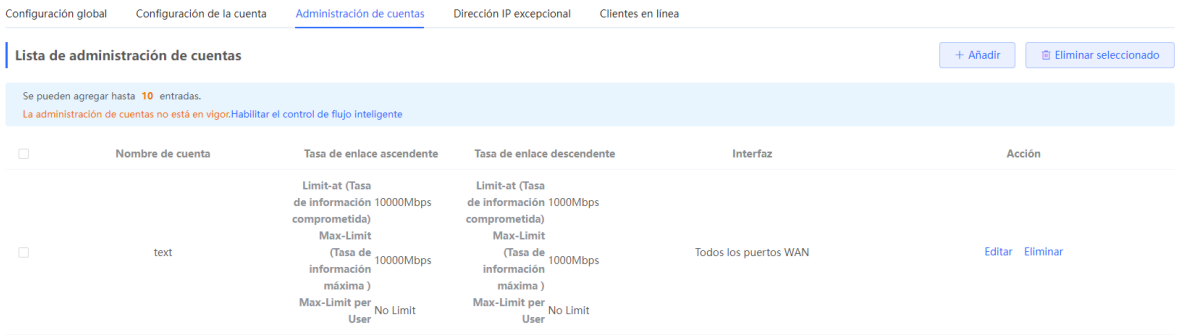
Parámetro	Descripción
Control de flujo	Especifique si se aplica el control de flujo a esta cuenta. Si decide habilitarlo, configure las directivas de control de flujo para la autenticación de usuarios PPPoE. Si deshabilita el control de flujo inteligente, deshabilite la opción **Control de flujo**. Para habilitar **Control de flujo**, habilite primero el control de flujo inteligente. Para conocer más sobre cómo configurar el control de flujo inteligente, consulte la sección 4.12.2 Control de flujo inteligente.
Administración de cuentas	Después de activar el control de flujo, configure un paquete de control de flujo para la cuenta actual con el fin de restringir el uso de ancho de banda de los usuarios en consecuencia. Para conocer más sobre cómo configurar y visualizar los paquetes de control de flujo, consulte la sección 4.14.4 Configuración de un paquete de control de flujo.

4.14.4 Configuración de un paquete de control de flujo

Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Servidor PPPoE** > **Administración de cuentas**.

Si el control de flujo inteligente se deshabilitó, el paquete de control de flujo para la cuenta no se hará efectivo. Antes de configurar un paquete, habilite el control de flujo inteligente. Para más información sobre cómo configurar el control de flujo inteligente, consulte la sección 4.12.2 Control de flujo inteligente.

Haga clic en **Añadir** para crear un paquete de control de flujo. Los paquetes creados se muestran en la **Lista de administración de cuentas**. Estos se pueden modificar o eliminar.



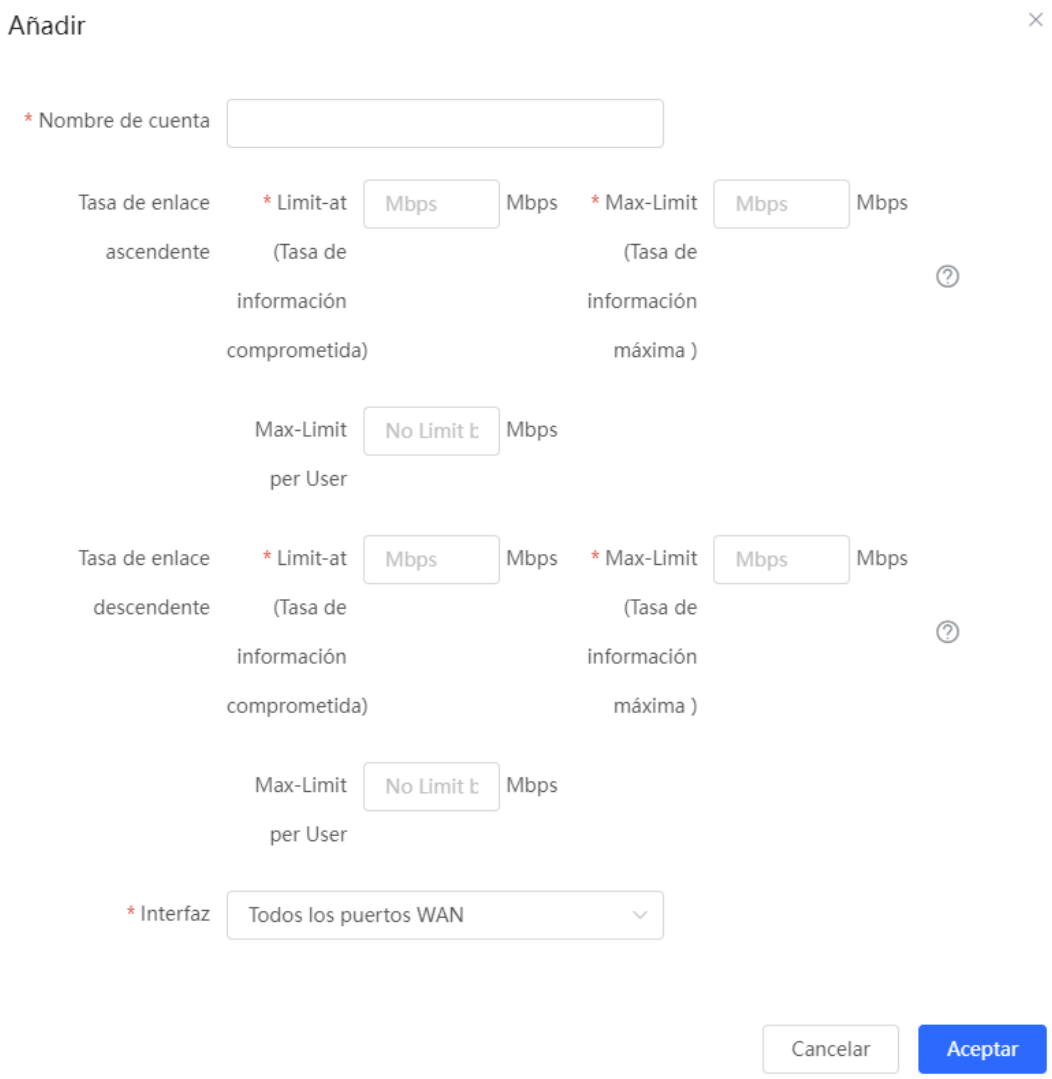


Tabla 4- 9 Configuración de paquetes de control de flujo de usuarios PPPoE

Parámetro	Descripción
Nombre de cuenta	Configure el nombre del paquete de control de flujo. Cuando configure una cuenta de autenticación, seleccione un paquete de control de flujo basado en el nombre.
Tasa de información comprometida de enlaces ascendentes/descendentes	Especifique la tasa de información comprometida (CIR) de los enlaces ascendentes y descendentes para una cuenta de autenticación cuando el ancho de banda sea insuficiente.
Tasa de información máxima de enlaces ascendentes/descendentes	Especifique la tasa de información máxima (PIR) de los enlaces ascendentes y descendentes que puede usar una cuenta de autenticación cuando el ancho de banda es suficiente.

Parámetro	Descripción
Tasa de información máxima por usuario de enlaces ascendentes/descendentes	Especifique la tasa de información máxima que puede consumir cada usuario. Este parámetro es opcional. Por defecto, la tasa de información máxima por usuario no se encuentra limitada.
Interfaz	Especifique la interfaz para la cual aplica el paquete de control de flujo.

4.14.5 Configuración de direcciones IP excepcionales

Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Servidor PPPoE** > **Dirección IP excepcional**.

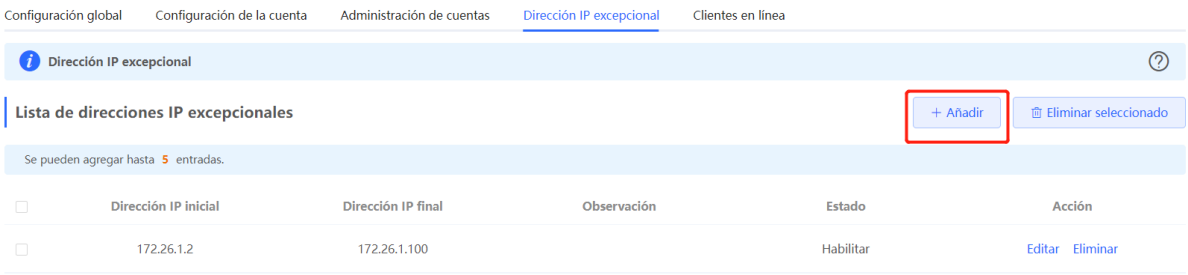
Para configurar clientes con algunas direcciones IP en una VLAN específica para tener acceso a Internet sin pasar por una cuenta y contraseña de autenticación, estas direcciones IP se pueden configurar como excepcionales en el dispositivo habilitado con un servidor PPPoE.

Las direcciones IP excepcionales creadas se muestran en **Lista de direcciones IP excepcionales**. Haga clic en **Editar** para modificar una dirección IP excepcional y en **Eliminar** para borrarlas.

Dirección IP inicial/ Dirección IP final: indica la dirección IP excepcional de inicio o la dirección IP excepcional final.

Observación: indica la descripción de una dirección IP excepcional.

Estado: indica si una dirección IP excepcional es válida.



4.14.6 Revisión de usuarios en línea

Cambie al modo **Dispositivo local**. Seleccione **Avanzado** > **Servidor PPPoE** > **Clientes en línea**.

Revise la información acerca de los usuarios finales que tienen acceso a Internet a través de la marcación PPPoE. Haga clic en **Desconectar** para desconectar al usuario del servidor PPPoE.

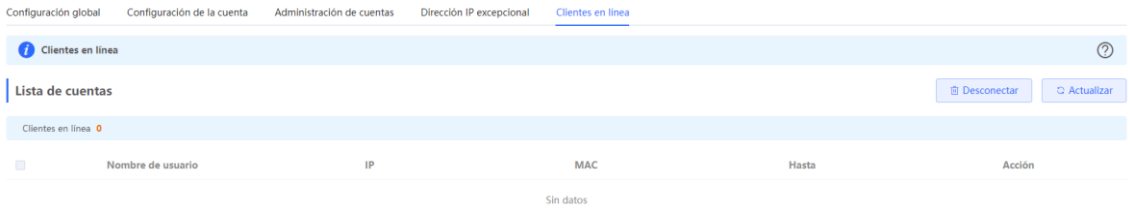


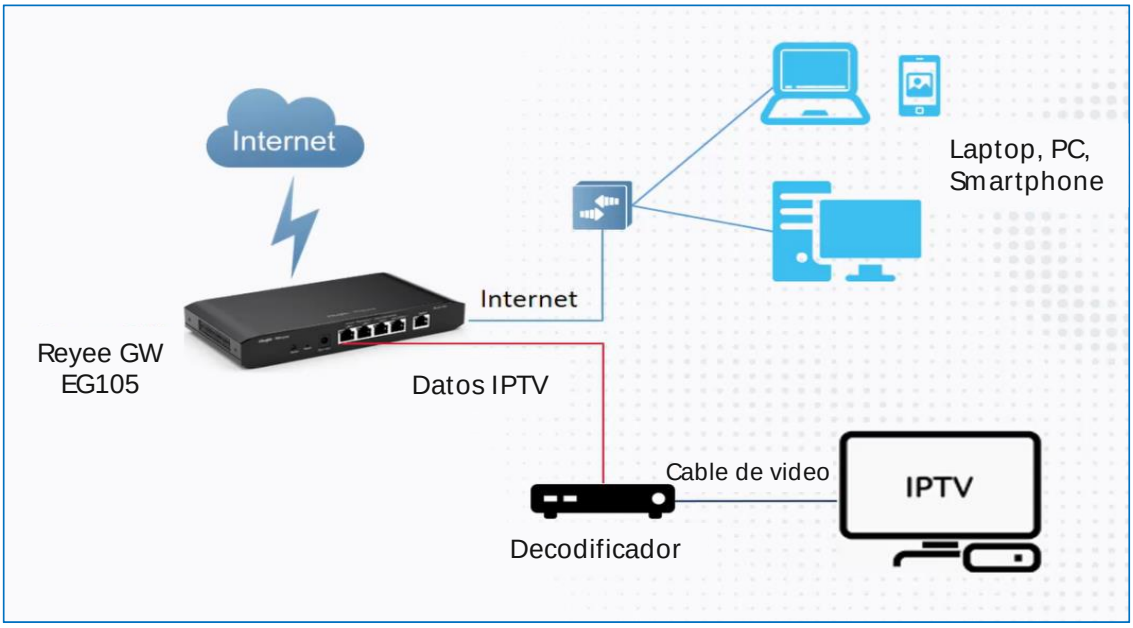
Tabla 4- 10 Información sobre los clientes PPPoE en línea

Parámetro	Descripción
Nombre de usuario	Número total de usuarios finales en línea que tienen acceso a Internet a través de la marcación PPPoE.
IP	Dirección IP del cliente.
MAC	Dirección MAC del cliente.
Tiempo en línea	Hora en la que el usuario accede a Internet.

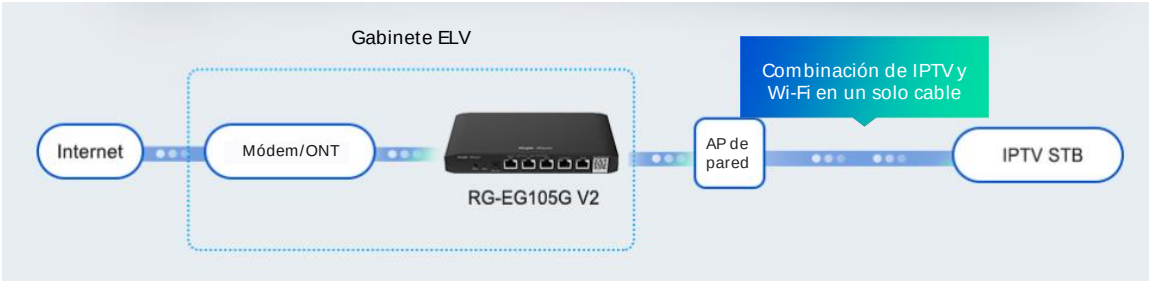
4.15 IPTV

4.15.1 Escenario de aplicación

- **Escenario 1: escenario de WAN dual**



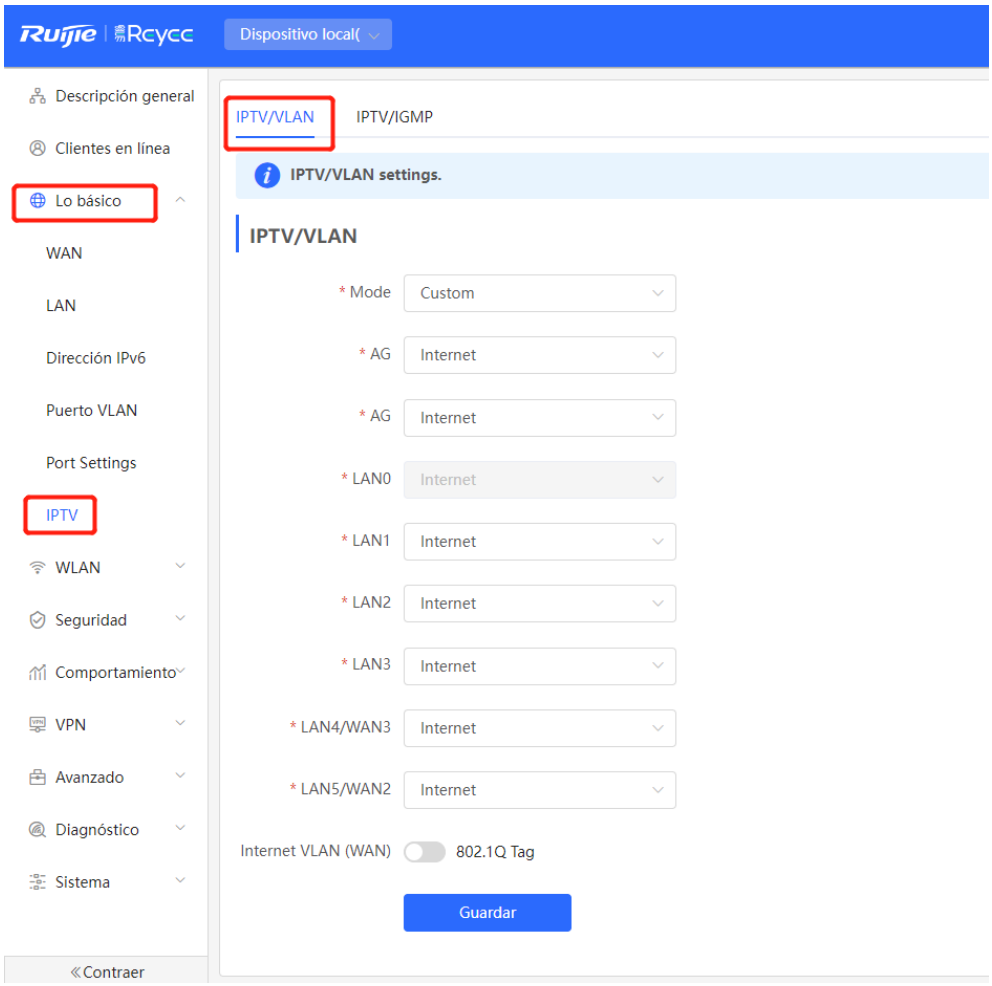
- **Escenario 2: escenario de WAN única**



4.15.2 Configuración de Dual WAN

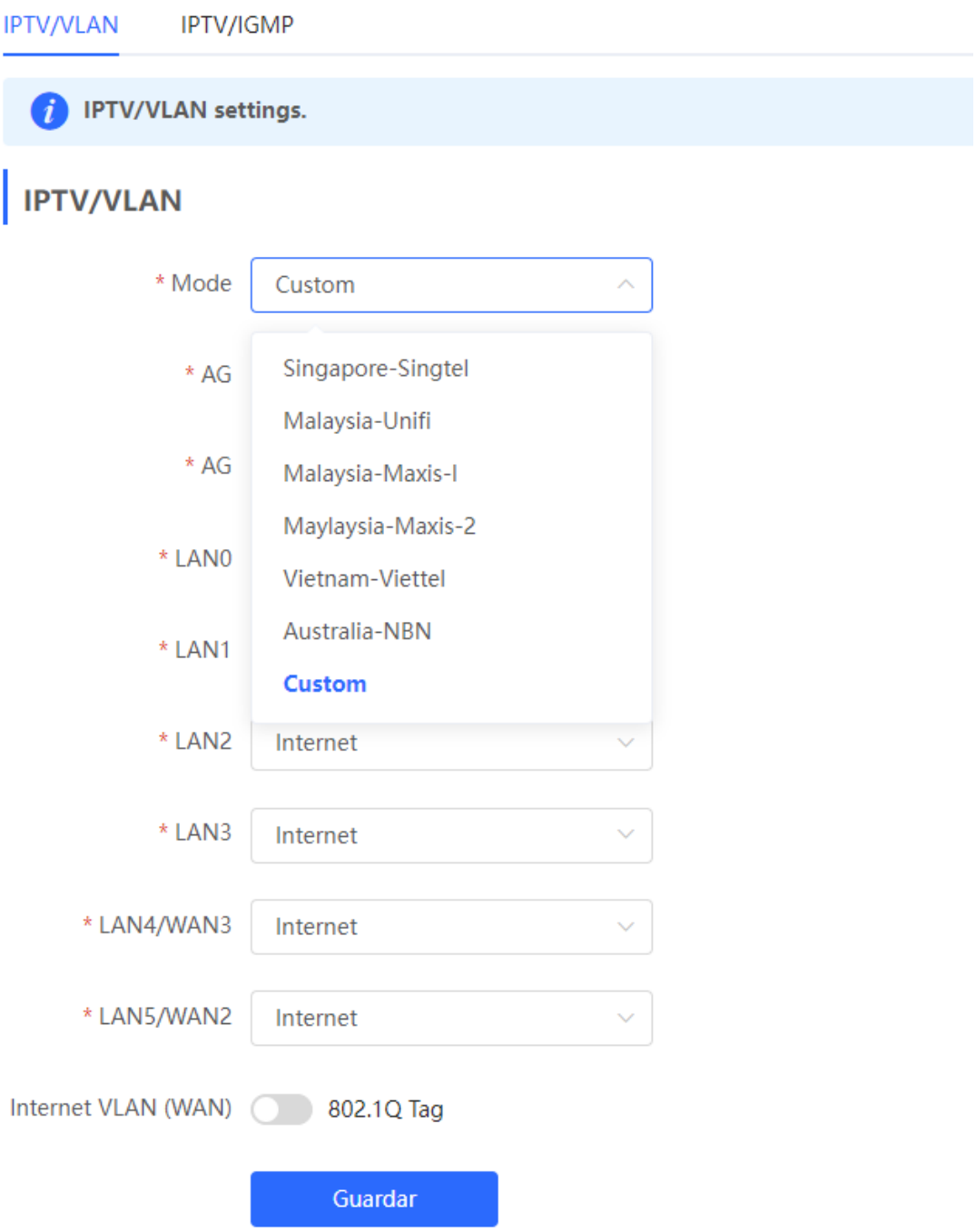
(1) Conecte el cable ISP a un puerto WAN y su PC a un puerto LAN. Utilice la dirección IP predeterminada 192.168.110.1 para iniciar sesión en su Reyee EG y configúrelo para acceder a Internet de manera exitosa, de acuerdo con el asistente de configuración.

(2) Cambie al modo **Dispositivo local**. Seleccione **Lo básico** > **IPTV** > **IPTV/VLAN**.

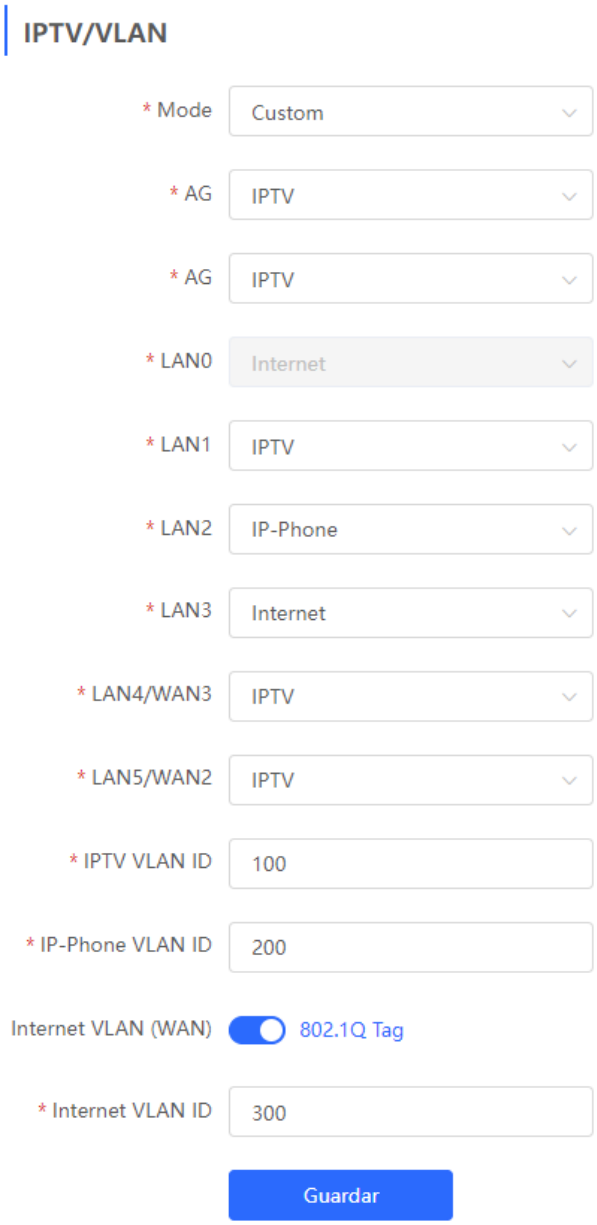


(3) Configure **IPTV VLAN ID** o **IP-Phone VLAN ID**.

- Si se encuentra en cualquiera de las siguientes regiones dentro de la lista del recuadro rojo, podrá seleccionar directamente el modo.



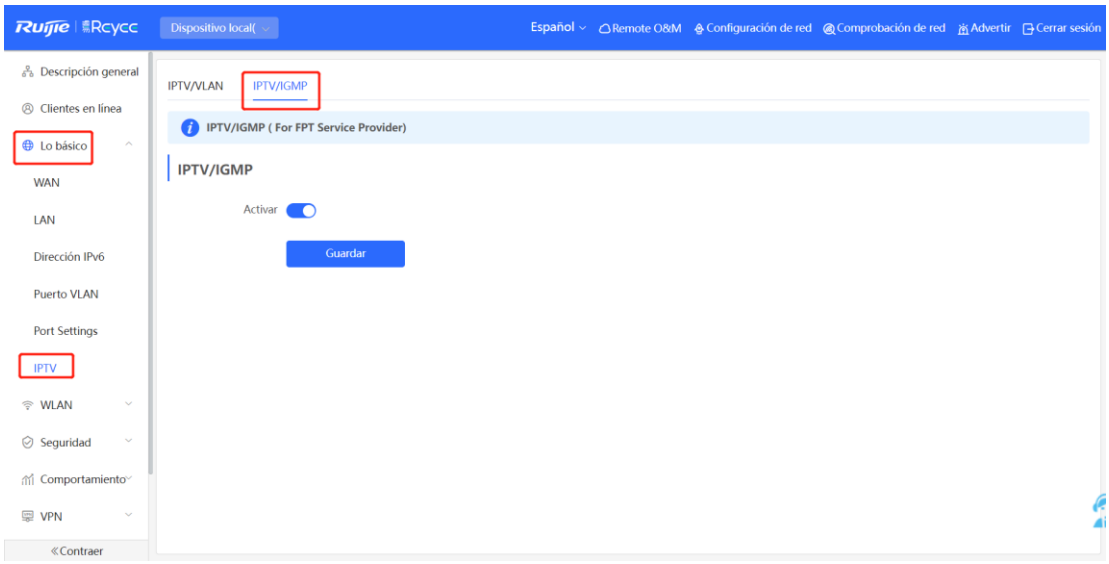
- Si no se encuentra en alguna de estas regiones, seleccione **Custom**. Luego, póngase en contacto con un ISP para la configuración de la IPTV y conéctela junto con el teléfono IP con puertos LAN. Por ejemplo, las VLAN ID para IPTV, el teléfono IP e Internet son 100, 200 y 300, respectivamente.



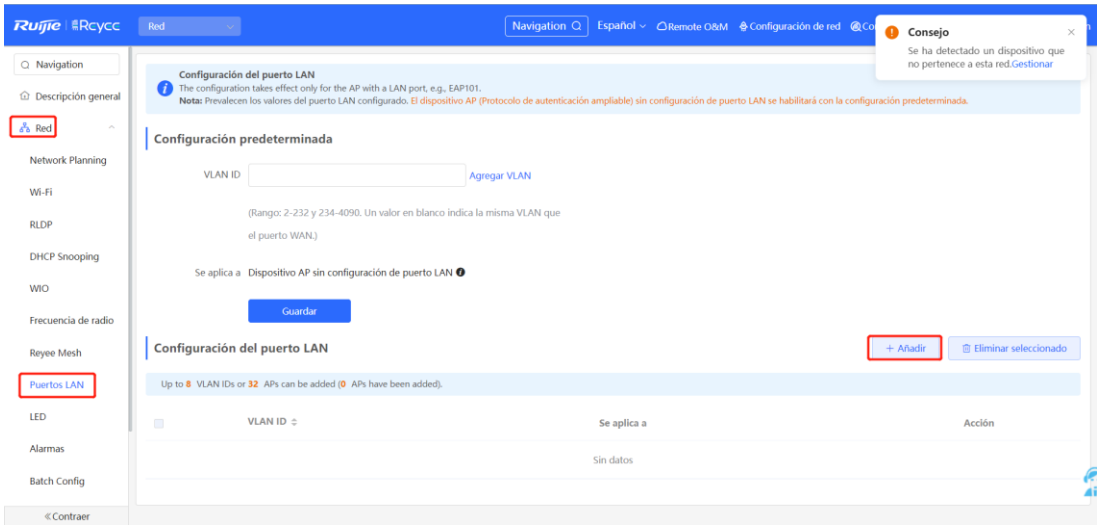
4.15.3 Configuración de una WAN individual

Después de que la configuración de la IPTV en el Reyee EG con un solo puerto WAN se haya completado, configure la IPTV VLAN 100 en el puerto LAN del AP de pared. Si el router tiene dos puertos WAN, ignore este paso.

