GUÍA DE ADMINISTRACIÓN

Router VPN multifunción RV130

Router VPN multifunción inalámbrico RV130W

Contenido

1

Introducción

En la página **Introducción**, se muestran las tareas de configuración más comunes del dispositivo. Utilice los enlaces que aparecen en la página web para ir a la página de configuración relevante.

Esta página aparecerá cada vez que inicie el Administrador de dispositivos. Para modificar esta opción, marque la opción **No mostrar al inicio**.

Configuración inicial

Cambiar contraseña de admin. predeterminada	Muestra la página **Usuarios**, donde puede modificar la contraseña de administrador y configurar una cuenta de invitado. Consulte **Configuración de cuentas de usuario**.
Iniciar Asistente de instalación	Inicia el Asistente de instalación. Siga las instrucciones que aparecen en la pantalla.
Configurar opciones WAN	Abre la página **Configuración de Internet** para cambiar los parámetros, como por ejemplo, el nombre de host para el dispositivo. Consulte **Configuración de opciones WAN**.
Configurar opciones LAN	Abre la página **Configuración de LAN** para modificar los parámetros LAN, como por ejemplo, la dirección IP de administración. Consulte **Configuración de opciones LAN**.
Configurar opciones inalámbricas	Abre la página **Configuración básica** para administrar la radio. Consulte **Configuración de redes inalámbricas**.

Acceso rápido

Actualizar firmware del router	Abre la página **Actualización del firmware/idioma** para actualizar el firmware del dispositivo o el paquete de idioma. Consulte **Actualización del Firmware o cambio de idioma**.
Agregar clientes VPN	Abre la página **Servidor PPTP** para configurar y administrar los túneles VPN. Consulte **Configuración de PPTP**.
Configurar acceso a admin. remota	Abre la página **Configuración básica** para activar las funciones básicas del dispositivo. Consulte **Configuración de los parámetros básicos de firewall**.

Estado del dispositivo

Resumen del sistema	Muestra la página **Resumen del sistema**, donde se observa el estado del firmware, el estado de configuración de IPv4 e IPv6, y el estado de las redes inalámbricas y del firewall del dispositivo. Consulte **Visualización del resumen del sistema**.
Estado inalámbrico	Muestra la página **Estadísticas inalámbricas**, la cual muestra el estado de la radio. Consulte **Visualización de estadísticas inalámbricas**.
Estado VPN	Muestra la página **Servidor VPN IPsec**, que proporciona una lista de las VPN administradas por este dispositivo. Consulte **Visualización del estado de conexión VPN IPsec de sitio a sitio**.

Otros recursos

Asistencia técnica	Haga clic en este vínculo para abrir la página de asistencia técnica de Cisco.
Foros	Haga clic en este vínculo para visitar los foros de asistencia técnica en línea de Cisco.

Cómo conectarse a la red inalámbrica

Para conectar un dispositivo cliente (por ejemplo, una computadora) a la red inalámbrica, configure la conexión inalámbrica en el dispositivo cliente con la información de seguridad inalámbrica que configuró para el router mediante el Asistente de instalación.

Los siguientes pasos se brindan como ejemplo; es posible que deba configurar el dispositivo de manera diferente. Para obtener instrucciones específicas para el dispositivo cliente, consulte la documentación correspondiente.

PASO 1 Abra la ventana o programa de configuración de conexiones inalámbricas del dispositivo.

Es posible que la computadora tenga instalado un software especial para administrar conexiones inalámbricas, o puede encontrar conexiones inalámbricas en el Panel de control en la ventana **Conexiones de red** o **Red e Internet**. (La ubicación depende del sistema operativo).

PASO 2 Escriba el nombre de la red (SSID) que eligió para la red en el Asistente de instalación.

PASO 3 Elija el tipo de cifrado y escriba la clave de seguridad que especificó en el Asistente de instalación.

Si no habilitó la seguridad (lo que no es recomendable), deje los campos de cifrado inalámbrico que se configuraron con el tipo de seguridad y la frase clave en blanco.

PASO 4 Verifique la conexión inalámbrica y guarde la configuración.

2

Visualización del estado del dispositivo

Para asegurarse de que los datos y las estadísticas se actualicen con frecuencia en las páginas de Estado, seleccione una velocidad de actualización en la lista desplegable **Velocidad de actualización**.

Visualización del panel de comando

Seleccione **Estado** > **Panel de comando** para ver una instantánea de la configuración del dispositivo. La página Panel de comando muestra información sobre la versión de firmware del dispositivo, el uso de CPU y memoria, la configuración de los registros de errores, LAN, WAN, redes inalámbricas, VPN IPsec de sitio a sitio, y ajustes del servidor VPN PPTP.

Para modificar la información que se visualiza, haga clic en el enlace **detalles** para ir a la página de configuración de la sección. Si desea obtener más información sobre la administración de configuraciones de la página **Panel de comando**, consulte:

- **Configuración de los valores de registro**
- **Configuración de VPN IPsec básicas de sitio a sitio**
- **Configuración de opciones LAN**
- **Configuración de conexiones WAN alámbricas**
- **Configuración de las opciones inalámbricas básicas**

En la lista desplegable **Velocidad de actualización**, seleccione la velocidad a la que se actualizarán los últimos valores de parámetros y estadísticas en el panel de comando.

En la página Panel de comando, también se muestra una vista interactiva del panel posterior del dispositivo cuando hace clic en **Mostrar vista de panel**. Desplace el mouse sobre cada puerto para ver información de conexión.

Visualización del resumen del sistema

Seleccione **Estado** > **Resumen del sistema** para ver detalles de las propiedades del dispositivo, de los ajustes de redes en los modos de direcciones IP, del firewall, de las redes inalámbricas y de los parámetros VPN. Haga clic en **Actualizar** para consultar la información más actualizada.

Haga clic en el enlace subrayado para ir a la ventana de configuración relacionada. Por ejemplo, para modificar la dirección IP de LAN, haga clic en **IP de LAN**. Se muestra la ventana de configuración de LAN.

La página **Resumen del sistema** muestra información en las siguientes secciones:

Información del sistema

- **Versión del firmware:** la versión actual del software que ejecuta el dispositivo.
- **Suma de comprobación MD5 de Firmware:** el algoritmo del resumen de mensaje utilizado para verificar la integridad de los archivos.
- **Configuración regional:** el idioma instalado en el router.
- **Versión del idioma**: la versión del paquete de idiomas instalado. La versión del paquete de idiomas debe ser compatible con el firmware actualmente instalado. En algunos casos, se puede usar un paquete de idiomas anterior con una nueva imagen de firmware. El router verifica la versión del paquete de idiomas para ver si es compatible con la versión de firmware actual.
- **Suma de comprobación de idioma MD5**: suma de comprobación MD5 del paquete de idiomas.
- **Modelo CPU:** conjunto de chips de la CPU utilizada actualmente.
- **Número de serie:** el número de serie del dispositivo.
- **Tiempo de act. del sist:** el tiempo de ejecución del sistema.
- **Hora actual:** la hora del día.
- **PID VID:** el Id. del producto y el Id. de la versión del dispositivo.

Configuración IPv4

- **IP de LAN:** la dirección IP de LAN del dispositivo.
- **IP de WAN:** la dirección IP de WAN del dispositivo. Para liberar la dirección IP actual y obtener una nueva, haga clic en **Liberar** o **Renovar**.

- **Puerta de enlace**: dirección IP de la puerta de enlace a la que el dispositivo está conectado (por ejemplo, el módem alámbrico).
- **Modo:** se muestra **Puerta de enlace**, si NAT está habilitada, o **Router**.
- **DNS 1:** dirección IP del servidor DNS primario del puerto WAN.
- **DNS 2:** dirección IP del servidor DNS secundario del puerto WAN.
- **DDNS:** indica si el DNS dinámico está habilitado o deshabilitado.

Configuración IPv6

- **IP de LAN:** la dirección IP de LAN del dispositivo.
- **IP de WAN:** la dirección IP de WAN del dispositivo.
- **Puerta de enlace**: dirección IP de la puerta de enlace a la que el dispositivo está conectado (por ejemplo, el módem alámbrico).
- **NTP**: servidor del Protocolo de hora en la red (nombre de host o dirección IPv6).
- **Delegación de prefijo**: el prefijo obtenido desde el dispositivo en el ISP que se le otorga a las direcciones IPv6 en el dispositivo.
- **DNS 1:** la dirección IP del servidor DNS primario.
- **DNS 2:** la dirección IP del servidor DNS secundario.

Resumen inalámbrico

Muestra el nombre público y los parámetros de seguridad para las redes inalámbricas configuradas en la página **Inalámbrica > Configuración básica**. Para obtener más información, consulte **Configuración de las opciones inalámbricas básicas**.

Estado de configuración de firewall

Muestra los ajustes de DoS, de solicitudes WAN y de administración remota configurados en la página **Firewall > Configuración básica**. Para obtener más información, consulte **Configuración de los parámetros básicos de firewall**.

Estado de configuración de VPN

Muestra las conexiones VPN IPsec y PPTP disponibles y los usuarios conectados para cada tipo de VPN.

- **Conexiones IPsec disponibles:** cantidad de conexiones VPN IPsec disponibles.

- **Conexiones VPN PPTP disponibles:** cantidad de conexiones VPN PPTP disponibles.
- **Usuarios IPsec conectados:** cantidad de usuarios VPN IPsec conectados.
- **Usuarios PPTP VPN conectados:** cantidad de usuarios PPTP VPN conectados.

Si desea obtener más información sobre cómo configurar cuentas de usuario y conexiones de servidor VPN, consulte **Configuración de VPN IPsec básicas de sitio a sitio** y **Configuración de PPTP**.

Visualización de servicios TCP/IP activos

Seleccione **Estado > Servicios TCP/IP activos** para ver las conexiones TCP/IP IPv4 e IPv6 activas en el dispositivo. La sección **Lista de servicios activos** para IPv4 e IPv6 muestra los protocolos y servicios activos en el dispositivo.

Visualización de estadísticas inalámbricas

Seleccione **Estado > Estadísticas inalámbricas** para consultar datos de estadísticas inalámbricas para el radio del dispositivo. En el campo **Velocidad de actualización**, seleccione la velocidad a la que se mostrarán las últimas estadísticas.

Para mostrar los bytes en kilobytes (KB) y los datos numéricos en valores redondeados, marque **Mostrar datos estadísticos simplificados** y haga clic en **Guardar**. De manera predeterminada, los datos de bytes se muestran en bytes y otros datos numéricos se muestran en versión larga.

Para restablecer los contadores de estadísticas inalámbricas, haga clic en **Borrar conteo**. Los contadores se restablecen cuando se reinicia el dispositivo.

Visualización del estado del portal cautivo

Seleccione **Estado > Portal cautivo** para ver información sobre los usuarios del portal cautivo conectados. Si desea obtener más información sobre cómo configurar portales cautivos en el dispositivo, consulte **Configuración de un portal cautivo**.

Visualización del estado de conexión VPN IPsec de sitio a sitio

Seleccione **Estado > VPN IPsec de sitio a sitio** para ver el estado de conexión de las políticas VPN IPsec de sitio a sitio activas en el dispositivo. Si desea obtener información sobre cómo configurar políticas VPN, consulte **Configuración de VPN IPsec básicas de sitio a sitio**.

Para cambiar la velocidad a la que se muestra el último estado de conexión en tiempo real, seleccione una velocidad de actualización en la lista desplegable **Velocidad de actualización**.

De manera predeterminada, los datos de bytes se muestran en bytes y otros datos numéricos se muestran en versión larga. Para mostrar los bytes en kilobytes (KB) y los datos numéricos en forma redondeada, marque **Mostrar datos estadísticos simplificados** y haga clic en **Guardar**.

Para finalizar una conexión VPN activa, haga clic en **Desconectar**.

Visualización del estado del servidor VPN IPsec

Seleccione **Estado > Servidor VPN IPsec** para ver la lista de conexiones VPN IPsec y la duración de cada conexión. Si desea obtener más información sobre cómo configurar las conexiones VPN IPsec, consulte **Configuración del servidor VPN IPsec**.

Visualización del servidor PPTP

Seleccione **Estado > Servidor PPTP** para ver una lista de las conexiones VPN PPTP, la duración de cada conexión y las acciones que puede realizar en esas conexiones. Si desea obtener más información sobre cómo configurar las conexiones VPN PPTP, consulte **Configuración de PPTP**.

Visualización de registros

Elija **Estado > Ver registros**. Haga clic en **Actualizar registros** para visualizar las últimas entradas de registro.

Para filtrar registros, o especificar la gravedad de los registros para mostrar, marque las casillas que están junto al tipo de registro y haga clic en **Ir**. Tenga en cuenta que todos los tipos de registro que están arriba de un tipo de registro seleccionado se incluyen automáticamente y no puede desactivarlos. Por ejemplo, si marca la casilla de verificación **Error**, se incluyen automáticamente registros de emergencia, alerta y críticos además de los registros de errores.

Los niveles de gravedad de los eventos se detallan de mayor gravedad a menor gravedad, de la siguiente manera:

- **Emergencia**: el sistema no se puede utilizar.
- **Alerta**: se necesita acción.
- **Crítico**: el sistema está en condición crítica.
- **Error**: el sistema está en condición de error.
- **Advertencia**: se presentó una advertencia del sistema.
- **Notificación**: el sistema está funcionando correctamente, pero se presentó un aviso del sistema.
- **Informativo**: información de dispositivos.
- **Depuración**: proporciona información detallada acerca de un evento.

Para eliminar todas las entradas en la ventana de registros, haga clic en **Borrar registros**.

Para guardar todos los mensajes de registro del dispositivo en el disco duro local, haga clic en **Guardar registros**.

Para especificar la cantidad de entradas que se debe mostrar por página, elija un número en el menú desplegable.

Para moverse entre páginas de registros, use los botones de navegación.

Visualización de dispositivos conectados

La página **Dispositivos conectados** muestra información sobre los dispositivos cliente activos conectados al router. Para ver los dispositivos conectados, seleccione **Estado** > **Dispositivos conectados**.

Para especificar los tipos de interfaz que desea visualizar, elija un valor en el menú desplegable **Filtro**:

- **Todos:** todos los dispositivos conectados al router.
- **Inalámbricos:** todos los dispositivos conectados mediante la interfaz inalámbrica.
- **Por cable:** todos los dispositivos conectados al router a través de los puertos Ethernet.
- **WDS:** todos los dispositivos con Sistema de distribución inalámbrica (WDS) conectados al router.

En la **Tabla IPv4 ARP**, se muestra la información de otros routers que han respondido la solicitud del Protocolo de resolución de direcciones (ARP) del dispositivo. Si un dispositivo no responde a la solicitud, se elimina de la lista.

En la **Tabla IPv6 NDP**, se muestran todos los dispositivos de protocolo de detección de vecinos (NDP) IPv6 conectados al enlace local del dispositivo.

Visualización de estadísticas del puerto

La página **Estadísticas del puerto** muestra la actividad detallada del puerto.

Para ver las estadísticas, seleccione **Estado > Estadísticas del puerto**.

Para actualizar la página a intervalos regulares, seleccione una velocidad de actualización en la lista desplegable **Velocidad de actualización**.

Para mostrar los bytes en kilobytes (KB) y los datos numéricos en forma redondeada, marque **Mostrar datos estadísticos simplificados** y haga clic en **Guardar**. De manera predeterminada, los datos de bytes se muestran en bytes y otros datos numéricos se muestran en versión larga.

Para restablecer los contadores de estadísticas del puerto, haga clic en **Borrar conteo**.

La página **Estadísticas del puerto** muestra la siguiente información:

Interfaz	Nombre de la interfaz de red.
Paquete	Cantidad de paquetes recibidos/enviados.
Byte	Cantidad de bytes de información recibidos/enviados por segundo.
Error	Cantidad de errores de paquetes recibidos/enviados.
Descartado	Cantidad de paquetes recibidos/enviados que se suprimieron.
Multidifusión	Cantidad de paquetes de multidifusión enviados por este radio.
Colisiones	Cantidad de colisiones de señales que se produjeron en este puerto. Una colisión se produce cuando el puerto intenta enviar datos al mismo tiempo que un puerto en otro router u otra computadora conectado a este puerto.

Visualización del estado de la red móvil

Las estadísticas de la red móvil sobre las redes 3G/4G y el dispositivo de comunicación se configuran en el dispositivo.

Para ver el estado de la red móvil, elija **Estado > Red móvil**. Aparece la siguiente información:

- **Conexión**: dispositivo conectado a la red de invitado.
- **Dirección IP de Internet**: la dirección IP asignada al dispositivo USB.
- **Máscara de subred:** máscara de subred del dispositivo USB.
- **Puerta de enlace predeterminada:** dirección IP de la puerta de enlace predeterminada.
- **Tiempo de act. de la conexión:** el tiempo de actividad del enlace.
- **Uso actual de la sesión:** volumen de datos que se reciben (Rx) y se transmiten (Tx) en el enlace móvil.
- **Uso mensual**: uso mensual de ancho de banda y descarga de datos.

- **Nombre del fabricante**: nombre del fabricante de la tarjeta.
- **Modelo de tarjeta:** número del modelo de tarjeta.
- **Firmware de la tarjeta:** versión de firmware de la tarjeta.
- **Estado SIM**: estado del módulo de identificación del suscriptor (SIM)
- **IMS:** identificación específica asociada con los usuarios de teléfonos móviles con redes GSM, UMTS o LTE.
- **Portadora:** portadora de la red móvil.
- **Tipo de servicio:** tipo de servicio al que se accede.
- **Intensidad de señal:** intensidad de la señal de la red móvil inalámbrica.
- **Estado de la tarjeta**: estado de la tarjeta de datos.

3

Configuración de red

Configuración de conexiones WAN alámbricas

La configuración de las propiedades WAN para una red IPv4 difiere según el tipo de conexión a Internet que tenga.

Configuración de DHCP (configuración automática)

Si su proveedor de servicios de Internet (ISP) usa el protocolo de control de host dinámico (DHCP) para asignarle una dirección IP, usted recibe una dirección IP que se genera de forma dinámica cada vez que inicia sesión.

Para configurar las opciones WAN DHCP, siga estos pasos:

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En la lista desplegable **Tipo de conexión a Internet**, seleccione **Configuración automática - DHCP**.

PASO 3 En la lista desplegable **Origen de servidor DNS**, escoja una de las siguientes formas de establecer la dirección del servidor DNS:

- Si su ISP ya le proporcionó direcciones de servidor DNS, seleccione **Usar estos servidores DNS** e ingrese las direcciones primaria y secundaria.
- Si su ISP no le proporcionó direcciones de servidor DNS, seleccione **Obtener del ISP de forma dinámica**.
- Para usar los servidores DNS proporcionados por OpenDNS (208.67.222.222, 208.67.220.220) para resolver las direcciones web, seleccione **Usar OpenDNS**.

PASO 4 Haga clic en **Guardar**.

Configuración de IP estática

Si su ISP le asignó una dirección IP permanente, siga los pasos a continuación para configurar sus opciones WAN:

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **IP estática**.

PASO 3 Escriba esta información:

Dir. IP de Internet	Dirección IP del puerto WAN
Máscara de subred	Máscara de subred del puerto WAN
Origen de servidor DNS	La dirección del servidor DNS. Si su ISP ya le proporcionó direcciones de servidor DNS, seleccione **Usar estos servidores DNS** e ingrese las direcciones primaria y secundaria en los campos **DNS estático 1** y **DNS estático 2**. Para usar los servidores DNS proporcionados por OpenDNS (208.67.222.222, 208.67.220.220) para resolver las direcciones web, seleccione **Usar OpenDNS**.
Puerta de enlace predet.	Dirección IP de la puerta de enlace predeterminada

PASO 4 Haga clic en **Guardar**.

Configuración de PPPoE

Para configurar los valores del protocolo punto a punto por Ethernet (PPPoE):

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **PPPoE**.

PASO 3 Seleccione un perfil PPPoE o haga clic en **Configurar perfil** para crear un nuevo perfil.

PASO 4 En la página Perfiles PPPoE, escriba la siguiente información (quizá deba comunicarse con su ISP para obtener información de inicio de sesión de su PPPoE):

Nombre del perfil	Un nombre único para el perfil PPPoE.
Nombre de usuario	El nombre de usuario asignado por el ISP.
Contraseña	La contraseña asignada por el ISP.
Origen de servidor DNS	La dirección del servidor DNS. Si su ISP ya le proporcionó direcciones de servidor DNS, seleccione **Usar estos servidores DNS** e ingrese las direcciones primaria y secundaria. De lo contrario, seleccione **Obtener del ISP de forma dinámica**. Para usar los servidores DNS proporcionados por OpenDNS (208.67.222.222, 208.67.220.220) para resolver las direcciones web, seleccione **Usar OpenDNS**.
Conectar a petición	Seleccione esta opción si su ISP le cobra en función del tiempo que está conectado. Cuando selecciona esta opción, la conexión a Internet solo está activa si hay tráfico. Si no hay flujo de tráfico, la conexión está inactiva; es decir, está cerrada. Si hace clic en **Conectar a petición**, escriba los minutos que deben transcurrir para que se desactive la conexión en el campo **Tiempo máx. de inactividad**.
Mantener conexión	Cuando selecciona esta opción, la conexión a Internet está siempre activa. En el campo Período de repetición de marcación, escriba los segundos que deben transcurrir para que el dispositivo intente volver a conectarse una vez desconectado.

Tipo de autenticación	**Negociación automática**: el servidor envía una solicitud de configuración que especifica el algoritmo de seguridad establecido. Luego, el dispositivo envía las credenciales de autenticación con el tipo de seguridad que envió el servidor. **PAP**: Protocolo de autenticación de contraseña (PAP); el protocolo de punto a punto lo utiliza para conectarse con el ISP. **CHAP**: Protocolo de confirmación de aceptación de la autenticación (CHAP) requiere que tanto el servidor como el cliente conozcan el texto simple de la clave para utilizar los servicios ISP. **MS-CHAP o MS-CHAPv2**: la versión de Microsoft de CHAP, utilizada para acceder a los servicios ISP.

PASO 5 Haga clic en **Guardar**.

Configuración de PPTP

Para configurar las opciones PPTP:

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **PPTP**.

PASO 3 Escriba esta información:

Dir. IP de Internet	Dirección IP del puerto WAN
Máscara de subred	Máscara de subred del puerto WAN
Puerta de enlace predet.	Dirección IP de la puerta de enlace predeterminada
Servidor PPTP	Dirección IP del servidor del protocolo de tunelización punto a punto
Nombre de usuario	El nombre de usuario asignado a usted por el ISP.
Contraseña	La contraseña asignada a usted por el ISP.

Conectar a petición	Seleccione esta opción si su ISP le cobra en función del tiempo que está conectado. Cuando selecciona esta opción, la conexión a Internet solo está activa si hay tráfico. Si no hay flujo de tráfico, la conexión está inactiva; es decir, está cerrada. Si hace clic en **Conectar a petición**, escriba los minutos que deben transcurrir para que se desactive la conexión en el campo **Tiempo máx. de inactividad**.
Mantener conexión	Cuando selecciona esta opción, la conexión a Internet está siempre activa. En el campo **Período de repetición de marcación**, escriba los segundos que deben transcurrir para que el dispositivo intente volver a conectarse una vez desconectado.
Tipo de autenticación	Seleccione el tipo de autenticación: **Negociación automática**: el servidor envía una solicitud de configuración que especifica el algoritmo de seguridad establecido. Luego, el dispositivo envía las credenciales de autenticación con el tipo de seguridad que envió anteriormente el servidor. **PAP**: el dispositivo usa el Protocolo de autenticación de contraseña (PAP) para realizar la conexión con el ISP. **CHAP**: el dispositivo usa el Protocolo de confirmación de aceptación de la autenticación (CHAP) al realizar la conexión con el ISP. **MS-CHAP o MS-CHAPv2**: el dispositivo usa el Protocolo de autenticación por desafío mutuo de Microsoft al realizar la conexión con el ISP.
Nombre del servicio	Introduzca el nombre del nuevo servicio PPTP.
Cifrado MPPE	Marque la casilla de verificación **Habilitar** para activar el Cifrado punto a punto de Microsoft para la conexión PPTP.

Origen de servidor DNS	La dirección del servidor DNS. Si su ISP ya le proporcionó direcciones de servidor DNS, seleccione **Usar estos servidores DNS** e ingrese las direcciones primaria y secundaria en los campos **DNS estático 1** y **DNS estático 2**. Para obtener direcciones de servidor DNS del ISP, seleccione **Obtener del ISP de forma dinámica**. Para usar los servidores DNS proporcionados por OpenDNS (208.67.222.222, 208.67.220.220) para resolver las direcciones web, seleccione **Usar OpenDNS**.

PASO 4 Haga clic en **Guardar**.

Configuración de L2TP

Para configurar las opciones L2TP:

PASO 1 Seleccione **Redes** > **WAN**.

PASO 2 En el menú desplegable **Tipo de conexión a Internet**, seleccione **L2TP**.

PASO 3 Escriba esta información:

Dir. IP de Internet	La dirección IP del puerto WAN
Máscara de subred	La máscara de subred del puerto WAN
Puerta de enlace predet.	La dirección IP de la puerta de enlace predeterminada
Servidor L2TP	La dirección IP del servidor L2TP
Versión	La versión de L2TP que desea usar. Si selecciona la versión 3, introduzca el Id. del proveedor y el Id. del circuito virtual.
Longitud de cookie	El tamaño de la cookie en el paquete de datos L2TP v3, que identifica la sesión L2TP.

Id. de proveedor	El Id. de proveedor incluido en el formato de codificación de AVP para L2TP. Para usar los valores del atributo adoptados por IETF en AVP, seleccione Estándar. Para implementar los valores del atributo privado y las extensiones L2TP de Cisco, seleccione Cisco.
Id. de circuito virtual	El identificador para el circuito de capa 2 a través del cual se envían los paquetes de datos L2TP. Esta información es obligatoria si selecciona Cisco como **Id. de proveedor** para L2TP v3.
Nombre de usuario	Escriba el nombre de usuario que le asignó su ISP.
Contraseña	Escriba la contraseña que le asignó su ISP.
Conectar a petición	Seleccione esta opción si su ISP le cobra en función del tiempo que está conectado. Cuando selecciona esta opción, la conexión a Internet solo está activa si hay tráfico. Si no hay flujo de tráfico, la conexión está inactiva; es decir, está cerrada. Si hace clic en **Conectar a petición**, escriba los minutos que deben transcurrir para que se desactive la conexión en el campo **Tiempo máx. de inactividad**.
Mantener conexión	Cuando selecciona esta opción, la conexión a Internet está siempre activa. En el campo Período de repetición de marcación, escriba los segundos que deben transcurrir para que el dispositivo intente volver a conectarse una vez desconectado.

