345138

GUÍA DE ADMINISTRACIÓN

Guía de Administración para Cisco Small Business 300 Series Managed Switch Versión 1.4

Índice

2

Introducción

Esta sección contiene una introducción a la configuración basada en Web y abarca los siguientes temas:

- **Inicio de la utilidad de configuración basada en la Web**
- **Configuración del dispositivo de inicio rápido**
- **Convenciones para la asignación de nombres a las interfaces**
- **Navegación por las ventanas**

Inicio de la utilidad de configuración basada en la Web

En esta sección se describe cómo navegar por la utilidad de configuración de switch basada en la Web.

Si está usando un bloqueador de ventanas emergentes, asegúrese de desactivarlo.

Restricciones de los navegadores

Si utiliza interfaces IPv6 en su estación de administración, use la dirección IPv6 global en lugar de la dirección IPv6 local de enlace para acceder al dispositivo desde el navegador.

Inicio de la utilidad de configuración

Para abrir la utilidad de configuración basada en la Web:

PASO 1 Abra un navegador Web.

PASO 2 Ingrese la dirección IP del dispositivo que está configurando en la barra de direcciones en el navegador y, luego, presione **Intro**.

NOTA Cuando el dispositivo usa la dirección IP predeterminada de fábrica 192.168.1.254, el indicador LED de alimentación parpadea continuamente. Cuando el dispositivo usa una dirección IP asignada por DHCP, o una dirección IP estática configurada por el administrador, el indicador LED de alimentación permanece encendido.

Inicio de sesión

El nombre de usuario predeterminado es **cisco** y la contraseña predeterminada es **cisco**. La primera vez que inicie sesión con el nombre de usuario y la contraseña predeterminados, deberá ingresar una nueva contraseña.

NOTA Si no ha definido anteriormente un idioma para la GUI (Graphical User Interface, interfaz gráfica de usuario), el idioma de la página de inicio de sesión se determinará según el idioma que requiera el navegador y los idiomas configurados en el dispositivo. Por ejemplo, si el navegador requiere chino y este idioma se ha cargado en el dispositivo, la página de inicio de sesión aparecerá automáticamente en chino. Si no se ha cargado tal idioma al dispositivo, la página de inicio de sesión aparecerá en inglés.

Los idiomas cargados al dispositivo poseen un idioma y un código de país (en-US, en-GB, etc.). Para que la página de inicio de sesión se vea automáticamente en un idioma determinado, según los requisitos del navegador, tanto el idioma como el código de país de la solicitud del navegador deben coincidir con el idioma cargado en el dispositivo. Si la solicitud del navegador posee únicamente el código de idioma sin el código de país (por ejemplo: fr). Se tomará el primer idioma con un código de idioma que coincida (sin código de país que coincida, por ejemplo: fr_CA).

Para iniciar sesión en la utilidad de configuración de dispositivos:

PASO 1 Introduzca el nombre de usuario y la contraseña. La contraseña puede contener hasta 64 caracteres ASCII. Las reglas de complejidad de la contraseña se describen en **Configuración de reglas de complejidad de la contraseña**.

PASO 2 Si no está usando el inglés, seleccione el idioma que desea en el menú desplegable *Idioma*. Para agregar un idioma nuevo al dispositivo o para actualizar el idioma actual, consulte **Actualización/copia de seguridad del firmware/idioma**.

PASO 3 Si esta es la primera vez que inicia sesión con el ID de usuario predeterminado (**cisco**) y la contraseña predeterminada (**cisco**) o su contraseña ha caducado, se abre la página Cambiar contraseña. Consulte **Vencimiento de contraseña** para obtener información adicional.

PASO 4 Seleccione si desea **Deshabilitar aplicación de complejidad de la contraseña** o no. Para obtener más información sobre la complejidad de la contraseña, consulte la sección **Configuración de reglas de complejidad de la contraseña**.

PASO 5 Ingrese la contraseña y haga clic en **Aplicar**.

Cuando el intento de inicio de sesión se realiza correctamente, se abre la página Introducción.

En caso de que haya ingresado un nombre de usuario incorrecto o una contraseña incorrecta, se mostrará un mensaje de error y la página Inicio sesión permanecerá abierta en pantalla. Si tiene problemas para iniciar sesión, consulte la sección **Inicio de la utilidad de configuración** en la Guía de administración para obtener más información.

Seleccione **No mostrar esta página durante el inicio** para impedir que la página Introducción se muestre cada vez que inicie sesión en el sistema. Si selecciona esta opción, se abre la página Resumen del sistema, en lugar de la página Introducción.

HTTP/HTTPS

Puede abrir una sesión HTTP (no segura) al hacer clic en **Iniciar sesión**, o bien puede abrir una sesión HTTPS (segura) al hacer clic en **Explorador seguro (HTTPS)**. Se le pedirá que apruebe el inicio de sesión con una clave RSA predeterminada y la sesión HTTPS se abrirá.

NOTA No es necesario ingresar el nombre de usuario o la contraseña antes de hacer clic en el botón **Explorador seguro (HTTPS).**

Para obtener información sobre la configuración de HTTP, consulte la sección **Servidor SSL**.

Vencimiento de contraseña

La página Nueva contraseña se muestra en los siguientes casos:

- La primera vez que accede al dispositivo con el nombre de usuario **cisco** y la contraseña **cisco** predeterminados. Esta página lo obliga a reemplazar la contraseña predeterminada de fábrica.
- Cuando la contraseña vence, esta página lo obliga a seleccionar una contraseña nueva.

Cierre de sesión

De forma predeterminada, la aplicación cierra sesión después de diez minutos de inactividad. Usted puede cambiar este valor predeterminado como se describe en la sección **Definición de la caducidad de sesión por inactividad**.

PRECAUCIÓN A menos que la configuración en ejecución se copie en la configuración de inicio, si se reinicia el dispositivo se perderán todos los cambios realizados desde la última vez que se guardó el archivo. Guarde la configuración en ejecución en la configuración de inicio antes de cerrar la sesión, a fin de conservar los cambios que hizo durante esta sesión.

Una X roja intermitente a la izquierda del enlace de la aplicación **Guardar** indica que los cambios en la configuración en ejecución aún no se han guardado en el archivo de configuración de inicio. La intermitencia se puede deshabilitar al hacer clic en el botón **Deshabilitar Guardar icono intermitente** en la página Copiar/guardar configuración.

Si el dispositivo detecta automáticamente un dispositivo, por ejemplo, un teléfono IP (consulte **¿Qué es un Smartport?**), y configura el puerto correctamente para el dispositivo. Los comandos de configuración se escriben en el archivo Configuración en ejecución. Esto hace que el icono Guardar comience a parpadear cuando usted se conecta, aunque no haya hecho ninguna modificación en la configuración.

Al hacer clic en **Guardar**, aparece la página Copiar/guardar configuración. Para guardar el archivo Configuración en ejecución, cópielo en el archivo de configuración de inicio. Luego de guardarlo, el ícono de la X de color rojo y el enlace de aplicación Guardar ya no se muestran.

Para cerrar sesión, haga clic en **Cerrar sesión** en la esquina superior derecha de cualquier página. El sistema cierra la sesión del dispositivo.

Cuando se agota el tiempo de espera o usted cierra sesión intencionalmente, se muestra un mensaje y se abre la página Iniciar sesión, con un mensaje que indica el estado de sesión cerrada. Después de iniciar sesión, la aplicación vuelve a la página inicial.

La página inicial que se muestra depende de la opción "No mostrar esta página durante el inicio" en la página Introducción. Si no seleccionó esta opción, la página inicial es la página Introducción. Si seleccionó esta opción, la página inicial es la página Resumen del sistema.

Configuración del dispositivo de inicio rápido

Para simplificar la configuración del dispositivo a través de la navegación rápida, la página Introducción proporciona enlaces a las páginas que se utilizan habitualmente.

Categoría	Nombre del enlace (en la página)	Página vinculada
	Cambiar servicios y aplicaciones de administración	Página Servicios TCP/UDP
	Cambiar dirección IP del dispositivo	Página Interfaz IPv4
	Crear VLAN	Página Crear VLAN
	Configurar los valores del puerto	Página Configuración de puertos
Estado del dispositivo	Resumen del sistema	Página Resumen del sistema
	Estadísticas del puerto	Página Interfaz
	Estadísticas RMON	Página Estadísticas
	Ver registro	Página Memoria RAM
Acceso rápido	Cambiar contraseña del dispositivo	Página Cuentas de usuario

Categoría	Nombre del enlace (en la página)	Página vinculada
	Actualizar software del dispositivo	Página Actualización/Copia de seguridad de firmware/Idioma
	Configuración del dispositivo de copia de seguridad	Página Descarga/Copia de seguridad de configuración/ Registro
	Crear ACL basada en MAC	Página ACL basada en MAC
	Crear ACL basada en IP	Página ACL basada en IPv4
	Configurar QoS	Página Propiedades de QoS
	Configurar duplicación de puertos	Página Duplicación de puertos y VLAN

En la página de introducción hay dos vínculos activos que lo llevan a las páginas web de Cisco para ofrecerle más información. Al hacer clic en el enlace **Asistencia técnica**, ingresa a la página de asistencia técnica del producto del dispositivo y, al hacer clic en el enlace **Foros**, ingresa a la página Comunidad de asistencia técnica de Small Business.

Convenciones para la asignación de nombres a las interfaces

Dentro de la GUI, las interfaces se designan mediante la concatenación de los siguientes elementos:

- **Tipo de interfaz:** En diversos tipos de dispositivos se encuentran los siguientes tipos de interfaces:
  - **Fast Ethernet (10/100 bits)**: aparecen como **FE**.
  - **Puertos Gigabit Ethernet (10/100/1000 bits)**: aparecen como **GE**.
  - **LAG (Canal de puerto)**: aparecen como **LAG**.
  - **VLAN**: aparecen como **VLAN.**
  - **Túnel**: aparecen como **Túnel.**
- **Número de interfaz Puerto, LAG, túnel o ID de VLAN**

Navegación por las ventanas

En esta sección, se describen las funciones de la utilidad de configuración de switch basada en la Web.

Encabezado de la aplicación

El encabezado de la aplicación aparece en todas las páginas. Proporciona los siguientes enlaces de las aplicaciones:

Nombre del enlace de la aplicación	Descripción
	Una X roja intermitente a la izquierda del enlace de la aplicación **Guardar** indica que se han realizado cambios en la configuración en ejecución que aún no se han guardado en el archivo de configuración de inicio. La X roja intermitente se puede deshabilitar en la página Copiar/ guardar configuración. Haga clic en **Guardar** para mostrar la página Copiar/ guardar configuración. Para guardar el archivo de configuración en ejecución, cópielo en el tipo de archivo de configuración de inicio en el dispositivo. Luego de guardarlo, el ícono de la X de color rojo y el enlace de aplicación Guardar ya no se muestran. Cuando el dispositivo se reinicia, se copia el tipo de archivo de configuración de inicio en la configuración en ejecución y se configuran los parámetros del dispositivo según los datos de la configuración en ejecución.
Nombre de usuario	Muestra el nombre del usuario que inició sesión en el dispositivo. El nombre de usuario predeterminado es **cisco**. (La contraseña predeterminada es **cisco**).

Nombre del enlace de la aplicación	Descripción
Menú de idiomas	Este menú ofrece las siguientes opciones: ▪ **Seleccionar idioma:** seleccione uno de los idiomas que aparecen en el menú. Este idioma será el idioma de la utilidad de configuración basada en la Web. ▪ **Descargar idioma:** agrega un nuevo idioma al dispositivo. ▪ **Eliminar idioma:** elimine el segundo idioma del dispositivo. El primer idioma (Inglés) no puede eliminarse. ▪ **Depuración:** para fines de traducción. Si selecciona esta opción, todas las etiquetas de la utilidad de configuración basada en la Web desaparecen y las reemplazan los ID de las cadenas que se corresponden con los ID del archivo de idioma. **NOTA** Para actualizar un archivo de idioma, use la página Actualización/Copia de seguridad de firmware/Idioma.
Cerrar sesión	Haga clic para cerrar sesión en la utilidad de configuración de switch basada en la Web.
Acerca de	Haga clic para ver el nombre del dispositivo y el número de versión del dispositivo.
Ayuda	Haga clic para ver la ayuda en línea.
	El icono Estado de alerta de SYSLOG aparece cuando se registra un mensaje SYSLOG, arriba del nivel de gravedad *crítico*. Haga clic en este icono para abrir la página Memoria RAM. Después de que acceda a esta página, el ícono de estado de alerta de SYSLOG ya no se muestra. Para ver la página cuando no hay un mensaje de SYSLOG activo, haga clic en **Estado y estadísticas** > **Ver registro** > **Memoria RAM**.

Botones de administración

En la siguiente tabla, se describen los botones más usados que aparecen en distintas páginas en el sistema.

Nombre del botón	Descripción
	Utilice el menú desplegable para configurar la cantidad de entradas por página.
	Indica un campo obligatorio.
Agregar	Haga clic para mostrar la página Añadir relacionada y agregue una entrada a la tabla. Introduzca la información y haga clic en **Aplicar** para guardar los cambios en la configuración en ejecución. Haga clic en **Cerrar** para volver a la página principal. Haga clic en **Guardar** para mostrar la página Copiar/guardar configuración y guardar la configuración en ejecución en el tipo de archivo de configuración de inicio en el dispositivo.
Aplicar	Haga clic para aplicar los cambios en la configuración en ejecución en el dispositivo. Si el dispositivo se reinicia, la configuración en ejecución se pierde, a menos que se guarde en el tipo de archivo de configuración de inicio u otro tipo de archivo. Haga clic en **Guardar** para mostrar la página Copiar/guardar configuración y guardar la configuración en ejecución en el tipo de archivo de configuración de inicio en el dispositivo.
Cancelar	Haga clic para restablecer los cambios realizados en la página.
Borrar todos los contadores de interfaz	Haga clic para borrar los contadores estadísticos para todas las interfaces.
Borrar contadores de interfaz	Haga clic para borrar los contadores estadísticos para la interfaz seleccionada.
Borrar registros	Borra los archivos de registro.
Borrar tabla	Borra las entradas de la tabla.

Nombre del botón	Descripción
Cerrar	Vuelve a la página principal. Si hay cambios que no se aplicaron a la configuración en ejecución, aparece un mensaje.
Copiar configuración	Por lo general, una tabla contiene una o más entradas con los valores de configuración. En lugar de modificar cada entrada individualmente, es posible modificar una entrada y luego copiarla en varias, como se describe a continuación. 1. Seleccione la entrada que desea copiar. Haga clic en **Copiar configuración** para mostrar la ventana emergente. 2. Ingrese los números de la entrada de destino en el campo **a**. 3. Haga clic en **Aplicar** para guardar los cambios y haga clic en **Cerrar** para volver a la página principal.
Eliminar	Una vez que haya seleccionado una entrada en la tabla, haga clic en **Eliminar** para borrarla.
Detalles	Haga clic para mostrar los detalles asociados con la entrada seleccionada.
Editar	Seleccione la entrada y haga clic en **Editar**. Aparece la página Editar y puede modificar la entrada. 1. Haga clic en **Aplicar** para guardar los cambios en la configuración en ejecución. 2. Haga clic en **Cerrar** para volver a la página principal.
Ir	Ingrese los criterios de filtrado de consulta y haga clic en **Ir a**. Se muestran los resultados en la página.
Refresh	Haga clic en **Actualizar** para actualizar los valores del contador.
Probar	Haga clic en **Prueba** para realizar las pruebas relacionadas.

3

Estado y estadísticas

En esta sección, se describe cómo ver las estadísticas del dispositivo.

Abarca los siguientes temas:

- **Resumen del sistema**
- **Interfaces Ethernet**
- **Estadísticas Etherlike**
- **Estadísticas de GVRP**
- **Estadísticas de EAP 802.1X**
- **Estadísticas de ACL**
- **Utilización de la TCAM**
- **Estado**
- **RMON**
- **Ver registro**

Resumen del sistema

Consulte **Configuración del sistema**.

Interfaces Ethernet

En la página Interfaz, se muestran las estadísticas del tráfico por puerto. Se puede seleccionar la velocidad de actualización de la información.

Esta página es útil para analizar la cantidad de tráfico que se envía y se recibe y su dispersión (unidifusión, multidifusión y difusión).

Para mostrar las estadísticas de Ethernet o establecer la velocidad de actualización, haga lo siguiente:

PASO 1 Haga clic en **Estado y estadísticas** > **Interfaz**.

PASO 2 Ingrese los parámetros.

- **Interfaz**: seleccione el tipo de interfaz y la interfaz específica para la que desea visualizar las estadísticas de Ethernet.
- **Vel. de actualización**: seleccione el período de tiempo que transcurre antes de que se actualicen las estadísticas de Ethernet de la interfaz.

En el área Recibir estadísticas se muestra información acerca de los paquetes entrantes.

- **Total de bytes (octetos)**: octetos recibidos, incluidos octetos FCS (Secuencia de verificación de tramas) y paquetes defectuosos, pero sin incluir bits de entramado.
- **Paquetes de unidifusión**: paquetes de unidifusión válidos recibidos.
- **Paquetes de multidifusión**: paquetes de multidifusión válidos recibidos.
- **Paquetes de transmisión**: paquetes de transmisión válidos recibidos.
- **Paquetes con errores**: paquetes con errores recibidos.

En el área Transmitir estadísticas se muestra información acerca de los paquetes salientes.

- **Total de bytes (octetos)**: octetos transmitidos, incluidos octetos FCS y paquetes defectuosos, pero sin incluir bits de entramado.
- **Paquetes de unidifusión**: paquetes de unidifusión válidos transmitidos.
- **Paquetes de multidifusión**: paquetes de multidifusión válidos transmitidos.
- **Paquetes de transmisión**: paquetes de transmisión válidos transmitidos.

Para borrar o ver los contadores de estadísticas:

- Haga clic en **Borrar contadores de interfaz** para borrar los contadores de la interfaz visualizada.
- Haga clic en **Ver todas las estadísticas de las interfaces** para ver todos los puertos en una sola página.

Estadísticas Etherlike

En la página Etherlike, se muestran las estadísticas por puerto según la definición estándar de MIB (Management Information Base, base de información de administración) Etherlike. Se puede seleccionar la velocidad de actualización de la información. En esta página se proporciona información más detallada sobre los errores en la capa física (capa 1), que pueden interrumpir el tráfico.

Para ver las estadísticas de Ethernet o establecer la velocidad de actualización, haga lo siguiente:

PASO 1 Haga clic en **Estado y estadísticas** > **Etherlike**.

PASO 2 Ingrese los parámetros.

- **Interfaz**: seleccione el tipo de interfaz y la interfaz específica para la que desea visualizar las estadísticas de Ethernet.
- **Vel. de actualización**: seleccione el tiempo que transcurre antes de que se actualicen las estadísticas Etherlike.

Se muestran los campos para la interfaz seleccionada.

- **Errores de secuencia de Verificación de Tramas (FCS)**: tramas recibidas que no pasaron la CRC (verificación cíclica de redundancia).
- **Tramas de colisión simple**: tramas que se incluyeron en una colisión simple, pero que se transmitieron correctamente.
- **Colisiones tardías**: colisiones que se detectaron luego de los primeros 512 bits de datos.
- **Colisiones excesivas**: transmisiones rechazadas debido a colisiones excesivas.
- **Paquetes de tamaño excesivo**: paquetes mayores de 2000 octetos recibidos.
- **Errores internos de recepción de MAC**: tramas rechazadas debido a errores del receptor.
- **Tramas de pausa recibidas**: tramas de pausa de control de flujo recibidas.
- **Tramas de pausa transmitidas**: tramas de pausa de control de flujo transmitidas de la interfaz seleccionada.

Para borrar los contadores de estadísticas:

- Haga clic en **Borrar contadores de interfaz** para borrar los contadores de las interfaces seleccionadas.
- Haga clic en **Ver todas las estadísticas de las interfaces** para ver todos los puertos en una sola página.

Estadísticas de GVRP

En la página GVRP, se muestra información sobre las tramas GVRP (GARP VLAN Registration Protocol, protocolo de registro de VLAN de GARP) que se enviaron o se recibieron de un puerto. GVRP es un protocolo de red de capa 2 basado en normas, para la configuración automática de información de VLAN en los switches. Se define en la enmienda 802.1ak de 802.1Q-2005.

Las estadísticas de GVRP para un puerto solo se muestran si GVRP está habilitado globalmente y en el puerto. Consulte la página GVRP.

Para ver las estadísticas de GVRP o establecer la velocidad de actualización, haga lo siguiente:

PASO 1 Haga clic en **Estado y estadísticas** > **GVRP**.

PASO 2 Ingrese los parámetros.

- **Interfaz**: seleccione la interfaz específica para la que desea visualizar las estadísticas de GVRP.
- **Velocidad de actualización**: seleccione el período de tiempo que transcurre antes de que se actualice la página de estadísticas de GVRP.

En el bloque Contador de atributos se muestran los contadores para varios tipos de paquetes por interfaz.

- **Unión vacía**: paquetes GVRP de Unión vacía recibidos/transmitidos.
- **Vacíos**: paquetes GVRP vacíos recibidos/transmitidos.
- **Dejar vacíos**: paquetes GVRP Dejar vacíos recibidos/transmitidos.
- **Unir**: paquetes GVRP Unir recibidos/transmitidos.
- **Dejar**: paquetes GVRP Dejar recibidos/transmitidos.
- **Dejar todos**: paquetes GVRP Dejar todos recibidos/transmitidos.

En la sección GVRP Estadísticas de error se muestran los contadores de errores GVRP.

- **ID de protocolo no válido**: errores de ID de protocolo no válido.
- **Tipo de atributo no válido**: errores de ID de atributo no válido.
- **Valor de atributo no válido**: errores de valor de atributo no válido.
- **Longitud de atributo no válida**: errores de longitud de atributo no válida.
- **Evento no válido**: eventos no válidos.

Para borrar los contadores de estadísticas:

- Haga clic en **Borrar contadores de interfaz** para borrar los contadores seleccionados.
- Haga clic en **Ver todas las estadísticas de las interfaces** para ver todos los puertos en una sola página.

Estadísticas de EAP 802.1X

En la página 802.1x EAP, se muestra información detallada sobre las tramas EAP (Extensible Authentication Protocol, protocolo de autenticación extensible) que se enviaron o se recibieron. Para configurar la función 802.1X, consulte la página Propiedades de 802.1X.

Para ver las estadísticas de EAP o establecer la velocidad de actualización, haga lo siguiente:

PASO 1 Haga clic en **Estado y estadísticas** > **802.1x EAP**.

PASO 2 Seleccione la **interfaz** para el que desean consultarse las estadísticas.

PASO 3 Seleccione la **Velocidad de actualización (**período de tiempo) que transcurre antes de que se actualicen las estadísticas de EAP.

Se muestran los valores para la interfaz seleccionada.

- **Tramas EAPOL recibidas**: tramas EAPOL válidas recibidas en el puerto.
- **Tramas EAPOL transmitidas**: tramas EAPOL válidas transmitidas por el puerto.
- **Tramas de inicio EAPOL recibidas**: las tramas de inicio EAPOL recibidas en el puerto.
- **Tramas de desconexión EAPOL recibidas**: las tramas de desconexión EAPOL recibidas en el puerto.
- **Tramas EAP de ID/de respuesta recibidas**: tramas EAP de ID/de respuesta recibidas en el puerto.
- **Tramas EAP de respuesta recibidas**: tramas EAP de respuesta recibidas por el puerto (diferentes a las tramas Resp/ID).
- **Tramas EAP de pedido/ID transmitidas**: tramas EAP de pedido/ID transmitidas por el puerto.
- **Tramas EAP de pedido transmitidas**: tramas EAP de pedido transmitidas por el puerto.
- **Tramas EAPOL no válidas recibidas**: las tramas EAPOL no reconocidas que se recibieron en este puerto.
- **Tramas de error de longitud EAP recibidas**: tramas EAPOL con una longitud de cuerpo del paquete no válida que se recibieron en este puerto.
- **Última versión de trama EAPOL**: número de versión del protocolo asociado con la última trama EAPOL recibida.
- **Último origen de trama EAPOL**: dirección MAC de origen asociada con la última trama EAPOL recibida.

Para borrar los contadores de estadísticas:

- Haga clic en **Borrar contadores de interfaz** para borrar los contadores de las interfaces seleccionadas.
- Haga clic en **Actualizar** para actualizar los contadores de las interfaces seleccionadas.
- Haga clic en **Ver todas las estadísticas de las interfaces** para borrar los contadores de todas las interfaces.

Estadísticas de ACL

Cuando se activa la función de registro de ACL, se genera un mensaje SYSLOG informativo para los paquetes que coinciden con las reglas ACL.

Para ver las interfaces en las que se reenvían o rechazan los paquetes en base a las ACL:

PASO 1 Haga clic en **Estado y estadísticas** > **ACL**.

PASO 2 Seleccione la **Velocidad de actualización** (tiempo en segundos) que pasa antes de que se actualice la página. Se crea un nuevo grupo de interfaces para cada período.

Se muestran las interfaces en las que se reenvían o rechazan los paquetes en base a reglas ACL.

Para administrar los contadores de estadísticas:

- Haga clic en **Actualizar** para restablecer los contadores.
- Haga clic en **Borrar contadores** para borrar los contadores de todas las interfaces.

Utilización de la TCAM

La arquitectura del dispositivo utiliza una TCAM (Ternary Content Addressable Memory, memoria direccionable de contenido ternario) para admitir acciones de paquete a la velocidad de cable.

TCAM incluye las reglas generadas por aplicaciones, como las ACL (Access Control Lists, listas de control de acceso), QoS (Quality of Service, calidad de servicio), enrutamiento IP y las reglas creadas por el usuario.

Algunas aplicaciones asignan reglas después de iniciarse. Además, los procesos que se inician durante el inicio del sistema utilizan algunas de sus reglas durante el proceso de arranque.

Para ver la utilización de la TCAM, haga clic en **Estado y estadísticas** > **Utilización de TCAM**.

En la página Utilización de TCAM, se muestran los siguientes campos:

- **Entradas máximas de la TCAM para IPv4 y no IP**: cantidad máxima de entradas de TCAM disponibles.
- **Enrutamiento IPv4**
  - **En uso**: cantidad de entradas de TCAM que se utilizan para el enrutamiento IPv4.
  - **Máximo**: cantidad de entradas de TCAM disponibles que se pueden utilizar para el enrutamiento IPv4.
- **Reglas no IP**
  - **En uso**: cantidad de entradas de TCAM que se utilizan para las reglas no IP.
  - **Máximo**: cantidad de entradas de TCAM disponibles que se pueden utilizar para las reglas no IP.

Estado

Consulte **Estado**.

RMON

RMON (Remote Networking Monitoring, monitoreo remoto de redes) que permite que un agente SNMP en el dispositivo monitoree de manera proactiva las estadísticas del tráfico durante un período determinado y envíe trampas a un administrador SNMP. El agente SNMP local compara los contadores de tiempo real con umbrales predefinidos y genera alarmas, sin necesidad de realizar consultas a través de una plataforma de administración SNMP central. Este es un mecanismo eficaz para la administración proactiva, siempre que los umbrales correctos estén establecidos en la base lineal de su red.

RMON disminuye el tráfico entre el administrador y el dispositivo, ya que el administrador SNMP no debe realizar consultas frecuentes de información al dispositivo, y permite que el administrador obtenga informes de estado oportunos, ya que el dispositivo informa los eventos a medida que ocurren.

Con esta función, puede realizar las siguientes acciones:

- Ver las estadísticas actuales (ya que se eliminaron los valores de contadores). También puede reunir los valores de estos contadores en un período de tiempo y, luego, ver la tabla de los datos recolectados, donde cada conjunto recolectado está representado en una línea de la ficha *Historial*.

- Definir cambios interesantes en valores de contadores, como "alcanzó un cierto número de colisiones tardías" (define la alarma), y, luego, especificar la acción que se realizará cuando ocurra este evento (registro, trampa o registro y trampa).

Estadísticas RMON

En la página Estadísticas, se muestra información detallada sobre los tamaños de los paquetes e información sobre los errores de la capa física. La información mostrada es acorde a la norma RMON. Un paquete de tamaño excesivo se define como una trama Ethernet con los siguientes criterios:

- La longitud del paquete es mayor que el tamaño de la unidad de recepción máxima (MRU) en bytes.
- No se detectó un evento de colisión.
- No se detectó un evento de colisión tardía.
- No se detectó un evento de error de Rx recibido.
- El paquete tiene una CRC válida.

Para ver las estadísticas de RMON o establecer la velocidad de actualización, haga lo siguiente:

PASO 1 Haga clic en **Estado y estadísticas > RMON > Estadísticas**.

PASO 2 Seleccione la **interfaz** para la que desea ver las estadísticas de Ethernet.

PASO 3 Seleccione la **Velocidad de actualización**, que es el período de tiempo que transcurre antes de que se actualicen las estadísticas de la interfaz.

Se muestran las siguientes estadísticas para la interfaz seleccionada.

- **Bytes recibidos**: octetos recibidos, incluidos los paquetes defectuosos y octetos FCS, pero no los bits de entramado.
- **Eventos descartados**: paquetes que se descartaron.
- **Paquetes recibidos**: paquetes correctos recibidos, incluidos los paquetes de multidifusión y de transmisión.
- **Paquetes de transmisión recibidos**: paquetes de transmisión válidos recibidos. Este número no incluye paquetes de multidifusión.
- **Paquetes de multidifusión recibidos**: paquetes de multidifusión válidos recibidos.
- **Errores de alineación y CRC**: errores de CRC y alineación que ocurrieron.
- **Paquetes más pequeños de lo normal**: paquetes más pequeños de lo normal (menos de 64 octetos) que se recibieron.

- **Paquetes de tamaño excesivo**: paquetes de tamaño excesivo (más de 2000 octetos) que se recibieron.
- **Fragmentos**: fragmentos que se recibieron (paquetes con menos de 64 octetos, sin incluir los bits de entramado, pero incluidos los octetos FCS).
- **Jabbers (trama sup.)**: paquetes recibidos que tenían más de 1632 octetos. Este número no incluye los bits de trama, pero incluye los octetos FCS que tienen una FCS (secuencia de verificación de tramas) defectuosa con un número integral de octetos (error FCS) o una FCS defectuosa con un número no integral de octetos (error de alineación). Un paquete jabber se define como una trama Ethernet que satisface los siguientes criterios:
  - La longitud de datos del paquete es mayor que la MRU.
  - El paquete tiene una CRC no válida.
  - No se detectó un evento de error de Rx recibido.
- **Colisiones**: colisiones recibidas. Si las tramas jumbo están habilitadas, el umbral de tramas jabber se eleva al tamaño máximo de tramas jumbo.
- **Tramas de 64 bytes**: tramas recibidas que contienen 64 bytes.
- **Tramas de 65 a 127 bytes**: tramas recibidas que contienen entre 65 y 127 bytes.
- **Tramas de 128 a 255 bytes**: tramas recibidas que contienen entre 128 y 255 bytes.
- **Tramas de 256 a 511 bytes**: tramas recibidas que contienen entre 256 y 511 bytes.
- **Tramas de 512 a 1023 bytes**: tramas recibidas que contienen entre 512 y 1023 bytes.
- **Tramas de 1024 bytes o más**: tramas que contienen entre 1024 y 2000 bytes y tramas jumbo que se recibieron.

Para borrar los contadores de estadísticas:

- Haga clic en **Borrar contadores de interfaz** para borrar los contadores de las interfaces seleccionadas.
- Haga clic en **Ver todas las estadísticas de las interfaces** para ver todos los puertos en una sola página.

Historial RMON

La función RMON permite controlar las estadísticas por interfaz.

En la página Tabla de control de historial, se definen la frecuencia de muestreo, la cantidad de muestras que se guardarán y el puerto del que se recolectan los datos.

Después del muestreo y del almacenamiento de datos, estos aparecen en la página Tabla de historial que se puede ver al hacer clic en **Tabla de historial**.

Pasos para ingresar la información de control RMON:

PASO 1 Haga clic en **Estado y estadísticas > RMON > Historial**. Los campos que se muestran en esta página se definen en la página Añadir historial RMON a continuación. El único campo que se encuentra en esta página y no está definido en la página Añadir es el siguiente:

- **Número de muestras actual**: por norma, RMON no puede otorgar todas las muestras solicitadas, sino que limita el número de muestras por solicitud. Por lo tanto, este campo representa el número de muestras que se otorga a la solicitud que es igual o menor al valor solicitado.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **Nueva entrada en historial**: muestra el número de la nueva entrada de la tabla Historial.
- **Interfaz de origen**: seleccione el tipo de interfaz del que se van a tomar las muestras del historial.
- **N.° máximo de muestras para guardar**: ingrese el número de muestras que se guardará.
- **Intervalo de muestreo**: ingrese el tiempo en segundos en que se recolectan muestras de los puertos. El intervalo del campo oscila entre 1 y 3600.
- **Propietario**: ingrese el usuario o la estación de RMON que solicitó la información de RMON.

PASO 4 Haga clic en **Aplicar**. Se agrega la entrada a la página Tabla de control de historial y se actualiza el archivo de configuración en ejecución.

PASO 5 Haga clic en **Tabla de historial** (descrita a continuación) para ver las estadísticas reales.

Tabla del historial de RMON

En la página Tabla de historial, se muestran los muestreos de red estadísticos específicos de una interfaz. Las muestras se configuraron en la tabla de control de historial descrita anteriormente.

Para ver las estadísticas del historial de RMON haga lo siguiente:

PASO 1 Haga clic en **Estado y estadísticas** > **RMON** > **Historial**.

PASO 2 Haga clic en la **Tabla de historial**.

PASO 3 En el menú desplegable **N.º de entrada de historial**, puede seleccionar, de manera optativa, el número de entrada de la muestra que se visualizará.

Se muestran los campos para la muestra seleccionada.

- **Propietario**: propietario de la entrada de la tabla del historial.
- **N.º de muestra**: se tomaron las estadísticas de esta muestra.
- **Eventos descartados**: paquetes descartados debido a falta de recursos de red durante el intervalo de muestreo. Usted puede no representar el número exacto de paquetes descartados, sino el número de veces que se detectaron paquetes descartados.
- **Bytes recibidos**: octetos recibidos, incluidos los paquetes defectuosos y octetos FCS, pero no los bits de entramado.
- **Paquetes recibidos**: paquetes recibidos, incluidos los paquetes defectuosos, de multidifusión y de difusión.
- **Paquetes de transmisión**: paquetes de transmisión válidos sin incluir los paquetes de multidifusión.
- **Paquetes de multidifusión**: paquetes de multidifusión válidos recibidos.
- **Errores de alineación y CRC**: errores de CRC y alineación que ocurrieron.
- **Paquetes más pequeños de lo normal**: paquetes más pequeños de lo normal (menos de 64 octetos) que se recibieron.
- **Paquetes de tamaño excesivo**: paquetes de tamaño excesivo (más de 2000 octetos) que se recibieron.
- **Fragmentos**: fragmentos (paquetes con menos de 64 octetos) que se recibieron, sin incluir los bits de entramado, pero incluidos los octetos FCS.
- **Jabbers**: total de paquetes recibidos que tenían más de 2000 octetos. Este número no incluye los bits de trama, pero incluye los octetos FCS que tienen una FCS (secuencia de verificación de tramas) defectuosa con un número integral de octetos (error FCS) o una FCS defectuosa con un número no integral de octetos (error de alineación).
- **Colisiones**: colisiones recibidas.
- **Utilización**: porcentaje de tráfico actual en la interfaz comparado con el tráfico máximo que admite la interfaz.

Control de eventos RMON

Puede controlar los eventos que activan una alarma y el tipo de notificación que se produce. Esto se realiza de la siguiente manera:

- **Página Eventos**: configura lo que ocurre cuando se activa una alarma. Este evento puede ser cualquier combinación de registros o trampas.
- **Página Alarmas**: configura los eventos que activan una alarma.

Para definir eventos RMON haga lo siguiente:

PASO 1 Haga clic en **Estado y estadísticas > RMON** > **Eventos**.

En esta página se muestran los eventos definidos anteriormente.

Los campos de esta página están definidos por el cuadro de diálogo *Agregar eventos RIMON*, a excepción del campo Tiempo.

- **Hora**: muestra la hora del evento. (Esta es una tabla de solo lectura en la ventana primaria y no se puede definir).

PASO 2 Haga clic en **Añadir**.

PASO 3 Ingrese los parámetros.

- **N.º de entrada de evento**: se muestra el número de índice del evento para la nueva entrada.
- **Comunidad**: ingrese la cadena de comunidad de SNMP que se incluirá al enviar trampas (optativo). Tenga en cuenta que la comunidad debe definirse desde las páginas **Definición de receptores de notificaciones SNMPv1,2** o **Definición de receptores de notificaciones SNMPv3** para que la trampa pueda alcanzar la estación de administración de red.
- **Descripción**: ingrese un nombre para el evento. Este nombre se usa en la página Añadir alarma RMON para vincular una alarma a un evento.
- **Tipo de notificación**: seleccione el tipo de acción que se genera a partir de este evento. Los valores son:
  - *Ninguna*: no ocurre ninguna acción cuando se apaga la alarma.
  - *Registro (Tabla de registro de eventos)*: se añade una entrada en la tabla de Registro de eventos cuando se activa la alarma.
  - *Trampa (SNMP Manager y servidor Syslog)*: se envía una trampa al servidor de registro remoto cuando se apaga la alarma.
  - *Registro y trampa*: se añade una entrada de registro en la tabla de Registro de eventos y se envía una trampa al servidor de registro remoto cuando se apaga la alarma.

- **Propietario**: ingrese el dispositivo o usuario que definió el evento.

PASO 4 Haga clic en **Aplicar**. El evento RMON se guarda en el archivo de configuración en ejecución.

PASO 5 Haga clic en **Tabla de registro de eventos** para mostrar el registro de alarmas que ocurrieron y que se han registrado (vea la descripción a continuación).

Registro de eventos RMON

En la página Tabla de registros de eventos, se muestra el registro de eventos (acciones) que ocurrieron. Se pueden registrar dos tipos de eventos: *Registro* o *Registro y trampa*. La acción en el evento se realiza cuando el evento está vinculado a una alarma (consulte la página Alarmas) y ocurrieron las condiciones de la alarma.

PASO 1 Haga clic en **Estado y estadísticas > RMON** > **Eventos.**

PASO 2 Haga clic en **Tabla de registros de eventos**.

Esta página muestra los siguientes campos:

- **N.º de entrada de evento**: el número de entrada del registro de eventos.
- **N.º de registro**: el número de registro (dentro del evento).
- **Hora de registro**: hora en que se introdujo la entrada del registro.
- **Descripción**: la descripción del evento que activó la alarma.

Alarmas RMON

Las alarmas RMON proporcionan un mecanismo para configurar umbrales e intervalos de muestreo a fin de generar eventos de excepción en los contadores o en cualquier otro contador de objetos SNMP que mantiene el agente. En la alarma deben configurarse los umbrales ascendentes y descendentes. Una vez que se atraviesa un umbral ascendente, no se genera otro evento ascendente hasta que se atraviesa el umbral descendente complementario. Luego de que se emite una alarma descendente, la siguiente alarma se genera cuando se atraviesa un umbral ascendente.

Una o más alarmas están vinculadas a un evento, que indica la acción que debe realizarse cuando ocurre la alarma.

Los contadores de alarmas pueden monitorearse mediante valores absolutos o cambios (delta) en los valores de los contadores.

Para ingresar alarmas RMON:

PASO 1 Haga clic en **Estado y estadísticas > RMON** > **Alarmas**. Se muestran todas las alarmas definidas anteriormente. Los campos se describen en la página Añadir alarma RMON a continuación. Además de esos campos, aparece el siguiente campo:

- **Valor del contador**: muestra el valor de la estadística durante el último período de muestreo.

PASO 2 Haga clic en **Añadir**.

PASO 3 Ingrese los parámetros.

- **Nº. de entrada de alarma**: se muestra el número de entrada de la alarma.
- **Interfaz**: seleccione el tipo de interfaz para el que se muestran las estadísticas de RMON.
- **Nombre del contador**: seleccione la variable MIB que indica el tipo de evento medido.
- **Valor del contador**: número de eventos.
- **Tipo de muestra**: seleccione el método de muestreo para generar una alarma. Las opciones son:
  - *Absoluto*: si se atraviesa el umbral, se genera una alarma.
  - *Delta*: se sustrae el último valor muestreado del valor actual. La diferencia en los valores se compara con el umbral. Si se atravesó el umbral, se genera una alarma.
- **Umbral ascendente**: ingrese el valor que activa la alarma de umbral ascendente.
- **Evento ascendente**: se selecciona un evento que se realizará cuando se active un evento ascendente. Los eventos se crean en la página Eventos.
- **Umbral descendente**: ingrese el valor que activa la alarma de umbral descendente.
- **Evento descendente**: se selecciona un evento que se realizará cuando se active un evento descendente.
- **Alarma de inicio**: seleccione el primer evento a partir del que se iniciará la generación de alarmas. El valor ascendente se define al atravesar el umbral de un umbral de bajo valor a un umbral de mayor valor.
  - *Alarma ascendente*: un valor ascendente activa la alarma de umbral ascendente.
  - *Alarma descendente*: un valor descendente activa la alarma de umbral descendente.
  - *Ascendente y descendente*: los valores ascendente y descendente activan la alarma.
- **Intervalo**: ingrese el tiempo del intervalo de la alarma en segundos.
- **Propietario**: ingrese el nombre del sistema de administración de red o usuario que recibe la alarma.

PASO 4 Haga clic en **Aplicar**. La alarma RMON se guarda en el archivo de configuración en ejecución.

Ver registro

Consulte **Visualización de los registros de memoria**.

4

Administración: Registro del sistema

En esta sección, se describe el registro del sistema, que permite que el dispositivo genere varios registros independientes. Cada registro es un conjunto de mensajes que describe los eventos del sistema.

El dispositivo genera los siguientes registros locales:

- Registro enviado a la interfaz de la consola.
- Registro escrito en una lista cíclica de eventos registrados en la memoria RAM y borrados cuando el dispositivo se reinicia.
- Registro escrito en un archivo de registro cíclico que se guarda en la memoria Flash y persiste de un reinicio al otro.

Además, puede enviar mensajes a servidores SYSLOG remotos en forma de trampas SNMP y mensajes SYSLOG.

En esta sección, se describen las siguientes secciones:

- **Configuración de los valores del registro del sistema**
- **Configuración de los valores de registro remoto**
- **Visualización de los registros de memoria**

Configuración de los valores del registro del sistema

Puede seleccionar los eventos que debe registrar por nivel de gravedad. Cada mensaje de registro tiene un nivel de gravedad marcado con la primera letra del nivel de gravedad concatenado con un guión (-) a cada lado (excepto para *Emergencia* que se indica con la letra F). Por ejemplo, el mensaje de registro "%INIT-I-InitCompleted ..." tiene un nivel de gravedad de **I**, que significa *Informativo*.

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 ha presentado una advertencia del sistema.
- *Nota*: el sistema está funcionando correctamente, pero se ha presentado un aviso del sistema.
- *Informativo*: información de dispositivos.
- *Depuración*: información detallada acerca de un evento.

Puede seleccionar distintos niveles de gravedad para los registros de memoria RAM y Flash. Estos registros se muestran en la página Memoria RAM y en la página Memoria Flash, respectivamente.

Al seleccionar un nivel de gravedad para almacenar en un registro, todos los eventos de mayor gravedad se almacenan automáticamente en el registro. Los eventos de menor gravedad no se almacenan en el registro.

Por ejemplo, si se selecciona **Advertencia**, todos los niveles de gravedad que sean **Advertencia** y los de mayor gravedad se almacenan en el registro (Emergencia, Alerta, Crítico, Error y Advertencia). No se almacena ningún evento con nivel de gravedad por debajo de **Advertencia** (Nota, Informativo y Depuración).

Para configurar parámetros de registro globales:

PASO 1 Haga clic en **Administración** > **Registro del sistema** > **Configuración de registro**.

PASO 2 Ingrese los parámetros.

- **Registro**: seleccione esta opción para habilitar el registro de mensajes.
- **Agregador de Syslog**: seleccione para habilitar la agrupación de mensajes y trampas SYSLOG. Si esta opción está habilitada, se agrupan mensajes y trampas SYSLOG idénticas y contiguas en el tiempo máximo de agrupamiento especificado y se envían en un único mensaje. Los mensajes agrupados se envían en el orden de llegada. Cada mensaje establece la cantidad de veces que se agrupó.
- **Tiempo máximo de agrupamiento**: ingrese el intervalo de tiempo en el que se agregan los mensajes SYSLOG.
- **Identificador de originador**: permite agregar un identificador de origen a los mensajes SYSLOG. Las opciones son:
  - *Ninguno*: no incluya el identificador de origen en los mensajes SYSLOG.
  - *Nombre de host*: incluya el nombre de host del sistema en los mensajes SYSLOG.
  - *Dirección IPv4*: incluya la dirección IPv4 de la interfaz de envío en los mensajes SYSLOG.
  - *Dirección IPv6*: incluya la dirección IPv6 de la interfaz de envío en los mensajes SYSLOG.
  - *Definido por el usuario*: ingrese una descripción que se incluirá en los mensajes SYSLOG.

- **Registro de memoria RAM**: seleccione los niveles de gravedad de los mensajes a registrar en la memoria RAM.
- **Registro de memoria Flash**: seleccione los niveles de gravedad de los mensajes a registrar en la memoria Flash.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Configuración de los valores de registro remoto

La página Servidores de registro remotos permite definir los servidores SYSLOG remotos donde se enviarán los mensajes del registro. Para cada servidor, puede configurar la gravedad de los mensajes que recibe.

Para definir los servidores SYSLOG:

PASO 1 Haga clic en **Administración** > **Registro del sistema** > **Servidores de registro remotos**.

PASO 2 Ingrese los siguientes campos:

- **Interfaz de origen IPv4**: seleccione la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen de los mensajes SYSLOG enviados a los servidores SYSLOG.
- **Interfaz de origen IPv6**: seleccione la interfaz de origen cuya dirección IPv6 se utilizará como dirección IPv6 de origen de los mensajes SYSLOG enviados a los servidores SYSLOG.

NOTA Si se selecciona la opción Automática, el sistema toma la dirección IP de origen de la dirección IP definida en la interfaz de salida.

Se describe la información para cada servidor de registro previamente configurado. Los campos se describen a continuación en la página **Añadir**.

PASO 3 Haga clic en **Add**.

PASO 4 Ingrese los parámetros.

- **Definición del servidor**: seleccione si el servidor de registro remoto se identificará por dirección IP o nombre.
- **Versión de IP**: seleccione el formato IP admitido.

- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: seleccione la interfaz local de enlace (si se selecciona Enlace local como Tipo de dirección IPv6) en la lista.
- **Nombre/dirección IP del servidor de registro:** ingrese la dirección IP o el nombre de dominio del servidor de registro.
- **Puerto UDP**: ingrese el puerto UDP a donde se envían los mensajes de registro.
- **Instalación**: seleccione un valor de instalación de donde se envían los registros del sistema al servidor remoto. Solo se puede asignar un valor de instalación por servidor. Si se asigna un segundo código de instalación, se anula el primer valor de instalación.
- **Descripción**: ingrese una descripción del servidor.
- **Gravedad mínima**: seleccione el nivel mínimo de mensajes de registro de sistema para enviar al servidor.

PASO 5 Haga clic en **Aplicar.** Se cierra la página Añadir servidor de registro remoto, se agrega el servidor SYSLOG y se actualiza el archivo de configuración en ejecución.

Visualización de los registros de memoria

El dispositivo puede escribir en los siguientes registros:

- Registro en memoria RAM (se borra durante el reinicio)
- Registro en memoria Flash (solo se borra por comando de usuario)

Usted puede configurar los mensajes que se escriben en cada registro por gravedad, y un mensaje puede ir a más de un registro, incluidos los registros que residen en servidores SYSLOG externos.

Memoria RAM

En la página Memoria RAM, se muestran todos los mensajes que se han guardado en la memoria RAM (caché) en orden cronológico. Las entradas se almacenan en el registro de memoria RAM según la configuración de la página Configuración de registro.

Para ver las entradas del registro, haga clic en **Estado y estadísticas** > **Ver registro** > **Memoria RAM**.

Al comienzo de la página hay un botón que le permite **Deshabilitar icono de alerta intermitente**. **Haga clic**. Este botón sirve para alternar entre activar y desactivar.

Umbral de registro actual indica los niveles de registro que se generan. Para modificarlos, haga clic en **Editar** junto al nombre del campo.

En esta página, se muestran los siguientes campos para cada archivo de registro:

- **Índice de registro**: número de entrada en el registro.
- **Hora de registro**: hora a la que se generó el mensaje.
- **Gravedad**: gravedad del evento.
- **Descripción**: texto del mensaje que describe el evento.

Para borrar los mensajes de registro, haga clic en **Borrar registros**. Se borran los mensajes.

Memoria Flash

En la página Memoria Flash, se muestran todos los mensajes que se han guardado en la memoria Flash en orden cronológico. La gravedad mínima para el registro se configura en la página Configuración de registro. Los registros de memoria Flash se conservan cuando el dispositivo se reinicia. Puede borrar los registros manualmente.

Para ver los registros de memoria Flash, haga clic en **Estado y estadísticas** > **Ver registro** > **Memoria Flash**.

Umbral de registro actual indica los niveles de registro que se generan. Para modificarlos, haga clic en **Editar** junto al nombre del campo.

En esta página, se muestran los siguientes campos para cada archivo de registro:

- **Índice de registro**: número de entrada en el registro.
- **Hora de registro**: hora a la que se generó el mensaje.
- **Gravedad**: gravedad del evento.
- **Descripción**: texto del mensaje que describe el evento.

Para borrar los mensajes, haga clic en **Borrar registros**. Se borran los mensajes.

5

Administración: Administración de archivos

Esta sección describe cómo se administran los archivos de sistema.

Se cubren los siguientes temas:

- **Archivos del sistema**
- **Actualización/copia de seguridad del firmware/idioma**
- **Imagen activa**
- **Descarga/Copia de seguridad de configuración/Registro**
- **Propiedades de archivos de configuración**
- **Copiar/guardar configuración**
- **Actualización de imágenes y configuración automáticas a través de DHCP**

Archivos del sistema

Los archivos de sistema son archivos que contienen información de configuración, imágenes de firmware y códigos de inicio.

Con estos archivos se pueden realizar diversas acciones, tales como: seleccionar el archivo de firmware a partir del cual se inicia el dispositivo, copiar internamente distintos tipos de archivos de configuración en el dispositivo o copiar archivos de o a un dispositivo externo, como un servidor externo.

Los posibles métodos de transferencia de archivos son:

- Copia interna
- HTTP/HTTPS, que utiliza los recursos que proporciona el explorador.
- Cliente TFTP/SCP, que requiere un servidor TFTP/SCP.

Los archivos de configuración del dispositivo se definen por su *tipo* y contienen las opciones y los valores de los parámetros para el dispositivo.

Cuando se hace referencia a una configuración en el dispositivo, esta se realiza a través de su *tipo de archivo de configuración (por ejemplo, Configuración de inicio o Configuración en ejecución)*, en vez de un nombre de archivo que el usuario puede modificar.

Se puede copiar el contenido de un tipo de configuración a otra, pero el usuario no puede cambiar los nombres de los tipos de archivo.

Otros archivos en el dispositivo incluyen archivos de firmware, código de inicio y registro, a los que se hace referencia como *archivos operativos*.

Los archivos de configuración son archivos de texto que se pueden editar en un editor de texto, como Bloc de notas, una vez que los copia en un dispositivo externo, como una PC.

Archivos y tipos de archivo

En el dispositivo, se encuentran los siguientes tipos de archivos de configuración y operativos:

- **Configuración en ejecución**: contiene los parámetros que el dispositivo está utilizando para funcionar. Es el único tipo de archivo que se modifica cuando se cambian los valores de los parámetros en el dispositivo.

  Si se reinicia el dispositivo, se pierde la configuración en ejecución. La configuración de inicio, que se almacena en Flash, se escribe en la configuración en ejecución, que se almacena en RAM.

  Para guardar los cambios que haya hecho en el dispositivo, debe guardar la configuración en ejecución en la configuración de inicio u otro tipo de archivo.

- **Configuración de inicio**: Los valores de los parámetros que guardó al copiar otra configuración (en general, la configuración en ejecución) en la configuración de inicio.

  La configuración de inicio se guarda en flash y se conserva cuando se reinicia el dispositivo. En ese momento, la configuración de inicio se copia en RAM y se identifica como la configuración en ejecución.

- **Configuración de duplicado**: una copia de la configuración de inicio, que el dispositivo crea cuando se presentan las siguientes condiciones:

  - El dispositivo ha estado funcionando continuamente durante 24 horas.
  - No se hayan realizado cambios de configuración en la configuración en ejecución en las 24 horas anteriores.
  - La configuración de inicio es idéntica a la configuración en ejecución.

  Solo el sistema puede copiar la configuración de inicio en la configuración de duplicado. Sin embargo, usted puede copiar desde la configuración de duplicado a otros tipos de archivo o a otro dispositivo.

La opción de copiar automáticamente la configuración en ejecución a la configuración de duplicado puede desactivarse en la página Propiedades de archivos de configuración.

- **Configuración de respaldo**: una copia manual de los archivos de configuración usados para brindar protección frente al apagado del sistema o para realizar el mantenimiento de un estado operativo específico. Usted puede copiar la configuración de duplicado, la configuración de inicio o la configuración en ejecución a un archivo de configuración de respaldo. La configuración de respaldo existe en flash y se conserva en caso de que se reinicie el dispositivo.
- **Firmware**: el programa que controla las operaciones y la funcionalidad del dispositivo que se conoce comúnmente como la *imagen*.
- **Código de inicio**: controla el inicio básico del sistema e inicia la imagen de firmware.
- **Archivo de idioma**: el diccionario que permite mostrar las ventanas de la utilidad de la configuración basada en la Web en el idioma seleccionado.
- **Registro flash**: los mensajes SYSLOG guardados en la memoria flash.

Acciones de archivos

Se pueden realizar las siguientes acciones para administrar los archivos de configuración y firmware:

- Actualizar el firmware o el código de inicio, o reemplazar un segundo idioma, tal como se describe en la sección **Actualización/copia de seguridad del firmware/idioma**.
- Ver la imagen de firmware en uso o seleccionar la imagen que se usará en el siguiente reinicio, tal como se describe en la sección **Imagen activa**.
- Guardar archivos de configuración en el dispositivo en un lugar en otro dispositivo, tal como se describe en la sección **Descarga/Copia de seguridad de configuración/Registro**.
- Borrar los tipos de archivo de configuración de inicio o configuración de respaldo, tal como se describe en la sección **Propiedades de archivos de configuración**.
- Copiar un tipo de archivo de configuración en otro tipo de archivo de configuración, tal como se describe en la sección **Copiar/guardar configuración**.
- Activar la carga automática de un archivo de configuración de un servidor DHCP al dispositivo, tal como se describe en la sección **Actualización de imágenes y configuración automáticas a través de DHCP**.

Esta sección abarca los siguientes temas:

- **Actualización/copia de seguridad del firmware/idioma**
- **Imagen activa**
- **Descarga/Copia de seguridad de configuración/Registro**
- **Propiedades de archivos de configuración**

- **Copiar/guardar configuración**
- **Actualización de imágenes y configuración automáticas a través de DHCP**

Actualización/copia de seguridad del firmware/idioma

El proceso **Actualización/respaldo de firmware/idioma** se puede usar para:

- Actualizar o realizar un respaldo de la imagen de firmware.
- Actualizar o realizar un respaldo del código de inicio.
- Importar o actualizar un segundo archivo de idioma.

Se admiten los siguientes métodos para transferir archivos:

- HTTP/HTTPS que utiliza los recursos que proporciona el explorador
- TFTP que requiere un servidor TFTP
- SCP (Secure Copy Protocol, protocolo de copia segura) que requiere un servidor SCP

Si se cargó un archivo de idioma nuevo en el dispositivo, el idioma nuevo puede seleccionarse en el menú desplegable (no es necesario reiniciar el dispositivo).

Hay dos imágenes de firmware almacenadas en el dispositivo. Una de las imágenes se identifica como la *imagen activa* y la otra imagen se identifica como la *imagen inactiva*.

Al actualizar el firmware, la nueva imagen siempre reemplaza a la imagen identificada como la imagen inactiva.

Después de cargar nuevo firmware en el dispositivo, éste continúa iniciándose con la imagen activa (la versión anterior) hasta que usted cambie el estado de la imagen nueva para que sea la imagen activa a través del procedimiento de la sección **Imagen activa**. Luego, inicie el dispositivo.

Actualización y copias de seguridad del firmware o de los archivos de idioma

Para actualizar o realizar una copia de seguridad de un archivo de idioma o una imagen de software:

PASO 1 Haga clic en **Administración** > **Administración de archivo** > **Actualización/respaldo de firmware/idioma**.

PASO 2 Haga clic en Método de transferencia. Proceda de la siguiente manera:

- Si seleccionó **TFTP**, vaya al **PASO 3**.
- Si seleccionó **vía HTTP/HTTPS**, vaya al **PASO 4**.

- Si seleccionó **a través de SCP**, vaya al **PASO 5**.

PASO 3 Si seleccionó **vía TFTP**, ingrese los parámetros tal como se describe en este paso. Caso contrario, siga con el **PASO 4**.

Seleccione uno de los siguientes **Métodos de guardar**:

- **Actualización**: especifica que el tipo de archivo en el dispositivo debe reemplazarse con una nueva versión de ese tipo de archivo que se encuentra en un servidor TFTP.
- **Copia de seguridad**: especifica que se debe guardar una copia del tipo de archivo en un archivo en otro dispositivo.

Ingrese los siguientes campos:

- **Tipo de archivo**: seleccione el tipo de archivo de destino. Solo aparecen los tipos de archivo válidos (los tipos de archivo se describen en la sección **Archivos y tipos de archivo**).
- **Definición del servidor TFTP**: seleccione si el servidor TFTP se especificará **Por dirección IP** o **Por nombre**.
- **Versión de IP**: seleccione si se usa una dirección IPv4 o IPv6.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - **Enlace local**: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de FE80, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - **Global**: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: seleccione la interfaz local de enlace (si se usa IPv6) en la lista.
- **Nombre/dirección IP del servidor TFTP**: ingrese la dirección IP o el nombre del servidor TFTP.
- **(Para actualización) Nombre del archivo de origen**: ingrese el nombre del archivo de origen.
- **(Para copia de seguridad) Nombre del archivo de origen**: ingrese el nombre del archivo de seguridad.

PASO 4 Si seleccionó **a través de HTTP/HTTPS**, solo podrá seleccionar el **Método de guardar: Actualizar**. Ingrese los parámetros como se describe en este paso.

- **Tipo de archivo**: seleccione uno de los siguientes tipos de archivo:
  - *Imagen de firmware*: seleccione esta opción para actualizar la imagen de firmware.
  - *Archivo de idioma*: seleccione un archivo para actualizar el idioma.
- **Nombre de archivo**: haga clic en **Examinar** para seleccionar un archivo o ingrese la ruta y el nombre de archivo de origen que se usará en la transferencia.

PASO 5 Si seleccionó a través de **SCP (por medio de SSH),** consulte la sección **Autenticación del cliente SSH** para obtener más instrucciones. Luego, ingrese los siguientes campos: (solo se describen los campos únicos, para campos no únicos, vea las descripciones anteriores).

- **Autenticación del servidor SSH remoto**: para habilitar la autenticación del servidor SSH (deshabilitado de manera predeterminada), haga clic en **Editar**. Esto lo lleva a la página **Autenticación del servidor SSH**, para configurar el servidor SSH y volver a la página. Use la página **Autenticación del servidor SSH** para seleccionar un método de autenticación del usuario SSH (contraseña o clave pública/privada), configurar un nombre de usuario y una contraseña en el dispositivo (si selecciona el método de contraseña) y generar una clave RSA o DSA si lo requiere.

Autenticación del cliente SSH: la autenticación del cliente puede hacerse de cualquiera de las siguientes formas:

- **Uso de credenciales del sistema cliente SSH**: establece credenciales de usuario SSH permanentes. Haga clic en **Credenciales de sistema** para ir a la página Autenticación del usuario SSH, donde puede configurar el nombre de usuario y la contraseña para usos futuros.
- **Utilizar credenciales de cliente SSH de uso único**. Ingrese lo siguiente:
  - *Nombre de usuario*: ingrese un nombre de usuario para esta acción de copia.
  - *Contraseña*: ingrese una contraseña para esta copia.

  NOTA El nombre de usuario y la contraseña para una credencial única no se guardarán en el archivo de configuración.

Seleccione uno de los siguientes **Métodos de guardar**:

- **Actualización**: especifica que el tipo de archivo en el dispositivo debe reemplazarse con una nueva versión de ese tipo de archivo que se encuentra en un servidor TFTP.
- **Copia de seguridad**: especifica que se debe guardar una copia del tipo de archivo en un archivo en otro dispositivo.

Ingrese los siguientes campos:

- **Tipo de archivo**: seleccione el tipo de archivo de destino. Solo aparecen los tipos de archivo válidos (los tipos de archivo se describen en la sección **Archivos y tipos de archivo**).
- **Definición del servidor**: seleccione si el servidor SCP se especificará por dirección IP o por nombre de dominio.
- **Versión de IP**: seleccione si se usa una dirección IPv4 o IPv6.

- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: seleccione la interfaz local de enlace en la lista.
- **Nombre/dirección IP del servidor SCP**: ingrese la dirección IP o el nombre de dominio del servidor SCP.
- **(Para actualización) Nombre del archivo de origen**: ingrese el nombre del archivo de origen.
- **(Para copia de seguridad) Nombre del archivo de origen**: ingrese el nombre del archivo de seguridad.

PASO 6 Haga clic en **Aplicar**. Si los archivos, las contraseñas y las direcciones del servidor son correctos, puede suceder lo siguiente:

- Si se activa la autenticación del servidor SSH (en la página Autenticación del servidor SSH) y el servidor SCP es confiable, la operación se lleva a cabo correctamente. Si el servidor SCP no es confiable, la operación falla y se muestra un mensaje de error.
- Si no se habilita la autenticación del servidor SSH, la operación se lleva a cabo correctamente para cualquier servidor SCP.

Imagen activa

Hay dos imágenes de firmware almacenadas en el dispositivo. Una de las imágenes se identifica como la *imagen activa* y la otra imagen se identifica como la *imagen inactiva*. El dispositivo se inicia desde la imagen que usted configura como *imagen activa*. Usted puede cambiar la imagen identificada como la *imagen inactiva* por la *imagen activa*. (Usted puede reiniciar el dispositivo mediante el proceso descrito en la sección **Interfaz de administración**).

Para seleccionar la imagen activa:

PASO 1 Haga clic en **Administración** > **Administración de archivo** > **Imagen activa**.

La página muestra lo siguiente:

- **Imagen activa**: se muestra el archivo de la imagen que está activa en el dispositivo.
- **Número de versión de imagen activa**: se muestra la versión del firmware de la imagen activa.

- **Imagen activa luego de reinicio**: muestra la imagen que permanece activa luego del reinicio.
- **Número de versión de imagen activa luego de reinicio**: muestra la versión de firmware de la imagen activa como sería luego del reinicio.

PASO 2 Seleccione la imagen en el menú **Imagen activa después de reiniciar** para identificar la imagen de firmware que se usa como la imagen activa después de que se reinicia el dispositivo. En **Número de versión de la imagen activa después de reiniciar**, se muestra la versión del firmware de la imagen activa que se usa una vez que se reinicia el dispositivo.

PASO 3 Haga clic en **Aplicar**. Se actualiza la selección de la imagen activa.

Descarga/Copia de seguridad de configuración/Registro

La página Descarga/Copia de seguridad de configuración/Registro permite:

- Realizar copias de seguridad de archivos de configuración o registros del dispositivo a un dispositivo externo.
- Restaurar archivos de configuración de un dispositivo externo al dispositivo.

Al restaurar un archivo de configuración a la configuración en ejecución, el archivo importado *agrega* los comandos de configuración que no existían en el archivo antiguo y *sobrescribe* los valores de parámetros en los comandos de configuración existentes.

Al restaurar un archivo de configuración a la configuración de inicio o un archivo de configuración de respaldo, el nuevo archivo *reemplaza* al archivo anterior.

Al restaurar a la configuración de inicio, es necesario reiniciar el dispositivo para que la configuración de inicio restaurada se utilice como la configuración en ejecución. Usted puede reiniciar el dispositivo mediante el proceso descrito en la sección **Interfaz de administración**.

Compatibilidad con versiones anteriores del archivo de configuración

Al restaurar archivos de configuración de un dispositivo externo al dispositivo, pueden surgir los siguientes problemas de compatibilidad:

- **Cambio del modo del sistema**: si el modo del sistema está incluido en un archivo de configuración que se descarga al dispositivo y el modo del sistema del archivo coincide con el modo del sistema actual, esta información se omite. De lo contrario, si se cambia el modo del sistema, son posibles los siguientes casos:

- Si el archivo de configuración se descarga en el dispositivo (mediante la página Descarga/Copia de seguridad de configuración/Registro), la operación se anula y se muestra un mensaje que indica que se debe cambiar el modo del sistema en la página Configuración del sistema.
- Si el archivo de configuración se descarga durante un proceso de configuración automático, el archivo de configuración de inicio se elimina y el dispositivo se reinicia automáticamente en el nuevo modo del sistema. El dispositivo se configura con un archivo de configuración vacío.

Descarga o copia de seguridad de un archivo de registro o configuración

Para realizar un respaldo o restaurar el archivo de configuración del sistema:

PASO 1 Haga clic en **Administración** > **Administración de archivo** > **Descarga/Respaldo de configuración/registro**.

PASO 2 Haga clic en el método de transferencia en **Método de transferencia**.

PASO 3 Si seleccionó **vía TFTP**, ingrese los parámetros. Caso contrario, siga con el **PASO 4**.

Seleccione **Descarga** o **Respaldo** como **Método de guardar**.

Descarga: especifica que el archivo de otro dispositivo reemplazará un tipo de archivo en el dispositivo. Ingrese los siguientes campos:

a. **Definición del servidor TFTP**: seleccione si el servidor TFTP se especificará por dirección IP o nombre de dominio.

b. **Versión de IP**: seleccione si se usa una dirección IPv4 o IPv6.

NOTA Si en Definición del servidor se selecciona el servidor por nombre, no es necesario seleccionar las opciones relacionadas con la Versión de IP.

c. **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa). Las opciones son:

- *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
- *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.

d. **Interfaz local de enlace**: seleccione la interfaz local de enlace en la lista.

e. **Nombre/dirección IP del servidor TFTP**: ingrese la dirección IP o el nombre del servidor TFTP.

f. **Nombre del archivo de origen**: ingrese el nombre de archivo de origen. Los archivos no pueden contener símbolos diagonales (\ o /), no pueden comenzar con un punto (.) y deben incluir entre 1 y 160 caracteres. (Caracteres válidos: A-Z, a-z, 0-9, ".", "-", "_").

g. **Tipo de archivo de destino**: ingrese el tipo de archivo de configuración de destino. Solo aparecen los tipos de archivo válidos (los tipos de archivo se describen en la sección **Archivos y tipos de archivo**).

Respaldo: especifica que se debe copiar un tipo de archivo en un archivo en otro dispositivo. Ingrese los siguientes campos:

a. **Definición del servidor TFTP**: seleccione si el servidor TFTP se especificará por dirección IP o nombre de dominio.

b. **Versión de IP**: seleccione si se usa una dirección IPv4 o IPv6.

c. **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa). Las opciones son:

- *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
- *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.

d. **Interfaz local de enlace**: seleccione la interfaz local de enlace en la lista.

e. **Nombre/dirección IP del servidor TFTP**: ingrese la dirección IP o el nombre del servidor TFTP.

f. **Tipo de archivo de origen**: ingrese el tipo de archivo de configuración de origen. Solo aparecen los tipos de archivo válidos (los tipos de archivo se describen en la sección **Archivos y tipos de archivo**).

g. **Datos confidenciales**: seleccione cómo deberían incluirse los datos confidenciales en el archivo de respaldo. Las opciones disponibles son las siguientes:

- *Excluir*: no incluir datos confidenciales en el respaldo.
- *Cifrado*: incluir datos confidenciales en el respaldo en forma cifrada.
- *Texto simple*: incluir datos confidenciales en el respaldo en forma de texto simple.

NOTA Las reglas SSD del usuario actual determinan las opciones de datos confidenciales disponibles. Para obtener más detalles, consulte la página Gestión de datos confidenciales > Reglas SSD.

h. **Nombre de archivo de destino**: ingrese el nombre de archivo de destino. Los nombres de archivo no pueden incluir símbolos diagonales (\ o /), la primera letra del nombre de archivo no debe ser un punto (.) y el nombre de archivo debe tener entre 1 y 160 caracteres. (Caracteres válidos: A-Z, a-z, 0-9, ".", "-", "_").

i. Haga clic en **Aplicar**. Se actualiza el archivo o se realiza una copia de seguridad de este.

PASO 4 Si seleccionó **vía HTTP/HTTPS**, ingrese los parámetros tal como se describe en este paso.

Seleccione la acción de guardado en **Método de guardar**.

Si la opción de **Método de guardar** es *Descarga* (reemplazo de un archivo en el dispositivo con una versión nueva de otro dispositivo), haga lo siguiente. En caso contrario, vaya al siguiente procedimiento en este paso.

a. **Nombre del archivo de origen**: haga clic en **Examinar** para seleccionar un archivo o ingrese la ruta y el nombre de archivo de origen que se usará en la transferencia.

b. **Tipo de archivo de destino**: seleccione el tipo de archivo de configuración. Solo aparecen los tipos de archivo válidos (los tipos de archivo se describen en la sección **Archivos y tipos de archivo**).

c. Haga clic en **Aplicar**. Se transfiere el archivo del otro dispositivo al dispositivo.

Si el **Método de guardar** es *Copia de seguridad* (copia un archivo a otro dispositivo), haga lo siguiente:

a. **Tipo de archivo de origen**: seleccione el tipo de archivo de configuración. Solo aparecen los tipos de archivo válidos (los tipos de archivo se describen en la sección **Archivos y tipos de archivo**).

b. **Datos confidenciales**: seleccione cómo deberían incluirse los datos confidenciales en el archivo de respaldo. Las opciones disponibles son las siguientes:

- *Excluir*: no incluir datos confidenciales en el respaldo.
- *Cifrado*: incluir datos confidenciales en el respaldo en forma cifrada.
- *Texto simple*: incluir datos confidenciales en el respaldo en forma de texto simple.

NOTA Las reglas SSD del usuario actual determinan las opciones de datos confidenciales disponibles. Para obtener más detalles, consulte la página Gestión de datos confidenciales > Reglas SSD.

c. Haga clic en **Aplicar**. Se actualiza el archivo o se realiza una copia de seguridad de este.

PASO 5 Si seleccionó vía **SCP (por SSH)**, consulte **Configuración del cliente SSH a través de la GUI** para obtener instrucciones. Luego, ingrese los siguientes campos:

- **Autenticación del servidor SSH remoto**: para habilitar la autenticación del servidor SSH (está deshabilitado de manera predeterminada), haga clic en **Editar**, lo cual lo redirige a la página **Autenticación del servidor SSH** para configurar esto y volver a la página. Use la página **Autenticación del servidor SSH** para seleccionar un método de autenticación del usuario SSH (contraseña o clave pública/privada), configurar un nombre de usuario y una contraseña en el dispositivo, si selecciona el método de contraseña, y generar una clave RSA o DSA si lo requiere.

Autenticación del cliente SSH: la autenticación del cliente puede hacerse de cualquiera de las siguientes formas:

- **Uso de credenciales del sistema cliente SSH**: establece credenciales de usuario SSH permanentes. Haga clic en **Credenciales de sistema** para ir a la página Autenticación del usuario SSH, donde puede configurar el nombre de usuario y la contraseña para usos futuros.
- **Utilizar credenciales de cliente SSH de uso único**. Ingrese lo siguiente:
  - *Nombre de usuario*: ingrese un nombre de usuario para esta acción de copia.
  - *Contraseña*: ingrese una contraseña para esta copia.
- **Método de guardar**: seleccione si desea respaldar o restaurar el archivo de configuración del sistema.
- **Definición del servidor SCP**: seleccione si el servidor SCP se especificará **por dirección IP** o por **nombre** de dominio.
- **Versión de IP**: seleccione si se usa una dirección IPv4 o IPv6.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: seleccione la interfaz local de enlace en la lista.
- **Nombre/dirección IP del servidor SCP**: ingrese la dirección IP o el nombre del servidor SCP.

Si la opción de **Método de guardar** es *Descarga* (reemplazo de un archivo en el dispositivo con una versión nueva de otro dispositivo), ingrese los siguientes campos.

- **Nombre del archivo de origen**: ingrese el nombre del archivo de origen.
- **Tipo de archivo de destino**: seleccione el tipo de archivo de configuración. Solo aparecen los tipos de archivo válidos (los tipos de archivo se describen en la sección **Archivos y tipos de archivo**).

Si el **Método de guardar** es *Copia de seguridad* (copia un archivo a otro dispositivo), ingrese los siguientes campos (además de aquellos campos que figuran más arriba):

- **Tipo de archivo de origen**: seleccione el tipo de archivo de configuración. Solo aparecen los tipos de archivo válidos (los tipos de archivo se describen en la sección **Archivos y tipos de archivo**).
- **Datos confidenciales**: seleccione cómo deberían incluirse los datos confidenciales en el archivo de respaldo. Las opciones disponibles son las siguientes:

- *Excluir*: no incluir datos confidenciales en el respaldo.
- *Cifrado*: incluir datos confidenciales en el respaldo en forma cifrada.
- *Texto simple*: incluir datos confidenciales en el respaldo en forma de texto simple.

NOTA Las reglas SSD del usuario actual determinan las opciones de datos confidenciales disponibles. Para obtener más detalles, consulte la página Gestión de datos confidenciales > Reglas SSD.

- **Nombre de archivo de destino**: nombre de archivo al cual se copia.

PASO 6 Haga clic en **Aplicar**. Se actualiza el archivo o se realiza una copia de seguridad de este.

Propiedades de archivos de configuración

La página Propiedades de archivos de configuración aparece cuando se crearon los distintos archivos de configuración del sistema. También permite eliminar los archivos de configuración de inicio o configuración de respaldo, pero no puede eliminar los otros tipos de archivo de configuración.

Para establecer si se crearán los archivos de configuración de duplicado, limpie los archivos de configuración y vea cuándo se crearon los archivos de configuración:

PASO 1 Haga clic en **Administración** > **Administración de archivo** > **Propiedades de archivo de configuración**.

Esta página muestra los siguientes campos:

- **Nombre del archivo de configuración**: tipo de archivo del sistema.
- **Hora de creación**: fecha y hora en que se modificó el archivo.

PASO 2 De ser necesario, deshabilite la **Configuración de duplicado automático**. Esta acción deshabilita la creación automática de archivos de configuración de duplicado. Al deshabilitar esta función, el archivo de configuración de duplicado, si existe, se elimina. Consulte la sección **Archivos del sistema** para obtener una descripción de los archivos de configuración y por qué no querría crear automáticamente archivos de configuración de duplicado.

PASO 3 De ser necesario, seleccione Configuración de inicio o Configuración de respaldo, o ambas, y haga clic en **Borrar archivos** para borrar estos archivos.

Copiar/guardar configuración

Al hacer clic en **Aplicar** en una ventana, los cambios que hizo en las opciones de configuración del dispositivo se guardan *solo* en la configuración en ejecución. Para conservar los parámetros en la configuración en ejecución, esta debe copiarse en otro tipo de configuración o guardarse en otro dispositivo.

PRECAUCIÓN A menos que la configuración en ejecución se copie en la configuración de inicio u otro archivo de configuración, al reiniciar el dispositivo se pierden todos los cambios realizados desde la última vez que se copió el archivo.

Se permiten las siguientes combinaciones de copiado de tipos de archivo internos:

- De la configuración en ejecución a la configuración de inicio o la configuración de respaldo.
- De la configuración de inicio a la configuración en ejecución, la configuración de inicio o la configuración de respaldo.
- De la configuración de respaldo a la configuración en ejecución, la configuración de inicio o la configuración de respaldo.
- De la configuración de duplicado a la configuración en ejecución, la configuración de inicio o la configuración de respaldo.

Para copiar un tipo de archivo de configuración a otro tipo de archivo de configuración:

PASO 1 Haga clic en **Administración** > **Administración de archivo** > **Copiar/guardar configuración**.

PASO 2 Seleccione el **Nombre de archivo de origen** que desea copiar. Solo los tipos de archivo se muestran (descritos en la sección **Archivos y tipos de archivo**).

PASO 3 Seleccione el **Nombre de archivo de destino** que sobrescribirá el archivo de origen.

PASO 4 Seleccione la opción **Datos confidenciales** si va a realizar una copia de seguridad de un archivo de configuración; seleccione uno de los siguientes formatos para el archivo de respaldo.

- **Excluir**: no se incluyen datos confidenciales en el respaldo.
- **Cifrado**: se incluyen datos confidenciales en el respaldo en forma cifrada.
- **Texto simple**: se incluyen datos confidenciales en el respaldo en forma de texto simple.

NOTA Las reglas SSD del usuario actual determinan las opciones de datos confidenciales disponibles. Para obtener más detalles, consulte la página Gestión de datos confidenciales > Reglas SSD.

PASO 5 El campo **Guardar icono intermitente** indica si un icono parpadea cuando hay datos sin guardar. Para habilitar o deshabilitar esta función, haga clic en **Habilitar/deshabilitar la opción de guardar icono intermitente**.

PASO 6 Haga clic en **Aplicar**. Se copia el archivo.

Actualización de imágenes y configuración automáticas a través de DHCP

La función de actualización de imágenes y configuración automáticas ofrece un método cómodo para configurar en una red, de manera automática, los switches Cisco Small Business de las series 200, 300 y 500, y actualizar el firmware. Este proceso permite al administrador asegurarse, de manera remota, que están actualizados la configuración y el firmware de esos dispositivos de la red.

Esta función está integrada por dos etapas:

- **Actualización automática de imágenes**: descarga automática de la imagen de firmware de un servidor TFTP/SCP remoto. Al finalizarse el proceso automático de actualización de imágenes y configuración, el dispositivo se reinicia con la imagen de firmware.
- **Configuración automática**: descarga automática de un archivo de configuración de un servidor TFTP/SCP remoto. Al finalizarse el proceso automático de imágenes y configuración, el dispositivo se reinicia con el archivo de configuración.

NOTA Si se solicitan las dos instancias de configuración y actualización de imágenes automáticas, primero se realiza la actualización de imágenes. Después de reiniciarse el dispositivo, se realiza la instancia de configuración automática seguida de un reinicio final.

Para usar esta función, configure un servidor DHCP en la red con las ubicaciones y los nombres del archivo de configuración y la imagen de firmware de los dispositivos. Los dispositivos de la red se configuran como clientes DHCP de forma predeterminada. Cuando los dispositivos reciben las direcciones IP del servidor DHCP, también reciben información del archivo de configuración y de la imagen de firmware. Si el archivo de configuración o la imagen de firmware son diferentes de los que se usan actualmente en el dispositivo, el dispositivo se reinicia luego de descargar el archivo o la imagen. En esta sección, se describen esos procesos.

Además de la capacidad para mantener actualizados los dispositivos de la red con los últimos archivos de configuración e imagen de firmware, la función de configuración y actualización de imágenes automáticas permite instalar rápidamente nuevos dispositivos en la red, ya que se configura un dispositivo de fábrica para recuperar su archivo de configuración en imagen de software desde la red sin la intervención manual del administrador del sistema. La primera vez que solicita la dirección IP del servidor DHCP, el dispositivo descarga el archivo de configuración o la imagen que indicó el servidor DHCP (y se reinicia).

El proceso de configuración automática también admite la descarga de un archivo de configuración que incluye información confidencial, como claves de servidor RADIUS y claves SSH/SSL, mediante el SCP (Secure Copy Protocol, protocolo de copia segura) y la función SSD (Secure Sensitive Data, datos confidenciales seguros) (consulte **Autenticación del cliente SSH** y **Seguridad: Gestión de datos confidenciales**).

Protocolos de descarga (TFTP o SCP)

Los archivos de configuración y las imágenes de firmware pueden descargarse desde un servidor TFTP o SCP.

El usuario configura el protocolo que desea utilizar, de la siguiente manera:

- **Extensión automática por archivo** (valor predeterminado): si está seleccionada esta opción, una extensión de archivo definida por el usuario indica que los archivos con esta extensión se descargan con SCP (por medio de SSH), mientras que los archivos con otras extensiones se descargan con TFTP. Por ejemplo, si el archivo de extensión especificado es *.xyz*, los archivos con la extensión *.xyz* se descargarán usando SCP, y los archivos con otras extensiones se descargarán mediante TFTP. La extensión predeterminada es .scp.
- **Solo TFTP**: la descarga se realiza a través de TFTP sin importar la extensión del archivo del nombre de archivo de configuración.
- **Solo SCP**: la descarga se realiza a través de SCP (por SSH) sin importar la extensión del archivo del nombre de archivo de configuración.

Autenticación del cliente SSH

SCP está basado en SSH. De manera predeterminada, la autenticación del servidor SSH remoto está desactivada, por lo que el dispositivo acepta cualquier servidor SSH remoto sin problemas. Puede activar la autenticación remota del servidor SSH para que puedan utilizarse únicamente los servidores que figuran en la lista de confianza.

Los parámetros de autenticación del cliente SSH se requieren para que el cliente acceda al servidor SSH (que es el dispositivo). Los parámetros de autenticación del cliente SSH predeterminados son:

- Método de autenticación SSH: nombre de usuario y contraseña
- Nombre de usuario SSH: anónimo

- Contraseña SSH: anónimo

NOTA Los parámetros de autenticación del cliente SSH también pueden usarse para descargar un archivo manualmente (descarga que no se realiza mediante la función de actualización de imágenes y configuración automáticas de DHCP).

Proceso automático de actualización de imágenes y configuración

La configuración automática de DHCP utiliza el nombre o la dirección del servidor de configuración y el nombre o la ruta del archivo de configuración (si corresponde) en los mensajes DHCP recibidos. Además,la actualización de imágenes de DHCP utiliza el nombre de archivo indirecto del firmware (si corresponde) en los mensajes. Esta información se indica como opciones de DHCP en el mensaje de **Oferta** que proviene de los servidores DHCPv4 y en los mensajes de **Respuesta de información** que provienen de los servidores DHCPv6.

Si esta información no está en los mensajes del servidor DHCP, se utiliza la información de respaldo que se configuró en la página Actualización de imágenes y configuración automáticas de DHCP.

Cuando se activa el proceso automático de actualización de imágenes y configuración (consulte **Disparador de la actualización de imágenes y configuración automáticas**), se produce la secuencia de eventos descrita a continuación.

Se inicia la actualización automática de imágenes:

- El switch utiliza el nombre de archivo indirecto de la opción 125 (DHCPv4) y la opción 60 (DHCPv6), si corresponde, del mensaje de DHCP recibido.
- Si el servidor DHCP no envió el nombre de archivo indirecto del archivo de imagen de firmware, se utilizará el nombre de archivo de imagen indirecto de respaldo (de la página Actualización de imágenes y configuración automáticas de DHCP).
- El switch descarga el archivo de imagen indirecto y le extrae el nombre del archivo de imagen del servidor TFTP/SCP.
- El switch compara la versión del archivo de imagen del servidor TFTP con la versión de la imagen activa del switch.
- Si las dos versiones son diferentes, se cargará la nueva versión a la imagen no activa, se reiniciará el sistema y la imagen no activa pasará a ser la imagen activa.
- Si se utiliza el protocolo SCP, se genera un mensaje SYSLOG que informará que está a punto de reiniciarse el sistema.
- Si se utiliza el protocolo SCP, se genera un mensaje SYSLOG que reconocerá que se completó el proceso de actualización automática.
- Si se utiliza el protocolo TFTP, el proceso de copia genera mensajes SYSLOG.

Se inicia la configuración automática:

- El dispositivo utiliza el nombre o la dirección del servidor TFTP/SCP y el nombre o la ruta del archivo de configuración (opciones de DHCPv4: 66,150 y 67; opciones de DHCPv6: 59 y 60), si corresponde, del mensaje DHCP recibido.
- Si el servidor DHCP no envía la información, se utilizará el nombre o la dirección IP del servidor de respaldo y el nombre del archivo de configuración de respaldo (de la página Actualización de imágenes y configuración automáticas de DHCP).
- Se utilizará el nuevo archivo de configuración si el nombre difiere del nombre del archivo de configuración que se utilizó anteriormente en el dispositivo, o si el dispositivo jamás antes fue configurado.
- El dispositivo se reinicia con el nuevo archivo de configuración tras concluirse el proceso automático de actualización de imágenes y configuración.
- El proceso de copia generará mensajes SYSLOG.

Opciones faltantes

- Si el servidor DHCP no envió la dirección del servidor TFTP/SCP en una opción de DHCP, y no se configuró el parámetro de dirección del servidor TFTP/SCP de respaldo, entonces:
  - ***SCP***: el proceso de configuración automática se detiene.
  - ***TFTP***: el dispositivo envía mensajes de solicitud TFTP a una dirección de difusión limitada (para IPv4) o a la dirección de TODOS LOS NODOS (para IPv6) en sus interfaces IP y continúa el proceso automático de actualización de imágenes y configuración con el primer servidor TFTP que responde.

Selección del protocolo de descarga

- Se selecciona el protocolo de copia (SCP/TFTP), como se describe en **Protocolos de descarga (TFTP o SCP)**.

SCP

- Al descargar con SCP, el dispositivo acepta cualquier servidor SCP/SSH especificado (sin autenticación) si alguna de las siguientes opciones es verdadera:
  - El proceso de autenticación de servidor SSH está deshabilitado. Por opción predeterminada, la autenticación del servidor SSH está deshabilitada para permitir la descarga de archivos de configuración para los dispositivos con configuración predeterminada de fábrica (por ejemplo, dispositivos sin red).
  - El servidor SSH se configura en la lista de Servidores confiables SSH.

Si se habilita el proceso de autenticación del servidor SSH, y el servidor SSH no se encuentra en la lista de servidores confiables de SSH, el proceso de configuración automática se detiene.

- Si la información está disponible, se accede al servidor SCP para descargar desde allí el archivo de configuración o la imagen.

Disparador de la actualización de imágenes y configuración automáticas

La actualización de imágenes y configuración automáticas a través de DHCPv4 se activa cuando se cumplen las siguientes condiciones:

- La dirección IP del dispositivo se asigna o renueva de forma dinámica durante el reinicio; o bien, se renueva explícitamente con una acción administrativa, o automáticamente por una concesión próxima a caducar. La renovación explícita puede activarse en la página Interfaz IPv4.
- Si está activada la actualización automática de imágenes, ese proceso se realiza cuando un servidor DHCP envía un nombre de archivo de imagen indirecto, o cuando se configura un nombre de archivo de imagen indirecto de respaldo. "Indirecto" significa que no se trata de la imagen en sí, sino de un archivo que mantiene el nombre de la ruta para la imagen.
- Si está activada la configuración automática, ese proceso se realiza cuando un servidor DHCP envía un nombre de archivo de configuración, o cuando se configura un nombre de archivo de configuración de respaldo.

La actualización de imágenes y configuración automáticas a través de DHCPv6 se activa cuando se cumplen las siguientes condiciones:

- Cuando un servidor DHCPv6 envía información al dispositivo. Esto ocurre en los siguientes casos:
  - Cuando una interfaz, que tiene activado IPv6, se define como cliente de configuración DHCPv6 sin estado.
  - Cuando se reciben mensajes DHCPv6 del servidor (por ejemplo, cuando presiona el botón **Reiniciar** en la página Interfaces IPv6).
  - Cuando el dispositivo actualiza la información de DHCPv6.
  - Después de reiniciar el dispositivo cuando el cliente DHCPv6 sin estado se activa.
- Cuando los paquetes de servidor DHCPv6 contienen la opción de nombre de archivo de configuración.
- El proceso de actualización automática de imágenes se activa cuando el servidor DHCP proporciona un nombre de archivo de imagen indirecto, o cuando se configura un nombre de archivo de imagen indirecto de respaldo. "Indirecto" significa que no se trata de la imagen en sí, sino de un archivo que mantiene el nombre de la ruta para la imagen.

Asegurar el rendimiento correcto

Para asegurar que la actualización de imágenes y configuración automáticas funcionan correctamente, observe lo siguiente:

- Un archivo de configuración que se coloca en el servidor TFTP/SCP debe coincidir con los requisitos de forma y formato de un archivo de configuración compatible. Se comprueba la forma y el formato del archivo, pero la validez de los *parámetros* de configuración no se comprueba antes de cargarlo a la configuración de inicio.
- En IPv4, para asegurarse de que el dispositivo descarga la configuración y el archivo de imagen de la forma prevista durante el proceso automático de actualización de imágenes y configuración, se recomienda que el dispositivo siempre tenga asignada la misma dirección IP. De esta forma, es posible asegurar que el dispositivo siempre tenga asignada la misma dirección IP y que obtenga la misma información utilizada en la actualización de imágenes y configuración automáticas.

Actualización de imágenes y configuración automáticas de DHCP

Las siguientes páginas de la GUI se utilizan para configurar el dispositivo.

- Administración > Administración de archivo > Actualización de imágenes y configuración automáticas de DHCP: para configurar el dispositivo como cliente DHCP.
- Administración > Interfaz de administración > Interfaz IPv4 (en L2) o Configuración IP > Administración e interfaces IPv4 > Interfaces IPv4 (en L3): para renovar la dirección IP a través de DHCP cuando el dispositivo está en el modo de sistema de Capa 2.

Configuración y valores predeterminados

Existen los siguientes valores predeterminados en el sistema:

- La configuración automática está activada.
- La actualización automática de imágenes está activada.
- El dispositivo está activado como cliente DHCP.
- La autenticación remota del servidor SSH está deshabilitada.

Antes de iniciar el proceso automático de actualización de imágenes y configuración

Para usar esta función, el dispositivo debe estar configurado como cliente DHCPv4 o DHCPv6. El tipo de cliente DHCP definido en el dispositivo tiene correlación con los tipos de interfaces definidos en el dispositivo.

Preparación de la configuración automática en el servidor

Para preparar los servidores DHCP y TFTP/SCP, realice lo siguiente:

Servidor TFTP/SCP

- Coloque un archivo de configuración en el directorio de trabajo. Ese archivo puede crearse si se copia un archivo de configuración desde un dispositivo. Cuando arranca el dispositivo, se convierte en el archivo de configuración en ejecución.

Servidor DHCP

Configure el servidor DHCP con las siguientes opciones:

- DHCPv4:
  - 66 (una sola dirección del servidor) o 150 (lista de direcciones del servidor)
  - 67 (nombre del archivo de configuración)
- DHCPv6
  - Opción 59 (dirección del servidor)
  - Opciones 60 (nombre del archivo de configuración y nombre del archivo de imagen indirecto separados por una coma)

Preparación de la actualización automática de imágenes

Para preparar los servidores DHCP y TFTP/SCP, realice lo siguiente:

Servidor TFTP/SCP

1. Cree un subdirectorio en el directorio principal. Colóquele un archivo de imagen de software.
2. Cree un archivo indirecto que contenga una ruta y el nombre de la versión de firmware (por ejemplo, indirecto-cisco.txt que contenga cisco\cisco-versión.ros).
3. Copie ese archivo indirecto al directorio principal del servidor TFTP/SCP.

Servidor DHCP

Configure el servidor DHCP con las siguientes opciones:

- DHCPv4: Opción 125 (nombre de archivo indirecto)
- DHCPv6: Opciones 60 (nombre del archivo de configuración y nombre del archivo de imagen indirecto separados por una coma)

Flujo de trabajo del cliente DHCP

PASO 1 Configure los parámetros de la configuración y actualización de imágenes automáticas en la página Administración > Administración de archivo > Actualización de imágenes y configuración automáticas de DHCP.

PASO 2 Establezca el tipo de dirección IP en Dinámica en las páginas **Definición de una interfaz IPv4 en modo del sistema Capa 2** o **Definición de una interfaz IPv4 en modo del sistema Capa 3**, y defina el dispositivo como cliente DHCPv6 sin estado en la página **Interfaz IPv6**.

Configuración Web

Para configurar los parámetros de la configuración y actualización de imágenes automáticas:

PASO 1 Haga clic en **Administración** > **Administración de archivo** > **Actualización de imágenes y configuración automáticas de DHCP**.

PASO 2 Ingrese los valores.

- **Configuración automática vía DHCP**: seleccione este campo para habilitar la configuración automática de DHCP. De manera predeterminada, esta función está activada y se puede desactivar aquí.
- **Protocolo de descarga**: seleccione una de las siguientes opciones:
  - *Extensión automática por archivo*: seleccione esta opción para indicar que la configuración automática utiliza el protocolo TFTP o SCP, según la extensión del archivo de configuración. Si selecciona esta opción, la extensión del archivo de configuración no necesariamente debe brindarse. En tal caso, se utilizará la extensión predeterminada (como se indica a continuación).
  - *Extensión de archivo para SCP*: si se selecciona **Extensión automática por archivo**, puede indicar la extensión del archivo aquí. Cualquier archivo con esta extensión se descargará mediante SCP. Si no se ingresa ninguna extensión, se utilizará la extensión de archivo predeterminada **.scp**.
  - *Solo TFTP*: seleccione esta opción para indicar que solamente el protocolo TFTP debe usarse para configuración automática.
  - *Solo SCP*: seleccione esta opción para indicar que solamente el protocolo SCP debe usarse para configuración automática.
- **Actualización automática de imágenes a través de DHCP**: seleccione este campo para activar la actualización de la imagen del firmware desde el servidor DHCP. De manera predeterminada, esta función está activada y se puede desactivar aquí.

- **Protocolo de descarga**: seleccione una de las siguientes opciones:
  - *Extensión automática por archivo*: seleccione esta opción para indicar que la actualización automática utiliza el protocolo TFTP o SCP, según la extensión del archivo de imagen. Si selecciona esta opción, la extensión del archivo de imagen no necesariamente debe brindarse. En tal caso, se utilizará la extensión predeterminada (como se indica a continuación).
  - *Extensión de archivo para SCP*: si se selecciona **Extensión automática por archivo**, puede indicar la extensión del archivo aquí. Cualquier archivo con esta extensión se descargará mediante SCP. Si no se ingresa ninguna extensión, se utilizará la extensión de archivo predeterminada **.scp**.
  - *Solo TFTP*: seleccione esta opción para indicar que solamente el protocolo TFTP debe usarse para la actualización automática.
  - *Solo SCP*: seleccione esta opción para indicar que solamente el protocolo SCP debe usarse para la actualización automática.
- **Configuración SSH para SCP**: cuando utilice SCP para descargar archivos de configuración, seleccione una de las siguientes opciones:
- **Autenticación del servidor SSH remoto**: haga clic en el enlace **Habilitar/Deshabilitar** para navegar hasta la página Autenticación del servidor SSH. Allí puede habilitar la autenticación del servidor SSH que se utilizará para la descarga e ingresar el servidor SSH si se le solicita.
- **Autenticación del cliente SSH**: haga clic en el enlace Credenciales de sistema para ingresar las credenciales de usuario en la página Autenticación del usuario SSH.
- **Definición del servidor de respaldo**: seleccione si el servidor de respaldo se especificará **Por dirección IP** o **Por nombre**.
- **Versión de IP**: seleccione si se usa una dirección IPv4 o IPv6.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - **Enlace local**: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de FE80, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - **Global**: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: seleccione la interfaz local de enlace (si se usa IPv6) en la lista.

PASO 3 Ingrese la siguiente información opcional que se utilizará si el servidor DHCP no proporciona la información solicitada.

- **Nombre o dirección IP del servidor de respaldo**: ingrese el nombre o la dirección IP del servidor de respaldo.

- **Nombre de archivo de configuración de respaldo**: ingrese el nombre del archivo de configuración de respaldo.
- **Nombre de archivo de imagen indirecto de respaldo**: ingrese el nombre de archivo de imagen indirecto que se utilizará. Se trata de un archivo que mantiene la ruta para la imagen. Ejemplo de un nombre de archivo de imagen indirecto: indirecto-cisco.scp. Este archivo contiene la ruta y el nombre de la imagen de firmware.

Se muestran los siguientes campos:

- **Dirección IP del último servidor de imagen o configuración automática**: dirección del último servidor de respaldo.
- **Último nombre de archivo de configuración automática**: nombre del último nombre de archivo de configuración.

PASO 4 Haga clic en **Aplicar**. Los parámetros se copian en el archivo de configuración en ejecución.

6

Administración

En esta sección, se describe cómo ver información del sistema y configurar varias opciones en el dispositivo.

Abarca los siguientes temas:

- **Modelos de dispositivo**
- **Configuración del sistema**
- **Configuración de consola (Soporte de velocidad autobaud)**
- **Interfaz de administración**
- **Cuentas de usuario**
- **Definición de la Caducidad de sesión por inactividad**
- **Configuración de la hora**
- **Registro del sistema**
- **Administración de archivos**
- **Reinicio del dispositivo**
- **Recursos de enrutamiento**
- **Estado**
- **Diagnósticos**
- **Detección: Bonjour**
- **Detección: LLDP**
- **Detección: CDP**
- **Ping**
- **Traceroute**

Modelos de dispositivo

Todos los modelos pueden administrarse completamente a través de la utilidad de configuración de switch basada en la Web.

En el modo del sistema Capa 2, el dispositivo funciona como un puente preparado para VLAN y reenvía los paquetes. En el modo del sistema Capa 3, el dispositivo realiza enrutamiento IPv4 y puenteo preparado para VLAN.

Cuando el dispositivo opera en el modo del sistema de capa 3, el límite de velocidad de VLAN y los reguladores de QoS no funcionan, pero sí otras funciones del modo avanzado de QoS.

NOTA Consulte **Convenciones para la asignación de nombres a las interfaces** para conocer las convenciones de denominación de puertos.

En la siguiente tabla, se describen varios modelos, la cantidad y tipo de puerto que poseen cada uno y la información de PoE.

Nombre de modelo	ID del producto (PID)	Descripción de los puertos del dispositivo	Energía dedicada a PoE	N.º de puertos compatibles con PoE
SG300-28	SRW2024-K9	24 puertos GE y 4 puertos de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	N/D	N/D
SG300-28P	SRW2024P-K9	24 puertos GE y 4 puertos de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	180W	24
SG300-52	SRW2048-K9	48 puertos GE y 4 puertos de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	N/D	N/D
SF300-08	SRW208-K9	8 puertos FE.	N/D	N/D
SF302-08	SRW208G-K9	8 puertos FE más 2 puertos GE	N/D	N/D
SF302-08MP	SRW208MP-K9	8 puertos FE más 2 puertos GE	124W	8
SF302-08P	SRW208P-K9	8 puertos FE más 2 puertos GE	62W	8

Nombre de modelo	ID del producto (PID)	Descripción de los puertos del dispositivo	Energía dedicada a PoE	N.º de puertos compatibles con PoE
SF300-24	SRW224G4-K9	24 puertos FE y 4 puertos GE de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	N/D	N/D
SF300-24P	SRW224G4P-K9	24 puertos FE y 4 puertos GE de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	180W	24
SF300-48	SRW248G4-K9	48 puertos FE y 4 puertos GE de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	N/D	N/D
SF300-48P	SRW248G4P-K9	48 puertos FE y 4 puertos GE de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	375 W	48
SF300-24MP	SF300-24M-K9	Switch administrable PoE 10/100 de 24 puertos	375 W	24
SG300-28MP	SRW2024P-K9	Switch Gigabit administrable PoE de 28 puertos	375 W	24
SG300-52P	SG300-52P-K9 V.0	Switch Gigabit administrable PoE de 52 puertos	375 W	48 puertos PoE
SG300-52MP	SG300-52MP-K9	Switch Gigabit administrable PoE de 52 puertos	740W	48
SG300-10SFP	SG300-10SFP-K9	Switch SFP Gigabit administrable de 10 puertos	N/D	N/D
ESW2-350G-52	ESW2-350G-52-K9	Switch Gigabit administrable de 52 puertos	N/D	N/D
ESW2-350G-52DC	ESW2-350G-52DC-K9	Switch Gigabit administrable de 52 puertos	N/D	N/D
SF302-08PP	SF302-08PP-K9 V.0	Switch administrable PoE 10/100 de 8 puertos	62W	8

Nombre de modelo	ID del producto (PID)	Descripción de los puertos del dispositivo	Energía dedicada a PoE	N.º de puertos compatibles con PoE
SF302-08MPP	SF302-08MPP-K9 V.0	Switch administrable PoE 10/100 de 8 puertos	124W	8
SG300-10PP	SG300-10PP-K9	Switch administrable PoE 10/100 de 8 puertos	62W	8
SG300-10MPP	SG300-10MPP-K9	Switch Gigabit administrable PoE de 10 puertos	124W	8
SF300-24PP	SF300-24PP-K9	Switch administrable PoE 10/100 de 24 puertos	180W	24
SF300-24PP	SF300-24PP-K9	Switch administrable PoE 10/100 de 24 puertos	180W	24
SF300-48PP	SF300-48PP-K9	Switch administrable PoE 10/100 de 48 puertos	375 W	48
SG300-28SFP	SG300-28SFP-K9	Switch SFP Gigabit administrable de 28 puertos	NA	NA

Configuración del sistema

En la página Resumen del sistema, se proporciona una vista gráfica del dispositivo, donde se muestra el estado del dispositivo, la información de hardware, la información de la versión del firmware, el estado general de PoE y otros elementos.

Visualización del resumen del sistema

Para ver información del sistema:

PASO 1 Haga clic en **Estado y estadísticas** > **Resumen del sistema**.

Información del sistema:

- Modo operativo del sistema: descripción del modo de funcionamiento del sistema.
- **Descripción del sistema**: una descripción del sistema.

- **Ubicación del sistema**: ubicación física del dispositivo. Haga clic en **Editar** para ir a la página Configuración del sistema e ingresar este valor.
- **Contacto del sistema**: el nombre de una persona de contacto. Haga clic en **Editar** para ir a la página Configuración del sistema e ingresar este valor.
- **Nombre del host**: el nombre del dispositivo. Haga clic en **Editar** para ir a la página Configuración del sistema e ingresar este valor. De manera predeterminada, el nombre de host del dispositivo está compuesto por la palabra *device* combinada con los tres bytes menos importantes de la dirección MAC del dispositivo (los seis dígitos hexadecimales del extremo derecho).
- **ID de objeto de sistema**: el sistema lo utiliza para administrar las funciones del dispositivo.
- **Tiempo de actividad del sistema**: el tiempo transcurrido desde el último reinicio.
- **Hora actual**: la hora actual del sistema.
- **Dirección MAC base**: la dirección MAC del dispositivo.
- **Tramas jumbo**: estado de compatibilidad con tramas jumbo. Esta compatibilidad se puede activar o desactivar a través de la página Configuración de puertos del menú Administración de puertos.

  NOTA La compatibilidad con tramas jumbo tiene efecto solo después de activarla y luego de reiniciar el dispositivo.

Estado de los servicios TCP/UDP:

- **Servicio HTTP**: muestra si HTTP está habilitado o deshabilitado.
- **Servicio HTTPS**: muestra si HTTPS está habilitado o deshabilitado.
- **Servicio SNMP**: muestra si SNMP está habilitado o deshabilitado.
- **Servicio Telnet**: muestra si Telnet está habilitado o deshabilitado.
- **Servicio SSH**: muestra si SSH está habilitado o deshabilitado.

Información del software:

- **Versión de firmware (imagen activa)**: número de versión del firmware de la imagen activa.
- **Suma de comprobación de firmware MD5 (imagen activa)**: suma de comprobación MD5 de la imagen activa.
- **Versión de firmware (no activa)**: número de versión del firmware de la imagen no activa.
- **Suma de comprobación de firmware MD5 (imagen no activa)**: suma de comprobación MD5 de la imagen no activa.
- **Versión de inicio**: número de versión de inicio.
- **Suma de comprobación MD5 del inicio**: suma de comprobación MD5 de la versión de inicio.

- **Configuración regional**: configuración regional del primer idioma. (Es siempre inglés).
- **Versión del idioma**: la versión del paquete de idiomas del primer idioma o inglés.
- **Suma de comprobación de idioma MD5**: suma de comprobación MD5 del archivo de idioma.

Información de energía para PoE: (en dispositivos que admiten PoE)

- **Máxima energía PoE disponible (W)**: energía máxima disponible que se puede suministrar a través de PoE.
- **Consumo de energía PoE total (W)**: energía PoE total suministrada a los dispositivos PoE conectados.
- **Modo de energía PoE**: límite del puerto o límite de la clasificación.

Configuración del sistema

Para ingresar la configuración del sistema:

PASO 1 Haga clic en **Administración** > **Configuración del sistema**.

PASO 2 Vea o modifique la configuración del sistema.

- **Descripción del sistema**: se muestra una descripción del dispositivo.
- **Ubicación del sistema**: ingrese la ubicación física del dispositivo.
- **Contacto del sistema**: ingrese el nombre de una persona de contacto.
- **Nombre del host**: seleccione el nombre de host de este dispositivo. Se utiliza en la solicitud de comandos CLI:
  - *Usar predeterminado*: el nombre de host predeterminado (nombre del sistema) de estos switches es: *switch123456*, donde 123456 representa los últimos tres bytes de la dirección MAC del dispositivo en formato hexadecimal.
  - *Definida por el usuario*: ingrese el nombre del host. Usted solo puede utilizar letras, dígitos y guiones. Los nombres de host no pueden comenzar ni terminar con un guión. No se permite ningún otro símbolo, carácter de puntuación ni espacio en blanco (como se especifica en RFC1033, 1034, 1035).
- **Modo del sistema**: seleccione el modo del sistema de este dispositivo.

  NOTA Si modifica el modo del sistema después de hacer clic en **Aplicar**, el sistema deberá reiniciarse y el archivo de configuración de inicio se eliminará luego del inicio.
  - *L2*: seleccione esta opción para colocar el dispositivo en modo de capa 2 del sistema.
  - *L3*: seleccione esta opción para colocar el dispositivo en modo de capa 3 del sistema.

- **Configuración de mensajes personalizados**: se pueden configurar los siguientes mensajes:
  - **Mensaje de registro**: ingrese el texto para que aparezca texto en la página de inicio sesión antes de iniciar sesión. Haga clic en **Vista previa** para ver los resultados.
  - **Mensaje de bienvenida**: ingrese el texto para que aparezca texto en la página de inicio sesión después de iniciar sesión. Haga clic en **Vista previa** para ver los resultados.

NOTA Cuando define un mensaje de registro de la utilidad de configuración de interfaz web, también activa el anuncio para las interfaces CLI (Consola, Telnet y SSH).

PASO 3 Haga clic en **Aplicar** para guardar los valores en el archivo de configuración en ejecución.

Configuración de consola (Soporte de velocidad autobaud)

La velocidad de puerto de consola se puede configurar en una de las siguientes velocidades: 4800, 9600, 19200, 38400, 57600 y 115200 o en detección automática.

Si se seleccionó la detección automática, el dispositivo detectará la velocidad de la consola de manera automática.

Cuando no se habilita la detección automática, la velocidad del puerto de la consola se configura automáticamente en la última velocidad configurada de forma manual a (115,200 de manera predeterminada).

Cuando la detección automática está habilitada pero la velocidad en baudios de la consola todavía es desconocida, el sistema utiliza la velocidad 115,200 para visualizar el texto (por ejemplo, la información de inicio).

Después de que la detección automática se haya activado en la página Configuración de la consola, puede activarse al conectar la consola al dispositivo y presionar la tecla Intro dos veces. El dispositivo detecta la velocidad en baudios de manera automática.

Para habilitar la detección automática o configurar manualmente la velocidad en baudios de la consola:

PASO 1 Haga clic en **Administración** > **Configuración de la consola**.

PASO 2 Seleccione uno de los siguientes:

- **Detección automática**: la velocidad en baudios de la consola se detecta automáticamente.
- **Estático**: seleccione una de las velocidades disponibles.

Interfaz de administración

Consulte **Administración e interfaces IPv4**.

Cuentas de usuario

Consulte **Definición de usuarios**.

Definición de la Caducidad de sesión por inactividad

La opción *Caducidad de sesión por inactividad* permite configurar los intervalos de tiempo que las sesiones de administración pueden permanecer inactivas antes de que caduquen y usted deba iniciar sesión nuevamente para establecer una de las siguientes sesiones:

- **Tiempo de espera de la sesión HTTP**
- **Tiempo de espera de la sesión HTTPS**
- **Caducidad de sesión de la consola**
- **Tiempo de espera de la sesión de Telnet**
- **Tiempo de espera de la sesión SSH**

Para configurar la caducidad de sesión por inactividad para diferentes tipos de sesiones:

PASO 1 Haga clic en **Administración** > **Caducidad de sesión por inactividad**.

PASO 2 Seleccione la caducidad para cada sesión en la lista correspondiente. El valor predeterminado de caducidad es de 10 minutos.

PASO 3 Haga clic en **Aplicar** para establecer la configuración en el dispositivo.

Configuración de la hora

Consulte **Administración: Configuración de hora**.

Registro del sistema

Consulte **Administración: Registro del sistema**.

Administración de archivos

Consulte **Administración: Administración de archivos**.

Reinicio del dispositivo

Algunos cambios de configuración, como activar el soporte de tramas jumbo, requieren que se reinicie el sistema para que surtan efecto. Sin embargo, al reiniciar el dispositivo se elimina la configuración en ejecución, por lo que es fundamental guardarla en la configuración de inicio antes de reiniciar el dispositivo. Al hacer clic en **Aplicar** no se guarda la configuración en la configuración de inicio. Para obtener más información sobre archivos y tipos de archivo, consulte la sección **Archivos del sistema**.

Usted puede hacer una copia de seguridad de la configuración del dispositivo a través de *Administración > Administración de archivos > Guardar/copiar configuración*, o al hacer clic en **Guardar** en la parte superior de la ventana. También puede cargar la configuración desde un dispositivo remoto. Consulte la sección **Descarga/Copia de seguridad de configuración/Registro**.

Puede que desee configurar la hora de reinicio para algún momento en el futuro. Esto podría ocurrir, por ejemplo, en uno de los siguientes casos:

- Está realizando acciones en un dispositivo remoto y estas acciones pueden provocar la pérdida de conectividad al dispositivo remoto. La programación previa de un reinicio restaura la configuración funcional y permite restaurar la conectividad al dispositivo remoto. Si estas acciones se realizan correctamente, se puede cancelar el reinicio con retardo.
- La recarga del dispositivo provoca la pérdida de conectividad en la red; al utilizar el reinicio con retardo, puede programar el reinicio a una hora que sea más conveniente para los usuarios (por ejemplo, a la noche).

Para reiniciar el dispositivo:

PASO 1 Haga clic en **Administración** > **Reiniciar**.

PASO 2 Haga clic en el botón **Reiniciar** para reiniciar el dispositivo.

- **Reiniciar**: reinicia el dispositivo. Dado que al reiniciar el dispositivo, se descarta la información que no se haya guardado de la configuración en ejecución, debe hacer clic en **Guardar** en la esquina superior derecha de cualquier ventana para conservar la configuración durante el proceso de inicio. Si la opción Guardar no aparece, la configuración en ejecución coincide con la configuración de inicio y no es necesario realizar acción alguna.
- **Cancelar reinicio**: cancela el reinicio que se haya programado para algún momento futuro.

  Las opciones disponibles son las siguientes:

  - *Inmediato*: se reinicia de inmediato.
  - *Fecha*: ingrese la fecha (mes/día) y hora (hora y minutos) del reinicio programado. Esto programa la recarga del software para que se produzca a la hora especificada (utilizando un reloj de 24 horas). Si especifica el mes y el día, la recarga se programa para que ocurra en la fecha y hora especificadas. Si no especifica el mes ni el día, la recarga ocurre en la hora especificada el día actual (si la hora especificada es posterior a la hora actual) o al día siguiente (si la hora especificada es anterior a la hora actual). Si especifica 00:00, la recarga se programa para la medianoche. La recarga debe ocurrir dentro de los 24 días.

    NOTA Esta opción solo se puede usar si la hora del sistema se estableció manualmente o mediante SNTP.

  - *En*: reinicia dentro de la cantidad de horas y minutos especificados. La cantidad de tiempo máximo que puede transcurrir es 24 días.
- **Restablecer valores predet. fábrica**: se reinicia el dispositivo utilizando la configuración predeterminada de fábrica. Este proceso elimina el archivo de Configuración de inicio y el archivo de configuración de respaldo.

  El archivo de configuración de duplicado no se pierde cuando se restablecen los valores predeterminados de fábrica.
- **Borrar archivo de configuración de inicio**: seleccione esta opción para borrar la configuración de inicio en el dispositivo la próxima vez que se inicie.

  NOTA La eliminación del archivo de configuración de inicio y el reinicio subsiguiente no es lo mismo que el restablecimiento a los valores predeterminados de fábrica. La restauración a valores predeterminados de fábrica es un proceso más intrusivo.

Recursos de enrutamiento

Use la página Recursos de enrutamiento para mostrar la asignación de TCAM y modificar el tamaño de TCAM total en el modo de Capa 3. Las entradas de la TCAM se dividen en los siguientes grupos:

- **Entradas IP**: las entradas de la TCAM reservadas para las rutas estáticas IP, las direcciones IP en el dispositivo y los hosts IP. Cada tipo genera la siguiente cantidad de entradas de la TCAM:
  - Rutas estáticas IPv4: una entrada por ruta
  - Direcciones IP: dos entradas por dirección IP
  - Hosts IP: una entrada por host
- **Entradas no IP**: entradas de la TCAM reservadas para otras aplicaciones, como reglas de ACL, reguladores de CoS y límites de velocidad de VLAN.

Para ver y modificar los recursos de enrutamiento cuando el dispositivo está en el modo de Capa 3:

PASO 1 Haga clic en **Administración** > **Recursos de enrutamiento**.

Se muestran los siguientes campos:

- **Vecinos (1 entrada de la TCAM por vecino)**: **Recuento** es la cantidad de vecinos registrados en el dispositivo y **Entradas de la TCAM** es la cantidad total de entradas de la TCAM que se utilizan para los vecinos.
- **Interfaces (2 entradas de la TCAM por interfaz)**: **Recuento** es la cantidad de direcciones IP en las interfaces del dispositivo y **Entradas de la TCAM** es la cantidad total de entradas de la TCAM que se utilizan para las direcciones IP.
- **Rutas (1 entrada de la TCAM por ruta)**: **Recuento** es la cantidad de rutas registradas en el dispositivo y **Entradas de la TCAM** es la cantidad de entradas de la TCAM que se utilizan para las rutas.
- **Total**: muestra la cantidad de entradas de la TCAM que se utilizan actualmente.
- **Entradas máximas**: seleccione una de las siguientes opciones**:**
  - *Usar predeterminado*: la cantidad de entradas de la TCAM disponibles para las entradas IP es el 25% del tamaño de la TCAM.
  - *Definido por el usuario*: ingrese un valor.

Tabla de recursos TCAM

Se muestran los siguientes campos para cada unidad:

- **Entradas máximas de la TCAM para reglas IPv4 y no IP**: cantidad máxima de entradas de TCAM disponibles para enrutamiento y enrutamiento de multidifusión.

- **Enrutamiento IPv4**
  - **En uso:** cantidad de entradas de TCAM que se utilizan para el enrutamiento IPv4.
  - **Máximo:** máximo de entradas de la TCAM disponibles para el enrutamiento IPv4.
- **Reglas no IP**
  - **En uso: cantidad de entradas de TCAM que se utilizan para las reglas no IP.**
  - **Máximo:** máximo de entradas de la TCAM disponibles para reglas no IP.

Debe guardar su configuración actual antes de cambiar la Configuración de asignación de TCAM.

NOTA En la parte inferior de esta página, se muestra un resumen de las entradas de la TCAM que están realmente en uso y disponibles. Si desea obtener una explicación de los campos, consulte **Utilización de la TCAM**.

PASO 2 Guarde la nueva configuración: haga clic en **Aplicar**. Esto comprueba la probabilidad de la asignación de TCAM. Si es incorrecta, se muestra un mensaje de error. Si es correcta, la asignación se guarda en el archivo de configuración en ejecución y se realiza un reinicio.

Estado

En la página Estado, se controla el estado de cada ventilador en todos los dispositivos con ventiladores. Según el modelo, hay uno o más ventiladores en un dispositivo. Algunos modelos no tienen ventiladores.

Algunos dispositivos cuentan con un sensor de temperatura para proteger el hardware del sobrecalentamiento. En ese caso, el dispositivo realiza lo siguiente si se sobrecalienta y durante el período de enfriamiento posterior al sobrecalentamiento:

Evento	Acción
Al menos un sensor de temperatura excede el umbral de advertencia.	Se genera lo siguiente: ▪ Mensaje SYSLOG ▪ Trampa SNMP

Evento	Acción
Al menos un sensor de temperatura excede el umbral crítico.	Se genera lo siguiente: ▪ Mensaje SYSLOG ▪ Trampa SNMP Se realizan las siguientes acciones: ▪ El indicador LED del sistema se establece en ámbar permanente (si el hardware lo admite). ▪ Desactivar los puertos: cuando la temperatura crítica se haya excedido durante dos minutos, todos los puertos se cerrarán. ▪ (En dispositivos que admiten PoE) Desactive los circuitos de PoE para que consuman menos energía y emitan menos calor.
Se excedió el período de enfriamiento después del umbral crítico (todos los sensores son inferiores al umbral de advertencia de -2 °C).	Después de que todos los sensores se enfrían al umbral de advertencia de -2 °C, se volverá a activar PHY y volverán a estar activos todos los puertos. Si el estado del ventilador es correcto, los puertos se activan. (En dispositivos que admiten PoE) Los circuitos de PoE están activados.

Para ver los parámetros de integridad del dispositivo, haga clic en **Estado y estadísticas** > **Estado**.

En la página Integridad se muestran los siguientes campos:

- **Estado del ventilador**: estado del ventilador. Los siguientes valores son posibles:
  - *Correcto*: el ventilador funciona normalmente.
  - *Error*: el ventilador no funciona normalmente.
  - *N/D*: el ID de ventilador no se corresponde con el modelo específico.
- **Dirección del ventilador**: (en dispositivos importantes) la dirección en que funcionan los ventiladores (por ejemplo: desde adelante hacia atrás).

- **Temperatura**: las opciones son:
  - *Correcto*: la temperatura está por debajo del umbral de advertencia.
  - *Advertencia*: la temperatura está entre el umbral de advertencia y el umbral crítico.
  - *Crítico*: la temperatura está por encima del umbral crítico.

Diagnósticos

Consulte **Administración: Diagnóstico**.

Detección: Bonjour

Consulte **Bonjour**.

Detección: LLDP

Consulte **Configuración de LLDP**.

Detección: CDP

Consulte **Configuración de CDP**.

Ping

Ping es una utilidad que prueba si se puede obtener acceso a un host remoto y mide el tiempo de viaje de ida y vuelta de los paquetes enviados desde el dispositivo a un dispositivo de destino.

Ping funciona enviando paquetes de petición de eco de Internet Control Message Protocol (ICMP, Protocolo de mensajes de control de Internet) al host de destino y esperando una respuesta ICMP, a veces llamada pong. Mide el tiempo de viaje de ida y vuelta y registra la pérdida de paquetes.

Para hacer ping a un host:

PASO 1 Haga clic en **Administración > Ping**.

PASO 2 Complete los siguientes campos para configurar el ping:

- **Definición de host**: seleccione si la interfaz de origen se especificará por dirección IP o nombre. Este cambio afecta a las interfaces que se muestran en el campo IP de origen, como se describe a continuación.
- **Versión de IP**: si la interfaz de origen se identifica por su dirección IP, seleccione IPv4 o IPv6 para indicar que se ingresará en el formato seleccionado.
- **IP de origen**: seleccione la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen para comunicarse con el destino. Si el campo Definición de host es Por nombre, se mostrarán todas las direcciones IPv4 e IPv6 en este campo desplegable. Si el campo Definición de host es Por dirección IP, solo se mostrarán las direcciones IP existentes del tipo especificado en el campo Versión IP.

  NOTA Si se selecciona la opción Automática, el sistema computa la dirección de origen en función de la dirección de destino.
- **Tipo de dirección IPv6 de destino**: seleccione Enlace local o Global como el tipo de dirección IPv6 para ingresar la dirección IP de destino.
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: si el tipo de dirección IPv6 es Enlace local, seleccione desde dónde se recibe.
- **Nombre/Dirección IP de destino**: dirección o nombre de host del dispositivo al que se hará ping. La definición del host determina si es una dirección IP o un nombre de host.
- **Intervalo de ping**: cantidad de tiempo que el sistema espera entre paquetes de ping. El ping repite la cantidad de tiempos configurados en el campo **Cantidad de pings**, ya sea que el ping sea correcto o no. Elija utilizar el intervalo predeterminado o especifique su propio valor.
- **Cantidad de pings:** la cantidad de veces que se realiza la operación de ping. Elija utilizar el valor predeterminado o especifique su propio valor.
- **Estado**: muestra si el ping se realizó con éxito o si falló.

PASO 3 Haga clic en **Activar ping** para hacer ping al host. Aparece el estado de ping y se agrega un mensaje a la lista de mensajes donde se indica el resultado de la operación de ping.

PASO 4 Visualice los resultados de ping en la sección **Estado y contadores de ping** de la página.

Traceroute

Traceroute detecta las rutas IP cuyos paquetes se reenviaron al enviar un paquete IP al host de destino y de regreso al dispositivo. En la página Traceroute, se muestra cada salto entre el dispositivo y el host de destino con el tiempo de viaje de ida y vuelta a cada uno de esos saltos.

PASO 1 Haga clic en **Administración > Traceroute**.

PASO 2 Configure Traceroute, ingrese la información en los siguientes campos:

- **Definición de host**: seleccione si desea que los hosts se identifiquen por su dirección IP o nombre.
- **Versión de IP**: si el host se identifica por su dirección IP, seleccione IPv4 o IPv6 para indicar que se ingresará en el formato seleccionado.
- **IP de origen**: seleccione la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen para los mensajes de comunicación. Si el campo Definición de host es Por nombre, se mostrarán todas las direcciones IPv4 e IPv6 en este campo desplegable. Si el campo Definición de host es Por dirección IP, solo se mostrarán las direcciones IP existentes del tipo especificado en el campo Versión IP.
- **Dirección IP/nombre del host**: ingrese el nombre o la dirección de host.
- **TTL**: ingrese la cantidad máxima de saltos que permite Traceroute. Se utiliza para evitar un caso en el que las tramas enviadas lleguen a un bucle sin fin. El comando traceroute termina cuando se alcanza el destino o cuando se llega a este valor. Para usar el valor predeterminado (30), seleccione **Usar predeterminado**.
- **Caducidad**: ingrese la cantidad de tiempo que el sistema espera el regreso de una trama antes de declararla perdida o seleccione **Usar predeterminado**.