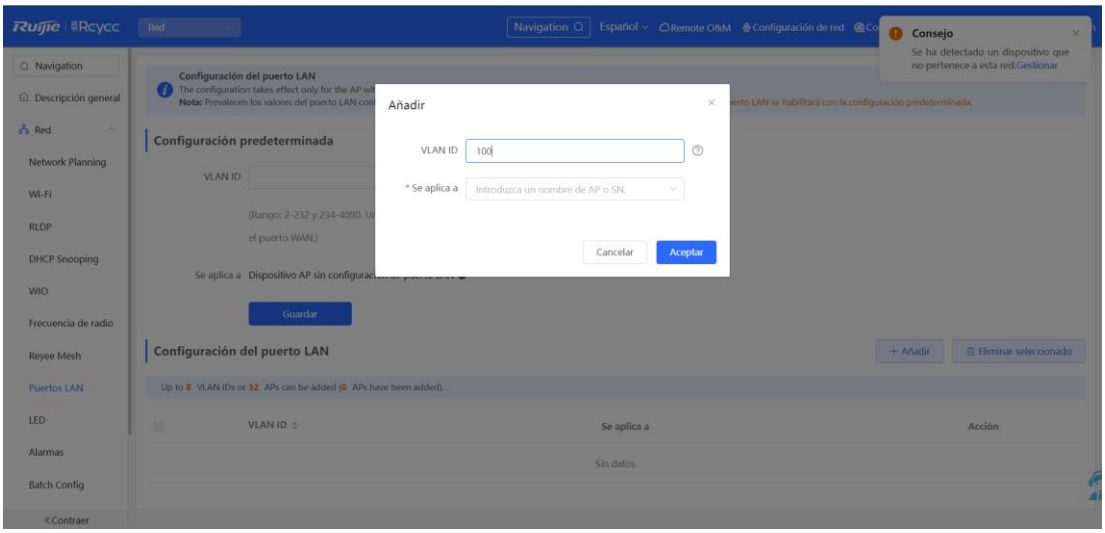
(1) Inicie sesión en el sistema de gestión web. Seleccione **Lo básico** > **IPTV** > **IPTV/IGMP** y habilite **IPTV/IGMP**.



(2) Inicie sesión en el sistema de gestión web de un AP de pared. Cambie al modo **Red** y seleccione **Red** > **Puertos LAN** > **Añadir**.



Ajuste la VLAN ID en 100 para el AP de pared.



Precaución

Solamente el Reyee OS 1.55 y versiones posteriores son compatibles con IPTV.

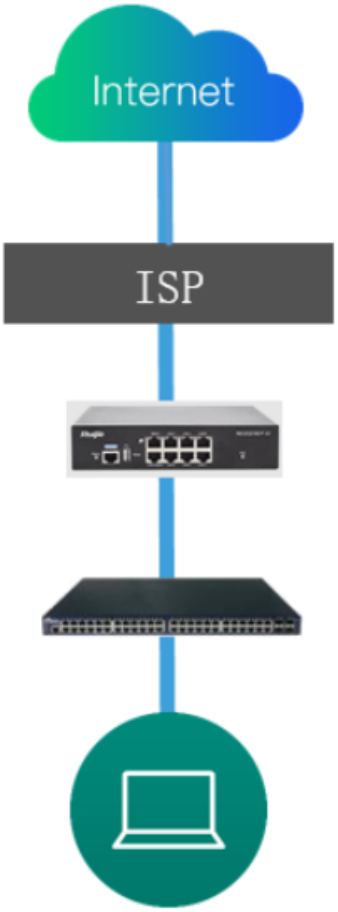
4.16 UPnP

Escenario de aplicación

Con la función Universal Plug and Play (UPnP) habilitada, el dispositivo puede cambiar el puerto utilizado por el servicio de Internet de la terminal, a solicitud de esta, logrando una conversión NAT. Cuando una terminal en Internet desea acceder a los recursos de la intranet del dispositivo, este puede añadir automáticamente entradas de mapeo de puertos para realizar la transmisión del servicio a través de las redes, tanto internas como externas. Entre las aplicaciones comunes que admiten el protocolo UPnP se encuentran MSN Messenger, Thunder, BTT y PPLive.

Existen tres requerimientos para utilizar UPnP:

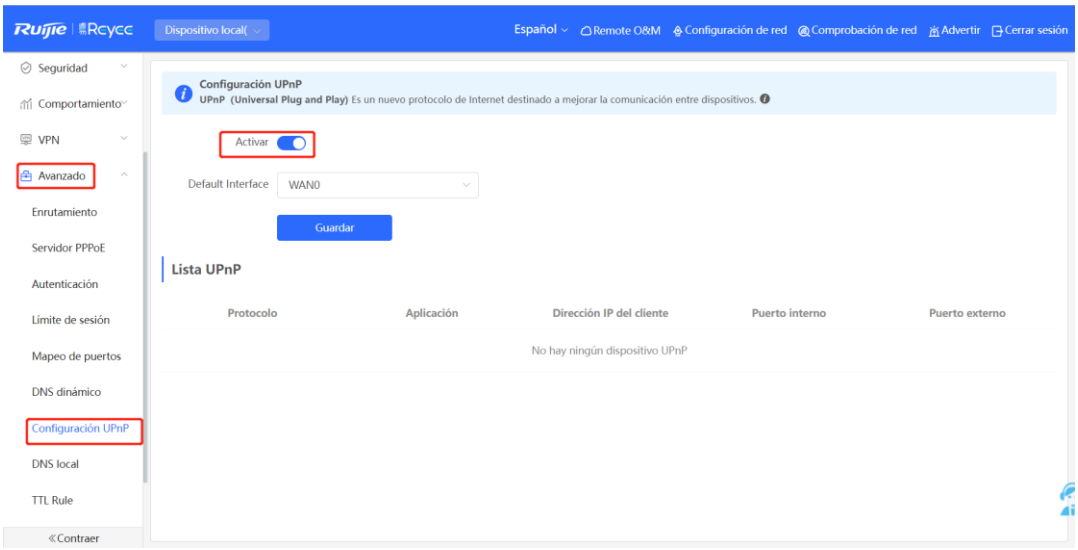
- El dispositivo debe estar habilitado con UPnP.
- El sistema operativo de los hosts internos debe ser compatible con UPnP.
- Las aplicaciones deben ser compatibles con UPnP.



Procedimiento

(1) Cambie al modo **Dispositivo local**. Seleccione **Avanzado > Configuración UPnP > Activar** para habilitar UPnP en su teléfono o PC.

(2) El router detectará automáticamente su dispositivo y habilitará el mapeo de puertos para el mismo. Finalmente, podrá utilizar la dirección IP y el puerto externos para acceder al servicio de su teléfono o PC.


Dispositivo local(
Español
Remote O&M
Configuración de red
Comprobación de red
Advertir
Cerrar sesión
Seguridad
Comportamiento
VPN
Avanzado
Enrutamiento
Servidor PPPoE
Autenticación
Límite de sesión
Mapeo de puertos
DNS dinámico
Configuración UPnP
DNS local
TTL Rule
«Contraer
Configuración UPnP
UPnP (Universal Plug and Play) Es un nuevo protocolo de Internet destinado a mejorar la comunicación entre dispositivos.
Activar
Default Interface
WAN0
Guardar
Lista UPnP
Protocolo
Aplicación
Dirección IP del cliente
Puerto interno
Puerto externo
No hay ningún dispositivo UPnP

5 Guía de soluciones avanzadas

5.1 Solución para el control de flujo en los dispositivos Reyee

5.1.1 Escenario de aplicación

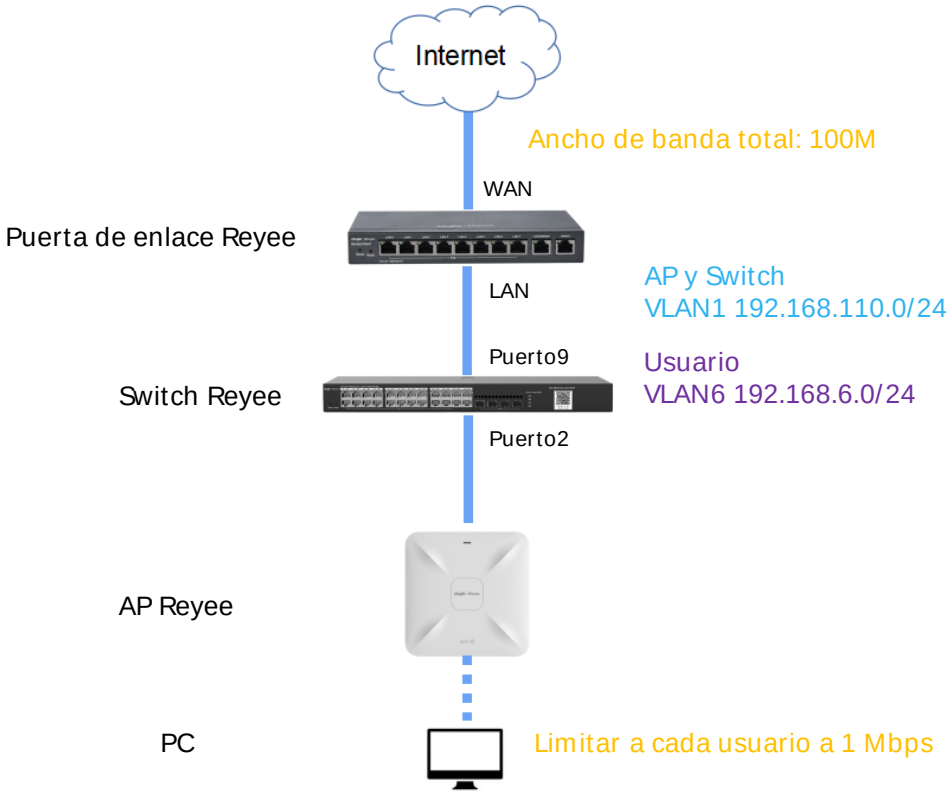
El control de flujo se utiliza para configurar los límites de velocidad de carga y descarga de datos de los clientes. Al configurar el control de flujo, el router puede proteger el ancho de banda de la red para que no sea demasiado ocupada por algunos clientes.

5.1.2 Ejemplo de configuración

Requisitos

El ancho de banda total del EG está limitado a 100 Mbps y la velocidad de cada usuario en el segmento de red de VLAN6 está limitado a 1 Mbps.

Topología de la red



Descripción de la red

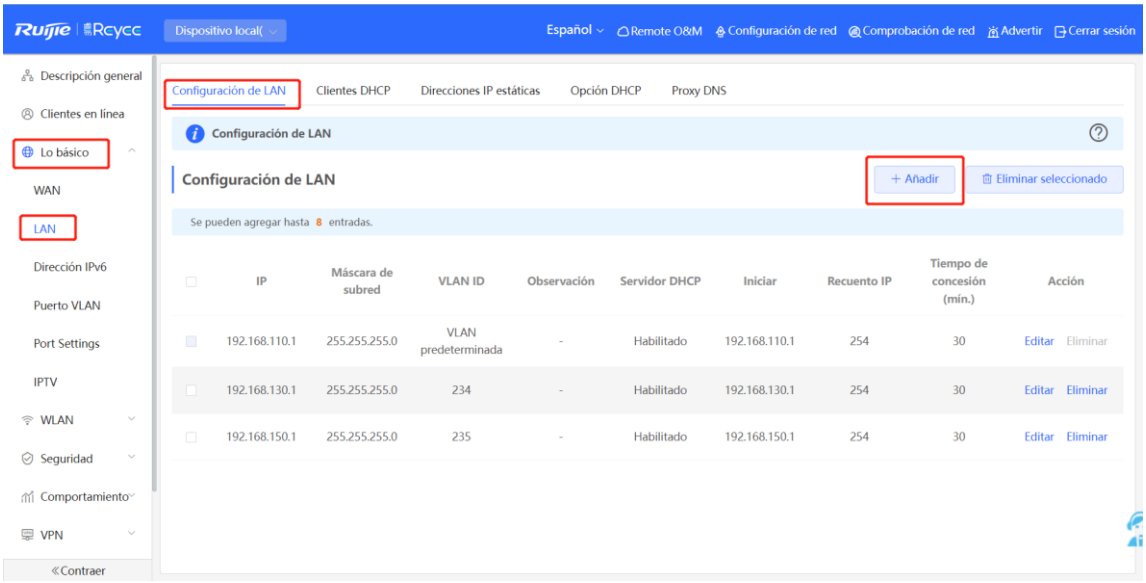
- El EG actúa como servidor DHCP para asignar direcciones IP a los usuarios, al AP Reyee y al switch Reyee.
- El AP y el switch Reyee obtienen la dirección IP 192.168.110.0/24 en el segmento de red de VLAN 1 para tener acceso a Internet.
- Los usuarios obtienen la dirección IP 192.168.6.0/24 en el segmento de red de VLAN 6 para tener acceso a

Internet.

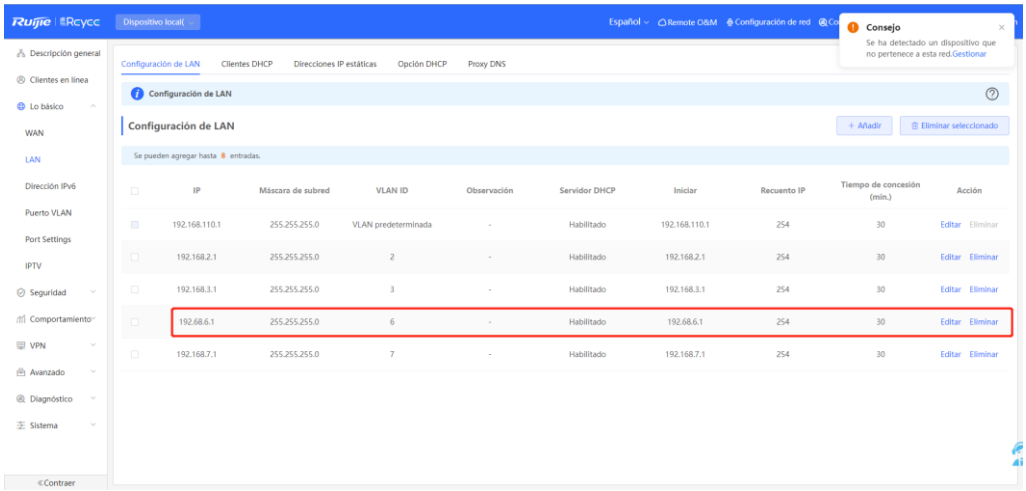
Pasos para la configuración

(1) Realice la configuración básica de la red.

a Cambie al modo **Dispositivo local**. Seleccione **Lo básico** > **LAN** > **Configuración de LAN** > **Añadir** y realice la configuración de la LAN y de los grupos de direcciones de DHCP de las VLAN 1 y VLAN 6 en el router.



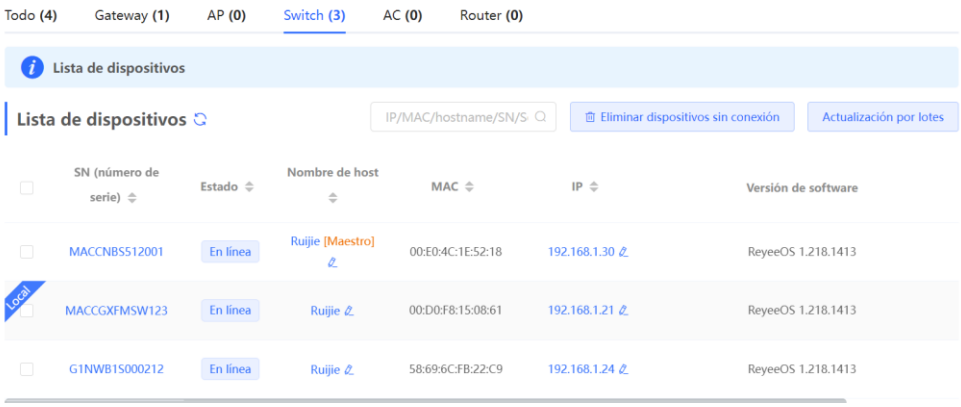

Añadir
* IP
192.168.120.1
* Máscara de subred
255.255.255.0
* VLAN ID
Observación
Observación
MAC
00:D0:F8:55:2E:56
Servidor DHCP
* Iniciar
192.168.120.1
* Recuento IP
254
* Tiempo de concesión (mín.)
30
Servidor DNS 192.168.120.1
Cancelar
Aceptar


Ruijie | Rcycc
Dispositivo local
Español
Remote O&M
Configuración de red
Consejo
Se ha detectado un dispositivo que no pertenece a esta red.Gestionar
Descripción general
Clientes en línea
Lo básico
WAN
LAN
Dirección IPv6
Puerto VLAN
Port Settings
IPTV
Seguridad
Comportamiento
VPN
Avanzado
Diagnóstico
Sistema
Contraer
Configuración de LAN
Clientes DHCP
Direcciones IP estáticas
Opción DHCP
Proxy DNS
Configuración de LAN
Configuración de LAN
+ Añadir
Eliminar seleccionado
Se pueden agregar hasta 8 entradas.
IP
Máscara de subred
VLAN ID
Observación
Servidor DHCP
Iniciar
Recuento IP
Tiempo de concesión (min.)
Acción
192.168.110.1 255.255.255.0 VLAN predeterminada - Habilitado 192.168.110.1 254 30 Editar Eliminar
192.168.2.1 255.255.255.0 2 - Habilitado 192.168.2.1 254 30 Editar Eliminar
192.168.3.1 255.255.255.0 3 - Habilitado 192.168.3.1 254 30 Editar Eliminar
192.68.6.1 255.255.255.0 6 - Habilitado 192.68.6.1 254 30 Editar Eliminar
192.168.7.1 255.255.255.0 7 - Habilitado 192.168.7.1 254 30 Editar Eliminar

Precaución

El segmento de red 192.168.110.0/24 está configurado para la VLAN 1.

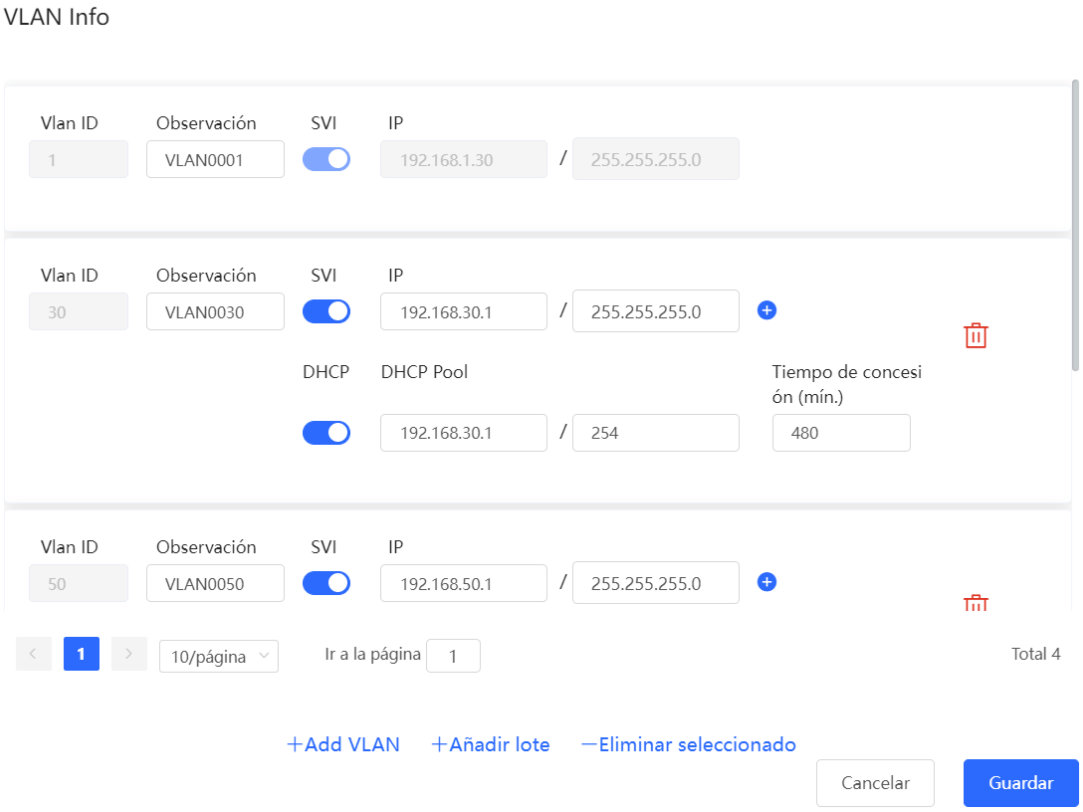
(2) Cambie al modo **Red**. Seleccione **Dispositivos > Switch**.



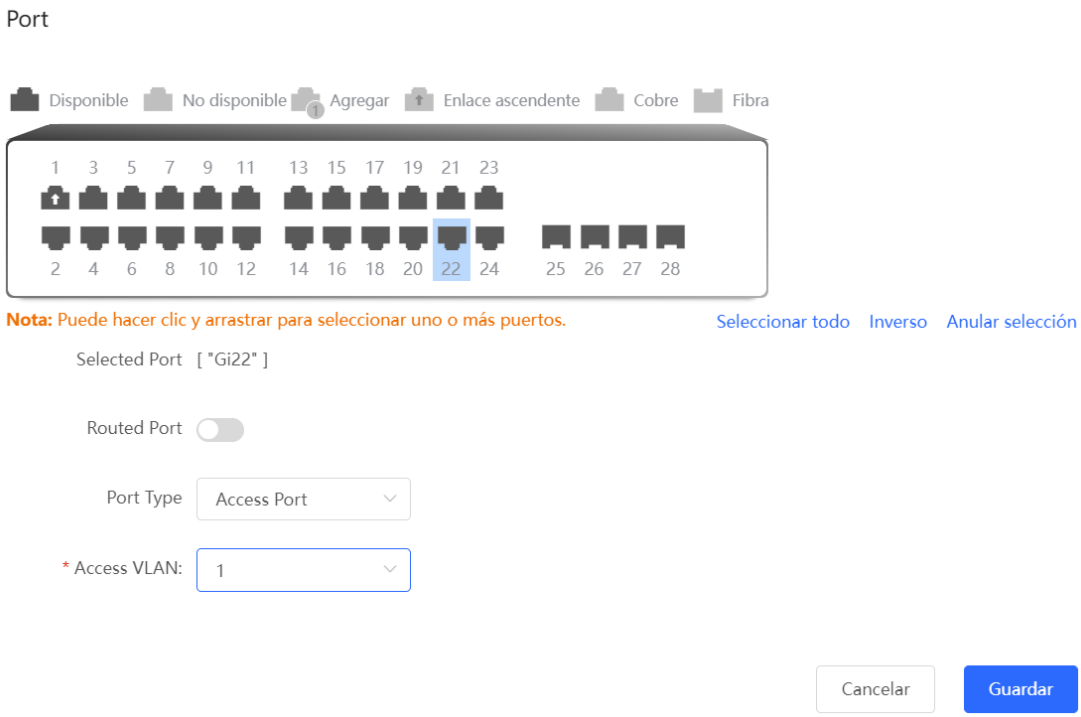
a Seleccione un dispositivo de **Lista de dispositivos** e ingrese a la página de configuración.

b En la ventana de **VLAN**, seleccione una VLAN y haga clic en **Edit** para configurarla.

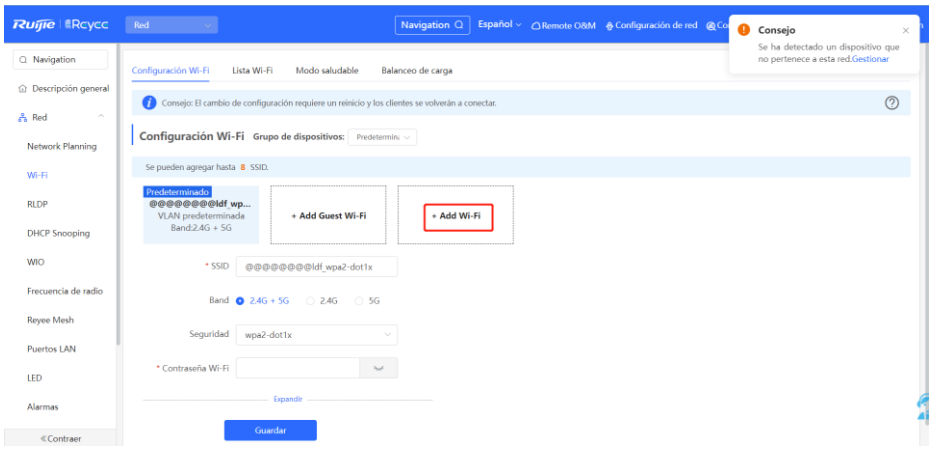
c Haga clic en **Add VLAN** para crear la VLAN 6 en el conmutador.

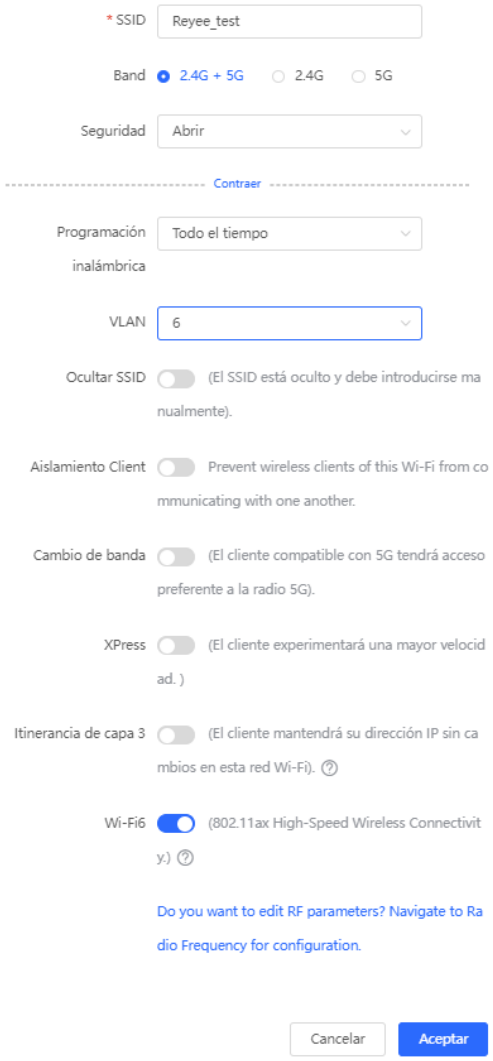


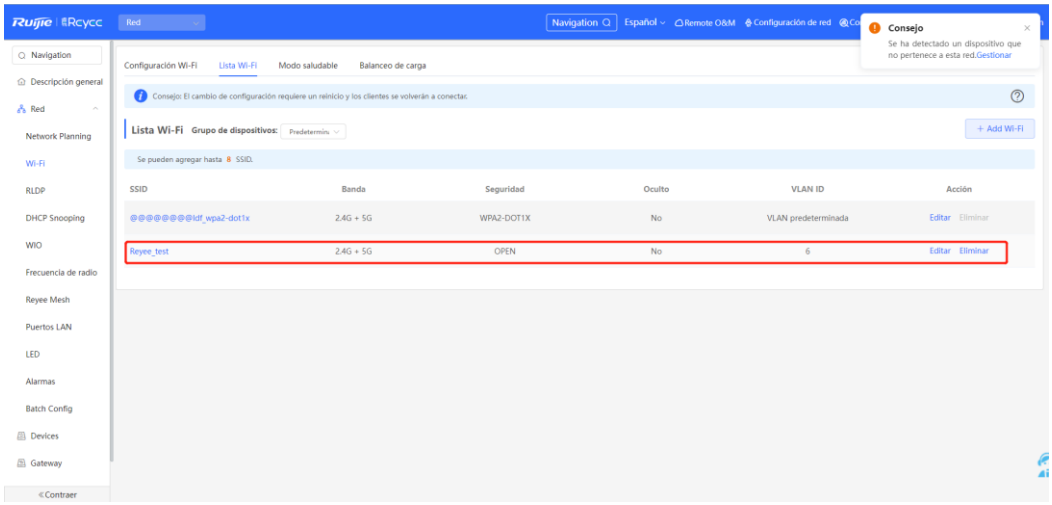
d En la ventana de **Port**, haga clic en **Edit**, configure el puerto2 y el puerto9 conectados al AP y el EG como puertos troncales y configúrelos para permitir que los paquetes de las VLAN 1 y VLAN 6 pasen. Luego, revise la configuración de puertos en el conmutador.



(3) Cambie al modo **Red**. Seleccione **Red > Wi-Fi > Configuración Wi-Fi**, configure el SSID como **Reyee_test** y asócielo con la VLAN 6.