Tipo de autenticación	**Negociación automática**: el servidor envía una solicitud de configuración que especifica el algoritmo de seguridad establecido. Luego, el dispositivo envía las credenciales de autenticación con el tipo de seguridad que envió el servidor. **PAP**: Protocolo de autenticación de contraseña (PAP); se utiliza para conectarse con el ISP. **CHAP**: Protocolo de confirmación de aceptación de la autenticación (CHAP); se utiliza para conectarse con el ISP. **MS-CHAP o MS-CHAPv2**: Protocolo de confirmación de aceptación de la autenticación de Microsoft (CHAP); se utiliza para conectarse con el ISP.
Nombre del servicio	Introduzca el nombre del nuevo servicio L2TP.
Cifrado MPPE	Marque la casilla de verificación **Habilitar** para activar el Cifrado punto a punto de Microsoft para la conexión L2TP.
Origen de servidor DNS	La dirección del servidor DNS. Si su ISP ya le proporcionó direcciones de servidor DNS, seleccione **Usar estos servidores DNS** e ingrese las direcciones primaria y secundaria en los campos **Servidor DNS primario** y **Servidor DNS secundario**. Para obtener direcciones de servidor DNS del ISP, seleccione **Obtener del ISP de forma dinámica**. Para usar los servidores DNS proporcionados por OpenDNS (208.67.222.222, 208.67.220.220) para resolver las direcciones web, seleccione **Usar OpenDNS**.

PASO 4 Haga clic en **Guardar**.

Configuración de parámetros de red opcionales

Para configurar los parámetros opcionales:

PASO 1 En la sección **Parámetros opcionales**, configure los siguientes parámetros:

MTU	La unidad de transmisión máxima (MTU) es el paquete más grande que puede enviarse a través de la red. A menos que su ISP exija algún cambio, le recomendamos que seleccione **Automática**. El tamaño predeterminado de MTU es de 1500 bytes. Si su ISP exige una configuración personalizada de MTU, seleccione **Manual** y escriba el tamaño de la MTU.
Tamaño	El tamaño personalizado de la MTU. El valor estándar de la MTU para las redes Ethernet en general es de 1500 bytes. Para las conexiones PPPoE, el valor es de 1492 bytes.
VLAN sin etiquetar	Marque la casilla para habilitar el etiquetado VLAN. Cuando esta opción está activada (de manera predeterminada), todo el tráfico se etiqueta con un ID de VLAN. De manera predeterminada, todo el tráfico del dispositivo usa VLAN1, la VLAN sin etiquetar predeterminada. Todo el tráfico está sin etiqueta hasta que deshabilita la VLAN sin etiquetar, cambia el Id. de VLAN de tráfico sin etiquetar o cambia el Id. de VLAN.

Id. de VLAN sin etiquetar	Un número que oscila entre 1 y 4094 para el Id. de VLAN sin etiquetar. El valor predeterminado es 1. El tráfico de la VLAN que se especifique en este campo no se etiquetará con un Id. de VLAN cuando se lo reenvíe a la red. VLAN 1 es la VLAN sin etiquetar predeterminada.
VLAN de administración AP	La VLAN asociada a la dirección IP que usa para acceder al dispositivo cuando se configura como punto de acceso. Si crea VLAN adicionales, por cuestiones de seguridad, elija un valor que corresponda con la VLAN configurada en otros switches de la red. Es posible que necesite cambiar la VLAN de administración para limitar el acceso al Administrador de dispositivos.

PASO 2 Haga clic en **Guardar**.

Configuración de una red móvil

Seleccione **Redes > WAN > Red móvil** para configurar el dispositivo que conectará a un módem USB de banda ancha móvil que esté conectado a su interfaz USB.

Configuración de parámetros globales de la red móvil

Para configurar los parámetros globales de los dispositivos USB compatibles:

PASO 1 Conecte el módem USB. Si el módem es compatible, se detectará automáticamente y aparecerá en la página Red móvil.

PASO 2 Seleccione modo de conexión **Automática** o **Manual**. La recuperación de conexión Ethernet solamente funciona si el modo de conexión se configura en automático.

- Para activar el módem y establecer una conexión automáticamente, seleccione modo **Automática**. Si selecciona Automático, configure una hora para **Conectar a petición** o seleccione **Mantener conexión**. La conexión a petición finaliza la conexión a Internet luego de que ha estado inactiva durante el período de tiempo especificado en el campo **Tiempo máx. de inactividad**.

Si la conexión actual a Internet finaliza debido a un período de inactividad, el módem volverá a establecer la conexión automáticamente cuando un usuario intente acceder a Internet. En el campo **Tiempo máx. de inactividad**, ingrese la cantidad de minutos de tiempo máximo que puede transcurrir antes de que finalice la conexión a Internet. Si elije la opción **Mantener conexión**, la conexión no finalizará en ningún momento.

- Para conectar o desconectar la conexión del módem manualmente, seleccione el modo **Manual**.

El dispositivo muestra el estado actual de la conexión del módem; incluye los estados de inicialización, conexión, desconexión o desconectado.

PASO 3 Verifique que el campo **Estado de tarjeta** le muestre que la tarjeta móvil está **Conectada**.

Configuración manual de los parámetros de la red móvil

Para cambiar los parámetros de la red móvil en el área **Configuración de la red móvil**, haga clic en el botón de radio **Manual**. El dispositivo detecta automáticamente los módems compatibles y proporciona una lista de los parámetros de configuración adecuados. Para anular los parámetros globales, seleccione **Manual**.

PASO 1 Ingrese información en los siguientes campos:

Campo	Descripción
Nombre del punto de acceso (APN)	Red de Internet a la cual se conectará el dispositivo móvil. Ingrese el nombre de punto de acceso provisto por el proveedor de servicio de red móvil. Si no lo sabe, comuníquese con el proveedor del servicio.
Número de discado	Número de discado provisto por el proveedor del servicio de red móvil para la conexión a Internet.
Nombre de usuario Contraseña	Nombre de usuario y contraseña provistos por el proveedor del servicio de red móvil.
Selección de SIM	Tarjeta SIM para habilitar o deshabilitar.
SIM PIN	Código de PIN asociado a la tarjeta SIM. Este campo se muestra solamente para las tarjetas SIM GMS. El PIN de la SIM puede modificarse tanto en el modo automático como en el manual.

Campo	Descripción
Nombre del servidor	Nombre del servidor para la conexión a Internet (en caso de que su proveedor de servicio se lo haya facilitado).
Autenticación	Autenticación que utiliza el proveedor del servicio. El valor puede modificarse seleccionando el tipo de autenticación en la lista desplegable. El modo predeterminado es Automática. Si no sabe qué tipo de autenticación usar, seleccione Automática.
Tipo de servicio	El tipo de servicio de conexión de datos móviles más común en función de la señal del área de servicio. Si la ubicación donde se encuentra admite únicamente servicio de datos móviles, puede limitar su opción preferida y reducir los tiempos configurados de conexión. La primera selección siempre busca el servicio HSPDA/3G/UMTS y cambia automáticamente a GPRS cuando está disponible.
Servicio LTE	Configuración del servicio de evolución a largo plazo (LTE). **Automático** selecciona una señal en base a la señal de servicio del área. **Solo 4G** únicamente busca señales 4G. **Solo 3G** únicamente busca señales 3G.

PASO 2 Haga clic en **Guardar** para guardar la configuración.

Configuración de la capacidad de banda ancha

El dispositivo controla la actividad de datos en la enlace de red móvil y cuando alcanza un umbral determinado, envía una notificación.

Para activar o desactivar el seguimiento de la capacidad de banda ancha y configurar los límites:

PASO 1 Haga clic en **Activado** o **Desactivado**.

PASO 2 Seleccione la Fecha mensual de renovación en la lista desplegable para indicar qué día del mes se reiniciará la capacidad de banda ancha.

PASO 3 El campo **Capacidad mensual de banda ancha**, ingrese una cantidad máxima de datos en megabytes que tenga permitido transmitir antes de que el dispositivo

realice una acción, como por ejemplo, enviar un correo electrónico a un administrador.

Config. de correo elec.

Cuando se alcanza el límite de datos, se puede enviar un mensaje de correo electrónico al administrador. Para configurar la dirección de correo electrónico del destinatario, consulte **Configuración del envío de registros por correo electrónico**.

Si selecciona la casilla para activar esta opción, se enviará un correo electrónico:

- Cuando el uso de la red móvil haya excedido cierto porcentaje.
- Cuando el dispositivo falle por la ruta de respaldo y se recupere.
- En cada intervalo especificado mientras enlace de red móvil esté activa.

Configuración de recuperación tras fallas

Si bien puede ser que tanto Ethernet como la enlace de red móvil estén disponibles, solo se puede usar una conexión a la vez para establecer un enlace WAN. Siempre que la conexión WAN falle, el dispositivo intentará establecer otra conexión en otra interfaz. Esta función se denomina Recuperación tras fallas. Cuando la conexión WAN primaria se restaura, esta revierte la ruta original y finaliza la conexión de respaldo. Esta función se denomina Recuperación.

PASO 1 Seleccione **Redes > WAN > Recuperación tras fallas y recuperación** para mostrar la ventana Recuperación tras fallas y recuperación.

PASO 2 Seleccione **Habilitar recuperación tras fallas para WAN 3G** para activar enlace de red móvil y establecer la recuperación desde el enlace Ethernet. Si el enlace Ethernet WAN no está activo, el dispositivo intenta habilitar enlace de red móvil en la interfaz USB. (Si la recuperación tras fallas no está activada, la enlace de red móvil siempre estará desactivada).

PASO 3 Seleccione **Habilitar recuperación de Ethernet WAN** para activar el enlace y regresar al enlace Ethernet, descartando así la enlace de red móvil. El modo de conexión de **WAN > Red móvil** debe estar configurado en automático para usar la recuperación de conexión WAN Ethernet.

PASO 4 En el campo **Intervalo de verificación de la recuperación tras fallas**, introduzca la frecuencia (en segundos) con la que el dispositivo intentará detectar la conexión física o la presencia de tráfico en la enlace de red móvil. Si el enlace está activo, el

dispositivo intentará hacer ping en un destino en este intervalo. Si no hay respuesta al paquete ping, el dispositivo supone que el enlace está inactivo y vuelve a intentar en la interfaz Ethernet WAN.

PASO 5 En el campo **Intervalo de verificación de la recuperación**, introduzca la frecuencia (en segundos) con la que el dispositivo intentará detectar la conexión física o la presencia de tráfico en el enlace Ethernet WAN. Si el enlace está activo, el dispositivo intentará hacer ping en un destino en el intervalo. Si hay respuesta al paquete ping, el dispositivo supone que el enlace está activo e intenta desactivar el enlace a la red móvil y activar el enlace a WAN Ethernet.

PASO 6 Haga clic en **Cambie a Ethernet inmediatamente cuando esta esté disponible** o en **Cambie a Ethernet en un rango de tiempo específico** e introduzca la hora de inicio y finalización para el rango.

PASO 7 En el campo **Sitio de validación de conexión**, seleccione el sitio desde el cual realizará la validación de la recuperación tras fallas. Use la siguiente puerta de enlace de salto (de forma predeterminada, el dispositivo hace ping a la puerta de enlace predeterminada), o seleccione un sitio personalizado e ingrese la dirección IPv4 o IPv6 del sitio.

PASO 8 Haga clic en **Guardar** para guardar la configuración.

La tabla de Interfaz WAN muestra el estado de WAN Ethernet y enlace de red móvil en Internet. Haga clic en el hipervínculo **Estado** para ver los detalles del puerto.

Configuración de opciones LAN

Las configuraciones DHCP y TCP/IP predeterminadas funcionan para la mayoría de las aplicaciones. Si desea que otra computadora de su red sea el servidor DHCP o si desea configurar manualmente las opciones de red de todos sus dispositivos, deshabilite el DHCP.

Además, en lugar de usar un servidor DNS, que asigna nombres de dominio de Internet (por ejemplo, www.cisco.com) a direcciones IP, puede usar un servidor de servicio de nombres de Internet de Windows (WINS). El servidor WINS es el servidor equivalente al servidor DNS, pero usa el protocolo NetBIOS para resolver los nombres de host. El dispositivo incluye la dirección IP del servidor WINS en la configuración DHCP que el dispositivo envía a los clientes de DHCP.

Si el dispositivo se conecta a un módem o a otro dispositivo que tiene una red configurada en la misma subred (192.168.1.x), el dispositivo modifica automáticamente la subred LAN a una subred aleatoria en función de 10.x.x.x, por lo que no hay un conflicto con la subred en la parte WAN del router.

Cambio de la dirección IP de administración de dispositivos

La dirección IP local de administración de dispositivos del dispositivo es estática y el valor predeterminado es 192.168.1.1.

Para modificar la dirección IP local de administración de dispositivos:

PASO 1 Seleccione **Redes** > **LAN** > **Configuración de LAN**.

PASO 2 En la sección **IPv4**, escriba esta información:

VLAN	El número de VLAN
Dirección IP local	Dirección IP local de LAN del dispositivo. Asegúrese de que otro dispositivo no esté usando la dirección IP.
Máscara de subred	Máscara de subred para la dirección IP local. La máscara de subred predeterminada es 255.255.255.0.

PASO 3 Haga clic en **Guardar**.

Una vez que modifique la dirección IP del dispositivo, su computadora ya no podrá mostrar el Administrador de dispositivos.

Para mostrar el Administrador de dispositivos, siga uno de los siguientes pasos:

- Si el DHCP está configurado en el dispositivo, libere y renueve la dirección IP de su computadora.
- Asigne manualmente una dirección IP a su computadora. La dirección debe estar en la misma subred que el dispositivo. Por ejemplo, si modifica la dirección IP del dispositivo a 10.0.0.1, asigne a su computadora una dirección IP en el rango de 10.0.0.2 a 10.0.0.255.

Abra una nueva ventana del explorador y escriba la nueva dirección IP del dispositivo para realizar nuevamente la conexión.

Configuración del servidor DHCP

Por opción predeterminada, el dispositivo funciona como servidor DHCP para los hosts en la LAN inalámbrica (WLAN) o la LAN alámbrica. Asigna direcciones IP y brinda direcciones de servidor DNS.

Con DHCP activado, el dispositivo asigna las direcciones IP a los otros dispositivos de red en la LAN de una agrupación de direcciones IPv4. El dispositivo prueba cada dirección antes de ser asignada para evitar direcciones duplicadas en la LAN.

La agrupación de direcciones IP predeterminadas abarca de 192.168.1.100 a 192.168.1.149. Para establecer una dirección IP estática en un dispositivo de red, utilice una dirección IP fuera de esta agrupación. Por ejemplo, si suponemos que el grupo DHCP tiene configurados los parámetros predeterminados, se pueden usar las direcciones IP estáticas de 192.168.1.2 a 192.168.1.99 en el grupo de direcciones IP para evitar conflictos con el grupo de direcciones IP de DHCP.

Para configurar las opciones DHCP:

PASO 1 Seleccione **Redes** > **LAN** > **Configuración de LAN**.

PASO 2 (Opcional) Seleccione una VLAN que desee editar en la lista desplegable.

PASO 3 En el campo **Servidor DHCP**, seleccione una de las siguientes opciones:

Habilitar	Permite que el dispositivo actúe como el servidor DHCP en la red.
Deshabilitar	Deshabilita DHCP en el dispositivo cuando usted desea configurar manualmente las direcciones IP de todos los dispositivos de red.
Retransmisión DHCP	Retransmite las direcciones IP asignadas por otro servidor DHCP a los dispositivos de red.

Si usted habilitó el servidor DHCP del dispositivo, ingrese esta información:

Dir. IP inicial	La primera dirección en la agrupación de direcciones IP. A cualquier cliente DHCP que se una a LAN se le asigna una dirección IP en este rango.

Cant. máx. de usuarios DHCP	La cantidad máxima de clientes DHCP
Rango de dir. IP	(Sólo lectura) El rango de direcciones IP disponibles para los clientes DHCP
Tiempo de concesión del cliente	Duración (en horas) que las direcciones IP se conceden a los clientes.
DNS estático 1	Dirección IP del servidor DNS primario
DNS estático 2	Dirección IP del servidor DNS secundario
DNS estático 3	Dirección IP del servidor DNS terciario
WINS	Dirección IP del servidor WINS primario

PASO 4 Si seleccionó **Retransmisión DHCP**, escriba la dirección de la puerta de enlace de retransmisión en el campo **Servidor DHCP remoto**. La puerta de enlace de retransmisión transmite mensajes DHCP al dispositivo de red, incluso a aquellos en otras subredes.

PASO 5 Haga clic en **Guardar**.

Configuración de VLAN

Una LAN virtual (VLAN) es un grupo de puntos finales en una red que se asocian según su función u otras características compartidas. A diferencia de las LAN que, en general, están basadas en zonas geográficas, las VLAN pueden agrupar puntos finales independientemente de la ubicación física del equipo o de los usuarios.

El dispositivo posee una VLAN predeterminada (VLAN 1) que no puede eliminarse. Puede crear hasta cuatro VLAN en el dispositivo.

Para crear una VLAN:

PASO 1 Seleccione **Redes** > **LAN** > **Afiliación a una VLAN**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 Introduzca la siguiente información:

ID de VLAN	ID numérica de VLAN para asignar los puntos finales en la afiliación VLAN. Debe escribir un número entre 3 y 4094. La ID de VLAN 1 está reservada para la VLAN predeterminada, que se usa para las tramas sin etiquetar recibidas en la interfaz.
Descripción	Descripción que identifica la VLAN
Puerto 1 **Puerto 2** **Puerto 3** **Puerto 4**	Puede asociar las VLAN del dispositivo a los puertos LAN del dispositivo. De forma predeterminada, todos los puertos VLAN pertenecen a VLAN1. Puede editar estos puertos para asociarlos a otras VLAN. Elija el tipo de trama saliente para cada puerto: **Sin etiquetar**: la interfaz es un miembro sin etiquetar de la VLAN. Las tramas de la VLAN se envían sin etiqueta a la VLAN del puerto. **Etiquetado**: el puerto es un miembro etiquetado de la VLAN. Las tramas de la VLAN se envían con etiqueta a la VLAN del puerto. **Excluido**: actualmente el puerto no es miembro de la VLAN. Esta es la opción predeterminada para todos los puertos cuando se crea la VLAN.

PASO 4 Haga clic en **Guardar**.

Para editar las configuraciones de una VLAN, seleccione la VLAN y haga clic en **Editar**. Para eliminar una VLAN seleccionada, haga clic en **Eliminar**. Haga clic en **Guardar** para aplicar los cambios.

Configuración de DHCP estático

Puede configurar el router para asignar una dirección IP específica a un dispositivo cliente con una dirección MAC específica.

Para configurar la DHCP estática:

PASO 1 Elija **Redes** > **LAN** > **DHCP estático**.

PASO 2 En el menú desplegable **VLAN**, seleccione un número de VLAN.

PASO 3 Haga clic en **Agregar fila**.

PASO 4 Introduzca la siguiente información:

Descripción	Descripción del cliente.
Dirección IP	La dirección IP que desea asignar al dispositivo cliente. La dirección IP asignada no debe pertenecer a la agrupación de direcciones DHCP. La asignación DHCP estática significa que el servidor DHCP asigna la misma dirección IP a una dirección MAC definida cada vez que el dispositivo cliente se conecta a la red. El servidor DHCP asigna la dirección IP reservada cuando el dispositivo cliente que usa la dirección MAC correspondiente solicita una dirección IP.
Dirección MAC	Dirección MAC del dispositivo cliente. El formato de una dirección MAC es XX:XX:XX:XX:XX:XX, donde X es un número de 0 a 9 (inclusive) o una letra entre la A y la F (inclusive).

Para editar las configuraciones de un cliente DHCP estático, seleccione el cliente y haga clic en **Editar**. Para eliminar un cliente DHCP seleccionado, haga clic en **Eliminar**. Haga clic en **Guardar** para aplicar los cambios.

Visualización de clientes DHCP alquilados

Puede ver una lista de puntos finales en la red (identificados por nombre de host, Dirección IP o Dirección MAC) y ver las direcciones IP que el servidor DHCP les asignó. También se muestra la VLAN de los puntos finales.

Para ver los clientes DHCP, elija **Redes** > **LAN** > **Cliente DHCP alquilado**.

Para cada VLAN definida en el dispositivo, una tabla muestra una lista de clientes asociados a la VLAN.

Para asignar una dirección IP estática a uno de los dispositivos conectados:

PASO 1 En la fila del dispositivo conectado, marque la casilla **Agregar al DHCP estático**.

PASO 2 Haga clic en **Guardar**.

El servidor DHCP del dispositivo siempre asignará la dirección IP que se muestra cuando el dispositivo solicita una dirección IP.

Configuración de un host DMZ

El dispositivo admite zonas desmilitarizadas (DMZ). La DMZ es una subred que está abierta al público pero que se encuentra detrás del firewall. La DMZ le permite redirigir los paquetes que se dirigen a su dirección IP del puerto WAN a una dirección IP determinada en su LAN.

Le recomendamos que use hosts que deban exponerse a la WAN (como servidores web o de correo electrónico) en la red DMZ. Puede configurar las reglas de firewall para permitir el acceso a servidores y puertos específicos en la DMZ desde la LAN o la WAN. En el caso de un ataque en cualquiera de los nodos DMZ, la LAN no necesariamente es vulnerable.

Debe configurar una dirección IP fija (estática) para el punto final que designe como host DMZ. Debe asignarle al host DMZ una dirección IP en la misma subred que la dirección IP LAN del dispositivo, pero no puede ser idéntica a la dirección IP otorgada a la interfaz LAN de esta puerta de enlace.

Para configurar la DMZ:

PASO 1 Seleccione **Redes** > **LAN** > **Host de DMZ**.

PASO 2 Marque **Habilitar** para habilitar la DMZ de la red.

PASO 3 En el menú desplegable **VLAN**, elija la Id. de la VLAN donde se habilita la DMZ.

PASO 4 En el campo **Dir. IP del host**, escriba la dirección IP del host DMZ. El host de DMZ es el punto final que recibe los paquetes redirigidos.

PASO 5 Haga clic en **Guardar**.

Configuración de RSTP

El Protocolo de árbol de expansión rápido (RSTP) es un protocolo de red que impide la presencia de bucles en la red y reconfigura de manera dinámica qué enlaces físicos deben enviar tramas. Para configurar el protocolo de árbol de expansión rápida (RTSP):

PASO 1 Seleccione **Redes** > **LAN** > **RSTP**.

PASO 2 Introduzca la siguiente información:

Prioridad del sistema	Seleccione la prioridad del sistema en el menú desplegable. Puede elegir de una prioridad de sistema de 0 a 61440 en incrementos de 4096. Los valores válidos son 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 y 61440. Cuanto más baja sea la prioridad del sistema, mayores serán las probabilidades de que el dispositivo sea la raíz en el árbol de expansión. El valor predeterminado es **327688**.
Tiempo de saludo	El tiempo de saludo es el período de tiempo que la raíz del árbol de expansión espera antes de enviar mensajes de saludo o hello. Escriba un número de 1 a 10. El número predeterminado es **2**.

Tiempo máximo	La tiempo máximo es el período de tiempo que el router espera para recibir un mensaje de saludo o hello. Si se alcanza el tiempo máximo, el router intenta modificar el árbol de expansión. Escriba un número de 6 a 40. El número predeterminado es **20**.
Retraso de reenvío	El retraso de reenvío es el intervalo después del cual una interfaz cambia de estado de bloqueo a estado de reenvío. Escriba un número de 4 a 30. El número predeterminado es **15**.
Forzar versión	Seleccione la versión de protocolo predeterminado que desea usar. Seleccione **Normal** (use RSTP) o **Compatible** (compatible con el STP anterior). El valor predeterminado es **Normal**.

PASO 3 En la **Tabla de config.**, configure los siguientes parámetros:

Protocolo habilitado	Marque la casilla para habilitar el RSTP en el puerto asociado. El protocolo RSTP está deshabilitado de manera predeterminada.
Borde	Marque esta casilla para especificar que el puerto asociado es un puerto de borde (estación final). Desmarque esta casilla para especificar que el puerto asociado es un enlace (puente) a otro dispositivo STP. El puerto de borde está habilitado de forma predeterminada.
Costo de ruta	Introduzca el costo de trayecto del RSTP para los puertos designados. Use 0 para el valor predeterminado (el dispositivo determina automáticamente el valor de la ruta). También puede ingresar un número del 2 al 200000000.

PASO 4 Haga clic en **Guardar**.

Administración de puertos

Puede configurar las opciones de velocidad y control de flujo de los cuatro puertos LAN del dispositivo.

Para configurar las velocidades del puerto y el control del flujo:

PASO 1 Elija **Redes** > **Administración de puertos**.

PASO 2 Configure esta información:

Puerto	El número del puerto.
Enlace	La velocidad del puerto. Si no hay un dispositivo conectado al puerto, este campo muestra **Inactivo**.
Modo	Seleccione en el menú desplegable una de las siguientes velocidades de puerto: • **Negociación automática**: el dispositivo y el dispositivo conectado seleccionan una velocidad común. • **Semi de 10 Mbps**: 10 Mbps en ambas direcciones, pero solo una dirección a la vez. • **Completo de 10 Mbps**: 10 Mbps en ambas direcciones de forma simultánea. • **Semi de 100 Mbps**: 100 Mbps en ambas direcciones, pero solo una dirección a la vez. • **Completo de 100 Mbps**: 100 Mbps en ambas direcciones de forma simultánea.
Trama jumbo	Marque para habilitar las tramas gigantes en el dispositivo y enviar tramas dentro de la LAN con 9000 bytes de datos por trama. Una trama Ethernet estándar contiene 1500 bytes de datos.