PASO 3 Haga clic en **Activar Traceroute**. Se realiza la operación.

Aparece una página donde se muestran el RTT (Round Trip Time, tiempo de viaje de ida y vuelta) y el estado de cada viaje en los campos:

- **Índice**: se muestra el número del salto.
- **Host**: muestra una parada a lo largo de la ruta hasta el destino.
- **Tiempo de viaje de ida y vuelta** *(1-3)*: muestra el tiempo del viaje de ida y vuelta en (ms) para la primera a tercera trama y el estado de la primera a la tercera operación.

7

Administración: Configuración de hora

Los relojes sincronizados del sistema brindan un marco de referencia entre todos los dispositivos de la red. La sincronización de la hora de la red es de importancia fundamental porque en todos los aspectos de la administración, la seguridad, la planificación y la depuración de una red se debe determinar cuándo se producen los eventos. Sin relojes sincronizados, la correlación exacta de archivos de registro entre estos dispositivos al realizar el seguimiento de las brechas en la seguridad o del uso de la red es imposible.

La hora sincronizada también reduce la confusión en los sistemas de archivos compartidos, ya que es importante que las horas de modificación concuerden, independientemente de la máquina en la que residen los sistemas de archivos.

Por estos motivos, es importante que la hora configurada en todos los dispositivos de la red sea exacta.

NOTA El dispositivo admite el SNTP (Simple Network Time Protocol, protocolo simple de tiempo de redes) y, cuando está activado, el dispositivo sincroniza dinámicamente la hora del dispositivo con la hora del servidor SNTP. El dispositivo funciona solo como cliente SNTP y no puede proporcionar servicios de hora a otros dispositivos.

En esta sección se describen las opciones para configurar la hora del sistema, la zona horaria y el horario de verano (DST, Daylight Savings Time). Abarca los siguientes temas:

- **Opciones de la hora del sistema**
- **Modos SNTP**
- **Configuración de la hora del sistema**

Opciones de la hora del sistema

El usuario puede configurar manualmente la hora del sistema, de forma dinámica desde un servidor SNTP, o sincronizarla desde la computadora que ejecuta la interfaz de usuario gráfica GUI. Si se elige un servidor SNTP, la configuración manual de hora se sobrescribe cuando se establecen las comunicaciones con el servidor.

Como parte del proceso de inicio, el dispositivo siempre configura la hora, la zona horaria y el DTS. Estos parámetros se obtienen desde la computadora que ejecuta la interfaz de usuario gráfica, del SNTP y valores configurados manualmente o, si todos los demás fallan, mediante los valores predeterminados de fábrica.

Hora

Los siguientes métodos están disponibles para configurar la hora del sistema en el dispositivo:

- **Manual**: el usuario debe configurar manualmente la hora.
- **Desde el explorador**: se puede recibir la hora desde la computadora a través de la información del explorador.

  La configuración de la hora de la computadora se guarda en el archivo Configuración en ejecución. Debe copiar la configuración en ejecución en la configuración de inicio para permitir que el dispositivo utilice la hora de la computadora tras el reinicio. La hora posterior al reinicio se establece durante la primera conexión web al dispositivo.

  Cuando se configura esta función por primera vez, si la hora no fue ya establecida, el dispositivo establece la hora desde la computadora.

  Este método de configuración de la hora funciona con conexiones HTTP y con conexiones HTTPS.
- **SNTP**: la hora se puede recibir de los servidores SNTP horario. El SNTP garantiza la sincronización exacta de la hora de la red del dispositivo hasta el milisegundo mediante el servidor SNTP para la fuente de reloj. Cuando deba especificar un servidor SNTP, si opta por identificarlos por nombre de host, la guía de interfaz del usuario da tres recomendaciones:
  - time-a.timefreq.bldrdoc.gov
  - time-b.timefreq.bldrdoc.gov
  - time-c.timefreq.bldrdoc.gov

Una vez que se haya establecido la hora con cualquiera de las fuentes antes mencionadas, el navegador no volverá a establecerla.

NOTA El método recomendado para la configuración de la hora es SNTP.

Zona horaria y horario de verano (DST)

La zona horaria y el DST se pueden configurar en el dispositivo de las siguientes maneras:

- Configuración dinámica del dispositivo a través de un servidor DHCP, en donde:
  - El DST dinámico, cuando está habilitado y disponible, siempre tiene prioridad sobre la configuración manual del DST.
  - Si el servidor que proporciona los parámetros de la fuente falla o el usuario deshabilita la configuración dinámica, se usa la configuración manual.
  - La configuración dinámica de la zona horaria y el DST continúa después de que el tiempo de concesión de la dirección IP ha finalizado.

- La configuración manual de la zona horaria y del DST se convierte en el DST y la zona horaria operativos, solo si la configuración dinámica se deshabilita o falla.

  NOTA El servidor DHCP debe suministrar la opción DHCP 100 para que se lleve a cabo la configuración dinámica de la zona horaria.

Modos SNTP

El dispositivo puede recibir la hora del sistema desde un servidor SNTP de una de las siguientes formas:

- **Recepción de difusión del cliente (modo pasivo)**: los servidores SNTP difunden la hora, y el dispositivo escucha esta difusión. Cuando el dispositivo está en este modo, no hay necesidad de definir un servidor SNTP de unidifusión.
- **Transmisión de difusión de cliente (modo activo)**: el dispositivo, como cliente SNTP, solicita periódicamente las actualizaciones de horario del SNTP. Este modo funciona de cualquiera de las dos maneras siguientes:
  - **Modo cliente de cualquier tipo de difusión SNTP**: el dispositivo difunde paquetes de solicitud de hora a todos los servidores SNTP en la subred y espera una respuesta.
  - **Modo de servidor SNTP de unidifusión**: el dispositivo envía consultas de unidifusión a la lista de servidores SNTP configurados manualmente y espera una respuesta.

El dispositivo admite todos los modos activos al mismo tiempo y selecciona el mejor sistema horario que proviene de un servidor SNTP, en función de un algoritmo basado en el estrato más cercano (distancia desde el reloj de referencia).

Configuración de la hora del sistema

Selección de la fuente de la hora del sistema

Utilice la página Hora del sistema para seleccionar la fuente de la hora del sistema. Si la fuente es manual, puede ingresar la hora aquí.

PRECAUCIÓN Si la hora del sistema se configura manualmente y el dispositivo se reinicia, es necesario volver a ingresar la configuración manual de la hora.

Para definir la hora del sistema:

PASO 1 Haga clic en **Administración** > **Configuración de la hora** > **Hora del sistema**.

Se muestran los siguientes campos:

- **Hora actual (estática)**: hora del sistema en el dispositivo. Muestra la zona horaria de DHCP o el acrónimo para la zona horaria definida por el usuario si ese fuera el caso.
- **Servidor sincronizado por última vez**: dirección, estrato y tipo de servidor SNTP desde el que se tomó la hora del sistema por última vez.

PASO 2 Ingrese los siguientes parámetros:

Configuración de fuente de reloj: seleccione la fuente usada para configurar el reloj del sistema.

- **Fuente de reloj principal (Servidores SNTP)**: si habilita esta opción, la hora del sistema se obtiene de un servidor SNTP. Para utilizar esta función, también debe configurar una conexión a un servidor SNTP en la página Configuración de la interfaz del SNTP. Como opción, aplique la autenticación de las sesiones SNTP mediante la página Autenticación de SNTP.
- **Fuente de reloj alternativa (PC a través de sesiones activas de HTTP/HTTPS)**: seleccione esta opción para establecer la fecha y la hora de la computadora de configuración que utiliza el protocolo HTTP.

  NOTA La Configuración de la fuente del reloj debe configurarse para cualquiera de las opciones anteriores, para que funcione la RIP con autenticación MD5. Esto también ayuda a las funciones asociadas con la hora, por ejemplo: ACL basada en horarios, Puerto, autenticación de puerto 802.1, funciones que están habilitadas en algunos dispositivos.

Configuración manual: establezca la fecha y la hora manualmente. La hora local se usa cuando no hay una fuente de hora alternativa, como un servidor SNTP:

- **Fecha**: ingrese la fecha del sistema.
- **Hora local**: ingrese la hora del sistema.

Configuración de la hora: la hora local se utiliza a través del servidor DHCP o del desplazamiento de zona horaria.

- **Obtener zona horaria desde el DHCP**: seleccione esta opción para activar la configuración dinámica de la zona horaria y del DST desde el servidor DHCP. La posibilidad de configurar uno de estos parámetros o ambos depende de la información que se encuentra en el paquete DHCP. Si se activa esta opción, *el cliente DHCP debe activarse en el dispositivo*.

  NOTA El cliente DHCP admite la opción 100, lo cual posibilita la configuración de zona horaria dinámica.
- **Zona horaria desde el DHCP**: muestra el acrónimo de la zona horaria que se configuró desde el servidor DHCP. Este acrónimo aparece en el campo **Hora real**.

- **Desplazamiento de zona horaria**: seleccione la diferencia de horas entre la *Hora del meridiano de Greenwich* (GMT) y la hora local. Por ejemplo, el desplazamiento de zona horaria para París es GMT +1, mientras que el desplazamiento de zona horaria para Nueva York es GMT –5.
- **Acrónimo de zona horaria**: ingrese un nombre que represente esta zona horaria. Este acrónimo aparece en el campo **Hora real**.

Configuración de horario de verano: seleccione cómo se define DST:

- **Horario de verano**: seleccione esta opción para habilitar el horario de verano.
- **Desplazamiento horario**: ingrese la cantidad de desplazamiento en minutos de GMT desde 1 hasta 1440. El valor predeterminado es 60.
- **Tipo de horario de verano**: haga clic en uno de los siguientes:
  - *EE. UU.*: el DST se establece de acuerdo con las fechas utilizadas en EE. UU.
  - *Europeo*: el DST se establece según las fechas que se usan en la Unión Europea y en otros países que usan este estándar.
  - *Por fechas*: el DST se establece manualmente, por lo general, para un país que no sea EE. UU. o un país europeo. Ingrese los parámetros descritos a continuación.
  - *Recurrente*: el DST se produce en la misma fecha todos los años.

  Al seleccionar *Por fechas* se puede personalizar el inicio y el fin del DST:

  - **Del**: día y hora en que comienza el DST.
  - **Al**: día y hora en que termina el DST.

  Al seleccionar *Recurrente* se puede personalizar el inicio y la detención del DST:

- **Del**: fecha en la que comienza el DST cada año.
  - *Día*: día de la semana en el que comienza el DST cada año.
  - *Semana*: semana dentro del mes desde la que comienza el DST cada año.
  - *Mes*: mes del año en el que el DST comienza cada año.
  - *Hora*: hora a la que el DST comienza cada año.
- **Al**: fecha en la que termina el DST cada año. Por ejemplo, el DST termina localmente cada cuarto viernes de octubre a las 5:00 a. m. Los parámetros son:
  - *Día*: día de la semana en el que termina el DST cada año.
  - *Semana*: semana dentro del mes en la que termina el DST cada año.
  - *Mes*: mes del año en el que el DST termina cada año.

- *Hora*: hora en la que el DST termina cada año.

PASO 3 Haga clic en **Aplicar**. Los valores de horario del sistema se escriben en el archivo Configuración en ejecución.

Incorporación de un servidor SNTP de unidifusión

Se pueden configurar hasta 16 servidores SNTP de unidifusión.

NOTA Para especificar un servidor SNTP de unidifusión por nombre, primero debe configurar los servidores DNS en el dispositivo (consulte **Configuración DNS**).

Para añadir un servidor SNTP de unidifusión:

PASO 1 Haga clic en **Administración** > **Configuración de la hora** > **SNTP de unidifusión**.

PASO 2 Ingrese los siguientes campos:

- **Unidifusión del cliente SNTP**: seleccione para activar en el dispositivo el uso de clientes de unidifusión predefinidos por SNTP con servidores SNTP de unidifusión.
- **Interfaz de origen IPv4**: seleccione la interfaz IPv4 cuya dirección IPv4 se utilizará como dirección IPv4 de origen en los mensajes usados para la comunicación con el servidor SNTP.
- **Interfaz de origen IPv6** : seleccione la interfaz IPv6 cuya dirección IPv6 se utilizará como dirección IPv6 de origen en los mensajes usados para la comunicación con el servidor SNTP.

  NOTA Si se selecciona la opción Automática, el sistema toma la dirección IP de origen de la dirección IP definida en la interfaz de salida.

En esta página se muestra la siguiente información de cada servidor de unidifusión SNTP:

- **Servidor SNTP**: dirección IP del servidor SNTP. El servidor preferido, o nombre de host, se elige según su nivel de estrato.
- **Intervalo de consulta**: muestra si las consultas están habilitadas o deshabilitadas.
- **ID de clave de autenticación**: identificación de la clave que se usa para establecer comunicaciones entre el servidor SNTP y el dispositivo.
- **Nivel de estrato**: distancia desde el reloj de referencia expresada como valor numérico. Un servidor SNTP no puede ser el servidor principal (nivel de estrato 1) a menos que se habilite el intervalo de consulta.

- **Estado**: estado del servidor SNTP. Los valores posibles son:
  - *Activo*: el servidor SNTP está funcionando normalmente.
  - *Inactivo*: el servidor SNTP no está disponible en este momento.
  - *Desconocido*: el dispositivo está buscando el servidor SNTP.
  - *En proceso*: se produce cuando el servidor SNTP no ha confía plenamente en su propio servidor horario (es decir, al iniciar el servidor NTP por primera vez).
- **Última respuesta**: fecha y hora de la última vez que se recibió una respuesta del servidor SNTP.
- **Desplazamiento**: el desplazamiento estimado del reloj del servidor en relación con el reloj local, en milisegundos. El host determina el valor de este desplazamiento con el algoritmo que se describe en RFC 2030.
- **Retraso**: el retraso de ida y vuelta estimado del reloj del servidor en relación con el reloj local en el trayecto de red que hay entre ellos, en milisegundos. El host determina el valor de este retraso con el algoritmo que se describe en RFC 2030.
- **Origen**: cómo se define el servidor SNTP, por ejemplo: manualmente o desde el servidor DHCPv6.
- **Interfaz**: interfaz en que se reciben los paquetes.

PASO 3 Para añadir un servidor SNTP de unidifusión, habilite la **Unidifusión de cliente SNTP**.

PASO 4 Haga clic en **Add**.

PASO 5 Ingrese los siguientes parámetros:

- **Definición del servidor**: seleccione si el servidor SNTP será identificado por su dirección IP o si usted seleccionará un servidor SNTP conocido por nombre de la lista.

NOTA Para especificar un servidor SNTP conocido, el dispositivo debe estar conectado a Internet y configurado con un servidor DNS o configurado de manera que un servidor DNS se identifique mediante DHCP. (Consulte **Configuración DNS**).

- **Versión de IP**: seleccione la versión de la dirección IP: **Versión 6** o **Versión 4**.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.

- **Interfaz local de enlace**: seleccione la interfaz local de enlace (si se selecciona Enlace local como Tipo de dirección IPv6) en la lista.
- **Dirección IP de servidor SNTP**: ingrese la dirección IP del servidor SNTP. El formato depende de qué tipo de dirección se ha seleccionado.
- **Servidor SNTP**: seleccione el nombre del servidor SNTP de una lista de servidores NTP conocidos. Si elige **otro**, ingrese el nombre de host del servidor SNTP en el campo adyacente.
- **Intervalo de consulta**: seleccione para habilitar las consultas del servidor SNTP sobre información de la hora del sistema. Se consultan todos los servidores NTP que están registrados para consultas, y se selecciona el reloj del servidor con el nivel de estrato (distancia que hay con respecto al reloj de referencia) más bajo accesible. El servidor con el estrato más bajo es el servidor primario. El servidor con el siguiente estrato más bajo es un servidor secundario, y así sucesivamente. Si el servidor primario está inactivo, el dispositivo consulta todos los servidores con la configuración de consulta activada y selecciona un nuevo servidor primario con el estrato más bajo.
- **Autenticación**: seleccione la casilla de verificación para habilitar la autenticación.
- **ID de clave de autenticación**: si la autenticación está activada, seleccione el valor del ID de clave. (Cree las claves de autenticación mediante la página Autenticación de SNTP).

PASO 6 Haga clic en **Aplicar**. Se añade el servidor STNP, y usted vuelve a la página principal.

Configuración del Modo de SNTP

El dispositivo puede estar en modo activo o pasivo (consulte la sección **Modos SNTP** para obtener más información).

Para habilitar la recepción de paquetes SNTP desde todos los servidores de la subred, o para habilitar la transmisión de solicitudes horarias a los servidores SNTP:

PASO 1 Haga clic en **Administración** > **Configuración de la hora** > **SNTP de multidifusión/difusión por proximidad**.

PASO 2 Seleccione alguna de las siguientes opciones:

- **Modo de cliente de multidifusión IPv4 de SNTP (recepción de difusión de cliente)**: seleccione esta opción para recibir las transmisiones de multidifusión IPv4 de la hora del sistema desde cualquier servidor SNTP de la subred.
- **Modo de cliente de multidifusión IPv6 de SNTP (recepción de difusión de cliente)**: seleccione esta opción para recibir las transmisiones de multidifusión IPv6 de la hora del sistema desde cualquier servidor SNTP de la subred.

- **Modo de cliente de cualq. tipo de difusión IPv4 SNTP (transmisión de difusión de cliente)**: seleccione esta opción para transmitir los paquetes de sincronización IPv4 SNTP que solicitan la información horaria del sistema. Los paquetes se transmiten a todos los servidores SNTP de la subred.
- **Modo de cliente de cualq. tipo de difusión IPv6 SNTP (transmisión de difusión de cliente)**: seleccione esta opción para transmitir los paquetes de sincronización IPv6 SNTP que solicitan la información horaria del sistema. Los paquetes se transmiten a todos los servidores SNTP de la subred.

PASO 3 Si el sistema se encuentra en modo de capa 3 de sistema, haga clic en **Añadir** para ingresar la interfaz para la recepción/transmisión de SNTP.

Seleccione una interfaz y las opciones de recepción/transmisión.

PASO 4 Haga clic en **Aplicar** para guardar los ajustes en el archivo de configuración en ejecución.

Definición de la autenticación de SNTP

Los clientes SNTP pueden autenticar las respuestas con HMAC-MD5. Un servidor SNTP está asociado a una clave, la cual se usa como dato de entrada junto con la respuesta para la función MD5. El resultado de MD5 también se incluye en el paquete de respuesta.

La página *Autenticación de SNTP*, permite la configuración de las claves de autenticación que se usan al establecer una comunicación con un servidor SNTP que requiere autenticación.

La clave de autenticación se crea en el servidor SNTP en un proceso aparte que depende del tipo de servidor SNTP que esté utilizando. Consulte con el administrador del servidor SNTP para obtener más información al respecto.

Flujo de trabajo

PASO 1 Active la autenticación en la página Autenticación de SNTP.

PASO 2 Cree una clave en la página Autenticación de SNTP.

PASO 3 Asocie la clave con un servidor SNTP en la página Unidifusión de SNTP.

Para habilitar la autenticación SNTP y definir las claves:

PASO 1 Haga clic en **Administración** > **Configuración de la hora** > **Autenticación de SNTP**.

PASO 2 Seleccione **Autenticación de SNTP** para posibilitar la autenticación de una sesión SNTP entre el dispositivo y un servidor SNTP.

PASO 3 Haga clic en **Aplicar** para actualizar el dispositivo.

PASO 4 Haga clic en **Añadir**.

PASO 5 Ingrese los siguientes parámetros:

- **ID de clave de autenticación**: ingrese el número que se usa para identificar esta clave de autenticación de SNTP internamente.
- **Clave de autenticación**: ingrese la clave que se usa para la autenticación (hasta ocho caracteres). El servidor SNTP debe enviar esta clave para que el dispositivo se sincronice con este.
- **Clave confiable**: seleccione esta opción para permitir que el dispositivo reciba información de sincronización solo de un servidor SNTP mediante esta clave de autenticación.

PASO 6 Haga clic en **Aplicar**. Los parámetros de autenticación de SNTP se escriben en el archivo Configuración en ejecución.

Intervalo de tiempo

Los intervalos de tiempo pueden definirse y asociarse con los siguientes tipos de comandos, de manera tal que se aplican solo durante dicho intervalo de tiempo:

- ACL
- Autenticación de puerto 802.1X
- Estado del puerto
- PoE basada en tiempo

Hay dos tipos de intervalos de tiempo:

- **Absoluto**: este tipo de intervalo de tiempo comienza en una fecha específica o de manera inmediata y finaliza en una fecha específica o se extiende de forma infinita. El intervalo se crea en las páginas Intervalo de tiempo. Se puede agregar un elemento recurrente.
- **Recurrente**: este tipo de intervalo de tiempo contiene un elemento de intervalo de tiempo que se añade a un intervalo absoluto y comienza y finaliza de manera periódica. Se define en las páginas Intervalo recurrente.

Si un intervalo de tiempo incluye intervalos absolutos y recurrentes, el proceso asociado al intervalo se activa solo si se alcanzó la hora de inicio absoluta y el intervalo de tiempo recurrente. El proceso se desactiva cuando cualquiera de los intervalos de tiempo se haya alcanzado.

El dispositivo admite un máximo de 10 intervalos de tiempo absolutos.

Todas las especificaciones de tiempo se interpretan como la hora local (la hora de ahorro de luz diurna no lo afecta). Para garantizar que las entradas del intervalo de tiempo entren en efecto en los momentos deseados, se debe configurar la hora del sistema.

La característica de intervalo de tiempo se puede usar para lo siguiente:

- Limitar el acceso de las computadoras a la red durante el horario de trabajo (por ejemplo), después del cual se bloquean los puertos de la red al igual que el acceso al resto de la red (consulte **Configuración de puertos** y **Configuración de los valores de LAG**).
- Limitar el funcionamiento de PoE a un período específico.

Intervalo de tiempo absoluto

Para definir un intervalo de tiempo absoluto:

PASO 1 Haga clic en **Administración** > **Configuración de la hora** > **Intervalo de tiempo**.

Se muestran los intervalos de tiempo existentes.

PASO 2 Para añadir un nuevo intervalo de tiempo, haga clic en **Añadir**.

PASO 3 Ingrese los siguientes campos:

- **Nombre del intervalo de tiempo**: ingrese un nuevo nombre para el intervalo de tiempo.
- **Tiempo de inicio absoluto**: para definir la hora de inicio, ingrese las siguientes opciones:
  - *Inmediato*: para que el intervalo de tiempo comience inmediatamente.
  - *Fecha, hora*: ingrese la fecha y la hora en la que comienza el intervalo de tiempo.
- **Tiempo de finalización absoluto**: para definir la hora de finalización, ingrese las siguientes opciones:
  - *Infinito*: para que el intervalo de tiempo nunca termine.
  - *Fecha, hora*: ingrese la fecha y la hora en la que finaliza el intervalo de tiempo.

PASO 4 Para añadir un nuevo intervalo de tiempo recurrente, haga clic en **Intervalo recurrente**.

Intervalo de tiempo recurrente

Se puede incorporar un elemento de tiempo recurrente a un intervalo de tiempo absoluto. Esto limita el funcionamiento a ciertos períodos de tiempo dentro del intervalo absoluto.

Para añadir un elemento de intervalo de tiempo recurrente a un intervalo de tiempo absoluto:

PASO 1 Haga clic en **Administración** > **Configuración de la hora** > **Intervalo recurrente**.

Se muestran los intervalos de tiempo recurrentes que ya existen (filtrados por cada intervalo de tiempo absoluto específico).

PASO 2 Seleccione el intervalo de tiempo absoluto al cual desea agregar un intervalo recurrente.

PASO 3 Para añadir un nuevo intervalo de tiempo recurrente, haga clic en **Añadir**.

PASO 4 Ingrese los siguientes campos:

- **Tiempo de inicio recurrente**: ingrese la fecha y la hora en la que comienza el intervalo de tiempo periódicamente.
- **Tiempo de finalización recurrente**: ingrese la fecha y la hora en la que finaliza el intervalo de tiempo periódicamente.

PASO 5 Haga clic en **Aplicar**

PASO 6 Haga clic en **Intervalo de tiempo** para acceder a Intervalo de tiempo absoluto

8

Administración: Diagnóstico

En esta sección se ofrece información para configurar la duplicación de puertos, ejecutar pruebas de cables y ver información operacional de dispositivos.

Abarca los siguientes temas:

- **Pruebas de puertos de cobre**
- **Visualización del estado del módulo óptico**
- **Configuración de duplicación de puertos y VLAN**
- **Visualización de la utilización de la CPU y tecnología de núcleo seguro**

Pruebas de puertos de cobre

En la página Prueba de cobre, se muestran los resultados de las pruebas de cable integradas realizadas en los cables de cobre con el VCT (Virtual Cable Tester, comprobador de cable virtual).

El comprobador de cable virtual realiza dos tipos de prueba:

- La tecnología de reflectometría en el dominio del tiempo (TDR) evalúa la calidad y las características de un cable de cobre conectado a un puerto. Se pueden realizar pruebas en cables de hasta 140 metros de largo. Estos resultados se muestran en el bloque Resultados de la prueba de la página Prueba de cobre.
- Las pruebas basadas en DSP se realizan en enlaces GE activos para medir la longitud del cable. Estos resultados se muestran en el bloque Información avanzada de la página Prueba de cobre.

Condiciones previas a la ejecución de la prueba de puertos de cobre

Antes de realizar la prueba, haga lo siguiente:

- (Obligatorio) Desactive el modo Alcance corto (consulte la página Administración de puertos > Green Ethernet > Propiedades).
- (Opcional) Desactive el modo EEE (consulte la página Administración de puertos > Green Ethernet > Propiedades).

Al realizar las pruebas en el cable (VCT), utilice un cable de datos CAT5.

La exactitud de los resultados de la prueba puede tener un margen de error de +/- 10 para las pruebas avanzadas y de +/- 2 para las pruebas básicas.

PRECAUCIÓN Cuando se realiza una prueba en un puerto, se le configura en el estado inactivo y se interrumpen las comunicaciones. Luego de la prueba, se vuelve a activar el puerto. No se recomienda realizar la prueba en un puerto de cobre que se esté usando para ejecutar la utilidad de configuración de switch basada en la Web, ya que se interrumpen las comunicaciones con ese dispositivo.

Para realizar una prueba en cables de cobre conectados a puertos:

PASO 1 Haga clic en **Administración** > **Diagnósticos** > **Prueba de cobre**.

PASO 2 Seleccione el puerto en el que se ejecutará la prueba.

PASO 3 Haga clic en **Prueba de cobre**.

PASO 4 Cuando aparezca el mensaje, haga clic en **Acept.** para confirmar que el enlace puede desactivarse o en **Cancelar** para cancelar la prueba.

En el bloque Resultados de la prueba se muestran los siguientes campos:

- **Última actualización**: hora de la última prueba realizada en el puerto.
- **Resultados de la prueba**: resultados de la prueba del cable. Los valores posibles son:
  - *Correcto*: el cable pasó la prueba.
  - *Sin cable*: el cable no está conectado al puerto.
  - *Cable abierto*: el cable está conectado solo en un lado.
  - *Cable corto*: ocurrió un cortocircuito en el cable.
  - *Resultado de la prueba desconocido*: ocurrió un error.
- **Distancia hasta la falla**: distancia desde el puerto hasta el lugar del cable donde se detectó la falla.
- **Estado del puerto operativo**: muestra si el puerto está activo o inactivo.

Si el puerto que se está sometiendo a prueba es un puerto Giga, el bloque **Información avanzada** contiene la siguiente información, que se actualiza cada vez que usted ingresa a la página:

- **Longitud del cable:** brindar una aproximación de la longitud.
- **Par**: par de cable en que se realiza la prueba.

- **Estado**: estado del par de cables. El color rojo indica una falla y el color verde indica un estado correcto.
- **Canal**: canal de cable que indica si los cables son directos o están cruzados.
- **Polaridad**: indica si se activó la detección y corrección automática de polaridad para el par de cables.
- **Desviación de pares**: diferencia en demora entre pares de cables.

NOTA No se pueden llevar a cabo pruebas TDR si la velocidad del puerto es 10 Mbit/s.

Visualización del estado del módulo óptico

En la página Estado del módulo óptico, se muestran las condiciones operativas que informa el transceptor SFP (Small Form-factor Pluggable, enchufable pequeño). Es posible que parte de la información no esté disponible para los SFP que no sean compatibles con la norma de monitoreo diagnóstico digital SFF-8472.

SFP compatibles con MSA

Se admiten los siguientes transceptores SFP FE (100 Mbps):

- MFEBX1: transceptor SFP 100BASE-BX-20U para fibra de modo simple, longitud de onda de 1310 nm, compatible con hasta 20 km.
- MFEFX1: transceptor SFP 100BASE-FX para fibra de modo múltiple, longitud de onda de 1310 nm, compatible con hasta 2 km.
- MFELX1: transceptor SFP 100BASE-LX para fibra de modo simple, longitud de onda de 1310 nm, compatible con hasta 10 km.

Se admiten los siguientes transceptores SFP GE (1000 Mbps):

- MGBBX1: transceptor SFP 1000BASE-BX-20U para fibra de modo simple, longitud de onda de 1310 nm, compatible con hasta 40 km.
- MGBLH1: transceptor SFP 1000BASE-LH para fibra de modo simple, longitud de onda de 1310 nm, compatible con hasta 40 km.
- MGBLX1: transceptor SFP 1000BASE-LX para fibra de modo simple, longitud de onda de 1310 nm, compatible con hasta 10 km.
- MGBSX1: transceptor SFP 1000BASE-SX para fibra de modo múltiple, longitud de onda de 850 nm, compatible con hasta 550 m.
- MGBT1: transceptor SFP 1000BASE-T para cable de cobre categoría 5, compatible con hasta 100 m.

Para ver los resultados de las pruebas ópticas, haga clic en **Administración** > **Diagnósticos** > **Estado del módulo óptico**.

Esta página muestra los siguientes campos:

- **Puerto**: número de puerto en el que está conectado el SFP.
- **Descripción**: descripción del transceptor óptico.
- **Número de serie**: el número de serie del transceptor óptico.
- **PID**: ID de VLAN.
- **VID**: ID del transceptor óptico.
- **Temperatura**: temperatura (Celsius) a la que funciona el SFP.
- **Voltaje**: el voltaje operativo del SFP.
- **Corriente**: el consumo de corriente del SFP.
- **Potencia de salida**: la potencia óptica transmitida.
- **Potencia de entrada**: la potencia óptica recibida.
- **Fallo en el transmisor**: el SFP remoto informa de una pérdida de señal. Los valores son verdadero, falso y sin señal (N/S, No signal).
- **Pérdida de señal**: el SFP local informa de una pérdida de señal. Los valores son verdadero y falso.
- **Datos listos**: el SFP está en modo operativo. Los valores son verdadero y falso.

Configuración de duplicación de puertos y VLAN

La duplicación de puertos se utiliza en el dispositivo de red para enviar una copia de los paquetes de red detectados en un puerto de dispositivo, varios puertos de dispositivo o una VLAN completa a una conexión de monitoreo de red en otro puerto de dispositivo. Esta función suele utilizarse para dispositivos de red que requieren el monitoreo del tráfico de red, como un sistema de detección de intrusos. Un analizador de red conectado al puerto de monitoreo procesa los paquetes de datos para realizar diagnóstico, depuración y monitoreo del rendimiento.

Se pueden duplicar hasta ocho orígenes, que puede ser cualquier combinación de ocho puertos o VLAN individuales.

Un paquete que se recibe en un puerto de red asignado a una VLAN que está sujeta a la duplicación, se duplica en el puerto del analizador, incluso si finalmente el paquete se capturó o descartó. Los paquetes que envía el dispositivo se duplican cuando la duplicación de transmisión (Tx) está activada.

La duplicación no garantiza que se reciba todo el tráfico de los puertos de origen en el puerto del analizador (destino). Si se envían más datos al puerto del analizador que los que admite, es posible que se pierdan algunos datos.

La duplicación de VLAN no está activa en una VLAN que no se creó manualmente. Por ejemplo, si la VLAN 23 se creó a través del GVRP (Generic VLAN Registration Protocol, Protocolo genérico de registro de VLAN), y usted creó manualmente VLAN 34 y se creó una duplicación de puerto que incluye VLAN 23, VLAN 34, o ambas y luego elimina VLAN 34, el estado de la duplicación de puertos se establece en **No está listo**, ya que la VLAN34 no está más en la base de datos y VLAN23 no se creó manualmente.

Solo se admite una instancia de duplicación en todo el sistema. El puerto del analizador (o puerto de destino para la duplicación de VLAN o de puertos) es el mismo para todas las VLAN duplicadas o los puertos.

Para habilitar la duplicación:

PASO 1 Haga clic en **Administración** > **Diagnósticos** > **Duplicación de puerto y VLAN**.

Se muestran los siguientes campos:

- **Puerto de destino**: puerto en el que se copiará el tráfico; el puerto del analizador.
- **Interfaz de origen**: interfaz, puerto o VLAN, desde la que se envía el tráfico al puerto del analizador.
- **Tipo**: tipo de monitoreo: entrante al puerto (Rx), saliente desde el puerto (Tx), o ambos.
- **Estado**: muestra uno de los siguientes valores:
  - *Activo*: las interfaces de origen y destino están activas y reenvían tráfico.
  - *No está listo*: el origen o el destino (o ambos) no están activos o no reenvían tráfico por algún motivo.

PASO 2 Haga clic en **Añadir** para añadir un puerto o una VLAN que desee duplicar.

PASO 3 Ingrese los parámetros:

- **Puerto de destino**: seleccione el puerto del analizador en el que se copian los paquetes. Un analizador de red, como una PC con Wireshark en ejecución, está conectado a este puerto. Si se identifica un puerto como puerto del analizador de destino, permanece con esta función hasta que se eliminan todas las entradas.
- **Interfaz de origen**: seleccione el puerto o VLAN de origen de donde debe duplicarse el tráfico.
- **Tipo**: seleccione si se duplica el tráfico entrante, saliente o de ambos tipos en el puerto del analizador. Si se selecciona **Puerto**, las opciones son:
  - *Solo Rx*: duplicación de puerto en paquetes entrantes.
  - *Solo Tx*: duplicación de puerto en paquetes salientes.
  - *Tx y Rx*: duplicación de puerto en paquetes entrantes y salientes.

PASO 4 Haga clic en **Aplicar**. La duplicación del puerto se añade a la configuración en ejecución.

Visualización de la utilización de la CPU y tecnología de núcleo seguro

El dispositivo maneja los siguientes tipos de tráfico, además de tráfico de usuario final:

- Tráfico de administración
- Tráfico de protocolo
- Tráfico de indagación

El tráfico excesivo carga la CPU y podría impedir el correcto funcionamiento del dispositivo. El dispositivo utiliza la función de SCT (Secure Core Technology, tecnología de núcleo seguro) para garantizar que el dispositivo reciba y procese el tráfico de protocolo y administración, independientemente de cuánto tráfico total se reciba. SCT está habilitado de forma predeterminado en el dispositivo y no se puede desactivar.

No hay interacciones con otras funciones.

Para ver la utilización de la CPU:

PASO 1 Haga clic en **Administración > Diagnósticos > Utilización de CPU**.

Aparece la página Utilización de CPU.

En el campo Velocidad entrada de la CPU, se muestra la velocidad de las tramas de entrada a la CPU por segundo.

La ventana contiene un gráfico de la utilización de la CPU. El eje Y representa el porcentaje de uso y el eje X es el número de muestra.

PASO 2 Asegúrese de marcar la casilla de verificación Utilización de CPU.

PASO 3 Seleccione la velocidad de actualización en **Velocidad de actualización** (tiempo en segundos) que pasa antes de que se actualicen las estadísticas. Se crea una nueva muestra para cada período.

PASO 4 Haga clic en **Aplicar**.

9

Administración: Detección

Esta sección contiene información para configurar Discovery.

Abarca los siguientes temas:

- **Bonjour**
- **LLDP y CDP**
- **Configuración de LLDP**
- **Configuración de CDP**

Bonjour

Como cliente de Bonjour, el dispositivo transmite periódicamente paquetes de protocolo Bonjour Discovery a las subredes IP conectadas directamente y anuncia su existencia y los servicios que ofrece, como por ejemplo, HTTP, HTTP y Telnet. (Use la página Seguridad > Servicios TCP/UDP para activar o desactivar los servicios del dispositivo). El dispositivo puede ser detectado por un sistema de administración de red u otras aplicaciones de terceros. Bonjour está habilitado de manera predeterminada en la VLAN de administración. La consola de Bonjour detecta automáticamente el dispositivo y lo muestra.

Bonjour en el modo del sistema de capa 2

Cuando el dispositivo está en el modo del sistema de capa 2, Bonjour Discovery está habilitado globalmente; no se puede habilitar por puerto o por VLAN. El dispositivo anuncia todos los servicios que activó el administrador según la configuración de la página Servicios.

Cuando la Detección de Bonjour e IGMP están activados, la dirección IP de multidifusión de Bonjour se muestra en la página Añadidura de direcciones IP de grupo de multidifusión.

Cuando la Detección de Bonjour está desactivada, el dispositivo detiene cualquier anuncio de tipo de servicio y no responde a las solicitudes de servicio de las aplicaciones de administración de red.

Para habilitar globalmente Bonjour cuando el sistema está en el modo del sistema de capa 2:

PASO 1 Haga clic en **Administración** > **Discovery - Bonjour**.

PASO 2 Seleccione **Habilitar** para activar la **Detección** de Bonjour globalmente en el dispositivo.

PASO 3 Haga clic en **Aplicar**. Bonjour se activa o desactiva en el dispositivo según la selección.

Bonjour en el modo del sistema de capa 3

En el modo del sistema de capa 3, se puede asignar una dirección IP a cada interfaz (VLAN, puerto o LAG). Cuando Bonjour está activado, el dispositivo puede enviar paquetes de Detección de Bonjour en todas las interfaces que tienen direcciones IP. Bonjour puede asignarse de forma individual por puerto o por VLAN. Cuando Bonjour está activado, el dispositivo puede enviar paquetes de Detección de Bonjour a las interfaces que tienen direcciones IP que se han asociado con Bonjour en la Tabla de control de interfaz de Detección de Bonjour. Cuando el dispositivo funciona en el modo del sistema Capa 3, vaya a **Configuración de IP** > **Administración e interfaces IP** > **Interfaz IPv4** para configurar una dirección IP para una interfaz.

Si una interfaz, como VLAN, se elimina, se envían paquetes de saludo final para anular el registro de los servicios que el dispositivo está anunciando desde la tabla de caché vecina dentro de la red local. La tabla de control de interfaz de Bonjour Discovery muestra las interfaces que tienen direcciones IP que están asociadas con la función Bonjour. Los anuncios de Bonjour solo se pueden transmitir a las interfaces que aparecen en esta tabla. Consulte la Tabla de control de interfaz de Detección de Bonjour en la página Administración > Detección de Bonjour. Si se cambian los servicios disponibles, esos cambios se anuncian, y se anula el registro de los servicios que están desactivados y se registran los servicios que están activados. Si se cambia una dirección IP, se anuncia ese cambio.

Si se desactiva Bonjour, el dispositivo no envía ningún anuncio de Detección de Bonjour, y no escucha los anuncios de Detección de Bonjour que envían otros dispositivos.

Para configurar Bonjour cuando el dispositivo está en el modo del sistema Capa 3:

PASO 1 Haga clic en **Administración** > **Discovery - Bonjour**.

PASO 2 Seleccione **Habilitar** para habilitar Bonjour **Discovery** globalmente.

PASO 3 Haga clic en **Aplicar** para actualizar el archivo Configuración en ejecución.

PASO 4 Para habilitar Bonjour en una interfaz, haga clic en **Añadir**.

PASO 5 Seleccione una interfaz y haga clic en **Aplicar**.

NOTA Haga clic en **Eliminar** para deshabilitar Bonjour en una interfaz (de esta manera, se realiza la operación eliminación sin operaciones adicionales, como Aplicar).

LLDP y CDP

El protocolo de detección de capa de enlace (LLDP, Link Layer Discovery Protocol) y el protocolo de detección de Cisco (CDP, Cisco Discovery Protocol) son protocolos de la capa de enlace para que los vecinos con LLDP y CDP directamente conectados se anuncien y anuncien sus capacidades. El dispositivo envía de forma predeterminada un anuncio de LLDP/CDP periódicamente a todas sus interfaces, y procesa los paquetes LLDP y CDP entrantes, según lo requieran los protocolos. En LLDP y CDP, los anuncios están cifrados como TLV (tipo, longitud, valor) en el paquete.

Se aplican las siguientes notas de configuración de CDP/LLDP:

- CDP/LLDP pueden estar habilitados o deshabilitados globalmente y por puerto. La capacidad de CDP/LLDP de un puerto es relevante solo si CDP/LLDP está habilitado globalmente.
- Si se activa CDP/LLDP globalmente, el dispositivo filtra los paquetes CDP/LLDP entrantes de los puertos que están deshabilitados por CDP/LLDP.
- Si se desactiva CDP/LLDP globalmente, el dispositivo puede configurarse para que descarte o realice un desborde que detecte la VLAN o uno que no detecte la VLAN de todos los paquetes CDP/LLDP entrantes. La inundación que detecta la VLAN envía de forma masiva un paquete CDP/LLDP entrante a la VLAN en la que se recibe el paquete, salvo al puerto de ingreso. La inundación que no detecta la VLAN emite en forma masiva un paquete CDP/LLDP entrante a todos los puertos, salvo al puerto de ingreso. El valor predeterminado es descartar los paquetes CDP/LLDP cuando el CDP/LLDP está deshabilitado globalmente. El descarte y la inundación de los paquetes CDP y LLDP entrantes se pueden configurar en la página Propiedades de CDP y en la página Propiedades de LLDP, respectivamente.
- Auto Smartport requiere que CDP o LLDP esté habilitada. Auto Smartport configura automáticamente una interfaz según el anuncio de CDP/LLDP que se recibe de la interfaz.
- Los dispositivos finales de CDP y LLDP, como por ejemplo, teléfonos IP, aprenden la configuración de VLAN por voz de los anuncios de CDP y LLDP. El dispositivo está activado de forma predeterminada para enviar el anuncio de CDP y LLDP según la VLAN por voz configurada en el dispositivo. Para obtener detalles, consulte **VLAN de voz**.

  NOTA CDP/LLDP no distingue si un puerto está en un LAG. Si hay varios puertos en un LAG, CDP/LLDP transmiten paquetes a cada puerto sin tener en cuenta el hecho de que los puertos están en un LAG.

El funcionamiento de CDP/LLDP es independiente del estado de STP de una interfaz.

Si el control de acceso de puerto 802.1x está activado en una interfaz, el dispositivo transmite paquetes CDP/LLDP a la interfaz y los recibe de ella, solo si la interfaz está autenticada y autorizada.

Si un puerto es el objetivo de la duplicación, entonces para CDP/LLDP se considera inactivo.

NOTA CDP y LLDP son protocolos de la capa de enlace para que los dispositivos con CDP LLDP directamente conectados se anuncien y anuncien sus capacidades. En las implementaciones en que los dispositivos con CDP/LLDP no están directamente conectados y están separados con dispositivos sin CDP/LLDP, los dispositivos con CDP/LLDP podrán recibir el anuncio de otros dispositivos, solo si en los dispositivos con CDP/LLDP se produce un desborde de los paquetes de CDP/LLDP que reciben. Si los dispositivos sin CDP/LLDP producen una inundación que detecta la VLAN, entonces los dispositivos con CDP/LLDP pueden escucharse entre sí, solo si están en la misma VLAN. Un dispositivo con CDP/LLDP podrá recibir un anuncio de más de un dispositivo si los dispositivos sin CDP/LLDP envían los paquetes CDP/LLDP en forma masiva.

Configuración de LLDP

En esta sección se describe cómo configurar el protocolo LLDP. Abarca los siguientes temas:

- **Información general sobre LLDP**
- **Propiedades LLDP**
- **Configuración de puerto LLDP**
- **Política de red LLDP MED**
- **Configuración de puertos MED LLDP**
- **Estado de puertos LLDP**
- **Información local de LLDP**
- **Información de vecinos LLDP**
- **Estadísticas LLDP**
- **Sobrecarga LLDP**

Información general sobre LLDP

LLDP es un protocolo que permite a los administradores de red resolver problemas y mejorar la administración de la red en entornos de varios proveedores. LLDP estandariza los métodos para que los dispositivos de red se anuncien en otros sistemas y almacenen la información detectada.

LLDP permite a un dispositivo anunciar su identificación, configuración y capacidades a dispositivos vecinos que luego almacenan los datos en una MIB (Management Information Base, base de información de administración). El sistema de administración de red imita la topología de la red consultando estas bases de datos de MIB.

LLDP es un protocolo de la capa de enlace. De forma predeterminada, el dispositivo termina y procesa todos los paquetes LLDP entrantes, según lo requiera el protocolo.

El protocolo LLDP posee una extensión denominada LLDP Media Endpoint Discovery (LLDP-MED), que suministra y acepta información de dispositivos de punto final de medios, como por ejemplo, teléfonos CoIP y teléfonos de video. Para obtener más información sobre LLDP-MED, consulte **Política de red LLDP MED**.

Flujo de trabajo de la configuración de LLDP

A continuación se muestran ejemplos de acciones que se pueden realizar con la función LLDP en un orden sugerido. Para obtener pautas adicionales sobre la configuración de LLDP, puede consultar la sección LLDP/CDP. El acceso a las páginas de configuración de LLDP es mediante el menú **Administración > Discovery - LLDP**.

1. Ingrese los parámetros globales de LLDP, como el intervalo de tiempo para enviar actualizaciones de LLDP, a través de la página Propiedades LLDP.
2. Configure LLDP por puerto mediante la página Configuración de puertos. En esta página, las interfaces pueden configurarse para que reciban y transmitan PDU de LLDP, envíen notificaciones SNMP, especifiquen qué TLV se anunciarán y anuncien la dirección de administración del dispositivo.
3. Cree las políticas de red LLDP MED mediante la página Política de red LLDP MED.
4. Asocie las políticas de red LLDP MED y los TLV de LLDP-MED opcionales con las interfaces deseadas mediante la página Configuración de puertos LLDP MED.
5. Si Smartport automático debe detectar las capacidades de los dispositivos LLDP, habilite LLDP en la página Propiedades de Smartport.
6. Muestre la información de sobrecarga mediante la página Sobrecarga LLDP.

Propiedades LLDP

La página Propiedades permite ingresar parámetros LLDP generales, que incluyen la activación/desactivación de la función a nivel global y la configuración de temporizadores.

Para ingresar propiedades LLDP:

PASO 1 Haga clic en **Administración** > **Discovery - LLDP** > **Propiedades**.

PASO 2 Ingrese los parámetros.

- **Estado LLDP**: seleccione esta opción para activar LLDP en el dispositivo (seleccionada de forma predeterminada).
- **Manejo de tramas de LLDP**: si LLDP no está habilitado, seleccione la acción que se realizará si se recibe un paquete que coincide con los criterios seleccionados.
  - *Filtrado*: elimine el paquete.
  - *Inundación*: reenvíe el paquete a todos los miembros de la VLAN.
- **Intervalo para anuncio TLV**: ingrese la velocidad en segundos a la que se envían las actualizaciones de anuncios de LLDP o utilice el valor predeterminado.
- **Intervalo para notificación SNMP de cambios en la topología**: ingrese el intervalo de tiempo mínimo entre las notificaciones SNMP.
- **Retener multiplicador**: ingrese la cantidad de tiempo que se retienen los paquetes LLDP antes de que se descarten, medida en múltiplos del Intervalo para anuncio TLV. Por ejemplo, si el Intervalo para anuncio TLV es 30 segundos, y el valor de Retener multiplicador es 4, los paquetes LLDP se descartan después de 120 segundos.
- **Retraso en el reinicio**: ingrese el intervalo de tiempo en segundos que transcurre entre que se deshabilita y se reinicia LLDP, después de un ciclo de habilitación/deshabilitación de LLDP.
- **Retraso de transmisión**: ingrese la cantidad de tiempo en segundos que transcurre entre las sucesivas transmisiones de trama LLDP por cambios en la MIB de los sistemas LLDP locales.
- **Aviso de ID de chasis**: seleccione una de las siguientes opciones para anunciar en los mensajes LLDP:
  - *Dirección MAC:* anunciar la dirección MAC del dispositivo.
  - *Nombre de host:* anunciar el nombre de host del dispositivo.

PASO 3 En el campo **Conteo repetido de inicio rápido**, ingrese la cantidad de veces que se envían paquetes LLDP cuando se inicializa el mecanismo "Fast Start" (Inicio rápido) de LLDP-MED. Esto se produce cuando un nuevo dispositivo del punto final se conecta al dispositivo. Para obtener una descripción de LLDP MED, consulte la sección Política de red LLDP MED.

PASO 4 Haga clic en **Aplicar**. Las propiedades de LLDP se añaden al archivo Configuración en ejecución.

Configuración de puerto LLDP

La página Configuración de puertos permite la activación de la notificación SNMP y LLDP por puerto y el ingreso de los TLV que se envían en la PDU de LLDP.

Los TLV de LLDP-MED que deben anunciarse pueden seleccionarse en la página Configuración de puertos LLDP MED, y podrá configurarse el TLV de la dirección de administración del dispositivo.

Para definir la configuración de puertos LLDP:

PASO 1 Haga clic en **Administración** > **Discovery - LLDP** > **Configuración de puertos**.

Esta página contiene la información de puertos LLDP.

PASO 2 Seleccione un puerto y haga clic en **Editar**.

En esta página se muestran los siguientes campos:

- **Interfaz**: seleccione un puerto para editar.
- **Estado administrativo**: seleccione la opción de publicación LLDP para el puerto. Los valores son:
  - *Solo Tx*: publica, pero no detecta.
  - *Solo Rx*: detecta, pero no publica.
  - *Tx y Rx*: publica y detecta.
  - *Deshabilitar*: indica que LLDP está deshabilitado en el puerto.
- **Notificación SNMP**: seleccione **Habilitar** para enviar notificaciones a los receptores de notificaciones SNMP, por ejemplo, un sistema de administración de SNMP, cuando se produce un cambio de topología.

  El intervalo de tiempo entre notificaciones se ingresa en el campo Intervalo para notificación SNMP de cambios en la topología de la página Propiedades LLDP. Defina los receptores de notificaciones SNMP mediante la página SNMP >Receptores de notificaciones v1,2 y SNMP > Receptores de notificación v3.
- **TLV opcionales seleccionados**: seleccione la información que el dispositivo publicará; para ello, mueva los TLV de la lista **TLV opcionales disponibles**. Los TLV disponibles contienen la siguiente información:
  - *Descripción del puerto*: información acerca del puerto, incluido el fabricante, el nombre del producto y la versión de hardware/software.

- *Nombre del sistema*: nombre asignado al sistema (en formato alfanumérico). El valor es igual al objeto sysName.
- *Descripción del sistema*: descripción de la entidad de red (en formato alfanumérico). Esto incluye el nombre del sistema y las versiones de hardware, sistema operativo y software de red que admite el dispositivo. El valor es igual al objeto sysDescr.
- *Capacidades del sistema*: funciones principales del dispositivo, y si estas funciones están activadas en el dispositivo. Dos octetos indican las capacidades. Los bits del 0 al 7 indican otro, repetidor, puente, WLAN AP, router, teléfono, dispositivo de cableado DOCSIS y estación, respectivamente. Los bits del 8 al 15 están reservados.
- *802.3 MAC-PHY*: capacidad de velocidad de bits y dúplex y la configuración actual de velocidad de bits y dúplex del dispositivo remitente. También indica si la configuración actual es por negociación automática o configuración manual.
- *802.3 Añadidura de enlaces*: indica si se puede añadir el enlace (asociado con el puerto en el que se transmite la PDU de LLDP). También indica si el enlace está actualmente añadido, y si lo está, proporciona el identificador del puerto añadido.
- *802.3 Tamaño máximo de trama*: capacidad de tamaño máximo de la trama de la implementación de MAC/PHY.

TLV opcional de la dirección de administración:

- **Modo de anuncio**: seleccione una de las siguientes formas de anunciar la dirección IP de administración del dispositivo:
  - *Anuncio automático*: especifica que el software elige automáticamente una dirección de administración para realizar el anuncio, entre todas las direcciones IP del dispositivo. En caso de varias direcciones IP, el software elige la dirección IP más baja entre las direcciones IP dinámicas. Si no hay direcciones dinámicas, el software elige la dirección IP más baja entre las direcciones IP estáticas.
  - *Ninguno*: no anunciar la dirección IP de administración.
  - *Anuncio manual*: seleccione esta opción y la dirección IP de administración para anunciar. Le recomendamos que seleccione esta opción cuando el dispositivo está en modo del sistema de capa 3 y configurado con varias direcciones IP (esto es siempre real en los dispositivos SG500X/ESW2-550X).
- **Dirección IP**: si se ha seleccionado el anuncio manual, seleccione la Dirección IP de administración entre las direcciones proporcionadas.

Los siguientes campos están relacionados con **802.1 VLAN y protocolo**:

- **PVID**: seleccione para anunciar el PVID en el TLV.
- **Puerto e ID de VLAN de protocolo**: seleccione para anunciar el puerto y el ID de VLAN del protocolo.

- **ID de VLAN**: seleccione las VLAN que se anunciarán.
- **ID de protocolo**: seleccione los protocolos que se anunciarán.
- ID de protocolo seleccionado: muestra los protocolos seleccionados.

PASO 3 Ingrese la información relevante y haga clic en **Aplicar**. La configuración del puerto se escribe en el archivo Configuración en ejecución.

Política de red LLDP MED

LLDP Media Endpoint Discovery (LLDP-MED) es una extensión de LLDP que proporciona las siguientes capacidades adicionales para admitir dispositivos de punto final de medios:

- Permite el anuncio y la detección de políticas de red para aplicaciones en tiempo real, como por ejemplo, voz y video.
- Detección de ubicación de dispositivos para permitir la creación de bases de datos de ubicación y, en el caso del VoIP (Voice over Internet Protocol, protocolo de voz a través de Internet), servicio de llamadas de emergencia (E-911) mediante el uso de la información de ubicación de teléfonos IP.
- Información sobre la resolución de problemas. LLDP MED envía alertas a los administradores de red sobre:
  - Conflictos en el modo dúplex y en la velocidad de los puertos
  - Errores de configuración de la política de QoS

Configuración de la política de red LLDP MED

Una política de red LLDP-MED es un conjunto de parámetros de configuración relacionados para una aplicación en tiempo real específica, como por ejemplo, voz o video. Una política de red, si se configura, se puede incluir en los paquetes LLDP salientes para el dispositivo de punto final de medios LLDP conectado. El dispositivo de punto final de medios debe enviar el tráfico según se especifica en la política de red que recibe. Por ejemplo, se puede crear una política para tráfico VoIP que le indique al teléfono VoIP:

- Enviar el tráfico de voz a través de la VLAN 10 como paquete etiquetado y con prioridad 5 de 802.1p.
- Enviar tráfico de voz con DSCP 46.

Las políticas de red se asocian con los puertos mediante la página Configuración de puertos LLDP MED. Un administrador puede configurar manualmente una o más políticas de red y las interfaces donde se enviarán las políticas. Es responsabilidad del administrador crear manualmente las VLAN y los miembros de sus puertos de acuerdo con las políticas de red y las interfaces asociadas.

Además, un administrador puede instruir al dispositivo para que genere automáticamente y anuncie una política de red para la aplicación de voz, según la VLAN de voz que mantiene el dispositivo. Para obtener detalles sobre cómo el dispositivo mantiene su VLAN de voz, consulte la sección VLAN de voz automática.

Para definir una política de red LLDP MED:

PASO 1 Haga clic en **Administración** > **Discovery - LLDP** > **Política de red LLDP MED**.

Esta página contiene políticas de red creadas previamente.

PASO 2 Seleccione **Automático** para Política de red LLDP-MED para aplicación de voz si el dispositivo debe generar automáticamente y anunciar una política de red para la aplicación de voz, según la VLAN de voz que mantiene el dispositivo.

NOTA Cuando esta casilla está marcada, usted no puede configurar manualmente una política de red de voz.

PASO 3 Haga clic en **Aplicar** para añadir esto al archivo Configuración en ejecución.

PASO 4 Para definir una política nueva, haga clic en **Añadir**.

PASO 5 Ingrese los valores:

- **Número de política de red**: seleccione el número de la política que desea crear.
- **Aplicación**: seleccione el tipo de aplicación (tipo de tráfico) para el que se está definiendo la política de red.
- **ID de VLAN**: ingrese el ID de VLAN al que se debe enviar el tráfico.
- **Tipo de VLAN**: seleccione si el tráfico debe estar etiquetado o sin etiquetas.
- **Prioridad del usuario**: seleccione la prioridad de tráfico aplicada al tráfico que se define en esta política de red. Este es el valor de CoS.
- **Valor DSCP**: seleccione el valor DSCP para asociar con los datos de las aplicaciones que envían los vecinos. Esto les informa cómo deben marcar el tráfico de aplicaciones que envían al dispositivo.

PASO 6 Haga clic en **Aplicar**. Se define la política de red.

NOTA Debe configurar las interfaces manualmente para incluir las políticas de red definidas manualmente para los paquetes LLDP salientes mediante la página Configuración de puertos LLDP MED.

Configuración de puertos MED LLDP

La página Configuración de puertos LLDP MED permite seleccionar los TLV de LLDP-MED y las políticas de red que se deben incluir en el anuncio LLDP saliente para las interfaces deseadas. Las políticas de red se configuran mediante la página Política red LLDP MED.

NOTA Si el valor de Política de red LLDP-MED para aplicación de voz (página Política de red LLDP-MED) es Automático y la VLAN de voz automática está en funcionamiento, el dispositivo generará automáticamente una política de red LLDP-MED para la aplicación de voz para todos los puertos que estén habilitados por LLDP-MED y son miembros de la VLAN de voz.

Para configurar LLDP MED en cada puerto:

PASO 1 Haga clic en **Administración** > **Discovery - LLDP** > **Configuración de puertos LLDP MED**.

Esta página muestra la siguiente configuración de LLDP MED para todos los puertos (solo se enumeran los campos no descritos en la página **Editar**):

- **Ubicación**: si se transmiten los TLV de la ubicación.
- **PoE**: si se transmiten los TLV de POE-PSE.
- **Inventario**: si se transmiten los TLV del inventario.

PASO 2 El mensaje de la parte superior de la página indica si la generación de la política de red LLDP MED para la aplicación de voz es automática o no (consulte **Información general de LLDP**). Haga clic en el vínculo para cambiar el modo.

PASO 3 Para asociar más TLV de LLDP MED y una o más políticas de red LLDP MED definidas por el usuario a un puerto, selecciónelo y haga clic en **Editar**.

PASO 4 Ingrese los parámetros:

- **Interfaz**: seleccione la interfaz que se debe configurar.
- **Estado LLDP MED**: habilitar/deshabilitar LLDP MED en este puerto.
- **Notificación SNMP**: seleccione si se envían notificaciones SNMP por puerto cuando se detecta una estación terminal que admite MED, por ejemplo, un sistema de administración de SNMP, cuando hay un cambio de topología.
- **TLV opcionales seleccionados**: seleccione los TLV que el dispositivo puede publicar; para ello, muévalos de la lista **TLV opcionales disponibles** a la lista TLV opcionales seleccionados.

- **Políticas de red disponibles**: seleccione las políticas de LLDP MED que LLDP publicará; para ello, muévalas de la lista **Políticas de red disponibles** a la lista Políticas de red seleccionadas. Estas políticas se crearon en la página Política de red LLDP MED. Para incluir una o más políticas de red definidas por el usuario en el anuncio, también debe seleccionar **Política de red** de los **TLV opcionales disponibles**.

  NOTA En los siguientes campos se deben ingresar caracteres hexadecimales en el formato de datos exacto que se define en la norma LLDP-MED (ANSI-TIA-1057_final_for_publication.pdf).

  - **Coordinación de ubicaciones**: ingrese la ubicación de coordinación que LLDP debe publicar.
  - **Dirección cívica de la ubicación**: ingrese la dirección cívica que LLDP debe publicar.
  - **Ubicación ELIN ECS**: ingrese la ubicación ELIN del Servicio de llamadas de emergencia (ECS) que LLDP debe publicar.

PASO 5 Haga clic en **Aplicar**. La configuración del puerto LLDP MED se escribe en el archivo Configuración en ejecución.

Estado de puertos LLDP

La página Tabla de estado de puertos LLDP contiene la información global de LLDP para cada puerto.

PASO 1 Para ver el estado LLDP de los puertos, haga clic en **Administración** > **Discovery - LLDP** > **Estado de puertos LLDP**.

PASO 2 Haga clic en **Detalles de información local de LLDP** para ver los detalles de LLDP y de los TLV de LLDP-MED enviados al vecino.

PASO 3 Haga clic en **Detalles de información de vecino de LLDP** para ver los detalles de LLDP y de los TLV de LLDP-MED recibidos del vecino.

Información global del estado de puertos LLDP

- **Subtipo de ID de chasis**: tipo de ID de chasis (por ejemplo, dirección MAC).
- **ID de chasis**: identificador de chasis. Cuando el subtipo de ID de chasis es una dirección MAC, se muestra la dirección MAC del dispositivo.
- **Nombre del sistema**: nombre del dispositivo.
- **Descripción del sistema**: descripción del dispositivo (en formato alfanumérico).
- **Capacidades del sistema admitidas**: funciones principales del dispositivo, como Puente, WLAN AP o Router.
- **Capacidades del sistema habilitadas**: funciones principales habilitadas del dispositivo.
- **Subtipo de ID de puerto**: tipo de identificador de puerto que se muestra.

Tabla de estado de puertos LLDP

- **Interfaz**: identificador de puerto.
- **Estado LLDP**: opción de publicación LLDP.
- **Estado LLDP MED**: habilitado o deshabilitado.
- **PoE local**: información de la PoE local anunciada.
- **PoE remota**: información de la PoE anunciada por el vecino.
- **N.° de vecinos**: cantidad de vecinos detectados.
- **Capacidad de vecino del 1.er dispositivo**: muestra las funciones principales del vecino; por ejemplo: Puente o Router.

Información local de LLDP

Para ver el estado de puertos locales LLDP anunciado en un puerto:

PASO 1 Haga clic en **Administración** > **Discovery - LLDP** > **Información local de LLDP**.

PASO 2 Seleccione la interfaz para la que debe mostrarse la información local LLDP.

En esta página se muestran los siguientes campos para la interfaz seleccionada:

Global

- **Subtipo de ID de chasis**: tipo de ID de chasis (por ejemplo, la dirección MAC).
- **ID de chasis**: identificador de chasis. Cuando el subtipo de ID de chasis es una dirección MAC, se muestra la dirección MAC del dispositivo.
- **Nombre del sistema**: nombre del dispositivo.
- **Descripción del sistema**: descripción del dispositivo (en formato alfanumérico).
- **Capacidades del sistema admitidas**: funciones principales del dispositivo, como Puente, WLAN AP o Router.
- **Capacidades del sistema habilitadas**: funciones principales habilitadas del dispositivo.
- **Subtipo de ID de puerto**: tipo de identificador de puerto que se muestra.
- **ID de puerto**: identificador de puerto.
- **Descripción del puerto**: información acerca del puerto, incluido el fabricante, el nombre del producto y la versión de hardware/software.

Dirección de administración

Muestra la tabla de direcciones de agente local LLDP. Otros administradores remotos pueden usar esta dirección para obtener información relacionada con el dispositivo local. La dirección consta de los siguientes elementos:

- **Subtipo de dirección**: tipo de dirección IP de administración que se incluye en el campo Dirección de administración, por ejemplo, IPv4.
- **Dirección**: dirección devuelta más apropiada para uso administrativo; por lo general, una dirección de capa 3.
- **Subtipo de interfaz**: método de numeración utilizado para definir el número de interfaz.
- **Número de interfaz**: interfaz específica asociada con esta dirección de administración.

Detalles de MAC/PHY

- **Negociación automática admitida**: estado de autonegociación de velocidad de puerto admitido.
- **Negociación automática habilitada**: estado de autonegociación de velocidad de puerto activo.
- **Capacidades anunciadas de negociación automática**: capacidades de autonegociación de velocidad de puerto, por ejemplo, modo semidúplex 1000BASE-T, modo dúplex completo 100BASE-TX.
- **Tipo de MAU operativa**: tipo de MAU (Medium Attachment Unit, unidad de conexión al medio). La MAU desempeña funciones de capa física, incluida la conversión de datos digitales de la detección de colisión de interfaces Ethernet y la inyección de bits en la red; por ejemplo, modo dúplex completo 100BASE-TX.

802.3 Detalles

- **802.3 Tamaño máximo de trama**: tamaño máximo de la trama IEEE 802.3 admitido.

802.3 Añadidura de enlaces

- **Capacidad de agrupación**: indica si la interfaz se puede añadir
- **Estado de agrupación**: indica si la interfaz está añadida
- **ID de puerto de agrupación**: ID de interfaz añadida anunciada.

802.3 Ethernet para uso eficiente de energía (EEE) (si el dispositivo es compatible con EEE)

- **Tx local**: indica el tiempo (en microsegundos) que el socio de enlace transmisor espera antes de comenzar a transmitir los datos dejando el modo de reposo de baja potencia (LPI, Low Power).
- **Rx local**: indica el tiempo (en microsegundos) que el socio de enlace receptor solicita que el socio de enlace transmisor espere antes de transmitir los datos después del modo de reposo de baja potencia (LPI, Low Power Idle).

- **Eco de Tx remoto**: indica la reflexión del socio de enlace local del valor Tx del socio de enlace remoto.
- **Eco de Rx remoto**: indica la reflexión del socio de enlace local del valor Rx del socio de enlace remoto.

Detalles de MED

- **Capacidades compatibles**: capacidades de MED admitidas en el puerto.
- **Capacidades actuales**: capacidades de MED habilitadas en el puerto.
- **Clasificación de dispositivo**: clasificación de dispositivo del punto de finalización de LLDP-MED. Las posibles clasificaciones de dispositivo son:
  - *Punto final clasificación 1*: clasificación de punto final genérica, que ofrece servicios LLDP básicos.
  - *Punto final clasificación 2*: clasificación de punto final de medios, que ofrece capacidades de transmisión por secuencias de medios, y todas las funciones de clasificación 1.
  - *Punto final clase 3*: clase de dispositivo de comunicaciones, que ofrece todas las características de las clases 1 y 2 más ubicación, 911, compatibilidad de dispositivo de Capa 2 y capacidades de administración de información de dispositivos.
- **Tipo de dispositivo PoE**: tipo de puerto PoE, por ejemplo, alimentado.
- **Fuente de alimentación PoE**: fuente de alimentación de puertos.
- **Prioridad de energía PoE**: prioridad de alimentación de puertos.
- **Valor de energía PoE**: valor de alimentación de puertos.
- **Revisión de hardware**: versión de hardware.
- **Revisión de firmware**: versión de firmware.
- **Revisión de software**: versión de software.
- **Número de serie**: número de serie del dispositivo.
- **Nombre del fabricante**: nombre del fabricante del dispositivo.
- **Nombre del modelo**: nombre del modelo del dispositivo.
- **ID de activos**: ID de activos.

Información de la ubicación

- **Cívica**: dirección postal.
- **Coordenadas**: coordenadas del mapa: latitud, longitud y altitud.
- **ECS ELIN**: Servicio de llamadas de emergencia (ECS), Número de identificación de la ubicación de la emergencia (ELIN).

Tabla de política de red

- **Tipo de aplicación**: tipo de aplicación de política de red; por ejemplo, voz.
- **ID de VLAN**: ID de VLAN para la que se define la política de red.
- **Tipo de VLAN**: tipo de VLAN para la que se define la política de red. Los valores posibles del campo son:
  - *Etiquetada*: indica que la política de red está definida para VLAN con etiqueta.
  - *Sin etiquetar*: indica que la política de red está definida para VLAN sin etiqueta.
- **Prioridad del usuario**: prioridad del usuario de política de red.
- **DSCP**: DSCP (Código del punto de servicios diferenciados) de política de red.

PASO 3 En la parte inferior de la página, haga clic en **Tabla de estado de puertos LLDP** para ver los detalles en la **Tabla de estado de puertos LLDP**.

Información de vecinos LLDP

La página Información de vecinos LLDP contiene la información que se recibió de los dispositivos vecinos.

Luego del tiempo de espera (según el valor recibido del TLV de Tiempo de funcionamiento de vecindad durante el cual no se recibió ninguna PDU de LLDP de un vecino), la información se elimina.

Para ver la información de vecinos LLDP:

PASO 1 Haga clic en **Administración** > **Discovery - LLDP** > **Información de vecinos LLDP**.

PASO 2 Seleccione la interfaz para la que debe mostrarse la información de vecinos LLDP.

En esta página se muestran los siguientes campos para la interfaz seleccionada:

- **Puerto local**: número de puerto local al que está conectado el vecino.
- **Subtipo de ID de chasis**: tipo de ID de chasis (por ejemplo, dirección MAC).
- **ID de chasis**: identificador de chasis del dispositivo de vecindad 802 LAN.
- **Subtipo de ID de puerto**: tipo de identificador de puerto que se muestra.
- **ID de puerto**: identificador de puerto.
- **Nombre del sistema**: nombre publicado del dispositivo.

- **Tiempo de func.**: intervalo de tiempo (en segundos) después del cual la información de este vecino se elimina.

PASO 3 Seleccione un puerto local y haga clic en **Detalles**.

La página Información vecina de LLDP contiene los siguientes campos:

Detalles del puerto

- **Puerto local**: número de puerto.
- **Entrada MSAP**: número de entrada de Punto de acceso al servicio de dispositivos de medios (MSAP, Device Media Service Access Point).

Detalles básicos

- **Subtipo de ID de chasis**: tipo de ID de chasis (por ejemplo, dirección MAC).
- **ID de chasis**: identificador de chasis de dispositivo de vecindad 802 LAN.
- **Subtipo de ID de puerto**: tipo de identificador de puerto que se muestra.
- **ID de puerto**: identificador de puerto.
- **Descripción del puerto**: información acerca del puerto, incluido el fabricante, el nombre del producto y la versión de hardware/software.
- **Nombre del sistema**: nombre del sistema que se publica.
- **Descripción del sistema**: descripción de la entidad de red (en formato alfanumérico). Esto incluye el nombre del sistema y las versiones de hardware, sistema operativo y software de red que admite el dispositivo. El valor es igual al objeto sysDescr.
- **Capacidades del sistema admitidas**: funciones principales del dispositivo. Dos octetos indican las capacidades. Los bits del 0 al 7 indican otro, repetidor, puente, WLAN AP, router, teléfono, dispositivo de cableado DOCSIS y estación, respectivamente. Los bits del 8 al 15 están reservados.
- **Capacidades del sistema habilitadas**: funciones principales habilitadas del dispositivo.

Tabla de direcciones de administración

- **Subtipo de dirección**: subtipo de dirección de administración, por ejemplo, MAC o IPv4.
- **Dirección**: dirección de administración.
- **Subtipo de interfaz**: subtipo de puerto.
- **Número de interfaz**: número de puerto.

Detalles de MAC/PHY

- **Negociación automática admitida**: estado de autonegociación de velocidad de puerto admitido. Los valores posibles son verdadero y falso.
- **Negociación automática habilitada**: estado de autonegociación de velocidad de puerto activo. Los valores posibles son verdadero y falso.
- **Capacidades anunciadas de negociación automática**: capacidades de autonegociación de velocidad de puerto, por ejemplo, modo semidúplex 1000BASE-T, modo dúplex completo 100BASE-TX.
- **Tipo de MAU operativa**: tipo de MAU (Medium Attachment Unit, unidad de conexión al medio). La MAU desempeña funciones de capa física, incluida la conversión de datos digitales de la detección de colisión de interfaces Ethernet y la inyección de bits en la red; por ejemplo, modo dúplex completo 100BASE-TX.

Potencia 802.3 a través de MDI

- **Clasificación de puerto con compatibilidad de alimentación MDI**: clasificación de puerto con compatibilidad de alimentación anunciada.
- **Compatibilidad de alimentación MDI PSE**: indica si la alimentación MDI se admite en el puerto.
- **Estado de alimentación MDI PSE**: indica si la alimentación MDI está habilitada en el puerto.
- **Capacidad de control de pares de alimentación PSE**: indica si el control de pares de alimentación se admite en el puerto.
- **Par de alimentación PSE**: tipo de control de pares de alimentación que se admite en el puerto.
- **Clasificación de alimentación PSE**: clasificación de alimentación anunciada del puerto.

802.3 Detalles

- **802.3 Tamaño máximo de trama**: tamaño máximo de la trama anunciado que se admite en el puerto.

802.3 Añadidura de enlaces

- **Capacidad de agrupación**: indica si el puerto se puede añadir.
- **Estado de agrupación**: indica si el puerto está actualmente añadido.
- **ID de puerto de agrupación**: ID de puerto añadido anunciado.

802.3 Ethernet para uso eficiente de energía (EEE)

- **Tx remoto**: indica el tiempo (en microsegundos) que el socio de enlace transmisor espera antes de comenzar a transmitir los datos dejando el modo de reposo de baja potencia (LPI, Low Power).
- **Rx remoto**: indica el tiempo (en microsegundos) que el socio de enlace receptor solicita que el socio de enlace transmisor espere antes de transmitir los datos después del modo de reposo de baja potencia (LPI, Low Power Idle).
- **Eco de Tx local**: indica la reflexión del socio de enlace local del valor Tx del socio de enlace remoto.
- **Eco de Rx local**: indica la reflexión del socio de enlace local del valor Rx del socio de enlace remoto.

Detalles de MED

- **Capacidades admitidas**: capacidades de MED habilitadas en el puerto.
- **Capacidades actuales**: TLV de MED anunciados por el puerto.
- **Clasificación de dispositivo**: clasificación de dispositivo del punto de finalización de LLDP-MED. Las posibles clasificaciones de dispositivo son:
  - *Punto final clasificación 1*: indica una clasificación de punto final genérica, que ofrece servicios LLDP básicos.
  - *Punto final clasificación 2*: indica una clasificación de punto final de medios, que ofrece capacidades de transmisión por secuencias de medios, y todas las funciones de clasificación 1.
  - *Punto final clasificación 3*: indica una clasificación de dispositivo de comunicaciones, que ofrece todas las funciones de clasificación 1 y 2 más ubicación, 911, soporte de switch de capa 2 y capacidades de administración de información de dispositivos.
- **Tipo de dispositivo PoE**: tipo de puerto PoE, por ejemplo, alimentado.
- **Fuente de alimentación PoE**: fuente de alimentación del puerto.
- **Prioridad de energía PoE**: prioridad de alimentación del puerto.
- **Valor de energía PoE**: valor de alimentación del puerto.
- **Revisión de hardware**: versión de hardware.
- **Revisión de firmware**: versión de firmware.
- **Revisión de software**: versión de software.
- **Número de serie**: número de serie del dispositivo.
- **Nombre del fabricante**: nombre del fabricante del dispositivo.

- **Nombre del modelo**: nombre del modelo del dispositivo.
- **ID de activos**: ID de activos.

802.1 VLAN y protocolo

- **PVID**: ID de VLAN de puerto anunciado.

PPVID

Tabla PPVID

- **VID**: ID de VLAN de protocolo.
- **Soportados**: ID de VLAN de protocolo y puerto admitidos.
- **Habilitados**: ID de VLAN de protocolo y puerto habilitados.

ID de VLAN

Tabla de ID de VLAN

- **VID**: ID de VLAN de protocolo y puerto.
- **Nombre de VLAN**: nombres de VLAN anunciados.

ID de protocolo

- **ID de protocolo**: ID de protocolo anunciado.

Información de la ubicación

Ingrese las siguientes estructuras de datos en caracteres hexadecimales como se describe en la sección 10.2.4 de la norma ANSI-TIA-1057:

- **Cívica**: dirección postal o cívica.
- **Coordenadas**: coordenadas del mapa de ubicación: latitud, longitud y altitud.
- **ECS ELIN**: Servicio de llamadas de emergencia (ECS), Número de identificación de la ubicación de la emergencia (ELIN) del dispositivo.
- **Desconocida**: información de ubicación desconocida.

Políticas de red

Tabla de política de red

- **Tipo de aplicación**: tipo de aplicación de política de red; por ejemplo, voz.
- **ID de VLAN**: ID de VLAN para la que se define la política de red.
- **Tipo de VLAN**: tipo de VLAN, con etiqueta o sin etiqueta, para la que se define la política de red.
- **Prioridad del usuario**: prioridad del usuario de política de red.
- **DSCP**: DSCP (Código del punto de servicios diferenciados) de política de red.

PASO 4 Seleccione un puerto y haga clic en **Tabla de estado de puertos LLDP** para ver los detalles en la Tabla de estado de puertos LLDP.

Estadísticas LLDP

En la página Estadísticas LLDP, se muestra información estadística de LLDP por puerto.

Para ver las estadísticas LLDP:

PASO 1 Haga clic en **Administración** > **Discovery - LLDP** > **Estadísticas LLDP**.

Para cada puerto, se muestran los campos:

- **Interfaz**: identificador de interfaz.
- **Cantidad (total) de tramas Tx**: cantidad de tramas transmitidas.
- **Tramas Rx**
  - *Total*: cantidad de tramas recibidas.
  - *Descartadas*: cantidad total de tramas recibidas que se han descartado.
  - *Errores*: cantidad total de tramas recibidas con errores.
- **TLV Rx**
  - *Descartados*: cantidad total de TLV recibidos que se han descartado.
  - *No reconocidos*: cantidad total de TLV recibidos que no se han reconocido.
- **Conteo de eliminación de información de vecinos**: cantidad de vencimientos de vecinos en la interfaz.

PASO 2 Haga clic en **Actualización** para ver las últimas estadísticas.

Sobrecarga LLDP

LLDP añade información como TLV de LLDP y LLDP-MED en los paquetes LLDP. La sobrecarga LLDP se produce cuando la cantidad total de información que se debe incluir en un paquete LLDP excede el tamaño máximo de PDU que admite una interfaz.

En la página Sobrecarga LLDP, se muestran la cantidad de bytes de la información de LLDP/LLDP-MED, la cantidad de bytes disponibles para información adicional de LLDP y el estado de sobrecarga de cada interfaz.

Para ver la información de sobrecarga LLDP:

PASO 1 Haga clic en **Administración** > **Discovery - LLDP** > **Sobrecarga LLDP**.

En esta página, se muestran los siguientes campos para cada puerto:

- **Interfaz**: identificador de puerto.
- **Total de bytes en uso**: cantidad total de bytes de información de LLDP en cada paquete.
- **Bytes restantes disponibles**: cantidad total de bytes disponibles que quedan para la información adicional de LLDP en cada paquete.
- **Estado**: indica si los TLV se están transmitiendo o si están sobrecargados.

PASO 2 Para ver los detalles de sobrecarga de un puerto, selecciónelo y haga clic en **Detalles**.

En esta página, se muestra la siguiente información para cada TLV que se envía por el puerto:

- **TLV obligatorios de LLDP**
  - *Tamaño (Bytes)*: tamaño total obligatorio en bytes de TLV.
  - *Estado*: si el grupo de TLV obligatorio se está transmitiendo o si el grupo de TLV estaba sobrecargado.
- **Capacidades LLDP MED**
  - *Tamaño (Bytes)*: tamaño total en bytes de paquetes de capacidades LLDP MED.
  - *Estado*: si los paquetes de capacidades LLDP MED se han enviado o si estaban sobrecargados.
- **Ubicación LLDP MED**
  - *Tamaño (Bytes)*: tamaño total en bytes de paquetes de ubicaciones LLDP MED.
  - *Estado*: si los paquetes de ubicaciones LLDP MED se han enviado o si estaban sobrecargados.

- **Política de red LLDP MED**
  - *Tamaño (Bytes)*: tamaño total en bytes de paquetes de políticas de red LLDP MED.
  - *Estado*: si los paquetes de políticas de red LLDP MED se han enviado o si estaban sobrecargados.
- **Energía extendida LLDP MED a través de MDI**
  - *Tamaño (Bytes)*: tamaño total en bytes de paquetes de energía extendida LLDP MED a través de MDI.
  - *Estado*: si los paquetes de energía extendida LLDP MED a través de MDI se han enviado o si estaban sobrecargados.
- **802.3 TLV**
  - *Tamaño (Bytes)*: tamaño total en bytes de paquetes de TLV LLDP MED 802.3.
  - *Estado*: si los paquetes de TLV LLDP MED 802.3 se han enviado o si estaban sobrecargados.
- **TLV opcionales de LLDP**
  - *Tamaño (Bytes)*: tamaño total en bytes de paquetes de TLV LLDP MED opcionales.
  - *Estado*: si los paquetes de TLV LLDP MED opcionales se han enviado o si estaban sobrecargados.
- **Inventario LLDP MED**
  - *Tamaño (Bytes)*: tamaño total en bytes de paquetes de TLV de inventario LLDP MED.
  - *Estado*: si los paquetes de inventario LLDP MED se han enviado o si estaban sobrecargados.
- **Total**
  - *Total (Bytes)*: cantidad total de bytes de información de LLDP en cada paquete.
  - *Bytes restantes disponibles*: cantidad total de bytes disponibles que quedan para enviar la información adicional de LLDP en cada paquete.

Configuración de CDP

En esta sección se describe cómo configurar el protocolo CDP.

Abarca los siguientes temas:

- **Propiedades de CDP**
- **Configuración de interfaz de CDP**
- **Información local de CDP**
- **Información de vecinos CDP**
- **Estadísticas de CDP**

Propiedades de CDP

Al igual que LLDP, el protocolo de detección de Cisco (CDP) es un protocolo de la capa de enlace para que los vecinos conectados directamente se anuncien y anuncien sus capacidades entre ellos. A diferencia de LLDP, CDP es un protocolo de propiedad de Cisco.

Flujo de trabajo de la configuración de CDP

A continuación, se muestra un ejemplo de flujo de trabajo al configurar el CDP en el dispositivo. También puede encontrar más pautas de configuración del CDP en la sección.

PASO 1 Ingrese los parámetros globales de CDP mediante la página Propiedades de CDP.

PASO 2 Configure el CDP por interfaz mediante la página Configuración de la interfaz.

PASO 3 Si Smartport automático se utiliza para detectar las capacidades de los dispositivos CDP, habilite CDP en la página Propiedades de Smartport.

Consulte **Identificación de un tipo de Smartport** para obtener una descripción de cómo el CDP se utiliza para identificar dispositivos para la función Smartport.

Para ingresar los parámetros CDP generales:

PASO 1 Haga clic en **Administración** > **Detección de CDP** > **Propiedades**.

PASO 2 Ingrese los parámetros.

- **Estado de CDP**: seleccione esta opción para activar CDP en el dispositivo.

- **Manejo de tramas de CDP**: si CDP no está habilitado, seleccione la acción que se realizará si se recibe un paquete que coincide con los criterios seleccionados.
  - *Conexión en puente*: reenvíe el paquete basándose en la VLAN.
  - *Filtrado*: elimine el paquete.
  - *Inundación*: inundación que no detecta la VLAN que reenvía paquetes CDP entrantes a todos los puertos, salvo el puerto de ingreso.
- **Anuncio de VLAN de voz de CDP**: seleccione esta opción para activar el dispositivo para que anuncie la VLAN de voz en CDP en todos los puertos que tienen el CDP habilitado y son miembros de la VLAN de voz. La VLAN de voz se configura en la página Propiedades de VLAN de voz.
- **Validación de TLV obligatoria de CDP**: si se selecciona esta opción, los paquetes CDP entrantes que no contienen las TLV obligatorias se descartan, y el contador de errores inválidos aumenta.
- **Versión de CDP**: seleccione la versión de CDP que se debe utilizar.
- **Tiempo de espera de CDP**: la cantidad de tiempo que se retienen los paquetes CDP antes de que se descarten, medida en múltiplos del Intervalo para anuncio TLV. Por ejemplo, si el Intervalo para anuncio TLV es 30 segundos, y el valor de Retener multiplicador es 4, los paquetes LLDP se descartan después de 120 segundos. Las opciones posibles son las siguientes:
  - *Usar predeterminado*: utilice el tiempo predeterminado (180 segundos).
  - *Definida por el usuario*: ingrese el tiempo en segundos.
- **Velocidad de transmisión de CDP**: la velocidad en segundos en que se envían las actualizaciones de anuncios del CDP. Las opciones posibles son las siguientes:
  - *Usar predeterminado*: utilice la velocidad predeterminada (60 segundos).
  - *Definida por el usuario*: ingrese la velocidad en segundos.
- **Formato de Id. de dispositivo**: seleccione el formato del Id. de dispositivo (dirección MAC o número de serie). Las opciones posibles son las siguientes:
  - *Dirección MAC:* use la dirección MAC del dispositivo como ID del dispositivo.
  - *Número de serie:* use el número de serie del dispositivo como ID del dispositivo.
  - *Nombre de host:* use el nombre el host del dispositivo como ID del dispositivo.
- **Interfaz de origen**: la dirección IP que se utilizará en el TLV de las tramas. Las opciones posibles son las siguientes:
  - *Usar predeterminado*: utilice la dirección IP de la interfaz saliente.
  - *Definida por el usuario*: utilice la dirección IP de la interfaz (en el campo **Interfaz**) en el TLV de dirección.

- **Interfaz**: Si se seleccionó *Definida por el usuario* para **Interfaz de origen**, seleccione la interfaz.
- **Discrepancia de VLAN de voz de Syslog**: marque esta opción para enviar un mensaje de SYSLOG cuando se detecta una discrepancia en la VLAN de voz. Esto significa que la información de la VLAN de voz en la trama entrante no coincide con la que anuncia el dispositivo local.
- **Discrepancia de VLAN nativa de Syslog**: marque esta opción para enviar un mensaje de SYSLOG cuando se detecta una discrepancia en la VLAN nativa. Esto significa que la información de la VLAN nativa en la trama entrante no coincide con la que anuncia el dispositivo local.
- **Discrepancia dúplex de Syslog**: marque esta opción para enviar un mensaje de SYSLOG cuando se detecta una discrepancia en la información de dúplex. Esto significa que la información de dúplex en la trama entrante no coincide con la que anuncia el dispositivo local.

PASO 3 Haga clic en **Aplicar**. Se definen las propiedades LLDP.

Configuración de interfaz de CDP

La página Configuración de interfaz le permite habilitar o deshabilitar el CDP por puerto. También se pueden activar notificaciones cuando se presentan conflictos con los vecinos de CDP. El conflicto puede ser de datos de la VLAN de voz, de la VLAN nativa o dúplex.

Si se configuran estas propiedades, es posible seleccionar los tipos de información que se proporcionan a dispositivos que admiten el protocolo LLDP.

Los TLV de LLDP-MED que se desea anunciar se pueden seleccionar en la página Configuración de interfaz LLDP MED.

Para definir la configuración de interfaz CDP:

PASO 1 Haga clic en **Administración** > **Detección de CDP** > **Configuración de interfaz**.

En esta página se muestra la siguiente información de CDP para cada interfaz.

- **Estado de CDP**: la opción de publicación del CDP para el puerto.
- **Informes de conflictos con vecinos de CDP**: muestra el estado de las opciones de informe que están habilitadas y deshabilitadas en la página **Editar** (VLAN de voz/VLAN nativa/Dúplex).
- **Número de vecinos**: el número de vecinos detectados.

En la parte inferior de la página hay cuatro botones:

- **Copiar configuración**: seleccione este botón para copiar una configuración de un puerto a otro.
- **Editar**: los campos se explican en el siguiente paso 2.

- **Detalles de información local de CDP**: esta opción lo lleva a la página Administración > Detección de CDP > Información local de CDP.
- **Detalles de información de vecinos CDP**: esta opción lo lleva a la página Administración > Detección de CDP > Información de vecinos CDP.

PASO 2 Seleccione un puerto y haga clic en **Editar**.

En esta página se muestran los siguientes campos:

- **Interfaz**: seleccione la interfaz que desea definir.
- **Estado de CDP**: seleccione esta opción para habilitar o deshabilitar la opción de publicación del CDP para el puerto.

NOTA Los tres campos siguientes son para que funcionen cuando el dispositivo ha sido configurado para enviar trampas a la estación de administración.

- **Discrepancia de VLAN de voz de Syslog**: marque esta opción para enviar un mensaje de SYSLOG cuando se detecta una discrepancia en la VLAN de voz. Esto significa que la información de la VLAN de voz en la trama entrante no coincide con la que anuncia el dispositivo local.
- **Discrepancia de VLAN nativa de Syslog**: marque esta opción para enviar un mensaje de SYSLOG cuando se detecta una discrepancia en la VLAN nativa. Esto significa que la información de la VLAN nativa en la trama entrante no coincide con la que anuncia el dispositivo local.
- **Discrepancia dúplex de Syslog**: seleccione este campo para habilitar la opción de enviar un mensaje de SYSLOG cuando se detecta una discrepancia en la información de dúplex. Esto significa que la información de dúplex en la trama entrante no coincide con la que anuncia el dispositivo local.

PASO 3 Ingrese la información relevante y haga clic en **Aplicar**. La configuración del puerto se escribe en el archivo Configuración en ejecución.

Información local de CDP

Para ver la información que anuncia el protocolo CDP sobre el dispositivo local:

PASO 1 Haga clic en **Administración** > **Detección de CDP** > **Información local de CDP**.

PASO 2 Seleccione un puerto local y se mostrarán los siguientes campos:

- **Interfaz**: número del puerto local.
- **Estado de CDP**: muestra si el CDP está habilitado o no.

- **TLV de Id. de dispositivo**
  - **Tipo de Id. de dispositivo**: el tipo del Id. de dispositivo que se anuncia en el TLV de Id. de dispositivo.
  - **Id. de dispositivo**: Id. de dispositivo que se anuncia en el TLV de Id. de dispositivo.
- **TLV del nombre del sistema**
  - **Nombre del sistema:** nombre del sistema del dispositivo.
- **TLV de dirección**
  - **Dirección 1-3:** direcciones IP (que se anuncian en el TLV de la dirección del dispositivo).
- **TLV de puerto**
  - **ID de puerto**: el identificador de puerto que se anuncia en el TLV del puerto.
- **TLV de capacidades**
  - **Capacidades**: las capacidades que se anuncian en el TLV del puerto.
- **TLV de versión**
  - **Versión**: la información sobre la versión de software en la que se ejecuta el dispositivo.
- **TLV de plataforma**
  - **Plataforma**: el identificador de plataforma que se anuncia en el TLV de plataforma.
- **TLV de VLAN nativa**
  - **VLAN nativa**: el identificador de VLAN nativa que se anuncia en el TLV de VLAN nativa.
- **TLV de semidúplex/dúplex completo**
  - **Dúplex**: indica si el puerto es medio o completo, según se anuncia en el TLV de semidúplex/dúplex completo.
- **TLV de aparato**
  - **ID del aparato**: el tipo de dispositivo conectado al puerto que se anuncia en el TLV del aparato.
  - **ID de VLAN del aparato**: la VLAN del dispositivo que usa el aparato; por ejemplo, si el aparato es un teléfono IP, es la VLAN de voz.

- **TLV de confianza extendida**
  - **Confianza extendida**: habilitado indica que el puerto es confiable, lo que significa que el host/servidor desde el que se recibe el paquete es confiable para marcar los mismos paquetes. En este caso, los paquetes que se reciben en ese puerto no pueden volver a marcarse. Deshabilitado indica que el puerto no es confiable, en cuyo caso, el siguiente campo es relevante.
- **TLV de CoS para puertos no fiables**
  - **CoS para puertos no fiables**: si el campo Confianza extendida está deshabilitado en el puerto, este campo muestra el valor CoS de la capa 2, lo que significa un valor de prioridad de 802.1D/802.1p. Es el valor COS con el que el dispositivo vuelve a marcar todos los paquetes que se reciben un puerto no fiable.
- **TLV de energía**
  - **ID de solicitud**: el ID de solicitud de baja energía produce un eco en el campo ID de solicitud que se recibió por última vez en el TLV de energía solicitada. Es 0, si no se recibió el TLV de energía solicitada desde que el último paso de la interfaz fue a Arriba.
  - **ID de administración de energía**: valor aumentado en 1 (o 2, para evitar 0) cada vez que se presenta cualquiera de los siguientes casos:

    Los cambios Energía disponible o Nivel de energía de administración cambian el valor.

    Se recibe un TLV de energía solicitada con un campo ID de solicitud, que es diferente del conjunto que se recibió por última vez (o cuando se recibe el primer valor)

    La interfaz pasa a Abajo
  - **Energía disponible**: cantidad de energía que consume el puerto.
  - **Nivel de energía de administración**: muestra la solicitud del proveedor para el dispositivo alimentado para su TLV de consumo de energía. El dispositivo siempre muestra "Sin preferencia" en este campo.

Información de vecinos CDP

En la página Información de vecinos CDP, se muestra la información de CDP que se recibió de los dispositivos vecinos.

Luego del tiempo de espera (según el valor recibido del TLV de Tiempo de funcionamiento de vecindad durante el cual no se recibió ninguna PDU de CDP de un vecino), la información se elimina.

Para ver la información de vecinos de CDP:

PASO 1 Haga clic en **Administración** > **Detección de CDP** > **Información de vecinos CDP**.

PASO 2 Para seleccionar un filtro, marque la **casilla de verificación Filtro**, seleccione una interfaz local y haga clic en **Ir**.

El filtro se activa, y **Borrar filtro** queda habilitado.

PASO 3 Haga clic en **Borrar filtro** si desea detener el filtro.

La página Información de vecinos de CDP muestra los siguientes campos para el socio de enlace (vecino):

- **Id. de dispositivo**: identificador de dispositivo del vecino.
- **Nombre del sistema**: nombre del sistema del vecino.
- **Interfaz local**: número del puerto local al que está conectado el vecino.
- **Versión de anuncio**: versión del protocolo CDP.
- **Tiempo de func. (seg.)**: intervalo de tiempo (en segundos) después del cual la información de este vecino se elimina.
- **Capacidades**: capacidades que anuncia el vecino.
- **Plataforma**: información del TLV de plataforma del vecino.
- **Interfaz de vecino**: interfaz saliente del vecino.

PASO 4 Seleccione un dispositivo y haga clic en **Detalles**.

Esta página contiene los siguientes campos sobre el vecino:

- **Id. de dispositivo**: identificador del Id. de dispositivo del vecino.
- **Nombre del sistema:** el nombre del identificador de dispositivo vecino.
- **Interfaz local**: número de interfaz del puerto por el cual arriba la trama.
- **Versión de anuncio**: versión del CDP.
- **Tiempo de func.**: intervalo de tiempo (en segundos) después del cual la información de este vecino se elimina.
- **Capacidades**: funciones principales del dispositivo. Dos octetos indican las capacidades. Los bits del 0 al 7 indican otro, repetidor, puente, WLAN AP, router, teléfono, dispositivo de cableado DOCSIS y estación, respectivamente. Los bits del 8 al 15 están reservados.
- **Plataforma**: identificador de la plataforma del vecino.

- **Interfaz del vecino**: número de interfaz del vecino por el cual arriba la trama.
- **VLAN nativa**: VLAN nativa del vecino.
- **Aplicación**: nombre de la aplicación que se ejecuta en el vecino.
- **Dúplex**: indica si la interfaz de los vecinos es semidúplex o dúplex completa.
- **Direcciones**: direcciones del vecino.
- **Energía extraída**: cantidad de energía que consume el vecino en la interfaz.
- **Versión**: versión de software del vecino.

NOTA Si hace clic en el botón **Borrar tabla**, se desconectan todos los dispositivos conectados desde el CDP y, si Smartport automático está habilitado, todos los tipos de puerto cambian al predeterminado.

Estadísticas de CDP

En la página Estadísticas de CDP, se muestra información sobre las tramas CDP que se enviaron a un puerto o que se recibieron de un puerto. Los paquetes CDP se reciben de los dispositivos conectados a las interfaces de los switches, y se utilizan para la función de Smartport. Para obtener más información, consulte **Configuración de CDP**.

Las estadísticas de CDP para un puerto solo se muestran si CDP está activado globalmente y en el puerto. Esto se hace en la página Propiedades de CDP y en la página Configuración de interfaz de CDP.

Para ver las estadísticas de CDP:

PASO 1 Haga clic en **Administración > Detección de CDP > Estadísticas de CDP.**

Los siguientes campos se muestran para todas las interfaces:

Paquetes recibidos/transmitidos:

- **Versión 1**: número de paquetes de la versión 1 de CDP recibidos/transmitidos.
- **Versión 2**: número de paquetes de la versión 2 de CDP recibidos/transmitidos.
- **Total**: número total de paquetes CDP recibidos/transmitidos.

En la sección Estadísticas de error de CDP se muestran los contadores de errores CDP.

- **Suma de comprobac. no permitida**: número de paquetes recibidos con valor de suma de comprobación no permitida.
- **Otros errores**: número de paquetes recibidos con errores, a diferencia de las sumas de comprobación no permitidas.
- **Vecinos superan el máximo**: número de veces que la información de los paquetes no se pudo almacenar en caché por falta de espacio.

Para borrar todos los contadores de todas las interfaces, haga clic en **Borrar todos los contadores de interfaz**. Para borrar todos los contadores en una interfaz, selecciónela y haga clic en **Borrar contadores de interfaz**.

10

Administración de puertos

En esta sección se describe la configuración de puertos, la añadidura de enlaces y la función Green Ethernet.

Abarca los siguientes temas:

- **Configuración de puertos**
- **Detección de bucle invertido**
- **Añadidura de enlaces**
- **UDLD**
- **Configuración de Green Ethernet**

Configuración de puertos

Flujo de trabajo

Para configurar puertos, siga los siguientes pasos:

1. Configure los puertos mediante la página Configuración de puertos.
2. Active o desactive el protocolo LAG (Link Aggregation Control, control de añadidura de enlaces) y configure los posibles puertos miembro a los LAG deseados mediante la página Administración de LAG. De forma predeterminada, todos los LAG están vacíos.
3. Configure los parámetros Ethernet, como velocidad y negociación automática, para los LAG mediante la página Configuración de LAG.
4. Configure los parámetros de LACP para los puertos que son miembros o candidatos de un LAG, mediante la página LACP.
5. Configure Green Ethernet y 802.3 Ethernet para uso eficiente de energía mediante la página Propiedades.

6. Configure el modo de energía Green Ethernet y 802.3 Ethernet para uso eficiente de energía por puerto mediante la página Configuración de puertos.
7. Si se admite y se activa la PoE (Power over Ethernet, alimentación por Ethernet), configure el dispositivo como se describe en **Administración de puertos: PoE**.

Configuración de puertos

Los puertos pueden configurarse en las siguientes páginas.

Configuración de puertos

En la página Configuración de puertos, se muestran los valores globales y por puerto de todos los puertos. Esta página le permite seleccionar y configurar los puertos que desea en la página Editar configuración de puerto.

Para configurar los valores de los puertos:

PASO 1 Haga clic en **Administración de puertos** > **Configuración de puertos**.

PASO 2 Seleccione **Tramas Jumbo** para admitir paquetes de hasta 10 Kb de tamaño. Si no se habilita **Tramas Jumbo** (predeterminado), el sistema admite paquetes de hasta 2,000 bytes. Para que las tramas jumbo tengan efecto, deberá reiniciarse el dispositivo después de activar la función.

PASO 3 Haga clic en **Aplicar** para actualizar la configuración global.

Los cambios en la configuración de tramas jumbo surten efecto *solo* después de que la configuración en ejecución se guarda explícitamente en el Archivo de configuración de inicio mediante la página Copiar/guardar configuración, y se reinicia el dispositivo.

PASO 4 Para actualizar los valores de los puertos, seleccione el puerto que desea y haga clic en **Editar.**

PASO 5 Modifique los siguientes parámetros:

- **Interfaz**: seleccione el número de puerto.
- **Descripción del puerto**: ingrese un comentario o el nombre de puerto definido por el usuario.
- **Tipo de puerto**: muestra el tipo de puerto y la velocidad. Las opciones posibles son:
  - *Puertos de cobre*: regulares, no combinados, admiten los siguientes valores: 10 M, 100 M y 1000 M (tipo: de cobre).
  - *Puertos combinados de cobre*: puerto combinado conectado con cable de cobre CAT5, admite los siguientes valores: 10 M, 100 M y 1000 M (tipo: ComboC).

- *Combo Fiber*: *puerto del Conversor de la Interfaz Gigabit SFP Fiber* con los siguientes valores: 100 M y 1000 M (tipo: ComboF).
- Fibra óptica de 10 G: puertos con velocidades de 1 G o 10 G.

NOTA SFP Fiber tiene prioridad en los puertos combinados cuando se están usando ambos puertos.

- **Estado administrativo**: seleccione esta opción si el puerto debe estar activo o inactivo cuando se reinicia el dispositivo.
- **Estado operativo**: muestra si el puerto actualmente está activo o inactivo. Si el puerto se desconecta debido a un error, aparecerá la descripción del error.
- **Trampas de SNMP de estado de enlace a la página**: seleccione para habilitar la generación de trampas SNMP que notifiquen los cambios en el estado de enlace del puerto.
- **Intervalo de tiempo**: seleccione esta opción para activar el intervalo de tiempo durante el cual el puerto estará en estado activo. Si el intervalo de tiempo no está activado, el puerto se encuentra apagado. Si hay un intervalo de tiempo configurado, tendrá efecto solo cuando el puerto esté activo administrativamente. Si aún no hay un intervalo de tiempo definido, haga clic en **Editar** para ir a la página Intervalo de tiempo.
- **Nombre del intervalo de tiempo**: seleccione el perfil que especifica el intervalo de tiempo.
- **Estado operativo del intervalo de tiempo**: muestra si el intervalo de tiempo está actualmente activo o no activo.
- **Negociación automática**: seleccione para habilitar la negociación automática en el puerto. La negociación automática habilita un puerto para anunciar su velocidad de transmisión, modo dúplex y capacidades de control de flujo al socio de enlace del puerto.
- **Negociación automática operativa**: muestra el estado de negociación automática actual en el puerto.
- **Velocidad del puerto administrativo**: seleccione la velocidad del puerto. El tipo de puerto determina las velocidades que están disponibles. Usted puede designar la *Velocidad administrativa* solo cuando la negociación automática de puertos está deshabilitada.
- **Velocidad del puerto operativo**: muestra la velocidad actual del puerto que es el resultado de la negociación.
- **Modo dúplex administrativo**: seleccione el modo dúplex de puerto. Este campo solo se puede configurar cuando la negociación automática está deshabilitada y la velocidad del puerto es 10 M o 100 M. En la velocidad de puerto de 1 G, el modo siempre es dúplex completo. Las opciones posibles son:
  - *Semi*: la interfaz admite la transmisión entre el dispositivo y el cliente solo en una dirección a la vez.
  - *Completo*: la interfaz admite la transmisión entre el dispositivo y el cliente en ambas direcciones simultáneamente.

- **Modo dúplex operativo**: muestra el modo dúplex actual de los puertos.
- **Anuncio automático**: seleccione las capacidades que anuncia la negociación automática cuando está habilitada. Las opciones son:
  - *Capacidad máxima*: se pueden aceptar todos los valores de velocidades de puerto y modo dúplex.
  - *10 Semi*: velocidad de 10 Mbps y modo semidúplex.
  - *10 Completo*: velocidad de 10 Mbps y modo dúplex completo.
  - *100 Semi*: velocidad de 100 Mbps y modo semidúplex.
  - *100 Completo*: velocidad de 100 Mbps y modo dúplex completo.
  - *1000 Completo*: velocidad de 1000 Mbps y modo dúplex completo.
- **Anuncio operativo**: muestra las capacidades que están publicadas actualmente en el vecino de los puertos. Las opciones posibles son las especificadas en el campo *Anuncio administrativo*.
- **Modo de preferencia**: seleccione el modo esclavos maestros de la interfaz para la operación de autonegociación. Seleccione una de las siguientes opciones:
  - *Esclavo*: comience la negociación con la preferencia de que el puerto del dispositivo sea esclavo en el proceso de autonegociación.
  - *Maestro*: comience la negociación con la preferencia de que el puerto del dispositivo sea maestro en el proceso de autonegociación.
- **Anuncio de vecino**: muestra las capacidades que anuncia el dispositivo vecino (socio de enlace).
- **Contrapresión**: seleccione el modo de contrapresión en el puerto (se usa con el modo semidúplex) para reducir la velocidad de la recepción de paquetes cuando el dispositivo está congestionado. Deshabilita el puerto remoto, lo que le impide enviar paquetes mediante la congestión de la señal.
- **Control de flujo**: habilite o deshabilite el control de flujo 802.3x o habilite la negociación automática del control de flujo en el puerto (solo cuando está en el modo dúplex completo).
- **MDI/MDIX**: el estado del puerto de *Interfaz dependiente de medios* (MDI, Media Dependent Interface)/ *Interfaz dependiente de medios con cruce* (MDIX, Media Dependent Interface with Crossover).

  Las opciones son:
  - *MDIX*: seleccione esta opción para intercambiar la transmisión y recibir pares.
  - *MDI*: seleccione esta opción para conectar este dispositivo a una estación mediante un cable de conexión directa.
  - *Automático*: seleccione esta opción para configurar este dispositivo para detectar automáticamente las clavijas correctas para la conexión con otro dispositivo.

- **MDI/MDIX operativo**: muestra la configuración de MDI/MDIX actual.
- **Miembro de LAG**: muestra si el puerto es miembro de un LAG.
- **Puerto protegido**: seleccione esta opción para que este sea un puerto protegido. (Un puerto protegido también se denomina borde de VLAN privada [PVE]). A continuación se definen las funciones de un puerto protegido:
  - Los puertos protegidos proporcionan aislamiento de capa 2 entre las interfaces (puertos Ethernet y LAG) que comparten la misma VLAN.
  - Los paquetes que se reciben de los puertos protegidos solo se pueden reenviar a los puertos de egreso desprotegidos. Las reglas de filtrado de puertos protegidos también se aplican a los paquetes que el software reenvía, como las aplicaciones de indagación.
  - La protección de puertos no está sujeta a la pertenencia a la VLAN. Los dispositivos conectados a puertos protegidos no pueden comunicarse entre sí, ni siquiera si son miembros de la misma VLAN.
  - Los puertos y los LAG pueden ser definidos como protegidos o desprotegidos. Los LAG protegidos se describen en la sección **Configuración de los valores de LAG**.
- **Miembro de LAG**: si el puerto es miembro de un LAG, se muestra el número de LAG aquí; de lo contrario, este campo queda en blanco.

PASO 6 Haga clic en **Aplicar**. La configuración del puerto se escribe en el archivo Configuración en ejecución.

Configuración de recuperación de error

Esta página permite reactivar automáticamente un puerto que se haya cerrado por una condición de error después de haber transcurrido el intervalo de recuperación automática.

Para configurar los ajustes de recuperación de error:

PASO 1 Haga clic en **Administración de puertos** > **Configuración de recuperación de error**.

PASO 2 Ingrese los siguientes campos:

- **Intervalo de recuperación automática**: indique la demora para la recuperación automática de errores, si está activada, después de que se apaga un puerto.

Recuperación ErrDisable automática

- **Seguridad de puertos**: seleccione para activar la recuperación automática de errores si el puerto se apaga debido a violaciones de seguridad.
- **Violación de host único 802.1x**: seleccione para activar la recuperación automática de errores si 802.1x apaga el puerto.

- **Rechazar ACL**: seleccione para activar el mecanismo de recuperación automática de errores de una acción del ACL.
- **Protección STP BPDU**: seleccione para activar el mecanismo de recuperación automática de errores cuando la protección STP BPDU apaga el puerto.
- **Protección de bucle invertido de STP**: active la recuperación automática cuando la protección de bucle invertido de STP apaga el puerto.
- **UDLD**: seleccione para habilitar el mecanismo de recuperación automática de errores para el estado apagado de UDLD.
- **Detección de bucle invertido**: seleccione para activar el mecanismo de recuperación de errores para los puertos que apagó la detección de bucle invertido.

PASO 3 Haga clic en **Aplicar** para actualizar la configuración global.

Para reactivar manualmente un puerto:

PASO 1 Haga clic en **Administración de puertos** > **Configuración de recuperación de error**.

Aparece la lista de interfaces desactivadas junto con el **Motivo de la suspensión**.

PASO 2 Seleccione la interfaz que se debe reactivar.

PASO 3 Haga clic en **Reactivar**.

Detección de bucle invertido

La detección de bucle invertido (LBD) brinda protección de bucle mediante el envío de paquetes de protocolos en bucle fuera de los puertos en donde se activó la protección de bucle. Cuando el switch envía un paquete de protocolo en bucle y luego recibe el mismo paquete, apaga el puerto que recibió el paquete.

La detección de bucle invertido funciona independiente de STP. Después de descubrir un bucle, el puerto que recibió los bucles queda en estado apagado. Se envía una trampa y se registra el evento. Los administradores de la red pueden definir un intervalo de detección que establezca el intervalo entre los paquetes LBD.

El protocolo de detección de bucle invertido puede detectar los siguientes casos de bucle:

- **Cable acortado**: puerto donde el tráfico que se recibe pasa por un bucle de retorno.
- **Bucle directo de varios puertos**: el switch se conecta a otro switch con más de un puerto y se deshabilita STP.
- **Bucle de segmento de LAN**: el switch se conecta con uno o más puertos a un segmento de LAN que tiene bucles.

Cómo funciona LBD

El protocolo LBD periódicamente transmite paquetes de detección de bucle invertido. Un switch detecta un bucle cuando recibe sus propios paquetes LBD.

Deben darse las siguientes condiciones para que un puerto tenga LBD activo:

- LBD se habilita globalmente.
- LBD está habilitado en el puerto.
- El estado operativo del puerto es activo.
- El estado del puerto es reenvío STP/desactivado (estado de reenvío de instancia de MSTP, instancia 0).

Las tramas de LBD se envían en la fila de máxima prioridad de los puertos LBD activos (en el caso de LAG, LBD se envía en cada miembro de puerto activo del LAG).

Cuando se detecta un bucle, el switch realiza las siguientes acciones:

- Establece los puertos receptores o LAG en el estado de desactivar error.
- Envía una trampa de SNMP adecuada.
- Genera un mensaje SYLOG adecuado.

Configuración de la detección de bucle invertido

Configuración y valores predeterminados

La detección de bucle invertido no se encuentra habilitada como opción predeterminada.

Interacciones con otras funciones

Si STP está activado en un puerto que tiene habilitada la detección de bucle invertido, el estado del puerto debe ser reenvío STP.

Configuración del flujo de trabajo de LBD

Para activar y configurar LBD:

PASO 1 Habilite la detección de bucle invertido en todo el sistema desde la página de configuración de la detección de bucle invertido.

PASO 2 Habilite la detección de bucle invertido en los puertos de acceso desde la página de configuración de la detección de bucle invertido.

PASO 3 Habilite la recuperación automática para la detección de bucle invertido desde la página Configuración de recuperación de error.

Para configurar la detección de bucle invertido:

PASO 1 Haga clic en **Administración de puertos** > **Configuración de la detección de bucle invertido**.

PASO 2 Seleccione **Habilitar** para el campo global **Detección de bucle invertido** a fin de activar esta función.

PASO 3 Ingrese el **Intervalo de detección**. Es el intervalo entre los envíos de paquetes LBD.

PASO 4 Haga clic en **Aplicar** para guardar la configuración en el archivo de configuración en ejecución.

Se visualizan los campos a continuación para cada interfaz independientemente del **Estado de detección de bucle invertido**:

- **Administrativo**: la detección de bucle invertido está activada.
- **Operativo**: la detección de bucle invertido está activada, pero desactivada en la interfaz.

PASO 5 Indique si desea activar LBD en los puertos o LAG en el campo **Tipo de interfaz igual a**.

PASO 6 Seleccione los puertos o LAG en donde debe habilitarse LBD, y haga clic en **Editar**.

PASO 7 Seleccione **Activar** en el campo Estado de detección de bucle invertido para el puerto o LAG seleccionado.

PASO 8 Haga clic en **Aplicar** para guardar la configuración en el archivo de configuración en ejecución.

Añadidura de enlaces

En esta sección se describe cómo configurar LAG. Abarca los siguientes temas:

- **Información general de la añadidura de enlaces**
- **Configuración y valores predeterminados**
- **Flujo de trabajo de LAG estático y dinámico**
- **Definición de la administración de LAG**
- **Configuración de los valores de LAG**
- **Configuración del LACP**

Información general de la añadidura de enlaces

El Protocolo de control de añadidura de enlaces (LACP, Link Aggregation Control Protocol) es parte de una especificación IEEE (802.3az) que lo habilita para incluir varios puertos físicos juntos para formar un solo canal lógico (LAG). Los LAG multiplican el ancho de banda, aumentan la flexibilidad de los puertos y proporcionan redundancia de enlaces entre dos dispositivos.

Se admiten dos tipos de LAG:

- **Estático**: un LAG es estático si el LACP está deshabilitado en él. Los puertos asignados a un LAG estático son siempre miembros activos. Una vez que se crea un LAG manualmente, la opción de LACP no se puede añadir ni eliminar hasta que el LAG se edite y se elimine un miembro (el que puede añadirse nuevamente antes de aplicarse); entonces, el botón LACP estará disponible para editarse.
- **Dinámico**: un LAG es dinámico si el LACP está habilitado en él. Los puertos asignados al LAG dinámico son puertos candidatos. El LACP determina qué puertos candidatos son puertos miembros activos. Los puertos candidatos no activos son puertos *en espera* listos para reemplazar cualquier puerto miembro activo que falle.

Balance de carga

Al tráfico que se reenvía a un LAG se le realiza un balance de carga en los puertos miembro activos y, de esta forma, se logra un ancho de banda efectivo similar a la combinación del ancho de banda de todos los puertos miembro activos del LAG.

El balance de carga del tráfico en los puertos miembro activos de un LAG es administrado por una función de distribución basada en el hash que distribuye tráfico unidifusión basado en la información de encabezado de paquetes de capa 2 o capa 3.

El dispositivo admite dos modos de equilibrio de carga:

- **Por direcciones MAC**: basado en las direcciones MAC de origen y de destino de todos los paquetes.
- **Por direcciones IP y MAC**: basado en las direcciones IP de origen y de destino para los paquetes IP, y las direcciones MAC de origen y de destino para los paquetes que no son IP.

Administración de LAG

En general, el sistema trata a un LAG como un puerto lógico único. En concreto, el LAG tiene atributos de puerto similares a un puerto regular, como el estado y la velocidad.

El dispositivo admite 32 LAG con hasta 8 puertos en un grupo LAG.

Cada LAG tiene las siguientes características:

- Todos los puertos de un LAG deben ser del mismo tipo de medio.
- Para añadir un puerto al LAG, este no puede pertenecer a ninguna VLAN, excepto a la VLAN predeterminada.
- Los puertos de un LAG no se deben asignar a otro LAG.
- A un LAG estático no se le pueden asignar más de ocho puertos, y para un LAG dinámico no puede haber más de 16 puertos candidatos.
- Todos los puertos de un LAG deben tener la negociación automática deshabilitada, aunque el LAG puede tenerla habilitada.
- Cuando un puerto se añade a un LAG, la configuración del LAG se aplica al puerto Cuando el puerto se elimina del LAG, se vuelve a aplicar su configuración original.
- Los protocolos, como el Spanning Tree (Protocolo de árbol de expansión), consideran que todos los puertos del LAG son un solo puerto.

Configuración y valores predeterminados

De forma predeterminada, los puertos no son miembros de un LAG ni candidatos para formar parte de un LAG.

Flujo de trabajo de LAG estático y dinámico

Una vez que se creó un LAG manualmente, no se puede añadir ni eliminar un LACP hasta que el LAG se edite y se elimine un miembro. Solo entonces el botón LACP estará disponible para editarse.

Para configurar un LAG **estático**, siga los siguientes pasos:

1. Deshabilite LACP en el LAG para que sea estático. Asigne hasta ocho puertos miembro activos al LAG estático seleccionando y pasando los puertos de la **Lista de puertos** a la lista de **Miembros de LAG**. Seleccione el algoritmo de equilibrio de carga para el LAG. Realice estas acciones en la página Administración de LAG.
2. Configure varios aspectos del LAG, como la velocidad y el control de flujo, mediante la página Configuración de LAG.

Para configurar un LAG **dinámico**, siga los siguientes pasos:

1. Habilite el LACP en el LAG. Asigne hasta 16 puertos candidatos al LAG dinámico seleccionando y pasando los puertos de la **Lista de puertos** a la lista **Miembros de LAG** mediante la página Administración de LAG.
2. Configure varios aspectos del LAG, como la velocidad y el control de flujo, mediante la página Configuración de LAG.
3. Defina el tiempo de espera y la prioridad de LACP de los puertos en el LAG mediante la página LACP.

Definición de la administración de LAG

En la página Administración de LAG, se muestran los valores globales y por LAG. La página también le permite configurar los valores globales, y seleccionar y editar el LAG que desea en la página Editar membresía LAG.

Para seleccionar el algoritmo de equilibrio de carga del LAG:

PASO 1 Haga clic en **Administración de puertos** > **Añadidura de enlaces** > **Administración de LAG**.

PASO 2 Seleccione uno de los siguientes **Algoritmo de balance de cargas**:

- *Dirección MAC*: realice el balance de carga por dirección MAC de origen y de destino en todos los paquetes.
- *Dirección IP/MAC*: realice el balance de carga por dirección IP de origen y de destino en los paquetes IP, y por dirección MAC de origen y de destino en los paquetes que no sean IP.

PASO 3 Haga clic en **Aplicar**. El algoritmo de equilibrio de carga se guarda en el archivo de configuración en ejecución.

Para definir los puertos miembro o candidato de un LAG.

PASO 1 Seleccione el LAG que desea configurar y haga clic en **Editar**.

Se muestran los siguientes campos para cada LAG (solo se describen los campos que no aparecen en la página Editar):

- **Estado de enlace**: indica si el puerto está activo o inactivo.
- **Miembro activo**: indica los puertos activos en el LAG.
- **Miembro en espera**: indica los puertos candidatos para ese LAG.

PASO 2 Ingrese los valores para los siguientes campos:

- **LAG**: seleccione el número de LAG.
- **Nombre de LAG**: ingrese el nombre de LAG o un comentario.
- **LACP**: seleccione esta opción para habilitar LACP en el LAG seleccionado. Esto lo transforma en un LAG dinámico. Este campo solo puede habilitarse después de mover un puerto al LAG del campo siguiente.
- **Lista de puertos**: mueva los puertos que desea asignar al LAG de la **Lista de puertos** a la lista de **Miembros de LAG**. A cada LAG estático se le pueden asignar hasta ocho puertos y a un LAG dinámico se le pueden asignar 16 puertos. Son los puertos candidatos.

PASO 3 Haga clic en **Aplicar**. La membresía LAG se guarda en el archivo de configuración en ejecución.

Configuración de los valores de LAG

En la página Configuración de LAG, se muestra una tabla de valores actuales de todos los LAG. Si inicia la página Editar configuración LAG, puede configurar los valores de los LAG seleccionados y reactivar los LAG suspendidos.

Para configurar los valores de LAG o reactivar un LAG suspendido:

PASO 1 Haga clic en **Administración de puertos** > **Añadidura de enlaces** > **Configuración de LAG**.

PASO 2 Seleccione un LAG, y haga clic en **Editar**.

PASO 3 Ingrese los valores para los siguientes campos:

- **LAG**: seleccione el número de ID de LAG.

- **Tipo de LAG**: muestra el tipo de puerto que incluye el LAG.
- **Descripción**: ingrese el nombre de LAG o un comentario.
- **Estado administrativo**: configure el LAG seleccionado en activo o inactivo.
- **Estado operativo**: muestra si el LAG está funcionando actualmente.
- **Trampas de SNMP de estado de enlace a la página**: seleccione para habilitar la generación de trampas SNMP que notifiquen los cambios en el estado de enlace de los puertos en LAG.
- **Intervalo de tiempo**: seleccione esta opción para activar el intervalo de tiempo durante el cual el puerto estará en estado activo. Si el intervalo de tiempo no está activado, el puerto se encuentra apagado. Si hay un intervalo de tiempo configurado, tendrá efecto solo cuando el puerto esté activo administrativamente. Si aún no hay un intervalo de tiempo definido, haga clic en **Editar** para ir a la página Intervalo de tiempo.
- **Nombre del intervalo de tiempo**: seleccione el perfil que especifica el intervalo de tiempo.
- **Estado operativo del intervalo de tiempo**: muestra si el intervalo de tiempo está actualmente activo o no activo.
- **Reactivar LAG suspendido**: seleccione esta opción para reactivar un puerto si el LAG se ha desactivado mediante la opción de seguridad de puerto bloqueado o a través de las configuraciones de ACL.
- **Negociación automática administrativa**: habilita o deshabilita la negociación automática en el LAG. La negociación automática es un protocolo entre dos socios de enlace que habilita un LAG para anunciar su velocidad de transmisión y control de flujo a su socio (el Control de flujo predeterminado está *deshabilitado*). Se recomienda mantener la negociación automática habilitada a ambos lados de un enlace añadido, o deshabilitada a ambos lados, mientras se asegura de que las velocidades de enlace sean idénticas.
- **Negociación automática operativa**: muestra la configuración de la negociación automática.
- **Velocidad administrativa**: seleccione la velocidad del LAG.
- **Velocidad operativa de LAG**: muestra la velocidad actual a la que está funcionando el LAG.
- **Anuncio administrativo**: seleccione las capacidades que el LAG anunciará. Las opciones son:
  - *Capacidad máxima*: todas las velocidades de LAG y ambos modos dúplex están disponibles.
  - *10 Completo*: el LAG anuncia una velocidad de 10 Mbps y el modo es dúplex completo.
  - *100 Completo*: el LAG anuncia una velocidad de 100 Mbps y el modo es dúplex completo.
  - *1000 Completo*: el LAG anuncia una velocidad de 1000 Mbps y el modo es dúplex completo.
  - *10000 Completo*: el LAG anuncia una velocidad de 10000 Mbps y el modo es dúplex completo.