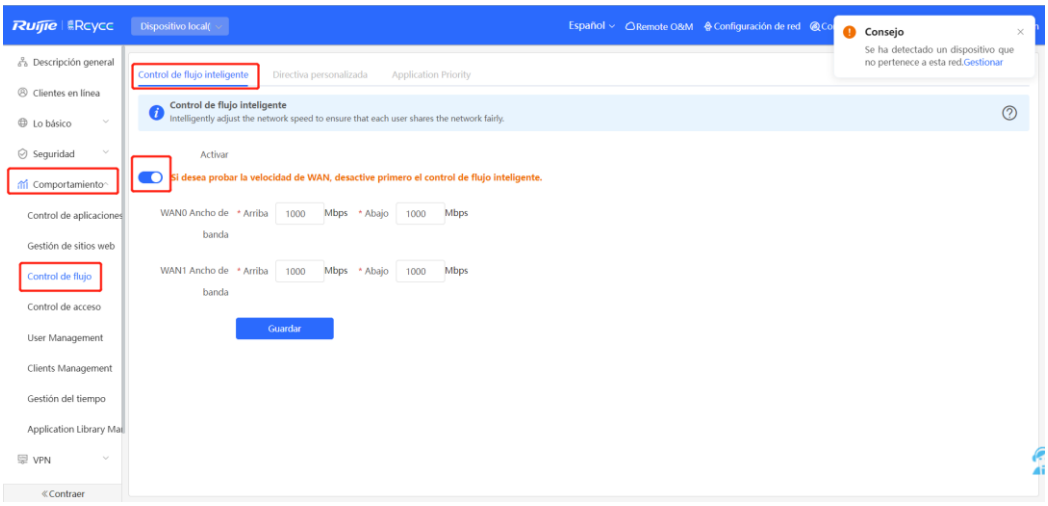




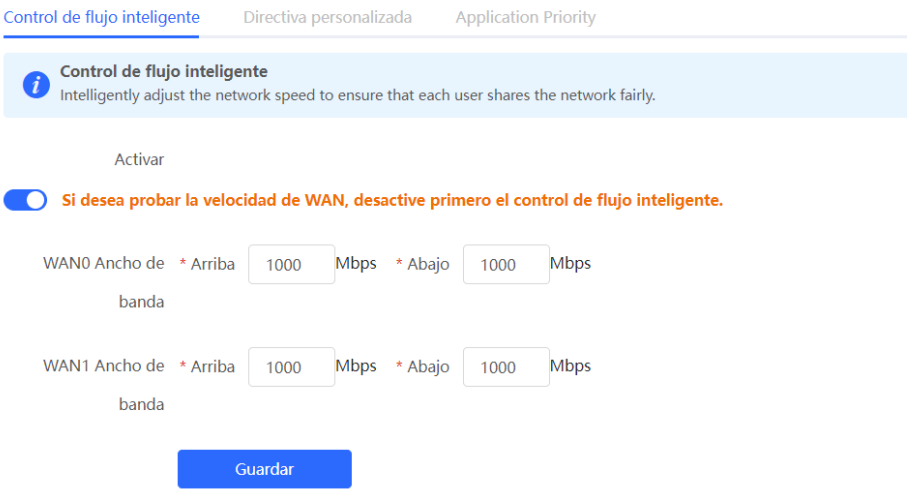


(4) Configure el control de flujo inteligente.

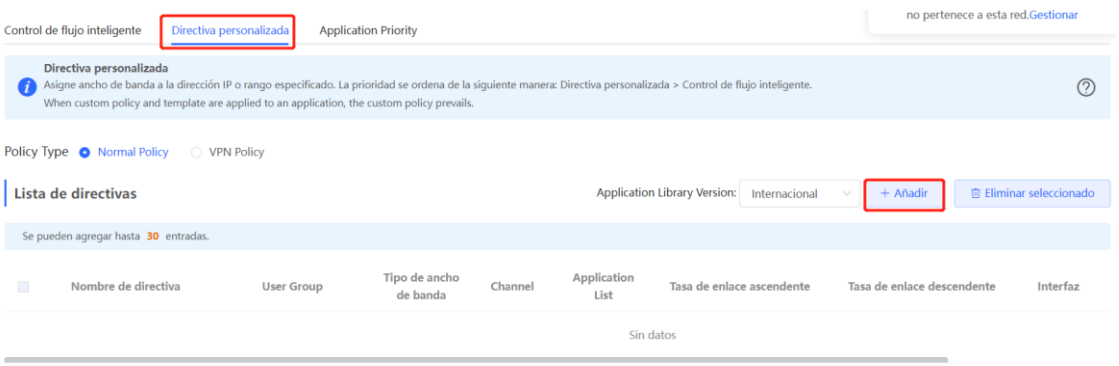
a Cambie al modo **Dispositivo local**. Seleccione **Comportamiento > Control de flujo > Control de flujo inteligente** y habilite el **Control de flujo inteligente**.



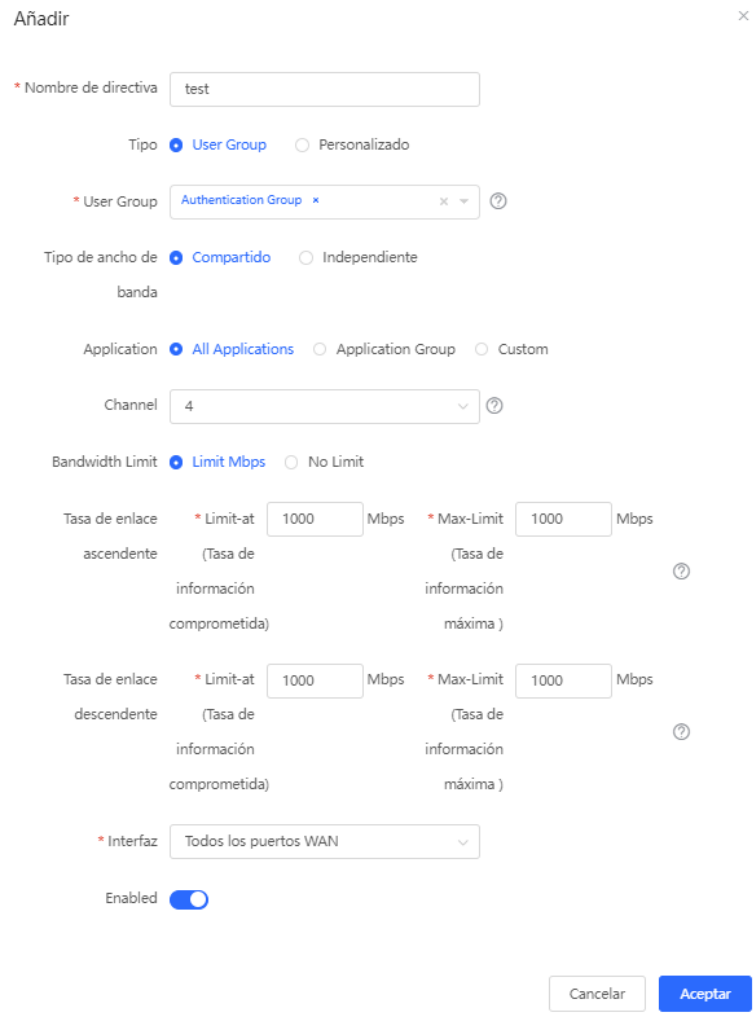
b Configure los valores del ancho de banda WAN de los enlaces ascendentes y descendentes en 100 Mbps, y haga clic en **Guardar**.



c Después de realizar el paso 2, se mostrará la **Directiva personalizada**. Haga clic en **Añadir** para agregar la directiva.



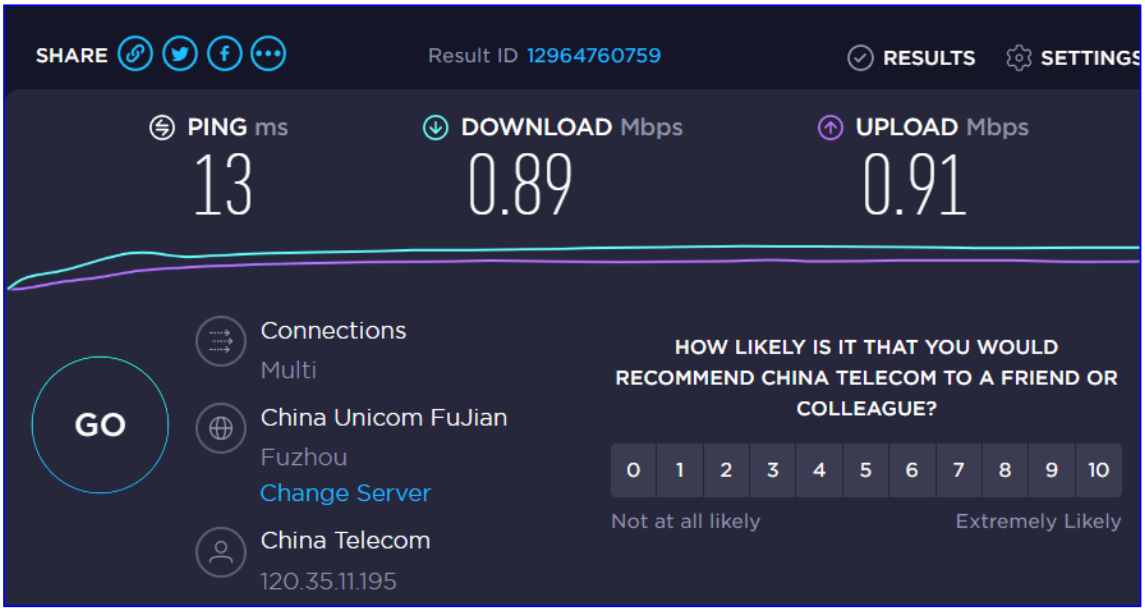
Configure el nombre de la directiva, el rango de IP, el tipo de ancho de banda y los demás parámetros.



- **Tipo de ancho de banda**
  - **Compartido**: indica que el ancho de banda total lo comparten todas las direcciones IP.
  - **Independiente**: indica que el límite de velocidad está configurado para cada dirección IP.
- **Tasa de información comprometida**: es la velocidad de la información comprometida.
- **Tasa de información máxima**: es el pico de la velocidad de la información.

5.1.3 Verificación de la configuración

Utilice la herramienta Speedtest para revisar que la velocidad de cada usuario se encuentre limitada a 1 Mbps.



5.2 Solución para la autenticación en la nube de dispositivos Reyee

5.2.1 Principio de funcionamiento

La autenticación en la nube permite controlar el acceso de los usuarios a la red inalámbrica. La configuración se sincronizará desde Ruijie Cloud al EG local. En la autenticación de portales, todas las solicitudes HTTP de los clientes se redirigirán primero a una página de autenticación en la que se les solicita a los clientes su autenticación, el pago y la aceptación del contrato de la licencia de usuario final, la política de uso adecuado y el completar la encuesta, entre otras credenciales válidas, para que puedan visitar Internet después de completar el proceso de autenticación de manera exitosa.

5.2.2 Escenario de aplicación

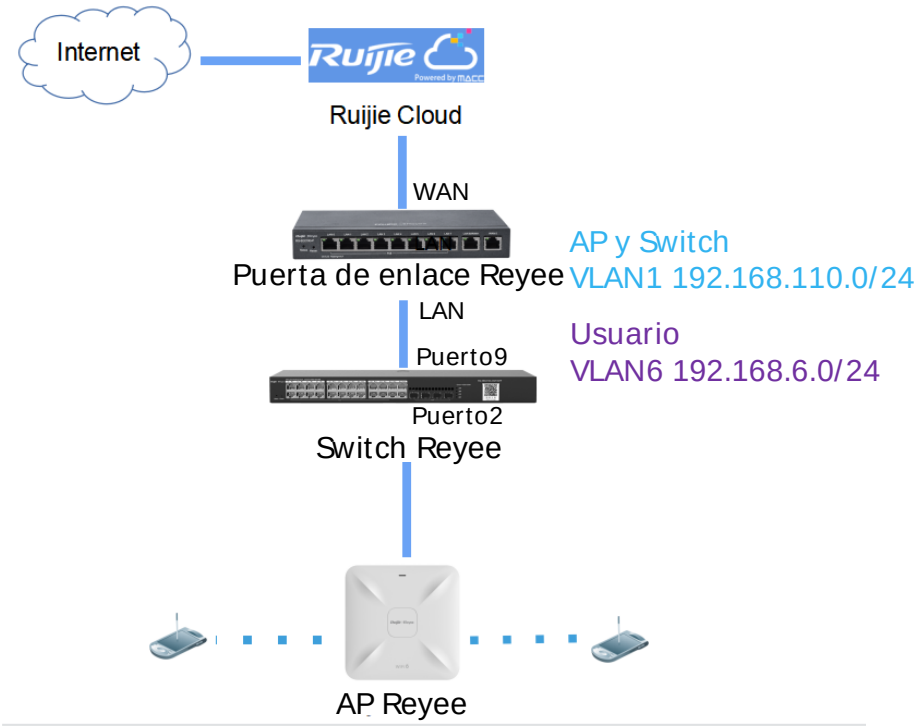
La autenticación mediante portal, también conocida como autenticación web, suele utilizarse en redes de acceso para invitados (como las de un hotel o una cafetería) para controlar el acceso a Internet de los clientes.

5.2.3 Ejemplo de configuración

Requisitos

Los usuarios deben hacer el proceso de autenticación antes de que se les permita el acceso a Internet. El AP Reyee no es compatible con la autenticación de la nube y el Reyee EG requiere autenticar a los usuarios.

Topología de la red



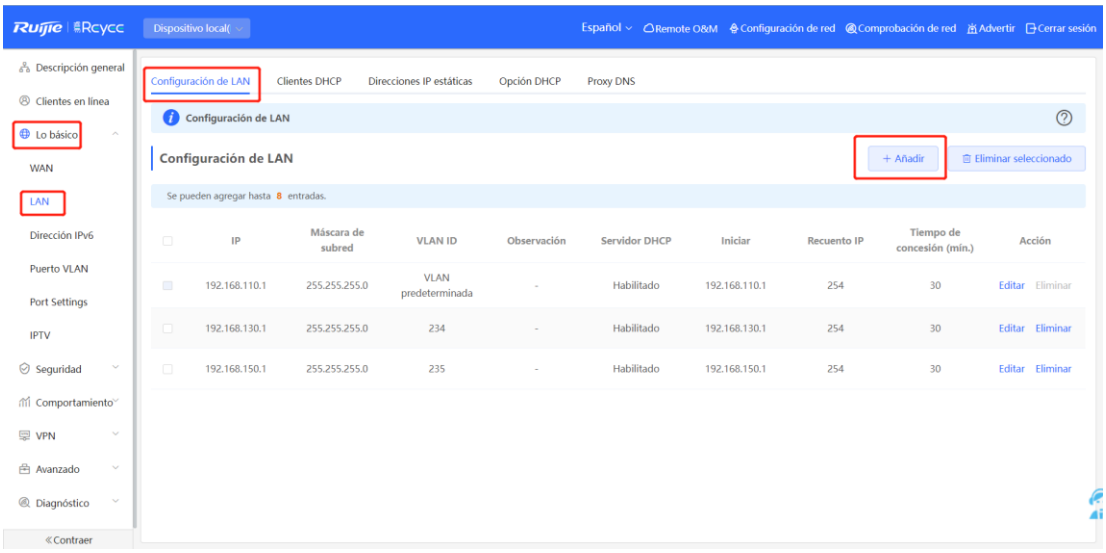
Descripción de la red

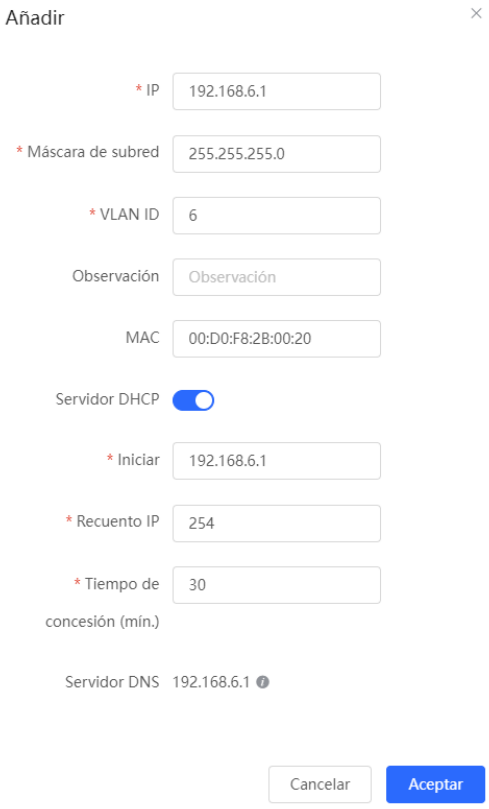
- El EG actúa como servidor DHCP para asignar direcciones IP a los usuarios, al AP Reyee y al switch Reyee.
- El AP y el switch Reyee obtienen la dirección IP 192.168.110.0/24 en el segmento de red de VLAN 1 para tener acceso a Internet.
- Los usuarios obtienen la dirección IP 192.168.6.0/24 en el segmento de red de VLAN 6 para tener acceso a Internet.
- Ruijie Cloud administra y monitorea el dispositivo, el estado del cliente y proporciona una autenticación de portal cautivo para los clientes.

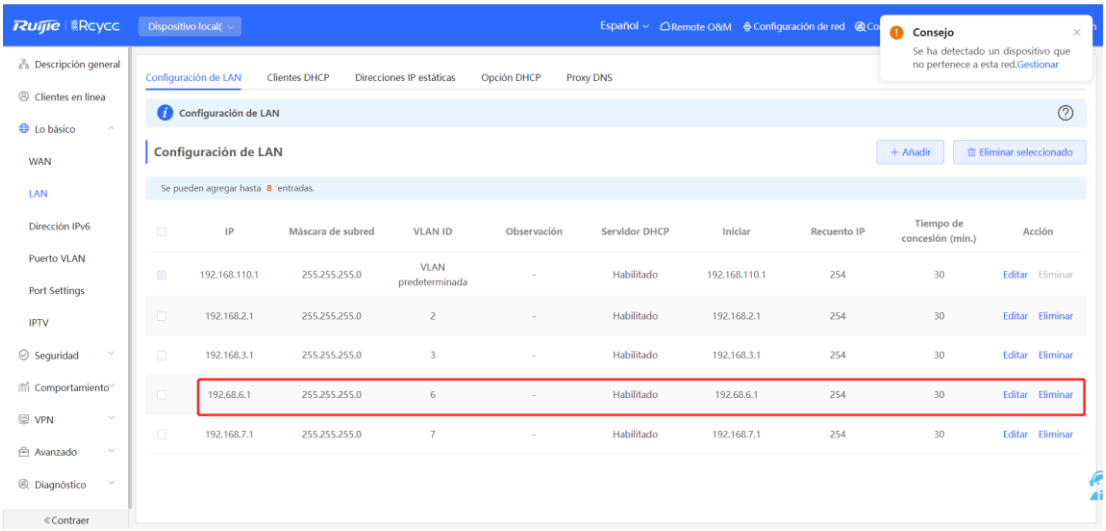
Pasos para la configuración

(1) Configure la red básica.

a Cambie al modo **Dispositivo local**. Seleccione **Lo básico** > **LAN** > **Configuración de LAN** > **Añadir** y configure una LAN y el grupo de direcciones de DHCP de las VLAN 1 y VLAN 6 en el router.


Dispositivo local(
Español
Remote O&M
Configuración de red
Comprobación de red
Advertir
Cerrar sesión
Descripción general
Clientes en línea
Lo básico
WAN
LAN
Dirección IPv6
Puerto VLAN
Port Settings
IPTV
Seguridad
Comportamiento
VPN
Avanzado
Diagnóstico
Contraer
Configuración de LAN
Clientes DHCP
Direcciones IP estáticas
Opción DHCP
Proxy DNS
Configuración de LAN
Configuración de LAN
+ Añadir
Eliminar seleccionado
Se pueden agregar hasta 8 entradas.
IP
Máscara de subred
VLAN ID
Observación
Servidor DHCP
Iniciar
Recuento IP
Tiempo de concesión (mín.)
Acción
192.168.110.1 255.255.255.0 VLAN predeterminada - Habilitado 192.168.110.1 254 30 Editar Eliminar
192.168.130.1 255.255.255.0 234 - Habilitado 192.168.130.1 254 30 Editar Eliminar
192.168.150.1 255.255.255.0 235 - Habilitado 192.168.150.1 254 30 Editar Eliminar

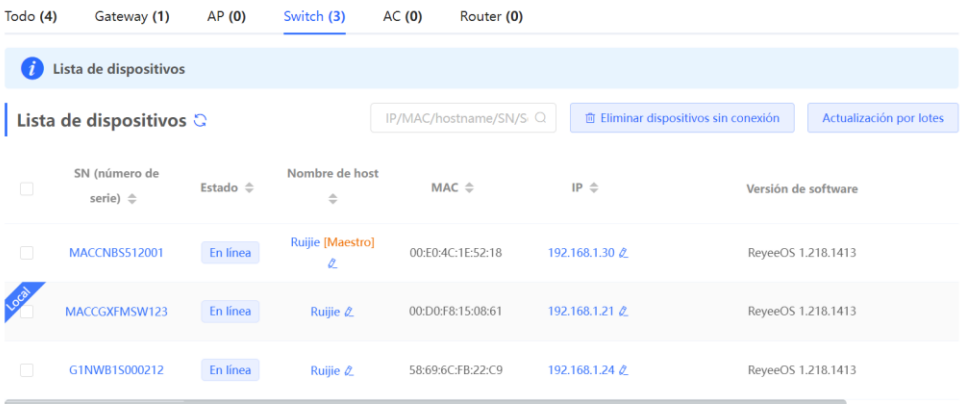

Añadir
* IP 192.168.6.1
* Máscara de subred 255.255.255.0
* VLAN ID 6
Observación Observación
MAC 00:D0:F8:2B:00:20
Servidor DHCP
* Iniciar 192.168.6.1
* Recuento IP 254
* Tiempo de concesión (mín.) 30
Servidor DNS 192.168.6.1
Cancelar
Aceptar



Precaución

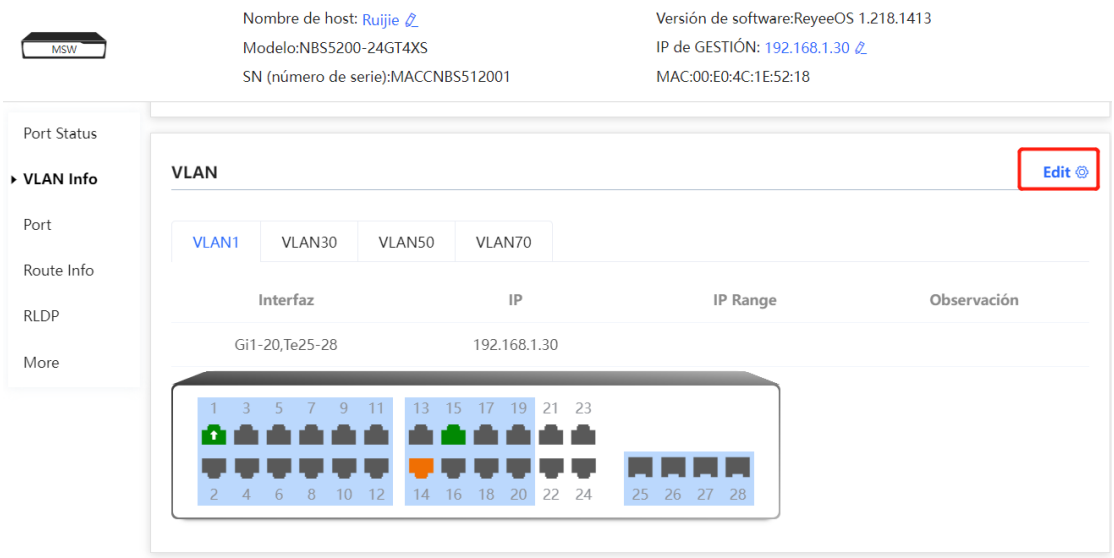
El segmento de red 192.168.110.0/24 está configurado para la VLAN 1.

(2) Cambie al modo **Red**. Seleccione **Dispositivos** > **Switch**.

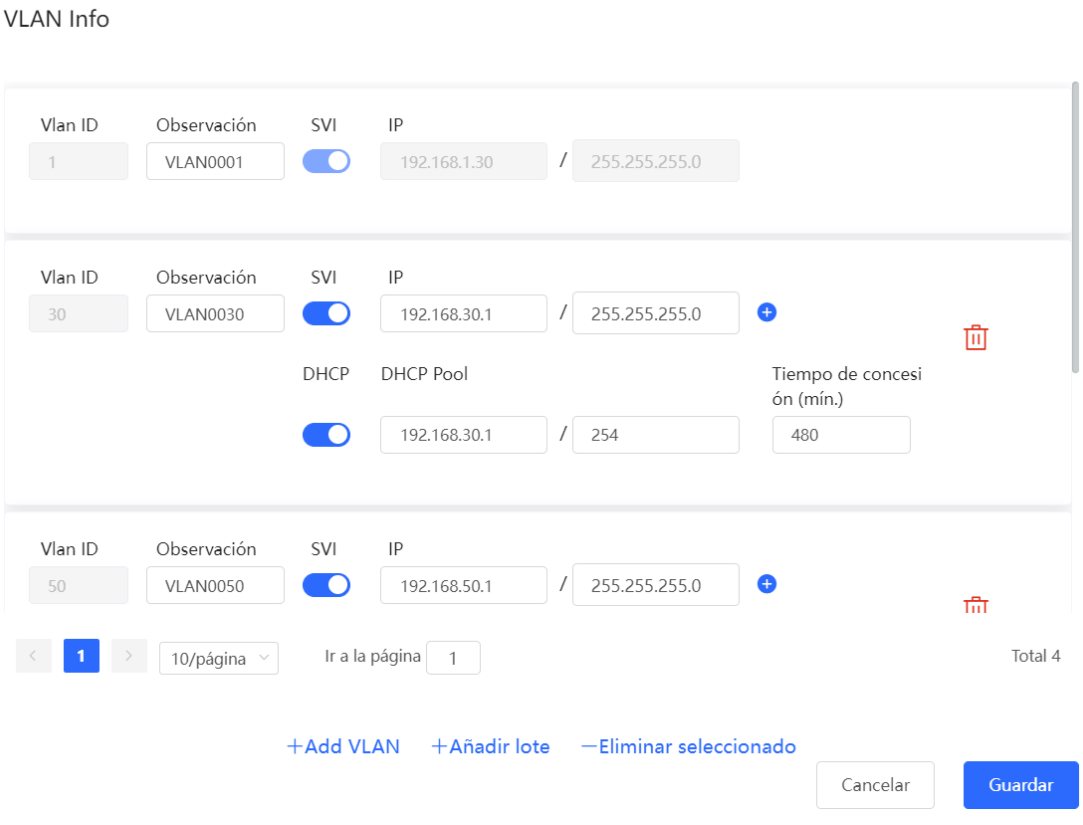


a Seleccione un dispositivo de **Lista de Dispositivos** e ingrese a la página de configuración.

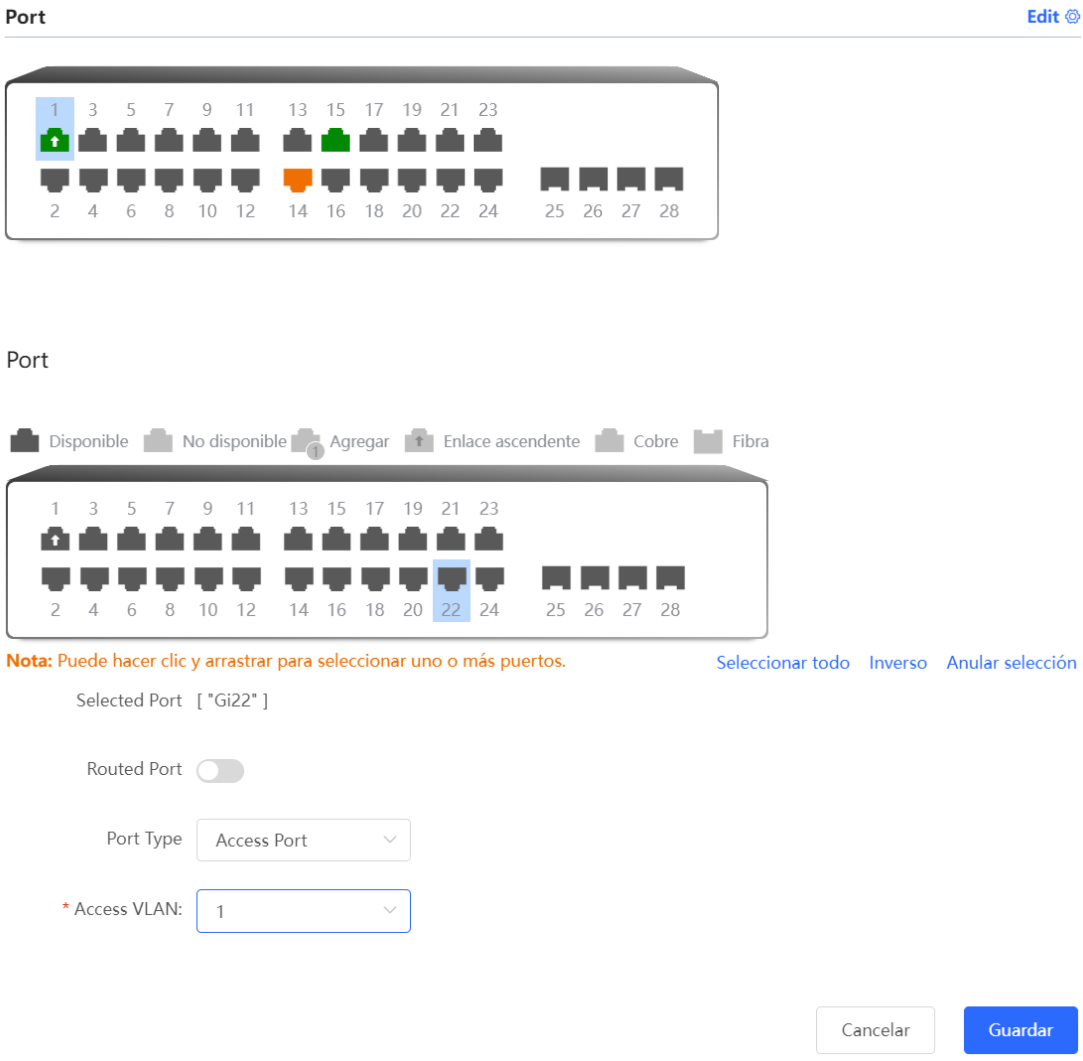
b En la ventana de **VLAN**, seleccione una VLAN y haga clic en **Edit** para configurarla.