Control de flujo	Marque la casilla para habilitar el control de flujo para este puerto. El control de flujo es el proceso de administración de la velocidad de transmisión de datos entre dos nodos para evitar que un remitente rápido exceda la velocidad de un receptor lento. Ofrece un mecanismo para que el receptor controle la velocidad de transmisión, de manera que el nodo de recepción no se sature con datos del nodo de transmisión.

PASO 3 Haga clic en **Guardar**.

Configuración de la agregación de enlaces

Use la página Agregación de enlaces para agrupar varios enlaces Ethernet en un solo canal lógico. Los grupos de la agregación de enlaces aumentan la eficiencia del dispositivo al incrementar el ancho de banda acumulativo sin necesitar actualizaciones de hardware. Además facilita el reenrutamiento sencillo en caso de fallas en un solo puerto o cable.

Para asignar puertos al grupo de agregación de enlaces:

PASO 1 Seleccione **Redes > LAN > Agregación de enlaces**. La sección **Estado del puerto** muestra el modo asociado con cada puerto del dispositivo y el estado.

PASO 2 En la sección **Tabla de configuración de agregación de enlaces**, marque la casilla de verificación para cada puerto que desee incluir en el grupo.

PASO 3 Haga clic en **Guardar**.

Clonación de la dirección MAC

Algunas veces, quizá necesite configurar la dirección MAC del puerto WAN del dispositivo para que sea igual a la dirección MAC de su computadora o a otra dirección MAC. Esto se denomina clonación de dirección MAC.

Por ejemplo, algunos ISP registran la dirección MAC de la tarjeta de su computadora cuando se instala el servicio. Cuando coloca un router detrás del módem por cable o el módem DSL, el ISP no reconoce la dirección MAC del puerto WAN del dispositivo.

En este caso, para configurar su dispositivo de manera que el ISP lo reconozca, puede clonar la dirección MAC del puerto WAN para que sea igual a la dirección MAC de su equipo.

Para configurar el clon de una dirección MAC:

PASO 1 Seleccione **Redes** > **Clon de dir. MAC**.

PASO 2 En el campo **Clon de dir. MAC**, marque **Habilitar**.

PASO 3 Para configurar la dirección MAC del puerto WAN del dispositivo, seleccione una de las siguientes opciones:

- Para configurar la dirección MAC del puerto WAN de manera que sea igual a la dirección MAC de su computadora, haga clic en **Clonar MAC de Mi PC**.
- Para especificar una dirección MAC diferente, escríbala en el campo **Dirección MAC**.

PASO 4 Haga clic en **Guardar**.

Configuración de enrutamiento

Use la página Enrutamiento para configurar el modo operativo y otras opciones de enrutamiento para el dispositivo.

Configuración del modo operativo

Para configurar el modo operativo:

PASO 1 Seleccione **Redes** > **Enrutamiento**.

PASO 2 En el campo **Modo operativo**, seleccione una de las siguientes opciones:

Puerta de enlace	Para configurar el dispositivo de manera tal que funcione como puerta de enlace. (Recomendado) Mantenga esta configuración predeterminada si el dispositivo es el host de la conexión de su red a Internet y desempeña las funciones de enrutamiento.
Router	(Solo para usuarios avanzados) Para configurar el dispositivo de tal manera que funcione como router. Seleccione esta opción si el dispositivo se encuentra en una red con otros routers. Al habilitar el modo Router, se deshabilita la NAT (Traducción de direcciones de red) en el dispositivo.

PASO 3 Haga clic en **Guardar**.

Configuración de enrutamiento dinámico

El protocolo de información de enrutamiento (RIP) es un protocolo de puerta de enlace interior (IGP) que se usa con frecuencia en las redes internas. Le permite al router intercambiar su información de enrutamiento de forma automática con otros routers y le permite ajustar de forma dinámica sus tablas de enrutamiento y adaptarla a los cambios en la red.

El enrutamiento dinámico (RIP) permite que el dispositivo se adapte de forma automática a los cambios físicos en el diseño de la red e intercambiar las tablas de enrutamiento con otros routers.

El router determina la ruta de los paquetes de red en función de la menor cantidad de saltos entre el origen y el destino.

NOTA El protocolo RIP está deshabilitado de manera predeterminada en el dispositivo.

Para configurar el enrutamiento dinámico:

PASO 1 Seleccione **Redes** > **Enrutamiento**.

PASO 2 Configure los siguientes valores:

RIP	Marque la casilla **Habilitar** para habilitar RIP. Esto permite que el dispositivo use el RIP para dirigir el tráfico.
Versión de envío de paquetes por RIP	Seleccione la versión de envío de paquetes por RIP (**RIPv1** o **RIPv2**). La versión de RIP que se usa para enviar las actualizaciones a otros routers en la red depende de los parámetros de configuración de los otros routers. RIPv2 tiene compatibilidad descendente con RIPv1.
Versión de recepción de paquetes por RIP	Seleccione la versión de recepción de paquetes por RIP.

PASO 3 Haga clic en **Guardar**.

Configuración del enrutamiento entre VLAN

Para permitir que una estación final de una VLAN se comunique con una estación final de otra VLAN, marque la casilla de verificación **Habilitar enrutamiento entre VLAN**.

Configuración de enrutamiento estático

Puede configurar las rutas estáticas para dirigir los paquetes a la red de destino. Una ruta estática es el trayecto predeterminado que el paquete debe recorrer para alcanzar un host o red específicos.

Algunos ISP necesitan rutas estáticas para crear su tabla de enrutamiento en lugar de usar protocolos de enrutamiento dinámicos. Las rutas estáticas no necesitan recursos de CPU para intercambiar información de enrutamiento con un router de par.

También puede usar rutas estáticas para alcanzar routers de par que no admiten protocolos de enrutamiento dinámico. Las rutas estáticas se pueden usar junto con las rutas dinámicas. El dispositivo admite hasta 30 rutas estáticas.

Asegúrese de no introducir bucles de enrutamiento en su red.

Para configurar el enrutamiento estático:

PASO 1 Seleccione **Redes** > **Enrutamiento**.

PASO 2 En el menú desplegable **Entradas de ruta**, elija una entrada de ruta.

Para eliminar la entrada de ruta, haga clic en **Eliminar esta entrada**.

PASO 3 Configure los siguientes parámetros para la entrada de ruta seleccionada:

Escribir nombre de ruta	Escriba el nombre de la ruta.
IP de LAN de destino	Escriba la dirección IP de la LAN de destino.
Máscara de subred	Escriba la máscara de subred de la red de destino.
Puerta de enlace	Escriba la dirección IP de la puerta de enlace usada para esta ruta.
Interfaz	Seleccione la interfaz a la que se envían los paquetes para esta ruta: • **LAN e inalámbrica**: haga clic en este botón para dirigir los paquetes a la LAN y la red inalámbrica. • **Internet (WAN)**: haga clic en este botón para dirigir los paquetes a Internet (WAN).

PASO 4 Haga clic en **Guardar**.

Visualización de la tabla de enrutamiento

En la tabla de enrutamiento, hay información acerca de la topología de la red que lo rodea de forma directa.

Para ver la información de enrutamiento de su red, seleccione **Redes** > **Tabla de enrutamiento** y elija una de las siguientes opciones:

- **Mostrar tabla de enrutamiento IPv4**: la tabla de enrutamiento se muestra con los campos configurados en las páginas **Redes** > **Enrutamiento**.

- **Mostrar tabla de enrutamiento IPv6**: la tabla de enrutamiento se muestra con los campos configurados en la página **Redes** > **IPv6**.

Configuración de DNS dinámico

El DNS dinámico (DDNS) es un servicio de Internet que permite localizar los routers con diferentes direcciones IP a través de nombres de dominio de Internet. Para usar el DDNS, debe configurar una cuenta con un proveedor DDNS como DynDNS.com, TZO.com, 3322.org, o noip.com.

El router notifica a los servidores DNS dinámicos los cambios en la dirección IP WAN, de manera que se pueda obtener acceso a cualquier servicio público en su red a través del nombre de dominio.

Para configurar el DDNS, haga lo siguiente:

PASO 1 Seleccione **Redes** > **DNS dinámico**.

PASO 2 Elija el **Intervalo de actualización** en la lista desplegable.

PASO 3 En la sección **Tabla Servicio DDNS**, se detallan los servicios DDNS que puede habilitar en el dispositivo.

PASO 4 Marque la casilla de verificación correspondiente al servicio que desea habilitar y haga clic en **Editar**.

PASO 5 Marque la casilla de verificación **Habilitar** correspondiente al servicio.

PASO 6 Configure esta información:

Nombre de usuario/Dir. de correo electrónico	El nombre de usuario para la cuenta DDNS o la dirección de correo electrónico que usó para crear la cuenta DDNS.
Contraseña	Contraseña de la cuenta DDNS.
Nombre de host/dominio	El nombre de host del servidor DDNS o el nombre del dominio que se usó para acceder a la red.
Dir. IP de Internet	(Solo lectura) La dirección IP de Internet del dispositivo.

Estado	(Solo lectura) Indica si la actualización del DDNS se completó correctamente o si la información de la actualización de la cuenta enviada al servidor DDNS no llegó a destino.

PASO 7 Haga clic en **Probar la configuración** para probar la configuración de DDNS.

PASO 8 Haga clic en **Guardar**.

Configuración del modo IP

Las propiedades de configuración de red de área ancha son configurables para las redes IPv4 e IPv6. Puede escribir información acerca de su tipo de conexión a Internet y otros parámetros en estas páginas.

Para seleccionar un modo de IP:

PASO 1 Seleccione **Redes** > **Modo IP**.

PASO 2 En el menú desplegable **Modo IP**, seleccione una de las siguientes opciones:

LAN:IPv4, WAN:IPv4	Para usar IPv4 en los puertos LAN y WAN.
LAN:IPv6, WAN:IPv4	Para usar IPv6 en los puertos LAN e IPv4 en los puertos WAN.
LAN:IPv6, WAN:IPv6	Para usar IPv6 en los puertos LAN y WAN.
LAN:IPv4+IPv6, WAN:IPv4	Para usar IPv4 e IPv6 en los puertos LAN e IPv4 en los puertos WAN.
LAN:IPv4+IPV6, WAN:IPv4+IPv6	Para usar IPv4 e IPv6 en los puertos LAN y WAN.
LAN:IPv4, WAN:IPv6	Para usar IPv4 en los puertos LAN e IPv6 en los puertos WAN.

PASO 3 (Opcional) Si usa tunelización 6to4, que permite que los paquetes IPv6 se transmitan en una red IPv4, haga lo siguiente:

a. Haga clic en **Mostrar entrada estática DNS 6to4**.

b. En los campos **Dominio** e **IP**, escriba hasta cinco asignaciones de dominio a IP.

La función de tunelización 6to4 se usa habitualmente cuando un sitio o usuario final desea conectarse a IPv6 Internet a través de la red IPv4 existente.

PASO 4 Haga clic en **Guardar**.

Configuración IPv6

La versión 6 del protocolo de Internet (IPv6) es una versión del protocolo de Internet (IP) que tiene como objetivo reemplazar la versión 4 del protocolo de Internet (IPv4). La configuración de las propiedades WAN para una red IPv6 depende del tipo de conexión a Internet que tenga.

Configuración de conexiones IPv6 WAN

Puede configurar el dispositivo para que sea un cliente DHCPv6 del ISP para esta WAN o usar una dirección IPv6 estática provista por el ISP.

Para configurar las opciones IPv6 WAN en su dispositivo, primero debe configurar el modo IP a uno de los siguientes modos:

- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

Consulte **Configuración del modo IP** para obtener instrucciones sobre cómo configurar el modo IP.

Configuración de SLAAC

Para asignar automáticamente una dirección en base al prefijo IPv6, puede configurar el dispositivo para que use la Configuración automática de dirección sin estado (SLAAC) en la asignación de direcciones de cliente IPv6.

Para usar SLAAC:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 WAN**.

PASO 2 En el campo **Tipo de conexión WAN**, seleccione SLAAC. En el caso de DHCP sin estado, no es necesario tener disponible un servidor DHCPv6 en el ISP. En cambio, para la configuración automática se usa un mensaje de detección ICMPv6 que se origina en el dispositivo.

PASO 3 Haga clic en **Guardar**.

Configuración de DHCPv6

Si su ISP le suministra una dirección asignada dinámicamente, configure el dispositivo que desea usar como cliente DHCPv6.

Para configurar el dispositivo como cliente DHCPv6:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 WAN**.

PASO 2 En el campo **Tipo de conexión WAN**, seleccione **Config. automática - DHCPv6**. La puerta de enlace se conecta al servidor DHCPv6 del ISP para obtener una dirección arrendada.

PASO 3 Para automatizar la asignación de prefijos a su dispositivo (el cliente DHCP), seleccione el botón de radio **Habilitar delegación de prefijo**.

PASO 4 Haga clic en **Guardar**.

Configuración de una dirección IPv6 estática de WAN

Si su ISP le asigna una dirección fija para obtener acceso a WAN, configure el dispositivo para usar una dirección IPv6 estática.

Para configurar una dirección IPv6 WAN estática:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 WAN**.

PASO 2 En el campo **Tipo de conexión WAN**, seleccione **IPv6 estática**.

PASO 3 Escriba esta información:

Dirección IPv6	Dirección IPv6 del puerto WAN.
Longitud de prefijo IPv6	Longitud del prefijo IPv6 (generalmente definida por el ISP). La red IPv6 (subred) se identifica a través de los bits iniciales de la dirección denominados prefijo. Todos los hosts en la subred poseen un prefijo idéntico. Por ejemplo, en la dirección IPv6 `2001:0DB8:AC10:FE01::`, el prefijo es `2001`.
Puerta de enlace IPv6 predeterminada	Dirección IPv6 de la puerta de enlace predeterminada. Generalmente se trata de la dirección IP del servidor en el ISP.
DNS estático 1	Dirección IP del servidor IPv6 DNS primario.
DNS estático 2	Dirección IP del servidor IPv6 DNS secundario.

PASO 4 Haga clic en **Guardar**.

Configuración de opciones PPPoE IPv6

Puede ejecutar IPv4 PPPoE, IPv6 PPPoE, o ambos. Si ejecuta ambos, la configuración de su IPv6 WAN PPPoE debe coincidir con la configuración de su IPv4 WAN PPPoE. Si no coinciden, aparecerá un mensaje que le preguntará si desea establecer el protocolo IPv6 para que coincida con el protocolo IPv4. Consulte **Configuración de PPPoE**.

Para configurar las opciones PPPoE IPv6, siga estos pasos:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 WAN**.

PASO 2 En el campo **Tipo de conexión WAN**, seleccione **PPPoE IPv6**.

PASO 3 Escriba la siguiente información (quizá deba comunicarse con su ISP para obtener información de inicio de sesión de su PPPoE):

Nombre de usuario	El nombre de usuario asignado a usted por el ISP.
Contraseña	La contraseña asignada a usted por el ISP.

Conectar a petición	Si el ISP le cobra en función de la cantidad de tiempo que estuvo conectado, seleccione el botón de radio. Cuando lo seleccione, la conexión a Internet estará activa solamente cuando haya tráfico. Si no hay flujo de tráfico, la conexión está inactiva; es decir, está cerrada. En el campo **Tiempo máx. de inact.**, ingrese la cantidad de minutos que deben transcurrir sin que se detecte tráfico para que el enlace se torne inactivo.
Mantener conexión	Mantiene el enlace WAN activo, ya que envía un mensaje de conexión activa mediante el puerto. En el campo Período de repetición de marcación, escriba los segundos que deben transcurrir para que el dispositivo intente volver a conectarse una vez desconectado.
Tipo de autenticación	Tipos de autenticación: **Negociación automática**: el servidor envía una solicitud de configuración que especifica el algoritmo de seguridad establecido en el servidor. El dispositivo responde con sus credenciales de autenticación, incluido el tipo de seguridad enviado por el servidor. **PAP**: usa el Protocolo de autenticación de contraseña (PAP) para realizar la conexión con el ISP. **CHAP**: usa el Protocolo de confirmación de aceptación de la autenticación (CHAP) para conectarse al ISP. **MS-CHAP o MS-CHAPv2**: usa el Protocolo de confirmación de aceptación de la autenticación de Microsoft (CHAP) para conectarse con el ISP.
Nombre del servicio	Nombre que puede necesitar el ISP para iniciar sesión en el servidor PPPoE.

MTU	La unidad de transmisión máxima es el paquete más grande que puede enviarse a través de la red. A menos que su ISP exija algún cambio, le recomendamos que seleccione **Automática**. El valor estándar de la MTU para las redes Ethernet es de 1500 bytes. Para las conexiones PPPoE, el valor es de 1492 bytes. Si su ISP requiere una configuración personalizada para la MTU, escoja **Manual**.
Tamaño	Tamaño de MTU. Si su ISP exige una configuración personalizada de MTU, ingrese el tamaño de la MTU.
Modo de dirección	Modo de dirección dinámico o estático. Si selecciona estático, introduzca la dirección IPv6 en el campo que se encuentra a continuación.
Longitud de prefijo IPv6	Longitud del prefijo IPv6.
Puerta de enlace IPv6 predeterminada	Dirección IP de la puerta de enlace IPv6 predeterminada.
DNS estático 1	Dirección IP del servidor DNS primario.
DNS estático 2	Dirección IP del servidor DNS secundario.

PASO 4 Haga clic en **Guardar**.

Configuración de conexiones IPv6 LAN

En el modo IPv6, el servidor LAN DHCP se habilita de forma predeterminada (similar al modo IPv4). El servidor DHCPv6 asigna direcciones IPv6 de las agrupaciones de direcciones configuradas que usan la longitud de prefijo IPv6 asignada a la LAN.

Para configurar las opciones IPv6 LAN en su dispositivo, primero debe configurar el modo IP a uno de los siguientes modos:

- LAN:IPv6, WAN:IPv4
- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

Consulte **Configuración del modo IP** para obtener más información sobre cómo configurar el modo IP.

Para configurar las opciones IPv6 LAN:

PASO 1 Elija **Redes** > **IPv6** > **Configuración IPv6 LAN**.

PASO 2 Escriba la siguiente información para configurar la dirección IPv6 LAN:

Dirección IPv6	Escriba la dirección IPv6 del dispositivo. La dirección IPv6 predeterminada para la puerta de enlace es fec0::1 (o FEC0:0000:0000:0000:0000:0000:0000:0001). Puede cambiar esta dirección IPv6 de 128 bits según los requisitos de la red.
Longitud de prefijo IPv6	Escriba la longitud de prefijo IPv6. La red IPv6 (subred) se identifica a través de los bits iniciales de la dirección denominados prefijo. De forma predeterminada, el prefijo tiene una longitud de 64 bits. Todos los hosts de la red tienen bits iniciales idénticos para su dirección IPv6; en este campo se establece la cantidad de bits iniciales comunes a las direcciones de red.

PASO 3 Haga clic en **Guardar** o continúe con la configuración de los valores de LAN DHCP IPv6.

PASO 4 Escriba la siguiente información para configurar la dirección DHCPv6:

Estado DHCP	Marque la casilla para habilitar el servidor DHCPv6. Cuando se habilita, el dispositivo asigna una dirección IP dentro del rango especificado y brinda información adicional a cualquier punto final LAN que solicite las direcciones DHCP.
Nombre de dominio	(Opcional) Nombre de dominio del servidor DHCPv6.

Preferencia de servidor	Nivel de preferencia del servidor en este servidor DHCP. Los mensajes de anuncios con el valor de preferencia de servidor más alto a un host LAN se prefieren a otros mensajes de anuncios de servidor DHCP. El valor predeterminado es 255.
DNS estático 1	Dirección IPv6 del servidor DNS primario en la red IPv6 del ISP.
DNS estático 2	Dirección IPv6 del servidor DNS secundario en la red IPv6 del ISP.
Tiempo de concesión del cliente	Duración del tiempo de concesión al cliente (en segundos) durante el cual las direcciones IPv6 se conceden a los puntos finales de la LAN.

PASO 5 Elija **Redes** > **IPv6** > **Configuración IPv6 LAN**.

PASO 6 En la **Tabla de agrupación de dir. IPv6**, haga clic en **Agregar fila**.

PASO 7 Escriba esta información:

Dirección inicial	Dirección IPv6 inicial de la agrupación.
Dirección final	Dirección IPv6 final de la agrupación.
Longitud de prefijo IPv6	Longitud del prefijo que determina la cantidad de bits iniciales comunes en las direcciones de la red.

PASO 8 Haga clic en **Guardar**.

Para editar las configuraciones de una agrupación, seleccione la agrupación y haga clic en **Editar**. Para eliminar una agrupación seleccionada, haga clic en **Eliminar**. Haga clic en **Guardar** para aplicar los cambios.

Configuración de enrutamiento estático IPv6

Puede configurar las rutas estáticas para dirigir los paquetes a la red de destino. Una ruta estática es el trayecto predeterminado que el paquete debe recorrer para alcanzar un host o red específicos.

Algunos ISP necesitan rutas estáticas para crear su tabla de enrutamiento en lugar de usar protocolos de enrutamiento dinámicos. Las rutas estáticas no necesitan recursos de CPU para intercambiar información de enrutamiento con un router de par.

También puede usar rutas estáticas para alcanzar routers de par que no admiten protocolos de enrutamiento dinámico. Las rutas estáticas se pueden usar junto con las rutas dinámicas. Asegúrese de no introducir bucles de enrutamiento en su red.

Para crear una ruta estática:

PASO 1 Seleccione **Redes** > **IPv6** > **Enrutamiento estático IPv6**.

PASO 2 En la lista de rutas estáticas, haga clic en **Agregar fila**.

PASO 3 Escriba esta información:

Nombre	Nombre de la ruta.
Destino	Dirección IPv6 del host o la red de destino para esta ruta.
Longitud del prefijo	Cantidad de bits del prefijo en la dirección IPv6 que define la subred de destino.
Puerta de enlace	Dirección IPv6 de la puerta de enlace a través de la cual puede alcanzarse el host o la red de destino.
Interfaz	Interfaz para la ruta: **LAN**, **WAN** o **6to4**.
Métrico	Prioridad de la ruta. Escoja un valor entre 2 y 15. Si existen diversas rutas para el mismo destino, se utilizará la ruta con la métrica más baja.
Activo	Marque la casilla para activar la ruta. Cuando agrega una ruta en el estado inactivo, se incluye en la lista de enrutamiento, pero el dispositivo no la utiliza. La incorporación de una ruta inactiva sirve si la ruta no está disponible cuando usted la incorpora. Cuando la red esté disponible, podrá habilitarla.

PASO 4 Haga clic en **Guardar**.

Para editar las configuraciones de una ruta, seleccione la ruta y haga clic en **Editar**. Para eliminar una ruta seleccionada, haga clic en **Eliminar**. Haga clic en **Guardar** para aplicar los cambios.

Configuración de enrutamiento (RIPng)

RIP Nueva generación (RIPng) es un protocolo de enrutamiento basado en el algoritmo de vector de distancia (D-V). RIPng usa los paquetes UDP para intercambiar la información de enrutamiento a través del puerto 521.

RIPng usa un conteo de saltos para medir la distancia a un destino. El conteo de saltos se denomina métrica o costo. El conteo de saltos de un router a una red conectada directamente es 0. El conteo de saltos entre dos routers conectados directamente es 1. Cuando el conteo de saltos es superior o igual a 16, la red o el host de destino no puede alcanzarse.

De forma predeterminada, la actualización del enrutamiento se envía cada 30 segundos. Si el router no recibe actualizaciones de un vecino después de 180 segundos, las rutas adquiridas del vecino se consideran inalcanzables. Después de otros 240 segundos, si no se recibe actualización de enrutamiento, el router elimina estas rutas de la tabla de enrutamiento.

En el dispositivo, el RIPng está deshabilitado de forma predeterminada.

Para configurar el RIPng:

PASO 1 Seleccione **Redes** > **IPv6** > **Enrutamiento (RIPng)**.

PASO 2 Haga clic en **Habilitar**.

PASO 3 Haga clic en **Guardar**.

Configuración de la tunelización

La tunelización IPv6 a IPv4 (tunelización 6to4) permite que los paquetes IPv6 sean transmitidos a través de una red IPv4. La tunelización IPv4 a IPv6 (tunelización 4to6) permite que los paquetes IPv4 sean transmitidos a través de una red IPv6.

Tunelización 6to4

6La tunelización -to-4 se usa habitualmente cuando un sitio o usuario final desea conectarse a Internet IPv6 a través de la red IPv4 existente.

Pasos para configurar la tunelización 6-to-4:

PASO 1 Seleccione **Redes** > **IPv6** > **Tunelización**.

PASO 2 En el campo **Tunelización 6to4**, marque **Habilitar**.

PASO 3 Escoja el tipo de tunelización:

- **6to4**
- **6RD** (Implementación rápida)
- **ISATAP** (Protocolo de direccionamiento automático de túnel dentro de un sitio) - Escoja **Automático** o **Manual**.

PASO 4 Para la tunelización 6RD, seleccione **Automática** o **Manual**. Si seleccionó **Manual**, escriba la siguiente información:

- **Prefijo IPv6**
- **Longitud de prefijo IPv6**
- **Retransmisión de borde**
- **Longitud de la máscara IPv4**

PASO 5 Para la tunelización ISATAP, seleccione **Automática** o **Manual**. Si seleccionó **Manual**, escriba la siguiente información:

- **Prefijo IPv6**
- **Longitud de prefijo IPv6**

PASO 6 Haga clic en **Guardar**.

Tunelización 4to6

Pasos para configurar la tunelización 4to6:

PASO 1 Seleccione **Redes** > **IPv6** > **Tunelización**.

PASO 2 En el campo **Tunelización 4 to 6**, marque **Habilitar**.

PASO 3 Escriba la dirección IPv6 local del puerto WAN en el dispositivo.

PASO 4 Escriba la dirección IPv6 remota o la dirección IP del punto final remoto.

PASO 5 Haga clic en **Guardar**.

Visualización del estado de túnel IPv6

Para ver el estado de túnel IPv6, haga lo siguiente:

PASO 1 Seleccione **Redes** > **IPv6** > **Estado de túneles IPv6**.

PASO 2 Haga clic en **Actualizar** para visualizar la información más actualizada.

Esta página muestra información acerca de la configuración automática del túnel a través de la interfaz WAN dedicada. La tabla muestra el nombre del túnel y la dirección IPv6 que se crea en el dispositivo.