- **Anuncio operativo**: muestra el estado de Anuncio administrativo. El LAG anuncia sus capacidades a su LAG vecino para iniciar el proceso de negociación. Los valores posibles son los que se especifican en el campo *Anuncio administrativo*.
- **Control de flujo administrativo:** determina el control de flujo para **Habilitar** o **Deshabilitar** o permitir la **Negociación automática** del Control de flujo en el LAG.
- **Control de flujo operativo**: muestra la configuración actual de Control de flujo.
- **LAG protegido**: seleccione esta opción para hacer que el LAG sea un puerto protegido para el aislamiento de capa 2. Consulte la descripción de Configuración de puertos en **Ajuste de la configuración básica de los puertos** para obtener detalles con respecto a puertos protegidos y LAG.

PASO 4 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Configuración del LACP

Un LAG dinámico tiene el LACP habilitado, y el LACP se ejecuta en todos los puertos candidatos definidos en el LAG.

Prioridad y reglas del LACP

La prioridad de sistema LACP y la prioridad de puerto LACP se utilizan para determinar qué puertos candidatos se transforman en puertos miembro activos en un LAG dinámico configurado con más de ocho puertos candidatos.

Los puertos candidatos seleccionados del LAG están todos conectados al mismo dispositivo remoto. Tanto los switches locales como remotos tienen una prioridad de sistema LACP.

El siguiente algoritmo se usa para determinar si las prioridades de puerto LACP se toman del dispositivo local o remoto: la prioridad de sistema LACP local se compara con la prioridad de sistema LACP remoto. El dispositivo con la prioridad menor controla la selección del puerto candidato al LAG. Si ambas prioridades son iguales, se compara la dirección MAC local y la remota. La prioridad del dispositivo con la dirección MAC más baja controla la selección del puerto candidato al LAG.

Un LAG dinámico puede tener hasta 16 puertos Ethernet del mismo tipo. Puede haber hasta ocho puertos activos, y puede haber hasta ocho puertos en modo en espera. Cuando hay más de ocho puertos en el LAG dinámico, el dispositivo del extremo de control del enlace usa prioridades de puerto para determinar qué puertos se agrupan en el LAG y qué puertos se ponen en el modo en espera. Se ignoran las prioridades de puerto del otro dispositivo (el extremo del enlace que no es de control).

A continuación se indican las reglas adicionales para seleccionar los puertos activos o en espera en un LACP dinámico:

- Se pone en espera a todo enlace que funcione a una velocidad distinta del miembro activo de velocidad más alta o que funciona en modo semidúplex. Todos los puertos activos de un LAG dinámico funcionan a la misma velocidad en baudios.
- Si la prioridad de LACP de puertos del enlace es más baja que la de los miembros de enlace actualmente activos, y la cantidad de miembros activos ya es la máxima, el enlace queda inactivo y se coloca en el modo en espera.

LACP sin socio de enlace

Para que LACP cree un LAG, los puertos de ambos extremos del enlace deben estar configurados para LACP. Esto significa que los puertos envían PDU (Protocol Data Unit, unidad de datos de protocolo) de LACP y manejan las PDU recibidas.

No obstante, a veces sucede que un socio de enlace no está configurado para LACP (temporalmente). Un ejemplo puede ser cuando el socio de enlace está en un dispositivo que espera recibir su configuración mediante el protocolo de configuración automática. Los puertos del dispositivo aún no se configuraron para LACP. Si el enlace LAG no puede conectarse, el dispositivo jamás podrá configurarse. Algo similar sucede con las computadoras con inicio de red y NIC (Network Interface Card, tarjeta de interfaz de red) dual (por ejemplo, PXE [Pre-Execution Environment, entorno de ejecución de inicio]), que reciben la configuración LAG solo después de iniciarse.

Cuando se configuran varios puertos para LACP y el enlace se conecta en uno o varios puertos, pero no hay respuestas de LACP desde el socio de enlace para esos puertos, el primer puerto que se conectó se agrega al LAG de LACP y se activa (los otros puertos quedan como no candidatos). De esta forma, el dispositivo vecino puede, por ejemplo, obtener su dirección IP mediante DHCP y su configuración mediante la configuración automática.

Configuración de valores de los parámetros de LACP

Use la página LACP para configurar los puertos candidatos para el LAG y para configurar los parámetros de LACP por puerto.

Con todos los factores iguales, cuando el LAG se configura con más puertos candidatos que la cantidad máxima de puertos activos permitidos (8), el dispositivo selecciona puertos como activos del LAG dinámico del dispositivo que tiene la prioridad más alta.

NOTA La configuración de LACP es irrelevante en los puertos que no son miembros de un LAG dinámico.

Para definir los valores de LACP:

PASO 1 Haga clic en **Administración de puertos** > **Añadidura de enlaces** > **LACP**.

PASO 2 Ingrese la prioridad de sistema LACP. Consulte **Prioridad y reglas del LACP**.

PASO 3 Seleccione un puerto y haga clic en **Editar**.

PASO 4 Ingrese los valores para los siguientes campos:

- **Puerto**: seleccione el número de puerto al que se le asignan los valores de tiempo de espera y prioridad.
- **Prioridad de puerto LACP**: ingrese el valor de prioridad de LACP para el puerto. Consulte **Configuración de valores de los parámetros de LACP**.
- **Caducidad de LACP**: intervalo de tiempo entre el envío y la recepción de PDU de LACP consecutivas. Seleccione las transmisiones periódicas de PDU de LACP que se producen a una velocidad de transmisión **Lenta** o **Rápida**, según la preferencia de caducidad de LACP expresada.

PASO 5 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

UDLD

Consulte **Administración de puertos: Detección de enlace unidireccional**.

PoE

Consulte **Administración de puertos: PoE**.

Configuración de Green Ethernet

En esta sección, se describe la función Green Ethernet que se asigna para ahorrar energía en el dispositivo.

Contiene las siguientes secciones:

- **Información general de Green Ethernet**
- **Propiedades globales de Green Ethernet**
- **Propiedades de Green Ethernet para puertos**

Información general de Green Ethernet

Green Ethernet es un nombre común para un conjunto de funciones que están diseñadas para no dañar el medio ambiente y reducir el consumo de energía de un dispositivo. Green Ethernet es distinto de EEE en el sentido de que la detección de energía de Green Ethernet está habilitada en todos los dispositivos en los que solo los puertos Gigabyte están habilitados con EEE.

La función Green Ethernet puede reducir el uso de energía general de dos formas:

- **Modo de detección de energía**: en un enlace inactivo, el puerto pasa al modo inactivo y ahorra energía mientras mantiene el estado administrativo del puerto activo. La recuperación de este modo al modo operativo completo es rápida, transparente y no se pierde ninguna trama. Este modo se admite en puertos GE y puertos FE.
- **Modo de alcance corto**: esta función permite ahorrar energía en un cable corto. Una vez analizado el cable, el uso de energía se ajusta a las distintas longitudes de cable. Si el cable es más corto que 50 metros, el dispositivo usa menos energía para enviar tramas por el cable y, de esta manera, ahorra energía. Este modo solo se admite en puertos RJ45 GE; no se aplica a puertos combinados.

  Este modo está deshabilitado globalmente en forma predeterminada, y no puede habilitarse si el modo EEE está habilitado (ver más abajo).

Además de las funciones de Green Ethernet arriba mencionadas, el modo **802.3az Ethernet para uso eficiente de energía (EEE)** se encuentra en los dispositivos que admiten los puertos GE. EEE reduce el consumo de energía cuando no hay tráfico en el puerto. Para obtener más información, consulte la sección **Función 802.3az Ethernet para uso eficiente de energía** (disponible en los modelos GE solamente).

EEE está habilitado globalmente de forma predeterminada. En un puerto dado, si EEE está habilitado, el modo de alcance corto estará deshabilitado. Si el modo de alcance corto está habilitado, EEE se verá gris.

Estos modos se configuran por puerto, sin tener en cuenta la membresía LAG de los puertos.

Los dispositivos LED consumen energía. Dado que la mayoría de los dispositivos se encuentran en una sala desocupada, tener estos LED encendidos es un desperdicio de energía. La función Green Ethernet le permite deshabilitar los LED del puerto (para enlaces, velocidad y PoE) cuando no se necesitan, y habilitarlos cuando los necesita (depuración, conexión de dispositivos adicionales, etcétera).

En la página Resumen del sistema, los indicadores LED que se muestran en las imágenes del tablero de dispositivos no se verán afectados por la desactivación de los indicadores LED.

El ahorro de energía, el consumo de energía actual y la energía acumulada ahorrada pueden monitorearse. La cantidad total de energía ahorrada se puede ver como un porcentaje de energía que las interfaces físicas habrían consumido si no se hubiesen ejecutado en el modo Green Ethernet.

La energía ahorrada que se muestra solo está relacionada a Green Ethernet. No se muestra la cantidad de energía que ahorra EEE.

Ahorro de energía al desactivar indicadores LED de puerto

La función Desactivar indicadores LED de puerto permite al usuario ahorrar la energía que consumen los indicadores LED del dispositivo. Dado los dispositivos normalmente se encuentran en una sala desocupada, tener estos LED encendidos es un desperdicio de energía. La función Green Ethernet le permite deshabilitar los LED del puerto (para enlaces, velocidad y PoE) cuando no se necesitan, y habilitarlos cuando los necesita (depuración, conexión de dispositivos adicionales, etcétera).

En la página Resumen del sistema, los indicadores LED que se muestran en las imágenes del tablero de dispositivos no se verán afectados por la desactivación de los indicadores LED.

Los indicadores LED del puerto pueden desactivarse desde la página Green Ethernet > Propiedades.

Función 802.3az Ethernet para uso eficiente de energía

En esta sección se describe la función 802.3az Ethernet para uso eficiente de energía (EEE).

Abarca los siguientes temas:

- **Información general de 802.3az EEE**
- **Anuncio de capacidades en la negociación**
- **Detección del nivel de enlace para 802.3az EEE**
- **Disponibilidad de 802.3az EEE**
- **Configuración predeterminada**
- **Interacciones entre funciones**
- **Flujo de trabajo de la configuración de 802.3az EEE**

Información general de 802.3az EEE

La función 802.3az EEE ha sido diseñada para ahorrar energía cuando no hay tráfico en el enlace. En Green Ethernet, la energía se reduce cuando el puerto está desactivado. Con 802.3az EEE, la energía se reduce cuando el puerto está activado, pero no hay tráfico en él.

802.3az EEE es compatible solo en dispositivos con puertos GE.

Al usar 802.3az EEE, los sistemas de los dos lados del enlace pueden deshabilitar porciones de su funcionalidad y ahorrar energía durante los períodos en los que no hay tráfico.

802.3az EEE admite el funcionamiento de MAC IEEE 802.3 a 100 Mbps y 1000 Mbps:

LLDP se usa para seleccionar el conjunto de parámetros óptimo para los dos dispositivos. Si el socio de enlace no admite el LLDP, o si está deshabilitado, 802.3az EEE aun será operativo, pero podría no serlo en el modo operativo óptimo.

La función 802.3az EEE se implementa utilizando un modo de puerto denominado modo de reposo de baja potencia (LPI, Low Power Idle). Cuando no hay tráfico y esta función está habilitada en el puerto, el puerto se coloca en modo LPI, el que reduce el consumo de energía significativamente.

Los dos lados de una conexión (el puerto del dispositivo y el dispositivo de conexión) deben admitir 802.3az EEE para que funcione. Cuando no hay tráfico, los dos lados envían señales que indican que la energía se va a reducir. Cuando se reciben señales de los dos lados, la señal Mantener conexión indica que los puertos están en estado LPI (y no en estado Desactivado), y la energía se reduce.

Para que los puertos estén en modo LPI, la señal Mantener conexión debe recibirse continuamente de los dos lados.

Anuncio de capacidades en la negociación

La compatibilidad de 802.3az EEE se anuncia durante la etapa de negociación automática. La negociación automática proporciona al dispositivo de enlace la capacidad de detectar las habilidades (los modos de funcionamiento) que admite el dispositivo en el otro extremo del enlace, determinar las habilidades comunes y configurarse para el funcionamiento conjunto. La negociación automática se realiza en el momento en el que se realiza el enlace, a pedido de la administración o al detectarse un error de enlace. Durante el proceso en el que se establece el enlace, los dos socios de enlace intercambian sus capacidades de 802.3az. Cuando la negociación automática está habilitada en el dispositivo, funciona automáticamente sin interacción del usuario.

> **NOTA** Si la negociación automática no está habilitada en un puerto, la EEE está deshabilitada. La única excepción se da si la velocidad del enlace es de 1 GB; entonces, EEE seguirá habilitada, aunque la negociación automática esté deshabilitada.

Detección del nivel de enlace para 802.3az EEE

Además de las capacidades arriba descritas, las capacidades y la configuración de 802.3az EEE también se anuncian mediante las tramas, según los TLV específicos organizativamente definidos en el Anexo G de la norma IEEE, protocolo 802.1AB (LLDP). LLDP se usa para optimizar aún más el funcionamiento de 802.3az EEE una vez completada la negociación automática. El TLV 802.3az se usa para ajustar las duraciones de reactivación y actualización del sistema.

Disponibilidad de 802.3az EEE

Consulte las notas de versión para obtener un listado completo de los productos que admiten EEE.

Configuración predeterminada

De forma predeterminada, 802.3az EEE y EEE LLDP están habilitadas globalmente y por puerto.

Interacciones entre funciones

A continuación se describen las interacciones de 802.3az EEE con otras funciones:

- Si la negociación automática no está habilitada en un puerto, el estado operativo de 802.3az EEE está deshabilitado. La única excepción a esta regla se da si la velocidad del enlace es de 1 GB; entonces, EEE seguirá habilitada, aunque la negociación automática esté deshabilitada.
- Si 802.3az EEE está habilitada y el puerto se está activando, entonces comienza a trabajar de inmediato de acuerdo con el valor de tiempo de reactivación máximo del puerto.
- En la GUI, el campo EEE para el puerto no está disponible cuando la opción Modo de alcance corto del puerto está marcada.
- Si la velocidad del puerto GE se cambia a 10 Mbit, 802.3az EEE se deshabilita. Esto solo se admite en los modelos GE.

Flujo de trabajo de la configuración de 802.3az EEE

En esta sección se describe cómo configurar la función 802.3az EEE y ver sus contadores.

PASO 1 Asegúrese de que la negociación automática esté habilitada en el puerto, abriendo la página **Administración de puertos > Configuración de puertos**.

a. Seleccione un puerto y abra la página Editar configuración de puerto.

b. Seleccione el campo **Negociación automática** para asegurarse de que esté habilitado.

PASO 2 Asegúrese de que la función **802.3 Ethernet para uso eficiente de energía (EEE)** esté activada globalmente en Administración de puertos > Green Ethernet > página Propiedades (está activada de forma predeterminada). Esta página también muestra cuánta energía se ha ahorrado.

PASO 3 Asegúrese de que 802.3az EEE esté activada en un puerto al abrir Green Ethernet > página Configuración de puertos.

a. Seleccione un puerto y abra la página Editar configuración de puerto.

b. Marque el modo **802.3 Ethernet para uso eficiente de energía (EEE)** en el puerto (está habilitado de forma predeterminada).

c. Seleccione si desea habilitar o deshabilitar el anuncio de las capacidades de 802.3az EEE mediante LLDP en **802.3 LLDP de Ethernet para uso eficiente de energía (EEE)** (está habilitado de forma predeterminada).

PASO 4 Para ver la información relacionada con 802.3 EEE en el dispositivo local, abra la página Administración > Detección de LLDP > Información local de LLDP y vea la información en el bloque 802.3 Ethernet para uso eficiente de energía (EEE).

PASO 5 Para mostrar la información de 802.3az EEE en el dispositivo remoto, abra Administración > Detección de LLDP > página Información de vecinos LLDP y vea la información en el bloque 802.3 Ethernet para uso eficiente de energía (EEE).

Propiedades globales de Green Ethernet

La página Propiedades contiene y permite activar la configuración del modo Green Ethernet para el dispositivo. También muestra el ahorro de energía actual.

Para habilitar Green Ethernet y EEE y ver los ahorros de energía:

PASO 1 Haga clic en **Administración de puertos** > **Green Ethernet** > **Propiedades**.

PASO 2 Ingrese los valores para los siguientes campos:

- **Modo de detección de energía**: deshabilitado por opción predeterminada. Seleccione la casilla de verificación para habilitarlo.
- **Alcance corto**: active o desactive globalmente el modo de alcance corto si hay puertos GE en el dispositivo.

  NOTA Si el modo de alcance corto está habilitado, EEE debe estar deshabilitado.

- **LED de puerto**: seleccione para habilitar los LED del puerto. Cuando están deshabilitados, no muestran el estado del enlace, la actividad, etcétera.
- **Ahorro de energía**: muestra el porcentaje de ahorro de energía al ejecutar el modo Green Ethernet y Alcance corto. Los ahorros energéticos que se muestran son relevantes únicamente para la energía que se ahorra en los modos Alcance corto y Detección de energía. La función de ahorro de energía de EEE es dinámica por naturaleza, ya que está basada en la utilización de puertos y, por lo tanto, no se toma en cuenta. El cálculo de ahorro de energía se realiza comparando el consumo máximo de energía sin ahorro con el consumo actual.

- **Energía ahorrada acumulativa**: muestra la cantidad de energía ahorrada desde la última vez que el dispositivo se ha reiniciado. Este valor se actualiza cada vez que hay un evento que afecta el ahorro de energía.
- **802.3 Ethernet para uso eficiente de energía (EEE)**: active o desactive globalmente el modo de EEE

PASO 3 Haga clic en **Restablecer contador de ahorro de energía** para restablecer la información sobre la energía ahorrada acumulativa.

PASO 4 Haga clic en **Aplicar**. Las propiedades de Green Ethernet se escriben en el archivo Configuración en ejecución.

Propiedades de Green Ethernet para puertos

La página Configuración de puertos contiene los modos Green Ethernet y EEE actuales por puerto y permite configurar Green Ethernet en un puerto mediante la página Editar configuración de puerto. Para que los modos Green Ethernet operen en un puerto, es necesario que los modos correspondientes se activen globalmente en la página Propiedades.

La configuración de EEE solo se muestra para los dispositivos que tienen puertos GE. EEE funciona solo cuando los puertos están configurados en Negociación automática. La excepción es que EEE sigue siendo funcional aun cuando la negociación automática está deshabilitada, pero el puerto está a 1 GB o más.

Para definir los valores de Green Ethernet por puerto:

PASO 1 Haga clic en **Administración de puertos** > **Green Ethernet** > **Configuración de puertos**.

En la página Configuración de puertos, se muestra lo siguiente:

- **Estado de los parámetros globales**: describe las funciones habilitadas.

Para cada puerto, se describen los siguientes campos:

- **Puerto**: el número de puerto.
- **Detección de energía**: el estado del puerto con respecto al modo Detección de energía:
  - *Administrativo*: muestra si se ha habilitado el modo Detección de energía.
  - *Operativo*: muestra si está funcionando el modo Detección de energía.
  - *Motivo*: si el modo Detección de energía no se encuentra operativo, muestra el motivo.

- **Alcance corto**: el estado del puerto con respecto al modo Alcance corto:
  - *Administrativo*: muestra si se ha habilitado el modo Alcance corto.
  - *Operativo*: muestra si está funcionando el modo Alcance corto.
  - *Motivo*: si el modo Alcance corto no se encuentra operativo, muestra el motivo.
  - *Longitud del cable*: muestra la longitud del cable de retorno del VCT en metros.

  NOTA El modo de alcance corto solo se admite en puertos RJ45 GE; no se aplica a puertos combinados.
- **802.3 Ethernet para uso eficiente de energía (EEE)**: el estado del puerto con respecto a la función EEE:
  - *Administrativo*: muestra si EEE estaba habilitado.
  - *Operativo*: muestra si EEE está funcionando actualmente en el puerto local. Esta función indica si ha sido habilitado (estado Administrativo), si ha sido habilitado en el puerto local y si está funcionando en el puerto local.
  - *LLDP administrativo*: muestra si se habilitó el anuncio de contadores EEE mediante LLDP.
  - *LLDP operativo*: muestra si el anuncio de contadores EEE mediante LLDP actualmente está funcionando.
  - *Soporte de EEE en remoto*: muestra si EEE es compatible en el socio de enlace. EEE debe ser compatible en los socios de enlace local y remoto.

  NOTA En la ventana, se muestran las configuraciones de Alcance corto, Detección de energía y EEE para cada puerto; no obstante, estas funciones no están activadas en ningún puerto, salvo que también se activen globalmente mediante la página Propiedades. Para habilitar el Alcance corto y la EEE de forma global, consulte la sección **Propiedades globales de Green Ethernet**.

PASO 2 Seleccione un **Puerto** y haga clic en **Editar**.

PASO 3 Seleccione para habilitar o deshabilitar el modo **Detección de energía** en el puerto.

PASO 4 Seleccione si se debe habilitar o deshabilitar el modo de **alcance corto** en el puerto, si hay puertos GE en el dispositivo.

PASO 5 Seleccione si se debe habilitar o deshabilitar el modo **802.3 Ethernet para uso eficiente de energía (EEE)** en el puerto, si hay puertos GE en el dispositivo.

PASO 6 Seleccione si se debe habilitar o deshabilitar el modo **802.3 LLDP de Ethernet para uso eficiente de energía (EEE)** en el puerto (anuncio de las capacidades de EEE mediante LLDP), si hay puertos GE en el dispositivo.

PASO 7 Haga clic en **Aplicar**. La configuración del puerto Green Ethernet se escribe en el archivo Configuración en ejecución.

11

Administración de puertos: Detección de enlace unidireccional

En esta sección, se describe la característica de detección de enlace unidireccional (UDLD).

Abarca los siguientes temas:

- **Información general de UDLD**
- **Funcionamiento de UDLD**
- **Pautas de uso**
- **Dependencias de otras funciones**
- **Configuración y valores predeterminados**
- **Antes de comenzar**
- **Tareas de UDLD comunes**
- **Configuración de UDLD**

Información general de UDLD

UDLD es un protocolo de Capa 2 que permite a los dispositivos conectados mediante cables Ethernet de par trenzado o fibra óptica detectar enlaces unidireccionales. Un enlace unidireccional se produce cuando el dispositivo local recibe tráfico de un dispositivo vecino, pero el vecino no recibe el tráfico del dispositivo local.

La finalidad de UDLD es detectar los puertos donde el vecino no recibe tráfico del dispositivo local (enlace unidireccional) y cerrar esos puertos.

Todos los dispositivos conectados deben admitir UDLD para que el protocolo pueda detectar con éxito los enlaces unidireccionales. Si solo el dispositivo local es compatible con UDLD, el dispositivo no podrá detectar el estado del enlace. En ese caso, el estado del enlace queda sin determinar. El usuario puede configurar si los puertos en estado indeterminado se cierran o simplemente disparan notificaciones.

Funcionamiento de UDLD

Estados y modos de UDLD

De acuerdo con el protocolo UDLD, los puertos llevan asignados los siguientes estados:

- **Detección**: el sistema intenta determinar si el enlace es bidireccional o unidireccional. Es un estado temporal.
- **Bidireccional**: se confirma que el vecino recibe el tráfico que envía el dispositivo local, y que el dispositivo local recibe el tráfico del vecino.
- **Cerrado**: el enlace es unidireccional. El vecino recibe el tráfico que envía el dispositivo local, pero el dispositivo local no recibe el tráfico del vecino.
- **Indeterminado**: el sistema no puede determinar el estado del puerto, ya que se produce uno de los siguientes escenarios:
  - El vecino no admite UDLD.

    o
  - El vecino no recibe tráfico del dispositivo local.

  La acción de UDLD en este caso depende del modo de UDLD del dispositivo, como se explica a continuación.

UDLD admite los siguientes modos de funcionamiento:

- **Normal**

  Si se determinó que el estado del enlace del puerto es bidireccional y el tiempo de la información de UDLD caduca mientras el enlace del puerto sigue activo, UDLD intenta reestablecer el estado del puerto.
- **Agresivo**

  Si se determinó que el estado del enlace del puerto es bidireccional y el tiempo de la información de UDLD caduca, UDLD cierra el puerto luego de un período amplio, en el que determinará que el enlace tiene fallas. El estado del puerto para UDLD será marcado como indeterminado.

UDLD está activado en un puerto ante uno de los siguientes escenarios:

- El puerto es de fibra y UDLD se activa globalmente.
- El puerto es de cobre y se le activa UDLD de manera específica.

Cómo funciona UDLD

Cuando en un puerto se activa UDLD, se realizan las siguientes acciones:

- UDLD inicia el estado de detección en el puerto.

  En este estado, UDLD envía periódicamente mensajes en todas las interfaces activas a todos los vecinos. Estos mensajes contienen el ID de dispositivo de todos los vecinos conocidos. Envía estos mensajes de acuerdo con un tiempo de mensajes definido por el usuario.

- UDLD recibe mensajes UDLD de dispositivos vecinos. Almacena en caché estos mensajes hasta cumplirse el tiempo de vencimiento (tres veces el tiempo del mensaje). Si se recibe un nuevo mensaje antes del tiempo de vencimiento, la información de ese mensaje reemplaza a la anterior.

- Cuando se cumple el tiempo de vencimiento, el dispositivo realiza lo siguiente con la información recibida:

  - **Si el mensaje del vecino contiene el ID del dispositivo local**: el estado de enlace del puerto se configura en bidireccional.

  - **Si el mensaje del vecino no contiene el ID del dispositivo local**: el estado de enlace del puerto se configura en unidireccional, y se cierra el puerto.

- Si no se reciben mensajes UDLD de un dispositivo vecino durante el intervalo de vencimiento, el estado de enlace del puerto queda indeterminado y se produce lo siguiente:

  - **El dispositivo está en modo UDLD normal:** se envía una notificación.

  - **El dispositivo está en modo UDLD agresivo.** Se cierra el puerto.

Mientras la interfaz se encuentra en estado bidireccional o indeterminado, el dispositivo envía periódicamente un mensaje cada segundo de tiempo de mensaje. Los pasos antes mencionados se realizan una y otra vez.

Para reactivar manualmente un puerto que se haya cerrado, vaya a la página Administración de puertos > Configuración de recuperación de error. Para obtener más información, consulte **Reactivar un puerto cerrado**.

Si una interfaz está cerrada y se habilita UDLD, el dispositivo elimina toda la información del vecino y envía al menos un mensaje UDLD a los vecinos para informarles que el puerto está cerrado. Cuando el puerto se reactiva, el estado de UDLD cambia a Detección.

UDLD no es compatible o está deshabilitado en un vecino

Si UDLD no es compatible o está deshabilitado en un vecino, no se recibirán mensajes UDLD de ese vecino. En ese caso, el dispositivo no puede determinar si el enlace es unidireccional o bidireccional. El estado de la interfaz pasa a ser indeterminado.

Reactivar un puerto cerrado

Es posible reactivar un puerto que UDLD haya cerrado en una de las siguientes maneras:

- **Automáticamente**: si desea configurar el sistema para que automáticamente reactive los puertos que UDLD haya cerrado, vaya a la página Administración de puertos > Configuración de recuperación de error. En ese caso, cuando UDLD cierra un puerto, se reactiva automáticamente al vencerse el intervalo de recuperación automática. UDLD vuelve a funcionar en el puerto. Si el enlace sigue unidireccional, por ejemplo, UDLD lo cierra nuevamente al cumplirse el tiempo de vencimiento de UDLD.
- **Manualmente**: si desea reactivar un puerto, vaya a la página Administración de puertos > Configuración de recuperación de error.

Pautas de uso

Cisco no recomienda activar UDLD en puertos conectados a dispositivos incompatibles con UDLD o que no lo tengan activado. Si se envían paquetes UDLD en un puerto conectado a un dispositivo incompatible con UDLD, puede causar más tráfico en el puerto sin brindar ningún beneficio.

Además, tenga en cuenta lo siguiente al configurar UDLD:

- Configure el tiempo del mensaje de acuerdo con la urgencia por cerrar los puertos con enlace unidireccional. Mientras más breve sea el tiempo del mensaje, más paquetes UDLD se enviarán y analizarán, pero más rápido se cerrará el puerto si el enlace es unidireccional.
- Si desea activar UDLD en un puerto de cobre, deberá activarlo por puerto. Cuando activa UDLD globalmente, solo se activará en los puertos de fibra.
- Establezca el modo UDLD en normal cuando no desee cerrar puertos, a menos que tenga la certeza de que el enlace es unidireccional.
- Establezca el modo UDLD en agresivo cuando desee una pérdida de los enlaces unidireccional y bidireccional.

Dependencias de otras funciones

- UDLD y Capa 1.

  Cuando se activa UDLD en un puerto, UDLD funcionará activamente en ese puerto mientras el puerto esté conectado. Cuando el puerto está apagado, UDLD pasa al estado apagado de UDLD. En ese estado, UDLD elimina todos los vecinos detectados. Cuando el puerto pasa de estar apagado a estar encendido, UDLD reanuda su funcionamiento.

- UDLD y protocolos de Capa 2

  UDLD funciona en un puerto independientemente de los protocolos de Capa 2 activados en ese mismo puerto, como STP o LACP. Por ejemplo, UDLD asigna al puerto un estado independientemente del estado de STP del puerto o independientemente de si el puerto pertenece o no a un LAG.

Configuración y valores predeterminados

En esta función, se observan los siguientes valores predeterminados:

- UDLD está desactivado de forma predeterminada en todos los puertos del dispositivo.
- El tiempo de mensaje predeterminado es de 15 segundos.
- El tiempo de vencimiento predeterminado es de 45 segundos (3 veces el tiempo del mensaje).
- Estado de UDLD del puerto predeterminado:
  - Las interfaces de fibra están en estado UDLD global.
  - Las interfaces que no son de fibra están en estado desactivado.

Antes de comenzar

No se requieren tareas preliminares.

Tareas de UDLD comunes

En esta sección, se describen algunas de las tareas comunes para configurar UDLD.

Flujo de trabajo 1: *para activar UDLD globalmente en los puertos de fibra, siga los siguientes pasos:*

PASO 1 Abra la página **Administración de puertos** > **Configuración global de UDLD**.

a. Ingrese el **Tiempo de mensaje**.

b. En el campo Estado predeterminado de UDLD del puerto de fibra, ingrese **Deshabilitado**, **Normal** o **Agresivo** como estado de UDLD global.

PASO 2 Haga clic en **Aplicar**

Flujo de trabajo 2: *para cambiar la configuración de UDLD en un puerto de fibra o para activar UDLD en un puerto de cobre, siga los siguientes pasos:*

PASO 1 Abra la página **Administración de puertos > Configuración global de UDLD**.

a. Seleccione un puerto.

b. Seleccione **Predeterminado**, **Deshabilitado**, **Normal** o **Agresivo** como estado UDLD del puerto. Si selecciona Predeterminado, el puerto recibe la configuración global.

PASO 2 Haga clic en **Aplicar**.

Flujo de trabajo 3: *para reactivar un puerto que fue apagado por UDLD y que no tiene configurada la reactivación automática:*

PASO 1 Abra la página **Administración de puertos** > **Configuración de recuperación de error**.

a. Seleccione un puerto.

b. Haga clic en **Reactivar**.

Configuración de UDLD

La función de UDLD puede configurarse simultáneamente para todos los puertos de fibra (en la página Configuración global de UDLD) o por puerto (en la página Configuración de interfaz de UDLD).

Configuración global de UDLD

El estado predeterminado de UDLD del puerto de fibra solo puede aplicarse a los puertos de fibra.

El campo Tiempo del mensaje se aplica a los puertos de cobre y de fibra.

Para configurar UDLD globalmente:

PASO 1 Haga clic en **Administración de puertos** > **UDLD** > **Configuración global de UDLD**.

PASO 2 Ingrese los siguientes campos:

- **Tiempo del mensaje**: introduzca el intervalo para el envío de mensajes UDLD. Este campo es relevante para los puertos de fibra y de cobre.
- **Estado predeterminado de UDLD del puerto de fibra**: este campo es relevante solo para los puertos de **fibra**. El estado de UDLD para los puertos de cobre debe configurarse individualmente en la página Configuración de interfaz de UDLD. Los estados posibles son:
  - *Deshabilitado*: UDLD está desactivado en todos los puertos del dispositivo.
  - *Normal*: el dispositivo cierra una interfaz si el enlace es unidireccional. Si el enlace es indeterminado, se envía una notificación.
  - *Agresivo*: el dispositivo cierra una interfaz si el enlace es unidireccional. Si el enlace es bidireccional, el dispositivo se cierra al caducarse el tiempo de la información de UDLD. El estado del puerto será marcado como indeterminado.

PASO 3 Haga clic en **Aplicar** para guardar los ajustes en el archivo Configuración en ejecución.

Configuración de interfaz de UDLD

Use la página Configuración de interfaz de UDLD para cambiar el estado de UDLD de un puerto específico. Aquí puede configurarse el estado para los puertos de cobre y de fibra.

Si desea copiar un conjunto de valores específico en más de un puerto, configure el valor para un puerto y use el botón **Copiar** para copiarlo a los demás puertos.

Para configurar UDLD en una interfaz:

PASO 1 Haga clic en **Administración de puertos** > **UDLD** > **Configuración de interfaz de UDLD**.

Se visualiza la información para todos los puertos que tengan UDLD activado; o bien, si filtró solo un grupo determinado de puertos, se visualiza la información para ese grupo de puertos.

- **Puerto**: el identificador del puerto.
- **Estado UDLD**: los estados posibles son:
  - *Deshabilitado*: UDLD está desactivado en todos los puertos de fibra del dispositivo.
  - *Normal*: el dispositivo cierra una interfaz si detecta que el enlace es unidireccional. Envía una notificación si el enlace es indeterminado.
  - *Agresivo*: el dispositivo cierra una interfaz si el enlace es unidireccional. Si el enlace es bidireccional, el dispositivo se cierra al caducarse el tiempo de la información de UDLD. El estado del puerto será marcado como indeterminado.
- **Estado bidireccional**: seleccione el valor de este campo para el puerto seleccionado. Los estados posibles son:
  - *Detección*: el último estado de UDLD del puerto está por determinarse. El tiempo de vencimiento aún no se cumplió desde la última determinación (si hubo alguna), o desde que UDLD comenzó a funcionar en ese puerto; por eso el estado está por determinarse.
  - *Bidireccional*: el vecino recibe el tráfico que envía el dispositivo local, y el dispositivo local recibe el tráfico del vecino.
  - *Indeterminado*: el estado del enlace entre el puerto y su puerto conectado no puede determinarse porque no se recibió ningún mensaje de UDLD o porque el mensaje de UDLD no incluía el ID del dispositivo local.
  - *Deshabilitado*: se desactivó UDLD en este puerto.
  - *Cerrado*: el puerto se cerró porque su enlace con el dispositivo conectado es indeterminado en modo agresivo.
- **Cantidad de vecinos**: cantidad de dispositivos conectados detectados.

PASO 2 Si desea modificar el estado de UDLD de un puerto específico, selecciónelo y haga clic en **Editar**.

PASO 3 Modifique el valor del estado de UDLD. Si selecciona **Predeterminado**, el puerto recibe el valor del **Estado predeterminado de UDLD del puerto de fibra** en la página Configuración global de UDLD.

PASO 4 Haga clic en **Aplicar** para guardar los ajustes en el archivo Configuración en ejecución.

Vecinos de UDLD

Para ver todos los dispositivos conectados al dispositivo local:

PASO 1 Haga clic en **Administración de puertos** > **UDLD** > **Vecinos de UDLD**.

Aparecen los siguientes campos para todos los puertos habilitados para UDLD:

- **Nombre de interfaz**: nombre del puerto local habilitado para UDLD.
- **Información de vecinos:**
  - *ID de dispositivo*: ID del dispositivo remoto.
  - *MAC del dispositivo*: la dirección MAC del dispositivo remoto.
  - *Nombre del dispositivo*: el nombre del dispositivo remoto.
  - *ID de puerto*: nombre del puerto remoto.
- **Estado**: estado del enlace entre el dispositivo local y el vecino en el puerto local. Los siguientes valores son posibles:
  - *Detección*: el último estado de UDLD del puerto está por determinarse. El tiempo de vencimiento aún no se cumplió desde la última determinación (si hubo alguna), o desde que UDLD comenzó a funcionar en ese puerto; por eso el estado está por determinarse.
  - *Bidireccional*: el vecino recibe el tráfico que envía el dispositivo local, y el dispositivo local recibe el tráfico del vecino.
  - *Indeterminado*: el estado del enlace entre el puerto y su puerto conectado no puede determinarse porque no se recibió ningún mensaje de UDLD o porque el mensaje de UDLD no incluía el ID del dispositivo local.
  - *Deshabilitado*: se desactivó UDLD en este puerto.
  - *Cerrado*: el puerto se cerró porque su enlace con el dispositivo conectado es indeterminado en modo agresivo.
- **Tiempo del vencimiento del vecino (seg.)**: muestra el tiempo que debe transcurrir antes de que el dispositivo intente determinar el estado de UDLD del puerto. Es tres veces el tiempo del mensaje.
- **Tiempo del mensaje del vecino (seg.)**: muestra el tiempo entre los mensajes de UDLD.

12

Smartport

En este documento se describe la función Smartport.

Contiene los siguientes temas:

Información general

La función Smartport ofrece una forma conveniente de guardar y compartir configuraciones comunes. Al aplicar el mismo macro de Smartport a varias interfaces, las interfaces comparten un conjunto común de configuraciones. Un macro de Smartport es una secuencia de comandos CLI (Command Line Interface, interfaz de línea de comandos).

Se puede aplicar un macro de Smartport a una interfaz según el nombre de macro o el tipo de Smartport asociado al macro. La aplicación de un macro de Smartport por nombre de macro se puede hacer únicamente mediante la CLI. Consulte la guía de CLI para obtener más detalles.

Hay dos formas de aplicar un macro de Smartport según el tipo de Smartport a una interfaz:

- **Smartport estático**: usted puede asignar manualmente un tipo de Smartport a una interfaz. Como resultado se aplica a la interfaz el macro de Smartport correspondiente.
- **Smartport automático**: Smartport automático espera que el dispositivo se conecte a la interfaz antes de aplicar una configuración. Si se detecta un dispositivo desde una interfaz, se aplica automáticamente el macro de Smartport (si está asignado) que corresponde al tipo de Smartport del dispositivo que se conecta.

La función Smartport consta de varios componentes y trabaja junto con otras funciones del dispositivo. Estos componentes y funciones se describen en las siguientes secciones:

- Smartport, los tipos de Smartport y los macro de Smartport se describen en esta sección.
- La VLAN de voz y Smartport se describen en la sección **VLAN de voz**.
- LLDP/CDP para Smartport se describe en las secciones **Configuración de LLDP** y **Configuración de CDP**, respectivamente.

Además, los flujos de trabajo típicos se describen en la sección **Tareas comunes de Smartport**.

¿Qué es un Smartport?

Un Smartport es una interfaz a la cual se le aplica un macro incorporado (o definido por el usuario). Estos macros están diseñados para ofrecer un medio de configuración rápida del dispositivo que sea compatible con los requisitos de comunicación y utilice las funciones de diversos tipos de dispositivos de red. Los requisitos de QoS y acceso de red varían si la interfaz está conectada a un teléfono IP, una impresora o un router o punto de acceso (AP).

Tipos de Smartport

Los tipos de Smartport hacen referencia a los tipos de dispositivos conectados o que se conectarán a los Smartports. El dispositivo admite los siguientes tipos de Smartport:

- Printer (Impresora)
- Equipo de escritorio
- Invitado
- Servidor
- Host
- Cámara IP
- Teléfono IP
- Teléfono IP+Escritorio
- Switch
- Router
- Punto de acceso inalámbrico

Los tipos de Smartport se nombran de manera tal que describan el tipo de dispositivo conectado a una interfaz. Cada tipo de Smartport está asociado a dos macros de Smartport. Un macro denominado "el macro" sirve para aplicar la configuración deseada. El otro, denominado "el antimacro" permite deshacer toda la configuración que realizó "el macro" cuando esa interfaz termina por convertirse en un tipo de Smartport diferente.

Usted puede aplicar un macro de Smartport mediante los siguientes métodos:

- El tipo de Smartport asociado.
- Estáticamente a partir de un macro de Smartport según el nombre desde la CLI.

Se puede aplicar un macro de Smartport según su tipo de Smartport estáticamente desde la CLI y la GUI y dinámicamente según el Smartport automático. El Smartport automático deriva los tipos de Smartport de todos los dispositivos conectados en función de las capacidades de CDP, las capacidades del sistema LLDP y las capacidades de LLDP-MED.

A continuación se describe la relación de los tipos de Smartport y Smartport automático.

Tipo de Smartport	Compatible con Smartport automático	Compatible con Smartport automático de forma predeterminada
Desconocido	No	No
Predeterminado	No	No
Printer (Impresora)	No	No
Equipo de escritorio	No	No
Invitado	No	No
Servidor	No	No
Host	Sí	No
Cámara IP	No	No
Teléfono IP	Sí	Sí
Escritorio del teléfono IP	Sí	Sí
Switch	Sí	Sí
Router	Sí	No
Punto de acceso inalámbrico	Sí	Sí

Tipos de Smartport especiales

Hay dos tipos de Smartport especiales: *predeterminado* y *desconocido*. Estos dos tipos no están asociados con macros, pero existen para expresar el estado de la interfaz en lo que a Smartport respecta.

A continuación se describen estos tipos de Smartport especiales:

- **Predeterminado**

  Una interfaz que aún no tiene un tipo de Smartport asignado a ella tiene el estado Smartport predeterminado.

  Si Smartport automático asigna un tipo de Smartport a una interfaz y la interfaz no está configurada como Smartport automático persistente, entonces, su tipo de Smartport se reinicia como predeterminado en los siguientes casos:

  - Se realiza una operación de enlace activo/inactivo en la interfaz.

- Se reinicia el dispositivo.
- Todos los dispositivos conectados a la interfaz caducaron, lo cual se define como la ausencia de anuncio de CDP o LLDP por parte del dispositivo durante un período de tiempo determinado.

- **Desconocido**

  Si se aplica un macro de Smartport a una interfaz y se produce un error, a la interfaz se le asigna el estado Desconocida. En este caso, las funciones Smartport y Smartport automático no funcionan en la interfaz hasta tanto se corrija el error y aplique la acción Reiniciar (que se ejecuta en las páginas Configuración de la interfaz) que restablece el estado de Smartport.

  Consulte el área del flujo de trabajo en la sección **Tareas comunes de Smartport** para obtener sugerencias para la resolución de problemas.

  NOTA A lo largo de esta sección, se utiliza el término "caducado" para describir los mensajes de LLDP y CDP a través de sus TTL. Si Smartport automático está habilitado, el estado persistente está deshabilitado y no se reciben más mensajes de CDP o LLDP en la interfaz antes de que ambos TTL de los paquetes CDP y LLDP más recientes disminuyan a 0, se ejecutará el antimacro y el tipo de Smartport regresará al predeterminado.

Macros de Smartport

Un macro de Smartport es una secuencia de comandos CLI que configuran correctamente una interfaz para un dispositivo de red en particular.

Los macros de Smartport no deben confundirse con los macros globales. Los macros globales configuran el dispositivo globalmente; sin embargo, el alcance de un macro de Smartport se limita a la interfaz en que se aplica.

La fuente del macro puede encontrarse al ejecutar el comando mostrar nombre de macro de analizador [macro_name] en modo exec privilegiado de la CLI o al hacer clic en el botón **Ver fuente de macro** en la página Configuración de tipo de Smartport.

Un macro y su antimacro correspondiente se agruparán de manera asociada con cada tipo de Smartport. El macro aplica la configuración y el antimacro la elimina.

Existen dos tipos de macros de Smartport:

- **Incorporado**: estos son los macros que proporciona el sistema. Un macro aplica el perfil de configuración y el otro lo elimina. Los nombres de macro de los macros de Smartport incorporados y el tipo de Smartport se asocian de la siguiente manera:
  - macro-name (por ejemplo: printer)
  - no_macro-name (por ejemplo: no_printer)

- **Definido por el usuario**: estos son los macros que escriben los usuarios. Consulte la *Guía de referencia de CLI* para obtener más información al respecto. Para asociar un macro definido por el usuario a un tipo de Smartport, también se debe definir su antimacro.
  - smartport-type-name (por ejemplo: my_printer)
  - no_smartport-type-name (por ejemplo: no_my_printer)

Los macros de Smartport están vinculados a los tipos de Smartport en la página Editar configuración de tipo de Smartport.

Consulte la sección **Macros de Smartport incorporados** para obtener una lista de los macros de Smartport incorporados para cada tipo de dispositivo.

Aplicación de un tipo de Smartport a una interfaz

Cuando se aplican tipos de Smartport a interfaces, los tipos de Smartport y la configuración en los macros de Smartport asociados se guardan en el archivo Configuración en ejecución. Si el administrador guarda el archivo de configuración en ejecución en el archivo de configuración de inicio, el dispositivo aplica los tipos de Smartport y los macros de Smartport a las interfaces luego del reinicio de la siguiente manera:

- Si el archivo de configuración de inicio no especifica el tipo de Smartport de una interfaz, su tipo de Smartport se establece como Predeterminado.
- Si el archivo de configuración de inicio especifica un tipo de Smartport estático, el tipo de Smartport de la interfaz se establece en este tipo estático.
- Si el archivo de configuración de inicio especifica un tipo de Smartport que el Smartport automático asignó dinámicamente:
  - Si están habilitados (**Habilitar**) los estados Smartport automático operativo, Smartport automático y Estado Persistente, el tipo de Smartport se establece en este tipo dinámico.
  - De lo contrario, se aplica el antimacro correspondiente y el estado de las interfaces se establece en Predeterminada.

Falla de macro y operación de reinicio

Es posible que un macro de Smartport falle si hay un conflicto entre la configuración existente de la interfaz y un macro de Smartport.

Si un macro de Smartport falla, se envía un mensaje de SYSLOG que contiene los siguientes parámetros:

- Número de puerto

- Tipo de Smartport
- El número de línea del comando CLI que falló en el macro.

Cuando un macro de Smartport falla en una interfaz, el estado de la interfaz se establece como *Desconocida*. El motivo de la falla se puede ver en la página Configuración de la interfaz, en la ventana emergente **Mostrar diagnósticos**.

Una vez que se determina el problema y se corrige la configuración existente o el macro de Smartport, debe realizar una operación de reinicio para restablecer la interfaz para que pueda volver a aplicar un tipo de Smartport (en las páginas Configuración de la interfaz). Consulte el área del flujo de trabajo en la sección **Tareas comunes de Smartport** para obtener sugerencias para la resolución de problemas.

Cómo funciona la función Smartport

Usted puede aplicar un macro de Smartport a una interfaz según el nombre de macro o según el tipo de Smartport asociado al macro. La aplicación de un macro de Smartport según el nombre de macro se puede realizar únicamente a través de CLI. Para obtener más detalles debe consultar la guía de CLI.

Ya que se suministra soporte para los tipos de Smartport que corresponden a dispositivos que no se permiten ser detectados a través de CDP o LLDP, estos tipos de Smartport deben estar estáticamente asignados a las interfaces deseadas. Esto se puede realizar al navegar la página Configuración de interfaz de Smartport, al seleccionar el botón de opción de la interfaz deseada y al hacer clic en **Editar**. A continuación, seleccione el tipo de Smartport que desea asignar y ajuste los parámetros que sean necesarios antes de hacer clic en **Aplicar**.

Hay dos formas de aplicar un macro de Smartport según el tipo de Smartport a una interfaz:

- **Smartport estático**

  Usted puede asignar manualmente un tipo de Smartport a una interfaz. Se aplica el Smartport correspondiente a la interfaz. Usted puede asignar manualmente un tipo de Smartport a una interfaz en la página Configuración de interfaz de Smartport.

- **Smartport automático**

  Si se detecta un dispositivo desde una interfaz, se aplica automáticamente el macro de Smartport (si existe) que corresponde al tipo de Smartport del dispositivo que se conecta. Smartport automático está habilitado globalmente de forma predeterminada y a nivel de interfaz.

En ambos casos, se ejecuta el antimacro asociado cuando se elimina el tipo de Smartport de la interfaz y el antimacro se ejecuta exactamente de la misma manera, al eliminar toda la interfaz.

Smartport automático

Para que Smartport automático pueda asignar automáticamente tipos de Smartport a las interfaces, la función Smartport automático debe estar habilitada globalmente y en las interfaces relevantes en las que está permitida la configuración de Smartport automático. De forma predeterminada, Smartport automático está habilitado para configurar todas las interfaces. El tipo de Smartport asignado a cada interfaz se determina mediante los paquetes de CDP y LLDP que se reciben en cada interfaz respectivamente.

- Si se conectan varios dispositivos a una interfaz, se aplica a la interfaz un perfil de configuración que sea apropiado para todos los dispositivos, siempre que sea posible.
- Si un dispositivo caduca (ya no recibe anuncios de otros dispositivos), la configuración de interfaz cambia de acuerdo con su Estado persistente. Si el Estado Persistente está habilitado, se conserva la configuración de interfaz. De lo contrario, Tipo de Smartport se revierte a Predeterminado.

Habilitación de Smartport automático

Smartport automático se puede activar globalmente en la página Propiedades de las siguientes maneras:

- **Habilitado**: esta opción habilita manualmente Smartport automático y lo pone en funcionamiento de inmediato.
- **Habilitar mediante VLAN de voz automática**: esta opción habilita Smartport automático para que funcione si VLAN de voz automática está habilitada y en funcionamiento. Habilitar mediante VLAN de voz automática es la opción predeterminada.

> **NOTA** Además de habilitar Smartport automático globalmente, usted también debe habilitar Smartport automático en la interfaz deseada. De forma predeterminada, Smartport automático está habilitado en todas las interfaces.

Consulte la sección **VLAN de voz** para obtener más información acerca de cómo habilitar la VLAN de voz

Identificación de un tipo de Smartport

Si Smartport automático está globalmente activado (en la página Propiedades) y, en la interfaz (en la página Configuración de la interfaz), el dispositivo aplica un macro de Smartport a la interfaz según el tipo de Smartport del dispositivo de conexión. Smartport automático deriva los tipos de Smartport de los dispositivos de conexión según los CDP y LLDP que los dispositivos anuncian.

Por ejemplo, si un teléfono IP está conectado a un puerto, transmite paquetes CDP y LLDP que anuncian sus capacidades. Tras la recepción de estos paquetes CDP o LLDP, el dispositivo deriva el tipo de Smartport apropiado para el teléfono y aplica el macro de Smartport correspondiente a la interfaz donde se conecta el teléfono IP.

A menos que Smartport automático persistente esté habilitado en una interfaz, se eliminará el tipo de Smartport y la configuración resultante que aplica Smartport automático si los dispositivos de conexión caducan, los vínculos están inactivos, se producen reinicios o se reciben capacidades en conflicto. Los tiempos de caducidad se determinan mediante la ausencia de anuncios CDP y LLDP por parte del dispositivo durante un período de tiempo específico.

Uso de información de CDP/LLDP para identificar tipos de Smartport

El dispositivo detecta el tipo de dispositivo conectado al puerto según las capacidades de CDP/LLDP.

Esta asignación se puede ver en las siguientes tablas:

Asignación de capacidades de CDP al tipo de Smartport

Nombre de la capacidad	Bit CDP	Tipo de Smartport
Router	0x01	Router
Bridge TB	0x02	Punto de acceso inalámbrico
Bridge SR	0x04	Ignorar
Switch	0x08	Switch
Host	0x10	Host
Filtrado condicional de IGMP	0x20	Ignorar
Repetidor	0x40	Ignorar
Teléfono VoIP	0x80	ip_phone
Dispositivo administrado en forma remota	0x100	Ignorar
Puerto de teléfono CAST	0x200	Ignorar
Retransmisión MAC de dos puertos	0x400	Ignorar

Asignación de capacidades de LLDP al tipo de Smartport

Nombre de la capacidad	Bit LLDP	Tipo de Smartport
Otro	1	Ignorar
Repetidor IETF RFC 2108	2	Ignorar
MAC Bridge IEEE Std. 802.1D	3	Switch
Punto de acceso a WLAN IEE Std. 802.11 MIB	4	Punto de acceso inalámbrico

Asignación de capacidades de LLDP al tipo de Smartport (Continuación)

Nombre de la capacidad	Bit LLDP	Tipo de Smartport
Router IETF RFC 1812	5	Router
Teléfono IETF RFC 4293	6	ip_phone
Dispositivo de cableado DOCSIS IETF RFC 4639 y IETF RFC 4546	7	Ignorar
Solo estación IETF RFC 4293	8	Host
Componente C-VLAN de un Bridge VLAN IEEE Std. 802.1Q	9	Switch
Componente S-VLAN de un Bridge VLAN IEEE Std. 802.1Q	10	Switch
Retransmisión MAC de dos puertos (TPMR) IEEE Std. 802.1Q	11	Ignorar
Reservado	12-16	Ignorar

NOTA Si solo se configuran los bits hosts y el teléfono IP, el tipo de Smartport es ip_phone_desktop.

Varios dispositivos conectados al puerto

El dispositivo deriva el tipo de Smartport de un dispositivo conectado a través de las capacidades que el dispositivo anuncia en sus paquetes CDP o LLDP.

Si se conectan varios dispositivos al dispositivo a través de una interfaz, Smartport automático considerará cada anuncio de capacidad que reciba a través de esa interfaz para asignar el tipo de Smartport correcto. Esta asignación se basa en el siguiente algoritmo:

- Si todos los dispositivos de una interfaz anuncian la misma capacidad (no hay conflicto), se aplica el tipo de Smartport compatible a la interfaz.
- Si uno de los dispositivos es un switch, se utiliza el tipo de Smartport *Switch*.
- Si uno de los dispositivos es un AP, se utiliza el tipo de Smartport *Punto de acceso inalámbrico*.
- Si uno de los dispositivos es un teléfono IP y el otro dispositivo es un host, se utiliza el tipo de Smartport *ip_phone_desktop*.
- Si uno de los dispositivos es un escritorio de teléfono IP y el otro dispositivo es un teléfono IP, se utiliza el tipo de Smartport *ip_phone_desktop*.
- En todos los otros casos se utiliza el tipo de Smartport predeterminado.

Para obtener más información acerca de LLDP/CDP, consulte las secciones **Configuración de LLDP** y **Configuración de CDP**, respectivamente.

Interfaz de Smartport automático persistente

Si está activado el estado persistente de una interfaz, su tipo de Smartport y la configuración que Smartport automático ya aplicó dinámicamente permanecerán en la interfaz aun después de que caduque el dispositivo de conexión, se desactive la interfaz y se reinicie el dispositivo (suponiendo que se está guardando la configuración). El tipo de Smartport y la configuración de interfaz no cambian a menos que Smartport automático detecte un dispositivo de conexión con un tipo de Smartport diferente. Si el estado persistente de una interfaz está desactivado, la interfaz se revierte al tipo de Smartport predeterminado en el momento en que caduca el dispositivo de conexión, se desactiva la interfaz o se reinicia el dispositivo. Al habilitar el estado persistente en una interfaz se elimina la demora de detección del dispositivo que, de otra manera, se produciría.

NOTA La persistencia de los tipos de Smartport aplicados a las interfaces solo es eficaz entre los reinicios si la configuración en ejecución con el tipo de Smartport aplicado a las interfaces se guarda en el archivo de configuración de inicio.

Gestión de errores

Cuando no logra aplicar un puerto inteligente a una interfaz, usted puede examinar el punto de la falla en la página Configuración de la interfaz, reiniciar el puerto y volver a aplicar el macro una vez corregido el error en las páginas Configuración de la interfaz y Edición de configuración de interfaz.

Configuración predeterminada

Smartport está siempre disponible. De forma predeterminada, Smartport automático se habilita mediante la VLAN de voz automática, depende tanto de CDP como de LLDP para detectar el tipo de Smartport del dispositivo de conexión y detecta el teléfono IP del tipo de Smartport, el teléfono IP + escritorio, el Smith y el punto de acceso inalámbrico.

Consulte la sección **VLAN de voz** para obtener una descripción de los valores predeterminados de fábrica de voz.

Relaciones con otras funciones y compatibilidad hacia atrás

Smartport automático está habilitado de forma predeterminada y se puede deshabilitar. OUI para telefonía no puede funcionar junto con Smartport automático y VLAN de voz automática. Smartport automático debe estar deshabilitado antes de que se habilite OUI para telefonía.

NOTA Al actualizar de una versión de firmware que no es compatible con Smartport automático a un nivel de firmware compatible con Smartport automático, se desactiva VLAN de voz automática después de la actualización. Si OUI para telefonía se habilitó antes de la actualización, entonces Smartport automático se deshabilita después de la actualización y OUI para telefonía permanece habilitado.

Tareas comunes de Smartport

Esta sección describe algunas de las tareas comunes para configurar Smartport y Smartport automático.

Flujo de trabajo 1: para activar globalmente Smartport automático en el dispositivo y configurar un puerto con Smartport automático, siga los siguientes pasos:

PASO 1 Para activar la función Smartport automático en el dispositivo, abra la página Smartport > Propiedades. Establezca **Smartport automático administrativo** en **Habilitar** o **Habilitar mediante VLAN de voz**.

PASO 2 Seleccione si desea que el dispositivo procese anuncios de CDP o LLDP de dispositivos conectados.

PASO 3 Seleccione qué tipo de dispositivos se detectarán en el campo **Detección de dispositivo Smartport automático**.

PASO 4 Haga clic en **Aplicar**

PASO 5 Para activar la función Smartport automático en una o más interfaces, abra la página Smartport > Configuración de la interfaz.

PASO 6 Seleccione la interfaz, y haga clic en **Editar**.

PASO 7 Seleccione Smartport automático en el campo **Aplicación de Smartport**.

PASO 8 Marque o desmarque **Estado persistente** si lo desea.

PASO 9 Haga clic en **Aplicar**.

Flujo de trabajo 2: para configurar una interfaz como Smartport estática, siga los siguientes pasos:

PASO 1 Para activar la función Smartport en la interfaz, abra la página Smartport > Configuración de la interfaz.

PASO 2 Seleccione la interfaz, y haga clic en **Editar**.

PASO 3 Seleccione el tipo de Smartport que se asignará a la interfaz en el campo **Aplicación Smartport**.

PASO 4 Establezca los parámetros del macro según sea necesario.

PASO 5 Haga clic en **Aplicar**.

Flujo de trabajo 3: para ajustar los valores predeterminados del parámetro del macro de Smartport o vincular un par de macros definidos por el usuario a un tipo de Smartport, siga los siguientes pasos:

Mediante este procedimiento, puede lograr lo siguiente:

- Ver la fuente del macro.
- Cambiar valores predeterminados del parámetro.
- Restaurar los valores predeterminados del parámetro a la configuración de fábrica.
- Vincular un par de macros definidos por el usuario (un macro y su antimacro correspondiente) a un tipo de Smartport.

1. Abra la página Smartport > Configuración de tipo de Smartport.
2. Seleccione el tipo de Smartport.
3. Haga clic en **Ver fuente de macro** para ver el macro de Smartport actual que está asociado con el tipo de Smartport seleccionado.
4. Haga clic en **Editar** para abrir una ventana nueva en la que puede vincular macros definidos por el usuario al tipo de Smartport seleccionado o modificar los valores predeterminados de los parámetros en los macros vinculados a ese tipo de Smartport. Estos valores predeterminados del parámetro se utilizarán cuando Smartport automático aplique el tipo de Smartport seleccionado (si corresponde) a una interfaz.
5. En la página Editar, modifique los campos.
6. Haga clic en **Aplicar** para volver a ejecutar el macro si se modificaron los parámetros o en **Restaurar valores predeterminados** para restaurar los valores del parámetro predeterminado a macros incorporados si es necesario.

Flujo de trabajo 4: para volver a ejecutar un macro de Smartport una vez que falló, siga los siguientes pasos:

PASO 1 En la página Configuración de la interfaz, seleccione una interfaz con tipo de Smartport desconocido.

PASO 2 Haga clic en **Mostrar diagnóstico** para ver el problema.

PASO 3 Determine cuál es la solución del problema, luego corríjalo. Considere la sugerencia para resolución de problemas a continuación.

PASO 4 Haga clic en **Editar.** Aparece una nueva ventana en la que puede hacer clic en **Reiniciar** para reiniciar la interfaz.

PASO 5 Vuelva a la página principal y vuelva a aplicar el macro con las opciones **Volver a aplicar** (para dispositivos que no son switches, routers o AP) o **Volver a aplicar macro de Smartport** (para switches, routers o AP) para ejecutar el macro de Smartport en la interfaz.

Un segundo método para reiniciar una sola interfaz desconocida o varias es:

PASO 1 En la página Configuración de la interfaz, seleccione el tipo de puerto que equivale a la marca de verificación.

PASO 2 Seleccione *Desconocida* y haga clic en **Ir.**

PASO 3 Haga clic en **Reiniciar todos los Smartports desconocidos**. Luego vuelva a aplicar el macro tal como se describe arriba.

CONSEJO El motivo de falla del macro puede deberse a un conflicto con la configuración en la interfaz previa a la aplicación del macro (generalmente por configuraciones de seguridad y control de saturación), un tipo de puerto erróneo, un error de tipeo o comando incorrecto dentro del macro definido por el usuario o una configuración de parámetros inválida. No se comprueba el tipo ni el límite de los parámetros antes de intentar aplicar el macro; por lo tanto, el ingreso incorrecto o no válido de un valor de parámetro casi seguramente causará una falla al aplicar el macro.

Configuración de Smartport con interfaz basada en Web

La función Smartport se configura en las páginas Smartport > Propiedades, Configuración de tipo de Smartport y Configuración de la interfaz.

Para obtener información sobre la configuración de la VLAN de voz, consulte la sección **VLAN de voz**.

Para obtener información sobre la configuración de LLDP/CDP, consulte las secciones **Configuración de LLDP** y **Configuración de CDP**, respectivamente.

Propiedades de Smartport

Para configurar la función Smartport globalmente:

PASO 1 Haga clic en **Smartport > Propiedades**.

PASO 2 Ingrese los parámetros.

- **Smartport automático administrativo**: seleccione habilitar o deshabilitar globalmente Smartport automático. Las opciones disponibles son las siguientes:
  - *Deshabilitar*: seleccione esta opción para deshabilitar Smartport automático en el dispositivo.
  - *Habilitar*: seleccione esta opción para habilitar Smartport automático en el dispositivo.
  - *Habilitar mediante VLAN de voz automática*: esta opción habilita Smartport automático, pero solo lo pondrá en funcionamiento si también se habilita y se pone en funcionamiento la VLAN de voz automática. Habilitar mediante VLAN de voz automática es la opción predeterminada.
- **Smartport automático operativo**: muestra el estado del Smartport automático.
- **Método de detección de dispositivo Smartport automático**: seleccione si el CDP o LLDP entrante, o ambos tipos de paquetes se utilizan para detectar el tipo de Smartport de los dispositivos de conexión. Se debe marcar al menos uno para que Smartport automático pueda identificar los dispositivos.
- **Estado CDP operativo**: muestra el estado operativo de CDP. Habilite CDP si Smartport automático debe detectar el tipo de Smartport según un anuncio de CDP.
- **Estado LLDP operativo**: muestra el estado operacional de LLDP. Habilite LLDP si Smartport automático debe detectar el tipo de Smartport según un anuncio de LLDP/LLDP-MED.
- **Detección de dispositivo Smartport automático**: seleccione cada tipo de dispositivo para el cual Smartport automático puede asignar tipos de Smartport a las interfaces. Si no se selecciona, Smartport automático no asignará ese tipo de Smartport a ninguna interfaz.

PASO 3 Haga clic en **Aplicar**. De esta manera, se establecen los parámetros de Smartport en el dispositivo.

Configuración de tipo de Smartport

Use la página Configuración de tipo de Smartport para editar la configuración del tipo de Smartport y ver la fuente de macro.

De forma predeterminada, cada tipo de Smartport está asociado a un par de macros de Smartport incorporados. Consulte **Tipos de Smartport** para obtener más información acerca del macro en comparación con el antimacro. Usted también puede asociar su propio par de macros definidos por el usuario con configuraciones personalizadas a un tipo de Smartport. Los macros definidos por el usuario solo se pueden preparar a través de CLI. Para obtener más detalles debe consultar la guía de referencia de CLI.

Los macros incorporados o definidos por el usuario pueden tener parámetros. Los macros incorporados cuentan con hasta tres parámetros.

La edición de estos parámetros para estos tipos de Smartport que Smartport automático aplica en la página Configuración de tipo de Smartport configura los valores predeterminados para estos parámetros. Smartport automático utiliza estos valores predeterminados.

NOTA Las modificaciones realizadas a los tipos de Smartport harán que se aplique la nueva configuración a las interfaces que ya asignaron ese tipo mediante Smartport automático. En este caso, vincular una configuración o un macro no válido con un valor de parámetro predeterminado no válido provocará que todos los puertos de ese tipo de Smartport se vuelvan desconocidos.

PASO 1 Haga clic en **Smartport > Configuración de tipo de Smartport**.

PASO 2 Para ver el macro de Smartport asociado a un tipo de Smartport, seleccione un tipo de Smartport y haga clic en **Ver fuente de macro**.

PASO 3 Para modificar los parámetros de un macro o asignar un macro definido por un usuario, seleccione un tipo de Smartport y haga clic en **Editar**.

PASO 4 Ingrese los campos.

- **Tipo de puerto**: seleccione el tipo de puerto.
- **Nombre de macro**: muestra el nombre del macro de Smartport actualmente asociado con el tipo de Smartport.
- **Tipo de macro**: seleccione si el par de macro y antimacro asociado a este tipo de Smartport es incorporado o definido por el usuario.
- **Macro definido por el usuario**: si lo desea, seleccione un macro definido por el usuario que se asociará con el tipo de Smartport seleccionado. El macro ya debe estar agrupado con un antimacro.

  La agrupación de dos macros se realiza por nombre y se describe en la sección Macro de Smartport.

- **Parámetros del macro**: muestra los siguientes campos para tres parámetros en el macro:
  - *Nombre de parámetro*: nombre de parámetro en el macro.
  - *Valor de parámetro*: valor actual de parámetro en el macro. Se puede cambiar aquí.
  - *Descripción de parámetro*: descripción de parámetro.

  Usted puede restaurar los valores de parámetro predeterminados al hacer clic en **Restaurar valores predeterminados**.

PASO 5 Haga clic en **Aplicar** para guardar los cambios en la configuración en ejecución. Si se modifican el macro de Smartport o sus valores de parámetro asociados al tipo de Smartport, Smartport automático vuelve a aplicar automáticamente el macro a las interfaces actualmente asignadas con el tipo de Smartport mediante Smartport automático. Smartport automático no aplica los cambios a las interfaces a las que se le asignó estáticamente un tipo de Smartport.

NOTA No existe un método que valide los parámetros de macro ya que no cuentan con una asociación de tipo. Por lo tanto, cualquier entrada es válida en este punto. Sin embargo, los valores de parámetros no válidos pueden generar errores al asignar un tipo de Smartport a una interfaz, al aplicar el macro asociado.

Configuración de interfaz de Smartport

Use la página Configuración de la interfaz para realizar las siguientes tareas:

- Aplicar estáticamente un tipo de Smartport específico a una interfaz con valores específicos de interfaz para los parámetros de macro.
- Habilitar Smartport automático en una interfaz.
- Diagnosticar un macro de Smartport que falló en la aplicación y provocó que el tipo de Smartport se volviera desconocido.
- Volver a aplicar un macro de Smartport luego de que falló para alguno de los siguientes tipos de interfaz: switch, router y AP. Se prevé que las correcciones necesarias se hayan realizado antes de hacer clic en **Volver a aplicar**. Consulte el área del flujo de trabajo en la sección **Tareas comunes de Smartport** para obtener sugerencias para la resolución de problemas.
- Volver a aplicar un macro de Smartport a una interfaz. En algunas circunstancias, es posible que usted desee volver a aplicar un macro de Smartport para que la configuración de interfaz esté actualizada. Por ejemplo, al volver a aplicar un macro de Smartport de switch en una interfaz de dispositivo convertirá la interfaz en miembro de las VLAN creadas desde la última aplicación del macro. Usted debe estar familiarizado con las configuraciones actuales en el dispositivo y la definición del macro para determinar si la nueva aplicación tiene impacto en la interfaz.
- Reiniciar interfaces desconocidas. Esto configura el modo Desconocido de las interfaces en Predeterminado.

Para aplicar un macro de Smartport:

PASO 1 Haga clic en **Smartport > Configuración de la interfaz**.

Vuelva a aplicar el macro de Smartport asociado de las siguientes maneras:

- Seleccione un grupo de tipos de Smartport (switches, routers o AP) y haga clic en **Volver a aplicar macro de Smartport.** Los macros se aplican a todos los tipos de interfaz seleccionados.
- Seleccione una interfaz que sea UP y haga clic en **Volver a aplicar** para volver a aplicar el último macro que se aplicó a la interfaz.

  La acción **Volver a aplicar** agrega la interfaz a todas las VLAN recientemente creadas.

PASO 2 Diagnóstico de Smartport.

Si un macro de Smartport falla, el tipo de Smartport de la interfaz es Desconocido. Seleccione una interfaz de tipo desconocido y haga clic en **Mostrar diagnóstico.** Esto le mostrará el comando en el cual falló la aplicación del macro. Consulte el área del flujo de trabajo en la sección **Tareas comunes de Smartport** para obtener sugerencias para la resolución de problemas. Proceda a volver a aplicar el macro una vez corregido el problema.

PASO 3 Restablecimiento de las interfaces en tipo Desconocido a tipo Predeterminado.

- Seleccione la casilla de verificación *Tipo de puerto equivale a*.
- Seleccione *Desconocida* y haga clic en **Ir**.
- Haga clic en **Reiniciar todos los Smartports desconocidos**. Luego vuelva a aplicar el macro tal como se describe arriba. Esto restablece todas las interfaces con tipo Desconocido, es decir todas las interfaces vuelven al tipo Predeterminado. Luego de corregir el error en el macro o en la configuración de interfaz actual o en ambos, se puede aplicar un macro nuevo.

NOTA Al reiniciar la interfaz de un tipo desconocido no se reinicia la configuración realizada por el macro que falló. Esta limpieza debe realizarse manualmente.

Para asignar un tipo de Smartport a una interfaz o activar Smartport automático en la interfaz:

PASO 1 Seleccione una interfaz, y haga clic en **Editar**.

PASO 2 Ingrese los campos.

- **Interfaz**: seleccione un puerto o LAG.
- **Tipo de Smartport**: muestra el tipo de Smartport actualmente asignado al puerto o LAG.
- **Aplicación de Smartport**: seleccione el tipo de puerto en la lista desplegable Aplicación de Smartport.

- **Método de aplicación de Smartport**: si se selecciona Smartport automático, este asignará automáticamente el tipo de Smartport según el anuncio de CDP o LLDP que reciba de los dispositivos conectados y también aplicará el macro de Smartport correspondiente. Para asignar estáticamente un tipo de Smartport y aplicar el macro de Smartport correspondiente a la interfaz, seleccione el tipo de puerto deseado.
- **Estado Persistente**: seleccione esta opción para habilitar el estado Persistente. Si está activada, la asociación de un tipo de Smartport a una interfaz se mantiene aunque la interfaz se desactive y el dispositivo se reinicie. Persistente solo es aplicable si la aplicación de Smartport de la interfaz es Smartport automático. Al habilitar Persistente en una interfaz se elimina la demora de detección del dispositivo que, de otra manera, se produciría.
- **Parámetros del macro**: muestra los siguientes campos para tres parámetros en el macro:
  - *Nombre de parámetro*: nombre de parámetro en el macro.
  - *Valor de parámetro*: valor actual de parámetro en el macro. Se puede cambiar aquí.
  - *Descripción de parámetro*: descripción de parámetro.

PASO 3 Haga clic en **Reiniciar** para establecer una interfaz en estado Predeterminado si se encuentra en estado Desconocido (como resultado de una aplicación de marco errónea). El macro puede volver a aplicarse en la página principal.

PASO 4 Haga clic en **Aplicar** para actualizar los cambios y asignar el tipo de Smartport a la interfaz.

Macros de Smartport incorporados

A continuación, se describe el par de macros incorporados para cada tipo de Smartport. Para cada tipo de Smartport hay un macro para configurar la interfaz y un antimacro para eliminar la configuración.

Se proporciona el código de macro para los siguientes tipos de Smartport:

- **equipo de escritorio**
- **impresora**
- **invitado**
- **servidor**
- **host**
- **ip_camera**
- **ip_phone**

- **ip_phone_desktop**
- **switch**
- **router**
- **ap**

escritorio

```
[desktop]
#interface configuration, para mayor seguridad y confiabilidad de red al conectar un dispositivo de
escritorio, como una PC a un puerto de switch.
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#                         $max_hosts: La cantidad máxima de dispositivos permitidos en el puerto
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#$max_hosts = 10
#
#el tipo de puerto no se puede detectar automáticamente
#
#el modo predeterminado es troncal
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
```

```
spanning-tree portfast auto
#
@
```

impresora

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#
#el tipo de puerto no se puede detectar automáticamente
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

invitado

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#
#el tipo de puerto no se puede detectar automáticamente
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

servidor

```
[server]
#macro description server
```

```
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#                         $max_hosts: La cantidad máxima de dispositivos permitidos en el puerto
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#$max_hosts = 10
#
#el tipo de puerto no se puede detectar automáticamente
#
#el modo predeterminado es troncal
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#                         $max_hosts: La cantidad máxima de dispositivos permitidos en el puerto
```

```
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#$max_hosts = 10
#
#el tipo de puerto no se puede detectar automáticamente
#
#el modo predeterminado es troncal
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#
```

```
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#                         $voice_vlan: El ID de VLAN de voz
#                         $max_hosts: La cantidad máxima de dispositivos permitidos en el puerto
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#$voice_vlan = 1
#$max_hosts = 10
#
#el modo predeterminado es troncal
smartport switchport trunk allowed vlan add $voice_vlan
```

```
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: El ID de VLAN de voz
#
#Los valores predeterminados son
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#                         $voice_vlan: El ID de VLAN de voz
#                         $max_hosts: La cantidad máxima de dispositivos permitidos en el puerto
#Los valores predeterminados son
```

```
#$native_vlan = VLAN predeterminada
#$voice_vlan = 1
#$max_hosts = 10
#
#el modo predeterminado es troncal
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: El ID de VLAN de voz
#
#Los valores predeterminados son
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

switch

```
[switch]
#macro description switch
```

```
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#                        $voice_vlan: El ID de VLAN de voz
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#$voice_vlan = 1
#
#el modo predeterminado es troncal
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: El ID de VLAN de voz
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
#                        $voice_vlan: El ID de VLAN de voz
#
#Los valores predeterminados son
#$native_vlan = VLAN predeterminada
#$voice_vlan = 1
#
#el modo predeterminado es troncal
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
```

```
spanning-tree link-type point-to-point
#
@
```

no_router

```
[no_router]
#macro description No router
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: El ID de VLAN de voz
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
no spanning-tree link-type
#
@
```

ap

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: La VLAN sin etiqueta que se configurará en el puerto
```

13

Administración de puertos: PoE

La función Power over Ethernet (PoE) solo está disponible en los dispositivos basados en PoE. Para obtener una lista de dispositivos basados en PoE, consulte la sección **Modelos de dispositivo**.

En esta sección se describe cómo usar la función PoE.

Abarca los siguientes temas:

- **PoE en el dispositivo**
- **Propiedades de PoE**
- **Configuración de PoE**

PoE en el dispositivo

Un dispositivo PoE es un PSE (Power Sourcing Equipment, equipo de fuente de alimentación) que ofrece energía eléctrica a PD (Powered Devices, dispositivos alimentados) conectados por cables de cobre existentes sin interferir en el tráfico de red, y que actualiza la red física o modifica la infraestructura de red.

Consulte la sección **Modelos de dispositivo** para obtener información sobre el soporte PoE en distintos modelos.

Funciones de PoE

PoE proporciona las siguientes funciones:

- Elimina la necesidad de alimentación eléctrica de 110/220 V CA en todos los dispositivos de una LAN con cable.
- Elimina la necesidad de colocar todos los dispositivos de red junto a fuentes de alimentación.
- Elimina la necesidad de implementar sistemas de cableado doble en una empresa, lo que reduce significativamente los costos de instalación.

Power over Ethernet se puede usar en cualquier red corporativa que utiliza dispositivos de potencia relativamente baja conectados a la LAN Ethernet, como:

- Teléfonos IP
- Puntos de acceso inalámbricos
- Puertas de enlace de IP
- Dispositivos de monitoreo remoto de audio y video

Funcionamiento de PoE

PoE se implementa en las siguientes etapas:

- **Detección**: envía pulsos especiales por el cable de cobre. Cuando un dispositivo de PoE está ubicado en el otro extremo, ese dispositivo responde a estos pulsos.
- **Clasificación**: la negociación entre el equipo de fuente de alimentación (PSE) y el dispositivo alimentado (PD) comienza después de la etapa de Detección. Durante la negociación, el PD especifica su clasificación, que es la cantidad de energía máxima que consume el PD.
- **Consumo de energía**: después de que se completa la etapa de clasificación, el PSE suministra energía al PD. Si el PD admite la PoE, pero sin clasificación, se asume que es clasificación 0 (lo máximo). Si un PD intenta consumir más energía de lo que permite la norma, el PSE detiene el suministro de energía al puerto.

PoE admite dos modos:

- **Límite del puerto**: el máximo de energía que el dispositivo acepta suministrar está limitado por el valor que configura el administrador del sistema, independientemente del resultado de la clasificación.
- **Límite de energía de clasificación**: el máximo de energía que el dispositivo acepta suministrar está determinado por los resultados de la etapa de clasificación. Esto significa que se configura según la solicitud del cliente.

Consideraciones de configuración de PoE

Existen dos factores que se deben considerar en la función PoE:

- La cantidad de energía que el PSE puede suministrar
- La cantidad de energía que el PD intenta consumir en realidad

Se pueden configurar las siguientes opciones:

- El máximo de energía que un PSE puede suministrar a un PD.
- Durante el funcionamiento de los dispositivos, cambiar del modo Límite de energía de clasificación al modo Límite del puerto y viceversa. Se conservan los valores de energía por puerto que se configuraron para el modo Límite del puerto.

  NOTA El cambio del modo de Límite de clasific. a Límite del puerto y viceversa cuando el dispositivo está en funcionamiento obliga al dispositivo alimentado a reiniciarse.
- Límite de puerto máximo permitido según el límite numérico por puerto en mW (modo Límite del puerto).
- Generar una trampa cuando un PD intenta consumir demasiado y en qué porcentaje del máximo de energía se genera esta trampa.

El hardware específico de PoE detecta automáticamente la clasificación del PD y su límite de energía según la clasificación del dispositivo conectado a cada puerto específico (modo Límite de clasificación).

Si en algún momento durante la conectividad un PD conectado necesita más energía del dispositivo que lo que permite la asignación configurada (independientemente de si el dispositivo está en el modo Límite de clasific. o Límite del puerto), el dispositivo realiza lo siguiente:

- Mantiene el estado activo/inactivo del enlace de puerto PoE
- Interrumpe el suministro de energía al puerto PoE
- Registra el motivo de la interrupción del suministro de energía
- Genera una trampa SNMP

PRECAUCIÓN Tenga en cuenta lo siguiente cuando conecte switches que puedan suministrar PoE:

Los modelos de PoE de los switches de las series Sx200, Sx300 y SF500 son PSE (equipamiento de fuente de alimentación) capaces de suministrar energía de CC a los (PD) dispositivos alimentados conectados. Entre estos dispositivos se incluyen los teléfonos VoIP, las cámaras IP y los puntos de acceso inalámbrico. Los switches PoE pueden detectar y suministrar energía a los dispositivos alimentados PoE heredados previos al estándar. Debido a la compatibilidad con la PoE heredada, es posible que un dispositivo PoE que actúa como PSE sea detectado por error y suministre energía a un PSE conectado, incluidos otros switches PoE, como un PD heredado.

A pesar de que los switches PoE Sx200/300/500 son PSE, y como tales deberían ser alimentados por CA, pueden recibir alimentación como PD heredados a través de otro PSE por detección falsa. Cuando ocurre esto, es posible que el dispositivo PoE no funcione correctamente y que no pueda suministrar energía correctamente a sus PD conectados.

Para evitar una detección falsa, debe desconectar PoE en los puertos de los switches PoE que se utilizan para conectar los PSE. También puede encender primero un dispositivo PSE antes de conectarlo al dispositivo PoE. Cuando se detecta un dispositivo, de manera falsa, como un PD, debe desconectar el dispositivo del puerto PoE y reciclar la energía del dispositivo con alimentación de CA antes de reconectar los puertos PoE.

Propiedades de PoE

La página Propiedades de PoE permite seleccionar el modo PoE Límite del puerto o Límite de clasific. y especificar las trampas de PoE que se deben generar.

Esta configuración se ingresa de antemano. Cuando el PD se conecta y está consumiendo energía, puede consumir mucho menos que el máximo de energía permitida.

La energía de salida se deshabilita durante el reinicio de encendido, la inicialización y la configuración del sistema para asegurarse de que no se dañen los PD.

Para configurar la PoE en el dispositivo y monitorear el uso de energía actual:

PASO 1 Haga clic en **Administración de puertos > PoE > Propiedades**.

PASO 2 Ingrese los valores para los siguientes campos:

- **Modo energía**: seleccione una de las siguientes opciones:
  - *Límite del puerto*: el usuario configura el límite máximo de energía por puerto.
  - *Límite de clasificación*: el límite máximo de energía por puerto lo determina la clasificación del dispositivo, que resulta de la etapa de clasificación.

  NOTA Cuando cambia de Límite del puerto a Límite de clasific. o viceversa, debe desactivar los puertos PoE y activarlos después de cambiar la configuración de alimentación.
- **Trampas**: habilite o deshabilite las trampas. Si las tramas están habilitadas, también debe habilitar el SNMP y configurar al menos un Destinatario de notificaciones de SNMP.
- **Umbral de trampa de energía**: ingrese el umbral de uso, que es un porcentaje del límite de energía. Si la energía supera este valor, se activa una alarma.

Se muestran los siguientes contadores:

- **Energía nominal**: la cantidad total de energía que el dispositivo puede suministrar a todos los PD conectados.
- **Energía consumida**: cantidad de energía que los puertos PoE están consumiendo.

- **Energía disponible**: energía nominal menos la cantidad de energía consumida.

PASO 3 Haga clic en **Aplicar** para guardar las propiedades de PoE.

Configuración de PoE

En la página Configuración de PoE, se muestra la información de PoE del sistema para activar PoE en las interfaces y monitorear el uso de energía actual y el límite máximo de energía por puerto.

NOTA Se puede configurar la PoE en el dispositivo por un período específico. Esta característica le permite definir, por puerto, los días de la semana y las horas que está activada la PoE. Si el intervalo de tiempo no está activado, la PoE está desactivada. Para utilizar esta característica, primero se debe definir un intervalo de tiempo en la página **Intervalo de tiempo**.

En esta página se limita la energía por puerto de dos formas según el modo de energía:

- **Límite del puerto:** la energía se limita a una potencia especificada. Para que estos valores estén activos, el sistema debe estar en el modo PoE Límite del puerto. Este modo se configura en la página Propiedades de PoE.

  Cuando la energía que se consume en el puerto supera el límite del puerto, se desconecta la energía del puerto.

- **Límite de clasificación:** la energía se limita según la clasificación del PD conectado. Para que estos valores estén activos, el sistema debe estar en el modo PoE Límite de clasificación. Este modo se configura en la página Propiedades de PoE.

  Cuando la energía que se consume en el puerto supera el límite de clasificación, se desconecta la energía del puerto.

Ejemplo de prioridad PoE:

Dado: un dispositivo de 48 puertos suministra un total de 375 vatios.

El administrador configura todos los puertos para asignen hasta 30 vatios. Esto significa 48 por 30 puertos, lo que equivale a 1440 vatios, que es demasiado. El dispositivo no puede proporcionar energía suficiente a cada puerto, por lo que proporciona energía según la prioridad.

El administrador establece la prioridad para cada puerto, asigna la cantidad de alimentación eléctrica que puede recibir.

Estas prioridades se ingresan en la página Configuración de PoE.

Consulte **Modelos de dispositivo** para obtener una descripción de los modelos de dispositivo que admiten PoE y la cantidad máxima de energía que se les puede asignar a los puertos PoE.

Para configurar los valores de los puertos PoE:

PASO 1 Haga clic en **Administración de puertos > PoE > Configuración**. La lista de campos a continuación es para el Modo energía Límite del puerto. Los campos varían levemente si el Modo energía es Límite de clasific.

PASO 2 Seleccione un puerto y haga clic en **Editar.**

PASO 3 Ingrese el valor para el siguiente campo:

- **Interfaz**: seleccione el puerto para configurar.
- **Estado administrativo de PoE**: habilite o deshabilite la PoE en el puerto.
- **Intervalo de tiempo**: seleccione esta opción para activar la PoE en el puerto.
- **Nombre del intervalo de tiempo**: si la opción Intervalo de tiempo está activada, seleccione el intervalo de tiempo que se utilizará. Los intervalos de tiempo se definen en la página **Intervalo de tiempo**.
- **Nivel de prioridad de energía**: seleccione la prioridad del puerto: baja, alta o crítica, para usar cuando el suministro de energía sea bajo. Por ejemplo, si el suministro de energía está funcionando al 99% del uso, y el puerto 1 tiene una prioridad alta y el puerto 3 tiene una prioridad baja, el puerto 1 recibe energía y al puerto 3 se le puede negar.
- **Asignación de energía administrativa**: este campo aparece únicamente si el Modo energía configurado en la página Propiedades de PoE es Límite del puerto. Si el modo Energía es Límite del puerto, ingrese la energía asignada al puerto en milivatios.
- **Asignación de energía máxima**: este campo aparece únicamente si el Modo energía configurado en la página Propiedades de PoE es Límite de energía. Muestra la cantidad máxima de energía permitida en este puerto.
- **Consumo de energía**: muestra la cantidad de energía en milivatios asignada al dispositivo alimentado conectado a la interfaz seleccionada.
- **Clasificación**: este campo aparece únicamente si el Modo energía configurado en la página Propiedades de PoE es Límite de clasific. La clasificación determina el nivel de energía:

Clase	Máximo de energía suministrada por puerto de dispositivo
0	15.4 vatios
1	4.0 vatios
2	7.0 vatios
3	15.4 vatios
4	30.0 vatios

- **Contador de sobrecargas**: muestra el número total de eventos de sobrecarga de energía.
- **Contador de cortos**: muestra el número total de eventos de insuficiencia de energía.
- **Contador de rechazos**: muestra la cantidad de veces que al dispositivo alimentado se le ha negado energía.
- **Contador de ausencias**: muestra la cantidad de veces que la energía se ha detenido para el dispositivo alimentado, porque ya no se detectaba el dispositivo.
- **Contador de firmas no válidas**: muestra la cantidad de veces que se recibió una firma no válida. Las firmas son las formas mediante las cuales el dispositivo alimentado se identifica en el PSE. Las firmas se generan durante la detección, la clasificación o el mantenimiento del dispositivo alimentado.

PASO 4 Haga clic en **Aplicar**. La configuración de PoE para el puerto se escribe en el archivo Configuración en ejecución.

14

Administración de VLAN

Esta sección abarca los siguientes temas:

- **Información general**
- **VLAN normales**
- **Configuración de VLAN privada**
- **Configuración del GVRP**
- **Grupos VLAN**
- **VLAN de voz**
- **VLAN de TV de multidifusión de puerto de acceso**
- **VLAN de TV de multidifusión de puerto de cliente**

Información general

Una VLAN es un grupo lógico de puertos que habilita a los dispositivos asociados a la VLAN comunicarse entre sí por la capa MAC Ethernet, independientemente del segmento LAN físico de la red conectada con puente con la que los dispositivos están conectados.

Una VLAN es un grupo lógico de puertos que habilita a los dispositivos asociados a la VLAN comunicarse entre sí por la capa MAC Ethernet, independientemente del segmento LAN físico de la red conectada con puente con la que los dispositivos están conectados.

Descripción de una VLAN

Cada VLAN está configurada con un VID (ID de VLAN) único con un valor de 1 a 4094. Un puerto de un dispositivo en una red conectada con puente es miembro de una VLAN si puede enviar y recibir datos de la VLAN. Un puerto es un miembro sin etiquetar de una VLAN si todos los paquetes destinados a ese puerto por la VLAN no tienen una etiqueta VLAN. Un puerto es un miembro etiquetado de una VLAN si todos los paquetes destinados a ese puerto por la VLAN tienen una etiqueta VLAN. Un puerto puede ser miembro solo de una VLAN sin etiquetar y puede ser miembro de varias VLAN etiquetadas.

Un puerto en el modo de acceso VLAN puede ser parte de una sola VLAN. Si se encuentra en el modo General o Troncal, el puerto puede ser parte de una o más VLAN.

Las VLAN tratan problemas de seguridad y escalabilidad. El tráfico de una VLAN se mantiene dentro de la VLAN y termina en dispositivos de la VLAN. También facilita la configuración de red ya que conecta de manera lógica los dispositivos sin reubicarlos físicamente.

Si una trama tiene una etiqueta VLAN, se añade una etiqueta VLAN de cuatro bytes a cada trama Ethernet. Esta etiqueta contiene una ID de VLAN entre 1 y 4094, y una VPT (*VLAN Priority Tag*, etiqueta de prioridad de VLAN) entre 0 y 7. Consulte la sección **Calidad del servicio** para obtener detalles sobre VPT.

Cuando una trama ingresa a un dispositivo que detecta la VLAN, se clasifica como perteneciente a una VLAN, según la etiqueta VLAN de cuatro bytes en la trama.

Si no hay etiqueta VLAN en la trama o si la trama solo tiene identificación prioritaria, se la clasifica para la VLAN según el PVID (identificador VLAN de puerto) configurado en el puerto de ingreso donde se recibe la trama.

La trama se descarta en el puerto de ingreso si Filtrado de acceso está habilitado y el puerto de ingreso no es miembro de la VLAN a la que pertenece el paquete. Se considera que una trama tiene identificación prioritaria solo si el VID de su etiqueta VLAN es 0.

Las tramas que pertenecen a una VLAN permanecen dentro de la VLAN. Esto se logra mediante el envío o reenvío de una trama solo a los puertos de egreso que son miembros de la VLAN de destino. Un puerto de egreso puede ser un miembro etiquetado o sin etiquetar de una VLAN.

El puerto de egreso:

- Añade una etiqueta VLAN a la trama si el puerto de egreso es un miembro etiquetado de la VLAN de destino y la trama original no tiene una etiqueta VLAN.
- Retira la etiqueta VLAN de la trama si el puerto de egreso es un miembro sin etiquetar de la VLAN de destino y la trama original tiene una etiqueta VLAN.

Roles de VLAN

Las VLAN funcionan en la capa 2. Todo tráfico de una VLAN (Undifusión/Difusión/Multidifusión) permanece dentro de esa VLAN. Los dispositivos conectados a distintas VLAN no tienen conectividad directa entre sí en la capa MAC Ethernet. Los dispositivos de diferentes VLAN pueden comunicarse entre sí únicamente a través de routers de capa 3. Por ejemplo, se requiere un router IP para enrutar tráfico IP entre VLAN si cada VLAN representa una subred IP.

El router IP puede ser un router tradicional, en donde cada una de sus interfaces se conecta a una sola VLAN. El tráfico de entrada y salida de un router IP tradicional debe ser VLAN sin etiquetar. El router IP puede ser un router que detecta la VLAN, donde cada una de sus interfaces se puede conectar a una o más VLAN. El tráfico de entrada y salida de un router IP que detecta la VLAN puede ser VLAN etiquetado o sin etiquetar.

Los dispositivos adyacentes que detectan la VLAN pueden intercambiar información de VLAN entre sí a través del Protocolo genérico del registro de la VLAN (GVRP, Generic VLAN Registration Protocol). Entonces, la información de VLAN se propaga por una red conectada con puente.

Las VLAN de un dispositivo se pueden crear de manera estática o dinámica, según la información del GVRP que intercambian los dispositivos. Una VLAN puede ser estática o dinámica (desde GVRP), pero no ambas. Si necesita más información acerca de GVRP, consulte la sección Configuración del GVRP.

Algunas VLAN pueden tener roles adicionales, como por ejemplo:

- VLAN de voz: para obtener más información, consulte la sección VLAN de voz.
- VLAN invitada: se configura en la página Editar autenticación de VLAN.
- VLAN predeterminada: para obtener más información, consulte la sección Configuración de los valores de la VLAN predeterminada.
- Administración de VLAN (en los sistemas de modo de capa 2 del sistema): para obtener más información, consulte la sección Direccionamiento IP de capa 2.

QinQ

QinQ proporciona aislamiento entre las redes del proveedor de servicio y las redes de los clientes. El dispositivo es un puente proveedor que admite una interfaz de servicio con etiqueta c basada en el puerto.

Al contar con QinQ, el dispositivo incorpora una etiqueta de ID conocida como etiqueta de servicio (etiqueta S) para reenviar tráfico por la red. La etiqueta S se utiliza para segregar el tráfico entre varios clientes, y al mismo tiempo preservar las etiquetas VLAN del cliente.

El tráfico del cliente se encapsula con una etiqueta S con TPID 0x8100, independientemente de si originalmente se le asignó una etiqueta c o ninguna. La etiqueta S permite que el tráfico se trate como un agregado dentro de una red de puente proveedor, donde el puente se basa en el VID de etiqueta S (S-VID) únicamente.

La etiqueta S se preserva mientras que el tráfico se reenvía a través de la infraestructura del proveedor de servicio de red y posteriormente un dispositivo de egreso la elimina.

Un beneficio adicional de QinQ es que no es necesario configurar los dispositivos de borde de los clientes.

QinQ se activa en Administración de VLAN > Configuración de la interfaz.

VLAN privadas

La característica de VLAN privadas ofrece aislamiento de capa 2 entre los puertos. Esto significa que, a nivel de puenteo de tráfico (a diferencia del enrutamiento IP), los puertos que comparten el mismo dominio de transmisión no pueden comunicarse entre sí. Los puertos de una VLAN privada pueden ubicarse en cualquier lugar de la red de capa 2; no necesariamente deben estar en el mismo switch. La VLAN privada está diseñada para recibir tráfico sin etiquetar y con etiquetado prioritario, y para enviar tráfico sin etiquetar.

Los siguientes tipos de puertos pueden ser miembros en una VLAN privada:

- **Promiscuo**: un puerto promiscuo puede comunicarse con todos los puertos de la misma VLAN privada. Esos puertos conectan servidores y routers.
- **De comunidades (host)**: los puertos de comunidades pueden definir a un grupo de puertos que son miembros del mismo dominio de capa 2. Están aislados en la capa 2 de otras comunidades y de los puertos aislados. Esos puertos conectan puertos host.
- **Aislado (host)**: este tipo de puerto tiene aislamiento de capa 2 total de los demás puertos aislados y de comunidad pertenecientes a la misma VLAN privada. Esos puertos conectan puertos host.

Existen los siguientes tipos de VLAN privadas:

- **VLAN principal**: la VLAN principal se utiliza para habilitar la conectividad de capa 2 desde los puertos promiscuos hasta los puertos aislados y de comunidad. Solo puede haber una única VLAN principal por cada VLAN privada.
- **VLAN aislada (también conocida como VLAN secundaria)**: una VLAN aislada se utiliza para habilitar el envío de tráfico desde los puertos aislados hasta la VLAN principal. Solo puede haber una única VLAN aislada por cada VLAN privada.
- **VLAN de comunidad (también conocida como VLAN secundaria)**: para crear un subgrupo de puertos (comunidad) dentro de una VLAN, debe agregarse una VLAN de comunidad a los puertos. La VLAN de comunidad se utiliza para habilitar la conectividad de capa 2 desde los puertos de comunidad hasta los puertos promiscuos y de comunidad de la misma comunidad. Puede haber una sola VLAN de comunidad por cada comunidad, y en el sistema pueden coexistir varias VLAN de comunidad para la misma VLAN privada.

Consulte **Figura 1** y **Figura 2** para obtener ejemplos del modo de uso de estas VLAN.

El tráfico del host se envía por VLAN aisladas y de comunidad, mientras que el tráfico del servidor y el router se envía por la VLAN principal.

Todas las VLAN que pertenecen a la misma VLAN privada admiten el aprendizaje de dirección MAC compartido (aunque el switch admita el aprendizaje de VLAN independiente). Esto habilita el tráfico de unidifusión, pese a que las VLAN aisladas y de comunidad aprenden las direcciones MAC del host, y la VLAN principal aprende las direcciones MAC de los routers y el servidor.

Solo puede agregarse un puerto de VLAN privada a una VLAN privada. Los otros tipos de puertos, como los troncales o de acceso, pueden agregarse a las VLAN individuales que integran la VLAN privada (ya que son VLAN 802.1Q comunes).

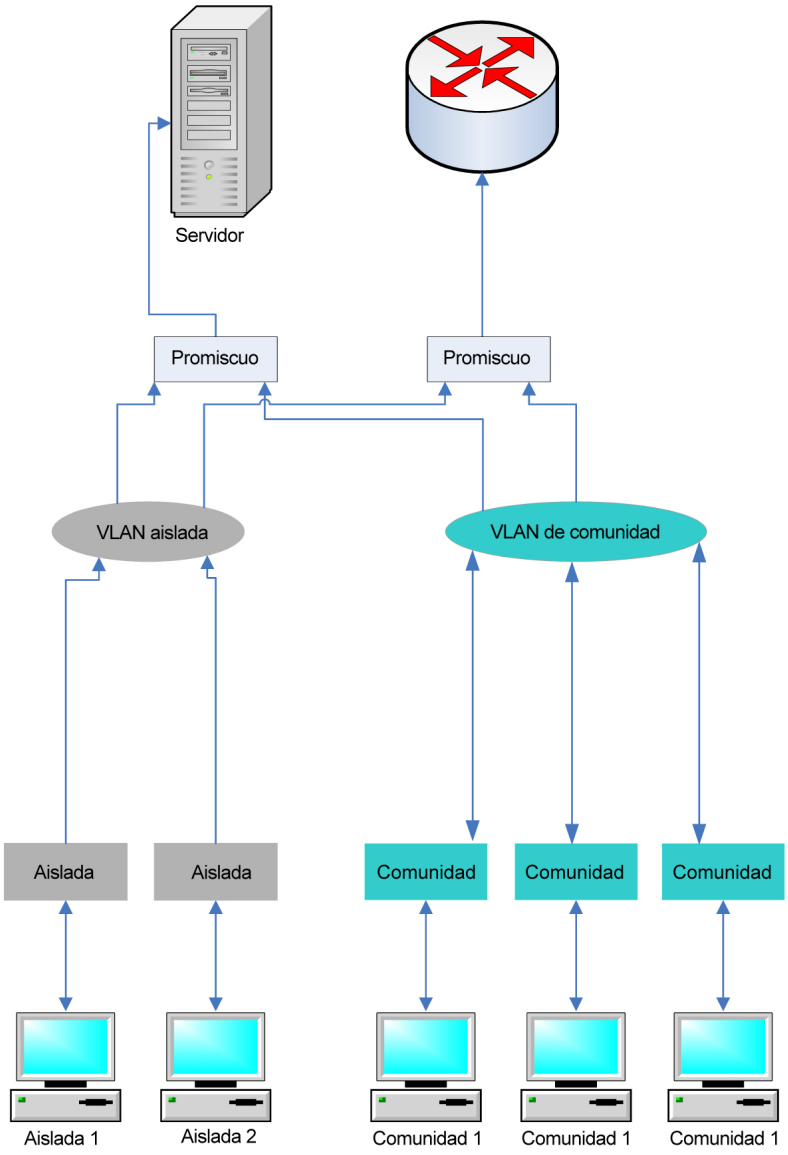
Es posible configurar una VLAN privada para que se expanda a varios switches. Para hacerlo, los puertos entre switches deben configurarse como puertos troncales y se los debe agregar a todas las VLAN de la VLAN privada. Los puertos troncales entre switches envían y reciben tráfico etiquetado de las diversas VLAN de la VLAN privada (principal, aislada y de comunidad).

El switch admite 16 VLAN principales y 256 VLAN secundarias.

Flujo de tráfico

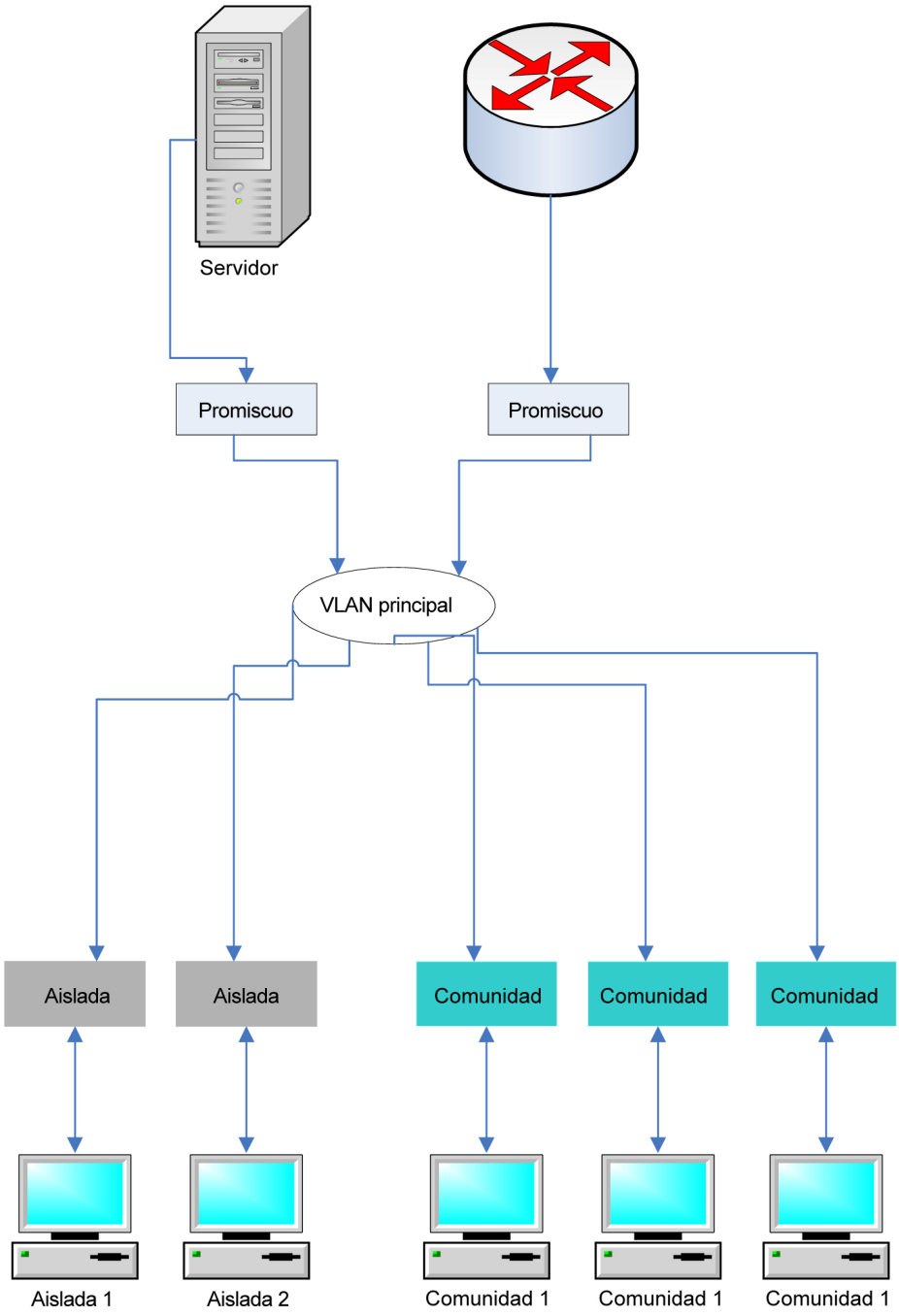
A continuación, se describe el flujo de tráfico desde los hosts hasta los servidores o routers, o a hasta otros hosts.

Figura 1 Tráfico desde los hosts hasta los servidores o routers



A continuación, se describe el tráfico del servidor o router (respuesta al host).

Figura 2 Tráfico desde el servidor o router hasta los hosts



Interacciones con otras funciones

En esta sección, se describe la interacción entre las VLAN privadas y otras funciones del sistema.

Funciones compatibles en una VLAN privada

Las siguientes características solo pueden habilitarse en una VLAN principal (y no en una VLAN aislada o de comunidad) aunque afecten a todas las VLAN de la VLAN privada.

- Indagación IGMP e indagación MLD. Los informes y las consultas de IGMP se detectan en todas las VLAN de la VLAN privada, mientras que las entradas de multidifusión resultantes solo se agregan a la FDB de la VLAN principal. Esto se realiza para que el tráfico de multidifusión pueda reenviarse y no enviarse en forma masiva en la VLAN principal. Las VLAN aisladas y de comunidad siguen enviando tráfico de multidifusión en forma masiva.
- Indagación DHCP.
- Inspección de ARP.
- Protección de la IP de origen.

El sistema no permite agregar ni eliminar VLAN aisladas o de comunidad en una VLAN privada, pero sí admite las características antes descritas.

Funciones no compatibles en una VLAN privada

Las siguientes funciones no son compatibles en las VLAN privadas ni en todas las VLAN que integran la VLAN privada:

- VLAN de voz automática
- VLAN predeterminada
- Retransmisión DHCP
- VLAN no autenticada para 802.1x
- VLAN invitada
- IPv4 e IPv6. Es posible definir IPv6/IPv6 en una VLAN principal. Los puertos aislados y de comunidad no permiten la conectividad IP. La conectividad IP requiere que el tráfico atraviese una VLAN principal.

Funciones no compatibles en modos de puerto de VLAN privadas

Las siguientes funciones no son compatibles en los modos de puerto de VLAN privadas:

- GVRP

- Detección automática de OUI de VLAN de voz
- VLAN de invitado en puerto 802.1x
- Asignación de VLAN dinámica en puerto 802.1x
- VLAN de TV multidifusión.

NOTA Tenga en cuenta las siguientes aclaraciones:

- Seguridad de puertos: las entradas MAC de la tabla de FDB de VLAN se descargan cuando se desbloquea el puerto.
- La afiliación de puertos en una VLAN privada es equivalente a la afiliación de puertos de las VLAN 802.1Q en lo que respecta a las limitaciones de la interacción de características, por ejemplo:
  - El puerto no debe agregarse a un LAG/LACP.
  - El puerto no debe configurarse como destino de supervisión de puerto.

Recursos necesarios

Como una VLAN privada está integrada por varias VLAN 802.1Q, el sistema requiere de otros recursos para las VLAN secundarias de una VLAN privada. Los recursos de las siguientes características se asignan por VLAN dentro de la VLAN privada.

- **Direcciones MAC dinámicas**: las direcciones MAC que se aprenden en las VLAN principales se copian a todas las VLAN de comunidad y a la VLAN aislada. Las direcciones MAC que se aprenden en las VLAN aisladas o de comunidad se copian a la VLAN principal.
- **Indagación de DHCP**: se requiere de una regla de TCAM para captar tráfico DHCP.
- **Inspección de ARP**: se requiere de una regla de TCAM para captar tráfico ARP.
- **Protección de IP de origen**: se requiere de una regla de TCAM para reenviar o descartar tráfico IP.
- **Seguridad del primer salto**: se requiere de una regla de TCAM para captar tráfico IPv6 (cuando está activada la protección de IPv6 de origen).

Pautas de configuración

Tenga en cuenta las siguientes pautas de configuración de características:

- **MSTP**: todas las VLAN de una VLAN privada deben estar asignadas a la misma instancia de MSTP.
- **Protección de la IP de origen**: no se recomienda vincular una ACL en los puertos con protección de IP de origen que tengan una VLAN privada debido a la cantidad de recursos de TCAM necesarios.

VLAN normales

En esta sección, se describen las páginas de la GUI que se utilizan para configurar los diversos tipos de VLAN. En esta sección, se describen los siguientes procesos:

- **Flujo de trabajo de la configuración de VLAN**
- **Configuración de VLAN predeterminada**
- **Configuración de VLAN: creación de VLAN**
- **Configuración de interfaz**
- **Afiliación a una VLAN**
- **Puerto a VLAN**
- **Afiliación VLAN de puertos**
- **Definición de la configuración del GVRP**

Flujo de trabajo de la configuración de VLAN

Para configurar VLAN:

1. Si es necesario, cambie la VLAN predeterminada tal como se describe en la sección **Configuración de VLAN predeterminada**.
2. Cree las VLAN necesarias tal como se describe en la sección **Configuración de VLAN: creación de VLAN**.
3. Establezca la configuración relacionada con VLAN deseada para los puertos y habilite QinQ en una interfaz tal como se describe en la sección **Configuración de interfaz**.
4. Asigne interfaces a las VLAN tal como se describe en la sección **Puerto a VLAN** o en la sección **Afiliación VLAN de puertos**.
5. Vea la afiliación VLAN de puertos actual para todas las interfaces tal como se describe en la sección **Afiliación VLAN de puertos**.

Configuración de VLAN predeterminada

Al utilizar la configuración predeterminada de fábrica, el dispositivo crea automáticamente la VLAN 1 como la VLAN predeterminada, el estado predeterminado de la interfaz de todos los puertos es Troncal y todos los puertos se configuran como miembros sin etiquetar de la VLAN predeterminada.

La VLAN predeterminada tiene las siguientes características:

- Es inconfundible, no estática/no dinámica y todos los puertos son miembros sin etiquetar de forma predeterminada.
- No se puede eliminar.
- No se le puede dar un rótulo.
- No se puede usar para ningún rol especial, como VLAN no autenticada o VLAN de voz. Únicamente relevante para la VLAN de voz habilitada para OUI.
- Si un puerto ya no es miembro de una VLAN, el dispositivo automáticamente configura el puerto como miembro sin etiquetar de la VLAN predeterminada. Un puerto ya no es miembro de una VLAN si la VLAN se elimina o el puerto se elimina de la VLAN.
- Los servidores RADIUS no pueden asignar la VLAN predeterminada a solicitantes 802.1x a través de la asignación de VLAN dinámica.

Cuando el VID de la VLAN predeterminada se cambia, el dispositivo realiza lo siguiente en todos los puertos de la VLAN después de guardar la configuración y reiniciar el dispositivo:

- Elimina la afiliación a VLAN de los puertos de la VLAN predeterminada original (solo se aplica después de reiniciar).
- Cambia el PVID (Identificador VLAN de puerto) de los puertos por el VID de la nueva VLAN predeterminada.
- El ID de VLAN predeterminada original se elimina del dispositivo. Para usarlo, es necesario volver a crearlo.
- Añade los puertos como miembros VLAN sin etiquetar de la nueva VLAN predeterminada.

Para cambiar la VLAN predeterminada:

PASO 1 Haga clic en **Administración de VLAN** > **Configuración de VLAN predeterminada**.

PASO 2 Ingrese el valor para el siguiente campo:

- **ID de VLAN predeterminada actual**: muestra el ID de VLAN predeterminada actual.

- **ID de VLAN predeterminada después del reinicio**: ingrese un nuevo ID de VLAN para reemplazar el ID de VLAN predeterminada después de reiniciar.

PASO 3 Haga clic en **Aplicar**.

PASO 4 Haga clic en **Guardar** (en la esquina superior derecha de la ventana) y guarde la configuración en ejecución en la configuración de inicio.

El **ID de VLAN predeterminada después del reinicio** se convierte en **ID de VLAN predeterminada actual** después de que usted reinicia el dispositivo.

Configuración de VLAN: creación de VLAN

Usted puede crear una VLAN, pero esto no tiene ningún efecto hasta que la VLAN esté conectada con al menos un puerto, ya sea de forma manual o dinámica. Los puertos siempre deben pertenecer a una o más VLAN.

Los dispositivos de la serie 300 admiten hasta 4000 VLAN, incluida la VLAN predeterminada.

Cada VLAN debe estar configurada con un VID único con un valor de 1 a 4094. El dispositivo reserva el VID 4095 como la VLAN para descarte. Todos los paquetes clasificados para la VLAN de descarte se descartan en la entrada y no se reenvían a un puerto.

Para crear una VLAN:

PASO 1 Haga clic en **Administración de VLAN** > **Configuración de VLAN**.

Se muestra información para todas las VLAN definidas. Los campos se definen a continuación en la página **Añadir**. El siguiente campo no está incluido en la página **Añadir**.

- **Originadores**: de qué manera se creó la VLAN:
  - *GVRP*: la VLAN se creó dinámicamente a través del Generic VLAN Registration Protocol (GVRP, Protocolo genérico de registro de VLAN).
  - *Estática*: el usuario define la VLAN.
  - *Predeterminada*: la VLAN es la VLAN predeterminada.

PASO 2 Haga clic en **Agregar** para añadir una o más VLAN nuevas.

La página habilita la creación de una sola VLAN o de un rango de VLAN.

PASO 3 Para crear una sola VLAN, seleccione el botón de radio **VLAN**, ingrese el **ID de VLAN** y opcionalmente el **Nombre de VLAN**.

Para crear un rango de VLAN, seleccione el botón de radio **Rango** y especifique el rango de VLAN que desea crear; para ello, ingrese el VID de inicio y el VID de finalización, ambos inclusive. Al utilizar la función **Intervalo**, la cantidad máxima de VLAN que puede crear a la vez es 100.

PASO 4 Agregue los siguientes campos para las nuevas VLAN.

- **Estado de la interfaz de VLAN**: seleccione para cerrar la VLAN. En ese estado, la VLAN no puede enviar ni recibir mensajes que provengan de niveles superiores o que ahí se dirijan. Por ejemplo, si cierra una VLAN que tiene configurada una interfaz IP, continuará la conexión en puente con la VLAN, pero el switch no podrá enviar ni recibir tráfico IP en la VLAN.
- **Trampas de SNMP de estado de enlace**: seleccione para activar la generación de trampas de SNMP de estado de enlace.

PASO 5 Haga clic en **Aplicar** para crear las VLAN.

Configuración de interfaz

En la página Configuración de la interfaz, se pueden ver y configurar parámetros relacionados con VLAN para todas las interfaces.

Para configurar los valores de VLAN:

PASO 1 Haga clic en **Administración de VLAN** > **Configuración de la interfaz**.

PASO 2 Seleccione un tipo de interfaz (puerto o LAG) y haga clic en **Ir**. Se muestran los puertos o LAG y sus parámetros VLAN.

PASO 3 Para configurar un puerto o LAG, selecciónelo y haga clic en **Editar.**

PASO 4 Ingrese los valores para los siguientes campos:

- **Interfaz**: seleccione un puerto/LAG.
- **Modo Interfaz VLAN**: seleccione el modo de interfaz para la VLAN. Las opciones son:
  - *General*: la interfaz puede admitir todas las funciones según se define en la especificación IEEE 802.1q. La interfaz puede ser un miembro etiquetado o sin etiquetar de una o más VLAN.
  - *Acceso*: la interfaz es un miembro sin etiquetar de una sola VLAN. Un puerto configurado en este modo se conoce como puerto de acceso.
  - *Troncal*: la interfaz es un miembro sin etiquetar de a lo sumo una VLAN, y es un miembro etiquetado de cero o más VLAN. Un puerto configurado en este modo se conoce como puerto troncal.

- *Cliente*: al seleccionar esta opción la interfaz se coloca en modo QinQ. Esto permite que usted utilice sus propias disposiciones de VLAN (PVID) en toda la red proveedora. El dispositivo estará en modo QinQ cuando tenga uno o más puertos de cliente. Consulte **QinQ**.
- VLAN privada - Host: seleccione para configurar la interfaz como aislada o de comunidad. Luego seleccione una VLAN aislada o de comunidad en el campo VLAN secundaria - Host.
- VLAN privada - Promiscua: seleccione para configurar la interfaz como promiscua.

- **PVID administrativo**: ingrese el ID de VLAN de puerto (PVID) de la VLAN para la que se clasifican las tramas entrantes sin etiquetar y con etiquetado prioritario. Los valores posibles son 1 a 4094.
- **Tipo de trama**: seleccione el tipo de trama que la interfaz puede recibir. Las tramas que no son del tipo de trama configurado se descartan en el ingreso. Estos tipos de trama solo están disponibles en el modo General. Los valores posibles son:
  - *Admitir todos*: la interfaz acepta todos los tipos de tramas: tramas sin etiquetar, tramas etiquetadas y tramas con etiquetado prioritario.
  - *Admitir solo los etiquetados*: la interfaz solo acepta tramas etiquetadas.
  - *Admitir solo sin etiquetas*: la interfaz solo acepta tramas sin etiquetar y de prioridad.
- **Filtrado de acceso**: (disponible solo en el modo General) seleccione esta opción para habilitar el filtrado de acceso. Cuando una interfaz tiene el filtrado de acceso habilitado, descarta todas las tramas entrantes clasificadas como VLAN de las que la interfaz no es miembro. El filtrado de acceso se puede deshabilitar o habilitar en los puertos generales. Siempre está habilitado en los puertos de acceso y puertos troncales.
- **VLAN principal**: seleccione la VLAN principal en la VLAN privada. La VLAN principal se utiliza para habilitar la conectividad de capa 2 desde los puertos promiscuos hasta los puertos aislados y de comunidad.
- **VLAN secundaria - Host**: seleccione una VLAN aislada o de comunidad para esos hosts que solo requieren una única VLAN secundaria.
- **VLAN secundarias seleccionadas**: en los puertos promiscuos, mueva todas las VLAN secundarias necesarias para el reenvío normal de paquetes desde las **VLAN secundarias disponibles**. Los puertos promiscuos y troncales pueden pertenecer a varias VLAN.

PASO 5 Haga clic en **Aplicar**. Los parámetros se escriben en el archivo Configuración en ejecución.

Afiliación a una VLAN

En las páginas Puerto a VLAN y Afiliación VLAN de puertos, se muestran las afiliaciones VLAN de los puertos en varias presentaciones. Usted puede usarlas para añadir afiliaciones a las VLAN o eliminarlas de ellas.

Cuando un puerto tiene prohibida la afiliación VLAN predeterminada, ese puerto no puede estar afiliado a ninguna otra VLAN. Al puerto se le asigna un VID interno de 4095.

Para reenviar los paquetes correctamente, los dispositivos intermedios que detectan la VLAN y transportan tráfico VLAN por la trayectoria entre los nodos extremos se deben configurar manualmente o deben aprender dinámicamente las VLAN y sus afiliaciones a puertos del Generic VLAN Registration Protocol (GVRP, protocolo genérico de registro de VLAN).

La afiliación de puertos sin etiquetar entre dos dispositivos que detectan la VLAN sin dispositivos intervinientes que detecten la VLAN debe ser a la misma VLAN. Es decir, el PVID de los puertos que hay entre los dos dispositivos debe ser el mismo si los puertos enviarán paquetes sin etiquetar a la VLAN y recibirán paquetes sin etiquetar de la VLAN. De lo contrario, el tráfico puede filtrarse de una VLAN a la otra.

Las tramas sin etiquetas VLAN pueden pasar por otros dispositivos de red que detectan o no la VLAN. Si un nodo extremo de destino no detecta la VLAN, pero debe recibir tráfico de una VLAN, el último dispositivo que detecta la VLAN (si hay uno) debe enviar tramas de la VLAN de destino al nodo extremo sin etiquetar.

Puerto a VLAN

Use la página Puerto a VLAN para mostrar y configurar los puertos dentro de una VLAN específica.

Para asignar puertos o LAG a una VLAN:

PASO 1 Haga clic en **Administración de VLAN** > **Puerto a VLAN**.

PASO 2 Seleccione una VLAN y el tipo de interfaz (puerto o LAG) y haga clic en **Ir** para mostrar o cambiar la característica del puerto con respecto a la VLAN.

El modo del puerto para cada puerto o LAG se muestra con su modo de puerto actual (Acceso, Troncal, General o Cliente) que se configura en la página Configuración de interfaz.

Cada puerto o LAG aparece con su registro actual en la VLAN.

PASO 3 Cambie el registro de una interfaz a la VLAN; para ello, seleccione **Nombre de interfaz** y la opción que desea de la siguiente lista:

- **Modo de VLAN**: tipo de puertos en la VLAN.

- **Tipo de afiliación**:
  - *Prohibido*: la interfaz tiene prohibido unirse a la VLAN ni siquiera desde el registro GVRP. Cuando un puerto no es miembro de ninguna otra VLAN, al habilitar esta opción en el puerto, este se convierte en parte de la VLAN 4095 interna (un VID reservado).
  - Excluido: actualmente la interfaz no es miembro de la VLAN. Esta es la opción predeterminada para todos los puertos y LAG. El puerto se puede unir a la VLAN a través del registro GVRP.
  - *Etiquetado*: la interfaz es un miembro etiquetado de la VLAN.
  - *Sin etiquetar*: la interfaz es un miembro sin etiquetar de la VLAN. Las tramas de la VLAN se envían sin etiqueta a la VLAN de la interfaz.
  - **PVID**: seleccione esta opción para establecer el PVID de la interfaz como el VID de la VLAN. El PVID se configura por puerto.

PASO 4 Haga clic en **Aplicar**. Las interfaces se asignan a la VLAN y se escriben en el archivo de configuración en ejecución.

Usted puede continuar visualizando y configurando la afiliación de puertos de otra VLAN a través de la selección de otro ID de VLAN.

Afiliación VLAN de puertos

En la página Afiliación VLAN de puertos, se muestran todos los puertos del dispositivo junto con una lista de las VLAN a la cuales pertenece cada puerto.

Si el método de autenticación basada en puertos para una interfaz es 802.1x y el Control del puerto administrativo es Auto, entonces:

- Hasta que se autentique el puerto, se lo excluye de todas las VLAN, a excepción de la invitada y la no autenticada. En la página VLAN a puerto, el puerto estará marcado con P (mayúscula).
- Cuando se autentica el puerto, recibe afiliación en la VLAN en la que se lo configuró.

Para asignar un puerto a una o varias VLAN:

PASO 1 Haga clic en **Administración de VLAN** > **Afiliación VLAN de puertos**.

PASO 2 Seleccione un tipo de interfaz (puerto o LAG) y haga clic en **Ir**. Se muestran los siguientes campos para todas las interfaces del tipo seleccionado:

- **Interfaz**: ID de puerto/LAG.
- **Modo**: modo de VLAN de interfaz que se ha seleccionado en la página Configuración de la interfaz.

- **VLAN administrativas**: lista desplegable donde figuran todas las VLAN de las que es miembro la interfaz.
- **VLAN operativas**: lista desplegable donde figuran todas las VLAN de las que es miembro la interfaz actualmente.
- **LAG**: si la interfaz seleccionada es Puerto, se muestra el LAG del que es miembro.