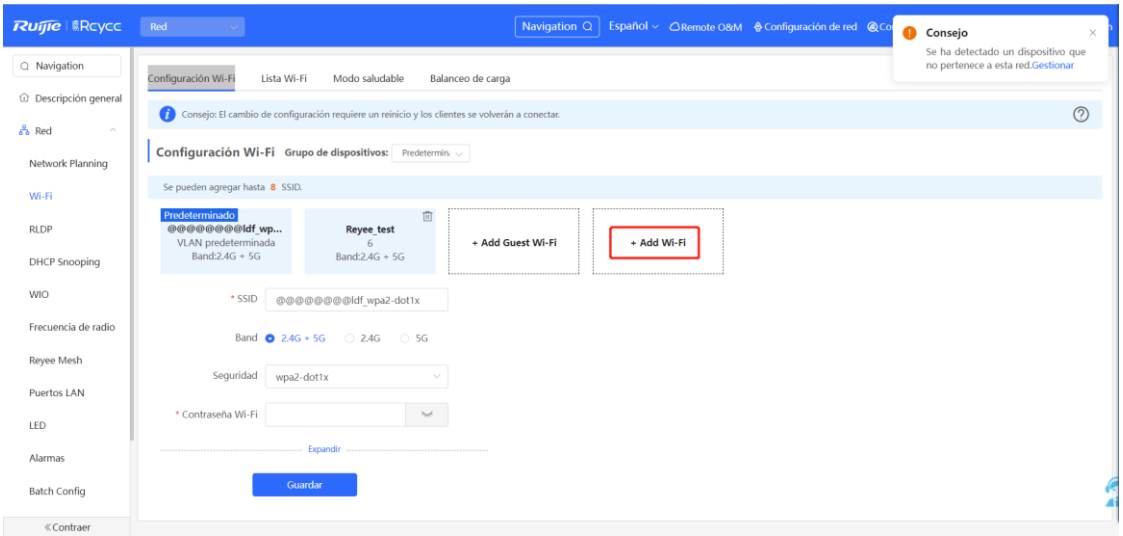
c Haga clic en **Add VLAN** para crear la VLAN 6 en el conmutador.



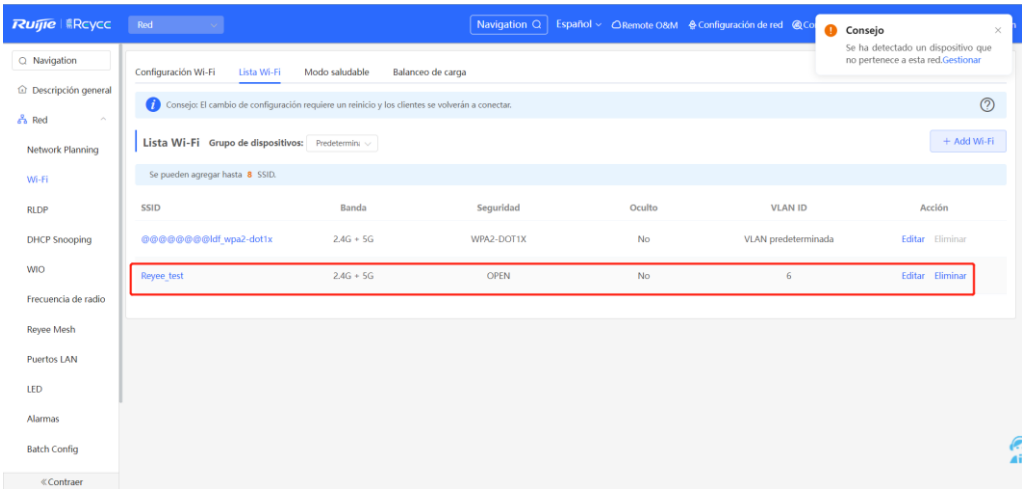
d En la ventana de **Port**, haga clic en **Edit**, configure el puerto2 y puerto9 conectados al AP y el EG como puertos troncales y configúrelos para que a los paquetes de las VLAN 1 y VLAN 6 se les permita el paso. Revise la configuración de puertos en el dispositivo.



(3) Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Configuración Wi-Fi**, configure el SSID como **Reyee_test** y asócielo con la VLAN 6.

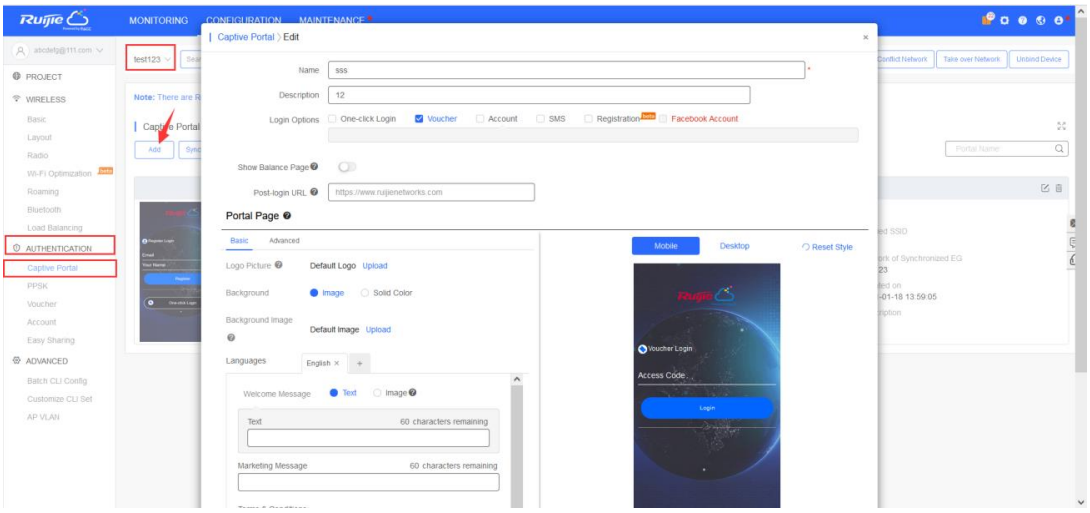


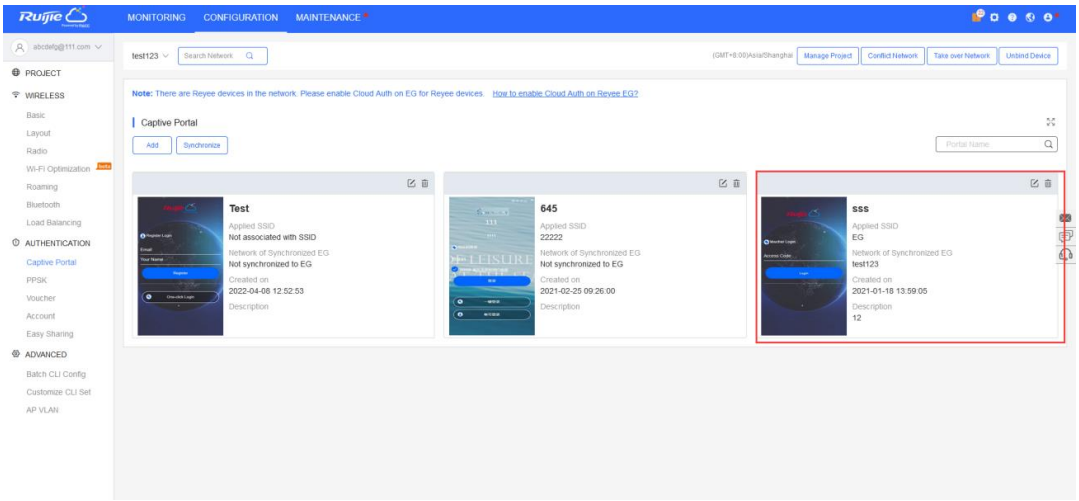

* SSID
Reyee_test
Band
2.4G + 5G
2.4G
5G
Seguridad
Abrir
Contraer
Programación inalámbrica
Todo el tiempo
VLAN
6
Ocultar SSID
(El SSID está oculto y debe introducirse manualmente).
Aislamiento Client
Prevent wireless clients of this Wi-Fi from communicating with one another.
Cambio de banda
(El cliente 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).
Wi-Fi6
(802.11ax High-Speed Wireless Connectivity.)
Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.
Cancelar
Aceptar


Navigation
Descripción general
Red
Network Planning
Wi-Fi
RLDP
DHCP Snooping
WIO
Frecuencia de radio
Reyee Mesh
Puertos LAN
LED
Alarmas
Batch Config
Contraer
Configuración Wi-Fi
Lista Wi-Fi
Modo saludable
Balanceo de carga
Lista Wi-Fi
Grupo de dispositivos:
+ Add Wi-Fi
SSID
Banda
Seguridad
Oculto
VLAN ID
Acción
Reyee_test
2.4G + 5G
OPEN
No
6
Editar
Eliminar
Consejo

(4) Configure la autenticación de la nube.

a Seleccione **CONFIGURATION** > **AUTHENTICATION** > **Captive Portal** para abrir la página del portal cautivo, haga clic en **Add** para crear una plantilla de portal y editarla.





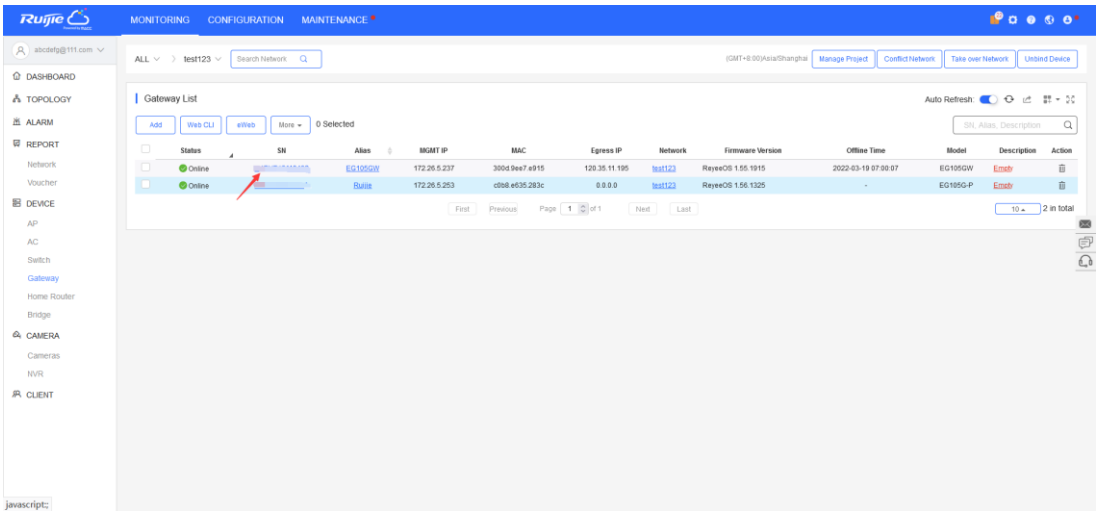
Nota

One-click Login: permite iniciar sesión sin utilizar el nombre de usuario y la contraseña. Puede configurar las opciones **Duración del acceso** y **Duración del acceso por día**.

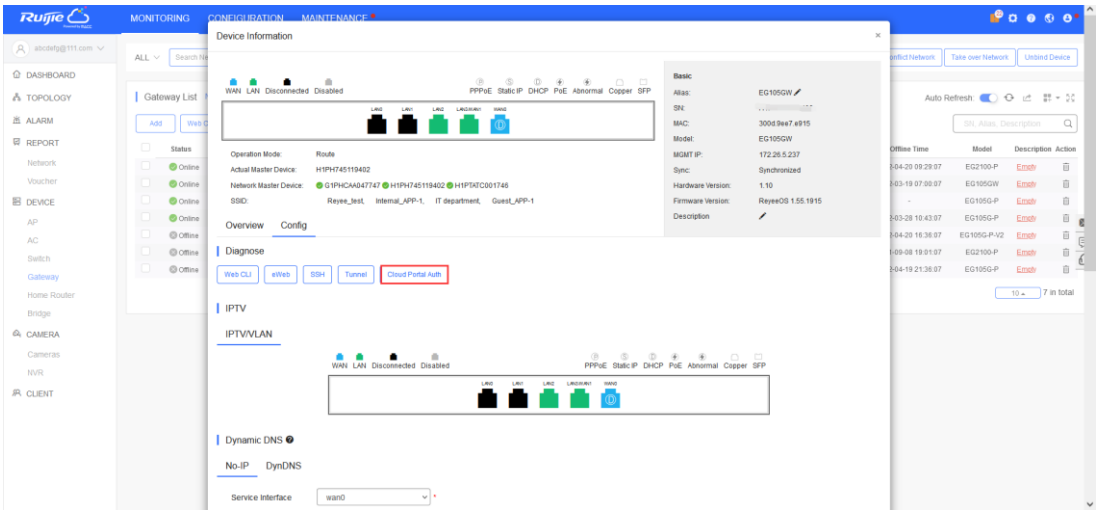
Voucher: indica el inicio de sesión con una contraseña aleatoria de ocho dígitos.

Account: indica el inicio de sesión con una cuenta y una contraseña.

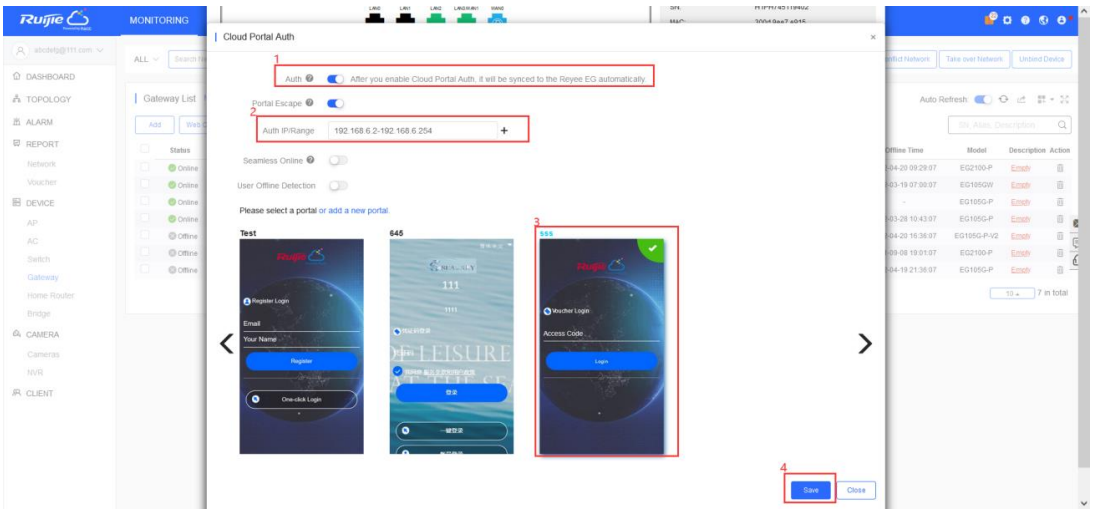
b Asegúrese de que el Reyee EG se encentre en línea en Ruijie Cloud. Haga clic en su SN en la lista para tener acceso a la página de configuración.



c Haga clic en **Cloud Portal Auth** para configurar la autenticación en Ruijie Cloud.



d Habilite **Auth**. En **Auth IP/Range** configure **192.168.6.2-192.168.6.254** para la autenticación y seleccione una plantilla de portal para utilizarla. Luego, haga clic en **Save** para guardar la configuración.

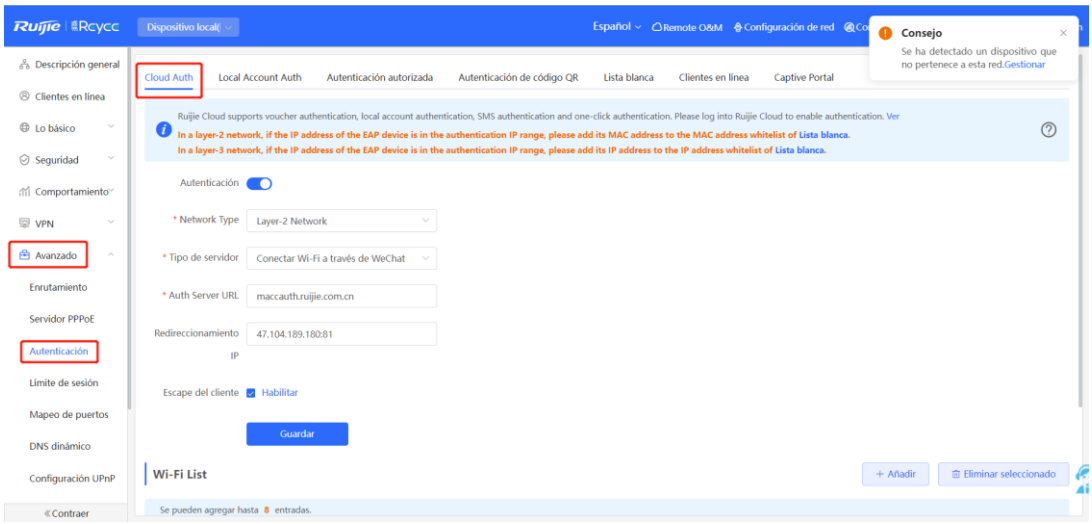


Nota

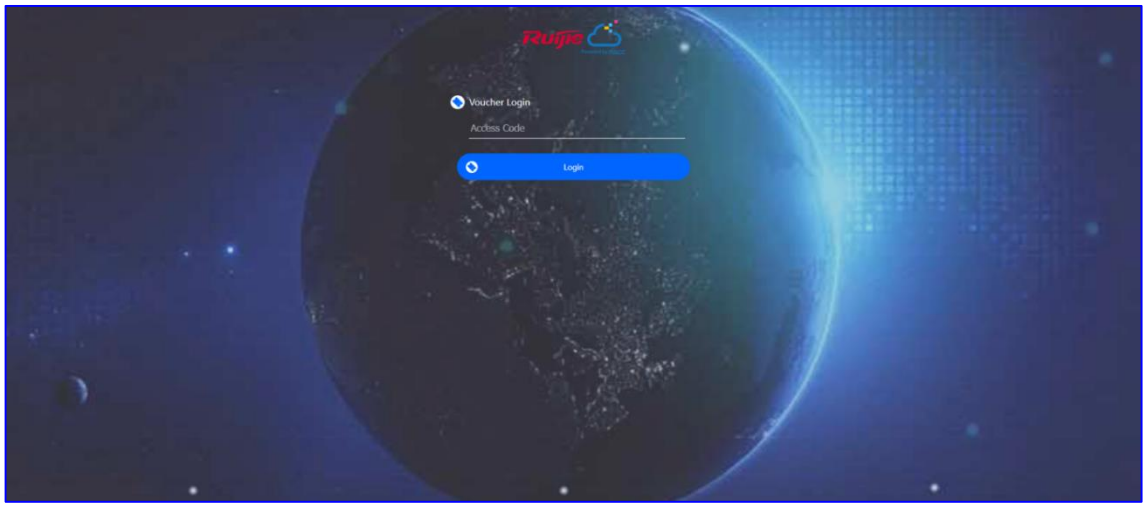
Se deben excluir las direcciones IP del switch EG y el AP; de lo contrario, el conmutador no tendrá acceso a Internet.

5.2.4 Verificación de la configuración

(1) Cambie al modo **Dispositivo local**, seleccione **Avanzado** > **Autenticación** > **Cloud Auth** para revisar si la configuración se sincronizó con el EG.



(2) Los usuarios con direcciones IP en el rango de 192.168.6.2 a 192.168.6.254 deben hacer el proceso de autenticación antes de acceder a Internet.



5.3 Solución para la red Wi-Fi de invitados en dispositivos Reyee

5.3.1 Principio de funcionamiento

Al usar el Wi-Fi de invitados, se crea una sola entrada a Internet. Los dispositivos que tienen permitido el acceso al Wi-Fi de invitados pueden acceder a Internet, pero no al Wi-Fi de la casa.

5.3.2 Escenario de aplicación

El Wi-Fi de invitados brinda un acceso seguro a la red de la casa u oficina para compartir con los invitados. Cuando alguien visite su casa, departamento o lugar de trabajo, puede habilitar la red Wi-Fi de invitados para ellos. Se pueden configurar diferentes opciones de acceso para invitados, lo cual es muy efectivo para garantizar la seguridad y privacidad de su red principal.

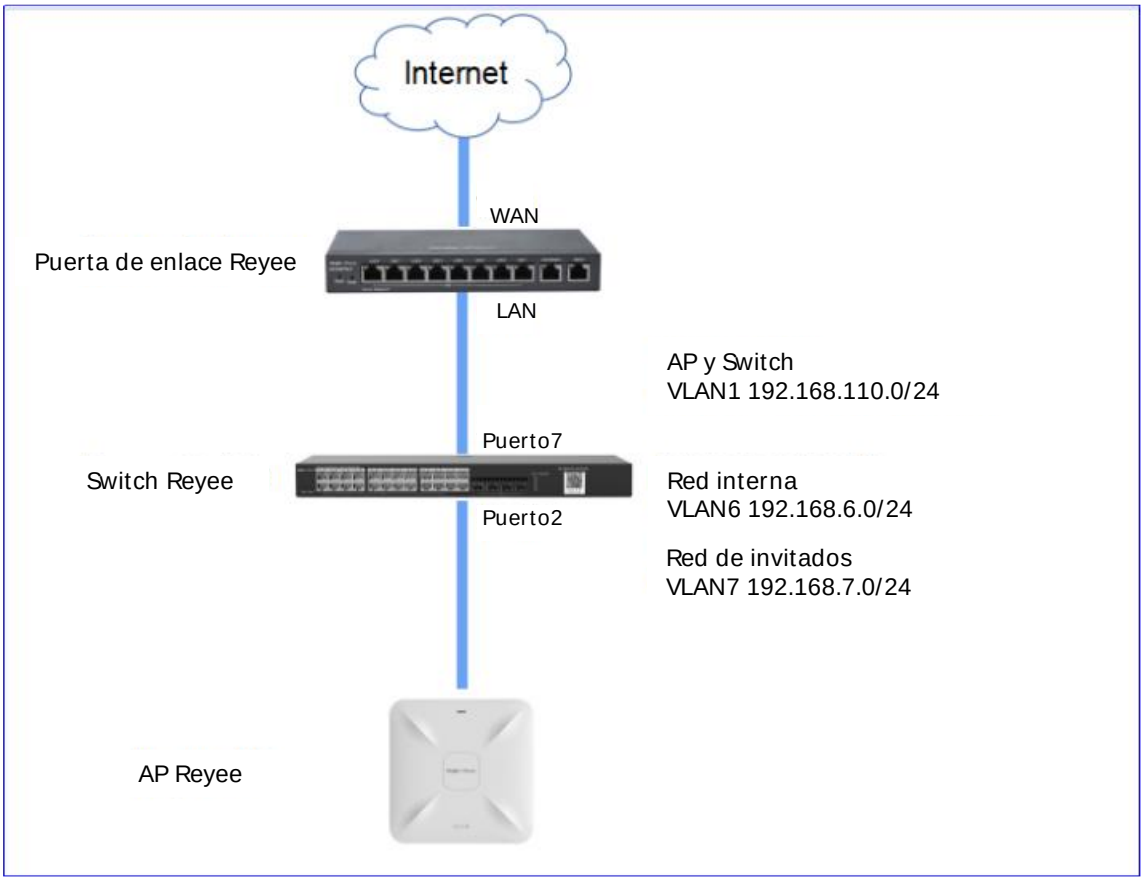
5.3.3 Ejemplo de configuración

1. Configuración a través de la Eweb del EG

Requisitos

Configure un Wi-Fi de invitados en el segmento de red de VLAN 7 para que los usuarios no tengan acceso a la red interna que se encuentra en el segmento de red de VLAN 6.

Topología de la red



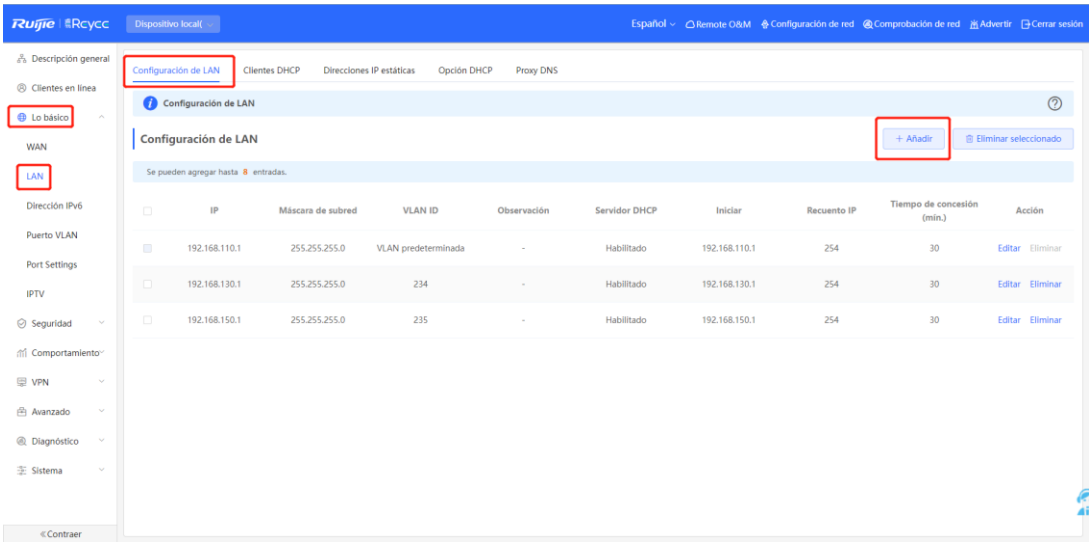
Descripción de la red

- El EG actúa como servidor DHCP para asignar direcciones IP a los usuarios, al AP Reyee y al switch Reyee.
- El AP y el switch Reyee obtienen la dirección IP en el segmento de red de VLAN 1 para tener acceso a Internet.
- Los usuarios internos obtienen direcciones IP en el segmento de red de VLAN 6 para tener acceso a Internet y los invitados las obtienen en el segmento de red de VLAN 7 para tener acceso a Internet.

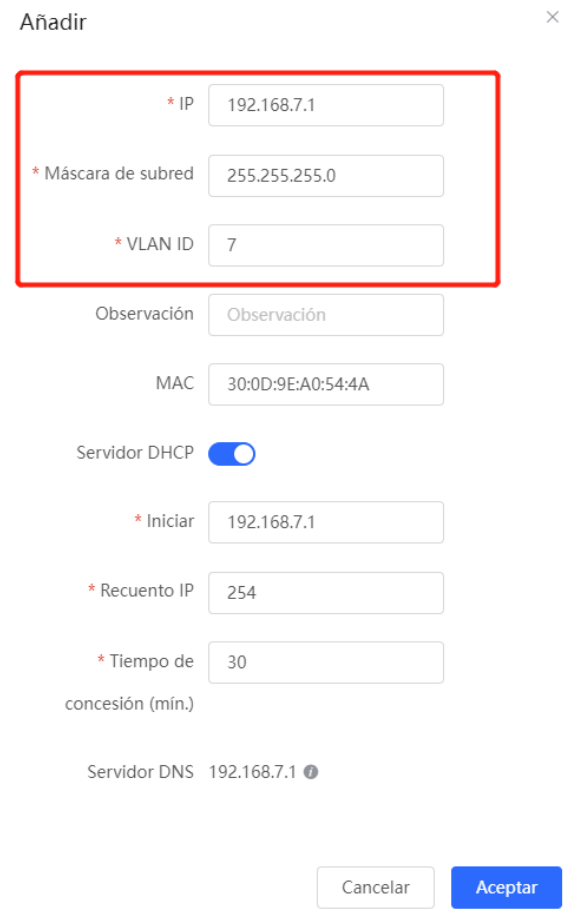
Pasos para la configuración

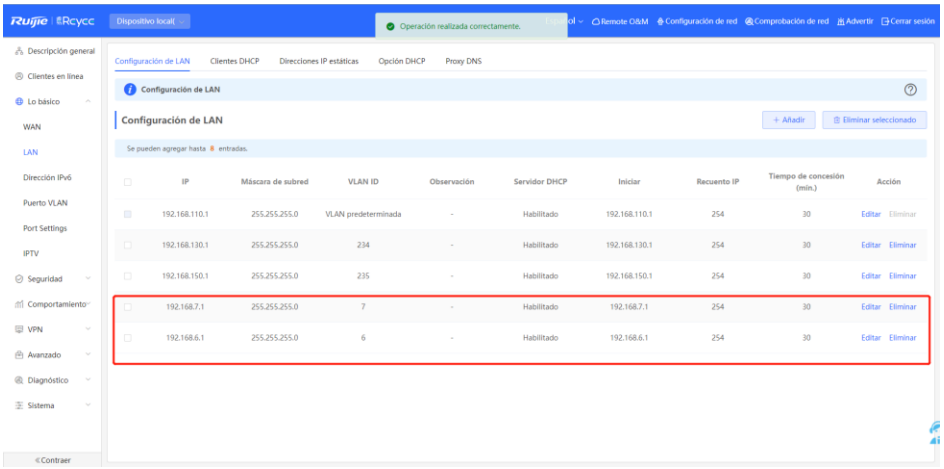
(1) Configure VLAN 6 y VLAN 7 en el router.

a Cambie al modo **Dispositivo local**. Seleccione **Lo básico** > **LAN** > **Configuración de LAN**.> **Añadir**.