Configuración de aviso de router

El Daemon de anuncio del router (RADVD) en el dispositivo escucha las solicitudes de router en la LAN IPv6 y responde con avisos de router, según corresponda. Esta es la configuración automática IPv6 sin estado y el dispositivo distribuye los prefijos IPv6 a todos los nodos en la red.

Para configurar el RADVD:

PASO 1 Seleccione **Redes** > **IPv6** > **Aviso de router**.

PASO 2 Escriba esta información:

Estado de RADVD	Marque la casilla **Habilitar** para habilitar el RADVD.
Modo de anuncios	Seleccione uno de los siguientes modos: **Multidifusión no solicitada**: envíe los avisos de router (RA) a todas las interfaces que pertenecen al grupo de multidifusión. **Solo unidifusión**: restrinja los avisos a las direcciones IPv6 conocidas solamente (las RA se envían a la interfaz que pertenece a la dirección conocida solamente).

Intervalo de anuncios	Intervalo de anuncios (4-1800) para la **Multidifusión no solicitada**. El valor predeterminado es 30. El intervalo de anuncios es un valor aleatorio entre el intervalo de aviso de router mínimo (MinRtrAdvInterval) y el intervalo de aviso de router máximo (MaxRtrAdvInterval). MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval
Indicadores RA	Marque la casilla **Administrado** para usar el protocolo con estado/administrado para la configuración automática de la dirección. Marque la casilla **Otro** para usar el protocolo con estado/administrado para la configuración de la información no relacionada con la dirección.
Preferencia del router	Seleccione **baja**, **media** o **alta** en el menú desplegable. El valor predeterminado es medio. La preferencia del router ofrece una métrica de preferencia para los routers predeterminados. Los valores bajos, medios y altos están señalizados en los bits sin usar en los mensajes RA. Esta extensión tiene compatibilidad descendente para los routers (al configurar el valor de preferencia del router) y los hosts (al interpretar el valor de preferencia del router). Estos valores son ignorados por los hosts que no implementan la preferencia del router. Esta característica es útil si hay otros dispositivos habilitados por RADVD en LAN.
MTU	Tamaño de MTU (0 o 1280 a 1500). El valor predeterminado es 1500 bytes. La unidad de transmisión máxima (MTU) es el paquete más grande que puede enviarse a través de la red. La MTU se usa en las RA para garantizar que todos los nodos de la red usen el mismo valor de MTU cuando la MTU de la LAN no se conoce.
Tiempo de vida del router	Valor de tiempo de vida del router, o el tiempo en segundos que los mensajes de anuncios existen en la ruta. El valor predeterminado es 3600 segundos.

PASO 3 Haga clic en **Guardar**.

Configuración de los prefijos de anuncios

Para configurar los prefijos disponibles de RADVD:

PASO 1 Seleccione **Redes** > **IPv6** > **Prefijos de anuncios**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 Escriba esta información:

Tipo de prefijo IPv6	Seleccione uno de los siguientes tipos: **6to4**: admite la transmisión de paquetes IPv6 por una red IPv4. Se usa cuando un usuario final desea conectarse a Internet IPv6 con su conexión IPv4 existente. **Global/Local**: una dirección IPv6 localmente única que puede usar en las redes privadas IPv6 o una dirección de Internet IPv6 globalmente única.
ID de SLA	Si elige **6to4** como el tipo de prefijo IPv6, escriba el identificador de agrupación según el sitio (SLA ID). La SLA ID en el prefijo de la dirección 6to4 se determina en la ID de interfaz en la que se envían los anuncios.
Prefijo IPv6	Si elige **Global/Local** como el tipo de prefijo IPv6, escriba el prefijo IPv6. El prefijo IPv6 especifica la dirección de red IPv6.
Longitud de prefijo IPv6	Si elige **Global/Local** como el tipo de prefijo IPv6, escriba la longitud de prefijo. La variable de longitud de prefijo es un valor decimal que indica la cantidad de bits contiguos de orden superior de la dirección que conforma la parte de la red de la dirección.
Tiempo de vida del prefijo	Tiempo de vida del prefijo, o el tiempo total que el router que solicita autenticación puede usar el prefijo.

PASO 4 Haga clic en **Guardar**.

4

Configuración de redes inalámbricas

Seguridad inalámbrica

Las redes inalámbricas son prácticas y fáciles de instalar. Debido a que la red inalámbrica opera mediante el envío de información a través de ondas de radio, puede ser más vulnerable a intrusos que una red alámbrica tradicional.

Consejos para la seguridad inalámbrica

No puede evitar físicamente que alguien se conecte a la red inalámbrica, pero puede tomar las siguientes medidas para mantener la red segura:

- Cambie el nombre de la red inalámbrica predeterminado o el SSID.

  Los dispositivos inalámbricos tienen un nombre de red inalámbrica o un SSID predeterminados. Este es el nombre de la red inalámbrica y puede tener hasta 32 caracteres de longitud.

  Para proteger la red, cambie el nombre de la red inalámbrica predeterminado a un nombre único para distinguir la red inalámbrica de otras redes inalámbricas que puedan existir alrededor suyo.

  Cuando elija los nombres, no utilice información personal porque cualquier persona puede verla cuando está buscando redes inalámbricas.

- Cambie la contraseña predeterminada.

  Cuando desea cambiar la configuración de los productos inalámbricos, como puntos de acceso, routers y puertas de enlace, se le pide una contraseña. Estos dispositivos tienen una contraseña predeterminada. La contraseña predeterminada generalmente es **cisco**.

  Los hackers conocen estos valores predeterminados y es posible que intenten usarlos para acceder al dispositivo inalámbrico y cambiar las configuraciones de la red. Para impedir el acceso no autorizado, personalice la contraseña del dispositivo, de modo que sea difícil de adivinar.

- Habilite el filtrado de direcciones MAC.

  Las puertas de enlace y los routers Cisco le permiten habilitar el filtrado de direcciones MAC. La dirección MAC es una serie única de números y letras asignada a cada dispositivo de redes.

  Con el filtrado de direcciones MAC habilitado, el acceso a la red inalámbrica se proporciona únicamente para los dispositivos inalámbricos con direcciones MAC específicas. Por ejemplo, puede especificar la dirección MAC de cada computadora en la red, de modo que solo esas computadoras puedan acceder a la red inalámbrica.

- Habilite el cifrado.

  El cifrado protege los datos transmitidos por una red inalámbrica. El acceso Wi-Fi protegido (WPA/WPA2) y el protocolo de equivalencia de cableado (WEP) ofrecen distintos niveles de seguridad para la comunicación inalámbrica. Actualmente, se requiere que los dispositivos que poseen certificado Wi-Fi admitan WPA2, pero no se requiere que admitan WEP.

  Una red cifrada con WPA/WPA2 es más segura que una red cifrada con WEP, ya que WPA/WPA2 usa el cifrado de clave dinámica.

  Para proteger la información cuando se transmite a través de las ondas de transmisión, habilite el nivel más alto de cifrado que admite el equipo de la red.

  WEP es un cifrado estándar más antiguo y es posible que sea la única opción disponible en algunos dispositivos más antiguos que no admiten WPA.

- Mantenga los routers, los puntos de acceso o las puertas de enlace inalámbricos lejos de paredes exteriores y ventanas.
- Apague los routers, los puntos de acceso o las puertas de enlace inalámbricos cuando no estén en uso (a la noche, durante las vacaciones).
- Utilice frases clave sólidas que tengan, por lo menos, ocho caracteres de longitud. Combine letras y números para evitar utilizar palabras clásicas que pueden encontrarse en el diccionario.

Pautas generales para la seguridad de la red

La seguridad de la red inalámbrica no tiene utilidad si la red subyacente no está segura. Recomendamos que tome las siguientes precauciones:

- Proteja todas las computadoras de la red con contraseñas y, de forma individual, proteja con contraseña los archivos confidenciales.
- Cambie las contraseñas regularmente.

- Instale un software antivirus y un software de firewall personal.
- Deshabilite el uso compartido de archivos (entre entidades pares) para evitar que las aplicaciones utilicen el uso compartido de archivos sin su consentimiento.

Redes inalámbricas en el dispositivo

El dispositivo proporciona cuatro redes inalámbricas virtuales o cuatro SSID (identificador de conjunto de servicios): ciscosb1, ciscosb2, ciscosb3 y ciscosb4. Estos son los nombres o los SSID predeterminados de estas redes, pero puede cambiarlos a nombres más significativos. En esta tabla, se describen las configuraciones predeterminadas de estas redes:

Nombre de SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Habilitado	Sí	No	No	No
Difusión de SSID	Habilitado	Deshabilitado	Deshabilitado	Deshabilitado
Modo de seguridad	Deshabilitado[1]	Deshabilitado	Deshabilitado	Deshabilitado
Filtro MAC	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado
VLAN	1	1	1	1
Aislamiento inalámbrico con SSID	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado
WMM	Habilitado	Habilitado	Habilitado	Habilitado
Botón de hardware WPS	Habilitado	Deshabilitado	Deshabilitado	Deshabilitado

1. Cuando use el Asistente de instalación, seleccione Seguridad óptima o Seguridad mejorada para proteger el dispositivo del acceso no autorizado.

Configuración de las opciones inalámbricas básicas

Escoja **Inalámbrica** > **Configuración básica** para configurar las opciones inalámbricas básicas.

Para configurar las opciones inalámbricas básicas:

PASO 1 Elija **Inalámbrica** > **Configuración básica**.

PASO 2 En el campo **Radio**, marque la casilla **Habilitar** para encender la radio inalámbrica. De forma predeterminada, hay una sola red inalámbrica habilitada, **ciscosb1**.

PASO 3 En el campo **Modo de red inalámbrica**, elija una de estas opciones en el menú desplegable:

B/G/N-Combinado	Si tiene dispositivos inalámbricos N, B y G en la red. Este es el valor predeterminado (recomendado).
Solo B	Elija esta opción si tiene solo dispositivos inalámbricos B en la red.
Solo G	Elija esta opción si tiene solo dispositivos inalámbricos G en la red.
Solo N	Elija esta opción si tiene solo dispositivos inalámbricos N en la red.
B/G-Combinado	Elija esta opción si tiene dispositivos inalámbricos B y G en la red.
G/N-Combinado	Elija esta opción si tiene dispositivos inalámbricos G y N en la red.

PASO 4 Si elige **B/G/N-combinado**, **Solo N** o **G/N-combinado**, en el campo **Selección de banda inalámbrica**, seleccione el ancho de banda inalámbrica de la red (**20 MHz** o **20/40 MHz**). Si elige Solo N, debe usar seguridad WPA2 en la red. Consulte **Configuración del modo de seguridad**.

PASO 5 En el campo **Canal inalámbrico**, elija el canal inalámbrico en el menú desplegable.

PASO 6 En el campo **VLAN de administración AP**, elija **VLAN 1** si utiliza los valores predeterminados.

Si crea VLAN adicionales, elija un valor que corresponda con la VLAN configurada en otros switches de la red. Esto se realiza para propósitos de seguridad. Es posible que necesite cambiar la VLAN de administración para limitar el acceso al Administrador de dispositivos.

PASO 7 (Opcional) En el campo **U-APSD (ahorro de energía WMM)**, active la casilla **Habilitar** para habilitar la función de ahorro de energía automático no programado (U-APSD), también conocida como ahorro de energía WMM, que le permite a la radio conservar energía.

U-APSD es un esquema de ahorro de energía optimizado para aplicaciones en tiempo real, como VoIP y que transfieren datos de dúplex completo a través de WLAN. Al clasificar el tráfico IP saliente como datos de voz, estos tipos de aplicación pueden aumentar la vida útil de la batería en un 25% aproximadamente y minimizar los retrasos de transmisión.

PASO 8 (Opcional) Configure las opciones de las cuatro redes inalámbricas (consulte **Edición de las opciones de las redes inalámbricas**).

PASO 9 Haga clic en **Guardar**.

Edición de las opciones de las redes inalámbricas

La **Tabla inalámbrica** en la página **Configuración básica** numera las opciones de las cuatro redes inalámbricas que admite el dispositivo.

Para configurar las opciones de las redes inalámbricas:

PASO 1 Active la casilla de las redes que desea configurar.

PASO 2 Haga clic en **Editar**.

PASO 3 Configure los siguientes valores:

Habilitar SSID	Haga clic en **Encendido** para habilitar la red.
Nombre de SSID	Escriba el nombre de la red.
Difusión de SSID	Active esta casilla para habilitar la difusión de SSID. Si la difusión SSID está habilitada, el router inalámbrico anuncia su disponibilidad a los dispositivos inalámbricos que se encuentran en el rango del router.

Modo de seguridad	Consulte **Configuración del modo de seguridad**.
Filtro MAC	Consulte **Configuración del filtrado MAC**.
VLAN	Elija la VLAN asociada con la red.
Aislamiento inalámbrico con SSID	Active esta casilla para habilitar el aislamiento inalámbrico en la SSID.
WMM (Wi-Fi Multimedia)	Active esta casilla para habilitar WMM.
Máx. de clientes asociados	La cantidad máxima de clientes que pueden conectarse a la red inalámbrica seleccionada. Introduzca un número del 1 al 64.
WPS	Active esta casilla para asignar a la red el botón WPS del dispositivo que se encuentra en el panel frontal.
Perfil del portal	Consulte **Configuración de un portal cautivo**.

PASO 4 Haga clic en **Guardar**.

Configuración del modo de seguridad

Puede configurar uno de los siguientes modos de seguridad para las redes inalámbricas:

-

Configuración de WEP

El modo de seguridad WEP ofrece una seguridad débil con un método de cifrado básico que no es tan seguro como WPA. Es posible que se deba utilizar WEP en caso de que sus dispositivos de red no admitan WPA.

NOTA Si no debe utilizar WEP, le recomendamos que utilice WPA2. Si está usando el modo Solo N inalámbrico, debe usar WPA2.

Para configurar el modo de seguridad WEP:

PASO 1 Elija **Inalámbrica** > **Configuración básica**. En la **Tabla inalámbrica**, active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Editar modo de seguridad**. Aparece la página **Configuración de seguridad**.

PASO 3 En el campo **Seleccionar SSID**, elija la SSID para la que se deben configurar las opciones de seguridad.

PASO 4 En el menú **Modo de seguridad**, elija **WEP**.

PASO 5 En el campo **Tipo de autenticación**, elija una de las siguientes opciones:

- **Sistema abierto**: esta es la opción predeterminada.
- **Clave compartida**: seleccione esta opción si el administrador de la red recomienda esta configuración. Si no está seguro, seleccione la opción predeterminada.

En ambos casos, el cliente inalámbrico debe proporcionar la clave compartida correcta (contraseña) para acceder a la red inalámbrica.

PASO 6 En el campo **Cifrado**, elija el tipo de cifrado:

- **10/64 bits (10 dígitos hexadecimales):** proporciona una clave de 40 bits.
- **26/128 bits (26 dígitos hexadecimales)**: proporciona una clave de 104 bits, que ofrece un cifrado más sólido, de modo que se genera una clave más difícil de descifrar. Recomendamos un cifrado de 128 bits.

PASO 7 (Opcional) En el campo **Frase clave**, escriba una clave alfanumérica (que tenga más de ocho caracteres para lograr una seguridad óptima) y haga clic en **Generar clave** para generar cuatro únicas claves WEP en los campos de **claves WEP**.

Si desea proporcionar su propia clave, ingrésela directamente en el campo **Clave 1** (recomendado). La longitud de la clave debe ser de 5 caracteres ASCII (o 10 caracteres hexadecimales) para una clave WEP de 64 bits y de 13 caracteres ASCII (o 26 caracteres hexadecimales) para una clave WEP de 128 bits. Los caracteres hexadecimales válidos son de 0 a 9 y de A a F.

PASO 8 En el campo **Clave TX**, elija qué clave utilizar como la clave compartida que deben utilizar los dispositivos para acceder a la red inalámbrica.

PASO 9 Haga clic en **Guardar** para guardar la configuración.

PASO 10 Haga clic en **Atrás** para volver a la página **Configuración básica**.

Configuración de WPA-Personal, WPA2-Personal y WPA2-Personal combinado

Los modos de seguridad de WPA Personal, WPA2 Personal y WPA2 Personal combinado ofrecen una seguridad fuerte para reemplazar a WEP.

- **WPA-Personal**: WPA es parte del estándar de seguridad inalámbrica (802.11i) estandarizada mediante Wi-Fi Alliance; estaba destinada como una medida intermedia para tomar el lugar de WEP mientras se preparaba el estándar 802.11i. WPA-Personal admite el protocolo de integridad de clave temporal (TKIP) y el cifrado del estándar de cifrado avanzado (AES).
- **WPA2-Personal**: (recomendado) WPA2 es la implementación del estándar de seguridad especificado en el estándar 802.11i final. WPA2 admite el cifrado AES y esta opción utiliza la clave precompartida (PSK) para la autenticación.
- **WPA2-Personal combinado**: le permite utilizar los clientes WPA y WPA2 para conectarlos simultáneamente mediante la autenticación de PSK.

La autenticación personal es la PSK, una frase clave alfanumérica compartida con un par inalámbrico.

Para configurar el modo de seguridad de WPA Personal:

PASO 1 En la **Tabla inalámbrica** (**Inalámbrica** > **Configuración básica**), active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Editar modo de seguridad**. Aparece la página **Configuración de seguridad**.

PASO 3 En el campo **Seleccionar SSID**, elija la SSID para la que se deben configurar las opciones de seguridad.

PASO 4 En el menú **Modo de seguridad**, elija una de las tres opciones de WPA Personal.

PASO 5 (Solo WPA-Personal) En el campo **Cifrado**, elija una de las siguientes opciones:

- **TKIP/AES**: elija **TKIP/AES** para garantizar la compatibilidad con dispositivos inalámbricos más antiguos que es posible que no admitan AES.
- **AES**: esta opción es más segura.

PASO 6 En el campo **Clave de seguridad**, escriba una frase alfanumérica (de 8 a 63 caracteres ASCII o de 64 dígitos hexadecimales). El medidor de seguridad de la contraseña muestra cuán segura es la clave: Por debajo del mínimo, débil, fuerte, muy fuerte o segura. Se recomienda el uso de una clave de seguridad que el medidor de seguridad registre como segura.

PASO 7 Para mostrar la clave de seguridad como la ingresa, marque la casilla **Exponer contraseña**.

PASO 8 En el campo **Renovación de clave**, escriba el período de tiempo (de 600 a 7200 segundos) entre las renovaciones de claves. El valor predeterminado es 3600.

PASO 9 Haga clic en **Guardar** para guardar la configuración. Haga clic en **Atrás** para volver a la página **Configuración básica**.

Configuración de WPA-Enterprise, WPA2-Enterprise y WPA2-Enterprise combinado

Los modos de seguridad de WPA Enterprise, WPA2 Enterprise y WPA2 Enterprise combinado le permiten utilizar la autenticación del servidor RADIUS.

- **WPA-Enterprise**: le permite utilizar WPA con la autenticación del servidor RADIUS.
- **WPA2-Enterprise**: le permite utilizar WPA2 con la autenticación del servidor RADIUS.
- **WPA2-Enterprise combinado**: le permite utilizar los clientes WPA y WPA2 para conectarlos simultáneamente mediante la autenticación de RADIUS.

Para configurar el modo de seguridad de WPA Enterprise:

PASO 1 En la **Tabla inalámbrica** (**Inalámbrica** > **Configuración básica**), active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Editar modo de seguridad**.

PASO 3 En el campo **Seleccionar SSID**, elija la SSID para la que se deben configurar las opciones de seguridad.

PASO 4 En el menú **Modo de seguridad**, elija una de las tres opciones de WPA Enterprise.

PASO 5 (Solo WPA-Enterprise) En el campo **Cifrado**, elija una de las siguientes opciones:

- **TKIP/AES**: elija **TKIP/AES** para garantizar la compatibilidad con dispositivos inalámbricos más antiguos que es posible que no admitan AES.
- **AES**: esta opción es más segura.

PASO 6 En el campo **Servidor RADIUS**, escriba la dirección IP del servidor RADIUS.

PASO 7 En el campo **Puerto RADIUS**, escriba el puerto que se utiliza para acceder al servidor RADIUS.

PASO 8 En el campo **Clave compartida**, escriba una frase alfanumérica.

PASO 9 En el campo **Renovación de clave**, escriba el período de tiempo (de 600 a 7200 segundos) entre las renovaciones de claves. El valor predeterminado es 3600.

PASO 10 Haga clic en **Guardar** para guardar la configuración.

PASO 11 Haga clic en **Atrás** para volver a la página **Configuración básica**.

Configuración del filtrado MAC

Puede utilizar el filtrado MAC para permitir o rechazar el acceso a la red inalámbrica con base en la dirección (hardware) MAC del dispositivo solicitante. Por ejemplo, puede escribir las direcciones MAC de un conjunto de computadoras y solo permitirles el acceso a la red a esas computadoras. Puede configurar el filtrado MAC para cada red o SSID.

Para configurar el filtrado MAC:

PASO 1 En la **Tabla inalámbrica** (**Inalámbrica** > **Configuración básica**), active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Editar filtrado MAC**. Se abre la página **Filtrado MAC inalámbrico**.

PASO 3 En el campo **Editar filtrado MAC**, active la casilla **Habilitar** para habilitar el filtrado MAC para esta SSID.

PASO 4 En el campo **Control de conexión**, elija el tipo de acceso a la red inalámbrica:

- **Impedir**: seleccione esta opción para impedir que las direcciones MAC enumeradas en la **Tabla de direcciones MAC** accedan a la red inalámbrica. Esta opción se selecciona de forma predeterminada.
- **Permitir**: seleccione esta opción para permitir que las direcciones MAC enumeradas en la **Tabla de direcciones MAC** accedan a la red inalámbrica.

PASO 5 Para mostrar las computadoras y otros dispositivos de la red inalámbrica, haga clic en **Mostrar lista de clientes**.

PASO 6 En **Guardar en lista de filtros de dir. MAC**, marque la casilla para agregar el dispositivo a la lista de dispositivos que se agregarán a la **Tabla de direcciones MAC**.

PASO 7 Haga clic en **Agregar a MAC** para agregar los dispositivos seleccionados en la **Tabla de lista de clientes** a la **Tabla de direcciones MAC**.

PASO 8 Haga clic en **Guardar** para guardar la configuración.

PASO 9 Haga clic en **Atrás** para volver a la página **Configuración básica**.

Configuración del acceso de hora del día

Para proteger más la red, puede restringir su acceso al especificar cuándo los usuarios pueden acceder a la red.

Para configurar el acceso de hora del día:

PASO 1 En la **Tabla inalámbrica** (**Inalámbrica** > **Configuración básica**), active la casilla de la red que desea configurar.

PASO 2 Haga clic en **Acceso de hora del día**. Aparece la página Acceso de hora del día.

PASO 3 En el campo **Hora activa**, active la casilla **Habilitar** para habilitar el acceso de hora del día.

PASO 4 En los campos **Hora de inicio** y **Hora de finalización**, especifique el período durante el cual está permitido el acceso a la red.

PASO 5 Haga clic en **Guardar**.

Configuración de las opciones inalámbricas avanzadas

Las opciones inalámbricas avanzadas deben ajustarse únicamente por un administrador experto; las opciones incorrectas pueden reducir el rendimiento inalámbrico.

Para configurar las opciones inalámbricas avanzadas:

PASO 1 Elija **Inalámbrica** > **Configuración avanzada**. Aparece la página Configuración avanzada.

PASO 2 Configure estas opciones:

Ráfaga de trama	Habilite esta opción para que las redes inalámbricas tengan un mayor rendimiento, según el fabricante de los productos inalámbricos. Si no está seguro de cómo se utiliza esta opción, mantenga la opción predeterminada (habilitada).
Sin reconocimiento WMM	Al habilitar la opción Sin reconocimiento WMM, se puede obtener un rendimiento más eficiente, pero puede generar tasas de error más altas en un entorno de radiofrecuencia (RF). Este parámetro está desactivado de forma predeterminada.
Velocidad básica	La configuración de la velocidad básica no es la velocidad de la transmisión, pero se trata de una serie de velocidades que Services Ready Platform puede transmitir. El dispositivo anuncia su velocidad básica a los dispositivos inalámbricos de la red para que sepan qué velocidades se utilizarán. La Services Ready Platform también anunciará que seleccionará de forma automática la mejor velocidad de transmisión. La configuración predeterminada es Predeterminada, en la cual el dispositivo puede transmitir a todas las velocidades inalámbricas estándar (1 Mbps, 2 Mbps, 5,5 Mbps, 11 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps y 54 Mbps). Además de las velocidades de B y G, el dispositivo admite la velocidad de N. Las otras opciones son de 1 a 2 Mbps cuando se lo utiliza con tecnología inalámbrica más antigua, y la opción Todo, cuando el dispositivo puede transmitir a todas las velocidades inalámbricas. La velocidad básica no es la velocidad real de la transmisión de datos. Si desea especificar la velocidad de la transmisión de datos del dispositivo, configure las opciones de la velocidad de transmisión.

Velocidad de transmisión	La velocidad de la transmisión de datos debe configurarse según la velocidad de la red inalámbrica. Puede seleccionar entre un rango de velocidades de transmisión o puede seleccionar **Automática** para que el dispositivo utilice de forma automática la velocidad de datos más rápida posible y para que habilite la función de repliegue automático. El repliegue automático negociará la mejor velocidad de conexión posible entre el dispositivo y un cliente inalámbrico. El modo predeterminado es Automática.
Velocidad de transmisión N	La velocidad de la transmisión de datos debe configurarse según la velocidad de las redes inalámbricas N. Puede seleccionar entre un rango de velocidades de transmisión o puede seleccionar **Automática** para que el dispositivo utilice de forma automática la velocidad de datos más rápida posible y para que habilite la función de repliegue automático. El repliegue automático negociará la mejor velocidad de conexión posible entre el dispositivo y un cliente inalámbrico. El modo predeterminado es Automática.
Modo de protección CTS	El dispositivo utilizará de forma automática el modo de protección CTS (Habilitar para enviar) cuando sus dispositivos inalámbricos N y G tengan problemas y no puedan transmitir al dispositivo en un entorno con tráfico de 802.11b pesado. Esta función aumenta la capacidad del dispositivo para capturar todas las transmisiones inalámbricas N y G, pero provocará una gran disminución en el rendimiento. El modo predeterminado es Automática.
Intervalo de señales	El valor del intervalo baliza indica el intervalo de frecuencia de la baliza. Una baliza es un paquete que transmite el dispositivo para sincronizar la red inalámbrica. Escriba un valor entre 40 y 3500 milisegundos. El valor predeterminado es 100.