PASO 3 Seleccione un puerto y haga clic en el botón **Unir VLAN**.

PASO 4 Ingrese los valores para los siguientes campos:

- **Interfaz**: seleccione un puerto o LAG.
- **Modo**: muestra el modo de VLAN de puerto que se ha seleccionado en la página Configuración de la interfaz.
- **Seleccionar VLAN**: para asociar un puerto con una o varias VLAN, use los botones de flecha para pasar los ID de VLAN de la lista de la izquierda a la lista de la derecha. La VLAN predeterminada puede aparecer en la lista de la derecha si tiene etiqueta, pero no se la puede seleccionar.
- **Etiqueta**: seleccione una de las siguientes opciones de etiquetado/PVID:
  - **Prohibido**: la interfaz tiene prohibido unirse a la VLAN ni siquiera desde el registro GVRP. Cuando un puerto no es miembro de ninguna otra VLAN, al habilitar esta opción en el puerto, este se convierte en parte de la VLAN 4095 interna (un VID reservado).
  - **Etiquetado**: seleccione si el puerto tiene etiqueta.
  - **Excluido**: actualmente la interfaz no es miembro de la VLAN. Esta es la opción predeterminada para todos los puertos y LAG. El puerto se puede unir a la VLAN a través del registro GVRP.
  - **Etiquetado**: seleccione si el puerto tiene etiqueta. Esto no es relevante para los puertos de acceso.
  - **Sin etiquetar**: seleccione si el puerto no tiene etiqueta. Esto no es relevante para los puertos de acceso.
  - **VLAN de multidifusión para TV**: interfaz que se usa para TV digital con IP de multidifusión. El puerto se una a la VLAN con una etiqueta de VLAN de VLAN de TV multidifusión. Para obtener más información, consulte **VLAN de TV de multidifusión de puerto de acceso**.
  - **PVID**: el PVID de puerto se configura para esta VLAN. Si la interfaz está en modo Acceso o Troncal, el dispositivo automáticamente convierte la interfaz en un miembro sin etiquetar de la VLAN. Si la interfaz está en el modo general, debe configurar la afiliación VLAN manualmente.

PASO 5 Haga clic en **Aplicar**. La configuración se modifica y se escribe en el archivo Configuración en ejecución.

Para ver las VLAN administrativas u operativas en una interfaz, haga clic en **Detalles**.

Configuración de VLAN privada

La página Configuración de VLAN privada muestra las VLAN privadas que se definieron.

Para crear una nueva VLAN privada:

PASO 1 Haga clic en **Administración de VLAN** > **Configuración de VLAN privada**.

PASO 2 Haga clic en el botón **Add** (Agregar).

PASO 3 Ingrese los valores para los siguientes campos:

- **ID de VLAN principal**: seleccione una VLAN para definirla como VLAN principal en la VLAN privada. La VLAN principal se utiliza para habilitar la conectividad de capa 2 desde los puertos promiscuos hasta los puertos aislados y de comunidad.
- **ID de VLAN aislada**: la VLAN aislada se usa para que los puertos aislados puedan enviar tráfico a la VLAN principal.
- **VLAN de comunidad disponibles**: mueva las VLAN que desea que funcionen como VLAN de comunidad a la lista **VLAN de comunidad seleccionadas**. Las VLAN de comunidad se utilizan para habilitar la conectividad de capa 2 desde los puertos de comunidad hasta los puertos promiscuos y de comunidad de la misma comunidad.

PASO 4 Haga clic en **Aplicar**. La configuración se modifica y se escribe en el archivo Configuración en ejecución.

Configuración del GVRP

Los dispositivos adyacentes que detectan la VLAN pueden intercambiar información de VLAN entre sí a través del Protocolo genérico del registro de la VLAN (GVRP, Generic VLAN Registration Protocol). El GVRP se basa en el Protocolo de registro de atributo genérico (GARP, Generic Attribute Registration Protocol) y propaga información VLAN por una red conectada con puente.

Como el GVRP debe ser compatible con el etiquetado, el puerto debe estar configurado en el modo Troncal o General.

Cuando un puerto se une a una VLAN a través del GVRP, este se agrega a la VLAN como miembro dinámico, a menos que esto se haya prohibido de forma expresa en la página Afiliación VLAN de puertos. Si la VLAN no existe, se crea dinámicamente cuando se activa la creación de VLAN dinámica para este puerto (en la página Configuración del GVRP).

GVRP se debe activar globalmente y también en cada puerto. Cuando está activado, transmite y recibe unidades de datos de paquetes de GARP (GPDU). Las VLAN que están definidas pero no activas no se propagan. Para propagar la VLAN, debe estar activa en al menos un puerto.

De forma predeterminada, GVRP se deshabilita globalmente y en cada puerto.

Definición de la configuración del GVRP

Para definir la configuración del GVRP para una interfaz:

PASO 1 Haga clic en **Administración de VLAN** > **Configuración del GVRP**.

PASO 2 Seleccione **Estado global GVRP** para habilitar GVRP globalmente.

PASO 3 Haga clic en **Aplicar** para establecer el estado global GVRP.

PASO 4 Seleccione un tipo de interfaz (Puerto o LAG), y haga clic en **Ir** para mostrar todas las interfaces de ese tipo.

PASO 5 Para definir la configuración del GVRP para un puerto, selecciónelo y haga clic en **Editar.**

PASO 6 Ingrese los valores para los siguientes campos:

- **Interfaz**: seleccione la interfaz (Puerto o LAG) que desea editar.
- **Estado GVRP**: seleccione para habilitar el GVRP en esta interfaz.
- **Creación VLAN dinámica**: seleccione esta opción para activar la creación de VLAN dinámica en esta interfaz.
- **Registro GVRP**: seleccione para habilitar el registro de VLAN a través de GVRP en esta interfaz.

PASO 7 Haga clic en **Aplicar**. La configuración del GVRP se modifica y se escribe en el archivo Configuración en ejecución.

Grupos VLAN

Esta sección describe cómo configurar grupos de VLAN. Describe los siguientes procesos:

- **Grupos basados en MAC**

Los grupos VLAN se usan para el equilibro de carga de tráfico en la red de capa 2.

Los paquetes se asignan a una VLAN en función de distintas clasificaciones que se han configurado (como los grupos VLAN).

Si se definen diversos esquemas de clasificación, los paquetes se asignan a una VLAN en el siguiente orden:

- **ETIQUETA**: si el paquete está etiquetado, la VLAN se extrae de esa etiqueta.
- **VLAN basada en MAC**: si se ha definido una VLAN basada en MAC, se obtiene la VLAN de la asignación de MAC a VLAN de origen de la interfaz de ingreso.
- **PVID**: la VLAN se obtiene del ID de VLAN predeterminado del puerto.

Grupos basados en MAC

La clasificación de VLAN basada en MAC permite que los paquetes se clasifiquen de acuerdo con la dirección MAC de origen. Luego, usted puede definir una asignación MAC a VLAN por interfaz.

Puede definir varios grupos VLAN basados en MAC, donde cada grupo contiene diferentes direcciones MAC.

Estos grupos basados en MAC se pueden asignar a puertos o LAG específicos. Los grupos VLAN basados en MAC no pueden contener intervalos superpuestos de direcciones MAC en el mismo puerto.

La siguiente tabla describe la disponibilidad de grupos de VLAN basadas en MAC en diversos SKU:

Tabla 1 Disponibilidad de grupos de VLAN basadas en MAC

SKU	Modo del sistema	Grupos de VLAN basadas en MAC compatibles
Sx300	**Capa 2**	Sí
	Capa 3	No
Sx500, Sx500ESW2-550X	**Capa 2**	Sí
	Capa 3	No
SG500X	**Nativo**	Sí
	Híbrido básico - Capa 2	Sí
	Híbrido básico - Capa 3	No
SG500XG	**Igual que Sx500**	Sí

Flujo de trabajo

Para definir un grupo VLAN basado en MAC:

1. Asigne una dirección MAC a un ID de grupo de VLAN (mediante la página Grupos basados en MAC).
2. Para cada interfaz requerida:
   a. Asigne el grupo de VLAN a una VLAN (para ello, use la página Grupos basados en MAC a VLAN). Las interfaces deben estar en el modo General.
   b. Si la interfaz no pertenece a la VLAN, asígnela manualmente a la VLAN a través de la página Puerto a VLAN.

Grupos de VLAN basadas en MAC

Consulte **Tabla 1** para obtener una descripción de la disponibilidad de esta característica.

Para asignar una dirección MAC a un Grupo de VLAN:

PASO 1 Haga clic en **Administración de VLAN** > **Grupos VLAN** > **Grupos basados en MAC**.

PASO 2 Haga clic en **Añadir**.

PASO 3 Ingrese los valores para los siguientes campos:

- **Dirección MAC**: ingrese una dirección MAC para asignar a un grupo de VLAN.

  NOTA Esta dirección MAC no se puede asignar a otro grupo de VLAN.

- **Máscara de prefijo**: ingrese una de las siguientes opciones:
  - *Host*: host de origen de la dirección MAC
  - *Longitud*: *prefijo* de la dirección MAC
- **ID de grupo**: ingrese un número de ID de grupo de VLAN creado por el usuario.

PASO 4 Haga clic en **Aplicar**. Se asigna la dirección MAC a un grupo de VLAN.

Grupo de VLAN a VLAN por interfaz

Consulte Tabla 1 para obtener una descripción de la disponibilidad de esta característica.

Los puertos/LAG deben estar en el modo General.

Para asignar un grupo VLAN basado en MAC a una VLAN en una interfaz:

PASO 1 Haga clic en **Administración de VLAN** > **Grupos VLAN** > **Grupos basados en MAC a VLAN**.

PASO 2 Haga clic en **Añadir**.

PASO 3 Ingrese los valores para los siguientes campos:

- **Tipo de grupo**: muestra que el grupo está basado en MAC.
- **Interfaz**: ingrese una interfaz general (Puerto o LAG) a través de la cual se recibe tráfico.
- **ID de grupo**: seleccione un grupo de VLAN, definido en la página Grupos basados en MAC.
- **ID de VLAN**: seleccione la VLAN a la cual se reenvía el tráfico del grupo de VLAN.

PASO 4 Haga clic en **Aplicar** para establecer la asignación del grupo VLAN a la VLAN. Esta asignación no vincula dinámicamente la interfaz a la VLAN; la interfaz debe añadirse manualmente a la VLAN.

VLAN de voz

En una LAN, los dispositivos de voz, como los teléfonos IP, los puntos finales VoIP y los sistemas de voz se colocan en la misma VLAN. Esta VLAN se denomina VLAN de voz. Si los dispositivos de voz se encuentran en diferentes VLAN de voz, se necesitan routers IP (Capa 3) que proporcionen comunicación.

Esta sección abarca los siguientes temas:

- **Descripción general de VLAN de voz**
- **Configuración de VLAN de voz**
- **OUI para telefonía**

Descripción general de VLAN de voz

Esta sección abarca los siguientes temas:

- **Modos de VLAN de voz dinámica**
- **VLAN de voz automática, Smartport automático, CDP y LLDP**
- **QoS de VLAN de voz**
- **Restricciones de la VLAN de voz**
- **Flujos de trabajo de VLAN de voz**

A continuación, se presentan situaciones típicas de implementación de voz con las configuraciones apropiadas:

- **UC3xx/UC5xx alojado:** todos los teléfonos y los puntos finales VoIP de Cisco admiten este modelo de implementación. Para este modelo, el UC3xx/UC5xx, los teléfonos y los puntos finales VoIP de Cisco residen en la misma VLAN de voz. La VLAN de voz de UC3xx/UC5xx muestra de forma predeterminada VLAN 100.
- **PBX de IP de tercero alojado:** los teléfonos SBTG CP-79xx, SPA5xx y los puntos finales SPA8800 de Cisco admiten este modelo de implementación. En este modelo, la VLAN que utilizan los teléfonos se determina mediante la configuración de red. Pueden haber o no VLAN de datos y de voz por separado. Los teléfonos y los puntos finales VoIP se registran con un PBX IP en las instalaciones.
- **Centrex/ITSP IP alojado:** los teléfonos CP-79xx, SPA5xx y los puntos finales SPA8800 de Cisco admiten este modelo de implementación. En este modelo, la VLAN que utilizan los teléfonos se determina mediante la configuración de red. Pueden haber o no VLAN de datos y de voz por separado. Los teléfonos y los puntos finales IP se registran con un proxy SIP fuera de las instalaciones en "la nube".

Desde el punto de vista de VLAN, los modelos anteriores funcionan tanto en entornos que detectan VLAN como en los que no lo hacen. En el entorno que detecta VLAN, la VLAN de voz es una de las tantas VLAN que se configuran en una instalación. El escenario donde no se detecta la VLAN equivale a un entorno que detecta VLAN con una sola VLAN.

El dispositivo siempre funciona como un switch que detecta VLAN.

El dispositivo admite una sola VLAN de voz. Por opción predeterminada, la VLAN de voz es VLAN 1. La VLAN 1 se elige como predeterminada para la VLAN de voz. Se puede configurar manualmente una VLAN de voz distinta. También se puede aprender de manera dinámica cuando se activa la VLAN de voz.

Los puertos se pueden agregar manualmente a la VLAN de voz a través de la configuración de VLAN básica descrita en la sección Configuración de los valores de las interfaces de VLAN, o al aplicar manualmente el macro de Smartport relacionado con la voz a los puertos. Como alternativa, se pueden agregar dinámicamente si el dispositivo está en modo OUI para telefonía o tiene la opción Smartport automático activada.

Modos de VLAN de voz dinámica

El dispositivo admite dos modos VLAN de voz dinámicos: OUI para telefonía (Organization Unique Identifier) y el modo VLAN de voz automática. Los dos modos afectan la forma en que se configuran la VLAN de voz y las afiliaciones de puerto VLAN de voz. Los dos modos se excluyen mutuamente.

- **OUI para telefonía**

  En modo OUI para telefonía, la VLAN de voz debe ser una VLAN manualmente configurada y no puede ser una VLAN predeterminada.

  Cuando el dispositivo se encuentra en modo OUI para telefonía y se configura manualmente un puerto como candidato para unirse a la VLAN de voz, el dispositivo agrega dinámicamente el puerto a la VLAN de voz, si recibe un paquete con una dirección MAC de origen que coincida con uno de los OUI para telefonía configurados. Un OUI son los primeros tres bytes de una dirección MAC de Ethernet. Para obtener más información acerca de la telefonía para OUI, consulte **OUI para telefonía**.

- **VLAN de voz automática**

  En modo VLAN de voz automática, la VLAN de voz puede ser una VLAN de voz predeterminada, una configurada manualmente o una que se aprenda de dispositivos externos como UC3xx/5xx y de switches que presenten VLAN de voz en CDP o VSDP. VSDP es un protocolo definido por Cisco para la detección de servicio de voz.

  A diferencia del modo OUI para telefonía que detecta dispositivos de voz según el OUI para telefonía, el modo VLAN de voz automática depende de Smartport automático para añadir dinámicamente los puertos a la VLAN de voz. Si Smartport automático está habilitado, agrega un puerto a la VLAN de voz si detecta un dispositivo de conexión al puerto que se anuncia como teléfono o puntos finales de medios a través de CDP o LLDP-MED.

Puntos finales de voz

Para que una VLAN de voz funcione correctamente, los dispositivos de voz como los teléfonos y los puntos finales VoIP de Cisco deben asignarse a la VLAN de voz donde envía y recibe su tráfico de voz. Algunos de los posibles escenarios son los siguientes:

- Un teléfono o punto final se puede configurar estadísticamente con la VLAN de voz.
- Un teléfono y punto final puede obtener la VLAN de voz en el archivo de inicio que se descarga de un servidor TFTP. Un servidor DHCP puede especificar el archivo de inicio y el servidor TFTP cuando asigna una dirección IP al teléfono.

- Un teléfono o punto final puede obtener información de la VLAN de voz desde anuncios de CPD y LLDP-MED que recibe de sus sistemas de voz y switches vecinos.

El dispositivo espera que los dispositivos de voz conectados envíen paquetes con etiquetas de VLAN de voz. En los puertos donde la VLAN de voz es también la VLAN nativa, se puede contar con paquetes sin etiquetar de VLAN de voz.

VLAN de voz automática, Smartport automático, CDP y LLDP

Valores predeterminados

De manera predeterminada de fábrica, las opciones CPD, LLDP y LLDP-MED están activadas en el dispositivo, están activados el modo Smartport automático, el modo Básico de QoS con DSCP de confianza y todos los puertos son miembros de la VLAN 1 predeterminada, que también es la VLAN de voz predeterminada.

Además, el modo VLAN de voz dinámica es el predeterminado para la VLAN de voz automática con la habilitación basada en la activación, y Smartport automático es el modo habilitado de forma predeterminada según la VLAN de voz automática.

Activaciones de la VLAN de voz

Cuando el modo VLAN de voz dinámica se encuentra habilitado como VLAN de voz automático, VLAN de voz automático funcionará únicamente si ocurren una o más activaciones. Las posibles activaciones son la configuración de VLAN de voz estática, la información de VLAN de voz recibida en el anuncio de CDP vecino y la información de VLAN de voz recibida en el protocolo de detección de VLAN de voz (VSDP). Si lo desea, puede activar VLAN de voz automática inmediatamente sin esperar una activación.

Si Smartport automático está habilitado, según el modo VLAN de voz automática, Smartport automático se habilitará cuando VLAN de voz automática se ponga en funcionamiento. Si lo desea, puede habilitar Smartport automático independientemente de VLAN de voz automática.

NOTA Aquí se aplica la lista de configuración predeterminada a los switches cuya versión de firmware admite VLAN de voz automática configurada de fábrica. También se aplica a switches sin configurar que han sido actualizados a la versión de firmware que admite VLAN de voz automática.

NOTA El diseño de los valores predeterminados y las activaciones de la VLAN de voz no afectan las instalaciones que no cuentan con una VLAN de voz ni los switches que ya fueron configurados. Usted puede deshabilitar y habilitar manualmente VLAN de voz automática o Smartport automático para adecuarlo a la implementación, si es necesario.

VLAN de voz automática

VLAN de voz automática es responsable de mantener la VLAN de voz, pero depende de Smartport automático para mantener las afiliaciones del puerto de VLAN de voz. VLAN de voz automática realiza las siguientes funciones cuando se encuentra en funcionamiento:

- Detecta información de la VLAN de voz en los anuncios de CDP de dispositivos vecinos conectados directamente.
- Si varios switches o routers vecinos, como los dispositivos Cisco Unified Communication (UC), anuncian sus VLAN de voz, se utiliza la VLAN de voz del dispositivo que tenga la dirección MAC más baja.

  NOTA Si se conecta el dispositivo a un dispositivo Cisco UC, es posible que deba configurar el puerto en el dispositivo UC con el comando `switchport voice vlan` para garantizar que el dispositivo UC anuncie su VLAN de voz en CDP en el puerto.
- Sincroniza los parámetros relacionados con la VLAN de voz con otros switches habilitados para VLAN de voz automática, mediante el protocolo de detección de servicio de voz (VSDP). El dispositivo siempre se configura con la VLAN de voz a partir de la fuente de prioridad más alto que reconoce. Esta prioridad se basa en el tipo de fuente y en la dirección MAC de la fuente que proporciona la información de VLAN de voz. Las prioridades del tipo de fuente de alta a baja son configuración de VLAN estática, anuncio de CDP y configuración predeterminada según la VLAN predeterminada modificada y la VLAN de voz predeterminada. Una dirección MAC baja numérica tiene una prioridad más alta que una dirección MAC alta numérica.
- Mantiene la VLAN de voz hasta que se detecta una VLAN de voz de fuente de prioridad más alta o hasta que el usuario reinicie la VLAN de voz automática. Al reiniciar, el dispositivo restablece la VLAN de voz a la VLAN de voz predeterminada y reinicia la detección de VLAN de voz automática.
- Si se configura o se detecta una nueva VLAN de voz, el dispositivo la crea automáticamente y reemplaza todas las afiliaciones del puerto de la VLAN de voz existente por la nueva VLAN de voz. Esto puede interrumpir o dar por terminada las sesiones de voz, lo cual se prevé cuando se altera la topología de la red.

  NOTA Si el dispositivo se encuentra en modo de capa 2 del sistema, puede sincronizarse solamente con switches compatibles con VSDP en la misma administración de VLAN. Si el dispositivo se encuentra en modo del sistema Capa 3, puede sincronizarse con switches compatibles con VSDP que están en las mismas subredes IP conectadas directamente en el dispositivo.

Smartport automático trabaja con CDP/LLDP para mantener las afiliaciones de puerto de la VLAN de voz cuando se detectan los puntos finales de voz desde los puertos:

- Si las opciones CDP y LLDP están activadas, el dispositivo envía periódicamente paquetes CDP y LLDP para anunciar la VLAN de voz a los puntos finales de voz para su utilización.

- Cuando un dispositivo que se conecta a un puerto se anuncia como punto final de voz a través de CDP o LLDP, el Smartport automático agrega automáticamente el puerto a la VLAN de voz al aplicar el macro de Smartport correspondiente al puerto (si no hay otros dispositivos del puerto que anuncie un conflicto o capacidad superior). Si un dispositivo se anuncia como teléfono, el macro de Smartport predeterminado es teléfono. Si un dispositivo se anuncia como teléfono y host o teléfono y puente, el macro de Smartport predeterminado es teléfono + escritorio.

QoS de VLAN de voz

La VLAN de voz puede propagar la configuración de CoS/802.1p y DSCP al utilizar políticas de red LLDP-MED. El LLDP-MED se establece de forma predeterminada en respuesta con la configuración de QoS de voz si un dispositivo envía paquetes de LLP-MED. Los dispositivos que admiten MED deben enviar su tráfico de voz con los mismos valores CoS/802.1p y DSCP que recibieron con la respuesta de LLDP-MED.

Puede deshabilitar la actualización automática entre la VLAN de voz y LLDP-MED y usar sus propias políticas de red.

Al trabajar con el modo OUI, el dispositivo también puede configurar la asignación y la remarcación (CoS/802.1p) del tráfico de voz en base al OUI.

De forma predeterminada, todas las interfaces cuentan con el modo de confianza CoS/802.1p. El dispositivo aplica la calidad del servicio según el valor CoS/802.1p encontrado en la secuencia de voz. En modo VLAN de voz automática, el usuario puede anular el valor de las secuencias de voz mediante un QoS avanzado. Para las secuencias de voz de OUI para telefonía, puede anular la calidad del servicio y, de manera opcional, remarcar el 802.1p de las secuencias de voz al especificar los valores CoS/802.1p deseados y usar la opción de remarcado de OUI para telefonía.

Restricciones de la VLAN de voz

Existen las siguientes restricciones:

- Solo se admite una VLAN de voz.
- Una VLAN que se define como VLAN de voz no puede ser eliminada.

Además, se aplican las siguientes restricciones en OUI para telefonía:

- La VLAN de voz no puede ser VLAN1 (la VLAN predeterminada).
- La VLAN de voz no puede tener Smartport habilitado.
- La VLAN de voz no puede admitir DVA (asignación de VLAN dinámica).
- La VLAN de voz no puede ser la VLAN invitada si el modo de VLAN de voz es OUI. Si el modo de VLAN de voz es Automático, la VLAN de voz no puede ser VLAN invitada.
- La decisión de QoS de la VLAN de voz tiene prioridad sobre cualquier otra decisión de QoS, excepto sobre la decisión de QoS de la política/ACL.

- Solo se puede configurar un ID de VLAN nuevo para la VLAN de voz si la VLAN de voz actual no tiene puertos candidatos.
- La VLAN de la interfaz de un puerto candidato debe estar en modo General o Troncal.
- La QoS de la VLAN de voz se aplica a los puertos candidatos que se han unido a la VLAN de voz y a puertos estáticos.
- El flujo de voz se acepta si la base de datos de reenvío (FDB) puede aprender la dirección MAC. (Si no hay espacio libre en la FDB, no se produce ninguna acción).

Flujos de trabajo de VLAN de voz

La configuración predeterminada del dispositivo en VLAN de voz automática, Smartport automático, CDP y LLDP cubre la mayoría de los escenarios comunes de implementación de voz. Esta selección describe cómo implementar VLAN de voz cuando no se aplica la configuración predeterminada.

Flujo de trabajo 1: para configurar la VLAN de voz automática:

PASO 1 Abra la página Administración de VLAN > VLAN de voz > Propiedades.

PASO 2 Seleccione el ID de VLAN de voz. No se puede establecer en ID de VLAN 1 (no se requiere este paso para la VLAN de voz dinámica).

PASO 3 Establezca **VLAN de voz dinámica** para Habilitar VLAN de voz automática.

PASO 4 Seleccione el método **Activación de VLAN de voz automática**.

NOTA Si el dispositivo se encuentra actualmente en modo OUI para telefonía, debe deshabilitarlo antes de configurar la VLAN de voz automática.

PASO 5 Haga clic en **Aplicar**.

PASO 6 Configure Smartport como se describe en la sección **Tareas comunes de Smartport**.

PASO 7 Configure LLDP/CDP tal como se describe en las secciones **Configuración de LLDP** y **Configuración de CDP**, respectivamente.

PASO 8 Active la función Smartport en los puertos correspondientes en Smartport > Configuración de la interfaz.

NOTA Los pasos 7 y 8 son opcionales, pues están habilitados por opción predeterminada.

Flujo de trabajo 2: para configurar el método OUI para telefonía:

PASO 1 Abra la página Administración de VLAN > VLAN de voz > Propiedades. Establezca **VLAN de voz dinámica** para Habilitar OUI para telefonía.

NOTA Si el dispositivo se encuentra actualmente en modo VLAN de voz automática, debe deshabilitarlo antes de configurar OUI para telefonía.

PASO 2 Configure OUI para telefonía en la página OUI para telefonía.

PASO 3 Configure la afiliación de VLAN de OUI para telefonía para los puertos en la página Interfaz de OUI para telefonía.

Configuración de VLAN de voz

Esta sección describe cómo configurar la VLAN de voz. Abarca los siguientes temas:

- **Configuración de las propiedades de VLAN de voz**
- **Configuración de VLAN de voz automática**
- **OUI para telefonía**

Configuración de las propiedades de VLAN de voz

Use la página Propiedades de VLAN de voz para realizar las siguientes acciones:

- Ver de qué manera está configurada actualmente la VLAN de voz.
- Configurar el ID de VLAN de la VLAN de voz.
- Establecer la configuración de QoS de VLAN de voz.
- Configurar el modo VLAN de voz (OUI para telefonía o VLAN de voz automática).
- Configurar de qué manera se activa la VLAN de voz automática.

Para ver y configurar las propiedades de VLAN de voz:

PASO 1 Haga clic en **Administración de VLAN** > **VLAN de voz** > **Propiedades**.

- La configuración de la VLAN de voz establecida en el dispositivo se muestra en el bloque **Configuración de VLAN de voz (estado administrativo)**.
- La configuración de VLAN de voz que en realidad se aplica a la implementación de VLAN de voz se muestra en el bloque **Configuración de VLAN de voz (estado operativo)**.

PASO 2 Ingrese los valores para los siguientes campos:

- **ID de VLAN de voz**: ingrese la VLAN que será la VLAN de voz.

  NOTA Los cambios realizados en el ID de VLAN de voz, CoS/802.1p y DSCP harán que el dispositivo anuncie la VLAN de voz administrativa como una VLAN de voz estática. Si se selecciona la opción *Activación de VLAN de voz automática* activada por la VLAN de voz externa, deben mantenerse los valores predeterminados.

- **CoS/802.1p**: seleccione un valor CoS/802.1p que LLDP-MED utilizará como política de red de voz. Consulte *Administración > Detección > LLDP > Política de red LLDP MED* para obtener información adicional.

- **DSCP**: seleccione los valores DSCP que LLDP-MED utilizará como política de red de voz. Consulte *Administración > Detección > LLDP > Política de red LLDP MED* para obtener información adicional.

- **VLAN de voz dinámica:** seleccione este campo para deshabilitar la función de VLAN de voz de una de las siguientes maneras:

  - *Habilitar VLAN de voz automática*: habilite la VLAN de voz dinámica en modo VLAN de voz automática.
  - *Habilitar OUI para telefonía*: habilite VLAN de voz dinámica en modo OUI para telefonía.
  - *Deshabilitar*: deshabilite VLAN de voz automática o OUI para telefonía.

- **Activación de VLAN de voz automática**: si se habilitó VLAN de voz automática, seleccione una de las siguientes opciones para activar VLAN de voz automática:

  - *Inmediato*: se activa la VLAN de voz automática en el dispositivo y se pone en funcionamiento de inmediato, si está activada la opción.
  - *Por activador externo de VLAN de voz*: se activa la VLAN de voz automática en el dispositivo y solo se pone en funcionamiento si el dispositivo detecta un dispositivo que anuncia la VLAN de voz.

  NOTA La reconfiguración manual del ID de VLAN de voz, CoS/802.1p o DSCP a partir de los valores predeterminados provoca una VLAN de voz estática que tiene una prioridad más alta que la VLAN de voz automática que se aprendió de fuentes externas.

PASO 3 Haga clic en **Aplicar**. Las propiedades de VLAN se escriben en el archivo Configuración en ejecución.

Configuración de VLAN de voz automática

Si está habilitado el modo VLAN de voz automática, utilice la página VLAN de voz automática para ver los parámetros de interfaz y globales correspondientes.

También puede usar esta página para reiniciar manualmente la VLAN de voz automática al hacer clic en **Reiniciar VLAN de voz automática**. Luego de una breve demora, se restablece la VLAN de voz a la VLAN de voz predeterminada y se reinicia la detección de VLAN de voz automática y el proceso de sincronización en todos los switches de la LAN que tienen habilitada la VLAN de voz automática.

NOTA Esto solamente permite restablecer la VLAN de voz a la VLAN de voz predeterminada si el Tipo de fuente se encuentra en estado *Inactivo*.

Para ver los parámetros de la VLAN de voz automática:

PASO 1 Haga clic en **Administración de VLAN** > **VLAN de voz** > **VLAN de voz automática**.

El bloque de estado de funcionamiento de esta página muestra información sobre la VLAN de voz actual y su fuente:

- **Estado de VLAN voz automática**: muestra si VLAN de voz automática está habilitada.
- **ID de VLAN de voz**: el identificador de la VLAN de voz actual
- **Tipo de fuente**: muestra el tipo de fuente donde el dispositivo raíz detecta la VLAN de voz.
- **CoS/802.1p**: muestra valores CoS/802.1p que LLDP-MED utilizará como política de red de voz.
- **DSCP**: muestra los valores DSCP que LLDP-MED utilizará como política de red de voz.
- **Dirección MAC del switch de la raíz**: la dirección MAC del dispositivo raíz de VLAN de voz automática que detecta o se configura con la VLAN de voz desde la cual se aprendió la VLAN de voz.
- **Dirección MAC del switch**: la dirección MAC base del dispositivo. Si la dirección MAC del switch del dispositivo es la dirección MAC del switch de la raíz, el dispositivo es el dispositivo raíz de VLAN automática.
- **Hora de cambio de Id. de VLAN de voz**: última vez que se actualizó la VLAN de voz.

PASO 2 Haga clic en **Reiniciar VLAN de voz automática** para restablecer la VLAN a la VLAN de voz predeterminada y reiniciar la detección de la VLAN de voz automática en todos los switches habilitados para VLAN de voz automática en la LAN.

En la Tabla de fuente local de VLAN de voz, se muestran la VLAN de voz configurada en el dispositivo y cualquier configuración de VLAN de voz que anuncien los dispositivos vecinos conectados directamente. Contiene los siguientes campos:

- **Interfaz**: muestra la interfaz en la cual se recibió y se configuró la configuración de VLAN de voz. Si aparece N/D, eso significa que la configuración se realizó en el mismo dispositivo. Si aparece una interfaz, eso significa que se recibió una configuración de voz desde un vecino.
- **Dirección MAC de origen**: dirección MAC de una UC desde la cual se recibió la configuración de voz.
- **Tipo de fuente**: tipo de UC desde la cual se recibió la configuración de voz. Las opciones disponibles son las siguientes:
  - *Predeterminada*: configuración predeterminada de VLAN de voz en el dispositivo.
  - *Estática*: configuración de VLAN de voz definida por el usuario en el dispositivo.
  - *CDP*: el UC que anunció la configuración de VLAN de voz ejecuta el CDP.
  - *LLDP*: el UC que anunció la configuración de VLAN de voz ejecuta el LLDP.
  - *ID de VLAN de voz*: el identificador de la VLAN de voz anunciada o configurada.
- **ID de VLAN de voz**: el identificador de la VLAN de voz actual.
- **CoS/802.1p**: valores CoS/802.1p anunciados o configurados, que LLDP-MED utiliza como política de red de voz.
- **DSCP**: valores DSCP configurados o anunciados, que LLDP-MED utiliza como política de red de voz.
- **Fuente local óptima**: muestra si el dispositivo utilizó esta VLAN de voz. Las opciones disponibles son las siguientes:
  - *Sí*: el dispositivo utiliza esta VLAN de voz para sincronizarse con otros switches habilitados para VLAN de voz automática. Esta VLAN de voz es la VLAN de voz de la red a menos que se detecte una VLAN de voz de una fuente de prioridad más alta. La fuente local óptima es una sola.
  - *No*: esta no es la fuente local óptima.

PASO 3 Haga clic en **Actualizar** para actualizar la información en la página.

OUI para telefonía

La autoridad de registro Electrical and Electronics Engineers, Incorporated (IEEE) asigna los Identificadores únicos organizadores (OUI). Debido a que la cantidad de fabricantes de teléfonos IP es limitada y conocida, los valores de OUI conocidos hacen que las tramas relevantes, y el puerto en el que se ven, se asignen automáticamente a la VLAN de voz.

La tabla Global de OUI puede contener hasta 128 OUI.

Esta sección abarca los siguientes temas:

- **Tabla de OUI para telefonía**
- **Interfaz de OUI para telefonía**

Tabla de OUI para telefonía

Use la página OUI para telefonía para configurar las propiedades de QoS de OUI para telefonía. Además se puede configurar el tiempo de desactualización automática de la afiliación. Si transcurre el período de tiempo especificado sin que se produzca actividad de telefonía, el puerto se elimina de la VLAN de voz.

Use la página OUI para telefonía para ver los OUI existentes y agregar nuevos OUI.

Para configurar OUI para telefonía y añadir una nueva OUI de VLAN de voz:

PASO 1 Haga clic en **Administración de VLAN** > **VLAN de voz** > **OUI para telefonía**.

La página OUI para telefonía contiene los siguientes campos:

- **Estado operativo de OUI para telefonía**: muestra si se utilizan los OUI para identificar el tráfico de voz.
- **CoS/802.1p**: seleccione la cola de CoS que se asignará al tráfico de voz.
- **Observación CoS/802.1p**: seleccione si desea remarcar el tráfico de egreso.
- **Tiempo de desactualización autom. de membresía**: ingrese la demora de tiempo para eliminar un puerto de la VLAN de voz después de que todas las direcciones MAC detectadas en los puertos caducaron.

PASO 2 Haga clic en **Aplicar** para actualizar la configuración en ejecución del dispositivo con estos valores.

Aparece la Tabla de OUI para telefonía:

- **OUI para telefonía**: los primeros seis dígitos de la dirección MAC que se reservan para los OUI.
- **Descripción**: descripción de OUI asignada por el usuario.

PASO 3 Haga clic en **Restablecer OUI predeterminados** para eliminar todos los OUI creados por el usuario y dejar solo los OUI predeterminados en la tabla. La información del OUI no podrá ser exacta hasta tanto se haya completado la restauración. Puede demorar varios segundos. Luego de algunos segundos, cierre la página y vuelva a ingresar para actualizarla.

Para eliminar todos los OUI, seleccione la casilla de verificación superior. Todos los OUI se seleccionan y se pueden eliminar si hace clic en **Eliminar**. Si luego hace clic en **Restablecer**, el sistema recupera los OUI conocidos.

PASO 4 Para añadir una nueva OUI, haga clic en **Añadir**.

PASO 5 Ingrese los valores para los siguientes campos:

- **OUI para telefonía**: ingrese un OUI nuevo.
- **Descripción**: ingrese un nombre de OUI.

PASO 6 Haga clic en **Aplicar**. Se agrega el OUI a la Tabla de OUI para telefonía.

Interfaz de OUI para telefonía

Los atributos de la QoS se pueden asignar por puerto a los paquetes de voz en uno de los siguientes modos:

- **Todo**: los valores de Calidad de servicio (QoS) configurados para la VLAN de voz se aplican a todas las tramas entrantes que se reciben en la interfaz y se clasifican para la VLAN de voz.
- **Dirección MAC de la fuente de telefonía (SRC)**: los valores de QoS configurados para la VLAN de voz se aplican a cualquier trama entrante que se clasifica para la VLAN de voz y contiene un OUI en la dirección MAC de fuente que coincide con un OUI para telefonía configurado.

Use la página Interfaz de OUI para telefonía para agregar una interfaz a la VLAN de voz según el identificador de OUI y para configurar el modo QoS de OUI de VLAN de voz.

Para configurar OUI para telefonía en una interfaz:

PASO 1 Haga clic en **Administración de VLAN** > **VLAN de voz** > **Interfaz de OUI para telefonía**.

La página Interfaz de OUI para telefonía contiene los parámetros OUI de VLAN de voz para todas las interfaces.

PASO 2 Para configurar que una interfaz sea un puerto candidato de la VLAN de voz basada en OUI para telefonía, haga clic en **Editar.**

PASO 3 Ingrese los valores para los siguientes campos:

- **Interfaz**: seleccione una interfaz.

- **Afiliación a una VLAN de OUI para telefonía**: si esta opción está habilitada, la interfaz es un puerto candidato de la VLAN de voz basada en OUI para telefonía. Cuando se reciben paquetes que coinciden con uno de los OUI para telefonía configurados, se agrega el puerto a la VLAN de voz.
- **Modo QoS VLAN de voz**: seleccione una de las siguientes opciones:
  - *Todo*: se aplican atributos QoS a todos los paquetes que se clasifican para la VLAN de voz.
  - *Dirección MAC de la fuente de telefonía*: los atributos QoS solo se aplican a paquetes de teléfonos IP.

PASO 4 Haga clic en **Aplicar**. Se añade el OUI.

VLAN de TV de multidifusión de puerto de acceso

Las VLAN de TV multidifusión habilitan transmisiones de multidifusión a los suscriptores que no se encuentren en la misma VLAN de datos (capa 2 aislada), sin replicar las tramas de transmisión por multidifusión para cada suscriptor de VLAN.

Los suscriptores, que no se encuentran en la misma VLAN de datos (capa 2 aislada) y están conectados al dispositivo con una afiliación con ID de VLAN distinta, pueden compartir la misma secuencia de multidifusión al unir los puertos al mismo ID de VLAN multidifusión.

El puerto de red, que está conectado al servidor de multidifusión, está configurado estáticamente como miembro en el ID de VLAN multidifusión.

Los puertos de red, que se comunican a través de suscriptores con el servidor de multidifusión (mediante el envío de mensajes IGMP), reciben las secuencias de multidifusión desde el servidor de multidifusión, a la vez que incluyen la VLAN de TV multidifusión en el encabezado de paquete de multidifusión. Por estos motivos, los puertos de red deben estar configurados estáticamente como se indica a continuación:

- Tipo de puerto general o troncal (consulte la sección **Configuración de interfaz**)
- Miembro en la VLAN de TV multidifusión

Los puertos receptores de suscripciones pueden asociarse con la VLAN de TV multidifusión solamente si esta se define de una de las dos siguientes maneras:

- Puerto de acceso
- Puerto de cliente (consulte la sección **VLAN de TV de multidifusión de puerto de cliente**)

Se pueden asociar uno o más grupos de dirección IP multidifusión con la misma VLAN de TV multidifusión.

Cualquier VLAN puede configurarse como VLAN de TV multidifusión. Un puerto asignado a una VLAN de TV multidifusión:

- Se une a la VLAN de TV multidifusión.
- Los paquetes que pasan por los puertos de egreso en la VLAN de TV multidifusión no tienen etiquetas.
- El parámetro de tipo de trama del puerto está establecido como **Admitir todos** y admite, entonces, paquetes sin etiquetas (consulte la sección **Configuración de interfaz**).

La configuración de VLAN de TV multidifusión se define por puerto. Los puertos de cliente están configurados para ser miembros de las VLAN de TV multidifusión; para ello, se utiliza la página VLAN de TV multidifusión.

Indagación IGMP

VLAN de TV multidifusión se basa en indagación IGMP, lo cual significa que:

- Los suscriptores utilizan mensajes IGMP para unirse o abandonar un grupo de multidifusión.
- El dispositivo realiza la indagación IGMP y configura el acceso al puerto según su afiliación de multidifusión en la VLAN de TV multidifusión.

Para cada paquete IGMP que llega a un puerto de acceso, el dispositivo decide si lo asociará con la VLAN de acceso o con la VLAN de TV multidifusión, conforme a las siguientes reglas:

- Si un mensaje IGMP llega a un puerto de acceso con una dirección IP multidifusión de destino que está asociada a la VLAN de TV multidifusión del puerto, entonces el software asocia el paquete IGMP a la VLAN de TV multidifusión.
- De lo contrario, el mensaje IGMP se asocia a la VLAN de acceso y solo se reenviará dentro de esta VLAN.
- El mensaje IGMP se descartará si:
  - El estado STP/RSTP en el puerto de acceso es **descartar**.
  - El estado de MSTP para la VLAN de acceso es **descartar**.
  - El estado de MSTP para la VLAN de TV multidifusión es **descartar** y el mensaje IGMP está asociado a esta VLAN de TV multidifusión.

Diferencias entre VLAN de TV multidifusión y normal

Características de las VLAN de TV multidifusión y normal

	VLAN normal	VLAN de TV multidifusión
Afiliación a una VLAN	La fuente y todos los puertos receptores deben ser estáticos en la misma VLAN de datos.	La fuente y los puertos receptores no pueden ser miembros en la misma VLAN de datos.
Registro del grupo	Todo el registro del grupo multidifusión es dinámico.	Los grupos deben asociarse a la VLAN multidifusión estáticamente, pero el registro real es dinámico.
Puertos receptores	VLAN puede usarse para enviar y recibir tráfico (multidifusión y unidifusión).	VLAN de multidifusión solo puede usarse para recibir tráfico de las estaciones en el puerto (solo multidifusión).
Seguridad y aislamiento	Los receptores de la misma secuencia de multidifusión están en la misma VLAN de datos y pueden comunicarse entre sí.	Los receptores de la misma secuencia de multidifusión están en VLAN de acceso distintas y están aislados entre sí.

Configuración

Flujo de trabajo

Configure la VLAN de TV con los dos siguientes pasos:

1. Defina una VLAN de TV mediante la asociación de un grupo de multidifusión a una VLAN (use la página Grupo multidifusión a VLAN).
2. Especifique los puertos de acceso en cada VLAN multidifusión (use la página Afiliación VLAN de multidifusión de puerto).

Grupo multidifusión a VLAN

Para definir la configuración de la VLAN de TV multidifusión:

PASO 1 Haga clic en **Administración de VLAN** > **Acceder a VLAN de TV multidifusión de puerto** > **Grupo multidifusión a VLAN**.

Se muestran los siguientes campos:

- **Grupo multidifusión**: dirección IP del grupo multidifusión.
- **VLAN de TV multidifusión**: VLAN a la cual se asignan los paquetes de multidifusión.

PASO 2 Haga clic en **Añadir** para asociar un grupo multidifusión a la VLAN. Puede seleccionar cualquier VLAN. Cuando se selecciona una VLAN, se convierte en una VLAN de TV multidifusión.

PASO 3 Haga clic en **Aplicar**. La configuración de la VLAN de TV multidifusión se modifica y se escribe en el archivo Configuración en ejecución.

Afiliación VLAN de multidifusión de puerto

Para definir la configuración de la VLAN de TV multidifusión:

PASO 1 Haga clic en **Administración de VLAN** > **VLAN de TV multidifusión de puerto de acceso** > **Afiliación VLAN de multidifusión de puerto**.

PASO 2 Seleccione una VLAN del campo **VLAN de TV multidifusión**.

PASO 3 Seleccione una interfaz en **Tipo de interfaz**.

PASO 4 La lista **Puertos candidatos de acceso** contiene todos los puertos de acceso configurados en el dispositivo. Mueva los puertos necesarios al campo **Puertos de acceso miembros**.

PASO 5 Haga clic en **Aplicar**. La configuración de la VLAN de TV multidifusión se modifica y se escribe en el archivo Configuración en ejecución.

VLAN de TV de multidifusión de puerto de cliente

Un servicio triple que proporciona tres servicios de banda ancha mediante una única conexión de banda ancha:

- Acceso de alta velocidad a Internet
- Video
- Voz

Este servicio triple se presenta para suscriptores prestadores del servicio, al mismo tiempo que mantiene el aislamiento de capa 2 entre ellos.

Cada suscriptor posee una caja CPE MUX. El MUX tiene varios puertos de acceso que están conectados a los dispositivos del suscriptor (computadora, teléfono, etc.) y un puerto de red que está conectado al dispositivo de acceso.

La caja reenvía los paquetes desde el puerto de red hacia los dispositivos del suscriptor según la etiqueta VLAN del paquete. Cada VLAN se asigna a uno de los puertos de acceso del MUX.

Los paquetes de los suscriptores para la red prestadora del servicio se reenvían como tramas VLAN etiquetadas, para poder distinguir los tipos de servicio, es decir, que para cada tipo de servicio existe un ID de VLAN único en la caja de CPE.

Todos los paquetes del suscriptor a la red prestadora de servicio están encapsulados por el dispositivo de acceso con la VLAN del suscriptor configurada como cliente VLAN (etiqueta exterior o S-VID), excepto para los mensajes de indagación IGMP de los receptores de TV, que están asociados con la VLAN de TV multidifusión. La información de VOD que también se envía desde los receptores de TV se envía como cualquier otro tipo de tráfico.

Los paquetes que recibe el puerto de red del suscriptor desde la red del prestador de servicios se envían por la red del prestador de servicio como paquetes con doble etiqueta, mientras que las etiquetas exteriores (etiquetas de servicio o etiquetas S) representan uno de los dos tipos de VLAN, como se indica a continuación:

- VLAN del suscriptor (incluye Internet y teléfonos IP)
- VLAN de TV multidifusión

La VLAN interna (Etiqueta C) es la etiqueta que determina el destino en la red del suscriptor (por el CPE MUX).

Flujo de trabajo

1. Configure un puerto de acceso como puerto de cliente (use Administración de VLAN > Configuración de la interfaz). Para obtener más información, consulte **QinQ**.
2. Configure el puerto de red como un puerto troncal o general con suscriptor, y la VLAN de TV multidifusión como VLAN etiquetadas. (Use Administración de VLAN > Configuración de la interfaz).

3. Cree una VLAN de TV multidifusión con hasta 4094 VLAN distintas. (La creación de la VLAN se hace mediante la configuración regular de la administración de VLAN).
4. Asocie el puerto de cliente a una VLAN de TV multidifusión; para ello, use la página Afiliación VLAN de multidifusión de puerto.
5. Asigne la VLAN de CPE (etiqueta C) a la VLAN de TV multidifusión (etiqueta S); para ello, utilice la página VLAN CPE a VLAN.

VLAN de CPE a VLAN

Para activar el CPE MUX con las VLAN de los suscriptores, es posible que los suscriptores requieran diversos prestadores de video y que cada prestador esté asignado a una VLAN externa distinta.

Las VLAN de multidifusión del CPE (internas) deben estar asignadas a las VLAN del prestador de multidifusión (externo).

Una vez que se ha asignado la VLAN del CPE a una VLAN de multidifusión, puede participar en la indagación de IGMP.

Para asignar las VLAN de CPE:

PASO 1 Haga clic en **Administración de VLAN** > **VLAN de TV de multidifusión de puerto de cliente** > **VLAN de CPE a VLAN**.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los siguientes campos:

- **VLAN de CPE**: ingrese la VLAN definida en la caja del CPE.
- **VLAN de TV multidifusión**: seleccione la VLAN de TV multidifusión que está asignada a la VLAN del CPE.

PASO 4 Haga clic en **Aplicar**. La asignación de la VLAN del CPE se modifica y se escribe en el archivo Configuración en ejecución.

Afiliación VLAN de multidifusión de puerto

Los puertos que estén asociados con las VLAN de multidifusión deben configurarse como puertos de cliente (consulte la sección **Configuración de interfaz**).

Para asignar puertos a VLAN de TV multidifusión:

PASO 1 Haga clic en **Administración de VLAN** > **VLAN de TV multidifusión de puerto cliente** > **Afiliación VLAN de multidifusión de puerto**.

PASO 2 Seleccione una VLAN del campo **VLAN de TV multidifusión**.

PASO 3 Seleccione una interfaz en **Tipo de interfaz**.

PASO 4 La lista **Puertos cliente candidatos** contiene todos los puertos de acceso configurados en el dispositivo. Mueva los puertos necesarios al campo **Puertos cliente miembros**.

Haga clic en **Aplicar**. La nueva configuración se modifica y se escribe en el archivo Configuración en ejecución.

15

Árbol de expansión

Esta sección describe al Protocolo de árbol de expansión (STP) (IEEE802.1D y IEEE802.1Q) y abarca los siguientes temas:

- **Tipos de STP**
- **Estado y configuración global del STP**
- **Configuración de interfaz del árbol de expansión**
- **Configuración del árbol de expansión rápido**
- **Árbol de expansión múltiple**
- **Propiedades MSTP**
- **VLAN a una instancia de MSTP**
- **Configuración de instancia MSTP**
- **Configuración de la interfaz del MSTP**

Tipos de STP

El STP protege al dominio de difusión de capa 2 de las tormentas de difusión, para ello configura selectivamente los enlaces en modo en espera, para evitar bucles. En el modo de espera, estos enlaces dejan de transferir datos de usuario temporalmente. Una vez que se modifica la topología para posibilitar la transferencia de datos, los enlaces se reactivan automáticamente.

Los bucles ocurren cuando existen rutas alternativas entre los hosts. En una red extendida, los bucles pueden hacer que los switches reenvíen el tráfico indefinidamente, lo que provoca una mayor carga de tráfico y una menor eficiencia de la red.

STP proporciona una topología de árbol para cualquier configuración de switches y enlaces de interconexión, y crea una ruta única entre las estaciones de extremo de una red, con lo que se eliminan los bucles.

El dispositivo admite las siguientes versiones de protocolo del árbol de expansión:

- STP clásico: proporciona una sola ruta entre dos estaciones de extremo, lo que evita y elimina los bucles.
- STP rápido (RSTP): detecta las topologías de red para proporcionar una convergencia más rápida del árbol de expansión. Tiene mayor eficacia cuando la topología de red tiene una estructura de árbol por naturaleza y, por lo tanto, es posible que la convergencia sea más rápida. RSTP está activado de manera predeterminada.
- El STP múltiple (MSTP) está basado en RSTP. Detecta los bucles de capa 2 e intenta mitigarlos al evitar que el puerto involucrado transmita tráfico. Dado que los bucles existen por dominio de capa 2, puede ocurrir una situación en la que haya un bucle en la VLAN A y no haya uno en la VLAN B. Si las dos VLAN están en el puerto X, y STP desea mitigar el bucle, detiene el tráfico en todo el puerto, incluido el tráfico en la VLAN B.

  El MSTP soluciona este problema al activar varias instancias de STP, de modo que sea posible detectar y mitigar los bucles en cada instancia de manera independiente. Al asociar las instancias con las VLAN, cada instancia se vincula con el dominio de capa 2 en el que realiza la detección y mitigación de bucles. Esto permite detener un puerto en una instancia, como el tráfico de la VLAN A que está provocando un bucle, mientras el tráfico puede permanecer activo en otro dominio donde no se detectó un bucle, como en la VLAN B.

Estado y configuración global del STP

La página Estado y configuración global del STP contiene parámetros para habilitar STP, RSTP o MSTP.

Use las páginas Configuración de la interfaz del STP, Configuración de la interfaz del RSTP y Propiedades MSTP para configurar cada modo, respectivamente.

Para establecer la configuración global y el estado de STP:

PASO 1 Haga clic en **Árbol de expansión** > **Estado y configuración global del STP**.

PASO 2 Ingrese los parámetros.

Configuración global:

- **Estado de árbol de expansión**: seleccione para activar en el dispositivo.
- **Protección de bucle invertido de STP**: seleccione para activar la protección de bucle invertido en el dispositivo.
- **Modo de operación del STP**: seleccione un modo STP.

- **Tratamiento de las BPDU**: seleccione la forma en que se manejan los paquetes de BPDU (Bridge Protocol Data Unit, unidad de datos de protocolo de puente) cuando STP está desactivado en el puerto o el dispositivo. Las BPDU se utilizan para transmitir información del árbol de expansión.
  - *Filtrado*: se filtran los paquetes BPDU cuando el árbol de expansión está desactivado en una interfaz.
  - *Inundación*: se envían los paquetes BPDU en forma masiva cuando el árbol de expansión está desactivado en una interfaz.
- **Valores predet. del costo de trayecto**: se selecciona el método utilizado para asignar costos de trayecto predeterminados a los puertos STP. El costo de trayecto predeterminado asignado a una interfaz varía según el método seleccionado.
  - *Breve*: se especifica el intervalo del 1 al 65 535 para los costos de ruta del puerto.
  - *Prolongado*: se especifica el intervalo del 1 al 200 000 000 para los costos de ruta del puerto.

Configuración del puente:

- **Prioridad**: se establece el valor de prioridad del puente. Luego de intercambiar BPDU, el dispositivo con la menor prioridad se convierte en el puente raíz. En el caso de que todos los puentes usen la misma prioridad, entonces se utilizan sus direcciones MAC para determinar el puente raíz. El valor de prioridad del puente se proporciona en incrementos de 4096. Por ejemplo, 4096, 8192, 12 288, y así sucesivamente.
- **Tiempo de saludo**: establezca el intervalo (en segundos) que espera un puente raíz entre mensajes de configuración.
- **Tiempo máximo**: establezca el intervalo (en segundos) que puede esperar el dispositivo sin recibir un mensaje de configuración, antes de intentar redefinir su propia configuración.
- **Retraso de reenvío**: establezca el intervalo (en segundos) que un puente permanece en estado de aprendizaje antes de reenviar paquetes. Para obtener más información, consulte **Configuración de interfaz del árbol de expansión**.

Raíz designada:

- **ID de puente**: la prioridad del puente combinada con la dirección MAC del dispositivo.
- **ID de puente raíz**: la prioridad del puente raíz combinada con la dirección MAC del puente raíz.
- **Puerto raíz**: el puerto que ofrece la ruta de menor costo de este puente al puente raíz. (Esto es relevante cuando el puente no es la raíz).
- **Costo del trayecto raíz**: el costo del trayecto desde este puente a la raíz.
- **Conteo de cambios de topología**: la cantidad total de cambios de la topología de STP que ocurrieron.

- **Último cambio de topología**: el intervalo de tiempo que transcurrió desde el último cambio de topología. El tiempo aparece con el formato días/horas/minutos/segundos.

PASO 3 Haga clic en **Aplicar**. La configuración global de STP se escribe en el archivo Configuración en ejecución.

Configuración de interfaz del árbol de expansión

En la página Configuración de la interfaz del STP, puede configurar STP por puerto y ver la información que aprendió el protocolo, como el puente designado.

La configuración definida que se ingresa es válida para todos los tipos de protocolo STP.

Para configurar STP en una interfaz:

PASO 1 Haga clic en **Árbol de expansión** > **Configuración de interfaz STP**.

PASO 2 Seleccione una interfaz, y haga clic en **Editar**.

PASO 3 Ingrese los parámetros

- **Interfaz**: seleccione el puerto o LAG en el que se configura el árbol de expansión.
- **STP**: se activa o desactiva STP en el puerto.
- **Puerto de borde**: se activa o desactiva Enlace rápido en el puerto. Si el modo Enlace rápido está activado en un puerto, el puerto se coloca automáticamente en Estado de reenvío cuando el enlace del puerto está activo. Enlace rápido optimiza la convergencia del protocolo STP. Las opciones son:
  - *Habilitar*: se activa Enlace rápido inmediatamente.
  - *Auto*: se activa Enlace rápido unos segundos después de que se activa la interfaz. Esto permite que STP resuelva los bucles antes de activar Enlace rápido.
  - *Deshabilitar*: se desactiva Enlace rápido.

  NOTA Se recomienda configurar el valor en Automático para que el dispositivo configure el puerto en modo de enlace rápido en caso que un host se conecte a este o para que lo configure como un puerto STP normal si se conecta a otro dispositivo. Esto ayudará a evitar bucles.
- **Protección de raíz**: activa o desactiva la protección de raíz en el dispositivo. La opción de protección de raíz proporciona una forma de imponer la ubicación del puente del router en la red.

La Protección de raíz garantiza que el puerto en el cual se habilite esta opción sea el puerto designado. Por lo general, todos los puertos con puente raíz son puertos designados, a menos que uno o más puertos del puente raíz estén conectados. Si el puente recibe BPDU superiores en un puerto con protección de raíz habilitada, la Protección de raíz mueve el puerto a un estado STP de no concordancia con la raíz. Este estado de no concordancia con la raíz es el mismo que un estado de escucha. No se reenvía tráfico a través de este puerto. De este modo, el protector de raíz impone la ubicación del puente raíz.

- **Protección BPDU**: habilita o deshabilita la función de Protección de la unidad de datos del protocolo puente (BPDU, Bridge Protocol Data Unit) del puerto.

  La protección BPDU lo habilita para imponer los límites del dominio STP y mantener predecible de la topología activa. Los dispositivos detrás de los puertos que tengan habilitada la protección BPDU no podrán influenciar la topología STP. En el momento de la recepción de BPDU, la función de protección de BPDU inhabilita el puerto que tiene configurado BPDU. En este caso, se recibirá un mensaje de BPDU y se generará una trampa SNMP adecuada.

- **Tratamiento de las BPDU**: seleccione la forma en que se manejan los paquetes de BPDU (Bridge Protocol Data Unit, unidad de datos de protocolo de puente) cuando STP está desactivado en el puerto o el dispositivo. Las BPDU se utilizan para transmitir información del árbol de expansión.
  - *Utilizar configuración global*: seleccione esta opción para usar la configuración definida en la página Configuración global y de estado de STP.
  - *Filtrado*: se filtran los paquetes BPDU cuando el árbol de expansión está desactivado en una interfaz.
  - *Inundación*: se envían los paquetes BPDU en forma masiva cuando el árbol de expansión está desactivado en una interfaz.
- **Costo de trayecto**: establezca la contribución del puerto al costo del trayecto raíz o utilice el costo predeterminado que genera el sistema.
- **Prioridad**: establezca el valor de la prioridad del puerto. El valor de la prioridad influye en la elección del puerto cuando un puente tiene dos puertos conectados en un bucle. La prioridad es un valor que oscila entre 0 y 240, configurado en incrementos de 16.
- **Estado del puerto**: se muestra el estado actual de STP de un puerto.
  - *Deshabilitado*: el STP está desactivado en el puerto. El puerto reenvía el tráfico mientras aprende direcciones MAC.
  - *Bloqueo*: el puerto está bloqueado y no puede reenviar tráfico (con la excepción de datos de BPDU) ni aprender direcciones MAC.
  - *Escucha*: el puerto está en modo de escucha. El puerto no puede reenviar tráfico ni aprender direcciones MAC.

  - *Aprendizaje*: el puerto está en modo de aprendizaje. El puerto no puede reenviar tráfico, pero puede aprender nuevas direcciones MAC.
  - *Reenvío*: el puerto está en modo de reenvío. El puerto puede reenviar tráfico y aprender nuevas direcciones MAC.
- **ID de puente designado**: se muestra la prioridad del puente y la dirección MAC del puente designado.
- **ID de puerto designado**: se muestra la prioridad y la interfaz del puerto seleccionado.
- **Costo designado**: se muestra el costo del puerto que participa en la topología de STP. Los puertos con menor costo tienen menos probabilidades de ser bloqueados si STP detecta bucles.
- **Transiciones de reenvío**: se muestra el número de veces que el puerto cambió del estado **Bloqueo** al estado **Reenvío**.
- **Velocidad**: se muestra la velocidad del puerto.
- **LAG**: se muestra el LAG al que pertenece el puerto. Si un puerto es miembro de un LAG, la configuración del LAG invalida la configuración del puerto.

PASO 4 Haga clic en **Aplicar**. La configuración de la interfaz se escribe en el archivo Configuración en ejecución.

Configuración del árbol de expansión rápido

El Protocolo de árbol de expansión rápido (RSTP) permite una convergencia del STP más rápida, sin tener que crear bucles de reenvío.

En la página Configuración de la interfaz del RSTP, puede configurar RSTP por puerto. La configuración realizada en esta página está activa cuando el modo STP global está configurado en RSTP o MSTP.

Para ingresar la configuración de RSTP:

PASO 1 Haga clic en **Árbol de expansión** > **Estado y configuración global del STP**. Active **RSTP**.

PASO 2 Haga clic en **Árbol de expansión** > **Configuración de interfaz de RSTP**. Se abre la página Configuración de la interfaz del RSTP:

PASO 3 Seleccione un puerto.

NOTA La opción Activar migración de protocolo solo está disponible luego de seleccionar el puerto conectado al socio del puente que se está probando.

PASO 4 Si se detecta un socio de enlace a través de STP, haga clic en **Activar migración de protocolo** para ejecutar una prueba de migración de protocolo. Esta detecta si el socio de enlace que usa STP aún existe y, si es así, si migró a RSTP o MSTP. Si aún existe como un enlace STP, el dispositivo continúa comunicándose con él a través de STP. En caso contrario, si migró a RSTP o MSTP, el dispositivo se comunica con él a través de RSTP o MSTP, respectivamente.

PASO 5 Seleccione una interfaz, y haga clic en **Editar**.

PASO 6 Ingrese los parámetros:

- **Interfaz**: establezca la interfaz y especifique el puerto o el LAG donde se configurará RSTP.
- **Estado administrativo punto a punto**: defina el estado del enlace punto a punto. Los puertos definidos como dúplex completos se consideran enlaces de puerto punto a punto.
  - *Habilitar*: este puerto es un puerto de borde RSTP cuando esta función está activada y lo lleva al modo de reenvío rápidamente (en general, en menos de 2 segundos).
  - *Deshabilitar*: este puerto no se considera punto a punto para RSTP, lo que significa que STP funciona en él a velocidad normal, en vez de a velocidad rápida.
  - *Automático*: determina automáticamente el estado del dispositivo a través de BPDU de RSTP.
- **Estado operativo punto a punto**: muestra el estado operativo punto a punto si la opción **Estado administrativo punto a punto** está configurada en Auto.
- **Rol**: muestra el rol del puerto que STP asignó para proporcionar trayectos STP. Los roles posibles son:
  - *Raíz*: trayecto de menor costo para reenviar paquetes al puente raíz.
  - *Designado*: la interfaz a través de la que el puente está conectado a la LAN, que proporciona el trayecto de menor costo desde la LAN hasta el puente raíz.
  - *Alternativo*: proporciona un trayecto alternativo al puente raíz desde la interfaz raíz.
  - *De respaldo*: proporciona un trayecto de respaldo para el trayecto del puerto designado hacia las hojas del árbol de expansión. Esto provee una configuración en la cual dos puertos están conectados en un bucle a través de un enlace punto a punto. Los puertos de respaldo también se usan cuando una LAN tiene dos o más conexiones establecidas con un segmento compartido.
  - *Deshabilitado*: el puerto no participa en el árbol de expansión.
- **Modo**: se muestra el modo actual del árbol de expansión: STP o STP clásico.

- **Estado operativo de enlace rápido**: se muestra si el Enlace rápido (puerto de borde) está habilitado, deshabilitado o en modo automático para la interfaz. Los valores son:
  - *Habilitado*: enlace rápido está activado.
  - *Deshabilitado*: enlace rápido está desactivado.
  - *Auto*: se activa el modo Enlace rápido unos segundos después de que se activa la interfaz.
- **Estado de puerto**: se muestra el estado RSTP en el puerto específico.
  - *Deshabilitado*: el STP está desactivado en el puerto.
  - *Bloqueo*: el puerto está bloqueado y no puede reenviar tráfico ni aprender direcciones MAC.
  - *Escucha*: el puerto está en modo de escucha. El puerto no puede reenviar tráfico ni aprender direcciones MAC.
  - *Aprendizaje*: el puerto está en modo de aprendizaje. El puerto no puede reenviar tráfico, pero puede aprender nuevas direcciones MAC.
  - *Reenvío*: el puerto está en modo de reenvío. El puerto puede reenviar tráfico y aprender nuevas direcciones MAC.

PASO 7 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Árbol de expansión múltiple

El Protocolo de árbol de expansión múltiple (MSTP) se usa para separar el estado del puerto STP en diversos dominios (en distintas VLAN). Por ejemplo, mientras el puerto A está bloqueado en una instancia de STP debido a un bucle en la VLAN A, el mismo puerto puede colocarse en estado de reenvío en otra instancia de STP. La página Propiedades MSTP le permite definir la configuración global de MSTP.

Para configurar MSTP:

1. Establezca el modo de operación de STP en MSTP, como se describe en la página **Estado y configuración global del STP**.
2. Defina las instancias de MSTP. Cada instancia de MSTP calcula y crea una topología libre de bucles para enviar los paquetes a través del puente desde las VLAN asignadas a la instancia. Consulte la sección **VLAN a una instancia de MSTP**.
3. Decida qué instancia de MSTP estará activa en qué VLAN y asocie esas instancias de MSTP a las VLAN como corresponda.

4. Configure los atributos de MSTP a través de:
   - **Propiedades MSTP**
   - **Configuración de instancia MSTP**
   - **VLAN a una instancia de MSTP**

Propiedades MSTP

El MSTP global configura un árbol de expansión independiente para cada grupo de VLAN y bloquea todas las rutas alternativas posibles a excepción de una dentro de cada árbol de expansión. El MSTP permite formar regiones de MST que pueden ejecutar varias instancias de MST (MSTI). Varias regiones y otros puentes STP se interconectan a través de un solo árbol de expansión común (CST).

El MSTP es totalmente compatible con los puentes RSTP, en el sentido de que una BPDU MSTP puede ser interpretada por un puente RSTP como una BPDU RSTP. Esto no solo permite la compatibilidad con los puentes RSTP sin cambios de configuración, sino que también hace que los puentes RSTP fuera de una región MSTP vean la región como un solo puente RSTP, independientemente de la cantidad de puentes MSTP dentro de la región en sí.

Para que haya uno o más switches en la misma región de MST, deben tener la misma asignación de VLAN a instancia de MST, el mismo número de revisión de configuración y el mismo nombre de región.

A los switches que deben estar en la misma región de MST nunca los separan switches de otra región de MST. Si se los separa, la región se convierte en dos regiones independientes.

Esta asignación se puede realizar en la página Asignación de VLAN a instancia MSTP.

Utilice esta página si el sistema opera en modo MSTP.

Para definir MSTP:

PASO 1 Haga clic en **Árbol de expansión** > **Estado y configuración global del STP**. Active MSTP.

PASO 2 Haga clic en **Árbol de expansión** > **Propiedades de MSTP**.

PASO 3 Ingrese los parámetros.

- **Nombre de región**: defina el nombre de una región MSTP.
- **Revisión**: defina un número de 16 bits sin firmar que identifique la revisión de la configuración de MST actual. El intervalo del campo oscila entre 0 y 65535.

- **Saltos máx.**: establezca el total de saltos que ocurren en una región específica antes de descartar la BPDU. Una vez que se descarta la BPDU, la información del puerto caduca. El intervalo del campo oscila entre 1 y 40.
- **Maestro IST**: se muestra el maestro de la región.

PASO 4 Haga clic en **Aplicar**. Se definen las propiedades de MSTP y se actualiza el archivo Configuración en ejecución.

VLAN a una instancia de MSTP

En la página Asignación de VLAN a instancia MSTP, puede asignar cada VLAN a una instancia de árbol de expansión múltiple (MSTI). Para que los dispositivos estén en la misma región, deben tener la misma asignación de VLAN a MSTI.

NOTA La misma MSTI puede asignarse a más de una VLAN, pero cada VLAN solo puede tener una instancia de MST vinculada.

La configuración en esta página (y todas las páginas de MSTP) se aplica si el modo STP del sistema es MSTP.

En los switches de la serie 300, se pueden definir hasta siete instancias de MST (predefinidas de 1 a 7), además de la instancia cero.

Para aquellas VLAN que no se asignen explícitamente a una de las instancias de MST, el switch las asigna automáticamente al CIST (árbol de expansión interno y común). La instancia de CIST es la instancia de MST 0.

Para asignar VLAN a instancias de MST:

PASO 1 Haga clic en **Árbol de expansión** > **Asignación de VLAN a instancia MSTP**.

En la página Asignación de VLAN a instancia MSTP, aparecen los siguientes campos:

- **ID de instancias de MSTP**: se muestran todas las instancias de MSTP.
- **VLAN**: se muestran todas las VLAN que pertenecen a la instancia de MST.

PASO 2 Para agregar una VLAN a una instancia de MSTP, seleccione la instancia de MST y haga clic en **Editar**.

PASO 3 Ingrese los parámetros:

- **ID de instancias de MSTP**: seleccione la instancia de MST.

- **VLAN**: defina las VLAN que se asignan a esta instancia de MST.
- **Acción**: defina si desea añadir (asignar) (**Añadir**) la VLAN a la instancia de MST o eliminarla (**Eliminar**).

PASO 4 Haga clic en **Aplicar**. Se definen las asignaciones de VLAN de MSTP y se actualiza el archivo Configuración en ejecución.

Configuración de instancia MSTP

En la página Configuración de instancia MSTP puede configurar y ver los parámetros por instancia de MST. Este es el equivalente por instancia del *Establecimiento del estado y configuración global del STP*.

Para ingresar la configuración de la instancia de MSTP:

PASO 1 Haga clic en **Árbol de expansión** > **Configuración de Instancias de MSTP**.

PASO 2 Ingrese los parámetros.

- **ID de instancia**: seleccione una instancia de MST para ver y definir.
- **VLAN incluida**: se muestran las VLAN asignadas a la instancia seleccionada. La asignación predeterminada es que todas las VLAN se asignan a la instancia del árbol de expansión interno y común (CIST) (instancia 0).
- **Prioridad de puente**: establezca la prioridad de este puente para la instancia de MST seleccionada.
- **ID de puente de raíz designado**: se muestra la prioridad y la dirección MAC del puente raíz para la instancia de MST.
- **Puerto de raíz**: se muestra el puerto raíz de la instancia seleccionada.
- **Costo de ruta a raíz**: se muestra el costo del trayecto de la instancia seleccionada.
- **ID de puente**: se muestra la prioridad del puente y la dirección MAC de este dispositivo para la instancia seleccionada.
- **Saltos restantes**: se muestra el número de saltos que faltan hasta el próximo destino.

PASO 3 Haga clic en **Aplicar**. Se define la configuración de la instancia de MST y se actualiza el archivo Configuración en ejecución.

Configuración de la interfaz del MSTP

En la página Configuración de interfaz de la MSTP puede establecer la configuración de MSTP de los puertos para cada instancia de MST y ver la información que el protocolo aprendió actualmente, como el puente designado por instancia de MST.

Para configurar los puertos en una instancia de MST:

PASO 1 Haga clic en **Árbol de expansión** > **Configuración de interfaz de MSTP**.

PASO 2 Ingrese los parámetros.

- **Instancia es igual a**: seleccione la instancia de MSTP que desea configurar.
- **Tipo de interfaz es igual a**: seleccione si desea ver la lista de puertos o LAG.

PASO 3 Haga clic en **Ir**. Se muestran los parámetros de MSTP para las interfaces en la instancia.

PASO 4 Seleccione una interfaz, y haga clic en **Editar**.

PASO 5 Ingrese los parámetros.

- **ID de instancia**: seleccione la instancia de MST que desea configurar.
- **Interfaz**: seleccione la interfaz para la que desea definir la configuración de la MSTI.
- **Prioridad de interfaz**: establezca la prioridad del puerto para la interfaz especificada y la instancia de MST.
- **Costo de trayecto**: establezca la contribución del puerto al costo del trayecto raíz en el cuadro de texto **Definido por el usuario** o seleccione **Usar predeterminados** para usar el valor predeterminado.
- **Estado de puerto**: se muestra el estado de MSTP del puerto específico en una instancia de MST específica. Los parámetros se definen como:
  - *Desactivado*: STP está desactivado.
  - *Bloqueo*: el puerto en esta instancia está bloqueado y no puede reenviar tráfico (con la excepción de datos BPDU) ni aprender direcciones MAC.
  - *Escucha*: el puerto en esta instancia está en modo de escucha. El puerto no puede reenviar tráfico ni aprender direcciones MAC.
  - *Aprendizaje*: el puerto en esta instancia está en modo de aprendizaje. El puerto no puede reenviar tráfico, pero puede aprender nuevas direcciones MAC.
  - *Reenvío*: el puerto en esta instancia está en modo de reenvío. El puerto puede reenviar tráfico y aprender nuevas direcciones MAC.
  - *Límite*: el puerto en esta instancia es un puerto límite. Hereda el estado a partir de la instancia 0 y puede verse en la página Configuración de la interfaz del STP.

- **Rol de puerto**: se muestra el rol del puerto o LAG, por puerto o LAG por instancia, que asignó el algoritmo MSTP para proporcionar rutas STP:
  - *Raíz*: el reenvío de paquetes a través de esta interfaz proporciona la ruta de menor costo para reenviar paquetes al dispositivo raíz.
  - *Designada*: la interfaz a través de la que el puente está conectado a la LAN, que proporciona el menor costo del trayecto raíz desde la LAN hasta el puente raíz para la instancia de MST.
  - *Alternativa*: la interfaz proporciona una ruta alternativa al dispositivo raíz desde la interfaz raíz.
  - *Respaldo*: la interfaz proporciona una ruta de respaldo para la ruta del puerto designado hacia las hojas del árbol de expansión. Los puertos de respaldo tienen lugar cuando dos puertos están conectados en un bucle a través de un enlace punto a punto. También existen cuando una LAN tiene dos o más conexiones establecidas con un segmento compartido.
  - *Desactivado*: la interfaz no participa en el árbol de expansión.
  - *Límite*: el puerto en esta instancia es un puerto límite. Hereda el estado a partir de la instancia 0 y puede verse en la página Configuración de la interfaz del STP.
- **Modo**: se muestra el modo actual del árbol de expansión de la interfaz.
  - Si el socio de enlace está usando MSTP o RSTP, el modo de puerto que se visualiza es RSTP.
  - Si el socio de enlace está usando STP, el modo de puerto que se visualiza es STP.
- **Tipo**: se muestra el tipo de MST del puerto.
  - *Puerto límite*: un puerto límite vincula puentes de MST a una LAN en una región remota. Si el puerto es un puerto límite, también indica si el dispositivo en el otro lado del enlace está funcionando en modo RSTP o STP.
  - *Interno*: el puerto es interno.
- **ID del puente designado**: se muestra el número de ID del puente que conecta el enlace o la LAN compartida con la raíz.
- **ID del puerto designado**: se muestra el número de ID del puerto en el puente designado que conecta el enlace o la LAN compartida con la raíz.
- **Costo designado**: se muestra el costo del puerto que participa en la topología de STP. Los puertos con menor costo tienen menos probabilidades de ser bloqueados si STP detecta bucles.
- **Saltos restantes**: se muestran los saltos que faltan hasta el próximo destino.
- **Transiciones de reenvío**: se muestra el número de veces que el puerto cambió del estado de reenvío al estado de bloqueo.

PASO 6 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

16

Administración de tablas de direcciones MAC

Esta sección describe cómo añadir direcciones MAC al sistema. Abarca los siguientes temas:

- **Direcciones MAC estáticas**
- **Direcciones MAC dinámicas**
- **Direcciones MAC reservadas**

Existen dos tipos de direcciones MAC: estática y dinámica. Según el tipo, las direcciones MAC se almacenan en la tabla de *Direcciones estáticas* o en la tabla de *Direcciones dinámicas*, junto con la información de puertos y VLAN.

El usuario es quien configura las direcciones estáticas; por lo tanto, no caducan.

Una nueva dirección MAC de origen que aparezca en la trama de llegada al dispositivo se agregará a la Tabla de direcciones dinámicas. Esta dirección MAC se retendrá para un período de tiempo configurable. Si otra trama con la misma dirección MAC de origen no llega al dispositivo antes de que caduque ese tiempo, la entrada MAC se elimina (caduca) de la tabla.

Cuando una trama llega al dispositivo, el dispositivo busca una dirección MAC de destino que coincida o se corresponda con una entrada de la tabla de direcciones estáticas o dinámicas. Si se encuentra una coincidencia, la trama se marca para salir por un puerto específico de la tabla. Si las tramas se envían a una dirección MAC que no se encuentra en las tablas, se transmiten/difunden a todos los puertos de la VLAN relevante. Tales tramas se conocen como tramas de unidifusión desconocidas.

El dispositivo admite un máximo de 8000 direcciones MAC estáticas y dinámicas.

Direcciones MAC estáticas

Las direcciones MAC se asignan a una VLAN y una interfaz física específicas del dispositivo. Si esta dirección se detectara en otra interfaz, se ignorará y no se escribirá en la tabla de direcciones.

Para definir una dirección estática:

PASO 1 Haga clic en **Tablas de direcciones MAC > Direcciones estáticas**.

La página Direcciones estáticas contiene las direcciones estáticas que se encuentran definidas actualmente.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **ID de VLAN**: seleccione el ID de la VLAN para el puerto.
- **Dirección MAC**: ingrese la dirección MAC de interfaz.
- **Interfaz**: seleccione una interfaz (puerto o LAG) para la entrada.
- **Estado**: seleccione cómo tratar la entrada. Las opciones son:
  - *Permanente*: el sistema nunca elimina esta dirección MAC. Si la dirección MAC estática se guarda en la dirección de inicio, se conservará luego del reinicio.
  - *Eliminar o restablecer*: se elimina la dirección MAC estática cuando se restablece el dispositivo.
  - *Eliminar en tiempo de espera*: la dirección MAC se elimina cuando caduca.
  - *Seguro*: la dirección MAC es segura cuando la interfaz está en el modo de bloqueo clásico (consulte la sección **Configuración de la seguridad de puertos**).

PASO 4 Haga clic en **Aplicar**. Aparece una nueva entrada en la tabla.

Direcciones MAC dinámicas

La Tabla de direcciones dinámicas (tabla de conexión en puente) contiene las direcciones MAC adquiridas mediante el control de las direcciones de origen de las tramas que ingresan al dispositivo.

Para evitar que esta tabla se desborde y hacer espacio para nuevas direcciones MAC, se borrará una dirección si no recibe tráfico correspondiente durante cierto período, conocido como tiempo de desactualización.

Configuración del tiempo de desactualización de direcciones MAC dinámicas

Para configurar el tiempo de desactualización para direcciones dinámicas:

PASO 1 Haga clic en **Tablas de direcciones MAC > Configuración de direcciones dinámicas**.

PASO 2 Ingrese el **Tiempo de desactualización**. El tiempo de desactualización es un valor entre el valor configurado por el usuario y dos veces ese valor menos 1. Por ejemplo, si ingresó 300 segundos, el tiempo de desactualización es entre 300 y 599 segundos.

PASO 3 Haga clic en **Aplicar**. Se actualiza el tiempo de desactualización.

Consulta a direcciones dinámicas

Para consultar por direcciones dinámicas:

PASO 1 Haga clic en **Tablas de direcciones MAC > Direcciones dinámicas**.

PASO 2 En el bloque *Filtro*, puede ingresar los siguientes criterios de consulta:

- **ID de VLAN**: ingrese el ID de VLAN para el que se consulta la tabla.
- **Dirección MAC**: ingrese la dirección MAC para la que se consulta la tabla.
- **Interfaz**: seleccione la interfaz para la que se consulta la tabla. La consulta puede buscar unidades/ranuras, LAG o puertos específicos.

PASO 3 Haga clic en **Ir**. Se consulta la tabla de direcciones MAC dinámicas y se muestran los resultados.

Para eliminar todas las direcciones MAC dinámicas, haga clic en **Borrar tabla**.

Direcciones MAC reservadas

Cuando el switch recibe una trama con una dirección MAC de destino que pertenece a un intervalo reservado (por estándar de IEEE), la trama puede descartarse o interligarse. La entrada en la Tabla para direcciones MAC reservadas puede especificar la dirección MAC reservada o la dirección MAC reservada y el tipo de trama:

Para añadir una entrada para una dirección MAC reservada:

PASO 1 Haga clic en **Tablas de direcciones MAC > Direcciones MAC reservadas**.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los valores para los siguientes campos:

- **Dirección MAC**: seleccione la dirección MAC para reservar.
- **Tipo de trama**: seleccione el tipo de trama según los siguientes criterios:
  - *Ethernet V2*: se aplica a los paquetes Ethernet V2 con la dirección MAC específica.
  - *LLC*: se aplica a paquetes de Logical Link Control (LLC, control de enlace lógico) con una dirección MAC específica.
  - *LLC-SNAP*: se aplica a paquetes Logical Link Control (control de enlace lógico)/Sub-Network Access Protocol (Protocolo de acceso a la subred) (LLC-SNAP) con una dirección MAC específica.
  - *Todos*: se aplica a todos los paquetes con la dirección MAC específica.
- **Acción**: seleccione una de las siguientes acciones a tomar con respecto al paquete entrante que coincide con los criterios seleccionados:
  - *Puente*: reenvíe el paquete a todos los miembros de la VLAN.
  - *Descartar*: elimine el paquete.

PASO 4 Haga clic en **Aplicar**. Se reserva una nueva dirección MAC.

17

Multidifusión

En esta sección se describe la función Reenvío de multidifusión y abarca los siguientes temas:

- **Reenvío multidifusión**
- **Propiedades de multidifusión**
- **Dirección de grupo MAC**
- **Direcciones IP de grupo de multidifusión**
- **Configuración de multidifusión IPv4**
- **Configuración de multidifusión IPv6**
- **Grupo de multidifusión IP de indagación IGMP/ML**
- **Puertos de router de multidifusión**
- **Reenviar todos**
- **Multidifusión sin registrar**

Reenvío multidifusión

El reenvío de multidifusión permite difundir información a uno o varios destinatarios. Las aplicaciones de multidifusión son útiles para difundir información a varios clientes, donde los clientes no requieren la recepción del contenido completo. Una de las aplicaciones típicas es un servicio como el de televisión por cable, donde los clientes pueden unirse a un canal en el medio de una transmisión y salir antes de que termine.

Los datos se envían solo a los puertos relevantes. Al reenviar los datos solo a los puertos relevantes, se conservan los recursos de host y ancho de banda en los enlaces.

De manera predeterminada, todas las tramas de multidifusión se envían en forma masiva a todos los puertos de la VLAN. Es posible reenviar de manera selectiva solo a los puertos relevantes y filtrar (descartar) la multidifusión en el resto de los puertos. Para eso, active el estado de filtrado de multidifusión de puente en la página Multidifusión > Propiedades.

Si el filtrado está activado, las tramas de multidifusión se reenvían a un subconjunto de los puertos en la VLAN relevante, según lo definido en la base de datos de reenvío de multidifusión (MFDB). El filtrado de multidifusión se aplica en todo el tráfico.

Una forma común de representar a los miembros de multidifusión es a través de la notación (S,G) donde la S es la (única) fuente que envía una secuencia de datos de multidifusión y la G es la dirección IPv4 o IPv6 de grupo. Si un cliente de multidifusión puede recibir tráfico de multidifusión de cualquier origen de un grupo de multidifusión específico, esto se guarda como (*,G).

Puede configurar una de las siguientes formas de reenviar tramas de multidifusión:

- **Dirección MAC de grupo**: se basa en la dirección MAC de destino en la trama Ethernet.

  NOTA Se pueden asignar una o más direcciones IP de grupo de multidifusión a una dirección MAC de grupo. El reenvío basado en la dirección MAC de grupo puede dar como resultado el reenvío de una secuencia de multidifusión IP a puertos sin un receptor para la secuencia.

- **Dirección IP del grupo**: se basa en la dirección IP de destino del paquete IP (*,G).
- **Dirección IP específica de origen del grupo**: se basa en la dirección IP de destino y en la dirección IP de origen del paquete IP (S,G).

(S,G) es compatible con IGMPv3 y MLDv2, mientras que IGMPv1/2 y MLDv1 solo admiten (*.G), que es solo el ID de grupo.

El dispositivo admite un máximo de 256 direcciones de grupo de multidifusión estáticas y dinámicas.

Se puede configurar solo una de estas opciones de filtrado por VLAN.

Configuración de multidifusión típica

Mientras los routers de multidifusión enrutan los paquetes de multidifusión entre subredes IP, los switches de capa 2 con capacidad de multidifusión reenvían paquetes de multidifusión a los nodos registrados dentro de una LAN o VLAN.

Una configuración típica incluye un router que reenvía las secuencias de multidifusión entre redes IP privadas o públicas, un dispositivo con capacidad de indagación IGMP/MLD y un cliente de multidifusión que desea recibir una secuencia de multidifusión. En esta configuración, el router envía consultas IGMP/MLD periódicamente.

Operación de multidifusión

En un servicio de multidifusión de capa 2, un switch de capa 2 recibe una sola trama dirigida a una dirección de multidifusión específica. y crea copias de la trama para transmitirla en cada puerto relevante.

Cuando el dispositivo está activado para indagación IGMP/MLD y recibe una trama de una secuencia de multidifusión, este la reenvía a todos los puertos que se hayan registrado para recibir la secuencia de multidifusión a través de mensajes de incorporación IGMP/MLD.

El sistema mantiene una lista de grupos de multidifusión para cada VLAN, y esto administra la información de multidifusión que cada puerto debe recibir. Los grupos de multidifusión y sus puertos receptores pueden configurarse estáticamente o aprenderse dinámicamente a través de la indagación de los protocolos IGMP o MLD.

Registro de multidifusión (indagación de IGMP/MLD)

El registro de multidifusión es el proceso de escuchar y responder a los protocolos de registro de multidifusión. Los protocolos disponibles son IGMP para IPv4 y MLD para IPv6.

Cuando un dispositivo tiene la indagación IGMP/MLD activada en una VLAN, analiza los paquetes IGMP/MLD que recibe de la VLAN conectada al dispositivo y los routers de multidifusión en la red.

Cuando un dispositivo aprende que un host usa mensajes IGMP/MLD para registrarse para recibir una secuencia de multidifusión, de manera optativa de un origen específico, el dispositivo agrega el registro a su MFDB.

A continuación se detallan las versiones admitidas:

- IGMP v1/v2/v3
- MLD v1/v2

NOTA El dispositivo admite la indagación IGMP/MLD solo en VLAN estáticas, no en VLAN dinámicas.

Cuando la indagación IGMP/MLD está habilitada en forma global o en una VLAN, todos los paquetes IGMP/MLD se reenvían a la CPU. La CPU analiza los paquetes entrantes y determina lo siguiente:

- Cuáles son los puertos que solicitan unirse a qué grupos de multidifusión en qué VLAN.
- Cuáles son los puertos conectados a los routers de multidifusión (Mrouters) que están generando consultas IGMP/MLD.
- Cuáles son los puertos que están recibiendo protocolos de consulta PIM, DVMRP, IGMP o MLD.

Estas VLAN aparecen en la página Indagación de IGMP/MLD.

Los puertos que solicitan unirse a un grupo de multidifusión específico emiten un informe IGMP/MLD que especifica los grupos a los que desea unirse el host. Como resultado, se crea una entrada de reenvío en la base de datos de reenvío de multidifusión.

Interrogador de indagación IGMP

El interrogador de indagación IGMP/MLD se utiliza para admitir un dominio de multidifusión de capa 2 de switch de indagación ante la ausencia de un router de multidifusión. Por ejemplo, donde un servidor local proporciona el contenido de multidifusión, pero el router (si existe) en esa red no admite la multidifusión.

El dispositivo puede configurarse como interrogador IGMP de respaldo, o en una situación donde no exista un interrogador IGMP común. El dispositivo no tiene todas las funciones de un interrogador IGMP.

Si el dispositivo está activado como interrogador IGMP, se inicia después de que hayan pasado 60 segundos sin que se haya detectado tráfico IGMP (consultas) de un router de multidifusión. Ante la presencia de otros interrogadores IGMP, el dispositivo puede (o no) dejar de enviar consultas, según los resultados del proceso de selección estándar de interrogadores.

La velocidad de la actividad del interrogador IGMP/MLD debe concordar con los switch habilitados para la indagación IGMP/MLD. Las consultas deben enviarse a una velocidad que concuerde con el tiempo de vencimiento latente de la tabla de indagaciones. Si las consultas se envían a una velocidad menor que el tiempo de vencimiento latente, el suscriptor no puede recibir los paquetes de multidifusión. Esto se realiza en la página Editar indagación IGMP/MLD.

Si no está activado el mecanismo de selección de interrogador IGMP/MLD, entonces el interrogador de indagación de IGMP/MLD tarda en enviar mensajes de consultas generales tras habilitarse por 60 segundos. Si no hay otro indagador, comenzará a enviar mensajes de consultas generales. Dejará de enviar mensajes de consultas generales si detecta a otro indagador.

El interrogador de indagación de IGMP/MLD reanudará el envío de mensajes de consultas generales si escucha otro interrogador por el siguiente intervalo:

Query passive interval = Robustness * Query Interval + 0.5*Query Response Interval.

NOTA Se recomienda desactivar el mecanismo de selección de interrogador de IGMP/MLD si hay un router de multidifusión IPM en la VLAN.

Propiedades de las direcciones de multidifusión

Las direcciones de multidifusión tienen las siguientes propiedades:

- Cada dirección IPv4 de multidifusión se encuentra en el intervalo 224.0.0.0 a 239.255.255.255.
- La dirección IPv6 de multidifusión es FF00:/8.
- Para asignar una dirección IP de grupo de multidifusión a una dirección de multidifusión de capa 2:
  - Para IPv4, la asignación se realiza tomando los 23 bits de bajo orden de la dirección IPv4 y añadiéndoselos al prefijo 01:00:5e. Como norma, los nueve bits superiores de la dirección IP se omiten, y las direcciones IP que solo difieran en el valor de estos bits superiores se asignan a la misma dirección de capa 2, ya que los 23 bits inferiores que se usan son idénticos. Por ejemplo,

234.129.2.3 se asigna a una dirección MAC de grupo de multidifusión 01:00:5e:01:02:03. Se pueden asignar hasta 32 direcciones IP de grupo de multidifusión a la misma dirección de capa 2.

- Para IPv6, esta asignación se realiza tomando los 32 bits de bajo orden de la dirección de multidifusión y añadiendo el prefijo 33:33. Por ejemplo, la dirección IPv6 de multidifusión FF00:1122:3344 se asigna a la dirección de multidifusión de capa 2 33:33:11:22:33:44.

Proxy IGMP/MLD

Proxy IGMP/MLD es un protocolo de multidifusión IP simple.

Utilizar Proxy IGMP/MLD para replicar el tráfico de multidifusión en dispositivos, como edgeboxes, puede simplificar enormemente el diseño y la implementación de esos dispositivos. Como no admite protocolos de enrutamiento de multidifusión más complejos, como la multidifusión con protocolo independiente (PIM) y el protocolo de enrutamiento de multidifusión del vector de distancia (DVMRP), reduce el costo de los dispositivos y la sobrecarga operativa. Otra de las ventajas es que permite que los dispositivos proxy sean independientes del protocolo de enrutamiento de multidifusión que utilizan los routers en el núcleo de la red. Por eso, los dispositivos proxy pueden implementarse fácilmente en cualquier red de multidifusión.

Árbol de Proxy IGMP/MLD

Proxy IGMP/MLD funciona en una tipología de árbol sencilla en la que no es necesario ejecutar un sólido protocolo de enrutamiento de multidifusión (por ejemplo, PIM). Basta con utilizar un protocolo de enrutamiento IPM simple que esté basado en obtener información de afiliación del grupo e información de afiliación del grupo proxy para reenviar paquetes de multidifusión en base a esa información.

El árbol debe configurarse manualmente con la designación de interfaces ascendentes y descendentes en cada dispositivo proxy. Además, debe configurarse el esquema de direccionamiento IP que se aplica a la topología de árbol de proxy para asegurar que el dispositivo proxy pueda seleccionar el interrogador IGMP/MLD y reenviar el tráfico de multidifusión. No debe haber otros routers de multidifusión aparte de los dispositivos proxy del árbol; también se prevé que la raíz del árbol esté conectada a una infraestructura de multidifusión más amplia.

Un dispositivo proxy que realiza reenvíos basados en IGMP/MLD tiene una sola interfaz ascendente y una o más interfaces descendentes. Esas designaciones se configuran de manera explícita; no hay un protocolo que determine el tipo de cada interfaz. Un dispositivo proxy realiza la parte de IGMP/MLD del router en sus interfaces descendentes, y la parte de IGMP/MLD del host en la interfaz ascendente.

Solo se admite un árbol.

Reglas de reenvío e interrogador

Se aplican las siguientes reglas:

- Un paquete de multidifusión que se reciba en la interfaz ascendente se reenviará a través de todas las interfaces descendentes que soliciten el paquete solo si el dispositivo proxy es el interrogador de las interfaces.
- Si el dispositivo proxy no es el interrogador de la interfaz, descartará los paquetes de multidifusión que se reciban en una interfaz descendente.
- El paquete de multidifusión que se reciba en una interfaz descendente donde el dispositivo proxy sea el interrogador se reenviará a través de la interfaz ascendente y de todas las interfaces descendentes que soliciten el paquete únicamente si el dispositivo proxy es el interrogador de las interfaces.

Protección de la interfaz descendente

De forma predeterminada, se reenvía el tráfico de multidifusión IP de una interfaz del árbol IGMP/MLD. Es posible desactivar el reenvío de tráfico de multidifusión IP que llega a las interfaces descendentes. Puede realizarse de forma global o en una interfaz descendente determinada.

Propiedades de multidifusión

Para habilitar el filtrado de multidifusión y seleccionar el método de reenvío:

PASO 1 Haga clic en **Multidifusión > Propiedades**.

PASO 2 Ingrese los parámetros.

- **Estado de filtrado de multidifusión de puente**: seleccione esta opción para habilitar el filtrado.
- **ID de VLAN**: seleccione el ID de la VLAN para configurar su método de reenvío.
- **Método de reenvío para IPv6**: defina uno de los siguientes método de reenvío para las direcciones IPv6: Dirección MAC de grupo, Dirección IP del grupo o Dirección IP específica de origen del grupo.
- **Método de reenvío para IPv4**: defina uno de los siguientes método de reenvío para las direcciones IPv4: Dirección MAC de grupo, Dirección IP del grupo o Dirección IP específica de origen del grupo.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Dirección de grupo MAC

En la página Direcciones MAC de grupo, se encuentran las siguientes funciones:

- Consultar y ver información de la MFDB (base de datos de reenvío de multidifusión) relacionada con un ID de VLAN específico o un grupo de direcciones MAC específico. Estos datos se adquieren en forma dinámica a través de la indagación IGMP/MLD o en forma estática mediante la entrada manual.
- Añadir o eliminar entradas estáticas a la MFDB que brinda información de reenvío estática basada en las direcciones MAC de destino.
- Mostrar una lista de todos los puertos/LAG que son miembros de cada grupo de direcciones MAC e ID de VLAN, e ingresar si el tráfico se reenvía a él o no.

Para definir y ver grupos de multidifusión MAC:

PASO 1 Haga clic en **Multidifusión > Dirección MAC de grupo**.

PASO 2 Ingrese los parámetros de filtro.

- **ID de VLAN igual a**: configure el ID de VLAN del grupo que desea ver.
- **Dirección MAC de grupo igual a**: configure la dirección MAC del grupo de multidifusión que desea ver. Si no se especifica una dirección MAC de grupo, la página contiene todas las direcciones MAC de grupo de la VLAN seleccionada.

PASO 3 Haga clic en **Ir** y aparecerán las direcciones MAC de grupo de multidifusión en el bloque inferior.

Se muestran las entradas que se crearon en esta página y en la página Dirección IP de grupo de multidifusión. Para las entradas que se crearon en la página Dirección IP de grupo de multidifusión, las direcciones IP se convierten en direcciones MAC.

PASO 4 Haga clic en **Añadir** para añadir una dirección MAC de grupo estática.

PASO 5 Ingrese los parámetros.

- **ID de VLAN**: se define el ID de la VLAN del nuevo grupo de multidifusión.
- **Dirección MAC de grupo**: se define la dirección MAC del nuevo grupo de multidifusión.

PASO 6 Haga clic en **Aplicar**. El grupo de multidifusión MAC se guarda en el archivo de configuración en ejecución.

Para configurar y ver el registro para las interfaces dentro del grupo, seleccione una dirección y haga clic en **Detalles**.

La página incluye:

- **ID de VLAN**: el ID de la VLAN del grupo de multidifusión.
- **Dirección MAC de grupo**: la dirección MAC del grupo.

PASO 7 Seleccione el puerto o LAG desde **Filtro: Tipo de interfaz**.

PASO 8 Haga clic en **Ir** para ver la afiliación de LAG o puerto de la VLAN.

PASO 9 Seleccione la forma en que cada interfaz está asociada con el grupo de multidifusión:

- **Estática**: la interfaz se asocia al grupo de multidifusión como un miembro estático.
- **Dinámico**: indica que la interfaz se añadió al grupo de multidifusión como resultado de indagación IGMP/MLD.
- **Prohibido**: especifica que este puerto tiene permitido unirse a este grupo de multidifusión en esta VLAN.
- **Ninguna**: se especifica que el puerto no es un miembro actual de este grupo de multidifusión en esta VLAN.

PASO 10 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

NOTA Las entradas que se crearon en la página Dirección IP de grupo de multidifusión no se pueden eliminar en esta página (aunque se seleccionen).

Direcciones IP de grupo de multidifusión

La página Dirección IP de grupo de multidifusión es similar a la página Direcciones MAC de grupo, excepto que los grupos de multidifusión están identificados por direcciones IP.

En la página Dirección IP de grupo de multidifusión, se puede realizar una consulta y agregar grupos de multidifusión IP.

Para definir y ver grupos de multidifusión IP:

PASO 1 Haga clic en **Multidifusión > Dirección IP de grupo de multidifusión**.

La página contiene todas las direcciones IP de grupo de multidifusión aprendidas mediante indagación.

PASO 2 Ingrese los parámetros requeridos para el filtrado.

- **ID de VLAN igual a**: defina el ID de la VLAN del grupo que desea ver.
- **Versión de IP igual a**: seleccione IPv6 o IPv4.
- **Dirección IP de grupo de multidifusión igual a**: defina la dirección IP del grupo de multidifusión que desea ver. Esto es relevante solo cuando el modo de reenvío es (S, G).
- **Dirección IP de origen igual a**: defina la dirección IP de origen del dispositivo remitente. Si el modo es (S, G), ingrese el remitente S. Esto junto con la dirección IP de grupo es el ID del grupo de multidifusión (S, G) que se mostrará. Si el modo es (*.G), ingrese un * para indicar que el grupo de multidifusión solo está definido por destino.

PASO 3 Haga clic en **Ir**. Los resultados aparecen en el bloque inferior. Cuando Bonjour e IGMP están activados en el dispositivo en el modo del sistema Capa 2, aparece la dirección IP de multidifusión de Bonjour. Haga clic en **Añadir** para añadir una dirección IP de grupo de multidifusión estática.

PASO 4 Ingrese los parámetros.

- **ID de VLAN**: se define el ID de la VLAN del grupo que se añadirá.
- **Versión de IP**: seleccione el tipo de dirección IP.
- **Dirección IP de grupo de multidifusión**: defina la dirección IP del nuevo grupo de multidifusión.
- **Específica de origen**: indica que la entrada contiene un origen específico y añade la dirección en el campo Dirección IP de origen. En caso contrario, la entrada se añade como (*,G), una dirección IP de grupo de cualquier origen IP.
- **Dirección IP de origen**: se define la dirección de origen que se incluirá.

PASO 5 Haga clic en **Aplicar**. Se añade el grupo de multidifusión IP y se actualiza el dispositivo.

PASO 6 Para configurar y ver el registro de una dirección IP de grupo, seleccione una dirección y haga clic en **Detalles**.

Las opciones ID de VLAN, Versión IP, Dirección IP de grupo de multidifusión y Dirección IP de origen seleccionadas se muestran como de solo lectura en la parte superior de la pantalla. Usted puede seleccionar el tipo de filtro:

- **Tipo de interfaz igual a**: seleccione si desea ver puertos o LAG.

PASO 7 Seleccione el tipo de asociación para cada interfaz. Las opciones son las siguientes:

- **Estática**: la interfaz se asocia al grupo de multidifusión como un miembro estático.
- **Dinámica**: la interfaz se asocia al grupo de multidifusión como un miembro dinámico.
- **Prohibido**: se especifica que este puerto tiene prohibido unirse a este grupo en esta VLAN.
- **Ninguna**: indica que el puerto no es un miembro actual de este grupo de multidifusión en esta VLAN. Esta opción se selecciona de forma predeterminada hasta que se selecciona Estático o Prohibido.

PASO 8 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Configuración de multidifusión IPv4

En las siguientes páginas, se establece la configuración de multidifusión IPv4:

- **Configuración de la indagación IGMP**
- **Configuración de IGMP en una VLAN**

Configuración de la indagación IGMP

Para admitir el reenvío selectivo de multidifusión IPv4, se debe activar el filtrado de multidifusión de puente (en la página Multidifusión > Propiedades) y se debe activar la indagación IGMP de forma global y para cada VLAN relevante en la página Indagación IGMP.

Para activar la indagación IGMP e identificar al dispositivo como interrogador de indagación IGMP en una VLAN:

PASO 1 Haga clic en **Multidifusión** > **Configuración de multidifusión IPv4** > **Indagación IGMP**.

Cuando la opción Indagación IGMP está habilitada en forma global, el dispositivo que controla el tráfico de la red puede determinar qué hosts solicitaron recibir tráfico de multidifusión. El dispositivo realiza la indagación IGMP solo si la indagación IGMP y el filtrado de multidifusión de puente están activados.

PASO 2 Active o desactive las siguientes funciones:

- **Estado de indagación IGMP**: seleccione para activar la indagación IGMP de forma global en todas las interfaces.
- **Estado de indagación IGMP**: seleccione para activar el interrogador IGMP de forma global en todas las interfaces.

PASO 3 Para configurar proxy IGMP en una interfaz, seleccione una VLAN estática y haga clic en **Editar**. Ingrese los siguientes campos:

- **Estado de indagación IGMP**: seleccione para activar la indagación IGMP en la VLAN. El dispositivo controla el tráfico de la red para determinar los hosts que solicitaron recibir tráfico de multidifusión. El dispositivo realiza la indagación IGMP sólo si la indagación IGMP y el filtrado de multidifusión de puente están habilitados.
- **Aprendizaje automático de los puertos de Mrouter**: seleccione para activar la función de autoaprendizaje para el router de multidifusión.
- **Ausencia inmediata**: seleccione para que el conmutador pueda quitar una interfaz que envía un mensaje de ausencia desde la tabla de reenvío sin enviar primero las consultas generales basadas en MAC a la interfaz. Cuando se recibe de un host un mensaje de ausencia de grupo IGMP, el sistema elimina el puerto del host de la entrada de tabla. Después de que retransmite las consultas IGMP del router de multidifusión, elimina las entradas de manera periódica si no recibe ningún informe de miembros IGMP de los clientes de multidifusión. Cuando se activa esta opción, se reduce el tiempo que lleva bloquear el tráfico MLD innecesario enviado a un puerto del dispositivo.
- **Contador de consultas del último miembro**: cantidad de consultas IGMP específicas del grupo enviadas antes de que el dispositivo suponga que no hay más miembros para el grupo, en caso de que el dispositivo sea el interrogador elegido.
- **Estado del interrogador IGMP**: seleccione esta función para activarla. Esta función es obligatoria si no hay un router de multidifusión.
- **Elección del interrogador IGMP**: indica si está activada o desactivada la selección del interrogador IGMP. Si está activado el mecanismo de selección del interrogador IGMP, el interrogador de indagación de IGMP admite el mecanismo de selección del interrogador IGMP estándar que se indica en RFC3810.

  Si no está activado el mecanismo de selección del interrogador IGMP, el interrogador de indagación de IGMP demora el envío de mensajes de consultas generales durante 60 segundos después de que se habilita. Si no hay otro interrogador, comienza a enviar mensajes de consultas generales. Dejará de enviar mensajes de consultas generales si detecta a otro indagador. El interrogador de indagación de IGMP reanuda el envío de mensajes de consultas generales si escucha otro interrogador por un intervalo Query Passive equivalente a: Robustness * (Query Interval) + 0.5 * Query Response Interval.

- **Versión del interrogador IGMP**: seleccione la versión de IGMP que se usará si el dispositivo se convierte en el interrogador elegido. Seleccione IGMPv3 si hay switch o routers de multidifusión en la VLAN que realizan reenvíos de multidifusión IP específicos del origen. De lo contrario, seleccione IGMPv2.
- **Dirección IP de origen del interrogador**: seleccione la interfaz de origen del dispositivo que se usará en los mensajes enviados. En MLD, el sistema selecciona automáticamente esa dirección.

  NOTA Si se selecciona la opción Automática, el sistema toma la dirección IP de origen de la dirección IP definida en la interfaz de salida.

PASO 4 Seleccione una VLAN y haga clic en **Editar**.

PASO 5 Ingrese los parámetros antes descritos.

PASO 6 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

NOTA Se realizaron algunos cambios en la configuración de los temporizadores de indagación IGMP, tales como: Solidez de consultas, Intervalo de consultas, etc., no tienen efecto en los temporizadores que ya se crearon.

Configuración de IGMP en una VLAN

Para configurar IGMP en una VLAN específica:

PASO 1 Haga clic en **Multidifusión** > **Configuración de multidifusión IPv4 > Configuración de IGMP en una VLAN**.

Los campos a continuación se muestran para cada VLAN donde está habilitado IGMP:

- **Nombre de la interfaz**: VLAN donde se definió la indagación de IGMP.
- **Versión de IGMP del router**: indique la versión de indagación de IGMP.
- **Solidez de consultas**: ingrese la cantidad de pérdidas de paquetes previstas en un enlace.
- **Intervalo de consultas (seg.)**: ingrese el intervalo entre las consultas generales que se usará si este dispositivo es el interrogador elegido.
- **Intervalo máximo de respuesta a consultas (seg.)**: ingrese la demora utilizada para calcular el código de respuesta máximo insertado en las consultas generales periódicas.
- **Intervalo de consultas del último miembro (mseg.)**: ingrese la demora máxima de respuesta que se usará si el dispositivo no puede leer el valor de Tiempo de respuesta máx. de las consultas específicas del grupo que envía el interrogador elegido.

PASO 2 Seleccione una interfaz y haga clic en **Editar**. Ingrese los valores de los campos antes descritos.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Configuración de multidifusión IPv6

En las siguientes páginas, se establece la configuración de multidifusión IPv6:

- **Indagación MLD**
- **Configuración de MLD en una VLAN**

Indagación MLD

Para admitir el reenvío selectivo de multidifusión IPv6, se debe activar el filtrado de multidifusión de puente (en la página Multidifusión > Propiedades) y se debe activar la indagación MLD de forma global y para cada VLAN relevante en la página Indagación MLD.

Para habilitar la indagación MLD y configurarla en una VLAN:

PASO 1 Haga clic en **Multidifusión** > **Configuración de multidifusión IPv6 > Indagación MLD**.

Cuando la opción Indagación MLD está habilitada en forma global, el dispositivo que controla el tráfico de la red puede determinar qué hosts solicitaron recibir tráfico de multidifusión. El dispositivo realiza la indagación MLD solo si la indagación MLD y el filtrado de multidifusión de puente están activados.

PASO 2 Active o desactive las siguientes funciones:

- **Estado de indagación MLD**: seleccione para activar la indagación MLD de forma global en todas las interfaces.
- **Estado de indagación MLD**: seleccione para activar el interrogador MLD de forma global en todas las interfaces.

PASO 3 Para configurar proxy MLD en una interfaz, seleccione una VLAN estática y haga clic en **Editar**. Ingrese los siguientes campos:

- **Estado de indagación MLD**: seleccione para activar la indagación MLD en la VLAN. El dispositivo controla el tráfico de la red para determinar los hosts que solicitaron recibir tráfico de multidifusión. El dispositivo realiza la indagación MLD sólo cuando la indagación MLD y el filtrado de multidifusión de puente están activados.
- **Aprendizaje automático de los puertos de Mrouter**: seleccione para activar la función de autoaprendizaje para el router de multidifusión.

- **Ausencia inmediata**: seleccione para que el conmutador pueda quitar una interfaz que envía un mensaje de ausencia desde la tabla de reenvío sin enviar primero las consultas generales basadas en MAC a la interfaz. Cuando se recibe de un host un mensaje de ausencia de grupo MLD, el sistema elimina el puerto del host de la entrada de tabla. Después de que retransmite las consultas MLD del router de multidifusión, elimina las entradas de manera periódica si no recibe ningún informe de miembros MLD de los clientes de multidifusión. Cuando se activa esta opción, se reduce el tiempo que lleva bloquear el tráfico MLD innecesario enviado a un puerto del dispositivo.
- **Contador de consultas del último miembro**: cantidad de consultas MLD específicas del grupo enviadas antes de que el dispositivo suponga que no hay más miembros para el grupo, en caso de que el dispositivo sea el interrogador elegido.
  - *Usar solidez de consultas*: este valor está establecido en la página **Configuración de MLD en una VLAN**.
  - *Definido por el usuario*: ingrese un valor definido por el usuario.
- **Estado del interrogador MLD**: seleccione esta función para activarla. Esta función es obligatoria si no hay un router de multidifusión.
- **Elección del interrogador MLD**: indica si está activada o desactivada la selección del interrogador MLD. Si está activado el mecanismo de selección del interrogador MLD, el interrogador de indagación de MLD admite el mecanismo de selección del interrogador MLD estándar que se indica en RFC3810.

  Si no está activado el mecanismo de selección del interrogador MLD, el interrogador de indagación de MLD demora el envío de mensajes de consultas generales durante 60 segundos después de que se habilita. Si no hay otro interrogador, comienza a enviar mensajes de consultas generales. Dejará de enviar mensajes de consultas generales si detecta a otro indagador. El interrogador de indagación de MLD reanuda el envío de mensajes de consultas generales si escucha otro interrogador por un intervalo Query Passive equivalente a: Robustness * (Query Interval) + 0.5 * Query Response Interval.
- **Versión del interrogador MLD**: seleccione la versión de MLD que se usará si el dispositivo se convierte en el interrogador elegido. Seleccione MLDv2 si hay switches o routers de multidifusión en la VLAN que realizan reenvíos de multidifusión IP específicos-del origen. De lo contrario, seleccione MLDv1.

PASO 4 Seleccione una VLAN y haga clic en **Editar**.

PASO 5 Ingrese los parámetros antes descritos.

PASO 6 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

NOTA Se realizaron algunos cambios en la configuración de los temporizadores de indagación MLD, tales como: Solidez de consultas, Intervalo de consultas, etc., no tienen efecto en los temporizadores que ya se crearon.

Configuración de MLD en una VLAN

Para configurar MLD en una VLAN específica:

PASO 1 Haga clic en **Multidifusión** > **Configuración de multidifusión IPv6 > Configuración de MLD en una VLAN**.

Los campos a continuación se muestran para cada VLAN donde está habilitado:

- **Nombre de la interfaz**: VLAN para la que se muestra información de MLD.
- **Versión de MLD del router**: indique la versión de MLD del router.
- **Solidez de consultas**: ingrese la cantidad de pérdidas de paquetes previstas en un enlace.
- **Intervalo de consultas (seg.)**: ingrese el intervalo entre las consultas generales que se usará si este dispositivo es el interrogador elegido.
- **Intervalo máximo de respuesta a consultas (seg.)**: ingrese la demora utilizada para calcular el código de respuesta máximo insertado en las consultas generales periódicas.
- **Intervalo de consultas del último miembro (mseg.)**: ingrese la demora máxima de respuesta que se usará si el dispositivo no puede leer el valor de Tiempo de respuesta máx. de las consultas específicas del grupo que envía el interrogador elegido.

PASO 2 Para configurar una VLAN, selecciónela y haga clic en **Editar**. Ingrese los campos antes descritos.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Grupo de multidifusión IP de indagación IGMP/ML

En la página Grupo de multidifusión IP de indagación IGMP/ML, se muestran las direcciones IPv4 e IPv6 de grupo que se aprendieron de los mensajes IGMP/MLD.

Puede haber una diferencia entre la información de esta página y la que aparece en la página Direcciones MAC de grupo. Aquí tiene un ejemplo: Si suponemos que el sistema filtra según grupos basados en MAC y un puerto que solicitó unirse a los siguientes grupos de multidifusión 224.1.1.1 y 225.1.1.1, los dos se asignan a la misma dirección MAC de multidifusión 01:00:5e:01:01:01. En este caso, hay una sola entrada en la página de multidifusión MAC, pero dos en esta página.

Para realizar una consulta para un grupo de multidifusión IP:

PASO 1 Haga clic en **Multidifusión** > **Grupo de multidifusión IP de indagación IGMP/MLD**.

PASO 2 Establezca el tipo de grupo de indagación para el que desea realizar la búsqueda: IGMP o MLD.

PASO 3 Ingrese algunos o todos los siguientes criterios de filtrado de consulta:

- **Dirección de grupo igual a**: se define la dirección MAC o la dirección IP del grupo de multidifusión para la que se realizará la consulta.
- **Dirección de origen igual a**: se define la dirección del remitente para la que se realizará la consulta.
- **ID de VLAN igual a**: se define el ID de la VLAN para el que se realizará la consulta.

PASO 4 Haga clic en **Ir**. Se muestran los siguientes campos para cada grupo de multidifusión:

- **VLAN**: el ID de la VLAN.
- **Dirección de grupo**: la dirección MAC o la dirección IP del grupo de multidifusión.
- **Dirección de origen**: la dirección del remitente para todos los puertos especificados del grupo.
- **Puertos incluidos**: la lista de puertos de destino para la secuencia de multidifusión.
- **Puertos excluidos**: la lista de puertos no incluidos en el grupo.
- **Modo de compatibilidad**: la versión IGMP/MLD más antigua de registro de los hosts que el dispositivo recibe en la dirección IP de grupo.

Puertos de router de multidifusión

Un puerto de router de multidifusión (Mrouter) es aquel que se conecta a un router de multidifusión. El dispositivo incluye a los números de puertos del router de multidifusión cuando reenvía las secuencias de multidifusión y los mensajes de registro IGMP/MLD. Esto es necesario para que, a su vez, todos los routers de multidifusión puedan reenviar las secuencias de multidifusión y propagar los mensajes de registro a otras subredes.

Para configurar estadísticamente o ver los puertos detectados dinámicamente conectados al router de multidifusión:

PASO 1 Haga clic en **Multidifusión** > **Puerto de router de multidifusión**.

PASO 2 Ingrese algunos o todos los siguientes criterios de filtrado de consulta:

- **ID de VLAN igual a**: seleccione el ID de la VLAN para los puertos del router descritos.
- **Versión de IP igual a**: seleccione la versión de IP que admite el router de multidifusión.
- **Tipo de interfaz igual a**: seleccione si desea ver puertos o LAG.

PASO 3 Haga clic en **Ir**. Aparecerán las interfaces que coincidan con los criterios de consulta.

PASO 4 Seleccione el tipo de asociación para cada puerto o LAG. Las opciones son las siguientes:

- **Estático**: el puerto se configura estáticamente como un puerto de router de multidifusión.
- **Dinámico**: (solo mostrar) el puerto se configura dinámicamente como un puerto de router de multidifusión mediante una consulta MLD/IGMP. Para habilitar el aprendizaje dinámico de puertos de router de multidifusión, vaya a página **Multidifusión** > **Indagación IGMP** y a la página **Multidifusión** > **Indagación MLD**.
- **Prohibido**: este puerto no debe configurarse como un puerto de router de multidifusión, incluso si se reciben consultas IGMP o MLD en este puerto. Si se habilita Prohibido en un puerto, este puerto no aprenderá el Mrouter (es decir, en este puerto no estará habilitada la opción de aprendizaje automático de los puertos de Mrouter).
- **Ninguna**: el puerto no es un puerto de router de multidifusión actualmente.

PASO 5 Haga clic en **Aplicar** para actualizar el dispositivo.

Reenviar todos

La página Reenviar todos permite la configuración de los puertos o LAG que deben recibir toda la secuencia de multidifusión de una VLAN específica. Esta función requiere que el filtrado de multidifusión de puente esté activado en la página Propiedades. Si está desactivado, todo el tráfico de multidifusión se envía en forma masiva a todos los puertos del dispositivo.

Usted puede configurar estáticamente (manualmente) un puerto para reenviar todo, si los dispositivos que se conectan al puerto no admiten IGMP o MLD.

Los mensajes IGMP o MLD no se reenvían a los puertos definidos como *Reenviar todos*.

NOTA La configuración afecta solo a los puertos que son miembros de la VLAN seleccionada.

Para definir el reenvío de toda la multidifusión:

PASO 1 Haga clic en **Multidifusión** > **Reenviar todos**.

PASO 2 Defina lo siguiente:

- **ID de VLAN igual a**: el ID de la VLAN de los puertos/LAG que se van a mostrar.
- **Tipo de interfaz igual a**: defina si desea ver puertos o LAG.

PASO 3 Haga clic en **Ir**. Se muestra el estado de todos los puertos/LAG.

PASO 4 Seleccione el puerto/LAG que se definirá como Reenviar todos mediante los siguientes métodos:

- **Estático**: el puerto recibe todas las secuencias de multidifusión.
- **Prohibido**: los puertos no pueden recibir secuencias de multidifusión, incluso si la indagación IGMP/MLD designó al puerto para que se uniera a un grupo de multidifusión.
- **Ninguna**: el puerto no es un puerto Reenviar todos actualmente.

PASO 5 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Multidifusión sin registrar

Esta función puede utilizarse para garantizar que el cliente reciba sólo los grupos de multidifusión solicitados (registrados) y no otros que puedan transmitirse en la red (no registrados).

En general, las tramas de multidifusión sin registrar se reenvían a todos los puertos en la VLAN.

Usted puede seleccionar un puerto para que reciba o rechace (filtre) las secuencias de multidifusión sin registrar. La configuración es válida para cualquier VLAN de la que el puerto sea miembro (o vaya a ser miembro).

Para definir la configuración de multidifusión sin registrar:

PASO 1 Haga clic en **Multidifusión** > **Multidifusión sin registrar**.

PASO 2 Seleccione **Tipo de interfaz igual a**: seleccione si desea ver puertos o LAG.

PASO 3 Haga clic en **Ir**.

PASO 4 Defina lo siguiente:

- **Puerto/LAG**: muestra el puerto o el ID de LAG.
- Se muestra el estado de reenvío de la interfaz seleccionada. Los valores posibles son:
  - *Reenvío*: se habilita el reenvío de tramas de multidifusión sin registrar a la interfaz seleccionada.
  - *Filtrado*: se habilita el filtrado (rechazo) de tramas de multidifusión sin registrar en la interfaz seleccionada.

PASO 5 Haga clic en **Aplicar**. Se guarda la configuración y se actualiza el archivo Configuración en ejecución.

18

Configuración de IP

El usuario puede configurar manualmente las direcciones de interfaz IP, o éstas se configuran automáticamente mediante un servidor DHCP. Esta sección brinda información para definir las direcciones IP del dispositivo, ya sea manualmente o con un dispositivo como cliente DHCP.

Esta sección abarca los siguientes temas:

- **Información general**
- **Administración e interfaces IPv4**
- **Servidor DHCP**
- **Administración e interfaces IPv6**
- **Nombre de dominio**

Información general

Algunas funciones, descritas a continuación, solo están disponibles para el modo del sistema Capa 2 o Capa 3:

- En el modo del sistema Capa 2, el dispositivo opera como dispositivo preparado para-VLAN de Capa 2, y no tiene capacidades de enrutamiento.
- En el modo del sistema Capa 3, el dispositivo tiene capacidades de enrutamiento IP y las mismas capacidades del modo del sistema Capa 2. En este modo del sistema, un puerto de capa 3 conserva gran parte de la funcionalidad de capa 2, como el protocolo de árbol de expansión y la afiliación VLAN.

  En el modo del sistema Capa 3, el dispositivo no admite VLAN basada en MAC, asignación dinámica de VLAN, límite de velocidad de VLAN, protección contra negación de servicio de velocidad SYN ni reguladores avanzados de QoS (Quality of Service, calidad de servicio).

La configuración del dispositivo para que funcione en cualquiera de los dos modos se lleva a cabo en Administración > Configuración del sistema.

NOTA Para cambiar de un modo de sistema (capa) a otro (en dispositivos Sx500), es obligatorio reiniciar el dispositivo, y la configuración de arranque del switch será eliminada.

Direccionamiento IP de capa 2

En el modo del sistema de Capa 2, el dispositivo tiene hasta una dirección IPv4 y un máximo de dos interfaces IPv6 ("nativa" o túnel) en la VLAN de administración. Esta dirección IP y la puerta de enlace predeterminada se pueden configurar manualmente, o mediante el DHCP. La dirección IP estática y la puerta de enlace predeterminada para el modo del sistema Capa 2 se configuran en las páginas Interfaz IPv4 e Interfaces IPv6. En el modo del sistema Capa 2, el dispositivo usa la puerta de enlace predeterminada, si está configurada, para comunicarse con dispositivos que no están en la misma subred IP que el dispositivo. De forma predeterminada, la VLAN 1 es la VLAN de administración, pero se puede modificar. Al funcionar en el modo del sistema Capa 2, el dispositivo solo se puede alcanzar en la dirección IP configurada a través de su VLAN de administración.

La configuración predeterminada de fábrica de la dirección IPv4 es *DHCPv4*. Esto significa que el dispositivo actúa como cliente DHCPv4 y envía una solicitud DHCPv4 mientras se inicia.

Si el dispositivo recibe una respuesta DHCPv4 del servidor DHCPv4 con una dirección IPv4, envía paquetes ARP (Address Resolution Protocol, protocolo de resolución de direcciones) para confirmar que la dirección IP es única. Si la respuesta ARP muestra que la dirección IPv4 está en uso, el dispositivo envía un mensaje DHCPDECLINE al servidor DHCP de oferta y envía otro paquete DHCPDISCOVER que reinicia el proceso.

Si el dispositivo no recibe una respuesta DHCPv4 en 60 segundos, continúa enviando consultas DHCPDISCOVER y adopta la dirección IPv4 predeterminada: 192.168.1.254/24.