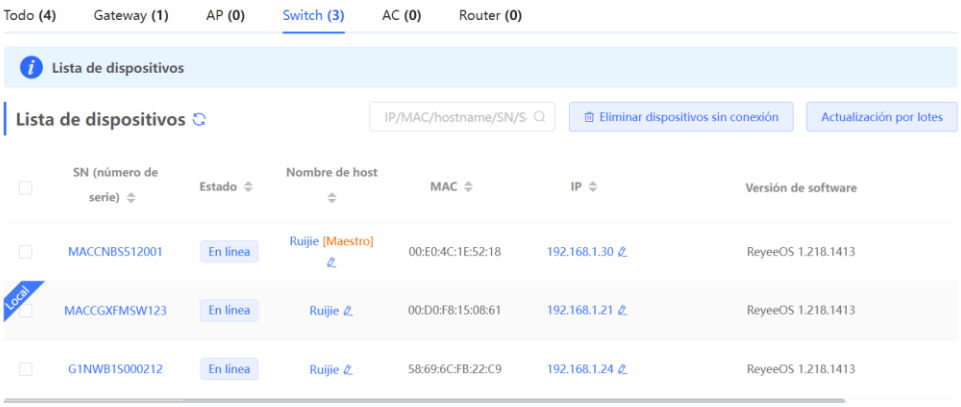
b Realice la configuración de LAN y configure los grupos de direcciones de DHCP para VLAN 6 y VLAN 7 en el router.





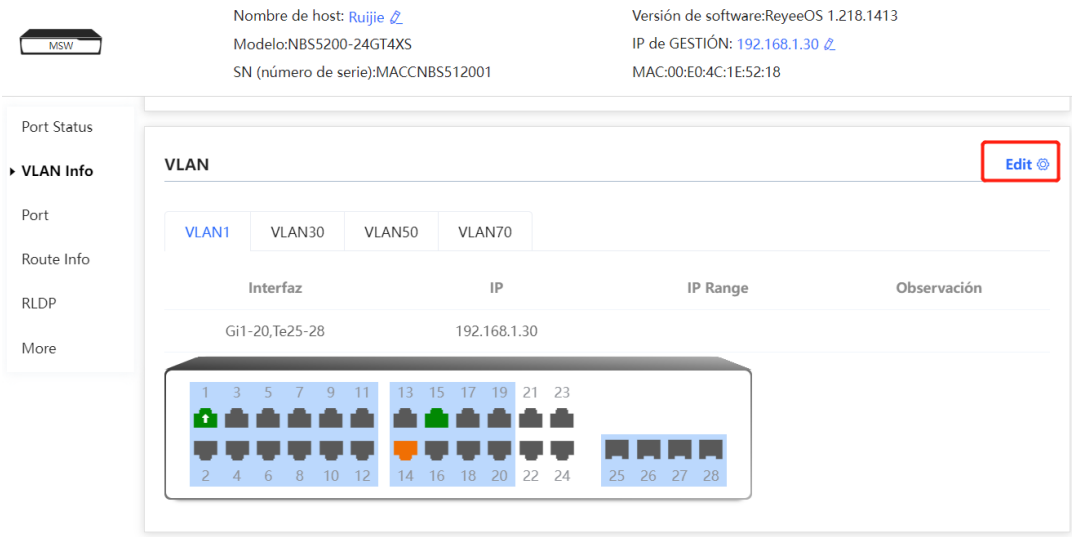
(2) Configure las VLAN para un conmutador.

a Cambie al modo **Red**. Seleccione **Dispositivos** > **Switch**.

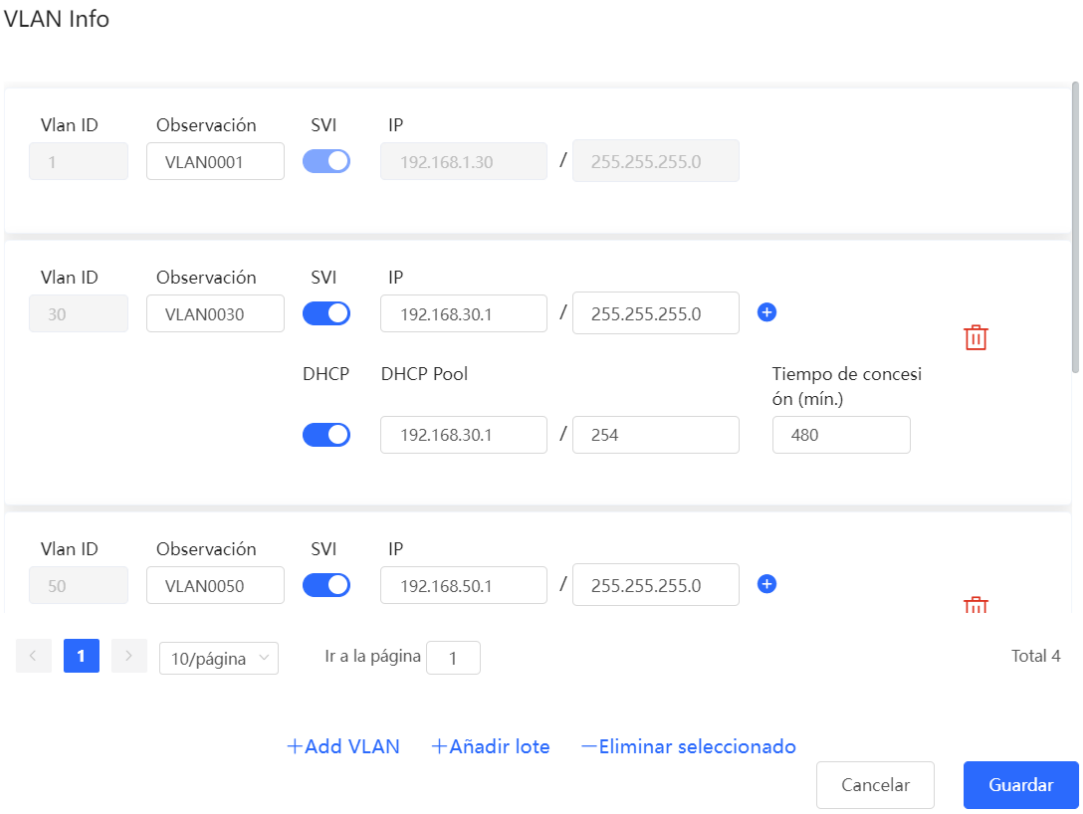


b Seleccione un dispositivo de **Lista de dispositivos** e ingrese a la página de configuración.

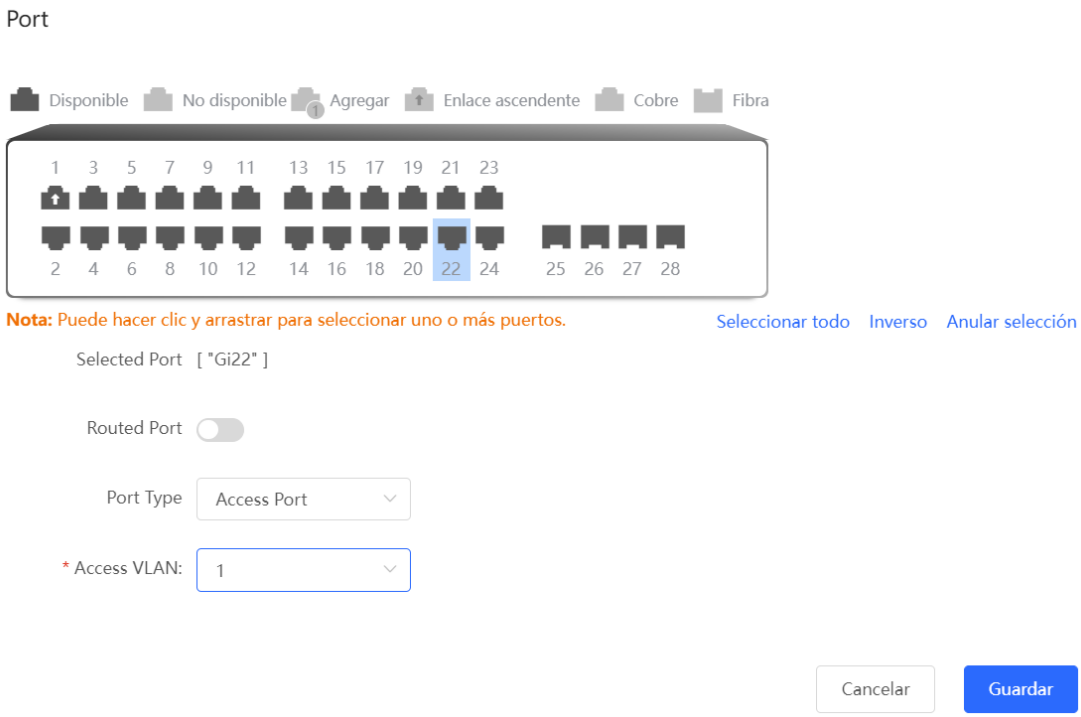
c En la ventana de **VLAN**, seleccione una VLAN y haga clic en **Edit** para configurarla.



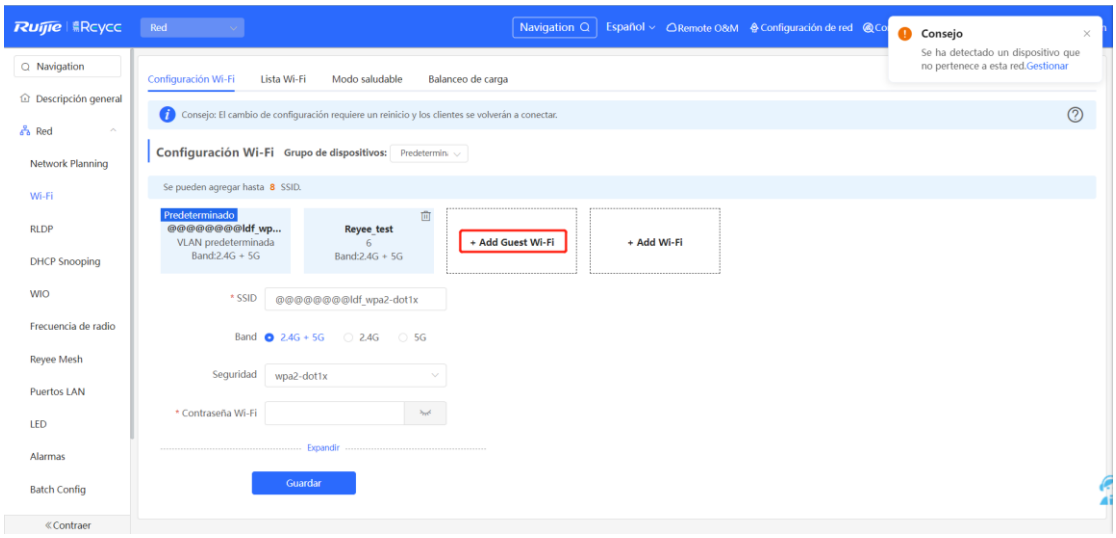
d Haga clic en **Add VLAN** para crear la VLAN 6 en el conmutador.

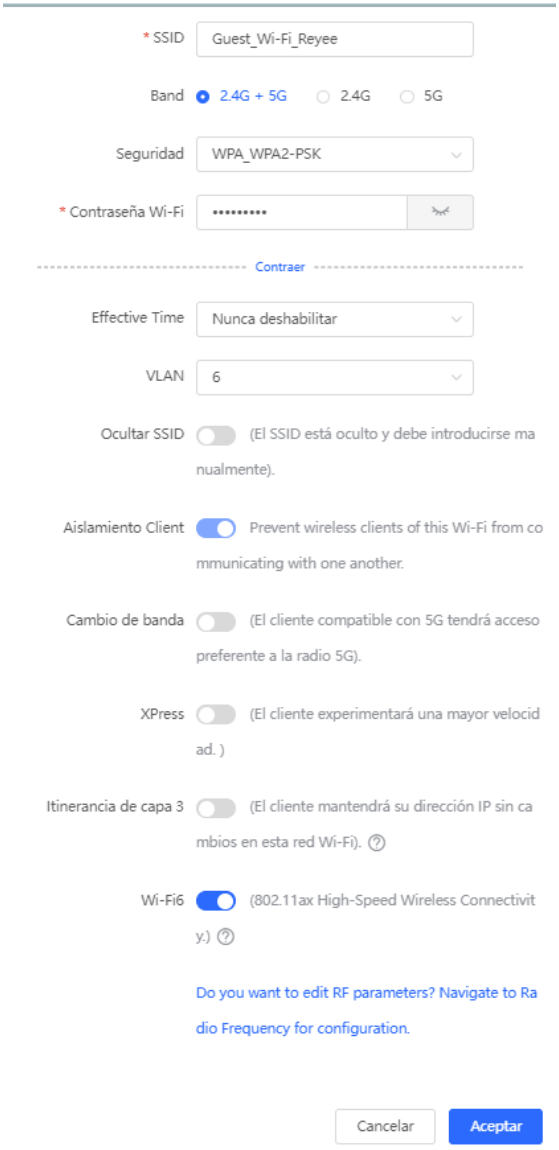


e En la ventana de **Port**, haga clic en **Edit**, configure el puerto2 y puerto9 conectados al AP y el EG como puertos troncales y configúrelos para que a los paquetes de las VLAN 1 y VLAN 6 se les permita el paso. Revise la configuración de puertos en el dispositivo.

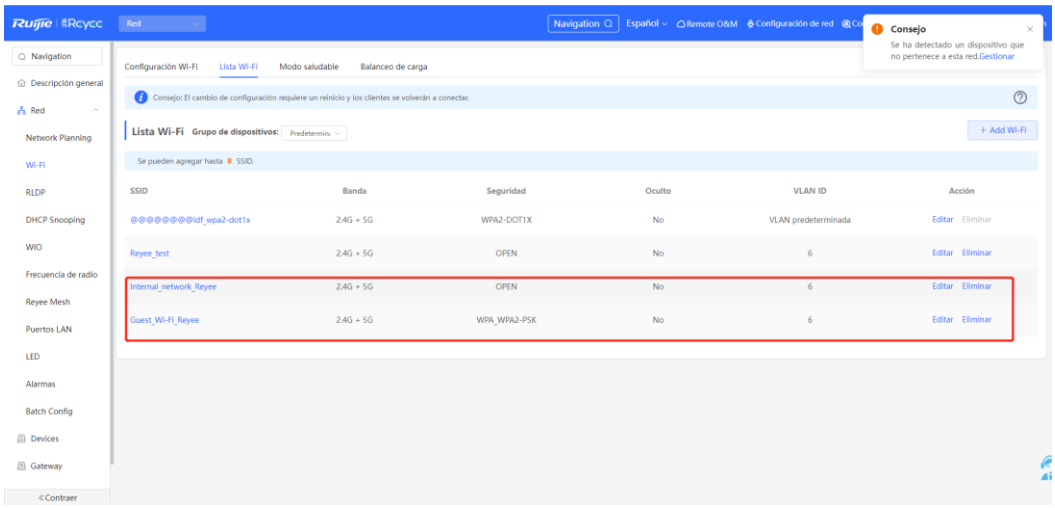


(3) Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Add Guest Wi-Fi**, configure un SSID para la Wi-Fi de invitados con el nombre **Guest_Wi-Fi_Reyee**, y asócielo con la VLAN 7.

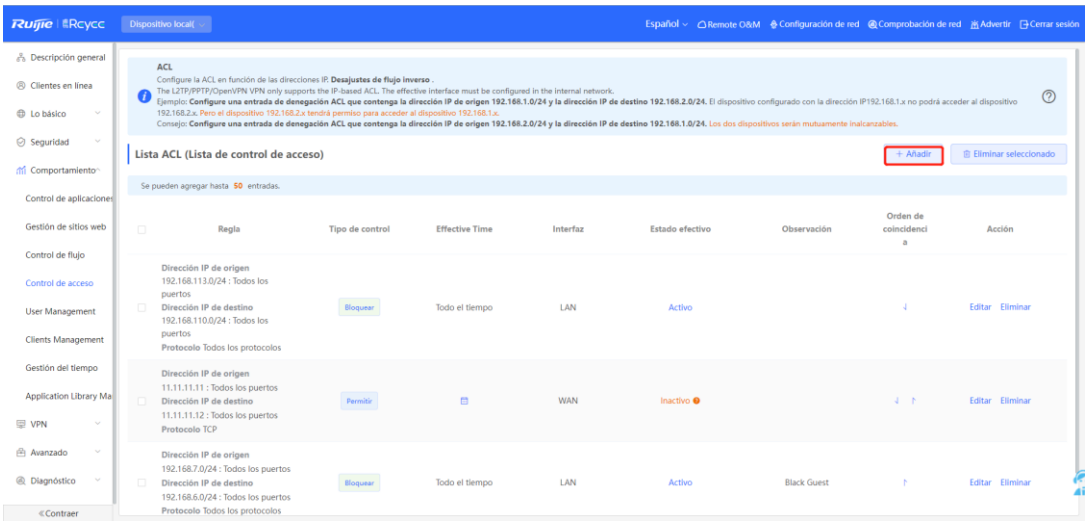


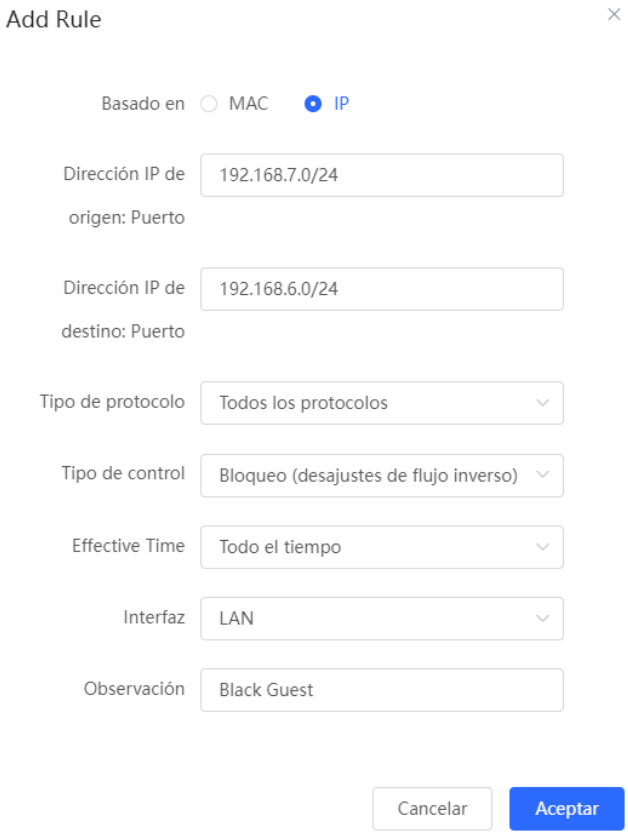


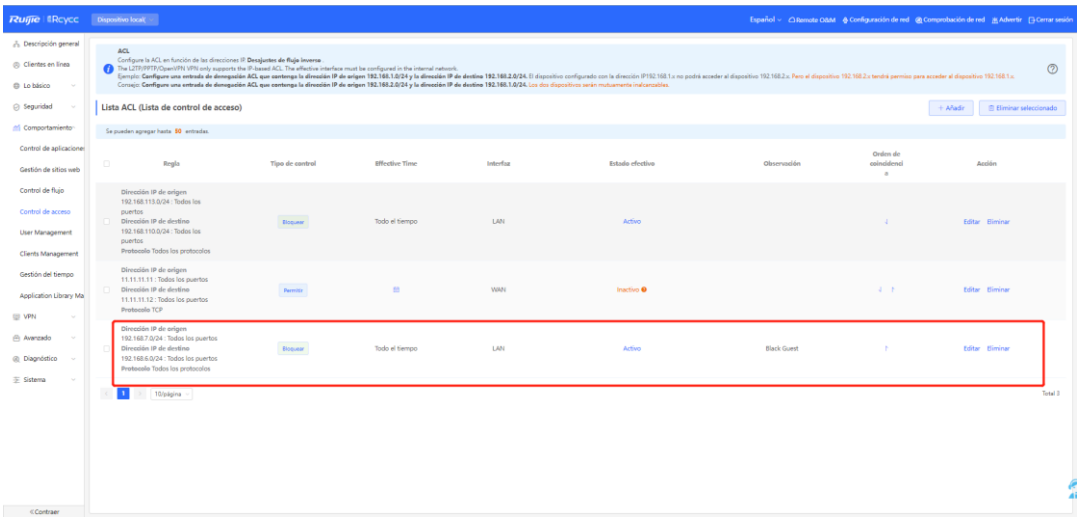
(4) Seleccione **Red** > **Wi-Fi** > **Lista Wi-Fi** > **Añadir Wi-Fi**, configure el SSID del usuario interno con el nombre **Internal_network_Reyee**, y asócielo con la VLAN 6; finalmente, revise la configuración de Wi-Fi en la Lista Wi-Fi.



(5) Cambie al modo **Dispositivo local**. Seleccione **Comportamiento** > **Control de acceso**, configure una ACL para bloquear el tráfico de los invitados en el segmento de red 192.168.7.0/24 de VLAN 7 a los usuarios internos en el segmento de red 192.168.6.0/24 de VLAN 6, y aplique la regla ACL a la interfaz de la LAN en el EG.


Ruijie | Rcycc
Dispositivo local
Español
Remote O&M
Configuración de red
Comprobación de red
Advertir
Cerrar sesión
Descripción general
Clientes en línea
Lo básico
Seguridad
Comportamiento
Control de aplicaciones
Gestión de sitios web
Control de flujo
Control de acceso
User Management
Clients Management
Gestión del tiempo
Application Library Ma
VPN
Avanzado
Diagnóstico
Contraer
ACL
Configure la ACL en función de las direcciones IP. Desajustes de flujo inverso .
The L2TP/PPTP/OpenVPN VPN only supports the IP-based ACL. The effective interface must be configured in the internal network.
Ejemplo: Configure una entrada de denegación ACL que contenga la dirección IP de origen 192.168.1.0/24 y la dirección IP de destino 192.168.2.0/24. El dispositivo configurado con la dirección IP192.168.1.x no podrá acceder al dispositivo 192.168.2.x. Pero el dispositivo 192.168.2.x tendrá permiso para acceder al dispositivo 192.168.1.x.
Consejo: Configure una entrada de denegación ACL que contenga la dirección IP de origen 192.168.2.0/24 y la dirección IP de destino 192.168.1.0/24. Los dos dispositivos serán mutuamente inalcanzables.
Lista ACL (Lista de control de acceso)
+ Añadir
Eliminar seleccionado
Se pueden agregar hasta 50 entradas.
Regla
Tipo de control
Effective Time
Interfaz
Estado efectivo
Observación
Orden de coincidencia
Acción
Dirección IP de origen 192.168.113.0/24 ; Todos los puertos
Dirección IP de destino 192.168.110.0/24 ; Todos los puertos
Protocolo Todos los protocolos
Bloquear
Todo el tiempo
LAN
Activo
Editar Eliminar
Dirección IP de origen 11.11.11.11 ; Todos los puertos
Dirección IP de destino 11.11.11.12 ; Todos los puertos
Protocolo TCP
Permitir
WAN
Inactivo
Editar Eliminar
Dirección IP de origen 192.168.7.0/24 ; Todos los puertos
Dirección IP de destino 192.168.6.0/24 ; Todos los puertos
Protocolo Todos los protocolos
Bloquear
Todo el tiempo
LAN
Activo
Black Guest
Editar Eliminar


Add Rule
Basado en
MAC
IP
Dirección IP de origen: Puerto
192.168.7.0/24
Dirección IP de destino: Puerto
192.168.6.0/24
Tipo de protocolo
Todos los protocolos
Tipo de control
Bloqueo (desajustes de flujo inverso)
Effective Time
Todo el tiempo
Interfaz
LAN
Observación
Black Guest
Cancelar
Aceptar



Verificación de la configuración

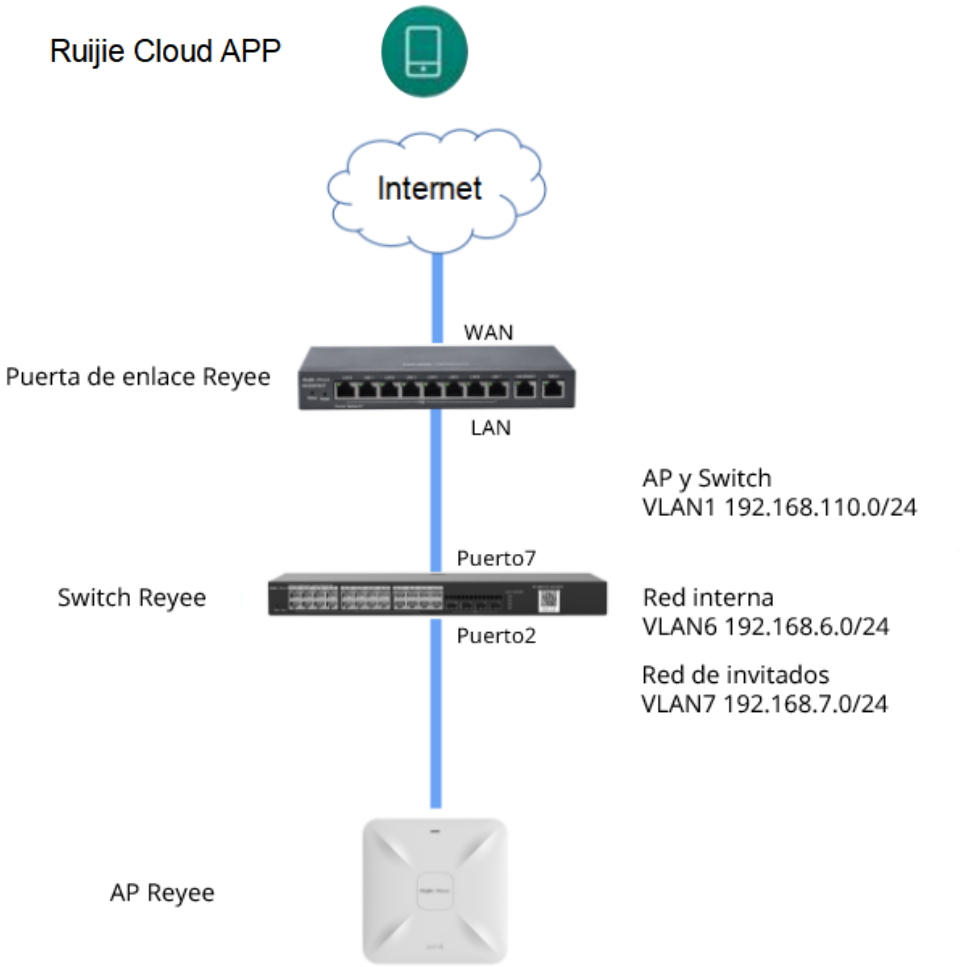
Un invitado en 192.168.7.2 no puede acceder al usuario de red interna en 192.168.6.2.

2. Configuración a través de Ruijie Cloud APP

Requisitos

Configure una red Wi-Fi de invitados a través de Ruijie Cloud App en el segmento de red de VLAN 7, para que los usuarios no tengan acceso a la red interna en el segmento de red de VLAN 6. Ruijie Cloud App descargará la configuración correspondiente en el dispositivo de manera automática.