Intervalo DTIM	Este valor, entre 1 y 255, indica el intervalo del mensaje de indicación del tráfico de entrega (DTIM). Un campo DTIM es un campo de cuenta regresiva que informa a los clientes de la siguiente ventana para escuchar los mensajes de multidifusión y difusión. Cuando el dispositivo ha almacenado en el búfer mensajes de multidifusión y difusión para los clientes asociados, envía el siguiente DTIM con un valor de intervalo DTIM. Sus clientes escuchan las balizas y se activan para recibir los mensajes de multidifusión y difusión. El valor predeterminado es 1.
Umbral de fragmentación	Este valor especifica el tamaño máximo de un paquete antes de que se fragmenten los datos en varios paquetes. Si tiene una alta tasa de error de paquete, puede aumentar ligeramente el umbral de fragmentación. Habilitar el umbral de fragmentación a un nivel muy bajo puede provocar un mal rendimiento de la red. Se recomienda solo una ligera reducción del valor predeterminado. En la mayoría de los casos, debe permanecer en su valor predeterminado de 2346.
Umbral RTS	Si encuentra un flujo de datos incoherente, escriba solo reducciones mínimas. Se recomienda el valor predeterminado de 2347. Si un paquete de red es más chico que el tamaño del umbral de Petición para enviar (RTS) predefinido, no se habilitará el mecanismo de RTS/Habilitar para enviar (CTS). Services Ready Platform envía las tramas de RTS a una estación de recepción particular y negocia el envío de las tramas de datos. Después de recibir una RTS, la estación inalámbrica responde con una trama de CTS para reconocer el permiso de comenzar con la transmisión.

PASO 3 Haga clic en **Guardar**.

Detección de puntos de acceso no autorizados

Un punto de acceso (AP) no autorizado es un punto de acceso que se ha instalado en una red segura sin contar con la autorización de un administrador del sistema. Los puntos de acceso no autorizados representan una amenaza a la seguridad porque cualquier individuo que tenga acceso a las instalaciones puede instalar un punto de acceso inalámbrico que posiblemente permita que terceros no autorizados accedan a la red.

Use la página Detección de puntos de acceso no autorizados para habilitar en el dispositivo la visualización de información sobre todos los puntos de acceso que detecta el dispositivo en el área de la red. Si el punto de acceso que aparece como no autorizado en realidad es legítimo, podrá agregarlo a la **Tabla de puntos de acceso autorizados**. Seleccione una velocidad de actualización para asegurarse de que la página Detección de puntos de acceso no autorizados siempre muestre la última información.

Para habilitar la detección de puntos de acceso no autorizados:

PASO 1 Seleccione **Inalámbrica > Puntos de acceso no autorizados**.

PASO 2 Haga clic en el botón de radio **Detección de puntos de acceso no autorizados activada**.

PASO 3 Haga clic en **Guardar**.

Para autorizar puntos de acceso detectados:

PASO 1 En la **Tabla de puntos de acceso no autorizados detectados**, marque la casilla de los puntos de acceso que desea autorizar.

PASO 2 Haga clic en **Autorizar**.

Para agregar un punto de acceso a la tabla de puntos de acceso autorizados:

PASO 1 Haga clic en **Agregar fila**.

PASO 2 Introduzca la dirección MAC del punto de acceso que desea autorizar.

PASO 3 Introduzca el SSID o nombre que identifique a la red inalámbrica.

PASO 4 Escoja el modo de seguridad asociado al punto de acceso.

PASO 5 Seleccione TKIP (Protocolo de integridad de clave temporal) o CCMP (Protocolo de modo de cifrado de contador) como algoritmo de cifrado asociado al punto de acceso.

PASO 6 Seleccione servidor RADIUS o PSK (Clave previamente compartida) para autenticar el punto de acceso.

PASO 7 Seleccione el modo de red inalámbrica que usa el punto de acceso.

PASO 8 Escoja la frecuencia de radio que usa el punto de acceso.

PASO 9 Haga clic en **Guardar**.

Importación de listas de puntos de acceso autorizados

Es posible importar, mediante un archivo CSV, una lista de puntos de acceso autorizados. Use los valores a continuación como referencia al crear el archivo CSV.

Campo	Valores
Seguridad	• 0 — Abierto • 1 — WEP • 2 — WPA-Personal • 3 — WPA-Enterprise • 4 — WPA2-Personal • 5 — WPA2-Enterprise
Modo de red	• 0 — Solo B • 1 — Solo G • 2 — Solo N • 3 — BG combinado • 4 — GN combinado • 5 — BGN combinado

Campo	Valores
Canal	• 0 — Automática • 1 — 2.412 • 2 — 2.417 • 3 — 2.422 • 4 — 2.427 • 5 — 2.432 • 6 — 2.437 • 7 — 2.442 • 8 — 2.447 • 9 — 2.452 • 10 — 2.457 • 11 — 2.462
Cifrado	• 2 — TKIP • 4 — CCMP
Autenticación	• 2 — PSK • 1 — RADIUS

Asegúrese de que el contenido del archivo CSV esté organizado tal como se muestra en el siguiente ejemplo:

BSSID	Seguridad	Cifrado	Autenticación	Red inalámbrica	Canal	SSID
00:1C:10:CE:44:48	4	2	2	3	1	Auth_Guest

Para importar una lista de puntos de acceso autorizados:

PASO 1 Haga clic en **Fusionar** para agregar la lista de los puntos de acceso que desea importar a los puntos de acceso que aparecen en la **Tabla de puntos de acceso autorizados**. Haga clic en **Reemplazar** para reemplazar los puntos de acceso de la tabla por los puntos de acceso de la lista que desea importar.

PASO 2 Haga clic en **Examinar** para buscar el archivo que desea importar.

PASO 3 Haga clic en **Guardar**.

Configuración de WDS

Un sistema de distribución inalámbrica (WDS) es un sistema que habilita la interconexión inalámbrica de puntos de acceso en una red. Permite que una red inalámbrica se expanda mediante varios puntos de acceso sin la necesidad de utilizar la estructura básica de cableado para conectarlos.

Para establecer un enlace de WDS, se deben configurar el dispositivo y otros pares remotos de WDS en el mismo modo inalámbrico, canal inalámbrico, selección de banda inalámbrica y tipos de cifrado (Ninguno o WEP).

Es posible configurar WDS en modo de puente, donde un punto de acceso actúa como enlace común entre varios puntos de acceso; o bien en modo repetidor, donde un punto de acceso se conecta a dos puntos de acceso sin una conexión cableada a la LAN mediante la repetición de señales a través de la conexión inalámbrica.

WDS solo se admite en un SSID.

Para configurar WDS en modo puente:

PASO 1 Elija **Inalámbrica** > **WDS**.

PASO 2 Para habilitar los WDS (*Wireless Domain Services*, servicios de dominio inalámbrico), marque la opción **Habilitar.**

PASO 3 Seleccione el botón de radio **Puente de WDS**.

PASO 4 En la sección **Dirección MAC del puente inalámbrico remoto**, ingrese las direcciones MAC de hasta cuatro puntos de acceso para usar como puentes en los campos **MAC 1**, **MAC 2**, **MAC 3** y **MAC 4**.

PASO 5 Haga clic en **Guardar**.

Para configurar WDS en modo repetidor:

PASO 1 Elija **Inalámbrica** > **WDS**.

PASO 2 Marque la casilla de verificación **WDS**.

PASO 3 Seleccione el modo repetidor. Si selecciona **Permitir que un repetidor repita la señal inalámbrica**, escriba las direcciones MAC hasta de tres puntos de acceso para utilizar como repetidores en los campos **MAC 1**, **MAC 2** y **MAC 3**.

PASO 4 Si selecciona **Repetir la señal inalámbrica de un punto de acceso remoto**:

- Ingrese la dirección MAC de un punto de acceso inalámbrico en el campo **MAC**.
- Haga clic en **Mostrar redes disponibles** para visualizar la **Tabla de redes disponibles.** Haga clic en **Conectar** para agregar la dirección MAC del punto de acceso seleccionado al campo **MAC**.

PASO 5 Haga clic en **Guardar**.

Configuración de WPS

Configure WPS para permitir que los dispositivos compatibles con WPS puedan conectarse fácilmente y de manera segura a la red inalámbrica. Consulte el dispositivo cliente o su documentación para obtener más instrucciones sobre cómo configurar WPS en el dispositivo cliente.

Para configurar WPS:

PASO 1 Elija **Inalámbrica** > **WPS**. Aparece la página de Wi-Fi Protected Setup

PASO 2 Seleccione la opción SSID (*Service Set Identifier*, identificador del conjunto de servicio) en el menú desplegable.

PASO 3 Configure la WPS en los dispositivos cliente en una de las siguientes tres maneras:

a. Haga clic o presione el botón WPS en el dispositivo de cliente y luego haga clic sobre el ícono WPS en esta página.

b. Ingrese el número de PIN WPS del cliente y haga clic en **Registrar**.

c. Un dispositivo de cliente solicita un número de PIN del router, use el número de PIN indicado del router.

Estado del PIN del dispositivo: estado del número de identificación personal (PIN) del dispositivo WPA.

PIN de dispositivo: identifica el PIN de un dispositivo que intenta conectarse.

Duración del PIN: duración de la clave. Si el tiempo caduca, se negociará una nueva red.

Después de configurar WPS, la siguiente información aparece en la parte inferior de la página **WPS**: Estado de Wi-Fi Protected Setup, nombre de la red (SSID) y seguridad.

Configuración de un portal cautivo

Use la característica de portal cautivo para proporcionar acceso controlado y autenticado a Internet y a los recursos de red sin comprometer la seguridad. Un portal cautivo muestra una página web especial para autenticar clientes antes de que puedan usar Internet. Se puede configurar la verificación del portal cautivo para permitir el acceso de usuarios autenticados e invitados.

Configure instancias del portal cautivo para cada red inalámbrica virtual del dispositivo mediante la asociación con un perfil del portal.

Creación de perfiles del portal cautivo

Para crear un perfil del portal cautivo:

PASO 1 Seleccione **Inalámbrica > Portal cautivo > Perfil del portal.** En la sección **Tabla de perfiles del portal**, haga clic en **Agregar fila**. Para modificar el perfil de portal proporcionado en el dispositivo, marque la casilla **Perfil_De_Portal_Predeterminado** y haga clic en **Editar**.

PASO 2 Escriba un nombre para el perfil del portal cautivo.

PASO 3 Seleccione si desea usar el perfil para autenticar usuarios invitados o usuarios de la red.

PASO 4 Para redirigir usuarios a una URL tras la autenticación, active **URL automática de redireccionamiento** e ingrese un nombre de dominio completamente calificado o una dirección IP en el campo **URL de redireccionamiento**. Por ejemplo, incluya http:// en la URL.

PASO 5 En el campo **Caducidad de sesión**, especifique la cantidad de minutos que el dispositivo mantendrá abierta la sesión de autenticación con el cliente inalámbrico asociado. El valor predeterminado es 60 minutos.

PASO 6 Seleccione un color de fuente para el texto que desea mostrar en la página.

PASO 7 Especifique el texto que desea mostrar, como el nombre de la organización, el texto de la etiqueta para el nombre de usuario y la contraseña, y la etiqueta del botón de inicio de sesión.

PASO 8 Ingrese el texto de Copyright estándar asociado con su empresa.

PASO 9 En los campos **Error 1** y **Error 2**, introduzca los mensajes de error que desea mostrar a los clientes cuando falla el inicio de sesión y cuando se supera la cantidad máxima de conexiones.

PASO 10 Para usar una casilla de verificación para permitir a los usuarios aceptar los términos de uso antes de continuar, habilite **Acuerdo.** El texto del campo **Texto del acuerdo** se mostrará como la etiqueta para la casilla de verificación.

PASO 11 Introduzca los términos de aceptación que desee mostrar a los usuarios en el campo **Política de uso aceptable**.

PASO 12 En la sección **Cargar archivos**, escoja los archivos para cargar el logotipo de la empresa y los archivos de fondo de acuerdo con las directivas de marca de la empresa. Guarde el perfil.

Para obtener una vista previa de este perfil, seleccione **Portal cautivo > Vista previa de la página del portal** y por último el perfil de la lista desplegable **Perfiles del portal**.

Configuración de instancias del portal cautivo

Para configurar una instancia del portal cautivo para el dispositivo:

PASO 1 Elija **Inalámbrica > Configuración básica**.

PASO 2 En la sección **Tabla inalámbrica**, marque la casilla **Habilitar** correspondiente al SSID para el que desea configurar un portal cautivo. Haga clic en **Editar**.

PASO 3 Seleccione un perfil de portal para SSID.

Es posible crear hasta cuatro portales cautivos con los SSID para su dispositivo. Para crear un nuevo perfil de portal, seleccione **Crear un nuevo perfil de portal** de la lista desplegable. Seleccione Perfil_De_Portal_Predeterminado para usar el perfil de portal proporcionado con el dispositivo.

PASO 4 Marque la casilla **Habilitar** para activar el portal cautivo para el SSID.

PASO 5 Guarde las instancias del portal cautivo.

Creación de cuentas de usuario del portal cautivo

Para crear una cuenta de usuario del portal cautivo:

PASO 1 Seleccione **Inalámbrica > Portal cautivo > Cuentas de usuario**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 Ingrese un nombre de usuario y una contraseña. Vuelva a escribir la contraseña para verificarla.

Recomendamos que la contraseña no sea una palabra del diccionario de ningún idioma y que incluya una combinación de letras (tanto minúsculas como mayúsculas), números y símbolos. La contraseña puede tener hasta 64 caracteres.

PASO 4 En el campo **Tiempo de acceso (minutos)**, especifique el tiempo que debe transcurrir hasta que caduque la sesión de autenticación.

PASO 5 Para importar nombres de usuario y contraseñas de un archivo CSV, haga clic en **Importar**. Se muestra la página **Administración > Usuarios**. En la sección **Importar nombre de usuario y contraseña**, haga clic en **Examinar** para buscar el archivo y luego en **Importar**. Para obtener más información, consulte **Importación de cuentas de usuario**.

PASO 6 Guarde las cuentas de usuario.

Configuración del modo del dispositivo

Es posible configurar el dispositivo para que funcione en los siguientes modos:

- **Router**: para funcionar como router inalámbrico.
- **AP (punto de acceso)**: para proporcionar conexiones inalámbricas a clientes y extender la capacidad de Wi-Fi a una red cableada actual. Todos los puertos LAN se deshabilitan cuando el dispositivo funciona como punto de acceso.

  Asegúrese de configurar la información de VLAN para administrar puntos de acceso en la página **Red > WAN > Configuración de WAN**. Para obtener más información, consulte **Configuración de parámetros opcionales**.

Para configurar el modo del dispositivo:

PASO 1 Seleccione **Inalámbrica > Modo del dispositivo** y escoja el modo en el que desea que funcione el dispositivo.

PASO 2 Haga clic en **Guardar**.

5

Configuración del firewall

Funciones del firewall

Puede asegurar la red mediante la creación y aplicación de las reglas que utiliza el dispositivo para bloquear y permitir de manera selectiva el tráfico de Internet entrante y saliente. A continuación, especifique cómo y a cuáles dispositivos se aplican las reglas. Para hacerlo, debe definir lo siguiente:

- Los tipos de servicio o de tráfico que el router debe permitir o bloquear. Por ejemplo, la navegación web, VoIP y otros servicios estándar y personalizados que defina.
- La dirección del tráfico al especificar el origen y el destino del tráfico; esto se realiza al especificar la Zona de origen (LAN/WAN/DMZ) y la Zona de destino (LAN/WAN/DMZ).
- Las programaciones que especifican cuándo el router debe aplicar las reglas.
- Las palabras clave (en un nombre de dominio o en una URL de una página web) que el router debe permitir o bloquear.
- Las reglas para permitir o bloquear el tráfico de Internet entrante y saliente para los servicios especificados en las programaciones especificadas.
- Las direcciones MAC de los dispositivos cuyo acceso entrante a la red el router debe bloquear.
- Activadores de puerto que indican al router permitir o bloquear el acceso a servicios especificados según el número de puerto.
- Los informes y las alertas que desea que el router le envíe.

Por ejemplo, puede establecer las políticas de acceso restringido de acuerdo con la hora del día, las direcciones web y las palabras clave de las direcciones web. Puede bloquear el acceso a Internet mediante las aplicaciones y los servicios en la red LAN, como salas de conversación o juegos. Puede bloquear el acceso desde la red DMZ pública o WAN solo a ciertos grupos de computadoras.

Las reglas (WAN a LAN/DMZ) entrantes restringen el acceso al tráfico que ingresa en la red, de modo que permiten, de manera selectiva, que solo determinados usuarios externos accedan a los recursos locales específicos. De forma predeterminada, se bloquea todo acceso desde la red WAN no segura a la red LAN segura, excepto en respuesta a solicitudes desde LAN o DMZ. Para permitir que los dispositivos externos accedan a servicios en la LAN segura, debe crear una regla de firewall para cada servicio.

Si desea permitir el tráfico entrante, debe dar a conocer al público la dirección IP del puerto WAN del router. Esto se denomina “exposición de su host”. Cómo dar a conocer su dirección depende de cómo están configurados los puertos WAN; para el dispositivo, puede utilizar la dirección IP si se asigna una dirección estática al puerto WAN o un nombre DDNS (DNS dinámico) si su dirección WAN es dinámica.

Las reglas (LAN/DMZ a WAN) salientes restringen el acceso al tráfico que sale de la red, de modo que permiten, de manera selectiva, que solo determinados usuarios locales accedan a los recursos externos específicos. La regla saliente predeterminada permite el acceso de la zona segura (LAN) a la red DMZ pública o WAN no segura. Para bloquear el acceso de los hosts en la LAN segura a servicios del exterior (WAN no segura), debe crear una regla de firewall para cada servicio.

Configuración de los parámetros básicos de firewall

Para configurar los parámetros básicos de firewall:

PASO 1 Elija **Firewall** > **Configuración básica**.

PASO 2 Configure los siguientes parámetros de firewall:

Protección de suplantación de direcciones IP	Para proteger la red de la suplantación de direcciones IP, marque la casilla de verificación **Habilitar**.
Protección contra DoS	Active **Habilitar** para habilitar la protección de denegación de servicio.
Bloquear solicitud WAN	Bloquea las solicitudes de ping al dispositivo desde WAN.

Acceso web LAN/VPN	Elija el tipo de acceso web que se puede utilizar para conectarse al firewall: HTTP o HTTPS (HTTP seguro).
Administración remota **Acceso remoto** **Actualización remota** **Dirección IP remota permitida** **Puerto de admin. remota**	Consulte **Configuración de la administración remota**.
Transmisión de multidifusión IPv4 (Proxy IGMP)	Active **Habilitar** para habilitar la transmisión de multidifusión para IPv4.
Transmisión de multidifusión IPv6 (Proxy IGMP)	Active **Habilitar** para habilitar la transmisión de multidifusión para IPv6.
SIP ALG	Para permitir que el tráfico de Protocolo de inicio de sesión (SIP) atraviese el firewall, marque la casilla de verificación **SIP ALG**. El dispositivo admite un máximo de 256 sesiones.
UPnP **Permitir a usuarios configurar** **Permitir a usuarios deshabilitar acceso a Internet**	Consulte **Configuración de Universal Plug and Play**.
Bloquear Java	Active para bloquear los applets de Java. Los applets de Java son pequeños programas integrados en páginas web que habilitan la funcionalidad dinámica de la página. Se puede utilizar un applet malicioso para comprometer o infectar computadoras. La habilitación de este parámetro no permite que se descarguen los applets de Java. Haga clic en **Automático** para bloquear automáticamente Java o haga clic en **Manual** y escriba un puerto específico en el cual bloquear Java.

Bloquear cookies	Active para bloquear las cookies. Los sitios web que generalmente requieren inicio de sesión utilizan las cookies para guardar la información de la sesión. Sin embargo, muchos sitios web utilizan cookies para guardar la información de seguimiento y los hábitos de navegación. La habilitación de esta opción elimina las cookies que se creen mediante un sitio web. Muchos sitios web requieren que se acepten cookies para que se pueda acceder al sitio correctamente. El bloqueo de las cookies puede causar que muchos sitios web no funcionen correctamente. Haga clic en **Automático** para bloquear automáticamente las cookies o haga clic en **Manual** y escriba un puerto específico en el cual bloquear las cookies.
Bloquear ActiveX	Active para bloquear el contenido ActiveX. Similares a los applets de Java, los controles ActiveX se instalan en una computadora que ejecuta Windows mientras se ejecuta Internet Explorer. Se puede utilizar un control ActiveX malicioso para comprometer o infectar computadoras. La habilitación de este parámetro no permite que se descarguen los applets de ActiveX. Haga clic en **Automático** para bloquear automáticamente ActiveX o haga clic en **Manual** y escriba un puerto específico en el cual bloquear ActiveX.

Bloquear proxy	Active para bloquear los servidores proxy. Un servidor proxy (o proxy) permite que las computadoras enruten más conexiones a otras computadoras a través de proxy, eludiendo así ciertas reglas de firewall. Por ejemplo, si están bloqueadas las conexiones a una dirección IP específica mediante una regla de firewall, las solicitudes pueden enrutarse a través de un proxy que no está bloqueado por la regla, de modo que deja sin efecto la restricción. La habilitación de esta función bloquea los servidores proxy. Haga clic en **Automático** para bloquear automáticamente los servidores proxy o haga clic en **Manual** y escriba un puerto específico en el cual bloquear los servidores proxy.

PASO 3 Haga clic en **Guardar**.

Configuración de la administración remota

Puede habilitar la administración remota para que pueda acceder al dispositivo desde una red WAN remota.

Para configurar la administración remota, configure estos parámetros en la página **Configuración básica**:

Administración remota	Marque **Habilitar** para habilitar la administración remota.
Acceso remoto	Elija el tipo de acceso web que se puede utilizar para conectarse al firewall: HTTP o HTTPS (HTTP seguro).
Actualización remota	Para permitir actualizaciones remotas del dispositivo, active **Habilitar**.

Dirección IP remota permitida	Haga clic en el botón **Cualquier dir. IP** para permitir la administración remota desde cualquier dirección IP o escriba una dirección IP específica en el campo de direcciones.
Puerto de admin. remota	Escriba el puerto en el que está permitido el acceso remoto. El puerto predeterminado es 443. Al acceder remotamente al router, debe ingresar el puerto de admin. remota como parte de la dirección IP. Por ejemplo: **https://<remote-ip>:<remote-port>**, o **https://168.10.1.11:443**

PRECAUCIÓN Cuando el acceso remoto está habilitado, cualquier persona que conozca la dirección IP puede acceder al router. Debido a que un usuario de WAN malintencionado puede volver a configurar el dispositivo y usarlo de forma incorrecta, se recomienda que cambie las contraseñas del administrador y de cualquier invitado antes de continuar.

Configuración de Universal Plug and Play

Universal Plug and Play (UPnP) permite la detección automática de dispositivos que se pueden comunicar con el dispositivo.

Para configurar UPnP, configure estos parámetros en la página **Configuración básica**:

UPnP	Marque la casilla **Habilitar** para habilitar UPnP.
Permitir a usuarios configurar	Active esta casilla para permitir que los usuarios que tienen habilitada la compatibilidad con UPnP en las computadoras o en otros dispositivos habilitados para UPnP configuren las reglas de asignación de puerto para UPnP. Si está deshabilitado, el dispositivo no permite que la aplicación agregue la regla de reenvío.
Permitir a usuarios deshabilitar acceso a Internet	Active esta casilla para permitir que los usuarios deshabiliten el acceso a Internet.

Administración de las programaciones de firewall

Puede crear las programaciones de firewall para aplicar las reglas de firewall en días específicos o en horas específicas del día.

Incorporación o edición de una programación de firewall

Para crear o editar una programación:

PASO 1 Elija **Firewall** > **Programar administración**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 En el campo **Nombre**, escriba un nombre único para identificar la programación. Este nombre está disponible en la página Configuración de reglas de firewall en la lista **Seleccionar programación**. (Consulte **Configuración de reglas de acceso**).

PASO 4 En la sección **Días programados**, seleccione si desea aplicar la programación a Todos los días o a Días específicos. Si elige **Días específicos**, active la casilla que se encuentra al lado de los días que desea incluir en la programación.

PASO 5 En la sección **Hora del día programada**, seleccione la hora a la cual desea que se aplique la programación. Si elige **A horas específicas**, escriba las horas de inicio y finalización.

PASO 6 Haga clic en **Guardar**.

Configuración de la administración de servicios

Cuando crea una regla de firewall, puede especificar un servicio que está controlado por la regla. Los tipos comunes de servicio están disponibles para su selección, también puede crear sus propios servicios personalizados.

La página **Administración de servicio** le permite crear los servicios personalizados para los cuales se pueden definir las reglas de firewall. Una vez definido, el nuevo servicio aparece en la tabla de lista de **Servicios personalizados disponibles**.

Para crear un servicio personalizado:

PASO 1 Elija **Firewall** > **Administración de servicio**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 En el campo **Nombre del servicio**, escriba el nombre del servicio para fines administrativos y de identificación.

PASO 4 En el campo **Protocolo**, elija el protocolo de capa 4 que utiliza el servicio en el siguiente menú desplegable:

- **TCP**
- **UDP**
- **TCP y UDP**
- **ICMP**

PASO 5 En el campo **Puerto de inicio**, escriba el primer puerto TCP o UDP del rango que utiliza el servicio.

PASO 6 En el campo **Puerto final**, escriba el último puerto TCP o UDP del rango que utiliza el servicio.

PASO 7 Haga clic en **Guardar**.

Para editar una entrada, seleccione la entrada y haga clic en **Editar**. Realice sus cambios y luego haga clic en **Guardar**.