Cuando más de un dispositivo usa la misma dirección IP en la misma subred IP, se producen colisiones de dirección IP. Las colisiones de dirección requieren acciones administrativas en el servidor DHCP o en los dispositivos que colisionan con el dispositivo.

Cuando una VLAN se configura para usar direcciones IPv4 dinámicas, el dispositivo emite solicitudes DHCPv4 hasta que un servidor DHCPv4 le asigna una dirección IPv4. En el modo del sistema Capa 2, solo la VLAN de administración se puede configurar con una dirección IP estática o dinámica. En el modo del sistema Capa 3, se pueden configurar todos los tipos de interfaces (puertos, LAG o VLAN) en el dispositivo con una dirección IP estática o dinámica.

Las reglas de asignación de dirección IP para el dispositivo son las siguientes:

- En el modo de capa 2 del sistema, a menos que el switch se configure con una dirección IP estática, emite solicitudes DHCPv4 hasta que recibe una respuesta del servidor DHCP.
- Si la dirección IP del dispositivo se cambia, el dispositivo emite paquetes ARP gratuitos a la VLAN correspondiente para verificar las colisiones de dirección IP. Esta regla también se aplica cuando el dispositivo vuelve a la dirección IP predeterminada.

- Cuando se recibe una nueva dirección IP única del servidor DHCP, el indicador luminoso LED del estado del sistema se pone verde. Si se ha configurado una dirección IP estática, el indicador luminoso LED del estado del sistema también se pone verde. El indicador LED parpadea cuando el dispositivo está adquiriendo una dirección IP y está usando la dirección IP predeterminada de fábrica 192.168.1.254.
- Las mismas reglas se aplican cuando un cliente debe renovar la concesión, antes de la fecha de vencimiento a través de un mensaje DHCPREQUEST.
- Con las opciones predeterminadas de fábrica, cuando no hay una dirección IP adquirida a través del servidor DHCP o una dirección definida de manera estática disponible, se usa la dirección IP predeterminada. Cuando las otras direcciones IP quedan disponibles, se usan automáticamente. La dirección IP predeterminada está siempre en la VLAN de administración.

Direccionamiento IP de capa 3

En el modo de capa 3 del sistema, el dispositivo puede tener varias direcciones IP. Cada dirección IP puede asignarse a puertos especificados, LAG o VLAN. En el modo del sistema Capa 3, estas direcciones IP se configuran en las páginas Interfaz IPv4 e Interfaces IPv6. De esta manera, la red tiene más flexibilidad que en el modo del sistema Capa 2, en el que solo puede configurarse una sola dirección IP. Al funcionar en el modo del sistema Capa 3, es posible alcanzar el dispositivo en todas sus direcciones IP desde las interfaces correspondientes.

En el modo de capa 3 del sistema, no se proporciona una ruta predefinida y predeterminada. Para administrar el dispositivo de forma remota, debe especificarse una ruta predeterminada. Todas las puertas de enlace predeterminadas asignadas por el-DHCP se almacenan como rutas predeterminadas. Las rutas predeterminadas también se pueden definir manualmente. Esto se define en las páginas Trayectos estáticos IPv4 y Rutas IPv6.

Todas las direcciones IP configuradas o asignadas al dispositivo se denominan direcciones IP de administración en esta guía.

Si las páginas para la capa 2 y la capa 3 son diferentes, se muestran las dos versiones.

Interfaz de bucle invertido

Información general

La interfaz de bucle invertido es una interfaz virtual que operativamente está siempre activa. Si la dirección IP que se configura en esta interfaz virtual se usa como dirección local al comunicarse con aplicaciones IP remotas, la comunicación no se cancelará incluso si se modificara la ruta real a la aplicación remota.

La interfaz de bucle invertido siempre está operativamente activa. Se le define una dirección IP (IPv4 o IPv6) que se utilizará como la dirección IP local para la comunicación IP con aplicaciones IP remotas. La comunicación permanecerá intacta siempre que pueda accederse a las aplicaciones remotas desde cualquiera de las interfaces IP activas del switch (que no sean de bucle invertido). Por otra parte, si se usa la dirección IP de una interfaz IP para comunicarse con aplicaciones remotas, la comunicación finalizará cuando la interfaz IP quede desactivada.

Una interfaz de bucle invertido no admite el puente, no puede integrar ninguna VLAN ni se le puede habilitar ningún protocolo de capa 2.

El identificador de la interfaz IPv6 de tipo local con enlace es 1.

Cuando el switch se encuentra en el modo del sistema de Capa 2, se admiten las siguientes reglas:

- Solo se admite una interfaz de bucle invertido.
- Pueden configurarse dos interfaces IPv4: una en una VLAN o puerto Ethernet, y otra en la interfaz de bucle invertido.
- Si la dirección IPv4 se configura en la VLAN predeterminada y se modifica esta VLAN predeterminada, el switch pasa la dirección IPv4 a la nueva VLAN predeterminada.

Configuración de una interfaz de bucle invertido

Para configurar una interfaz de bucle invertido IPv4, realice lo siguiente:

- En Capa 2, habilite la interfaz de bucle invertido y configure su dirección en la página Administración > Interfaz de administración > Interfaz IPv4.
- En Capa 3, agregue una interfaz de bucle invertido en Configuración IP > Administración e interfaces IPv4 > Interfaz IPv4.

Para configurar una interfaz de bucle invertido IPv6, realice lo siguiente:

- En Capa 2, agregue una interfaz de bucle invertido en la página Administración > Interfaz de administración > Interfaces IPv6. Configure la dirección IPv6 de esa interfaz en la página Administración > Interfaz de administración > Direcciones IPv6. Esta página no está disponible en los dispositivos SG500X, ESW2-550X y SG500XG.
- En Capa 3, agregue una interfaz de bucle invertido en Configuración IP > Administración e interfaces IPv6 > Interfaz IPv6. Configure la dirección IPv6 de esa interfaz en la página Configuración IP > Administración e interfaces IPv6 > Direcciones IPv6.

Administración e interfaces IPv4

Interfaz IPv4

Las interfaces IPv4 se pueden definir en el dispositivo cuando este está en el modo del sistema Capa 2 o Capa 3.

Definición de una interfaz IPv4 en modo del sistema Capa 2

Para administrar el dispositivo mediante la utilidad de configuración basada en la Web, es necesario definir y conocer la dirección IP de administración del dispositivo IPv4. La dirección IP del dispositivo se puede configurar manualmente o se puede recibir automáticamente de un servidor DHCP.

Para configurar la dirección IP del dispositivo IPv4:

PASO 1 Haga clic en **Administración > Interfaz de administración > Interfaz IPv4**.

PASO 2 Ingrese los valores para los siguientes campos:

- **VLAN de administración**: seleccione la VLAN de administración que se usa para acceder al dispositivo a través de Telnet o la GUI Web. La VLAN1 es la VLAN de administración predeterminada.
- **Tipo de dirección IP**: seleccione una de las siguientes opciones:
  - *Dinámica*: descubra la dirección IP mediante DHCP de la VLAN de administración.
  - *Estática*: defina manualmente una dirección IP estática.

  NOTA La opción 12 de DHCP (opción de nombre de host) está habilitada cuando el dispositivo es un cliente DHCP. Si la opción 12 de DHCP se recibe desde un servidor DHCP, se guardará como el nombre de host del servidor. El dispositivo no solicitará la opción 12 de DHCP. El servidor DHCP debe estar configurado para enviar la opción 12, sin importar lo que se solicite, para poder hacer uso de la función.

Para configurar una dirección IP estática, configure los siguientes campos.

- **Dirección IP**: ingrese la dirección IP y configure uno de los siguientes campos **Máscara**:
  - **Máscara de red**: seleccione e ingrese la máscara de dirección IP.
  - **Longitud del prefijo**: seleccione e ingrese la longitud del prefijo de la dirección IPv4.
- **Interfaz de bucle invertido**: seleccione para habilitar la configuración de una interfaz de bucle invertido (consulte **Interfaz de bucle invertido**).
- **Dirección IP de bucle invertido**: introduzca la dirección IPv4 de la interfaz de bucle invertido.

Introduzca uno de los siguientes campos para **Másc. de bucle invertido**:

- **Máscara de red**: introduzca la máscara de la dirección IPv4 de la interfaz de bucle invertido.
- **Longitud del prefijo**: introduzca la longitud del prefijo de la dirección IPv4 de la interfaz de bucle invertido.

- **Puerta de enlace administrativa predet.**: seleccione **Definida por el usuario** e ingrese la dirección IP de puerta de enlace predeterminada o seleccione **Ninguna** para eliminar la dirección IP de puerta de enlace predeterminada seleccionada de la interfaz.
- **Puerta de enlace operativa predeterminada**: muestra el estado actual de la puerta de enlace predeterminada.

  NOTA Si el dispositivo no está configurado con una puerta de enlace predeterminada, no se puede comunicar con otros dispositivos que no están en la misma subred IP.

Si se obtiene una dirección IP dinámica del servidor DHCP, seleccione aquellos de los siguientes campos que están habilitados:

- **Renovar la dirección IP ahora**: la dirección IP dinámica del dispositivo se puede renovar en cualquier momento después de que el servidor DHCP la haya asignado. Tenga en cuenta que, según la configuración del servidor DHCP, el dispositivo podrá recibir una nueva dirección IP después de la renovación que requiere la configuración de la utilidad de configuración basada en la Web para la nueva dirección IP.
- **Configuración automática a través de DHCP**: muestra el estado de la función de configuración automática. Usted puede configurarlo desde *Administración* > *Administración de archivo* > *Configuración automática de DHCP*.

PASO 3 Haga clic en **Aplicar**. La configuración de la interfaz IPv4 se escribe en el archivo Configuración en ejecución.

Definición de una interfaz IPv4 en modo del sistema Capa 3

La página Interfaz IPv4 se usa cuando el dispositivo está en el modo del sistema Capa 3. Este modo activa la configuración de varias direcciones IP para la administración del dispositivo y proporciona servicios de enrutamiento.

La dirección IP se puede configurar en un puerto, LAG, VLAN o interfaz de bucle invertido.

Al funcionar en el modo Capa 3, el dispositivo envía el tráfico entre las subredes IP conectadas directamente configuradas en el dispositivo. El dispositivo continúa puenteando el tráfico entre los dispositivos de la misma VLAN. En la página Trayectos estáticos IPv4, se pueden configurar rutas IPv4 adicionales para enrutamiento a subredes no conectadas directamente.

NOTA El software del dispositivo consume una VID (VLAN ID, ID de VLAN) por cada dirección IP que se configura en un puerto o LAG. El dispositivo toma la primera VID que no está usada comenzando por 4094.

- *Local*: indica que la ruta es un trayecto local. Ese tipo no puede seleccionarse, pero lo crea el sistema.

ARP

El dispositivo mantiene una tabla de ARP para todos los dispositivos conocidos que residen en las subredes IP conectadas directamente a este. Una subred IP conectada directamente es la subred a la que se conecta una interfaz IPv4 del dispositivo. Cuando se requiere que el dispositivo envíe o enrute un paquete a un dispositivo local, busca en la tabla de ARP para obtener la dirección MAC del dispositivo. La tabla ARP contiene direcciones estáticas y dinámicas. Las direcciones estáticas se configuran manualmente y no vencen. El dispositivo crea direcciones dinámicas de los paquetes ARP que recibe. Las direcciones dinámicas vencen después de un tiempo configurado.

NOTA En el modo Capa 2, el dispositivo usa la información de asignación de dirección IP/MAC de la tabla de ARP para reenviar el tráfico que origina el dispositivo. En el modo Capa 3, la información de asignación se usa para el enrutamiento de capa 3 y también para reenviar el tráfico generado.

Para definir las tablas ARP:

PASO 1 Haga clic en **Configuración de IP > Administración e interfaces IPv4** > **ARP**.

PASO 2 Ingrese los parámetros.

- **Vencimiento de entrada del ARP**: ingrese la cantidad de segundos que las direcciones dinámicas pueden permanecer en la tabla ARP. Una dirección dinámica vence después de que el tiempo que está en la tabla supera el tiempo de Vencimiento de entrada del ARP. Cuando una dirección dinámica se vence, se elimina de la tabla y solo vuelve cuando se vuelve a aprender.
- **Borrar entradas de la tabla ARP**: seleccione el tipo de entradas ARP que se deben borrar del sistema.
  - *Todas*: elimina todas las direcciones estáticas o dinámicas inmediatamente.
  - *Dinámicas*: elimina todas las direcciones dinámicas inmediatamente.
  - *Estáticas*: elimina todas las direcciones estáticas inmediatamente.
  - *Vencimiento normal*: elimina todas las direcciones dinámicas según el tiempo de Vencimiento de entrada del ARP configurado.

PASO 3 Haga clic en **Aplicar.** La configuración de la interfaz global de ARP se escribe en el archivo Configuración en ejecución.

La tabla ARP muestra los siguientes campos:

- **Interfaz**: la interfaz IPv4 de la subred IP directamente conectada donde reside el dispositivo IP.
- **Dirección IP**: la dirección IP del dispositivo IP.
- **Dirección MAC**: la dirección MAC del dispositivo IP.
- **Estado**: si la entrada se ha ingresado manualmente o se ha aprendido dinámicamente.

PASO 4 Haga clic en **Añadir**.

PASO 5 Ingrese los parámetros:

- **Versión de IP**: el formato de dirección IP que admite el host. Solo admite IPv4.

  Interfaz (Capa 3): puede configurarse una interfaz IPv4 en un puerto, LAG o VLAN. Seleccione la interfaz que desea en la lista de interfaces IPv4 configuradas en el dispositivo.

- **Interfaz (Capa 2)** interfaz IPv4 en el dispositivo.

  Para los dispositivos en el modo Capa 2, solo hay una subred IP conectada directamente, que está siempre en la VLAN de administración. Todas las direcciones dinámicas y estáticas de la Tabla ARP residen en la VLAN de administración.

- **Dirección IP**: ingrese la dirección IP del dispositivo local.
- **Dirección MAC**: ingrese la dirección MAC del dispositivo local.

PASO 6 Haga clic en **Aplicar**. La entrada de ARP se guarda en el archivo de configuración en ejecución.

Proxy ARP

La técnica Proxy ARP es utilizada por el dispositivo en una subred IP determinada para responder consultas ARP para una dirección de red que no está en esa red.

NOTA La función Proxy ARP solo está disponible cuando el dispositivo se encuentra en modo Capa 3.

El Proxy ARP está al tanto del destino del tráfico y ofrece otra dirección MAC en respuesta. Al servir como Proxy ARP para otro host, dirige de manera eficaz el destino del tráfico de LAN al host. El tráfico capturado, por lo general, es ruteado por el Proxy al destino deseado mediante otra interfaz o mediante un túnel.

El proceso en que una solicitud de consulta ARP de una dirección IP diferente para los fines del proxy hace que el nodo responda con su propia dirección MAC a veces se denomina publicación.

Para activar el Proxy ARP en todas las interfaces IP:

PASO 1 Haga clic en **Configuración de IP > Administración e interfaces IPv4** > **Proxy ARP**.

PASO 2 Seleccione **Proxy ARP** para activar el dispositivo para que responda a solicitudes ARP de nodos remotamente ubicados con la dirección MAC del dispositivo.

PASO 3 Haga clic en **Aplicar**. Se habilita el proxy ARP y se actualiza el archivo Configuración en ejecución.

Retransmisión UDP/Aplicación aux. IP

La función Retransmisión UDP/Aplicación aux. IP solo está disponible cuando el dispositivo está en el modo del sistema Capa 3. Por lo general, los switches no enrutan los paquetes de difusión IP entre subredes IP. Sin embargo, esta función permite que el dispositivo retransmita paquetes de difusión UDP (User Datagram Protocol, protocolo de datagrama de usuario) específicos recibidos de sus interfaces IPv4 a direcciones IP de destino específicas.

Para configurar la retransmisión de paquetes UDP recibidos de una interfaz IPv4 específica con un puerto UDP de destino específico, añada una Retransmisión UDP:

PASO 1 Haga clic en **Configuración de IP > Administración e interfaces IPv4** > **Retransmisión UDP/Aplicación aux. IP**.

PASO 2 Haga clic en **Añadir**.

PASO 3 Seleccione la **Interfaz IP de origen** a donde desea que el dispositivo retransmita los paquetes de difusión UDP según un puerto de destino UDP configurado. La interfaz debe ser una de las interfaces IPv4 configuradas en el dispositivo.

PASO 4 Ingrese el número de **Puerto de destino UDP** para los paquetes que el dispositivo retransmitirá. Seleccione un puerto conocido en la lista desplegable o haga clic en el botón de opción del puerto para ingresar el número manualmente.

PASO 5 Ingrese la **Dirección IP de destino** que recibe las retransmisiones de paquetes UDP. Si este campo es 0.0.0.0, los paquetes UDP se descartan. Si este campo es 255.255.255.255, los paquetes UDP se envían en forma masiva a todas las interfaces IP.

PASO 6 Haga clic en **Aplicar**. La configuración de la retransmisión UDP se escribe en el archivo Configuración en ejecución.

Retransmisión/Indagación DHCPv4

Indagación DHCPv4

La indagación DHCP brinda un mecanismo de seguridad para prevenir la recepción de paquetes falsos de respuesta DHCP y para registrar direcciones DHCP. Para ello, trata los puertos del dispositivo como confiables o no confiables.

Un puerto confiable es un puerto conectado a un servidor DHCP y al cual se le permite asignar direcciones DHCP. A los mensajes DHCP que se reciben en puertos confiables se les permite pasar a través del dispositivo.

Un puerto no confiable es un puerto al cual no se le permite asignar direcciones DHCP. De manera predeterminada, todos los puertos se consideran como no confiables hasta que usted los declare confiables (en la página Configuración de interfaz de indagación de DHCP).

Retransmisión DHCPv4

La retransmisión DHCP retransmite los paquetes DHCP al servidor DHCP.

DHCPv4 en Capa 2 y Capa 3

En el modo del sistema Capa 2, el dispositivo reenvía los mensajes DHCP que provienen de las VLAN donde se ha activado la Retransmisión DHCP.

En el modo del sistema Capa 3, el dispositivo también puede retransmitir los mensajes DHCP recibidos de las VLAN que no tienen direcciones IP. Siempre que la Retransmisión DHCP esté habilitada en una VLAN sin dirección IP, se insertará la opción 82 automáticamente. Esta inserción se efectúa en la VLAN específica y no influencia el estado global de administración de la inserción de opción 82.

Retransmisión DHCP transparente

Para una Retransmisión DHCP transparente, cuando está en uso un agente de retransmisión DHCP externo, haga lo siguiente:

- Habilite la Indagación DHCP.
- Habilite la Inserción de Opción 82.
- Deshabilite la Retransmisión DHCP.

Para una Retransmisión DHCP común:

- Habilite la Retransmisión DHCP.
- No es necesario habilitar la inserción de la Opción 82.

Opción 82

La Opción 82 (Opción de información de agente de retransmisión DHCP) transfiere información del puerto y del agente a un servidor DHCP central y le indica dónde se conecta físicamente una dirección IP asignada a la red.

El objetivo principal de la Opción 82 es ayudar al servidor DHCP a seleccionar la mejor subred IP (de la agrupación de redes) de la cual obtener una dirección IP.

En el dispositivo, se encuentran disponibles las siguientes opciones de la Opción 82:

- **Inserción DHCP**: añade información de la opción 82 a los paquetes que no tienen información remota de la opción 82.
- **Envío de DHCP**: reenvía o rechaza los paquetes DHCP que contengan información de la opción 82 que provenga de puertos no confiables. En puertos confiables, los paquetes DHCP que contienen información de la Opción 82 siempre se reenvían.

La tabla a continuación muestra el flujo de paquetes a través de los módulos de Retransmisión DHCP, Indagación DHCP y Opción 82:

Las siguientes opciones son posibles:

- Cliente DHCP y servidor DHCP conectados a la misma VLAN. En este caso, una conexión de puente normal pasa los mensajes DHCP entre el cliente DHCP y el servidor DHCP.
- Cliente DHCP y servidor DHCP conectados a VLAN distintas. En este caso, únicamente la Retransmisión DHCP difunde los mensajes DHCP entre el cliente DHCP y el servidor DHCP. Los mensajes DHCP de unidifusión se transfieren por routers comunes y, por lo tanto, si se activa la Retransmisión DHCP en una VLAN sin dirección IP o si el dispositivo no es un router (dispositivo de capa 2), se necesitará un router externo.

Retransmisión DHCP, solamente la Retransmisión DHCP retransmite los mensajes DHCP a un servidor DHCP.

Interacciones entre Indagación DHCPv4, Retransmisión DHCPv4 y Opción 82

En las tablas a continuación, se describe el comportamiento del dispositivo con diversas combinaciones de Indagación DHCP, Retransmisión DHCP y Opción 82.

Se describe la manera en que se tratan los paquetes solicitados por DHCP cuando no está habilitada la Indagación DHCP y la Retransmisión DHCP sí está habilitada.

	Retransmisión DHCP VLAN con dirección IP		Retransmisión DHCP VLAN sin dirección IP	
	El paquete llega sin Opción 82	El paquete llega con Opción 82	El paquete llega sin Opción 82	El paquete llega con Opción 82
Inserción de opción 82 deshabilitada	Se envía el paquete sin Opción 82	Se envía el paquete con la Opción 82 original	Retransmisión: inserta la Opción 82 Conexión puente: no se inserta ninguna Opción 82	Retransmisión: descarta el paquete Conexión puente: se envía el paquete con la Opción 82 original
Inserción de opción 82 habilitada	Retransmisión: se envía el paquete sin Opción 82 Conexión puente: no se envía ninguna Opción 82	Se envía el paquete con la Opción 82 original	Retransmisión: se envía el paquete sin Opción 82 Conexión puente: no se envía ninguna Opción 82	Retransmisión: descarta el paquete Conexión puente: se envía el paquete con la Opción 82 original

Se describe la manera en que se tratan los paquetes solicitados por DHCP cuando están habilitadas la Indagación DHCP y la Retransmisión DHCP.

	Retransmisión DHCP VLAN con dirección IP		Retransmisión DHCP VLAN sin dirección IP	
	El paquete llega sin Opción 82	El paquete llega con Opción 82	El paquete llega sin Opción 82	El paquete llega con Opción 82

	Retransmisión DHCP VLAN con dirección IP		Retransmisión DHCP VLAN sin dirección IP	
Inserción de opción 82 deshabilitada	Se envía el paquete sin Opción 82	Se envía el paquete con la Opción 82 original	Retransmisión: inserta la Opción 82 Conexión puente: no se inserta ninguna Opción 82	Retransmisión: descarta el paquete Conexión puente: se envía el paquete con la Opción 82 original
Inserción de opción 82 habilitada	Retransmisión: se envía con Opción 82 Conexión puente: se añade la Opción 82 (si el puerto es confiable, se comporta como si la Indagación DHCP no estuviera habilitada)	Se envía el paquete con la Opción 82 original	Retransmisión: se envía con Opción 82 Conexión puente: se inserta la Opción 82 (si el puerto es confiable, se comporta como si la Indagación DHCP no estuviera habilitada)	Retransmisión: descarta el paquete Conexión puente: se envía el paquete con la Opción 82 original

La tabla a continuación describe como se manejan los paquetes de Retransmisión DHCP cuando la Indagación DHCP está deshabilitada:

	Retransmisión DHCP VLAN con dirección IP		Retransmisión DHCP VLAN sin dirección IP	
	El paquete llega sin Opción 82	El paquete llega con Opción 82	El paquete llega sin Opción 82	El paquete llega con Opción 82

	Retransmisión DHCP VLAN con dirección IP		Retransmisión DHCP VLAN sin dirección IP	
Inserción de opción 82 deshabilitada	Se envía el paquete sin Opción 82	Se envía el paquete con la Opción 82 original	Retransmisión: descarta la opción 82 Conexión puente: se envía el paquete sin Opción 82	Retransmisión: 1. Si se origina una retransmisión en el dispositivo, el paquete se envía sin la Opción 82. 2. Si la retransmisión no se origina en el dispositivo, el paquete se descarta. Conexión puente: se envía el paquete con la Opción 82 original
Inserción de opción 82 habilitada	Se envía el paquete sin Opción 82	Retransmisión: se envía el paquete sin Opción 82 Conexión puente: se envía el paquete con la Opción 82	Retransmisión: descarta la opción 82 Conexión puente: se envía el paquete sin Opción 82	Retransmisión: se envía el paquete sin Opción 82 Conexión puente: se envía el paquete con la Opción 82

Se describe la manera en que se tratan los paquetes de retransmisión DHCP cuando están habilitadas la Indagación DHCP y la Retransmisión DHCP.

	Retransmisión DHCP VLAN con dirección IP		Retransmisión DHCP VLAN sin dirección IP	
	El paquete llega sin Opción 82	El paquete llega con Opción 82	El paquete llega sin Opción 82	El paquete llega con Opción 82
Inserción de opción 82 deshabilitada	Se envía el paquete sin Opción 82	Se envía el paquete con la Opción 82 original	La retransmisión la opción 82 Conexión puente: se envía el paquete sin Opción 82	Retransmisión 1. Si se origina una retransmisión en el dispositivo, el paquete se envía sin la Opción 82. 2. Si no se origina una retransmisión en el dispositivo, descarta el paquete. Conexión puente: se envía el paquete con la Opción 82 original
Inserción de opción 82 habilitada	Se envía el paquete sin Opción 82	Se envía el paquete sin Opción 82	Retransmisión: descarta la opción 82 Conexión puente: se envía el paquete sin Opción 82	Se envía el paquete sin Opción 82

Base de datos de vinculación de indagación de DHCP

La Indagación DHCP crea una base de datos (conocida como la base de datos de vinculación de indagación de DHCP) que deriva de la información tomada de los paquetes DHCP que ingresan al dispositivo mediante puertos confiables.

La base de datos de vinculación de indagación de DHCP contiene los siguientes datos: puerto de entrada, VLAN de entrada, dirección MAC del cliente y dirección IP del cliente, si existe.

Las funciones de Configuración de protección de la IP e Inspección de ARP dinámica también utilizan la base de datos de vinculación de indagación DHCP para determinar fuentes de paquete legítimas.

Puertos DHCP confiables

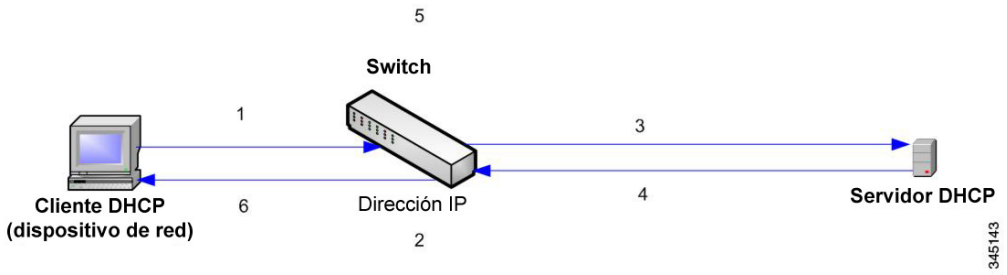
Los puertos pueden ser DHCP confiables o no confiables. De forma predeterminada, todos los puertos son no confiables. Para crear un puerto como confiable, use la página Configuración de interfaz de indagación de DHCP. Los paquetes de estos puertos se reenvían automáticamente. Los paquetes de los puertos confiables se usan para crear la base de datos de vinculación y se manejan tal como se describe a continuación.

Si la indagación de DHCP no está habilitada, todos los puertos son confiables, por opción predeterminada.

Construcción de la base de datos de vinculación de indagación DHCP

A continuación, se describe cómo el dispositivo maneja los paquetes DHCP cuando tanto el cliente DHCP como el servidor DHCP son confiables. En este proceso se construye la base de datos de vinculación de indagación DHCP.

Manejo de los paquetes DHCP confiables



Las acciones son:

PASO 1 El dispositivo envía DHCPDISCOVER para solicitar una dirección IP o DHCPREQUEST para aceptar una dirección IP y una concesión.

PASO 2 El dispositivo indaga el paquete y agrega información de IP/MAC a la base de datos de vinculación de indagación de DHCP.

PASO 3 El dispositivo envía paquetes DHCPDISCOVER o DHCPREQUEST.

PASO 4 El servidor DHCP envía el paquete DHCPOFFER para ofrecer una dirección IP, DHCPACK para asignarla o DHCPNAK para denegar la solicitud de la dirección.

PASO 5 El dispositivo indaga el paquete. Si existe una entrada en la tabla de vinculación de indagación de DHCP que coincida con el paquete, el dispositivo la reemplaza con una vinculación IP/MAC al recibir DHCPACK.

PASO 6 El dispositivo reenvía DHCPOFFER, DHCPACK o DHCPNAK.

A continuación se resume la forma en que los paquetes DHCP se tratan tanto desde puertos confiables como puertos no confiables. La base de datos de vinculación de indagación de DHCP se almacena en una memoria no volátil.

Tratamiento de paquete de indagación DHCP

Tipo de paquete	Proviene de una interfaz de ingreso no confiable	Proviene de una interfaz de ingreso confiable
DHCPDISCOVER	Reenvío solo a interfaces confiables.	Se reenvía solo a interfaces confiables.
DHCPOFFER	Filtro.	Reenvía el paquete según la información de DHCP. Si la dirección de destino es desconocida, el paquete se filtra.
DHCPREQUEST	Reenvío solo a interfaces confiables.	Reenvío solo a interfaces confiables.
DHCPACK	Filtro.	Igual que DHCPOFFER, se añade una entrada a la base de datos de vinculación de indagación de DHCP.
DHCPNAK	Filtro.	Igual que DHCPOFFER. Elimina la entrada si existe.
DHCPDECLINE	Verifica si hay información en la base de datos. Si hay información y no coincide con la interfaz en la cual se recibió el mensaje, el paquete se filtra. De lo contrario, el paquete se reenvía únicamente a interfaces confiables y la entrada se elimina de la base de datos.	Reenvío solo a interfaces confiables.

Tipo de paquete	Proviene de una interfaz de ingreso no confiable	Proviene de una interfaz de ingreso confiable
DHCPRELEASE	Igual que DHCPDECILNE.	Igual que DHCPDECILNE.
DHCPINFORM	Reenvío solo a interfaces confiables.	Reenvío solo a interfaces confiables.
DHCPLEASEQUERY	Filtrado.	Reenvío.

Indagación DHCP junto con retransmisión DHCP

Si tanto la indagación de DHCP como la retransmisión de DHCP están globalmente habilitadas, entonces la indagación de DHCP se habilita en la VLAN del cliente, se aplican las reglas de indagación de DHCP contenidas en la base de datos de vinculación de indagación de DHCP, y la misma base de datos se actualiza en la VLAN del cliente y del servidor DHCP, para paquetes retransmitidos.

Configuración predeterminada de DHCP

A continuación se describen las opciones predeterminadas de indagación de DHCP y retransmisión de DHCP.

Opciones predeterminadas de DHCP

Opción	Estado predeterminado
Indagación de DHCP	**Habilitado**
Inserción de opción 82	**No aplicable**
Traspaso de la Opción 82	**No aplicable**
Verificar la dirección MAC	**Habilitado**
Respaldo de la base de datos de vinculación de indagación de DHCP	**No aplicable**
Retransmisión DHCP	**Deshabilitado**

Configuración del flujo de trabajo de DHCP

Para configurar la retransmisión de DHCP y la indagación de DHCP:

PASO 1 Active la indagación DHCP o la retransmisión DHCP en **Configuración de IP > DHCP > Propiedades** o en **Seguridad > Indagación de DHCP > Propiedades**.

PASO 2 Defina las interfaces sobre las cuales se habilitará la indagación de DHCP en la página **Configuración de IP > DHCP > Configuraciones de interfaz**.

PASO 3 Configure las interfaces como confiables o no confiables en **Configuración de IP > DHCP > Interfaz de indagación de DHCP**.

PASO 4 Opcional. Agregue entradas a la base de datos de vinculación de indagación de DHCP en **Configuración de IP > DHCP > Base de datos de vinculación de indagación de DHCP**.

Indagación/Retransmisión DHCP

Esta sección describe la forma en que se implementan las funciones de Indagación y Retransmisión DHCP a través de la interfaz basada en Web.

Propiedades

Para configurar la retransmisión DHCP, la indagación DHCP y la opción 82:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Indagación/Retransmisión DHCP > Propiedades**, o bien haga clic en **Seguridad** > **Indagación de DHCP**.

Ingrese los siguientes campos:

- **Opción 82:** seleccione **Opción 82** para insertar información de la Opción 82 a los paquetes.
- **Retransmisión DHCP:** seleccione para habilitar la retransmisión DHCP.
- **Estado de indagación de DHCP:** seleccione para habilitar la indagación DHCP. Si la indagación DHCP está habilitada, se pueden habilitar las siguientes opciones:
  - *Transferencia de la opción 82*: seleccione esta opción para dejar la información remota de Opción 82 cuando reenvía paquetes.
  - *Verificar dirección MAC*: verifica que la dirección MAC de origen del encabezado de capa 2 coincida con la dirección de hardware del cliente tal como aparece en el Encabezado de DHCP (parte de la carga) en los puertos no confiables de DHCP.

- *Base de datos de respaldo*: respalda la base de datos de vinculación de indagación de DHCP en la memoria flash del dispositivo.
- *Intervalo de actualización del respaldo de la base de datos*: ingrese con cuánta frecuencia se respaldará la base de datos de vinculación de indagación de DHCP (**si se selecciona la Base de datos**).

PASO 2 Haga clic en **Aplicar**. La configuración se escribe en el archivo Configuración en ejecución.

PASO 3 Para definir un servidor DHCP, haga clic en **Añadir**.

PASO 4 Ingrese la dirección IP del servidor DHCP y haga clic en **Aplicar**. La configuración se escribe en el archivo Configuración en ejecución.

Configuración de la interfaz

En capa 2, la retransmisión y la indagación de DHCP solo pueden habilitarse en VLAN con direcciones de IP.

En capa 3, la retransmisión y la indagación de DHCP pueden habilitarse en cualquier interfaz con una dirección IP y en VLAN con o sin direcciones IP.

Para habilitar la indagación/retransmisión de DHCP en interfaces específicas:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Indagación/Retransmisión DHCP** > **Configuración de la interfaz**.

PASO 2 Para habilitar la indagación o la retransmisión de DHCP en una interfaz, haga clic en **AÑADIR**.

PASO 3 Seleccione la interfaz y las funciones que desea activar: **Retransmisión DHCP** o **Indagación DHCP**.

PASO 4 Haga clic en **Aplicar**. La configuración se escribe en el archivo Configuración en ejecución.

Interfaces confiables de indagación de DHCP

Los paquetes que provienen de puertos o LAG no confiables se comparan con la base de datos de vinculación de indagación de DHCP (consulte la página Base de datos de vinculación de indagación de DHCP).

Las interfaces son confiables de forma predeterminada.

Para designar una interfaz como no confiable:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Indagación/Retransmisión DHCP** > **Interfaces confiables de indagación de DHCP**.

PASO 2 Seleccione la interfaz y haga clic en **Editar**.

PASO 3 Seleccione **Interfaz confiable** (**Sí** o **No**).

PASO 4 Haga clic en **Aplicar** para guardar los ajustes en el archivo Configuración en ejecución.

Base de datos de vinculación de indagación de DHCP

Consulte la sección **Construcción de la base de datos de vinculación de indagación DHCP** para acceder a una descripción de cómo se añaden entradas dinámicas a la base de datos de indagación de DHCP.

Tenga en cuenta los siguientes puntos sobre el mantenimiento de la base de datos de vinculación de indagación DHCP:

- El dispositivo no actualiza la base de datos de vinculación de indagación de DHCP cuando una estación se mueve a otra interfaz.
- Si hay un puerto caído, las entradas para ese puerto no se eliminan.
- Cuando se deshabilita la indagación de DHCP para una VLAN, las entradas de vinculación que se recolectaron para esa VLAN se eliminan.
- Si la base de datos está llena, la indagación de DHCP sigue con el reenvío de paquetes pero no se generan entradas nuevas. Tenga en cuenta que si las funciones de protección de IP de origen o inspección ARP están activas, los clientes que no estén escritos en la base de datos de vinculación de indagación de DHCP no podrán conectarse a la red.

Para añadir entradas a la base de datos de vinculación de indagación de DHCP:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Indagación/Retransmisión DHCP** > **Base de datos de vinculación de indagación de DHCP**.

Para ver un subconjunto de entradas en la base de datos de vinculación de indagación de DHCP, ingrese los criterios de búsqueda correspondientes y haga clic en **Ir**.

Se muestran los campos de la Base de datos de vinculación de indagación de DHCP. Se describen en la página Añadir, a excepción del campo **Protección de la IP de origen**:

- **Estado:**
  - Activa: la protección de la IP de origen está activa en el dispositivo.
  - Inactiva: la protección de la IP de origen no está activa en el dispositivo.
- **Motivo:**
  - Sin problema
  - Sin recurso
  - VLAN sin indagación
  - Puerto de seguridad

PASO 2 Para añadir una entrada, haga clic en **Añadir**.

PASO 3 Ingrese los campos:

- **ID de VLAN:** VLAN en la que se espera el paquete.
- **Dirección MAC**: dirección MAC del paquete.
- **Dirección IP**: dirección IP del paquete.
- **Interfaz:** unidad/ranura/interfaz en la que se espera el paquete.
- **Tipo:** los valores posibles del campo son:
  - *Dinámico*: la entrada tiene tiempo de concesión limitado.
  - *Estático*: la entrada se configuró de manera estática.
- **Tiempo de concesión**: si la entrada es dinámica, ingrese la cantidad de tiempo que la entrada permanecerá activa en la base de datos de DHCP. (Si no hay Tiempo de concesión, seleccione la opción Infinito).

PASO 4 Haga clic en **Aplicar**. Se define la configuración y se actualiza el dispositivo.

Servidor DHCP

La función Servidor DHCPv4 le permite configurar el dispositivo como servidor DHCPv4. Un servidor DHCPv4 se utiliza para asignar una dirección IPv4 u otra información a otro dispositivo (cliente DHCP).

El servidor DHCPv4 asigna direcciones IPv4 de un conjunto de direcciones IPv4 definidas por el usuario.

Pueden estar en los siguientes modos:

- **Asignación estática**: la dirección de hardware o identificador de cliente de un host se asigna manualmente a una dirección IP. Esto se realiza en la página Hosts estáticos.
- **Asignación dinámica**: un cliente obtiene una dirección IP concedida por un período de tiempo especificado (que puede ser infinito). Si el cliente DHCP no renueva la dirección IP asignada, la dirección IP se anula al final de este período y el cliente debe solicitar otra dirección IP. Esto se realiza en la página Conjuntos de redes.

Dependencias entre funciones

- No es posible configurar en simultáneo en el sistema el servidor DHCP y el cliente DHCP; esto significa lo siguiente: si una interfaz está habilitada por un cliente DHCP, es imposible habilitar globalmente el servidor DHCP.
- Si la opción Retransmisión DHCPv4 está activada, el dispositivo no se puede configurar como servidor DHCP.

Configuraciones y valores predeterminados

- El dispositivo no se configura como servidor DHCPv4 de manera predeterminada.
- Si el dispositivo está activado para ser servidor DHCPv4, no hay conjuntos de redes de direcciones definidas de manera predeterminada.

Flujo de trabajo para habilitar la función del servidor DHCP

Para configurar el dispositivo como servidor DHCPv4:

PASO 1 Active el dispositivo como servidor DHCP en Servidor DHCP > Propiedades.

PASO 2 Si hay algunas direcciones IP a las que no desea que lo asignen, configúrelas utilizando la página Direcciones excluidas.

PASO 3 Defina hasta 8 conjuntos de redes de direcciones IP utilizando la página Conjuntos de redes.

PASO 4 Configure los clientes a los que se les asignará una dirección IP permanente, utilizando la página Hosts estáticos.

PASO 5 Configure las opciones DHCP requeridas en la página Opciones DHCP. Esto configura los valores que deben obtenerse para cada opción DHCP relevante.

PASO 6 Agregue una interfaz IP en el intervalo de uno de los conjuntos DHCP configurados en la página Conjuntos de redes. El dispositivo responde consultas DHCP de esta interfaz IP. Por ejemplo: si el intervalo del conjunto es 1.1.1.1 -1.1.1.254, agregue una dirección IP al intervalo, si desea que los clientes directamente conectados reciban la dirección IP del conjunto configurado. Realice este paso en la página Configuración de IP > Interfaz IPv4.

PASO 7 Vea las direcciones IP asignadas utilizando la página Vinculación de direcciones. Las direcciones IP se pueden eliminar en esta página.

Servidor DHCPv4

Para configurar el dispositivo como servidor DHCPv4:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Servidor DHCP** > **Propiedades** para mostrar la página Propiedades.

PASO 2 Seleccione **Habilitar** para configurar el dispositivo como servidor DHCP.

PASO 3 Haga clic en **Aplicar**. El dispositivo comienza a funcionar de inmediato como servidor DHCP. Sin embargo, no asigna direcciones IP a los clientes hasta que se crea un conjunto.

Conjunto de redes

Cuando el dispositivo sirve como servidor DHCP, se deben definir uno o más conjuntos de direcciones IP desde los que el dispositivo asignará direcciones IP a los clientes. Cada conjunto de redes contiene un rango de direcciones que pertenecen a una subred específica. Estas direcciones se asignan a varios clientes dentro de esa subred.

Cuando un cliente solicita una dirección IP, el dispositivo como servidor DHCP asigna una dirección IP según lo siguiente:

- **Cliente directamente conectado**: el dispositivo asigna una dirección del conjunto de redes cuya subred coincide con la subred configurada en la interfaz IP del dispositivo desde la que se recibió la solicitud DHCP.

- **Cliente remoto**: el dispositivo toma una dirección IP del conjunto de redes cuya primera subred de retransmisión, que se conecta directamente al cliente, coincide con la subred configurada en una de las interfaces IP de los dispositivos.
  - Si el mensaje arriba directamente (no a través de la retransmisión DHCP), el conjunto es local y pertenece a una de loas subredes IP definidas en la interfaz de capa 2 de entrada. En ese caso, la máscara IP del conjunto equivale a la máscara IP de la interfaz IP, y las direcciones IP mínimas y máximas del conjunto pertenecen a la subred IP.
  - Si el mensaje arriba a través de la retransmisión DHCP, la dirección utilizada pertenece a la subred IP especificada por la dirección IP mínima y la máscara IP del conjunto, y el conjunto es remoto.

Se pueden definir hasta ocho conjuntos de redes.

Para crear un conjunto de direcciones IP y definir sus duraciones de concesión:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Servidor DHCP** > **Conjuntos de redes** para mostrar la página Conjuntos de redes.

Se muestran los conjuntos de redes definidos anteriormente.

PASO 2 Haga clic en **Añadir** para definir un nuevo conjunto de redes. Tenga en cuenta que ingresa la dirección IP de subred y la máscara, o bien, la máscara, el inicio de conjunto de direcciones y el fin de conjunto de direcciones.

PASO 3 Ingrese los campos:

- **Nombre de conjunto**: ingrese el nombre del conjunto.
- **Dirección IP de subred**: ingrese la subred en que reside el conjunto de redes.
- **Máscara**: ingrese una de las siguientes opciones:
  - **Máscara de red**: seleccione e ingrese la máscara de red del conjunto.
  - **Longitud de prefijo**: seleccione e ingrese la cantidad de bits que conforman el prefijo de la dirección.
- **Inicio de conjunto de direcciones**: ingrese la primera dirección IP del rango del conjunto de redes.
- **Fin de conjunto de direcciones**: ingrese la última dirección IP del rango del conjunto de redes.
- **Duración de la concesión**: ingrese la cantidad de tiempo que un cliente DHCP puede utilizar una dirección IP de este conjunto. Usted puede configurar una duración de concesión de hasta 49 710 días o una duración infinita.
  - **Infinito**: la duración de la concesión es ilimitada.
  - **Días**: la duración de la concesión en cantidad de días. El rango es de 0 a 49 710 días.

  - **Horas**: la cantidad de horas de la concesión. Se debe proporcionar un valor de días antes de agregar un valor de horas.
  - **Minutos**: la cantidad de minutos de la concesión. Debe agregar un valor de días y un valor de horas antes de agregar un valor de minutos.
- **Dirección IP del router predeterminado (Opción 3)**: ingrese el router predeterminado para el cliente DHCP.
- **Dirección IP del servidor de nombres de dominio (Opción 6)**: seleccione uno de los servidores DNS del dispositivo (si ya está configurado) o seleccione **Otro** e ingrese la dirección IP del servidor DNS disponible en el cliente DHCP.
- **Nombre de dominio (Opción 15)**: ingrese el nombre de dominio para un cliente DHCP.
- **Dirección IP del servidor WINS NetBIOS (Opción 44)**: ingrese el servidor de nombres WINS NetBIOS disponible para un cliente DHCP.
- **Tipo de nodo NetBIOS (Opción 46)**: seleccione cómo resolver el nombre NetBIOS. Los tipos de nodo válidos son:
  - *Híbrido*: se utiliza una combinación híbrida de b-node y p-node. Cuando se configura para usar h-node, una computadora siempre prueba p-node primero y utiliza b-node solamente si p-node falla. Ésta es la opción predeterminada.
  - *Combinado*: se utiliza una combinación de comunicaciones de b-node y p-node para registrar y resolver los nombres NetBIOS. La opción m-node primero usa b-node; después, si es necesario, p-node. La opción m-node por lo general no es la mejor para redes más grandes, ya que su preferencia por las difusiones de b-node aumenta el tráfico de red.
  - *Punto a punto*: las comunicaciones punto a punto con un servidor de nombres NetBIOS se utilizan para registrar y resolver los nombres de computadora para las direcciones IP.
  - *Difusión*: los mensajes de difusión IP se utilizan para registrar y resolver nombres NetBIOS para las direcciones IP.
- **Dirección IP del servidor SNTP (Opción 4)**: seleccione uno de los servidores SNTP del dispositivo (si ya está configurado) o seleccione **Otro** e ingrese la dirección IP del servidor horario para el cliente DHCP.
- **Dirección IP del servidor de archivos (siaddr)**: ingrese la dirección IP del servidor TFTP/SCP de la que se descarga el archivo de configuración.
- **Nombre de host del servidor de archivos (sname/opción 66)**: ingrese el nombre del servidor TFTP/SCP.
- **Nombre del archivo de configuración (file/opción 67)**: ingrese el nombre del archivo que se utiliza como archivo de configuración.

PASO 4 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Direcciones excluidas

De forma predeterminada, el servidor DHCP supone que todas las direcciones de grupo en un conjunto pueden asignarse a los clientes. Se puede excluir una sola dirección IP o un rango de direcciones IP. Las direcciones excluidas se excluyen de todos los conjuntos DHCP.

Para definir un rango de direcciones excluidas:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Servidor DHCP** > **Direcciones excluidas** para mostrar la página Direcciones excluidas.

Se muestran las direcciones IP excluidas definidas anteriormente.

PASO 2 Para agregar un rango de direcciones IP que se deben excluir, haga clic en **Añadir** e ingrese los campos:

- **Dirección IP de inicio**: primera dirección IP en el rango de direcciones IP excluidas.
- **Dirección IP de finalización**: última dirección IP en el rango de direcciones IP excluidas.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Hosts estáticos

Es posible que desee asignar una dirección IP permanente que nunca cambie a algunos clientes DHCP. Este cliente se conoce como host estático.

Para asignar manualmente una dirección IP permanente a un cliente específico:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Servidor DHCP** > **Hosts estáticos** para mostrar la página Hosts estáticos.

Se muestran los hosts estáticos.

PASO 2 Para agregar un host estático, haga clic en **Añadir** e ingrese los campos:

- **Dirección IP**: ingrese la dirección IP que se asignó estáticamente al host.
- **Nombre de host**: ingrese el nombre del host, que puede ser una cadena de símbolos y un entero.
- **Máscara**: ingrese la máscara de red del host estático.
  - *Máscara de red*: seleccione e ingrese la máscara de red del host estático.
  - *Longitud de prefijo*: seleccione e ingrese la cantidad de bits que conforman el prefijo de la dirección.

- **Tipo de identificador**: establezca cómo desea identificar el host estático específico.
  - *Identificador de cliente*: ingrese una identificación única del cliente especificado en notación hexadecimal, como: 01b60819681172.

o bien:

  - *Dirección MAC*: ingrese la dirección MAC del cliente.

- **Nombre de cliente**: ingrese el nombre del host estático, utilizando un conjunto estándar de caracteres ASCII. El nombre de cliente no debe incluir el nombre de dominio.
- **Dirección IP del router predeterminado (Opción 3)**: ingrese el router predeterminado para el host estático.
- **Dirección IP del servidor de nombres de dominio (Opción 6)**: seleccione uno de los servidores DNS del dispositivo (si ya está configurado) o seleccione **Otro** e ingrese la dirección IP del servidor DNS disponible en el cliente DHCP.
- **Nombre de dominio (Opción 15)**: ingrese el nombre de dominio para el host estático.
- **Dirección IP del servidor WINS NetBIOS (Opción 44)**: ingrese el servidor de nombres WINS NetBIOS disponible para el host estático.
- **Tipo de nodo NetBIOS (Opción 46)**: seleccione cómo resolver el nombre NetBIOS. Los tipos de nodo válidos son:
  - *Híbrido*: se utiliza una combinación híbrida de b-node y p-node. Cuando se configura para usar h-node, una computadora siempre prueba p-node primero y utiliza b-node solamente si p-node falla. Ésta es la opción predeterminada.
  - *Combinado*: se utiliza una combinación de comunicaciones de b-node y p-node para registrar y resolver los nombres NetBIOS. La opción m-node primero usa b-node; después, si es necesario, p-node. La opción m-node por lo general no es la mejor para redes más grandes, ya que su preferencia por las difusiones de b-node aumenta el tráfico de red.
  - *Punto a punto*: las comunicaciones punto a punto con un servidor de nombres NetBIOS se utilizan para registrar y resolver los nombres de computadora para las direcciones IP.
  - *Difusión*: los mensajes de difusión IP se utilizan para registrar y resolver nombres NetBIOS para las direcciones IP.
- **Dirección IP del servidor SNTP (Opción 4)**: seleccione uno de los servidores SNTP del dispositivo (si ya está configurado) o seleccione **Otro** e ingrese la dirección IP del servidor horario para el cliente DHCP.
- **Dirección IP del servidor de archivos (siaddr)**: ingrese la dirección IP del servidor TFTP/SCP de la que se descarga el archivo de configuración.

- **Nombre de host del servidor de archivos (sname/opción 66)**: ingrese el nombre del servidor TFTP/SCP.
- **Nombre del archivo de configuración (file/opción 67)**: ingrese el nombre del archivo que se utiliza como archivo de configuración.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Opciones de DHCP

Cuando el dispositivo actúa como servidor DHCP, las opciones DHCP se pueden configurar con la opción HEX. En RFC2131 pueden obtenerse descripciones de estas opciones.

La configuración de estas opciones determina la respuesta que se envía a los clientes DHCP, cuyos paquetes incluyen una solicitud (mediante la opción 55) para las opciones DHCP configuradas.

Ejemplo: la opción DHCP 66 se configura con el nombre de un servidor TFTP en la página Opciones DHCP. Cuando el paquete DHCP de un cliente contiene la opción 66, el servidor TFTP es devuelto como valor de la opción 66.

Para configurar una o más opciones DHCP:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Servidor DHCP** > **Opciones DHCP**.

Se visualizarán las opciones DHCP previamente configuradas.

PASO 2 Para configurar una opción que aún no se haya configurado e ingresar el campo:

- **El nombre del conjunto del servidor DHCP equivale a:** seleccione uno de los conjuntos de direcciones de redes definidos en la página Conjuntos de redes.

PASO 3 Haga clic en **Añadir** e ingrese los campos:

- **Código:** ingrese el código de opción DHCP.
- **Tipo:** los botones de radio para este campo cambian de acuerdo con el tipo de parámetro de opción DHCP. Seleccione uno de los siguientes códigos e ingrese el valor para el parámetro de las opciones DHCP:
  - *Hex*: seleccione si desea ingresar el valor hexadecimal del parámetro para la opción DHCP. El valor hexadecimal puede proporcionarse en lugar de cualquier otro tipo de valor. Por ejemplo, puede proporcionar el valor hexadecimal de una dirección IP en lugar de la misma dirección IP.

    El valor hexadecimal no se valida. Por eso si ingresa un valor HEX, que representa un valor ilegal, no aparecerá ningún error y el cliente probablemente no pueda manejar el paquete DHCP desde el servidor.
  - *IP*: seleccione si desea ingresar una dirección IP cuando sea relevante para la opción DHCP escogida.

- *Lista de IP*: ingrese una lista de direcciones IP separadas por comas.
- *Entero*: seleccione si desea ingresar el valor entero del parámetro para la opción DHCP escogida.
- *Booleano*: seleccione si el parámetro de la opción DHCP escogida es un booleano.

- **Valor booleano:** si el tipo es booleano, seleccione el valor que se devolverá: **Verdadero** o **Falso**.
- **Valor:** si el tipo no es un booleano, ingrese el valor que se enviará para este código.
- **Descripción:** introduzca una descripción del texto para fines de documentación.

PASO 4 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Vinculación de direcciones

Use la página Vinculación de direcciones para ver y eliminar las direcciones IP asignadas por el dispositivo y sus direcciones MAC correspondientes.

Para ver o eliminar vinculaciones de direcciones:

PASO 1 Haga clic en **Configuración de IP** > **Administración e interfaces IPv4** > **Servidor DHCP** > **Vinculación de direcciones** para mostrar la página Vinculación de direcciones.

Se muestran los siguientes campos para las vinculaciones de direcciones:

- **Dirección IP**: las direcciones IP de los clientes DHCP.
- **Tipo de dirección**: si la dirección del cliente DHCP aparece como dirección MAC o con un identificador de cliente.
- **Dirección MAC/Identificador de cliente**: una identificación única del cliente especificado como dirección MAC o en notación hexadecimal, por ejemplo: 01b608196811 72.
- **Vencimiento de la concesión**: la fecha y hora de vencimiento de la concesión de la dirección IP del host o Infinito si es así como se definió la duración de la concesión.
- **Tipo**: la manera en que se asignó la dirección IP al cliente. Las opciones posibles son:
  - *Estático*: la dirección del hardware del host se asignó a una dirección IP.
  - *Dinámico*: la dirección IP, que se obtiene dinámicamente del dispositivo, es propiedad del cliente durante un período de tiempo especificado. La dirección IP se anula al final de este período, momento en que el cliente debe solicitar otra dirección IP.

- **Estado**: las opciones posibles son:
  - *Asignado*: se asignó la dirección IP. Cuando se configura un host estático, se asigna su estado.
  - *Rechazado*: se ofreció una dirección IP, pero no fue aceptada; por ende, no se asignó.
  - *Vencido*: la concesión de la dirección IP venció.
  - *Preasignado*: una entrada tendrá el estado preasignado desde el momento entre la oferta y la hora en que el cliente envía DHCP ACK. Luego pasa a ser asignado.

PASO 2 Haga clic en **Eliminar**. Se actualiza el archivo Configuración en ejecución.

Administración e interfaces IPv6

La versión 6 del protocolo de Internet (IPv6) es un protocolo de la capa de red para interconexiones entre redes de conmutación de paquetes. IPv6 se diseñó para reemplazar a IPv4, el protocolo de Internet implementado de manera predominante.

IPv6 presenta mayor flexibilidad en la asignación de direcciones IP porque el tamaño de las direcciones aumenta de 32 bits a 128 bits. Las direcciones IPv6 se escriben como ocho grupos de cuatro dígitos hexadecimales, por ejemplo, FE80:0000:0000:0000:0000:9C00:876A:130B. La forma abreviada, en la que un grupo de ceros puede quedar afuera y ser reemplazado por '::', también se acepta, por ejemplo, ::-FE80::9C00:876A:130B.

Los nodos IPv6 requieren un mecanismo de asignación intermediario para comunicarse con otros nodos IPv6 en una red solo con IPv4. Este mecanismo, denominado túnel, permite a los hosts solo IPv6 alcanzar los servicios IPv4, y permite a las redes y a los hosts IPv6 aislados alcanzar un nodo IPv6 en la infraestructura IPv4.

La tunelización utiliza un mecanismo ISATAP o manual (consulte **Túnel IPv6**). La tunelización trata la red IPv4 como enlace local IPv6 virtual, con asignaciones de cada dirección IPv4 a una dirección IPv6 local de enlace.

El dispositivo detecta tramas IPv6 mediante Ethertype IPv6.

Configuración global IPv6

Para definir los parámetros globales de IPv6 y las configuraciones de cliente DHCPv6:

PASO 1 En el modo del sistema Capa 2, haga clic en **Administración** > **Interfaz de administración** > **Configuración global IPv6**.

En el modo del sistema Capa 3, haga clic en **Configuración de IP** > **Administración e interfaces IPv6** > **Configuración global IPv6**.

PASO 2 Ingrese los valores para los siguientes campos:

- **Intervalo de límite de velocidad ICMPv6**: ingrese la frecuencia con que se generan los mensajes de error de ICMP.
- **Tamaño de cubeta de límite de velocidad ICMPv6**: ingrese el número máximo de mensajes de error de ICMP que puede enviar el dispositivo por intervalo.

Configuración del cliente DHCPv6

- **Formato de identificador único (DUID)**: este es el identificador del cliente DHCP que utiliza el servidor DHCP para ubicar al cliente. Puede estar en uno de los siguientes formatos:
  - *Capa del enlace* (predeterminado): si selecciona esta opción, se utiliza la dirección MAC del dispositivo.
  - *Número de empresa*: si selecciona esta opción, debe ingresar los siguientes campos.
- **Número de empresa**: el número de empresa privado registrado por el proveedor como lo mantiene IANA (Internet Assigned Numbers Authority, autoridad de números asignados de Internet).
- **Identificador**: la cadena hexadecimal definida por el proveedor (hasta 64 caracteres hexadecimales). Si el número del carácter no es par, se agrega un cero a la derecha. Dos caracteres hexadecimales pueden estar separados por un punto o por dos puntos.
- **Identificador DHCPv6 único (DUID)**: muestra el identificador seleccionado.

PASO 3 Haga clic en **Aplicar**. Los parámetros globales de IPv6 y las configuraciones de cliente DHCPv6 están actualizados.

Interfaz IPv6

Una interfaz IPv6 se puede configurar en un puerto, un LAG, una VLAN, una interfaz de bucle invertido o un túnel.

A diferencia de otros tipos de interfaces, una interfaz de túnel se crea primero en la página Túnel IPv6 y luego la interfaz IPv6 se configura en el túnel de esta página.

Para definir una interfaz IPv6:

PASO 1 En el modo del sistema Capa 2, haga clic en **Administración** > **Interfaz de administración** > **Interfaces IPv6**.
En el modo del sistema Capa 3, haga clic en **Configuración de IP** > **Administración e interfaces IPv6** > **Interfaces IPv6**.

PASO 2 Haga clic en **Aplicar** para configurar la zona predeterminada.

PASO 3 Haga clic en **Añadir** para añadir una interfaz nueva en la que se habilite la interfaz IPv6.

PASO 4 Ingrese los campos:

- **Interfaz IPv6**: seleccione un puerto, un LAG, una VLAN, una interfaz de bucle invertido o un túnel ISATAP específico para la dirección IPv6.

PASO 5 Para configurar la interfaz como cliente DHCPv6, es decir, para activar la interfaz para que reciba información del servidor DHCPv6, como: configuración SNTP e información DNS, ingrese los campos **Cliente DHCPv6**:

- **Sin estado**: seleccione esta opción para activar la interfaz como cliente DHCPv6 sin estado. Esto permite recibir información de configuración de un servidor DHCP.
- **Tiempo mínimo de actualización de información**: este valor se utiliza para fijar un piso en el valor del tiempo de actualización. Si el servidor envía una opción de tiempo de actualización menor que este valor, se usa este valor. Seleccione **Infinito** (no hay actualización, a menos que el servidor envíe esta opción) o **Definido por el usuario** para establecer un valor.
- **Tiempo de actualización de información**: este valor indica la frecuencia con que el dispositivo actualizará la información recibida del servidor DHCPv6. Si no se recibe esta opción del servidor, se utiliza el valor ingresado aquí. Seleccione **Infinito** (no hay actualización, a menos que el servidor envíe esta opción) o **Definido por el usuario** para establecer un valor.

PASO 6 Para configurar parámetros de IPv6 adicionales, ingrese los siguientes campos:

- **Configuración automática de dirección IPv6**: seleccione esta opción para activar la configuración automática de dirección de los avisos de router enviados por los vecinos.

NOTA El dispositivo no admite la configuración automática de dirección con estado de un servidor DHCPv6.

- **Número de intentos de DAD**: ingrese la cantidad de mensajes de solicitud de vecinos consecutivos que se envían mientras se realiza la Duplicate Address Detection (DAD, Detección de direcciones duplicadas) en las direcciones IPv6 de unidifusión de la interfaz. DAD verifica que haya una sola dirección IPv6 de unidifusión nueva antes de que se asigne. Las direcciones nuevas permanecen en estado tentativo durante la verificación de DAD. Si usted ingresa **0** en este campo, se deshabilita el procesamiento de detección de direcciones duplicadas en la interfaz especificada. Si usted ingresa **1** en este campo, se indica una sola transmisión sin transmisiones de seguimiento.

- **Enviar mensajes ICMPv6**: habilite la generación de mensajes de destino inalcanzables.

PASO 7 Haga clic en **Aplicar** para activar el procesamiento de IPv6 en la interfaz seleccionada. Las interfaces IPv6 regulares tienen las siguientes direcciones automáticamente configuradas:

- Dirección local de enlace mediante el ID de interfaz de formato EUI-64 basado en la dirección MAC de un dispositivo
- Todas las direcciones de multidifusión locales de enlace de nodo (FF02::1)
- Dirección de multidifusión de nodo solicitado (formato FF02::1:FFXX:XXXX)

PASO 8 Haga clic en **Tabla de dirección IPv6** para asignar manualmente direcciones IPv6 a la interfaz, si es necesario. Esta página se describe en la sección **Definición de direcciones IPv6**.

PASO 9 Para agregar un túnel, seleccione una interfaz (que se definió como túnel en la página Interfaces IPv6) en la Tabla de túnel IPv6 y haga clic en **Tabla de túnel IPv6**. Consulte **Túnel IPv6**.

PASO 10 Presione el botón **Reiniciar** para iniciar la actualización de la información sin estado recibida del servidor DHCPv6.

Detalles del cliente DHCPv6

El botón **Detalles** muestra la información recibida en la interfaz de un servidor DHCPv6.

Se activa cuando la interfaz seleccionada se define como cliente DHCPv6 sin estado.

Cuando se presiona el botón, muestra los siguientes campos (para la información que se recibió del servidor DHCP):

- **Modo operativo de DHCPv6**: muestra Habilitado si se cumplen las siguientes condiciones:
  - La interfaz está activa.
  - IPv6 está activado.
  - El cliente DHCPv6 sin estado está activado.
- **Servicio sin estado**: el cliente está definido como sin estado (recibe información de configuración de un servidor DHCP) o no.
- **Dirección del servidor DHCPv6**: dirección del servidor DHCPv6.
- **DUID del servidor DHCPv6**: identificador único del servidor DHCPv6.
- **Preferencia del servidor DHCPv6**: prioridad de este servidor DHCPv6.

- **Tiempo mínimo de actualización de información**: consulte los datos anteriores.
- **Tiempo de actualización de información**: consulte los datos anteriores.
- **Tiempo de actualización de información recibido**: tiempo de actualización recibido del servidor DHCPv6.
- **Tiempo restante de actualización de información**: tiempo restante hasta la próxima actualización.
- **Servidores DNS**: lista de servidores DNS recibida del servidor DHCPv6.
- **Lista de búsqueda de dominio DNS**: lista de dominios recibida del servidor DHCPv6.
- **Servidores SNTP**: lista de servidores SNTP recibida del servidor DHCPv6.
- **Cadena de zona horaria POSIX**: zona horaria recibida del servidor DHCPv6.
- **Servidor de configuración**: servidor que contiene el archivo de configuración recibido del servidor DHCPv6.
- **Nombre de la ruta de configuración**: ruta al archivo de configuración en el servidor de configuración recibida del servidor DHCPv6.

Túnel IPv6

Los túneles permiten la transmisión de paquetes IPv6 en redes IPv4. Cada túnel tiene una dirección IPv4 de origen y, si es un túnel manual, también tiene una dirección IPv4 de destino. El paquete IPv6 se encapsula entre estas direcciones.

Túneles ISATAP

El tipo de túnel que se puede configurar en el dispositivo se llama túnel ISATAP (Intra-Site Automatic Tunnel Addressing Protocol, protocolo de direccionamiento automático de túnel dentro de un sitio), que es un túnel de punto a varios puntos. La dirección de origen es la dirección IPv4 (o una de las direcciones IPv4) del dispositivo.

Cuando se configura un túnel ISATAP, la dirección IPv4 de destino la proporciona el router. Tenga en cuenta lo siguiente:

- Se asigna una dirección local de enlace IPv6 a la interfaz ISATAP. La dirección IP inicial se asigna a la interfaz, que luego se activa.
- Si una interfaz ISATAP está activa, la dirección IPv4 del router ISATAP se resuelve mediante el DNS utilizando la asignación de ISATAP a IPv4. Si el registro DNS de ISATAP no se resuelve, se busca la asignación de nombre de host de ISATAP a dirección en la Tabla de asignación de host.
- Cuando una dirección IPv4 del router ISATAP no se resuelve mediante el proceso de DNS, la interfaz IP de ISATAP permanece activa. El sistema no tiene un router predeterminado para el tráfico de ISATAP hasta que se resuelve el proceso de DNS.

Configuración de túneles

NOTA Después de configurar un túnel, configure la interfaz IPv6 en la página Interfaces IPv6.

Para configurar un túnel IPv6:

PASO 1 En el modo del sistema Capa 2, haga clic en **Administración > Interfaz de administración > Túnel IPv6**.

En el modo del sistema Capa 3, haga clic en **Configuración de IP > Administración e interfaces IPv6 > Túnel IPv6**.

PASO 2 Ingrese los valores para los siguientes campos:

- **Número de túnel**: muestra el número de dominio del router del túnel automático.
- **Tipo de túnel**: siempre ISATAP.
- **Dirección IPv4 de origen**: la dirección IPv4 de la interfaz seleccionada en el dispositivo actual que se usa para que forme parte de la dirección IPv6.
  - *Automática*: selecciona automáticamente la dirección IPv4 más baja de todas sus interfaces IPv4 configuradas en el dispositivo. Esta opción es equivalente a la opción Interfaz en la Capa 3, porque en la Capa 2 hay solamente una interfaz.

    NOTA Si se cambia la dirección IPv4, la dirección local de la interfaz de túnel también se cambia.
  - *Manual*: ingrese la dirección IPv4 de origen que se usará. La dirección IPv4 configurada debe ser una de las direcciones IPv4 de las interfaces IPv4 de los dispositivos.
  - *Interfaz* (en la Capa 3): seleccione la interfaz IPv4 que se utilizará.
- **Nombre del router ISATAP**: una cadena global que representa un nombre de dominio de router de túnel automático específico. El nombre puede ser el nombre predeterminado (ISATAP) o un nombre definido por el usuario.
- **Intervalo de solicitud de ISATAP**: la cantidad de segundos entre mensajes de solicitud de router ISATAP, cuando no hay ningún router ISATAP activo. El intervalo puede ser el valor predeterminado o un intervalo definido por el usuario.
- **Solidez de ISATAP**: se usa para calcular el intervalo para las consultas DNS o de solicitud de router. Cuanto más grande sea el número, más frecuentes serán las consultas.

  NOTA El túnel ISATAP no está en funcionamiento si la interfaz IPv4 subyacente no está en funcionamiento.

PASO 3 Haga clic en **Aplicar**. El túnel se guarda en el archivo de configuración en ejecución.

NOTA Para crear un túnel ISATAP, haga clic en el botón **Crear túnel ISATAP**. Se crea un túnel con una dirección IPv4 de origen con configuración automática. Cuando se crea un túnel ISATAP, este botón se convierte en **Eliminar túnel ISATAP**. Si hace clic en este botón, se eliminará el túnel ISATAP.

NOTA Para cerrar un túnel, haga clic en **Editar** y quite la selección de Estado del túnel.

Definición de direcciones IPv6

Para asignar una dirección IPv6 a una interfaz IPv6:

PASO 1 En el modo del sistema Capa 2, haga clic en **Administración** > **Interfaz de administración** > **Direcciones IPv6**.
En el modo del sistema Capa 3, haga clic en **Configuración de IP** > **Administración e interfaces IPv6** > **Direcciones IPv6**.

PASO 2 Para filtrar la tabla, seleccione un nombre de interfaz y haga clic en **Ir**. La interfaz aparece en la Tabla de direcciones IPv6.

PASO 3 Haga clic en **Add**.

PASO 4 Ingrese los valores para los campos.

- **Interfaz IPv6**: muestra la interfaz sobre la cual se definirá la dirección IPv6. Si se muestra un *, significa que la interfaz IPv6 no está activada, pero se configuró.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 que desea agregar.
  - *Enlace local*: una dirección IPv6 que identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: una dirección IPv6 que es un tipo de dirección IPv6 de unidifusión global que es visible y accesible desde otras redes.
  - *Cualquier tipo de difusión*: la dirección IPv6 es una dirección de cualquier tipo de difusión. Esta es una dirección que se asigna a un grupo de interfaces que, por lo general, pertenecen a distintos nodos. Un paquete enviado a una dirección de cualquier tipo de difusión se entrega a la interfaz más cercana (según lo definido por los protocolos de enrutamiento en uso), identificada por la dirección de cualquier tipo de difusión.

- **Dirección IPv6**: en Capa 2, el dispositivo admite una interfaz IPv6. Además de las direcciones de multidifusión y locales de enlace predeterminadas, el dispositivo también agrega automáticamente direcciones globales a la interfaz según los avisos de router que recibe. El dispositivo admite un máximo de 128 direcciones en la interfaz. Cada dirección debe ser una dirección IPv6 válida, especificada en formato hexadecimal mediante valores de 16 bits separados por dos puntos.

  Pueden agregarse los siguientes tipos de direcciones a diversos tipos de túneles:

  - A túneles manuales: dirección global o de cualquier tipo de difusión.
  - A túneles ISATAP: dirección global con EUI-6.
  - A túneles 6to4: ninguna dirección.

- **Longitud del prefijo**: la longitud del prefijo IPv6 global es un valor de 0 a 128 que indica la cantidad de bits contiguos de orden superior de la dirección comprende el prefijo (la porción de red de la dirección).
- **EUI-64**: seleccione el parámetro EUI-64 para identificar la porción del ID de interfaz de la dirección IPv6 global mediante el formato EUI-64 según la dirección MAC de un dispositivo.

PASO 5 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Lista de routers predeterminados IPv6

La página Lista de routers predeterminados IPv6 permite configurar y ver las direcciones de router IPv6 predeterminadas. Esta lista contiene los routers que son candidatos a convertirse en el router predeterminado del dispositivo para el tráfico no local (puede estar vacía). El dispositivo selecciona aleatoriamente un router de la lista. El dispositivo admite un router predeterminado IPv6 estático. Los routers predeterminados dinámicos son routers que han enviado avisos de router a la interfaz IPv6 del dispositivo.

Al añadir o eliminar direcciones IP, se producen los siguientes eventos:

- Al eliminar una interfaz IP, se eliminan todas las direcciones IP del router predeterminado. Las direcciones IP dinámicas no se pueden eliminar.
- Aparece un mensaje de alerta después de que se hace el intento de insertar más de una dirección definida por el usuario.
- Aparece un mensaje de alerta al intentar insertar una dirección de tipo local sin enlace, es decir, "fe80:".

Para definir un router predeterminado:

PASO 1 En el modo del sistema Capa 2, haga clic en **Administración > Interfaz de administración > Lista de routers predeterminados IPv6**.
En el modo del sistema Capa 3, haga clic en **Configuración de IP** > **Administración e interfaces IPv6** > **Lista de routers predeterminados IPv6**.

En esta página se muestran los siguientes campos para cada router predeterminado:

- **Interfaz**: interfaz IPv6 de salida donde reside el router predeterminado.
- **Dirección IPv6 de router predeterminada**: dirección IP local de enlace del router predeterminado.
- **Tipo**: la configuración del router predeterminado que incluye las siguientes opciones:
  - *Estática*: el router predeterminado se ha añadido manualmente a esta tabla mediante el botón **Añadir**.
  - *Dinámica*: el router predeterminado se ha configurado dinámicamente.
- **Estado**: especifica el estado del router. Los valores son:
  - *Alcanzable*: se sabe que el router es accesible.
  - *Inalcanzable*: se sabe que el router es inaccesible.

PASO 2 Haga clic en **Añadir** para añadir un router predeterminado estático.

PASO 3 Ingrese los siguientes campos:

- **Interfaz de enlace local (Capa 2)**: muestra la interfaz local de enlace de salida.
- **Dirección IPv6 de router predeterminada**: la dirección IP del router predeterminado.

PASO 4 Haga clic en **Aplicar**. El router predeterminado se guarda en el archivo de configuración en ejecución.

Definición de la información de vecinos IPv6

La página Vecinos IPv6 permite configurar y ver la lista de vecinos IPv6 en la interfaz IPv6. En la Tabla de vecinos IPv6 (también conocida como Caché de detección de vecinos IPv6), se muestran las direcciones MAC de los vecinos IPv6 que están en la misma subred IPv6 que el dispositivo. Esto es el equivalente IPv6 de la tabla ARP para IPv4. Cuando el dispositivo necesita comunicarse con sus vecinos, usa la Tabla de vecinos IPv6 para determinar las direcciones MAC basadas en sus direcciones IPv6.

La página muestra los vecinos que se han detectado automáticamente o las entradas configuradas manualmente. Cada entrada muestra con qué interfaz está conectado el vecino, las direcciones MAC e IPv6 del vecino, el tipo de entrada (estática o dinámica) y el estado del vecino.

Para definir vecinos IPv6:

PASO 1 En el modo del sistema Capa 2, haga clic en **Administración > Interfaz de administración > Vecinos IPv6**.
En el modo del sistema Capa 3, haga clic en **Configuración de IP** > **Administración e interfaces IPv6** > **Vecinos IPv6**.

Usted puede seleccionar la opción **Borrar tabla** para borrar algunas o todas las direcciones IPv6 en la Tabla de vecino IPv6.

- **Solo estático**: elimina las entradas de direcciones IPv6 estáticas.
- **Solo dinámica**: elimina las entradas de direcciones IPv6 dinámicas.
- **Dinámicas y estáticas**: elimina las entradas de direcciones IPv6 dinámicas y estáticas.

Para las interfaces de vecindad se muestran los siguientes campos:

- **Interfaz**: tipo de interfaz IPv6 de vecindad.
- **Dirección IPv6**: dirección IPv6 de un vecino.
- **Dirección MAC**: dirección MAC asignada a la dirección IPv6 especificada.
- **Tipo**: tipo de entrada de información de caché de detección de vecinos (estática o dinámica).
- **Estado**: especifica el estado de los vecinos IPv6. Los valores son:
  - *Incompleto*: la resolución de dirección está funcionando. El vecino aún no ha respondido.
  - *Alcanzable*: se sabe que el vecino es accesible.
  - *Obsoleto*: el vecino anteriormente conocido es inalcanzable. No se toma ninguna medida para verificar su accesibilidad hasta que se deba enviar el tráfico.
  - *Retraso*: el vecino anteriormente conocido es inalcanzable. La interfaz está en estado de Retraso durante un Tiempo de retraso predefinido. Si no se recibe confirmación de accesibilidad, el estado cambia a Sonda.
  - *Sonda*: ya no se sabe si el vecino es accesible, y se están enviando sondas de solicitudes de vecinos de unidifusión para verificar la accesibilidad.
- **Router**: especifica si el vecino es un router (**Sí** o **No**).

PASO 2 Para añadir un vecino a la tabla, haga clic en **Añadir**.

PASO 3 Ingrese los valores para los siguientes campos:

- **Interfaz**: la interfaz IPv6 de vecindad para añadir.
- **Dirección IPv6**: ingrese la dirección de red IPv6 asignada a la interfaz. La dirección debe ser una dirección IPv6 válida.

- **Dirección MAC**: ingrese la dirección MAC asignada a la dirección IPv6 especificada.

PASO 4 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

PASO 5 Para cambiar el tipo de una dirección IP de **Dinámico** a **Estático**, seleccione la dirección, haga clic en **Editar** y use la página Editar vecinos IPv6.

Lista de prefijos IPv6

Cuando se configura Seguridad de primer salto, es posible definir reglas de filtrado en base a prefijos IPv6. Estas listas se pueden definir en la página Lista de prefijos IPv6.

Las listas de prefijos se configuran con las palabras clave **permit** o **deny** para permitir o rechazar un prefijo en base a una condición de coincidencia. Se aplica un rechazo implícito al tráfico que no coincide con ninguna entrada de la lista de prefijos.

Una entrada de lista de prefijos está compuesta por una dirección IP y una máscara de bits. La dirección IP puede ser para una red con clase, subred o ruta de un solo host. La máscara de bits es un número que oscila entre 1 y 32.

Las listas de prefijos se configuran para filtrar el tráfico en base a una coincidencia de longitud de prefijo exacta o a una coincidencia dentro de un intervalo cuando se usan las palabras clave ge y le.

Los parámetros **Mayor que** y **Menor que** se usan para indicar un intervalo de longitudes de prefijos y proporcionar una configuración más flexible que cuando se usa solo el argumento red/longitud. La lista de prefijos se procesa con una coincidencia exacta cuando no se indican los parámetros **Mayor que** ni **Menor que**. Si solo se indica el parámetro **Mayor que**, el intervalo es el valor que se ingresa para **Mayor que** hasta una longitud total de 32 bits. Si solo se especifica el parámetro **Menor que**, el intervalo es desde el valor que se ingresó para el argumento red/longitud hasta **Menor que**. Si se introducen los dos argumentos **Mayor que** y **Menor que**, el intervalo está entre los valores usados para **Mayor que** y **Mayor que**.

Para crear una lista de prefijos:

PASO 1 (En Capa 3) Haga clic en **Configuración de IP > Interfaces de administración IPv6 > Lista de prefijos IPv6**.

o

(En Capa 2) Haga clic en **Administración > Interfaces de administración IPv6 > Lista de prefijos IPv6**.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los siguientes campos:

- **Nombre de lista**: seleccione una de las siguientes opciones:
  - *Usar lista existente*: seleccione una lista previamente definida para agregarle un prefijo.
  - *Crear nueva lista*: introduzca un nombre para crear una lista nueva.

- **Número de secuencia**: indica el lugar del prefijo dentro de la lista de prefijos. Seleccione una de las siguientes opciones:
  - *Numeración automática*: coloca el nuevo prefijo IPV6 después de la última entrada de la lista de prefijos. El número de secuencia equivale al último número de secuencia más 5. Si la lista está vacía, la primera entrada de lista de prefijo tiene asignado el número 5 y las entradas de lista de prefijos subsiguientes aumentan de a 5.
  - *Definido por el usuario*: coloca el nuevo prefijo IPV6 en el lugar especificado por el parámetro. Si ya existe una entrada con ese número, será reemplazado por uno nuevo.
- **Tipo de regla**: introduzca la regla para la lista de prefijos:
  - *Permitir*: permite las redes que coinciden con la condición.
  - *Rechazar*: rechaza las redes que coinciden con la condición.
  - *Descripción*: texto.
- **Prefijo IPv6**: prefijo de la ruta IP.
- **Longitud de prefijo**: longitud de prefijo de la ruta IP.
- **Mayor que**: longitud de prefijo mínima para usar en la coincidencia. Seleccione una de las siguientes opciones:
  - *Sin límite*: longitud de prefijo sin límite mínimo para usar en la coincidencia.
  - *Definido por el usuario*: longitud de prefijo mínima para coincidir.
- **Menor que**: longitud de prefijo máxima para usar en la coincidencia. Seleccione una de las siguientes opciones:
  - *Sin límite*: longitud de prefijo sin límite máximo para usar en la coincidencia.
  - *Definido por el usuario*: longitud de prefijo máxima para coincidir.
- **Descripción**: introduzca una descripción de la lista de prefijos.

PASO 4 Haga clic en **Aplicar** para guardar la configuración en el archivo de configuración en ejecución.

Visualización de la tabla de rutas IPv6

La Tabla de reenvíos IPv6 contiene las distintas rutas que se configuraron. Una de estas rutas es una ruta predeterminada (dirección IPv6: 0) que usa el router predeterminado seleccionado de la Lista de routers predeterminados IPv6 para enviar paquetes a dispositivos de destino que no están en la misma subred IPv6 que el dispositivo. Además de la ruta predeterminada, la tabla también contiene rutas dinámicas que son rutas de redirección ICMP recibidas de routers IPv6 mediante mensajes de redirección ICMP. Esto puede suceder cuando el router predeterminado que usa el dispositivo no es el router para el tráfico a las subredes IPv6 con el que el dispositivo desea comunicarse.

Para ver las rutas IPv6:

Para ver las entradas de enrutamiento IPv6 en el modo del sistema Capa 2:

PASO 1 Haga clic en **Administración > Interfaz de administración > Rutas IPv6**.

o

Para ver las entradas de enrutamiento IPv6 en el modo de capa 3 del sistema:
Haga clic en **Configuración de IP** > **Administración e interfaces IPv6** > **Rutas IPv6**.

Esta página muestra los siguientes campos:

- **Prefijo IPv6**: prefijo de ruta IP para la dirección de subred IPv6 de destino.
- **Longitud de prefijo**: longitud del prefijo de la ruta IP para la dirección de subred IPv6 de destino. Está precedida por una diagonal.
- **Interfaz**: interfaz que se usa para reenviar el paquete.
- **Salto siguiente**: Por lo general, es la dirección de un router vecino y puede ser uno de los siguientes tipos.
  - *Enlace local*: una dirección IPv6 y una interfaz IPv6 que identifican hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: una dirección IPv6 que es un tipo de dirección IPv6 de unidifusión global que es visible y accesible desde otras redes.
  - *Punto a punto*: un túnel punto a punto.
- **Métrico**: valor que se usa para comparar esta ruta con otras rutas con el mismo destino en la tabla de routers IPv6. Todas las rutas predeterminadas tiene el mismo valor.

- **Duración**: período de tiempo durante el cual el paquete se puede enviar y reenviar, antes de su eliminación.
- **Tipo de ruta**: cómo está conectado el destino y el método que se usa para obtener la entrada. Los siguientes valores son:
  - *Local*: red conectada directamente cuyo prefijo deriva de una dirección IPv6 de un dispositivo configurado manualmente.
  - *Dinámica*: el destino está indirectamente conectado (remoto) a la dirección de subred IPv6. La entrada se ha obtenido dinámicamente a través del protocolo ICMP o ND.
  - *Estática*: el usuario ha configurado manualmente la entrada.

Retransmisión DHCPv6

La retransmisión DHCPv6 se usa para retransmitir mensajes DHCPv6 a los servidores DHCPv6. Se define en RFC 3315.

Cuando el cliente DHCPv6 no se conecta directamente al servidor DHCPv6, un agente de retransmisión DHCPv6 (el dispositivo) al que este cliente DHCPv6 está directamente conectado encapsula los mensajes recibidos del cliente DHCPv6 directamente conectado y los reenvía al servidor DHCPv6.

En la dirección opuesta, el agente de retransmisión desencapsula los paquetes recibidos del servidor DHCPv6 y los reenvía al cliente DHCPv6.

El usuario debe configurar la lista de servidores DHCP a los que se reenvían los paquetes. Se pueden configurar dos conjuntos de servidores DHCPv6:

- **Destinos globales**: los paquetes siempre se retransmiten a estos servidores DHCPv6.
- **Lista de interfaces**: esta es una lista de servidores DHCPv6 por interfaz. Cuando se recibe un paquete DHCPv6 en una interfaz, el paquete se retransmite a los servidores de la lista de interfaces (si existe) y a los servidores de la lista de destinos globales.

Dependencias con otras funciones

El cliente DHCPv6 y las funciones de retransmisión DHCPv6 son mutuamente exclusivos en una interfaz.

Destinos globales

Para configurar una lista de servidores DHCPv6 a los que se retransmiten todos los paquetes DHCPv6:

PASO 1 Haga clic en **Configuración de IP > Administración e interfaces IPv6 > Retransmisión DHCPv6 > Destinos globales**.

PASO 2 Para agregar un servidor DHCPv6 predeterminado, haga clic en **Añadir**.

PASO 3 Ingrese los campos:

- **Tipo de dirección IPv6**: ingrese el tipo de dirección de destino a la que se reenvían los mensajes del cliente. El tipo de dirección puede ser **Enlace local**, **Global** o **Multidifusión** (All_DHCP_Relay_Agents_and_Servers).
- **Dirección IP del servidor DHCPv6**: ingrese la dirección del servidor DHCPv6 a la que se reenvían los paquetes.
- **Interfaz IPv6 (destino)**: ingrese la interfaz en que se transmiten los paquetes cuando el tipo de dirección del servidor DHCPv6 es **Enlace local** o **Multidifusión**.

PASO 4 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Configuración de la interfaz

Para activar la función Retransmisión DHCPv6 en una interfaz y configurar una lista de servidores DHCPv6 a los que se retransmiten los paquetes DHCPv6 cuando se reciben en esta interfaz:

PASO 1 Haga clic en **Configuración de IP > Administración e interfaces IPv6 > Retransmisión DHCPv6 > Configuración de la interfaz**.

PASO 2 Para activar DHCPv6 en una interfaz y agregar opcionalmente un servidor DHCPv6 para una interfaz, haga clic en **Añadir**.

Ingrese los campos:

- **Interfaz de origen**: seleccione la interfaz (puerto, LAG, VLAN o túnel) para la que está activada la opción Retransmisión DHCPv6.
- **Usar destinos globales solamente**: seleccione esta opción para reenviar los paquetes a los servidores de destino global DHCPv6 solamente.
- **Tipo de dirección IPv6**: ingrese el tipo de dirección de destino a la que se reenvían los mensajes del cliente. El tipo de dirección puede ser **Enlace local**, **Global** o **Multidifusión** (All_DHCP_Relay_Agents_and_Servers).
- **Dirección IP del servidor DHCPv6**: ingrese la dirección del servidor DHCPv6 a la que se reenvían los paquetes.
- **Interfaz IPv6 (destino)**: ingrese la interfaz en que se transmiten los paquetes cuando el tipo de dirección del servidor DHCPv6 es **Enlace local** o **Multidifusión**.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Nombre de dominio

El DNS (Domain Name System, sistema de nombres de dominio) traduce nombres de dominio en direcciones IP a los fines de ubicar y dirigir hosts.

Como cliente DNS, el dispositivo convierte los nombres de dominio en direcciones IP mediante uno o más servidores DNS configurados.

Configuración DNS

Utilice la página Configuración DNS para activar la función DNS, para configurar servidores DNS y para establecer el dominio predeterminado que usará el dispositivo.

PASO 1 Haga clic en **Configuración de IP** > **Sistema de nombres de dominio** > **Configuración DNS**.

PASO 2 Ingrese los parámetros.

- **DNS**: seleccione esta opción para designar el dispositivo como cliente DNS, que puede convertir los nombres DNS en direcciones IP mediante uno o más servidores DNS configurados.
- **Reintentos de sondeo**: ingrese el número de veces que desea enviar una consulta DNS a un servidor DNS hasta que el dispositivo decida que el servidor DNS no existe.
- **Tiempo de espera de sondeo**: especifique la cantidad de segundos que el dispositivo esperará por una respuesta a una consulta DNS.
- **Intervalo de sondeo**: ingrese la frecuencia (en segundos) con que el dispositivo envía paquetes de consulta DNS una vez agotada la cantidad de reintentos.
  - *Usar predeterminado*: seleccione esta opción para usar el valor predeterminado.

    Este valor = 2* (Reintentos de sondeo + 1)* Tiempo de espera de sondeo.
  - *Definido por el usuario*: seleccione esta opción para ingresar un valor definido por el usuario.
- **Parámetros predeterminados**: ingrese los siguientes parámetros predeterminados:
  - **Nombre de dominio predeterminado**: ingrese el nombre de dominio DNS que se utilizó para completar un nombre de host no calificado. El dispositivo lo agrega a todos los NFQDN (Non-Fully Qualified Domain Names, nombres de dominio que no están completamente calificados) y los transforma en FQDN (Fully Qualified Domain Names, nombres de dominio completamente calificados).

    NOTA No incluya el punto inicial que separa un nombre no calificado del nombre de dominio (como cisco.com).

- **Lista de búsqueda de dominio DHCP**: haga clic en **Detalles** para ver la lista de servidores DNS configurados en el dispositivo.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Tabla del servidor DNS: se muestran los siguientes campos para cada servidor DNS configurado:

- **Servidor DNS**: la dirección IP del servidor DNS.
- **Preferencia**: cada servidor tiene un valor de preferencia; un valor inferior significa mayor probabilidad de que se use.
- **Origen**: origen de la dirección IP del servidor (estático, DHCPv4 o DHCPv6).
- **Interfaz**: interfaz de la dirección IP del servidor.

PASO 4 Se pueden definir hasta ocho servidores DNS. Para añadir un servidor DNS, haga clic en **Añadir**.

Ingrese los parámetros.

- **Versión IP**: seleccione Versión 6 para IPv6 o Versión 4 para IPv4.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: si el tipo de dirección IPv6 es Enlace local, seleccione la interfaz a través de la cual se recibe.
- **Dirección IP del servidor DNS**: ingrese la dirección IP del servidor DNS.
- **Preferencia**: seleccione un valor que determine el orden en que se usan los dominios (de bajo a alto). Esto determina de manera efectiva el orden en que se completan los nombres no calificados durante las consultas DNS.

PASO 5 Haga clic en **Aplicar**. El servidor DNS se guarda en el archivo de configuración en ejecución.

Lista de búsqueda

La lista de búsqueda puede contener una entrada estática definida por el usuario en la página Configuración DNS y entradas dinámicas recibidas de los servidores DHCPv4 y DHCPv6.

Para ver los nombres de dominio que se configuraron en el dispositivo:

PASO 1 Haga clic en **Configuración de IP** > **Sistema de nombres de dominio** > **Lista de búsqueda**.

Se muestran los siguientes campos para cada servidor DNS configurado en el dispositivo:

- **Nombre de dominio**: nombre de dominio que se puede usar en el dispositivo.
- **Origen**: origen de la dirección IP del servidor (estático, DHCPv4 o DHCPv6) para este dominio.
- **Interfaz**: interfaz de la dirección IP del servidor para este dominio.
- **Preferencia**: este es el orden en que se usan los dominios (de bajo a alto). Esto determina de manera efectiva el orden en que se completan los nombres no calificados durante las consultas DNS.

Asignación de host

Las asignaciones de nombre de host o direcciones IP se almacenan en la Tabla de asignación de host (Caché de DNS).

Esta caché puede contener el siguiente tipo de entradas:

- **Entradas estáticas**: son pares de asignaciones que se agregaron manualmente a la caché. Puede haber hasta 64 entradas estáticas.
- **Entradas dinámicas**: son partes de asignaciones que agregó el sistema como resultado de su uso por porte del usuario, o una entrada para cada dirección IP configurada en el dispositivo por DHCP. Puede haber 256 entradas dinámicas.

La resolución de nombre siempre comienza verificando las entradas estáticas, continúa verificando las entradas dinámicas y termina enviando solicitudes al servidor DNS externo.

Se admiten ocho direcciones IP por servidor DNS por nombre de host.

Para agregar un nombre de host y su dirección IP:

PASO 1 Haga clic en **Configuración de IP** > **Sistema de nombres de dominio**> **Asignación de host**.

PASO 2 Si lo requiere, puede seleccionar la opción **Borrar tabla** para borrar algunas o todas las entradas de la Tabla de asignación de host.

- **Sólo estático**: elimina los hosts estáticos.
- **Sólo dinámico**: elimina los hosts dinámicos.
- **Dinámicos y estáticos**: elimina los hosts dinámicos y estáticos.

En la Tabla de asignación de host, se muestran los siguientes campos:

- **Nombre del host**: nombre de host definido por el usuario o nombre completamente calificado.
- **Dirección IP**: la dirección IP del host.
- **Versión de IP**: versión de IP de la dirección IP del host.
- **Tipo**: puede ser una entrada **Dinámica** o **Estática** en la caché.
- **Estado**: muestra los resultados de los intentos de acceso al host.
  - *Acep.*: el intento se realizó correctamente.
  - *Caché negativa*: el intento falló; no intente nuevamente.
  - *Sin respuesta*: no hubo respuesta, pero el sistema puede volver a intentarlo en el futuro.
- **TTL (Seg.)**: si esta es una entrada dinámica, esta opción indica cuánto tiempo permanecerá en la caché.
- **TTL restante (Seg.)**: si esta es una entrada dinámica, esta opción indica cuánto tiempo más permanecerá en la caché.

PASO 3 Para añadir una asignación de host, haga clic en **Añadir**.

PASO 4 Ingrese los parámetros.

- **Versión de IP**: seleccione **Versión 6** para IPv6 o **Versión 4** para IPv4.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: si el tipo de dirección IPv6 es Enlace local, seleccione la interfaz a través de la cual se recibe.

- **Nombre del host**: ingrese un nombre de host definido por el usuario o un nombre completamente calificado. Los nombres de host están restringidos a las letras A a Z de ASCII (se distingue entre mayúsculas y minúsculas), los dígitos 0 a 9, el guión bajo y el guión. Se utiliza un punto (.) para separar las etiquetas.
- **Dirección IP**: ingrese una sola dirección o hasta ocho direcciones IP asociadas (IPv4 o IPv6).

PASO 5 Haga clic en **Aplicar**. La configuración se guarda en el archivo Configuración en ejecución.

19

Seguridad

En esta sección, se describe la seguridad del dispositivo y el control de acceso. El sistema admite diferentes tipos de seguridad.

En la lista de temas que figura a continuación se detallan los diferentes tipos de funciones de seguridad descritos en esta sección. Algunas funciones se utilizan para más de un tipo de seguridad o control, por lo que aparecen dos veces en la lista de temas siguiente.

El permiso para administrar el dispositivo se describe en las siguientes secciones:

- **Definición de usuarios**
- **Configuración de TACACS+**
- **Configuración de RADIUS**
- **Método de acceso a administración**
- **Autenticación de acceso a administración**
- **Gestión de datos confidenciales**
- **Servidor SSL**

La protección contra ataques dirigidos a la CPU del dispositivo se describe en las siguientes secciones:

- **Configuración de servicios TCP/UDP**
- **Definición del control de saturación**
- **Control de acceso**

El control de acceso de los usuarios finales a la red a través del dispositivo se describe en las siguientes secciones:

- **Método de acceso a administración**
- **Método de acceso a administración**
- **Configuración de TACACS+**
- **Configuración de RADIUS**

- Configuración de la seguridad de puertos
- 802.1x
- Intervalo de tiempo

La protección contra otros usuarios de la red se describe en las siguientes secciones. Estos son ataques que pasan a través del dispositivo, pero que no están dirigidos a este.

- Prevención de negación de servicio
- Indagación de DHCP
- Servidor SSL
- Definición del control de saturación
- Configuración de la seguridad de puertos
- Protección de la IP de origen
- Inspección de ARP
- Control de acceso
- Seguridad de primer salto

Definición de usuarios

El nombre de usuario y la contraseña predeterminados son **cisco/cisco**. La primera vez que inicie sesión con el nombre de usuario y la contraseña predeterminados, deberá ingresar una nueva contraseña. La opción Complejidad de la contraseña está activada de manera predeterminada. Si la contraseña que elige no es lo suficientemente compleja, (la opción **Configuración de complejidad de la contraseña** se activa en la página Seguridad de la contraseña), se le solicitará que cree otra contraseña.

Configuración de cuentas de usuario

En la página Cuentas de usuario, se puede ingresar usuarios adicionales que tienen permitido acceder al dispositivo (solo lectura o solo escritura) o cambiar las contraseñas de usuarios existentes.

Después de añadir un usuario de nivel 15 (como se describe a continuación), se elimina al usuario predeterminado del sistema.

NOTA No es posible eliminar a todos los usuarios. Al seleccionar todos los usuarios, el botón **Eliminar** no está disponible.

Para añadir un nuevo usuario:

PASO 1 Haga clic en **Administración** > **Cuentas de Usuario**.

Esta página muestra los usuarios definidos en el sistema y su nivel de privilegio de usuario.

PASO 2 Seleccione **Servicio de recuperación de contraseña** para habilitar esta función. Una vez habilitada, un usuario final, que tiene acceso físico al puerto de la consola del dispositivo, puede ingresar al menú de inicio y activar el proceso de recuperación de la contraseña. Cuando el proceso de inicio del sistema finaliza, usted puede iniciar sesión en el dispositivo sin la autenticación de la contraseña. El ingreso al dispositivo solo se permite a través de la consola y únicamente si la consola está conectada al dispositivo con acceso físico.

Cuando el mecanismo de recuperación de la contraseña está deshabilitado, igualmente puede acceder al menú de inicio y activar el proceso de recuperación de la contraseña. La diferencia es que en ese caso, todos los archivos de usuario y de configuración se eliminan durante el proceso de inicio del sistema y se genera un mensaje de registro correspondiente al terminal.

PASO 3 Haga clic en **Añadir** para añadir un nuevo usuario o en **Editar** para modificar un usuario.

PASO 4 Ingrese los parámetros.

- **Nombre de usuario**: ingrese un nombre de usuario nuevo con hasta un máximo de 20 caracteres. No se permiten los caracteres UTF-8.
- **Contraseña**: ingrese una contraseña (los caracteres UTF-8 no están permitidos). Si la seguridad y la complejidad de la contraseña están definidas, la contraseña del usuario debe cumplir con la política configurada en **Configuración de reglas de complejidad de la contraseña**.
- **Confirmar contraseña**: ingrese la contraseña nuevamente.
- **Medidor de seguridad de la contraseña**: indica la seguridad de la contraseña. La política para la seguridad y la complejidad de las contraseñas se configura en la página Seguridad de la contraseña.
- **Nivel de usuario**: seleccione el nivel de privilegio del usuario que se está añadiendo o editando.
  - *Acceso a la CLI de sólo lectura (1)*: el usuario no puede acceder a la GUI, sino sólo a los comandos de la CLI que no cambian la configuración del dispositivo.
  - *Acceso a la CLI de lectura/escritura limitada (7)*: el usuario no puede acceder a la GUI, sino sólo a los comandos de la CLI que no cambian la configuración del dispositivo. Para obtener mayor información, consulte la *Guía de referencia de CLI*.
  - *Acceso de administración de lectura/escritura (15)*: el usuario puede acceder a la GUI y configurar el dispositivo.

PASO 5 Haga clic en **Aplicar**. El usuario se agrega al archivo de configuración en ejecución del dispositivo.

Configuración de reglas de complejidad de la contraseña

Las contraseñas se utilizan para autenticar a los usuarios que acceden al dispositivo. Las contraseñas simples son posibles peligros a la seguridad. Por lo tanto, de forma predeterminada se imponen los requisitos de complejidad de la contraseña, y pueden configurarse como sea necesario. Los requisitos de complejidad de la contraseña se configuran en la página **Seguridad de la contraseña**, a la que se accede mediante el menú desplegable Seguridad. En esta página, también puede configurarse el tiempo de vencimiento de la contraseña.

Para definir las reglas de complejidad de la contraseña:

PASO 1 Haga clic en **Seguridad** > **Seguridad de la contraseña**.

PASO 2 Ingrese los siguientes parámetros de vencimiento para las contraseñas:

- **Vencimiento de la contraseña**: si se selecciona esta opción, se le pide al usuario que cambie la contraseña cuando el **Tiempo de vencimiento de la contraseña** caduque.
- **Tiempo de vencimiento de la contraseña**: ingrese el número de días que pueden transcurrir antes de que se solicite al usuario que cambie la contraseña.

NOTA El vencimiento de la contraseña también se aplica a las contraseñas de longitud cero (sin contraseña).

PASO 3 Seleccione **Configuración de complejidad de la contraseña** para habilitar las reglas de complejidad para las contraseñas.

Si la complejidad de la contraseña está habilitada, las nuevas contraseñas deben ajustarse a los siguientes parámetros predeterminados:

- Tener un mínimo de ocho caracteres.
- Contener caracteres de, al menos, tres clases (mayúsculas, minúsculas, números y caracteres especiales disponibles en un teclado estándar).
- Ser diferentes de la contraseña actual.
- No contener caracteres repetidos más de tres veces consecutivas.
- No repetir ni invertir el nombre de los usuarios ni ninguna variante que se obtenga al cambiar el tamaño de los caracteres.
- No repetir ni invertir el nombre de los fabricantes ni ninguna variante que se obtenga al cambiar el tamaño de los caracteres.

PASO 4 Si la **Configuración de complejidad de la contraseña** está habilitada, deben configurarse los siguientes parámetros:

- **Longitud mínima de la contraseña**: ingrese el número mínimo de caracteres necesarios para las contraseñas.

  NOTA Está permitido ingresar una contraseña de longitud cero (sin contraseña), e incluso se le puede asignar un vencimiento.

- **Repetición de caracteres permitida**: ingrese la cantidad de veces que se puede repetir un carácter.
- **Cantidad mínima de clases de caracteres**: ingrese el número de las clases de caracteres que deben conformar una contraseña. Las clases de caracteres son: minúsculas (1), mayúsculas (2), dígitos (3) y símbolos o caracteres especiales (4).
- **La contraseña nueva debe ser distinta de la actual**: si se selecciona este parámetro, la nueva contraseña no puede ser la misma que la actual.

PASO 5 Haga clic en **Aplicar**. La configuración de la contraseña se escribe en el archivo Configuración en ejecución.

NOTA La configuración de la equivalencia de nombre de usuario y contraseña y de la equivalencia de fabricante y contraseña se puede realizar mediante la CLI. Para obtener más información, consulte la *Guía de referencia de CLI*.

Configuración de TACACS+

Una organización puede instalar un servidor TACACS+ (*Terminal Access Controller Access Control System*, sistema de control de acceso al controlador de acceso al terminal) para proporcionar seguridad centralizada a todos sus dispositivos. De esta forma, la autenticación y la autorización pueden manejarse desde un solo servidor para todos los dispositivos de la organización.

El dispositivo puede ser un cliente TACACS+ que usa el servidor TACACS+ para los siguientes servicios:

- **Autenticación**: proporciona la autenticación de los usuarios que inician sesión en el dispositivo con nombres de usuario y contraseñas definidas por el usuario.
- **Autorización**: se realiza al iniciar sesión. Cuando finaliza la sesión de autenticación, comienza una sesión de autorización con el nombre de usuario autenticado. El servidor TACACS+ luego comprueba los privilegios del usuario.
- **Contabilidad**: active la contabilidad de las sesiones de conexión mediante el servidor TACACS+. Esto permite al administrador del sistema generar informes de contabilidad desde el servidor TACACS+.

Además de proporcionar servicios de autenticación y autorización, el protocolo TACACS+ permite asegurar la protección de los mensajes TACACS a través del cifrado del cuerpo del mensaje TACACS.

TACACS+ solo es compatible con IPv4.

Algunos servidores TACACS+ admiten una sola conexión que permite que el dispositivo reciba toda la información en una sola conexión. Si el servidor TACACS+ no admite una sola conexión, el dispositivo vuelve a varias conexiones.

Contabilidad con un servidor TACACS+

El usuario puede activar la contabilidad de las sesiones de conexión con un servidor RADIUS o TACACS+.

El puerto TCP configurado por el usuario que se usa para la contabilidad de servidor TACACS+ es el mismo puerto TCP que se usa para la autenticación y la autorización de servidor TACACS+.

El dispositivo envía la siguiente información al servidor TACACS+ cuando un usuario inicia o cierra sesión.

Tabla 2:

Argumento	Descripción	En mensaje de inicio	En mensaje de detención
task_id	Un identificador exclusivo de la sesión de contabilidad.	Sí	Sí
usuario	El nombre de usuario que se ingresa para autenticar el inicio de sesión.	Sí	Sí
rem-addr	La dirección IP del usuario.	Sí	Sí
elapsed-time	Indica cuánto tiempo estuvo conectado el usuario.	No	Sí
reason	Indica por qué se finalizó la sesión.	No	Sí

Valores predeterminados

Los siguientes valores predeterminados son relevantes para esta función:

- No se define ningún servidor TACACS+ de forma predeterminada.
- Si configura un servidor TACACS+, la función de contabilidad está desactivada de forma predeterminada.

Interacciones con otras funciones

No es posible activar la contabilidad en un servidor RADIUS y un servidor TACACS+ a la vez.

Flujo de trabajo

Para usar un servidor TACACS+, realice lo siguiente:

PASO 1 Abra una cuenta para un usuario en el servidor TACACS+.

PASO 2 Configure ese servidor y los demás parámetros en las páginas TACACS+ y Añadir servidor TACACS+.

PASO 3 Seleccione **TACACS+** en la página Autenticación de acceso a administración para que cuando un usuario inicie sesión en el dispositivo, se realice la autenticación en el servidor TACACS+, y no en la base de datos local.

NOTA Si se configura más de un servidor TACACS+, el dispositivo usa las prioridades configuradas de los servidores TACACS+ disponibles para seleccionar el servidor TACACS+ que usará el dispositivo.

Configuración de un servidor TACACS+

La página TACACS+ permite configurar servidores TACACS+.

Solo los usuarios que tienen el nivel de privilegio 15 en el servidor TACACS+ pueden administrar el dispositivo. El nivel de privilegio 15 se le asigna a un usuario o a un grupo de usuarios en el servidor TACACS+ mediante la siguiente cadena en la definición del usuario o del grupo:

```
service = exec {
priv-lvl = 15
}
```

Para configurar los parámetros del servidor TACACS+:

PASO 1 Haga clic en **Seguridad** > **TACACS+**.

PASO 2 Active la **Contabilidad TACACS+** si lo requiere. Consulte la explicación en la sección **Contabilidad con un servidor TACACS+**.

PASO 3 Ingrese los siguientes parámetros predeterminados:

- **Secuencia de clave**: ingrese la **secuencia de clave** predeterminada que se usa para comunicar todos los servidores TACACS+ en el modo **Cifrado** o **Texto simple**. El dispositivo puede configurarse para utilizar esta clave o para utilizar una clave ingresada para un servidor específico (que se ingresa en la página Añadir servidor TACACS+).

Si no ingresa una secuencia de clave en este campo, la clave de servidor que se ingrese en la página Añadir servidor TACACS+ deberá coincidir con la clave de cifrado que usa el servidor TACACS+.

Si ingresa tanto una cadena de clave aquí como una cadena de clave para un servidor TACACS+ en particular, la cadena de clave configurada para el servidor TACACS+ en particular tiene prioridad.

- **Tiempo de espera para respuesta**: ingrese el tiempo que debe transcurrir antes de que la conexión entre el dispositivo y el servidor TACACS+ se agote. Si no se ingresa un valor en la página Añadir servidor TACACS+ para un servidor específico, el valor se toma de este campo.
- **Interfaz IPv4 de origen**: seleccione la interfaz de origen IPv4 del dispositivo que se usará en los mensajes enviados para la comunicación con el servidor TACACS+.
- **Interfaz IPv6 de origen**: seleccione la interfaz de origen IPv6 del dispositivo que se usará en los mensajes enviados para la comunicación con el servidor TACACS+.

  NOTA Si se selecciona la opción Automática, el sistema toma la dirección IP de origen de la dirección IP definida en la interfaz de salida.

  PASO 4 Haga clic en **Aplicar**. La configuración de TACACS+ predeterminada se agrega al archivo de configuración en ejecución. Se usa si no se definen los parámetros equivalentes en la página Añadir.

  PASO 5 Para añadir un servidor TACACS+, haga clic en **Añadir**.

  PASO 6 Ingrese los parámetros.

- **Definición del servidor**: seleccione una de las siguientes maneras para identificar el servidor TACACS+:
  - *Por dirección IP*: si esta opción está seleccionada, ingrese la dirección IP del servidor en el campo **Dirección IP/Nombre del servidor**.
  - *Por nombre*: si esta opción está seleccionada, ingrese el nombre del servidor en el campo **Dirección IP/Nombre del servidor**.
- **Versión IP**: seleccione la versión IP admitida de la dirección de origen: IPv6 o IPv4.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.

- **Interfaz local de enlace**: seleccione la interfaz local de enlace (si se selecciona Enlace local como Tipo de dirección IPv6) en la lista.
- **Dirección IP/Nombre del servidor**: ingrese la dirección IP o el nombre del servidor TACACS+.
- **Prioridad**: ingrese el orden en el que se usa este servidor TACACS+. El cero corresponde al servidor TACACS+ de mayor prioridad y al que se usa primero. Si no puede establecer una sesión con el servidor de alta prioridad, el dispositivo lo intenta con el servidor que le sigue en prioridad.
- **Secuencia de clave**: ingrese la secuencia de clave predeterminada que se usa para la autenticación y el cifrado entre el dispositivo y el servidor TACACS+. Esta clave debe coincidir con la clave configurada en el servidor TACACS+.

  Una cadena de clave se utiliza para cifrar las comunicaciones mediante MD5. Puede seleccionar la clave predeterminada en el dispositivo, o bien podrá ingresar la clave en el formato **Cifrado** o **Texto simple**. Si no tiene una cadena de clave cifrada (de otro dispositivo), ingrese la cadena de clave en modo de texto simple y haga clic en **Aplicar**. Se genera y se muestra la cadena de clave cifrada.

  Si ingresa una clave, esa clave anulará la secuencia de clave predeterminada si se definió una para el dispositivo en la página principal.
- **Tiempo de espera para respuesta**: seleccione **Definido por el usuario** e ingrese el tiempo que debe transcurrir antes de que la conexión entre el dispositivo y el servidor TACACS+ se agote. Seleccione **Usar predeterminado** para usar el valor predeterminado que aparece en la página.
- **Puerto IP de autenticación**: ingrese el número de puerto a través del que tiene lugar la sesión de TACACS+.
- **Conexión simple**: seleccione esta opción para habilitar la recepción de toda la información en una conexión simple. Si el servidor TACACS+ no admite una sola conexión, el dispositivo vuelve a varias conexiones.

PASO 7 Haga clic en **Aplicar**. El servidor TACACS+ se agrega al archivo de configuración en ejecución del dispositivo.

PASO 8 Para mostrar los datos confidenciales en texto simple en esta página, haga clic en **Mostrar datos confidenciales como texto simple**.

Configuración de RADIUS

Los servidores del Servicio de acceso telefónico con autorización remota para el usuario (RADIUS) proporcionan un control de acceso de red centralizado basado en 802.1X o MAC. El dispositivo es un cliente RADIUS que puede utilizar un servidor RADIUS para proporcionar seguridad centralizada.

Una organización puede instalar un servidor RADIUS (Remote Authorization Dial-In User Service, servicio de usuario de acceso telefónico de autenticación remota) para proporcionar control centralizado de acceso a redes 802.1X o basadas en MAC para todos sus dispositivos. De esta forma, la autenticación y la autorización pueden manejarse desde un solo servidor para todos los dispositivos de la organización.

El dispositivo puede ser un cliente RADIUS que usa el servidor RADIUS para los siguientes servicios:

- **Autenticación**: proporciona la autenticación de usuarios regulares y 802.1X que inician sesión en el dispositivo con nombres de usuario y contraseñas definidas por el usuario.
- **Autorización**: se realiza al iniciar sesión. Cuando finaliza la sesión de autenticación, comienza una sesión de autorización con el nombre de usuario autenticado. El servidor RADIUS luego comprueba los privilegios del usuario.
- **Contabilidad**: active la contabilidad de las sesiones de conexión mediante el servidor RADIUS. Esto permite al administrador del sistema generar informes de contabilidad desde el servidor RADIUS.

Contabilidad con un servidor RADIUS

El usuario puede activar la contabilidad de las sesiones de conexión con un servidor RADIUS.

El puerto TCP configurado por el usuario que se usa para la contabilidad de servidor RADIUS es el mismo puerto TCP que se usa para la autenticación y la autorización de servidor RADIUS.

Valores predeterminados

Los siguientes valores predeterminados son relevantes para esta función:

- No se define ningún servidor RADIUS de forma predeterminada.
- Si configura un servidor RADIUS, la función de contabilidad está desactivada de forma predeterminada.

Interacciones con otras funciones

No es posible activar la contabilidad en un servidor RADIUS y un servidor TACACS+ a la vez.

Flujo de trabajo de RADIUS

Para usar un servidor RADIUS, realice lo siguiente:

PASO 1 Abra una cuenta para el dispositivo en el servidor RADIUS.

PASO 2 Configure ese servidor y los demás parámetros en las páginas RADIUS y Añadir servidor RADIUS.

NOTA Si se configura más de un servidor RADIUS, el dispositivo usa las prioridades configuradas de los servidores RADIUS disponibles para seleccionar el servidor RADIUS que usará el dispositivo.

Para configurar los parámetros del servidor RADIUS:

PASO 1 Haga clic en **Seguridad** > **RADIUS**.

PASO 2 Ingrese la opción de contabilidad RADIUS. Las opciones disponibles son las siguientes:

- **Control de acceso basado en puertos (Autenticación web, 802.1X y basado en MAC)**: especifica que el servidor RADIUS se usa para la contabilidad del puerto 802.1x. La autenticación basada en la Web solo es compatible en el modo de Capa 2 en dispositivos Sx300 y SG500. En dispositivos SG500XG y SG500X, es compatible en el modo Nativo e Híbrido avanzado XG.
- **Acceso a administración**: especifica que el servidor RADIUS se usa para la contabilidad de inicio de sesión del usuario.
- **Control de acceso basado en puertos y acceso a administración**: especifica que el servidor RADIUS se usa tanto para la contabilidad de inicio de sesión del usuario como para la contabilidad del puerto 802.1X.
- **Ninguna**: especifica que el servidor RADIUS no se usa para la contabilidad.

PASO 3 Ingrese los parámetros predeterminados de RADIUS, si es necesario. Los valores ingresados en Parámetros predeterminados se aplican a todos los servidores. Si no se ingresa un valor para un servidor específico (en la página Añadir servidor RADIUS), el dispositivo usa los valores de estos campos.

- **Reintentos**: ingrese el número de solicitudes transmitidas que se envían al servidor RADIUS antes de que se considere que ocurrió una falla.
- **Tiempo de espera para respuesta**: ingrese la cantidad de segundos que el dispositivo espera una respuesta del servidor RADIUS antes de volver a intentar realizar la consulta, o cambiar al siguiente servidor.
- **Tiempo muerto**: ingrese el número de minutos que transcurren antes de que se desvíen las solicitudes de servicio de un servidor RADIUS que no responde. Si el valor es 0, no se desvía del servidor.

- **Secuencia de clave**: ingrese la secuencia de clave predeterminada que se usa para la autenticación y el cifrado entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con la clave configurada en el servidor RADIUS. Una cadena de clave se utiliza para cifrar las comunicaciones mediante MD5. La clave se puede ingresar en formato **cifrado** o de **texto simple**. Si no tiene una cadena de clave cifrada (de otro dispositivo), ingrese la cadena de clave en modo de texto simple y haga clic en **Aplicar**. Se genera y se muestra la cadena de clave cifrada.

De este modo se anula la cadena de clave predeterminada.

- **Interfaz IPv4 de origen**: seleccione la interfaz de origen IPv4 del dispositivo que se usará en los mensajes para la comunicación con el servidor RADIUS.
- **Interfaz IPv6 de origen**: seleccione la interfaz de origen IPv6 del dispositivo que se usará en los mensajes para la comunicación con el servidor RADIUS.

NOTA Si se selecciona la opción Automática, el sistema toma la dirección IP de origen de la dirección IP definida en la interfaz de salida.

PASO 4 Haga clic en **Aplicar**. La configuración predeterminada de RADIUS para el dispositivo se actualiza en el archivo de configuración en ejecución.

Para añadir un servidor RADIUS, haga clic en **Añadir**.

PASO 5 Ingrese los valores en los campos de cada servidor RADIUS. Para usar los valores predeterminados ingresados en la página RADIUS, seleccione **Usar predeterminado**.

- **Definición del servidor**: seleccione si el servidor RADIUS se identificará por dirección IP o nombre.
- **Versión IP**: seleccione la versión IP de la dirección IP del servidor RADIUS.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: seleccione la interfaz local de enlace (si se selecciona Enlace local como Tipo de dirección IPv6) en la lista.
- **Dirección IP/Nombre del servidor**: ingrese el servidor RADIUS por dirección IP o por nombre.
- **Prioridad**: ingrese la prioridad del servidor. La prioridad determina el orden en que el dispositivo intenta comunicarse con los servidores para autenticar a un usuario. El dispositivo comienza con el servidor RADIUS de mayor prioridad, que corresponde al cero.

Secuencia de clave: ingrese la secuencia de clave que se usa para la autenticación y el cifrado entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con la clave configurada en el servidor RADIUS. La clave se puede ingresar en el formato **Cifrado** o **Texto simple**. Si se selecciona **Usar predeterminado**, el dispositivo intenta autenticarse con el servidor RADIUS al usar la secuencia de clave predeterminada.

- **Tiempo de espera para respuesta**: seleccione **Definido por el usuario** e ingrese la cantidad de segundos que el dispositivo espera una respuesta del servidor RADIUS antes de volver a intentar realizar la consulta o de cambiar al siguiente servidor si se alcanzó el número máximo de reintentos. Si se selecciona **Usar predeterminado**, el dispositivo usa el valor predeterminado para el tiempo de espera.
- **Puerto de autenticación**: ingrese el número del puerto UDP del servidor RADIUS para las solicitudes de autenticación.
- **Puerto de contabilidad**: ingrese el número del puerto UDP del servidor RADIUS para las solicitudes de cuentas.
- **Reintentos**: seleccione **Definido por el usuario** e ingrese el número de solicitudes que se envían al servidor RADIUS antes de que se considere que ocurrió una falla. Si se selecciona **Usar predeterminado**, el dispositivo usa el valor predeterminado para la cantidad de reintentos.
- **Tiempo muerto**: seleccione **Definido por el usuario** e ingrese el número de minutos que deben transcurrir antes de que se desvíen las solicitudes de servicio de un servidor RADIUS que no responde. Si se selecciona **Usar predeterminado**, el dispositivo usa el valor predeterminado para el tiempo muerto. Si ingresa 0 minutos, no hay tiempo muerto.
- **Tipo de uso**: ingrese el tipo de autenticación del servidor RADIUS. Las opciones son:
  - *Inicio de sesión*: el servidor RADIUS se usa para autenticar a los usuarios que solicitan administrar el dispositivo.
  - *802.1X*: el servidor RADIUS se usa para la autenticación de 802.1X.
  - *Todo*: el servidor RADIUS se usa para autenticar a un usuario que solicita administrar el dispositivo y para la autenticación de 802.1X.

PASO 6 Haga clic en **Aplicar**. El servidor RADIUS se agrega al archivo de configuración en ejecución del dispositivo.

PASO 7 Para mostrar los datos confidenciales en texto simple en esta página, haga clic en **Mostrar datos confidenciales como texto simple**.

Método de acceso a administración

Los perfiles de acceso determinan cómo autenticar y autorizar a los usuarios el acceso al dispositivo a través de diversos métodos de acceso. Los perfiles de acceso pueden limitar el acceso de administración de fuentes específicas.

Solo se les otorga acceso de administración al dispositivo a los usuarios que pasan los dos métodos de autenticación del acceso de administración y del perfil de acceso activo.

En el dispositivo, puede haber un solo perfil de acceso activo por vez.

Los perfiles de acceso pueden consistir en una o más reglas. Las reglas se ejecutan en el orden de su prioridad dentro del perfil de acceso (de arriba hacia abajo).

Las reglas están compuestas por filtros que incluyen los siguientes elementos:

- **Métodos de acceso**: métodos para acceder al dispositivo y administrarlo:
  - Telnet
  - Telnet seguro (SSH)
  - Hypertext Transfer Protocol (HTTP, protocolo de transferencia de hipertexto)
  - HTTP seguro (HTTPS)
  - Protocolo de administración de red simple (SNMP)
  - Todos los anteriores
- **Acción**: permitir o rechazar el acceso a una interfaz o dirección de origen.
- **Interfaz**: los puertos, LAG o VLAN que tienen permitido o negado el acceso a la utilidad de configuración basada en la Web.
- **Dirección IP de origen**: subredes o direcciones IP. El acceso a los métodos de administración puede diferir entre los grupos de usuarios. Por ejemplo, un grupo de usuarios puede tener acceso al módulo del dispositivo solo mediante una sesión HTTPS, mientras que otro grupo de usuarios puede acceder al módulo del dispositivo mediante sesiones HTTPS y Telnet.

Perfil de acceso activo

En la página Perfiles de acceso, se muestran los perfiles de acceso que están definidos y, allí, usted puede seleccionar un perfil de acceso para que sea el activo.

Cuando un usuario intenta acceder al dispositivo mediante un método de acceso, el dispositivo busca información para ver si el perfil de acceso activo permite el acceso de administración explícitamente al dispositivo mediante este método. Si no encuentra una coincidencia, se niega el acceso.

Cuando un intento para acceder al dispositivo no cumple con el perfil de acceso activo, el dispositivo genera un mensaje SYSLOG para advertir al administrador del sistema sobre el intento.

Si se activó un perfil de acceso de solo consola, la única forma de desactivarlo es a través de una conexión directa de la estación de administración al puerto físico de la consola en el switch.

Para obtener más información, consulte **Definición de reglas de perfiles**.

Utilice la página Perfiles de acceso para crear un perfil de acceso y agregar su primera regla. Si el perfil de acceso solo contiene una sola regla, habrá finalizado. Para añadir más reglas al perfil, utilice la página Reglas de perfil.

PASO 1 Haga clic en **Seguridad** > **Método de acceso a administración** > **Perfiles de acceso**.

Esta página muestra todos los perfiles de acceso, activos e inactivos.

PASO 2 Para cambiar el perfil de acceso activo, seleccione un perfil en el menú desplegable **Perfil de acceso activo** y haga clic en **Aplicar**. De esta manera, el perfil elegido se convierte en el perfil de acceso activo.

NOTA Si seleccionó Solo consola, aparece un mensaje de advertencia. Si continúa, se lo desconecta inmediatamente de la utilidad de configuración basada en la Web y puede acceder al dispositivo solo a través del puerto de consola. Esto solo se aplica a los tipos de dispositivo que ofrecen un puerto de consola.