Topología de la red

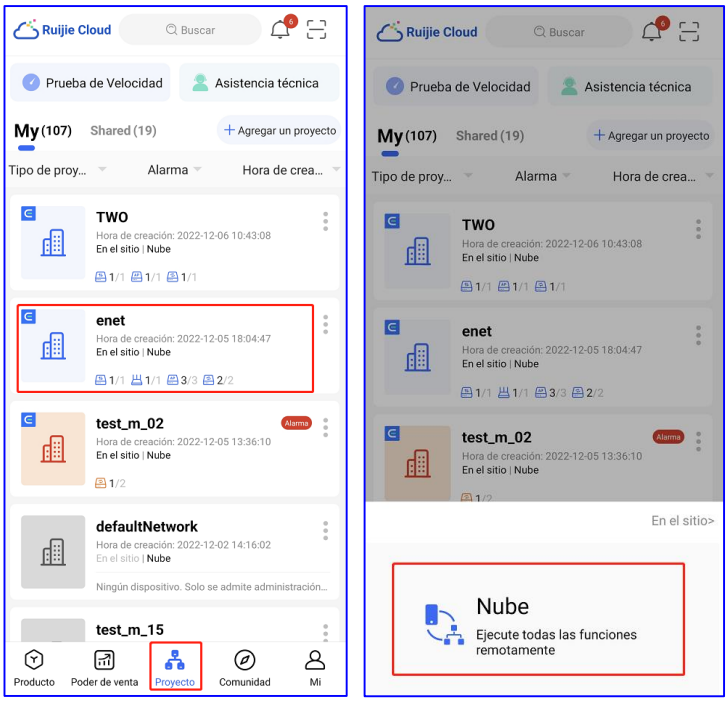


Descripción de la red

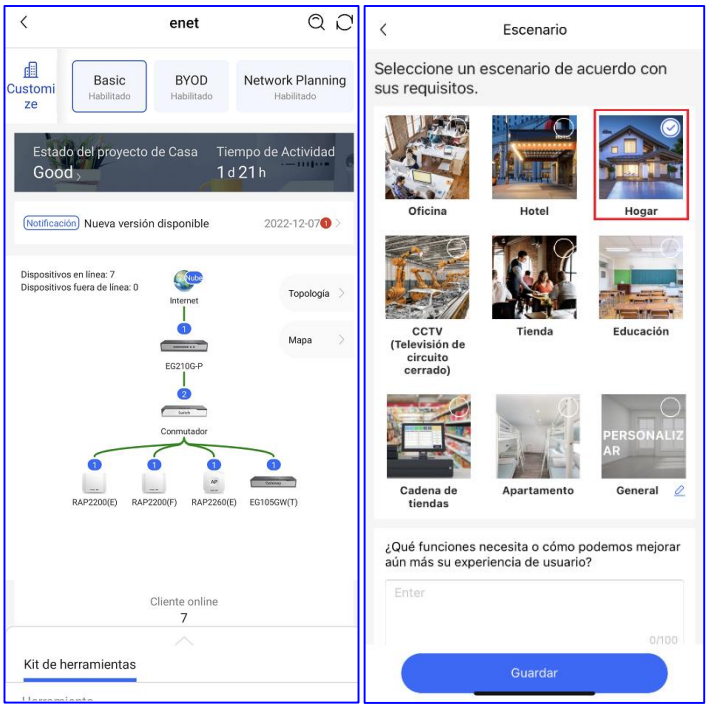
- El EG actúa como servidor DHCP para asignar direcciones IP a los usuarios, al AP Reyee y al switch Reyee.
- El AP y el switch Reyee obtienen la dirección IP en el segmento de red de VLAN 1 para tener acceso a Internet.
- Los usuarios internos obtienen direcciones IP en el segmento de red de VLAN 6 para tener acceso a Internet y los invitados las obtienen en el segmento de red de VLAN 7 para tener acceso a Internet.

Pasos para la configuración

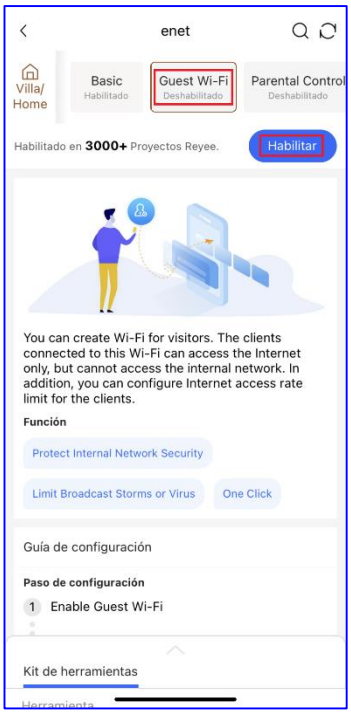
(1) Inicie sesión en su Ruijie Cloud App desde su smartphone e ingrese al proyecto con el router y la RAP Reyee.



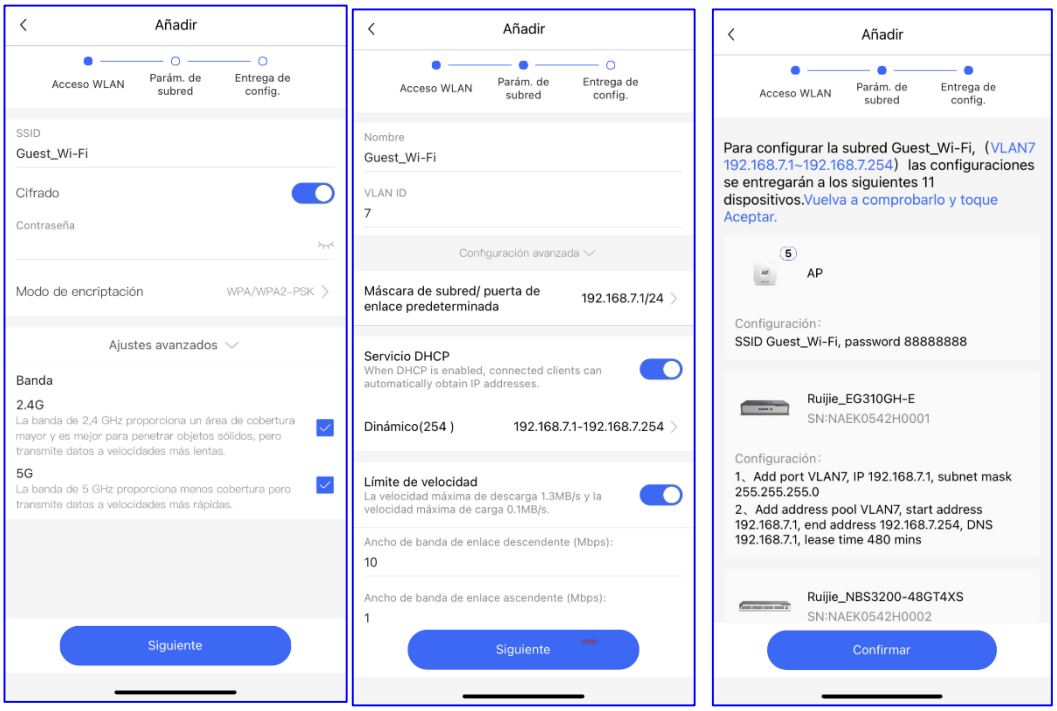
(2) Seleccione **Villa/Hogar** en **Escenario**. Luego, podrá ver el botón **Guest Wi-Fi** .

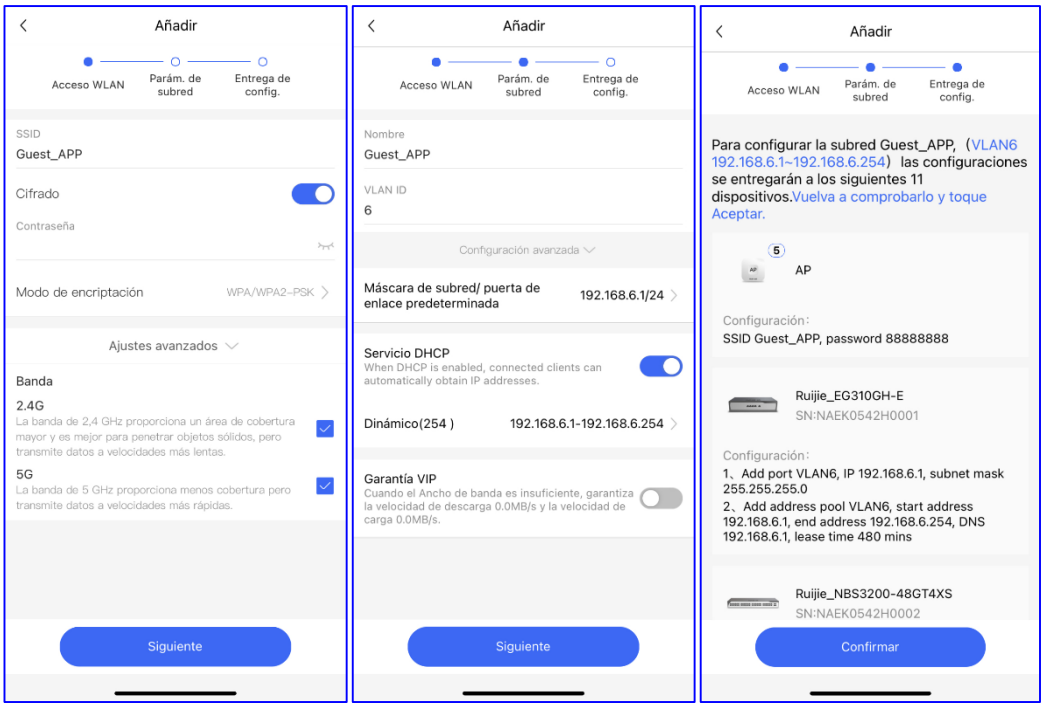


(3) Seleccione **Guest Wi-Fi** y haga clic en el botón **Habilitar**.

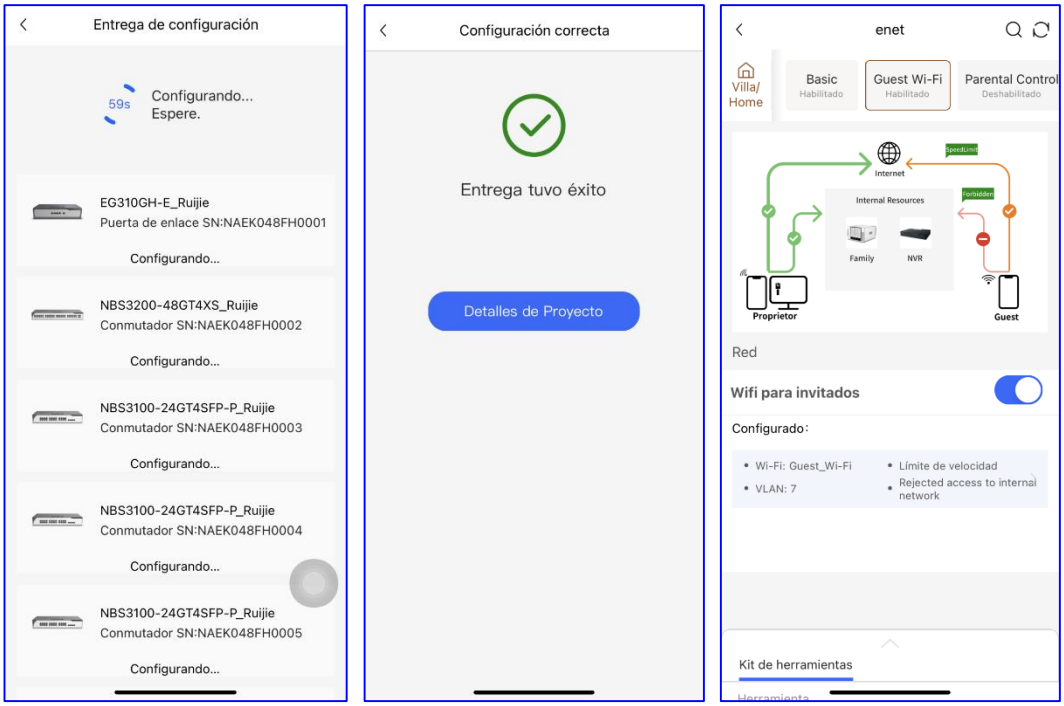


(4) Modifique la información de la red Wi-Fi de invitados, configure un SSID de usuario interno con el nombre **Guest_APP** y asócielo con VLAN 6. De igual forma, configure un SSID de Wi-Fi de invitados con el nombre **Guest_Wi-Fi** y asócielo con VLAN 7. Luego, haga clic en **Confirmar** para guardar la configuración.





(5) Espere alrededor de 1 minuto a que el sistema descargue la configuración en el dispositivo.



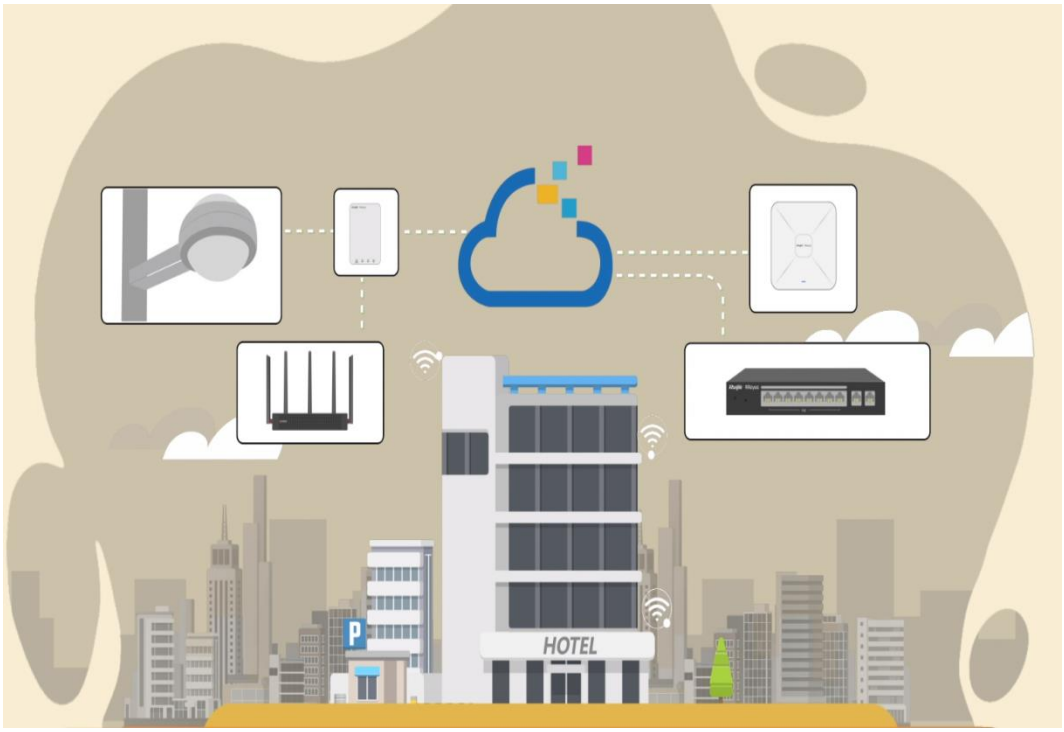
Verificación de la configuración

Un invitado en 192.168.7.97 no puede acceder al usuario interno en 192.168.6.147.

5.4 Solución de red Reyee económica para hoteles

5.4.1 Escenario de aplicación

La solución de red Reyee económica para hoteles proporciona una red Wi-Fi asequible para ofrecer un servicio de 5 estrellas a los clientes. Actualmente, puede operar a 2.4 GHz y 5 GHz, suministrando un acceso inalámbrico de alta velocidad de 574 Mbps a 2.4 GHz, 1201 Mbps a 5 GHz, y hasta 1775 Mbps por AP. El AP de pared proporciona un puerto LAN al frente para facilitar la expansión de terminales IPTV y teléfonos IP, entre otras.

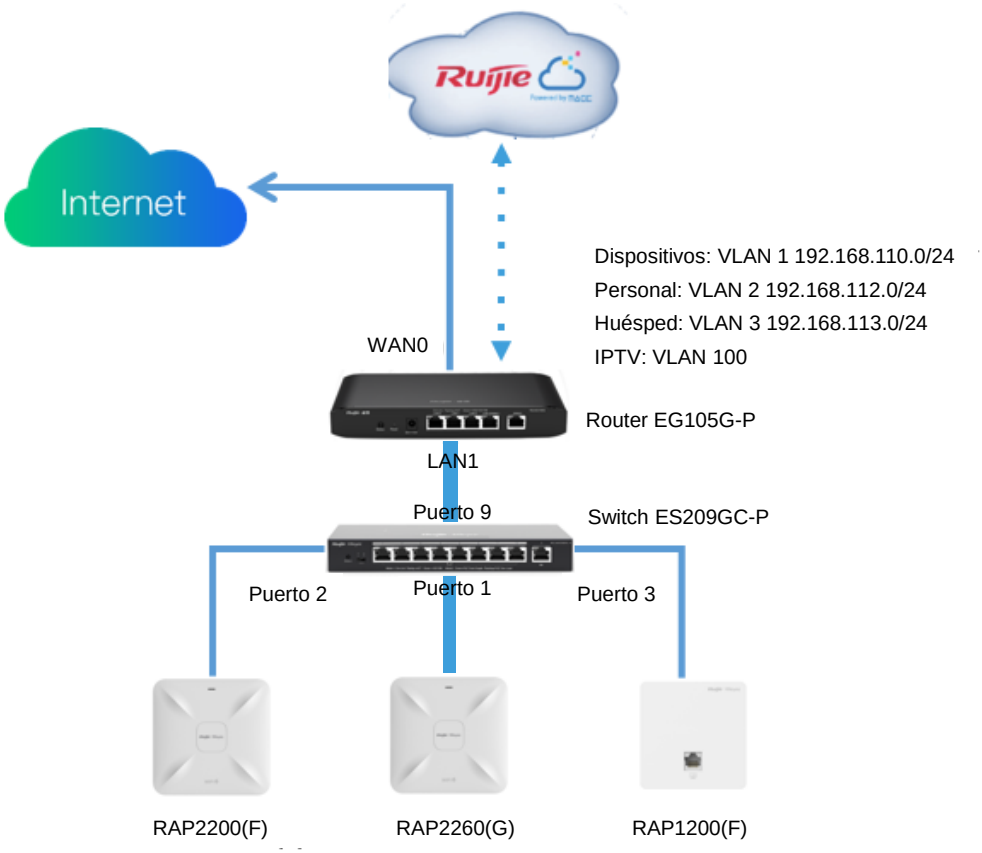


5.4.2 Ejemplo de configuración

Requisitos

- Es necesario construir una red inalámbrica para el hotel, los huéspedes deben pasar una autenticación por cupón antes de acceder a Internet; y no pueden tener acceso a la red interna del hotel.
- Contar con conexiones cableadas configuradas para IPTV.

Topología de la red



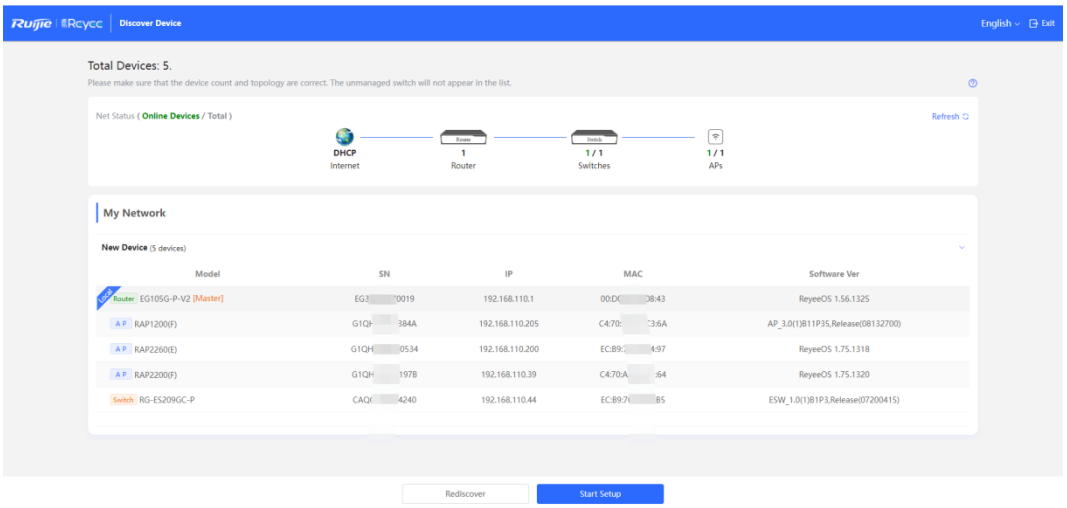
Lista de dispositivos

Tipo	Modelo	Función
Router	EG105G-P	● Se conecta a Internet y funciona como servidor DHCP para dispositivos de enlace descendente y clientes. ● Administra al AP y al conmutador localmente. ● Admite la autenticación por cupón con Ruijie Cloud
Switch	ES209GC-P	Proporciona conexiones cableadas y de PoE.
AP de pared	RAP1200(F)	Permite conectarse a Internet de forma inalámbrica desde las habitaciones. Permite conectarse al servicio de IPTV por cable.
AP para interiores	RAP2200(F) y RAP2260(G)	Permite conectarse a Internet de forma inalámbrica desde la recepción y los pasillos.

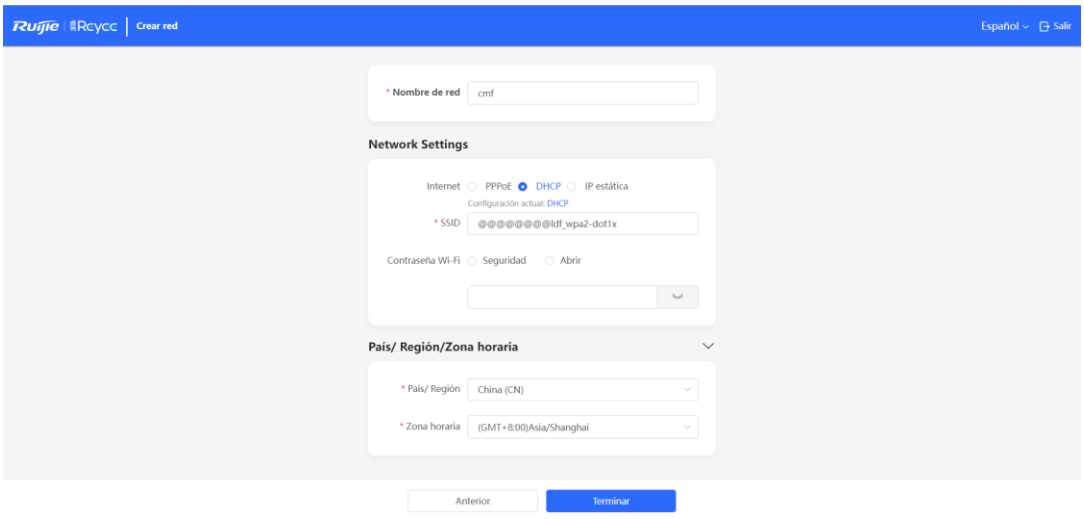
Pasos para la configuración

(1) Encienda y conecte el dispositivo de acuerdo con la topología.

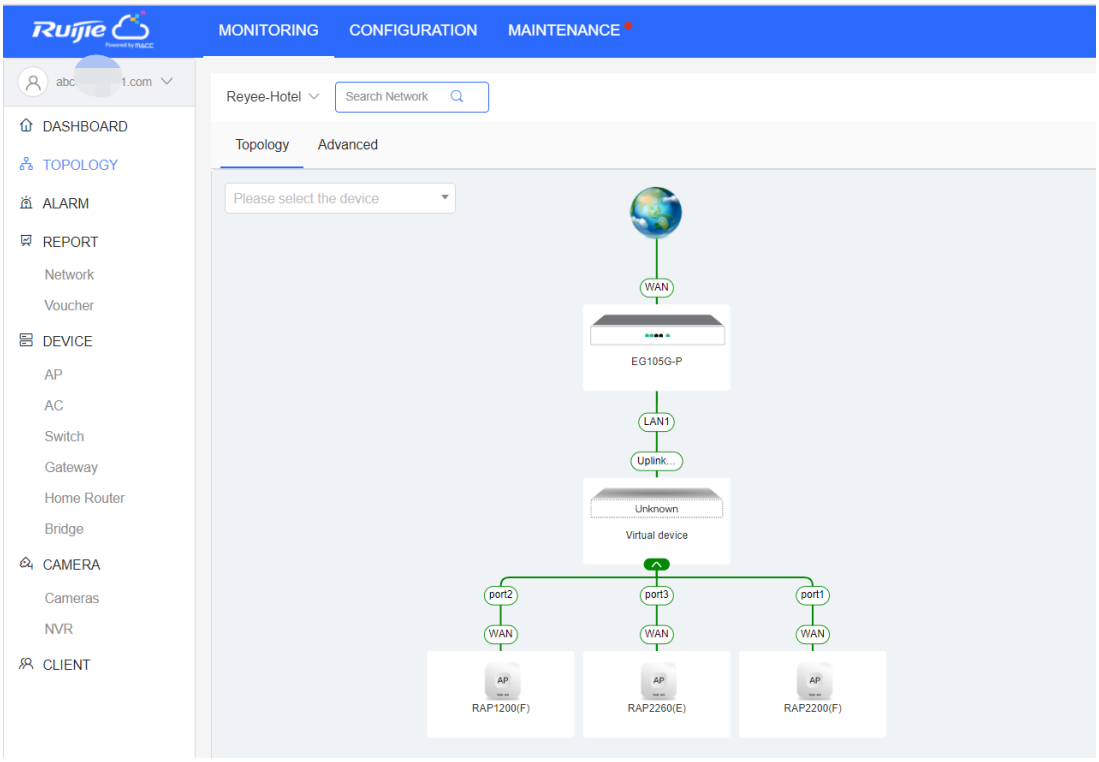
(2) Por defecto, la dirección IP del router es 192.168.110.1. Haga clic en **Start Setup** para realizar la configuración básica de red.



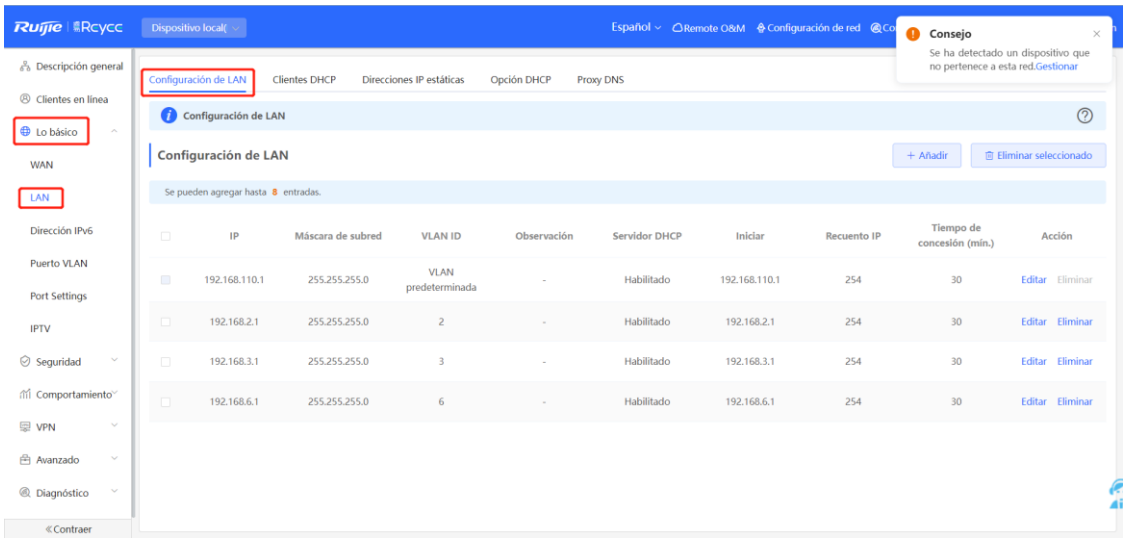
a Configure **Nombre de red**, **Network Settings**, **SSID** para el personal y **Contraseña de gestión**.



b Haga clic en **Terminar** para activar la configuración y añadir los dispositivos a Ruijie Cloud.