Configuración de reglas de acceso

Configuración de política de salida predeterminada

La página **Reglas de acceso** le permite configurar la política de salida predeterminada del tráfico que se dirige de la red segura (LAN) a la red no segura (WAN dedicada/opcional).

La política de entrada predeterminada del tráfico que fluye de la zona no segura a la zona segura siempre está bloqueada y no se puede cambiar.

NOTA Las políticas de acceso a Internet anulan las reglas de acceso si ambas están configuradas en el dispositivo.

Para configurar la política de salida predeterminada:

PASO 1 Elija **Firewall** > **Reglas de acceso**.

PASO 2 Elija **Permitir** o **Rechazar**.

Nota: Asegúrese de que el soporte IPv6 esté habilitado en el dispositivo para configurar el firewall IPv6. Consulte **Configuración IPv6**.

PASO 3 Haga clic en **Guardar**.

Reorganización de las reglas de acceso

El orden en el que las reglas de acceso se muestran en la tabla de reglas de acceso indica el orden en el que se aplican. Es posible que desee reorganizar la tabla para que determinadas reglas se apliquen antes que otras. Por ejemplo, es posible que desee aplicar una regla que permita ciertos tipos de tráfico antes de bloquear otros tipos de tráfico.

Para reorganizar las reglas de acceso:

PASO 1 Elija **Firewall** > **Reglas de acceso**.

PASO 2 Haga clic en **Reorganizar**.

PASO 3 Marque la casilla que se encuentra en la fila de la regla que desea mover hacia arriba o hacia abajo y haga clic en la flecha arriba o en la flecha abajo para subir o bajar la regla una línea o seleccione la posición deseada para la regla en la lista desplegable y haga clic en **Mover a**.

PASO 4 Haga clic en **Guardar**.

Agregar reglas de acceso

Todas las reglas de firewall configuradas en el dispositivo se muestran en la **Tabla de reglas de acceso**. Esta lista también indica si la regla está habilitada (activa) y proporciona un resumen de la zona de origen/destino así como los servicios y los usuarios a los que afecta la regla.

Para crear una regla de acceso:

PASO 1 Elija **Firewall** > **Reglas de acceso**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 En el campo **Tipo de conexión**, elija el origen del tráfico de origen:

- **Saliente (LAN > WAN)**: elija esta opción para crear una regla saliente.
- **Entrante (WAN > LAN)**: elija esta opción para crear una regla entrante.
- **Entrante (WAN > DMZ)**: elija esta opción para crear una regla entrante.

PASO 4 En el menú desplegable **Acción**, elija la acción:

- **Bloquear siempre**: siempre bloquea el tipo de tráfico seleccionado.
- **Permitir siempre**: nunca bloquea el tipo de tráfico seleccionado.
- **Bloquear por programación**: bloquea el tipo de tráfico seleccionado de acuerdo con la programación.
- **Permitir por programación**: permite el tipo de tráfico seleccionado de acuerdo con la programación.

PASO 5 En el menú desplegable **Servicios**, elija el servicio a permitir o bloquear mediante esta regla. Elija **Todo el tráfico** para permitir que la regla se aplique a todas las aplicaciones y servicios, o elija una única aplicación para bloquear:

- Sistema de nombres de dominio (DNS), UDP o TCP
- Protocolo de transferencia de archivos (FTP)
- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo de transferencia de hipertexto seguro (HTTPS)
- Protocolo trivial de transferencia de archivos (TFTP)
- Protocolo de acceso a mensajes por Internet (IMAP)
- Protocolo de transporte de noticias en red (NNTP)

- Protocolo de oficina de correos (POP3)
- Protocolo de administración de red simple (SNMP)
- Protocolo simple de transferencia de correo (SMTP)
- Telnet
- STRMWORKS
- Sistema de control de acceso al controlador de acceso al terminal (TACACS)
- Telnet (comando)
- Telnet secundario
- Telnet SSL
- Voz (SIP)

PASO 6 En el campo **IP de origen**, seleccione los usuarios a los que se les aplica la regla de firewall:

- **Cualquiera**: la regla se aplica al tráfico que se origina en cualquier host en la red local.
- **Dirección única**: la regla se aplica al tráfico que se origina en una dirección IP única en la red local. Escriba la dirección en el campo **Iniciar**.
- **Rango de direcciones**: la regla se aplica al tráfico que se origina en una dirección IP ubicada en un rango de direcciones. Escriba la dirección IP de inicio en el campo **Iniciar** y la dirección IP de finalización en el campo **Finalizar**.

PASO 7 En el campo **Registro**, especifique si deben registrarse los paquetes para esta regla.

Para registrar los detalles de todos los paquetes que coinciden con esta regla, elija **Siempre** en el menú desplegable. Por ejemplo, si una regla saliente para una programación está seleccionada como **Bloquear siempre**, para cada paquete que intente hacer una conexión saliente para ese servicio, se graba un mensaje en el registro con la dirección de origen y la dirección de destino del paquete (y más información).

La habilitación del registro puede generar un volumen significativo de mensajes de registro y se la recomienda para fines de depuración únicamente.

Elija **Nunca** para deshabilitar el registro.

Nota: Cuando el tráfico va desde LAN o DMZ a WAN, el sistema requiere que se vuelva a escribir la dirección IP de origen o destino de los paquetes IP entrantes a medida que pasan por el firewall.

PASO 8 Marque la casilla de verificación **Habilitar estado de la regla** para habilitar la nueva regla de acceso.

PASO 9 Haga clic en **Guardar**.

Creación de la política de acceso a Internet

El dispositivo admite varias opciones para bloquear el acceso a Internet. Puede bloquear todo el tráfico de Internet, bloquear el tráfico de Internet a ciertos equipos o puntos finales o bloquear el acceso a sitios de Internet al especificar palabras clave para bloquear. Si estas palabras clave se encuentran en el nombre del sitio (por ejemplo, el nombre del grupo de noticias o la dirección URL del sitio web), el sitio se bloquea.

Incorporación o edición de una política de acceso a Internet

Para crear una política de acceso a Internet:

PASO 1 Elija **Firewall** > **Política de acceso a Internet**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 Marque la casilla de verificación **Habilitar estado**.

PASO 4 Escriba el nombre de una política para fines administrativos o de identificación.

PASO 5 En el menú desplegable **Acción**, elija el tipo de restricción de acceso que necesita:

- **Bloquear siempre**: bloquear siempre el tráfico de Internet. Esta opción bloquea el tráfico de Internet a puntos finales y de puntos finales. Si desea bloquear todo el tráfico pero permitir que ciertos puntos finales reciban tráfico de Internet, consulte el Paso 7.
- **Permitir siempre**: permitir siempre el tráfico de Internet. Puede redefinir esta opción para bloquear el tráfico de Internet de ciertos puntos finales; consulte el Paso 7. También puede permitir todo el tráfico de Internet excepto para ciertos sitios web; consulte el Paso 8.
- **Bloquear por programación**: bloquea el tráfico de Internet según una programación (por ejemplo, si desea bloquear el tráfico de Internet durante los días de semana en el horario de trabajo, pero permitirlo después del horario de trabajo y durante el fin de semana).
- **Permitir según programación**: permite tráfico de Internet según una programación.

Si elige **Bloquear por programación** o **Permitir por programación**, haga clic en **Configurar programaciones** para crear una programación. Consulte **Administración de las programaciones de firewall**.

PASO 6 Seleccione una programación en el menú desplegable.

PASO 7 (Opcional) Aplique la política de acceso a ciertos equipos para permitir o bloquear el tráfico proveniente de ciertos dispositivos:

a. En la tabla **Aplicar la política de acceso a los siguientes equipos**, haga clic en **Agregar fila**.

b. En el menú desplegable **Tipo**, elija cómo identificar la computadora (mediante una dirección MAC, una dirección IP o mediante la especificación de un rango de direcciones IP).

c. En el campo **Valor**, de acuerdo con lo que eligió en el paso anterior, escriba una de las siguientes opciones:

- Dirección MAC (xx:xx:xx:xx:xx:xx) de la computadora en la que se aplica la política.
- La dirección IP de la computadora en la que se aplica la política.

- Las direcciones IP de inicio y finalización del rango de direcciones que se deben bloquear (por ejemplo, 192.168.1.2-192.168.1.253).

PASO 8 Para bloquear el tráfico de sitios web específicos:

a. En la tabla **Palabra clave y nombre de dominio de sitio web**, haga clic en **Agregar fila**.

b. En el menú desplegable **Tipo**, elija cómo bloquear un sitio web (mediante la especificación del nombre de dominio o de una palabra clave que aparece en la URL).

c. En el campo **Valor**, escriba la URL o la palabra clave que se utiliza para bloquear el sitio web.

Por ejemplo, para bloquear la URL ejemplo.com, elija **Dirección URL** en el menú desplegable y escriba **ejemplo.com** en el campo **Valor**. Para bloquear una URL que tiene la palabra clave “ejemplo” en la URL, elija **Palabra clave** en el menú desplegable y escriba **ejemplo** en el campo **Valor**.

PASO 9 Haga clic en **Guardar**.

Configuración de la traducción de direcciones de red (NAT) una a una

Use la página NAT una a una para asignar direcciones IP locales detrás del firewall a direcciones IP globales. NAT una a una es una forma de que los sistemas configurados con direcciones IP privadas, que se encuentran detrás de un firewall, aparenten tener direcciones IP públicas.

Para agregar una regla NAT una a una:

PASO 1 Seleccione **Firewall > NAT una a una**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 En el campo **Inicio del intervalo privado**, introduzca la dirección IP inicial en el rango de direcciones IP (LAN) privadas.

PASO 4 En el campo **Inicio del intervalo público**, introduzca la dirección IP inicial en el rango de direcciones IP (WAN) públicas.

PASO 5 En **Longitud del intervalo**, introduzca el número de direcciones IP públicas que deben asignarse a direcciones privadas.

PASO 6 En el campo **Servicio**, seleccione el servicio para el cual se aplica la regla. Los servicios para NAT una a una permiten configurar el servicio que aceptará la dirección IP (LAN) privada cuando se envía tráfico a la dirección IP pública correspondiente. Los servicios configurados en las direcciones IP privadas del rango se aceptan cuando el tráfico está disponible en la dirección IP pública correspondiente.

PASO 7 Haga clic en **Guardar**.

Configuración de reenvío de puertos

El reenvío de puertos se utiliza para redireccionar el tráfico de Internet de un puerto en WAN a otro puerto en LAN. Los servicios comunes están disponibles o puede definir un servicio personalizado y los puertos asociados que deben reenviarse.

Las páginas **Reglas de reenvío de un solo puerto** y **Reglas de reenvío de rango de puertos** enumeran todas las reglas de reenvío de puertos disponibles para este dispositivo y le permiten configurar las reglas de reenvío de puertos.

NOTA El reenvío de puertos no es apropiado para los servidores en LAN, ya que se depende de que el dispositivo LAN realice una conexión saliente antes de que se abran los puertos entrantes.

Algunas aplicaciones requieren que, cuando se conecten dispositivos externos, se reciban datos en un puerto o en un rango de puertos específicos para funcionar correctamente. El router debe enviar todos los datos entrantes para esa aplicación solamente en el puerto o rango de puertos requerido.

La puerta de enlace tiene una lista de los juegos y de las aplicaciones comunes con los puertos entrantes y salientes correspondientes que deben abrirse. También puede especificar una regla de reenvío de puertos mediante la definición del tipo de tráfico (TCP o UDP) y el rango de puertos entrantes y salientes que deben abrirse cuando están habilitados.

Configuración de reenvío de un solo puerto

Para agregar una regla de reenvío de un solo puerto:

PASO 1 Elija **Firewall** > **Reenvío de un solo puerto**. Se muestra una lista de las aplicaciones preexistentes.

PASO 2 En el campo **Aplicación**, escriba el nombre de la aplicación para la que debe configurarse el reenvío de puerto.

PASO 3 En el campo **Puerto externo**, escriba el número de puerto que activa esta regla cuando se realiza una solicitud de conexión desde el tráfico saliente.

PASO 4 En el campo **Puerto interno**, escriba el número de puerto que utiliza el sistema remoto para responder a la solicitud que recibe.

PASO 5 En el menú desplegable **Interfaz**, elija **Ambos (Ehternet y 3G)**, **Ethernet** o **3G**.

PASO 6 En el menú desplegable **Protocolo**, elija un protocolo (**TCP**, **UDP** o **TCP** y **UDP**).

PASO 7 En el campo **Dirección IP**, escriba la dirección IP del host del lado de LAN a donde se reenviará el tráfico IP específico. Por ejemplo, puede enviar tráfico HTTP al puerto 80 de la dirección IP de un servidor web del lado de LAN.

PASO 8 En el campo **Habilitar**, active la casilla **Habilitar** para habilitar la regla.

PASO 9 Haga clic en **Guardar**.

Configuración de reenvío de rango de puertos

Para agregar una regla de reenvío de rango de puertos:

PASO 1 Elija **Firewall** > **Reenvío de rango de puertos**.

PASO 2 En el campo **Aplicación**, escriba el nombre de la aplicación para la que debe configurarse el reenvío de puerto.

PASO 3 En el campo **Puerto externo**, especifique el número de puerto que activará esta regla cuando se realice una solicitud de conexión desde el tráfico saliente.

PASO 4 En el campo **Iniciar**, especifique el número de puerto que comienza el rango de puertos que debe reenviarse.

PASO 5 En el campo **Finalizar**, especifique el número de puerto que finaliza el rango de puertos que debe reenviarse.

PASO 6 En el menú desplegable **Interfaz**, elija **Ambos (Ehternet y 3G)**, **Ethernet** o **3G**.

PASO 7 En el menú desplegable **Protocolo**, elija un protocolo (**TCP**, **UDP** o **TCP** y **UDP**).

PASO 8 En el campo **Dirección IP**, escriba la dirección IP del host del lado de LAN a donde se reenviará el tráfico IP específico.

PASO 9 En el campo **Habilitar**, active la casilla **Habilitar** para habilitar la regla.

PASO 10 Haga clic en **Guardar**.

Configuración de la activación de rango de puertos

La activación de puertos permite que los dispositivos en LAN o DMZ soliciten uno o más puertos de reenvío. La activación de puertos espera una solicitud saliente de LAN/DMZ en uno de los puertos salientes definidos y, luego, abre un puerto entrante para ese tipo de tráfico determinado.

La activación de puertos es una forma de reenvío de puertos dinámica cuando una aplicación transmite datos a través de los puertos salientes o entrantes abiertos. La activación de puertos abre un puerto entrante para un tipo de tráfico específico en un puerto saliente definido. La activación de puertos es más flexible que el reenvío de puertos estático (disponible durante la configuración de las reglas de firewall), ya que una regla no debe referir a una IP de LAN o un rango de IP. Los puertos tampoco quedan abiertos cuando no están en uso, de modo que proporciona un nivel de seguridad que el reenvío de puertos no ofrece.

NOTA La activación de puertos no es apropiada para los servidores en LAN, ya que se depende de que el dispositivo LAN realice una conexión saliente antes de que se abran los puertos entrantes.

Algunas aplicaciones requieren que, cuando se conecten dispositivos externos, se reciban datos en un puerto o en un rango de puertos específicos para funcionar correctamente. El router debe enviar todos los datos entrantes para esa aplicación solamente en el puerto o rango de puertos requerido. La puerta de enlace tiene una lista de los juegos y de las aplicaciones comunes con los puertos entrantes y salientes correspondientes que deben abrirse. También puede especificar una regla de activación de puertos mediante la definición del tipo de tráfico (TCP o UDP) y del rango de puertos entrantes y salientes que deben abrirse cuando están habilitados.

Para agregar una regla de activación de puertos:

PASO 1 Elija **Firewall** > **Activación de rango de puertos**.

PASO 2 En el campo **Aplicación**, escriba el nombre de la aplicación para la que debe configurarse el reenvío de puerto.

PASO 3 En los campos **Rango activado**, escriba el número de puerto o el rango de número de puertos que activará esta regla cuando se realice una solicitud de conexión desde el tráfico saliente. Si la conexión saliente utiliza solamente un puerto, escriba el mismo número de puerto en los dos campos.

PASO 4 En los campos **Rango reenviado**, escriba el número de puerto o el rango de número de puertos que utiliza el sistema remoto para responder a la solicitud que recibe. Si la conexión entrante utiliza solamente un puerto, especifique el mismo número de puerto en los dos campos.

PASO 5 En el menú desplegable **Interfaz**, elija **Ambos (Ehternet y 3G)**, **Ethernet** o **3G**.

PASO 6 En el campo **Habilitar**, active la casilla **Habilitar** para habilitar la regla.

PASO 7 Haga clic en **Guardar**.

6

Configuración de VPN

Tipos de túnel de VPN

Es posible configurar VPN en el dispositivo para proporcionar un túnel o canal de comunicaciones seguras entre:

- Dos routers de puerta de enlace
- Un dispositivo cliente remoto y un router de puerta de enlace

Configuración de VPN IPsec básicas de sitio a sitio

El dispositivo es compatible con la VPN IPsec de sitio a sitio para un túnel de VPN simple de puerta de enlace a puerta de enlace. Después de configurar los parámetros de VPN básicos, podrá conectarse de forma segura a otro router habilitado para VPN. Por ejemplo, puede configurar el dispositivo en un sitio secundario para conectar el router que conecta túneles VPN de sitio a sitio en el sitio corporativo, de manera que el sitio secundario pueda acceder de forma segura a la red corporativa.

Pasos para configurar opciones de VPN básicas en una conexión IPsec de sitio a sitio:

PASO 1 Seleccione **VPN > VPN IPsec de sitio a sitio > Configuración básica de VNP**.

PASO 2 En el campo **Nuevo mombre de la conexión**, escriba un nombre para el túnel de VPN.

PASO 3 En el campo **Clave previamente compartida**, introduzca la clave previamente compartida, o la contraseña, que será intercambiada entre los dos routers. Debe contener entre 8 y 49 caracteres.

PASO 4 En los campos **Información de punto final**, introduzca la siguiente información:

- **Punto final remoto**: seleccione si el router al que se conectará el dispositivo estará identificado por su dirección IP o por un nombre de dominio totalmente calificado. Por ejemplo, una dirección IP como 192.168.1.1 o un nombre de dominio totalmente calificado como cisco.com.
- **Dirección IP remota de WAN (Internet)**: introduzca la dirección IP pública o el nombre de dominio del terminal remoto.
- **Dirección IP local de WAN (Internet)**: introduzca la dirección IP pública o el nombre de dominio del dispositivo.

PASO 5 En los campos **Accesibilidad remota de conexión segura**, introduzca la siguiente información:

- **Dirección IP remota de LAN (red local)**: la dirección de la red privada (LAN) del terminal remoto. Esta es la dirección IP de la red interna en el sitio remoto.
- **Máscara de subred remota de LAN**: la máscara de subred de la red privada (LAN) del terminal remoto.
- **Dirección IP local de LAN (red local)**: la dirección de la red privada (LAN) de la red local. Esta es la dirección IP de la red interna del dispositivo.
- **Máscara de subred local de LAN (red local)**: la máscara de subred de la red privada (LAN) de la red local.

Nota: Las direcciones IP de WAN y LAN remotas no pueden existir en la misma subred. Por ejemplo, una dirección IP de LAN de 192.168.1.100 y una dirección IP local de LAN de 192.168.1.115 ocasionan un conflicto cuando el tráfico se enruta por medio de la VPN. El tercer octeto debe ser diferente para que las direcciones IP se encuentren en subredes diferentes. Por ejemplo, se aceptan una dirección IP de LAN remota de 192.168.1.100 y una dirección IP de LAN local de 192.168.2.100.

PASO 6 Haga clic en **Guardar**.

Visualización de valores predeterminados

Haga clic en **Ver configuración predeterminada** para ver los valores predeterminados de las opciones VPN básicas. Estos valores son propuestos por el consorcio de la VPN y suponen que utiliza una clave previamente compartida o una contraseña, que es conocida tanto para el dispositivo como para el terminal remoto.

Configuración de parámetros avanzados de VPN IPsec de sitio a sitio

Los parámetros avanzados de VPN, como IKE y otras políticas de VPN, controlan la forma en que el dispositivo se inicia y recibe conexiones VPN.

Para configurar los parámetros avanzados de VPN, seleccione **VPN > VPN IPsec de sitio a sitio > Configuración de VPN avanzada**.

Administración de políticas IKE

El protocolo de Intercambio de claves de Internet (IKE) intercambia las claves entre dos hosts IPsec de forma dinámica. Es posible crear políticas de IKE para definir los parámetros de seguridad que se usarán al intercambiar datos con el router remoto a través de la conexión VPN IPsec. Por ejemplo, es posible crear políticas de IKE para definir los parámetros para la autenticación de pares y los algoritmos de cifrado. Asegúrese de que el cifrado, la autenticación y los parámetros de clave-grupo de la política de VPN sean compatibles con la configuración del router remoto.

Para agregar una política de IKE**:**

PASO 1 En la página **Configuración de VPN avanzada**, haga clic en **Agregar fila**.

PASO 2 Escriba un nombre único para la política de IKE para identificarla y administrarla fácilmente.

PASO 3 En el campo **Modo intercambio**, escoja uno de los siguientes modos para la política:

- **Principal**: negocia el túnel con mayor seguridad, pero es más lento.
- **Agresivo**: establece una conexión más rápida, pero con menos seguridad.

PASO 4 En los campos **Identificador local** e **Identificador remoto**, indique si desea identificar al dispositivo y al router remoto mediante su dirección IP verdadera o su dirección IP pública. Si selecciona dirección IP, introduzca la dirección IP verdadera del dispositivo y del router remoto.

PASO 5 En la sección **Parámetros de SA IKE**, configure los parámetros para definir la potencia y el modo para negociar la Asociación de Seguridad (SA) entre el dispositivo y el router remoto:

a. En el campo **Algoritmo de cifrado**, seleccione el algoritmo para cifrar datos.

b. En el campo **Algoritmo de autenticación**, especifique el algoritmo de autenticación del encabezado de la VPN. Asegúrese de que el algoritmo de autenticación esté configurado de forma idéntica en los dos lados del túnel de VPN.

c. En el campo **Clave previamente compartida**, introduzca la clave o contraseña. Asegúrese de que la contraseña no contenga comillas dobles (“).

d. En el campo **Grupo Diffie-Hellman (DH)**, especifique el algoritmo del grupo DH que se usa al intercambiar una clave previamente compartida. El grupo DH establece la potencia del algoritmo en bits. Asegúrese de que el grupo DH esté configurado de forma idéntica en los dos lados de la política IKE.

e. En el campo **Vida útil**, introduzca el intervalo, en segundos, después del cual la asociación de seguridad pierde validez.

f. Para activar la función **Detección del par inactivo**, marque la casilla **Habilitar**. La detección del par inactivo (DPD) se utiliza para detectar si el par está activo. Si el par es detectado como inactivo, el dispositivo elimina las asociaciones de seguridad IKE e IPsec. Si habilita esta función, introduzca además los siguientes parámetros:

- **Retraso de DPD:** el intervalo, en segundos, entre los mensajes DPD R-U-THERE consecutivos. Los mensajes DPD R-U-THERE se envían solo cuando el tráfico IPsec está inactivo.
- **Caducidad de DPD:** el tiempo máximo que el dispositivo debería esperar para recibir una respuesta al mensaje DPD antes de considerar que el par está inactivo.

PASO 6 Haga clic en **Guardar**.

NOTA Si ya tiene una conexión VPN configurada, no puede agregar otra sin eliminar la conexión de VPN existente.

Administración de las políticas VPN

NOTA Antes de crear una política VPN automática, asegúrese de crear una política IKE en base a la cual desea crear la política de VPN automática.

Para administrar las políticas VPN:

PASO 1 Seleccione **VPN > VPN IPsec de sitio a sitio > Configuración de VPN avanzada**. Haga clic en **Agregar fila**.

PASO 2 En la sección **Agregar/Editar configuración de la Política VNP**:

a. En el campo **Nombre de la política**, escriba un nombre único para identificar la política.

b. En el campo **Tipo de política**, elija una de las siguientes opciones:

- **Política automática**: algunos parámetros del túnel de VPN se generan de manera automática. Esto requiere utilizar el protocolo de Intercambio de claves de Internet (IKE) para realizar negociaciones entre los dos terminales de la VPN.
- **Política manual**: todas las configuraciones (incluidas las claves) del túnel de VPN se ingresan en forma manual para punto final. No se requiere ningún servidor de terceros ni ninguna organización.

c. **Punto final remoto:** seleccione el tipo de identificador que desea proporcionar para la puerta de enlace que se encuentra en el punto final remoto: **Dirección IP** o **FQDN** (Nombre de dominio completamente calificado). Introduzca la dirección IP o FQDN.

PASO 3 En las secciones **Selección de tráfico local** y **Selección de tráfico remoto**:

- **En los campos IP local e IP remota**, indique cuántos terminales contendrá la política de VPN:
  - **Simple**: limita la política a un host. Introduzca la dirección IP del host que formará parte de la VPN en el campo **Dirección IP**.
  - **Subred**: permite que una subred completa se conecte con la VPN. Introduzca la dirección de red en el campo **Dirección IP** y la máscara de subred en el campo **Máscara de subred**. Escriba la dirección IP de la subred en el campo **Dirección IP**. Introduzca la máscara de la subred, como 255.255.255.0, en el campo **Máscara de subred**. El campo muestra automáticamente la dirección de subred predeterminada basada en la dirección IP.

NOTA No utilice superposición de subredes para los selectores de tráfico remoto o local. Para el uso de estas subredes, será necesario agregar rutas estáticas en el router y en los hosts que se utilizarán. Evite, por ejemplo:

Selector de tráfico local: 192.168.1.0/24

Selector de tráfico remoto: 192.168.0.0/16

PASO 4 En el tipo de política **Manual**, introduzca los parámetros de la sección **Parámetros de política manual**:

- **SPI entrante, SPI saliente**: introduzca un valor hexadecimal que contenga entre 3 y 8 caracteres, por ejemplo, 0x1234. El Índice de parámetros de seguridad (SPI) identifica la asociación de seguridad de las secuencias de tráfico entrantes y salientes.
- **Algoritmo de cifrado manual:** seleccione el algoritmo utilizado para cifrar los datos.
- **Clave de entrada y clave de salida**: introduzca la clave de cifrado de la política de entrada y salida. La longitud de la clave depende del algoritmo de cifrado elegido:
  - DES: 8 caracteres
  - 3DES: 24 caracteres
  - AES-128: 16 caracteres
  - AES-192: 24 caracteres
  - AES-256: 32 caracteres
- **Algoritmo de integridad manual:** seleccione el algoritmo utilizado para verificar la integridad de los datos.
- **Clave de entrada y clave de salida**: introduzca la clave de integridad (para ESP, con modo de integridad) para la política de entrada y de salida. La longitud de la clave depende del algoritmo elegido:
  - MD5: 16 caracteres
  - SHA-1: 20 caracteres
  - SHA2-256: 32 caracteres

PASO 5 En el tipo de política **Automática**, introduzca los parámetros de la sección **Parámetros de política automática**.