Si usted seleccionó cualquier otro perfil de acceso, aparece un mensaje que le advierte que, según el perfil de acceso seleccionado, es posible que se lo desconecte de la utilidad de configuración basada en la Web.

PASO 3 Haga clic en **Aceptar** para seleccionar el perfil de acceso activo o en **Cancelar** para interrumpir la acción.

PASO 4 Haga clic en **Añadir** para abrir la página Añadir perfil de acceso. En esta página puede configurar un nuevo perfil y una regla.

PASO 5 Ingrese el **Nombre del perfil de acceso**. El nombre puede contener hasta 32 caracteres.

PASO 6 Ingrese los parámetros.

- **Prioridad de las reglas**: ingrese la prioridad de la regla. Cuando el paquete coincide con una regla, a los grupos de usuarios se les otorga o niega el acceso al dispositivo. La prioridad de la regla es esencial para hacer concordar los paquetes con las reglas, ya que se busca la primera coincidencia de los paquetes. Uno es la mayor prioridad.

- **Método de administración**: seleccione el método de administración para el que está definida la regla. Las opciones son:
  - *Todos*: se asignan todos los métodos de administración a la regla.
  - *Telnet*: a los usuarios que solicitan acceso al switch y que reúnen los criterios del perfil de acceso de Telnet se les otorga o deniega el acceso.
  - *Telnet seguro (SSH)*: a los usuarios que solicitan acceso al dispositivo y que reúnen los criterios del perfil de acceso de SSH se les otorga o deniega el acceso.
  - *HTTP*: a los usuarios que solicitan acceso al dispositivo y que reúnen los criterios del perfil de acceso de HTTP se les otorga o deniega el acceso.
  - *HTTP seguro (HTTPS)*: a los usuarios que solicitan acceso al dispositivo y que reúnen los criterios del perfil de acceso de HTTPS se les otorga o deniega el acceso.
  - *SNMP*: a los usuarios que solicitan acceso al dispositivo y que reúnen los criterios del perfil de acceso de SNMP se les otorga o deniega el acceso.
- **Acción**: seleccione la acción asociada a la regla. Las opciones son:
  - *Permitir*: se permite el acceso al dispositivo si el usuario coincide con la configuración del perfil.
  - *Rechazar*: se niega el acceso al dispositivo si el usuario coincide con la configuración del perfil.
- **Se aplica a la interfaz**: seleccione la interfaz asociada a la regla. Las opciones son:
  - *Todos*: se aplica a todos los puertos, las VLAN y los LAG.
  - *Definida por el usuario*: se aplica a la interfaz seleccionada.
- **Interfaz**: ingrese el número de interfaz si se seleccionó Definida por el usuario.
- **Se aplica a la dirección IP de origen**: seleccione el tipo de dirección IP de origen al que se aplica el perfil de acceso. El campo *Dirección IP de Origen* es válido para una subred. Seleccione uno de los siguientes valores:
  - *Todos*: se aplica a todos los tipos de direcciones IP.
  - *Definida por el usuario*: se aplica solo a aquellos tipos de direcciones IP definidos en los campos.
- **Versión IP**: ingrese la versión IP de la dirección de origen: Versión 6 o Versión 4.
- **Dirección IP**: ingrese la dirección IP de origen.
- **Máscara**: seleccione el formato de la máscara de subred para la dirección IP de origen e ingrese un valor en uno de los campos:
  - *Máscara de red*: seleccione la subred a la que pertenece la dirección IP de origen e ingrese la máscara de subred en formato decimal con punto.

- *Longitud de prefijo*: seleccione la longitud del prefijo e ingrese el número de bits que componen el prefijo de la dirección IP de origen.

PASO 7 Haga clic en **Aplicar**. El perfil de acceso se escribe en el archivo Configuración en ejecución. Ahora puede seleccionar este perfil de acceso como el perfil activo.

Definición de reglas de perfiles

Los perfiles de acceso pueden incluir hasta 128 reglas para determinar a quién se le permite administrar el dispositivo y acceder a este, y los métodos de acceso que pueden usarse.

Cada regla en un perfil de acceso incluye una acción y un criterio (uno o más parámetros) que deben cumplirse. Cada regla tiene una prioridad; las reglas con menor prioridad se verifican primero. Si el paquete entrante coincide con una regla, se lleva a cabo la acción asociada con la regla. Si no se encuentra una regla coincidente dentro del perfil de acceso activo, el paquete se descarta.

Por ejemplo, usted puede limitar el acceso al dispositivo de todas las direcciones IP, a excepción de aquellas asignadas al centro de administración de TI. De esta forma, el dispositivo podrá administrarse y tendrá otra capa de seguridad.

Para añadir reglas de perfiles a un perfil de acceso:

PASO 1 Haga clic en **Seguridad** > **Método de acceso a administración** > **Reglas de perfiles**.

PASO 2 Seleccione el campo Filtro y un perfil de acceso. Haga clic en **Ir**.

El perfil de acceso seleccionado aparece en la Tabla de reglas de los perfiles.

PASO 3 Haga clic en **Añadir** para agregar una regla.

PASO 4 Ingrese los parámetros.

- **Nombre del perfil de acceso**: seleccione un perfil de acceso.
- **Prioridad de las reglas**: ingrese la prioridad de la regla. Cuando el paquete coincide con una regla, a los grupos de usuarios se les otorga o niega el acceso al dispositivo. La prioridad de la regla es esencial para hacer concordar los paquetes con las reglas, ya que se busca la primera coincidencia de los paquetes.
- **Método de administración**: seleccione el método de administración para el que está definida la regla. Las opciones son:
  - *Todos*: se asignan todos los métodos de administración a la regla.
  - *Telnet*: a los usuarios que solicitan acceso al switch y que reúnen los criterios del perfil de acceso de Telnet se les otorga o deniega el acceso.

- *Telnet seguro (SSH)*: a los usuarios que solicitan acceso al switch y que reúnen los criterios del perfil de acceso de Telnet se les otorga o deniega el acceso.
- *HTTP*: se asigna acceso HTTP a la regla. A los usuarios que solicitan acceso al dispositivo y que reúnen los criterios del perfil de acceso de HTTP se les otorga o deniega el acceso.
- *HTTP seguro (HTTPS)*: a los usuarios que solicitan acceso al dispositivo y que reúnen los criterios del perfil de acceso de HTTPS se les otorga o deniega el acceso.
- *SNMP*: a los usuarios que solicitan acceso al dispositivo y que reúnen los criterios del perfil de acceso de SNMP se les otorga o deniega el acceso.

- **Acción**: seleccione **Permitir** para permitir el acceso a los usuarios que intentan acceder al dispositivo mediante el método de acceso configurado de la interfaz y el origen IP definidos en esta regla. O bien, seleccione **Rechazar** para rechazar el acceso.
- **Se aplica a la interfaz**: seleccione la interfaz asociada a la regla. Las opciones son:
  - *Todos*: se aplica a todos los puertos, las VLAN y los LAG.
  - *Definida por el usuario*: se aplica solo al puerto, la VLAN o el LAG que se haya seleccionado.
- **Interfaz**: ingrese el número de interfaz.
- **Se aplica a la dirección IP de origen**: seleccione el tipo de dirección IP de origen al que se aplica el perfil de acceso. El campo *Dirección IP de Origen* es válido para una subred. Seleccione uno de los siguientes valores:
  - *Todos*: se aplica a todos los tipos de direcciones IP.
  - *Definida por el usuario*: se aplica solo a aquellos tipos de direcciones IP definidos en los campos.
- **Versión IP**: seleccione la versión IP admitida de la dirección de origen: IPv6 o IPv4.
- **Dirección IP**: ingrese la dirección IP de origen.
- **Máscara**: seleccione el formato de la máscara de subred para la dirección IP de origen e ingrese un valor en uno de los campos:
  - *Máscara de red*: seleccione la subred a la que pertenece la dirección IP de origen e ingrese la máscara de subred en formato decimal con punto.
  - *Longitud de prefijo*: seleccione la longitud del prefijo e ingrese el número de bits que componen el prefijo de la dirección IP de origen.

PASO 5 Haga clic en **Aplicar** y se añade la regla al perfil de acceso.

Autenticación de acceso a administración

Usted puede asignar métodos de autorización y autenticación para los diversos métodos de acceso a administración, como SSH, consola, Telnet, HTTP y HTTPS. La autenticación puede realizarse en forma local o en un servidor TACACS+ o RADIUS.

Si está activada la autorización, se verifican la identidad y los privilegios de lectura y escritura del usuario. Si no está activada la autorización, solo se verifica la identidad del usuario.

El método de autorización o autenticación que se utilice estará determinado por el orden en que se seleccionan los métodos de autenticación. Si el primer método de autenticación no está disponible, se usa el siguiente método seleccionado. Por ejemplo, si los métodos de autenticación seleccionados son RADIUS y Local, y se realiza una consulta a todos los servidores RADIUS configurados en orden de prioridad, pero ninguno responde, el usuario se autentica o autoriza de manera local.

Si la autorización está activada y un método de autenticación falla, o el usuario no tiene un nivel de privilegio suficiente, al usuario se le niega el acceso al dispositivo. En otras palabras, si la autenticación falla con un método de autenticación, el dispositivo se detiene ante tal intento; no continúa ni intenta usar el siguiente método de autenticación.

De igual manera, si la autorización no está activada y falla la autenticación de un método, el dispositivo detiene el intento de autenticación.

Para definir los métodos de autenticación para un método de acceso:

PASO 1 Haga clic en **Seguridad** > **Autenticación de acceso a administración**.

PASO 2 Ingrese la **Aplicación** (tipo) del método de acceso de administración.

PASO 3 Seleccione **Autorización** para activar la autenticación y la autorización del usuario por medio de la lista de métodos descritos a continuación. Si el campo no está seleccionado, solo se realizará la autenticación. Si la autorización está activada, se controlan los privilegios de lectura y escritura de los usuarios. Este nivel de privilegios se configura en la página Cuentas de usuario.

PASO 4 Use las flechas para mover el método de autorización o autenticación de la columna **Métodos opcionales** a la columna **Métodos seleccionados**. Los métodos se van ejecutando en el orden en el que aparecen.

PASO 5 Use las flechas para mover el método de autenticación de la columna **Métodos opcionales** a la columna **Métodos seleccionados**. El primer método seleccionado es el primero que se usa.

- *RADIUS*: el usuario se autoriza o autentica en un servidor RADIUS. Debe haber uno o más servidores RADIUS configurados. Para que el servidor RADIUS otorgue acceso a la utilidad de configuración basada en la Web, este debe devolver cisco-avpair=shell:priv-lvl=15.

- *TACACS+*: el usuario se autoriza o autentica en el servidor TACACS+. Debe haber uno o más servidores TACACS+ configurados.
- *Ninguno*: el usuario puede acceder al dispositivo sin autorización o autenticación.
- *Local*: se comprueban el nombre de usuario y la contraseña con los datos almacenados en el dispositivo local. Estos pares de nombre de usuario y contraseña se definen en la página Cuentas de usuario.

NOTA El método de autenticación **Local** o **Ninguna** siempre debe seleccionarse en último lugar. Se omiten todos los métodos de autenticación seleccionados después de **Local** o **Ninguna**.

PASO 6 Haga clic en **Aplicar**. Se asocian los métodos de autenticación seleccionados con el método de acceso.

Gestión de datos confidenciales

Consulte **Seguridad: Gestión de datos confidenciales**.

Servidor SSL

En esta sección se describe la función Capa de socket seguro (SSL, Secure Socket Layer).

Información general de SSL

La función Capa de socket seguro (SSL) se utiliza para abrir una sesión HTTPS para el dispositivo.

Una sesión HTTPS se puede abrir con el certificado predeterminado que existe en el dispositivo.

Algunos exploradores generan advertencias utilizando un certificado predeterminado debido a que este certificado no está firmado por una autoridad de certificación (CA, Certification Authority). Contar con un certificado firmado por una CA confiable es una mejor práctica.

Para abrir una sesión HTTPS a través de un certificado creado por el usuario, realice las siguientes acciones:

1. Genere un certificado.
2. Solicite que el certificado esté certificado por una CA.
3. Importe el certificado firmado en el dispositivo.

Configuración y valores predeterminados

De manera predeterminada, el dispositivo contiene un certificado que se puede modificar.

El HTTPS se activa de manera predeterminada.

Configuración de la autenticación del servidor SSL

Es posible que sea necesario generar un certificado nuevo para reemplazar el certificado predeterminado que se encuentra en el dispositivo.

Para crear un nuevo certificado:

PASO 1 Haga clic en **Seguridad > Servidor SSL > Configuración de la autenticación del servidor SSL**.

Se muestra la información para el certificado 1 y 2 en la Tabla de claves del servidor SSL. Estos campos están definidos en la página **Editar**, con la excepción de los siguientes campos:

- **Válido desde**: especifica la fecha a partir de la cual el certificado es válido.
- **Válido hasta**: especifica la fecha hasta la cual el certificado es válido.
- **Origen del certificado**: especifica si el certificado fue generado por el sistema (Generado de forma automática) o por el usuario (Definido por el usuario).

PASO 2 Seleccione un certificado activo.

PASO 3 Haga clic en **Generar solicitud de certificado**.

PASO 4 Ingrese los siguientes campos:

- **ID del certificado**: seleccione el certificado activo.
- **Nombre común**: especifica la URL o dirección IP completamente calificada del dispositivo. Si no se especifica, queda el valor predeterminado más bajo de la dirección IP del dispositivo (cuando se genera el certificado).
- **Unidad de organización**: especifica la unidad de organización o el nombre del departamento.
- **Nombre de la organización**: especifica el nombre de la organización.
- **Ubicación**: especifica la ubicación o el nombre de la ciudad.
- **Estado**: especifica el nombre del estado o de la provincia.
- **País**: especifica el nombre del país.

- **Solicitud de certificado**: muestra la clave creada cuando se presiona el botón **Generar solicitud de certificado**.

PASO 5 Haga clic en **Generar solicitud de certificado**. Esto crea una clave que se debe introducir en la autoridad de certificación (CA). Cópielo del campo **Solicitud de certificado**.

Para importar un certificado:

PASO 1 Haga clic en **Seguridad > Servidor SSL > Configuración de la autenticación del servidor SSL**.

PASO 2 Haga clic en **Importar certificado**.

PASO 3 Ingrese los siguientes campos:

- **ID del certificado**: seleccione el certificado activo.
- **Origen del certificado**: muestra que el certificado está definido por el usuario.
- **Certificado**: copie el certificado recibido.
- **Importar par de claves RSA**: seleccione esta opción para habilitar la copia en el nuevo par de claves RSA.
- **Clave pública**: copie la clave pública RSA.
- **Clave privada (cifrada)**: seleccione y copie la clave privada RSA en forma cifrada.
- **Clave privada (texto sin formato)**: seleccione y copie la clave privada RSA como texto sin formato.

PASO 4 Haga clic en **Aplicar** para aplicar los cambios en la configuración en ejecución.

PASO 5 Haga clic en **Mostrar datos confidenciales como cifrados** para mostrar esta clave como cifrada. Cuando se hace clic en este botón, las claves privadas se escriben en el archivo de configuración con formato cifrado (cuando se hace clic en Aplicar). Cuando el texto aparece cifrado, el botón pasa a ser **Mostrar datos confidenciales como texto sin formato**, y usted podrá ver el texto nuevamente sin formato.

El botón **Detalles** muestra el certificado y el par de claves RSA. Esto se usa para copiar el certificado y el par de claves RSA a otro dispositivo (utilizando copiar/pegar). Cuando hace clic en **Mostrar datos confidenciales como cifrados**, las claves privadas se muestran en forma cifrada.

Servidor SSH

Consulte **Seguridad: Servidor SSH**.

Cliente SSH

Consulte **Seguridad: Cliente SSH**.

Configuración de servicios TCP/UDP

En la página Servicios TCP/UDP, se pueden activar servicios basados en TCP o UDP en el dispositivo, en general, por motivos de seguridad.

El dispositivo ofrece los siguientes servicios TCP/UDP:

- **HTTP**: activado de fábrica.
- **HTTPS**: activado de fábrica.
- **SNMP**: desactivado de fábrica.
- **Telnet**: desactivado de fábrica.
- **SSH**: desactivado de fábrica.

En esta ventana, también aparecen las conexiones TCP activas.

Para configurar los servicios TCP/UDP:

PASO 1 Haga clic en **Seguridad** > **Servicios TCP/UDP**.

PASO 2 Active o desactive los siguientes servicios TCP/UDP en los servicios mostrados.

- **Servicio HTTP**: indica si el servicio HTTP está activado o desactivado.
- **Servicio HTTPS**: indica si el servicio HTTPS está activado o desactivado.
- **Servicio SNMP**: indica si el servicio SNMP está activado o desactivado.
- **Servicio Telnet**: indica si el servicio Telnet está activado o desactivado.
- **Servicio SSH**: indica si el servicio del servidor de SSH está habilitado o deshabilitado.

PASO 3 Haga clic en **Aplicar**. Los servicios se escriben en el archivo Configuración en ejecución.

En la Tabla de servicio TCP, se muestran los siguientes campos para cada servicio:

- **Nombre del servicio**: método de acceso a través del cual el dispositivo ofrece el servicio TCP.
- **Tipo**: protocolo IP que usa el servicio.
- **Dirección IP local**: dirección IP local a través de la cual el dispositivo ofrece el servicio.
- **Puerto local**: puerto TCP local a través del que el dispositivo ofrece el servicio.
- **Dirección IP remota**: dirección IP del dispositivo remoto que solicita el servicio.
- **Puerto remoto**: puerto TCP del dispositivo remoto que solicita el servicio.
- **Estado**: estado del servicio.

La tabla Servicios UDP incluye la siguiente información:

- **Nombre del servicio**: método de acceso a través del cual el dispositivo ofrece el servicio UDP.
- **Tipo**: protocolo IP que usa el servicio.
- **Dirección IP local**: dirección IP local a través de la cual el dispositivo ofrece el servicio.
- **Puerto local**: puerto UDP local a través del que el dispositivo ofrece el servicio.
- **Instancia de la aplicación**: la instancia del servicio UDP (por ejemplo, cuando dos remitentes envían datos al mismo destino).

Definición del control de saturación

Al recibir tramas de difusión, multidifusión y unidifusión desconocidas, se duplican y se envía una copia a todos los puertos de egreso posibles. En la práctica, esto significa que se envían a todos los puertos que pertenecen a la VLAN relevante. De esta forma, una trama de ingreso se convierte en varias, y así crea la posibilidad de una saturación de tráfico.

La protección contra la saturación le permite limitar la cantidad de tramas que ingresan al dispositivo y definir los tipos de tramas que se tienen en cuenta para este límite.

Cuando la velocidad de las tramas de difusión, multidifusión y unidifusión desconocidas sea mayor que el umbral definido por el usuario, se descartarán las tramas recibidas que superen el umbral.

Para definir el control de la saturación:

PASO 1 Haga clic en **Seguridad** > **Control de saturación**.

En la página Editar control de saturación, se describen todos los campos de esta página, a excepción del campo **Umbral de velocidad del control de saturación (%)**, que muestra el porcentaje del total de ancho de banda disponible para paquetes de unidifusión, multidifusión y difusión desconocidos antes de que el control de saturación se aplique al puerto. El valor predeterminado es 10% de la velocidad máxima del puerto y se configura en la página Editar control de saturación.

PASO 2 Seleccione un puerto y haga clic en **Editar**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: seleccione el puerto para el que está habilitado el control de saturación.
- **Control de saturación**: seleccione esta opción para activar el control de saturación.
- **Umbral de velocidad del control de saturación**: ingrese la velocidad máxima a la que se pueden reenviar los paquetes desconocidos. El valor predeterminado para este umbral es 10,000 para los dispositivos FE y 100,000 para los dispositivos GE.
- **Modo del control de saturación**: seleccione uno de los modos:
  - *Unidifusión, multidifusión y difusión desconocidas*: se tiene en cuenta el tráfico de unidifusión, difusión y multidifusión desconocido para el umbral del ancho de banda.
  - *Difusión y multidifusión*: se tiene en cuenta el tráfico de multidifusión y difusión para el umbral del ancho de banda.
  - *Solo difusión*: se tiene en cuenta solo el tráfico de difusión para el umbral del ancho de banda.

PASO 4 Haga clic en **Aplicar**. Se modifica el control de saturación y se actualiza el archivo Configuración en ejecución.

Configuración de la seguridad de puertos

La seguridad de la red puede incrementarse al limitar el acceso en un puerto a usuarios con direcciones MAC específicas. Las direcciones MAC pueden aprenderse dinámicamente o configurarse estáticamente.

La seguridad de los puertos controla los paquetes recibidos y aprendidos. El acceso a los puertos bloqueados se limita a los usuarios con direcciones MAC específicas.

La seguridad de puertos tiene cuatro modos:

- **Bloqueo clásico**: se bloquean todas las direcciones MAC aprendidas en el puerto, y el puerto no aprende ninguna dirección MAC nueva. Las direcciones aprendidas no están sujetas a vencimiento ni reaprendizaje.
- **Bloqueo dinámico limitado**: el dispositivo aprende direcciones MAC hasta el límite configurado de direcciones permitidas. Una vez alcanzado el límite, el dispositivo no aprende más direcciones. En este modo, las direcciones están sujetas a vencimiento y reaprendizaje.
- **Seguro permanente**: mantiene las direcciones MAC dinámicas actuales asociadas con el puerto y aprende hasta el máximo de direcciones permitidas en el puerto (especificadas por el n.º máx. de direcciones permitidas). El reaprendizaje y el vencimiento están deshabilitados.
- **Eliminar en reinicio seguro**: elimina las direcciones MAC dinámicas actuales asociadas con el puerto después del reinicio. Se pueden aprender direcciones MAC nuevas tomándolas como parte de la acción Eliminar en reinicio hasta el máximo de direcciones permitidas en el puerto. El reaprendizaje y el vencimiento están deshabilitados.

Cuando se detecta una trama de una nueva dirección MAC en un puerto donde no está autorizada (el puerto está bloqueado de manera clásica y hay una nueva dirección MAC; o el puerto está bloqueado de manera dinámica y se ha superado la cantidad máxima de direcciones permitidas), se invoca el mecanismo de protección y tiene lugar una de las siguientes acciones:

- Se descarta la trama
- Se reenvía la trama
- Se cierra el puerto

Cuando otro puerto detecta la dirección MAC segura, la trama se reenvía, pero ese puerto no aprende la dirección MAC.

Además de una de estas acciones, usted también puede generar trampas y limitar su frecuencia y número para evitar sobrecargar los dispositivos.

NOTA Para utilizar 802.1X en un puerto, debe ser en modo de varios hosts o en modo de varias sesiones. La seguridad de puertos en un puerto no se puede definir si el puerto está en modo único (consulte la página 802.1X, Autenticación de host y sesión).

Para configurar la seguridad de los puertos:

PASO 1 Haga clic en **Seguridad** > **Seguridad de puerto**.

PASO 2 Seleccione la interfaz que desee modificar y haga clic en **Editar**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: seleccione el nombre de la interfaz.
- **Estado de la interfaz**: seleccione esta opción para bloquear el puerto.
- **Modo de aprendizaje**: seleccione el tipo de bloqueo del puerto. Para configurar este campo, la interfaz debe estar en estado desbloqueado. El campo Modo de aprendizaje está habilitado solo si el campo *Estado de la interfaz* está bloqueado. Para cambiar el modo de aprendizaje, se debe desactivar Estado de la interfaz. Luego de cambiar el modo, se puede volver a activar Estado de la interfaz. Las opciones son:
  - *Bloqueo clásico*: el puerto se bloquea inmediatamente, independientemente del número de direcciones que se hayan aprendido.
  - *Bloqueo dinámico limitado*: se bloquea el puerto al eliminar las direcciones MAC dinámicas actuales asociadas con el puerto. El puerto aprende hasta el máximo de direcciones permitidas en el puerto. Tanto el reaprendizaje como el vencimiento de las direcciones MAC están habilitados.
  - *Seguro permanente*: mantiene las direcciones MAC dinámicas actuales asociadas con el puerto y aprende hasta el máximo de direcciones permitidas en el puerto (especificadas por **el n.º máx. de direcciones permitidas**). El reaprendizaje y el vencimiento están habilitados.
  - *Eliminar en reinicio seguro*: elimina las direcciones MAC dinámicas actuales asociadas con el puerto después del reinicio. Se pueden aprender direcciones MAC nuevas tomándolas como parte de la acción Eliminar en reinicio hasta el máximo de direcciones permitidas en el puerto. El reaprendizaje y el vencimiento están deshabilitados.
- **N.º máx. de direcciones permitidas**: ingrese el número máximo de direcciones MAC que el puerto puede aprender si el modo de aprendizaje *Bloqueo dinámico limitado* está seleccionado. El número 0 indica que la interfaz solo admiten direcciones estáticas.
- **Acción en incumplimiento**: seleccione una acción para aplicar a los paquetes que llegan a un puerto bloqueado. Las opciones son:
  - *Descartar*: se descartan los paquetes de cualquier origen no aprendido.
  - *Reenviar*: se reenvían los paquetes de un origen desconocido sin aprender la dirección MAC.
  - *Cerrar*: se descartan los paquetes de cualquier origen no aprendido y se cierra el puerto. El puerto permanece cerrado hasta que se lo reactive o hasta que se reinicie el dispositivo.
- **Trampa**: seleccione esta opción para activar las trampas cuando se recibe un paquete en un puerto bloqueado. Esto es relevante para las violaciones de bloqueo. Para el bloqueo clásico, esto se aplica a cualquier dirección nueva recibida. Para el bloqueo dinámico limitado, esto se aplica a cualquier dirección nueva que supere el número de direcciones permitidas.
- **Frecuencia de trampas**: ingrese el tiempo mínimo (en segundos) que debe transcurrir entre trampas.

PASO 4 Haga clic en **Aplicar**. Se modifica la seguridad de puertos y se actualiza el archivo Configuración en ejecución.

802.1x

Consulte el capítulo **Seguridad: Autenticación 802.1X** para obtener información sobre la autenticación 802.1X. Incluye la autenticación basada en MAC y web.

Prevención de negación de servicio

Un ataque DoS (Denial of Service, negación de servicio) es un intento de pirata informático de impedir a los usuarios disponer de un dispositivo.

Los ataques DoS saturan el dispositivo con solicitudes de comunicación externas para que no pueda responder al tráfico legítimo. Estos ataques, por lo general, provocan una sobrecarga de la CPU del dispositivo.

Tecnología de núcleo seguro (SCT)

Un método para resistir los ataques DoS que emplea el dispositivo es usar la SCT (Secure Core Technology, tecnología de núcleo seguro). SCT está habilitado de forma predeterminado en el dispositivo y no se puede desactivar.

El dispositivo Cisco es un dispositivo avanzado que maneja tráfico de administración, tráfico de protocolo y tráfico de indagación, además del tráfico de usuario final (TCP).

La SCT asegura que el dispositivo reciba y procese el tráfico de administración y de protocolo, independientemente de la cantidad de tráfico total que reciba. Esto se realiza limitando la velocidad del tráfico TCP a la CPU.

No hay interacciones con otras funciones.

La SCT se puede monitorear en la página Negación de servicio > Prevención de negación de servicio > Configuración del conjunto de seguridad (botón **Detalles**).

Tipos de ataques DoS

Los siguientes tipos de paquetes u otras estrategias pueden estar involucrados en un ataque de negación de servicio:

- **Paquetes TCP SYN**: estos paquetes por lo general tienen una dirección de remitente falsa. Estos paquetes se manejan como una solicitud de conexión: hacen que el servidor establezca una conexión semiabierta, devuelven un paquete TCP/SYN-ACK (reconocimiento) y esperan un paquete como respuesta de la dirección del remitente (respuesta al paquete ACK). No obstante, como la dirección de remitente es falsa, la respuesta nunca llega. Estas conexiones semiabiertas saturan la cantidad de conexiones disponibles que el dispositivo puede establecer, y le impiden responder solicitudes legítimas.
- **Paquetes TCP SYN-FIN**: se envían paquetes SYN para establecer una nueva conexión TCP. Los paquetes TCP FIN se envían para cerrar una conexión. Nunca debe existir un paquete con los indicadores SYN y FIN. Por eso, estos paquetes podrían representar un ataque al dispositivo y deben bloquearse.
- **Direcciones "martian"**: las direcciones "martian" son ilegales desde el punto de vista del protocolo IP. Consulte **Direcciones "martian"** para obtener más detalles.
- **Ataque ICMP**: envío de paquetes ICMP de formato incorrecto o una cantidad abrumadora de paquetes ICMP a la víctima, que podría causarle una caída del sistema.
- **Fragmentación IP**: se envían al dispositivo fragmentos IP alterados con cargas útiles superpuestas demasiado grandes. Esto puede dañar diversos sistemas operativos por causa de un error en el código de reensamblado de fragmentación TCP/IP. Los sistemas operativos Windows 3.1x, Windows 95 y Windows NT, y las versiones de Linux anteriores a 2.0.32 y 2.1.63 son vulnerables a este ataque.
- **Distribución de Stacheldraht**: el atacante usa un programa cliente para conectarse con los administradores, que son sistemas comprometidos que envían comandos a agentes inertes que, a su vez, facilitan un ataque DoS. Los agentes están comprometidos por el atacante por medio de los administradores.

  Uso de rutinas automatizadas para explotar las vulnerabilidades en programas que aceptan conexiones remotas en los hosts remotos destinados. Cada administrador puede controlar hasta mil agentes.
- **Invasor troyano**: un troyano permite al atacante descargar un agente inerte (o el troyano puede contener uno). Los atacantes también pueden ingresar a los sistemas con herramientas automatizadas que explotan defectos de programas que escuchan conexiones de hosts remotos. Este escenario le concierne principalmente al dispositivo cuando funciona como servidor en la Web.
- **Troyano Back Orifice**: es una variación de un troyano que usa el software Back Orifice para implantar el troyano.

Defensa contra ataques DoS

*La función Prevención de negación de servicio (Do*S) brinda asistencia al administrador del sistema para resistirse a los ataques DoS de las siguientes maneras:

- Activar la protección de SYN de TCP. Si está activada esta función, se envían informes cuando se identifica un ataque de un paquete SYN, y el puerto atacado puede apagarse temporalmente. Se identifica un ataque SYN si la cantidad de paquetes SYN por segundo supera el umbral configurado por el usuario.
- Bloquear paquetes SYN-FIN.
- Bloquear paquetes que contengan direcciones "martian" reservadas (página Direcciones "martian").
- Impedir las conexiones TCP de una interfaz específica (página Filtrado SYN) y limitar la velocidad para los paquetes (página Protección de velocidad SYN).
- Configurar el bloqueo de ciertos paquetes ICMP (página Filtrado del ICMP).
- Descartar paquetes IP fragmentados de una interfaz específica (página Filtrado de fragmentos IP).
- Rechazar ataques de distribución de Stacheldraht, invasor troyano y troyano Back Orifice (página Configuración del conjunto de seguridad).

Dependencias entre funciones

Las políticas avanzadas de QoS y ACL no están activas cuando un puerto tiene protección de negación de servicio. Aparece un mensaje de error si intenta activar la prevención de DoS cuando se define una ACL en la interfaz o si intenta definir una ACL en una interfaz que tiene activada la prevención de DoS.

Un ataque SYN no puede bloquearse si hay una ACL activa en la interfaz.

Configuración predeterminada

La función Prevención de DoS tiene los siguientes valores predeterminados:

- De forma predeterminada, la función Prevención de DoS está desactivada.
- La protección de SYN-FIN está activada de forma predeterminada (incluso si la opción Prevención de DoS está desactivada).
- Si la protección de SYN está activada, el modo de protección predeterminado es **Bloquear e informar**. El umbral predeterminado es 30 paquetes SYN por segundo.
- Todas las demás funciones de la prevención de DoS están desactivadas de forma predeterminada.

Configuración de la prevención de DoS

Las siguientes páginas se utilizan para configurar esta función.

Configuración del conjunto de seguridad

NOTA Antes de activar la prevención de DoS, usted debe desvincular todas las políticas avanzadas de calidad de servicio (QoS) o listas de control de acceso (ACL) que estén asociadas a un puerto. Las políticas avanzadas de QoS y ACL no están activas cuando un puerto tiene protección contra negación de servicio.

Para definir la configuración global de la prevención de DoS y controlar la SCT:

PASO 1 Haga clic en **Seguridad** > **Prevención de negación de servicio** > **Configuración del conjunto de seguridad**. Se muestra la *Configuración del conjunto de seguridad*.

Mecanismo de protección de la CPU: Habilitado indica que la SCT está habilitada.

PASO 2 Haga clic en **Detalles** al lado de **Utilización de CPU** para ir a la página Utilización de CPU y consultar la información sobre el uso de recursos de la CPU.

PASO 3 Haga clic en **Editar** al lado de **Protección de SYN de TCP** para ir a la página Protección de SYN de TCP y activar esta función.

PASO 4 Seleccione **Prevención de DoS** para habilitar la función.

- **Deshabilitar**: desactive la función.
- **Prevención a nivel de sistema**: habilite la parte de la función que impide ataques de distribución de Stacheldraht, invasor troyano y troyano Back Orifice.
- **Prevención a nivel de sistema y a nivel de interfaz**: habilite la parte de la función que impide ataques de distribución de Stacheldraht, invasor troyano y troyano Back Orifice.

PASO 5 Si **Prevención a nivel de sistema** o **Prevención a nivel de sistema y a nivel de interfaz** está seleccionada, active una o más de las siguientes opciones de prevención de DoS:

- **Distribución Stacheldraht**: se descartan los paquetes TCP con puerto TCP de origen equivalente a 16660.
- **Invasor troyano**: se descartan los paquetes TCP con puerto TCP de destino equivalente a 2140 y puerto TCP de origen equivalente a 1024.
- **Troyano Back Orifice**: se descartan los paquetes UDP con puerto UDP de destino equivalente a 31337 y puerto UDP de origen equivalente a 1024.

PASO 6 Haga clic en las siguientes opciones según la necesidad:

- **Direcciones martian**: haga clic en **Editar** para ir a la página Direcciones martian.
- **Filtrado SYN**: haga clic en **Editar** para ir a la página Filtrado SYN.
- **Protección de velocidad SYN** (solo en Capa 2): haga clic en **Editar** para ir a la página Protección de velocidad SYN.
- **Filtrado ICMP**: haga clic en **Editar** para ir a la página Filtrado ICMP.
- **IP fragmentada**: haga clic en **Editar** para ir a la página Filtrado de fragmentos IP.

Protección de SYN

Los piratas informáticos pueden usar los puertos de red para atacar al dispositivo en un ataque SYN, que consume recursos TCP (búferes) y potencia de la CPU.

Como la CPU está protegida con SCT, está limitado el tráfico TCP a la CPU. Sin embargo, si se atacan uno o varios puertos con un alto índice de paquetes SYN, la CPU recibe solo los paquetes del atacante y genera así la negación de servicio.

Al usar la función Protección de SYN, la CPU cuenta los paquetes SYN que le ingresan por segundo de cada puerto de red.

Si el número es mayor al específico (umbral definido por el usuario), en el puerto se aplica una regla de negación de SYN con "MAC-to-Me". Esta regla se desvincula del puerto a cada intervalo definido por el usuario (período de protección de SYN).

Para configurar la protección de SYN:

PASO 1 Haga clic en **Seguridad** > **Prevención de negación de servicio** > **Protección de SYN**.

PASO 2 Ingrese los parámetros.

- **Bloquear paquetes SYN-FIN**: seleccione para habilitar la función. Todos los paquetes TCP con los indicadores SYN y FIN se descartan en todos los puertos.
- **Modo de protección de SYN**: seleccione entre tres modos:
  - *Deshabilitar*: la función se deshabilita en una interfaz específica.
  - *Informar*: se genera un mensaje SYSLOG. El estado del puerto cambia a **Atacado** cuando se supera el umbral.

- *Bloquear e informar*: cuando se identifica un ataque TCP SYN, se descartan los paquetes TCP SYN destinados para el sistema y el estado del puerto cambia a **Bloqueado**.

- **Umbral de protección de SYN**: cantidad de paquetes SYN por segundo antes de que se bloqueen los paquetes SYN (en el puerto, se aplicará la regla de negación de SYN con "MAC-to-Me").
- **Período de protección de SYN**: tiempo en segundos antes de desbloquear los paquetes SYN (la regla de negación de SYN con "MAC-to-Me" está desvinculada del puerto).

PASO 3 Haga clic en **Aplicar**. Se define la protección de SYN y se actualiza el archivo de configuración en ejecución.

En la Tabla de interfaz de protección de SYN, se muestran los siguientes campos para cada puerto o LAG (según lo solicitado por el usuario).

- **Estado actual**: estado de la interfaz. Los valores posibles son:
  - *Normal*: no se identificó ningún ataque en esta interfaz.
  - *Bloqueado*: el tráfico no se reenvía en esta interfaz.
  - *Atacado*: se identificó un ataque en esta interfaz.
- **Último ataque**: fecha del último ataque SYN-FIN identificado por el sistema y la acción del sistema (**Informado** o **Bloqueado e informado**).

Direcciones "martian"

En la página Direcciones martian se pueden ingresar direcciones IP que indican un ataque si se las detecta en la red. Los paquetes de esas direcciones se descartan.

El dispositivo admite un conjunto de direcciones "martian" reservadas que son ilegales desde el punto de vista del protocolo IP. Las direcciones martian reservadas admitidas son:

- Direcciones definidas como ilegales en la página Direcciones "martian".
- Direcciones que son ilegales desde el punto de vista del protocolo, como las direcciones de bucle de retorno, que incluyen los siguientes intervalos:
  - **0.0.0.0/8 (excepto 0.0.0.0/32 como dirección de origen)**: las direcciones en este bloque se refieren a hosts de origen en esta red.
  - **127.0.0.0/8**: se utiliza como la dirección de bucle de retorno de host de Internet.
  - **192.0.2.0/24**: se utiliza como TEST-NET en códigos de ejemplo y documentación.
  - **224.0.0.0/4 (como dirección IP de origen)**: se utiliza en asignaciones de direcciones de multidifusión IPv4, y se conocía anteriormente como el espacio de direcciones clase D.
  - **240.0.0.0/4 (excepto 255.255.255.255/32 como una dirección de destino)**: intervalo de direcciones reservado que se conocía anteriormente como el espacio de direcciones clase E.

También puede añadir nuevas direcciones martian para la prevención de DoS. Los paquetes que tienen direcciones martian se descartan.

Para definir direcciones martian:

PASO 1 Haga clic en **Seguridad** > **Prevención de negación de servicio** > **Direcciones marcianas**.

PASO 2 Seleccione **Direcciones martian reservadas** y haga clic en **Aplicar** para incluir las direcciones martian reservadas en la lista de prevención a nivel de sistema.

PASO 3 Para añadir una dirección martian, haga clic en **Añadir**.

PASO 4 Ingrese los parámetros.

- **Versión IP**: indica la versión IP admitida. Actualmente, solo se admite IPv4.
- **Dirección IP**: ingrese una dirección IP que se deba rechazar. Los valores posibles son:
  - *De la lista reservada*: seleccione una dirección IP conocida de la lista reservada.
  - *Dirección IP nueva*: ingrese una dirección IP.
- **Máscara**: ingrese la máscara de la dirección IP para definir un rango de direcciones IP que se deben rechazar. Los valores son:
  - *Máscara de red*: máscara de red en formato decimal con punto.
  - *Longitud de prefijo*: ingrese el prefijo de la dirección IP para definir el rango de direcciones IP para las que la Prevención de negación de servicio está activada.

PASO 5 Haga clic en **Aplicar**. Las direcciones martian se escriben en el archivo Configuración en ejecución.

Filtrado SYN

En la página Filtrado SYN se pueden filtrar los paquetes TCP que contienen un indicador SYN y que se dirigen a uno o más puertos.

Para definir un filtrado SYN:

PASO 1 Haga clic en **Seguridad** > **Prevención de negación de servicio** > **Filtrado SYN**.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: seleccione la interfaz en la que está definido el filtro.

- **Dirección IPv4**: ingrese la dirección IP para la que está definido el filtro, o seleccione *Todas las direcciones*.
- **Máscara de red**: ingrese la máscara de red para la que el filtro está activado en formato de dirección IP.
- **Puerto TCP**: seleccione el puerto TCP de destino al que se aplica el filtro:
  - *Puertos conocidos*: seleccione un puerto de la lista.
  - *Definida por el usuario*: ingrese un número de puerto.
  - *Todos los puertos*: seleccione esta opción para indicar que se filtran todos los puertos.

PASO 4 Haga clic en **Aplicar**. Se define el filtrado SYN y se actualiza el archivo Configuración en ejecución.

Protección de velocidad SYN

En la página Protección de velocidad SYN se puede limitar el número de paquetes SYN recibidos en el puerto de ingreso. De esta manera, se disminuye el efecto de una inundación SYN contra servidores y, por velocidad, se limita el número de conexiones nuevas abiertas para administrar paquetes.

Esta característica está disponible únicamente cuando el dispositivo está en modo de sistema de Capa 2 en los modelos Sx300 y SG500, y en modo nativo en los modelos SG500X y SG500XG.

Para definir la protección de velocidad SYN:

PASO 1 Haga clic en **Seguridad** > **Prevención de negación de servicio** > **Protección de velocidad SYN**.

En esta página, aparece la protección de velocidad SYN definida actualmente por interfaz.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: seleccione la interfaz en la que desea definir la protección de velocidad.
- **Dirección IP**: ingrese la dirección IP para la que está definida la protección de velocidad SYN, o seleccione *Todas las direcciones*. Si ingresa la dirección IP, ingrese la máscara o la longitud del prefijo.
- **Máscara de red**: seleccione el formato de la máscara de subred para la dirección IP de origen e ingrese un valor en uno de los campos:
  - *Máscara*: seleccione la subred a la que pertenece la dirección IP de origen e ingrese la máscara de subred en formato decimal con punto.

- *Longitud de prefijo*: seleccione la longitud del prefijo e ingrese el número de bits que componen el prefijo de la dirección IP de origen.

- **Límite de velocidad de SYN**: ingrese el número de paquetes SYN que se deben recibir.

PASO 4 Haga clic en **Aplicar**. Se define la protección de velocidad SYN y se actualiza el archivo Configuración en ejecución.

Filtrado del ICMP

En la página Filtrado ICMP se pueden bloquear los paquetes ICMP de ciertas fuentes. lo que puede reducir la carga en la red en caso de un ataque de ICMP.

Para definir el filtrado ICMP:

PASO 1 Haga clic en **Seguridad** > **Prevención de negación de servicio** > **Filtrado ICMP**.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: seleccione la interfaz en la que desea definir el filtrado ICMP.
- **Dirección IP**: ingrese la dirección IPv4 para la que está activado el filtrado de paquetes ICMP o seleccione *Todas las direcciones* para bloquear los paquetes ICMP de todas las direcciones de origen. Si ingresa la dirección IP, ingrese la máscara o la longitud del prefijo.
- **Máscara de red**: seleccione el formato de la máscara de subred para la dirección IP de origen e ingrese un valor en uno de los campos:
  - *Máscara*: seleccione la subred a la que pertenece la dirección IP de origen e ingrese la máscara de subred en formato decimal con punto.
  - *Longitud de prefijo*: seleccione la longitud del prefijo e ingrese el número de bits que componen el prefijo de la dirección IP de origen.

PASO 4 Haga clic en **Aplicar**. Se define el filtrado ICMP y se actualiza el archivo Configuración en ejecución.

Filtrado de IP fragmentada

En la página IP fragmentada, se puede bloquear los paquetes IP fragmentados.

Para configurar el bloqueo de IP fragmentadas:

PASO 1 Haga clic en **Seguridad** > **Prevención de negación de servicio** > **Filtrado de fragmentos IP**.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: seleccione la interfaz en la que desea definir la fragmentación IP.
- **Dirección IP**: ingrese una red IP de la que se filtran los paquetes IP fragmentados o seleccione *Todas las direcciones* para bloquear los paquetes IP fragmentados de todas las direcciones. Si ingresa la dirección IP, ingrese la máscara o la longitud del prefijo.
- **Máscara de red**: seleccione el formato de la máscara de subred para la dirección IP de origen e ingrese un valor en uno de los campos:
  - *Máscara*: seleccione la subred a la que pertenece la dirección IP de origen e ingrese la máscara de subred en formato decimal con punto.
  - *Longitud de prefijo*: seleccione la longitud del prefijo e ingrese el número de bits que componen el prefijo de la dirección IP de origen.

PASO 4 Haga clic en **Aplicar**. Se define el filtrado IP y se actualiza el archivo Configuración en ejecución.

Indagación de DHCP

Consulte **Retransmisión/Indagación DHCPv4**.

Protección de la IP de origen

La protección de la IP de origen es una función de seguridad que se puede usar para impedir los ataques de tráfico provocados cuando un host intenta utilizar la dirección IP de su vecino.

Cuando la protección de la IP de origen está activada, el dispositivo solo transmite el tráfico IP del cliente a las direcciones IP incluidas en la base de datos de vinculación de indagación de DHCP. Esto incluye tanto las direcciones añadidas mediante la indagación de DHCP como las entradas añadidas manualmente.

Si el paquete coincide con una entrada de la base de datos, el dispositivo lo reenvía. De lo contrario, lo descarta.

Interacciones con otras funciones

Los siguientes puntos son pertinentes a la protección de la IP de origen:

- La indagación de DHCP debe estar habilitada globalmente para que se pueda habilitar la protección de la IP de origen en una interfaz.
- La protección de la IP de origen puede estar activa en una interfaz únicamente si:
  - La indagación de DHCP está habilitada en por lo menos una de las VLAN del puerto.
  - La interfaz es DHCP no confiable. Todos los paquetes que se encuentran en puertos confiables se reenvían.
- Si un puerto es DHCP confiable, se puede configurar el filtrado de direcciones IP estáticas, incluso si la protección de la IP de origen no está activa en esa condición, al habilitar la protección de la IP de origen en el puerto.
- Cuando el estado de un puerto cambia de DHCP no confiable a DHCP confiable, las entradas de filtrado de la dirección IP estática permanecen en la base de datos de vinculación, pero se vuelven inactivas.
- La seguridad de puertos no se puede habilitar si se configura el filtrado de la IP de origen y de la dirección MAC en un puerto.
- La protección de la IP de origen utiliza recursos TCAM y necesita una sola regla TCAM por entrada de dirección con protección de IP de origen. Si la cantidad de entradas con protección de la IP de origen excede la cantidad de reglas TCAM disponibles, las direcciones extra están inactivas.

Filtrado

Si la protección de la IP de origen está habilitada en un puerto:

- Se permite el acceso a los paquetes DHCP admitidos mediante la indagación de DHCP.
- Si la dirección IP de origen está habilitada:
  - Tráfico IPv4: solo se admite el tráfico con una dirección IP de origen que esté asociada con el puerto.
  - Tráfico no IPv4: se admite (incluidos los paquetes ARP).

Configuración del flujo de trabajo de la protección de la IP de origen

Para configurar la protección de la IP de origen:

PASO 1 Active la indagación de DHCP en la página Configuración de IP > DHCP > Propiedades o en la página Seguridad > Indagación de DHCP > Propiedades.

PASO 2 Defina las VLAN donde está activada la indagación de DHCP en la página Configuración de IP > DHCP > Configuración de la interfaz.

PASO 3 Configure las interfaces como confiables o no confiables en la página Configuración de IP > DHCP > Interfaz de indagación de DHCP.

PASO 4 Active la protección de la IP de origen en la página Seguridad > Protección de la IP de origen > Propiedades.

PASO 5 Active la protección de la IP de origen en las interfaces no confiables como se requiere en la página Seguridad > Protección de la IP de origen > Configuración de la interfaz.

PASO 6 Consulte las entradas de la base de datos de vinculación en la página Seguridad > Protección de la IP de origen > Base de datos de vinculación.

Habilitación de la protección de la IP de origen

Para habilitar la protección de la IP de origen globalmente:

PASO 1 Haga clic en **Seguridad** > **Protección de la IP de origen** > **Propiedades**.

PASO 2 Seleccione **Habilitar** para habilitar la protección de la IP de origen globalmente.

PASO 3 Haga clic en **Aplicar** para habilitar la protección de la IP de origen.

Configuración de la protección de la IP de origen en las interfaces

Si la protección de la IP de origen está habilitada en un puerto/LAG no confiable, se transmiten paquetes DHCP admitidos mediante la indagación de DHCP. Si el filtrado de dirección IP de origen está habilitado, la transmisión de paquetes se admite de la siguiente manera:

- **Tráfico IPv4:** solo se admitirá el tráfico IPv4 que tenga una dirección IP de origen que esté asociada con el puerto específico.
- **Tráfico no IPv4:** se admite todo el tráfico que no es IPv4.

Consulte **Interacciones con otras funciones** para obtener más información sobre cómo habilitar la protección de la IP de origen en las interfaces.

Para configurar la protección de la IP de origen en las interfaces:

PASO 1 Haga clic en **Seguridad** > **Protección de la IP de origen** > **Configuración de la interfaz.**

PASO 2 Seleccione puerto/LAG en el campo **Filtro** y haga clic en **Ir**. Los puertos/LAG de esta unidad se muestran junto con lo siguiente:

- **Protección de la IP de origen**: indica si la protección de la IP de origen está habilitada en el puerto.
- **Interfaz confiable de indagación de DHCP**: indica si se trata de una interfaz confiable de DHCP.

PASO 3 Seleccione el puerto/LAG y haga clic en **Editar**. Seleccione **Habilitar** en el campo **Protección de la IP de origen** para habilitar la protección de la IP de origen en la interfaz.

PASO 4 Haga clic en **Aplicar** para copiar la configuración en el archivo Configuración en ejecución.

Base de datos de vinculación

La protección de la IP de origen usa la base de datos de vinculación de indagación de DHCP para comprobar los paquetes provenientes de puertos no confiables. Si el dispositivo intenta escribir demasiadas entradas en la base de datos de vinculación de indagación de DHCP, las entradas excedentes se mantienen en un estado inactivo. Las entradas se eliminan cuando su tiempo de validez caduca; por lo tanto, las entradas inactivas pueden volverse activas.

Consulte **Retransmisión/Indagación DHCPv4**.

NOTA En la página Base de datos de vinculación, **solo** se muestran las entradas en la base de datos de vinculación de indagación de DHCP definidas en los puertos activados para protección de la IP de origen.

Para consultar la base de datos de vinculación de indagación de DHCP y ver el uso de TCAM, establezca **Insertar inactivo**:

PASO 1 Haga clic en **Seguridad** > **Protección de la IP de origen** > **Base de datos de vinculación**.

PASO 2 La base de datos de vinculación de indagación de DHCP usa recursos TCAM para administrar la base de datos. Complete el campo **Insertar inactivo** para seleccionar con qué frecuencia el dispositivo debe tratar de activar las entradas inactivas. Tiene las siguientes opciones:

- **Frecuencia de reintento**: frecuencia con la que se comprueban los recursos TCAM.
- **Nunca**: nunca intente reactivar las direcciones inactivas.

PASO 3 Haga clic en **Aplicar** para guardar los cambios anteriores en Configuración en ejecución o en **Reintentar ahora** para comprobar los recursos TCAM.

Se muestran las entradas de la base de datos de vinculación:

- **ID de VLAN:** VLAN en la que se espera el paquete.
- **Dirección MAC:** dirección MAC que se hará coincidir.
- **Dirección IP:** dirección IP que se hará coincidir.
- **Interfaz**: interfaz en la que se espera el paquete.
- **Estado**: muestra si la interfaz está activa.
- **Tipo**: muestra si la entrada es dinámica o estática.
- **Razón**: si la interfaz no está activa, se muestra la razón. Las siguientes razones son posibles:
  - *Sin problema*: la interfaz está activa.
  - *Sin indagación de VLAN*: la indagación de DHCP no está habilitada en la VLAN.
  - *Puerto confiable*: puerto que se ha vuelto confiable.
  - *Problema de recurso*: se han agotado los recursos TCAM.

Para ver un subconjunto de estas entradas, ingrese los criterios de búsqueda relevantes y haga clic en **Ir**.

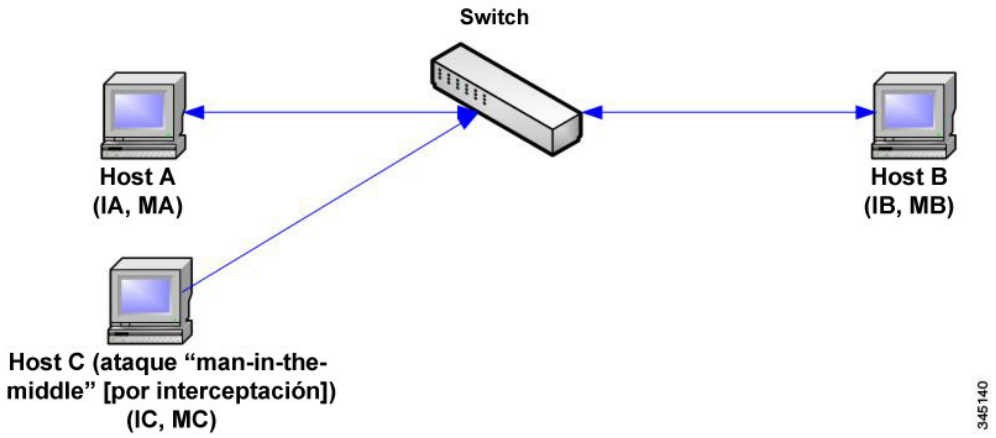
Inspección de ARP

ARP habilita la comunicación IP dentro de un dominio de difusión de capa 2 al asignar direcciones IP a las direcciones MAC.

Un usuario malintencionado puede atacar a los hosts, los switches y los routers conectados a una red de capa 2 al envenenar las memorias caché ARP de los sistemas conectados a la subred y al interceptar el tráfico que se dirige a otros hosts de la subred. Esto puede ocurrir porque ARP permite una respuesta gratuita por parte de un host incluso si no se recibió una solicitud ARP. Después del ataque, todo el tráfico proveniente del dispositivo que recibió el ataque fluye a través del equipo del atacante y luego se dirige al router, al switch o al host.

Lo siguiente muestra un ejemplo de envenenamiento de memoria caché de ARP.

Envenenamiento de memoria caché de ARP



Los hosts A, B y C se conectan con el switch en las interfaces A, B y C, de las cuales todas se encuentran en la misma subred. Sus direcciones IP y MAC aparecen en paréntesis; por ejemplo, el host A usa la dirección IP IA y la dirección MAC MA. Cuando el host A necesita comunicarse con el host B en la capa de IP, transmite una solicitud ARP para la dirección MAC asociada con la dirección IP IB. El host B responde con una respuesta ARP. El switch y el host A actualizan su caché ARP con las direcciones MAC e IP del host B.

El host C puede envenenar las memorias caché de ARP del switch, el host A y el host B al transmitir respuestas ARP falsificadas con vinculaciones para un host con una dirección IP de IA (o IB) y una dirección MAC de MC. Los hosts con memorias caché de ARP envenenadas usan la dirección MAC MC como dirección MAC de destino para el tráfico que se dirige a IA o IB, lo que habilita al host C a interceptar ese tráfico. Debido a que el host C conoce las verdaderas direcciones MAC asociadas con IA e IB, puede reenviar el tráfico

interceptado a los hosts al usar la dirección MAC correcta como destino. El host C se ha insertado en el flujo de tráfico desde el host A hasta el host B, que es el clásico ataque "man-in-the-middle" (por interceptación).

De qué manera ARP evita el envenenamiento de caché

La función de inspección de ARP se relaciona con las interfaces, ya sean confiables o no confiables (consulte la página Seguridad > Inspección de ARP > Configuración de la interfaz).

A las interfaces las clasifica el usuario de la siguiente manera:

- **Confiables:** no se inspeccionan los paquetes.
- **No confiables:** se inspeccionan los paquetes como se describió anteriormente.

La inspección de ARP se realiza únicamente en interfaces no confiables. Los paquetes ARP que se reciben en la interfaz confiable simplemente se reenvían.

Ante la llegada de un paquete a las interfaces no confiables, se implementa la siguiente lógica:

- Busque las reglas de control de acceso ARP para las direcciones IP/MAC del paquete. Si se encuentra la dirección IP y la dirección MAC que aparece en la lista coincide con la dirección MAC del paquete, significa que el paquete es válido; de lo contrario, no lo es.
- Si no se encuentra la dirección IP del paquete y la indagación de DHCP está habilitada para la VLAN del paquete, busque en la base de datos de vinculación de indagación de DHCP el par <dirección IP - VLAN> del paquete. Si no se encuentra el par <VLAN - dirección IP> y la dirección MAC y la interfaz que figuran en la base de datos coinciden con la dirección MAC del paquete y la interfaz de ingreso, significa que el paquete es válido.
- Si no se encontró la dirección IP del paquete en las reglas de control de acceso ARP ni en la base de datos de vinculación de indagación de DHCP, significa que el paquete no es válido y se descarta. Se genera un mensaje SYSLOG.
- Si el paquete es válido, se reenvía y la memoria caché ARP se actualiza.

Si la opción Validación de paquete de ARP está seleccionada (página Propiedades), se realizan las siguientes comprobaciones de validación adicionales:

- **MAC de origen**: compara la dirección MAC de origen del paquete que aparece en el encabezado Ethernet con la dirección MAC del remitente que aparece en la solicitud ARP. La comprobación se realiza tanto en las solicitudes como en las respuestas ARP.
- **MAC de destino**: compara la dirección MAC de destino del paquete que aparece en el encabezado Ethernet con la dirección MAC de la interfaz de destino. Esta comprobación se realiza para las respuestas ARP.

- **Direcciones IP**: compara el cuerpo ARP para detectar direcciones IP no válidas o inesperadas. Las direcciones incluyen 0.0.0.0, 255.255.255.255 y todas las direcciones IP de multidifusión.

Los paquetes con vinculaciones de inspección de ARP no válidos se registran y se descartan.

Se puede definir un máximo de 1024 entradas en la tabla de control de acceso ARP.

Interacción entre Inspección de ARP e Indagación de DHCP

Si la indagación de DHCP está habilitada, la inspección de ARP usa la base de datos de vinculación de indagación de DHCP además de las reglas de control de acceso de ARP. Si la indagación de DHCP no está habilitada, solo se usan las reglas de control de acceso de ARP.

Valores predeterminados de ARP

La siguiente tabla describe los valores predeterminados de ARP:

Opción	Estado predeterminado
Inspección de ARP dinámica	No aplicable
Validación de paquete de ARP	No aplicable
Inspección de ARP habilitada en VLAN	No aplicable
Intervalo de búfer de registro	La generación de mensajes SYSLOG para paquetes descartados se habilita en un intervalo de 5 segundos.

Flujo de trabajo de la inspección de ARP

Para configurar la inspección de ARP:

PASO 1 Active la inspección de ARP y configure las diversas opciones en la página Seguridad > Inspección de ARP > Propiedades.

PASO 2 Configure las interfaces como ARP confiables o no confiables en la página Seguridad > Inspección de ARP > Configuración de la interfaz.

PASO 3 Agregue reglas en las páginas Seguridad > Inspección de ARP > Control de acceso ARP y Reglas de control de acceso ARP.

PASO 4 Defina las VLAN donde está activada la inspección de ARP y las reglas de control de acceso ARP para cada VLAN en la página Seguridad > Inspección de ARP > Configuración de VLAN.

Definición de las propiedades de la inspección de ARP

Para configurar la inspección de ARP:

PASO 1 Haga clic en **Seguridad** > **Inspección de ARP** > **Propiedades**.

Ingrese los siguientes campos:

- **Estado de inspección de ARP:** seleccione esta opción para habilitar la inspección de ARP.
- **Validación de paquete de ARP**: seleccione esta opción para habilitar las siguientes comprobaciones de validación:
  - **MAC de origen**: compara la dirección MAC de origen del paquete que aparece en el encabezado Ethernet con la dirección MAC del remitente que aparece en la solicitud ARP. La comprobación se realiza tanto en las solicitudes como en las respuestas ARP.
  - **MAC de destino**: compara la dirección MAC de destino del paquete que aparece en el encabezado Ethernet con la dirección MAC de la interfaz de destino. Esta comprobación se realiza para las respuestas ARP.
  - **Direcciones IP**: compara el cuerpo ARP para detectar direcciones IP no válidas o inesperadas. Las direcciones incluyen 0.0.0.0, 255.255.255.255 y todas las direcciones IP de multidifusión.
- **Intervalo de búfer de registro**: seleccione una de las siguientes opciones:
  - **Frecuencia de reintento:** habilite el envío de mensajes SYSLOG para los paquetes descartados. Queda ingresada la frecuencia con la que se envían lo mensajes.
  - **Nunca:** los mensajes SYSLOG para paquetes descartados están deshabilitados.

PASO 2 Haga clic en **Aplicar**. Se define la configuración y se actualiza el archivo Configuración en ejecución.

Definición de la configuración de las interfaces de inspección de ARP dinámica

Los paquetes de puertos/LAG no confiables se comprueban en comparación con la tabla de reglas de acceso ARP y la base de datos de vinculación de indagación de DHCP si la indagación de DHCP está activada (consulte la página Base de datos de vinculación de indagación de DHCP).

De forma predeterminada, los puertos/LAG corresponden a la inspección de ARP no confiable.

Para cambiar un puerto/LAG ARP al estado confiable:

PASO 1 Haga clic en **Seguridad** > **Inspección de ARP** > **Configuración de interfaz**.

Se muestran los puertos/LAG y sus estados ARP confiable/no confiable.

PASO 2 Para establecer un puerto/LAG como no confiable, seleccione el puerto/LAG y haga clic en **Editar**.

PASO 3 Seleccione **Confiable** o **No confiable** y haga clic en **Aplicar** para guardar la configuración en el archivo Configuración en ejecución.

Definición del control de acceso de inspección de ARP

Para añadir entradas en la tabla de inspección de ARP:

PASO 1 Haga clic en **Seguridad** > **Inspección de ARP > Control de acceso ARP**.

PASO 2 Para añadir una entrada, haga clic en **Añadir**.

PASO 3 Ingrese los campos:

- **Nombre de control de acceso ARP**: ingrese un nombre creado por el usuario.
- **Dirección IP**: dirección IP del paquete.
- **Dirección MAC**: dirección MAC del paquete.

PASO 4 Haga clic en **Aplicar**. Se define la configuración y se actualiza el archivo Configuración en ejecución.

Definición de las reglas de control de acceso de inspección de ARP

Para añadir más reglas a un grupo de control de acceso de ARP creado anteriormente:

PASO 1 Haga clic en **Seguridad** > **Inspección de ARP > Reglas de control de acceso ARP**.

Se muestran las reglas de acceso actualmente definidas.

PASO 2 Para añadir más reglas a un grupo, haga clic en **Añadir**.

PASO 3 Seleccione un Grupo de control de acceso e ingrese los campos:

- **Dirección IP**: dirección IP del paquete.
- **Dirección MAC**: dirección MAC del paquete.

PASO 4 Haga clic en **Aplicar**. Se define la configuración y se actualiza el archivo Configuración en ejecución.

Definición de la configuración de la VLAN de inspección de ARP

Para habilitar la inspección de ARP en las VLAN y asociar los grupos de control de acceso con una VLAN:

PASO 1 Haga clic en **Seguridad** > **Inspección de ARP > Configuración de VLAN**.

PASO 2 Para habilitar la inspección de ARP en una VLAN, mueva la VLAN de la lista **VLAN disponibles** a la lista **VLAN habilitadas**.

PASO 3 Para asociar un grupo de control de acceso ARP con una VLAN, haga clic en **Añadir**. Seleccione el número de VLAN y seleccione un grupo de **Control de acceso ARP** definido anteriormente.

PASO 4 Haga clic en **Aplicar**. Se define la configuración y se actualiza el archivo Configuración en ejecución.

Seguridad de primer salto

Seguridad: Seguridad del primer salto de IPv6

20

Seguridad: Autenticación 802.1X

Esta sección describe la autenticación 802.1X.

Abarca los siguientes temas:

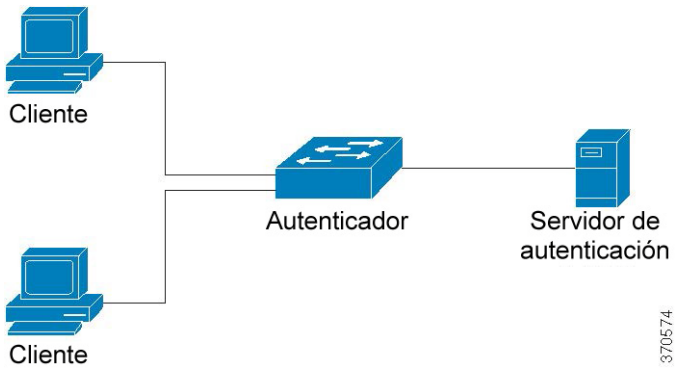
- **Descripción general de 802.1X**
- **Información general del autenticador**
- **Tareas comunes**
- **Configuración de 802.1X mediante GUI**
- **Definición de intervalos de tiempo**
- **Compatibilidad de modo de puerto y método de autenticación**

Descripción general de 802.1X

La autenticación 802.1x impide a los clientes no autorizados conectarse a una LAN mediante puertos de acceso público. La autenticación 802.1x es un modelo cliente-servidor. En este modelo, los dispositivos de red tienen los siguientes roles específicos.

- Cliente o solicitante
- Autenticador
- Servidor de autenticación

Esto se ilustra en la siguiente figura:



Un dispositivo de red puede ser cliente o solicitante, autenticador o ambos por puerto.

Cliente o solicitante

Un cliente o solicitante es un dispositivo de red que solicita acceso a la LAN. El cliente se conecta a un autenticador.

Si el cliente usa el protocolo 802.1x para la autenticación, ejecuta la parte solicitante del protocolo 802.1x y la parte cliente del protocolo EAP.

No se requiere ningún software especial en el cliente para usar la autenticación basada en la Web o en MAC.

Autenticador

Un autenticador es un dispositivo de red que proporciona servicios de red y al que se conectan los puertos solicitantes.

Se admiten los siguientes modos de autenticación en los puertos (estos modos están establecidos en Seguridad > Autenticación 802.1X/MAC/web > Autenticación de host y sesión):

- **Host único**: admite la autenticación basada en puertos con un solo cliente por puerto.
- **Host múltiple**: admite la autenticación basada en puertos con varios clientes por puerto.
- **Sesión múltiple**: admite la autenticación basada en el cliente con varios clientes por puerto.

Para obtener más información, consulte **Modos de host del puerto**.

Se admiten los siguientes métodos de autenticación:

- **Basado en 802.1x**: compatible con todos los modos de autenticación.
- **Basado en MAC**: compatible con todos los modos de autenticación.
- **Basado en la Web**: compatible solo con modos de sesión múltiple.

En la autenticación basada en 802.1x, el autenticador extrae los mensajes EAP de los mensajes 802.1x (tramas EAPOL) y los envía al servidor de autenticación mediante el protocolo RADIUS.

En la autenticación basada en MAC o web, el autenticador es quien ejecuta la parte cliente EAP del software.

Servidor de autenticación

Un servidor de autenticación lleva a cabo la autenticación real del cliente. El servidor de autenticación para el dispositivo es un servidor de autenticación RADIUS con extensiones EAP.

Open Access

La función Open Access (Monitoring) es útil para separar las fallas de autenticación reales de aquellas fallas ocasionadas por errores de configuración o falta de recursos en un entorno 802.1x.

Open Access ayuda a los administradores de sistemas a comprender los problemas de configuración de los hosts conectados a la red, controla situaciones erróneas y facilita la resolución de problemas.

Cuando se habilita Open Access en una interfaz, el switch trata como éxito a las fallas que recibe de un servidor RADIUS y habilita el acceso a la red de las estaciones conectadas a interfaces, independientemente de los resultados de la autenticación.

Open Access cambia el comportamiento normal de bloqueo de tráfico en un puerto habilitado por la autenticación hasta que se realicen con éxito la autenticación y la autorización. El comportamiento predeterminado de la autenticación sigue siendo bloquear todo el tráfico, salvo el Protocolo de autenticación extensible sobre LAN (EAPoL). No obstante, Open Access ofrece al administrador la posibilidad de brindar acceso ilimitado a todo el tráfico, aunque esté habilitada la autenticación (basada en 802.1X, en MAC o WEB).

Cuando está habilitada la contabilidad RADIUS, puede registrar los intentos de autenticación y obtener visibilidad de quién y qué se conecta a la red gracias a un rastro de auditoría.

Todos esos beneficios se consiguen sin afectar al usuario final ni a los hosts conectados a la red. Open Access puede activarse en la página **Autenticación de puertos 802.1X**.

Información general del autenticador

Estados de autenticación administrativa del puerto

El estado administrativo del puerto determina si el cliente tiene acceso a la red.

El estado administrativo del puerto puede configurarse en la página Seguridad > Autenticación 802.1X/ MAC/web > Autenticación de puertos.

Los siguientes valores están disponibles:

- **force-authorized**

  La autenticación del puerto está desactivada y el puerto envía todo el tráfico de acuerdo con su configuración estratégica sin requerir ninguna autenticación. El switch envía el paquete EAP 802.1x con el mensaje de éxito EAP cuando recibe el mensaje de inicio de EAPOL 802.1x.

  Este es el estado predeterminado.

- **force-unauthorized**

  La autenticación de puertos está desactivada y el puerto envía todo el tráfico mediante la VLAN invitada y las VLAN no autenticadas. Para obtener más información, consulte **Definición de la Autenticación de host y sesión**. El switch envía los paquetes EAP 802.1x con el mensaje de falla EAP cuando recibe los mensajes de inicio de EAPOL 802.1x.

- **automático**

  Habilita las autenticaciones 802.1 x de acuerdo con el modo de host del puerto configurado y los métodos de autenticación configurados en el puerto.

Modos de host del puerto

Los puertos pueden configurarse en los siguientes modos de host de puerto (configurados en la página Seguridad > Autenticación 802.1X/MAC/web > Host y autenticación):

- **Modo de host único**

  Un puerto está autorizado si hay un cliente autorizado. Solo puede configurarse un host en un puerto.

  Cuando un puerto no está autorizado y la VLAN invitada está activada, el tráfico sin etiqueta se reasigna a la VLAN invitada. El tráfico etiquetado se descarta, a menos que pertenezca a la VLAN invitada o a una VLAN no autenticada. Si no hay una VLAN invitada activa en el puerto, solo se interliga el tráfico etiquetado que pertenezca a las VLAN no autenticadas.

  Si un puerto está autorizado, el tráfico etiquetado y sin etiquetar proveniente del host autorizado se interliga en base a la configuración de puertos miembro de la VLAN estática. Se descarta el tráfico de otros hosts.

  Un usuario puede especificar que el tráfico sin etiquetar proveniente del host autorizado se reasigne a una VLAN asignada por un servidor RADIUS durante el proceso de autenticación. El tráfico etiquetado se descarta, a menos que pertenezca a la VLAN asignada por RADIUS o a las VLAN no autenticadas. La asignación Radius de VLAN en un puerto puede configurarse en la página Seguridad > Autenticación 802.1X/MAC/web > Autenticación de puertos.

- **Modo de host múltiple**

  Un puerto está autorizado si hay al menos un cliente autorizado.

  Cuando un puerto no está autorizado y hay una VLAN invitada activada, el tráfico sin etiqueta se reasigna a la VLAN invitada. El tráfico etiquetado se descarta, a menos que pertenezca a la VLAN invitada o a una VLAN no autenticada. Si no hay una VLAN invitada activa en el puerto, solo se interliga el tráfico etiquetado que pertenezca a las VLAN no autenticadas.

  Si un puerto está autorizado, se interliga el tráfico etiquetado y sin etiquetar proveniente de todos los hosts conectados al puerto en base a la configuración de puertos miembro de la VLAN estática.

  Usted puede especificar que el tráfico sin etiquetar proveniente del puerto autorizado se reasigne a una VLAN asignada por un servidor RADIUS durante el proceso de autenticación. El tráfico etiquetado se descarta, a menos que pertenezca a la VLAN asignada por RADIUS o a las VLAN no autenticadas. La asignación Radius de VLAN en un puerto se configura en la página Autenticación de puertos.

- **Modo de sesión múltiple**

  A diferencia de los modos de host único y múltiple, si un puerto está en el modo de sesión múltiple, no tiene un estado de autenticación. Este estado se asigna a cada cliente conectado al puerto. Este modo requiere una búsqueda en TCAM. Como los switches del modo de capa 3 no tienen una búsqueda en TCAM asignada para el modo de sesión múltiple, admiten una forma limitada de modo de sesión múltiple que no es compatible con los atributos de VLAN invitada y RADIUS VLAN. En la página Autenticación de puertos, se configura la cantidad máxima de hosts autorizados permitidos en un puerto.

  El tráfico etiquetado que pertenece a una VLAN no autenticada siempre se interliga independientemente de si el host está o no autorizado.

  El tráfico etiquetado y sin etiquetar proveniente de los hosts no autorizados que no pertenecen a una VLAN no autenticada se reasigna a la VLAN invitada si está definida y habilitada en la VLAN. O bien, se descarta si la VLAN no está habilitada en el puerto.

  Si un servidor RADIUS asignó un host autorizado a una VLAN, todo el tráfico etiquetado y no etiquetado que no pertenece a las VLAN no autenticadas se interliga a través de la VLAN. Si la VLAN no está asignada, todo el tráfico se interliga en base a la configuración de puertos miembro de la VLAN estática.

  El Sx300 en un modo de router de capa 3 admite el modo de sesión múltiple sin asignar una VLAN invitada ni RADIUS-VLAN:

Métodos de autenticación múltiples

Si en el switch se activa más de un método de autenticación, se aplica la siguiente jerarquía de métodos de autenticación:

- Autenticación 802.1x: más alta
- Autenticación basada en web
- Autenticación basada en MAC: más baja

Pueden ejecutarse varios métodos al mismo tiempo. Si un método se completa correctamente, se autoriza el cliente, se detienen los métodos con menor prioridad y continúan los métodos con mayor prioridad.

Si falla uno de los métodos de autenticación que se ejecuta en simultáneo, los demás métodos continúan.

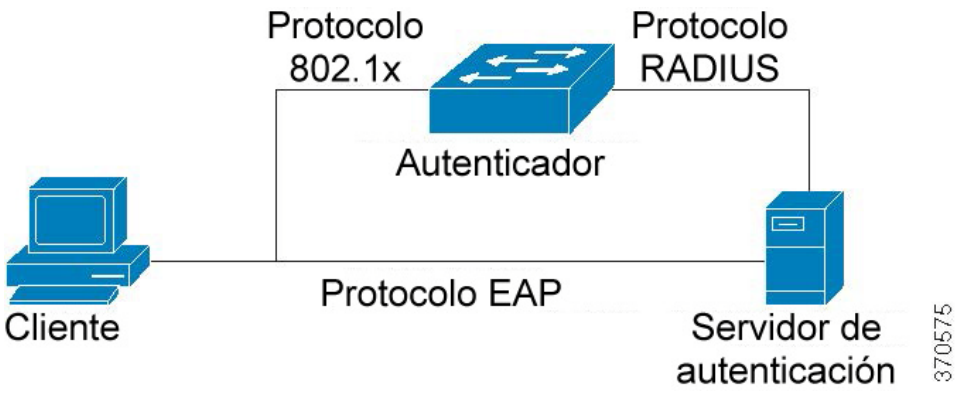
Si un método de autenticación se completa correctamente para un cliente autenticado por un método de autenticación con menor prioridad, se aplican los atributos del nuevo método de autenticación. Cuando el nuevo método falla, el cliente queda autorizado con el método anterior.

Autenticación basada en 802.1x

El autenticador basado en 802.1x retransmite mensajes EAP transparentes entre los solicitantes 802.1x y los servidores de autenticación. Los mensajes EAP entre los solicitantes y el autenticador se encapsulan en mensajes 802.1x, y los mensajes EAP entre el autenticador y los servidores de autenticación se encapsulan en mensajes RADIUS.

Esto se describe a continuación:

Figura 3 Autenticación basada en 802.1x

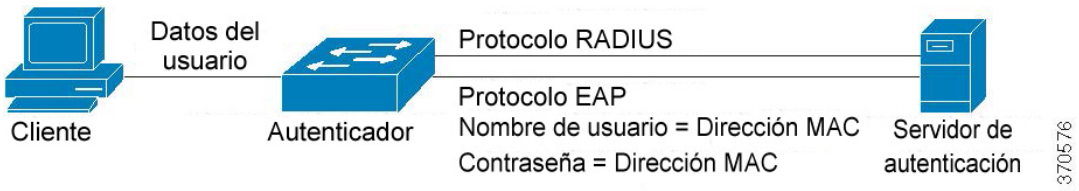


Autenticación basada en MAC

La autenticación basada en MAC es una alternativa de la autenticación 802.1X que permite a los dispositivos sin capacidad de solicitantes 802.1X (p. ej., impresoras y teléfonos IP) acceder a la red. La autenticación basada en MAC usa la dirección MAC del dispositivo que se conecta para otorgar o denegar acceso a la red.

En este caso, el switch admite la funcionalidad EAP MD5 con el nombre de usuario y contraseña equivalente a la dirección MAC del cliente, como se muestra a continuación.

Figura 4 Autenticación basada en MAC



El método no tiene ninguna configuración específica.

Autenticación basada en web

La autenticación basada en web se usa para autenticar a los usuarios finales que solicitan el acceso a la red a través de un switch. Permite a los clientes conectarse directamente al switch para autenticarse mediante un mecanismo de Captive Portal antes de que el cliente tenga acceso a la red. La autenticación basada en web esta basada en el cliente; es compatible con el modo de sesión múltiple de capa 2 y 3.

Este método de autenticación se activa por puerto; cuando un puerto se activa, cada host debe autenticarse para acceder a la red. Por eso en un puerto activo, es posible tener hosts autenticados y no autenticados.

Cuando en un puerto se activa la autenticación basada en web, el switch descarta todo el tráfico que pretende ingresar al puerto desde clientes no autorizados, salvo para los paquetes ARP, DHCP y DNS. El switch puede reenviar estos paquetes para que incluso los clientes no autorizados puedan obtener una dirección IP y resolver los nombres de host y dominio.

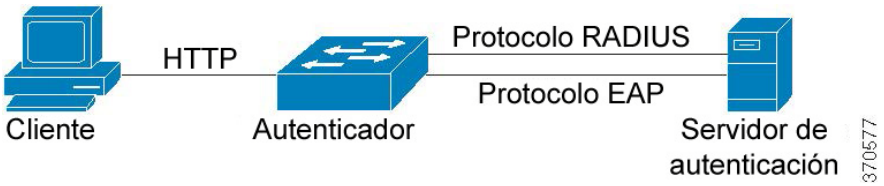
Todos los paquetes HTTP/HTTPS sobre IPv4 provenientes de clientes no autorizados quedan capturados en la CPU del switch. Si un usuario final solicita acceso a la red en un puerto que tiene activada la autenticación basada en web, se muestra una página de inicio de sesión antes de abrirse la página solicitada. El usuario debe ingresar su nombre de usuario y contraseña, a los que debe autenticar un servidor RADIUS mediante un protocolo EAP. Si la autenticación se realiza correctamente, el usuario será informado.

El usuario contará con una sesión autenticada. La sesión permanece abierta mientras se utiliza. Si no se usa durante un intervalo específico, se cerrará la sesión. Este intervalo está configurado por el administrador del sistema y se denomina Tiempo de silencio. Si se agota el tiempo de espera de la sesión, se descartarán el nombre de usuario y la contraseña, y el invitado deberá volver a ingresarlos para abrir una nueva sesión.

Consulte **Métodos de autenticación y modos de puerto**.

Tras completarse la autenticación, el switch reenvía todo el tráfico que llega del cliente en el puerto, como se muestra en la siguiente figura.

Figura 5 Autenticación basada en web



La autenticación basada en web no puede configurarse en un puerto que tenga activada la característica de VLAN invitada o VLAN asignada por RADIUS.

La autenticación basada en web es compatible con las siguientes páginas:

- Página de inicio de sesión
- Página de inicio de sesión con éxito

Existe un conjunto predefinido e integrado de estas páginas.

Estas páginas pueden modificarse en la página Seguridad > Autenticación 802.1X/MAC/Web> Personalización de la autenticación web.

Usted puede obtener una vista previa de las páginas personalizadas. La configuración se guarda en el archivo de Configuración en ejecución.

La siguiente tabla describe los SKU que admiten la autenticación basada en web y en qué modos del sistema:

SKU	Modo del sistema	Compatible con WBA
Sx300	**Capa 2**	Sí
	Capa 3	No
Sx500, Sx500ESW2-550X	**Capa 2**	Sí
	Capa 3	No

SKU	Modo del sistema	Compatible con WBA
SG500X	**Nativo**	Sí
	Híbrido básico - Capa 2	Sí
	Híbrido básico - Capa 3	No
SG500XG	**Igual que Sx500**	Sí

NOTA

- Si la autenticación basada en web no es compatible, la VLAN invitada y DVA no pueden configurarse en modo de sesión múltiple.
- Si la autenticación basada en web es compatible, la VLAN invitada y DVA pueden configurarse en modo de sesión múltiple.

VLAN no autenticadas y la VLAN invitada

Las VLAN no autenticadas y la VLAN invitada proporcionan acceso a servicios que no requieren que los dispositivos o puertos solicitantes se autentiquen y autoricen mediante 802.1x o según MAC.

La VLAN invitada es la VLAN que se asigna a un cliente no autorizado. Usted puede configurar la VLAN invitada y una o más VLAN para anular la autenticación en la página Seguridad > Autenticación 802.1X/MAC/Web > Propiedades.

Una VLAN no autenticada es una VLAN que permite el acceso de dispositivos o puertos tanto autorizados como no autorizados.

Una VLAN no autenticada tiene las siguientes características:

- Debe ser una VLAN estática y no puede ser la VLAN invitada ni la predeterminada.
- Los puertos miembro deben configurarse manualmente como miembros etiquetados.
- Los puertos miembro deben ser puertos troncales o generales. Un puerto de acceso no puede ser miembro de una VLAN no autenticada.

La VLAN invitada, si la configura, es una VLAN estática con las siguientes características:

- Debe definirse manualmente a partir de una VLAN estática existente.
- La VLAN invitada no puede usarse como la VLAN de voz o una VLAN no autenticada.

Consulte **Asignación de VLAN y RADIUS-VLAN** para ver un resumen de los modos compatibles con la VLAN invitada.

Modos de host con VLAN invitada

Los modos de host funcionan con la VLAN invitada de la siguiente manera:

- **Modo de host único y host múltiple**

  El tráfico no etiquetado y el tráfico etiquetado que pertenecen a la VLAN invitada que llegan en un puerto no autorizado se interligan a través de la VLAN invitada. Todo el otro tráfico se descarta. El tráfico que pertenece a una VLAN no autenticada se interliga a través de la VLAN.

- **Modo de sesión múltiple en Capa 2**

  El tráfico no etiquetado y el tráfico etiquetado, que no pertenecen a las VLAN no autenticadas y que llegan de clientes no autorizados, se asignan a la VLAN invitada con una regla TCAM y que se interligan a través de la VLAN invitada. El tráfico etiquetado que pertenece a una VLAN no autenticada se interliga a través de la VLAN.

  Este modo no se puede configurar en la misma interfaz con VLAN basadas en políticas.

- **Modo de sesión múltiple en Capa 3**

  El modo no admite la VLAN invitada.

Asignación dinámica de VLAN o asignación RADIUS VLAN

A un cliente no autorizado se le puede asignar una VLAN mediante el servidor RADIUS si esta opción está habilitada en la página Autenticación de puertos. Esto se denomina asignación dinámica de VLAN (DVA) o asignación RADIUS VLAN. En esta guía, se usa el término VLAN asignada por RADIUS.

Cuando un puerto está en el modo de sesión múltiple y está habilitado para VLAN asignada por RADIUS, el dispositivo se añade automáticamente al puerto como un miembro sin etiquetar de la VLAN asignada por el servidor RADIUS durante el proceso de autenticación. El dispositivo clasifica los paquetes sin etiquetar a la VLAN asignada si los paquetes provienen de los dispositivos o puertos autenticados y autorizados.

Consulte **Asignación de VLAN y RADIUS-VLAN** para obtener más información sobre el comportamiento de los diversos modos cuando se habilita la asignación RADIUS VLAN en el dispositivo.

NOTA En el modo de sesión múltiple, la asignación RADIUS VLAN solo es compatible cuando el dispositivo está en el modo del sistema de Capa 2.

Para que se autentique y autorice un dispositivo en un puerto que está activado para DVA:

- El servidor RADIUS debe autenticar el dispositivo y asignar dinámicamente una VLAN al dispositivo. En la página Autenticación de puertos, se puede configurar el campo de la asignación RADIUS VLAN en estática. Esto permite al host interligarse de acuerdo con la configuración estática.
- Un servidor RADIUS debe admitir DVA con los atributos RADIUS tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6) y tunnel-private-group-id = un ID de VLAN.

Cuando se activa la característica de VLAN asignada por RADIUS, los modos de host se comportan de la siguiente manera:

- **Modo de host único y host múltiple**

  El tráfico no etiquetado y el tráfico etiquetado que pertenecen a la VLAN asignada por RADIUS se interligan a través de esta VLAN. Se descarta todo el otro tráfico que no pertenece a las VLAN no autenticadas.

- **Modo de sesión múltiple completo**

  El tráfico no etiquetado y el tráfico etiquetado que no pertenecen a las VLAN no autenticadas y que llegan del cliente se asignan a la VLAN asignada por RADIUS mediante reglas de TCAM y se interligan a través de la VLAN.

- **Modo de sesión múltiple en el modo del sistema de Capa 3**

  Este modo no admite la VLAN asignada por RADIUS,

La siguiente tabla describe la compatibilidad de la VLAN invitada y la asignación RADIUS VLAN en función del método de autenticación y el modo de puerto.

Asignación de VLAN y RADIUS-VLAN

Método de autenticación	Host único	Host múltiple	Sesión múltiple	
			Dispositivo en Capa 3	Dispositivo en Capa 2
802.1x	†	†	N/D	†
MAC	†	†	N/D	†
WEB	N/D	N/D	N/D	N/D

Leyenda:

†: el modo de puerto admite la VLAN invitada y la asignación RADIUS VLAN.

N/D: el modo de puerto no admite el método de autenticación.

Modo de incumplimiento

En el modo de host único, es posible configurar la acción por aplicar cuando un host no autorizado en un puerto autorizado intenta acceder a la interfaz. Esto se realiza en la página Autenticación de host y sesión.

Las opciones disponibles son las siguientes:

- **restrict**: genera una trampa cuando una estación, cuya dirección MAC no es la dirección MAC solicitante, intenta acceder a la interfaz. El tiempo mínimo entre las trampas es de 1 segundo. Estas tramas se reenvían, pero las direcciones de origen no se aprenden.
- **protect**: descarta tramas con otras direcciones de origen que no son solicitantes.
- **shutdown**: descarta tramas con otras direcciones de origen que no son solicitantes y cierra el puerto.

También puede configurar el dispositivo para enviar trampas SNMP con un tiempo mínimo configurable entre las trampas consecutivas. Si los segundos son = 0, las trampas se deshabilitan. Si no se indica un tiempo mínimo, el valor predeterminado es de 1 segundo para el modo restringido y 0 para los otros modos.

Período de silencio

El período de silencio es un intervalo en el que el puerto (modos de host único y múltiple) o el cliente (modo de sesión múltiple) no pueden intentar la autenticación luego de un intercambio de autenticación fallido. En el modo de host único o múltiple, el período se define por puerto; en el modo de sesiones múltiples, el período se define por cliente. Durante el período de silencio, el switch no acepta ni inicia solicitudes de autenticación.

El período se aplica solo a las autenticaciones basadas en 802.1x o web.

También puede especificar la cantidad máxima de intentos de inicio de sesión antes de iniciarse el período de silencio. Un valor de 0 indica la cantidad ilimitada de intentos de inicio de sesión.

La duración del período de silencio y la cantidad máxima de intentos de inicio de sesión pueden establecerse en la página Autenticación de puertos.

Tareas comunes

Flujo de trabajo 1: para habilitar la autenticación 802.1x en un puerto:

PASO 1 Haga clic en **Seguridad > Autenticación 802.1X/MAC/Web > Propiedades**.

PASO 2 Habilite la autenticación basada en puertos.

PASO 3 Seleccione el **Método de autenticación**.

PASO 4 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

PASO 5 Haga clic en **Seguridad > Autenticación 802.1X/MAC/Web > Host y sesión**.

PASO 6 Seleccione el puerto requerido y haga clic en **Editar**.

PASO 7 Establezca el modo de autenticación de host.

PASO 8 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

PASO 9 Haga clic en **Seguridad > Autenticación 802.1X/MAC/Web > Autenticación de puertos**.

PASO 10 Seleccione un puerto y haga clic en **Editar**.

PASO 11 Establezca el campo Control del puerto administrativo en **Automático**.

PASO 12 Defina los métodos de autenticación.

PASO 13 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

Flujo de trabajo 2: para configurar las trampas

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Propiedades**.

PASO 2 Seleccione las trampas requeridas.

PASO 3 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

Flujo de trabajo 3: para configurar la autenticación basada en 802.1x o web

PASO 1 Haga clic en **Seguridad > Autenticación 802.1X/MAC/Web > Autenticación de puertos**.

PASO 2 Seleccione el puerto requerido y haga clic en **Editar**.

PASO 3 Introduzca los campos requeridos para el puerto.

Los campos de esta página están descritos en **Autenticación de puertos 802.1X**.

PASO 4 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

Use el botón **Copiar configuración** para copiar la configuración de un puerto a otro.

Flujo de trabajo 4: para configurar el período de silencio

PASO 1 Haga clic en **Seguridad > Autenticación 802.1X/MAC/Web > Autenticación de puertos**.

PASO 2 Seleccione un puerto y haga clic en **Editar**.

PASO 3 Introduzca el período de silencio en el campo Período de silencio.

PASO 4 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

Flujo de trabajo 5: para configurar la VLAN invitada:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Propiedades**.

PASO 2 Seleccione **Habilitar** en el campo VLAN invitada.

PASO 3 Seleccione la VLAN invitada en el campo ID de VLAN invitada.

PASO 4 Configure Tiempo de espera de VLAN invitada en Inmediato, o bien ingrese un valor en el campo Definido por el usuario.

PASO 5 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

Flujo de trabajo 6: para configurar las VLAN no autenticadas:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Propiedades**.

PASO 2 Seleccione una VLAN y haga clic en **Editar**.

PASO 3 Seleccione una VLAN.

PASO 4 Como opción, desmarque **Autenticación** para convertir a la VLAN en una VLAN no autenticada.

PASO 5 Haga clic en **Aplicar**, y se actualizará el archivo Configuración en ejecución.

Configuración de 802.1X mediante GUI

NOTA La autenticación basada en la Web solo es compatible en el modo de Capa 2 en dispositivos Sx300 y SG500. En dispositivos SG500XG y SG500X, es compatible en el modo Nativo e Híbrido avanzado XG.

Definición de propiedades de 802.1X

La página Propiedades de 802.1X se utiliza para activar 802.1X globalmente y definir cómo se autenticarán los puertos. Para que 802.1X funcione, se la debe activar tanto en forma global como individual en cada puerto.

Para definir la autenticación basada en el puerto:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Propiedades**.

PASO 2 Ingrese los parámetros.

- **Autenticación basada en puertos**: active o desactive la autenticación basada en puertos.

  Si está desactivado, la autenticación basada en 802.1X, MAC o web estará desactivada.

- **Método de autenticación**: seleccione los métodos de autenticación del usuario. Las opciones son:

  - *RADIUS, Ninguno*: la autenticación del puerto se realiza primero a través del servidor RADIUS. Si no se recibe respuesta por parte de RADIUS (por ejemplo, si el servidor no funciona), no se realiza la autenticación y se permite la sesión. Si el servidor está disponible, pero las credenciales del usuario son incorrectas, el acceso se rechaza y la sesión finaliza.

  - *RADIUS*: el usuario se autentica en el servidor RADIUS. Si no se realiza la autenticación, no se permite la sesión.

  - *Ninguna*: no se autentica al usuario, y se permite la sesión.

- **VLAN invitada**: seleccione esta opción para permitir usar una VLAN invitada para los puertos no autorizados. Si se habilita una VLAN invitada, todos los puertos no autorizados se unen automáticamente a la VLAN seleccionada en el campo *ID de VLAN invitada*. Si luego se autoriza un puerto, se le elimina de la VLAN invitada.

- **ID de VLAN invitada**: seleccione la VLAN invitada de la lista de VLAN.

- **Tiempo de espera de VLAN invitada**: defina un período de tiempo:

  - Luego de establecer el enlace, si el software no detecta al solicitante 802.1X, o si la autenticación no pudo realizarse, el puerto se añade a la VLAN invitada, solo después de que el período indicado en *Tiempo de espera de VLAN invitada* haya pasado.

  - Si el estado del puerto cambia de *Autorizado* a *No autorizado*, se añade el puerto a la VLAN invitada solo después de que el tiempo de espera de *VLAN invitada* se haya agotado.

- **Configuración de trampa**: para habilitar las trampas, seleccione una o varias de las siguientes opciones:

  - *Trampas de falla de la autenticación 802.1x*: seleccione para generar una trampa si falla la autenticación 802.1x.

  - *Trampas de éxito de la autenticación 802.1x*: seleccione para generar una trampa si prospera la autenticación 802.1x.

  - *Trampas de falla de la autenticación MAC*: seleccione para generar una trampa si falla la autenticación MAC.

  - *Trampas de éxito de la autenticación MAC*: seleccione para generar una trampa si prospera la autenticación MAC.

- Cuando el switch está en el modo de sistema de Capa 2 o en dispositivos SG500XG y SG500X:

  - *Trampas de falla de la autenticación web*: seleccione para generar una trampa si falla la autenticación web.

- *Trampas de éxito de la autenticación web*: seleccione para generar una trampa si prospera la autenticación web.
- *Trampas de silencio de la autenticación web*: seleccione para generar una trampa si se inicia el período de silencio.

Cuando el dispositivo está en modo de router de Capa 3, la tabla de autenticación de VLAN muestra todas las VLAN e indica si la autenticación les fue o no habilitada.

PASO 3 Haga clic en **Aplicar**. Las propiedades de 802.1X se escriben en el archivo Configuración en ejecución.

Autenticación de puertos 802.1X

La página Autenticación de puertos permite la configuración de los parámetros de 802.1X para cada puerto. Dado que algunos de los cambios de configuración solo pueden realizarse mientras el puerto está en estado Fuerza autorizada, como la autenticación de host, se recomienda cambiar el control del puerto a Fuerza autorizada antes de realizar cambios. Una vez finalizada la configuración, vuelva a colocar el control del puerto en su estado anterior.

NOTA Un puerto con 802.1X definida no puede convertirse en miembro de un LAG.

Para definir la autenticación 802.1X:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Autenticación de puertos**.

Esta página incluye los parámetros de autenticación para todos los puertos.

PASO 2 Seleccione un puerto y haga clic en **Editar**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: seleccione un puerto.
- **Control de puerto actual**: se muestra el estado actual de autorización del puerto. Si el estado es *Autorizado*, el puerto se autentica o *Control de puerto administrativo* está en *Fuerza autorizada*. Por el contrario, si el estado es *No autorizado*, entonces el puerto no se autentica o *Control de puerto administrativo* está en *Fuerza no autorizada*.
- **Control de puerto administrativo**: seleccione el estado de autorización administrativa del puerto. Las opciones son:
  - *Fuerza no autorizada*: se niega acceso a la interfaz y se coloca en estado no autorizado. El dispositivo no brinda servicios de autenticación al cliente a través de la interfaz.

- *Automático*: se activa la autenticación y la autorización basadas en el puerto en el dispositivo. La interfaz se mueve entre estado autorizado o no autorizado según el intercambio de autenticación entre el dispositivo y el cliente.
- *Fuerza autorizada*: se autoriza la interfaz sin autenticación.

- **Asignación RADIUS VLAN**: seleccione esta opción para activar la asignación dinámica de VLAN en el puerto seleccionado.
  - ***Disable***: la característica no está habilitada.
  - ***Reject***: si el servidor RADIUS autorizó al solicitante pero no proporcionó una VLAN del solicitante, se rechaza al solicitante.
  - ***Static***: si el servidor RADIUS autorizó al solicitante pero no proporcionó una VLAN del solicitante, se acepta al solicitante.
- **VLAN invitada**: seleccione esta opción para indicar que el uso de una VLAN invitada definida previamente está habilitado para el dispositivo. Las opciones son:
  - *Seleccionada*: permite usar una VLAN invitada para puertos no autorizados. Si se habilita una VLAN invitada, el puerto no autorizado se une automáticamente a la VLAN seleccionada en el campo ID de VLAN invitada en la página Autenticación de puertos 802.1X.
    Luego de una falla de autenticación, y si la opción VLAN invitada está activada en forma global en un puerto dado, se asigna automáticamente la VLAN invitada a los puertos no autorizados como una VLAN sin etiquetar.
  - *Borrado*: se desactiva la VLAN invitada en el puerto.
- **Open Access**: seleccione para autenticar correctamente el puerto aunque falle la autenticación. Consulte **Open Access**.
- **Autenticación basada en 802.1X**: la autenticación 802.1X es el único método de autenticación que se realiza en el puerto.
- **Autenticación basada en MAC**: el puerto se autentica en función de la dirección MAC del solicitante. Solo se pueden usar 8 autenticaciones basadas en MAC en el puerto.

  NOTA Para que la autenticación MAC se realice correctamente, el nombre de usuario y la contraseña del solicitante del servidor RADIUS deben ser la dirección MAC del solicitante. La dirección MAC debe ingresarse en minúsculas y sin los separadores "." ni "-"; por ejemplo: 0020aa00bbcc.
- **Autenticación basada en web**: solo está disponible en el modo de switch de Capa 2 o en SG500XG y SG500X. Seleccione para habilitar la autenticación basada en web en el switch.
- **Reautenticación periódica**: seleccione esta opción para activar intentos de reautenticación del puerto luego del período de reautenticación especificado.

- **Período de reautenticación**: ingrese la cantidad de segundos después de los que se volverá a autenticar el puerto seleccionado.
- **Reautenticar ahora**: seleccione esta opción para activar la reautenticación inmediata del puerto.
- **Estado del autenticador**: se muestra el estado de autorización del puerto definido. Las opciones son:
  - *Inicializar*: en proceso de activación.
  - *Fuerza autorizada*: el estado del puerto controlado está configurado como Fuerza autorizada (reenviar tráfico).
  - *Fuerza no autorizada*: el estado del puerto controlado está configurado como Fuerza no autorizada (descartar tráfico).

    NOTA Si el puerto no está en Fuerza autorizada o Fuerza no autorizada, está en modo Auto y el autenticador muestra el estado de la autenticación en curso. Una vez que se autentica el puerto, el estado aparece como autenticado.
- **Rango de tiempo**: permite establecer un límite en el tiempo que el puerto específico se autoriza para el uso, en caso de que se haya habilitado 802.1x (la autenticación basada en el puerto está seleccionada).
- **Nombre del intervalo de tiempo**: seleccione el perfil que especifica el intervalo de tiempo.
- **Intentos de inicio de sesión de WBA máximos**: disponible solo en switches de Capa 2 o en SG500XG y SG500X. Ingrese la cantidad máxima de intentos de inicio de sesión permitidos en la interfaz. Seleccione **Infinito** para que no haya límites, o **Definido por el usuario** para establecer un límite.
- **Período de silencio de WBA máximo**: disponible solo en modo de switch de Capa 2 o en SG500XG y SG500X. Ingrese el período de silencio máximo permitido en la interfaz. Seleccione **Infinito** para que no haya límites, o **Definido por el usuario** para establecer un límite.
- **Hosts máximos**: ingrese la cantidad máxima de hosts autorizados permitidos en la interfaz. Seleccione **Infinito** para que no haya límites, o **Definido por el usuario** para establecer un límite.

  NOTA Establezca este valor en 1 para simular el modo de host único para la autenticación basada en web en el modo de sesión múltiple.
- **Período de silencio**: ingrese la cantidad de segundos que el dispositivo permanece en estado silencioso luego de un intercambio de autenticación incorrecto.
- **Reenviar EAP**: ingrese la cantidad de segundos que el dispositivo espera una respuesta para una trama de identidad/solicitud EAP (*Extensible Authentication Protocol*, protocolo de autenticación extensible) del solicitante (cliente) antes de reenviar la solicitud.
- **Solicitudes de EAP máximas**: ingrese el número máximo de solicitudes EAP que se pueden enviar. Si no se recibe una respuesta después del período definido (tiempo de espera para solicitantes), se reinicia el proceso de autenticación.

- **Tiempo de espera para solicitantes**: ingrese la cantidad de segundos que deben transcurrir antes de que se reenvíen las solicitudes EAP al solicitante.
- **Tiempo de espera de servidor**: ingrese la cantidad de segundos que deben transcurrir antes de que el dispositivo reenvíe una solicitud al servidor de autenticación.

PASO 4 Haga clic en **Aplicar**. La configuración del puerto se escribe en el archivo Configuración en ejecución.

Definición de la Autenticación de host y sesión

En la página Autenticación de host y sesión, se puede definir el modo en que 802.1X funciona en el puerto y la acción que debe realizarse en caso de que se haya detectado un incumplimiento.

Consulte **Modos de host del puerto** para obtener una explicación de estos modos.

Para definir la configuración avanzada de 802.1X para los puertos:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Autenticación de host y sesión**.

Los parámetros de autenticación 802.1X se describen para todos los puertos. Todos los campos a excepción de los siguientes están descritos en la página **Editar**.

- **Número de incumplimientos**: se muestra el número de paquetes que llegan a la interfaz en modo de host único, de un host cuya dirección MAC no es la dirección MAC del solicitante.

PASO 2 Seleccione un puerto y haga clic en **Editar**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: ingrese un número de puerto para el que la autenticación del host esté activada.
- **Autenticación de host**: seleccione uno de los modos. Estos modos se describen más arriba en **Modos de host del puerto**.

Configuración de incumplimiento de host único (solo se muestra si la autenticación del host es Host único):

- **Acción en incumplimiento**: seleccione la acción que se aplicará a los paquetes que lleguen en el modo Sesión única/Host único, de un host cuya dirección MAC no sea la dirección MAC del solicitante. Las opciones son:
  - *Proteger (Descartar)*: se descartan los paquetes.
  - *Restringir (Reenviar)*: se reenvían los paquetes.

  - *Cerrar*: se descartan los paquetes y se cierra el puerto. Los puertos permanecen cerrados hasta que se los reactive o hasta que se reinicie el dispositivo.

- **Trampas**: seleccione esta opción para activar las trampas.
- **Frecuencia de trampas**: se define la frecuencia con la que se envían trampas al host. Este campo puede definirse solo si varios hosts están desactivados.

PASO 4 Haga clic en **Aplicar**. La configuración se escribe en el archivo Configuración en ejecución.

Visualización de hosts autenticados

Para ver detalles sobre usuarios autenticados:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Hosts autenticados**.

Esta página muestra los siguientes campos:

- **Nombre de usuario**: los nombres de los solicitantes que se autenticaron en cada puerto.
- **Puerto**: número del puerto.
- **Tiempo de sesión (DD:HH:MM:SS)**: cantidad de tiempo que el solicitante estuvo conectado en el puerto.
- **Método de autenticación**: método mediante el que se autenticó la última sesión.
- **Servidor de autenticación**: servidor RADIUS.
- **Dirección MAC**: se muestra la dirección MAC del solicitante.
- **ID de VLAN**: la VLAN del puerto.

Clientes bloqueados

Para ver los clientes que se bloquearon por intentos de inicio de sesión fallidos y para desbloquear a un cliente bloqueado:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Cliente bloqueado**.

Se muestran los siguientes campos:

- **Interfaz**: el puerto que está bloqueado.
- **Dirección MAC**: se muestra el estado de autorización del puerto actual. Si el estado es *Autorizado*, el puerto se autentica o *Control de puerto administrativo* está en *Fuerza autorizada*. Por el contrario, si el estado es *No autorizado*, entonces el puerto no se autentica o *Control de puerto administrativo* está en *Fuerza no autorizada*.
- **Tiempo restante (seg.)**: el tiempo que resta para que el puerto se bloquee.

PASO 2 Seleccione un puerto.

PASO 3 Haga clic en **Desbloquear**.

Personalización de la autenticación web

Esta página permite designar en varios idiomas las páginas de autenticación basada en web.

Se pueden agregar hasta 4 idiomas.

NOTA Hasta 5 usuarios HTTP y un usuario HTTPS puede solicitar la autenticación basada en web al mismo tiempo. Cuando estos usuarios están autenticados, más usuarios pueden solicitar la autenticación.

Para agregar un idioma para la autenticación basada en web:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Personalización de la autenticación web**.

PASO 2 Haga clic en **Add**.

PASO 3 Seleccione un idioma de la lista desplegable **Idioma**.

PASO 4 Seleccione **Configurar como idioma de visualización predeterm.** si este idioma es el predeterminado. Las páginas de idioma predeterminado se muestran si el usuario final no selecciona un idioma.

PASO 5 Haga clic en **Aplicar** para guardar la configuración en el archivo Configuración en ejecución.

Para personalizar las páginas de autenticación web:

PASO 1 Haga clic en **Seguridad** > **Autenticación 802.1X/MAC/Web** > **Personalización de la autenticación web.**

Esta página muestra los idiomas que pueden personalizarse.

PASO 2 Haga clic en **Editar pág. de inicio de sesión**.

PASO 3 Haga clic en **Edit1**. Se muestran los siguientes campos:

- **Idioma**: muestra el idioma de la página.
- **Esquema de colores**: seleccione una de las opciones de contraste.

  Si se selecciona el esquema de colores **Personalizado**, están disponibles las siguientes opciones:

  - *Color de fondo de la página*: ingrese el código ASCII del color de fondo. El color seleccionado se muestra en el campo Texto.
  - *Color de fondo del encabezado y pie de página*: ingrese el código ASCII del color de fondo del encabezado y pie de página. El color seleccionado se muestra en el campo Texto.
  - *Color de texto del encabezado y pie de página*: ingrese el código ASCII del color de texto del encabezado y pie de página. El color seleccionado se muestra en el campo Texto.
  - *Color del hipervínculo*: ingrese el código ASCII del color del hipervínculo. El color seleccionado se muestra en el campo Texto.
- **Imagen del logotipo actual**: Seleccione una de las siguientes opciones:
  - *Ninguna*: sin logotipo.
  - *Predeterminado*: use el logotipo predeterminado.
  - *Otro*: seleccione para ingresar un logotipo personalizado.

  Si se selecciona la opción de logotipo **Otro**, están disponibles las siguientes opciones:

  - *Nomb. de archivo de imagen de logotipo*: ingrese el nombre de archivo del logotipo o **Navegue** hasta la imagen.
  - *Texto de la aplicación*: introduzca el texto que acompañará el logotipo.
  - *Texto del título de la ventana*: introduzca un título para la página de inicio de sesión.

PASO 4 Haga clic en **Aplicar** para guardar la configuración en el archivo Configuración en ejecución.

PASO 5 Haga clic en **Edit2**. Se muestran los siguientes campos:

- **Credenciales de usuario no válidas**: introduzca el texto del mensaje que aparecerá cuando el usuario final ingrese un nombre de usuario o contraseña no válidos.
- **Servicio no disponible**: introduzca el texto del mensaje que aparecerá cuando el servicio de autenticación no esté disponible.

PASO 6 Haga clic en **Aplicar** para guardar la configuración en el archivo Configuración en ejecución.

PASO 7 Haga clic en **Edit3**. Se muestran los siguientes campos:

- **Mensaje de bienvenida**: introduzca el texto del mensaje que aparecerá cuando el usuario final inicie sesión.
- **Mensaje instructivo**: introduzca las instrucciones que se mostrarán al usuario final.
- **Autenticación RADIUS**: muestra si la autenticación RADIUS está habilitada. De ser así, el nombre de usuario y la contraseña deben incluirse en la página de inicio de sesión.
- **Cuad. de texto del nomb. usuario**: seleccione el cuadro de texto del nombre de usuario que se mostrará.
- **Etiq. cuad. de texto del nombre usuario**: seleccione la etiqueta que se mostrará antes del cuadro de texto del nombre de usuario.
- **Cuad. de texto de contraseña**: seleccione el cuadro de texto de contraseña que se mostrará.
- **Etiq. cuad. de texto de contraseña**: seleccione la etiqueta que se mostrará antes del cuadro de texto de contraseña.
- **Selección de idioma**: seleccione para permitirle al usuario escoger un idioma.
- **Etiqueta desplegable de idioma**: ingrese la etiqueta de la lista desplegable de selección de idiomas.
- **Etiq. del botón de inicio de sesión**: ingrese la etiqueta del botón de inicio de sesión.
- **Etiq. del progreso del inicio de sesión**: ingrese el texto que aparecerá durante el proceso de inicio de sesión.

PASO 8 Haga clic en **Aplicar** para guardar la configuración en el archivo Configuración en ejecución.

PASO 9 Haga clic en **Edit4**. Se muestran los siguientes campos:

- **Términos y condiciones**: seleccione para habilitar un cuadro de texto de términos y condiciones.
- **Advertencia de los términos y condiciones**: ingrese el texto del mensaje que aparecerá como instrucciones para introducir los términos y condiciones.
- **Contenido de los términos y condiciones**: ingrese el texto del mensaje que aparecerá como términos y condiciones.

PASO 10 Haga clic en **Aplicar** para guardar la configuración en el archivo Configuración en ejecución.

PASO 11 **Edit5**. Se muestran los siguientes campos:

- **Copyright**: seleccione para habilitar la visualización del texto de copyright.
- **Texto de copyright**: introduzca el texto de copyright.

PASO 12 Haga clic en **Aplicar** para guardar la configuración en el archivo Configuración en ejecución.

PASO 13 Haga clic en **Editar página de éxito**.

PASO 14 Haga clic en el botón **Edit** en el lado derecho de la página.

PASO 15 Introduzca el **Mensaje de éxito**, que es el texto que se visualizará si el usuario final inicia sesión correctamente.

PASO 16 Haga clic en **Aplicar** para guardar la configuración en el archivo Configuración en ejecución.

Para obtener una vista previa del mensaje de inicio de sesión o éxito, haga clic en **Vista preliminar**.

Para configurar el idioma predeterminado de la interfaz GUI como el idioma predeterminado para la autenticación basada en web, haga clic en **Configurar idioma de visualización predeterminado**.

Definición de intervalos de tiempo

Consulte **Intervalo de tiempo** para obtener una explicación de esta función.

Compatibilidad de modo de puerto y método de autenticación

La siguiente tabla muestra las combinaciones de método de autenticación y modo de puerto compatibles.

Métodos de autenticación y modos de puerto

Método de autenticación	Host único	Host múltiple	Sesión múltiple	
			Dispositivo en Capa 3	Dispositivo en Capa 2
802.1x	†	†	†	†
MAC	†	†	†	†
WEB	N/D	N/D	N/D	†

Leyenda:

†: el modo de puerto también admite la VLAN invitada y la asignación RADIUS VLAN.

N/D: el método de autenticación no admite el modo de puerto.

NOTA La autenticación basada en la web requiere compatibilidad TCAM para clasificar el tráfico de entrada y solo es compatible con el modo de sesión múltiple. Es posible simular el modo de host único al establecer el parámetro de hosts máximos en 1 en la página Autenticación de puertos.

Comportamiento del modo

La siguiente tabla describe cómo se controla el tráfico autenticado y no autenticado en diversas situaciones.

	Tráfico no autenticado				Tráfico autenticado			
	Con VLAN invitada		Sin VLAN invitada		Con RADIUS de VLAN		Sin RADIUS de VLAN	
	Sin etiquetar	Etiquetado	Sin etiquetar	Etiquetado	Sin etiquetar	Etiquetado	Sin etiquetar	Etiquetado
Host único	Las tramas se reasignan a la VLAN invitada.	Las tramas se descartan a menos que pertenezcan a la VLAN invitada o a las VLAN no autenticadas.	Las tramas se descartan.	Las tramas se descartan a menos que pertenezcan a las VLAN no autenticadas.	Las tramas se reasignan a la VLAN con asignación de RADIUS.	Las tramas se descartan a menos que pertenezcan a RADIUS de VLAN o a las VLAN no autenticadas.	Las tramas se interligan en base a la configuración de VLAN estática.	Las tramas se interligan en base a la configuración de VLAN estática.
Host múltiple	Las tramas se reasignan a la VLAN invitada.	Las tramas se descartan a menos que pertenezcan a la VLAN invitada o a las VLAN no autenticadas.	Las tramas se descartan.	Las tramas se descartan a menos que pertenezcan a las VLAN no autenticadas.	Las tramas se reasignan a la VLAN con asignación de Radius.	Las tramas se descartan a menos que pertenezcan a Radius de VLAN o a las VLAN no autenticadas.	Las tramas se interligan en base a la configuración de VLAN estática.	Las tramas se interligan en base a la configuración de VLAN estática.

	Tráfico no autenticado				Tráfico autenticado			
	Con VLAN invitada		Sin VLAN invitada		Con RADIUS de VLAN		Sin RADIUS de VLAN	
	Sin etiquetar	Etiquetado	Sin etiquetar	Etiquetado	Sin etiquetar	Etiquetado	Sin etiquetar	Etiquetado
Sesión múltiple Lite	N/D	N/D	Las tramas se descartan.	Las tramas se descartan a menos que pertenezcan a las VLAN no autenticadas.	N/D	N/D	Las tramas se interligan en base a la configuración de VLAN estática.	Las tramas se interligan en base a la configuración de VLAN estática.
Sesión múltiple completa	Las tramas se reasignan a la VLAN invitada.	Las tramas se reasignan a la VLAN invitada a menos que pertenezcan a las VLAN no autenticadas.	Las tramas se descartan.	Las tramas se descartan a menos que pertenezcan a las VLAN no autenticadas.	Las tramas se reasignan a la VLAN con asignación de RADIUS.	Las tramas se reasignan a Radius de VLAN invitada a menos que pertenezcan a las VLAN no autenticadas.	Las tramas se interligan en base a la configuración de VLAN estática.	Las tramas se interligan en base a la configuración de VLAN estática.

21

Seguridad: Seguridad del primer salto de IPv6

Esta sección describe el funcionamiento de la seguridad del primer salto (FHS) de IPv6 y su configuración en la interfaz de usuario gráfica (GUI).

Abarca los siguientes temas:

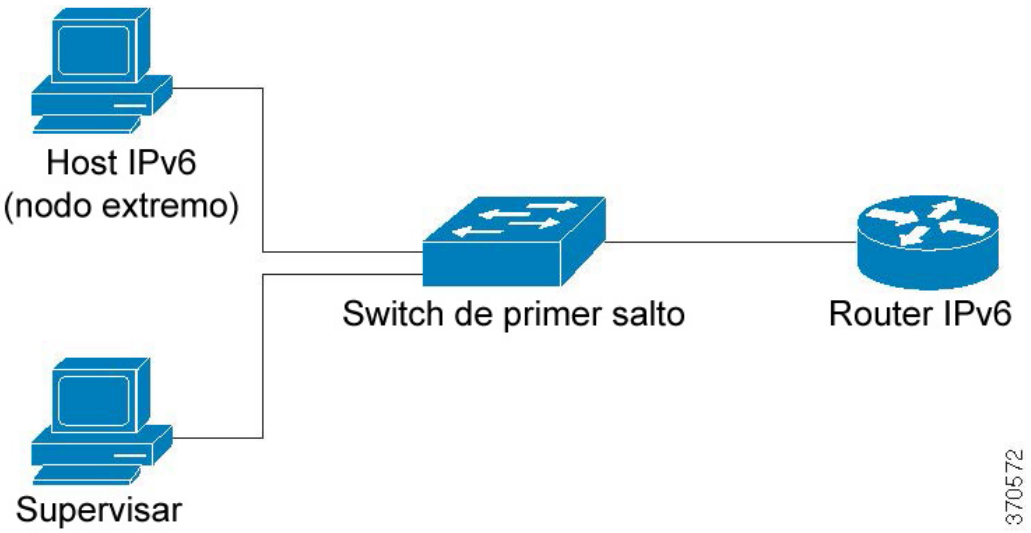
- **Información general sobre la seguridad del primer salto de IPv6**
- **Protección del anuncio del router**
- **Inspección de detección de vecinos**
- **Protección de DHCPv6**
- **Integridad de vinculación de vecinos**
- **Protección de origen IPv6**
- **Protección contra ataques**
- **Políticas, parámetros globales y valores predeterminados del sistema**
- **Tareas comunes**
- **Configuración y valores predeterminados**
- **Configuración y valores predeterminados**
- **Configuración de la seguridad del primer salto de IPv6 mediante la GUI web**

Información general sobre la seguridad del primer salto de IPv6

La FHS de IPv6 es una serie de funciones diseñadas para proteger las operaciones de enlace en cualquier red habilitada para IPv6. Está basada en el protocolo de detección de vecinos y los mensajes DHCPv6.

En esta función, un switch de capa 2 (como se muestra en la **Figura 6**) filtra los mensajes del protocolo de detección de vecinos, los mensajes DHCPv6 y los mensajes de datos del usuario conforme a ciertas reglas.

Figura 6 Configuración de la seguridad del primer salto de IPv6



Una instancia independiente y separada de la seguridad del primer salto de IPv6 se ejecuta en cada VLAN en la que la función está habilitada.

Abreviaturas

Nombre	Descripción
Mensaje de CPA	Mensaje de anuncio de ruta de certificación
Mensaje de CPS	Mensaje de solicitud de ruta de certificación
Mensaje de DAD-NS	Mensaje de solicitud de vecinos de detección de direcciones duplicadas
FCFS-SAVI	Mejora de validación de la dirección de origen - Por orden de llegada
Mensaje de NA	Mensaje de anuncio de vecinos
NDP	Protocolo de detección de vecinos
Mensaje de NS	Mensaje de solicitud de vecinos
Mensaje de RA	Mensaje de anuncio del router
Mensaje de RS	Mensaje de solicitud del router
SAVI	Mejora de validación de la dirección de origen

Componentes de la seguridad del primer salto de IPV6

La seguridad del primer salto de IPv6 incluye las siguientes funciones:

- Seguridad común del primer salto de IPV6.
- Protección de RA
- Inspección de ND
- Integridad de vinculación de vecinos
- Protección de DHCPv6
- Protección de origen IPv6

Estos componentes pueden habilitarse o deshabilitarse en las VLAN.

Hay dos políticas vacías predefinidas por cada función con los siguientes nombres: vlan_default y port_default. La primera se adjunta a cada VLAN no adherida a una política definida por el usuario y la segunda se conecta a cada interfaz y VLAN no adherida a una política definida por el usuario. El usuario no puede adjuntar explícitamente estas políticas. Consulte **Políticas, parámetros globales y valores predeterminados del sistema**.

Conducto de seguridad del primer salto de IPV6

Si se habilita la seguridad del primer salto de IPv6 en una VLAN, el switch captura los siguientes mensajes:

- Mensajes de anuncio del router (RA).
- Mensajes de solicitud del router (RS).
- Mensajes de anuncio de vecinos (NA).
- Mensajes de solicitud de vecinos (NS).
- Mensajes de redirección ICMPv6.
- Mensajes de anuncio de ruta de certificación (CPA).
- Mensajes de solicitud de ruta de certificación (CPS).
- Mensajes DHCPv6.

Los mensajes de RA, CPA y redirección ICMPv6 capturados se pasan a la función de protección de RA. La protección de RA valida estos mensajes, elimina los mensajes ilegales y pasa los mensajes legales a la función de inspección de ND.

La inspección de RA valida estos mensajes, elimina los mensajes ilegales y pasa los mensajes legales a la función de protección de IPv6 de origen.

Los mensajes DHCPv6 capturados se pasan a la función de protección de DHCPv6. La protección de DHCPv6 valida estos mensajes, elimina los mensajes ilegales y pasa los mensajes legales a la función de protección de IPv6 de origen.

Los mensajes de datos capturados se pasan a la función de protección de IPv6 de origen. La protección de IPv6 de origen valida los mensajes recibidos (mensajes DHCPv6 de la protección de DHCPv6, mensajes de NDP de la inspección de ND y mensajes de datos capturados) con la tabla de vinculación de vecinos, elimina los mensajes ilegales y pasa los mensajes legales al desvío.

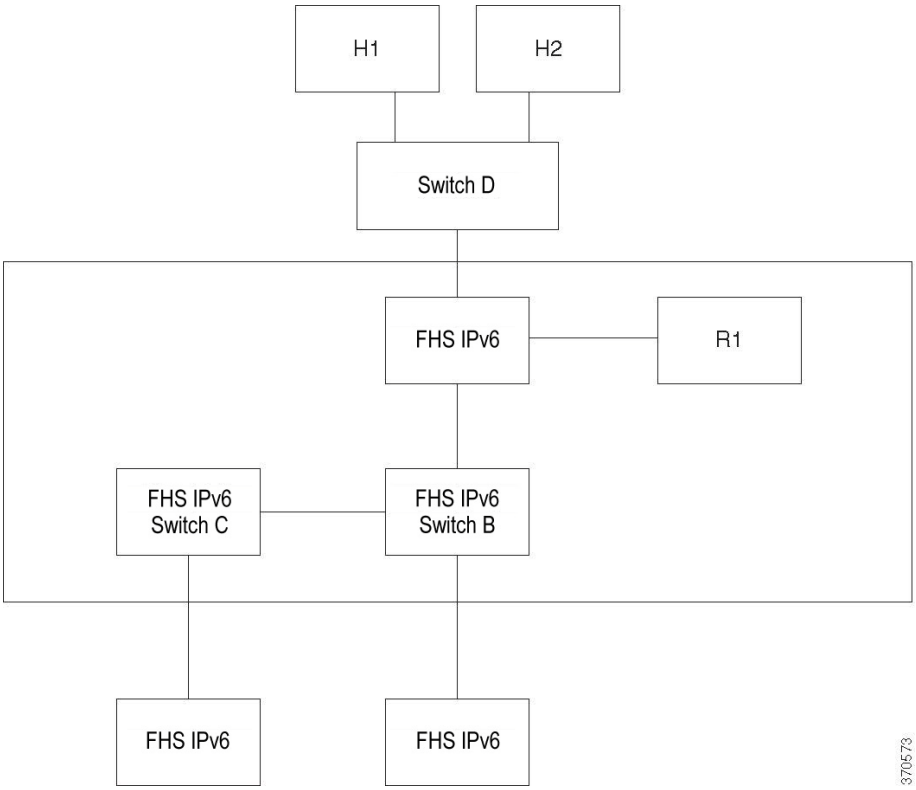
La integridad de vinculación de vecinos detecta los vecinos de los mensajes recibidos (mensajes de NDP y DHCPv6) y los almacena en la tabla de vinculación de vecinos. Además, se pueden agregar entradas estáticas de forma manual. Después de detectar las direcciones, la función NBI pasa las tramas al desvío.