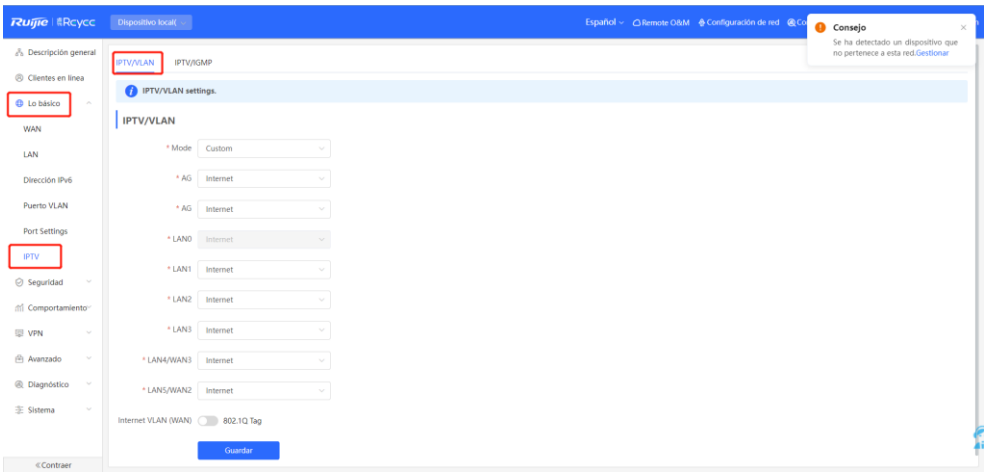


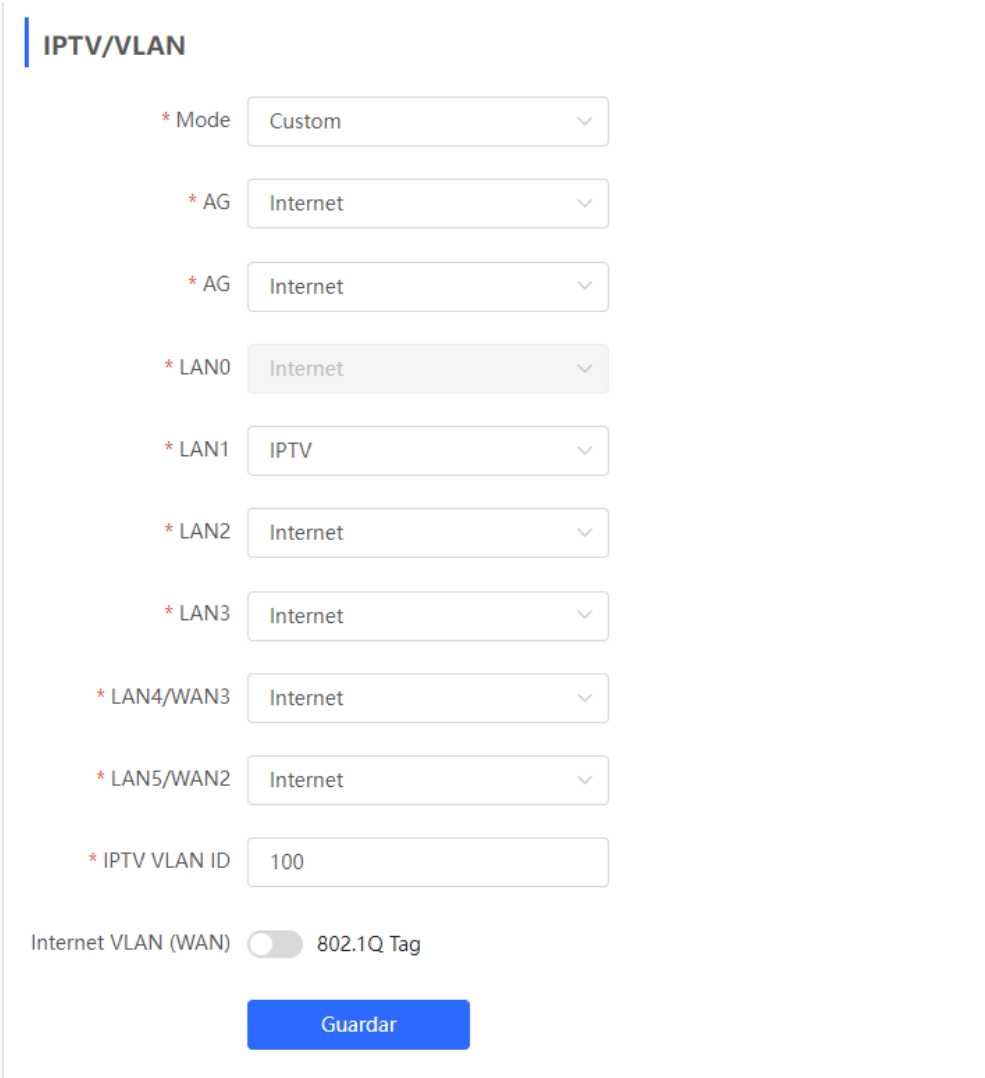
(3) Cambie al modo **Dispositivo local**. Seleccione **Lo básico** > **LAN** > **Configuración de LAN** para crear las VLAN 2 y VLAN 3 para el personal y los huéspedes.



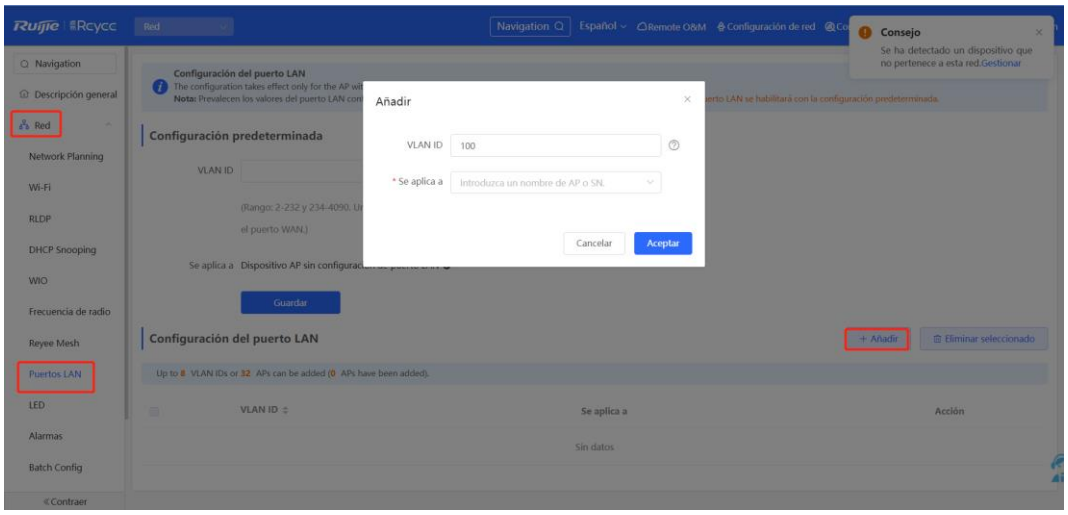
(4) Cambie al modo **Dispositivo local**. Seleccione **Lo básico** > **IPTV** para configurar los ajustes del servicio IPTV proporcionado por el ISP.

Por ejemplo, la VLAN ID para el IPTV es 100.

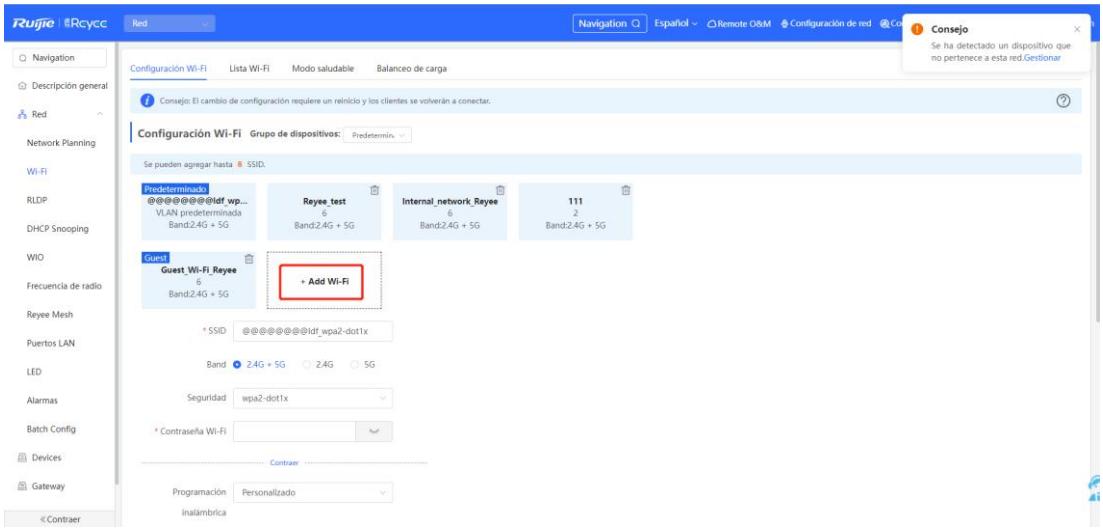


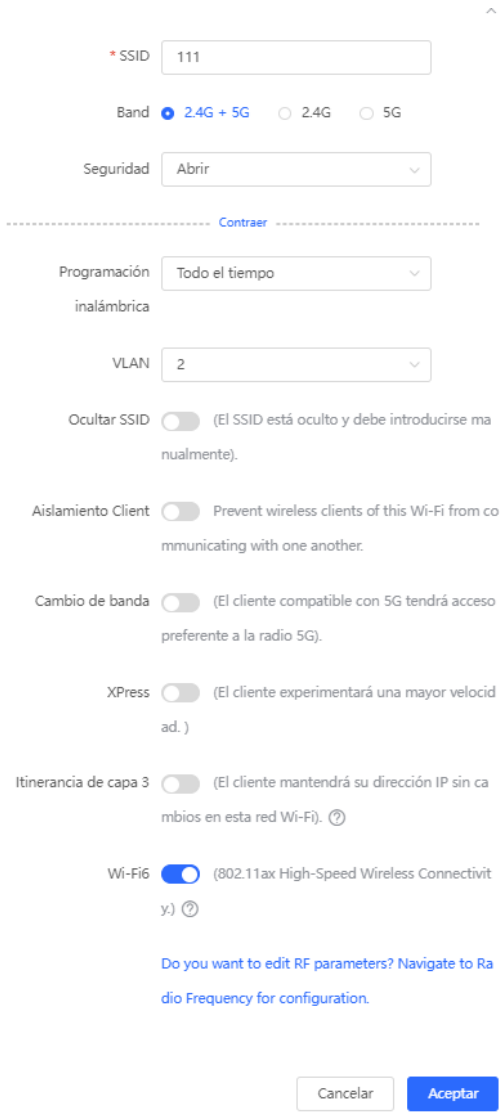


(5) Cambie al modo **Red**, seleccione **Red** > **Puertos LAN** > **Añadir** y configure VLAN 100 para IPTV. Si se utiliza la VLAN 1 predeterminada, ignore este paso.



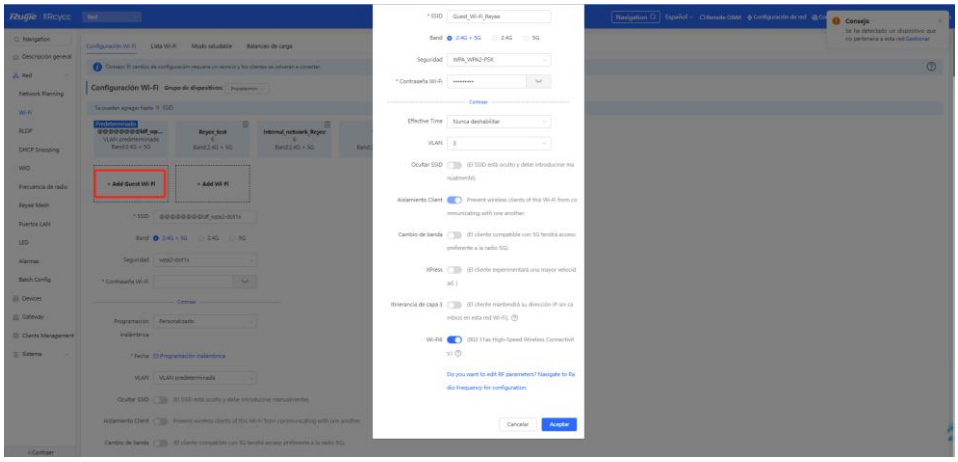
(6) Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Configuración Wi-Fi** y configure la red Wi-Fi para el personal y los huéspedes, y seleccione la VLAN 2 para el personal.





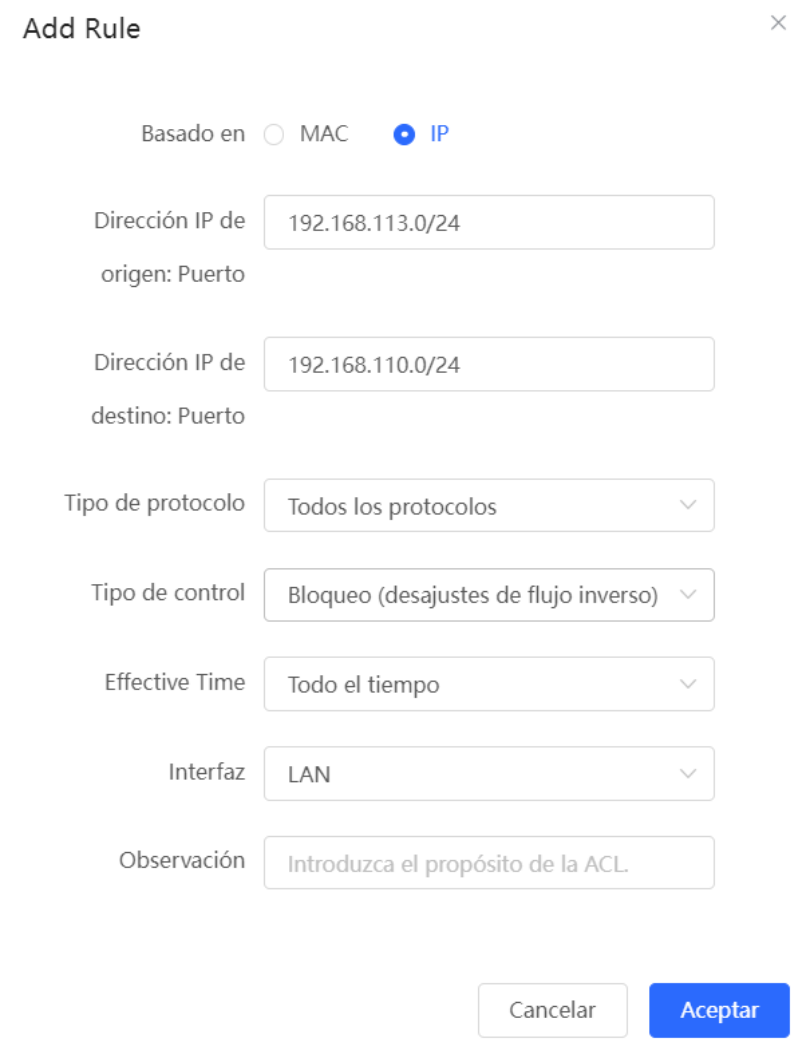
(7) Habilite el Wi-Fi de invitados y seleccione VLAN 3 para este.

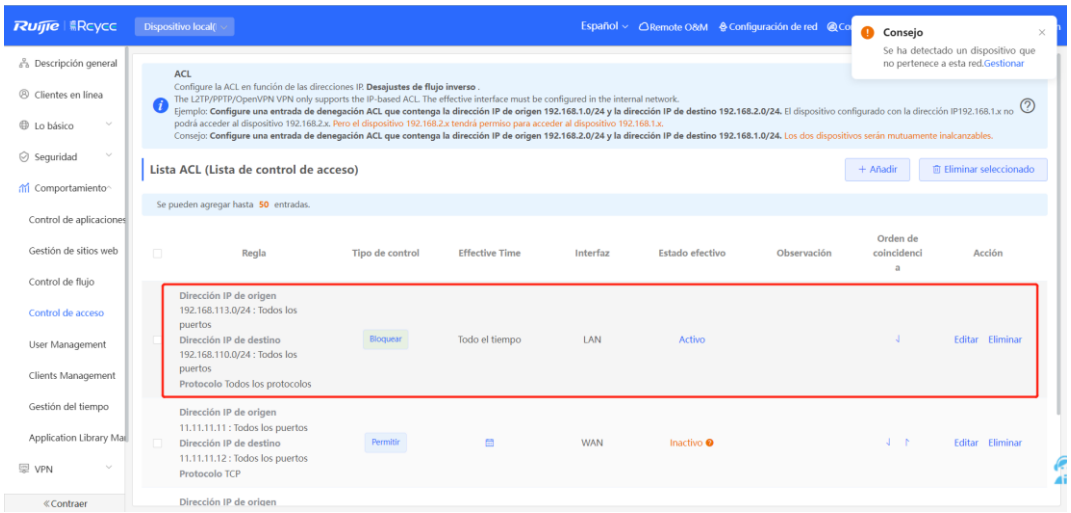
Cambie al modo **Red**. Seleccione **Red** > **Wi-Fi** > **Add Guest Wi-Fi**.



(8) Cambie al modo **Dispositivo local**. Seleccione **Comportamiento** > **Control de acceso** y configure una ACL para evitar que los huéspedes tengan acceso a la red interna.

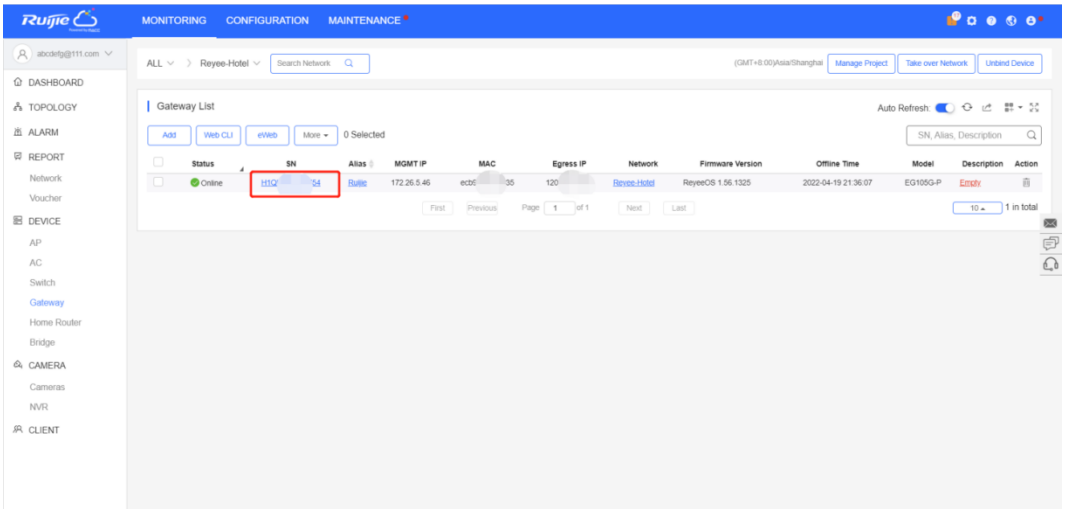
Añada dos reglas ACL para bloquear el acceso de los hosts en VLAN 3 a los hosts de VLAN1 y VLAN 2, y aplíquelas al puerto LAN.



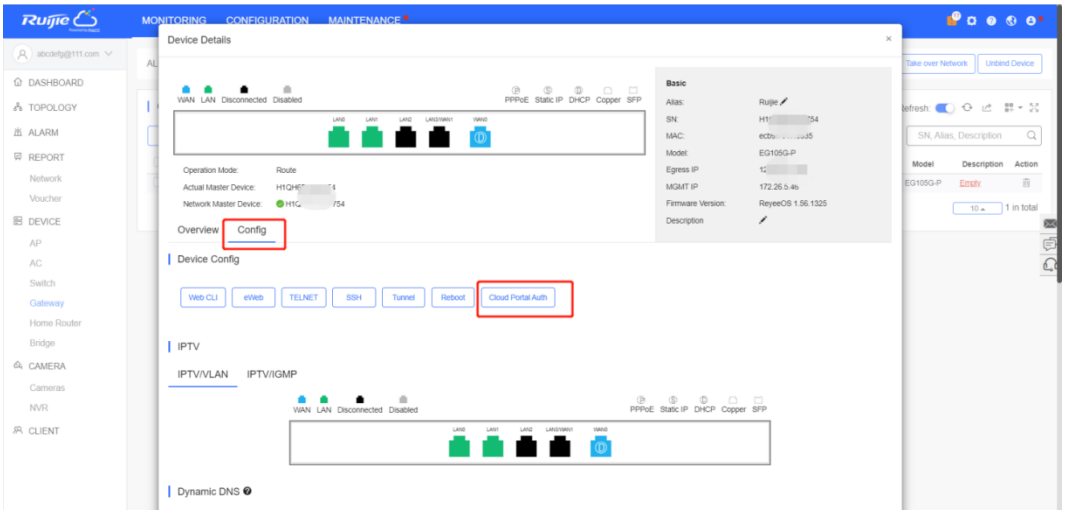


(9) Inicie sesión en Ruijie Cloud para configurar la autenticación por cupón en la nube para los huéspedes.

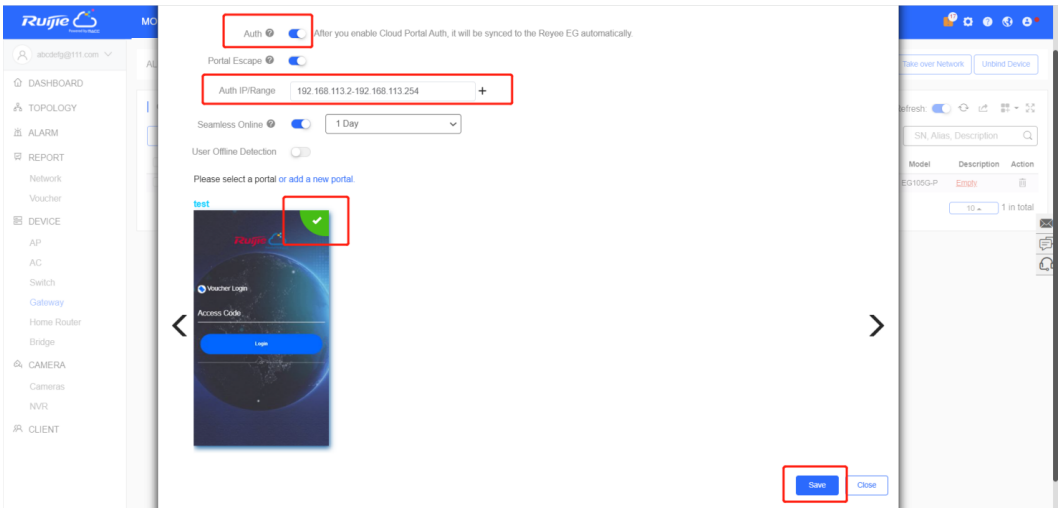
a Haga clic en el SN del EG para acceder a la página de los detalles del dispositivo.



b Seleccione **Config** > **Cloud Portal Auth.**

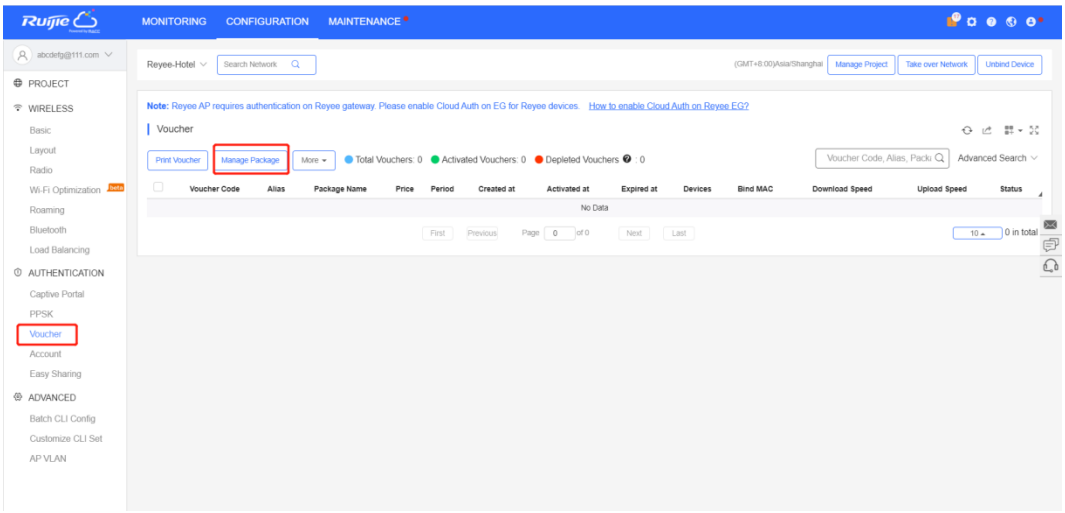


c Habilite la autenticación y configure las direcciones IP de los huéspedes en un rango de 192.168.113.2 a 192.168.113.254.

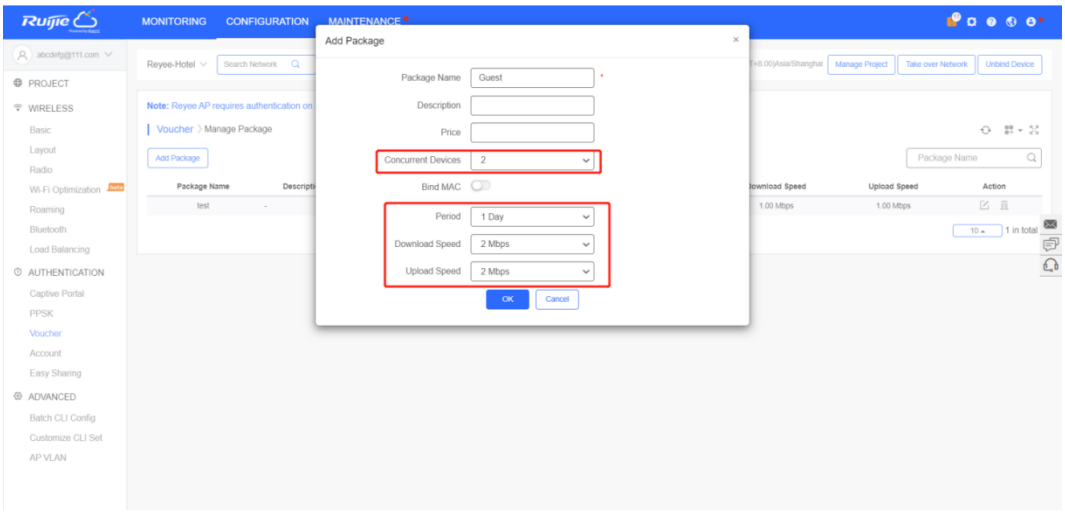


d Añada el paquete de cupones para los huéspedes.

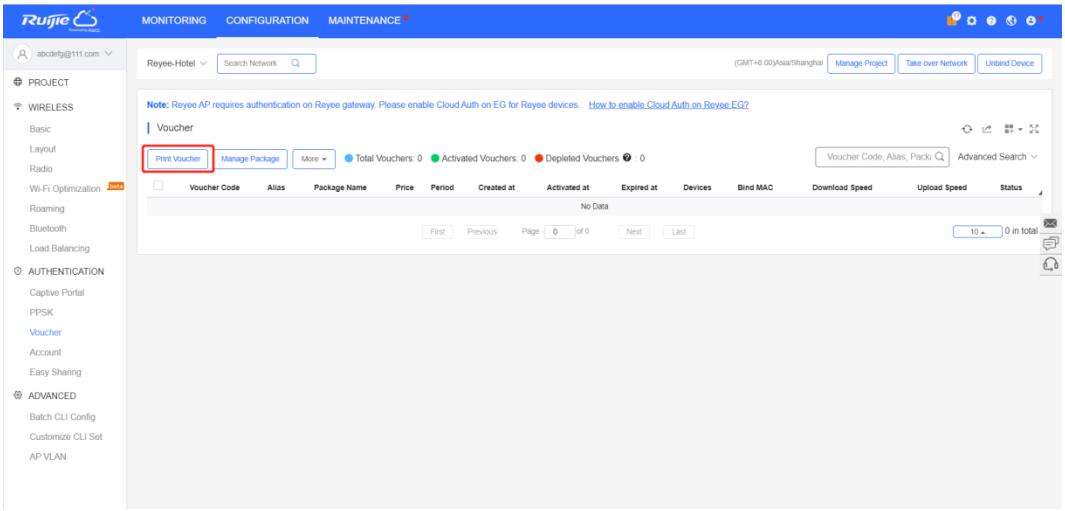
Seleccione **Voucher** > **Manage Package** > **Add Package** para añadir un paquete de cupones para los huéspedes.