- **Vida útil de SA**: introduzca la duración de la asociación de seguridad en segundos. Una vez que transcurre la cantidad de segundos, la asociación de seguridad se vuelve a negociar. El valor predeterminado es 3600 segundos. El valor mínimo es de 300 segundos.
- **Algoritmo de cifrado:** seleccione el algoritmo utilizado para cifrar los datos.
- **Algoritmo de integridad:** seleccione el algoritmo utilizado para verificar la integridad de los datos.

- **Grupo de claves PFS:** marque la casilla **Habilitar** para habilitar Confidencialidad directa perfecta (PFS) y mejorar la seguridad. Aunque es más lento, este protocolo ayuda a evitar curiosos al garantizar que se realice un intercambio Diffie-Hellman en todas las negociaciones de la fase 2.
- **Grupo DH:** especifique el algoritmo del grupo DH que se usa al intercambiar una clave previamente compartida. El grupo DH establece la potencia del algoritmo en bits. Asegúrese de que el grupo DH esté configurado de forma idéntica en los dos lados de la política IKE.
- **Seleccionar política IKE:** seleccione la política IKE que definirá las características de la negociación de SA.

PASO 6 Haga clic en **Guardar**.

Configuración del servidor VPN IPsec

El uso de VPN IPsec habilita el acceso remoto seguro a los recursos de la empresa, ya que establece un túnel cifrado por Internet. El dispositivo admite los siguientes clientes VPN IPsec:

- TheGreenBow
- ShrewSoft

Configuración del servidor VPN IPsec

Para configurar el servidor VPN IPsec:

PASO 1 Elija **VPN > Configuración básica del servidor> VPN**.

PASO 2 Marque la casilla de verificación **Habilitar servidor**.

PASO 3 En la sección **Fase 1**, configure los parámetros para autenticar los dos terminales VPN entre sí y negociar la asociación de seguridad (SA) IKE a fin de establecer un canal seguro para negociar las SA en la Fase 2.

a. En el campo **Clave previamente compartida**, introduzca la clave previamente compartida, o la contraseña, que será intercambiada entre el dispositivo y el terminal remoto. La contraseña debe contener entre 8 y 49 caracteres.

b. En el campo **Modo intercambio**, escoja uno de los siguientes modos para la conexión VPN IPsec:

- **Principal**: negocia el túnel con mayor seguridad, pero es más lento.
- **Agresivo**: establece una conexión más rápida, pero con menos seguridad.

c. Escoja el **Algoritmo de cifrado** para cifrar los datos, y el **Algoritmo de autenticación** para el encabezado de la VPN. Asegúrese de que el algoritmo de autenticación esté configurado de forma idéntica en el dispositivo y en el terminal remoto.

d. En el campo **Grupo Diffie-Hellman (DH)**, especifique el algoritmo del grupo Diffie-Hellman que se usa al intercambiar una clave previamente compartida. Establece la potencia del algoritmo en bits. Asegúrese de que el grupo DH esté configurado de forma idéntica en el dispositivo y en el terminal remoto.

e. En el campo **Vida útil de SA IKE**, introduzca la duración, en segundos, después de la cual se renegociará la asociación de seguridad para la conexión VPN.

PASO 4 En la sección **Configuración de la Fase 2**, configure los parámetros para negociar la asociación de seguridad (SA) IPsec para el túnel IPsec:

a. En el campo **IP local**, indique cuántos terminales contendrá la política de VPN:

- **Simple**: limita la política a un host. Introduzca la dirección IP del host que formará parte de la VPN en el campo **Dirección IP**.

- **Subred**: permite que una subred completa se conecte con la VPN. Introduzca la dirección de red en el campo **Dirección IP** y la máscara de subred en el campo **Máscara de subred**. Escriba la dirección IP de la subred en el campo **Dirección IP**. Introduzca la máscara de la subred, como 255.255.255.0, en el campo **Máscara de subred**. El campo muestra automáticamente la dirección de subred predeterminada basada en la dirección IP.

b. En el campo **Vida útil de SA IPsec**, introduzca la duración, en segundos, después de la cual se renegociará la asociación de seguridad IPsec para la conexión VPN.

c. Escoja el **Algoritmo de cifrado** para cifrar los datos, y el **Algoritmo de autenticación** para el encabezado de la VPN. Asegúrese de que el algoritmo de autenticación esté configurado de forma idéntica en el dispositivo y en el terminal remoto.

d. Para crear una conexión VPN IPsec más segura, marque la casilla de verificación **Habilitar grupo de claves PFS** para asegurar un nuevo intercambio de claves Diffie-Hellman en la Fase 2. Confidencialidad directa perfecta (PFS) crea otro nivel de seguridad al proteger sus datos con una nueva clave en caso de que la clave de DH generada en la Fase 1 se comprometa en tránsito. Asegúrese de que los dos terminales IPsec tengan habilitado PFS.

PASO 5 Haga clic en **Guardar**.

Configuración de cuentas de usuario VPN IPsec

PASO 1 Seleccione **VPN > Servidor VPN IPsec > Usuario**.

PASO 2 Haga clic en **Agregar fila**.

PASO 3 Ingrese un nombre de usuario y una contraseña.

Recomendamos que la contraseña no sea una palabra del diccionario de ningún idioma y que incluya una combinación de letras (tanto minúsculas como mayúsculas), números y símbolos. La contraseña puede tener hasta 64 caracteres.

PASO 4 Para importar nombres de usuario y contraseñas de un archivo CSV, haga clic en **Importar**. Se muestra la página **Administración > Usuarios**. En la sección **Importar nombre de usuario y contraseña**, haga clic en **Examinar** para buscar el archivo y luego en **Importar**.

PASO 5 Guarde las cuentas de usuario.

Configuración de PPTP

El protocolo de tunelización punto a punto (PPTP) es un protocolo de red que permite la transferencia de datos segura desde un cliente remoto hasta una red comercial al crear una conexión VPN segura en redes públicas, como Internet.

Configuración del servidor PPTP

Para configurar el servidor VPN PPTP:

PASO 1 Elija **VPN** > **Servidor PPTP**.

PASO 2 En la sección **Configuración de servidor PPTP**, configure los parámetros VPN PPTP:

a. Marque la casilla de verificación **Habilitar servidor PPTP**.

b. Escriba la dirección IP del servidor PPTP.

c. Escriba el rango de direcciones IP para los clientes PPTP.

d. Para cifrar los datos que atraviesan la conexión VPN PPTP, marque la casilla de verificación **Habilitar cifrado MPPE**.

PASO 3 Haga clic en **Guardar**.

Creación y administración de usuarios PPTP

Para crear y habilitar usuarios PPTP:

PASO 1 Seleccione **VPN > Servidor PPTP**. En **Tabla de cuenta de usuario PPTP**, haga clic en **Agregar fila**.

PASO 2 Escriba el nombre de usuario y la contraseña que autenticarán al usuario PPTP. Introduzca valores de 4 a 32 caracteres de longitud.

PASO 3 Marque la casilla de verificación **Habilitar** para el usuario.

PASO 4 Para importar nombres de usuario y contraseñas de un archivo CSV, haga clic en **Importar**. Se muestra la página **Administración > Usuarios**. En la sección **Importar nombre de usuario y contraseña**, haga clic en **Examinar** para buscar el archivo y luego en **Importar**.

PASO 5 Guarde las cuentas de usuario.

Configuración de transmisión VPN

La transmisión VPN permite que el tráfico de VPN que se origina en clientes VPN pase por el dispositivo.

Para configurar la transmisión VPN:

PASO 1 Elija **VPN** > **Transmisión VPN**.

PASO 2 Marque la casilla de verificación **Habilitar** para escoger qué tipo de tráfico podrá pasar por el dispositivo.

PASO 3 Haga clic en **Guardar**.

Certificado de SSL

Cisco RV130/RV130W admite la autenticación de certificado para la VPN (*Virtual Private Network*, red privada virtual) IPsec. El certificado de SSL (*Secure Socket Layer*, capa de socket seguro) proporciona el cifrado de datos y autentica el servidor antes de que se establezca la sesión de SSL.

Para administrar el certificado de SSL, haga clic en **VPN > Certificado de SSL.**

- **Tabla de certificados confiables (certificado de la CA [*Certification Authority*, autoridad de certificación])**
  - Haga clic en **Cargar** para ir a la página **Certificados**. Haga clic en **Explorar** para seleccionar un certificado confiable en la unidad local, y haga clic en **Importar**.
- **Certificados propios activos**
  - Haga clic en **Cargar** para ir a la página **Certificados**. Haga clic en **Explorar** para seleccionar un certificado propio activo en la unidad local, y haga clic en **Importar**.
- **Solicitudes de certificados propios**

  Un certificado propio es un certificado emitido por una CA en el que se identifica su dispositivo (o un certificado firmado por la autoridad que certifica, si no desea la protección de identidad de una CA). Para solicitar un certificado propio que será firmado por una CA, puede generar una Solicitud de firma de certificado en la puerta de enlace, para lo cual debe ingresar los parámetros de identificación y enviarlos a la CA para que

coloque su firma. Una vez firmado, el certificado confiable de la CA y el certificado firmado por la CA se cargan para activar el certificado propio que valida la identidad de esta puerta de enlace. A continuación, el certificado propio se utiliza en IPsec con pares para validar la autenticidad de la puerta de enlace.

- **Generar certificado:** para generar una solicitud de certificado de SSL, haga clic en **Generar certificado**; se muestra una nueva página de solicitud con información del certificado.

  Nombre: ingrese el nombre del nuevo certificado.

  Asunto: use el formato 'CN=xxx'; 'CN' debe introducirse en mayúsculas.

  Algoritmo de hash: seleccione el algoritmo de hash correspondiente en la lista desplegable.

  Algoritmo de firma: seleccione el algoritmo de firma correspondiente en la lista desplegable.

  Longitud de la clave de firma: seleccione la longitud de la clave de firma correspondiente en la lista desplegable.

  Dirección IP (opcional): ingrese la dirección IP del router.

  Nombre de dominio (opcional): ingrese el nombre de dominio del router.

  Dirección de correo electrónico (opcional): ingrese la dirección de correo electrónico de los solicitantes.

  - **Exportar para Admin.:** exportar las solicitudes de certificado en la unidad local.

- **Exportar certificado:** para descargar el certificado del router, haga clic en el botón **Exportar para el cliente**.

Haga clic en **Guardar** para guardar la configuración o haga clic en **Cancelar** para recuperar la configuración.

Asistente de instalación de VPN

Para utilizar el Asistente de instalación de VPN:

PASO 1 Haga clic en **VPN > Asistente de instalación de VPN**.

PASO 2 Aparece la ventana del asistente. Siga las instrucciones que se muestran en la pantalla para configurar el dispositivo.

7

Configuración de la calidad de servicio (QoS)

La Calidad de servicio (QoS) asigna prioridad a diversas aplicaciones, usuarios o flujos de datos, o garantiza cierto nivel de rendimiento para un flujo de datos. Estas garantías son importantes cuando la capacidad de la red no es suficiente. Por ejemplo, para aplicaciones multimedia de flujo de datos en tiempo real, como Voz sobre IP, juegos en línea y IP-TV, puesto que estas aplicaciones generalmente requieren de una tasa de bits fija y son sensibles al retardo, y en redes donde la capacidad es un recurso limitado.

Configuración de la administración del ancho de banda

Usted puede usar la función de administración del ancho de banda del dispositivo para administrar el ancho de banda del tráfico que fluye de la red segura (LAN) a la red insegura (WAN).

Configuración del ancho de banda

Usted puede limitar el ancho de banda para reducir la velocidad a la que el dispositivo transmite datos. Puede, además, usar un perfil de ancho de banda para limitar el tráfico saliente, lo que impide que los usuarios LAN consuman todo el ancho de banda de la conexión a Internet.

Para configurar el ancho de banda ascendente y descendente:

PASO 1 Seleccione **QoS** > **Administración del ancho de banda**.

PASO 2 En el campo **Administración del ancho de banda**, marque **Habilitar**. El ancho de banda máximo proporcionado por su ISP aparece en la sección **Ancho de banda**.

PASO 3 En la **Tabla de ancho de banda**, escriba la siguiente información para la interfaz WAN:

Flujo ascendente	Ancho de banda (Kbps) utilizado para enviar datos a Internet.
Flujo descendente	Ancho de banda (Kbps) utilizado para recibir datos de Internet. (solo aplica a la VLAN predeterminada)

PASO 4 Haga clic en **Guardar**.

Configuración de la prioridad de ancho de banda

En la **Tabla de prioridad de ancho de banda**, puede asignar prioridades a servicios para administrar el uso del ancho de banda.

Para configurar la prioridad de ancho de banda:

PASO 1 En la **Tabla de prioridad de ancho de banda**, haga clic en **Agregar fila**.

PASO 2 Ingrese información en los siguientes campos:

Habilitar	Marque esta casilla para habilitar la administración del ancho de banda para este servicio.
Dirección	Seleccione si desea establecer prioridades para el tráfico entrante o saliente.
Categoría	Seleccione si desea establecer prioridades de ancho de banda para un servicio, VLAN/SSID, IP de origen (tráfico entrante) o IP de destino (tráfico saliente).
Servicio	Elija el servicio que desea priorizar.
VLAN/SSID	Seleccione la VLAN o SSID para el que desea establecer la prioridad.
Dirección IP	Si selecciona IP de origen o IP de destino en el campo **Categoría**, escriba la dirección IP y máscara de subred del origen y el destino.
Máscara de subred	

Prioridad	Establezca la prioridad (**baja**, **media** o **alta**) para la categoría seleccionada.
Remarcación	Marque para habilitar la remarcación en el Punto de código de servicios diferenciados (DSCP). Al habilitar esta función, se prioriza el tráfico de red en LAN según la asignación de filas de espera de DSCP en la página **Configuración DSCP**.
DSCP	Introduzca el valor de remarcación para los paquetes de esta red.

PASO 3 Haga clic en **Guardar**.

Para editar la configuración de una entrada en la tabla, marque la casilla correspondiente y haga clic en **Editar**. Cuando haya terminado de hacer cambios, haga clic en **Guardar**.

Para eliminar una entrada de la tabla, marque la casilla correspondiente y haga clic en **Eliminar**. Haga clic en **Guardar**.

Para agregar la definición de un nuevo servicio, haga clic en el botón **Administración de servicio**. Usted puede definir un nuevo servicio con el fin de usarlo para todas las definiciones de firewall y QoS. Consulte **Configuración de la administración de servicios**.

Configuración de QoS basada en puertos

Usted puede configurar los valores de QoS para cada puerto del dispositivo. El admite cuatro colas de prioridad que permiten la priorización del tráfico para cada puerto.

Para configurar los valores de QoS para los puertos del dispositivo:

PASO 1 Seleccione **QoS** > **Configuración de QoS basada en puertos**.

PASO 2 Para cada puerto en la **Tabla de config. de QoS basada en puertos**, escriba esta información:

Modo de confianza	Elija una de las siguientes opciones en el menú desplegable: • **Puerto**: habilita la configuración de QoS basada en puertos. Puede, posteriormente, establecer la prioridad del tráfico para un puerto en particular. Las filas de tráfico pueden tener una prioridad de 1, que es la más baja, y alcanzar una prioridad de 3, que es la más alta. • **DSCP**: punto de código de servicios diferenciados (DSCP). Al habilitar esta función, se prioriza el tráfico de red en LAN según la asignación de filas de espera de DSCP en la página **Configuración DSCP**. • **CoS**: clase de servicio (CoS).
Fila de reenvío de tráfico predeterminada para dispositivos no confiables	Elija un nivel de prioridad (de 1 a 3) para el tráfico saliente.

PASO 3 Haga clic en **Guardar**.

Para restaurar la configuración de QoS basada en puertos predeterminada, haga clic en **Restaurar valor predet.** y guarde los cambios.

Configuración de valores de CoS

Puede usar el enlace a la página Configuración de QoS basada en puertos para asignar los valores de prioridad de CoS a la fila de espera de QoS.

Para asignar valores de prioridad de CoS a la fila de reenvío de tráfico:

PASO 1 Elija **QoS** > **Configuración de CoS**.

PASO 2 Para cada nivel de prioridad de CoS en la **Tabla de config. de CoS**, elija un valor de prioridad en el menú desplegable **Fila de reenvío de tráfico**.

Estos valores marcan tipos de tráfico con mayor o menor prioridad de tráfico según el tipo de tráfico.

PASO 3 Haga clic en **Guardar**.

Para restaurar la configuración de QoS basada en puertos predeterminada, haga clic en **Restaurar valor predet.** y haga clic en **Guardar**.

Configuración de los valores de DSCP

Usted puede usar la página **Configuración DSCP** para configurar la asignación de DSCP a la fila de espera de QoS.

Para configurar la asignación de DSCP a la fila de espera de QoS:

PASO 1 Elija **QoS** > **Configuración DSCP**

PASO 2 Elija si solo incluir valores RFC o todos los valores DSCP en la **Tabla de config. de DSCP**; para ello, haga clic en el botón correspondiente.

PASO 3 Para cada valor DSCP en la **Tabla de config. de DSCP**, elija un nivel de prioridad en el menú desplegable **Cola de espera**.

De esta manera, se asigna el valor DSCP a la fila de espera de QoS seleccionada.

PASO 4 Haga clic en **Guardar**.

Para restaurar la configuración de DSCP predeterminada, haga clic en **Restaurar valor predet.** y **Guardar**.

8

Administración del dispositivo

Configuración de propiedades del dispositivo

Asigne al dispositivo un nombre y un nombre de dominio para asegurarse de que otros dispositivos lo identifiquen fácilmente.

Para configurar las propiedades del dispositivo:

PASO 1 Seleccione **Administración > Propiedades del dispositivo**.

PASO 2 En el campo **Nombre de host**, introduzca un nombre para identificar al dispositivo de forma exclusiva en la red. Por ejemplo, RTR141.

PASO 3 En el campo **Nombre de dominio**, introduzca el dominio donde se encuentra el dispositivo. Por ejemplo, abcbusiness.com. Si desconoce el nombre de dominio de la organización, comuníquese con el administrador de red.

PASO 4 Guarde los cambios.

Configuración de complejidad de la contraseña

Puede imponer requisitos mínimos de complejidad de la contraseña para cambios de contraseña.

Para configurar los valores de complejidad de la contraseña:

PASO 1 Elija **Administración** > **Seguridad de la contraseña**.

PASO 2 En el campo **Configuración de complejidad de la contraseña**, marque **Habilitar**.

PASO 3 Configure los valores de complejidad de la contraseña:

Longitud mínima de la contraseña	Escriba la longitud mínima de la contraseña (de 0 a 64 caracteres).
Cantidad mínima de clases de caracteres	Escriba un número que represente una de las siguientes clases de caracteres: • Letras mayúsculas • Letras minúsculas • Números • Caracteres especiales disponibles en un teclado estándar De manera predeterminada, las contraseñas deben incluir caracteres de, al menos, tres de estas clases.
La contraseña nueva debe ser distinta de la actual	Marque **Habilitar** para solicitar que las contraseñas nuevas difieran de la actual.
Vencimiento de la contraseña	Marque **Habilitar** para que las contraseñas caduquen después de un tiempo especificado.
Tiempo de vencimiento de la contraseña	Escriba el número de días después de los cuales caduca la contraseña (de 1 a 365). El valor predeterminado es 180 días.

PASO 4 Haga clic en **Guardar**.

Configuración de cuentas de usuario

El dispositivo admite dos cuentas de usuario para administrar y visualizar configuraciones: un usuario administrativo (nombre de usuario y contraseña predeterminados: cisco) y un usuario invitado (nombre de usuario predeterminado: invitado).

La cuenta de invitado tiene acceso de solo lectura. Usted puede configurar y cambiar el nombre de usuario y la contraseña para la cuenta de administrador y la cuenta de invitado.

Para configurar las cuentas de usuario:

PASO 1 Elija **Administración** > **Usuarios**.

PASO 2 En el campo **Activación de cuenta**, marque las casillas de las cuentas que desea activar. (La cuenta de administrador debe estar activa).

PASO 3 (Opcional) Para editar la cuenta de administrador, marque **Editar config. de administrador** en **Config. de cuenta de administrador**. Para editar la cuenta de invitado, marque **Editar config. de invitado** en Config. de invitado. Introduzca la siguiente información:

Nuevo nombre de usuario	Escriba un nuevo nombre de usuario.
Antigua contraseña	Escriba la contraseña actual.
Nueva contraseña	Escriba la nueva contraseña. Recomendamos que la contraseña no sea una palabra del diccionario de ningún idioma y que incluya una combinación de letras (tanto minúsculas como mayúsculas), números y símbolos. La contraseña puede tener hasta 64 caracteres.
Vuelva a escribir la nueva contraseña	Vuelva a escribir la nueva contraseña.

PASO 4 Haga clic en **Guardar**.

Importación de cuentas de usuario

Es posible importar varios usuarios al mismo tiempo mediante un archivo CSV.

Asegúrese de que los datos del archivo CSV estén organizados tal como se muestra en las siguientes tablas:

TIPO	NOMBRE DE USUARIO	CONTRASEÑA
Admin.	Admin123	Admin123

TIPO	NOMBRE DE USUARIO	CONTRASEÑA
Invitado	Invitado123	Invitado123

TIPO	NOMBRE DE USUARIO	CONTRASEÑA	HABILITAR
PPTP	PPTP-user-1	12345678	habilitar
PPTP	PPTP-user-2	345123678	inhabilitar

TIPO	NOMBRE DE USUARIO	CONTRASEÑA
Servidor VPN	vpn-user-1	12345678
Servidor VPN	vpn-user-2	33245678

TIPO	NOMBRE DE USUARIO	CONTRASEÑA	TIEMPO_DE_ACCESO
guestnet	guestnet-user-1	12345678	1440
guestnet	guestnet-user-2	33245678	60

NOTA Los nombres de las columnas distinguen entre mayúsculas y minúsculas. No cambie el orden ni los nombres de las columnas.

Para importar cuentas de usuario desde un archivo CSV:

PASO 1 En el campo **Importar nombre de usuario y contraseña**, haga clic en **Examinar**.

PASO 2 Ubique el archivo y haga clic en **Abrir**.

PASO 3 Haga clic en **Importar**.

Configuración del valor del tiempo de espera de la sesión

El valor del tiempo de espera es la cantidad de minutos de inactividad que pueden transcurrir hasta que finalice la sesión del administrador de dispositivos. Usted puede configurar el tiempo de espera para las cuentas de administrador e invitado.

Para configurar el tiempo de espera de la sesión:

PASO 1 Elija **Administración** > **Tiempo de espera de la sesión**.

PASO 2 En el campo **Caducidad por inactividad de admin.**, escriba la cantidad de minutos, en número, que pueden transcurrir hasta que una sesión caduque por inactividad. Elija **Nunca** para permitir que el administrador se mantenga permanentemente conectado.

PASO 3 En el campo **Caducidad por inactividad de invitado**, escriba la cantidad de minutos, en número, que pueden transcurrir hasta que una sesión caduque por inactividad. Elija **Nunca** para permitir que el administrador se mantenga permanentemente conectado.

PASO 4 Haga clic en **Guardar**.

Configuración del protocolo de administración de red simple (SNMP)

El protocolo de administración de red simple (SNMP) le permite supervisar y administrar el router desde un administrador SNMP. El SNMP proporciona un medio remoto para supervisar y controlar los dispositivos de red y para administrar configuraciones, la obtención de estadísticas, el rendimiento y la seguridad.

Configuración de información del sistema SNMP

NOTA Para poder usarlo, instale el software SNMP en su computadora. El dispositivo admite solo SNMPv3 para la administración SNMP y SNMPv1/2/3 para mensajes trampa SNMP.

Para habilitar el SNMP:

PASO 1 Elija **Administración** > **SNMP**.

PASO 2 Marque **Habilitar** para habilitar el SNMP.

PASO 3 Marque la opción **Habilitar** para **Permitir acceso del usuario mediante Internet** o **Permitir acceso del usuario mediante VPN.**

PASO 4 Seleccione la versión de SNMP en el campo **Modo**.

PASO 5 Escriba esta información:

SysContact	Introduzca el nombre de la persona de contacto para este dispositivo. Por ejemplo, el administrador de la red.
SysLocation	Indique la ubicación física del dispositivo. Por ejemplo, Rack nro. 2, 4.º piso.
SysName	Introduzca un nombre para identificar fácilmente al dispositivo. Por ejemplo, RTR 141.

PASO 6 Haga clic en **Guardar**.

PASO 7 Haga clic en **Ver registros** para ver la tabla de registro del sistema.

Edición de usuarios SNMPv3

Usted puede configurar parámetros SNMPv3 para las dos cuentas de usuario predeterminadas del dispositivo (administrador e invitado).

Para configurar los valores de SNMPv3:

PASO 1 Elija **Administración** > **SNMP**.

PASO 2 En **Config. de usuario SNMPv3**, configure los siguientes valores:

Nombre de usuario	Seleccione la cuenta que desea configurar (**administrador** o **invitado**).

Privilegio de acceso	Se muestran los privilegios de acceso de la cuenta de usuario seleccionada.
Nivel de seguridad	Elija el nivel de seguridad de SNMPv3: **Sin autenticación ni privilegios**: no se requiere ninguna autenticación ni privacidad. **Autenticación y sin privilegios**: se requiere solamente algoritmo y contraseña de autenticación. **Autenticación y privilegios**: se requiere algoritmo y contraseña de autenticación/privacidad.
Servidor de algoritmo de autenticación	Seleccione el tipo de algoritmo de autenticación (**MD5** o **SHA**).
Contraseña de autenticación	Escriba la contraseña de autenticación.
Algoritmo de privacidad	Elija el tipo de algoritmo de privacidad (**DES** o **AES**).
Contraseña de privacidad	Escriba la contraseña de privacidad.