Los mensajes de RS, CPS NS y NA capturados también se pasan a la función de inspección de ND. La inspección de ND valida estos mensajes, elimina los mensajes ilegales y pasa los mensajes legales a la función de protección de IPv6 de origen.

Perímetro de seguridad del primer salto de IPv6

Los switches de la seguridad del primer salto de IPv6 pueden formar un perímetro que separa las áreas no confiables de las áreas confiables. Todos los switches dentro del perímetro admiten la seguridad del primer salto de IPv6; los hosts y los routers dentro del perímetro son dispositivos confiables. Por ejemplo, en la **Figura 7**, Switch B y Switch C son vínculos internos dentro del área protegida.

Figura 7 Perímetro de seguridad del primer salto de IPv6



El comando **device-role** de la pantalla de configuración de la política de vinculación de vecinos especifica el perímetro.

Cada switch de la seguridad del primer salto de IPv6 establece la vinculación de los vecinos particionada por el perímetro. De esta manera, las entradas de vinculación se distribuyen en los dispositivos de seguridad del primer salto de IPv6 formando un perímetro. Los dispositivos de seguridad del primer salto de IPv6 luego brindan integridad de vinculación al interior del perímetro sin configurar las vinculaciones de cada dirección en cada dispositivo.

Protección del anuncio del router

La protección del anuncio del router (RA) es la primera función de la FHS que trata los mensajes de RA. La protección de RA admite las siguientes funciones:

- Filtrado de mensajes de RA, CPA y redirección ICMPv6 recibidos.
- Validación de mensajes de RA recibidos.

Filtrado de mensajes de RA, CPA y redirección IPCMv6 recibidos

La protección de RA descarta los mensajes de RA y CPA recibidos en las interfaces cuya función no es de enrutamiento. La función de la interfaz se configura en la página de configuración de la protección de RA de la > seguridad del primer salto de IPv6 > de seguridad.

Validación de mensajes de RA

La protección de RA valida los mensajes de RA mediante el filtrado en función de la política de protección de RA adjunta a la interfaz. Estas políticas pueden configurarse en la página de configuración de la protección de RA.

Si un mensaje no pasa la verificación, se elimina. Si se habilita la configuración de eliminación del paquete de registro en el componente común de la FHS, se envía un mensaje de SYSLOG de velocidad limitada.

Inspección de detección de vecinos

La inspección de detección de vecinos (ND) admite las siguientes funciones:

- Validación de mensajes de protocolo de detección de vecinos recibidos.
- Filtrado de egreso.

Validación de mensajes

La inspección de ND valida los mensajes de protocolo de detección de vecinos en función de la política de inspección de ND adjunta a la interfaz. Esta política puede definirse en la página de configuración de la inspección de ND.

Si un mensaje no pasa la verificación definida en la política, se elimina y se envía un mensaje de SYSLOG de velocidad limitada.

Filtrado de egreso

La inspección de ND bloquea el desvío de los mensajes de RS y CPS en las interfaces configuradas como interfaz de host.

Protección de DHCPv6

La protección de DHCPv6 trata los mensajes DHCPv6 capturados. La protección de DHCPv6 admite las siguientes funciones:

- Filtrado de mensajes DHCPv6 recibidos.

  La protección de DHCP descarta los mensajes de respuesta de DHCPv6 recibidos en las interfaces cuya función es la de cliente. La función de la interfaz se configura en la página de configuración de la protección de DHCP.

- Validación de mensajes DHCPv6 recibidos.

  La protección de DHCPv6 valida los mensajes DHCPv6 que coinciden con el filtrado en función de la política de protección de DHCPv6 adjunta a la interfaz.

Si un mensaje no pasa la verificación, se elimina. Si se habilita la configuración de eliminación del paquete de registro en el componente común de la FHS, se envía un mensaje de SYSLOG de velocidad limitada.

Integridad de vinculación de vecinos

La integridad de vinculación de vecinos (NB) establece la vinculación de vecinos.

Una instancia independiente y separada de la integridad de NB se ejecuta en cada VLAN en la que la función está habilitada.

Detección de prefijos IPv6 anunciados

La integridad de NB detecta los prefijos IPv6 anunciados en los mensajes de RA y los guarda en la tabla de prefijos de vecino. Los prefijos se utilizan para verificar las direcciones IPv6 globales asignadas.

Esta validación está desactivada de forma predeterminada. Cuando está habilitada, las direcciones se validan en función de los prefijos en la página de configuración de la vinculación de vecinos.

Los prefijos estáticos utilizados para la validación de las direcciones pueden agregarse en la página de la tabla de prefijos de vecinos.

Validación de direcciones IPv6 globales

La integridad de NB lleva a cabo las siguientes validaciones:

- Si la dirección de destino de un mensaje de NS o NA es una dirección IPv6 global, debe pertenecer a uno de los prefijos definidos en la tabla de prefijos de RA.
- La dirección IPv6 global provista por el servidor DHCPv6 debe pertenecer a uno de los prefijos definidos en la lista de prefijos IPv6 (en la página de la lista de prefijos IPv6 > en la configuración de IP).

Si un mensaje no pasa esta verificación, se elimina y se envía un mensaje de SYSLOG de velocidad limitada.

Desbordamiento de la tabla de vinculación de vecinos

Si no hay espacio libre para crear una nueva entrada, no se crea ninguna entrada y se envía un mensaje SYSLOG.

Establecimiento de la vinculación de vecinos

El switch de la seguridad del primer salto de IPv6 detecta y registra la información de vinculación a través de los siguientes métodos:

- **Método NBI-NDP**: detección de direcciones IPv6 de los mensajes del protocolo de detección de vecinos indagados.
- **Método NBI-DHCP**: detección de direcciones IPv6 de los mensajes DHCPv6 indagados.
- **Método NBI-Manual:** configuración manual.

La dirección IPv6 está vinculada a una propiedad de capa de enlace de la conexión de red del host. Esta propiedad, llamada "anclaje", consta de un identificador de interfaz (ifIndex) al que se conecta el host y la dirección MAC del host.

El switch de la seguridad del primer salto de IPv6 establece la vinculación solo en las interfaces perimetrales (consulte **Perímetro de seguridad del primer salto de IPv6**).

La información de vinculación se guarda en la tabla de vinculación de vecinos.

Método NBI-NDP

El método NBI-NDP utilizado se basa en el método FCFS-SAVI especificado en RFC6620 con las siguientes diferencias:

- A diferencia de FCFS-SAVI, que admite solo la vinculación de las direcciones IPv6 de enlace local, NBI-NDP además admite la vinculación de las direcciones IPv6 globales.

- NBI-NDP admite la vinculación de la dirección IPv6 solo para las direcciones IPv6 detectadas en los mensajes de NDP. La validación de la dirección de origen para los mensajes de datos se proporciona mediante la protección de la dirección IPv6 de origen.
- En NBI-NDP, la prueba de propiedad de la dirección se basa en el principio de orden de llegada. El primer host que reclama una dirección de origen determinada es el propietario de dicha dirección hasta nuevo aviso. Dado que no se acepta la modificación de los hosts, debe encontrarse la forma de confirmar la propiedad de la dirección sin la necesidad de un nuevo protocolo. Por este motivo, siempre que se detecta primero una dirección IPv6 de un mensaje de NDP, el switch vincula la dirección con la interfaz. Los mensajes de NDP subsecuentes que contienen esta dirección IPV6 pueden compararse con el mismo anclaje para confirmar que el originador posee la dirección IP de origen.

  La excepción a esta regla se da cuando un host IPv6 se traspasa al dominio L2 o cambia su dirección MAC. En este caso, el host sigue siendo el propietario de la dirección IP, pero es posible que cambie el anclaje asociado. Para abordar este caso, el comportamiento NBI-NDP definido implica verificar si el host aún se puede alcanzar enviando mensajes de DAD-NS a la interfaz de vinculación anterior. Si el host ya no es alcanzable en el anclaje registrado con anterioridad, NBI-NDP asume que el anclaje nuevo es válido y lo modifica. Si el host aún es alcanzable con el anclaje registrado anteriormente, la interfaz de vinculación no se modifica.

Para reducir el tamaño de la tabla de vinculación de vecinos, NBI-NDP establece la vinculación solo en las interfaces perimetrales (consulte **Perímetro de seguridad del primer salto de IPv6**) y distribuye la información de vinculación mediante las interfaces internas con los mensajes de NS y NA. Antes de crear una vinculación NBI-NDP local, el dispositivo envía un mensaje de DAD-NS consultando la dirección implicada. Si un host responde a dicho mensaje con un mensaje de NA, el dispositivo que envió el mensaje de DAD-NS infiere que la vinculación de esa dirección existe en otro dispositivo y no crea una vinculación local. Si no se recibe ningún mensaje de NA como respuesta al mensaje de DAD-NS, el dispositivo local infiere que no existe ninguna vinculación para dicha dirección en otros dispositivos y crea una vinculación local para esa dirección.

NBI-NDP admite el temporizador de vida útil. Los valores del temporizador se configuran en la página de configuración de la vinculación de vecinos. El temporizador se reinicia cada vez que se confirma la dirección IPv6 vinculada. Si el temporizador expira, el dispositivo envía hasta 2 mensajes de DAD-NS en intervalos cortos para validar el vecino.

Método NBI-DHCP

El método NBI-NDP se basa en el método SAVI-DHCP especificado en la solución SAVI para DHCP, draft-ietf-savi-dhcp-15, 11 de septiembre de 2012.

Al igual que NBI-NDP, NBI-DHCP permite la vinculación perimetral de la escalabilidad. Existe la siguiente diferencia entre los métodos NBI-DHCP y NBI-FCFS: NBI-DHCP sigue el estado indicado en los mensajes DHCPv6, por lo que no es necesario distribuir el estado en los mensajes de NS/NA.

Política de integridad de NB

De la misma manera en que funcionan las demás características de la seguridad del primer salto de IPv6, la política de integridad de NB adjunta a la interfaz especifica el comportamiento de la integridad de NB en la interfaz. Estas políticas se configuran en la página de configuración de la vinculación de vecinos.

Protección de origen IPv6

Si está activada la integridad de vinculación de vecinos (integridad de NB), la protección de IPv6 de origen valida las direcciones IPv6 de origen de los mensajes NDP y DHCPv6 independientemente de si está activada o no la protección de IPv6 de origen. Si está activada la protección de IPv6 de origen junto con la integridad de NB, la protección de IPv6 de origen configura la TCAM para que indique cuáles son las tramas de datos IPv6 que deben reenviarse, descartarse o capturarse en la CPU, y valida las direcciones IPv6 de origen de los mensajes de datos IPv6 capturados. Si no está activada la integridad de NB, la protección de IPv6 de origen no se activa independientemente de si está o no habilitada.

Si la TCAM no tiene espacio libre para agregar una nueva regla, el contador de desbordamiento de la TCAM se incrementa y se envía un mensaje SYSLOG con límite de velocidad que contiene el identificador de la interfaz, la dirección MAC del host y la dirección IPv6 del host.

La protección de IPv6 de origen valida las direcciones de origen de todos los mensajes IPv6 recibidos mediante la tabla de vinculación de vecinos, a excepción de los siguientes mensajes que acceden sin validación:

- Mensajes de RS: si la dirección IPv6 de origen es igual a la dirección IPv6 no especificada.
- Mensajes de NS: si la dirección IPv6 de origen es igual a la dirección IPv6 no especificada.
- Mensajes de NA: si la dirección IPv6 de origen es igual a la dirección de destino.

La protección de IPv6 de origen descarta todos los otros mensajes IPv6 cuya dirección IPv6 de origen sea igual a la dirección IPv6 no especificada.

La protección de IPv6 de origen se ejecuta únicamente en las interfaces no fiables que pertenecen al perímetro.

La protección de IPv6 de origen descarta un mensaje IPv6 de entrada en los siguientes casos:

- Si la tabla de vinculación de vecinos no contiene la dirección IPv6.
- Si la tabla de vinculación de vecinos contiene la dirección IPv6, pero está vinculada a otra interfaz.

Si la protección de IPv6 de origen inicia el proceso de recuperación de vecino mediante el envío de mensajes DAD_NS a las direcciones IPv6 de origen desconocidas.

Protección contra ataques

Esta sección describe la protección contra ataques provista por la seguridad del primer salto de IPv6

Protección contra la suplantación del router IPv6

El host IPv6 puede utilizar el mensaje de RA recibido para:

- Detectar el router IPv6.
- Configurar la dirección sin estado.

Un host malintencionado puede enviar mensajes de RA que se autoanuncian como router IPv6 y proporcionar prefijos falsificados para la configuración de la dirección sin estado.

La protección de RA brinda protección contra dichos ataques mediante la configuración de la función de la interfaz como interfaz de host para todas las interfaces donde no se pueden conectar los routers IPv6.

Protección contra la suplantación de la resolución de direcciones IPv6

Un host malintencionado puede enviar mensajes de NA que se autoanuncian como host IPv6 con la dirección IPv6 proporcionada.

La integridad de NB brinda protección contra dichos ataques de las siguientes maneras:

- Si la dirección IPv6 proporcionada es desconocida, el mensaje de solicitud de vecinos (NS) se desvía solo en las interfaces internas.
- Si la dirección IPv6 proporcionada es conocida, el mensaje de NS se desvía solo en la interfaz a la que está vinculada la dirección IPv6.
- El mensaje de anuncio de vecinos (NA) se elimina si la dirección IPv6 de destino está vinculada a otra interfaz.

Protección contra la suplantación de la detección de duplicación de las direcciones IPv6

El host IPv6 debe llevar a cabo la detección de duplicación de las direcciones en cada dirección asignada a IPv6 mediante el envío de un mensaje de NS especial (mensaje de solicitud de vecinos de detección de duplicación de las direcciones [DAD_NS]).

Un host malintencionado puede responder un mensaje de DAD_NS que se autoanuncia como host IPv6 con la dirección IPv6 proporcionada.

La integridad de NB brinda protección contra dichos ataques de las siguientes maneras:

- Si la dirección IPv6 proporcionada es desconocida, el mensaje de DAD_NS se desvía solo en las interfaces internas.
- Si la dirección IPv6 proporcionada es conocida, el mensaje de DAD_NS se desvía solo en la interfaz donde está vinculada la dirección IPv6.
- El mensaje de NA se elimina si la dirección IPv6 de destino está vinculada a otra interfaz.

Protección contra la suplantación del servidor DHCPv6

El host IPv6 puede utilizar el protocolo DHCPv6 para:

- Configurar la información sin estado.
- Configurar las direcciones con estado.

Un host malintencionado puede enviar mensajes de respuesta de DHCPv6 que se autoanuncian como servidor DHCPv6 y proporcionan direcciones IPv6 e información sin estado falsificadas. La protección de DHCPv6 brinda protección contra dichos ataques mediante la configuración de la función de la interfaz como puerto de cliente para todos los puertos a los que no se pueden conectar los servidores DHCPv6.

Protección contra la suplantación de la caché de NBD

El router IPv6 admite la caché del protocolo de detección de vecinos (NDP) que asigna la dirección IPv6 a la dirección MAC para el último enrutamiento de salto.

Un host malintencionado puede enviar mensajes IPv6 con una dirección IPv6 diferente para el último desvío del salto, lo que ocasiona un desbordamiento de la caché de NBD.

Un mecanismo integrado a la implementación de NDP, que limita la cantidad de entradas permitidas en el estado INCOMPLETO de la caché de detección de vecinos. Brinda protección contra los piratas informáticos que intentan realizar envíos masivos a la tabla.

Políticas, parámetros globales y valores predeterminados del sistema

Cada función de la FHS puede activarse o desactivarse individualmente. No hay ninguna función activada de forma predeterminada.

Las funciones deben activarse inicialmente en las VLAN específicas. Cuando activa la función, también puede definir los valores de configuración local para las reglas de verificación de dicha función. Si no define la política que contiene los diferentes valores de las reglas de verificación, los valores globales se utilizan para aplicar la función a los paquetes.

Políticas

Las políticas contienen las reglas de verificación que se aplican en los paquetes de entrada. Pueden adjuntarse a las VLAN y también a los puertos y los LAG. Si la función no está activada en la VLAN, las políticas no surten efecto.

Las políticas pueden ser políticas predeterminadas o definidas por el usuario (consulte a continuación).

Políticas predeterminadas

Existen políticas predeterminadas vacías para cada función de la FHS y se adjuntan de manera predeterminada a todas las VLAN e interfaces. Los nombres de las políticas predeterminadas son: "vlan_default" y "port_default" (para cada función):

- Se pueden agregar reglas a estas políticas predeterminadas. Usted no puede adjuntar manualmente las políticas predeterminadas a las interfaces. Se adjuntan de manera predeterminada.
- Las políticas predeterminadas nunca pueden eliminarse. Usted solo puede eliminar la configuración agregada por el usuario.

Políticas definidas por el usuario

Puede definir otras políticas aparte de las políticas predeterminadas.

Cuando se adjunta una política definida por el usuario a una interfaz, se separa la política predeterminada para dicha interfaz. Si se separa la política definida por el usuario de la interfaz, se vuelve a adjuntar la política predeterminada.

Las políticas no entran en vigencia hasta que:

- La función de la política se activa en la VLAN que contiene la interfaz.
- La política se adjunta a la interfaz (VLAN, puerto o LAG).

Cuando adjunta una política, la política predeterminada para dicha interfaz se separa. Cuando quita la política de la interfaz, la política predeterminada se vuelve a adjuntar.

Usted solo puede adjuntar 1 política (para una función específica) a una VLAN.

Puede adjuntar varias políticas (para una función específica) a una interfaz si las políticas especifican las diferentes VLAN.

Niveles de las reglas de verificación

El conjunto final de reglas que se aplica a un paquete de entrada en una interfaz se construye de la siguiente manera:

- Las reglas configuradas en las políticas adjuntas a la interfaz (puerto o LAG) a la que arribó el paquete se añaden al conjunto.
- Las reglas configuradas en la política adjunta a la VLAN se añaden al conjunto si no se han añadido a nivel del puerto.
- Las reglas globales se añaden al conjunto si no se han agregado a nivel del puerto o la VLAN.

Las reglas definidas a nivel del puerto anulan las reglas establecidas a nivel de la VLAN. Las reglas definidas a nivel de la VLAN anulan las reglas configuradas globalmente. Las reglas configuradas globalmente anulas los valores predeterminados del sistema.

Tareas comunes

Flujo de trabajo común de la seguridad del primer salto de IPv6

PASO 1 En la página de configuración de la FHS, ingrese la lista de VLAN en la que esta función está activada.

PASO 2 En la misma página, configure la función de registro de eliminación del paquete global.

PASO 3 Si es necesario, configure una política definida por el usuario o agregue reglas a las políticas predeterminadas para esta función.

PASO 4 Adjunte la política a la VLAN, el puerto o el LAG a través de las páginas de adjunción de políticas (VLAN) o adjunción de políticas (puerto).

Flujo de trabajo de la protección del anuncio del router

PASO 1 En la página de configuración de la protección de RA, ingrese la lista de VLAN en la que esta función está activada.

PASO 2 En la misma página, establezca los valores de la configuración global que se utilizan si no se configura ningún valor en la política.

PASO 3 Si es necesario, configure una política definida por el usuario o agregue reglas a las políticas predeterminadas para esta función.

PASO 4 Adjunte la política a la VLAN, el puerto o el LAG a través de las páginas de adjunción de políticas (VLAN) o adjunción de políticas (puerto).

Flujo de trabajo de la protección de DHCPv6

PASO 1 En la página de configuración de la protección de DHCPv6, ingrese la lista de VLAN en la que esta función está activada.

PASO 2 En la misma página, establezca los valores de la configuración global que se utilizan si no se configura ningún valor en la política.

PASO 3 Si es necesario, configure una política definida por el usuario o agregue reglas a las políticas predeterminadas para esta función.

PASO 4 Adjunte la política a la VLAN, el puerto o el LAG a través de las páginas de adjunción de políticas (VLAN) o adjunción de políticas (puerto).

Flujo de trabajo de la inspección de detección de vecinos

PASO 1 En la página de configuración de la inspección de ND, ingrese la lista de VLAN en la que esta función está activada.

PASO 2 En la misma página, establezca los valores de la configuración global que se utilizan si no se configura ningún valor en la política.

PASO 3 Si es necesario, configure una política definida por el usuario o agregue reglas a las políticas predeterminadas para esta función.

PASO 4 Adjunte la política a la VLAN, el puerto o el LAG a través de las páginas de adjunción de políticas (VLAN) o adjunción de políticas (puerto).

Flujo de trabajo de la vinculación de vecinos

PASO 1 En la página de configuración de la vinculación de vecinos, ingrese la lista de VLAN en la que esta función está activada.

PASO 2 En la misma página, establezca los valores de la configuración global que se utilizan si no se configura ningún valor en la política.

PASO 3 Si es necesario, configure una política definida por el usuario o agregue reglas a las políticas predeterminadas para esta función.

PASO 4 Agregue cualquier entrada manual requerida en la página de la tabla de vinculación de vecinos.

PASO 5 Adjunte la política a la VLAN, el puerto o el LAG a través de las páginas de adjunción de políticas (VLAN) o adjunción de políticas (puerto).

Flujo de trabajo de la protección de IPv6 de origen

PASO 1 En la página de configuración de la protección de IPv6 de origen, ingrese la lista de VLAN en la que esta función está activada.

PASO 2 Si es necesario, configure una política definida por el usuario o agregue reglas a las políticas predeterminadas para esta función.

PASO 3 Adjunte la política a la VLAN, el puerto o el LAG a través de las páginas de adjunción de políticas (VLAN) o adjunción de políticas (puerto).

Configuración y valores predeterminados

Si se habilita la seguridad del primer salto de IPv6 en una VLAN, el switch captura los siguientes mensajes de manera predeterminada:

- Mensajes de anuncio del router (RA).
- Mensajes de solicitud del router (RS).
- Mensajes de anuncio de vecinos (NA).
- Mensajes de solicitud de vecinos (NS).
- Mensajes de redirección ICMPv6.
- Mensajes de anuncio de ruta de certificación (CPA).
- Mensaje de solicitud de ruta de certificación (CPS).
- Mensajes DHCPv6.

Las funciones de la FHS están desactivadas de manera predeterminada.

Antes de comenzar

No se requieren tareas preliminares.

Configuración de la seguridad del primer salto de IPv6 mediante la GUI web

Configuración común de la FHS

Utilice la página de configuración de la FHS para activar la función común de la FHS en un grupo de VLAN especificado y establecer los valores de la configuración global para la eliminación de paquetes de registro. Si es necesario, se puede agregar una política o el registro de eliminación de paquetes a la política predeterminada definida por el sistema.

Para configurar los parámetros comunes de la seguridad del primer salto de IPv6:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Configuración de la FHS**.

Se muestran las políticas definidas actualmente.

PASO 2 Complete los siguientes campos de configuración global:

- **Lista de VLAN de la FHS**: ingrese una o más VLAN en las que la seguridad del primer salto de IPv6 esté habilitada.
- **Registro de eliminación de paquetes**: seleccione para crear un SYSLOG cuando elimine un paquete mediante una política de la seguridad del primer salto. Este es el valor global predeterminado si no se define ninguna política.

PASO 3 Haga clic en **Aplicar** para añadir configuraciones al archivo de configuración en ejecución.

PASO 4 Cree una política de FHS si es necesario haciendo clic en **Agregar**.

Ingrese los siguientes campos:

- **Nombre de la política**: ingrese el nombre de la política definida por el usuario.
- **Registro de eliminación de paquetes**: seleccione para crear un SYSLOG cuando elimine un paquete como resultado de una función de la seguridad del primer salto dentro de esta política.
  - *Heredar*: utilice el valor de la VLAN o la configuración global.
  - *Habilitar*: cree un SYSLOG cuando elimine un paquete como resultado de la seguridad del primer salto.
  - *Deshabilitar*: no cree un SYSLOG cuando elimine un paquete como resultado de la seguridad del primer salto.

Para adjuntar esta política a una interfaz:

- **Adjuntar política a la VLAN**: haga clic para ir a la página **Adjunto de la política (VLAN)** desde donde podrá adjuntar esta política a una VLAN.
- **Adjuntar política a la interfaz**: haga clic para ir a la página **Adjunto de la política (puerto)** desde donde podrá adjuntar esta política a un puerto.

Configuración de protección de RA

Utilice la página de configuración de la protección de RA para activar la función de protección de RA en un grupo de VLAN especificado y establecer los valores de la configuración global para esta función. Si es necesario, puede agregar una política o configurar las políticas de protección de RA predeterminadas definidas por el sistema en esta página.

Para configurar la protección de RA:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Configuración de la protección de RA**.

PASO 2 Complete los siguientes campos de configuración global:

- **Lista de VLAN de la protección de RA**: ingrese una o más VLAN en las que la protección de RA esté habilitada.
- **Función del dispositivo**: muestra una de las siguientes opciones para indicar la función del dispositivo conectado al puerto para la protección de RA.
  - *Heredada*: la función del dispositivo se hereda de la VLAN o los valores predeterminados del sistema (cliente).
  - *Router*: la función del dispositivo es la de router.
  - *Host*: la función del dispositivo es la de host.
- **Límite de salto mínimo**: este campo indica si la política de protección de RA verificará el límite de salto mínimo del paquete recibido.
  - *Sin verificación*: deshabilita la verificación del límite inferior de conteo de saltos.
  - *Definido por el usuario*: verifica que el límite de conteo de saltos sea superior o equivalente a este valor.

- **Límite de salto máximo**: este campo indica si la política de protección de RA verificará el límite de salto máximo del paquete recibido.
  - *Sin verificación*: deshabilita la verificación del límite superior de conteo de saltos.
  - *Definido por el usuario*: verifica que el límite de conteo de saltos sea menor o equivalente a este valor. El valor del límite máximo debe ser equivalente o superior al valor del límite mínimo.
- **Indicador de configuración administrada**: este campo especifica la verificación del indicador de configuración de dirección administrada anunciado dentro de la política de protección de RA de IPv6.
  - *Sin verificación*: deshabilita la verificación del indicador de configuración de dirección administrada anunciado.
  - *Activado*: habilita la verificación del indicador de configuración de dirección administrada anunciado.
  - *Desactivado*: el valor del indicador debe ser 0.
- **Otro indicador de configuración**: este campo especifica la verificación de otro indicador de configuración anunciado dentro de la política de protección de RA de IPv6.
  - *Sin verificación*: deshabilita la verificación de otro indicador de configuración anunciado.
  - *Activado*: habilita la verificación de otro indicador administrado anunciado.
  - *Desactivado*: el valor del indicador debe ser 0.
- **Preferencia mínima del router**: este campo indica si la política de protección de RA verificará el valor mínimo de la preferencia del router predeterminada anunciada en los mensajes de RA dentro de la política de protección de RA.
  - *Sin verificación*: deshabilita la verificación del límite inferior de la preferencia del router predeterminada anunciada.
  - *Bajo*: especifica el mínimo permitido para el valor de la preferencia del router predeterminada anunciada. Los siguientes valores son aceptables: bajo, medio y alto (consulte RFC4191).
  - *Medio*: especifica el mínimo permitido para el valor de la preferencia del router predeterminada anunciada. Los siguientes valores son aceptables: bajo, medio y alto (consulte RFC4191).
  - *Alto*: especifica el mínimo permitido para el valor de la preferencia del router predeterminada anunciada. Los siguientes valores son aceptables: bajo, medio y alto (consulte RFC4191).
- **Preferencia máxima del router**: este campo indica si la política de protección de RA verificará el valor máximo de la preferencia del router predeterminada anunciada en los mensajes de RA dentro de la política de protección de RA.
  - *Sin verificación*: deshabilita la verificación del límite superior de la preferencia del router predeterminada anunciada.

- *Bajo*: especifica el máximo permitido para el valor de la preferencia del router predeterminada anunciada. Los siguientes valores son aceptables: bajo, medio y alto (consulte RFC4191).
- *Medio*: especifica el máximo permitido para el valor de la preferencia del router predeterminada anunciada. Los siguientes valores son aceptables: bajo, medio y alto (consulte RFC4191).
- *Alto*: especifica el máximo permitido para el valor de la preferencia del router predeterminada anunciada. Los siguientes valores son aceptables: bajo, medio y alto (consulte RFC4191).

Si desea crear una política de protección de RA, haga clic en **Agregar** e ingrese los parámetros antes descritos. Para configurar las políticas predeterminadas definidas por el sistema, o la política actual definida por el usuario, seleccione la política en la lista de políticas y haga clic en **Editar**.

Para adjuntar esta política a una interfaz:

- **Adjuntar política a la VLAN**: haga clic para ir a la página **Adjunto de la política (VLAN)** desde donde podrá adjuntar esta política a una VLAN.
- **Adjuntar política a la interfaz**: haga clic para ir a la página **Adjunto de la política (puerto)** desde donde podrá adjuntar esta política a un puerto.

Configuración de protección de DHCPv6

Utilice la página de configuración de la protección de DHCPv6 para activar la función de protección de DHCPv6 en un grupo de VLAN especificado y establecer los valores de la configuración global para esta función. Si es necesario, se puede agregar una política o configurar las políticas de protección de DHCPv6 predeterminadas definidas por el sistema en esta página.

Para configurar la protección de DHCPv6:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Configuración de la protección de DHCPv6**.

PASO 2 Complete los siguientes campos de configuración global:

- **Lista de VLAN de la protección de DHCPv6**: ingrese una o más VLAN en las que la protección de DHCPv6 esté habilitada.
- **Función del dispositivo**: muestra la función del dispositivo. Consulte la definición en la página **Agregar**.
- **Preferencia mínima**: este campo indica si la política de protección de DHCPv6 verificará el valor mínimo de la preferencia anunciada del paquete recibido.
  - *Heredada*: la preferencia mínima se hereda de la VLAN o los valores predeterminados del sistema (cliente).

- *Sin verificación*: deshabilita la verificación del valor mínimo de la preferencia anunciada del paquete recibido.
- *Definido por el usuario*: verifica que el valor de la preferencia anunciada sea superior o equivalente a este valor. Este valor debe ser inferior al valor máximo de la preferencia.

- **Preferencia máxima**: este campo indica si la política de protección de DHCPv6 verificará el valor máximo de la preferencia anunciada del paquete recibido. Este valor debe ser superior al valor mínimo de la preferencia.
  - *Heredada*: la preferencia máxima se hereda de la VLAN o los valores predeterminados del sistema (cliente).
  - *Sin verificación*: deshabilita la verificación del límite inferior de conteo de saltos.
  - *Definido por el usuario*: verifica que el valor de la preferencia anunciada sea inferior o equivalente a este valor.

PASO 3 Si es necesario, haga clic en **Agregar** para crear una política de DHCPv6.

PASO 4 Ingrese los siguientes campos:

- **Nombre de la política**: ingrese el nombre de la política definida por el usuario.
- **Función del dispositivo**: seleccione **Servidor** o **Cliente** para especificar la función del dispositivo adjunto al puerto para la protección de DHCPv6.
  - *Heredada*: la función del dispositivo se hereda de la VLAN o los valores predeterminados del sistema (cliente).
  - *Cliente*: la función del dispositivo es la de cliente.
  - *Servidor*: la función del dispositivo es la de servidor.
- **Coincidencia de prefijos de respuesta**: seleccione para habilitar la verificación de los prefijos anunciados en los mensajes de respuesta de DHCP recibidos dentro de la política de protección de DHCPv6.
  - *Heredado*: el valor se hereda de la VLAN o los valores predeterminados del sistema (sin verificación).
  - *Sin verificación*: los prefijos anunciados no están verificados.
  - *Coincidencia de listas*: la lista de prefijos IPv6 debe coincidir.
- **Coincidencia de direcciones de servidor**: seleccione para habilitar la verificación de las direcciones IPv6 de la retransmisión y el servidor DHCP en los mensajes de respuesta de DHCP recibidos dentro de la política de protección de DHCPv6.
  - *Heredado*: el valor se hereda de la VLAN o los valores predeterminados del sistema (sin verificación).
  - *Sin verificación*: deshabilita la verificación de la dirección IPv6 de la retransmisión y el servidor DHCP.
  - *Coincidencia de listas*: la lista de prefijos IPv6 debe coincidir.

- **Preferencia mínima**: vea más arriba.
- **Preferencia máxima**: vea más arriba.

PASO 5 Haga clic en **Aplicar** para añadir configuraciones al archivo de configuración en ejecución.

Para adjuntar esta política a una interfaz:

- **Adjuntar política a la VLAN**: haga clic para ir a la página **Adjunto de la política (VLAN)** desde donde podrá adjuntar esta política a una VLAN.
- **Adjuntar política a la interfaz**: haga clic para ir a la página **Adjunto de la política (puerto)** desde donde podrá adjuntar esta política a un puerto.

Configuración de la inspección de detección de vecinos

Utilice la página de configuración de la inspección de detección de vecinos (ND) para activar la función de inspección de ND en un grupo de VLAN especificado y establecer los valores de la configuración global para esta función. Si es necesario, se puede agregar una política o configurar las políticas de inspección de ND predeterminadas definidas por el sistema en esta página.

Para configurar la inspección de ND:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Configuración de la inspección de ND**.

PASO 2 Complete los siguientes campos de configuración global:

- **Lista de VLAN de la inspección de ND**: ingrese una o más VLAN en las que la inspección de ND esté habilitada.
- **Función del dispositivo**: muestra la función del dispositivo que se explica a continuación.
- **Eliminación no segura**: seleccione para habilitar la eliminación de mensajes sin opción de firma CGA o RSA dentro de la política de inspección de ND de IPv6.
- **Nivel de seguridad mínimo**: si los mensajes no seguros no se eliminan, seleccione el nivel de seguridad por debajo del cual los mensajes no se desvían.
  - *Sin verificación*: deshabilita la verificación del nivel de seguridad.
  - *Definido por el usuario*: especifica el nivel de seguridad de los mensajes que se deben desviar.

- **Validación de MAC de origen**: especifique si desea habilitar globalmente la comparación de la dirección MAC de origen con la dirección de capa de enlace:
  - *Heredado*: valor heredado de la VLAN o los valores predeterminados del sistema (deshabilitados).
  - *Habilitar*: habilita la comparación de la dirección MAC de origen con la dirección de capa de enlace.
  - *Deshabilitar*: deshabilita la comparación de la dirección MAC de origen con la dirección de capa de enlace.

PASO 3 Si es necesario, haga clic en **Agregar** para crear una política de inspección de ND.

PASO 4 Ingrese los siguientes campos:

- **Nombre de la política**: ingrese el nombre de la política definida por el usuario.
- **Función del dispositivo**: seleccione **Servidor** o **Cliente** para especificar la función del dispositivo adjunto al puerto para la inspección de ND.
  - *Heredada*: la función del dispositivo se hereda de la VLAN o los valores predeterminados del sistema (cliente).
  - *Host*: la función del dispositivo es la de host.
  - *Router*: la función del dispositivo es la de router.
- **Eliminación no segura**: vea más arriba.
- **Preferencia de seguridad mínima**: vea más arriba.
- **Validación de MAC de origen**: consulte arriba.

PASO 5 Haga clic en **Aplicar** para añadir configuraciones al archivo de configuración en ejecución.

Para adjuntar esta política a una interfaz:

- **Adjuntar política a la VLAN**: haga clic para ir a la página **Adjunto de la política (VLAN)** desde donde podrá adjuntar esta política a una VLAN.
- **Adjuntar política a la interfaz**: haga clic para ir a la página **Adjunto de la política (puerto)** desde donde podrá adjuntar esta política a un puerto.

Configuración de vinculación de vecinos

La tabla de vinculación de vecinos es una tabla de base de datos de vecinos IPv6 conectados a un dispositivo creada a partir de fuentes de información tales como la indagación del protocolo de detección de vecinos (NDP). Varias funciones de protección de IPv6 utilizan esta tabla de base de datos o vinculación para evitar la suplantación y redireccionar los ataques.

Utilice la página de configuración de la vinculación de vecinos para activar la función de vinculación de vecinos en un grupo de VLAN especificado y establecer los valores de la configuración global para esta función. Si es necesario, se puede agregar una política o configurar las políticas de vinculación de vecinos predeterminadas definidas por el sistema en esta página.

Para configurar la vinculación de vecinos:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Configuración de la vinculación de vecinos**.

PASO 2 Complete los siguientes campos de configuración global:

- **Lista de VLAN de la vinculación de vecinos**: ingrese una o más VLAN en las que la vinculación de vecinos esté habilitada.
- **Función del dispositivo**: muestra la función predeterminada global del dispositivo (perímetro).
- **Vida útil de la vinculación de vecinos**: ingrese el tiempo de permanencia de las direcciones en la tabla de vinculación de vecinos.
- **Registro de la vinculación de vecinos**: seleccione para activar el registro de los eventos principales de la tabla de vinculación de vecinos.
- **Validación de prefijos de direcciones**: seleccione para activar la validación de direcciones de la protección de IPv6 de origen.

Configuración de la vinculación de direcciones globales:

- **Vincular desde mensajes de NDP**: para cambiar la configuración global de los métodos de configuración permitidos de las direcciones IPv6 globales que integran una política de vinculación de vecinos IPv6, seleccione una de las siguientes opciones:
  - *Cualquiera*: se permite cualquier método de configuración (sin estado y manual) para la vinculación de IPv6 global desde mensajes de NDP.
  - *Sin estado*: solo se permite la configuración automática sin estado para la vinculación de IPv6 global desde mensajes de NDP.
  - *Deshabilitar*: está desactivada la vinculación desde mensajes de NDP.
- **Vincular desde mensajes de DHCPv6**: está autorizada la vinculación desde DHCPv6.

Límites de entrada de la vinculación de vecinos: especifique la cantidad máxima de entradas de la vinculación de vecinos por tipo de interfaz o dirección:

- **Entradas por VLAN**: especifican el límite de vinculación de vecinos por VLAN. Seleccione Sin límite o ingrese un valor definido por el usuario.
- **Entradas por interfaz**: especifican el límite de vinculación de vecinos por interfaz. Seleccione Sin límite o ingrese un valor definido por el usuario.
- **Entradas por dirección MAC**: especifican el límite de vinculación de vecinos por dirección MAC. Seleccione **Sin límite** o ingrese un valor **definido por el usuario**.

PASO 3 Si es necesario, haga clic en **Agregar** para crear una política de vinculación de vecinos.

PASO 4 Ingrese los siguientes campos:

- **Nombre de la política**: ingrese el nombre de la política definida por el usuario.
- **Función del dispositivo**: seleccione **una** de las siguientes opciones para especificar la función del dispositivo adjunto al puerto para la política de vinculación de vecinos.
  - *Heredada*: la función del dispositivo se hereda de la VLAN o los valores predeterminados del sistema (cliente).
  - *Perímetro*: el puerto está conectado a dispositivos que no admiten la seguridad del primer salto de IPv6.
  - *Interno*: el puerto está conectado a dispositivos que admiten la seguridad del primer salto de IPv6.
- **Registro de la vinculación de vecinos**: seleccione una de las siguientes opciones para especificar el registro:
  - *Heredado*: la opción de registro es la misma que el valor global.
  - *Habilitar*: se activa el registro de los principales eventos de la tabla de vinculación.
  - *Deshabilitar*: se desactiva el registro de los principales eventos de la tabla de vinculación.
- **Validación de prefijos de direcciones**: seleccione una de las siguientes opciones para especificar la validación de direcciones:
  - *Heredado*: la opción de validación es la misma que el valor global.
  - *Habilitar*: se activa la validación de direcciones.
  - *Deshabilitar*: se desactiva la validación de direcciones.

Configuración de la vinculación de direcciones globales:

- *Heredar configuración de la vinculación de direcciones*: se activa el uso de la configuración de la vinculación de direcciones globales.
- *Vincular desde mensajes de NDP*: para cambiar la configuración global de los métodos de configuración permitidos de las direcciones IPv6 globales que integran una política de vinculación de vecinos IPv6, seleccione una de las siguientes opciones:
  - *Cualquiera*: se permite cualquier método de configuración (sin estado y manual) para la vinculación de IPv6 global desde mensajes de NDP.
  - *Sin estado*: solo se permite la configuración automática sin estado para la vinculación de IPv6 global desde mensajes de NDP.
  - *Deshabilitar*: está desactivada la vinculación desde mensajes de NDP.

  Vincular desde mensajes de DHCPv6: seleccione para habilitar la vinculación desde DHCPv6.

Límites de entrada de la vinculación de vecinos: **vea más arriba.**

- **Entradas por VLAN**: seleccione **Heredada** para usar el valor global, **Sin límite** para no establecer ningún límite para la cantidad de entradas, y **Definido por el usuario** para establecer un valor especial para la política.
- **Entradas por interfaz**: seleccione **Heredada** para usar el valor global, **Sin límite** para no establecer ningún límite para la cantidad de entradas, y **Definido por el usuario** para establecer un valor especial para la política.
- **Entradas por dirección MAC**: seleccione **Heredada** para usar el valor global, **Sin límite** para no establecer ningún límite para la cantidad de entradas, y **Definido por el usuario** para establecer un valor especial para la política.

PASO 5 Haga clic en **Aplicar** para añadir configuraciones al archivo de configuración en ejecución.

Para adjuntar esta política a una interfaz:

- **Adjuntar política a la VLAN**: haga clic para ir a la página **Adjunto de la política (VLAN)** desde donde podrá adjuntar esta política a una VLAN.
- **Adjuntar política a la interfaz**: haga clic para ir a la página **Adjunto de la política (puerto)** desde donde podrá adjuntar esta política a un puerto.

Configuración de la protección de origen IPv6

Use la página Configuración de la protección de origen IPv6 para activar la función de protección de origen IPv6 en un grupo de VLAN específico. Si es necesario, puede agregar una política o configurar las políticas de protección de origen IPv6 predeterminadas definidas por el sistema en esta página.

Para configurar la protección de origen IPv6:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Configuración de la protección de origen IPv6**.

PASO 2 Complete los siguientes campos de configuración global:

- **Lista de VLAN de la protección de origen IPv6**: ingrese una o más VLAN en las que la protección de origen IPv6 esté habilitada.
- **Confianza de puerto**: muestra que, de forma predeterminada, las políticas son para puertos no fiables. Estos valores pueden modificarse por política.

PASO 3 Si es necesario, haga clic en **Agregar** para crear una política de seguridad del primer salto.

PASO 4 Ingrese los siguientes campos:

- **Nombre de la política**: ingrese el nombre de la política definida por el usuario.
- **Confianza de puerto**: seleccione el estado de confianza de puerto de la política:
  - *Heredada*: cuando la política se adjunta a un puerto no fiable.
  - *Fiable*: cuando la política se adjunta a un puerto fiable.

PASO 5 Haga clic en **Aplicar** para adjuntar la política.

Para adjuntar esta política a una interfaz:

- **Adjuntar política a la VLAN**: haga clic para ir a la página **Adjunto de la política (VLAN)** desde donde podrá adjuntar esta política a una VLAN.
- **Adjuntar política a la interfaz**: haga clic para ir a la página **Adjunto de la política (puerto)** desde donde podrá adjuntar esta política a un puerto.

Adjunto de la política (VLAN)

Para adjuntar una política a una o varias VLAN:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Adjunción de políticas (VLAN)**.

La lista de políticas ya adjuntadas se muestra junto con el **Tipo de política**, el **Nombre de la política** y la **Lista de VLAN**.

PASO 2 Para adjuntar una política a una VLAN, haga clic en **Agregar** e ingrese los siguientes campos:

- **Tipo de política**: seleccione el tipo de política para adjuntar a la interfaz.
- **Nombre de la política**: seleccione el nombre de la política para adjuntar a la interfaz.
- **Lista de VLAN**: seleccione las VLAN a las que se adjuntan las políticas. Seleccione **Todas las VLAN** o ingrese un intervalo de VLAN.

PASO 3 Haga clic en **Aplicar** para añadir configuraciones al archivo de configuración en ejecución.

Adjunto de la política (puerto)

Para adjuntar una política a uno o varios puertos o LAG:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Adjunción de políticas (puerto)**.

La lista de políticas ya adjuntadas se muestra junto con el **Número de** interfaz, el **Tipo de política**, el **Nombre de la política** y la **Lista de VLAN**.

PASO 2 Para adjuntar una política a un puerto o LAG, haga clic en **Agregar** e ingrese los siguientes campos:

- **Interfaz**: seleccione la interfaz a la que se adjuntará la política.
- **Tipo de política**: seleccione el tipo de política para adjuntar a la interfaz.
- **Nombre de la política**: seleccione el nombre de la política para adjuntar a la interfaz.
- **Lista de VLAN**: seleccione las VLAN a las que se adjuntan las políticas. Seleccione **Todas las VLAN** o ingrese un intervalo de VLAN.

PASO 3 Haga clic en **Aplicar** para añadir configuraciones al archivo de configuración en ejecución.

Tabla de vinculación de vecinos

Para consultar las entradas de la tabla de vinculación de vecinos:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Tabla de vinculación de vecinos**.

PASO 2 Seleccione una de las siguientes opciones de borrar tabla:

- **Solo estáticas**: borra todas las entradas estadísticas de la tabla.
- **Solo dinámicas**: borra todas las entradas dinámicas de la tabla.
- **Todo Estáticas y dinámicas**: borra todas las entradas estáticas y dinámicas de la tabla.

Ingrese los siguientes campos:

- **ID de VLAN**: ID de VLAN de la entrada.
- **Dirección IPv6**: dirección IPv6 de origen de la entrada.
- **Nombre de la interfaz**: puerto en el que se recibe el paquete.
- **Dirección MAC**: dirección MAC del vecino del paquete.
- **Origen**: protocolo que agregó la dirección IPv6 (disponible únicamente para entradas dinámicas):
  - *Estática*: ingresada manualmente.
  - *NDP*: se reconoce de los mensajes del protocolo de detección de vecinos.
  - *DHCP*: se reconoce de los mensajes del protocolo DHCPv6.
- **Estado**: estado de la entrada:
  - *Tentativo*: la nueva dirección IPv6 del host está en proceso de validación. El vencimiento no se muestra, ya que dura menos de 1 segundo.
  - *Válido*: la dirección IPv6 del host no se vinculó.
- **Vencimiento (seg.)**: tiempo remanente en segundos para que se elimine la entrada en caso de no confirmarse.
- **Desbordamiento de la TCAM**: las entradas marcadas con un **No** no se agregaron a la TCAM debido a un desbordamiento de la TCAM.

Tabla de prefijos de vecinos

Es posible agregar prefijos estáticos a las direcciones IPv6 globales que se vincularon desde mensajes de NDP en la tabla de prefijos de vecinos. Se reconocen las entradas dinámicas, tal como se describe en **Detección de prefijos IPv6 anunciados**.

Para añadir entradas en la tabla de prefijos de vecinos:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Tabla de prefijos de vecinos**.

PASO 2 Seleccione una de las opciones a continuación para borrar la tabla de prefijos de vecinos:

- **Solo estático**: elimina las entradas estáticas.
- **Solo dinámico**: elimina las entradas dinámicas.
- **Dinámicas y estáticas**: elimina las entradas dinámicas y estáticas.

PASO 3 Para las entradas de salida, se muestran los siguientes campos:

- **ID de VLAN**: VLAN en la que son relevantes los prefijos.
- **Prefijo IPv6**: prefijo IPv6.
- **Longitud del prefijo**: la longitud del prefijo IPv6.
- **Origen**: la entrada es dinámica (reconocida) o estática (configurada manualmente).
- **Configuración automática**: el prefijo puede utilizarse para la configuración sin estado.
- **Vencimiento (seg.)**: tiempo de permanencia de la entrada antes de eliminarla.

PASO 4 Haga clic en **Agregar** para añadir una nueva entrada a la tabla y complete los campos antes descritos para la nueva entrada.

Estado de FHS

Para ver la configuración global de las funciones de la FHS:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Estado de la FHS**.

PASO 2 Seleccione un puerto, un LAG o una VLAN para informar el estado de la FHS.

PASO 3 Se muestran los siguientes campos para la interfaz seleccionada:

- **Estado de FHS**
  - *Estado de la FHS en la VLAN actual:* es la FHS habilitada en la VLAN actual.
  - *Registro de eliminación de paquetes*: indica si esta función está activada para la interfaz actual (a nivel de la configuración global o en una política adjunta a la interfaz).
- **Estado de protección de RA**
  - *Estado de la protección de RA en la VLAN actual:* es la protección de RA habilitada en la VLAN actual.
  - *Función del dispositivo*: función del dispositivo de RA.
  - *Indicador de configuración administrada*: es la verificación del indicador de configuración administrada habilitado.
  - *Otro indicador de configuración*: es la verificación de otro indicador de configuración habilitado.
  - *Lista de direcciones de RA*: lista de direcciones de RA que deben coincidir.
  - *Lista de prefijos de RA*: lista de prefijos de RA que deben coincidir.
  - *Límite mínimo del salto*: es la verificación del límite mínimo del salto de RA habilitada.
  - *Límite máximo del salto*: es la verificación del límite máximo del salto de RA habilitada.
  - *Preferencia mínima del router*: es la verificación de la preferencia mínima del router habilitada.
  - *Preferencia máxima del router*: es la verificación de la preferencia máxima del router habilitada.
- **Estado de protección de DHCPv6**
  - *Estado de la protección de DHCPv6 en la VLAN actual:* es la protección de DHCPv6 habilitada en la VLAN actual.
  - *Función del dispositivo*: función del dispositivo de DHCP.
  - *Coincidencia de prefijos de respuesta*: es la verificación de los prefijos de respuesta de DHCP habilitada.
  - *Coincidencia de direcciones de servidor*: es la verificación de las direcciones de servidor DHCP habilitada.
  - *Preferencia mínima*: es la verificación de la preferencia mínima habilitada.
  - *Preferencia máxima*: es la verificación de la preferencia máxima habilitada.

- **Estado de inspección de ND**
  - *Estado de la inspección de ND en la VLAN actual:* es la inspección de ND habilitada en la VLAN actual.
  - *Función del dispositivo*: función del dispositivo de inspección de ND.
  - *Eliminación no segura*: son los mensajes no seguros eliminados.
  - *Nivel mínimo de seguridad*: es el nivel mínimo de seguridad para los paquetes que se deben desviar si los mensajes no seguros no se eliminan.
  - *Validación de MAC de origen*: es la verificación de la dirección MAC de origen habilitada.
- **Estado de la vinculación de vecinos**
  - *Estado de la vinculación de vecinos en la VLAN actual:* es la vinculación de vecinos habilitada en la VLAN actual.
  - *Función del dispositivo*: función del dispositivo de vinculación de vecinos.
  - *Vinculación de registro*: es el registro de los eventos de la tabla de vinculación de vecinos habilitado.
  - *Validación de prefijos de direcciones*: la validación de prefijos de direcciones está activada.
  - *Configuración de direcciones globales*: indica cuáles son los mensajes validados.
  - *Entradas máximas por VLAN*: máxima cantidad de entradas dinámicas de la tabla de vinculación de vecinos por VLAN permitida.
  - *Entradas máximas por interfaz*: máxima cantidad de entradas de la tabla de vinculación de vecinos por interfaz permitida.
  - *Entradas máximas por dirección MAC*: máxima cantidad de entradas de la tabla de vinculación de vecinos por dirección MAC permitida.
- **Estado de la protección de origen IPv6:**
  - *Estado de la protección de origen IPv6 en la VLAN actual:* la protección de origen IPv6 está habilitada en la VLAN actual.
  - *Confianza de puerto*: indica si el puerto es fiable y cómo recibió ese estado.

Estadísticas de FHS

Para ver las estadísticas de la FHS:

PASO 1 Haga clic en **Seguridad** > **Seguridad del primer salto de IPv6** > **Estadísticas de la FHS**.

PASO 2 En **Vel. de actualización** seleccione el período de tiempo que transcurre antes de que se actualicen las estadísticas.

PASO 3 Se muestran los siguientes contadores de desbordamiento global:

- **Tabla de vinculación de vecinos**: cantidad de entradas que no pudieron agregarse a la tabla porque ya se alcanzó el tamaño máximo.
- **Tabla de prefijos de vecinos**: cantidad de entradas que no pudieron agregarse a la tabla porque ya se alcanzó el tamaño máximo.
- **TCAM**: cantidad de entradas que no pudieron agregarse debido a un desbordamiento de la TCAM.

PASO 4 Seleccione una interfaz y se mostrarán los siguientes campos:

- **Mensajes de NDP (protocolo de detección de vecinos)**: la cantidad de mensajes descartados y recibidos se muestra para los siguientes tipos de mensaje:
  - *RA*: mensajes de anuncio del router.
  - *REDIR*: redirigir mensajes.
  - *NS*: mensajes de solicitud de vecinos.
  - *NA*: mensajes de anuncio de vecinos.
  - *RS*: mensajes de solicitud del router.
- **Mensajes DHCPv6**: la cantidad de mensajes descartados y recibidos se muestra para los siguientes tipos de mensajes DHCPv6:
  - *ADV*: mensajes de anuncios
  - *REP*: mensajes de respuesta
  - *REC*: mensajes de reconfiguración
  - *REL-REP*: mensajes de respuesta de retransmisión
  - *LEAS-REP*: mensajes de respuesta de consulta de concesión
  - *RLS*: mensajes enviados
  - *DEC*: mensajes rechazados

Los siguientes campos se muestran en la tabla de mensajes eliminados de la FHS:

- **Característica**: tipo de mensaje descartado (protección de DHCPv6, protección de RA, etc.).
- **Conteo**: cantidad de mensajes eliminados.
- **Motivo**: motivo por el que se eliminaron los mensajes.

22

Seguridad: Gestión de datos confidenciales

Los datos confidenciales seguros (SSD, Secure Sensitive Data) son una arquitectura que facilita la protección de los datos confidenciales de un dispositivo, como las contraseñas y las claves. La facilidad utiliza frases clave, cifrado, control de acceso y autenticación de usuarios para brindar una solución segura a la administración de datos confidenciales.

La facilidad se extiende para proteger la integridad de los archivos de configuración, para asegurar el proceso de configuración y admitir la configuración automática zero-touch de SSD.

Introducción

SSD protege los datos confidenciales de los dispositivos, como las contraseñas y claves, permite y rechaza el acceso a los datos confidenciales cifrados y sin formato de las credenciales del usuario y las reglas SSD y evita que los archivos de configuración que contienen datos confidenciales sean alterados.

Además, SSD permite que se realice la copia de respaldo segura y que se compartan los archivos de configuración que contienen datos confidenciales.

SSD brinda a los usuarios la flexibilidad para configurar el nivel de protección deseado de sus datos confidenciales; desde sin protección con datos confidenciales en texto sin formato, protección mínima con cifrado según la frase clave predeterminada y mejor protección con cifrado según la frase clave definida por el usuario.

SSD otorga permiso de lectura de los datos confidenciales solo a los usuarios autenticados y autorizados y según las reglas SSD. Un dispositivo autentica y autoriza el acceso de administración para los usuarios a través del proceso de autenticación de usuarios.

Se utilice SSD o no, se recomienda que un administrador asegure el proceso de autenticación utilizando la base de datos de autenticación local o que asegure la comunicación al servidor de autenticación externo utilizado en el proceso de autenticación de usuarios.

En resumen, SSD protege los datos confidenciales de un dispositivo con reglas SSD, propiedades SSD y autenticación de usuarios. Y las reglas SSD, las propiedades SSD y la configuración de autenticación de usuarios del dispositivo cuentan con datos confidenciales protegidos en sí mismos por SSD.

Administración de SSD

La administración de SSD incluye una colección de parámetros de configuración que definen el manejo y la seguridad de los datos confidenciales. Los parámetros de configuración SSD son datos confidenciales en sí mismos y están protegidos por SSD.

Toda la configuración de SSD se realiza a través de las páginas SSD, que solo se encuentran disponibles para usuarios que tienen los permisos correctos (consulte **Reglas SSD**).

Reglas SSD

Las reglas SSD definen los permisos de lectura y el modo lectura predeterminada dado a la sesión de un usuario en un canal de administración.

Una regla SSD es identificada de manera única por su usuario y canal de administración SSD. Pueden existir reglas SSD diferentes para el mismo usuario, pero para canales diferentes y, pueden existir distintas reglas para el mismo canal, pero para usuarios diferentes.

Los permisos de lectura determinan la forma en la que se pueden ver los datos confidenciales: en forma de solo cifrado, en forma de solo texto sin formato, en forma de cifrado y texto sin formato o sin permiso para ver los datos confidenciales. Las reglas SSD están protegidas como datos confidenciales por sí mismas.

Un dispositivo puede admitir un total de 32 reglas SSD.

Un dispositivo otorga a un usuario el permiso de lectura SSD de la regla SSD que más coincide con la identidad/credencial del usuario y el tipo de canal de administración desde el cual el usuario accede/accederá los datos confidenciales.

Un dispositivo incluye un conjunto de reglas SSD predeterminadas. Un administrador puede añadir, eliminar y cambiar las reglas SSD según lo desee.

NOTA Es posible que un dispositivo no admita todos los canales definidos por SSD.

Elementos de una regla SSD

Una regla SSD incluye los siguientes elementos:

- **Tipo de usuario**: los tipos de usuario admitidos en orden de mayor preferencia a menor preferencia son los siguientes: (En caso de que un usuario coincida con varias reglas SSD, se aplicará la regla que tenga el tipo de usuario con mayor preferencia).
  - **Específico**: la regla se aplica a un usuario específico.
  - **Usuario predeterminado (cisco)**: la regla se aplica al usuario predeterminado (cisco).
  - **Nivel 15**: la regla se aplica a los usuarios que cuentan con el nivel de privilegio 15.
  - **Todos**: la regla se aplica a todos los usuarios.
- **Nombre de usuario**: si el tipo de usuario es específico, se requiere un nombre de usuario.
- **Canal.** Tipo de canal de administración SSD al cual se aplica la regla. Los tipos de canal admitidos son los siguientes:
  - **Seguro**: especifica que la regla solo se aplica a los canales seguros. Según el dispositivo, puede admitir todos los siguientes canales seguros, o solo algunos:
    interfaz del puerto de la consola, SCP, SSH y HTTPS.
  - **Inseguro**: especifica que la regla solo se aplica a los canales inseguros. Según el dispositivo, puede admitir todos los siguientes canales inseguros, o solo algunos:
    Telnet, TFTP y HTTP.
  - **XML SNMP seguro**: especifica que esta regla se aplica solo a XML a través de HTTPS o SNMPv3 con privacidad. Un dispositivo puede admitir todos los canales XML y SNMP seguros o no.
  - **XML SNMP inseguro**: especifica que esta regla se aplica solo a XML a través de HTTP o SNMPv1/v2 y SNMPv3 sin privacidad. Un dispositivo puede admitir todos los canales XML y SNMP seguros o no.
- **Permiso de lectura**: los permisos de lectura se relacionan con las reglas. Pueden ser los siguientes:
  - (El más bajo) **Excluir**: los usuarios no tienen permiso para acceder a los datos confidenciales de ninguna forma.
  - (Medio) **Solo cifrado**: los usuarios tienen permiso para acceder a los datos confidenciales como solo cifrado.
  - (Más alto) **Solo texto sin formato**: los usuarios tienen permiso para acceder a los datos confidenciales como solo texto sin formato. Los usuarios también tendrán permiso de lectura y escritura para los parámetros SSD.
  - (El más alto) **Ambos**: los usuarios tienen permisos de cifrado y de texto sin formato y tienen permiso para acceder a los datos confidenciales como cifrados y en texto sin formato. Los usuarios también tendrán permiso de lectura y escritura para los parámetros SSD.

Cada canal de administración otorga permisos de lectura específicos. Se resumen a continuación.

Canal de administración	Opciones de permiso de lectura permitidas
Segura	Ambos, solo cifrado
No seguro	Ambos, solo cifrado
XML SNMP seguro	Excluir, solo texto sin formato
XML SNMP no seguro	Excluir, solo texto sin formato

- **Modo lectura predeterminado**: todos los modos de lectura predeterminados están sujetos al permiso de lectura de la regla. Existen las siguientes opciones, pero algunas se pueden rechazar, según el permiso de lectura. Si el permiso de lectura definido por el usuario para un usuario es Excluir (por ejemplo) y el modo de lectura predeterminado es Cifrado, prevalece el permiso de lectura definido por el usuario.
  - **Excluir**: no permite la lectura de datos confidenciales.
  - **Cifrado**: los datos confidenciales se presentan en forma cifrada.
  - **Texto sin formato**: los datos confidenciales se presentan en forma de texto sin formato.

  Cada canal de administración permite presunciones de lectura específicas. Se resumen a continuación.

Permiso de lectura	Modo lectura predeterminado permitido
Excluir	Excluir
Sólo cifrado	*Cifrado
Sólo texto simple	*Texto sin formato
Ambos	*Texto sin formato, cifrado

  * El modo de lectura de una sesión puede cambiarse temporalmente en la página Propiedades SSD si el modo de lectura nuevo no viola el permiso de lectura.

NOTA Tenga en cuenta lo siguiente:

- El modo de lectura predeterminado de los canales de administración XML SNMP seguro y XML SNMP inseguro debe ser idéntico a su permiso de lectura.
- El permiso de lectura Excluir está permitido solo para los canales de administración XML SNMP seguro y XML SNMP inseguro; Excluir no está permitido para los canales seguro e inseguro habituales.

- Excluir datos confidenciales en canales de administración XML-SNMP seguro e inseguro significa que los datos confidenciales se presentan como un 0 (que significa cadena nula o 0 numérico). Si el usuario desea ver los datos confidenciales, la regla se debe cambiar a texto sin formato.
- De manera predeterminada, se considera que un usuario SNMPv3 con permisos de privacidad y XML sobre canales seguros es un usuario de nivel 15.
- Los usuarios SNMP en el canal XML y SNMP inseguro (SNMPv1,v2 y v3 sin privacidad) son considerados como Todos los usuarios.
- Los nombres de la comunidad SNMP no se utilizan como nombres de usuario para que coincidan con las reglas SSD.
- Se puede controlar el acceso por un usuario SNMPv3 determinado configurando una regla SSD con un nombre de usuario que coincida con el nombre de usuario SNMPv3.
- Debe haber al menos una regla con permiso de lectura: Texto sin formato o Ambos, porque solo los usuarios con esos permisos pueden acceder a las páginas SSD.
- Los cambios del modo de lectura predeterminado y los permisos de lectura de una regla entrarán en vigencia y se aplicarán a los usuarios y al canal afectados de todas las sesiones de administración activas de inmediato, excepto la sesión en la que se realicen los cambios aunque la regla sea aplicable. Cuando se modifica una regla (añadir, eliminar, editar), un sistema actualizará todas las sesiones CLI/GUI afectadas.

  NOTA Cuando se modifica la regla SSD aplicada a de la sesión de conexión desde esa sesión, el usuario debe cerrar la sesión y volver para ver el cambio.

  NOTA Al realizar una transferencia de archivos iniciada por un comando XML o SNMP, se utiliza el protocolo subyacente TFTP. Por lo tanto, se aplicará la regla SSD para canales inseguros.

Reglas SSD y autenticación del usuario

SSD otorga permiso SSD solo a los usuarios autenticados y autorizados de acuerdo con las reglas SSD. La autenticación y autorización del acceso de administración por parte de un dispositivo depende del proceso de autenticación de su usuario. Para proteger un dispositivo y sus datos, incluidos los datos confidenciales y la configuración de SSD del acceso no autorizado, se recomienda que el proceso de autenticación del usuario del dispositivo se asegure. Para asegurar el proceso de autenticación del usuario, puede utilizar la base de datos de autenticación local, así como asegurar la comunicación a través de servidores de autenticación externos, como el servidor RADIUS. La configuración de la comunicación segura a los servidores de autenticación externos son datos confidenciales están protegidos por SSD.

NOTA La credencial de usuario de la base de datos autenticada local ya se encuentra protegida por un mecanismo SSD no relacionado

Si el usuario de un canal emite una acción que utiliza un canal alternativo, el dispositivo aplica el permiso de lectura y el modo de lectura predeterminado de la regla SSD que coincide con la credencial del usuario y el canal alternativo. Por ejemplo, si un usuario inicia sesión a través de un canal seguro e inicia una sesión TFTP de carga, se aplica el permiso de lectura SSD del usuario del canal inseguro (TFTP).

Reglas SSD predeterminadas

El dispositivo tiene las siguientes reglas predeterminadas de fábrica:

Tabla 3

Clave de regla		Acción de regla	
Usuario	**Canal**	**Permiso de lectura**	**Modo lectura predeterminado**
Nivel 15	XML SNMP seguro	Sólo texto simple	Texto simple
Nivel 15	Segura	Ambos	Cifrada
Nivel 15	No seguro	Ambos	Cifrada
Todos	XML SNMP no seguro	Excluir	Excluir
Todos	Segura	Sólo cifrado	Cifrada
Todos	No seguro	Sólo cifrado	Cifrada

Las reglas predeterminadas se pueden modificar, pero no se pueden eliminar. Si se han cambiado las reglas SSD predeterminadas, se pueden restaurar.

Anulación de la sesión del modo de lectura SSD predeterminado

El sistema contiene los datos confidenciales en una sesión, como cifrados o en texto sin formato, según el permiso de lectura y el modo de lectura predeterminado del usuario.

El modo de lectura predeterminado se puede anular temporalmente, siempre que no entre en conflicto con el permiso de lectura SSD de la sesión. Este cambio se aplica de inmediato en la sesión actual, hasta que ocurra algo de lo siguiente:

- El usuario lo cambia nuevamente.
- La sesión finaliza.
- El permiso de lectura de la regla SSD que se aplica al usuario de la sesión cambia y ya no es compatible con el modo de lectura actual de la sesión. En este caso, el modo de lectura de la sesión regresa al modo de lectura predeterminado de la regla SSD.

Propiedades SSD

Las propiedades SSD son un conjunto de parámetros que, junto con las reglas SSD, definen y controlan el entorno de SSD de un dispositivo. El entorno SSD consta de las siguientes propiedades:

- Control de cómo se cifran los datos confidenciales
- Control del nivel de seguridad de los archivos de configuración
- Control de cómo se ven los datos confidenciales dentro de la sesión actual

Frase clave

La frase clave es la base del mecanismo de seguridad de la función SSD y se utiliza para generar la clave para el cifrado y el descifrado de los datos confidenciales. Las series de switches Sx200, Sx300, Sx500 y SG500X/SG500XG/ESW2-550X que tienen la misma frase clave pueden descifrar los datos confidenciales cifrados entre sí con la clave generada a partir de la frase clave.

Las frases claves deben cumplir las siguientes reglas:

- **Longitud**: entre 8 y 16 caracteres.
- **Clases de caracteres**: la frase clave debe contener al menos un carácter en mayúscula, uno en minúscula, uno numérico y uno especial, p. ej., #, $.

Frases claves predeterminadas y definidas por el usuario

Todos los dispositivos incluyen una frase clave predeterminada y configurada de fábrica que es transparente para los usuarios. La frase clave predeterminada nunca se muestra en el archivo de configuración ni en el CLI/GUI.

Si desea una mejor seguridad y protección, un administrador debe configurar SSD en un dispositivo para utilizar una frase clave definida por el usuario en lugar de la frase clave predeterminada. La frase clave definida por el usuario debe ser tratada como un secreto bien guardado, para que no se comprometa la seguridad de los datos confidenciales del dispositivo.

Se puede configurar la frase clave definida por el usuario manualmente, en texto sin formato. También se puede derivar de un archivo de configuración. (Consulte **Configuración automática zero-touch de datos confidenciales**). Los dispositivos siempre muestran las frases claves definidas por el usuario en forma cifrada.

Frase clave local

Los dispositivos mantienen una frase clave local que es la frase local de su configuración en ejecución. SSD generalmente realiza el cifrado y descifrado de datos confidenciales con la clave generada desde la frase clave local.

La frase clave local se puede configurar para que sea la frase clave predeterminada o una frase clave definida por el usuario. De manera predeterminada, la frase clave local y la frase clave predeterminada son idénticas. Se puede cambiar a través de acciones administrativas desde la interfaz de línea de comandos (si está disponible) o desde la interfaz basada en la Web. Se cambia automáticamente a la frase clave del archivo de configuración de inicio, cuando la configuración de inicio se convierte en la configuración en ejecución del dispositivo. Cuando se restablecen los valores predeterminados de fábrica de un dispositivo, la frase clave local se restablece a la frase clave predeterminada.

Control de frase clave del archivo de configuración

El control de frase clave del archivo ofrece protección adicional para una frase clave definida por el usuario y los datos confidenciales cifrados con la clave generada a partir de la frase clave definida por el usuario en los archivos de configuración basados en texto.

A continuación, se encuentran los modos de control de frase clave existentes:

- **Sin restricciones** (predeterminado): el dispositivo incluye su frase clave al crear un archivo de configuración. Esto permite que cualquier dispositivo acepte el archivo de configuración para obtener la frase clave del archivo.
- **Con restricciones**: el dispositivo no permite que su frase clave sea exportada a un archivo de configuración. El modo con restricciones protege los datos confidenciales cifrados de un archivo de configuración de dispositivos que no tienen la frase clave. Este modo se debe utilizar cuando el usuario no desea exponer la frase clave en un archivo de configuración.

Después de que se restablecen los valores predeterminados de fábrica de un dispositivo, su frase clave local se restablece a la frase clave predeterminada. Como resultado, el dispositivo no podrá descifrar ningún dato confidencial basado en una frase clave definida por el usuario ingresada desde una sesión de administración (GUI/CLI) ni ningún archivo de configuración con modo restringido, incluidos los archivos creados por el dispositivo mismo, antes de que se restablezcan sus valores predeterminados de fábrica. Esto permanece así hasta que se vuelve a configurar manualmente el dispositivo con la frase clave definida por el usuario o se obtiene la frase clave definida por el usuario a partir de un archivo de configuración.

Control de integridad del archivo de configuración

Los usuarios pueden proteger un archivo de configuración de su alteración o modificación creando el archivo de configuración con el control de integridad del archivo de configuración. Se recomienda habilitar el control de integridad del archivo de configuración cuando el dispositivo utiliza una frase clave definida por el usuario con control de frase clave del archivo de configuración sin restricciones.

PRECAUCIÓN Cualquier modificación realizada en un archivo de configuración que esté protegido íntegramente se considera alteración.

Los dispositivos determinan si la integridad de un archivo de configuración está protegida al examinar el comando de control de integridad del archivo en el bloqueo de control SSD del archivo. Si el archivo está protegido íntegramente, pero el dispositivo descubre que la integridad del archivo no está intacta, el dispositivo rechaza el archivo. De lo contrario, el archivo es aceptado para continuar con el procesamiento.

El dispositivo verifica la integridad de un archivo de configuración basado en texto cuando este se descarga o se copia en el archivo de configuración de inicio.

Modo lectura

Cada sesión tiene un modo de lectura. Esto determina cómo se muestran los datos confidenciales. El modo de lectura puede ser texto sin formato, en cuyo caso los datos confidenciales se muestran como texto normal, o cifrado, donde los datos confidenciales se muestran en su forma cifrada.

Archivos de configuración

Los archivos de configuración contienen la configuración de un dispositivo. Los dispositivos tienen un archivo de configuración en ejecución, un archivo de configuración de inicio, un archivo de configuración de duplicado (opcional) y un archivo de configuración de respaldo. Los usuarios pueden cargar los archivos de configuración en forma manual desde un servidor de archivos remoto o descargarlos desde este. Los dispositivos pueden descargar su configuración de inicio en forma automática desde un servidor de archivos remoto durante la etapa de configuración automática utilizando DHCP. Los archivos de configuración almacenados en servidores de archivos remotos se conocen como archivos de configuración remotos.

El archivo Configuración en ejecución contiene la configuración que un dispositivo está utilizando actualmente. La configuración de un archivo de configuración de inicio se convierte en la configuración en ejecución después del reinicio. Los archivos de configuración en ejecución y de inicio se formatean en formato interno. Los archivos de configuración de duplicado, de respaldo y remotos son archivos basados en texto que generalmente se mantienen para archivos, registros o recuperación. Durante el copiado, la carga y la descarga de un archivo de configuración de origen, si los dos archivos están en formato distinto, el dispositivo transforma el contenido de origen al formato del archivo de destino automáticamente.

Indicador de SSD de archivo

Al copiar el archivo de configuración en ejecución o de inicio a un archivo de configuración basado en texto, el dispositivo genera el indicador de archivo SSD y lo coloca en el archivo de configuración basado en texto para indicar que el archivo contiene datos confidenciales cifrados o datos confidenciales con texto sin formato o que los datos confidenciales no están incluidos.

- El indicador SSD, si existe, debe estar en el archivo de encabezado de configuración.
- Se considera que la configuración basada en texto que no incluye un indicador SSD no contiene datos confidenciales.
- El indicador SSD se utiliza para reforzar los permisos de lectura de SSD en los archivos de configuración basados en texto, pero es ignorado al copiar los archivos de configuración al archivo de configuración en ejecución o de inicio.

El indicador SSD de un archivo se establece según las instrucciones del usuario, durante la copia, para incluir texto cifrado o sin formato, o bien para excluir los datos confidenciales de un archivo.

Bloqueo de control SSD

Cuando un dispositivo crea un archivo de configuración basado en texto a partir de su archivo de configuración de inicio o en ejecución, inserta un bloqueo de control SSD en el archivo si el usuario solicita que el archivo incluya datos confidenciales. El bloqueo de control SSD, que está protegido de alteraciones, contiene reglas SSD y propiedades SSD del dispositivo que crea el archivo. Un bloqueo de control SSD comienza y termina con "ssd-control-start" y "ssd-control-end", respectivamente.

Archivo de configuración de inicio

El dispositivo actualmente admite la copia desde los archivos de configuración, en ejecución, de respaldo, de duplicado y remotos al archivo de configuración de inicio. Los parámetros de la configuración de inicio tienen efecto y se convierte en la configuración en ejecución después del reinicio. Los usuarios pueden recuperar los datos confidenciales cifrados o en texto sin formato a partir del archivo de configuración de inicio, sujeto al permiso de lectura SSD y el modo de lectura SSD actual de la sesión de administración.

El acceso de lectura de los datos confidenciales de la configuración de inicio en cualquier forma queda excluido si la frase clave del archivo de configuración de inicio y la frase clave local son distintas.

SSD agrega las siguientes reglas al copiar los archivos de configuración de respaldo, de duplicado y remotos al archivo de configuración de inicio:

- Una vez que se restablecen los valores predeterminados de fábrica de un dispositivo, se restablecen todos los valores predeterminados de su configuración, incluidas las reglas y propiedades SSD.
- Si un archivo de configuración de origen contiene datos confidenciales cifrados, pero le falta un bloqueo de control SSD, el dispositivo rechaza el archivo de origen y la copia falla.

- Si no hay bloqueo de control SSD en el archivo de configuración de origen, se restablecen los valores predeterminados de la configuración SSD del archivo de configuración de inicio.
- Si hay una frase clave en el bloqueo de control SSD del archivo de configuración de origen, el dispositivo rechazará el archivo de origen. La copia fallará si hay datos confidenciales cifrados en el archivo que no están cifrados por la clave generada a partir de la frase clave del bloqueo de control de SSD.
- Si no hay un bloqueo de control SSD en el archivo de configuración de origen y el archivo no puede realizar la verificación de la integridad de SSD o la verificación de la integridad del archivo, el dispositivo rechaza el archivo de origen y la copia falla.
- Si no hay una frase clave en el bloqueo de control SSD del archivo de configuración de origen, todos los datos confidenciales cifrados del archivo se deben cifrar por la clave generada a partir de la frase clave local, o bien por la clave generada a partir de la frase clave predeterminada, pero no por las dos. De lo contrario, el archivo de origen es rechazado y la copia falla.
- El dispositivo configura la frase clave, el control de la frase clave y la integridad de los archivos, si hubiera, desde el bloqueo de control SSD en el archivo de configuración de origen hasta el archivo de configuración de inicio. Configura el archivo de configuración de inicio con la frase clave que se utiliza para generar la clave a fin de descifrar los datos confidenciales del archivo de configuración de origen. La configuración SSD que no se encuentre se restablece al valor predeterminado.
- Si no hay un bloqueo de control SSD en el archivo de configuración de origen y el archivo contiene texto sin formato y datos confidenciales sin incluir la configuración SSD en el bloqueo de control SSD, el archivo es aceptado.

Archivo Configuración en ejecución

El archivo Configuración en ejecución contiene la configuración que el dispositivo está utilizando actualmente. Los usuarios pueden recuperar los datos confidenciales cifrados o en texto sin formato a partir de un archivo Configuración en ejecución, sujeto al permiso de lectura SSD y el modo de lectura SSD actual de la sesión de administración. El usuario puede cambiar la configuración en ejecución copiando los archivos de configuración de respaldo o de duplicado mediante otras acciones de administración a través de CLI, XML, SNMP, etc.

Los dispositivos aplican las siguientes reglas cuando un usuario cambia directamente la configuración SSD de la configuración en ejecución:

- Si el usuario que abrió la sesión de administración no tiene permisos SSD (lo que significa los permisos de lectura de ambos o solo de texto sin formato) el dispositivo rechaza todos los comandos SSD.
- Cuando el indicador de SSD de archivo, la integridad de bloqueo de control SSD y la integridad del archivo SSD son copiados de un archivo de origen no son ni verificados ni aplicados.
- Cuando son copiados de un archivo de origen, la copia fallará si la frase clave del archivo de origen se encuentra en texto sin formato. Si la frase clave está cifrada, se ignora.

- Cuando se configura la frase clave directamente (copia no basada en archivo), en la configuración en ejecución, la frase clave del comando se debe ingresar en texto sin formato. De no ser así, el comando es rechazado.
- Los comandos de configuración con datos confidenciales cifrados, que están cifrados con la clave generada a partir de la frase clave local, están configurados en la configuración en ejecución. De lo contrario, el comando de configuración mostrará error y no se incorporará al archivo Configuración en ejecución.

Archivo de configuración de respaldo y de duplicado

Los dispositivos periódicamente generan su archivo de configuración de duplicado a partir del archivo de configuración de inicio si el servicio de configuración de duplicado está habilitado. Los dispositivos siempre generan un archivo de configuración de duplicado con datos confidenciales cifrados. Por lo tanto, el indicador SSD de archivo de un archivo de configuración de duplicado siempre indica que el archivo contiene datos confidenciales cifrados.

De manera predeterminada, el servicio de configuración de duplicado se encuentra habilitado. Para configurar los parámetros la configuración de duplicado automática a fin de que esté activada o desactivada, haga clic en **Administración > Administración de archivos > Propiedades de archivos de configuración**.

Los usuarios pueden mostrar, copiar y cargar los archivos de configuración de duplicado y de respaldo completos, sujetos a los permisos de lectura de SSD, el modo de lectura actual de la sesión y el indicador de archivo SSD del archivo de origen de la siguiente manera:

- Si no hay ningún indicador SSD de archivo en un archivo de configuración de duplicado o de respaldo, todos los usuarios pueden acceder al archivo.
- Los usuarios con ambos permisos de lectura pueden acceder a todos los archivos de configuración de duplicado y de respaldo. Sin embargo, si el modo de lectura actual de la sesión es diferente al indicador SSD de archivo, se le presenta una ventana al usuario una que indica que esta acción no está permitida.
- Los usuarios con permiso de solo texto sin formato pueden acceder a los archivos de configuración de duplicado y de respaldo si su indicador SSD de archivo muestra datos confidenciales excluir o solo de texto sin formato.
- Los usuarios con permiso de solo cifrado pueden acceder a los archivos de configuración de duplicado y de respaldo si su indicador SSD de archivo muestra datos confidenciales excluir o cifrado.
- Los usuarios con permiso excluir no pueden acceder a los archivos de configuración de duplicado y de respaldo si su indicador SSD de archivo muestra datos confidenciales cifrados o de texto sin formato.

El usuario no debe cambiar manualmente el indicador SSD de archivo que entra en conflicto con los datos confidenciales en el archivo. De lo contrario, los datos confidenciales de texto sin formato pueden quedar expuestos inesperadamente.

Configuración automática zero-touch de datos confidenciales

La configuración automática zero-touch de datos confidenciales es la configuración automática de los dispositivos de destino con datos confidenciales cifrados, sin la necesidad de configurar previamente y manualmente los dispositivos de destino con la frase clave cuya clave se utiliza para los datos confidenciales cifrados.

El dispositivo actualmente admite la configuración automática, que está habilitada de manera predeterminada. Cuando la configuración automática está habilitada en un dispositivo y este recibe opciones DHCP que especifican un servidor de archivo y un archivo de arranque, el dispositivo descarga el archivo de arranque (archivo de configuración remota) en el archivo de configuración de inicio de un servidor de archivo y, a continuación, se reinicia.

> **NOTA** El servidor del archivo puede estar especificado por los campos bootp siaddr y sname, así como por la opción DHCP 150 y configurados de forma estática en el dispositivo.

El usuario puede configurar dispositivos de destino con datos confidenciales cifrados de manera automática y segura, creando primero el archivo de configuración que será utilizado en la configuración automática de un dispositivo que contiene las configuraciones. El dispositivo debe estar configurado e instruido para que haga lo siguiente:

- cifrar los datos confidenciales en el archivo;
- aplicar la integridad del contenido del archivo e
- incluir los comandos seguros de configuración de autenticación y las reglas SSD que controlan y aseguran de manera adecuada el acceso a los dispositivos y a los datos confidenciales.

Si el archivo de configuración fue generado con la frase clave de un usuario y el control de la frase clave del archivo SSD es con restricciones, el archivo de configuración resultante puede configurarse automáticamente para los dispositivos de destino deseados. Sin embargo, para que la configuración automática resulte exitosa con una frase clave definida por el usuario, los dispositivos de destino deben estar configurados previamente y manualmente con la misma frase clave que el dispositivo que genera los archivos, que no es zero-touch.

Si el dispositivo que crea el archivo de configuración se encuentra en el modo de control de frase clave sin restricciones, el dispositivo incluye la frese clave en el archivo. Como resultado, el usuario puede configurar automáticamente los dispositivos de destino, incluidos los dispositivos configurados de fábrica o con configuración predeterminada de fábrica, con el archivo de configuración sin configurar previamente y manualmente los dispositivos de destino con la frase clave. Esto es zero-touch porque los dispositivos de destino obtienen la frase clave directamente a partir del archivo de configuración.

> **NOTA** Los dispositivos que tienen estados configurados de fábrica o con configuración predeterminada de fábrica utilizan el usuario anónimo predeterminado para acceder al servidor SCP.

Canales de administración de SSD

Los dispositivos pueden administrarse a través de los canales de administración, como telnet, SSH y Web. SSD divide a los canales en categorías de los siguientes tipos, según su seguridad o protocolos: seguro, inseguro, XML-SNMP seguro y XML-SNMP inseguro.

A continuación se describe si SSD considera que cada canal de administración es seguro o inseguro. Si es inseguro, la tabla indica el canal seguro paralelo.

Canal de administración	Tipo de canal de administración SSD	Canal de administración asegurado paralelo
Consola	Segura	
Telnet	No seguro	SSH
SSH	Segura	
GUI/HTTP	No seguro	GUI/HTTPS
GUI/HTTPS	Segura	
XML/HTTP	XML-SNMP no seguro	XML/HTTPS
XML/HTTPS	XML-SNMP seguro	
SNMPv1/v2/v3 sin privacidad	XML-SNMP no seguro	XML-SNMP seguro
SNMPv3 con privacidad	XML-SNMP seguro (usuarios de nivel 15)	
TFTP	No seguro	SCP
SCP (copia segura)	Segura	
Transferencia del archivo basada en HTTP	No seguro	Transferencia del archivo basada en HTTPS
Transferencia del archivo basada en HTTPS	Segura	

Menú CLI y recuperación de contraseña

La interfaz del menú CLI solo se permite a los usuarios si sus permisos de lectura son ambos o solo texto sin formato. Los demás usuarios son rechazados. Los datos confidenciales del menú CLI siempre se muestran como texto sin formato.

La recuperación de contraseña se encuentra activada actualmente desde el menú de arranque y permite que el usuario inicie la sesión en la terminal sin autenticación. Si se admite SSD, esta opción solo está permitida si la frase clave local es idéntica a la frase clave predeterminada. Si el dispositivo se configura con una frase clave definida por el usuario, el usuario no puede activar la recuperación de contraseña.

Configuración de SSD

La función SSD está configurada en las siguientes páginas:

- Las propiedades SSD se definen en la página Propiedades.
- Las reglas SSD se definen en la página Reglas SSD.

Propiedades SSD

Solo los usuarios que tienen permiso de lectura SSD de solo texto sin formato o ambos pueden establecer propiedades SSD.

Pasos para configurar las propiedades SSD globales:

PASO 1 Haga clic en **Seguridad** > **Gestión de datos confidenciales** > **Propiedades**. Aparece el siguiente campo:

- **Tipo de frase clave local actual**: muestra si actualmente se está utilizando una frase clave predeterminada o una frase clave definida por el usuario.

PASO 2 Ingrese los siguientes campos de **Configuración persistente**:

- **Control de frase clave del archivo de configuración**: seleccione una opción, como se describe en **Control de frase clave del archivo de configuración**.
- **Control de integridad del archivo de configuración**: selecciónelo para habilitar esta función. Consulte **Control de integridad del archivo de configuración**.

PASO 3 Seleccione un modo de lectura para la sesión actual (consulte **Elementos de una regla SSD**).

PASO 4 Haga clic en **Aplicar**. La configuración se guarda en el archivo Configuración en ejecución.

Pasos para cambiar la frase clave local:

PASO 1 Haga clic en **Cambiar frase clave local** e ingrese una **frase clave local** nueva:

- **Predeterminada**: se utiliza la frase clave predeterminada del dispositivo.

- **Definida por el usuario (texto sin formato)**: ingrese una frase clave nueva.
- **Confirmar frase clave**: confirme la nueva frase clave.

PASO 2 Haga clic en **Aplicar**. La configuración se guarda en el archivo Configuración en ejecución.

Reglas SSD Configuración

Solo los usuarios que tienen permiso de lectura SSD de solo texto sin formato o ambos pueden establecer reglas SSD.

Pasos para configurar reglas SSD:

PASO 1 Haga clic en **Seguridad** > **Gestión de datos confidenciales** > **Reglas**.

Se muestran las reglas definidas actualmente.

PASO 2 Para añadir una regla nueva, haga clic en **Añadir**. Ingrese los siguientes campos:

- **Usuario**: esto define a los usuarios a quienes se aplica la regla: seleccione una de las siguientes opciones:
  - *Usuario específico*: seleccione el nombre de usuario específico al que se aplica esta regla e ingréselo (no es necesario que este usuario sea definido).
  - *Usuario predeterminado (cisco)*: indica que la regla se aplica al usuario predeterminado.
  - *Nivel 15*: indica que esta regla se aplica a todos los usuarios que cuentan con el nivel de privilegio 15.
  - *Todos*: indica que esta regla se aplica a todos los usuarios.
- **Canal**: esto define el nivel de seguridad del canal de entrada al que se aplica la regla: seleccione una de las siguientes opciones:
  - *Seguro*: indica que esta regla se aplica solo a los canales seguros (consola, SCP, SSH y HTTPS); no se incluyen los canales SNMP y XML.
  - *Inseguro*: indica que esta regla se aplica solo a los canales inseguros (Telnet, TFTP y HTTP); no se incluyen los canales SNMP y XML.
  - *XML SNMP seguro*: indica que esta regla se aplica solo a XML a través de HTTPS y SNMPv3 con privacidad.
  - *XML SNMP inseguro*: indica que esta regla se aplica solo a XML a través de HTTP o SNMPv1/v2 y SNMPv3 sin privacidad.

- **Permiso de lectura**: los permisos de lectura se relacionan con la regla. Pueden ser los siguientes:
  - *Excluir*: permiso de lectura más bajo. Los usuarios no tienen permiso para obtener datos confidenciales de ninguna forma.
  - *Solo texto sin formato*: permiso de lectura más alto que los anteriores. Los usuarios tienen permiso para obtener datos confidenciales solo en texto sin formato.
  - *Solo cifrado*: permiso de lectura media. Los usuarios tienen permiso para obtener datos confidenciales solo como cifrados.
  - *Ambos (texto sin formato y cifrado)*: permiso de lectura más alto. Los usuarios tienen ambos permisos, de cifrado y de texto sin formato, y tienen permitido obtener los datos confidenciales como cifrados y en texto sin formato.
- **Modo lectura predeterminado**: todos los modos de lectura predeterminados están sujetos al permiso de lectura de la regla. Existen las siguientes opciones, pero algunas se pueden rechazar, según el permiso de lectura de la regla.
  - *Excluir*: no se permite la lectura de datos confidenciales.
  - *Cifrado*: los datos confidenciales se presentan en forma cifrada.
  - *Texto sin formato*: los datos confidenciales se presentan en forma de texto sin formato.

PASO 3 Haga clic en **Aplicar**. La configuración se guarda en el archivo Configuración en ejecución.

PASO 4 Se pueden realizar las siguientes acciones en algunas reglas:

- **Agregar**, **Editar** o **Eliminar** reglas
- **Restaurar valor predet.**: se restaura la regla predeterminada modificada por el usuario a la regla predeterminada.

23

Seguridad: Cliente SSH

En esta sección, se describe el dispositivo cuando funciona como cliente SSH.

Abarca los siguientes temas:

- **Copia segura (SCP) y SSH**
- **Métodos de protección**
- **Autenticación del servidor SSH**
- **Autenticación del cliente SSH**
- **Antes de empezar**
- **Tareas comunes**
- **Configuración del cliente SSH a través de la GUI**

Copia segura (SCP) y SSH

Copia segura o SSH es un protocolo de red que habilita el intercambio de datos entre un cliente SSH (en este caso, el dispositivo) y un servidor SSH en un canal seguro.

El cliente SSH ayuda al usuario a administrar una red compuesta por uno o más switches en los que se almacenan varios archivos de sistema en un servidor SSH central. Cuando los archivos de configuración son transferidos a través de una red, Copia segura (SCP), que es una aplicación que utiliza el protocolo SSH, asegura que los datos confidenciales, como el nombre de usuario/contraseña no pueden ser interceptados.

Copia segura (SCP) se utiliza para transferir de forma segura firmware, imágenes de inicio, archivos de configuración, archivos de idioma y archivos de registro de un servidor SCP central a un dispositivo.

Con respecto a SSH, la SCP en ejecución en el dispositivo es una aplicación de cliente SSH y el servidor SCP es una aplicación de servidor SSH.

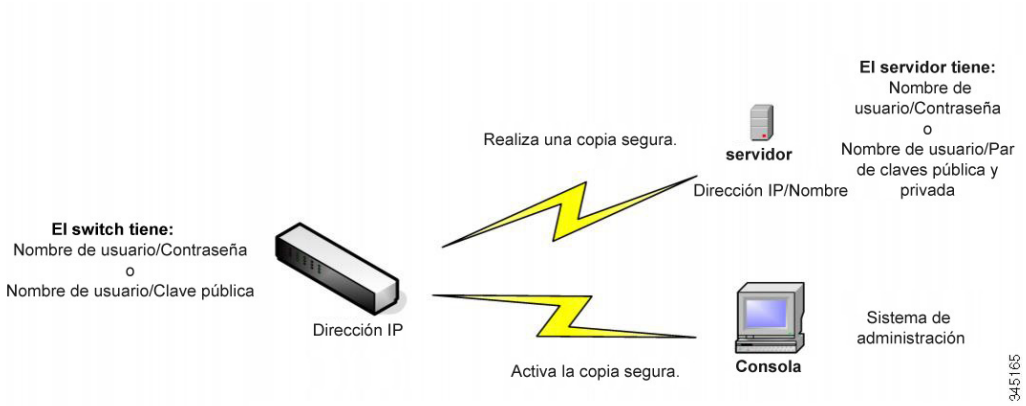
Cuando los archivos se descargan mediante TFTP o HTTP, la transferencia de datos es insegura.

Cuando los archivos se descargan mediante SCP, la información se descarga del servidor SCP al dispositivo mediante un canal seguro. La creación de este canal seguro está precedida de la autenticación, que asegura que el usuario tiene permiso para realizar la operación.

La información de autenticación debe ser ingresada por el usuario, tanto en el dispositivo como en el servidor SSH, a pesar de que en esta guía no se describen las operaciones del servidor.

A continuación, se muestra una configuración de red típica en la que se puede utilizar la función SCP.

Configuración de red típica



Métodos de protección

Cuando los datos se transfieren de un servidor SSH a un dispositivo (cliente), el servidor SSH utiliza varios métodos para la autenticación del cliente. Se describen a continuación.

Contraseñas

Para utilizar el método de contraseña, primero asegúrese de que se haya establecido un nombre de usuario/contraseña en el servidor SSH. Esto no se realiza a través del sistema de administración del dispositivo, aunque una vez que el nombre de usuario se haya establecido en el servidor, la contraseña del servidor se puede cambiar a través del sistema de administración del dispositivo.

El nombre de usuario o la contraseña se debe crear en el dispositivo. Cuando los datos se transfieren del servidor al dispositivo, el nombre de usuario y la contraseña suministrados por el dispositivo deben coincidir con el nombre de usuario y la contraseña del servidor.

Los datos se pueden cifrar utilizando una clave simétrica de uso único que se negocia durante la sesión.

Cada dispositivo que se administre debe tener su propio nombre de usuario y su propia contraseña, aunque se puede utilizar el mismo nombre de usuario o la misma contraseña para varios switches.

El método de contraseña es el método predeterminado del dispositivo.

Claves públicas/privadas

Para utilizar el método de clave pública/privada, cree un nombre de usuario y clave pública en el servidor SSH. La clave pública se genera en el dispositivo, como se describe a continuación, y después se copia al servidor. Las acciones de creación de un nombre de usuario en el servidor y copiado de una clave pública en el servidor no se describen en esta guía.

Los pares de claves predeterminados RSA y DSA se generan para el dispositivo cuando se inicia. Una de estas claves se utiliza para cifrar los datos que se descargan del servidor SSH. De forma predeterminada, se utiliza la clave RSA.

Si el usuario elimina una o dos de estas claves, se vuelven a generar.

Las claves públicas/privadas se cifran y se almacenan en la memoria del dispositivo. Las claves son parte del archivo de configuración del dispositivo, y la clave privada se puede mostrar al usuario en forma cifrada o de texto sin formato.

Debido a que la clave privada no se puede copiar a la clave privada de otro dispositivo de forma directa, existe un método de importación que permite copiar las claves privadas de dispositivo a dispositivo (que se describe en **Claves de importación**).

Claves de importación

En el método de clave, se deben crear claves individuales públicas/privadas para cada dispositivo individual, y estas claves privadas no se pueden copiar directamente de un dispositivo a otro debido a consideraciones de seguridad.

Si hay varios switches en la red, el proceso de creación de claves públicas/privadas de todos los switches puede llevar mucho tiempo porque se debe crear cada clave pública/privada y después, se deben cargar en el servidor SSH.

Para facilitar este proceso, hay una función adicional que permite la transferencia segura de la clave privada cifrada a todos los switches del sistema.

Cuando se crea una clave privada en un dispositivo, también es posible crear una *frase clave* relacionada. Esta frase clave se utiliza para cifrar la clave privada y para importarla a los switches restantes. De esta forma, todos los switches pueden utilizar la misma clave pública/privada.

Autenticación del servidor SSH

Un dispositivo, al igual que un cliente SSH, solo se comunica con un servidor SSH confiable. Cuando la autenticación del servidor SSH se encuentra deshabilitada (la configuración predeterminada) cualquier servidor SSH se considera confiable. Cuando se habilita la autenticación del servidor SSH, el usuario debe agregar una entrada para los servidores confiables en la tabla de servidores SSH confiables. Esta tabla almacena la siguiente información por cada servidor SSH confiable de un máximo de 16 servidores y contiene la siguiente información:

- Dirección IP/Nombre de host del servidor
- Huella dactilar de la clave pública del servidor

Cuando se activa la autenticación del servidor SSH, el cliente SSH en ejecución en el dispositivo autentica el servidor SSH utilizando el siguiente proceso de autenticación:

- El dispositivo calcula la huella dactilar de la clave pública del servidor SSH recibido.
- El dispositivo busca la tabla de servidores SSH confiables para la dirección IP o el nombre de host del servidor SSH. Puede ocurrir una de las siguientes situaciones:
  - Si se encuentra una coincidencia, tanto para la dirección IP o el nombre de host de servidor como para su huella dactilar, el servidor es autenticado.
  - Si se encuentra una dirección IP/un nombre de host que coincide, pero no hay una huella dactilar que coincida, la búsqueda continúa. Si no se encuentra ninguna huella dactilar que coincida, la búsqueda se completa y la autenticación falla.
  - Si no se encuentra ninguna dirección IP/ningún nombre de host que coincida, la búsqueda se completa y la autenticación falla.
- Si la entrada para el servidor SSH no se encuentra en la lista de servidores confiables, el proceso falla.

Autenticación del cliente SSH

La autenticación del cliente SSH a través de una contraseña se activa de forma predeterminada, con el usuario y la contraseña "anónimos".

El usuario debe configurar la siguiente información para la autenticación:

- El método de autenticación que se utilizará.
- El nombre de usuario/la contraseña o par de claves público/privado.

Para poder admitir la configuración automática de un dispositivo configurado de fábrica (dispositivo con configuración predeterminada de fábrica), la autenticación del servidor SSH está desactivada de forma predeterminada.

Algoritmos admitidos

Cuando se establece una conexión entre un dispositivo (como un cliente SSH) y un servidor SSD, el cliente y el servidor SSH intercambian datos para determinar los algoritmos con el fin de utilizarlos en la capa de transporte SSH.

Los siguientes algoritmos son admitidos en el lado del cliente:

- Intercambio de claves algoritmo-diffie-hellman
- Algoritmos de cifrado
  - aes128-cbc
  - 3des-cbc
  - arcfour
  - aes192-cbc
  - aes256-cbc
- Algoritmos de código de autenticación de mensajes
  - hmac-sha1
  - hmac-md5

NOTA No se admiten los algoritmos de compresión.

Antes de empezar

Se deben realizar las siguientes acciones antes de utilizar la función SCP:

- Al utilizar el método de autenticación de contraseña, se debe establecer un nombre de usuario/contraseña en el servidor SSH.
- Al utilizar un método de autenticación de clave pública/privada, la clave pública se debe almacenar en el servidor SSH.

Tareas comunes

En esta sección se describen algunas tareas comunes realizadas utilizando el cliente SSH. Todas las páginas a las que se hace referencia se pueden encontrar en la rama Cliente SSH del árbol de menú.

Flujo de trabajo 1: para configurar un cliente SSH y transferir datos a un servidor SSH o de este, siga los siguientes pasos:

PASO 1 Decida qué método se va a utilizar: contraseña o clave pública/privada. Utilice la página Autenticación del usuario SSH.

PASO 2 Si se seleccionó el método contraseña, siga los siguientes pasos:

a. Cree una contraseña global en la página Autenticación del usuario SSH o cree una temporal en la página Actualización/Copia de seguridad de firmware/Idioma o Copia de seguridad de configuración/Registro cuando realmente active la transferencia de datos seguros.

b. Actualice el firmware, la imagen de inicio o el archivo de idioma utilizando SCP y seleccionando la opción **a través de SCP (por medio de SSH)** en la página Actualización/Copia de seguridad de firmware/Idioma. La contraseña se puede ingresar directamente en esta página o se puede utilizar la contraseña ingresada en la página Autenticación del usuario SSH.

c. Descargue o realice una copia de seguridad del archivo de configuración utilizando SCP y seleccionando la opción **a través de SCP (por medio de SSH)** en la página Descarga/Copia de seguridad de configuración/Registro. La contraseña se puede ingresar directamente en esta página o se puede utilizar la contraseña ingresada en la página Autenticación del usuario SSH.

PASO 3 Establezca un nombre de usuario y una contraseña en el servidor SSH o modifique la contraseña del servidor SSH. Esta actividad depende del servidor y no se describe aquí.

PASO 4 Si se está utilizando el método de clave pública/privada, siga los siguientes pasos:

a. Seleccione si utilizará una clave RSA o DSA, cree un nombre de usuario y, a continuación, genere las claves públicas/privadas.

b. Vea la clave generada haciendo clic en el botón **Detalles**, y transfiera el nombre de usuario y la clave pública al servidor SSH. Esta acción depende del servidor y no se describe en esta guía.

c. Actualice o realice una copia de seguridad del firmware o del archivo de idioma utilizando SCP y seleccionando la opción **a través de SCP (por medio de SSH)** en la página Actualización/Copia de seguridad de firmware/Idioma.

d. Descargue o realice una copia de seguridad del archivo de configuración utilizando SCP y seleccionando la opción **a través de SCP (por medio de SSH)** en la página Descarga/Copia de seguridad de configuración/Registro.

Flujo de trabajo 2: para importar las claves públicas/privadas de un dispositivo a otro, haga lo siguiente:

PASO 1 Genere una clave pública/privada en la página Autenticación del usuario SSH.

PASO 2 Establezca las propiedades SSD y cree una frase clave local nueva en la página Gestión de datos confidenciales > Propiedades.

PASO 3 Haga clic en **Detalles** para ver las claves cifradas generadas y cópielas (incluidos los pies de página de inicio y de fin) de la página Detalles a un dispositivo externo. Copie las claves pública y privada por separado.

PASO 4 Inicie sesión en otro dispositivo y abra la página Autenticación del usuario SSH. Seleccione el tipo de clave requerida y haga clic en **Editar**. Pegue las claves privadas/públicas.

PASO 5 Haga clic en **Aplicar** para copiar las claves privadas/públicas en el segundo dispositivo.

Flujo de trabajo 3: para cambiar la contraseña de un servidor SSH, haga lo siguiente:

PASO 1 Identifique el servidor en la página Cambiar contraseña de usuario en el servidor SSH.

PASO 2 Escriba la nueva contraseña.

PASO 3 Haga clic en **Aplicar**.

Flujo de trabajo 4: para definir un servidor confiable, haga lo siguiente:

PASO 1 Active la autenticación de servidor SSH en la página Autenticación del usuario SSH.

PASO 2 Haga clic en **Añadir** para agregar un servidor nuevo e ingresar su información identificatoria.

PASO 3 Haga clic en **Aplicar** para agregar el servidor en la tabla de servidores SSH confiables.

Configuración del cliente SSH a través de la GUI

En esta sección se describen las páginas utilizadas para configurar la función Cliente SSH.

Autenticación del usuario SSH

Utilice esta página para seleccionar un método de autenticación de usuarios SSH, establecer un nombre de usuario y una contraseña en el dispositivo, si está seleccionado el método de contraseña o para generar una clave RSA o DSA si está seleccionado el método de claves pública/privada.

Para seleccionar un método de autenticación y establecer el nombre de usuario/la contraseña/las claves.

PASO 1 Haga clic en **Seguridad** > **Cliente SSH** > **Autenticación del usuario SSH**.

PASO 2 Seleccione un **Método de autenticación del usuario SSH**. Este es el método global definido para la copia segura (SCP). Seleccione una de las opciones:

- **Por contraseña**: este es el valor predeterminado. Si esta opción está seleccionada, ingrese una contraseña o mantenga la predeterminada.
- **Por clave pública RSA**: si esta opción está seleccionada, cree una clave pública y privada RSA en el bloque **Tabla de clave de usuario SSH**.
- **Por clave pública DSA**: si esta opción está seleccionada, cree una clave pública/privada DSA en el bloque **Tabla de clave de usuario SSH**.

PASO 3 Ingrese el **nombre de usuario** (sin importar el método que haya utilizado) o utilice el nombre de usuario predeterminado. Esto debe coincidir con el nombre de usuario definido en el servidor SSH.

PASO 4 Si se seleccionó el método *Por contraseña*, ingrese una contraseña (**Cifrada** o **Texto sin formato**) o deje la contraseña cifrada predeterminada.

PASO 5 Realice una de las siguientes acciones:

- **Aplicar**: se relacionan los métodos de autenticación seleccionados con el método de acceso.
- **Restaurar credenciales predeterminadas**: se restauran el nombre de usuario y contraseña (anónimo).
- **Mostrar datos confidenciales como texto simple**: los datos confidenciales de la página actual se muestran como texto sin formato.

En la **Tabla de clave de usuario SSH**, se muestran los siguientes campos para cada clave:

- **Tipo de clave**: RSA o DSA.
- **Origen de la clave**: generada automáticamente o definida por el usuario.
- **Huella dactilar**: huella dactilar generada a partir de la clave.

PASO 6 Para manejar una clave RSA o DSA, seleccione RSA o DSA y realice una de las siguientes acciones:

- **Generar**: generar una clave nueva.
- **Editar**: mostrar las claves para copiarlas/pegarlas a otro dispositivo.
- **Eliminar**: eliminar la clave.
- **Detalles**: muestra las claves.

Autenticación del servidor SSH

Para habilitar una autenticación de servidor SSH y definir los servidores confiables, haga lo siguiente:

PASO 1 Haga clic en **Seguridad** > **Cliente SSH** > **Autenticación del servidor SSH**.

PASO 2 Seleccione **Habilitar** para habilitar la autenticación del servidor SSH.

- **Interfaz de origen IPv4**: seleccione la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen en los mensajes usados para la comunicación con los servidores SSH IPv4.
- **Interfaz de origen IPv6**: seleccione la interfaz de origen cuya dirección IPv6 se utilizará como dirección IPv6 de origen en los mensajes usados para la comunicación con los servidores SSH IPv6.

NOTA Si se selecciona la opción Automática, el sistema toma la dirección IP de origen de la dirección IP definida en la interfaz de salida.

PASO 3 Haga clic en **Añadir** e ingrese los siguientes campos para el servidor SSH confiable:

- **Definición del servidor**: seleccione una de las siguientes maneras para identificar el servidor SSH:
  - *Por dirección IP*: si esta opción está seleccionada, ingrese la dirección IP del servidor en los campos a continuación.
  - *Por nombre*: si esta opción está seleccionada, ingrese el nombre del servidor en el campo **Dirección IP/Nombre del servidor**.
- **Versión de IP**: si seleccionó especificar el servidor SSH por dirección IP, indique si esa dirección IP es IPv4 o IPv6.
- **Tipo de dirección IP**: si la dirección IP del servidor SSH es IPv6, seleccione el tipo de dirección IPv6. Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de FE80, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.

- **Interfaz de enlace local**: seleccione la interfaz de enlace local en la lista de interfaces.
- **Dirección IP/Nombre del servidor**: ingrese la dirección IP del servidor SSH o su nombre, según lo que seleccione en **Definición del servidor**.
- **Huella dactilar**: ingrese la huella dactilar del servidor SSH (copiado de ese servidor).

PASO 4 Haga clic en **Aplicar**. La definición del servidor confiable se almacena en el archivo Configuración en ejecución.

Modificación de la contraseña del usuario en el servidor SSH

Para cambiar la contraseña de un servidor SSH, haga lo siguiente:

PASO 1 Haga clic en **Seguridad** > **Cliente SSH** > **Cambiar contraseña de usuario en el servidor SSH**.

PASO 2 Ingrese los siguientes campos:

- **Definición del servidor**: defina el servidor SSH seleccionando **Por dirección IP** o **Por nombre**. Ingrese el nombre del servidor o la dirección IP del servidor en el campo **Dirección IP/Nombre del servidor**.
- **Versión de IP**: si seleccionó especificar el servidor SSH por dirección IP, indique si esa dirección IP es IPv4 o IPv6.
- **Tipo de dirección IP**: si la dirección IP del servidor SSH es IPv6, seleccione el tipo de dirección IPv6. Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de FE80, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz de enlace local**: seleccione la interfaz de enlace local en la lista de interfaces.
- **Dirección IP/Nombre del servidor**: ingrese la dirección IP del servidor SSH o su nombre, según lo que seleccione en **Definición del servidor**.
- **Nombre de usuario**: debe coincidir con el nombre de usuario del servidor.
- **Antigua contraseña**: debe coincidir con la contraseña del servidor.
- **Nueva contraseña**: ingrese la contraseña nueva y confírmela en el campo **Confirmar contraseña**.

PASO 3 Haga clic en **Aplicar**. Se modifica la contraseña del servidor SSH.

24

Seguridad: Servidor SSH

En esta sección se describe cómo establecer una sesión SSH en el dispositivo.

Abarca los siguientes temas:

- **Información general**
- **Tareas comunes**
- **Páginas de configuración del servidor SSH**

Información general

La función del servidor SSH permite a los usuarios crear una sesión SSH para el dispositivo. Esto es similar a establecer una sesión telnet, con la excepción de que la sesión se asegura.

Las claves públicas y privadas se generan automáticamente en el dispositivo. Esto puede ser modificado por el usuario.

La sesión SSH se abre utilizando una aplicación de cliente SSH especial, como PuTTY.

El servidor SSH puede funcionar en los siguientes modos:

- **A través de claves RSA/DSA generadas en forma interna (configuración predeterminada)**: se generan una clave RSA y una DSA. Los usuarios inician sesión en la aplicación del servidor SSH y son autenticados automáticamente para abrir una sesión en el dispositivo cuando suministran la dirección IP del dispositivo.
- **Modo clave pública**: los usuarios se definen en el dispositivo. Sus claves RSA/DSA se generan en una aplicación de servidor SSH externa, como PuTTY. Las claves públicas se ingresan en el dispositivo. Los usuarios después pueden abrir una sesión SSH en el dispositivo a través de la aplicación externa del servidor SSH.

Tareas comunes

En esta sección se describen algunas tareas comunes realizadas utilizando la función del servidor SSH.

Flujo de trabajo 1: para iniciar sesión en el dispositivo por medio de SSH con la clave del dispositivo creada automáticamente (predeterminada), realice lo siguiente:

PASO 1 Active el servidor SSH en la página Servicios TCP/UDP y verifique que la autenticación del usuario SSH por clave pública esté desactivada en la página Autenticación del usuario SSH.

PASO 2 Inicie sesión en una aplicación de cliente SSH externa, como PuTTY, utilizando la dirección IP del dispositivo (no es necesario usar un nombre de usuario o una clave que sean conocidos para el dispositivo).

Flujo de trabajo 2: para crear un usuario SSH e iniciar sesión en el dispositivo por medio de SSH utilizando este usuario, siga los siguientes pasos:

PASO 1 Genere una clave RSA o DSA en una aplicación de cliente SSH externa, como PuTTY.

PASO 2 Active la autenticación del usuario SSH por clave pública o contraseña en la página Autenticación del usuario SSH.

PASO 3 Active el inicio de sesión automático si lo requiere (consulte **Inicio de sesión automático** a continuación).

PASO 4 Agregue un usuario en la página Autenticación del usuario SSH y copie la clave pública generada de manera externa.

PASO 5 Inicie sesión en una aplicación de cliente SSH externa, como PuTTY, utilizando la dirección IP del dispositivo y el nombre de usuario del usuario.

Flujo de trabajo 3: para importar una clave RSA o DSA del dispositivo A al dispositivo B, siga los siguientes pasos:

PASO 1 En el dispositivo A, seleccione una clave RSA o DSA en la página Autenticación del servidor SSH.

PASO 2 Haga clic en **Detalles** y copie la clave pública del tipo de clave seleccionado en Bloc de notas u otra aplicación similar de editor de texto.

PASO 3 Inicie sesión en el dispositivo B y abra la página Autenticación del usuario SSH. Seleccione la clave RSA o la DSA, haga clic en **Editar** y pegue la clave del dispositivo A.

Páginas de configuración del servidor SSH

En esta sección, se describen las páginas utilizadas para configurar la función **Servidor SSH**.

Autenticación del usuario SSH

Utilice la página Autenticación del usuario SSH para activar la autenticación del usuario SSH por clave pública o contraseña y (cuando se use la autenticación por clave pública) para agregar un usuario de cliente SSH que se usará para crear una sesión SSH en una aplicación SSH externa (como PuTTY).

Para poder agregar un usuario, debe generar una clave RSD o DSA para el usuario en la aplicación de cliente/generación de claves SSH externa (como PuTTY).

Inicio de sesión automático

Si usa la página Autenticación del usuario SSH para crear un nombre de usuario SSH para un usuario que ya está configurado en la base de datos local del usuario, puede evitar otro tipo de autenticación al configurar la función **Inicio de sesión automático**, que funciona de la siguiente manera:

- **Habilitado**: si hay un usuario definido en la base de datos local y este usuario pasa la autenticación SSH con una clave pública, se omite la autenticación por el nombre de usuario y la contraseña de la base de datos local.

  NOTA El método de autenticación configurado para este método de administración específico (consola, Telnet, SSH, etc.) debe ser *Local* (es decir, no *RADIUS* ni *TACACS+*). Consulte **Método de acceso a administración** para obtener más detalles.

- **No habilitado**: después de realizar correctamente la autenticación por clave pública SSH, el usuario se autentica nuevamente de acuerdo con los métodos de autenticación configurados en la página Autenticación de acceso a administración, incluso si el nombre de usuario está configurado en la base de datos local del usuario.

Esta página es opcional. No es necesario que trabaje con autenticación de usuarios en SSH.

Pasos para habilitar la autenticación y agregar un usuario.

PASO 1 Haga clic en **Seguridad** > **Servidor SSH** > **Autenticación del usuario SSH**.

PASO 2 Seleccione los siguientes campos:

- **Autenticación de usuario SSH mediante contraseña**: seleccione esta opción para realizar la autenticación del usuario de cliente SSH con el nombre de usuario o la contraseña configurados en la base de datos local (consulte **Definición de usuarios**).

- **Autenticación de usuario SSH por clave pública**: seleccione esta opción para realizar la autenticación del usuario de cliente SSH con una clave pública.
- **Inicio de sesión automático**: este campo puede activarse si se selecciona la función **Autenticación de usuario SSH por clave pública**. Consulte **Inicio de sesión automático**.

PASO 3 Haga clic en **Aplicar**. La configuración se guarda en el archivo Configuración en ejecución.

Para los usuarios configurados, se muestran los siguientes campos:

- **Nombre de usuario SSH**: nombre de usuario del usuario.
- **Tipo de clave**: indica si es una clave RSA o DSA.
- **Huella dactilar**: huella dactilar generada a partir de las claves públicas.

PASO 4 Haga clic en **Añadir** para agregar un usuario nuevo e ingrese los campos:

- **Nombre de usuario SSH**: ingrese un nombre de usuario.
- **Tipo de clave**: seleccione **RSA** o **DSA**.
- **Clave pública**: copie la clave pública generada por una aplicación de cliente SSH externa (como PuTTY) en este cuadro de texto.

PASO 5 Haga clic en **Aplicar** para guardar el nuevo usuario.

Para todos los usuarios activos se muestran los siguientes campos:

- **Dirección IP**: la dirección IP del usuario activo.
- **Nombre de usuario SSH**: nombre de usuario del usuario activo.
- **Versión de SSH**: versión del SSH que utiliza el usuario activo.
- **Cifrado**: cifrado del usuario activo.
- **Código de autenticación**: código de autenticación del usuario activo.

Autenticación del servidor SSH

Cuando el dispositivo se inicia desde la configuración predeterminada de fábrica, se genera automáticamente una clave pública y privada RSA y DSA. Cada clave también se crea automáticamente cuando el usuario elimina la clave configurada por el usuario adecuada.

Pasos para volver a generar una clave RSA o DSA o para copiar una clave RSA/DSA generada en otro dispositivo:

PASO 1 Haga clic en **Seguridad** > **Servidor SSH** > **Autenticación del servidor SSH**.

Se muestran los siguientes campos para cada clave:

- **Tipo de clave**: RSA o DSA.
- **Origen de la clave**: generada automáticamente o definida por el usuario.
- **Huella dactilar**: huella dactilar generada a partir de la clave.

PASO 2 Seleccione una clave RSA o DSA.

PASO 3 Puede realizar cualquiera de las siguientes acciones:

- **Generar**: genera una clave del tipo especificado.
- **Editar**: le permite copiar una clave a partir de otro dispositivo.
- **Eliminar**: le permite eliminar una clave.
- **Detalles**: le permite ver la clave generada. La ventana Detalles también le permite hacer clic en **Mostrar datos confidenciales como texto sin formato**. Si esto está marcado, las claves se muestran como texto sin formato y no en forma cifrada. Si la clave ya se muestra como texto sin formato, puede hacer clic en **Mostrar datos confidenciales como cifrado** para mostrar el texto en forma cifrada.

25

Control de acceso

La función Lista de control de acceso (ACL) es parte del mecanismo de seguridad. Las definiciones de ACL sirven como uno de los mecanismos para definir flujos de tráfico a los que se da una Calidad de Servicio (QoS) específica. Para obtener más información, consulte **Calidad del servicio**.

Las ACL permiten a los administradores de red definir patrones (filtros y acciones) para el tráfico de ingreso. Los paquetes, que ingresan al dispositivo en un puerto o LAG con una ACL activa, se admiten o se rechazan.

Esta sección contiene los siguientes temas:

- **Listas de control de acceso**
- **ACL basadas en MAC**
- **ACL basadas en IPv4**
- **ACL basadas en IPv6**
- **Vinculación de ACL**

Listas de control de acceso

Una Lista de control de acceso (ACL) es una lista ordenada de acciones y filtros de Clasificación. Cada regla de clase, junto con la acción, se denomina Elemento de control de acceso (ACE).

Cada ACE está formado por filtros que distinguen grupos de tráfico y acciones asociadas. Una sola ACL puede contener uno o más ACE, que se comparan con el contenido de las tramas entrantes. A las tramas cuyo contenido coincide con el filtro, se les aplica una acción para RECHAZAR o PERMITIR.

El dispositivo admite un máximo de 512 ACL y un máximo de 512 ACE.

Cuando un paquete coincide con un filtro ACE, se toma la acción ACE y se detiene el procesamiento de esa ACL. Si el paquete no coincide con el filtro ACE, se procesa el siguiente ACE. Si todos los ACE de una ACL se han procesado sin encontrar una coincidencia, y si existe otra ACL, esta se procesa de manera similar.

NOTA Si no se encuentra coincidencia con ningún ACE en todas las ACL relevantes, el paquete se descarta (como acción predeterminada). Debido a esta acción de descarte predeterminada, usted debe agregar los ACE explícitamente en la ACL para permitir el tráfico deseado, como Telnet, HTTP o SNMP, que se dirige al dispositivo. Por ejemplo, si no desea descartar todos los paquetes que no coinciden con las condiciones de un ACL, debe agregar un ACE con la prioridad más baja explícitamente en la ACL que permite todo el tráfico.

Si se activa la indagación de IGMP/MLD en un puerto conectado a la ACL, agregue filtros ACE en la ACL para reenviar paquetes IGMP/MLD al dispositivo. De lo contrario, la indagación de IGMP/MLD fracasa en el puerto.

El orden de los ACE dentro de la ACL es importante, debido a que se aplican según el algoritmo del primer ajuste (first-fit). Los ACE se procesan secuencialmente, comenzando por el primer ACE.

Las ACL se pueden usar para seguridad, por ejemplo, si se permiten o se rechazan ciertos flujos de tráfico, y también para la clase de tráfico y la priorización en el modo Avanzado de QoS.

NOTA Un puerto se puede asegurar con las ACL o se puede configurar con una política de QoS avanzada.

Solo puede haber una ACL por puerto, con la excepción de que se puede asociar una ACL basada en IP y una ACL basada en IPv6 con un solo puerto.

Para asociar más de una ACL con un puerto, se debe usar una política con uno o más mapas de clase.

Los siguientes tipos de ACL se pueden definir (según qué parte del encabezado de la trama se examine):

- ACL de MAC: solo examina campos de Capa 2, como se describe en *Definición de ACL basadas en MAC*
- ACL de IP: examina la capa 3 de las tramas IP, como se describe en *ACL basadas en IPv4*
- ACL de IPv6: examina la capa 3 de tramas IPv4, como se describe en *Definición de ACL basada en IPv6*

Si una trama coincide con el filtro en una ACL, se define como flujo con el nombre de esa ACL. En QoS avanzada, estas tramas se pueden mencionar mediante este Nombre de flujo, y la QoS se puede aplicar a estas tramas.

Registro ACL

Esta función permite agregar una opción de registro a los ACE. Cuando se activa esta función, los paquetes que ACE haya permitido o denegado generan un mensaje SYSLOG informativo relacionado.

Si está activado el registro ACL, puede especificarse por interfaz mediante la asociación de la ACL con una interfaz. En ese caso, se generan mensajes SYSLOG para los paquetes que coinciden con los ACE de permiso o denegación relacionados con la interfaz.

Se define un flujo, como un flujo de paquetes con características idénticas, de la siguiente manera:

- **Paquetes de Capa 2**: direcciones MAC de origen y destino idénticas.
- **Paquetes de Capa 3**: direcciones IP de origen y destino idénticas.
- **Paquetes de Capa 4**: puerto L4 e IP de origen y destino idénticos.

Para cualquier flujo nuevo, el primer paquete capturado de una interfaz específica provoca la generación de un mensaje SYSLOG informativo. Los otros paquetes del mismo flujo son capturados al CPU, pero los mensajes SYSLOG para este flujo se limitan a un mensaje cada 5 minutos. Este SYSLOG informa que al menos un paquete se capturó en los últimos 5 minutos.

Luego de manejar el paquete capturado, los paquetes se reenvían si tienen permiso, o se descartan si los deniegan.

La cantidad de flujos admitidos por unidad es 150.

SYSLOG

Los mensajes SYSLOG tienen gravedad informativa e indican si el paquete coincidió con una regla de denegación o permiso.

- Para los paquetes de Capa 2, el SYSLOG incluye la siguiente información (si corresponde): MAC de origen, MAC de destino, Ethertype, ID de VLAN y cola de CoS.
- Para los paquetes de Capa 3, el SYSLOG incluye la siguiente información (si corresponde): IP de origen, IP de destino, protocolo, valor DSCP, tipo de ICMP, código de ICMP y tipo de IGMP.
- Para los paquetes de Capa 4, el SYSLOG incluye la siguiente información (si corresponde): puerto de origen, puerto de destino e indicador TCP.

A continuación, se muestran algunos ejemplos de posibles SYSLOG:

- Para un paquete no IP:
  - 06-Jun-2013 09:49:56 %3SWCOS-I-LOGDENYMAC: gi0/1: deny ACE 00:00:00:00:00:01 -> ff:ff:ff:ff:ff:ff, Ethertype-2054, VLAN-20, CoS-4, trapped
- Para un paquete IP (v4 y v6):
  - 06-Jun-2013 12:38:53 %3SWCOS-I-LOGDENYINET: gi0/1: deny ACE IPv4(255) 1.1.1.1 -> 1.1.1.10, protocol-1, DSCP-54, ICMP Type-Echo Reply, ICMP code-5, trapped
- Para un paquete L4:
  - 06-Jun-2013 09:53:46 %3SWCOS-I-LOGDENYINETPORTS: gi0/1: deny ACE IPv4(TCP) 1.1.1.1(55) -> 1.1.1.10(66), trapped

Cómo configurar ACL

En esta sección, se describe cómo crear ACL y agregarles reglas (ACE).