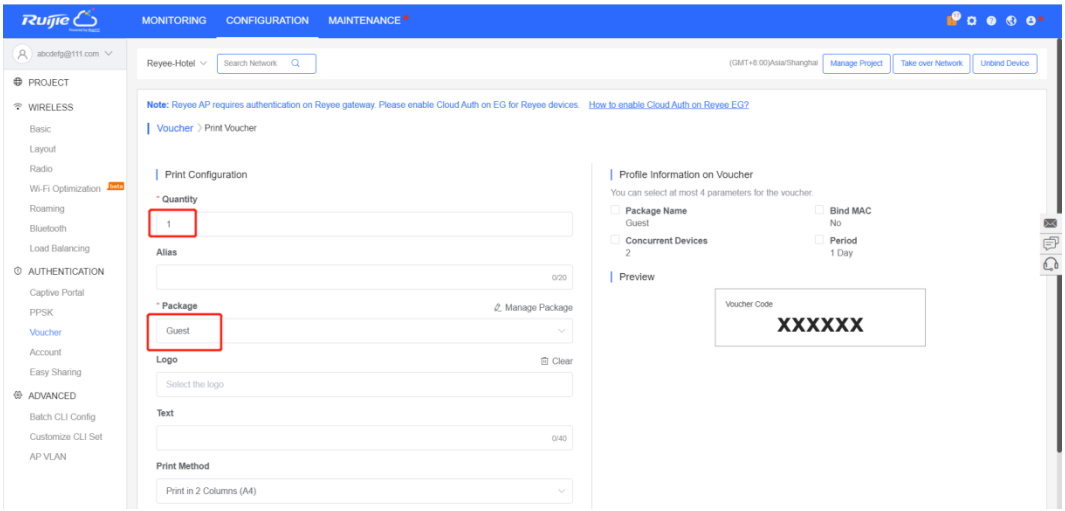


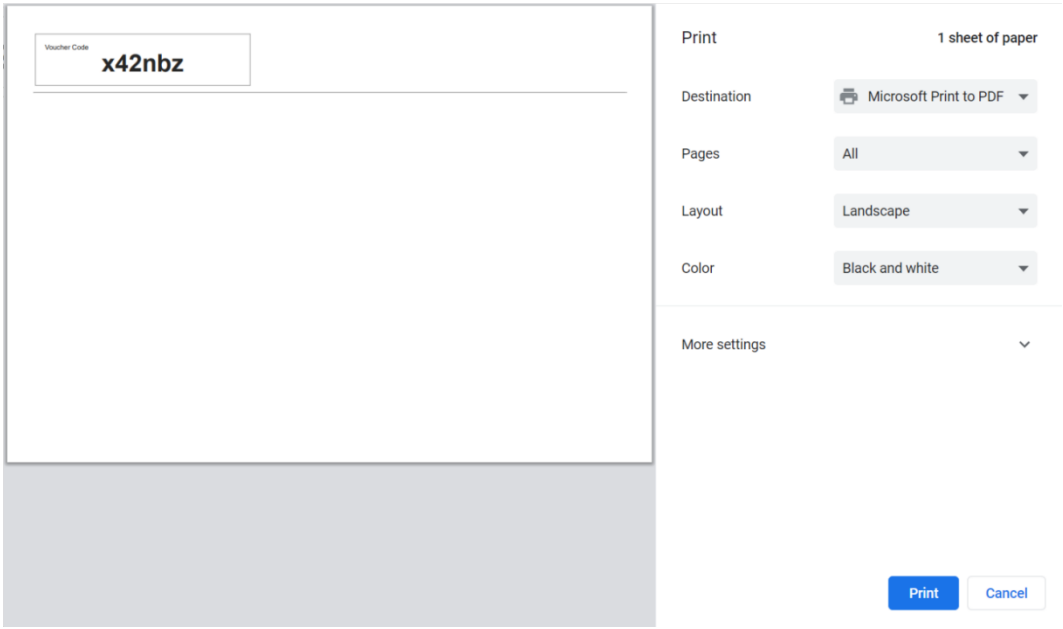
Ejemplo: configure los dispositivos concurrentes en 2, el periodo en 1 día, y la velocidad de carga y descarga en 2 Mbps.



e Haga clic en **Print Voucher** para obtener un código de invitado.

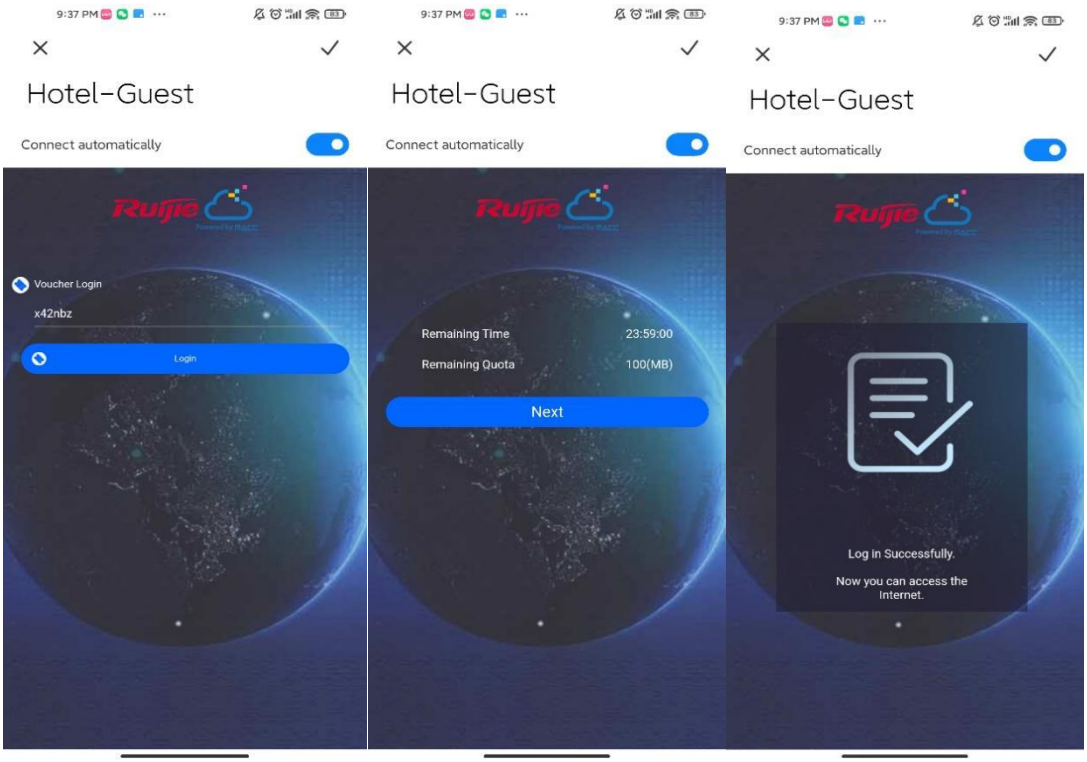






5.4.3 Verificación de la configuración

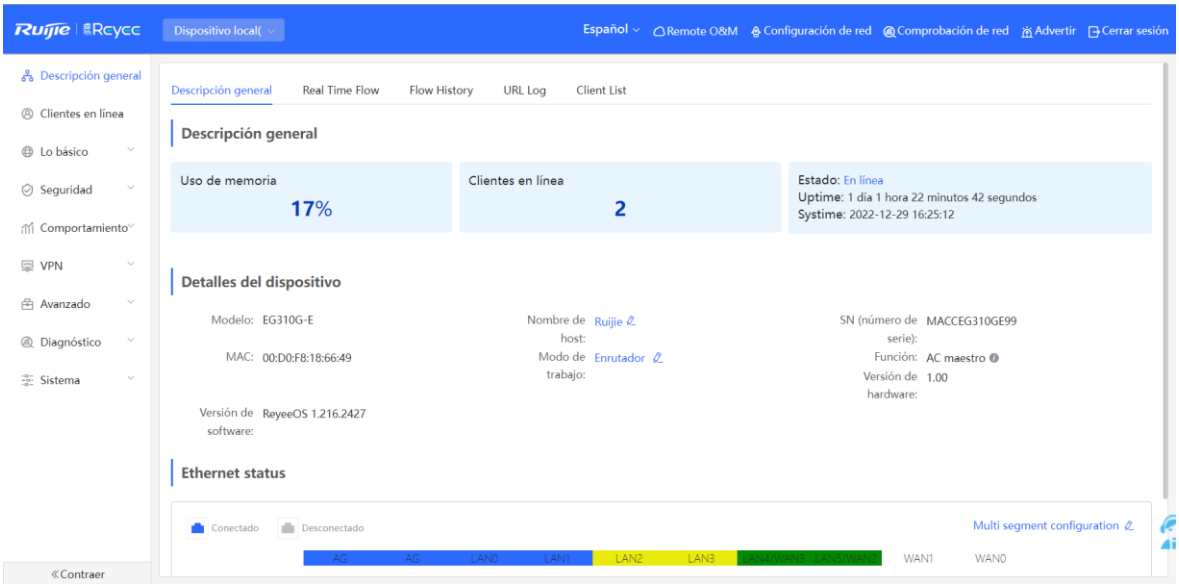
Conéctese al Wi-Fi de invitados. Verá que no le permite acceder a la dirección IP interna 192.168.110.1.



6 Preguntas frecuentes

7 Anexos: Vigilancia

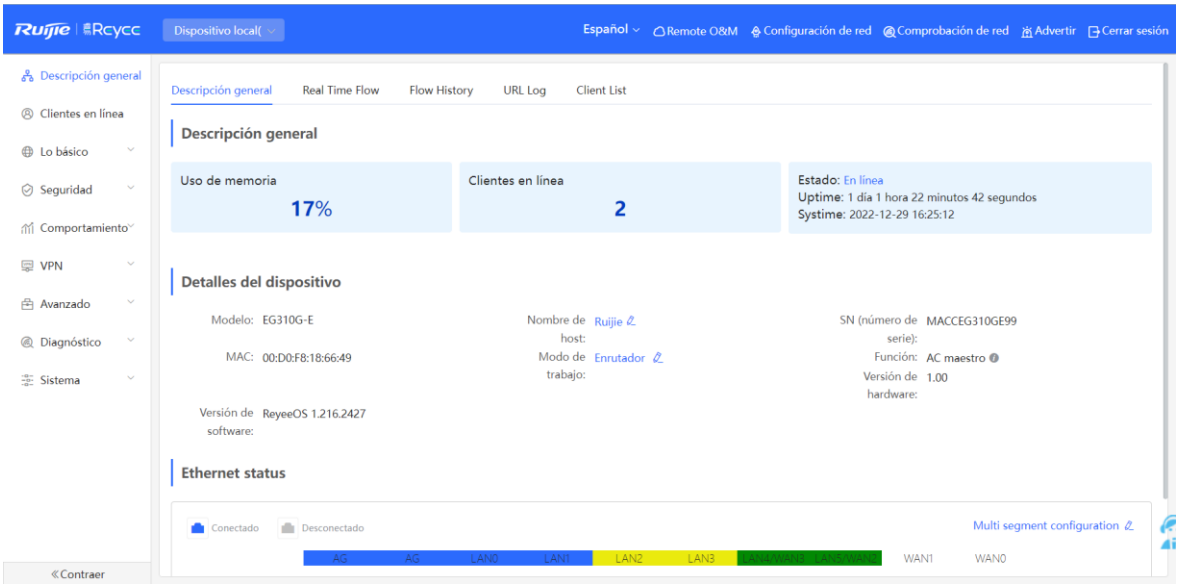
La página de descripción general muestra información sobre las secciones **Detalles del dispositivo**, **Wi-Fi**, **Estado de la Red** y **Real Time Flow**.



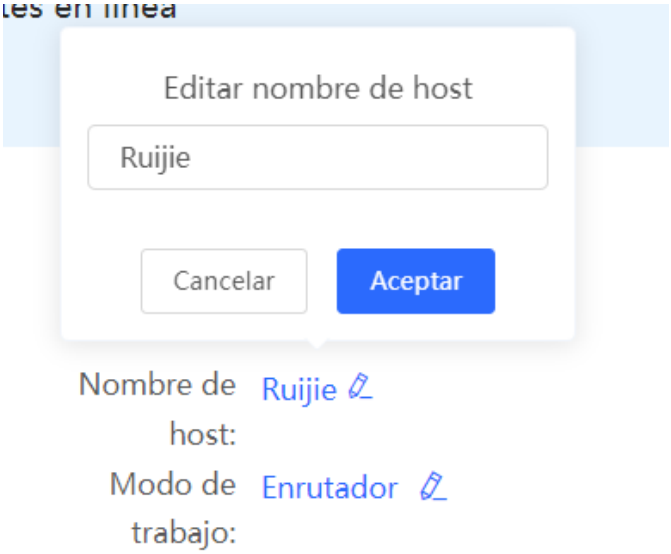
7.1 Información del dispositivo

Cambie al modo **Dispositivo local**. Seleccione **Descripción general > Descripción general**. En la página **Detalles del dispositivo** se muestran el modelo, el nombre de host, la dirección IP, la dirección MAC, la versión del software y el SN del router.

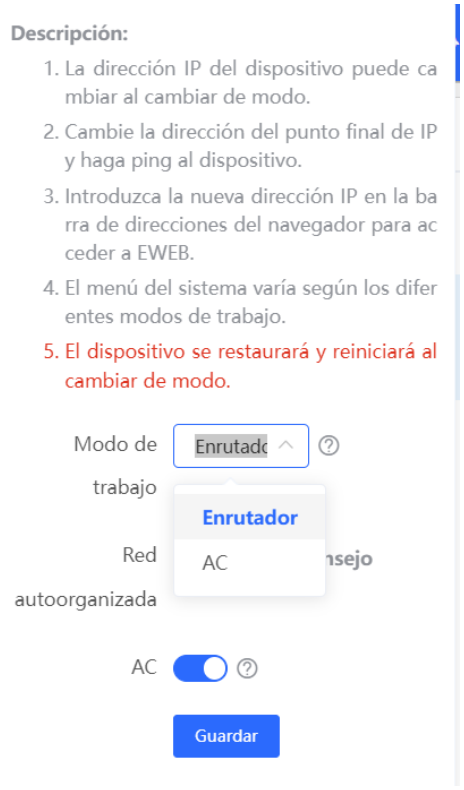
En la ventana **Descripción general** se muestran el uso de la memoria, el número de clientes en línea, el estado, el tiempo de actividad y la hora del sistema.



- El estado **En línea** indica el estado SON de los dispositivos Reyee, pero no el de Ruijie Cloud.
- Haga clic en **Nombre de host** para modificar el nombre del dispositivo.



- Haga clic en **Modo de trabajo** para cambiar el modo del dispositivo. Hay dos modos disponibles: modo **Enrutador** y modo **AC**. El modo predeterminado es **Enrutador**.



  - **Modo Enrutador:** indica el reenvío NAT.
  - **Modo AC:** indica el reenvío de puentes de red.

- **Red autoorganizada**:
  - -Si SON se habilita, se muestra la función del dispositivo.
  - -Si SON se deshabilita, el dispositivo funciona en modo independiente.
  - -Por defecto, SON se encuentra habilitado en modo AC.
- **AC**:
  - -Esta opción se encuentra habilitada de forma predeterminada. El dispositivo actúa como un controlador de acceso virtual para administrar dispositivos de enlace descendente.
  - -Cuando se deshabilita, el dispositivo debe elegirse como el AC antes de poder administrar los dispositivos de enlace descendente.

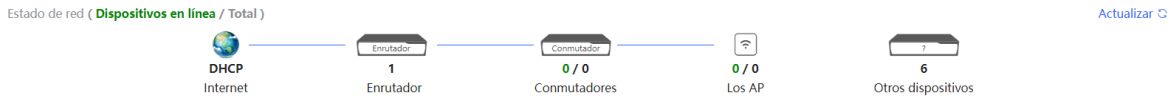
7.2 Información de Wi-Fi

Se puede asignar un nombre al Wi-Fi de la red y habilitar el Wi-Fi de invitados.

Add Wi-Fi: vaya a la página de configuración de Wi-Fi.

7.3 Estado de la red

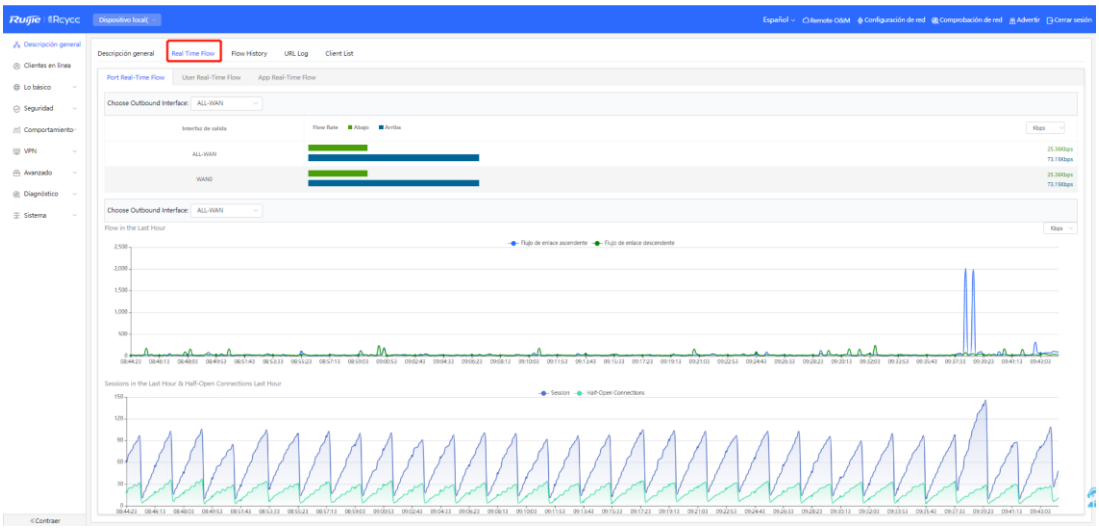
La página **Estado de red** muestra la topología y el estado de conexión de la red.



7.4 Flujo en tiempo real

Cambie al modo **Dispositivo local**. Seleccione **Descripción General** > **Real Time Flow**. La página **Real Time Flow** se abrirá.

Revise los flujos de tráfico en tiempo real con base en los puertos, los usuarios y las aplicaciones, incluyendo los flujos de los enlaces ascendentes y descendentes. Por defecto, la unidad es Kbps. Se puede cambiar a bps y Mbps.



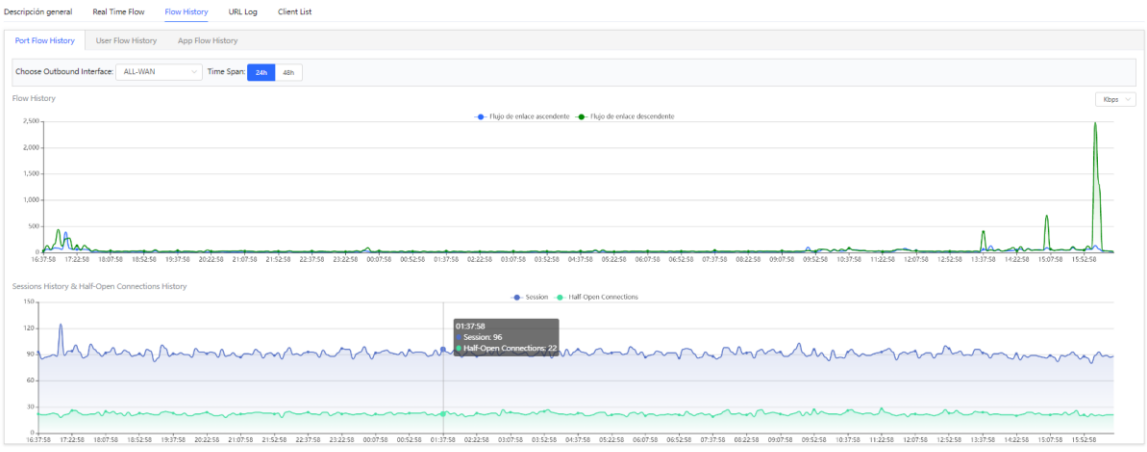
7.5 Historial de flujos

Nota

Esta función solo les compatible con el R202 y versiones posteriores.

Cambie al modo **Dispositivo local**. Seleccione **Descripción general** > **Flow History**. La página **Flow History** se abrirá.

Revise los flujos de tráfico con base en los puertos, los usuarios y las aplicaciones, incluyendo los flujos de los enlaces ascendentes y descendentes.



7.6 Registros de URL

Los registros de acceso de URL son aquellos relativos a los URL que tuvieron acceso a los dispositivos en la red interna, incluyendo el número y el resultado de auditoría.

Nota

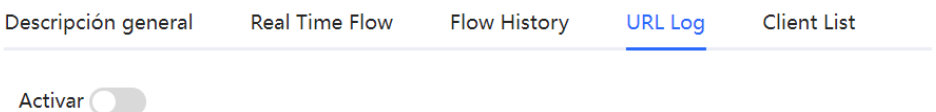
Esta función solo es compatible con los routers de la serie EG3, como el EG310G-E.

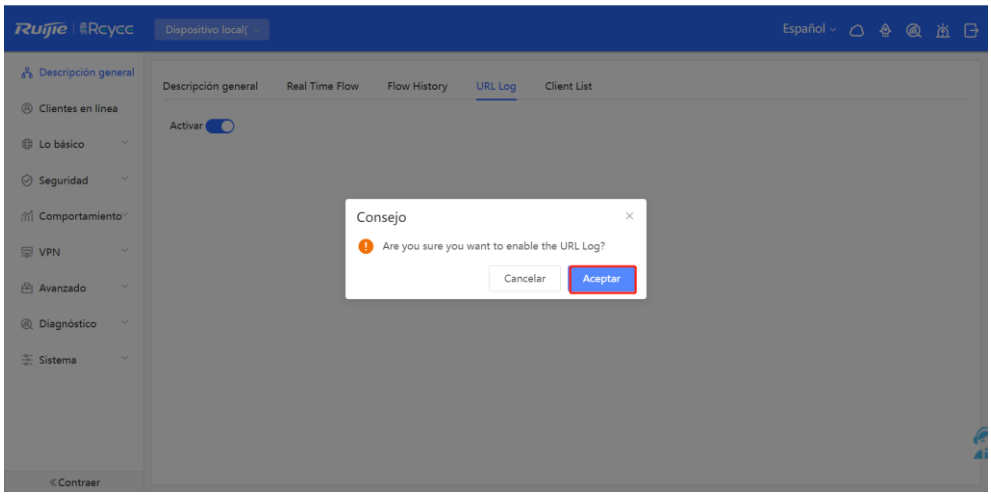
(1) Cambie al modo **Dispositivo local**.

(2) Seleccione **Descripción general** > **URL Log**.

(3) Habilite la función de registro de acceso de URL.

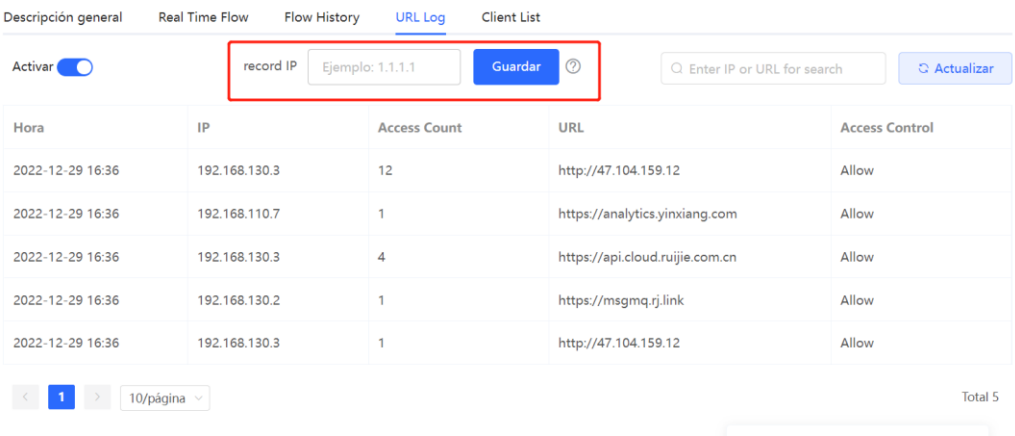
Cambie el interruptor a **Activar** y haga clic en **Aceptar** en el cuadro de diálogo.





(4) (Opcional) Configure una dirección IP para visualizar los registros de URL que tuvieron acceso a su dispositivo.

Por defecto, el sistema guarda todos los registros de URL que acceden a todos los dispositivos en la red interna. Para visualizar los registros de acceso de URL de un dispositivo en específico, configure una dirección IP en el cuadro de texto de **record IP** y haga clic en **Guardar**.



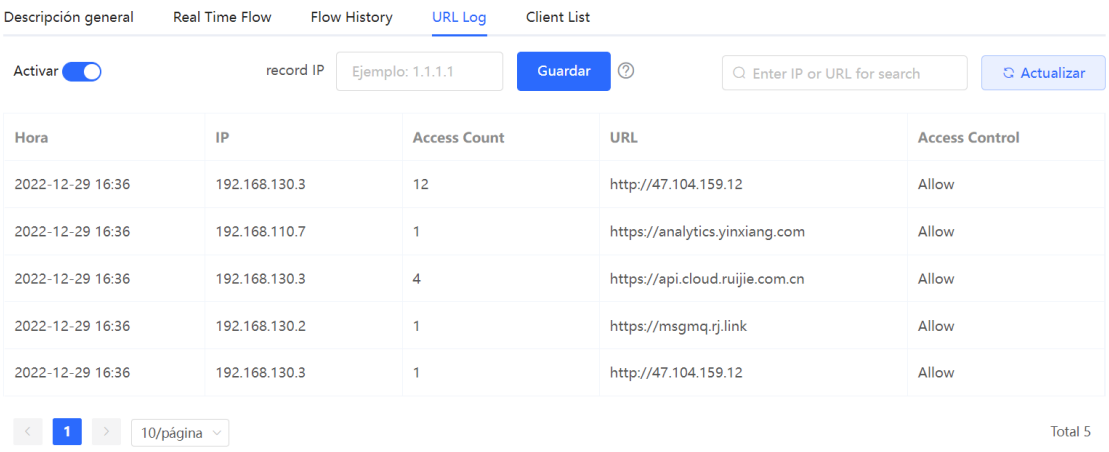
Nota

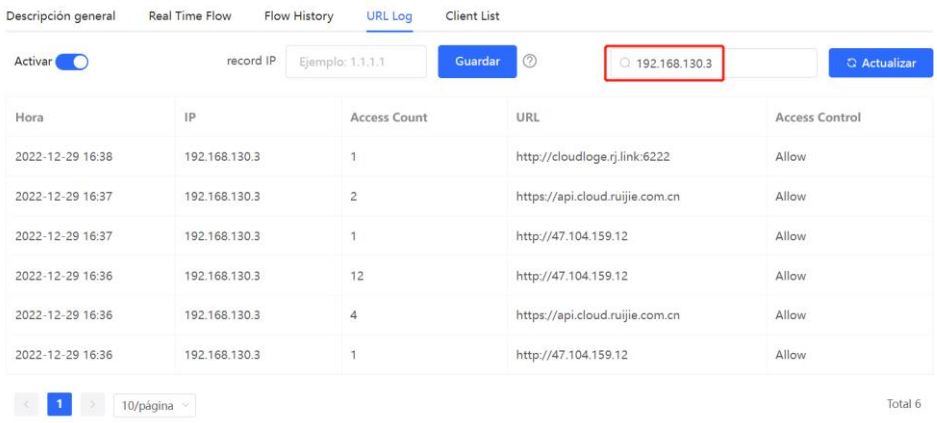
Para restaurar los registros de acceso de URL de todos los dispositivos en la red interna, borre la información del cuadro de texto de **record IP** y haga clic en **Guardar**.

(5) Revise los detalles de los registros de URL.

Cada registro incluye la hora de acceso, la dirección IP y el número de accesos.

Se pueden buscar registros por dirección IP o URL.

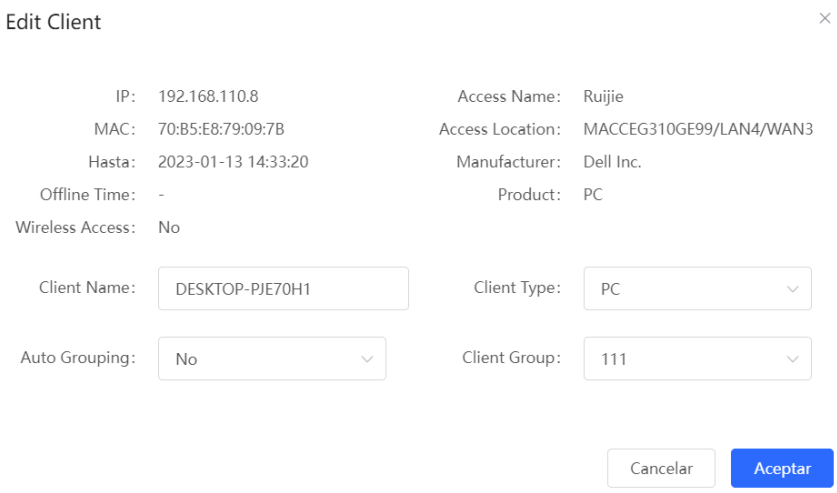




7.7 Clientes en línea

Cambie al modo **Dispositivo local**. Seleccione **Descripción general** > **Client List**. Se abrirá la página **Client List**.

Seleccione un cliente de la lista y haga clic en **Ver detalles/Editar**. Aquí podrá visualizar los nombres de usuario de los clientes, el tipo de cliente (por cable o inalámbrico), su dirección IP o MAC, la velocidad actual, el nombre de la red Wi-Fi a la que se conecta y el estado del control de acceso.


Edit Client
IP: 192.168.110.8
MAC: 70:B5:E8:79:09:7B
Hasta: 2023-01-13 14:33:20
Offline Time: -
Wireless Access: No
Access Name: Ruijie
Access Location: MACCEG310GE99/LAN4/WAN3
Manufacturer: Dell Inc.
Product: PC
Client Name: DESKTOP-PJE70H1
Client Type: PC
Auto Grouping: No
Client Group: 111
Cancelar
Aceptar