PASO 3 Haga clic en **Guardar**.

Configuración de trampas SNMP

Los campos de la sección **Configuración de trampas SNMP** le permiten configurar un agente SNMP al que el dispositivo le envía mensajes trampa (notificaciones).

Para configurar las trampas:

PASO 1 Elija **Administración** > **SNMP**.

PASO 2 En **Configuración de trampas**, configure los siguientes valores:

Dirección IP	Escriba la dirección IP del administrador SNMP o agente de mensajes trampa.

Puerto	Escriba el puerto de trampas SNMP de la dirección IP a la que se enviarán los mensajes trampa.
Comunidad	Escriba la cadena de comunidad a la que pertenece el agente. La mayoría de los agentes están configurados para escuchar trampas en la comunidad pública.
Versión de SNMP	Seleccione la versión de SNMP: **v1**, **v2c** o **v3**.
Nivel de gravedad de trampas SNMP	Seleccione el nivel de gravedad en el cual el dispositivo debe enviar mensajes trampa.

PASO 3 Haga clic en **Guardar**.

Uso de herramientas de diagnóstico

El dispositivo ofrece varias herramientas de diagnóstico para ayudarlo a solucionar problemas de red.

- **Herramientas de red**
- **Configuración de duplicación de puertos**

Herramientas de red

Utilice herramientas de red para resolver problemas de la red.

Uso de PING

Usted puede usar la utilidad PING para probar la conectividad entre el router y otro dispositivo en la red. Puede, además, usar la herramienta Ping para probar la conectividad a Internet al hacer ping a un nombre de dominio totalmente calificado (como www.cisco.com).

Para usar PING:

PASO 1 Elija **Administración** > **Diagnósticos** > **Herramientas de red**.

PASO 2 En el campo **Dirección IP/Nombre de dominio**, escriba la dirección IP del dispositivo o un nombre de dominio totalmente calificado, como www.cisco.com, al que hacer ping.

PASO 3 Haga clic en **Ping**. Aparecen los resultados de ping, que le indican si el dispositivo está accesible.

Uso de Traceroute

La utilidad Traceroute muestra todos los routers presentes entre la dirección IP de destino y este router. El router muestra hasta 30 saltos (routers intermedios) entre este router y el destino.

Para usar Traceroute:

PASO 1 Elija **Administración** > **Diagnósticos** > **Herramientas de red**.

PASO 2 En el campo **Dirección IP/Nombre de dominio**, escriba la dirección IP que desea rastrear.

PASO 3 Haga clic en **Traceroute**. Aparecen los resultados de Traceroute.

Realización de una búsqueda de DNS

Usted puede usar la herramienta de búsqueda para encontrar la dirección IP del host (por ejemplo, un servidor web, FTP o de correo) en Internet.

Para recuperar la dirección IP de un servidor web, FTP o de correo, o de cualquier otro servidor en Internet, escriba el nombre de Internet en el cuadro de texto y haga clic en **Buscar**. Si el host o el dominio que se escribió existe, verá una respuesta con la dirección IP. El mensaje “Host desconocido” indica que el nombre de Internet especificado no existe.

Para usar la herramienta de búsqueda:

PASO 1 Elija **Administración** > **Diagnósticos** > **Herramientas de red**.

PASO 2 En el campo **Nombre de Internet**, escriba el nombre de Internet del host.

PASO 3 Haga clic en **Buscar**. Aparecen los resultados de nslookup.

Configuración de duplicación de puertos

La duplicación de puertos supervisa el tráfico de red al enviar copias de todos los paquetes entrantes y salientes de un puerto a un puerto de supervisión. La duplicación de puertos se puede usar como una herramienta de diagnóstico o depuración, especialmente cuando se rechaza un ataque o visualiza el tráfico de usuario desde LAN hasta WAN para ver si los usuarios acceden a información o sitios web a los que no deben acceder.

El host de LAN (equipo) debe usar una dirección IP estática para evitar problemas con la duplicación de puertos. Los arrendamientos DHCP pueden vencer para un host LAN y pueden hacer que la duplicación de puertos falle si la dirección IP estática no está configurada para el host LAN.

Para configurar la duplicación de puertos:

PASO 1 Elija **Administración** > **Diagnósticos** > **Duplicación de puertos**.

PASO 2 En el campo **Duplicar origen**, seleccione los puertos que desea duplicar.

PASO 3 En el menú desplegable **Duplicar puerto**, elija un puerto para duplicar. Si usa un puerto como duplicado, no lo use para ningún otro tráfico.

PASO 4 Haga clic en **Guardar**.

Configuración del registro y del correo electrónico

Configure registros para monitorear la actividad que indique el estado y el rendimiento del dispositivo.

Configuración de los valores de registro

Para configurar el registro:

PASO 1 Elija **Administración** > **Registro** > **Config. de registro**.

PASO 2 En el campo **Modo de registro**, marque **Habilitar**.

PASO 3 Marque la casilla de verificación **Habilitar alerta de correo electrónico** para que el dispositivo envíe correos electrónicos de alerta a una dirección específica ante eventos o comportamientos que puedan afectar el rendimiento, funcionamiento y

seguridad del dispositivo, o bien para fines de depuración. Marque la casilla correspondiente para habilitar las alertas de correo electrónico ante los siguientes eventos:

WAN activada/desactivada	Envía un correo electrónico cuando el enlace WAN está desactivado y envía otro correo electrónico cuando el enlace vuelve a activarse.
Túnel VPN IPsec de sitio a sitio activado/desactivado	Envía un correo electrónico cuando el túnel VPN IPsec de sitio a sitio se desactiva y envía otro correo electrónico cuando el túnel vuelve a activarse.
Sobrecarga de la CPU	Envía un correo electrónico de alerta cuando el uso de la CPU supera al umbral y envía otro correo electrónico de alerta cuando el uso retoma la normalidad.
Inicio del sistema	Envía un alerta de correo electrónico cuando el dispositivo se está iniciando.
Nuevo firmware disponible	Envía un alerta de correo electrónico cuando hay un nuevo firmware para el dispositivo.

PASO 4 Haga clic en **Agregar fila**.

PASO 5 Configure los siguientes valores:

Servidor de registro remoto	Escriba la dirección IP del servidor de registro que conservará registros.

Gravedad de registro para correo electrónico y registro local	Seleccione la gravedad de los eventos para los que desea conservar los registros y enviarlos a una dirección de correo electrónica específica. Se incluirán automáticamente todos los tipos de registro que sean más graves que el tipo de registro seleccionado; no podrán excluirse. Por ejemplo, si selecciona registros de errores, también se seleccionarán Emergencia, Alerta y Crítico. Los niveles de gravedad de los eventos se detallan de mayor gravedad a menor gravedad: • **Emergencia**: el sistema no se puede utilizar. • **Alerta**: se necesita acción. • **Crítico**: el sistema está en condición crítica. • **Error**: el sistema está en condición de error. • **Advertencia**: se presentó una advertencia del sistema. • **Notificación**: el sistema está funcionando correctamente, pero se presentó un aviso del sistema. • **Información**: información de dispositivos. • **Depuración**: información detallada de eventos. Si selecciona esta gravedad de registros, se genera una extensa lista de registros no recomendable durante el funcionamiento normal del router.
Habilitar	Para habilitar estos valores de registro, marque esta casilla.

PASO 6 Haga clic en **Guardar**.

Para editar una entrada en la **Tabla de config. de registro**, seleccione la entrada y haga clic en **Editar**. Realice sus cambios y luego haga clic en **Guardar**.

Configuración del envío de registros por correo electrónico

Usted puede configurar el dispositivo para que envíe registros por correo electrónico. Se recomienda configurar una cuenta de correo electrónico aparte para enviar y recibir registros.

Primero debe configurar la gravedad de los registros que desea capturar; consulte **Configuración de los valores de registro**.

Pasos para configurar el envío de registros por correo electrónico:

PASO 1 Elija **Administración** > **Registro** > **Config. de correo elec.**

PASO 2 Para habilitar el envío de registros por correo electrónico, marque **Habilitar**.

Aparece la gravedad de registro de correo electrónico mínima que desea capturar. Para realizar cambios, haga clic en **Configurar gravedad**.

PASO 3 Configure los siguientes valores:

Dir. de serv. de correo elec.	Escriba la dirección del servidor SMTP. Este es el servidor de correo asociado con la cuenta de correo electrónico que ha configurado (por ejemplo, mail.companyname.com).
Puerto de serv. de correo elec.	Escriba el puerto del servidor SMTP. Si su proveedor de correo electrónico requiere un puerto especial para correo electrónico, ingréselo aquí. De lo contrario, use el predeterminado (25).
Dir. de correo elec. de devolución	Ingrese una dirección de correo electrónico de devolución a la que el dispositivo enviará mensajes si no se pueden entregar los registros del router enviados a la dirección de correo electrónico establecida.

Enviar a dir. de correo elec. (1)	Escriba una dirección de correo electrónico a la cual enviar registros (por ejemplo, logging@companyname.com).
Enviar a dir. de correo elec. (2) (opcional)	
Enviar a dir. de correo elec. (3) (opcional)	
Cifrado de correo electrónico	Seleccione SSL o TSL como método de cifrado de correo electrónico. Seleccione Deshabilitar si no desea usar ningún método de cifrado de correo electrónico.
Autenticación con servidor SMTP	Si el servidor SMTP (correo) solicita autenticación antes de aceptar conexiones, elija el tipo de autenticación en el menú desplegable: **Ninguna**, **INICIO DE SESIÓN**, **SENCILLO** y **CRAM-MD5**.
Nombre de usuario de autent. de c. elec.	Escriba el nombre de usuario de autenticación de correo electrónico (por ejemplo, logging@companyname.com).
Contraseña de autent. de c. elec.	Escriba la contraseña de autenticación de correo electrónico (por ejemplo, la contraseña que se usó para ingresar a la cuenta de correo electrónico que configuró para enviar registros).
Prueba de autent. de c. elec.	Haga clic en **Prueba** para realizar la prueba de autenticación de correo electrónico.

PASO 4 En la sección **Enviar registro c. elec. según prog.**, configure los siguientes valores:

Unidad	Elija la unidad de tiempo para los registros (**Nunca**, **Por hora**, **Por día** o **Por semana**). No se envían registros si elige la opción **Nunca**.
Día	Si opta por una programación por semana para el envío de registros, elija un día de la semana en el que enviar los registros.

Hora	Si opta por una programación por día o por semana para el envío de registros, elija la hora del día a la que enviar los registros.

PASO 5 Haga clic en **Guardar**.

Configuración de Bonjour

Bonjour es un protocolo de detección y anuncio de servicios. En el dispositivo, Bonjour solamente anuncia los servicios predeterminados configurados en el dispositivo cuando Bonjour está habilitado.

Para habilitar Bonjour:

PASO 1 Elija **Administración** > **Bonjour**.

PASO 2 Marque **Habilitar** para habilitar Bonjour.

PASO 3 A fin de habilitar Bonjour para una VLAN incluida en la **Tabla de control de interfaz de Bonjour**, marque la casilla de verificación correspondiente **Habilitar Bonjour**.

Usted puede habilitar Bonjour en VLAN específicas. Al habilitar Bonjour en una VLAN, los dispositivos presentes en la VLAN pueden detectar servicios Bonjour disponibles en el router (como HTTP/HTTPS).

Por ejemplo, si la ID de una VLAN es 2, los dispositivos y hosts presentes en VLAN 2 no pueden detectar servicios Bonjour que se ejecutan en el router a menos que Bonjour esté habilitado para VLAN 2.

PASO 4 Haga clic en **Guardar**.

Configuración de los valores de fecha y hora

Usted puede configurar su zona horaria, ajustar o no valores del horario de verano y con cuál servidor de Protocolo de hora en la red (NTP) se debe sincronizar la fecha y la hora. El router luego obtiene la información de su fecha y hora del servidor NTP.

Para configurar valores de NTP y hora:

PASO 1 Elija **Administración** > **Configuración de hora**. Se muestra la hora actual.

PASO 2 Ingrese información en los siguientes campos:

Zona horaria	Seleccione su zona horaria en relación con la hora del meridiano de Greenwich (GMT).
Ajustar valores del horario de verano	Si su región lo admite, marque la casilla **Ajustar valores del horario de verano**. Esta casilla de verificación está atenuada si hace clic en **Manual** en el campo **Configurar fecha y hora**.
Modo horario de verano	Si selecciona **Por fecha**, introduzca la fecha específica en la que comienza el modo horario de verano. Si selecciona **Recurrente**, introduzca el mes, la semana, el día de la semana y la hora en que comienza el modo horario de verano. Ingrese la información apropiada en los campos **Desde** y **Hasta**.
Desplazamiento del horario de verano	Elija el desplazamiento de la Hora Universal Coordinada (UTC) en el menú desplegable.
Configurar fecha y hora	Seleccione si desea configurar la fecha y la hora del dispositivo de forma manual o automática. Si selecciona **Manual**, introduzca la fecha y la hora en los campos **Escribir fecha y hora**.
Servidor NTP	Para usar los servidores NTP predeterminados, haga clic en el botón **Usar predeterminado**. Para usar un servidor NTP específico, haga clic en **Servidor NTP definido por usuario** y escriba el nombre de dominio totalmente calificado o la dirección IP de los servidores NTP en los dos campos disponibles.

PASO 3 Haga clic en **Guardar**.

Copia de respaldo y restauración del sistema

Usted puede hacer copias de respaldo de valores de configuración personalizada para una restauración posterior o restaurar la configuración personalizada a partir de una copia de respaldo anterior en la página **Administración >Config. de respaldo/restauración**.

Cuando el firewall funciona tal como se configuró, usted puede hacer una copia de respaldo de la configuración para una posterior restauración. Durante la copia de respaldo, la configuración se guarda en forma de archivo en su computadora. La configuración del firewall se puede restaurar a partir de este archivo.

PRECAUCIÓN Durante una operación de restauración, no intente conectarse a Internet, desactivar el firewall, apagar la computadora ni usar el firewall hasta que se haya completado la operación, que debería llevar un minuto aproximadamente. Una vez que la luz de prueba se apague, espere unos segundos más antes de usar el firewall.

Respaldo de los valores de configuración

Para realizar una copia de respaldo de la configuración o restaurarla:

PASO 1 Elija **Administración** > **Config. de respaldo/restauración**.

PASO 2 Seleccione la configuración que desea borrar o de la que quiere una copia de respaldo:

Configuración de inicio	Seleccione esta opción para descargar la configuración de inicio. La configuración de inicio es la configuración en ejecución más actual que usa el dispositivo. Si se ha perdido la configuración de inicio del router, use esta página para copiar la configuración de respaldo en la configuración de inicio y para que toda la información de la configuración previa permanezca intacta. Usted puede descargar la configuración de inicio a otros dispositivos RV130/RV130W para una fácil implementación.

Configuración de duplicado	Seleccione esta opción si el dispositivo debe realizar una copia de respaldo de la configuración de inicio después de 24 horas de operación sin ninguna modificación en la configuración de inicio.
Configuración de respaldo	Seleccione esta opción para hacer una copia de respaldo de los valores de la configuración actual.

PASO 3 Para descargar un archivo de respaldo de acuerdo con la opción de configuración seleccionada, haga clic en **Descargar**.

De manera predeterminada, el archivo (startup.cfg, mirror.cfg o backup.cfg) se descarga en la carpeta Descargas; por ejemplo, C:\Documents and Settings\admin\My Documents\Downloads\.

PASO 4 Para borrar la configuración seleccionada, haga clic en **Borrar**.

Restauración de los valores de configuración

Para restaurar un archivo de configuración guardado anteriormente:

PASO 1 Elija **Administración** > **Config. de respaldo/restauración**.

PASO 2 En el campo Carga de configuración, seleccione la configuración que desea cargar (**Configuración de inicio** o **Configuración de respaldo**).

PASO 3 Haga clic en **Examinar** para ubicar el archivo.

PASO 4 Seleccione el archivo y haga clic en **Abrir**.

PASO 5 Haga clic en **Iniciar la carga**.

El dispositivo carga el archivo de configuración y usa los valores que contiene para actualizar la configuración de inicio. Posteriormente, el dispositivo se reinicia y usa la nueva configuración.

Copia de los valores de configuración

Copie la configuración de inicio en la configuración de respaldo para asegurarse de contar con una copia de respaldo en caso de que olvide su nombre de usuario y contraseña y no pueda acceder al Administrador de dispositivos. Para ingresar nuevamente al Administrador de dispositivos, restablezca el dispositivo para que vuelva a los valores predeterminados de fábrica.

El archivo de configuración de respaldo permanece en la memoria y permite que la información de la configuración de la que se hizo copia de respaldo se copie en la configuración de inicio, que restablece todos los valores.

Para copiar una configuración (por ejemplo, para copiar una configuración de inicio en la configuración de respaldo):

PASO 1 Elija **Administración** > **Config. de respaldo/restauración**.

PASO 2 En el campo **Copiar**, elija las configuraciones de origen y de destino en los menús desplegables.

PASO 3 Haga clic en **Iniciar la copia**.

Generación de una clave de cifrado

El router le permite generar una clave de cifrado para proteger los archivos de respaldo.

Para generar una clave de cifrado:

PASO 1 Elija **Administración** > **Config. de respaldo/restauración**.

PASO 2 Haga clic en **Mostrar config. avanzada**.

PASO 3 En la casilla, escriba la frase simiente para generar la clave.

PASO 4 Haga clic en **Guardar**.

Actualización del Firmware o cambio de idioma

Puede actualizar el firmware a una versión más reciente o cambiar el idioma del router con la página **Administración** > **Actualización del firmware/idioma**.

PRECAUCIÓN Durante una actualización del firmware, no intente conectarse a Internet, desactivar el dispositivo, apagar la computadora ni interrumpir el proceso de ninguna manera hasta que se haya completado la operación, que dura un minuto aproximadamente, incluido el proceso de reinicio. La interrupción del proceso de actualización en momentos específicos cuando se escribe en la memoria flash puede dañarla e inutilizar el router.

Cómo actualizar el firmware

Pasos para actualizar el router a una versión más reciente del firmware:

PASO 1 Elija **Administración** > **Actualización del firmware/idioma**.

PASO 2 (Opcional) Haga clic en **Descargar** para descargar la última versión del firmware.

PASO 3 En el campo **Tipo de archivo**, haga clic en el botón **Imagen de firmware**.

PASO 4 Haga clic en **Examinar** para ubicar y seleccionar el firmware descargado.

PASO 5 (Opcional) Para restablecer el dispositivo de modo que vuelva a los valores predeterminados de fábrica una vez actualizado el firmware, marque **Restablecer toda la configuración a los valores predet. de fábrica**.

PRECAUCIÓN Al restablecer el dispositivo de modo que vuelva a los valores predeterminados de fábrica, se borran todos sus parámetros de configuración.

PASO 6 Haga clic en **Iniciar actualización**.

Una vez validada la imagen del firmware nuevo, la nueva imagen se guarda en la memoria flash y el router se reinicia automáticamente con el firmware nuevo.

PASO 7 Elija **Estado** > **Resumen del sistema** para asegurarse de que el router instaló la nueva versión del firmware.

Cambio del idioma

Para cambiar el idioma en el dispositivo:

PASO 1 Elija **Administración** > **Actualización del firmware/idioma**.

PASO 2 En el campo **Tipo de archivo**, haga clic en el botón **Archivo de idioma**.

PASO 3 Haga clic en **Examinar** para ubicar y seleccionar el archivo de idioma.

PASO 4 (Opcional) Para restaurar la configuración del dispositivo a los valores predeterminados de fábrica, seleccione **Restablecer toda la configuración a los valores predet. de fábrica**.

PASO 5 Haga clic en **Iniciar actualización**.

Reinicio del dispositivo

Para reiniciar el router:

PASO 1 Elija **Administración** > **Reiniciar**.

PASO 2 Haga clic en **Reiniciar**.

Restauración de los valores predeterminados de fábrica

PRECAUCIÓN Durante una operación de restauración, no intente conectarse a Internet, desactivar el router, apagar la computadora ni usar el router hasta que se haya completado la operación, que debería llevar un minuto aproximadamente. Una vez que la luz de prueba se apague, espere unos segundos más antes de usar el router.

Para restaurar los valores predeterminados de fábrica en el router:

PASO 1 Elija **Administración** > **Restaurar valores predet. de fábrica**.

PASO 2 Haga clic en **Predeterminado**.

9

Filtrado web

El filtrado web es una característica del router que le permite administrar el acceso a sitios web no apropiados. Puede mejorar una red que ya es segura y promover la productividad en el lugar de trabajo al analizar las solicitudes de acceso web de un cliente para determinar si se permite o rechaza ese sitio web.

Es posible que el administrador cuente con pautas sobre la seguridad general de la red, la Internet de las cosas o reglas que desee implementar en una red personalizada para un departamento en particular. El administrador puede crear reglas programadas personalizadas y asignarlas a las listas de excepción para, por ejemplo, otorgar acceso a sitios web específicos a usuarios específicos en horarios específicos.

Configuración del filtrado web

Esta sección pretende demostrar cómo configurar el filtrado web en el router y resaltar la importancia de esta característica. Para habilitar y configurar el filtrado web en el router, siga estos pasos:

PASO 1 Haga clic en **Web Filtering** (Filtrado web).

PASO 2 En la sección Web Filtering, seleccione una de las siguientes opciones:

- **Always On** (Habilitado siempre): el filtrado web está siempre habilitado
- **Scheduled** (Programado): establezca un programa para implementar el filtrado web
- **Always Off** (Deshabilitado siempre): se deshabilita el filtrado web

NOTA De manera predeterminada, el filtrado web se configura en Deshabilitado siempre.

PASO 3 En la sección Web Reputation (Reputación web), marque **Enable** (Habilitar) para habilitar el filtrado de acuerdo con la categoría de filtrado seleccionada.

PASO 4 Haga clic en Categories (Categorías) y seleccione una de las siguientes opciones para administrar y aplicar filtros.

- **Low** (Bajo): se habilita el contenido y la seguridad para adultos. Seleccione y marque las opciones disponibles para personalizar su filtro.
- **Medium** (Medio): se habilita el contenido y la seguridad para adultos, ilegal/cuestionable. Seleccione y marque las opciones disponibles para personalizar su filtro.
- **High** (Alto): se habilita el contenido y la seguridad para adultos, comercial/inversión, entretenimiento, ilegal/cuestionable, recursos de TI, estilo de vida/cultura. Seleccione y marque las opciones disponibles para personalizar su filtro.
- **Custom** (Personalizado): no se permiten los valores predeterminados para el filtrado web personalizado.

PASO 5 Haga clic en **Save** (Guardar) y **Back** (Atrás) para regresar a la página Filter (Filtro) para continuar con la configuración.

PASO 6 Marque **Enable HTTPS Filtering** (Habilitar filtrado HTTPS) para filtrar el contenido de acuerdo con la dirección IP de la Web en lugar de la URL. Será posible acceder a los sitios web con HTTP o HTTPS asegurados. Para bloquear los sitios web independientemente de una URL asegurada, no marque **Enable HTTPS Filtering**.

NOTA El filtrado HTTPS se basa en la dirección IP del servidor web en lugar de en la URL dado que esta está cifrada. En general, múltiples sitios web utilizarán la misma dirección IP del servidor web. Si ese es el caso, el router no bloqueará esa página si hay múltiples categorías de sitios web relacionadas con esa dirección IP. Sin embargo, el router bloqueará la página si hay contenido para adultos en esa dirección IP, o si se sabe que la dirección IP aloja o distribuye malware.

PASO 7 Si seleccionó **Scheduled** como opción de filtrado web, aparecerá la tabla Schedule (Programa). En la tabla Schedule, haga clic en **Add Row** (Agregar fila) para crear una regla o política programada para implementar.

PASO 8 En la tabla Schedule, ingrese un nombre y una descripción en el campo Name (Nombre) y Description (Descripción).

PASO 9 Luego, marque el día o los días de la semana para habilitar el filtro en esos días.

PASO 10 A continuación, con el reloj de 24 horas, ingrese la hora para que la regla entre en vigencia.

PASO 11 Por último, marque **Active** (Activo) para habilitar la regla programada.

NOTA No existe un límite para el número de reglas a implementar.

PASO 12 Haga clic en **Save.**

PASO 13 (Opcional). Cree una lista para permitir, rechazar o excluir sitios web/contenido en el proceso de filtrado. Seleccione el tipo entre una de las siguientes opciones:

- **White List** (Lista blanca): haga clic en **Add Row**, seleccione **Domain Name** (Nombre de dominio) o **Keyword** (Palabra clave) en la lista del menú desplegable. Luego, ingrese un valor para identificar esta política.
- **Black List** (Lista negra): haga clic en **Add Row**, seleccione **Domain Name** o **Keyword** en la lista del menú desplegable. Luego, ingrese un valor para identificar esta política.
- **Exclusion List** (Lista de exclusión): haga clic en **Add Row**, seleccione **Domain Name** o **Keyword** en la lista del menú desplegable. Luego, ingrese un valor para identificar esta política.

PASO 14 Para editar o eliminar una política de filtrado web, marque la política en la lista y haga clic en **Edit** (Editar) o **Delete** (Eliminar).

PASO 15 Haga clic en **Save.**

A

Cómo seguir

Asistencia técnica	
Comunidad de Soporte Cisco	www.cisco.com/go/smallbizsupport
Soporte y recursos de Cisco	www.cisco.com/go/smallbizhelp
Contactos de asistencia técnica telefónica	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Descargas de Firmware Cisco	www.cisco.com/cisco/software/navigator.html?i=!ch Seleccione un enlace para descargar el firmware. No se debe iniciar sesión.
Solicitudes de código abierto para Cisco	www.cisco.com/go/smallbiz_opensource_request
Central para socios Cisco (deberá iniciar sesión como socio)	www.cisco.com/web/partners/sell/smb
Documentación del producto	
Router VPN inalámbrico multifunción Cisco RV130/RV130W	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html

Para conocer los resultados relacionados de EU Lot 26, consulte www.cisco.com/go/eu-lot26-results.