Creación de un flujo de trabajo de ACL

Para crear ACL y asociarlas con una interfaz, haga lo siguiente:

1. Cree uno o más de los siguientes tipos de ACL:
   a. ACL basada en MAC mediante la página ACL basada en MAC y la página ACE basado en MAC
   b. ACL basada en IP mediante la página ACL basada en IPv4 y la página ACE basado en IPv4
   c. ACL basada en IPv6 mediante la página ACL basada en IPv6 y la página ACE basado en IPv6
2. Asocie la ACL con las interfaces mediante la página Vinculación de ACL.

Modificación de un flujo de trabajo de ACL

Una ACL solo se puede modificar si no está en uso. A continuación se describe el proceso de desvinculación de una ACL para modificarla:

1. Si la ACL no pertenece a un mapa de clase en Modo avanzado de QoS, pero se ha asociado con una interfaz, desvincúlela de la interfaz mediante la página *Vinculación de ACL*.
2. Si la ACL es parte del mapa de clase y no está vinculado a una interfaz, entonces puede modificarse.
3. Si la ACL es parte de un mapa de clase que se encuentra en una política vinculada a una interfaz, debe realizar la cadena de desvinculación de la siguiente manera:
   - Desvincule la política que contiene el mapa de clase de la interfaz mediante página *Vinculación de política*.
   - Elimine el mapa de clase que contiene la ACL de la política mediante *Configuración de una política* (**Editar**).
   - Elimine el mapa de clase que contiene la ACL mediante *Definición de asignación de clases*.

Solo entonces se podrá modificar la ACL, como se describe en esta sección.

ACL basadas en MAC

Las ACL basadas en MAC se usan para filtrar el tráfico basado en campos de Capa 2 y verifican todas las tramas para ver si coinciden.

Las ACL basadas en MAC se definen en la página ACL basada en MAC. Las reglas se definen en la página ACE basado en MAC.

Para definir una ACL basada en MAC:

PASO 1 Haga clic en **Control de acceso** > **ACL basada en MAC**.

Esta página contiene una lista de todas las ACL basadas en MAC que se encuentran definidas actualmente.

PASO 2 Haga clic en **Add**.

PASO 3 En el campo **Nombre de ACL**, ingrese el nombre de la nueva ACL. Los nombres de ACL distinguen entre mayúsculas y minúsculas.

PASO 4 Haga clic en **Aplicar**. La ACL basada en MAC se guarda en el archivo de configuración en ejecución.

Incorporación de reglas a una ACL basada en MAC

NOTA Cada regla basada en MAC consume una regla de TCAM. Tenga en cuenta que la asignación de TCAM se realiza en pares: para el primer ACE, se asignan 2 reglas de TCAM; la segunda regla de TCAM se asigna al siguiente ACE, y así sucesivamente.

Para agregar reglas (ACE) a una ACL:

PASO 1 Haga clic en **Control de acceso** > **ACE basado en MAC**.

PASO 2 Seleccione una ACL y haga clic en **Ir**. Se detallan los ACE de la ACL.

PASO 3 Haga clic en **Add**.

PASO 4 Ingrese los parámetros.

- **Nombre de ACL**: muestra el nombre de la ACL a la que se agrega el ACE.
- **Prioridad**: ingrese la prioridad del ACE. Los ACE con mayor prioridad se procesan primero. Uno es la mayor prioridad.
- **Acción**: seleccione la acción para una coincidencia. Las opciones son:
  - *Permitir*: reenviar los paquetes que cumplen con los criterios del ACE.
  - *Denegar*: descartar los paquetes que cumplen con los criterios del ACE.
  - *Apagar*: descartar los paquetes que cumplen con los criterios del ACE, y deshabilitar el puerto de donde se recibieron los paquetes. Estos puertos se pueden reactivar en la página Configuración de puertos.

- **Registro**: seleccione para activar el registro de flujos de ACL que coinciden con la regla de ACL.
- **Intervalo de tiempo**: seleccione esta opción para habilitar que se limite el uso de la ACL en un intervalo de tiempo específico.
- **Nombre del intervalo de tiempo**: si la opción **Intervalo de tiempo** está seleccionada, seleccione el intervalo de tiempo que se utilizará. Los intervalos de tiempo están definidos en la sección **Configuración de la hora del sistema**.
- **Dirección MAC de destino**: seleccione *Cualquier (dirección)* si todas las direcciones de destino son aceptables o *Definida por el usuario* para ingresar una dirección de destino o un rango de direcciones de destino.
- **Valor de dirección MAC de destino**: ingrese una dirección MAC con la cual se hará coincidir la dirección MAC de destino y su máscara (si es pertinente).
- **Máscara comodín de MAC de destino**: ingrese la máscara para definir un rango de direcciones MAC. Tenga en cuenta que esta máscara es distinta de otros usos, como la máscara de subred. En este caso, la configuración de un bit como **1** indica que no importa y **0** indica que se debe enmascarar ese valor.

  NOTA Si se da una máscara de 0000 0000 0000 0000 0000 0000 1111 1111 (significa que usted hace coincidir los bits en los que existe un valor de 0 y que no hace coincidir los bits en los que existe un valor de 1). Debe convertir los 1 en un entero decimal y escribir un 0 cada cuatro ceros. En este ejemplo, puesto que 1111 1111 = 255, la máscara se debe escribir de la siguiente manera: 0.0.0.255.
- **Dirección MAC de origen**: seleccione *Cualq.* si todas las direcciones de origen son aceptables o *Definido por el usuario* para ingresar una dirección de origen o un rango de direcciones de origen.
- **Valor de dirección MAC de origen**: ingrese una dirección MAC con la cual se hará coincidir la dirección MAC de origen y su máscara (si es pertinente).
- **Máscara comodín de MAC de origen**: ingrese la máscara para definir un rango de direcciones MAC.
- **ID de VLAN**: ingrese la sección ID de VLAN de la etiqueta VLAN para hacer coincidir.
- **802.1p**: seleccione **Incluir** para usar 802.1p.
- **Valor 802.1p**: ingrese el valor 802.1p para agregarlo a la etiqueta VPT.
- **Máscara 802.1p**: ingrese la máscara comodín para aplicarla a la etiqueta VPT.
- **Ethertype**: ingrese el Ethertype de la trama para hacer coincidir.

PASO 5 Haga clic en **Aplicar**. El ACE basado en MAC se guarda en el archivo de configuración en ejecución.

ACL basadas en IPv4

Las ACL basadas en IPv4 se usan para verificar paquetes IPv4, mientras que otros tipos de tramas, como los ARP, no se verifican.

Se pueden hacer coincidir los siguientes campos:

- Protocolo IP (por nombre para los protocolos conocidos, o directamente por valor)
- Puertos de origen/destino para el tráfico TCP/UDP
- Valores de indicadores para tramas TCP
- Código y tipo de ICMP e IGMP
- Direcciones IP de origen/destino (incluidos los comodines)
- Valor de precedencia DSCP/IP

NOTA Las ACL también se usan como elementos de construcción de definiciones de flujo para el manejo de QoS por flujo.

La página ACL basada en IPv4 permite agregar ACL al sistema. Las reglas se definen en la página ACE basado en IPv4.

Las ACL basadas en IPv6 se definen en la página ACL basada en IPv6.

Definición de una ACL basada en IPv4

Para definir una ACL basada en IPv4:

PASO 1 Haga clic en **Control de acceso** > **ACL basada en IPv4**.

Esta página contiene todas las ACL basadas en IPv4 que se encuentran definidas actualmente.

PASO 2 Haga clic en **Add**.

PASO 3 En el campo **Nombre de ACL**, ingrese el nombre de la nueva ACL. Los nombres distinguen entre mayúsculas y minúsculas.

PASO 4 Haga clic en **Aplicar**. La ACL basada en IPv4 se guarda en el archivo de configuración en ejecución.

Incorporación de reglas (ACE) a una ACL basada en IPv4

NOTA Cada regla basada en IPv4 consume una regla de TCAM. Tenga en cuenta que la asignación de TCAM se realiza en pares: para el primer ACE, se asignan 2 reglas de TCAM; la segunda regla de TCAM se asigna al siguiente ACE, y así sucesivamente.

Para agregar reglas (ACE) a una ACL basada en IPv4:

PASO 1 Haga clic en **Control de acceso** > **ACE basado en IPv4**.

PASO 2 Seleccione una ACL y haga clic en **Ir**. Se muestran todos los ACE de IP actualmente definidos para la ACL seleccionada.

PASO 3 Haga clic en **Add**.

PASO 4 Ingrese los parámetros.

- **Nombre de ACL**: muestra el nombre de la ACL.
- **Prioridad**: ingrese la prioridad. Los ACE con mayor prioridad se procesan primero.
- **Acción**: seleccione la acción asignada al paquete que coincide con el ACE. Las opciones son las siguientes:
  - *Permitir*: reenviar los paquetes que cumplen con los criterios del ACE.
  - *Denegar*: descartar los paquetes que cumplen con los criterios del ACE.
  - *Cerrar*: descartar el paquete que cumple con los criterios del ACE, y deshabilitar el puerto a donde se dirigió el paquete. Los puertos se reactivan en la página Administración de puertos.
- **Registro**: seleccione para activar el registro de flujos de ACL que coinciden con la regla de ACL.
- **Intervalo de tiempo**: seleccione esta opción para habilitar que se limite el uso de la ACL en un intervalo de tiempo específico.
- **Nombre del intervalo de tiempo**: si la opción **Intervalo de tiempo** está seleccionada, seleccione el intervalo de tiempo que se utilizará. Los intervalos de tiempo están definidos en la sección **Configuración de la hora del sistema**.
- **Protocolo**: seleccione crear un ACE basado en una ID de protocolo o protocolo específico. Seleccione *Cualquier (IPv4)* para aceptar todos los protocolos IP. De lo contrario, seleccione uno de los siguientes protocolos de la lista desplegable **Seleccionado de la lista**:
  - *ICMP*: Internet Control Message Protocol (Protocolo de mensajes de control de Internet)
  - *IGMP*: Internet Group Management Protocol (Protocolo de administración de grupos de Internet)

- *IP en IP*: encapsulación IP en IP
- *TCP*: Transmission Control Protocol (Protocolo de control de transmisión)
- *EGP*: Exterior Gateway Protocol (Protocolo de gateway exterior)
- *IGP*: Interior Gateway Protocol (Protocolo de gateway interior)
- *UDP*: User Datagram Protocol (Protocolo de datagrama de usuario)
- *HMP*: Host Mapping Protocol (Protocolo de mapping de host)
- *RDP*: Reliable Datagram Protocol (Protocolo de datagrama confiable).
- *IDPR*: Inter-Domain Policy Routing Protocol (Protocolo de enrutamiento de políticas entre dominios)
- *IPV6*: tunelización de IPv6 por IPv4
- *IPV6:ROUT*: hace coincidir paquetes pertenecientes a la ruta IPv6 con la ruta IPv4 a través de una gateway
- *IPV6:FRAG*: hace coincidir paquetes pertenecientes a IPv6 con el encabezado de fragmentación IPv4
- *IDRP*: Inter-Domain Routing Protocol (Protocolo de enrutamiento entre dominios)
- *RSVP*: ReSerVation Protocol (Protocolo de reserva)
- *EA*: Encabezamiento de autenticación
- *IPV6:ICMP*: Internet Control Message Protocol (Protocolo de mensajes de control de Internet)
- *EIGRP*: Enhanced Interior Gateway Routing Protocol (Protocolo de enrutamiento de gateway interior mejorado)
- *OSPF*: Abrir la ruta de acceso más corta primero
- *IPIP*: IP en IP
- *PIM*: Protocol Independent Multicast (Multidifusión independiente de protocolo)
- *L2TP*: Layer 2 Tunneling Protocol (protocolo de tunelización de capa 2)
- *ISIS*: IGP-specific Protocol (Protocolo IGP específico)
- *ID de Protocolo para coincidencia*: en vez de seleccionar el nombre, ingrese el ID de protocolo.

- **Dirección IP de origen**: seleccione *Cualquier (dirección)* si todas las direcciones de origen son aceptables o *Definida por el usuario* para ingresar una dirección de origen o un rango de direcciones de origen.
- **Valor de dirección IP de origen**: ingrese la dirección IP con la que se hará coincidir la dirección IP de origen.

- **Máscara comodín de IP de origen**: ingrese la máscara para definir un rango de direcciones IP. Tenga en cuenta que esta máscara es distinta de otros usos, como la máscara de subred. En este caso, la configuración de un bit como 1 indica que no importa y 0 indica que se debe enmascarar ese valor.

  NOTA Si se da una máscara de 0000 0000 0000 0000 0000 0000 1111 1111 (significa que usted hace coincidir los bits en los que existe un valor de 0 y que no hace coincidir los bits en los que existe un valor de 1). Debe convertir los 1 en un entero decimal y escribir un 0 cada cuatro ceros. En este ejemplo, puesto que 1111 1111 = 255, la máscara se debe escribir de la siguiente manera: 0.0.0.255.

- **Dirección IP de destino**: seleccione *Cualquier (dirección)* si todas las direcciones de destino son aceptables o *Definida por el usuario* para ingresar una dirección de destino o un rango de direcciones de destino.
- **Valor de dirección IP de destino**: ingrese la dirección IP con la que se hará coincidir la dirección IP de destino.
- **Máscara comodín de IP de destino**: ingrese la máscara para definir un rango de direcciones IP.
- **Puerto de origen**: seleccione una de las siguientes opciones:
  - *Cualquier (puerto)*: coincidencia con todos los puertos de origen.
  - *Uno de la lista*: seleccione un solo puerto de origen TCP/UDP con el que se hacen coincidir los paquetes. El campo está activo solo si se selecciona 800/6-TCP o 800/17-UDP en el menú desplegable Seleccionar de la lista.
  - *Uno del número*: ingrese un solo puerto de origen TCP/UDP con el que se hacen coincidir los paquetes. El campo está activo solo si se selecciona 800/6-TCP o 800/17-UDP en el menú desplegable Seleccionar de la lista.
  - *Rango*: seleccione un rango de puertos de origen TCP/UDP con los que se hace coincidir el paquete. Hay ocho rangos de puertos distintos que pueden configurarse (compartidos entre puertos de origen y destino). Cada protocolo TCP y UDP tiene ocho rangos de puertos.
- **Puerto de destino**: seleccione uno de los valores disponibles que son los mismos que para el campo Puerto de Origen descrito anteriormente.

  NOTA Debe especificar el protocolo IP para el ACE antes de ingresar el puerto de origen o destino.

- **Indicadores TCP**: seleccione uno o más indicadores TCP con los cuales filtrar los paquetes. Los paquetes filtrados se reenvían o se descartan. El filtrado de paquetes mediante indicadores TCP aumenta el control de los paquetes, lo que aumenta la seguridad de la red.
- **Tipo de servicio**: **el tipo de servicio del paquete IP.**
  - *Cualquier (tipo)*: cualquier tipo de servicio
  - *DSCP para coincidencia*: Punto de código de servicios diferenciados (DSCP) para hacer coincidir

- *Precedencia IP para hacer coincidir*: la precedencia IP es un modelo de tipo de servicio (TOS) que la red utiliza para proporcionar los compromisos QoS apropiados. Este modelo utiliza los tres bits más significativos del byte del tipo de servicio en el encabezado IP, como se describe en RFC 791 y RFC 1349.

- **ICMP**: si el protocolo IP de la ACL es ICMP, seleccione el tipo de mensaje ICMP utilizado para fines de filtrado. Seleccione el tipo de mensaje por nombre, o bien, ingrese el número de tipo de mensaje:
  - *Cualquier (tipo)*: se aceptan todos los tipos de mensajes.
  - *Seleccionar de la lista*: seleccione el tipo de mensaje por nombre.
  - *Tipo ICMP para coincidencia*: número de tipo de mensaje para usar para fines de filtrado.
- **Código ICMP**: los mensajes ICMP pueden tener un campo de código que indica cómo manejar el mensaje. Seleccione una de las siguientes opciones para configurar si se debe aplicar filtro a este código:
  - *Cualquier (código)*: aceptar todos los códigos.
  - *Definida por el usuario*: ingrese un código ICMP para fines de filtrado.
- **IGMP**: si la ACL se basa en IGMP, seleccione el tipo de mensaje IGMP para usar para fines de filtrado. Seleccione el tipo de mensaje por nombre, o bien, ingrese el número de tipo de mensaje:
  - *Cualquier (tipo)*: se aceptan todos los tipos de mensajes.
  - *Seleccionar de la lista*: seleccione el tipo de mensaje por nombre.
  - *Tipo IGMP para coincidencia*: número de tipo de mensaje que se usará para fines de filtrado.

PASO 5 Haga clic en **Aplicar**. El ACE basado en IPv4 se guarda en el archivo de configuración en ejecución.

ACL basadas en IPv6

La página ACL basada en IPv6 contiene y permite la creación de ACL basadas en IPv6, que verifican el tráfico basado en IPv6 puro. Las ACL IPv6 no verifican los paquetes ARP ni los IPv6 por IPv4.

NOTA Las ACL también se usan como elementos de construcción de definiciones de flujo para el manejo de QoS por flujo.

Definición de una ACL basada en IPv6

Para definir una ACL basada en IPv6:

PASO 1 Haga clic en **Control de acceso** > **ACL basada en IPv6**.

Esta ventana contiene la lista de ACL definidas y su contenido.

PASO 2 Haga clic en **Add**.

PASO 3 En el campo **Nombre de ACL**, ingrese el nombre de la nueva ACL. Los nombres distinguen entre mayúsculas y minúsculas.

PASO 4 Haga clic en **Aplicar**. La ACL basada en IPv6 se guarda en el archivo de configuración en ejecución.

Incorporación de reglas (ACE) para una ACL basada en IPv6

NOTA Cada regla basada en IPv6 consume dos reglas de TCAM.

PASO 1 Haga clic en **Control de acceso** > **ACE basado en IPv6**.

Esta ventana contiene el ACE (reglas) para una ACL específica (grupo de reglas).

PASO 2 Seleccione una ACL y haga clic en **Ir**. Se muestran todos los ACE de IP actualmente definidos para la ACL seleccionada.

PASO 3 Haga clic en **Add**.

PASO 4 Ingrese los parámetros.

- **Nombre de ACL**: muestra el nombre de la ACL a la que se agrega el ACE.
- **Prioridad**: ingrese la prioridad. Los ACE con mayor prioridad se procesan primero.
- **Acción**: seleccione la acción asignada al paquete que coincide con el ACE. Las opciones son las siguientes:
  - *Permitir*: reenviar los paquetes que cumplen con los criterios del ACE.
  - *Denegar*: descartar los paquetes que cumplen con los criterios del ACE.
  - *Cerrar*: descartar los paquetes que cumplen con los criterios del ACE, y deshabilitar el puerto a donde se dirigieron los paquetes. Los puertos se reactivan en la página Administración de puertos.
- **Registro**: seleccione para activar el registro de flujos de ACL que coinciden con la regla de ACL.

- **Intervalo de tiempo**: seleccione esta opción para habilitar que se limite el uso de la ACL en un intervalo de tiempo específico.
- **Nombre del intervalo de tiempo**: si la opción **Intervalo de tiempo** está seleccionada, seleccione el intervalo de tiempo que se utilizará. Los intervalos de tiempo se describen en la sección **Configuración de la hora del sistema**.
- **Protocolo**: seleccione para crear un ACE basado en un protocolo específico. Seleccione *Cualquier (IPv6)* para aceptar todos los protocolos IP. De lo contrario, seleccione uno de los siguientes protocolos:
  - *TCP*: Transmission Control Protocol (Protocolo de control de transmisión). Permite que dos hosts se comuniquen e intercambien flujos de datos. El TCP garantiza la entrega de paquetes, y que los paquetes se transmitan y se reciban en el orden en el que han sido enviados.
  - *UDP*: User Datagram Protocol (Protocolo de datagrama de usuario). Transmite paquetes pero no garantiza su entrega.
  - *ICMP*: hace coincidir los paquetes con el Internet Control Message Protocol (ICMP, Protocolo de mensajes de control de Internet).
- **ID de Protocolo para coincidencia**: ingrese el ID del protocolo con el que se debe hacer coincidir.
- **Dirección IP de origen**: seleccione *Cualquier (dirección)* si todas las direcciones de origen son aceptables o *Definida por el usuario* para ingresar una dirección de origen o un rango de direcciones de origen.
- **Valor de dirección IP de origen**: ingrese una dirección IP con la cual se hará coincidir la dirección IP de origen y su máscara (si es pertinente).
- **Longitud del prefijo IP de origen**: ingrese la longitud de prefijo de la dirección IP de origen.
- **Dirección IP de destino**: seleccione *Cualquier (dirección)* si todas las direcciones de destino son aceptables o *Definida por el usuario* para ingresar una dirección de destino o un rango de direcciones de destino.
- **Valor de dirección IP de destino**: ingrese una dirección IP con la cual se hará coincidir la dirección MAC de destino y su máscara (si es pertinente).
- **Longitud del prefijo IP de destino**: ingrese la longitud de prefijo de la dirección IP.
- **Puerto de origen**: seleccione una de las siguientes opciones:
  - *Cualquier (puerto)*: coincidencia con todos los puertos de origen.
  - *Uno de la lista*: seleccione un solo puerto de origen TCP/UDP con el que se hacen coincidir los paquetes. El campo está activo solo si se selecciona 800/6-TCP o 800/17-UDP en el menú desplegable Protocolo IP.

- *Uno del número*: ingrese un solo puerto de origen TCP/UDP con el que se hacen coincidir los paquetes. El campo está activo solo si se selecciona 800/6-TCP o 800/17-UDP en el menú desplegable Protocolo IP.
- *Rango*: seleccione un rango de puertos de origen TCP/UDP con los que se hace coincidir el paquete.

- **Puerto de destino**: seleccione uno de los valores disponibles. (Son los mismos que para el campo Puerto de origen descrito anteriormente).

  NOTA Debe especificar el protocolo IPv6 para la ACL antes de poder configurar el puerto de origen o destino.

- **Indicadores TCP**: seleccione uno o más indicadores TCP con los cuales filtrar los paquetes. Los paquetes filtrados se reenvían o se descartan. El filtrado de paquetes mediante indicadores TCP aumenta el control de los paquetes, lo que aumenta la seguridad de la red.
  - Establecido: hacer coincidir si el indicador está configurado en ESTABLECIDO.
  - No establecido: hacer coincidir si el indicador está configurado en NO ESTABLECIDO.
  - No importa: ignorar el indicador TCP.
- **Tipo de servicio**: el tipo de servicio del paquete IP.
- **ICMP**: si la ACL se basa en ICMP, seleccione el tipo de mensaje ICMP que se usa para fines de filtrado. Seleccione el tipo de mensaje por nombre, o bien, ingrese el número de tipo de mensaje. Si se aceptan todos los tipos de mensajes, seleccione *Cualquier (tipo)*.
  - *Cualquier (tipo)*: se aceptan todos los tipos de mensajes.
  - *Seleccionar de la lista*: seleccione el tipo de mensaje por nombre de la lista desplegable.
  - *Tipo de IGMP para coincidencia*: número de tipo de mensaje que se usará para fines de filtrado.
- **Código ICMP**: los mensajes ICMP pueden tener un campo de código que indica cómo manejar el mensaje. Seleccione una de las siguientes opciones para configurar si se debe aplicar el filtro a este código:
  - *Cualquier (código)*: aceptar todos los códigos.
  - *Definida por el usuario*: ingrese un código ICMP para fines de filtrado.

PASO 5 Haga clic en **Aplicar**.

Vinculación de ACL

Cuando una ACL está vinculada con una interfaz (puerto, LAG o VLAN), sus reglas ACE se aplican a paquetes que llegan a la interfaz. Los paquetes que no coinciden con ningún ACE de la ACL se hacen coincidir con una regla predeterminada, cuya acción es descartar los paquetes que no tienen coincidencias.

Si bien cada interfaz se puede vincular con una sola ACL, se pueden vincular varias interfaces con la misma ACL si se agrupan en una asignación de políticas y esa asignación de políticas se vincula con la interfaz.

Después de que una ACL se vincula con una interfaz, no se puede editar, modificar ni eliminar hasta que se borre de todos los puertos con los que está vinculada o en uso.

NOTA Es posible vincular una interfaz (puerto, LAG o VLAN) con una política o a un ACL, pero no pueden vincularse tanto con una política como con una ACL.

Para vincular una ACL con una VLAN:

PASO 1 Haga clic en **Control de acceso** > **Vinculación de ACL (VLAN)**.

PASO 2 Seleccione una VLAN y haga clic en **Editar**.

Si la VLAN que requiere no se visualiza, agregue una nueva.

PASO 3 Seleccione uno de los siguientes:

- **Seleccionar ACL basada en MAC**: seleccione una ACL basada en MAC para vincular con la interfaz.
- **Seleccionar ACL basada en IPv4**: seleccione una ACL basada en IPv4 para vincular con la interfaz.
- **Seleccionar ACL basada en IPv6**: seleccione una ACL basada en IPv6 para vincular con la interfaz.
- **Acción predeterminada**: seleccione una de las siguientes opciones:
  - *Rechazar cualquiera*: si el paquete no coincide con una ACL, es rechazado (descartado).
  - *Permitir cualquiera*: si el paquete no coincide con una ACL, es permitido (reenviado).

  NOTA La opción Acción predeterminada se puede definir únicamente si la Protección de la IP de origen no está activada en la interfaz.

PASO 4 Haga clic en **Aplicar**. La vinculación de ACL se modifica y se actualiza el archivo Configuración en ejecución.

NOTA Si no se selecciona ninguna ACL, las ACL que se han vinculado previamente con la VLAN se desvinculan.

Para vincular un ACL con un puerto o LAG:

PASO 1 Haga clic en **Control de acceso** > **Vinculación de ACL (Puerto)**.

PASO 2 Seleccione un tipo de interfaz **Puertos/LAG** (Puerto o LAG).

PASO 3 Haga clic en **Ir**. Para cada tipo de interfaz que se selecciona, se muestran todas las interfaces de ese tipo con una lista de sus ACL actuales.

- **Interfaz**: identificador o interfaz en la que está definida la ACL.
- **ACL de MAC**: ACL de tipo MAC que están vinculadas con la interfaz (si las hubiere).
- **ACL de IPv4**: ACL de tipo IPv4 que están vinculadas con la interfaz (si las hubiere).
- **ACL de IPv6**: ACL de tipo IPv6 que están vinculadas con la interfaz (si las hubiere).
- **Acción predeterminada**: acción de las reglas ACL (descartar cuaqluiera/permitir cualquiera).

NOTA Para desvincular todas las ACL de una interfaz, seleccione la interfaz, y luego haga clic en **Borrar**.

PASO 4 Seleccione una interfaz, y haga clic en **Editar**.

PASO 5 Seleccione uno de los siguientes:

- **Seleccionar ACL basada en MAC**: seleccione una ACL basada en MAC para vincular con la interfaz.
- **Seleccionar ACL basada en IPv4**: seleccione una ACL basada en IPv4 para vincular con la interfaz.
- **Seleccionar ACL basada en IPv6**: seleccione una ACL basada en IPv6 para vincular con la interfaz.
- **Acción predeterminada**: seleccione una de las siguientes opciones:
  - *Rechazar cualquiera*: si el paquete no coincide con una ACL, es rechazado (descartado).
  - *Permitir cualquiera*: si el paquete no coincide con una ACL, es permitido (reenviado).

NOTA La opción Acción predeterminada se puede definir únicamente si la Protección de la IP de origen no está activada en la interfaz.

PASO 6 Haga clic en **Aplicar**. La vinculación de ACL se modifica y se actualiza el archivo Configuración en ejecución.

NOTA Si no se selecciona ninguna ACL, las ACL que se han vinculado previamente con la interfaz se desvinculan.

26

Calidad del servicio

La función Calidad de servicio se aplica en toda la red para garantizar que el tráfico de red se priorice de acuerdo con los criterios requeridos y que el tráfico deseado reciba un trato preferencial.

Esta sección abarca los siguientes temas:

- **Funciones y componentes de QoS**
- **Configuración de QoS - General**
- **Modo básico de QoS**
- **Modo avanzado de QoS**
- **Administración de estadísticas de QoS**

Funciones y componentes de QoS

La función de QoS se utiliza para optimizar el rendimiento de la red.

QoS proporciona lo siguiente:

- Clasificación del tráfico entrante en clases de tráfico, según los atributos, que incluyen:
  - Configuración del dispositivo
  - Interfaz de acceso
  - Contenido del paquete
  - Combinación de estos atributos

QoS incluye lo siguiente:

- **Clasificación del tráfico**: clasifica cada paquete entrante como perteneciente a un flujo de tráfico específico, según los contenidos del paquete o el puerto. La ACL (Access Control List, lista de control de acceso) se encarga de realizar la clasificación; solamente el tráfico que cumpla con los criterios de ACL estará sujeto a la clasificación CoS o QoS.
- **Asignación de filas de espera de hardware**: los paquetes entrantes se asignan a filas de espera de reenvío. Los paquetes se envían a una fila de espera en particular para manejarlos como una función de la clasificación de tráfico a la que pertenecen. Consulte **Configuración de filas de espera de QoS**.
- **Otros atributos de manejo de clasificación de tráfico**: se aplican mecanismos de QoS a varias clasificaciones, incluida la administración del ancho de banda.

Funcionamiento de QoS

El tipo de campo del encabezado en que debe confiarse se ingresa en la página Configuración global. Para cada valor de ese campo, se asigna una fila de espera de egreso, que indica mediante qué fila de espera se envía la trama, en la página CoS/802.1p a la fila de espera o la página DSCP a la fila de espera (según si el modo de confianza es CoS/802.1p o DSCP, respectivamente).

Modos de QoS

El modo de QoS seleccionado se aplica a todas las interfaces del sistema.

- **Modo básico**: Clase de servicio (CoS).

  Todo el tráfico de la misma clase recibe el mismo trato, que es la única acción de QoS para determinar la fila de espera de egreso en el puerto de egreso, en función del valor de QoS indicado en la trama entrante. Puede ser el valor 802.1p de la etiqueta de prioridad de VLAN (VPT) en la capa 2 y el valor del punto de código de servicios diferenciados (DSCP) para IPv4 o el valor de la clase de tráfico (TC) para IPv6 en la capa 3. Al funcionar en modo básico, el dispositivo confía en este valor externo asignado de QoS. El valor externo asignado de QoS de un paquete determina su clase de tráfico y QoS.

  El campo del encabezado en que debe confiarse se ingresa en la página Configuración global. Para cada valor en ese campo, se asigna una fila de espera de egreso a donde se envía la trama en la página CoS/802.1p a la fila de espera o la página DSCP a la fila de espera (según si el modo de confianza es CoS/802.1p o DSCP, respectivamente).

- **Modo avanzado**: Calidad de servicio (QoS) por flujo.

  En modo avanzado, una QoS por flujo consta de una asignación de clasificación y un regulador:

  - Una asignación de clasificación define el tipo de tráfico en un flujo y contiene una o más ACL. Los paquetes que coinciden con las ACL pertenecen al flujo.
  - Un regulador aplica la QoS configurada a un flujo. La configuración de QoS de un flujo puede constar de la fila de espera de egreso, el valor DSCP o CoS/802.1p y acciones sobre el tráfico fuera de perfil (exceso).

- **Deshabilitar modo**: en este modo, todo el tráfico se asigna a una sola fila de espera de mejor esfuerzo, de modo que ningún tipo de tráfico tenga prioridad sobre otro.

Solo puede haber un modo activo a la vez. Cuando el sistema está configurado para funcionar en el modo avanzado de QoS, la configuración para el modo básico de QoS no está activa y viceversa.

Al cambiar el modo, ocurre lo siguiente:

- Cuando se cambia del modo avanzado de QoS a cualquier otro modo, se eliminan las definiciones de perfiles de política y las asignaciones de clasificación. Las ACL vinculadas directamente a las interfaces permanecen vinculadas.
- Al cambiar del modo básico de QoS al modo avanzado, no se conserva la configuración del modo de confianza de QoS en el modo básico.
- Al desactivar QoS, se restablecen los valores predeterminados del modelador y la fila de espera (configuración del ancho de banda de ordenamiento cíclico ponderado/prioridad estricta [WRR/SP]).

El resto de las configuraciones de usuario permanecen intactas.

Flujo de trabajo de QoS

Para configurar los parámetros generales de QoS, realice lo siguiente:

PASO 1 Seleccione el modo QoS (básico, avanzado o deshabilitado, como se describe en la sección **"Modos QoS"**) para el sistema a través de la página Propiedades de QoS. Los siguientes pasos del flujo de trabajo suponen que seleccionó habilitar QoS.

PASO 2 Asigne a cada interfaz una prioridad CoS predeterminada mediante la página Propiedades de QoS.

PASO 3 Asigne el método de programación (prioridad estricta o WRR) y la asignación del ancho de banda para WRR a las filas de espera de egreso a través de la página Fila de espera.

PASO 4 Designe una fila de espera de egreso para cada valor de DSCP/TC IP con la página DSCP a la fila de espera. Si el dispositivo está en el modo de confianza DSCP, los paquetes entrantes se colocan en las filas de espera de egreso según su valor DSCP/TC.

PASO 5 Designe una fila de espera de egreso para cada prioridad de CoS/802.1p. Si el dispositivo está en el modo de confianza CoS/802.1, todos los paquetes entrantes se colocan en las filas de espera de egreso designadas, según la prioridad de CoS/802.1p en los paquetes. Esto se hace mediante la página CoS/802.1p a la fila de espera.

PASO 6 Si es necesario solo para el tráfico de Capa 3, asigne una fila de espera a cada valor DSCP/TC a través de la página DSCP a la fila de espera.

PASO 7 Ingrese los límites de ancho de banda y velocidad en las siguientes páginas:

a. Configure el moldeado saliente por fila de espera mediante la página Moldeado saliente por fila de espera.

b. Configure el límite de velocidad de ingreso y la velocidad de moldeado saliente por puerto a través de la página Ancho de banda.

PASO 8 Configure el modo seleccionado a través de una de las siguientes opciones:

a. Configure el modo Básico, según se describe en *Flujo de trabajo para configurar modo QoS básico*.

b. Configure el modo Avanzado, según se describe en *Flujo de trabajo para configurar modo QoS avanzado*.

Configuración de QoS - General

La página Propiedades de QoS incluye campos para configurar el modo de QoS del sistema (básico, avanzado o deshabilitado, como se describe en la sección **"Modos QoS"**). Además, se puede definir la prioridad predeterminada de CoS para cada interfaz.

Configuración de propiedades de QoS

Para seleccionar el modo de QoS:

PASO 1 Haga clic en **Calidad de servicio** > **General** > **Propiedades de QoS**.

PASO 2 Seleccione el modo de QoS. Las opciones disponibles son las siguientes:

- **Deshabilitar**: se deshabilita QoS en el dispositivo.
- **Básico**: se deshabilita QoS en el dispositivo en modo básico.
- **Avanzado**: se deshabilita QoS en el dispositivo en modo Avanzado.

PASO 3 Seleccione **Puerto/LAG** y haga clic en **IR A** para ver o modificar todos los puertos o LAG en el dispositivo y su información de CoS.

Aparecen los siguientes campos para todos los puertos/LAG:

- **Interfaz**: tipo de interfaz.
- **CoS predeterminada**: valor predeterminado de VPT para los paquetes entrantes que no tienen una etiqueta VLAN. La CoS predeterminada es 0. El valor predeterminado es solo relevante para las tramas sin etiquetas, y solo si el sistema está en modo básico y la opción CoS de confianza está seleccionada en la página Configuración global.

Seleccione **Restaurar valores predet.** para restaurar la configuración predeterminada de fábrica de CoS para esta interfaz.

Para configurar QoS en una interfaz, selecciónela y haga clic en **Editar**.

PASO 1 Ingrese los parámetros.

- **Interfaz**: seleccione un puerto o LAG.
- **CoS predeterminada**: seleccione el valor predeterminado de CoS (Clasificación de servicio) que se asignará a los paquetes entrantes (que no tengan una etiqueta VLAN).

PASO 2 Haga clic en **Aplicar**. El valor predeterminado de CoS de la interfaz se guarda en el archivo de configuración en ejecución.

Configuración de filas de espera de QoS

El dispositivo admite 4 para cada interfaz. La fila de espera número cuatro es la de mayor prioridad, mientras que la fila de espera número uno es la de menor prioridad.

Existen dos formas de determinar cómo se maneja el tráfico en las filas de espera: Prioridad estricta y Ordenamiento cíclico ponderado (WRR).

- **Prioridad estricta**: el tráfico de egreso de la fila de espera de mayor prioridad se transmite en primer lugar. El tráfico de las filas de espera inferiores se procesa solo después de que la fila de espera superior se haya transmitido. De esta manera, se proporciona el mayor nivel de prioridad del tráfico a la fila de espera con número más alto.
- **Ordenamiento cíclico ponderado (WRR, Weighted Round Robin)**: en el modo WRR, el número de paquetes enviados desde la fila de espera es proporcional al peso de la fila de espera (cuanto mayor es el peso, se envía mayor cantidad de tramas). Por ejemplo, si hay un máximo de cuatro filas de espera posibles y todas están en WRR y se utilizan los pesos predeterminados, la fila de espera 1 recibe 1/15 del ancho de banda (si suponemos que todas las filas de espera están saturadas y que hay congestión), la fila de espera 2 recibe 2/15, la fila de espera 3 recibe 4/15 y la fila de espera 4 recibe 8/15 del ancho de banda. El tipo de algoritmo de WRR utilizado en el dispositivo no es el WRR con déficit (DWRR) estándar, sino el WRR deficitado (SDWRR).

Los modos de almacenamiento en fila de espera pueden seleccionarse en la página Fila de espera. Cuando el modo de almacenamiento en fila de espera es por prioridad estricta, la prioridad establece el orden en que se procesan las filas de espera: se comienza con la fila de espera 4 o la fila de espera 8 (la de mayor prioridad) y se continúa con la siguiente fila de espera inferior tras completar cada fila de espera.

Cuando el modo de almacenamiento en fila de espera es por ordenamiento cíclico ponderado, las filas de espera se procesan hasta que se haya agotado su cuota, y luego se procesa otra fila de espera.

También es posible asignar algunas de las filas de espera inferiores a WRR, mientras se mantienen algunas de las filas de espera superiores en prioridad estricta. En este caso, el tráfico para las filas de espera de prioridad estricta siempre se envía antes que el tráfico de las filas de espera de WRR. El tráfico de las filas de espera de WRR se reenvía solo una vez que se hayan vaciado las filas de espera de prioridad estricta. (La porción relativa de cada fila de espera de WRR depende de su peso).

Para seleccionar el método de prioridad e ingresar datos de WRR:

PASO 1 Haga clic en **Calidad de servicio** > **General** > **Fila de espera**.

PASO 2 Ingrese los parámetros.

- **Fila de espera**: se muestra el número de fila de espera.

- **Método de planificación:** Elija una de las siguientes opciones:
  - *Prioridad estricta*: la programación del tráfico para la fila de espera seleccionada y todas las filas de espera superiores se basa estrictamente en la prioridad de la fila de espera.
  - *WRR*: la programación del tráfico para la fila de espera seleccionada se basa en WRR. El período de tiempo se divide entre las filas de espera de WRR que no estén vacías, lo que significa que tienen descriptores para el egreso. Esto sucede solo si las filas de espera de prioridad estricta están vacías.
  - *Peso de WRR*: si WRR está seleccionado, ingrese el peso de WRR asignada a la fila de espera.
  - *% de ancho de banda de WRR*: se muestra la cantidad de ancho de banda asignado a la fila de espera. Estos valores representan el porcentaje del peso de WRR.

PASO 3 Haga clic en **Aplicar**. Se configuran filas de espera y se actualiza el archivo Configuración en ejecución.

Asignación de CoS/802.1p a la fila de espera

En la página CoS/802.1p a la fila de espera, se asignan las prioridades de 802.1p a las filas de espera de egreso. La tabla de CoS/802.1p a una fila de espera determina las filas de espera de egreso de los paquetes entrantes en función de la prioridad de 802.1p en sus etiquetas VLAN. Para los paquetes entrantes sin etiquetar, la prioridad de 802.1p es la prioridad predeterminada de CoS/802.1p asignada a los puertos de ingreso.

La siguiente tabla describe la asignación predeterminada cuando hay 4 filas de espera:

Valor 802.1p (0 a 7, donde 7 es el mayor)	Fila de espera (4 filas de espera 1 a 4, donde 4 es la de mayor prioridad)	Notas
0	1	Fondo
1	1	Mejor esfuerzo
2	2	Excelente esfuerzo
3	3	Aplicación esencial: SIP de teléfono LVS
4	3	Video
5	4	Voz: valor predeterminado de teléfono IP de Cisco

Valor 802.1p (0 a 7, donde 7 es el mayor)	Fila de espera (4 filas de espera 1 a 4, donde 4 es la de mayor prioridad)	Notas
6	4	Control de interconexión: RTP de teléfono LVS
7	4	Control de red

Al cambiar la asignación de CoS/802.1p a la fila de espera (CoS/802.1p a la fila de espera) y la asignación del ancho de banda y del método de programación de la fila de espera (página Fila de espera), es posible obtener la calidad de servicio deseada en una red.

La asignación de CoS/802.1p a la fila de espera se aplica solo si existe una de las siguientes condiciones:

- El dispositivo está en el modo básico de QoS y en el modo de confianza CoS/802.1p.
- El dispositivo está en el modo avanzado de QoS y los paquetes pertenecen a flujos de confianza CoS/802.1p.

La fila de espera 1 tiene la prioridad más baja; la fila de espera 4 u 8 tiene la prioridad más alta.

Para asignar valores de CoS a filas de espera de egreso:

PASO 1 Haga clic en **Calidad de servicio** > **General** > **CoS/802.1p a fila de espera**.

PASO 2 Ingrese los parámetros.

- **802.1p**: se muestran los valores de las etiquetas de prioridad de 802.1p que se asignarán a una fila de espera de egreso, donde 0 es la menor prioridad y 7 es la mayor prioridad.
- **Fila de espera de salida**: seleccione la fila de espera de egreso a la que la prioridad de 802.1p está asignada. Se admiten cuatro u ocho filas de espera de egreso, donde la fila de espera 4 o la fila de espera 8 es la fila de espera de egreso de mayor prioridad y la fila de espera 1 es la de menor prioridad.

PASO 3 Para cada prioridad de 802.1p, seleccione la fila de espera de salida a la que está asignada.

PASO 4 Haga clic en **Aplicar, Cancelar** o **Restaurar valores predet**. Se asignan los valores de prioridad de 801.1p a las filas de espera y se actualiza el archivo Configuración en ejecución. Los cambios que se hayan ingresado se cancelan, o bien, se restauran los valores previamente definidos.

Asignación de DSCP a la fila de espera

La página DSCP a la fila de espera permite asignar valores de DSCP de IP a filas de espera de egreso. La tabla DSCP a la fila de espera permite determinar las filas de espera de egreso de los paquetes IP entrantes en función de sus valores DSCP. La VPT (etiqueta de prioridad VLAN) original del paquete no se modifica.

Al cambiar la asignación de DSCP a la fila de espera y la asignación del ancho de banda y el método de programación de la fila de espera, es posible obtener la calidad de servicio deseada en una red.

La asignación de DSCP a la fila de espera se aplica a los paquetes IP si:

- El dispositivo está en el modo básico de QoS y DSCP es el modo de confianza.
- O bien, el dispositivo está en el modo avanzado de QoS y los paquetes pertenecen a flujos de confianza DSCP.

Los paquetes que no son IP siempre se clasifican en la fila de espera de mejor esfuerzo.

En las siguientes tablas, se describe la asignación de DSCP a la fila de espera predeterminada para sistemas de 4 filas de espera:

DSCP	63	55	47	39	31	23	15	7
Fila de espera	3	3	4	3	3	2	1	1
DSCP	62	54	46	38	30	22	14	6
Fila de espera	3	3	4	3	3	2	1	1
DSCP	61	53	45	37	29	21	13	5
Fila de espera	3	3	4	3	3	2	1	1
DSCP	60	52	44	36	28	20	12	4
Fila de espera	3	3	4	3	3	2	1	1
DSCP	59	51	43	35	27	19	11	3
Fila de espera	3	3	4	3	3	2	1	1
DSCP	58	50	42	34	26	18	10	2
Fila de espera	3	3	4	3	3	2	1	1
DSCP	57	49	41	33	25	17	9	1
Fila de espera	3	3	4	3	3	2	1	1
DSCP	56	48	40	32	24	16	8	0
Fila de espera	3	3	4	3	3	2	1	1

Para asignar DSCP a filas de espera:

PASO 1 Haga clic en **Calidad de servicio** > **General** > **DSCP a la fila de espera**.

La página DSCP a la fila de espera contiene **Acceder a DSCP**, que muestra el valor DSCP en el paquete entrante y su clasificación asociada.

PASO 2 Seleccione la fila de espera de salida en **Fila de espera de salida** (fila de espera de reenvío de tráfico) a la que el valor DSCP está asignado.

PASO 3 Seleccione **restaurar configuración predeterminada** para restaurar la configuración predeterminada de fábrica de CoS para esta interfaz.

PASO 4 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Configuración del ancho de banda

En la página Ancho de banda, los usuarios pueden definir dos conjuntos de valores, Límite de velocidad de ingreso y Velocidad de moldeado saliente, que determinan la cantidad de tráfico que el sistema puede recibir y enviar.

El límite de velocidad de ingreso es el número de bits por segundo que se pueden recibir de la interfaz de ingreso. El exceso de ancho de banda por encima de este límite se descarta.

Se ingresan los siguientes valores para el moldeado saliente:

- **Velocidad de información comprometida (CIR)** establece la cantidad promedio máxima de datos que se permite enviar en la interfaz de egreso, medida en bits por segundo.
- **Tamaño de ráfaga comprometida (CBS)** es la ráfaga de datos que se permite enviar, aunque esté por encima de la CIR. Se define en número de bytes de datos.

Para ingresar la limitación del ancho de banda:

PASO 1 Haga clic en **Calidad de servicio** > **General** > **Ancho de banda**.

En la página Ancho de banda, se proporciona información sobre el ancho de banda para cada interfaz.

La columna % es el límite de velocidad de ingreso para el puerto dividido entre el ancho de banda total del puerto.

PASO 2 Seleccione una interfaz, y haga clic en **Editar**.

PASO 3 Seleccione la interfaz **Puerto o LAG**.

PASO 4 Ingrese los campos para la interfaz seleccionada:

- **Límite de velocidad de ingreso**: seleccione esta opción para habilitar el límite de velocidad de ingreso, que se define en el campo que figura debajo.
- **Límite de velocidad de ingreso**: ingrese la cantidad máxima de ancho de banda permitida en la interfaz.

  NOTA Los dos campos de **Límite de velocidad de ingreso** no aparecen cuando el tipo de interfaz es LAG.
- **Tamaño de ráfaga comprometida (CBS) de ingreso**: ingrese el tamaño máximo de la ráfaga de datos para la interfaz de ingreso en bytes de datos. Esta cantidad puede enviarse incluso si incrementa temporalmente el ancho de banda más allá del límite permitido. Este campo solo está disponible si la interfaz es un puerto.
- **Velocidad de moldeado saliente**: seleccione esta opción para habilitar el moldeado saliente en la interfaz.
- **Velocidad de información comprometida (CIR, Committed Information Rate)**: ingrese el ancho de banda máximo para la interfaz de egreso.
- **Tamaño de ráfaga comprometida (CBS) de egreso**: ingrese el tamaño máximo de la ráfaga de datos para la interfaz de egreso en bytes de datos. Esta cantidad puede enviarse incluso si incrementa temporalmente el ancho de banda más allá del límite permitido.

PASO 5 Haga clic en **Aplicar**. La configuración del ancho de banda se escribe en el archivo Configuración en ejecución.

Configuración del moldeado saliente por fila de espera

Además de limitar la velocidad de transmisión por puerto, que se realiza en la página Ancho de banda, el dispositivo puede limitar la velocidad de transmisión de tramas de egreso seleccionadas por fila de espera y por puerto. El establecimiento del límite de la velocidad de egreso se realiza mediante el moldeado de la carga de salida.

El dispositivo limita todas las tramas, a excepción de las tramas de administración. Las tramas que no se limitan se omiten en los cálculos de velocidad, lo que significa que su tamaño no se incluye en el total del límite.

El moldeado de velocidad de egreso por fila de espera puede desactivarse.

Para definir el moldeado saliente por fila de espera:

PASO 1 Haga clic en **Calidad de servicio** > **General** > **Moldeado saliente por fila de espera**.

La página Moldeado saliente por fila de espera incluye el límite de velocidad y el tamaño de ráfaga para cada fila de espera.

PASO 2 Seleccione un tipo de interfaz (puerto o LAG) y haga clic en **Ir**.

PASO 3 Seleccione un puerto o un LAG, y haga clic en **Editar**.

En esta página, se puede moldear el egreso de hasta ocho filas de espera en cada interfaz.

PASO 4 Seleccione la interfaz en **Interfaz**.

PASO 5 Ingrese los siguientes campos para cada fila de espera que se necesite:

- **Habilitar**: seleccione esta opción para habilitar el moldeado saliente en esta fila de espera.
- **Velocidad de información comprometida (CIR, Committed Information Rate)**: ingrese la velocidad máxima (CIR) en Kbits por segundo (Kbps). CIR es la cantidad máxima promedio de datos que se puede enviar.
- **Tamaño de ráfaga comprometida (CBS, Committed Burst Size)**: ingrese el tamaño máximo de ráfaga (CBS) en bytes. CBS es la ráfaga máxima de datos que se puede enviar, incluso si una ráfaga excede la CIR.

PASO 6 Haga clic en **Aplicar**. La configuración del ancho de banda se escribe en el archivo Configuración en ejecución.

Límite de velocidad de ingreso VLAN

NOTA La función Límite de velocidad de VLAN no está disponible cuando el dispositivo está en el modo Capa 3.

La limitación de la velocidad por VLAN, que se realiza en la página Límite de velocidad de ingreso de VLAN, permite limitar el tráfico en las VLAN. Al configurar la limitación de la velocidad de ingreso de VLAN, se limita el tráfico agregado de todos los puertos del dispositivo.

Las siguientes restricciones se aplican a las limitaciones de velocidad por VLAN:

- Tiene menos prioridad que cualquier otra política de tráfico definida en el sistema. Por ejemplo, si un paquete está sujeto a límites de velocidad de QoS, pero también lo está a límites de velocidad de VLAN, y los límites de velocidad están en conflicto, los límites de velocidad de QoS tienen prioridad.
- Se aplica a nivel del dispositivo y dentro del dispositivo a nivel del procesador de paquetes. Si hay más de un procesador de paquetes en el dispositivo, se aplica el valor de velocidad límite de la VLAN configurada para cada uno de los procesadores de paquetes, de manera independiente. Los dispositivos con hasta 24 puertos poseen un procesador de paquete simple, mientras que los dispositivos de 48 puertos o más poseen dos procesadores de paquetes.

Para definir el límite de velocidad de ingreso de VLAN:

PASO 1 Haga clic en **Calidad de servicio** > **General** > **Límite de velocidad de ingreso de VLAN**.

En esta página se muestra la tabla de límite de velocidad de ingreso de VLAN.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **ID de VLAN**: seleccione una VLAN.
- **Velocidad de información comprometida (CIR)**: ingrese la cantidad máxima promedio de datos que la VLAN puede aceptar en Kilobytes por segundo.
- **Tamaño de ráfaga comprometida (CBS)**: ingrese el tamaño máximo de la ráfaga de datos para la interfaz de egreso en bytes de datos. Esta cantidad puede enviarse incluso si incrementa temporalmente el ancho de banda más allá del límite permitido. No se puede ingresar para las LAG.

PASO 4 Haga clic en **Aplicar**. Se añade el límite de velocidad de VLAN y se actualiza el archivo Configuración en ejecución.

Prevención de congestión de TCP

En la página Prevención de congestión de TCP, se puede activar un algoritmo de prevención de congestión de TCP. El algoritmo divide o evita la sincronización global de TCP en un nodo congestionado, donde la congestión se debe a que varios orígenes envían paquetes con el mismo conteo de bytes.

Para configurar la prevención de congestión de TCP:

PASO 1 Haga clic en **Calidad de servicio** > **General** > **Prevención de congestión de TCP**.

PASO 2 Haga clic en **Habilitar** para habilitar la prevención de congestión de TCP y luego en **Aplicar**.

Modo básico de QoS

En el modo básico de QoS, se puede definir un dominio específico en la red como de confianza. Dentro de ese dominio, los paquetes se marcan con prioridad 802.1p o DSCP para indicar el tipo de servicio que requieren. Los nodos dentro del dominio usan estos campos para asignar el paquete a una fila de espera de salida específica. La clasificación inicial de los paquetes y el marcado de estos campos se realizan en el ingreso del dominio de confianza.

Flujo de trabajo para configurar el modo básico de QoS

Para configurar el modo básico de QoS, realice lo siguiente:

1. Seleccione el modo Básico para el sistema a través de la página Propiedades de QoS.
2. Seleccione el comportamiento de confianza a través de la página Configuración global. El dispositivo admite el modo de confianza CoS/802.1p y el modo de confianza DSCP. El modo de confianza CoS/802.1p utiliza la prioridad 802.1p en la etiqueta VLAN. El modo de confianza DSCP utiliza el valor DSCP en el encabezado IP.

Si existe un puerto que, como excepción, no debe confiar en la marca CoS entrante, deshabilite el estado QoS de ese puerto a través de la página Configuración de interfaz.

Habilite o deshabilite el modo de confianza global en los puertos mediante la página Configuración de interfaz. Si se desactiva un puerto sin modo de confianza, todos sus paquetes de ingreso se reenvían en el mejor esfuerzo. Se recomienda desactivar el modo de confianza en los puertos en los que los valores CoS/802.1p o DSCP en los paquetes entrantes no sean de confianza. En caso contrario, podría afectar negativamente el rendimiento de la red.

Configuración de los valores globales

La página Configuración global incluye información para activar la confianza en el dispositivo (consulte el campo Modo de confianza a continuación). Esta configuración está activa cuando el modo de QoS es básico. Los paquetes que ingresan a un dominio de QoS se clasifican en el borde del dominio de QoS.

Para definir la configuración de confianza:

PASO 1 Haga clic en **Calidad de servicio** > **Modo básico de QoS** > **Configuración global**.

PASO 2 Seleccione el **Modo de confianza** mientras el dispositivo está en modo básico. Si la etiqueta DSCP y el nivel de CoS de un paquete están asignados a filas de espera separadas, el modo de confianza determina la fila de espera a la que se asigna el paquete:

- **CoS/802.1p**: el tráfico se asigna a las filas de espera según el campo VPT en la etiqueta VLAN, o según el valor predeterminado de CoS/802.1p por puerto (si no hay una etiqueta VLAN en el paquete entrante); la asignación en sí de VPT a la fila de espera puede configurarse en la página Asignación de CoS/802.1p a la fila de espera.
- **DSCP**: todo el tráfico IP se asigna a las filas de espera según el campo DSCP en el encabezado IP. La asignación real de DSCP a la fila de espera puede configurarse en la página DSCP a la fila de espera. Si el tráfico no es tráfico IP, se asigna a la fila de espera de mejor esfuerzo.
- **CoS/802.1p-DSCP**: CoS/802.1p o DSCP, lo que se haya configurado.

PASO 3 Seleccione **Anular ingreso DSCP** para anular los valores DSCP originales en los paquetes entrantes con los nuevos valores según la tabla de anulación de DSCP. Cuando la opción Anular ingreso DSCP está activada, el dispositivo usa los nuevos valores de DSCP para el almacenamiento en fila de espera de egreso. También reemplaza los valores DSCP originales en los paquetes con los nuevos valores DSCP.

NOTA La trama se asigna a una fila de espera de egreso usando el nuevo valor reescrito, y no según el valor DSCP original.

PASO 4 Si se habilitó la opción **Anular ingreso DSCP**, haga clic en **Tabla de anulación de DSCP** para volver a configurar DSCP.

DSCP dentro muestra el valor DSCP del paquete entrante que debe remarcarse con un valor alternativo.

PASO 5 Seleccione el valor **DSCP fuera** para indicar que el valor entrante está asignado.

PASO 6 Haga clic en **Aplicar**. El archivo Configuración en ejecución se actualiza con los nuevos valores de DSCP.

Configuración de QoS de interfaz

En la página Configuración de la interfaz, se puede configurar QoS en cada puerto del dispositivo, de la siguiente manera:

Estado de QoS deshabilitado en una interfaz: todo el tráfico entrante en el puerto se asigna a la fila de espera de mejor esfuerzo y no se realiza clasificación ni priorización alguna.

El estado de QoS del puerto está habilitado: la priorización del tráfico al ingreso del puerto se basa en el modo de confianza configurado en todo el sistema, que es el modo de confianza CoS/802.1p o el modo de confianza DSCP.

Para ingresar la configuración de QoS por interfaz:

PASO 1 Haga clic en **Calidad de servicio** > **Modo básico de QoS** > **Configuración de interfaz**.

PASO 2 Seleccione **Puerto** o **LAG** para ver la lista de puertos o LAG.

En **Estado de QoS** se muestra si la QoS está habilitada en la interfaz.

PASO 3 Seleccione una interfaz, y haga clic en **Editar**.

PASO 4 Seleccione la interfaz **Puerto** o **LAG**.

PASO 5 Haga clic para habilitar o deshabilitar **Estado de QoS** para esta interfaz.

PASO 6 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Modo avanzado de QoS

Las tramas que coinciden con una ACL y a las que se les permitió el ingreso se etiquetan de forma implícita con el nombre de la ACL que les permitió el acceso. Luego se pueden aplicar acciones del modo avanzado de QoS a estos flujos.

En modo avanzado de QoS, el dispositivo utiliza políticas para admitir la QoS por flujo. Una política y sus componentes tienen las siguientes características y relaciones:

- Una política contiene una o más asignaciones de clasificación.
- Una asignación de clasificación define a un flujo con una o más ACL asociadas. Se considera que los paquetes que coinciden solo con las reglas de ACL (ACE, entrada de control de acceso) en una asignación de clasificación con acción de permiso (reenviar) pertenecen al mismo flujo y están sujetos a la misma calidad de servicios. Por lo tanto, una política contiene uno o más flujos, cada uno con una QoS definida por el usuario.
- La QoS de una asignación de clasificación (flujo) se aplica a través del regulador asociado. Existen dos tipos de reguladores: regulador único y regulador agregado. Cada regulador se configura con una especificación de QoS. Un regulador único aplica la QoS a una sola asignación de clasificación y, por lo tanto, a un solo flujo, en función de la especificación de QoS del regulador. Un regulador agregado aplica la QoS a una o más asignaciones de clasificación y, por lo tanto, a uno o más flujos. Este regulador puede admitir asignaciones de clasificación de diferentes políticas.
- La QoS por flujo se aplica a los flujos al asociar las políticas con los puertos deseados. Una política y sus asignaciones de clasificación pueden asociarse a uno o más puertos, pero cada puerto se asocia con una política como máximo.

Notas:

- El regulador único y el regulador agregado están disponibles cuando el dispositivo está en el modo Capa 2.
- Una ACL puede configurarse para una o más asignaciones de clasificación, independientemente de las políticas.
- Una asignación de clasificación puede pertenecer solo a una política.
- Cuando se asocia una asignación de clasificación usando un regulador único a varios puertos, cada puerto tiene su propia instancia del regulador único; cada uno aplica la QoS en la asignación de clasificación (flujo) en un puerto independiente.
- Un regulador agregado aplica la QoS a todos sus flujos en conjunto, independientemente de las políticas y los puertos.

La configuración avanzada de QoS consta de tres partes:

- Definiciones de las reglas que deben cumplirse. Todas las tramas que coincidan con un solo grupo de reglas se consideran un *flujo*.
- Definición de las acciones que se aplicarán a las tramas en cada flujo que coincida con las reglas.
- Asociación de las combinaciones de reglas y acción a una o más interfaces.

Flujo de trabajo para configurar el modo avanzado de QoS

Para configurar el modo avanzado de QoS, realice lo siguiente:

1. Seleccione el modo Avanzado para el sistema a través de la página Propiedades de QoS. Seleccione comportamiento de confianza a través de la página Configuración global. Si la etiqueta DSCP y el nivel de CoS de un paquete están asignados a filas de espera separadas, el modo de confianza determina la fila de espera a la que se asigna el paquete:
   - Si los valores DSCP internos son diferentes a los usados en los paquetes entrantes, asigne los valores externos a los valores internos a través de la página Asignación de DSCP fuera de perfil. A su vez, abre la página Remarcación de DSCP.
2. Cree ACL, como se describe en Crear flujo de trabajo de ACL.
3. Si se definieron ACL, cree asignaciones de clasificación y asocie las ACL con ellos a través de la página Asignación de clasificación.

4. Cree una política a través de la página Tabla de políticas y asocie la política con una o más asignaciones de clasificación a través de la página Asignaciones de clasificación de políticas. Si es necesario, también puede especificar la QoS al asignar un regulador a una asignación de clasificación cuando asocie la asignación de clasificación a la política.
   - **Regulador único**: cree una política que asocie una asignación de clasificación con un regulador único a través de la página Tabla de políticas y la página Asignación de clasificación. Dentro de la política, defina el regulador único.
   - **Regulador agregado**: cree una acción de QoS para cada flujo que envíe todas las tramas coincidentes al mismo regulador (regulador agregado) a través de la página Regulador agregado. Cree una política que asocie una asignación de clasificación con el regulador agregado a través de la página Tabla de políticas.
5. Asocie la política a una interfaz a través de la página Vinculación de políticas.

Configuración de los valores globales

La página Configuración global contiene información para activar la confianza en el dispositivo. Los paquetes que ingresan a un dominio de QoS se clasifican en el borde del dominio de QoS.

Para definir la configuración de confianza:

PASO 1 Haga clic en **Calidad de servicio** > **Modo avanzado de QoS** > **Configuración global**.

PASO 2 Seleccione **Modo de confianza** mientras el dispositivo está en modo avanzado. Si la etiqueta DSCP y el nivel de CoS de un paquete están asignados a filas de espera separadas, el modo de confianza determina la fila de espera a la que se asigna el paquete:

- **CoS/802.1p**: el tráfico se asigna a las filas de espera según el campo VPT en la etiqueta VLAN, o según el valor predeterminado de CoS/802.1p por puerto (si no hay una etiqueta VLAN en el paquete entrante); la asignación en sí de VPT a la fila de espera puede configurarse en la página Asignación de CoS/802.1p a la fila de espera.
- **DSCP**: todo el tráfico IP se asigna a las filas de espera según el campo DSCP en el encabezado IP. La asignación real de DSCP a la fila de espera puede configurarse en la página DSCP a la fila de espera. Si el tráfico no es tráfico IP, se asigna a la fila de espera de mejor esfuerzo.
- **CoS/802.1p-DSCP**: seleccione esta opción para usar el modo CoS de confianza para tráfico no IP y DSCP de confianza para tráfico IP.

PASO 3 Seleccione el modo avanzado predeterminado, modo de confianza de QoS (ya sea confiable o no confiable) para las interfaces del campo **Estado de modo predeterminado**. De esta manera, se proporciona la funcionalidad básica de QoS, de manera que se puede confiar en CoS o DSCP en QoS avanzado de forma predeterminada (sin tener que crear una política).

En el **Modo avanzado de QoS**, cuando el estado de modo predeterminado está definido en No confiable, los valores predeterminados de CoS configurados en la interfaz se ignoran y todo el tráfico pasa a la fila de espera 1. Para obtener más detalles, consulte la página Calidad de servicio > Modo avanzado de QoS > Configuración global.

Si tiene una política en una interfaz, entonces el modo predeterminado es irrelevante, la acción será conforme a la configuración de la política y el tráfico que no coincide se cae.

PASO 4 Seleccione **Anular ingreso DSCP** para anular los valores DSCP originales en los paquetes entrantes con los nuevos valores según la tabla de anulación de DSCP. Cuando la opción Anular ingreso DSCP está activada, el dispositivo usa los nuevos valores de DSCP para el almacenamiento en fila de espera de egreso. También reemplaza los valores DSCP originales en los paquetes con los nuevos valores DSCP.

NOTA La trama se asigna a una fila de espera de egreso usando el nuevo valor reescrito, y no según el valor DSCP original.

PASO 5 Si se habilitó la opción **Anular ingreso DSCP**, haga clic en **Tabla de anulación de DSCP** para volver a configurar DSCP. Para obtener detalles, consulte la página Tabla de anulación de DSCP.

Configuración de asignación de DSCP fuera de perfil

Cuando un regulador se asigna a asignaciones de clasificación (flujos), se puede especificar la acción que se realizará cuando la cantidad de tráfico en los flujos supere los límites-especificados de QoS. Se hace referencia a la parte del tráfico que hace que el flujo supere su límite de QoS como *paquetes fuera-de-perfil*.

Si la acción de exceso es DSCP fuera de perfil, el dispositivo reasigna el valor DSCP original de los paquetes IP fuera-de-perfil con un nuevo valor basado en la Tabla de asignación de DSCP fuera de perfil. El dispositivo utiliza los nuevos valores para asignar recursos y las filas de espera de egreso a estos paquetes. Además, reemplaza físicamente el valor DSCP original en los paquetes fuera de perfil con el nuevo valor DSCP.

Para usar la acción de exceso de DSCP fuera de perfil, reasigne el valor DSCP en la tabla de asignación de DSCP fuera de perfil. En caso contrario, la acción es nula, dado que el valor DSCP en la tabla se reasigna los paquetes a sí mismo de manera predeterminada de fábrica.

Esta función permite cambiar las etiquetas DSCP para el tráfico entrante intercambiado entre dominios de confianza de QoS. Al cambiar los valores DSCP utilizados en un dominio, se configura la prioridad de ese tipo de tráfico en el valor DSCP utilizado en el otro dominio a fin de identificar el mismo tipo de tráfico.

Esta configuración está activa cuando el sistema está en el modo básico de QoS, y se activa en forma global una vez habilitada.

Por ejemplo: suponga que hay tres niveles de servicio: plata, oro, platino, y los valores entrantes de DSCP que se usan para marcar estos niveles son 10, 20 y 30, respectivamente. Si este tráfico se reenvía a otro proveedor de servicio que tiene los mismos tres niveles de servicio, pero que utiliza los valores DSCP 16, 24 y 48, **Asignación de DSCP fuera de perfil** cambia los valores entrantes a medida que se los asigna a los valores salientes.

Para asignar valores DSCP:

PASO 1 Haga clic en **Calidad de servicio > Modo avanzado de QoS > Asignación de DSCP fuera de perfil**. En esta página, se puede configurar el valor de cambio de DSCP del tráfico que entra o sale del dispositivo.

DSCP dentro muestra el valor DSCP del paquete entrante que debe remarcarse con un valor alternativo.

PASO 2 Seleccione el valor **DSCP fuera** al que está asignado el valor entrante.

PASO 3 Haga clic en **Aplicar**. El archivo Configuración en ejecución se actualiza con la nueva tabla Asignación de DSCP.

PASO 4 Seleccione **Restaurar valores predet.** para restaurar la configuración predeterminada de fábrica de CoS para esta interfaz.

Definición de asignación de clasificación

Una asignación de clasificación define un flujo de tráfico con ACL (Access Control Lists, listas de control de acceso). En una asignación de clasificación se pueden combinar ACL MAC, ACL IP y ACL IPv6. Las asignaciones de clasificación se configuran de modo que coincidan con los criterios de los paquetes, que pueden ser todos o cualquiera de ellos. Se utiliza la primera coincidencia con los paquetes, lo que significa que la acción asociada con la asignación de clasificación que coincida primero es aquella que ejecuta el sistema. Se considera que los paquetes que coinciden con la misma asignación de clasificación pertenecen al mismo flujo.

NOTA La definición de asignaciones de clasificación no tiene efecto alguno en la QoS; sino que es un paso intermedio que permite utilizar las asignaciones de clasificación más adelante.

Si se requieren conjuntos de reglas más complejos, se pueden agrupar varias asignaciones de clasificación en un supergrupo llamado una política (consulte la sección **Configuración de política**).

En la página Asignación de clasificación, se muestra la lista de asignaciones de clasificación definidas y las ACL que componen cada una, y se puede agregar o eliminar asignaciones de clasificación.

Para definir una asignación de clasificación:

PASO 1 Haga clic en **Calidad de servicio** > **Modo avanzado de QoS** > **Asignación de clase**.

En esta página se muestran las asignaciones de clasificación ya definidas.

PASO 2 Haga clic en **Add**.

Se añade una nueva asignación de clasificación al seleccionar una o dos ACL y asignarle un nombre. Si una asignación de clasificación tiene dos ACL, puede especificar que una trama debe coincidir con ambas ACL, o que debe coincidir con cualquiera de las dos o las dos ACL seleccionadas.

PASO 3 Ingrese los parámetros.

- **Nombre de asignación de clasificación**: ingrese el nombre de una nueva asignación de clasificación.
- **Hacer coincidir tipo de ACL**: los criterios con los que un paquete debe coincidir a fin de considerarse perteneciente al flujo definido en la asignación de clasificación. Las opciones son:
  - *IP*: un paquete debe coincidir con cualquiera de las ACL basadas en IP en la asignación de clasificación.
  - *MAC*: un paquete debe coincidir con la ACL basada en MAC en la asignación de clasificación.
  - *IP y MAC*: un paquete debe coincidir con la ACL basada en IP y con la ACL basada en MAC en la asignación de clasificación.
  - *IP o MAC*: un paquete debe coincidir con la ACL basada en IP o con la ACL basada en MAC en la asignación de clasificación.
- **IP**: seleccione la ACL basada en IPv4 o la ACL basada en IPv6 para la asignación de clasificación.
- **MAC**: seleccione la ACL basada en MAC para la asignación de clasificación.
- **ACL preferida**: seleccione si se busca una primera coincidencia de los paquetes con una ACL basada en IP o una ACL basada en MAC.

PASO 4 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Reguladores de QoS

NOTA No se admiten los reguladores de QoS cuando los dispositivos Sx500 están en el modo del sistema Capa 3. Siempre se admiten en los dispositivos SG500X.

Usted puede medir la velocidad del tráfico que coincide con un conjunto predefinido de reglas y aplicar límites; por ejemplo, puede medir la velocidad del tráfico de transferencia de archivo que se permite en un puerto.

Esto se puede realizar mediante las ACL en las asignaciones de clasificación para que coincidan con el tráfico deseado, y mediante un regulador para aplicar la QoS en el tráfico coincidente.

Un regulador se configura con una especificación de QoS. Hay dos tipos de reguladores:

- **Regulador único**: un regulador único aplica la QoS a una sola asignación de clasificación y a un solo flujo en función de la especificación de QoS del regulador. Cuando se asocia una asignación de clasificación usando un regulador único a varios puertos, cada puerto tiene su propia instancia del regulador único; cada uno aplica la QoS en la asignación de clasificación (flujo) en puertos que de otra manera son independientes entre sí. Un regulador único se crea en la página Tabla de políticas.
- **Regulador agregado**: un regulador agregado aplica la QoS a una o más asignaciones de clasificación y a uno o más flujos. Este regulador puede admitir asignaciones de clasificación de diferentes políticas. Un regulador agregado aplica la QoS a todos sus flujos en conjunto, independientemente de las políticas y los puertos. Un regulador agregado se crea en la página Regulador agregado.

  Un regulador agregado se define si el regulador se va a compartir con más de una clasificación. Los reguladores de un puerto no pueden compartirse con otros reguladores en otro dispositivo.

Cada regulador se define con su propia especificación de QoS con una combinación de los siguientes parámetros:

- Una velocidad máxima permitida, llamada Velocidad de información comprometida (CIR, Committed Information Rate), medida en Kbps.
- Una cantidad de tráfico, medido en bytes, llamada Tamaño de ráfaga comprometida (CBS, Committed Burst Size). A este tráfico se le permite el paso como una ráfaga temporal, incluso si supera la velocidad máxima definida.
- Una acción que se aplicará a las tramas que superen los límites (llamadas tráfico fuera de perfil), donde dichas tramas pueden transmitirse tal como están, descartarse o transmitirse, pero reasignarse a un nuevo valor DSCP que las marca como tramas de menor prioridad para todo el manejo posterior dentro del dispositivo.

La asignación de un regulador a una asignación de clasificación se realiza al añadir una asignación de clasificación a una política. Si el regulador es del tipo agregado, debe crearlo a través de la página Regulador agregado.

Definición de reguladores añadidos

Un regulador agregado aplica la QoS a una o más asignaciones de clasificación y, por lo tanto, a uno o más flujos. Este tipo de regulador puede admitir asignaciones de clasificación de diferentes políticas y aplica la QoS a todos sus flujos en conjunto, independientemente de las políticas y los puertos.

NOTA El dispositivo admite reguladores agregados y únicos solo cuando funciona en el modo Capa 2 en dispositivos que admiten un modo de sistema de Capa 2 aparte.

Para definir un regulador agregado:

PASO 1 Haga clic en **Calidad de servicio** > **Modo avanzado de QoS** > **Regulador agregado**.

En esta página aparecen los reguladores agregados existentes.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **Nombre del regulador agregado**: ingrese el nombre del regulador agregado.
- **Ingrese la velocidad de información comprometida** (CIR): ingrese el ancho de banda máximo permitido en bits por segundo. Consulte la descripción en la página Ancho de banda.
- **Tamaño de ráfaga comprometida (CBS) de ingreso**: ingrese el tamaño máximo de ráfaga (incluso si supera la CIR) en bytes. Consulte la descripción en la página Ancho de banda.
- **Acción excedente**: seleccione la acción que se realizará en los paquetes entrantes que superen la CIR. Los valores posibles son:
  - *Reenviar*: se reenvían los paquetes que superan el valor de CIR definido.
  - *Descartar*: se descartan los paquetes que superan el valor de CIR definido.
  - *DSCP fuera de perfil*: los valores DSCP de los paquetes que superan el valor de CIR definido se reasignan a un valor basado en la tabla de asignación de DSCP fuera de perfil.

PASO 4 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Configuración de una política

En la página Tabla de políticas, se muestra la lista de políticas avanzadas de QoS definidas en el sistema. Aquí también se pueden crear y eliminar políticas. Solo están activas aquellas políticas asociadas a una interfaz (consulte la página Vinculación de políticas).

Cada política consta de:

- Una o más asignaciones de clasificación de ACL que definen los flujos de tráfico en la política.
- Uno o más agregados que aplican la QoS a los flujos de tráfico en la política.

Después de agregar una política, se pueden agregar asignaciones de clasificación mediante la página Tabla de políticas.

Para añadir una política de QoS:

PASO 1 Haga clic en **Calidad de servicio** > **Modo avanzado de QoS** > **Tabla de políticas**.

En esta página se muestra la lista de políticas definidas.

PASO 2 Haga clic en **Tabla asignación de clasific. de política** para ver la página Asignación de clasificación de política.
o
Haga clic en **Añadir** para abrir la página Añadir tabla de políticas.

PASO 3 Ingrese el nombre de la política nueva en el campo **Nombre de la política nueva**.

PASO 4 Haga clic en **Aplicar**. Se añade el perfil de política de QoS y se actualiza el archivo Configuración en ejecución.

Tabla de políticas

Se puede agregar una o más asignaciones de clasificación a una política. Una asignación de clasificación define el tipo de paquetes que se consideran pertenecientes al mismo flujo de tráfico.

NOTA No se puede configurar un regulador a una asignación de clasificación cuando el dispositivo funciona en el modo Capa 3. El dispositivo admite reguladores solo en el modo Capa 2.

Para añadir una asignación de clasificación a una política:

PASO 1 Haga clic en **Calidad de servicio** > **Modo avanzado de QoS** > **Asignación de clasificación de políticas**.

PASO 2 Seleccione una política en Filtro, y haga clic en **Ir**. Aparecen todas las asignaciones de clasificación en esa política.

PASO 3 Para añadir una nueva asignación de clasificación, haga clic en **Añadir**.

PASO 4 Ingrese los parámetros.

- **Nombre de la política**: se muestra la política a la que se añade la asignación de clasificación.
- **Nombre de la asignación de clasificación**: seleccione una asignación de clasificación existente para asociarla con la política. Las asignaciones de clasificación se crean en la página Asignación de clasificación.
- **Tipo de acción**: seleccione la acción sobre el valor CoS/802.1p o DSCP de ingreso de todos los paquetes coincidentes.
  - *Usar modo de confianza predeterminado*: ignore el valor CoS/802.1p o DSCP de ingreso. Los paquetes coincidentes se envían como el mejor esfuerzo.
  - *Confiar siempre*: si se selecciona esta opción, el dispositivo confiará en el valor CoS/802.1p y DSCP del paquete coincidente. Si un paquete es un paquete IP, el dispositivo lo coloca en la fila de espera de egreso según su valor DSCP y la tabla DSCP a la fila de espera. En caso contrario, la fila de espera de egreso del paquete se basa en el valor CoS/802.1p y la tabla de CoS/802.1p a la fila de espera del paquete.
  - *Establecer*: si se selecciona esta opción, utilice el valor ingresado en el cuadro **Nuevo valor** para determinar la fila de espera de egreso de los paquetes coincidentes de la siguiente manera:

    Si el nuevo valor (0... 7) es una prioridad de CoS/802.1p, utilice el valor de prioridad y la tabla de CoS/802.1p a la fila de espera para determinar la fila de espera de egreso de todos los paquetes coincidentes.

    Si el nuevo valor (0... 63) es un DSCP, utilice el nuevo DSCP y la tabla de DSCP a la fila de espera para determinar la fila de espera de egreso de los paquetes IP coincidentes.

    En caso contrario, use el nuevo valor (1... 8) como el número de fila de espera de egreso para todos los paquetes coincidentes.
- **Tipo de política**: disponible solo en modo del sistema Capa 2. Seleccione el tipo de regulador para la política. Las opciones son:
  - *Ninguna*: no se utiliza ninguna política.
  - *Único*: el regulador para la política es un regulador único.

- *Agregado*: el regulador para la política es un regulador agregado.

- **Regulador agregado**: disponible solo en modo del sistema Capa 2. Si el valor de **Tipo de política** es *Agregado*, seleccione un regulador agregado definido previamente (en la página Regulador agregado).

Si el **Tipo de política** es *Única*, ingrese los siguientes parámetros de QoS:

- **Ingrese velocidad de información comprometida (CIR)**: ingrese la CIR en Kbps. Consulte la descripción de esto en la página Ancho de banda.
- **Tamaño de ráfaga comprometida (CBS) de ingreso**: ingrese el CBS en bytes. Consulte la descripción de esto en la página Ancho de banda.
- **Acción excedente**: seleccione la acción asignada a los paquetes entrantes que superan la CIR. Las opciones son:
  - *Ninguna*: sin acción.
  - *Descartar*: se descartan los paquetes que superan el valor de CIR definido.
  - *DSCP fuera de perfil*: los paquetes IP que superan la CIR definida se reenvían con un nuevo valor DSCP derivado de la tabla de asignación de DSCP fuera de perfil.

PASO 5 Haga clic en **Aplicar**.

Vinc. con las políticas

En la página Vinculación de políticas, se muestra qué perfil de política está vinculado y a qué puerto. Cuando un perfil de política está vinculado a un puerto específico, este está activo en ese puerto. Solo se puede configurar un perfil de política en un puerto, pero una sola política puede vincularse a más de un puerto.

Cuando una política está vinculada a un puerto, filtra el tráfico de ingreso que pertenece a los flujos definidos en la política y le aplica QoS. La política no se aplica al egreso de tráfico al mismo puerto.

Para editar una política, primero se la debe quitar (desvincular) de todos los puertos a los que esté vinculada.

NOTA Se puede vincular un puerto con una política o con una ACL pero no con ambos elementos.

Para definir la vinculación de las políticas:

PASO 1 Haga clic en **Calidad de servicio** > **Modo avanzado de QoS** > **Vinculación de política**.

PASO 2 Seleccione un **Nombre de política** y **Tipo de interfaz**, si corresponde.

PASO 3 Haga clic en **Ir**. Se selecciona una política.

PASO 4 Seleccione lo siguiente para la política o interfaz:

- **Vinculación**: seleccione para vincular la política a la interfaz.
- **Permitir cualquiera**: seleccione esta opción para reenviar paquetes de la interfaz si no coinciden con ninguna política.

NOTA La opción Permitir cualquiera se puede definir únicamente si la Protección de la IP de origen no está activada en la interfaz.

PASO 5 Haga clic en **Aplicar**. Se define la vinculación con las políticas de QoS y se actualiza el archivo Configuración en ejecución.

PASO 6 Haga clic en **Mostrar Vinculación de políticas por puerto** para mostrar los tipos de interfaz (puerto de unidad 1/1 o LAG) por interfaz:

Aparecen los siguientes campos para todos los puertos/LAG:

- Nombre de la política
- Permitir todas

Administración de estadísticas de QoS

En estas páginas, se pueden administrar las opciones Regulador único, Regulador agregado y ver las estadísticas de las filas de espera.

Estadísticas de regulador

Un regulador único se vincula a una asignación de clasificación de una sola política. Un regulador agregado se vincula a una o más asignaciones de clasificación de una o más políticas.

Visualización de estadísticas de regulador único

En la página Estadísticas de regulador único, se indica el número de paquetes dentro del perfil y fuera del perfil que se reciben de una interfaz y que reúnen las condiciones definidas en la asignación de clasificación de una política.

NOTA Esta página no se muestra cuando el dispositivo está en el modo Capa 3.

Para ver las estadísticas del regulador:

PASO 1 Haga clic en **Calidad de servicio** > **Estadísticas de QoS** > **Estadísticas de regulador único**.

Esta página muestra los siguientes campos:

- **Interfaz**: se muestran las estadísticas para esta interfaz.
- **Política**: se muestran las estadísticas para esta política.
- **Asignación de clasificación**: se muestran las estadísticas para esta asignación de clasificación.
- **Bytes dentro del perfil**: número de bytes dentro del perfil recibidos.
- **Bytes fuera del perfil**: número de bytes fuera del perfil recibidos.

PASO 2 Haga clic en **Añadir**.

PASO 3 Ingrese los parámetros.

- **Interfaz**: seleccione la interfaz para la que se acumulan las estadísticas.
- **Nombre de la política**: seleccione el nombre de la política.
- **Nombre de la clasif. de política**: seleccione el nombre de la clasificación.

PASO 4 Haga clic en **Aplicar**. Se crea una solicitud adicional de estadísticas y se actualiza el archivo Configuración en ejecución.

Visualización de estadísticas de regulador añadido

Para ver las estadísticas del regulador agregado:

PASO 1 Haga clic en **Calidad de servicio** > **Estadísticas de QoS** > **Estadísticas de regulador agregado**.

Esta página muestra los siguientes campos:

- **Nombre del regulador agregado**: regulador sobre el que se basan las estadísticas.
- **Bytes dentro del perfil**: número de paquetes dentro del perfil que se recibieron.
- **Bytes fuera del perfil**: número de paquetes fuera del perfil que se recibieron.

PASO 2 Haga clic en **Add**.

PASO 3 En **Nombre del regulador agregado**, seleccione uno de los reguladores agregados creados previamente para el que desea ver las estadísticas.

PASO 4 Haga clic en **Aplicar**. Se crea una solicitud adicional de estadísticas y se actualiza el archivo Configuración en ejecución.

Visualización de estadísticas de filas de espera

En la página Estadísticas de filas de espera, se muestran las estadísticas de las filas de espera, que incluyen aquellas de paquetes reenviados y descartados, según la interfaz, la fila de espera y la prioridad de eliminación.

Para ver las estadísticas de filas de espera:

PASO 1 Haga clic en **Calidad de servicio** > **Estadísticas de QoS** > **Estadísticas de filas de espera**.

Esta página muestra los siguientes campos:

- **Vel. de actualización**: seleccione el período de tiempo que transcurre antes de que se actualicen las estadísticas de Ethernet de la interfaz. Las opciones disponibles son:
  - *Sin actualización*: las estadísticas no se actualizan.
  - *15 seg.*: las estadísticas se actualizan cada 15 segundos.
  - *30 seg.*: las estadísticas se actualizan cada 30 segundos.
  - *60 seg.*: las estadísticas se actualizan cada 60 segundos.
- **Contador configurado**: las opciones son:
  - *Conjunto 1*: se muestran las estadísticas para el conjunto 1 que contiene todas las interfaces y filas de espera con una prioridad de eliminación (DP) alta.
  - *Conjunto 2*: se muestran las estadísticas para el conjunto 2 que contiene todas las interfaces y filas de espera con una DP baja.
- **Interfaz**: se muestran las estadísticas de fila de espera para esta interfaz.
- **Fila de espera**: los paquetes se reenviaron o se descartaron de esta fila de espera.
- **Prioridad de eliminación**: la prioridad de eliminación más baja tiene la menor probabilidad de descarte.
- **Paquetes totales**: número de paquetes reenviados o descartados en fila de espera.

- **Paquetes de eliminación de fila de espera**: porcentaje de paquetes que se descartaron al llegar a la fila de espera.

PASO 2 Haga clic en **Añadir**.

PASO 3 Ingrese los parámetros.

- **Contador configurado**: seleccione el contador configurado:
  - *Conjunto 1*: se muestran las estadísticas para el conjunto 1 que contiene todas las interfaces y filas de espera con una prioridad de eliminación (DP) alta.
  - *Conjunto 2*: se muestran las estadísticas para el conjunto 2 que contiene todas las interfaces y filas de espera con una DP baja.
- **Interfaz**: seleccione los puertos para los que se muestran las estadísticas. Las opciones son:
  - *Puerto*: se selecciona el puerto en el número de unidad seleccionado para el que se muestran las estadísticas.
  - *Todos los puertos*: se especifica que las estadísticas se muestran para todos los puertos.
- **Fila de espera**: seleccione la fila de espera para la que se muestran las estadísticas.
- **Prioridad de eliminación**: ingrese la prioridad de eliminación que indica la probabilidad de descarte.

PASO 4 Haga clic en **Aplicar**. Se añade el contador de estadísticas de filas de espera y se actualiza el archivo Configuración en ejecución.

27

SNMP

En esta sección se describe la función Protocolo de administración de red simple (SNMP, Simple Network Management Protocol) que proporciona un método para administrar dispositivos de red.

Abarca los siguientes temas:

- **Flujos de trabajo y versiones de SNMP**
- **ID de objeto de modelos**
- **ID de motor de SNMP**
- **Configuración de las vistas SNMP**
- **Creación de grupos SNMP**
- **Administración de usuarios SNMP**
- **Definición de comunidades SNMP**
- **Definición de la configuración de trampa**
- **Receptores de una notificación**
- **Filtros de notificaciones SNMP**

Flujos de trabajo y versiones de SNMP

El dispositivo funciona como agente SNMP y admite SNMPv1, v2 y v3. También informa al sistema los eventos para retener receptores mediante las trampas recibidas en las bases de información de administración (MIB, Management Information Base) compatibles.

SNMPv1 y v2

Para controlar el acceso al sistema, se define una lista de entradas a la comunidad. Cada entrada a la comunidad consta de una *cadena de comunidad* y su privilegio de acceso. El sistema solo responde a los mensajes SNMP que especifiquen la comunidad con los permisos correctos y la operación apropiada.

Los agentes SNMP mantienen una lista de variables que se usan para administrar el dispositivo. Las variables se definen en la *Base de datos de información de administración* (MIB, Management Information Base).

NOTA Debido a las vulnerabilidades de seguridad de las otras versiones, se recomienda usar SNMPv3.

SNMPv3

Además de la funcionalidad que proporciona SNMP v1 y v2, SNMP v3 aplica el control de acceso y nuevos mecanismos de trampa a las PDU de SNMPv1 y SNMPv2. SNMPv3 también define un Modelo de seguridad de usuario (USM, User Security Model) que incluye:

- **Autenticación**: proporciona integridad de datos y autenticación de origen de datos.
- **Privacidad**: protege contra la divulgación del contenido del mensaje. El modo *Cipher Block-Chaining* (CBC-DES) se usa para el cifrado. En un mensaje SNMP se habilita la autenticación sola, o bien, se habilita la autenticación y la privacidad. Sin embargo, la privacidad no se puede habilitar sin autenticación.
- **Vigencia**: protege contra el retraso de los mensajes o los ataques de reproducción. El agente SNMP compara la marca de tiempo del mensaje entrante con la hora de llegada del mensaje.
- **Administración de claves**: define la generación de claves, la actualización de claves y el uso de claves. El dispositivo admite filtros de notificaciones de SNMP según *ID de objeto*. El sistema usa los OID para administrar las funciones de los dispositivos.

Flujo de trabajo de SNMP

NOTA Por razones de seguridad, SNMP está deshabilitado de forma predeterminada. Antes de administrar el dispositivo mediante SNMP, debe activar SNMP en la página Seguridad > Servicios TCP/UDP.

A continuación, se describen las series de acciones recomendadas para configurar el SNMP:

Si decide usar SNMP v1 o v2:

PASO 1 Vaya a SNMP > página Comunidades y haga clic en **Añadir**. La comunidad puede asociarse con derechos de acceso y una vista en el modo Básico o con un grupo en el modo Avanzado. Existen dos formas de definir los derechos de acceso a una comunidad:

- **Modo básico**: los derechos de acceso de una comunidad pueden configurarse como Solo lectura, Lectura-escritura o Admin. de SNMP. Además, puede restringir el acceso a la comunidad solo para ciertos objetos MIB seleccionando una vista (que se define en la página Vistas).

- **Modo avanzado**: los derechos de acceso a una comunidad se definen por un grupo (que se define en la página Grupos). Usted puede configurar el grupo con un modelo de seguridad específico. Los derechos de acceso de un grupo son Lectura, Escritura y Notificación.

PASO 2 Seleccione si desea restringir la estación de administración SNMP a una dirección o permitir la administración SNMP desde todas las direcciones. Se elige restringir la administración SNMP a una dirección, entonces ingrese la dirección de su PC de administración SNMP en el campo Dirección IP.

PASO 3 Ingrese la cadena de comunidad única en el campo Cadena de comunidad.

PASO 4 Como otra opción, habilite las trampas mediante la página Configuración de trampa.

PASO 5 Si desea, defina filtros de notificaciones mediante la página Filtro de notificaciones.

PASO 6 Configure los receptores de notificaciones en la página Receptores de una notificación SNMPv1,2.

Si decide usar SNMPv3:

PASO 1 Defina el motor SNMP mediante la página ID de motor. Cree un ID de motor único o use el ID de motor predeterminado. Al aplicar el ID de motor, la configuración se borrará de la base de datos SNMP.

PASO 2 Como otra opción, defina vistas SNMP mediante la página Vistas. De esta manera, se limitará el rango de OID disponibles para una comunidad o un grupo.

PASO 3 Defina los grupos mediante la página Grupos.

PASO 4 Defina usuarios mediante la página Usuarios de SNMP, donde se pueden asociar con un grupo. Si el ID de motor de SNMP no está definido, los usuarios no podrán crearse.

PASO 5 Como otra opción, active o desactive las trampas mediante la página Configuración de trampa.

PASO 6 Si desea, defina filtros de notificaciones mediante la página Filtro de notificaciones.

PASO 7 Defina receptores de notificaciones mediante la página Receptores de una notificación SNMPv3.

MIB compatibles

Para obtener una lista de los MIB compatibles, visite la siguiente URL y navegue al área de descarga que figura como **Cisco MIBS**:

www.cisco.com/cisco/software/navigator.html

ID de objeto de modelos

A continuación, se muestran los *ID de objeto* de los modelos de los dispositivos:

Nombre de modelo	Descripción	ID de objeto
SG300-10	8 puertos GE y 2 puertos combinados de aplicación especial (GE/SFP)	9.6.1.83.10.1
SG300-10MP	8 puertos GE y 2 puertos combinados de aplicación especial (GE/SFP)	9.6.1.83.10.3
SG300-10P	8 puertos GE y 2 puertos combinados de aplicación especial (GE/SFP)	9.6.1.83.10.2
SG300-20	16 puertos GE y 4 puertos de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	9.6.1.83.20.1
SG300-28	24 puertos GE y 4 puertos de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	9.6.1.83.28.1
SG300-28P	24 puertos GE y 4 puertos de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	9.6.1.83.28.2
SG300-52	48 puertos GE y 4 puertos de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	9.6.1.83.52.1
SF300-08	8 puertos FE.	9.6.1.82.08.4
SF302-08	8 puertos FE más 2 puertos GE	9.6.1.82.08.1
SF302-08MP	8 puertos FE más 2 puertos GE	9.6.1.82.08.3
SF302-08P	8 puertos FE más 2 puertos GE	9.6.1.82.08.2

Nombre de modelo	Descripción	ID de objeto
SF300-24	24 puertos FE y 4 puertos GE de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	9.6.1.82.24.1
SF300-24P	24 puertos FE y 4 puertos GE de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	9.6.1.82.24.2
SF300-48	48 puertos FE y 4 puertos GE de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	9.6.1.82.48.1
SF300-48P	48 puertos FE y 4 puertos GE de aplicación especial, 2 enlaces ascendentes y 2 puertos combinados	9.6.1.82.48.2
SG300-52P	Switch Gigabit administrable PoE de 52 puertos	9.6.1.83.52.2
SG300-52MP	Switch Gigabit administrable PoE de 52 puertos	9.6.1.83.52.3
SG300-10SFP	Switch SFP Gigabit administrable de 10 puertos	9.6.1.83.10.5
ESW2-350G-52	Switch Gigabit administrable de 52 puertos	9.6.1.86.52.1
ESW2-350G-52DC	Switch Gigabit administrable de 52 puertos	9.6.1.86.52.6
SF300-24MP	Switch administrable PoE 10/100 de 24 puertos	9.6.1.82.24.3
SG300-28MP	Switch Gigabit administrable PoE de 28 puertos	9.6.1.83.28.3
SF302-08P	8 puertos FE más 2 puertos GE	9.6.1.82.08.2
SF302-08PP	Switch administrable PoE 10/100 de 8 puertos	9.6.1.82.08.2
SF302-08MPP	Switch administrable PoE 10/100 de 8 puertos	9.6.1.82.08.3
SG300-10PP	Switch administrable PoE 10/100 de 8 puertos	9.6.1.83.10.2

Nombre de modelo	Descripción	ID de objeto
SF300-24PP	Switch administrable PoE 10/100 de 8 puertos	9.6.1.82.24.1
SG300-28PP	Switch Gigabit administrable PoE de 10 puertos	9.6.1.83.28.2
SF300-24PP	Switch administrable PoE 10/100 de 24 puertos	9.6.1.82.24.1
SG300-28PP	Switch Gigabit administrable PoE de 28 puertos	9.6.1.83.28.2
SF300-48PP	Switch administrable PoE 10/100 de 48 puertos	9.6.1.82.48.2
SG300-28SFP	Switch SFP Gigabit administrable de 28 puertos	9.6.1.83.28.5

Los ID de objeto privados se colocan debajo de: enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101).

ID de motor de SNMP

Las entidades SNMPv3 usan el ID de motor para identificarlos de manera exclusiva. Un agente SNMP se considera un motor SNMP autorizado. Esto significa que el agente responde los mensajes entrantes (Get, GetNext, GetBulk, Set) y envía mensajes trampa a un administrador. La información local del agente se encapsula en campos del mensaje.

Cada agente SNMP mantiene la información local que se usa en los intercambios de mensajes SNMPv3. El ID de motor SNMP predeterminado está compuesto por el número de empresa y la dirección MAC predeterminada. Este ID de motor SNMP debe ser único para el dominio administrativo, de manera que no haya dos dispositivos en una red que tengan el mismo ID de motor.

La información local se almacena en cuatro variables MIB de solo lectura (snmpEngineId, snmpEngineBoots, snmpEngineTime y snmpEngineMaxMessageSize).

PRECAUCIÓN Cuando se cambia la ID de motor, se borran todos los usuarios y grupos configurados.

Para definir la ID de motor SNMP:

PASO 1 Haga clic en **SNMP** > **ID de motor**.

PASO 2 Seleccione cuál usar para **ID de motor local**.

- **Usar predeterminado**: seleccione esta opción para usar un ID de motor generado por el dispositivo. El ID de motor predeterminado se basa en la dirección MAC del dispositivo y se define por norma de la siguiente manera:
  - *Primeros 4 octetos*: primer bit = 1, el resto es el número de empresa IANA.
  - *Quinto octeto*: configurado en 3 para indicar la dirección MAC que sigue.
  - *Últimos 6 octetos*: la dirección MAC del dispositivo.
- **Ninguna**: no se usa ningún ID de motor.
- **Definida por el usuario**: ingrese el ID de motor del dispositivo local. El valor del campo es una cadena hexadecimal **(rango: 10 - 64)**. Cada byte de las cadenas de caracteres hexadecimales está representado por dos dígitos hexadecimales.

Todos los ID de motor remoto y las direcciones IP correspondientes se muestran en la tabla ID de motor remoto.

PASO 3 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

La tabla de ID de motor remoto muestra las asignaciones entre las direcciones IP del motor y el ID del motor. Para añadir la dirección IP de un ID de motor:

PASO 4 Haga clic en **Add**. Ingrese los siguientes campos:

- **Definición del servidor**: seleccione si el servidor de ID de motor se especificará por dirección IP o nombre.
- **Versión de IP**: seleccione el formato IP admitido.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: seleccione la interfaz local de enlace (si se selecciona Enlace local como Tipo de dirección IPv6) en la lista.

- **Nombre/dirección IP del servidor**: ingrese la dirección IP o el nombre de dominio del servidor de registro.
- **ID de motor**: ingrese el ID de motor.

PASO 5 Haga clic en **Aplicar**. Se actualiza el archivo Configuración en ejecución.

Configuración de las vistas SNMP

Una vista es una etiqueta definida por el usuario para una colección de subárboles de MIB. Cada ID de subárbol se define mediante el *ID de objeto* (OID) de la raíz de los subárboles relevantes. Se puede usar cualquiera de los nombres conocidos para especificar la raíz del subárbol que desea o se puede ingresar un ID de objeto (consulte la sección **ID de objeto de modelos**).

Cada subárbol se incluye en la vista que se está definiendo o se excluye de esta.

En la página Vistas, se puede crear y editar vistas SNMP. Las vistas predeterminadas (Default, DefaultSuper) no se pueden cambiar.

Las vistas se pueden conectar a grupos en la página Grupos o a una comunidad que emplea el modo de acceso básico mediante la página Comunidades.

Para definir vistas SNMP:

PASO 1 Haga clic en **SNMP** > **Vistas**.

PASO 2 Haga clic en **Añadir** para definir vistas nuevas.

PASO 3 Ingrese los parámetros.

- **Ver nombre**: ingrese un nombre de vista de 0 a 30 caracteres.
- **Subárbol de ID de objeto**: seleccione el nodo en el árbol de MIB que se incluye en la vista SNMP seleccionada o que se excluye de esta. Las opciones para seleccionar el objeto son las siguientes:
  - *Seleccionar de la lista*: le permite navegar el árbol de MIB. Presione la flecha *Up* (Arriba) para ir al nivel del nodo padre y nodo hermanos del nodo seleccionado; presione la flecha *Down* (abajo) para bajar al nivel de los descendientes del nodo seleccionado. Haga clic en los nodos de la vista para pasar de un nodo a su hermano. Use la barra de desplazamiento para poder ver los nodos hermanos.
  - *Definida por el usuario*: ingrese un OID que no se ofrezca en la opción *Seleccionar de la lista*.

PASO 4 Seleccione o cancele la selección **Incluir en la vista.** Si se selecciona, las MIB seleccionadas se incluirán en la vista; de lo contrario, no se incluirán.

PASO 5 Haga clic en **Aplicar**.

PASO 6 Para verificar la configuración de su vista, seleccione las vistas definidas por el usuario de la lista **Filtro: Ver nombre**. De forma predeterminada, existen las siguientes vistas:

- **Default**: vista SNMP predeterminada para vistas de lectura y lectura/escritura.
- **DefaultSuper**: vista SNMP predeterminada para vistas de administrador.

Se pueden agregar otras vistas.

- **Subárbol de ID de objeto**: muestra el subárbol para incluir o excluir de la vista SNMP.
- **Vista de subárbol de ID de objeto**: muestra si el subárbol definido se incluye en la vista SNMP seleccionada o se excluye de esta.

Creación de grupos SNMP

En SNMPv1 y SNMPv2, se envía una cadena de la comunidad junto con las tramas SNMP. La cadena de la comunidad actúa como contraseña para obtener el acceso a un agente SNMP. Sin embargo, ni las tramas ni la cadena de la comunidad están cifradas. Por lo tanto, SNMPv1 y SNMPv2 no son seguros.

En SNMPv3, pueden configurarse los siguientes mecanismos de seguridad.

- **Autenticación**: el dispositivo verifica que el usuario SNMP sea un administrador del sistema autorizado. Esto se hace para cada trama.
- **Privacidad**: las tramas SNMP pueden transportar datos cifrados.

Por lo tanto, en SNMPv3, existen tres niveles de seguridad:

- Sin seguridad (sin autenticación ni privacidad)
- Autenticación (con autenticación y sin privacidad)
- Autenticación y privacidad

SNMPv3 proporciona un medio para controlar el contenido que cada usuario puede leer o escribir y las notificaciones que reciben. Un grupo define privilegios de lectura/escritura y un nivel de seguridad. Cuando está asociado con una comunidad o un usuario SNMP, comienza a funcionar.

NOTA Para asociar una vista no predeterminada a un grupo, primero cree la vista en la página Vistas.

Para crear un grupo SNMP:

PASO 1 Haga clic en **SNMP** > **Grupos**.

En esta página, se muestran los grupos SNMP existentes y los niveles de seguridad correspondientes.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **Nombre de grupo**: ingrese un nuevo nombre de grupo.
- **Modelo de seguridad**: seleccione la versión de SNMP asociada al grupo, SNMPv1, v2 o v3.

Se pueden definir tres tipos de vistas con diversos niveles de seguridad. Para cada nivel de seguridad, seleccione las vistas para Lectura, Escritura y Notificación. Para ello, ingrese los siguientes campos:

- **Habilitar**: seleccione este campo para habilitar el Nivel de seguridad.
- **Nivel de seguridad**: defina el nivel de seguridad asociado al grupo. SNMPv1 y SNMPv2 no admite autenticación ni privacidad. Si se selecciona SNMPv3, elija una de las siguientes opciones:
  - *Sin autenticación y sin privacidad*: no se asignan al grupo ni los niveles de seguridad de privacidad ni de autenticación.
  - *Autenticación sin privacidad*: autentica mensajes SNMP y garantiza que el origen de los mensajes SNMP se autentica, pero no los cifran.
  - *Autenticación y privacidad*: autentica mensajes SNMP y los cifra.
- **Vista**: seleccione para asociar la vista con los privilegios de acceso de lectura, escritura y notificaciones del grupo limita el alcance del árbol MIB al que el grupo tiene acceso de lectura, escritura y notificaciones.
  - *Lectura*: el acceso de administración es de solo lectura para la vista seleccionada. De lo contrario, un usuario o una comunidad asociada con este grupo puede leer todas las MIB, salvo aquellas que controlan el mismo SNMP.
  - *Escritura*: el acceso de administración es de escritura para la vista seleccionada. De lo contrario, un usuario o una comunidad asociada con este grupo puede escribir todas las MIB, salvo aquellas que controlan el mismo SNMP.
  - *Notificaciones*: limita el contenido disponible de trampas a los incluidos en la vista seleccionada. De lo contrario, no hay restricción en el contenido de las trampas. Esta opción solo se puede seleccionar para SNMPv3.

PASO 4 Haga clic en **Aplicar**. El grupo SNMP se guarda en el archivo de configuración en ejecución.

Administración de usuarios SNMP

Un usuario SNMP se define por las credenciales de inicio de sesión (nombre de usuario, contraseñas y método de autenticación), y por el contexto y el alcance donde opera por asociación a un grupo y un ID de motor.

El usuario configurado tendrá los atributos de su grupo, y los privilegios de acceso se configuran en la vista asociada.

Los grupos permiten a los administradores de redes asignar derechos de acceso a un grupo de usuarios en lugar de a un solo usuario.

Un usuario puede pertenecer a un solo grupo.

Para crear un usuario SNMPv3, primero debe existir lo siguiente:

- Un ID de motor primero debe configurarse en el dispositivo. Esto se realiza en la página ID de motor.
- Debe estar disponible un grupo SNMPv3. Un grupo SNMPv3 se define en la página Grupos.

Para mostrar los usuarios SNMP y definir nuevos usuarios:

PASO 1 Haga clic en **SNMP** > **Usuarios**.

En esta página, se muestran los usuarios existentes.

PASO 2 Haga clic en **Añadir**.

En esta página se proporciona información a los usuarios SNMP para asignar privilegios de control de acceso a SNMP.

PASO 3 Ingrese los parámetros.

- **Nombre de usuario**: ingrese un nombre para el usuario.
- **ID de motor**: seleccione la entidad de SNMP local o remota a la que el usuario está conectado. Al cambiar o eliminar el ID de motor SNMP local se elimina la base de datos del usuario SNMPv3. Para recibir informes y solicitar información, debe definir un usuario local y un usuario remoto.
  - *Local*: el usuario está conectado al dispositivo local.
  - *Dirección IP remoto*: el usuario está conectado a una entidad SNMP diferente, además del dispositivo local. Si se define el ID de motor remoto, los dispositivos remotos reciben mensajes de informe, pero no pueden solicitar información.

    Ingrese el ID de motor remoto.

- **Nombre de grupo**: seleccione el grupo SNMP al que pertenece el usuario SNMP. Los grupos SNMP se definen en la página Añadir grupo.

  NOTA Los usuarios, que pertenecen a grupos que se han eliminado, permanecen, pero están inactivos.

- **Método de autenticación**: seleccione un método de autenticación que varíe según el nombre de grupo asignado. Si el grupo no requiere autenticación, entonces el usuario no puede configurar ninguna autenticación. Las opciones son:

  - *Ninguna*: no se usa ninguna autenticación de usuario.
  - *MD5*: contraseña que se utiliza para generar una clave mediante el método de autenticación MD5.
  - *SHA*: contraseña que se utiliza para generar una clave mediante el Algoritmo de hash seguro (SHA, Secure Hash Algorithm).

- **Contraseña de autenticación**: si se logra la autenticación mediante una contraseña de MD5 o SHA, ingrese la contraseña de usuario local **Cifrada** o en **Texto simple**. Las contraseñas de usuario local se comparan con las de la base de datos local y pueden contener hasta 32 caracteres ASCII.

- **Método de privacidad**: seleccione una de las siguientes opciones:

  - *Ninguna*: la clave de privacidad no está cifrada.
  - *DES*: la clave de privacidad está cifrada según el Estándar de cifrado de datos (DES, Data Encryption Standard).

- **Contraseña de privacidad**: si se optó por el método de privacidad DES, se requieren 16 bytes (clave de cifrado DES). Este campo debe tener exactamente 32 caracteres hexadecimales. Se puede seleccionar el modo **Cifrado** o **Texto simple**.

PASO 4 Haga clic en **Aplicar** para guardar las configuraciones.

Definición de comunidades SNMP

Los derechos de acceso en SNMPv1 y SNMPv2 se administran al definir comunidades en la página Comunidades. El nombre de comunidad es un tipo de contraseña compartida entre la estación de administración de SNMP y el dispositivo. Este nombre se usa para autenticar la estación de administración de SNMP.

Las comunidades solo se definen en SNMPv1 y v2 porque SNMPv3 trabaja con usuarios, en lugar de comunidades. Los usuarios pertenecen a grupos que tienen derechos de acceso asignados.

En la página Comunidades, se asocian comunidades con derechos de acceso, ya sea directamente (Modo básico) o a través de grupos (Modo avanzado):

- **Modo básico**: los derechos de acceso de una comunidad pueden configurarse como Solo lectura, Lectura-escritura o Admin. de SNMP. Además, puede restringir el acceso a la comunidad solo para ciertos objetos MIB seleccionando una vista (que se define en la página Vistas SNMP).
- **Modo avanzado**: los derechos de acceso a una comunidad se definen por un grupo (que se define en la página Grupos). Usted puede configurar el grupo con un modelo de seguridad específico. Los derechos de acceso de un grupo son Lectura, Escritura y Notificación.

Para definir comunidades SNMP:

PASO 1 Haga clic en **SNMP** > **Comunidades**.

En esta página, se muestra una tabla de comunidades SNMP configuradas y sus propiedades.

PASO 2 Haga clic en **Añadir**.

Esta página permite a los administradores de red definir y configurar nuevas comunidades SNMP.

PASO 3 **Estación de administración de SNMP**: haga clic en **Definida por el usuario** para ingresar la dirección IP de la estación de administración que puede acceder a la comunidad SNMP. Haga clic en **Todos** para indicar que cualquier dispositivo puede acceder a la comunidad SNMP.

- **Versión de IP**: seleccione IPv4 o IPv6.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6, si se usa IPv6. Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: si el tipo de dirección IPv6 es Enlace local, seleccione si se recibe a través de VLAN o ISATAP.
- **Dirección IP**: ingrese la dirección IP de la estación de administración SNMP.
- **Cadena de comunidad**: ingrese el nombre de la comunidad que se usa para autenticar la estación de administración al dispositivo.

- **Básico**: seleccione este modo para una comunidad seleccionada. En este modo, no hay conexión con ningún grupo. Solo se puede elegir el nivel de acceso de la comunidad (Solo lectura, Lectura-escritura o Admin. de SNMP) y, como otra opción, puede calificarlo para una vista específica. De forma predeterminada, se aplica a toda la MIB. Si está seleccionado, complete los siguientes campos:
  - *Modo de acceso*: seleccione los derechos de acceso de la comunidad. Las opciones son:

    Sólo lectura: el acceso de administración está restringido a sólo lectura. No se puede hacer cambios a la comunidad.

    Lectura-escritura: el acceso de administración es de escritura-lectura. Se puede hacer cambios a la configuración del dispositivo, pero no a la comunidad.

    Administrador de SNMP: el usuario tiene acceso a todas las opciones de configuración del dispositivo, como así también a permisos para modificar la comunidad. Admin. de SNMP es equivalente a lectura-escritura para todas las MIB, excepto para las MIB del SNMP. Se requiere Admin. de SNMP para acceder a las MIB del SNMP.
  - *Ver nombre*: seleccione una vista SNMP (una colección de subárboles de MIB a la que se le ha otorgado acceso).
- **Avanzado**: seleccione este modo para una comunidad seleccionada.
  - *Nombre del grupo*: seleccione un grupo SNMP que determine los derechos de acceso.

PASO 4 Haga clic en **Aplicar**. Se define la comunidad de SNMP y se actualiza el archivo Configuración en ejecución.

Definición de la configuración de trampa

En la página Configuración de trampa, se puede configurar si las notificaciones de SNMP se envían desde el dispositivo y en qué casos. Los receptores de notificaciones de SNMP se pueden configurar en la página Receptores de una notificación SNMPv1,2 o en la página Receptores de una notificación SNMPv3.

Para definir la configuración de trampa:

PASO 1 Haga clic en **SNMP** > **Configuración de trampa**.

PASO 2 Seleccione **Habilitar** para **Notificaciones de SNMP** para especificar que el dispositivo puede enviar notificaciones de SNMP.

PASO 3 Seleccione **Habilitar** para **Notificaciones de autenticación** para habilitar la notificación de falla de autenticación de SNMP.

PASO 4 Haga clic en **Aplicar**. La configuración Trampas SNMP se escribe en el archivo Configuración en ejecución.

Receptores de una notificación

Los mensajes trampa se generan para notificar los eventos del sistema, según se define en RFC 1215. El sistema puede generar trampas definidas en la MIB que admite.

Los receptores de trampas (también conocidos como receptores de notificaciones) son nodos de red a donde el dispositivo envía los mensajes trampa. Se define una lista de receptores como destinos de mensajes trampa.

Una entrada de receptor de trampa contiene la dirección IP del nodo y las credenciales SNMP correspondientes a la versión que se incluye en el mensaje de trampa. Cuando surge un evento que requiere que se envíe un mensaje trampa, éste se envía a cada nodo que se incluye en la Tabla de destinatarios de notificaciones.

En la página Receptores de una notificación SNMPv1,2 y en la página Receptores de una notificación SNMPv3, se pueden configurar el destino al que se envían las notificaciones de SNMP, y los tipos de notificaciones de SNMP que se envían a cada destino (trampas o informes). Las ventanas emergentes Añadir/Editar permiten configurar los atributos de las notificaciones.

Una notificación de SNMP es un mensaje que se envía desde el dispositivo hacia la estación de administración SNMP, donde se indica que se ha producido cierto evento, como una activación o desactivación de enlace.

También es posible filtrar ciertas notificaciones. Para ello, se debe crear un filtro en la página Filtro de notificaciones y asociarlo a un receptor de una notificación de SNMP. El filtro de notificaciones le permite activar el tipo de notificaciones de SNMP que se envían a la estación de administración según el OID de la notificación que se va a enviar.

Definición de receptores de notificaciones SNMPv1,2

Para definir un receptor en SNMPv1,2:

PASO 1 Haga clic en **SNMP** > **Receptores de una notificación SNMPv1,2**.

En esta página se muestran los receptores de SNMPv1,2.

PASO 2 Ingrese los siguientes campos:

- **Informa interfaz de origen IPv4**: seleccione la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen en los mensajes usados para la comunicación con el servidor SNMP IPv4.
- **Atrapa interfaz de origen IPv4**: seleccione la interfaz de origen cuya dirección IPv6 se utilizará como dirección IPv6 de origen en los mensajes trampa usados para la comunicación con el servidor SNMP IPv6.
- **Informa interfaz de origen IPv6**: seleccione la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen en los mensajes usados para la comunicación con el servidor SNMP IPv4.

- **Atrapa interfaz de origen IPv6**: seleccione la interfaz de origen cuya dirección IPv6 se utilizará como dirección IPv6 de origen en los mensajes trampa usados para la comunicación con el servidor SNMP IPv6.

  NOTA Si se selecciona la opción Automática, el sistema toma la dirección IP de origen de la dirección IP definida en la interfaz de salida.

  PASO 3 Haga clic en **Añadir**.

  PASO 4 Ingrese los parámetros.

- **Definición del servidor**: seleccione si el servidor de registro remoto se especificará por dirección IP o nombre.
- **Versión de IP**: seleccione IPv4 o IPv6.
- **Tipo de dirección IPv6**: seleccione *Enlace local* o *Global*.
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.
- **Interfaz local de enlace**: si el tipo de dirección IPv6 es Enlace local, seleccione si se recibe a través de VLAN o ISATAP.
- **Nombre/Dirección IP del receptor**: ingrese la dirección IP o el nombre de servidor de donde se envían las trampas.
- **Puerto UDP**: ingrese el puerto UDP que se usa para notificaciones en el dispositivo receptor.
- **Tipo de notificación**: seleccione si se deben enviar mensajes trampa o de informe. Si se necesitan los dos, deben crearse dos receptores.
- **Tiempo de espera**: ingrese la cantidad de segundos que el dispositivo espera antes de volver a enviar las notificaciones de información.
- **Reintentos**: ingrese la cantidad de veces que el dispositivo vuelve a enviar un pedido de informe.
- **Cadena de comunidad**: seleccione de la lista desplegable, la cadena de comunidad del administrador de trampas. Los nombres de las cadenas de comunidad se generan de los que están enumerados en la página Comunidad.
- **Versión de notificación**: seleccione la versión del SNMP de trampas.
  Se puede usar SNMPv1 o SNMPv2 como versión de trampas, con solo una versión habilitada por vez.
- **Filtro de notificaciones**: seleccione esta opción para habilitar el filtrado del tipo de notificaciones SNMP que se envían a la estación de administración. Los filtros se crean en la página Filtro de notificaciones.

- **Nombre de filtro**: seleccione el filtro SNMP que define la información que contienen las trampas (que se define en la página Filtro de notificaciones).

PASO 5 Haga clic en **Aplicar**. La configuración Recepción de notificaciones SNMP se escriben en el archivo Configuración en ejecución.

Definición de receptores de notificaciones SNMPv3

Para definir un receptor en SNMPv3:

PASO 1 Haga clic en **SNMP** > **Receptores de una notificación SNMPv3**.

En esta página se muestran los receptores de SNMPv3.

- **Informa interfaz de origen IPv4**: seleccione la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen en los mensajes usados para la comunicación con el servidor SNMP IPv4.
- **Atrapa interfaz de origen IPv4**: seleccione la interfaz de origen cuya dirección IPv6 se utilizará como dirección IPv6 de origen en los mensajes trampa usados para la comunicación con el servidor SNMP IPv6.
- **Informa interfaz de origen IPv6**: seleccione la interfaz de origen cuya dirección IPv4 se utilizará como dirección IPv4 de origen en los mensajes usados para la comunicación con el servidor SNMP IPv4.
- **Atrapa interfaz de origen IPv6**: seleccione la interfaz de origen cuya dirección IPv6 se utilizará como dirección IPv6 de origen en los mensajes trampa usados para la comunicación con el servidor SNMP IPv6.

PASO 2 Haga clic en **Agregar**.

PASO 3 Ingrese los parámetros.

- **Definición del servidor**: seleccione si el servidor de registro remoto se especificará por dirección IP o nombre.
- **Versión de IP**: seleccione IPv4 o IPv6.
- **Tipo de dirección IPv6**: seleccione el tipo de dirección IPv6 (si se usa IPv6). Las opciones son:
  - *Enlace local*: la dirección IPv6 identifica hosts de manera exclusiva en un enlace de red simple. Una dirección local de enlace tiene un prefijo de **FE80**, no es enrutable y se puede usar para comunicaciones solo en la red local. Solo se admite una dirección local de enlace. Si existe una dirección local de enlace en la interfaz, esta entrada reemplaza a la dirección en la configuración.
  - *Global*: la dirección IPv6 es un tipo de dirección IPV6 de unidifusión global que es visible y accesible desde otras redes.

- **Interfaz local de enlace**: seleccione la interfaz local de enlace (si se selecciona Enlace local como Tipo de dirección IPv6) en la lista desplegable.
- **Nombre/Dirección IP del receptor**: ingrese la dirección IP o el nombre de servidor de donde se envían las trampas.
- **Puerto UDP**: ingrese el puerto UDP que se usa para notificaciones en el dispositivo receptor.
- **Tipo de notificación**: seleccione si se deben enviar mensajes trampa o de informe. Si se necesitan los dos, deben crearse dos receptores.
- **Tiempo de espera**: ingrese la cantidad de tiempo (segundos) que el dispositivo espera antes de volver a enviar las notificaciones de información/trampas. Tiempo de espera: Rango 1-300, predeterminado 15.
- **Reintentos**: ingrese la cantidad de veces que el dispositivo vuelve a enviar un pedido de informe. Reintentos: Rango 1-255, predeterminado 3.
- **Nombre de usuario**: seleccione, de la lista desplegable, el usuario a donde se envían las notificaciones SNMP. Para recibir notificaciones, este usuario debe estar definido en la página Usuario SNMP y su ID de motor debe ser remoto.
- **Nivel de seguridad**: seleccione cuánta autenticación se aplica al paquete.

  NOTA El nivel de seguridad de aquí depende del nombre de usuario seleccionado. Si el nombre de usuario se configuró como Sin autenticación, el nivel de seguridad será Sin autenticación únicamente. Sin embargo, si se ha asignado Autenticación y Privacidad a este nombre de usuario en la página Usuario, el nivel de seguridad en esta pantalla puede ser Sin autenticación, Solo autenticación o Autenticación y Privacidad.

  Las opciones son:

  - *Sin autenticación*: indica que el paquete no está autenticado ni cifrado.
  - *Autenticación*: indica que el paquete está autenticado, pero no cifrado.
  - *Privacidad*: indica que el paquete está autenticado y cifrado.
- **Filtro de notificaciones**: seleccione esta opción para habilitar el filtrado del tipo de notificaciones SNMP que se envían a la estación de administración. Los filtros se crean en la página Filtro de notificaciones.
- **Nombre de filtro**: seleccione el filtro SNMP que define la información que contienen las trampas (que se define en la página Filtro de notificaciones).

PASO 4 Haga clic en **Aplicar**. La configuración Recepción de notificaciones SNMP se escriben en el archivo Configuración en ejecución.

Filtros de notificaciones SNMP

En la página Filtro de notificaciones, es posible configurar los filtros de notificaciones de SNMP e ID de objetos que están marcados. Después de crear un filtro de notificaciones, es posible asociarlo a un receptor de notificaciones en la página Receptores de una notificación SNMPv1,2 y en la página Receptores de una notificación SNMPv3.

El filtro de notificaciones le permite activar el tipo de notificaciones de SNMP que se envían a la estación de administración según el OID de la notificación a enviarse.

Para definir un filtro de notificaciones:

PASO 1 Haga clic en **SNMP** > **Filtro de notificaciones**.

La página Filtro de notificaciones incluye información sobre las notificaciones para cada filtro. La tabla puede filtrar entradas de notificaciones por Nombre de filtro.

PASO 2 Haga clic en **Add**.

PASO 3 Ingrese los parámetros.

- **Nombre de filtro**: ingrese un nombre de 0 a 30 caracteres.
- **Subárbol de ID de objeto**: seleccione el nodo en el árbol de MIB que se incluye en el filtro SNMP seleccionado o que se excluye de este. Las opciones para seleccionar el objeto son las siguientes:
  - *Seleccionar de la lista*: le permite navegar el árbol de MIB. Presione la flecha *Up* (Arriba) para ir al nivel del nodo padre y nodo hermanos del nodo seleccionado; presione la flecha *Down* (abajo) para bajar al nivel de los descendientes del nodo seleccionado. Haga clic en los nodos de la vista para pasar de un nodo a su hermano. Use la barra de desplazamiento para poder ver los nodos hermanos.
  - Si se usa *ID de objeto*, el **identificador de objeto ingresado** se incluye en la vista, si la opción **Incluir en filtro** está seleccionada.

PASO 4 Seleccione o cancele la selección **Incluir en el filtro.** Si se selecciona, las MIB seleccionadas se incluirán en el filtro; de lo contrario, no se incluirán.

PASO 5 Haga clic en **Aplicar**. Se definen las vistas SNMP y se actualiza el archivo Configuración en ejecución.